NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002 Transmission Owner Control Centers (TOCCs) Field Test

Project 2021-03

Overview

On May 14, 2020, the NERC Board of Trustees (Board) adopted proposed Reliability Standard CIP-002-6. The proposed standard revised Criterion 2.12 to categorize non-high impact Bulk Electric System (BES) Cyber Systems associated with Control Centers performing the reliability tasks of a Transmission Operator (TOP) as medium impact, while moving a subset not meeting the Criterion to be categorized as low impact. This revision was intended to remove uncertainty surrounding the multiple interpretations of the language "used to perform the functional obligation of" in the current Standard and recognize the existence of certain Transmission Owner Control Centers (TOCCs) performing TOP reliability functions as medium impact based on an aggregate weighted value of their Transmission Lines. Further, the revision also recognized the existence of small, registered TOP entity Control Centers having minimal impact to the BES that should be categorized as low impact. The Project 2016-02 SAR was accepted by the Standards Committee on July 20, 2016, which includes the scope for addressing the TOCC obligations.

On June 12, 2020, NERC staff filed with the Federal Energy Regulatory Commission (FERC) a petition for approval of proposed CIP-002-6. On June 23, 2020, the proposed standard was filed with the applicable regulatory authorities in Canada.

At its February 4, 2021 meeting, the Board withdrew proposed Reliability Standard CIP-002-6. In addition, the Board issued a resolution stating "that NERC Staff, working with stakeholders, is directed to promptly conduct further study of the need to readdress the applicability of the CIP Reliability Standards to such Control Centers[1] to safeguard reliability, for the purpose of recommending further action to the Board." On February 5, 2021, NERC filed a notice of withdrawal for CIP-002-6 with FERC.

The 2021-03 CIP-002 TOCC Standard Drafting Team (SDT) was created to conduct further study and recommend next steps, in response to the following SAR language:

> *Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations – V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:*
>
> - *The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.*
> - *The definition of Control Center.*
> - *The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.*

As such, the SDT has designed a Field Test to obtain data from TOs and TOPs for the explicit purpose to validate that the proposed bright line Criterion 2.12 shown below is appropriate and does not expose the Bulk Electric System to vulnerabilities. The inclusion of TOPs in the Field Test is necessary since the functional registration of an entity is not expressly assigned. Further, the SDT recognizes the TOs' need for clarification on identifying whether they may own and operate a control room that could qualify as a *Control Center used to perform the reliability tasks of a Transmission Operator,* and is provided in Attachment A.

The expected outcome of the Field Test is to recommend the appropriate bright line criteria. This may mean that: (1) the current bright line Criterion 2.12 language (shown below) is retained, (2) the proposed bright line Criterion 2.12 language (shown below) remains justified with additional technical basis, or (3) a new bright line Criterion 2.12 is recommended based on the technical results obtained from the Field Test.

Current bright line Criterion 2.12 from CIP-002-5.1a:

> [Each BES Cyber System, not included in Section 1 above, associated with] Each Control Center or backup Control Center used to perform the functional obligations of a Transmission Operator, not included in High Impact Rating above [shall be Medium Impact].

Proposed bright line Criterion 2.12 from withdrawn CIP-002-6:

> [Each BES Cyber System, not included in Section 1 above, associated with] Each Control Center or backup Control Center, not included in the High Impact Rating, used to perform the reliability tasks of a Transmission Operator in real-time to monitor and control BES Transmission Lines with an "aggregated weighted value" exceeding 6000 according to the table below [shall be Medium Impact]. The "aggregated weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a Line	Weight Value per Line
less than 100 kV (not applicable)	(not applicable)
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

TOCC Field Test Preparation

Successful completion of the Field Test requires an adequate pool of participants whose aggregated weighted value as defined in the proposed Criterion 2.12 falls near 6000, both above and below. While assuring all BES Cyber Systems are appropriately categorized as medium impact is paramount, it is also important to assure compliance resources are expended commensurate to the reliability risk. Entities owning BES Transmission Lines with an "aggregated weighted value" exceeding 6000 and have a lower

inherent risk to the BES are encouraged to participate in the TOCC Field Test. The following guideline should be followed to determine if participating in the Field Test is appropriate.

- TOCC Entity formerly afforded discretionary enforcement designating a Control Center as low impact.
- TOCC Entity holding a contractual agreement with a second party who provides cover as the registered TOP, and owns/operates a "TO Dispatch Center" as defined in Attachment A.
- TOP Entity whose "aggregated weighted value" is 6000 or less and has no high impact BES Cyber System associated with its Control Center or Backup Control Center.
- TOP Entity whose "aggregated weighted value" is 6000 or greater and has no:
  - Identified Interconnection Reliability Operating Limit (IROL)
  - Remedial Action Scheme (RAS)
  - Substantial role in voltage or frequency control, such as:
    - Control of, or directly interconnected BES Generation above 1500 MW or BES reactive resource above 1000 MVAR.
    - Automatic Load Shedding of 300 MW or more

Transmission Owners and Transmission Operators who would like to participate in the TOCC Field Test are encouraged to contact Jordan Mallory. Each entity interested in participating in the TOCC Field Test must provide the following:

1. Provide NERC staff with the name, phone number, and email address of:
   a. The primary contact for the TOCC Field Test,
   b. The contact for the director/manager/supervisor over CIP Compliance,
   c. The contact for the CIP Senior Manager, if different from the above, and
   d. The primary compliance contact for its registered entity

Participating entities should have the capability to perform necessary steady state and dynamic simulations OR be willing to engage with a consultant (individually or jointly) to perform such studies. After the Field Test has been approved, the Reliability and Security Technical Committee can identify other Field Test participants. Information received from participating TOs and TOPs will be treated as confidential.

TOCC Field Test Compliance and Enforcement Discretion

The SDT will keep the participant and proposed participant list non-public and protect any information meeting the NERC Rules of Procedure (ROP) definition of Confidential Information as required by Section 1500 of the NERC ROP.

The name of a participant may be released to a participating entity's Regional Entity, at the request of the participant, as necessary to facilitate waivers of compliance that have been issued by CMEP staff.

The purpose of collecting information from participants is to support the SDT's assessment of impact to the BES rather than for compliance purposes. Nevertheless, entities must continue to comply with all applicable Reliability Standards, except as described in this section.

Per Section 6.1.2 of the Standard Processes Manual, the NERC Compliance Monitoring and Enforcement Program (CMEP) staff, at its discretion, may grant waivers of compliance to Field Test participants if participation in the Field Test renders them incapable of complying with the currently-enforceable Reliability Standard.

Participating TOPs, and TOs already complying with medium impact requirements, will continue to be responsible for compliance under the NERC Standards, including but not limited to, CIP-002-5.1a "Cyber Security – BES Cyber System Categorization" for the duration of the TOCC Field Test.

If TOs currently applying low impact requirements to a Control Center meeting Criterion 2.12 and were notified they need to become medium impact by October 1, 2023, participation in the Field Test will permit them to continue applying low impact requirements until conclusion of the Field Test, with a reasonable period of time permitted for them to become compliant with medium impact requirements if applicable once the revised standard language is developed.

TOCC Field Test Questionnaires and Reporting

During the TOCC Field Test, the TOCC SDT will issue participants a series of questionnaires with the ultimate intention of determining whether there is adequate technical justification to modify CIP-002 such that BES Cyber Assets at additional TOP and TOCCs can be classified as low impact without jeopardizing BES system reliability. The initial questionnaire, provided in Attachment B, is designed to obtain information about various company-specific attributes that will aid the TOCC SDT in developing additional questionnaires that consider BES system response to a variety of cyber-attacks levied against the individual Control Centers. These subsequent questionnaires will require that detailed analysis be performed to identify if a specific cyber event scenario will result in instability, uncontrolled separation, or Cascading that adversely impact the reliability of the BES. The analysis may require that steady-state, dynamic stability and/or transient stability studies be performed.

For the purpose of this field test, a cyber event scenario will be classified as an event during which a BES Cyber Asset is rendered unavailable, degraded or misused. The TOCC SDT will confer with (1) cyber security subject matter experts and (2) power flow analysis subject matter experts during scenario development to ensure that cyber events included in defined scenarios are realistic and will yield informative and actionable simulation results. The scenarios developed are intended to represent worst-case scenarios in order to demonstrate the worst-case impact to the BES. As such, scenarios will likely be beyond the N-1 and extreme events required under the TPL standards. Care will be taken to ensure that the selected scenarios are not redundant with any of the existing CIP-002 criteria that would elevate BES Cyber Assets to high impact.

A successful Field Test will allow the SDT to advance to the industry a revision to Criterion 2.12, with sufficient technical justification, within a new version of NERC Reliability Standard CIP-002. The SDT will

propose a bright line for IRC 2.12 based on data collected from field test participants such that there is a high level of confidence that a compromised BES Cyber Asset classified as low impact will not result in instability, uncontrolled separation, or Cascading that adversely impacts the reliability of the BES.

Implementation Schedule and Periodic Updates

Kick off the Field Test in January 2022. Periodic updates will be provided to the RSTC, as necessary, but no later than six months after the Field Test initiates.

DATE	ACTIVITIES	RETURN DATE
December 1, 2021	Confirm field test participants with input from RSTC	December 31, 2021
January 10, 2022	Send initial questionnaire	February 4, 2022
February 7, 2022	Analysis of responses to initial questionnaire	March 4, 2022
March 7, 2022	Send second questionnaire, if necessary*	April 1, 2022
April 4, 2022	Analysis of responses to second questionnaire	April 29, 2022
May 2, 2022	Prepare interim report on analysis	May 27, 2022
June 2022	Provide interim report or update on field test progress to RSTC	N/A
July 11, 2022	Send third questionnaire, if necessary*	August 5, 2022
August 8, 2022	Analysis of responses to third questionnaire	September 2, 2022
September 6, 2022	Send fourth questionnaire, if necessary*	September 30, 2022
October 3, 2022	Analysis of responses to fourth questionnaire	October 28, 2022
October 31, 2022	Prepare final report on analysis and findings	November 18, 2022
December 2022	Provide report on field test findings to RSTC	N/A
December 16, 2022	Post final report and results	N/A
January 2023	Start drafting revisions to CIP-002 based on field test	N/A

*The implementation schedule provides a timeline that includes four questionnaires, but the SDT may be able to complete its analysis and findings with fewer than four, depending on the data received. In that case, the schedule would be revised and the timeline shortened.

Early Withdrawal from the TOCC Field Test

Any participating TOP or TO may withdraw from the TOCC Field Test upon notification to Jordan Mallory. This will effectively terminate the waiver of compliance for participating TOs.

Attachment A

TOCC Configuration and Relationship with Associated TOP

Per the ROP, every BES transmission asset is required to have a registered TO and registered TOP. In many cases the registered TO has acquired a registered TOP for their BES assets via a contract or agreement. There are several different Operating Protocols and system configurations between the TOP and TO supervisory control and data acquisition (SCADA) systems and the BES.

A Control Center is currently defined as "One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities[1] at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations." (A Facility is defined as a set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)

Further, a TOP is defined as "The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission Facilities."

The purpose of this Attachment is to define a Technical Rationale for determining if the TO's cyber system and associated Operating Protocols are used to perform the functional obligations of the Transmission Operator under Criterion 2.12.

For the evaluation of evaluation of Attachment A examples, the TO Dispatch Center has the following characteristics:

- TO organization is not affiliated with the TOP organization
- TO organization has a contract or agreement with the TOP organization to be their NERC registered TOP for the TO owned BES assets.
- TO organization is not required to have NERC-certified System Operators
- TO Dispatch Center location contains Cyber Assets that are connected (hardwired, routable or serial) to Cyber assets located at two or more BES locations (substations or plant switchyards).

The term "TO dispatcher" used in the Attachment A examples is a generic term for personnel located at TO Dispatch Center that have access to Cyber Assets that are connected (hardwired, routable or serial) to Cyber assets located at two or more BES locations (substations or plant switchyards). These personnel could be, but not limited to the following job titles

- Transmission Dispatcher
- Distribution Dispatcher
- Power dispatchers

[1] (A Facility is defined as set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)

- Dispatcher
- Crew / work dispatcher
- Switching Supervisor

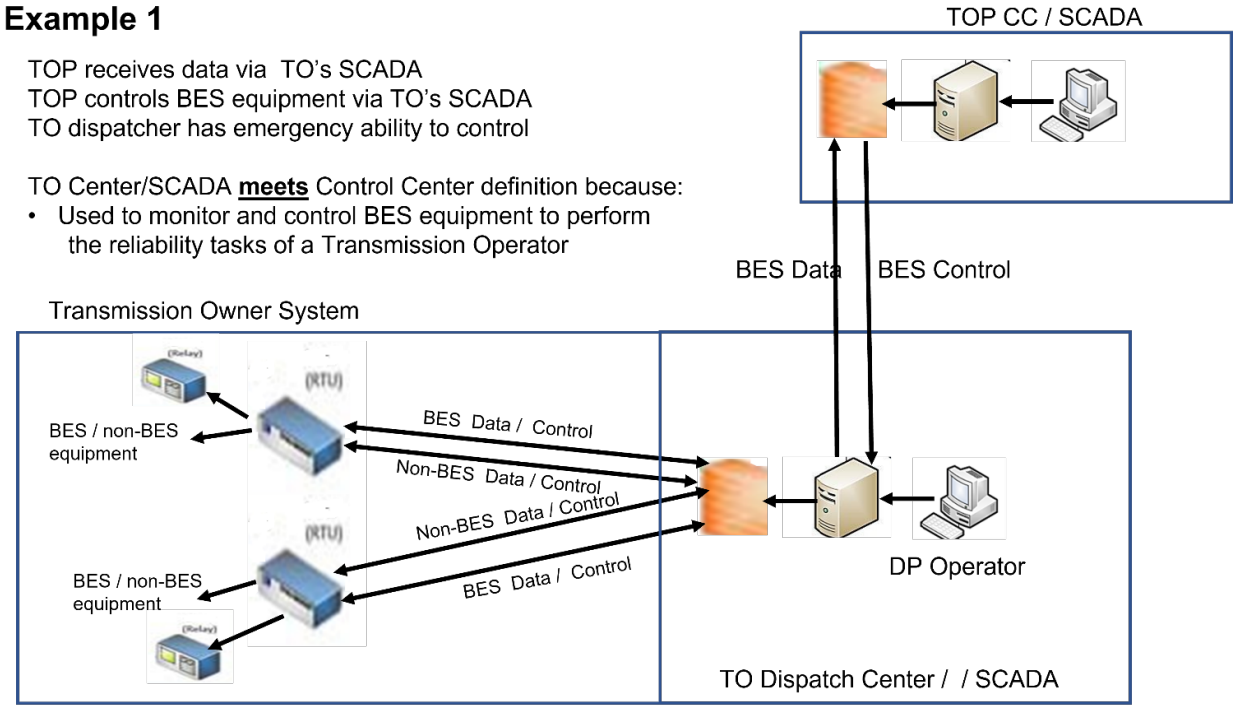
Based on these characteristics, the TO Dispatch Center should have the TOP – TO functional relationship per the Attachment A examples. The evaluation should be used to determine if the TO Dispatch Center meets the definition of a Control Center used to perform the functional obligations of the Transmission Operator under Criterion 2.12.

Example 1:

TOP receives data via TO's SCADA
TOP controls BES equipment via TO's SCADA
TO dispatcher has emergency ability to control

TO Center/SCADA **meets** Control Center definition because:

- Used to monitor and control BES equipment to perform the reliability tasks of a TOP

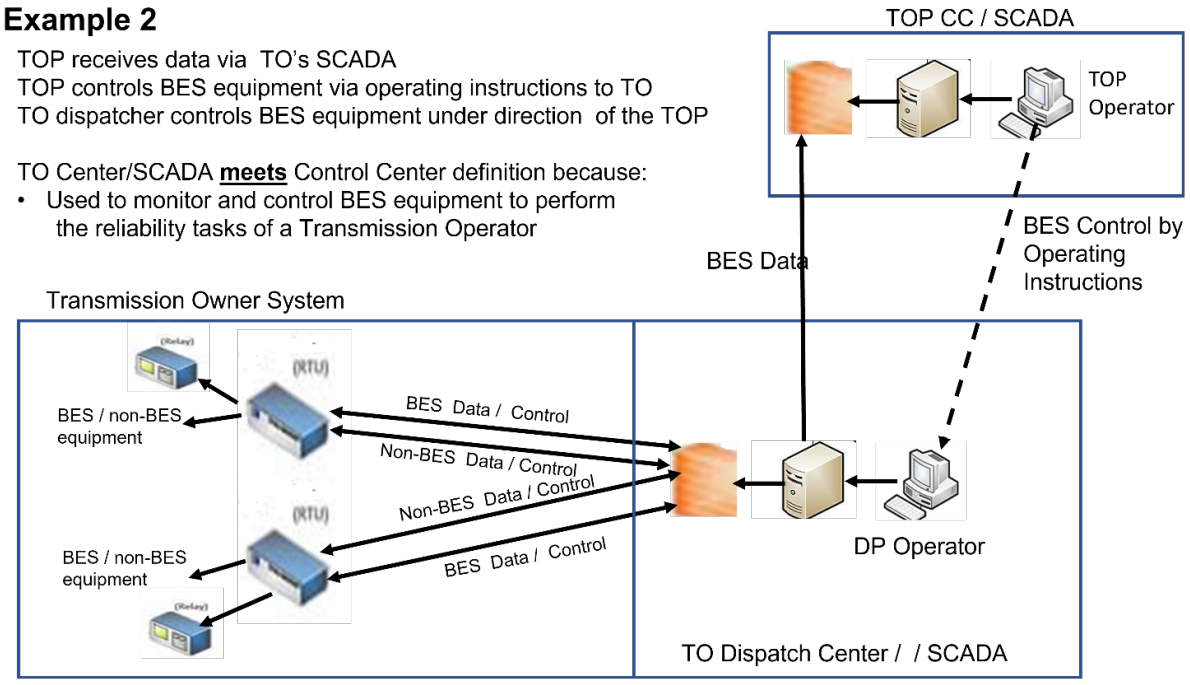


Example 2:

TOP receives data via TO's SCADA
TOP controls BES equipment via operating instructions to TO
TO dispatcher controls BES equipment under direction of the TOP

TO Center/SCADA **meets** Control Center definition because:

- Used to monitor and control BES equipment to perform the reliability tasks of a TOP

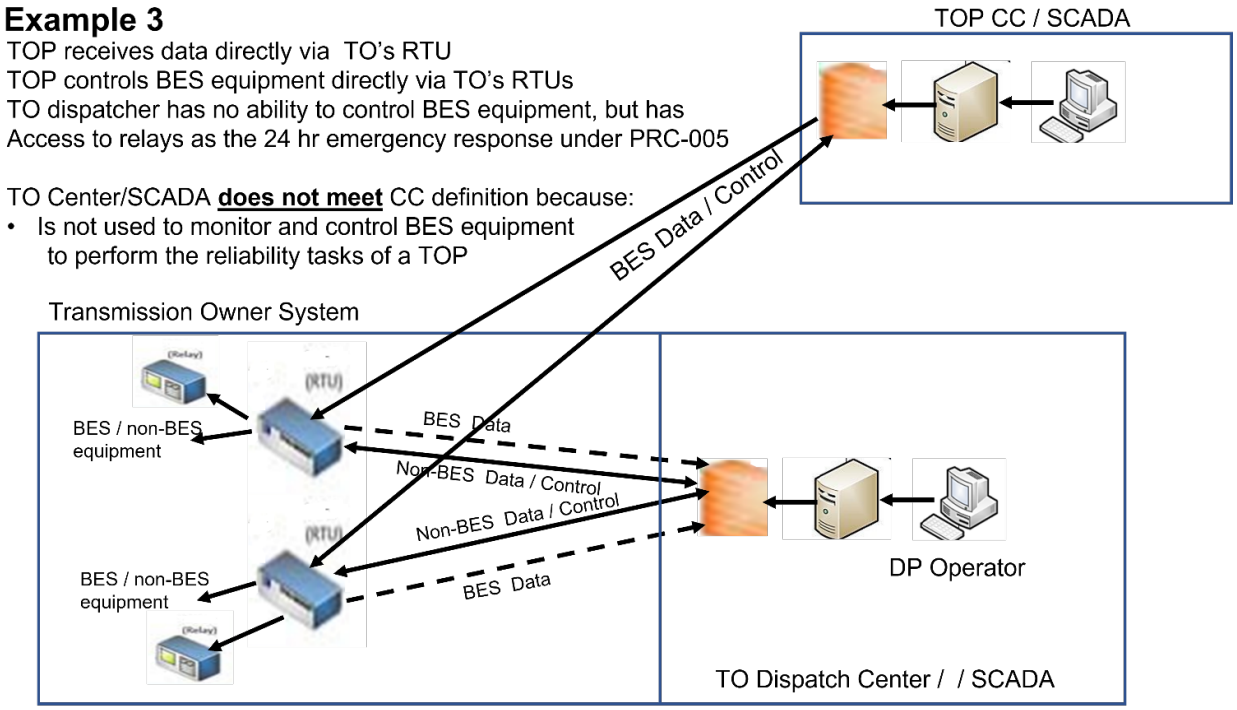


Example 3:

TOP receives data directly via TO's RTU
TOP controls BES equipment directly via TO's RTUs
TO dispatcher has no ability to control BES equipment, but has access to relays as the 24-hr emergency response center under PRC-005

TO Center/SCADA **does not meet** Control Center definition because:

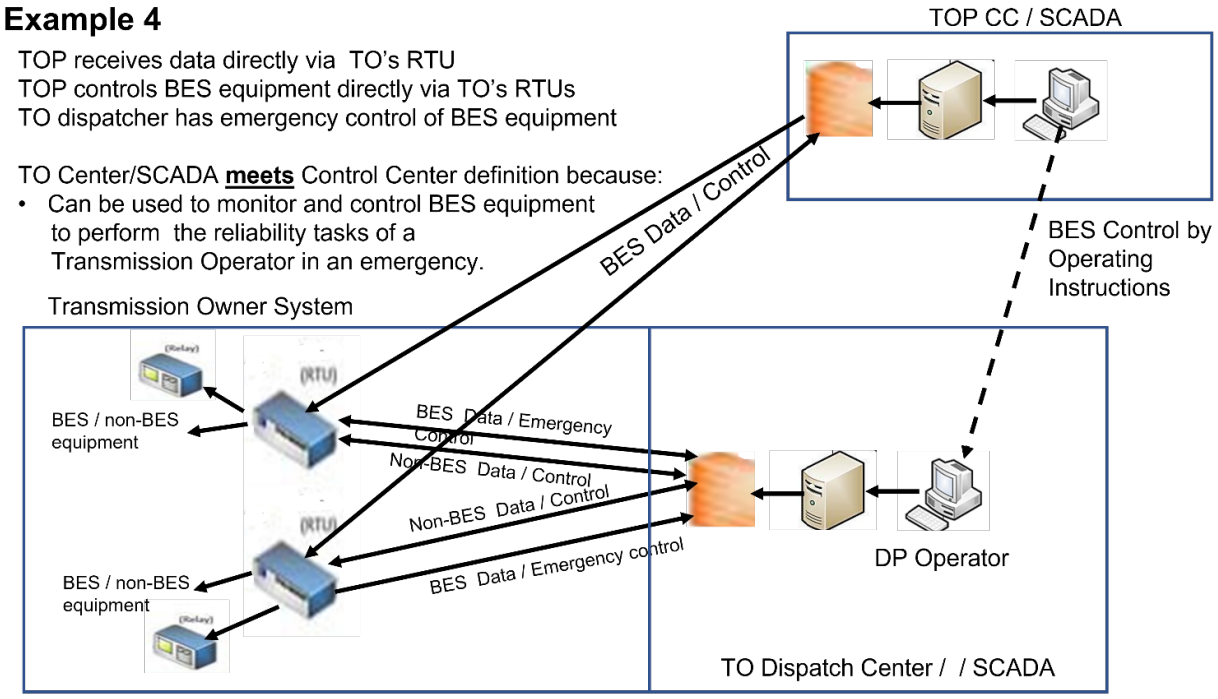
- Is not used to monitor and control BES equipment to perform the reliability tasks of a TOP
- Transmission Operator monitors and controls BES equipment directly via TO's RTU's



Example 4:
TOP receives data directly via TO's RTU
TOP controls BES equipment directly via TO's RTUs
TO dispatcher has emergency control of BES equipment

TO Center/SCADA **meets** Control Center definition because:

- Can be used to monitor and control BES equipment to perform the reliability tasks of a TOP in an emergency.



Attachment B

TOCC Field Test Entry Questionnaire

Please complete the following questions to help us better understand your system.

As a NERC Control Center is applicable to specific configurations, an entity may have no CC, may have one, or could possibly have multiple CC locations. To the extent that an entity has multiple CC locations that control different Facilities, the entity should complete a separate questionnaire for each CC location or clearly delineate between each CC location on the questionnaire as the individual outcomes of the application of Criterion 2.12 could be different.

1. NERC Registration (e.g., RC/BA/TO/TOP/DP/etc.): _____
2. Do you have a site that is staffed by operating personnel, from which you can remotely operate Facilities at two or more locations?

   ☐ Yes ☐ No
3. Based on the impact to the BES of a cyber event in your footprint, do you believe the site(s) referenced in Question 2 should be low impact, medium impact or high impact? Why?

   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
4. What was the peak load served by your system for the period 1/1/2020 – 10/1/2021, which could be interrupted remotely from the site referenced in Question 2?

   _____
5. What is the total capacity of conventional BES generation Facilities connected to your system, which could be interrupted remotely from the site referenced in Question 2?

   _____
6. What is the total capacity of intermittent (e.g., wind, solar) BES generation Facilities connected to your system, which could be interrupted remotely from the site referenced in Question 2?

   _____

Answer all of the following questions for each location for which the response to Question 2 was "yes".

7. Is there external connectivity to any BES Cyber Asset(s) housed at the site(s) referenced in Question 2? If so, please provide access means for each connection (e.g., dial-up, internet, VPN).

   ☐ Yes ☐ No Access means: _____

8. Do third parties have direct communications access for change management or other managed service provider purposes for the site(s) referenced in Question 2?

   ☐ Yes ☐ No

9. How does your organization conduct its change management activities?

   _____
   _____
   _____
   _____
   _____
   _____
   _____

10. Does your company have supply chain or other internal control protocols in place for the purchase and maintenance of computer systems that are housed at the site(s) referenced in Question 2?

    ☐ Yes ☐ No

For the purpose of responding to the remainder of this questionnaire, a Transmission Line is defined by the protection system(s) that would be used to isolate a fault on a line. Typically, all sources of fault current for a line fault will be interrupted by breakers. Transmission Lines can be single-ended, two-ended, or three-ended. After identifying your Transmission Lines, the NERC definition of BES should be applied to each line to determine if it is a BES Transmission Line. Single-ended, or radial lines, are not typically considered to be BES assets.

Only include Transmission Lines where you have the ability to remotely operate a device to interrupt network flow (through-flow across the line). If you have remote control of multiple devices on a single Transmission Line as defined above, you should only count that line one time in your response. You should still count the line even if another entity controls the remote end of the line.

11. Provide the following information:

	Total number of BES Transmission Lines where you have the ability to remotely operate a device to interrupt network flow on the line.	Total number of BES Transmission Lines where you have the ability to remotely operate a device to interrupt network flow on the line AND another entity has the ability to remotely operate a device to interrupt flow on the same element or a series element.
100 kV to 199 kV		
200 kV to 299 kV		
300 kV to 499 kV		
500 kV and above		