NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

This is a Compliance Monitoring and Enforcement Program (CMEP) Practice Guide. It is developed exclusively by the ERO Enterprise under its obligations for independence and objectivity. This CMEP Practice Guide is intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities. This CMEP Practice Guide is posted publicly solely to provide transparency.

ERO Enterprise CMEP Practice Guide:

Determinations of "Redundant" and "Diversely Routed" for TOP-001-4 R20, R21, R23, and R24 and IRO-002-5 R2 and R3

June 2018

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]

Purpose

The purpose of this CMEP Practice Guide is to address how ERO Enterprise CMEP staff (CMEP staff) will assess a registered entity's "redundant and diversely routed data exchange infrastructure" and "redundant functionality" with TOP-001-4 R20, R21, R23, and R24 and IRO-002-5 R2 and R3. The principles below provide guidance when evaluating "redundant and diversely routed data exchange infrastructure" and "redundant functionality".[4]

Consideration of the Terms "Redundant and Diversely Routed Data Exchange Infrastructure" and "Redundant Functionality"

While specific facts and circumstances ultimately shape compliance monitoring, CMEP staff will consider and apply the principles identified below. This is written in terms of Transmission Operators (TOP-001-4 R20 and R21) but when auditing Balancing Authorities or Reliability Coordinators the specific functions of the applicable registered entity will be considered (TOP-001-4 R23 and R24, and IRO-002-5 R2 and R3).

Data Exchange Capabilities with Other Entities

Redundancy within a primary Control Center is needed for a registered entity's data exchange capability with other entities (RCs, BAs, and entities it has identified it needs data from in order to perform its Real-time monitoring and Real-time Assessments).[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: http://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.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] Per FERC's Order that reliance on backup facilities per EOP-008 is not sufficient.
Order No. 817, Transmission Operations Reliability Standards and Interconnection Reliability Operations and Coordination Reliability Standards, 153 FERC ¶ 61,178 (2015)

[5] Varies slightly for BAs and RCs. As mentioned before, this is written in terms of TOPs. For BAs, the other entities are RCs, TOPs, and entities it has identified it needs data from in order to perform its Real-time monitoring and analysis functions. For RCs, the other entities are BAs, TOPs, and entities it has deemed necessary for performing its Real-time monitoring and Real-time Assessments.

In order to determine the entities with which data exchange infrastructure must be established, the registered entity needs to determine: (i) what data is necessary to perform its Real-time monitoring and Real-time Assessments; and (ii) the source of the data. Therefore, CMEP staff should understand the following:

- What data has the registered entity determined it needs for Real-time monitoring and Real-time Assessments? Where does that data originate?
  - The data specifications from TOP-003-3 may be submitted by the registered entity to verify what data is coming from other entities in order to perform Real-time Assessments.
- What data exchange capabilities does the TOP use to exchange data with the Reliability Coordinator, Balancing Authority, and other entities from which the TOP needs data?

Knowing this, CMEP staff can proceed to understand how a registered entity ensures its data exchange infrastructure is redundant and diversely routed. If there is data that is not covered by this requirement but is used for Real-time monitoring or Real-time Assessments (such as internal data from within the registered entity itself, or data that is needed by another entity), CMEP staff should obtain an understanding of whether redundancy and diverse routing were considered and update the registered entity's risk profile through its Inherent Risk Assessment or Compliance Oversight Plan if necessary.

In order to understand an entity's data exchange capabilities, CMEP staff should:

- Verify the capability of the data exchange infrastructure's physical components to include sending data to and/or receiving data from other entities as needed.
  - Physical components are the switches, routers, servers, power supplies, network cabling, etc., and communication paths between these components.
  - Registered entities are not exempt from these requirements even if their RCs and/or BAs do not currently require data.
  - For periods of planned or unplanned outages of individual data exchange components, there is not an expectation for additional redundant data exchange infrastructure components.
  - Testing the infrastructure per TOP-001-4 R21 or R24 should identify the outage of the physical components. Any outage identified should initiate action within two hours per these requirements.
- Verify that redundant and diversely routed infrastructure is achieved at the primary Control Center, including its associated data center, independent of the backup Control Center.

Primary Control Centers

The requirements apply to data exchange infrastructure within the primary Control Center[6], including its associated data center. If registered entities operate one or more Control Centers that receive data for

[6] From the NERC Glossary of Terms, Control Center is 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 at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

normal Real-time operations (i.e., operating in a "hot – hot" configuration), CMEP staff should understand the registered entity's approach and system design to achieve the required redundancy and diverse routing. CMEP staff should use risk-based principles to determine whether both or either Control Center will be monitored for this requirement.

As noted above, the NERC Glossary definition of Control Center includes the associated data center(s). When verifying redundant and diverse routing for data exchange infrastructure, CMEP staff will also review, where applicable the infrastructure that connects the primary Control Center to its associated data center. The requirements necessitate redundancy and diverse routing between the primary Control Center and its associated data center the same as if they had been located in the same physical facility. Additional redundant functionality outside of the primary Control Centers may be useful information to inform the risk profile of the registered entity.

Avoiding Single Points of Failure

Redundant and diversely routed data exchange capabilities preclude single points of failure in primary Control Center data exchange infrastructure from halting the flow of Real-time data. The reliability objective of redundancy is to provide for continued data exchange functionality during component failure, outages, maintenance, or testing of data exchange infrastructure.[7] In order to understand whether the risk of single points of failure within a primary Control Center is mitigated, CMEP staff should:

- Determine how the registered entity understands, designed for, and constructed the data exchange infrastructure within their primary Control Center and its data center(s) to address single points of failure. The requirements are designed to provide entities with flexibility in designing an architecture within the constraints of a registered entity's facilities and systems.
- Ensure that redundant components are not routed through shared network infrastructure (i.e., switches, routers, and firewalls) in order to provide continued data exchange functionality during component outages.
    - Unpowered components, such as connection panels, do not necessarily require redundancy if they are not reliant on shared elements, such as power supplies, to operate.

While the Reliability Standard does not directly contemplate specific physical criteria or distances, CMEP staff may address whether adequate diversity in routing has been achieved using professional judgment and an understanding of the entity's overall strategy to meet the objective of the requirements. Monitoring should focus on possible component failure or outages rather than large impact physical events, which could trigger the entity's plans for loss of Control Center Functionality under EOP-008.

[7] TOP-001-4, Supplemental Material, Rationale for Requirements R19 and R20