NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-2

October 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

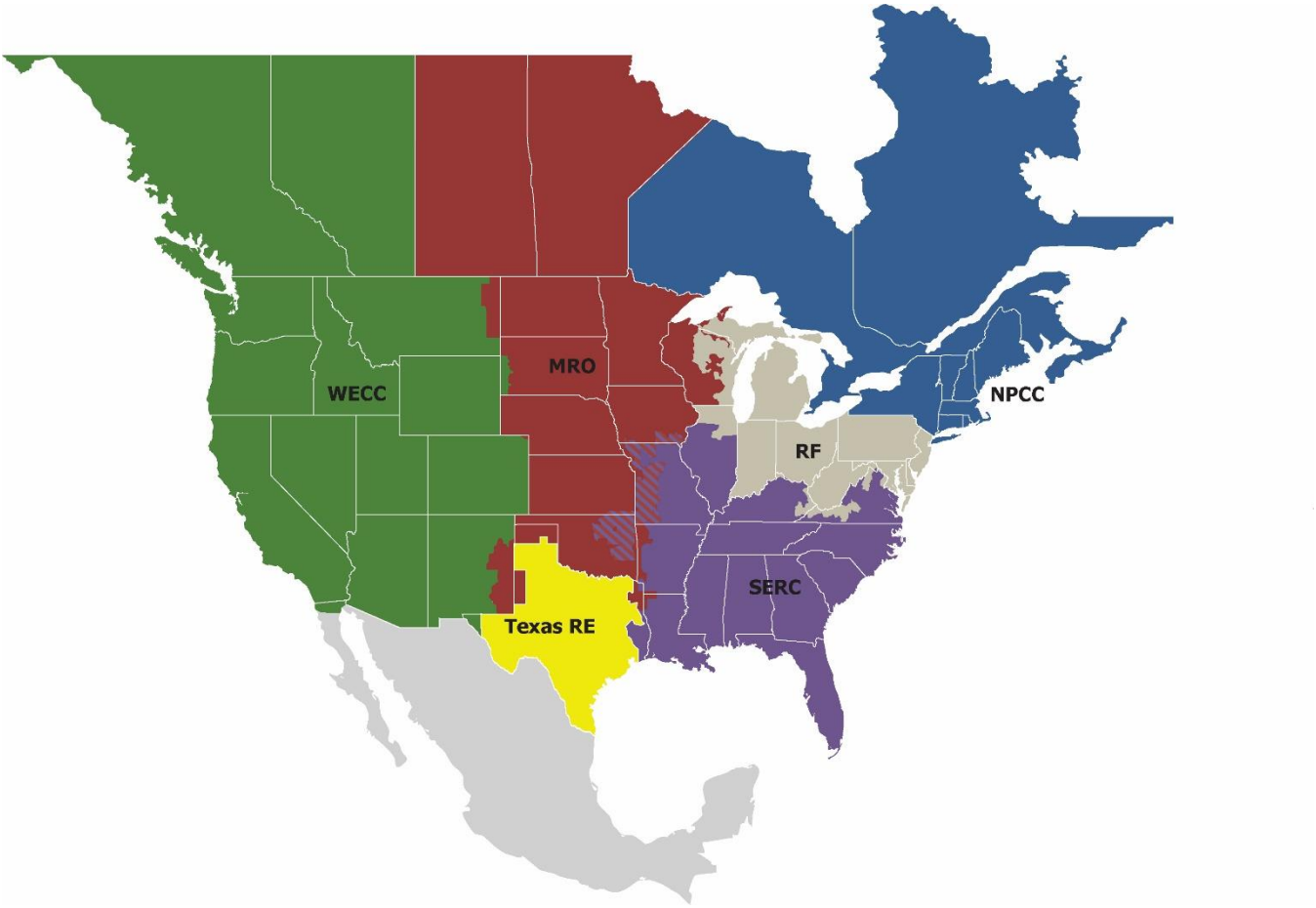
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the standard drafting team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-012 is not a Reliability Standard and should not be considered mandatory and enforceable.

CIP-012-1

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive Bulk Electric System (BES) data communicated between BES Control Centers in a manner that is appropriately tailored to address the risks posed to the BES by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive BES data and communication links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, and low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate for securing the data. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection–addressed in CIP-006 Requirement R1 Part 1.10 does not apply.

CIP-012-2

On January 23, 2020, the Federal Energy Regulatory Commission (FERC) issued Order No. 866 approving CIP-012-1 and directing NERC to develop modifications to CIP-012-1 to require Responsible Entities to develop one or more plan(s) to implement protections for the *availability* of communication links and data communicated between the BES Control Centers. In response to the directive in Order No. 866, the Project 2020-04 SDT refined the subparts of R1, including a Part requiring entities to identify methods used to mitigate the risk of the loss of communication links transmitting Real-time Assessment and Real-time monitoring data.

In Order No. 866, FERC also stated that "maintaining the availability of communication networks and data should include provisions for incident recovery and continuity of operations in a Responsible Entity's compliance plan." FERC recognized that the redundancy of communication links cannot always be guaranteed and acknowledged there should be plans for both recovery of compromised communication links and use of backup communication capability[2]. The SDT recognized that Responsible Entities may already have plans to address these contingencies in

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.
[2] See Order No. 866 at PP 35-36.

their existing recovery and/or incident response plan(s). These may be referenced as part of their CIP-012 plan to meet Requirement R1.3, avoiding duplication of effort.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both to mitigate the associated risks, consistent with the capabilities of the Responsible Entity's operational environment.

CIP-012 Exemption (4.2.3) for certain Control Centers

In the process of drafting CIP-012, the SDT became aware of certain generating plant or Transmission substation situations where such field assets could be dual-classified as Control Centers based on the current Control Center definition. Communication from these assets to their BA or TOP Control Centers, however, is not included in the intended scope of CIP-012. This is because the communications do not differ from those of any other generating plant or substation. The SDT wrote an exemption (Section 4.2.3 within CIP-012) for this particular scenario which is described in further detail below.

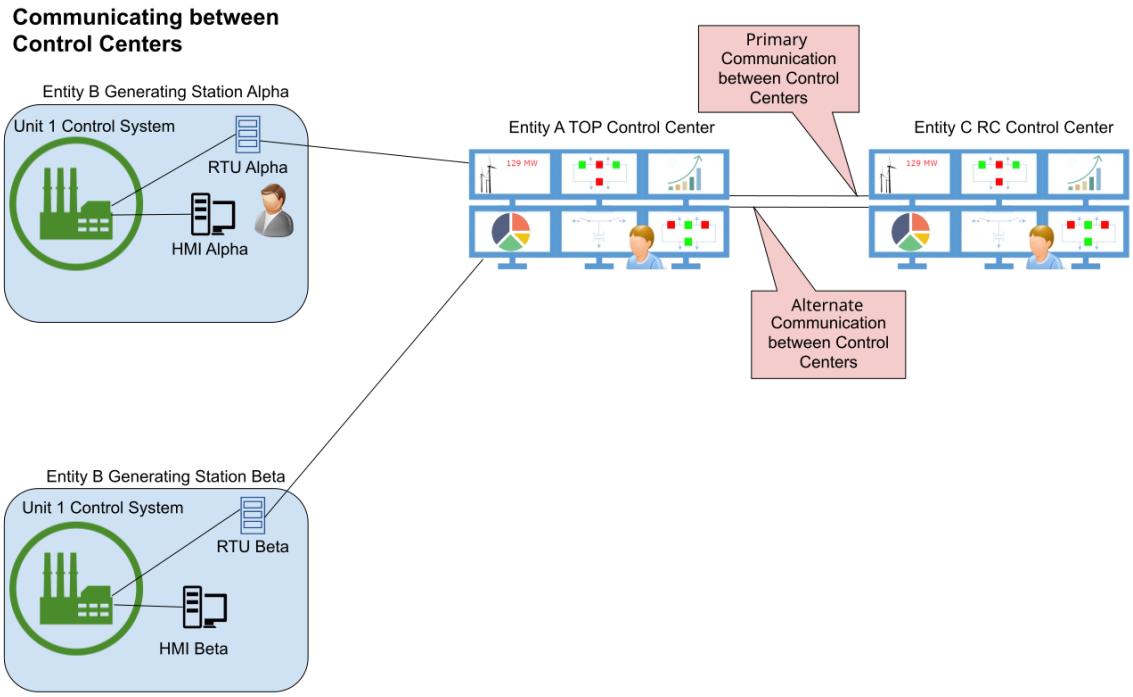


Figure 1

Figure 1 presents a typical scenario with two Control Centers communicating – in this instance Entity C's RC Control Center and Entity A's TOP Control Center. The communication between them is the intended scope of CIP-012's requirements if they meet the types of data inclusions and exclusions within the standard. The TOP Control Center is communicating with an RTU at two of Entity B's generating plants (Stations Alpha and Beta). Those RTU's are gathering information from each generating unit's control system. Each generating unit at each plant has an HMI (Human/Machine Interface; an operator workstation) that the local personnel use to operate their respective units. Entity B decides that the generating unit at Station Beta, a small peaking facility, will only have an operator on site during the day. The operator at Station Alpha should be able to remotely start the unit at Station Beta if necessary.

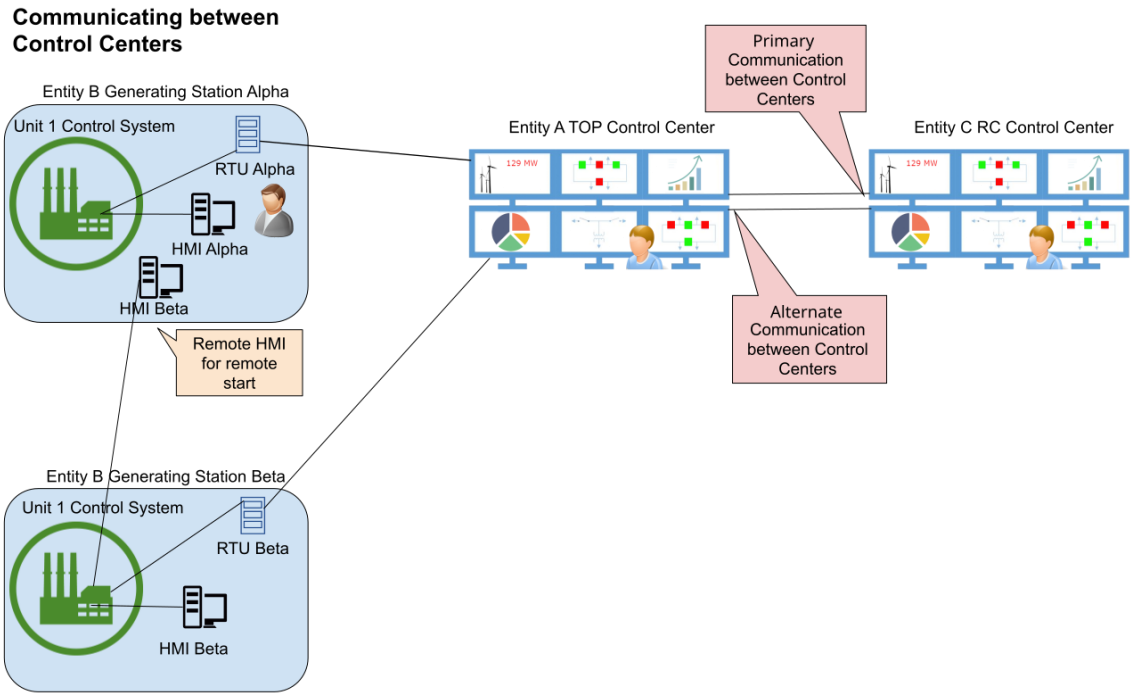


Figure 2

In Figure 2, Entity B installs a dedicated communications circuit from the control system on Station Beta's control system and puts a dedicated HMI at Station Alpha for operator use. Station Alpha is now "one or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks of . . . a Generator Operator for generation Facilities at two or more locations" because stations Alpha and Beta are two different plant locations. Station Alpha can now be dual classified not only as a generation resource but also as a Control Center.

The communications to the TOP and RC Control Centers in Figure 1 have not changed. No new cyber systems are in place that can impact multiple units. In addition, no cyber systems have been added performing Control Center functions. The only change is that an HMI for Station Beta has been moved within close physical proximity to an HMI for Station Alpha.

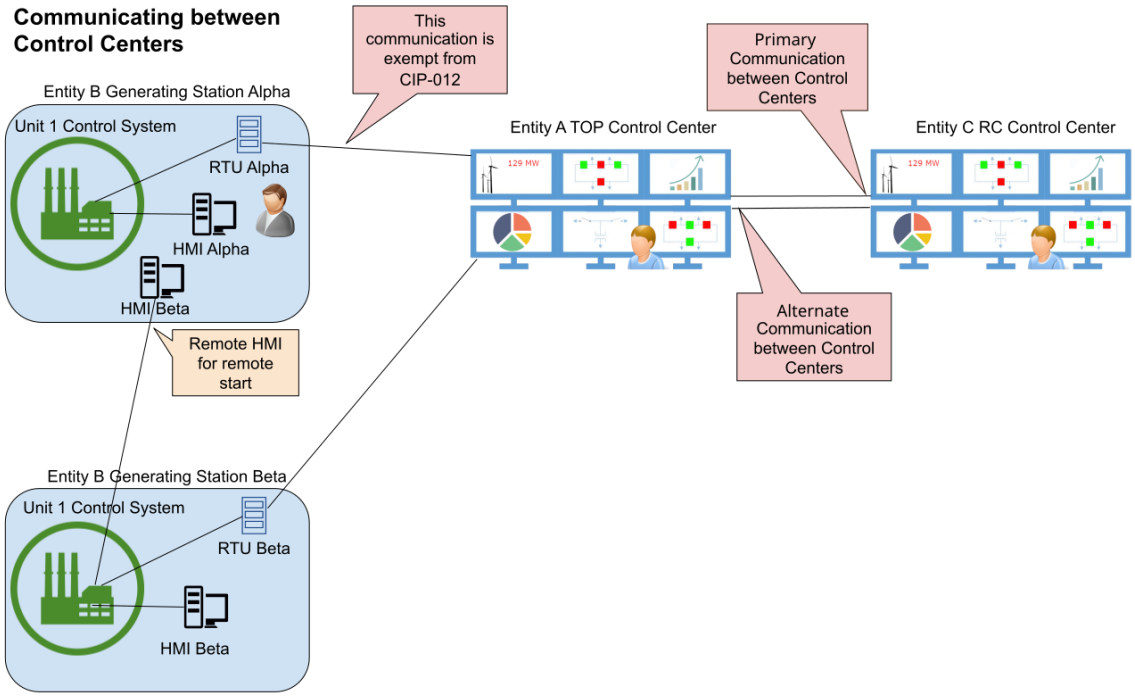


Figure 3

Although nothing has changed between them, this proximity (without the exemption preventing it), would make the communication noted in Figure 3 between Station Alpha and Entity A's TOP Control Center subject to CIP-012. Two HMIs have been moved into the same room and a new NERC CIP Standard applies to two entities. Because of exemption 4.2.3, the communication is out of scope of CIP-012.

This is an anomaly of the current Control Center definition of a facility, room, or building from which certain functions can be performed without regard to how they are done or what systems they are using. This is a generation specific example, but the potential situation exists where there are substations with an HMI or protective relay that "operating personnel" within the substation could use to impact an adjacent substation. It is also clear that in the criteria for TOs and GOPs, the "two or more locations" is not a precise enough filter for defining what a Control Center truly is. The SDT's attempts to address this issue by clarifying the definition of Control Center pointed out larger issues that are not within the SDT's SAR to address. Accordingly, the SDT is handling the issue through the 4.2.3 exemption within the CIP-012 standard which reads:

> 4.2.3. A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.

This exemption is to exclude from CIP-012 the normal RTU-style communication from a field asset providing that field asset's status. Throughout this scenario or others like it, that communication has not changed and is still the same data pertaining only to the single location. The SDT recognizes that this communication is not the intent of the Standard for protecting communications between Control Centers and this type of equipment may be using older legacy communication technology and protocols.

The 4.2.3 exemption covers generation resources or Transmission station or substation locations that host operating personnel and can control BES Facilities at more than one location, possibly making them co-located Control Centers. The communication is exempt from CIP-012 if each location is communicating the Real-time Assessment or Real-time monitoring data with another Control Center pertaining only to its own location.

The above diagrams were generation specific. The following diagram is a more generic example:

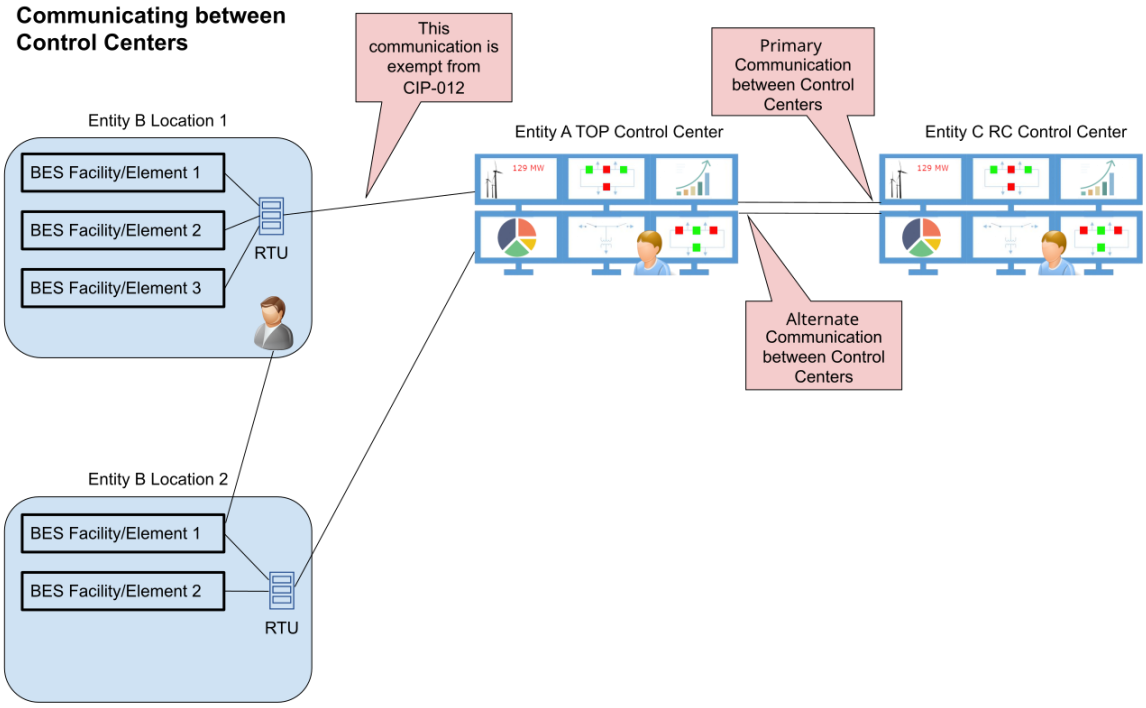


Figure 4

In Figure 4, each location only communicates its own Real-time Assessment or Real-time monitoring data pertaining to that single location, not Real-time Assessment or Real-time Monitoring data from any other location. The communication from Entity B location one (1) to Entity A would be exempt from CIP-012.

If Location 2 communicates its data through Location 1 and Location 1 was both controlling and aggregating data from multiple locations to Entity A's TOP Control Center, the communication between Location 1 and Entity A's TOP Control Center would not be exempt from CIP-012.

Requirement R1

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure, unauthorized modification, and loss of availability of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** Identification of method(s) used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;
- **1.2.** Identification of method(s) used to mitigate the risk(s) posed by loss of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;
- **1.3.** Identification of method(s) used to recover communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers;
- **1.4.** Identification of where the Responsible Entity implemented method(s) as required in Parts 1.1 and 1.2; and
- **1.5.** If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for implementing method(s) as required in Parts 1.1 and 1.2.

General Considerations for Requirement R1

Requirement R1 focuses on implementing a documented plan to protect information that is critical to the Real-time operations of the BES while in transit between applicable Control Centers. The SDT does not intend for the listed order of the requirement parts to convey any sequence or significance. The SDT also chose to revise the subparts of R1 based on industry feedback to require the identification of methods or measures to help entities quantify what was needed to satisfy the requirements.

Part 1.1 requires the Responsible Entity to identify within the CIP-012 plan the security protections of this data. This requirement focuses on Real-time Assessment and Real-time monitoring data while it is in transit between applicable Control Centers. Security protections include physical protection of components and equipment as well logical protection of the data in transit.

Part 1.2 requires the identification of methods within the CIP-012 plan to mitigate the risks posed by a loss of data transmission capability. A loss of data transmission capability can occur as the result of many scenarios. These may include misconfiguration of equipment, a physical break of transmission medium, or cyber-attack. As a CIP Standard, the focus of CIP-012 remains cyber protections around maintaining availability. Circuit redundancy, alternate systems of data transmission, and cyber protections for the circuit(s) are a few potential methods of maintaining availability of data circuits.

Part 1.3 addresses the need to identify methods to recover communication links. An important element of data communications is the availability of the communication links themselves. Communication links are the medium by which the data is transmitted between Control Centers (e.g. fiber, copper lines, satellite, etc.). Being able to recover

them from a failure, regardless of cause, is important to the overall movement of the data. This can be handled directly within the CIP-012 plan, or the CIP-012 plan may point to other applicable plans that accomplish the objective of this requirement.

Part 1.4 requires the identification of where protections are applied. Identifying where these protections are implemented will achieve appropriate coverage of protections. This can be accomplished with a document describing the locations of the components, diagrams indicating the locations or a combination of both, within the plan.

Part 1.5 addresses requirements for each side of the data transfer when Control Centers are owned or managed by different Responsible Entities. Having a clear understanding of where each side of a link each entity's responsibilities begin and end facilitates timely restoration when there is a problem with the transmission of the data.

Again, the SDT does not intend for the listed order of the requirement subparts to convey any sequence or significance.

Overview of Confidentiality, Integrity and Availability

The SDT drafted CIP-012 to address the confidentiality, integrity and availability of Real-time Assessment and Real-time monitoring data. This is accomplished by drafting the requirement to mitigate the risks posed by unauthorized disclosure (confidentiality), unauthorized modification (integrity) and transmission of information (availability). For this Standard, the SDT relied on the definitions of confidentiality, integrity, and availability as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[3]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[4]
- Based on the NIST definition[5], Availability is defined by the SDT as, "Providing timely and reliable access to information."

The CIP-012 Requirement to preserve the availability of the data is included to mitigate the risks posed by loss of data flow (availability) between applicable Control Centers. The SDT acknowledges that the availability and use of Real-time Assessment and Real-time monitoring data is required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012 to address the data while in motion between applicable Control Centers. The SDT maintains that this data, while at rest, resides within BES Cyber Systems and is explicitly protected by other CIP Standards. The use of this data is an Operations and Planning concern and is explicitly covered in the O&P Standards.

When Real-time Assessment or Real-time monitoring data is lost, an entity does not have the data needed for secure operation of the BES. Mitigating the risk posed by loss of Real-time Assessment and Real-time monitoring data may be achieved in a number of ways. These include the use of redundant circuits traversing discrete paths, or acquiring the same data points from multiple Control Centers, among other options.

Alignment with IRO and TOP Standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references

[3] NIST Special Publication 800-53A, Revision 4, page B-3
[4] NIST Special Publication 800-53A, Revision 4, page B-6
[5] NIST SP 800-59 under "Availability" from 44 U.S.C., Sec. 3542 (b)(1)(C)

to drive the identification of sensitive BES data and chose to base the CIP-012 requirements on the Real-time data specification elements in these standards. This approach provides consistent scoping of identified data and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP. Data requiring protection in CIP-012 consists of a subset of data that is identified by the RC, BA, and TOP in the TOP-003 and IRO-010 data specification standards, limited to Real-time Assessment data and Real-time monitoring data. CIP-012 excludes other data typically transferred between Control Centers such as Operational Planning Analysis data, weather data, market data, and other data that is not used by the RC, BA, and TOP to perform Real-time reliability assessments and analysis identified in TOP-003 and IRO-010. The SDT determined that Operational Planning Analysis data, if rendered unavailable, degraded, or misused, would not adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise as detailed in CIP-002-5.1a. The SDT notes that there may be special instances during which Real-time Assessment or Real-time monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

If Responsible Entities incorporate CIP-012 protections that introduce new data exchange infrastructure into the primary Control Center, they must ensure continued compliance with the provisions of TOP-001 and IRO-002, which require redundant and diversely routed data exchange infrastructure implementation and testing.

Identification of Where Protections are Applied by the Responsible Entity

The SDT noted the need for a Responsible Entity to identify where it will apply protections for applicable data. The SDT did not specify the location where CIP-012 security and availability protections must be applied. This allows latitude for Responsible Entities to implement the security and availability controls in a manner best fitting their individual circumstances. This latitude ensures entities can still take advantage of measures, such as deep packet inspection implemented at or near the Electronic Access Point (EAP) when Electronic Security Perimeters (ESPs) are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

The SDT also recognizes that CIP-012 protections may be applied to a Cyber Asset that is not an identified BES Cyber Asset (BCA), Protected Cyber Asset (PCA), or Electronic Access Control or Monitoring System (EACMS). The identification of the Cyber Asset at the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under the full complement of the Cyber Security Standards.

The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link. The SDT intends for a Responsible Entity to identify only where it applied security and availability protection. The Responsible Entity should coordinate with a neighboring entity in instances where the neighboring entity has applied protections at the neighboring entity's facility that affect the Responsible Entity's data flows to ensure appropriate protections are in place.

A Responsible Entity may decide to take responsibility for both ends of a communication link. For example, it may place a router in a neighboring entity's data center. In a scenario where a Responsible Entity has taken responsibility for applying protections on both ends of the communication link, the Responsible Entity should identify where it applied protections at both ends of the link. The SDT intends for there to be alignment between the identification of where protections are applied in CIP-012 Requirement R1, Part 1.4 and the identification of Responsible Entity responsibilities in CIP-012 Requirement R1, Part 1.5.

Control Center Ownership

The CIP-012 Standard Requirement addresses protection for Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers owned by a single Responsible Entity. It also covers the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection

between a single Responsible Entity's Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirement does not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure the security objective is met. An example noted in FERC Order No. 822 Paragraph 59 is, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, Figure 5 shows several in-scope data transmissions between Control Centers that a Responsible Entity should consider. The reference model example does not include all possible scenarios. The solid green lines are in-scope communications and the dashed red lines are out-of-scope communications.

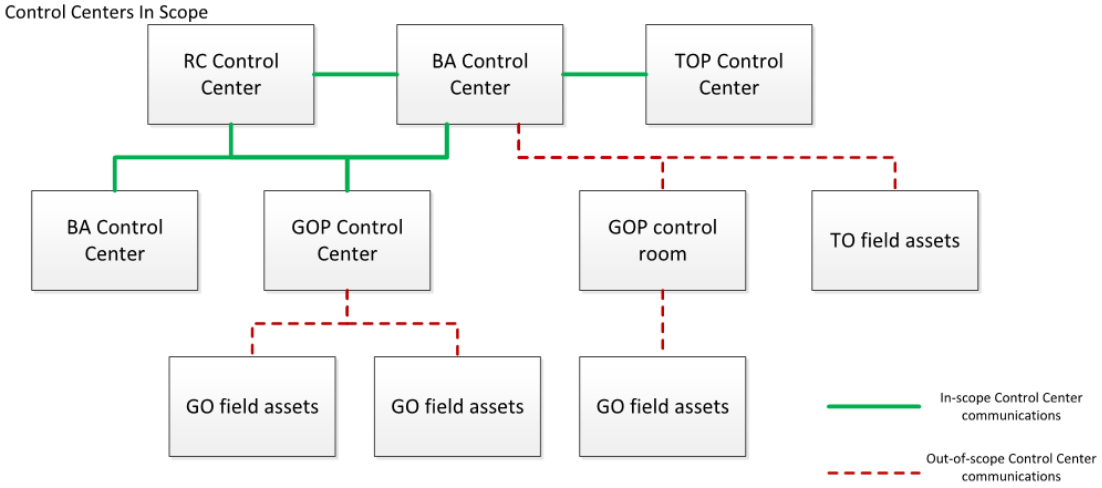


Figure 5: This reference model is an example and does not include all possible scenarios.

The SDT included Part 1.5 of the plan to address the situation when multiple registered entities are involved with protecting the data transmitted between Control Centers. Part 1.5 provides a mechanism to specify which entity is responsible for the application of security and availability controls. The SDT included this requirement part to address security and availability concerns as well as audit concerns. Where data is transmitted between different entities, the SDT asserts that it is necessary for both entities to understand the responsibilities of applying controls to ensure the data is protected through its entire transmission and there is no gap in security or availability protections. The SDT also asserts this requirement part will provide evidence which may prevent the simultaneous auditing of multiple entities for each communication link between Control Centers when operated by different Responsible Entities. Controls applied by the entity to achieve compliance with Parts 1.1 through 1.4 of the plan should correlate to the documented responsibilities in Part 1.5 of the entity's plan.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems