NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

May 2018

RELIABILITY | ACCOUNTABILITY



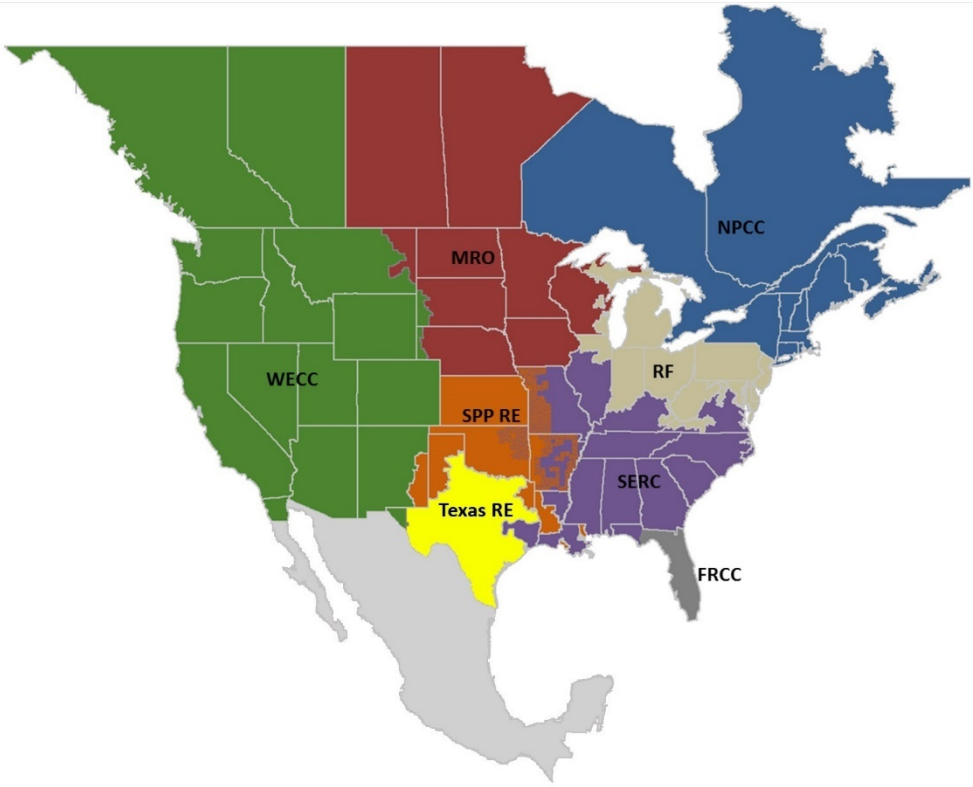

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs), is a highly reliable 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.

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012-1. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable.

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 data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system 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 Bulk Electric System (BES) data and communications 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, or 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. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 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 contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

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

CIP-012 Exemption (4.2.3) for certain Control Centers

As the SDT drafted CIP-012, it 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. However, their communications to their normal BA or TOP Control Center are not the type of communications that are the intended scope of CIP-012 as they do not differ from 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.

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

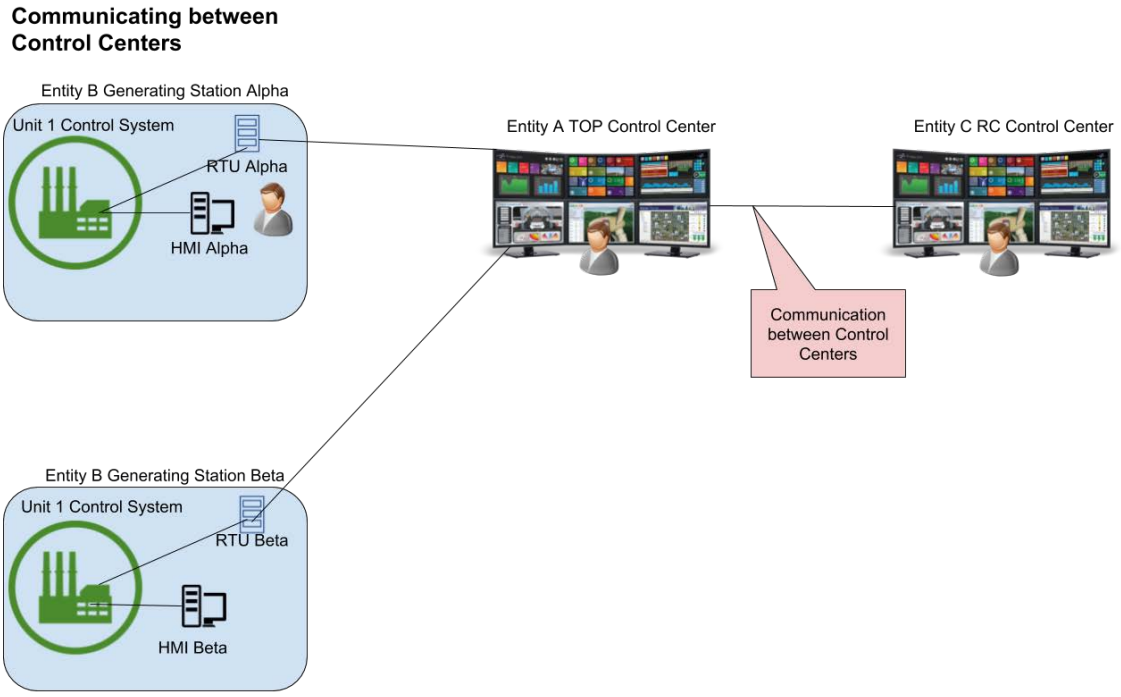


Figure 1

Figure 1 above pictures 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 it meets 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) and 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 and the operator at Station Alpha should be able to remotely start the unit at Station Beta if necessary.

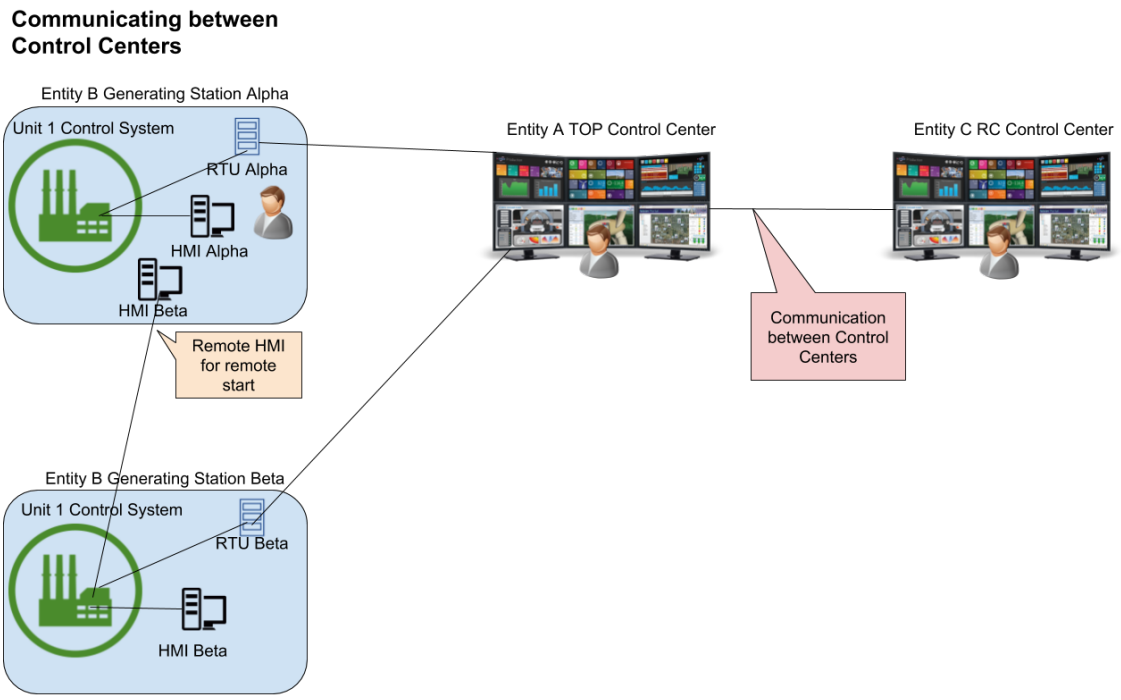


Figure 2

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 the operator can 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." It 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 from Figure 1 have not changed at all. No new cyber systems are in place that can impact multiple units. No cyber systems have been added performing Control Center functions. No additional risk from cyber systems has been added. The only thing that has changed is an HMI for Station Beta has been moved within close physical proximity to an HMI for Station Alpha.

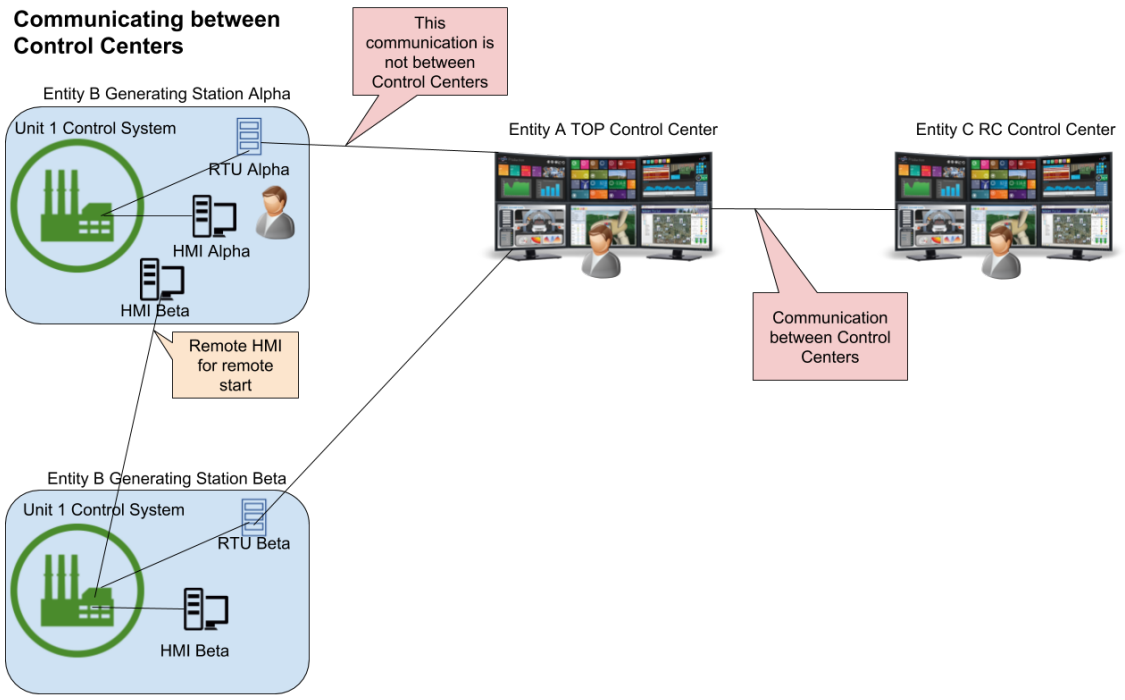


Figure 3

The SDT realized how this suddenly makes the communication noted in Figure 3 between Station Alpha and Entity A's TOP Control Center subject to CIP-012 although nothing has changed between them. There is no new risk involved. Two HMI's have been moved into the same room and suddenly a new NERC CIP standard applies to two entities.

This is an anamoly of the current Control Center definition defining a facility, room, or building from which something can be done without regard to how its done or with what systems. This is a generation specific example, but the SDT can envision substations with an HMI or protective relay that "operating personnel" within the substation could use to impact an adjacent substation. The SDT realizes that in the criteria for TO's and GOP's the "two or more geographic locations" is not a precise enough filter for capturing 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 at this time. Therefore the SDT is handling the issue this creates for CIP-012 by the 4.2.3 exemption within the CIP-012 standard which reads:

> 4.2.3. A Control Center at a generation resource or Transmission station or substation 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 at which the transmitting Control Center is located.

The intent of this exemption is to exclude the normal RTU-style communication from a field asset about that field asset's status from CIP-012. 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 communications can be using older legacy communication technology and protocols.

Requirement R1

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while 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 security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring while being transmitted between Control Centers;*

1.2 *Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and*

1.3 *If he Control Centers are owned or operated by different Responsible Entities,identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.*

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 Bulk Electric System while in transit between applicable Control Centers. The SDT does not intend for the listed order of the three requirement parts to convey any sequence or significance.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring data. This is accomplished by drafting the requirement to mitigate the risk of unauthorized disclosure (confidentiality) or modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity 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."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011.

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 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. The SDT asserts that typically the RC, BA or TOP will identify

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

all data requiring protection for CIP-012-1 through the TOP-003 and IRO-010 Reliability Standards. However, the SDT noted 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.

Identification of Where Security Protection is Applied by the Responsible Entity

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

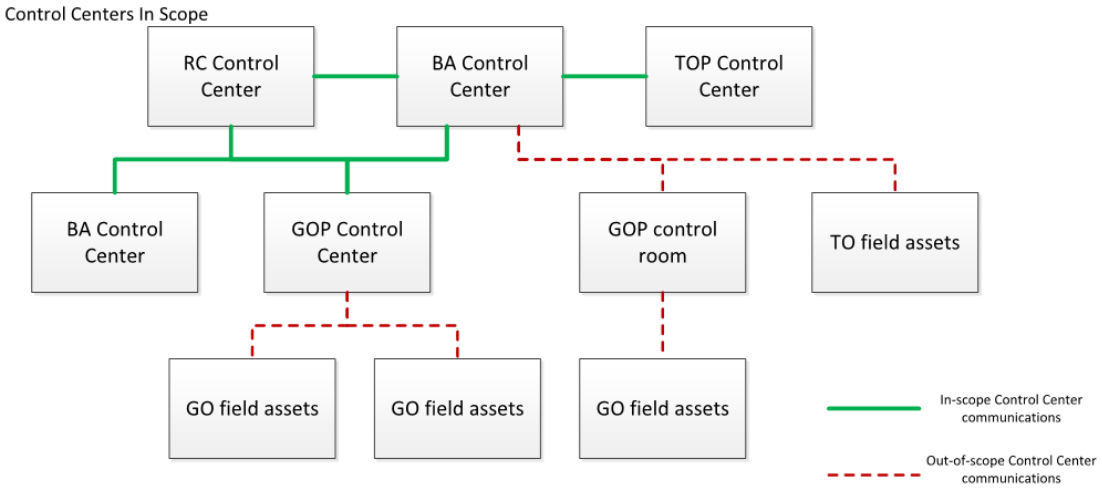
The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under Cyber Security Standards CIP-002 through CIP-011.

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 protection. The Responsible Entity should not be held accountable for identifying where a neighboring entity applied security protection at the neighboring entity's facility. A Responsible Entity, however, 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 like this, where a Responsible Entity has taken responsibility for applying security protection on both ends of the communication link, the Responsible Entity should identify where it applied security protection at both ends of the link. The SDT intends for there to be alignment between the identification of where security protection is applied in CIP-012 R1, Part 1.2 and the identification of Responsible Entity responsibilities in CIP-012 R1, Part 1.3.

Control Center Ownership

The requirements address protection for Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover 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 requirements do 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, the reference model below shows some of the data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications. The dashed red lines are out-of-scope communications.



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

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