NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda item 4b
Standards Committee
February 16, 2022

Request for Interpretation (RFI)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the RFI to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

Note: an Interpretation cannot be used to change a standard.

Interpretation 2022-INT-01: Request for an Interpretation of CIP-002-5.1a, Requirement R1, for Burns & McDonnell
Date submitted: 10-22-2021
Contact information for person requesting the interpretation:
Name: Terry Brinker
Organization: Burns & McDonnell
Telephone: 219-614-1321
Email: tlbrinker@burnsmcd.com
Identify the standard that needs clarification:
Standard Number (include version number): CIP-002-5.1a, R1
Standard Title: Cyber Security – BES Cyber System Categorization
Identify specifically what requirement needs clarification:
Requirement Number and Text of Requirement: Req. R1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: • Clarification needed: Specifically, if system-to-system serial communications between a Transmission Owner's (TO) medium impact Bulk Electric System Cyber System[1] (BCS) connects to a Transmission Operator's (TOP) BCS must any and all converters protect the connection by either enforcing an authentication break or by residing inside a defined Electronic Security Perimeter[2] (ESP) (thereby relying upon the ESP to provide the necessary protections)?

[1] One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

[2] The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

- In such cases, is it a pre-requisite that said converters must meet the definition of a Bulk Electric System Cyber Asset[3] (BCA) to justify such protections?

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

The material impact caused by the lack of clarity for such communication devices extends the delineation points beyond the defined Electronic Security Perimeters and creates various interpretations. The various interpretations are not just to the CIP Standards, but also the responsibilities and ownership of the reliability tasks found in the NERC Functional Model.

Version History

Version	Date	Owner	Change Tracking
1	April 22, 2011		
1	May 27, 2014	Standards Information Staff	Updated template and email address for submittal.
1	June 28, 2017	Standards Information Staff	Updated template.
2	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
3	February 25, 2020	Standards Information Staff	Updated template.

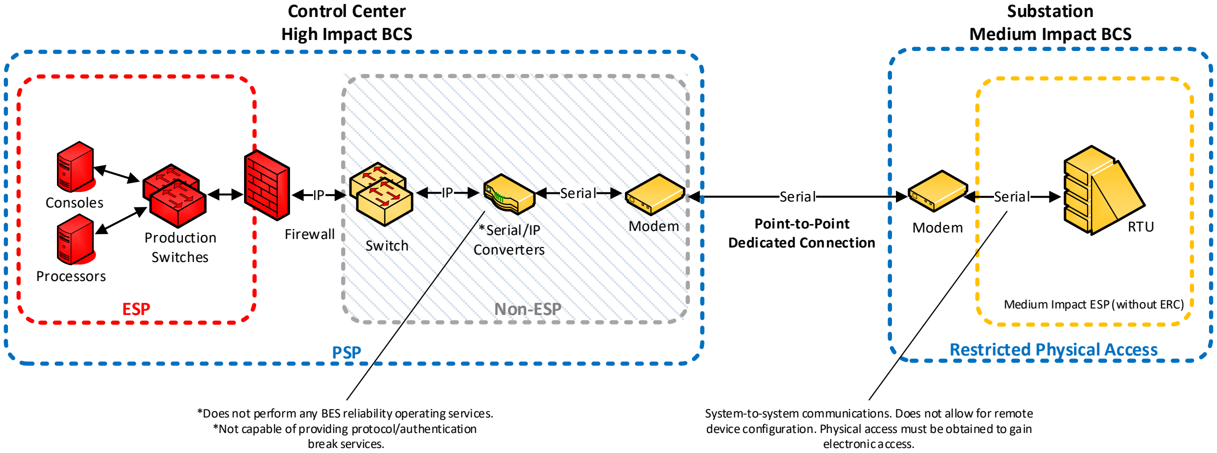
[3] A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Request for Interpretation - CIP-002-5.1a R1

Background

Burns & McDonnell is representing a client that has Internet Protocol (IP) to serial converters (converters) physically located at Control Centers but outside of any defined Electronic Security Perimeters (ESPs). The converters are used as part of the communications network to convert serial traffic from medium impact BES Cyber Systems (BCS) at Transmission substations (without ERC) to IP enabling data communication. The converters also do not perform any BES reliability operating services as found in the Guidance and Technical Basis of CIP-002-5.1a. Burns and McDonnell has confirmed the converters are not technically capable of providing protocol/authentication break services. The client had classified the converters as out of scope under its CIP-002 methodology as falling under the CIP-002-5.1a Applicability Exemption 4.2.3.2. “*Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters*”.

A visual depiction of the client’s architecture to provide context of the converters in relationship to upstream and downstream BES Cyber Assets and ESPs is depicted per the following network diagram.


Control Center
High Impact BCS
Substation
Medium Impact BCS
Consoles
Production
Switches
Processors
Firewall
IP
Switch
IP
*Serial/IP
Converters
Serial
Modem
ESP
Non-ESP
PSP
Serial
Point-to-Point
Dedicated Connection
Modem
Serial
RTU
Medium Impact ESP (without ERC)
Restricted Physical Access
*Does not perform any BES reliability operating services.
*Not capable of providing protocol/authentication
break services.
System-to-system communications. Does not allow for remote
device configuration. Physical access must be obtained to gain
electronic access.

The Issue

Our client was told by its Regional Entity (RE) upon review of the converters and their infrastructure that:

> *“Whenever a serially connected BCA (such as an RTU) is accessed through a network via a routable protocol using a protocol converter (such as a <manufacturer specific>), the protocol converter must protect the connection by either enforcing an authentication break or by residing inside a defined ESP (thereby relying upon the ESP to provide the necessary protections). If used, an authentication break must be an interactive process that interrupts the connection and forces the end user to respond to an authentication challenge.”*

The RE also indicated the following:

> *"Per CIP-005-5 R1, Part 1.1, all applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined Electronic Security Perimeter (ESP). Applicable Cyber Assets include high and medium impact BES Cyber Systems and their associated Protected Cyber Asset (PCA) (Reference: CIP-005-5 Table R1). Residing within a defined ESP requires that an applicable Cyber Asset's interfaces that communicate via a routable protocol be physically connected to the ESP network.*
>
> *The <converters> referenced in the <client's> inquiry are serially connected to medium impact BES Cyber Assets. The terminal servers are also connected via a routable protocol to the <client's> Internet Protocol (IP) network. The terminal servers provide protocol conversion, without an authentication break, for the serially connected BES Cyber Assets so these devices may communicate via a routable protocol with other assets located on the IP network. This configuration effectively connects the medium impact BES Cyber Assets to a network via a routable protocol; therefore, they must reside within a defined ESP. Specifically, the interfaces that communicate via a routable protocol (which in this case are attached to the <converters> must be physically connected to a defined ESP network."*

One fundamental issue with RE's position is not distinguishing between Interactive Remote Access (IRA) and system-to-system process communications. As shown in the provided network diagram, the communications between the Control Centers and substations are strictly system-to-system. Any configuration or modification to the application BES Cyber Assets (BCA) requires physical access and the use of a port separate than the serial port.

The client is thereby being asked by its RE to do one of the following:

1) Implement on the converters, an authentication/protocol break service to the serially connected transmissions stations and classify and protect the converters as Electronic Access Control or Monitoring Systems (EACMS) associated with medium impact BES Cyber Systems.
   a. The converters do not have the technical capability to perform any type of "*electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems*". After discussion with the RE, it was agreed EACMS was not an appropriate categorization for the converters due to the technical capability limitation.

2) Move the converters into adjacent high impact ESPs and classify and protect the converters as Protected Cyber Assets associated with high impact BES Cyber Systems.
   a. This approach lowers the client's security posture since moving the converters inside the existing high-impact ESP would then bypass any Electronic Access Points (EAP). The proposed architecture would directly connect the Ethernet port of the converters to the front-end processors (FEP) and no longer be afforded the protections of the EAP. The RE agreed that this was not an ideal solution for the

same reasons. Additionally, the RE's position to classify the converters as PCAs also highlights they do not meet the definition of a BCA.

3) Classify the converters as BCAs associated with the medium impact BES assets where the serially connected BES Cyber Assets reside. This would necessitate defining the network segment in which the converters reside as an ESP and ensuring compliance thereof with CIP-005-5 R1.

   a. In Option 2, the RE states a PCA categorization is acceptable. This statement highlights, and confirms the initial categorization, these Cyber Assets do not meet definition of a BCA based on their function. Additionally, the converters are physically located at the Transmission Operator's (TOP) Control Centers and not at the Transmission Owner's (TO) substations with medium impact BCSs. Such an approach blurs the delineations in the NERC Functional Model between the Functional Entity types of TOP and the TO as each have separate roles and equipment for their respective reliability tasks. In various situations, the TOP and the TO may or may not be the same registered entity and ownership of communication equipment may be split or be owned and managed by a third party.

FERC and NERC have attempted to clarify these types of components with publications. First, NERC provided a lessons learned document that addressed converters in 2015 in a document titled Lesson Learned CIP Version 5 Transition Program - Communications to BES Cyber Systems and BES Cyber Assets. The following are key extracts from the document:

> ***Communications to serially connected BES Cyber Systems.*** *When BES Cyber Systems or BES Cyber Assets were connected using serial data links, the communication networks, including protocol converters and terminal servers, were reviewed to identify risks. Communications were grouped into two categories;*
>
> *• Interactive Remote Access:*
> *The CIP version 5 standard requirements for Interactive Remote Access to BES Cyber Asset do not include serial communications. However, when BES Cyber Systems or BES Cyber Assets are connected using serial data links that provide a way for a user-initiated remote access with a BES Cyber Asset, security risks can arise. Associated communication networks were reviewed to identify these risks. In order to help reduce this risk, while not required to demonstrate compliance, study participants chose to utilize two-factor authentication and access controls, where possible, similar to an Intermediate System.*
>
> *• System-to-system process controls:*
> *The CIP version 5 standard requirements for Interactive Remote Access do not include system-to-system processes using serial communications. However, study participants identified routable connectivity to an asset containing medium impact rating BES Cyber Assets as a possible security risk when there was an IP-to serial conversion between a BES Cyber Asset and an external network.*

> *In order to help reduce this risk, while not required to demonstrate compliance, study participants chose to implement a firewall with strict inbound and outbound access permissions allowing only network traffic documented as essential to the proper functioning of the BES Cyber Asset. Also, study participants provided additional measures in their physical security plan for these types of assets to provide an extra level of protection against unauthorized access. No additional controls were implemented for relay-to-relay communications.*

The client's existing architecture follows this guidance by locating the converters inside a Physical Security Perimeter (PSP) and forcing the routable communications from the converters through an EAP (firewall) with a strict ruleset.

Second, is FERC's Lessons Learned from Commission-Led CIP Reliability Audits from 2020, which we understand to not be enforceable, was used as a basis from the RE to state the converters required some type of NERC CIP applicability. This is an extract from item 1. under Section V. Lessons Learned Discussion (page 6):

> *"While entities generally identified BES Cyber Assets effectively, in some cases entities did not identify BES Cyber Assets equipment performing supporting functions. For example, several entities misidentified Cyber Assets as communications equipment instead of BES Cyber Assets. Cybers Assets that seem to serve only a communication function such as switches and protocol converters may pose an impact to the BES within 15 minutes of their misuse. NERC, in a lessons learned document, recommends assessing whether all Cyber Assets can impact the BES within 15 minutes including communication Cyber Assets."*

The third publication is a set of proposed recommendations for clarity under a Standards Authorization Request titled CIP V5 TAG Modifications ERC and IRA under Project 2016-02 CIP Modifications from May 7, 2020. This document shows multiple diagrams with serial to IP converters being categorized as EACMS with system-to-system communications. As stated earlier, this is an improper categorization as no "*electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems*" is performed by the converters.

Inherently, communication networks and data communication links pose some level of risk to the BES. The client assessed devices on communications networks and links, such as a converters and transport routers/switches, and determined there is a limited possibility that compromise or misuse of could cause disruption to the BES within 15 minutes; but only in an event where a malicious actor altered telemetry data coming from the serially connected BCAs (such as an Remote Terminal) at the transmission stations to the Control Center, and the system operator then took manual action based on the data transmitted over the communication network and links. However, the probability of compromise or misuse was determined low and mitigated by the fact that such devices on communication networks and links are protected from unauthorized physical access as they are located within a secured PSP as the must connect to Electronic Access Points. Further, if communication networks and links with the Transmission substations were to be lost, the client could manually control the assets at its substations.

However, based on the position indicated by the RE above in regard to converters in relation to BCAs, the RE agreed that regardless of whether the converters meets the definition of a BCA, they wanted them or their associated network switches to be placed within an ESP given that they are technically incapable of providing authentication/protocol break services to qualify as EACMS. As a result, they would need to be classified or protected as either BCAs and PCAs respectively or protected vice versa.

The Request

In light of the RE's communicated position per 'The Issue' section above, has NERC's formal position to the REs changed regarding the classification and protection of such devices used in communication networks and links?

- Specifically, if system-to-system serial communications between a TO's medium impact BCS connects to a TOP's BCS must any and all converters protect the connection by either enforcing an authentication break or by residing inside a defined ESP (thereby relying upon the ESP to provide the necessary protections)?
- In such cases, is it a pre-requisite that said converters must meet the definition of a BCA to justify such protections?