NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned
CIP Version 5 Transition Program

Communications to BES Cyber Systems and BES Cyber Assets

Version: November 9, 2015

This document is designed to convey lessons learned from NERC's various CIP version 5 transition activities. It is not intended to establish new requirements under NERC's Reliability Standards, modify the requirements in any existing reliability standards, or provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Purpose

The purpose of this lesson learned is to provide guidance when connecting a BES Cyber System or BES Cyber Asset to a communication network external to the BES Cyber System or BES Cyber Asset.

Guidance

This lesson learned presents approaches used by Implementation Study participants.[1] Study participants reviewed the different types of communications to BES Cyber Systems, controls to reduce or eliminate the risks and reviewed how these controls met the requirements of the CIP standards. Study participants noted that access to serial connected medium impact BES Cyber Assets through the use of serial data links, protocol converters or terminal servers presented possible security risks and applied controls to reduce or eliminate the risks. Some of the applied controls were not necessarily required by the CIP standards, but were implemented as good security practices.

Non-essential Communications to BES Cyber Systems

An effective way to reduce or eliminate risks to the reliable operation of the BES associated with connecting a BES Cyber System to a communication network is to minimize connectivity to BES Cyber Systems. Following a review of all communications to BES Cyber Systems, study participants disconnected all non-essential communication paths to decrease potential attack vectors.

Essential Communications to BES Cyber Systems

Examples of essential communication include:

[1] Ref. Implementation Study Final Report http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPv5_Implem_Study_Final_Report_Oct2014.pdf

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

- Remote terminal units at a substation communicating with an energy management system at a Control Center
- An engineer using a computer to communicate with a protective relay

Routable communications to BES Cyber Systems[2]. When the BES Cyber Systems or BES Cyber Assets were connected to a network via a routable protocol to support essential communications, an Electronic Security Perimeter (ESP) was established for the BES Cyber Systems or BES Cyber Assets. Controls were added to mitigate risks to BES Cyber Systems or BES Cyber Assets that have the ability to be accessed from outside their ESP via a routable bi-directional routable protocol. The Cyber Assets used to control electronic access to the BES Cyber Systems or BES Cyber Assets were identified as Electronic Access Control or Monitoring Systems (EACMS). Additionally, participants identified the Electronic Access Points (EAP) to ESPs, and the Intermediate System when there is Interactive Remote Access.

Dial-up Connectivity to BES Cyber Systems[3]. When BES Cyber Systems or BES Cyber Assets could be accessed via Dial-up Connectivity that supported essential communications, Cyber Assets were installed to perform authentication and were identified as an EACMS.

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.

[2] Ref. Reliability Standard CIP-005-5, Requirement R1 and R2

[3] Ref. Reliability Standard CIP-005-5, Requirement R2

The CIP version 5 standards do not specifically address access to serial devices from networks that use a routable protocol. Serially connected BES Cyber Assets that can be accessed via a protocol converter (identified as a port server in Figure 1) were not considered to be BES Cyber Assets with External Routable Connectivity as defined below.

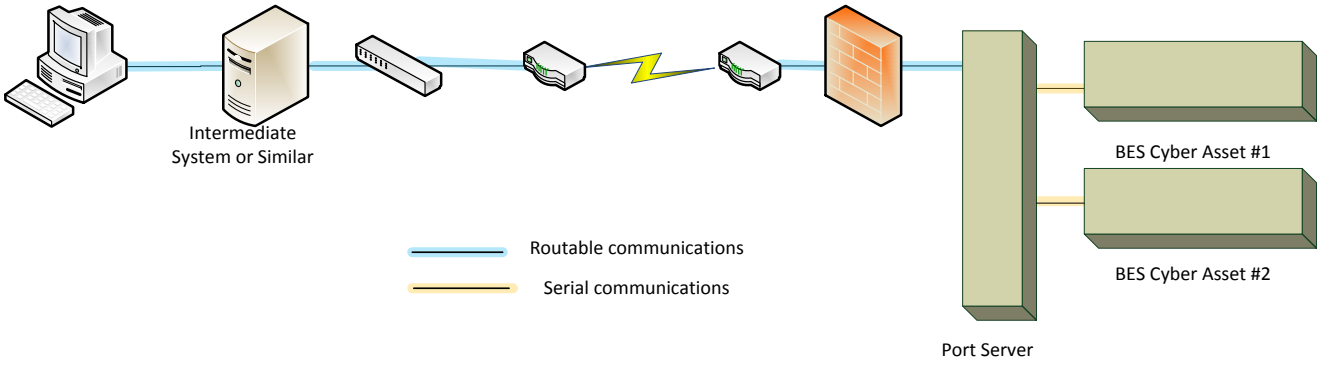

Figure 1

Serial-IP converters were evaluated to determine "if [they were] rendered unavailable, degraded, or misused would [they], within 15 minutes of [their] 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." If Serial-IP converters were determined to be BES Cyber Assets according to the above definition, then the related ESP architecture would be applied as necessary consistent with CIP-005-5 and all other controls applicable to BES Cyber Systems with External Routable Connectivity.

Referral for Future Standards Development

The implementation study participants found a lack of clarity in the CIP version 5 Reliability Standards because they do not specifically address remote access to serially connected BES Cyber Asset or BES Cyber Systems. Consequently, the CIP version 5 implementation study participants referred the identified issue to the CIP standards drafting team to be evaluated for future standards development.

Background Information

Relevant NERC Glossary Terms

BES Cyber Asset – 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. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP,

A Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber System – One or more BES Cyber Assets logically grouped by a Responsible Entity to perform one or more reliability tasks for a functional entity.

Electronic Access Control or Monitoring Systems (EACMS) – Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.

External Routable Connectivity (ERC) – The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access – User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate System – A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.