NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned
CIP Version 5 Transition Program

CIP-002-5: BES Cyber Assets

Version: December 7, 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 foundational definition for the CIP version 5 Reliability Standards is Cyber Assets. When Cyber Assets meet a threshold of BES impact they become BES Cyber Assets (BCA) which may be grouped by responsible entities into BES Cyber Systems (BCS). In Order 791, the Commission identified the definition of BCA "is intended to capture assets involved in real-time operations, such as systems that provide input to an operator for real-time operations or trigger automated real-time operations." This lesson learned document provides examples of approaches used by Implementation Study participants[1] to identify BES Cyber Assets. Participants found that the definitions of Cyber Assets and BES Cyber Assets cover an extremely broad range of sophistication and capability, from server farms running control centers to a printed circuit board in a smart pressure transmitter. There is a level of sophistication or capability below which many of the cyber security controls can no longer be applied.

Guidance

Study participants used various methods to identify their BES Cyber Systems and the adverse impact due to unavailability, degradation, or misuse. Some study participants assessed each functional system at a site or facility to determine its potential to adversely impact the BES in 15 minutes or less. If there was a 15 minute impact, then that system's individual Cyber Assets associated with that functional system were evaluated for impact. After all functional systems were assessed, all associated Cyber Assets with a 15 minute or less adverse impact were grouped into BES Cyber Systems. These BES Cyber Systems would then be evaluated according to the impact rating criteria identified in CIP-002-5 Requirement R1, Attachment 1. Other study

[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

participants identified all Cyber Assets, grouped them into BES Cyber Systems, and evaluated the impact of the resulting system.

As described below, study participants considered the device's functions and capabilities to determine whether a device was a BCA, another type of Cyber Asset within the CIP Reliability Standards[2], or out of scope of the standards.

Function: Did the device's function impact the reliable operation of a BES asset? For example, a protective relay's function is to constantly monitor conditions and operate breakers to protect BES assets. A vibration monitoring system on a generating unit may be configured to trip the unit offline if certain critical equipment's vibration exceeds defined thresholds. Other devices such as data historians or digital fault recorders only monitor and/or record information and have no impact.

Impact Timeframe: Was the impact within 15 minutes or less? As stated in the BES Cyber Asset survey filed with FERC[3], certain devices and systems may have an impact on the reliable operation of a BES asset, but the impact's timeframe is not 'real time' and instead allows sufficient time for operations processes to respond to avoid sudden BES disturbances and resulting Adverse Reliability Impacts. Examples include a fuel handling system at a coal-fired plant that loads the bunkers inside the plant. Any impact to the fuel handling system does not affect generation within 15 minutes as the bunkers usually have many hours of coal supply inside the plant.

Security Function: Did the device function as an EACMS, PACS, or Intermediate System? These types of devices, such as firewalls, intrusion prevention systems or physical access controllers and others that perform security functions may indeed have an adverse impact if they are unavailable or misused to allow unauthorized access or deny authorized electronic or physical access. These devices have their own definitions and requirements in the CIP version 5 Reliability Standards and therefore are not considered BCAs.

Communication Function[4]: Did network devices or other devices involved in communications affect the reliability of the BES asset within 15 minutes when considering the nature and impact of the communications they host? For example, a network switch that directly connects BCAs to each other and is integral to the ability of those BCA's to perform their reliability function within an Electronic Security Perimeter (ESP) were assessed to be a BCA. However, an identical network switch utilized outside of an ESP and used to connect devices to Wide Area Network (WAN) communications equipment may not be a BCA.

Connection Duration: Was the device's ability to impact the BES due to the temporary or transient nature of its connectivity? A device that is connected to a BCS or within an ESP for 30 consecutive calendar days or

[2] E.g., Protected Cyber Asset (PCA), Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS)

[3] Ref. http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Info_Filing-BES_Cyber_Asset_Survey_RM13-5_02032015.pdf

[4] A "Communications and Networking Cyber Assets" lesson learned document is currently being drafted.

less and used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes is not a BCA[5]. Examples include a laptop used by support personnel or a configuration/calibration handset.

Capability: The participants recognized that the CIP standard definitions do not address the level of sophistication or capability of programmable electronic devices nor does it define the term 'programmable.' The reliability risk from a cyber perspective posed by a device is often tied to the level of sophistication or capability of that device. Does the device have a level of cyber capability or functionality for which the cyber security controls would be applicable? The risk and potential impact from a compromised operator human-machine interface (HMI) is typically much higher than a single miscalibrated instrument. There are programmable devices that have no concept of a user or authentication, have no ports/services, have no network connectivity, no concept of event logs or alerting, no patches or updates, and are located in areas where physical security perimeters cannot be established. However, the upstream devices to which they connect (e.g., PCs, servers, distributed control system (DCS) controller modules, programmable logic controllers (PLC)) often do have sufficient capability, are clearly Cyber Assets, and were considered as BCAs and afforded CIP protections based on their BES impact categorization.

For example, study participants set the scope to be evaluated as those devices that have a microprocessor and can accept firmware, software or logic. Additionally, the study participants considered devices that had a physical or wireless port or a web interface that can be used to "flash" firmware to be Cyber Assets and then evaluated them to determine whether they meet the BES Cyber Asset definition. Conversely, generating plants have many instruments and actuators that measure temperatures, pressures, flows, or actuate valves and may be digitally calibrated or configured locally through an interface of some kind (e.g., keypad or handheld configurator) and were considered examples of non-programmable devices by some study participants. However, the controllers to which they were connected (e.g., PLCs, DCS controllers) were considered Cyber Assets and evaluated as BES Cyber Assets. Similarly, substations typically have numerous remote input/output (I/O) modules that allow several copper wire based signals to be consolidated and brought into the control house over a single fiber optic cable. These modules may have internal firmware but there is no field-accessible way to modify the program as configuration is performed using a local DIP switch or the device required field disassembly; these too were considered examples of non-programmable devices by some study participants.

The BES Cyber Asset survey provided several examples of devices considered to be Cyber Assets and included for evaluation as BCA's by study participants. As stated in the survey from the NERC comments to the Order 791 Notice of Proposed Rulemaking (NOPR), "because there are differences in the way certain Cyber Assets are used across the BES, a determination of whether a particular Cyber Asset meets the definition of a BES Cyber Asset necessarily depends upon the individual facts and circumstances of how an entity uses the Cyber Asset (i.e., the functions of the Cyber Asset and the Facilities, systems or equipment it supports)." In response to the survey, the participants identified the following Cyber Asset types at Controls Centers, Transmission Station / Substation, and Generation Plants. These Cyber Assets would typically be evaluated to determine whether they meet the 15-minute and other criteria of a BES Cyber Asset (ref. Table 1).

[5] Ref. Definition of BES Cyber Asset in the NERC Glossary of Terms and as used in the CIP version 5 Reliability Standards.

Table 1: Cyber Assets Typically Evaluated as BES Cyber Assets		
Control Centers	**Transmission Station/Substation**	**Generation Plants**
Application servers	Intelligent Electronic Devices (IED) / protective relay	Programmable Logic Controller (PLC)
Data servers	Remote Terminal Unit (RTU)	Distributed Control System (DCS)
HMI workstations	Programmable Logic Controllers (PLC)	HMI workstation
Data acquisition	Data concentrator	Application server
Data interchange	Meter / indicator	Data server
Computer networking	Tap changer	Computer networking
Communication processing	HMI workstation	Intelligent Electronic Device (IED)/ relay
Precision time device	Computer networking	Remote Terminal Unit (RTU)
	Communications processing	

Examples of devices that may or may not be Cyber Assets but were evaluated and determined not to be a BCA by some study participants included the following types of devices.

- A solid state relay that allows the user to set when the relay will operate but not how the relay operates.
- A HART (Highway Addressable Remote Transmitter) compatible smart pressure transmitter
- A HART compatible smart actuator for a final control element, such as a control valve or damper
- A handheld HART configurator (the 30 day connection exclusion normally applies to these devices)
- Output only/sealed devices
- Media converters and Remote I/O modules (i.e., Copper to fiber converter)

Documenting the Rationale Used to Identify BCAs and non-BCAs

As part of the Implementation Study, participants identified that documenting the approaches they used to evaluate devices to determine which were identified as BCAs and which were not, helped to create a repeatable process. Additionally, documenting the methodology assisted when explaining to the regional auditors and the NERC Implementation Study team why certain devices were determined to not meet the threshold of a BCA. Study participants also chose to document their rationale by either BES Cyber System, groups of similar devices, or device class to reduce the effort required.

Observation

Study participants noted that the CIP version 5 Reliability Standards did not sufficiently define the "programmable electronic device" component of the BCA NERC Glossary term, and the considerations provided in this lesson learned helped the study participants to assess and identify their Cyber Assets.

Referral to Standards Development

The transition study participants found a lack of clarity in the CIPV5 Reliability Standards because they do not specifically define the "programmable electronic device" component of the BES Cyber Asset NERC Glossary term. Consequently, the CIP V5 Transition Advisory Group referred the identified issues to be evaluated for standards development.

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.

Cyber Assets – Programmable electronic devices, including the hardware, software, and data in those devices.