


Network Perception

Using NP-View to prepare for a NERC CIP-003 audit

Version 1

November, 2022



Key Summary	2
Introduction	3
Important NERC CIP Concepts	3
Bulk Electric System (BES) Assets	3
Cyber Assets	4
BES Cyber Asset or System (BCA / BCS)	5
Asset Boundary Considerations	5
Summary of Concepts	6
CIP-003 Obligations	7
Example Type 1: Non-Routed	7
Example Type 2: Wireless	8
Example Type 3: Routed	10
Example Type 4: Firewalled	11
Summary of Examples	11
Audit Preparation Workflow	12
Prerequisite Activities	12
Routable Protocols	12
Type 1: Non-Routed	13
Type 2: Wireless	14
Type 3: Routed	16
Type 4: Firewalled	17
Time-Sensitive Protocols	17
Type 1: Non-Routed	18
Type 2: Wireless	18
Type 3: Routed & Type 4: Firewalled	19
About NP-View	20



Key Summary

Compliance with NERC¹ CIP Reliability Standards requires NERC registered entities to adopt precise procedures and to verify their implementation. This white paper describes the requirements under CIP-003, the Standard for Security Management Controls, particularly the obligations for Low Impact Bulk Electric System described in Attachment 1. It illustrates how a NERC registered entity can utilize technological solutions such as NP-View to save time and resources assessing and managing its compliance with the obligations of CIP-003.

¹ NERC is the acronym for the North American Electric Reliability Corporation. NERC is a non-profit organization tasked by the Federal Energy Regulatory Commission (part of the US Department of Energy) with ensuring the reliability of the North American electric power grid. Among its tasks are drafting and auditing standards for cybersecurity of the systems that monitor and control the grid. Known as NERC Critical Infrastructure Protection (CIP), this body of Standards currently number from CIP-002 through CIP-014.

Introduction

Successfully managing compliance means gaining a clear understanding of requirements and building a workflow that enables a team to coordinate while reviewing evidence and preparing reports. Used efficiently, technology can bring automation to this workflow, in order to save time and minimize the risk of human error. In the context of CIP-003, mis-identifying an asset or missing an electronic access control can lead to serious consequences, including fines. This white paper provides a step-by-step guidance towards building such a workflow for CIP-003 requirements.

An effective CIP-003 audit preparation workflow begins with a clear understanding of the network communications within the asset.

Important NERC CIP Concepts

A general understanding of the terms and concepts employed within this whitepaper greatly enhances its meaning and application. These terms, defined below for convenience, in no way supersede the official NERC Glossary of Terms².

Bulk Electric System (BES) Assets

The North American power grid consists of a huge network of fixed assets linked by transmission lines. The NERC Cyber Security Standard CIP-002-5.1a³ uses the word “assets” in Requirement 1 to refer to distinct locations or sites that an entity must consider for BES impact. As the Standard uses the word without capitalization, no entry exists for it in the NERC Glossary as currently published. CIP-003-8⁴ Attachment 1 also uses this word, again uncapitalized, in Sections 3 and 6, therefore understanding the term becomes critical to CIP-003 Compliance. The NERC Glossary (among other places) defines the Bulk Electric System (BES) to only include electrical components that operate above 100 kV⁵. CIP-002-5.1a, Requirement 1, then further filters the possible population of assets with a list of six specific types in romanette numerals (see Table 1). Since the listed items are plural, therefore, this list sets the boundary of the word “asset” as a geographical

² The [NERC Glossary of Terms](#) undergoes continual updates.

³ Cyber Security - BES Cyber System Categorization; [CIP-002-5.1a](#)

⁴ Cyber Security - Security Management Controls; [CIP-003-8](#)

⁵ *Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.*

site at the largest end of the spectrum down to a single generation unit or system at the smallest end.

Without further definition, this list must serve as a comprehensive, since page 3 of CIP-002-5.1a states that: *Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an “or,” and numbered items are items that are linked with an “and.”*

- i. Control Centers and backup Control Centers;*
- ii. Transmission stations and substations;*
- iii. Generation resources;*
- iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;*
- v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and*
- vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above*

Table 1: CIP-002-5.1a Requirement 1 assets for risk assessment consideration

Cyber Assets

NERC entities use many types of computing systems to monitor the BES. Therefore NERC, under the direction of FERC⁶, developed the Critical Infrastructure Protection (CIP) Standards to secure these systems against cyberattacks, whether targeted (as in individual hacking attempts), broadcast (e.g. computer viruses and worms), or inadvertent (a user clicks on a phishing email that installs ransomware and renders his system unusable).

Many cyber assets are recognizable as common-off-the-shelf information technology systems (computers) used throughout the modern business world. Other devices look and operate very differently from these “normal” IT systems. Often referred to as OT, or operational technology, these systems serve real-time critical reliability functions. However, since both types of devices have roles in controlling the BES, the NERC CIP standards introduced the fundamental concept of a Cyber Asset, defined in part as a “programmable electronic device.”

⁶ The [Federal Energy Regulatory Commission \(FERC\)](#) is the United States federal agency that regulates the transmission and wholesale sale of electricity.

$$PED = M \text{ and } ((L \text{ or } S \text{ or } F) \text{ and } U)$$

Table 2: Programmable Electronic Device formula

While initially causing a great deal of argument, a Programmable Electronic Device (PED) has generally been recognized to follow the pseudo-formula below. A PED is any device that utilizes a digital Microprocessor and that contains field-updatable Logic, Software, or Firmware, and allows Field Updates, which includes flashable EEPROM and socketed ROM packages.

Following this formula may reveal surprising results. Naturally, computer-based equipment, and general information technology devices must be considered. However, many control boards mounted in field cabinets will also match this description, as they have a microprocessor and often socketed PROMS. Relays, communications processors, and similar devices will fall into this category.

BES Cyber Asset or System (BCA / BCS)


While entities may employ many cyber assets in monitoring and controlling the BES, not all may be included within the scope of NERC CIP compliance. When the loss, mis-operation, or degradation of a cyber asset could cause an impact on the BES within 15 minutes, they fall under the special NERC CIP category of BES Cyber Assets or BES Cyber Systems⁷. Most of the requirements in the CIP standards apply to BES Cyber Systems but may additionally divide into three groups based on their degree of impact on the BES: High, Medium and Low impact.

Asset Boundary Considerations

CIP-003-8, Attachment 1, Section 3 (hereafter referred to as Section 3) does not employ an Electronic Security Perimeter (ESP) as does CIP-005. Section 3 uses the term Electronic Access Controls, which in this context, is capitalized only as a title, not to signify the presence of a glossary definition.

While the concept of an “asset boundary” does not exist within the CIP Standards, it provides the critical ability for measurement. Section 3 makes a boundary (by any name) irreducible when it contemplates routable communications between a Low Impact BCS (LIBCS) / Low Impact BCA

⁷ BES Cyber Systems can be composed of one or many cyber assets. The individual cyber assets may or may not have a 15-minute BES impact, but the system as a whole does. Note that a BCS must be located at one of the six types of assets listed in CIP-002-5.1a R1.1, to be in scope for CIP.



(LIBCA) and any other system that exists “outside” of that local asset. Without a boundary, it cannot be known if a system resides locally or external.

Finally, NERC discontinued development of the concepts of a Low Impact Electronic Access Point (LEAP) and Low Impact External Routable Connectivity (LERC). These concepts and terms should not be utilized or referenced in a CIP-003 Compliance Program.

Summary of Concepts

When taken together, the scope of “controls” for the “electronic access” include any routable protocol that either enters or leaves the asset boundary with a source or destination that is a LIBCS. From this perspective, a LIBCS can communicate over any protocol with another LIBCS or a non-LIBCS within the asset without electronic access controls. These communications may cross to other networks (even across firewalls) as long as they do not leave the boundary of the asset.

Only when that LIBCS communicates with (a) routable protocol and (b) outside of the boundary of its asset, does CIP-003 obligate the entity to employ, document, and maintain electronic access controls.

CIP-003 Obligations⁸

In the following examples, four different types of connections are made to a cyber asset outside of the asset boundary. The switch icon represents general connectivity, usually a switching fabric.

Example Type 1: Non-Routed

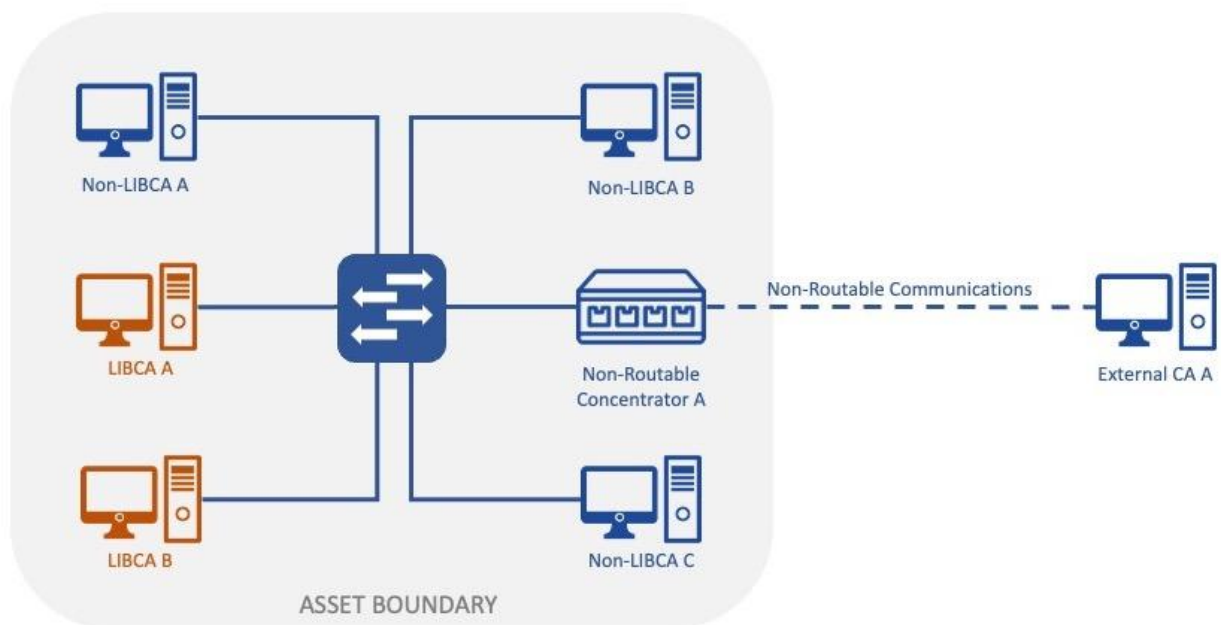


Fig. 1: Asset without Routable Ingress/Egress

Using the aggregate definition of asset, Figure 1 depicts a small system containing two LIBCA within its boundary. Section 3 does not obligate the systems depicted in this diagram to deploy electronic access controls from a strict compliance standpoint. Please note that the implications of compliance obligations does not release the owner or manager from practicing good cyber security to lower overall cyber risk. By definition, serial communications must be point-to-point.

Within the asset boundary from figure 1, LIBCA A may communicate over routable protocols with LIBCA B without electronic access controls. LIBCA A may also communicate with all Non-LIBCA cyber assets without electronic access controls.

A non-LIBCA cyber asset would take the form of any cyber asset that either does not operate at 100 kV or above, or any cyber asset that does not match the description of “Cyber Assets that, if

⁸ CIP-003-8 Attachments do not use the term requirement, as would occur within the body of the Standard itself. The Supplemental Material section seems to center on the word obligation instead. In other words, the Standard requires (R2) entities to implement plans and controls in Attachment 1, Section 3, but these obligations (plans and controls) are not prescriptive in the same way as Requirements.

rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise.”

Please be advised that the use of two media converters, whether back-to-back or at any distance and configured such as to convert IP to serial then back to IP, does not eliminate routable communications entering or leaving the asset! This first example network only contemplates a cyber asset directly connected via serial.

Example Type 2: Wireless

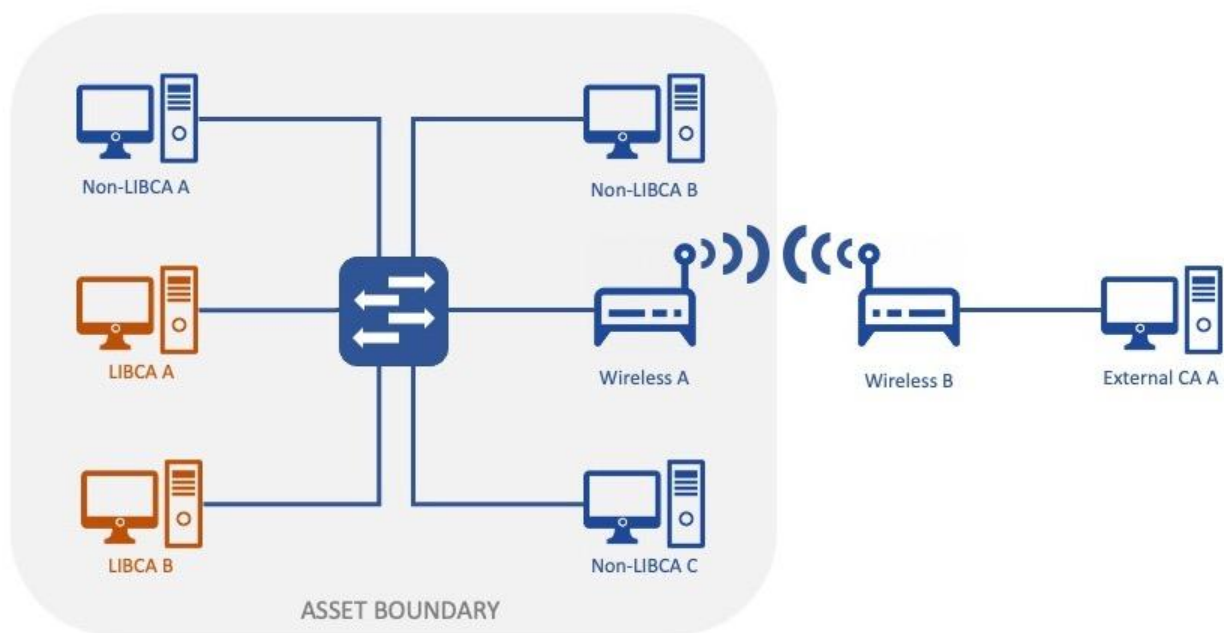


Fig. 2: Asset with Routable Wireless Connection

This second example (Figure 2) demonstrates an asset with wireless access beyond the asset boundary itself. This may typify the connections within a Wind Farm, Solar Power Array, or any other similarly dispersed facility. The boundary of the asset must be determined by the entity.

In this example, LIBCA A and LIBCA B may communicate with each other and the Non-LIBCA systems with the boundary without electronic access controls. However, if incoming or outgoing routable communications will exist between LIBCA A or LIBCA B and External CA A, electronic access controls must be employed.

In a situation such as this, host-based electronic access controls may be adequate, for example IPChains on Linux hosts or IPSec Firewall Policies on Windows hosts, as long as strict white-listing can be technologically enforced. Because the words “permit only necessary” imply a

deny-by-default obligation, the default blacklisting-style host-based firewalls may require additional configuration.

Wireless devices generally exist on layer 2 of the OSI model and below. They may have an IP address for administrative access, but will function in one of two ways. A Wireless Access Point (WAP, not pictured in the diagram) deploys some functionality similar to a network switch, controlling the fabric that allows many devices to communicate to each other or to wired devices. The second type takes the form of a Point-to-Point (PTP) connection from a distant device or network.

For the purposes of analysis against the asset boundary, the WAP usually has a relatively limited range; it may not be capable of connecting to devices external to its asset. However, if it does, the wireless connection should be considered equivalently to wired connections.

Finally, please note that the network in Type 2 poses the greatest challenge to demonstrating electronic security controls comprehensively. The amount of compliance effort may far exceed the cost of a simple firewall.

Example Type 3: Routed

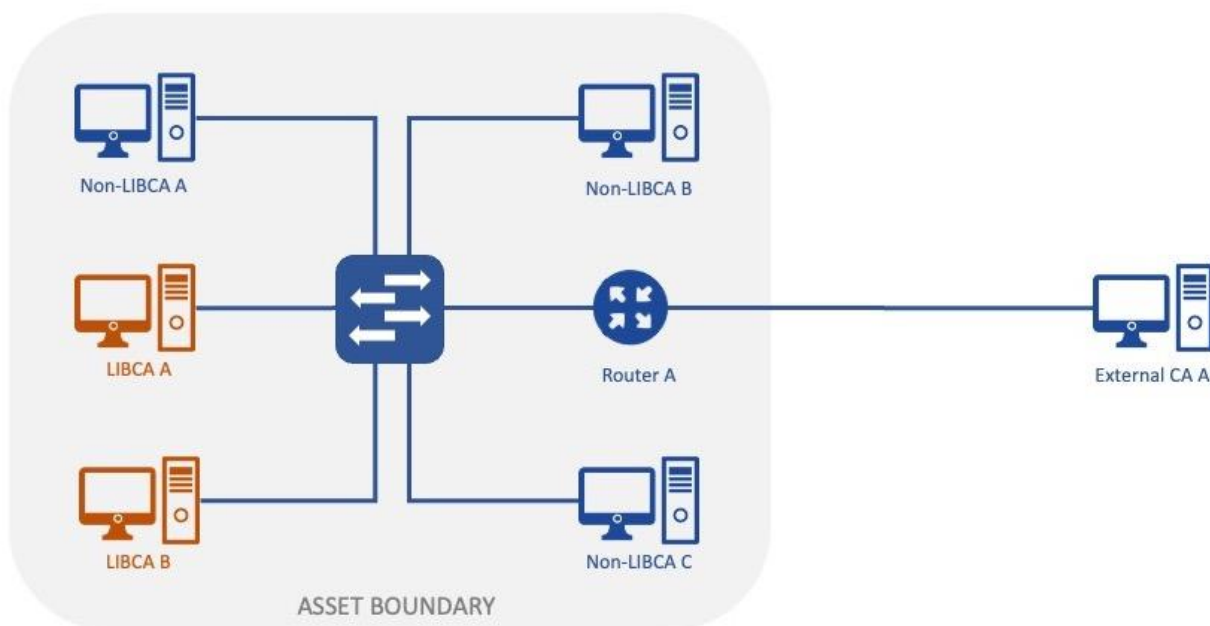


Fig. 3: Asset with Routed Network Connection

Figure 3 deploys a router to divide two subnets. This router allows through only traffic destined for the subnet beyond, but applies no additional filtering. Many older generation sites implement simple routers to break up broadcast domains to protect real-time monitoring and control traffic.

Much like example 2, if only a small number of LIBCS exist within the asset boundary, the entity may elect to use host-based firewalls to create electronic access control. In larger networks, this may quickly become unwieldy, as each single asset adds to the overall compliance burden. Therefore, entities may add a firewalling module to the existing router (if possible) or replace it entirely with a firewall.

This example illustrates a very common network albeit generally built decades ago. Electronic access controls on routers, often called Access Control Lists (ACL), may play a vital role in an entity's CIP-003 program but cannot always serve comprehensively. For instance, a Cisco Standard ACL cannot filter by TCP/IP port. Port-level filtering uses a Cisco Extended ACL.

Example Type 4: Firewalled

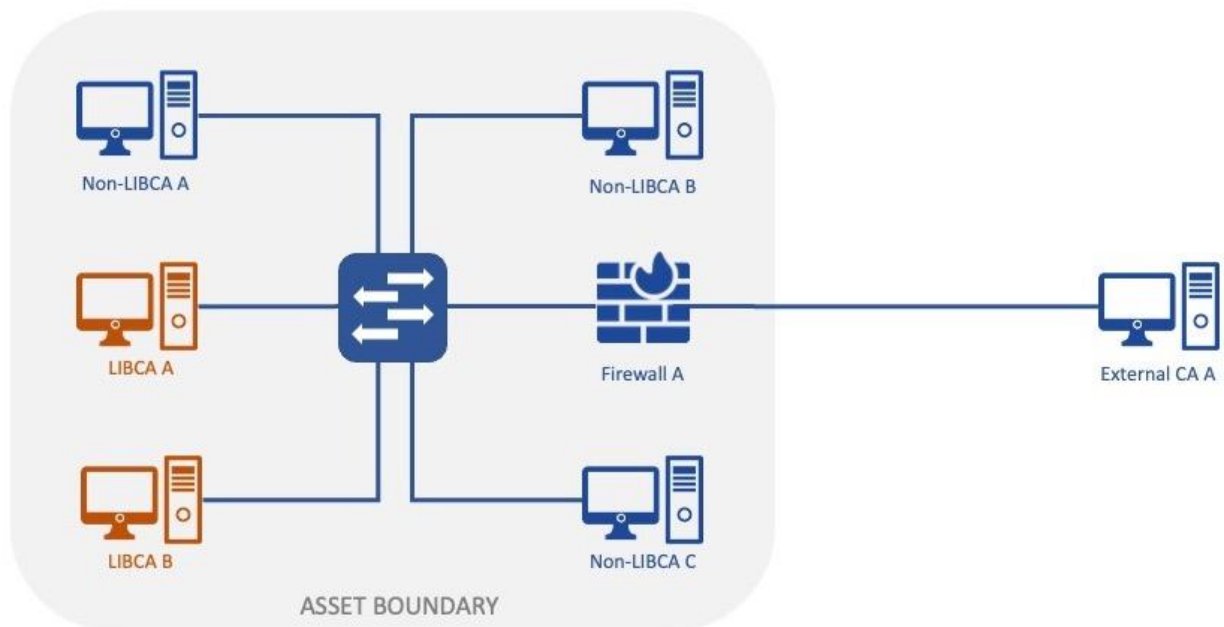



Fig. 4: Asset with Network Firewalling Device

Finally, the fourth example uses a dedicated network firewall, commonly associated with electronic access controls and prevalent in the CIP-005 ESP. While not expressly required to control electronic access to the LIBCS inside an asset, many entities find this way most efficient, particularly when paired with an enterprise-level firewall management system.

Summary of Examples

Electronic access modeling and visualization solutions, like [NP-View](#), will function most efficiently for networks similar to examples 3 and 4, as they operate at the OSI Layer 3 and above. However,



in cases similar to example 2, NP-View may also serve effectively when used with Nmap scans against or Netstat files from the cyber assets running host-based firewalls. For example 1, the entity must demonstrate that no routable communication exists within the asset.

The compliance obligations found in CIP-003-8 Attachment 1, Section 3, Electronic Access Controls work together. These controls form a single concept as each point relates inextricably to the others. Viewed in paragraph form, rather than in outline form, the interaction becomes clear.

For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to permit only necessary inbound and outbound electronic access as determined by the Responsible Entity[...].

[Applicable] communications [...] are [any communications] between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) [that use] a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s) [and are] not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR 61850-90-5 R-GOOSE).

In other words, systems need electronic access controls that deny by default for any Cyber Asset outside of an asset bi-directionally communicates to a LIBCS over routable protocols except for time-sensitive communications.

Audit Preparation Workflow

The following sections explain how to use NP-View to manage compliance with the important Section 3 obligations. These obligations start with wrapping the system in deny-by-default controls, then accounting for all routable communications that exist (both incoming and outgoing) between any LIBCS and a Cyber Asset beyond the asset boundary. Finally, entities may then exclude any time-sensitive communications from the electronic access controls. The audit preparation workflow below attempts to account for each example in every step.



Prerequisite Activities

The entity must fully describe each asset containing LIBCS and, therefore, the asset boundary. This work falls outside the scope of this whitepaper, but will almost certainly involve CIP-002. Evidence here remains most critical when presenting a non-routable asset. Use evidence stacking, or multiple confirming artifacts, to demonstrate the lack of routable protocols incoming or outgoing across the asset boundary.

As described in Attachment 2 of CIP-003-8, Section 3, such evidence may take the form of diagrams. However, this section, similar to the Measures of other CIP Standards, does not discuss how to “prove the negative” when no routable connections exist to systems external to the asset. Therefore, entities should prepare additional artifacts for these assets beyond just a simple diagram.

For instance, while CIP-003 does not require a list of LIBCA/LIBCS⁹, a list created for the purpose of stacking confirming evidence for the absence of what would ordinarily be considered External Routable Connectivity (ERC) becomes useful. A diagram shows the asset with its constituent cyber assets. The inventory for that asset, with accompanying vendor documentation, supports the contention that no asset has unknown or uncontrolled routable communication capabilities. Stacking evidence in this way only considers the natural questions an auditor might ask and seeks to provide comprehensive and ready answers.

⁹ [Lighthouse Consolidated](#); Reliability First, Lew Folkerth, pgs. 58 & 59

Please also note that all Cyber Assets categorized as LIBCA/LIBCS must implement electronic access controls. This includes access to the switches, routers, and firewalls themselves. Please consult the manufacturer for a guide to only allow administrative access to certain IP addresses.

Routable Protocols

While listed second, filtering routable protocols (see Table 3) provides an excellent starting point.

- i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
- ii. *using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s);*

Table 3: CIP-003-8 Attachment 1, Section 3 - routable protocol obligations

Type 1: Non-Routed

Many entities struggle for good network diagrams of assets with LIBCS. NP-View serves well in this capacity, to automatically create network diagrams.

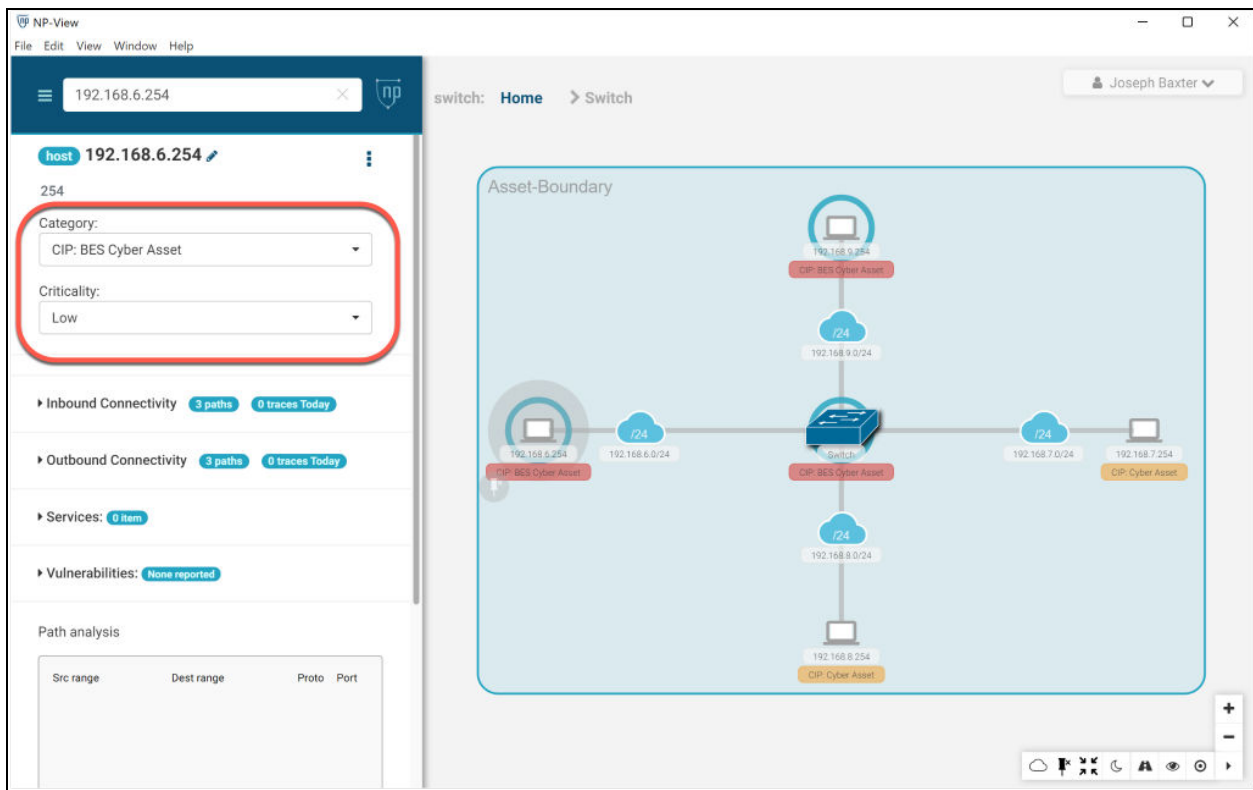


Figure 5: Example of a switched network topology diagram automatically generated by NP-View

1. Import the configuration file(s) of any switches or routers within the asset into NP-View. Blue clouds represent an IP subnet, each with its own CIDR network address, and may have a single VLAN assigned to it. In this example, all VLANs exist within the asset boundary. Be careful to locate the routing function device if utilizing VLANs, as it may indicate the existence of routable connection with an external cyber asset¹⁰.
2. Once the topology is constructed, import a simple (non-invasive) Nmap scan of the network collected on outage to populate hosts not identified within the switch or router configuration files. If an Nmap scan is not available or not advisable, an entity may make a documented manual inventory of the asset and import the resulting list to NP-View via a HOSTS.TXT file or ARP table export. Once added, ensure that all auxiliary data endpoints have been added to the custom view.
3. Select the LIBCA/LIBCS and mark their category as "CIP: BES Cyber Asset" and set the criticality rating as "Low" from the left hand information panel (see fig. 5).
4. Select all non-LIBCS cyber assets and mark their category as CIP: Cyber Asset.

¹⁰ [ERO Enterprise CMEP Practice Guide: Assessing Virtualized Networks](#); NERC, Feb. 26, 2021

5. Holding the Shift Key, multi-select all objects that reside within the asset boundary and create an NP-View Zone.
6. From the Search Bar Menu, select the command Export Map (see fig. 6).

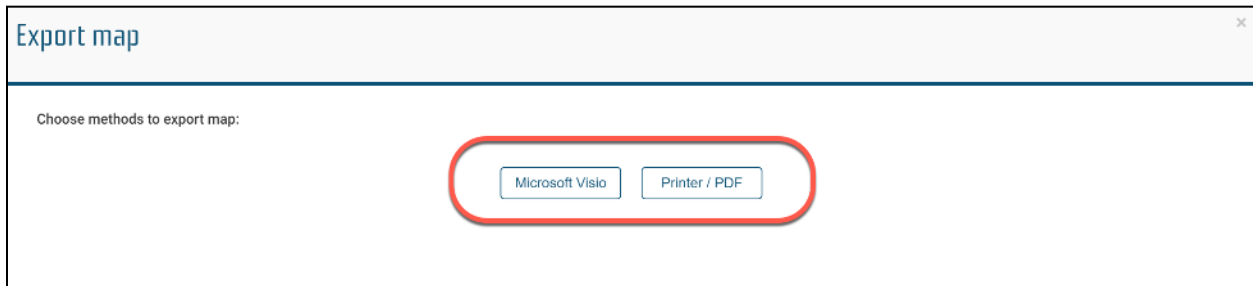


Figure 6: Options to export the topology diagram generated by NP-View to a Visio or PDF file.

Type 2: Wireless

An entity must carefully examine the subnet of the network against the boundary of the asset, as wireless presents an unusual arrangement between the physical and the logical.

- IF NO PATHS exist over routable protocols (wired or wireless) to cyber assets beyond the asset boundary, then follow the steps outlined ABOVE to document evidence for Type 1 networks.
 - IF ONE OR MORE PATHS exist over routable protocols (wired or wireless) to cyber assets beyond the asset boundary, then all LIBCS must implement and document electronic access controls.
1. Follow Steps 1-5 from the Type 1 procedure above.
 2. Export the configuration files for the Windows or Linux firewall policies. Archive these files for evidence.
 3. To demonstrate the listening and allowed ports on each LIBCA, particularly if implementing a host-based firewall, follow the Network Perception Knowledge Base article on [Auxiliary Data](#) to create a NETSTAT.TXT file for each LIBCA/LIBCS. Alternatively, under certain safe conditions (such as an outage), Nmap scans against the LIBCA/LIBCS host-based firewalls may be used.
 4. Import the NETSTAT.TXT or Nmap Scan files into the NP-View topology. This will help demonstrate the incoming ports allowed by the LIBCS. Evidence of outgoing ports for the LIBCS cannot be modeled in NP-View.

- Under the NP-View Search Bar Menu, go to Asset Inventory and turn on the Services column (see fig. 7). Export “All Visible Data to Excel” for comparison and evidence stacking with the host-based firewall policies.
- From the Search Bar Menu, select the command Export Map (see fig. 6).

Name	Type	Category	Criticality	Alias	IP Address
10.10.1.100	host				10.10.1.100
10.10.1.101	host				10.10.1.101
10.10.1.102	host				10.10.1.102
10.10.1.103	host				10.10.1.103
10.10.1.104	host				10.10.1.104
10.10.1.105	host				10.10.1.105
10.10.1.106	host				10.10.1.106
10.10.1.107	host				10.10.1.107
10.10.1.108	host				10.10.1.108

Figure 7: Adding services information to the asset inventory table within NP-View

Type 3: Routed

Simple routed networks do not control electronic access by default. Routers will forward all packets, both those desired and undesired, to their destination network subnets without any inspection. Therefore, the basic workflow will be similar to the above version for Wireless networks.

- IF NO ACLs exist to control electronic access over routable protocols to Cyber Assets beyond the asset boundary, then follow the steps outlined ABOVE to document evidence for Type 2 networks.
- IF STANDARD ACLs exist to control electronic access over routable protocols to Cyber Assets beyond the asset boundary, then follow the Type 3 network workflow steps.

- IF EXTENDED ACLs exist to control electronic access over routable protocols to Cyber Assets beyond the asset boundary, then follow the steps outlined BELOW to document evidence for Type 4 networks.

Standard Access Control Lists in traditional routers can filter by address but not address and port. Therefore, to demonstrate control of electronic access, additional steps must be taken.

1. Follow Steps 1-5 from the Type 1 procedure above.
2. Follow Steps 2-6 from the Type 2 procedure above.
3. Run the NP-View Best Practices report to review Deny by Default status.

Type 4: Firewalled

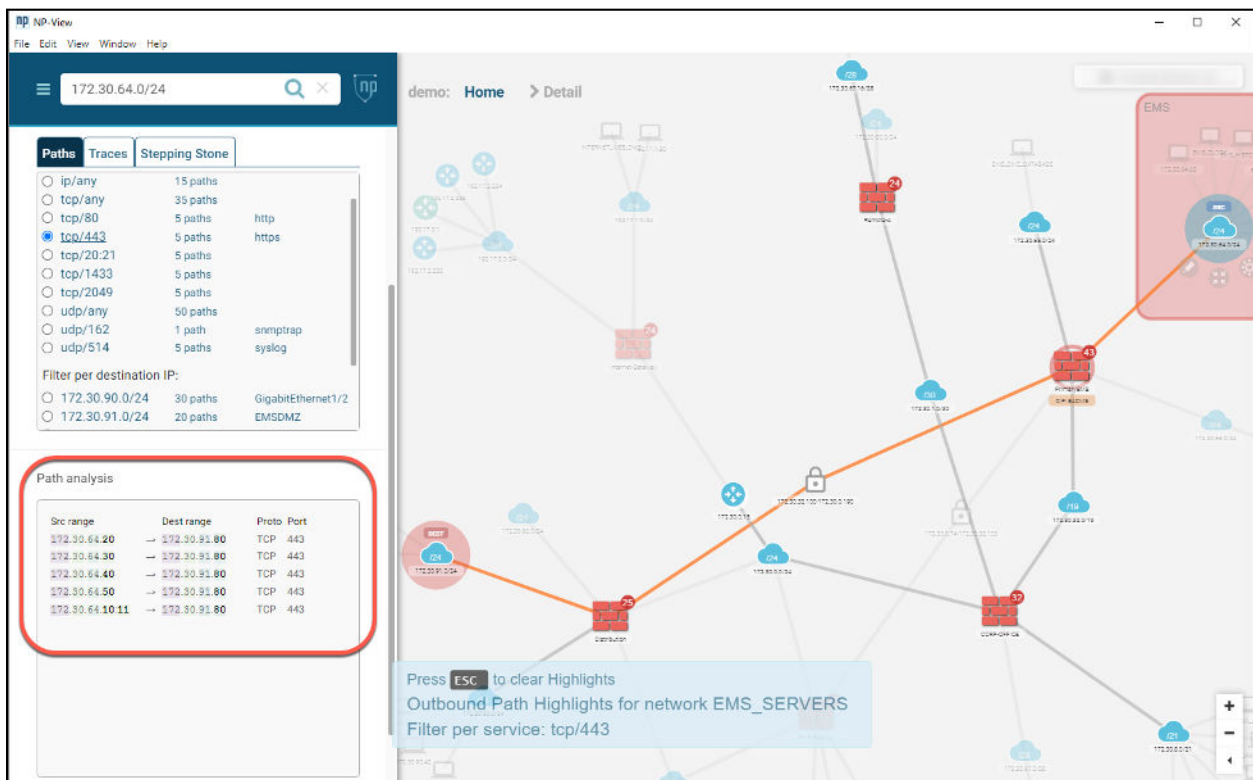


Figure 8: Network path analysis results represented inside NP-View for a network with multiple firewalls.

1. Follow Steps 1-5 from the Type 1 procedure above.
2. Select the asset boundary within the zone(s) created under the prior steps.
3. Using the path analysis functions, review the incoming and outgoing paths reported by NP-View (see fig. 8). Verify that all paths transit across an identified EAP.

- 4. Investigate any external paths that don't come through an EACMS.

Time-Sensitive Protocols

Use vendor documentation and support for full listing of TCP and UDP ports used by systems within the asset. Common ports to consider include, but are not limited to:

- TCP/502 for ModBusTCP
- TCP/102 for GOOSE/IEC-61850
- TCP/102 for Simatic S7

For evidence in the presence of time-sensitive protocols (see Table 4), network example 2 becomes very challenging. Electronic access controls on LIBCS that allow time-sensitive communications from outside of the asset without a firewall or router ACL, most commonly take the form of white-listing host-based firewalls on the LIBCS themselves. These host-based firewalls should be configured to allow only those ports needed for time-sensitive communications and only from the exact source and destination addresses needed.

- i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
- iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Table 4: CIP-003-8 Attachment 1, Section 3 - time-sensitive protocol obligations

Please remember that romanette iii serves as a negated sentence and is used to deduct any type of demonstrable real-time or time-sensitive protocols from the burden of electronic access control.

Type 1: Non-Routed

If no routable communications (including time-sensitive protocols) enters or leaves the asset, as demonstrated in the topology artifacts created in the prior section, no additional work must be completed here.

Type 2: Wireless

Without additional hardware or software, demonstrating time-sensitive protocols remains difficult for a PTP type of wireless network. Therefore, entities in this situation should follow the least risky

tactic possible, and create electronic access controls that INCLUDE Time-Sensitive protocols rather than trying to exclude them.

Type 3: Routed & Type 4: Firewalled

	Source	Destination	Service	Action	Description
+	172.30.64.42	172.30.70.42	IP/any to any	permit	**** BEGIN BKEMS VPN ACL ****
+	EMS_DMZ_DATABASE	any	IP/any to any	permit	**** BEGIN FromDMZ ACL - USING MIXED PROTOCOL GROUP****
+	any	any	IP/any to any	deny	**** BEGIN FromEMSCorp ACL ****
+	EMS	172.30.8.30	UDP/any to 514	permit	**** BEGIN FromINSIDE ACL **** Allow logs out to log management s
+	EMS_WAN_REMOTE	EMS	TCP/any to any	permit	**** BEGIN FromOUTSIDE ACL **** allow remote A access to EMS
+	EMS	DIST_EMS	IP/any to any	permit	**** Start DST VPN ACL*****
+	EMS	172.30.90.0/24	TCP/any to any	permit	ALLOW 8.4 Firewall access to EMS Wide network CIP example rules be
-	FMS	FMS WAN_REMOTE	TCP/any to any	permit	allow access to remote A

Row Count: 29

Figure 9: Access Rules Table

1. Excellent vendor documentation will play a key role in excluding time-sensitive protocols from the CIP-003 electronic access control program. Once the topology is built in NP-View using a router or firewall, the entity may use the Access Rules table to filter on sources, destinations, services, and even search for any time-sensitive communications paths.
2. As a final step, it is recommended to review any risks and warnings generated by NP-View. These risks and warnings originate from the NP-View policy manager and reflect potentially overly-permissive rules. Regarding time-sensitive communications, some - but not all - of the warnings raised may be acceptable in the context of LIBCS devices. However, these risks and warnings should still undergo review and documentation using the NP-View metadata features.
3. Use the Access Rules Table export button (see fig. 9) to bring the information to Excel for archiving to evidence.



About NP-View

NP-View is a software product developed by a team of networking and security experts at Network Perception. It works offline and generates a network topology diagram by analyzing configuration files from firewalls, routers, and switches. The interface design of NP-View allows users to easily identify and track overly-permissive network access policies, as well as recording justifications for rules, ports and services. If you have questions or would like to know more about NP-View, please contact the Network Perception team at:

+1 (872) 245-4100 | info@network-perception.com | <https://kb.network-perception.com>