

10
**Security Guideline for the Electricity Sector:
Identifying Critical Cyber Assets**

15

Preamble:

20
It is in the public interest for NERC to develop guidelines that are useful for improving the reliability of the Bulk Power System (BPS)¹. Guidelines provide suggested guidance on a particular topic for use by BPS users, owners, and operators according to each entity's facts and circumstances and are not to provide binding norms, establish mandatory reliability standards, or be used to create parameters by which compliance to standards is monitored or enforced.

25

This Guideline provides an approach to developing a list of Critical Cyber Assets essential to the reliable operation of Critical Assets. It builds on earlier guidance that provides a methodology to identify Critical Assets essential to the reliability and operability of the BPS.

30

Purpose:

This Guideline is intended to inform an entity on identification of Critical Cyber Assets as described in CIP-002 R3,

35

Applicability:

40
NERC Standard CIP-002 R3 requires that Responsible Entities develop a list of Critical Cyber Assets essential to the operation of the Critical Assets. This list is to be based on a list of Critical Assets created beforehand through a risk-based assessment methodology.

45

The term Critical Asset is defined in the NERC Glossary of Terms Used in Reliability Standards as: "Facilities, systems, and equipment which if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System" The term Critical Cyber Assets is defined in the NERC glossary as

50

¹ Note: For purposes of this document, the terms "Bulk Power System" and "Bulk Electric System" are considered to be identical.

55

“Cyber Assets essential to the reliable operation of Critical Assets.” This Guideline provides guidance for determining Critical Cyber Assets by evaluating potential impacts to “reliable operation” of a Critical Asset.

10

As further specified by the NERC CIP-002 Section 4.2, this guideline does not directly apply to facilities regulated by the U.S. Nuclear Regulatory Commission (NRC) or the Canadian Nuclear Safety Commission, with one exception described in FERC Order 706-B. In a nuclear facility, non-safety-related balance of plant equipment not subject to NRC cyber security regulations is subject to the NERC CIP standards. If a Responsible Entity determines that it has non-safety Critical Assets not subject to NRC cyber security regulations through application of a risk-based methodology as specified in CIP-002 R1, then this guideline is applicable to the determination of the Critical Cyber Assets for the identified Critical Asset.

15

20

In addition, this guideline does not apply to the identification of cyber assets that are directly associated with communication networks and data communication links between discrete Electronic Security Perimeters. Those assets are exempt from standard CIP-002.

25

Definitions:

30

NERC Glossary Terms Used:

- Critical Assets**
- Cyber Assets**
- Critical Cyber Assets**
- ESP
- PSP

35

Additional Terms Used in the Document Not Defined as NERC Glossary Terms:

40

Common Mode Impact – Impact on multiple components, systems, units or facilities with similar, same or related functions due to a single event.

45

Control Center – A control center is defined to perform one or more of the functions listed below for multiple (i.e., two or more) BPS assets such as generation plants and transmission substations. Functions of a control center typically include one or more of the following:

50

- Supervisory control of BPS assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems and automatic load-shedding systems
- Acquisition, aggregation, processing, inter-utility exchange, and display of BPS reliability or operability data.
- BPS and system status monitoring and processing for reliability and asset management purposes (e.g., for situational awareness)
- Alarm monitoring and processing
- Support for, or coordination of, BPS restoration activities

Control Room – A control room is typically located within the facility and operates control systems limited to controlling:

- A single generation plant with one or more generation units,
- A single transmission asset such as a transmission substation.

Adequate Level of Reliability – “The Bulk Power System (“System”) will achieve an adequate level of reliability when it processes the following characteristics:

1. The System is controlled to stay within acceptable limits during normal conditions;
2. The System performs acceptably after credible Contingencies;
3. The System limits the impact and scope of instability and Cascading outages when they occur;
4. The System’s Facilities are protected from unacceptable damage by operating them within Facility Ratings;
5. The System’s integrity can be restored promptly if it is lost; and
6. The System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.”²

² From NERC’s May 5, 2008 filing to FERC to define “Adequate Level of Reliability”. Additional information about each of the six characteristics is available at http://www.nerc.com/files/Adequate_Level_of_Reliability_Defintion_05052008.pdf.

Guideline Details:

Overall Approach

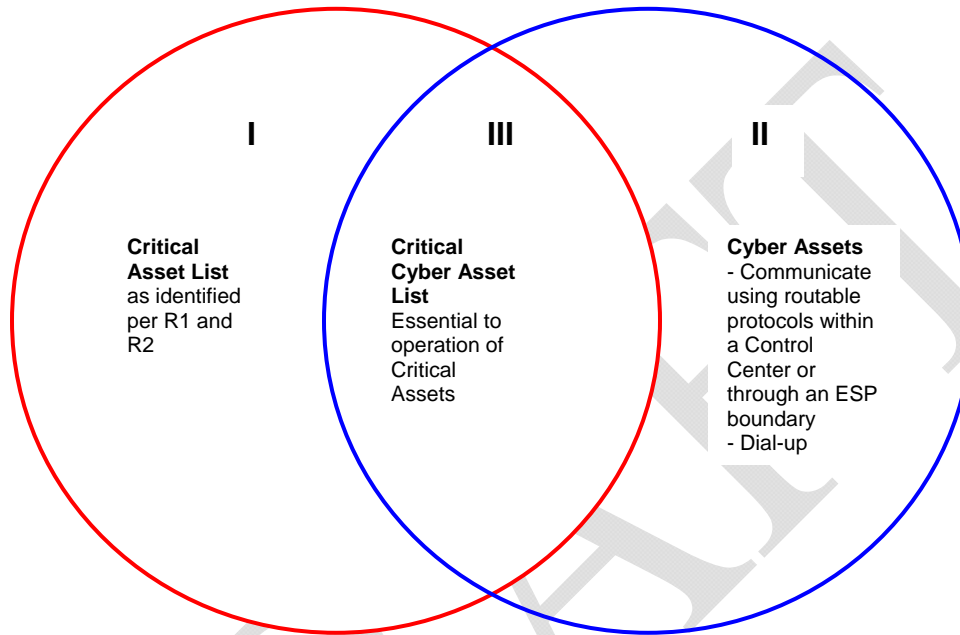
This Guideline defines a process to identify Cyber Assets at an entity's Critical Asset and to determine if these Cyber Assets are Critical Cyber Assets. This approach assumes that the Responsible Entity has already identified its Critical Assets and has defined the essential functions of those Critical Assets. Defining the essential functions of the Critical Asset helps determine whether any particular Cyber Asset is essential to the operation of the Critical Asset. Cyber Assets that are connected to support systems (such as environmental and continuous power systems) that are indirectly essential to the operation of the Critical Asset could also be addressed. The suggested process described in this guideline consists of the following five steps:

- A. Identifying Cyber Assets associated with a Critical Asset.
- B. Grouping Cyber Assets by application
- C. Identifying Cyber Assets supporting essential functions of Critical Assets
- D. Identifying Cyber Assets with CIP-002 R3 qualifying characteristics
- E. Compiling the list of Critical Cyber Assets.

Section A describes how to identify Cyber Assets associated with a Critical Asset and why a complete list is important. Section B describes grouping Cyber Assets by application and how it could assist in the overall determination of criticality. Section C describes how to assess the Cyber Assets and narrow the list based on identifying those Cyber Assets that support one or more essential functions. Section D describes the application of qualifying communications characteristics to further narrow the list. . Section E discusses compiling the final list of Critical Cyber Assets.

This approach assumes that an entity has a significant number of Cyber Assets that have qualifying connectivity. If this assumption is not true (for example, an entity has already identified a small number of Cyber Assets that meet the CIP-002 R3 characteristics), the steps could be performed in another order for efficiency (e.g. Step D could be substituted for Step A). The order of the steps is not as important as comprehensive identification of those Cyber Assets at the intersection of I and II (i.e. III) in Figure 1 – that is, Cyber Assets that support the Critical Asset's essential functions and meet the qualifying characteristics.

Figure 1 Critical Cyber Asset Venn Diagram



A. Identification of Cyber Assets Associated with a Critical Asset

An entity should first identify Cyber Assets associated with the operation of an identified Critical Asset. This is not intended to be a complete inventory³ of all Cyber Assets at the facility, but rather an evaluation and then identification of all Cyber Assets that may have direct or indirect impact on the essential function of a Critical Asset. Entities may want to perform complete inventories of Cyber Assets if there are questions about the nature of their impact on essential functions – this will ensure that all appropriate Cyber Assets have been considered in the assessment. A Cyber Asset is defined⁴ to be “Programmable electronic devices and communication networks including hardware, software and data.” For the purposes

³ Although a comprehensive Cyber Asset inventory would be helpful in supporting CIP-005-1

⁴ In the NERC *Glossary of Terms Used in Reliability Standards*

of this guideline, software, data and cabling are considered to exist within the framework of the Cyber Asset and therefore are not separate Cyber Assets.

10

In general Cyber Assets are digital elements that are part of either control systems, data acquisition systems, or the networking equipment used by a control or data acquisition system.

15

- Control systems comprise devices or sets of devices that act to manage, command, or regulate the behavior of processes, devices, or other systems.
- Data acquisition systems are a collection of sensors and communication links that act to sample, collect, and provide data regarding the plant systems to a centralized location for display, archiving, or further processing.
- Networking equipment includes devices such as routers, hubs, switches, firewalls, and modems.

20

Cyber Assets in secondary or supporting systems essential for the reliable operation of a Critical Assets or related Critical Cyber Assets may be considered:

25

- Installed Cyber Assets used in a standby mode or spare Cyber Assets which may be used during recovery and restoration
- Environmental systems such as heating, ventilation, and air conditioning (HVAC)
- Support systems such as uninterruptable power supplies (UPS) and alarm systems

30

The basis for this consideration should be supported by engineering walk downs and technical descriptions and drawings including topological diagrams showing the location and the relationship of Cyber Assets to the Critical Asset and the Cyber Asset's connectivity to other Cyber Assets.

35

When identifying Cyber Assets consider the different roles and functions that Cyber Assets play which might directly or indirectly affect the essential functionality of a Critical Asset such as:

40

- Provides operation information in real time
- Controls parameters manual or automated
- Calculates important parameters or limits
- Prompts or alarms
- Provides connectivity between Cyber Assets within the ESP
- Supports continuity of operations of the Critical Assets or local recovery plans

45

50

B. Application Based Grouping of Cyber Assets

Grouping Cyber assets by “application⁵ or system⁶” can be used to simplify the determination process. One might make the simplifying assumption that if an application or system supports an essential function, then by extension the Cyber Assets that play a role in the application function also support the essential function. For example if loss or compromise⁷ of a particular application can be shown to fail or degrade the essential function of a Critical Asset then it might be assumed that all the Cyber Assets that play a role in the function provided by the application could cause the same failure or degradation. Once the effect of the loss or compromise of an application or system is known then the effect of the loss or compromise of supporting Cyber Assets is assumed to be known.

C. Determination of Cyber Assets that are Essential

To determine whether Cyber Assets are essential, all essential functions of all Critical Assets should be identified prior to the evaluation of the associated Cyber Assets. If a Cyber Asset is associated with, exists within the boundaries of, or is connected to the Critical Asset but has no impact on the essential function or functions of the Critical Asset, then it can be removed from further consideration as a Critical Cyber Asset.

Cyber Assets should be considered essential to a Critical Asset if any one of the following criteria are met:

1. The Cyber Asset is involved in, or capable of, supervisory or autonomous control that supports an essential function of a Critical Asset
2. The Cyber Asset displays, transfers, or contains information used to make real time operational decisions that supports an essential function of a Critical Asset
3. The Cyber Asset if lost would degrade the essential function of a Critical Asset.

⁵ The term “application” is used here to mean digital application software that functions and is operated by means of a computer, with the purpose of supporting functions needed by an asset owner.

⁶ The term system is used here to mean computer program and corresponding hardware that performs a specific set of functions and may have a user interface.

⁷ The term compromise is meant to include misuse.

4. The Cyber Asset if compromised could impact the essential function of a Critical Asset

Loss, degradation, or compromise of a Cyber Asset can lead to loss of confidentiality, integrity or availability of data or system function. Loss of confidentiality means that unauthorized disclosure of information has occurred. Loss of integrity means that the state of a system or data in a system has been modified in an unauthorized manner. Loss of availability means that the function of a system or asset has been impeded.

The concepts of degradation and compromise are used in specific ways in this Guideline. In Criterion #3 above, the term “would degrade” means that loss of the Cyber Asset would not immediately fail the essential function of the Critical Asset but would fail its function over time if not recovered. The time from initial degradation to failure of the essential function is situational and should be considered in use of this criterion. Similarly the time necessary to recover should also be considered.

In Criterion #4 above, the term “compromised” means that information or control is modified in a way to produce an undesirable outcome that impacts the essential function of the Critical Asset. The purpose of including Criterion #4 is to promote consideration of possible effects beyond just loss of the Cyber Asset.

The criteria presented above, in the form of questions, can be used to determine whether a Cyber Asset supports Critical Asset essential functions. Tables B-1, B-2, B-3 and B-4 illustrate this approach. These example tables present questions to ask for each of the four criteria. These questions, as presented, are directed at applications or systems, rather than Cyber Assets, based on the assumption that the Cyber Assets are grouped as described in Section B of this guideline. If an application or system supports a Critical Asset essential function (i.e. If the answer is “Yes” to any of these questions) then the cyber assets supporting the application or system could be designated Critical Cyber Assets.

In general, environmental or support systems for Critical Cyber Assets do not require the same protection as the associated Critical Cyber Asset⁸. However, it is suggested that evaluation of Cyber Assets include consideration of secondary support systems HVAC and UPS if their loss or compromise can lead to degradation (as defined in this Guideline). Asset owners are encouraged, whenever possible, to provide environmental or support systems with the same protection as their associated Critical Cyber Asset. Similar protections should be given to voice

⁸ Per NERC CIP-002-1 FAQ-12 at:

http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.pdf

10 systems and private branch exchange (PBX) systems as appropriate. If the support systems are network-connected (e.g., on the same LAN segment) to the Critical Cyber Assets, they must be afforded the same protection given Critical Cyber Assets required in other Cyber Security Standards.

15 Redundancy should not be considered to reduce the criticality of any Cyber Asset. Redundancy will only affect availability and reliability while not improving integrity or information confidentiality and may in fact increase the Cyber Asset's exposure to a cyber attack. For the purpose of security, each Critical Cyber Asset and redundant Critical Cyber Asset must be protected under the Cyber Security Standards as Critical Cyber Assets.

Table C-1 Example Determination of Cyber Assets Supporting Essential Functions for Transmission Substations

Critical Asset: Transmission Substation					
Essential Functions⁹ (EFs): 1. Essential to BPS restoration. 2. Essential to critical generation for the BPS. 3. Essential for voltage support on the BPS 4. Essential for frequency support on the BPS. 5. Essential for BPS stability.					
Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
Telemetry	No (Does not provide supervisory control.)	Yes (Provides real-time information to Control Center.)	Yes	Yes	1,2,5
Remote Terminal Unit (RTU)	Yes (Provides input, monitoring and control for Control Center SCADA.)	Yes (Provides real-time information to Control Center; may provide local alarming, monitoring and short term historical information.)	Yes	Yes	1,2,5
Substation automation system (normally comprised of multiple Cyber Assets)	Yes (Provides local SCADA and RTU function to the Control Center.)	Yes (Provides information to staff that operate or maintain substation equipment.)	Yes	Yes	1,2,3,4,5

⁹ Based on Column 2 of Table C-1 of the NERC Critical Asset identification guideline

10

15

20

25

30

35

40

45

Critical Asset: Transmission Substation					
Essential Functions⁹ (EFs): 1. Essential to BPS restoration. 2. Essential to critical generation for the BPS. 3. Essential for voltage support on the BPS 4. Essential for frequency support on the BPS. 5. Essential for BPS stability.					
Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
Protective relaying	Yes (Performs real-time protection function; may provide monitoring and historical information)	Yes (Normally provides power system monitoring and historical information locally into substation automation system and Control Center.)	Yes	Yes	1,2,3,5
Special protection systems (SPS/RAS) – the remote end	Yes (SPS master or remote system end providing autonomous control.)	No (Normally provides control and not information used to make real-time decisions.)	Yes	Yes	3,4,5
Phasor Measurement Unit (PMU ¹⁰)	No (In the future may provide input for control actions at Control Center.)	No (In the future may provide wide area monitoring (WAM) for Control Centers.)	No	No	1,5

¹⁰ NERC has not yet acknowledged these systems as there are no current implemented applications.

10

15

20

25

30

35

40

45

Critical Asset: Transmission Substation					
Essential Functions⁹ (EFs): 1, Essential to BPS restoration. 2. Essential to critical generation for the BPS. 3. Essential for voltage support on the BPS 4. Essential for frequency support on the BPS. 5. Essential for BPS stability.					
Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
Historical long-term database supporting offsite storage.	No (Does not affect real-time operation.)	No (Provided short-term storage is available to support monitoring and logging functions as required by CIP-002 through CIP-009.	No	No	n/a
Fault Recorders	No	No	No (Important but not critical to BPS)	No	n/a
Equipment monitoring	No	No	No (Important but not critical to BPS)	No	n/a
Digital networks that connects control functions between assets within a single ESP	<u>Yes</u>	<u>Yes</u>	<u>Yes</u>	<u>Yes</u>	1,2,3,4,5

Table C-2 Example Determination of Cyber Assets Supporting Essential Functions for a Generation Resource

Critical Asset: Hydro Generator					
Essential Functions¹¹ (EFs): 1. Essential to generation for the BPS. 2. Essential to known constraint mitigation for the BPS including voltage support and frequency response. 3. Essential to BPS Restoration.					
Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
Main turbine speed digital control	Yes (Controls key parameters)	Yes (Display key control parameters)	Yes (Loss of the Cyber Asset could produce out-of-limit conditions that could over time fail the essential function)	Yes (Manipulation of control parameters could directly impact the essential function)	1,2,3
Seal water flow digital control to Main turbine	Yes (Controls key parameters)	No (Does not display, inform, prompt or store key control parameter information)	Yes (If seal is not supplied by manual or remote manual control, then bearing temperatures will increase to failure)	Yes (Manipulation that causes inadequate flow can have the same effect as no flow)	1,2,3

¹¹ Based on Column 2 of Table C-2 of the NERC Critical Asset identification guideline

10	Engineering workstation access to main turbine set-points.	No (Cannot affect supervisory control)	No (Is that the primary display or information used in real-time decision making)	Yes (Key set-points can be altered to produce out-of-limit conditions that could over time fail the essential function)	Yes (Set points could be altered produce a trip of the turbine)	1,2,3
15	Turbine trending analysis database	No (not used in control)	No (Not used in real-time decision)	No	No	1,2,3
20	Electrical generator efficiency calculator	No (Does not calculate or control parameters that can affect the essential function)	No (Does not calculate display, inform, prompt or store information related to essential functions control parameters)	No	No	n/a
25	Digital networks that connects control functions between assets within a single ESP	<u>Yes</u>	Yes	<u>Yes</u>	<u>Yes</u>	1,2,3

30

35

40

45

10

Critical Asset: Coal-Fired Generating Plant**Essential Functions¹² (EFs):**

1, Essential to generation for the BPS.

2. Essential to known constraint mitigation for the BPS including voltage support and frequency response.

15

Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
Integrated Plant Control System (integrated turbine, steam generator, treatment controls)	Yes (Controls key parameters)	Yes (Display key control parameters)	Yes (Displays and controls that support an essential function)	Yes	1,2
Continuous Emissions Monitoring System (CEMS)	No (not used in supervisory or autonomous control impacting the essential functions)	No (Does not display, inform, prompt or store key control parameter information)	No (No other essential functions supported)	No	None
Turbine control system	Yes (Sets set-points for key control parameters)	Yes (Displays key control parameters)	Yes (controls essential function)	Yes	1,2
Main feedwater control system	Yes (Controls key parameters)	No (does not display key control parameters)	Yes (controls support an essential function)	Yes	1,2

35

40

¹² Based on Column 2 of Table C-2 of the NERC Critical Asset identification guideline

45

10

15

20

25

30

35

40

45

Critical Asset: Coal-Fired Generating Plant					
Essential Functions¹² (EFs): 1, Essential to generation for the BPS. 2. Essential to known constraint mitigation for the BPS including voltage support and frequency response.					
Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
Digital networks that connects control functions between assets within a single ESP	Yes	Yes	Yes	Yes	1,2,3,4

Table C-3 Example Determination of Cyber Assets Supporting Essential Functions for a Control Center

Critical Asset: Control Center					
Essential Functions ¹³ (EFs):					
1, Essential by virtue of their functions supporting reliability or operability of the BPS 2, Essential for providing information used by Responsible Entities to make operational decisions regarding the reliability and operability of the BPS. 3, Essential for inter-utility data exchange critical to reliable BPS operation. 4, Essential for control or data acquisition for a BPS asset determined to be a Critical Asset 5, Essential for control center functionality for a set of BPS assets determined collectively to be critical to reliability and operability of the BPS.					
Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
SCADA Supervisory Control	Yes	Yes (Information required to perform control function)	Yes (Direct control of a Critical Asset or a set of assets determined collectively to be critical to reliability and operability of the BPS)	Yes	4,5
SCADA Alarms	No	Yes	Yes (Real-time alarm data used to make operational decisions)	Yes (Compromise could allow an attacker to either suppress actual alarms or generate spurious alarms)	1,2,3,4,5

¹³ Based on Column 2 of Table C-3 of the NERC Critical Asset identification guideline

10

15

20

25

30

35

40

45

Critical Asset: Control Center					
Essential Functions¹³ (EFs): 1, Essential by virtue of their functions supporting reliability or operability of the BPS 2. Essential for providing information used by Responsible Entities to make operational decisions regarding the reliability and operability of the BPS. 3. Essential for inter-utility data exchange critical to reliable BPS operation. 4. Essential for control or data acquisition for a BPS asset determined to be a Critical Asset 5. Essential for control center functionality for a set of BPS assets determined collectively to be critical to reliability and operability of the BPS.					
Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
SCADA/ICCP Applications	Yes (in some instances)	Yes	Yes (ICCP functions handle exchange and processing of data used to make operational decisions, <i>may</i> be used for remote control)	Yes (Compromise could allow an attacker to manipulate data in a manner that caused operations personnel to make incorrect operational decisions)	1,2,3,4,5
State Estimation	No	Yes	Yes (Provides information to control center operators used to make operational decisions)	Yes (Compromise could allow an attacker to manipulate data in a manner that caused operations personnel to make incorrect operational decisions)	1,2

10

15

20

25

30

35

40

45

Critical Asset: Control Center					
Essential Functions¹³ (EFs):					
1, Essential by virtue of their functions supporting reliability or operability of the BPS					
2. Essential for providing information used by Responsible Entities to make operational decisions regarding the reliability and operability of the BPS.					
3. Essential for inter-utility data exchange critical to reliable BPS operation.					
4. Essential for control or data acquisition for a BPS asset determined to be a Critical Asset					
5. Essential for control center functionality for a set of BPS assets determined collectively to be critical to reliability and operability of the BPS.					
Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
Voltage Stability Analysis	No	Yes	Yes (Provides information to control center operators used to make operational decisions)	Yes (Compromise could allow an attacker to manipulate data in a manner that caused operations personnel to make incorrect operational decisions)	1,2
Digital networks that connects control functions between assets within a single ESP	<u>Yes</u>	Yes	<u>Yes</u>	<u>Yes</u>	1,2,3,4,5

Table C-4 Example Determination of Cyber Assets Supporting Essential Functions for a Special System

Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
Special protection systems (SPS/RAS)	Yes (SPS master or remote system end providing autonomous control.)	No (Normally provides control and not information used to make real-time decisions.)	Yes	Yes	1,2,3
Protection System (Could be a CA, CCA or grouped CCAs)	Yes (Reference to systems identified in PRC standards) Operates as protective controls	No (Depends if autonomous action also provides information)	Yes	Yes	<u>1</u>
Under frequency load shedding (UFLS) (Includes aggregation and/or centralized control or common component)	Yes	No (Depends if autonomous action also provides information)	Yes	Yes	<u>2</u>

¹⁴ Based on Column 2 of Table C-4 of the NERC Critical Asset identification guideline

Critical Asset: Special System						
Essential Functions¹⁴ (EFs):						
10	1. Essential Remedial Action Scheme/Special Protection System that supports the reliability or operability of the BPS 2. Essential to automatic load shedding supporting the reliability or operability of the BPS. 3. Essential Demand-Side Management or Direct Control Load Management that supports the reliability or operability of the BPS. 4. Essential by virtue of their functions supporting reliability or operability of the BPS.					
15	Applications or systems using cyber elements	<i>Used in supervisory or autonomous control impacting the essential function?</i>	<i>Used in display, transfer or contains information used to make real-time decisions impacting the essential function?</i>	<i>Would the Cyber Asset if lost degrade the essential function of the Critical Asset?</i>	<i>Could the Cyber Asset if compromised impact the essential function of a Critical Asset?</i>	EFs
20	UVLS Includes aggregation and/or centralized control or common component)	Yes	No (Depends if autonomous action also provides information)	Yes	Yes	2
25	DSM/DCLM (Includes aggregation and/or centralized control or common component)	Yes	No (Depends if autonomous action also provides information)	Yes	Yes	3
30	DSM (Does not Include centralized control or common component)	No	Yes (Information provided to influence individual customers)	No	Yes (Common mode failure for aggregate group of assets large enough to affect BPS)	3
35	Dynamic feeder rating system (Includes aggregation and/or centralized control or common component)	Yes	Yes (Normally provides continuous information)	Yes (Depends on implementation or contingency occurring)	Yes (Depends on implementation or contingency occurring)	4

40

45

10

Critical Asset: Special System**Essential Functions¹⁴ (EFs):**

1. Essential Remedial Action Scheme/Special Protection System that supports the reliability or operability of the BPS
2. Essential to automatic load shedding supporting the reliability or operability of the BPS.
3. Essential Demand-Side Management or Direct Control Load Management that supports the reliability or operability of the BPS.
4. Essential by virtue of their functions supporting reliability or operability of the BPS.

15

Applications or systems using cyber elements

*Used in supervisory or autonomous control impacting the essential function?**Used in display, transfer or contains information used to make real-time decisions impacting the essential function?**Would the Cyber Asset if lost degrade the essential function of the Critical Asset?**Could the Cyber Asset if compromised impact the essential function of a Critical Asset?*

EFs

20

Digital networks that connects control functions between assets within a single ESP

Yes

Yes

Yes

Yes

1,2,3,4

25

30

35

40

45

D. Identification of Cyber Assets with Qualifying Connectivity

10

Standard CIP-002-1 R3 further qualifies Critical Cyber Assets as those assets that meet any of the following qualifying connectivity requirements:

15

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

20

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

25

If the steps were done in the order suggested by this Guideline this step would reduce the potential list of Critical Cyber Assets to those that have the qualifying connectivity. (This step might be done first.)

30

Determining whether or not a Cyber Asset meets either the second or third qualifying characteristic (routable protocol within a control center or dial-up accessible) will generally be a simple, one-step exercise. However, determining whether or not a Cyber Asset uses a routable protocol to communicate outside an Electronic Security Perimeter will generally require multiple steps, including defining a preliminary ESP.

35

One approach to defining a preliminary ESP that may be useful is to examine network drawings and address plan information for the site in question (e.g., plant or substation). If the Cyber Assets being evaluated are connected to a network with an IP address that is unique to that site, then there should generally be at least one router or similar Layer 3 networking¹⁵ device linking that network to other local or wide-area networks. That router (or routers) can then be considered as being the access points of a preliminary Electronic Security Perimeter. Determining whether the qualifying requirement of CIP-002-1 Requirement R3.1 applies then becomes a matter of asking whether or not the Cyber Assets within the preliminary Electronic Security Perimeter either send routable traffic to or receive routable traffic from other networks through the default ESP's access points.

40

45

It should be noted that any Cyber Asset that uses a routable protocol connection to a device outside the ESP or within a control center, even if it is dual homed equipment or behind a data concentrator (e.g. terminal server, or going from a routable to non-routable protocol converter), should be considered to have qualifying connectivity.

50

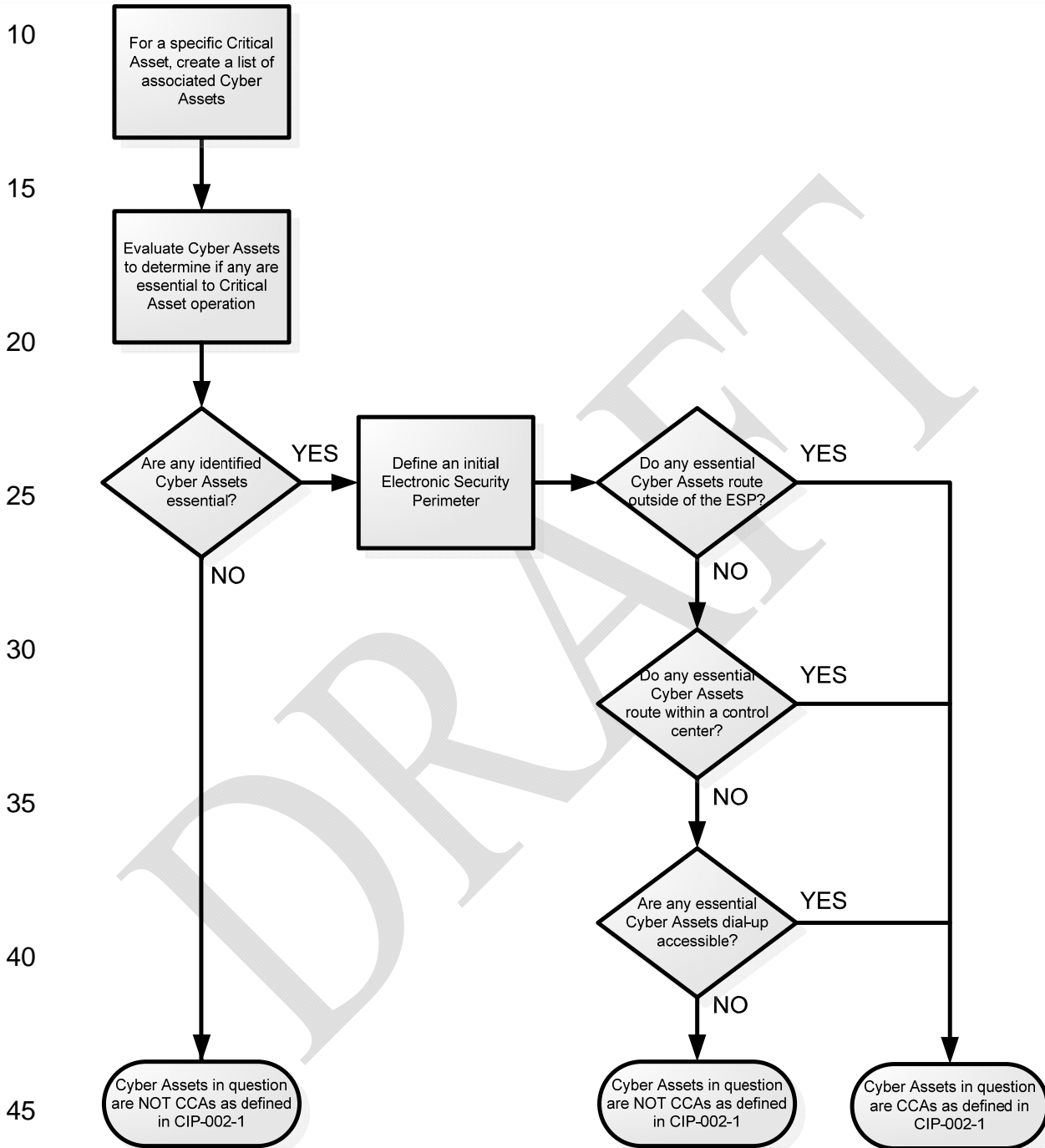
¹⁵ Per the Open System Interconnection reference model Layer 3 and the NERC Frequency Asked Questions No. 6 for Standard CIP-002-1.

10 Figure 2, below, illustrates a process that could be used to determine whether Cyber Assets determined to be essential to the operation of a particular Critical Asset (or set of Critical Assets) meet any of the qualifying characteristics of CIP-002-1 R3.

15 Figure 3 illustrates how that process might be modified in cases where a Responsible Entity elects to identify Cyber Assets with qualifying connectivity as the first step in its overall process of identifying Critical Cyber Assets.

20 Attachment 1 provides example configurations of essential-to-Critical-Asset and not-essential-to-Critical-Asset Cyber Assets connected by routable protocols. These configurations are considered to represent the different possible arrangements of dial-up and ESP access points, ESP boundaries and position within or outside a Control Center. Suggested Critical Cyber designations for Cyber Assets because they are considered to meet one of the qualifying characteristic defined in R3.1, R3.2 and R3.3 are given for each of nine cases.

Figure 2. Evaluating CIP-002-1 R3 Qualifying Communication Characteristics



10

15

20

25

30

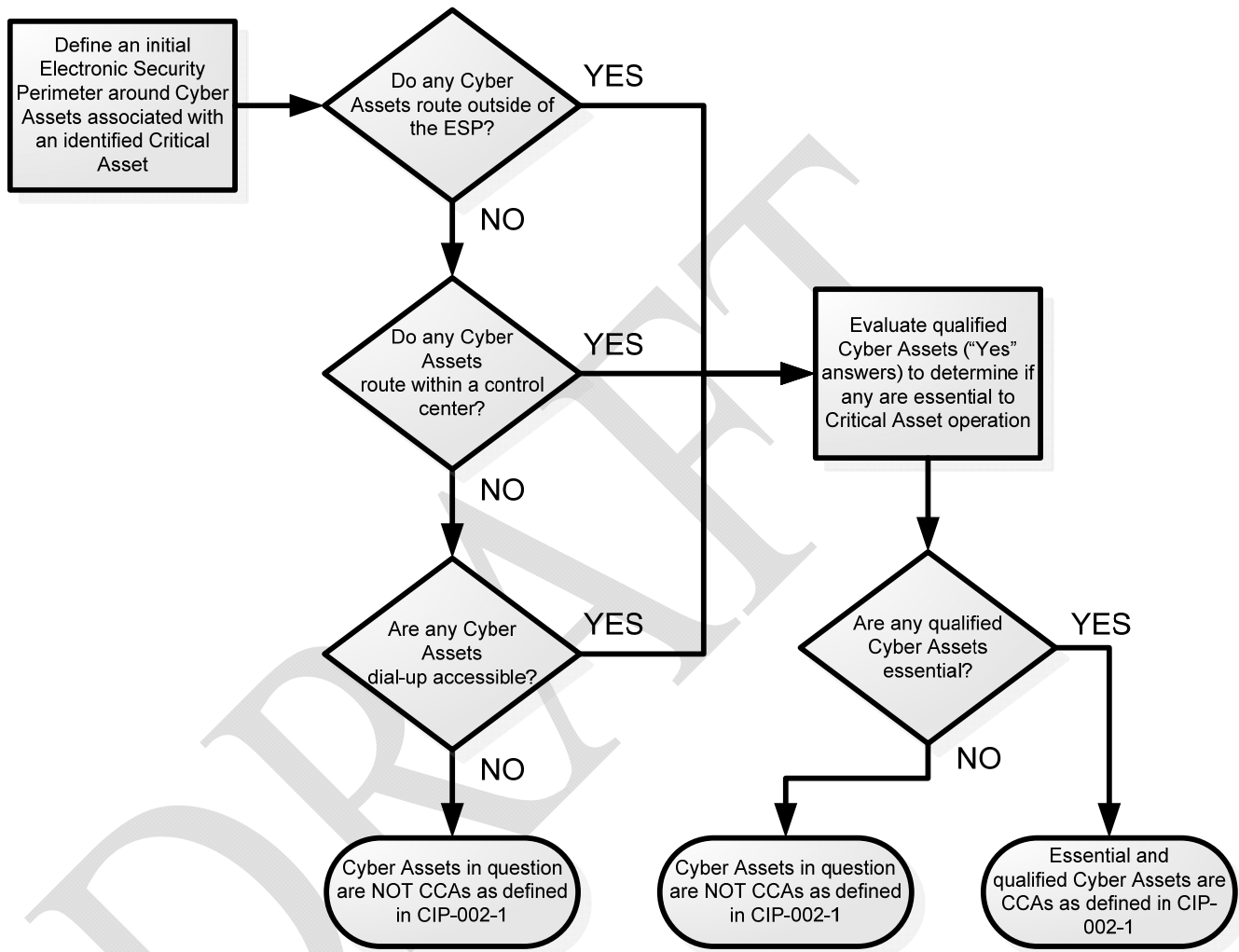
35

40

45

50

Figure 3. Evaluating CIP-002-1 R3 Qualifying Communication Characteristics as the First Step in Overall CCA Identification Process



E. Compilation of the List of Critical Cyber Assets

After narrowing down the complete list of Cyber Assets to only those that are both essential to a Critical Asset and meet the qualifying connectivity criteria, a final list of Critical Cyber Assets should be compiled and documented. An example list of Critical Cyber Assets and supporting information in that determination is shown in Attachment 2.

Related Documents and Links:

10

NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, July 2002.

15

<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

NERC CIP Guideline, *Control System – Business network Electronic Connectivity*, Critical Infrastructure Protection Committee, North American Electric Reliability Corporation, May 2005.

20

http://www.esisac.com/publicdocs/Guides/SecGuide_ElectronicSec_BOTapprvd3may05.pdf

NERC Glossary of Terms Used in Reliability Standards, May 2007.

25

http://www.nerc.com/files/Glossary_12Feb08.pdf

30

35

40

45

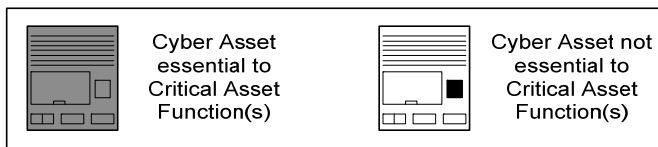
50

55

Attachment 1

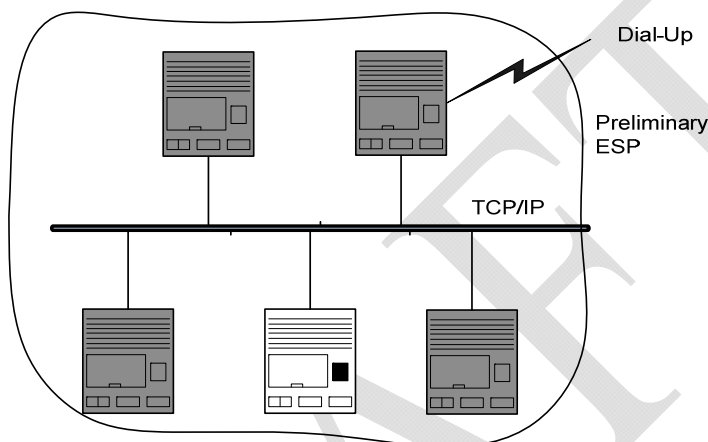
Interpretation of Qualification per CIP-002-1 R3 for Example Configurations

10



15

20

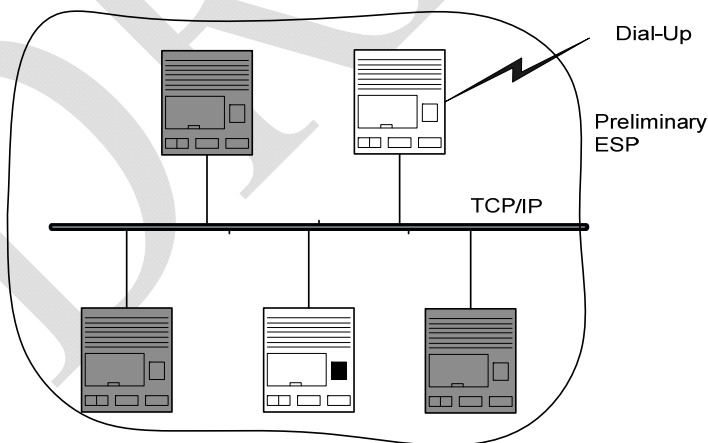


25

30

(1) Cyber Assets on an autonomous LAN outside of a Control Center communicate with each other using a routable protocol. One essential Cyber Asset is dial-up accessible and is therefore a Critical Cyber Asset per CIP-002-1 R3.3. We assume that it might be possible to gain access to the dial-up host and then to other Cyber Assets on the LAN, therefore all essential Cyber Assets shown should be identified as Critical Cyber Assets.
 NOTE: If dial-up access is removed, none of these Cyber Assets are Critical Cyber Assets per current CIP-002 R3 qualifiers.

35

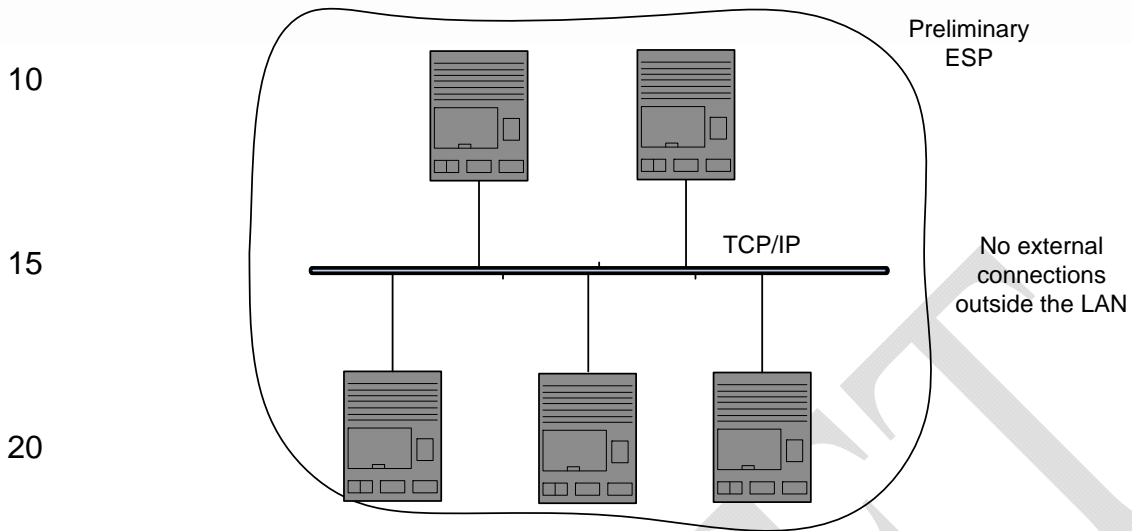


40

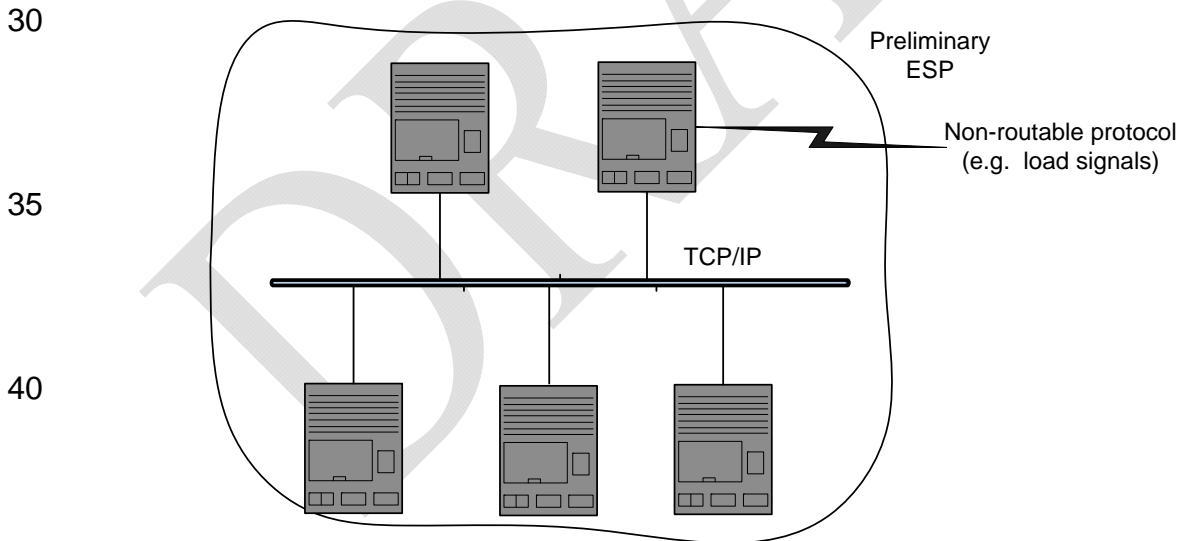
45

(2) Cyber Assets on an autonomous LAN outside of a Control Center communicate with each other using a routable protocol. One non-essential Cyber Asset is dial-up accessible. We assume that it might be possible to gain access to the dial-up host and then to other Cyber Assets on the LAN, therefore all essential Cyber Assets shown should be identified as Critical Cyber Assets.
 NOTE: If dial-up access is removed, none of these Cyber Assets are Critical Cyber Assets per current CIP-002-1 R3 qualifiers.

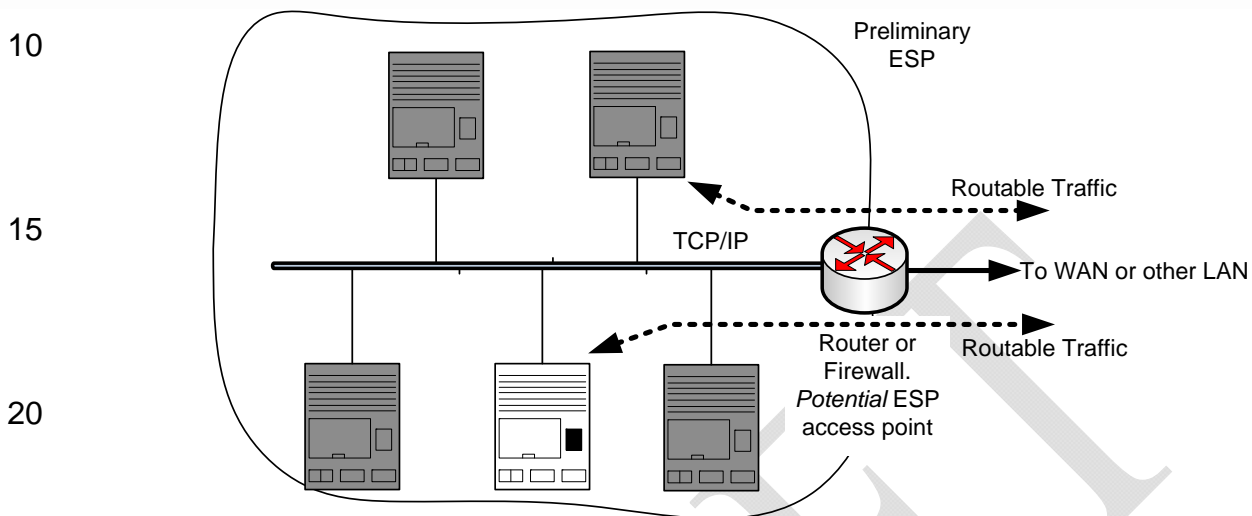
50



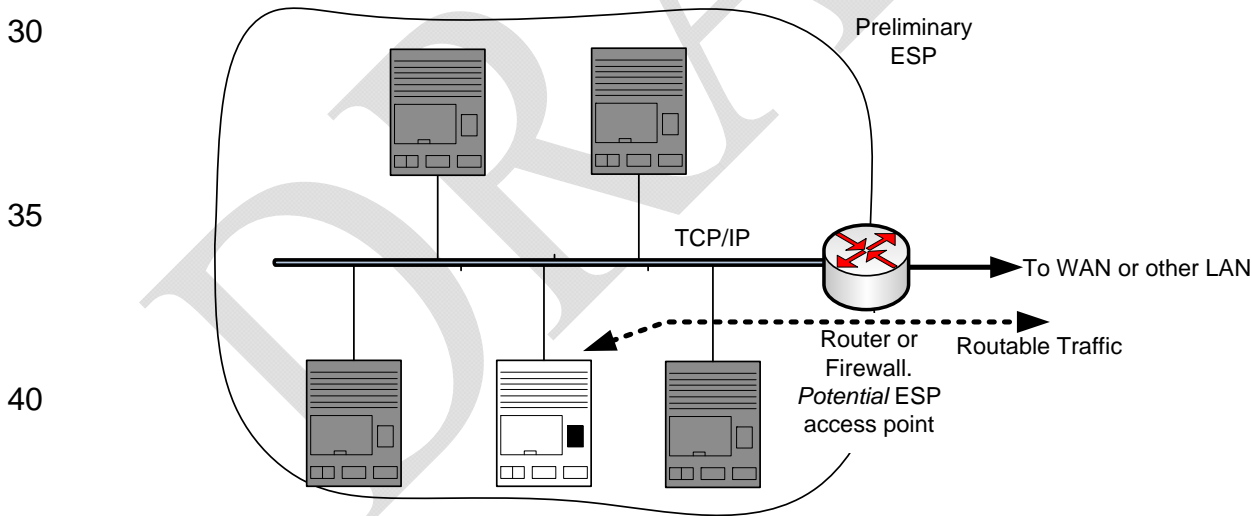
(3) Essential Cyber Assets on an autonomous LAN outside of a Control Center communicate with each other using a routable protocol. There are no external connections of this network to allow routable protocol communications outside the preliminary ESP. Therefore, these Cyber Assets are not Critical Cyber Assets.



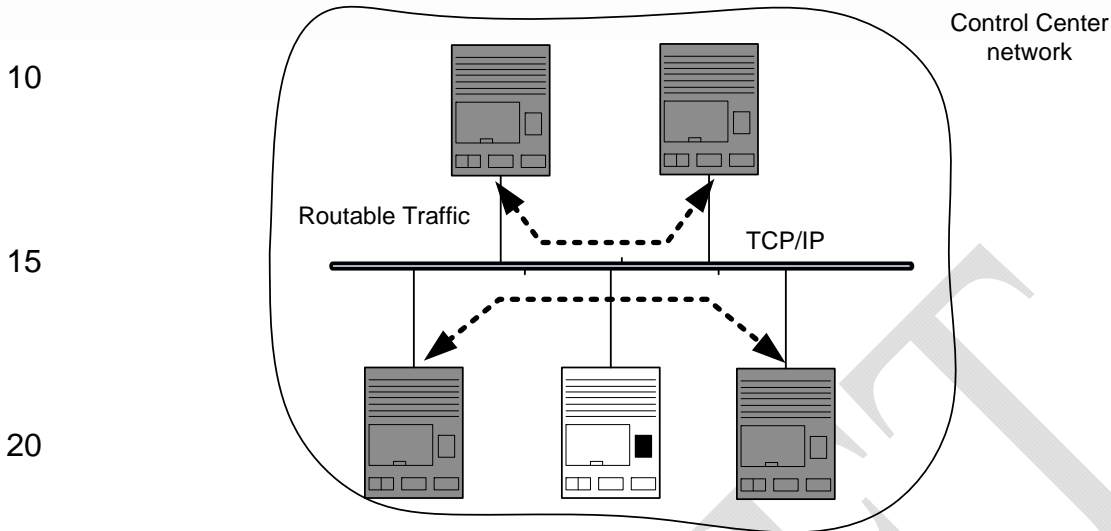
(4) Essential Cyber Assets on an autonomous LAN outside of a Control Center communicate with each other using a routable protocol. One essential cyber asset communicates outside the preliminary ESP using a non-routable protocol. This is the only connection outside the preliminary ESP. Since this does not meet the criteria of CIP-002-1 R3.1 or R3.3, the Cyber Assets are not Critical Cyber Assets.



(5) Cyber Assets on a LAN outside of a Control Center communicate with each other and with systems on WAN or other LAN using a routable protocol. Essential Cyber Assets are Critical Cyber Assets per CIP-002-1 R3.1 based on preliminary ESP design. The fact that the essential Cyber Assets communicate outside the ESP using a routable protocol qualifies them as Critical Cyber Assets.



(6) Cyber Assets on a LAN outside of a control center communicate with each other using a routable protocol. Only non-essential Cyber Assets communicate with systems on WAN or other LAN. The fact that the essential Cyber Assets could communicate outside the ESP using a routable protocol or could be reached from outside via a non-essential Cyber Asset qualifies them as Critical Cyber Assets.



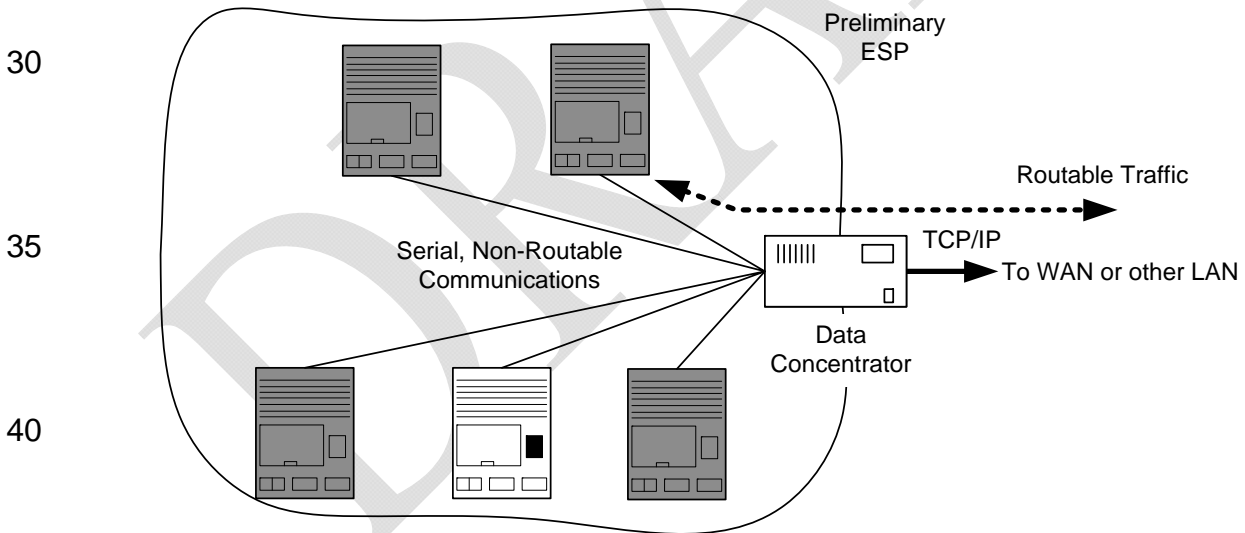
10

15

20

(7) Cyber Assets on a LAN within a Control Center communicate with each other using a routable protocol. Essential Cyber Assets are Critical Cyber Assets per CIP-002-1 R3.2. NOTE: Communication outside the Control Center is not a consideration for Critical Cyber Asset identification.

25



30

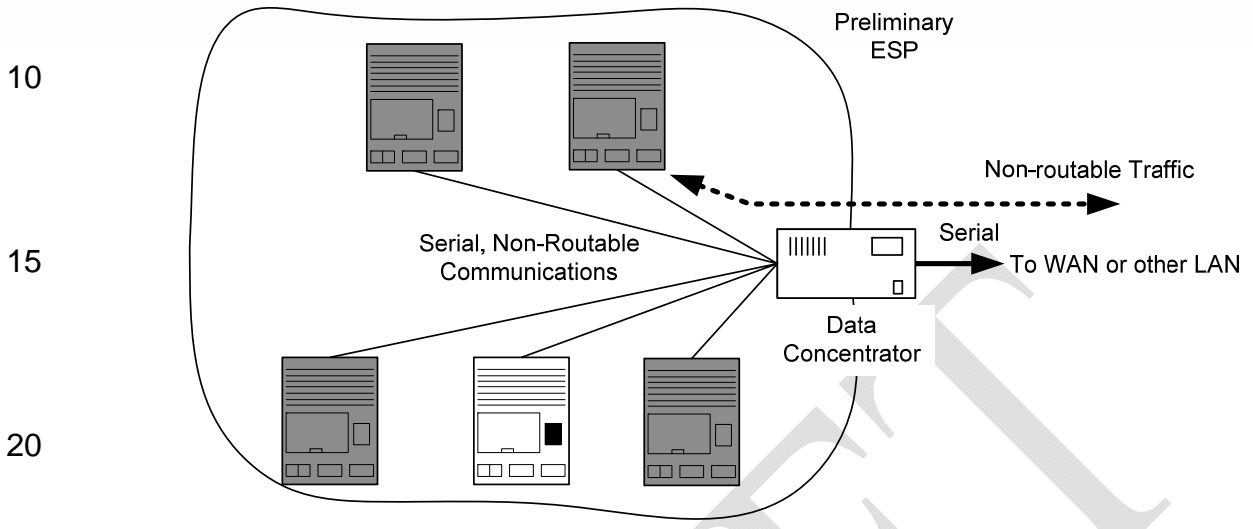
35

40

(8) Cyber Assets outside of a Control Center communicate to remote systems (e.g., SCADA) via a data concentrator that performs protocol conversion and communicates outside preliminary ESP using a routable protocol. Essential Cyber Assets are Critical Cyber Assets per CIP-002-1 R3.1. The fact that the essential Cyber Assets communicate outside the ESP using a routable protocol qualifies them as Critical Cyber Assets.

45

50



(9) Cyber Assets outside of a Control Center communicate to remote systems (e.g., SCADA) via a data concentrator that communicates outside preliminary ESP using a non-routable protocol. Essential Cyber Assets are not Critical Cyber Assets. The fact they communicate outside the preliminary ESP using a non-routable protocol removes them from consideration as Critical Cyber Assets.

Attachment 2 Example Cyber Inventory List

10

15

20

25

30

35

40

Cyber Asset	Network Address	Application or Function	Associated Critical Asset	Used in supervisory or autonomous control impacting the essential function?	Used in display, transfer or contains information used to make real-time decisions impacting the essential function?	Would the Cyber Asset if lost degrade the essential function of the Critical Asset?	Could the Cyber Asset if compromised impact the essential function of a Critical Asset?	Routable Protocol Outside An ESP?	Routable Protocol within a Control Center ?	Dial-up Accessible?	Critical Cyber Asset?
(Entity-specific identifier)	192.168.5.8	SCADA Supervisory Control - Primary Server	Primary Control Center	Supervisory Control	Yes	Yes	Yes	No	Yes	No	YES
(Entity-specific identifier)	192.168.5.9	SCADA Supervisory Control - Backup Server			Yes	Yes	Yes	No	Yes	No	YES
(Entity-specific identifier)	192.168.5.10	State Estimator - App Server			Operational Decision Support	Yes	Yes	No	Yes	No	YES
(Entity-specific identifier)	192.168.5.11	State Estimator - DB Server			No	Yes	Yes	No	Yes	No	YES
(Entity-specific identifier)	192.168.5.25	Print Server		None	N/A	N/A	No	No	Yes	No	NO

45

Revision History:

10

Date	Version Number	Reason/Comments
9/18/08	0.0	Initial version in NERC template
10/03/08	0.1	Results of October 3rd 2008 RAWG teleconference.
10/23/08	0.2	Results of October 23 rd 2008 RAWG teleconference.
10/30/08	0.3	Results of October 30th 2008 RAWG teleconference.
03/09/09	0.4	Results of March 9th 2009 RAWG teleconference.
04/03/09	0.5	Results of April 3th 2009 RAWG teleconference.
04/17/09	0.6	Results of April 17th 2009 RAWG teleconference.
04/24/09	0.7	Results of April 24th 2009 RAWG teleconference.
05/08/09	0.8	Results of May 8th 2009 RAWG teleconference.
05/15/09	0.9	Results of May 15th 2009 RAWG teleconference.
05/22/09	0.901	Results of May 22nd 2009 RAWG teleconference.
06/05/09	0.902	Results of June 5th 2009 RAWG teleconference.

15

20

25

30

35

40

45

50