NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline for the Electricity Sector:
Identifying Critical Cyber Assets

Disclaimer:

This Guideline may explain or facilitate implementation of reliability standard CIP-002 – Cyber Security – Critical Cyber Asset Identification, but does not contain mandatory requirements subject to compliance review.

Preamble:

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.

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.

Purpose:

This Guideline is intended to assist a Responsible Entity in identifying Critical Cyber Assets as described in CIP-002 R3. In this Guideline references to CIP-002 refer to CIP-002-1, CIP-002-2 and CIP-002-3.

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

Applicability:

NERC Standard CIP-002 R3 requires that Responsible Entities develop a list of Critical Cyber Assets essential to the operation of its Critical Assets, which in turn have been previously identified through a risk-based assessment methodology.

The term Critical Assets is defined in the *NERC Glossary of Terms Used in Reliability Standards* ("NERC Glossary") 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 "Cyber Assets essential to the reliable operation of Critical Assets." This Guideline provides guidance for identifying Critical Cyber Assets by evaluating potential impacts to "reliable operation" of a Critical Asset.

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-nuclear-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, through application of a risk-based methodology as specified in CIP-002 R1 that it has non-safety Critical Assets not subject to NRC cyber security regulations, then this Guideline is applicable to the determination of the Critical Cyber Assets for the identified Critical Asset.

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 (ESPs). Those assets are exempt from standard CIP-002.

Definitions:

NERC Glossary Terms Used:

Automatic Generation Control
Bulk Electric System
Critical Assets
Cyber Assets
Critical Cyber Assets
Electronic Security Perimeter (ESP)
Facility

Physical Security Perimeter (PSP)
Special Protection System (SPS)
Real-time
Remedial Action Scheme (RAS)
Wide Area

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

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

Compromise - The misuse or unauthorized modification of a Cyber Asset or supporting system.

Degradation - Decline in the quality of performance of the Cyber Asset or supporting system.

Loss – Complete unavailability of the Cyber Asset or supporting system.

Control Center – A Control Center is capable of performing 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 that support Real-time operations of a Control Center typically include one or more of the following:

- 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, or display of BPS reliability and/or operability data, used for Real-time operations
- BPS and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing specific to operation and restoration functions
- Coordination of BPS restoration activities

Guideline Details:

Overall Approach

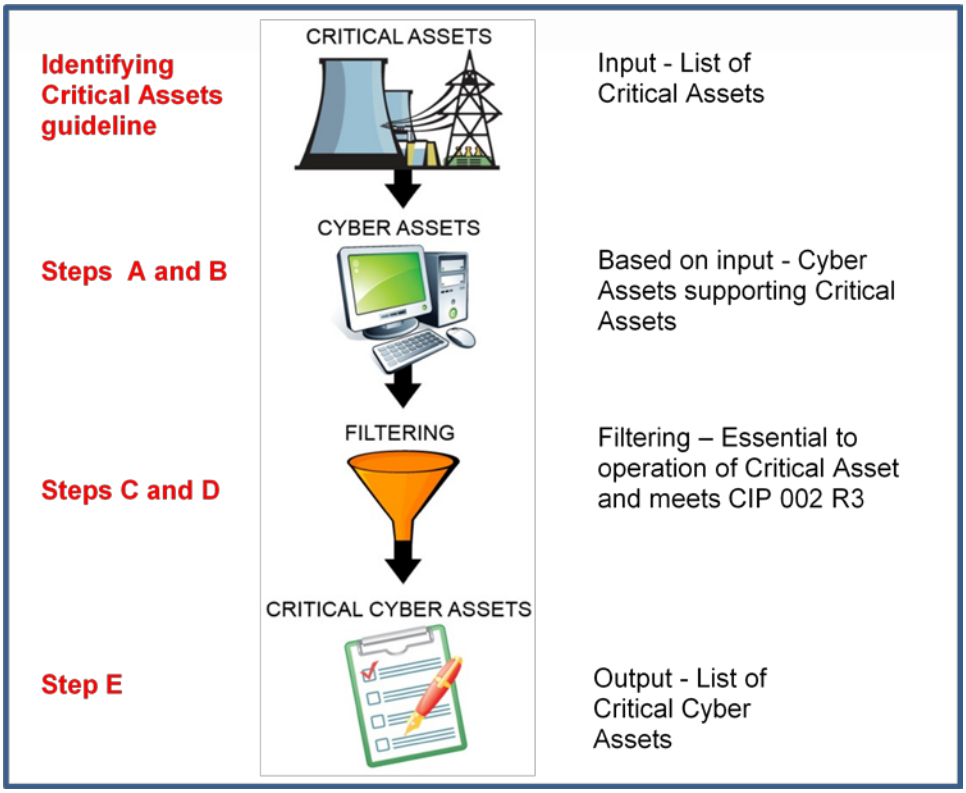
This Guideline is intended to assist Responsible Entities in developing a process for identification of Cyber Assets associated with its Critical Assets and to determine if these Cyber Assets are Critical Cyber Assets. This approach assumes that the Responsible Entity has already identified its Critical Assets and the essential functions of those Critical Assets as described in the earlier Guideline, "Security Guideline for the Electricity Sector: Identifying Critical Assets". Understanding the functionality that makes a particular BPS asset critical can help in identifying Cyber Assets that are essential to reliable operation of the Critical Asset. Cyber Assets that are connected to support systems (such as environmental, continuous power, or alarm systems) that support the operation of the Critical Cyber Assets could also be addressed. The process described in this Guideline consists of the following five steps:

A. Identify Cyber Assets associated with a Critical Asset
B. Group Cyber Assets
C. Determine Cyber Assets which are essential
D. Identify Cyber Assets with qualifying connectivity
E. Compile the list of Critical Cyber Assets

Section A describes how to identify Cyber Assets associated with a Critical Asset and why a complete list of Cyber Assets is important. Section B describes grouping Cyber Assets by application and how this 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 of a Critical Asset. Section D describes the application of qualifying connectivity requirements to further narrow the list. Section E discusses compiling the final list of Critical Cyber Assets.

This approach assumes that a large percentage of the Responsible Entity's Cyber Assets have qualifying connectivity as described in Section D of this document. If this assumption is not true (for example, a Responsible Entity has already determined that only a small percentage of its Cyber Assets meet the CIP-002 R3 characteristics), the steps could be performed in another order for efficiency (e.g., Step D could be exchanged with Step A). The order of the steps is not as important as the comprehensive identification of affected Cyber Assets. The determination process flow described in this Guideline is shown in Figure 1.

Figure 1 Critical Cyber Asset Determination



A. Identify Cyber Assets Associated with a Critical Asset

A Responsible Entity should first identify Cyber Assets associated with the operation of each identified Critical Asset. This is not intended to be a complete inventory[2] of all Cyber Assets at the facility, but rather an evaluation and then identification of all Cyber Assets that could impact the reliable operation of a Critical Asset. Responsible Entities may want to perform complete inventories of Cyber Assets if there are questions about the nature of their impact on reliable operation. This will ensure that all appropriate Cyber Assets have been considered in the assessment. Because Cyber Assets are defined to be "[p]rogrammable electronic devices and communication networks including hardware, software, and data.", software, data and cabling are considered to exist within the framework of the Cyber Asset and therefore are not separate Cyber Assets themselves.

[2] Although a comprehensive Cyber Asset inventory would be helpful in supporting CIP-005-1 compliance

Cyber Assets that should be considered include, at a minimum:

- Control systems comprising devices or sets of devices that act to manage, command, or regulate the behavior of processes[3], devices, or other systems
- Data acquisition systems comprising collections of sensors and communication links that act to sample, collect, and provide data regarding the facility's systems to a centralized location for display, archiving, or further processing
- Networking equipment including devices such as routers, hubs, switches, firewalls, and modems
- Hardware platforms running virtual machines or virtual storage

When identifying Cyber Assets, the entity should consider the different roles and functions that Cyber Assets play which could impact the reliable operation of a Critical Asset such as:

- Provides operation information in Real-time
- Controls manual or automated parameters
- Calculates parameters or limits
- Generates or displays prompts or alarms to an operator
- Provides connectivity between Cyber Assets
- Supports continuity of operations of the Critical Assets or local recovery plans

Consideration of Cyber Assets in secondary or supporting systems whose Loss, Degradation, or Compromise impacts both operation of Critical Cyber Asset(s) and their associated Critical Asset(s) is suggested. These secondary or supporting systems may include:

- Cyber Assets deployed in installed standby mode or installed spare Cyber Assets which may be used during recovery and restoration
- Stand alone virus and malware scanners, archival, backup and restore systems, and log monitoring systems (except Cyber Assets used in the access control and/or monitoring of the ESP or Physical Security Perimeter)
- Environmental systems such as heating, ventilation, and air conditioning (HVAC)
- Support systems such as uninterruptable power supplies (UPS) and alarm systems

The basis for this consideration may be supported by engineering walk downs[4] and technical descriptions and drawings including topological diagrams showing the

[3] Processes and systems that contribute to the successful function of the Critical Asset like cooling systems or lube oil systems should not be overlooked.

location and the relationship of Cyber Assets to the Critical Asset and the Cyber Assets' connectivity to other Cyber Assets.

B. Group Cyber Assets

In addition to applying the general guidance provided in Section A, entities may find it helpful in the Critical Cyber Asset identification process to consider grouping Cyber Assets as a way to simplify the process. Cyber Assets might be grouped according to the computer application software they communicate with in support of a function associated with a Critical Asset. Another grouping might be Cyber Assets associated with a specific operational function that supports a Critical Asset.

For example, if Loss, Degradation, or Compromise of a particular computer software application can be shown to fail or degrade reliable operation of a Critical Asset, then it might be assumed that all the Cyber Assets that play a role in the function provided by the computer software application could cause the same failure or Degradation. Once the effect of the Loss, Degradation, or Compromise of a grouping of Cyber Assets is known, then the effect of the Loss, Degradation or Compromise of supporting Cyber Assets can be assumed to be known.

C. Determine Cyber Assets Which are Essential

To determine whether Cyber Assets are essential, their impact on the reliable operation of a Critical Asset should be evaluated. If a Cyber Asset is associated with or is connected to a Critical Asset, but has no impact on the reliable operation of the Critical Asset, then it can be removed from further consideration as a Critical Cyber Asset. Cyber Assets that have any impact require further consideration.

A Cyber Asset could be considered essential to the reliable operation of a Critical Asset, if one or more of the following criteria is met:

1. The Cyber Asset participates in, or is capable of, supervisory or autonomous control that is essential to the reliable operation of a Critical Asset.

2. The Cyber Asset displays, transfers, or contains information relied on to make Real-time operational decisions that are essential to the reliable operation of a Critical Asset.

[4] An engineering walk down is an inspection where an engineer or team walks through a plant, following pipes, cable trays and other equipment with blueprints to confirm that the existing condition matches what is described in plant documentation.

3. The Cyber Asset fulfils another function essential to the reliable operation of the associated Critical Asset and its Loss, Degradation, or Compromise would affect the reliability or operability of the BPS.

The concepts of Loss, Degradation, and Compromise are used in specific ways in this Guideline. In Criterion #3, the term "Loss" means that the loss of the Cyber Asset would have an immediate adverse impact on the reliable operation of the Critical Asset. The term "Degradation" means that the Cyber Asset is not fully functional and could adversely impact the reliable operation of a Critical Asset. The term "Compromise" means that information or control is modified in a way to produce an undesirable outcome that impacts the reliable operation of the Critical Asset.

The criteria presented, in the form of questions, can be used to determine whether a Cyber Asset is essential to the reliable operation of a Critical Asset. Tables C-1, C-2, C-3 and C-4 illustrate this approach. These example tables present questions to be asked for each of the three 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 reliable operation of a Critical Asset (i.e., if the answer to any of these questions is "Yes") then the Cyber Assets supporting the application or system could be designated as Critical Cyber Assets.

Environmental (e.g., HVAC) or other support systems (e.g., UPS) for Critical Cyber Assets do not always require the same protection as the associated Critical Cyber Asset.[5] However, it is suggested that evaluation of Cyber Assets include consideration of these secondary support systems if their Loss, Degradation, or Compromise can impact both operation of Critical Cyber Assets and their associated Critical Assets(s). For example, Loss or Compromise of HVAC can lead to Loss, Degradation or Compromise of a Critical Cyber Asset which in-turn cause the Critical Asset to unacceptably affect the reliability or operability of the BPS. Similar consideration should be given to voice systems and private branch exchange (PBX) systems, as appropriate, based on the functions they perform. Note that if the support systems are within the same ESP as a Critical Cyber Asset, they must be afforded the same protection given Critical Cyber Assets required in other Cyber Security Standards.

Redundancy is not a factor in the determination of the criticality of any Cyber Asset; instead redundancy used to improve reliability and availability may indicate that each redundant Cyber Asset is critical.[6] Because redundancy may increase the

[5] Per NERC CIP-002-1 FAQ-12 at: http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.pdf.
[6] Per NERC CIP-002-1 FAQ-5 at: http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.pdf.

opportunities for a successful cyber attack, each Critical Cyber Asset and redundant Critical Cyber Asset should be protected under the Cyber Security Standards as Critical Cyber Assets.

Table C-1 Example Determination of Cyber Assets Supporting Reliable Operations for Transmission Substations

Critical Asset: Transmission Substation				
Essential functions (EFs) found in Column 2 of Table C-1 of *Security Guideline for the Electrical Sector: identifying Critical Assets*: 1. Essential to BPS restoration. 2. Essential to critical generation for the BPS. 3. Essential for voltage or frequency support or stability of the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays, transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
Telemetering	No (Does not provide supervisory control.)	Yes (Provides Real-time information to Control Center.)	Yes	1,2,3
Remote Terminal Unit (RTU)	Yes (Provides input, monitoring and control for Control Center Supervisory Control and Data Acquisition (SCADA).)	Yes (Provides Real-time information to Control Center; may provide local alarming, monitoring and short term historical information.)	Yes	1,2,3
Substation automation system (normally comprised of multiple Cyber Assets)	Yes (Provides local SCADA, process control, and RTU function to the Control Center.)	Yes (Provides information to staff that operate or maintain substation equipment.)	Yes	1,2,3

Critical Asset: Transmission Substation				
Essential functions (EFs) found in Column 2 of Table C-1 of *Security Guideline for the Electrical Sector: identifying Critical Assets*: 1. Essential to BPS restoration. 2. Essential to critical generation for the BPS. 3. Essential for voltage or frequency support or stability of the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays, transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	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	1,2,3
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	3
Phasor Measurement Unit (PMU[7])	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	1,3

[7] NERC has not yet acknowledged these systems as there are no current implemented applications.

Critical Asset: Transmission Substation				
Essential functions (EFs) found in Column 2 of Table C-1 of *Security Guideline for the Electrical Sector: identifying Critical Assets*: 1. Essential to BPS restoration. 2. Essential to critical generation for the BPS. 3. Essential for voltage or frequency support or stability of the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays, transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	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	None
Fault Recorders	No	No	No (Important but not critical to BPS.)	None
Equipment monitoring	No	No	No (Important but not critical to BPS.)	None
Computer networks that connects control functions between assets within a single ESP	Yes	Yes	Yes (Failures due to Common Mode Impact for an aggregate group of assets large enough to affect BPS.)	1,2,3
Revenue Meter	No	No	No	None

Critical Asset: Transmission Substation				
Essential functions (EFs) found in Column 2 of Table C-1 of *Security Guideline for the Electrical Sector: identifying Critical Assets*: 1. Essential to BPS restoration. 2. Essential to critical generation for the BPS. 3. Essential for voltage or frequency support or stability of the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays, transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
Station computer	Yes (Runs an algorithm related to autonomous control.)	Yes	Yes	1,2,3
Station computer HMI	Yes	Yes	Yes	1,2,3

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

Critical Asset: Hydro Generator				
Essential functions(Efs) found in Column 2 of Table C-2 of the *Security Guideline for the Electrical Sector: Identifying Critical Assets:* 1. Essential generation for the BPS. 2. Essential to mitigate known BPS constraint(s), including voltage or frequency support or stability. 3. Essential to BPS Restoration.				
Applications or systems using cyber assets	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays, transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
Main turbine speed computer control	Yes (Controls key parameters.)	Yes (Display key control parameters.)	Yes (Loss or manipulation of control parameters could impact reliable operations immediately or over time.)	1,2,3
Seal water flow computer control to Main turbine	Yes (Controls key parameters.)	No (Does not display, inform, prompt or store key control parameter information.)	Yes (Loss or manipulation of seal water flow could impact reliable operations immediately or over time.)	1,2,3
Engineering workstation access to main turbine set-points.	No (Cannot affect supervisory control.)	No (Is not the primary display of information used in Real-time decision-making.)	Yes (Key set-points that are altered could produce out-of-limit conditions that could impact reliable operations immediately or over time.)	1,2,3

Critical Asset: Hydro Generator				
Essential functions(Efs) found in Column 2 of Table C-2 of the *Security Guideline for the Electrical Sector: Identifying Critical Assets:* 1. Essential generation for the BPS. 2. Essential to mitigate known BPS constraint(s), including voltage or frequency support or stability. 3. Essential to BPS Restoration.				
Applications or systems using cyber assets	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays, transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
Turbine trending analysis database	No (Not used in control.)	No (Not used in Real-time decision.)	No	None
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	None
Computer networks that connects control functions between assets within a single ESP	Yes	Yes (Failures due to Common Mode Impact for an aggregate group of assets large enough to affect BPS.)	Yes	1,2,3
Revenue Meter	No	No	No	None

Critical Asset: Coal-Fired Generating Plant				
Essential functions (Efs) found in Column 2 of Table C-2 of *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets:* 1. Essential to generation for the BPS. 2. Essential to mitigate known BPS constraint(s), including voltage or frequency support or stability. 3. Essential to BPS Restoration.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
Integrated Plant Control System (integrated turbine, steam generator, water treatment controls)	Yes (Controls key parameters.)	Yes (Display key control parameters.)	Yes (Displays and controls that support an essential function.)	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.)	None
Turbine control system	Yes (Sets set-points for key control parameters)	Yes (Displays key control parameters)	Yes (controls essential function)	1,2
Main feed water control system	Yes (Controls key parameters.)	No (Does not display key control parameters.)	Yes (Controls support an essential function.)	1,2

Critical Asset: Coal-Fired Generating Plant				
Essential functions (Efs) found in Column 2 of Table C-2 of *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets:* 1. Essential to generation for the BPS. 2. Essential to mitigate known BPS constraint(s), including voltage or frequency support or stability. 3. Essential to BPS Restoration.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
Computer networks that connect control functions between assets within a single ESP	Yes (Failures due to Common Mode Impact for an aggregate group of assets large enough to affect BPS.)	Yes	Yes (Manipulation of aggregate control function could impact reliable operations.)	1,2,3
Revenue Meter	No	No	No	None

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

Critical Asset: Control Center				
Essential functions (Efs) found in Column 2 of Table C-3 of *Security Guideline for the Electricity Sector: Identifying Critical Assets:* 1. Essential by virtue of their functions supporting reliability or operability of the BPS. 2. Essential for providing information used by a Responsible Entity to make Real-time operational decisions regarding the reliability and operability of the BPS. 3. Essential for Real-time 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 to collectively impact reliability and operability of the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
SCADA Supervisory Control	Yes	Yes (Information required to perform a 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.)	4,5
SCADA Alarms	No	Yes (Real-time alarm data used to make operational decisions.)	Yes (Loss of alarms or spurious alarms could lead to operational decisions that impact reliable operation.)	1,2,3, 4,5

Critical Asset: Control Center				
Essential functions (Efs) found in Column 2 of Table C-3 of *Security Guideline for the Electricity Sector: Identifying Critical Assets:* 1. Essential by virtue of their functions supporting reliability or operability of the BPS. 2. Essential for providing information used by a Responsible Entity to make Real-time operational decisions regarding the reliability and operability of the BPS. 3. Essential for Real-time 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 to collectively impact reliability and operability of the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
SCADA/Inter-Control Center Communications Protocol (ICCP) Applications	Yes (In some instances.)	Yes (ICCP functions handle exchange and processing of data used to make operational decisions, may be used for remote control.)	Yes (Loss or manipulation of data could lead to operational decisions that impact reliable operation).	1,2,3, 4,5
State Estimation	No	Yes (Provides information to Control Center operators used to make operational decisions.)	Yes (Loss or manipulation of information could lead to operational decisions that impact reliable operation.)	1,2
Voltage Stability Analysis	No	Yes (Provides information to Control Center operators used to make operational decisions.)	Yes (Loss or manipulation of analysis could lead to operational decisions that impact reliable operation.)	1,2

Critical Asset: Control Center				
Essential functions (Efs) found in Column 2 of Table C-3 of *Security Guideline for the Electricity Sector: Identifying Critical Assets:* 1. Essential by virtue of their functions supporting reliability or operability of the BPS. 2. Essential for providing information used by a Responsible Entity to make Real-time operational decisions regarding the reliability and operability of the BPS. 3. Essential for Real-time 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 to collectively impact reliability and operability of the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
Computer networks that connect control functions between assets within a single ESP	Yes (Failures due to Common Mode Impact for an aggregate group of assets large enough to affect BPS.)	Yes	Yes (Manipulation of aggregate control function could impact reliable operations.)	1,2,3, 4,5

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

Critical Asset: Special System				
Essential functions (Efs) found in Column 2 of Table C-4 of *Security Guideline for the Electrical Sector: Identifying Critical Assets:* 1. Essential Remedial Action Scheme/Special Protection System that supports the reliability or operability of the BPS 2. System critical to automatic load shedding supporting the reliability or operability of the BPS. 3. Demand-Side Management or Direct Control Load Management that supports the reliability or operability of the BPS. 4. Essential by virtue of their functions to the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays, transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	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	1,2,3
Protection System	Yes (Reference to systems indentified in PRC standards Operates as protective controls.)	No (Depends if autonomous action also provides information.)	Yes	1
Under frequency load shedding (UFLS) (Includes aggregation and/or centralized control or common component)	Yes	No (Depends if autonomous action also provides information.)	Yes	2

Critical Asset: Special System				
Essential functions (Efs) found in Column 2 of Table C-4 of *Security Guideline for the Electrical Sector: Identifying Critical Assets:* 1. Essential Remedial Action Scheme/Special Protection System that supports the reliability or operability of the BPS 2. System critical to automatic load shedding supporting the reliability or operability of the BPS. 3. Demand-Side Management or Direct Control Load Management that supports the reliability or operability of the BPS. 4. Essential by virtue of their functions to the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays, transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
UVLS Includes aggregation and/or centralized control or common component)	Yes	No (Depends if autonomous action also provides information.)	Yes	2
Demand Side Management (DSM)/Direct Control Load Management (DCLM) (Includes aggregation and/or centralized control or common component)	Yes	No (Depends if autonomous action also provides information.)	Yes	3
DSM (Does not Include centralized control or common component)	No	Yes (Information provided to influence individual customers.)	Yes (Manipulation of an aggregate group of assets large enough to affect BPS.)	3
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.)	4

Critical Asset: Special System				
Essential functions (Efs) found in Column 2 of Table C-4 of *Security Guideline for the Electrical Sector: Identifying Critical Assets:* 1. Essential Remedial Action Scheme/Special Protection System that supports the reliability or operability of the BPS 2. System critical to automatic load shedding supporting the reliability or operability of the BPS. 3. Demand-Side Management or Direct Control Load Management that supports the reliability or operability of the BPS. 4. Essential by virtue of their functions to the BPS.				
Applications or systems using cyber elements	*Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?*	*Displays, transfers or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?*	*Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?*	Efs
Computer networks that connect control functions between assets within a single ESP	Yes (Failures due to Common Mode Impact for an aggregate group of assets large enough to affect BPS.)	Yes	Yes (Manipulation of aggregate control function could impact reliable operations.)	1,2,3,4

D. Identify Cyber Assets with Qualifying Connectivity

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

> **"R3.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
> **R3.2.** The Cyber Asset uses a routable protocol within a Control Center; or,
> **R3.3.** The Cyber Asset is dial-up accessible."

Determining whether or not a Cyber Asset meets the third qualifying requirement (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 ESP or within a Control Center will generally require multiple steps, including defining a "preliminary" ESP.

Preliminary ESP

One possible approach to defining a preliminary ESP is to examine network drawings and network address plan information for the site in question (e.g., plant, substation, or Control Center). 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 networking[8] device linking that network to other local or wide-area networks. That router can then be considered as being the access point of a preliminary ESP.

Once a preliminary ESP has been defined, determining whether the qualifying requirement of CIP-002 Requirement R3.1 applies is a matter of asking whether or not a Cyber Asset: a) uses either serial or routable protocols within the preliminary ESP, and b) communicates outside the preliminary ESP via a routable protocol. Likewise, once a preliminary ESP has been defined for a Control Center, evaluating a given Cyber Asset's connectivity against CIP-002 Requirement R3.2 can be done by determining whether or not it communicates using a routable protocol.

After determination of the preliminary ESP, non-critical Cyber Assets that are within the ESP could be examined to determine if they could be moved outside of the ESP without impacting the functionality of the Critical Cyber Assets. Any non-critical Cyber Assets remaining within the ESP must be identified as per CIP-

[8] Per the Open System Interconnection reference model Layer 3 and the NERC Frequently Asked Questions No. 6 for Standard CIP-002-1.

005. Non-critical Cyber Assets virtualized on the same hardware platform as a Critical Cyber Asset should also be identified.

The Open System Interconnection Reference Model

The Open System Interconnection (OSI) Reference Model describes a communications architecture comprising seven “layers” arranged in a stack. Each layer provides services to the layer above it and requests services from the layer below.

Information from a given layer is treated as data by the layer below it, which will generally add its own header information before forwarding it “down” the protocol stack to the next lower layer during transmission. Similarly, a layer will remove header information during receipt before sending data “up” the protocol stack to the next higher layer.

Communicating devices such as computers, typically referred to as nodes in this context, generally implement communications software corresponding to each of the layers. In any communication between two nodes, each node’s individual layers are considered to be communicating with the corresponding layers in the other node (e.g., Layer 7 on the first node talks to Layer 7 on the second node, while simultaneously Layer 4 on the first node talks to Layer 4 on the second node).

This guideline is concerned with the bottom 3 layers of the model, namely:

- Layer 1, the physical layer
- Layer 2, the data link layer, and,
- Layer 3, the network layer.

Layer 1 consists of basic communications functions, generally implemented in hardware. It describes the electrical (e.g., voltage), optical (e.g., frequency), or radio (e.g., wave shape) characteristics of the data transmission at its most fundamental level. Examples of Layer 1 technologies include RS-232, T1, DSL, 802.11 (PHY), and Ethernet (the Ethernet specification defines both Layer 1 and Layer 2).

Layer 2 consists of the hardware and software necessary to transmit and receive data transmitted on a single Layer 1 network. Any Layer 1 communications media that allows more than one node (e.g., Ethernet) uses an addressing scheme at Layer 2 to ensure that data is received by the correct node. Examples of Layer 2 protocols include ARP, SLIP, PPP, Frame Relay, and Ethernet (the Ethernet specification defines both Layer 1 and Layer 2).

Layer 3 provides for communication between different Layer 1 or Layer 2 networks even if the Layer 1 or Layer 2 implementation is different on the two nodes. Examples of Layer 3 protocols include IP, and IPX.

Routable vs. Non-Routable Protocols

Routable protocols use addresses and require those addresses to have at least two parts: A "network" address and a "device" address. Routable protocols allow devices to communicate between two different networks by forwarding packets between the two networks. Non-routable protocols only use a "device" address, and do not allow messages to be sent from one network to another, thus allowing communications to take place only on a single network.

Routing takes place at Layer 3 (also called the routing layer), thus using a routing protocol, such as IP, to route data from one local area network to another.

In general, if the communications uses "IP" ("Internet protocol") or IPX/SPX ("Internetwork Packet Exchange/Sequenced Packet Exchange"**)**, it is considered routable; if the communications does not use IP or IPX/SPX, it is not routable. (Note that other routable protocols such as OSI exist, but are not widely used in North America.) Thus, "DNP over IP" is routable, while "DNP" over a serial connection is not routable.

Also, Layer 3 protocols such as IP are often encapsulated in Layer 2 protocols such as Frame Relay, ATM ("Asynchronous Transfer Mode"), and MPLS ("Multiprotocol Label Switching") for delivery of packets to distant networks. When such mechanisms are employed, the IP routable protocol is still in use.

Legacy protocols and Supervisory Control and Data Acquisition (SCADA) communications existed before the OSI Reference Model existed, and therefore don't fit into the model. These protocols combine the necessary characteristics of multiple layers of the model into their data streams, and do not allow for the interchangeability of different layer-specific implementations. They do, however, need to provide Layer 2 functionality, by embedding "device" addresses as part of the data. This is not a communication problem in these instances, because all the communication happens between the central site where the SCADA system resides, and the remote site where the Remote Terminal Unit (RTU) resides. A SCADA central system would communicate with an RTU by specifying the "line" and addressing a command to the "device". The "line" designation was only used at the SCADA system to ensure communication via the correct physical communications circuit; the line designation never appeared in the communication. Based on communication loading (i.e., the amount of data needed from a given RTU), and telephone line physical connections, multiple devices could reside on a given communications line (e.g., one "large" RTU, or

three to five “small” RTUs), each with a “device” address unique to that line. Individual devices did not communicate with each other on the same communications line, much less between communications lines.

With the advent of large wide-area networks and the requirement for communications between “devices” located on multiple local area networks, routing was introduced to allow “devices” on one local area network to communicate to “devices” on another local area network. This required that the local area network component of the address be communicated along with the “device” component of the address. Since both the local area network address and “device” address are included in the transmitted data, devices called “routers” are used to determine how to get packets from the source local area network to the destination local area network address. Once on the destination local area network, the “device” component of the address is used to ensure the data is sent to the correct end “device”.

Examples of routable protocols used in the power industry include:

- DNP/IP
- ICCP (IEC 60870-6/TASE.2)/IP
- IEC 60870-5-104/IP
- IEC 61850/IP
- MODBUS/TCP
- Telegyr 8979/ UDP

Examples of non-routable protocols used in the power industry include:[9]

- CONITEL
- CDC Type 1 and Type 2
- DNP (serial)
- GETAC
- Harris 9000
- IEC 60870-5-101
- MODBUS / MODBUS RTU (serial)
- TRW 2000
- SCI RDACS

Examples of Layer 1 and Layer 2 communication protocols used in power industry which could support either non-routable or routable protocols, or could use an out-of-band but routable protocol for network management include:

- ANSI T1.40x (T-1, E-1, T-3, etc.)
- x DSL
- SONET

[9] There are over 100 legacy non-routable protocols.

- ATM
- Frame Relay
- WDM / DWDM

Any Cyber Asset that uses a routable protocol to connect to a device outside the ESP or within a Control Center should be considered to have qualifying connectivity. An essential Cyber Asset using a non-routable protocol (e.g., serially-connected) within a preliminary ESP would still be considered to have qualifying connectivity if it communicates outside the preliminary ESP via another device using a routable protocol. A Cyber Asset which can communicate via dial-up (routable or non-routable) would be considered to have qualifying connectivity.

Serial Cyber Assets that are Accessible via Routable Protocol

Requirement 3.1 requires that the Cyber Asset "use a routable protocol to communicate outside the Electronic Security Perimeter" to be considered as having qualifying connectivity. The requirement does not state that the Cyber Asset itself must be directly connected by a routable protocol. Thus, serially-connected Cyber Assets can meet the qualifying connectivity criterion in Requirement 3.1, if a routable connection is used to communicate outside the preliminary ESP.

Essential serially-connected Cyber Assets that meet the qualifying connectivity criterion described above must be located within an ESP.
Nonessential serially-connected Cyber Assets that meet the qualifying connectivity criterion described above are not required to be located within an ESP.

Essential or nonessential serially-connected Cyber Assets that do not communicate with systems outside the preliminary ESP using a routable protocol are not required to be located within an ESP.
Essential serially-connected Cyber Assets, such as RTUs, which communicate outside the preliminary ESP using a routable protocol, for example to an Energy Management System (EMS), meet the qualifying connectivity requirement of R3.1, regardless of whether they communicate using a data concentrator or through a local control system.

Serially-connected Cyber Assets, such as a temperature or pressure sensor or a feed-water pump control (i.e., sensors and actuators) at a generating plant may be connected to a plant control system, which, in turn communicates outside the preliminary ESP, for example to an EMS. The temperature or pressure data is not transmitted to the EMS; only information resulting from processing that primary data is transmitted to the EMS. Similarly, the EMS does not directly

control the feed-water pump; it is controlled by the plant control system, perhaps as a result of receiving a command from the EMS. Because none of these example Cyber Assets send data to or receive control inputs from the EMS directly, they do not use a routable protocol to communicate to the EMS.

Serial Cyber Assets that are Accessible via Dial-up

Requirement 3.3 addresses to Cyber Assets that are "dial-up accessible", not those directly connected to a modem. Many Cyber Assets are accessible via a dial-up connection through the use of modem-sharing switches and other modem-sharing technologies, such as remote access gateways or data concentrators, that allow a single telephone line or dial-up connection to access multiple Cyber Assets simultaneously. Because these Cyber Assets are "accessible" from a dial-up connection, they meet the qualifying connectivity requirement of R3.3.

As with the serially-connected Cyber Assets described previously, essential dial-up-accessible Cyber Assets that meet the qualifying connectivity criterion described above must be located within an ESP.

As provided in the response to Question 7 in the CIP-002 FAQs, dial-up-accessible access refers to any temporary (non-permanent), interruptible, or not continuously-connected communication access to a Cyber Asset from any remote site. Access to a Cyber Asset via a permanent communication connection from a specific computer over a dedicated communication circuit would not be considered dial-up-accessible-access.

Process Diagrams

Figure 2, below, illustrates a process 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 R3.

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.

Figure 2. Evaluating CIP-002 R3 Qualifying Communication Characteristics

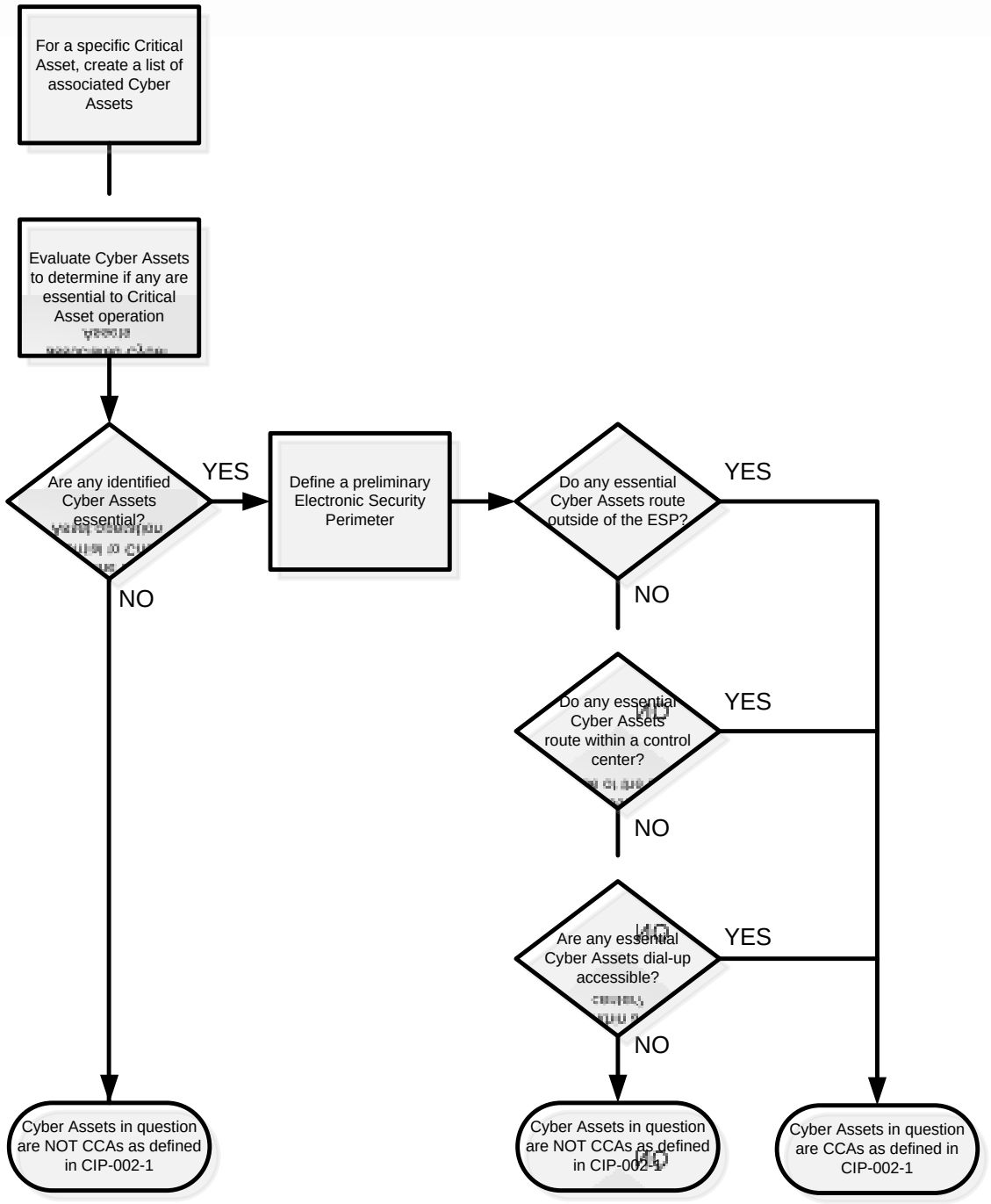
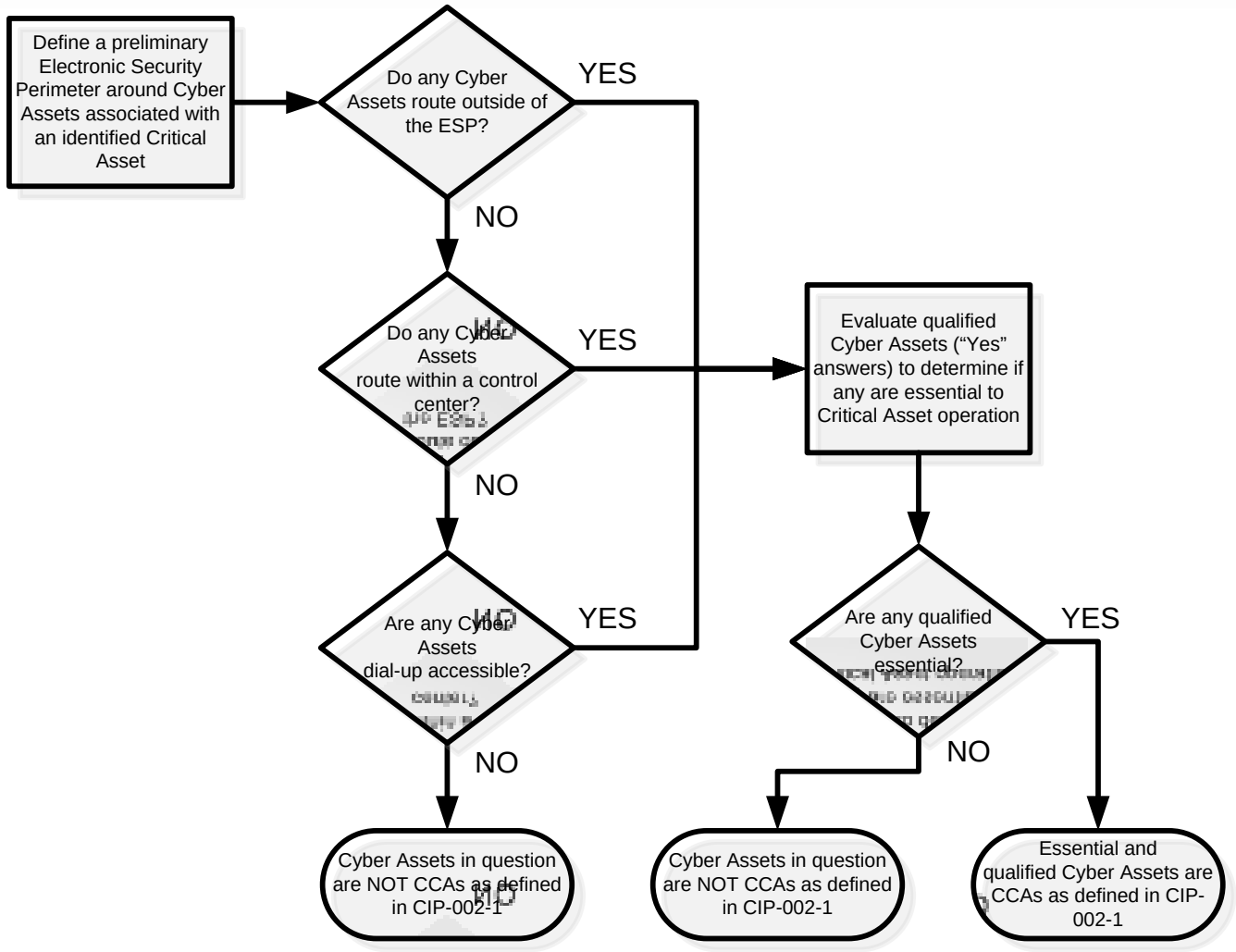


Figure 3. Evaluating CIP-002 R3 Qualifying Communication Characteristics as the First Step in Overall CCA Identification Process



Example Configurations

Attachment 1 provides example configurations of essential-to-Critical-Asset and not-essential-to-Critical-Asset Cyber Assets that communicate using routable and non-routable protocols, as well as via dial-up access. These configurations are considered to represent different possible arrangements of dial-up and ESP access points, ESP boundaries and position within or outside a Control Center. For each example configuration, Critical Cyber Asset designations are suggested for those essential Cyber Assets that are considered to meet one of the qualifying characteristics defined in CIP-002 R3.1, R3.2 or R3.3. These drawings are high-level and many variations of configurations are not shown.

E. Compile the List of Critical Cyber Assets

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

Related Documents and Links:

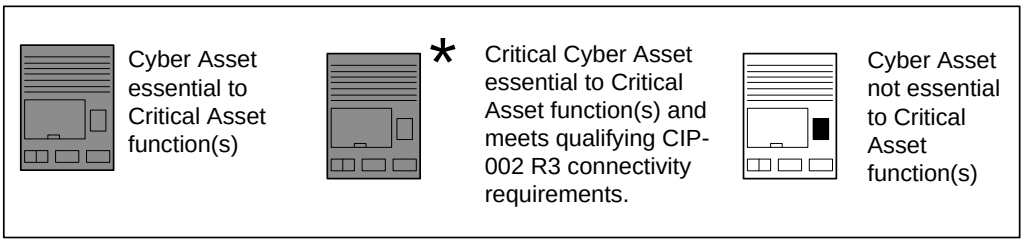
NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems,* computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, July 2002.
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

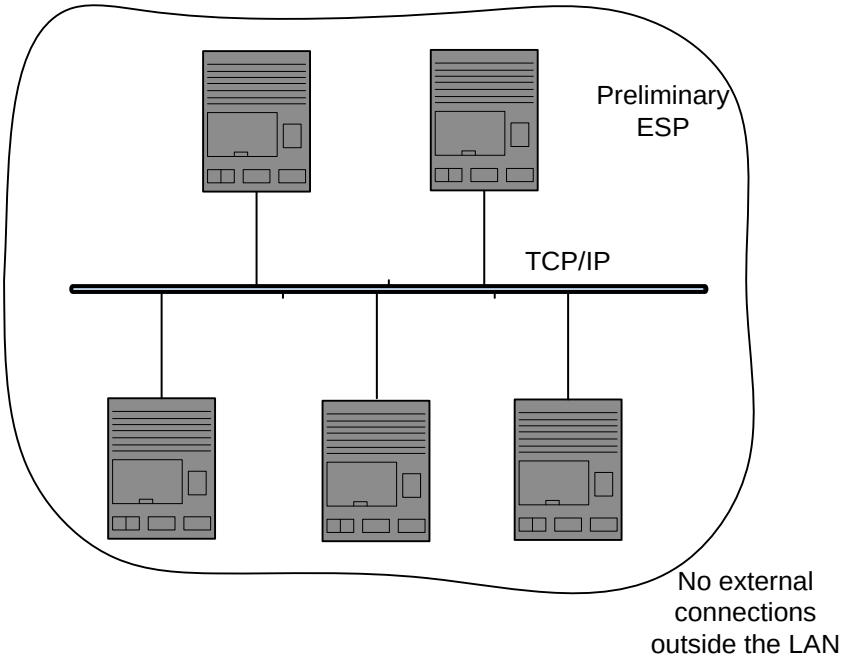
NERC CIP Guideline, *Control System – Business network Electronic Connectivity*, Critical Infrastructure Protection Committee, North American Electric Reliability Corporation, May 2005.
http://www.esisac.com/publicdocs/Guides/SecGuide_ElectronicSec_BOTapprvd3may05.pdf

NERC Glossary of Terms Used in Reliability Standards, April 2009.
www.nerc.com/files/Glossary_2009April20.pdf

NERC Security Guideline for the Electrical Sector: *Identifying Critical Assets*. Sept 2009.
http://www.nerc.com/docs/cip/sgwg/Critical_Asset_ID_Final_Clean.pdf

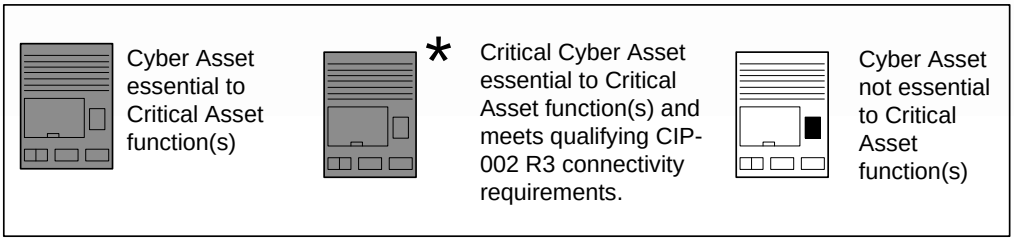
Attachment 1
Interpretation of Qualification per CIP-002 R3 Qualifying Connectivity Requirements for Example Configurations

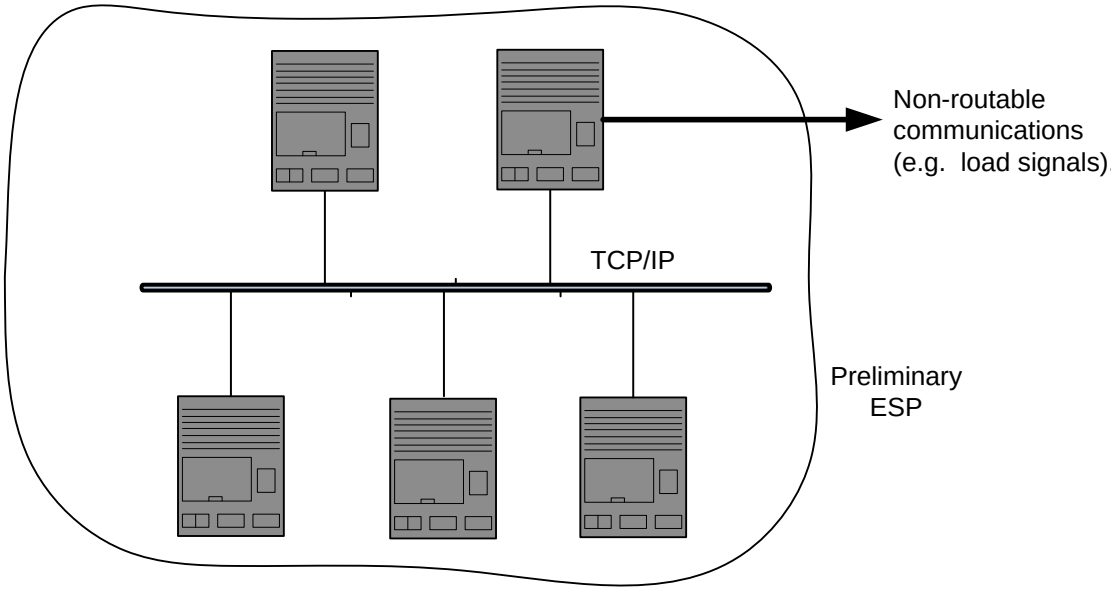




Drawing 1

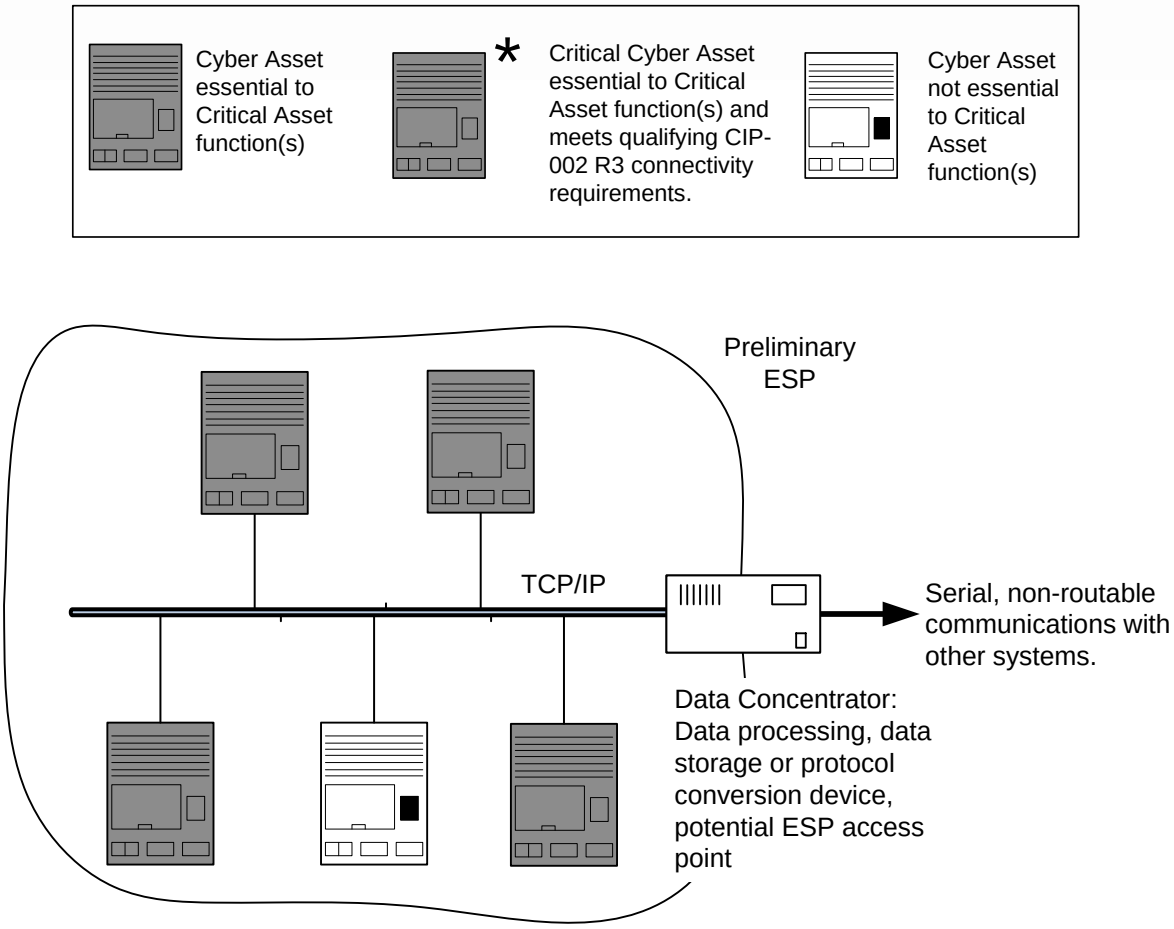
Essential Cyber Assets on an autonomous LAN outside of a Control Center communicate with each other using a routable protocol. There are no external connections to this network. Therefore, these essential Cyber Assets are not Critical Cyber Assets.





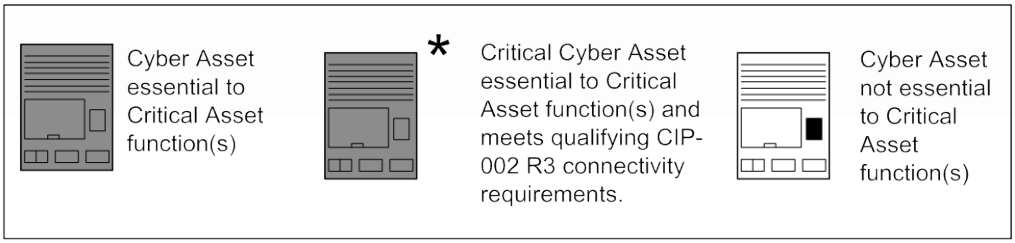
Drawing 2

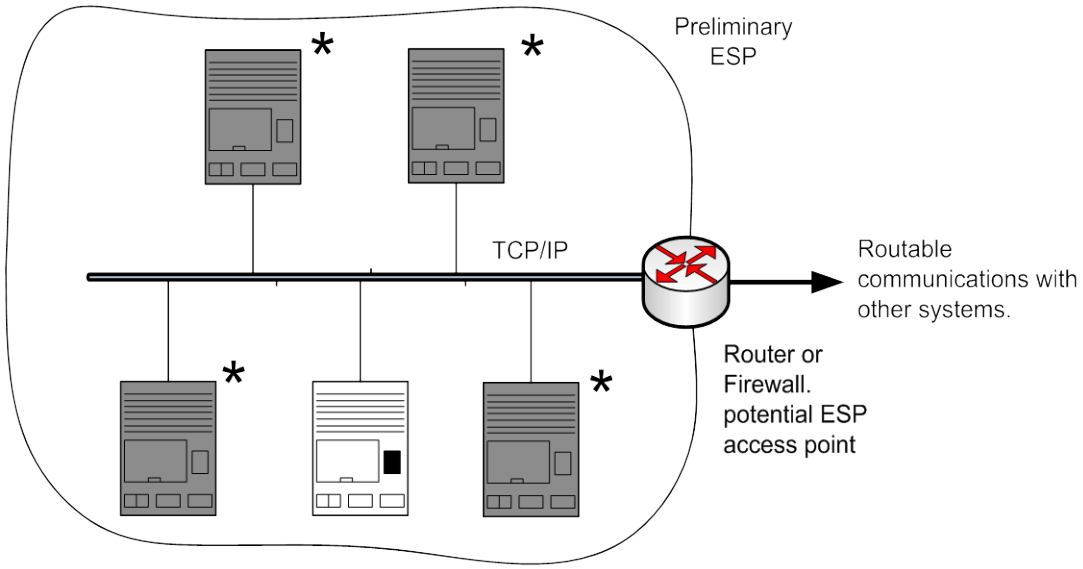
Essential Cyber Assets on an autonomous LAN outside of a Control Center communicate with each other using a routable protocol. One essential Cyber Asset communicates with systems outside the preliminary ESP using a non-routable protocol on a permanent connection. This is the only connection outside the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



Drawing 3

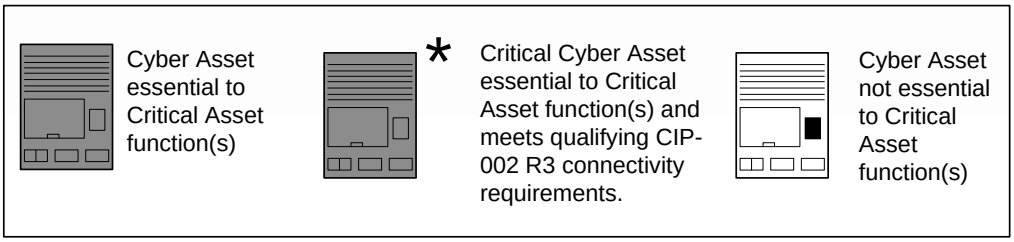
Essential and nonessential Cyber Assets on a LAN outside of a Control Center communicate with each other using a routable protocol. They also communicate with remote systems via a data concentrator that performs protocol conversion for communication outside the preliminary ESP using a serial non-routable connection. The essential Cyber Assets shown do not use a routable protocol to communicate with systems outside of the preliminary ESP and do not meet the criterion of CIP-002 R3.1; therefore they are not Critical Cyber Assets. Because there are no Critical Cyber Assets, no ESP or is needed and the data concentrator does not need to be designated as an ESP access point.

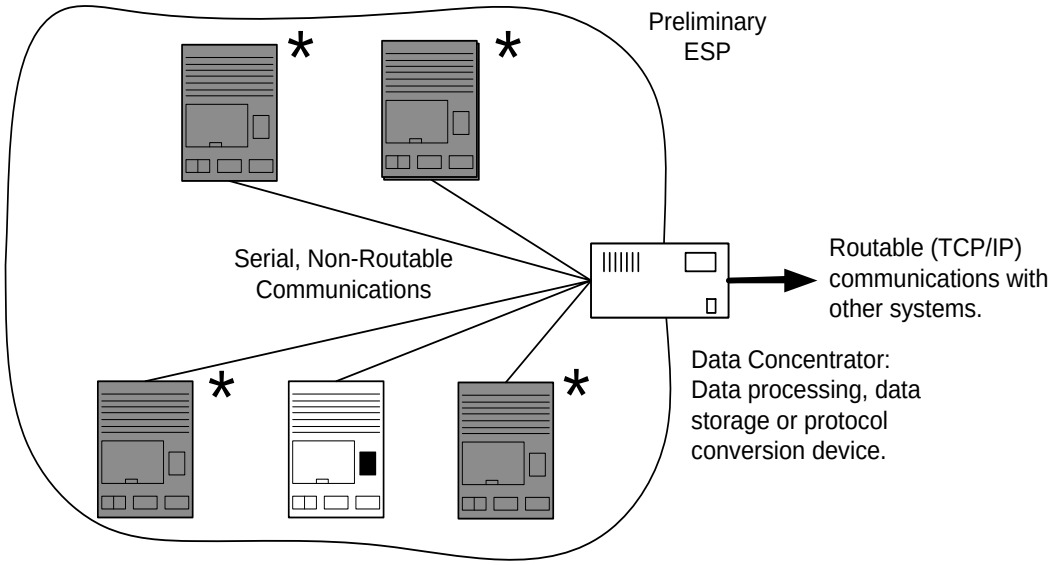




Drawing 4

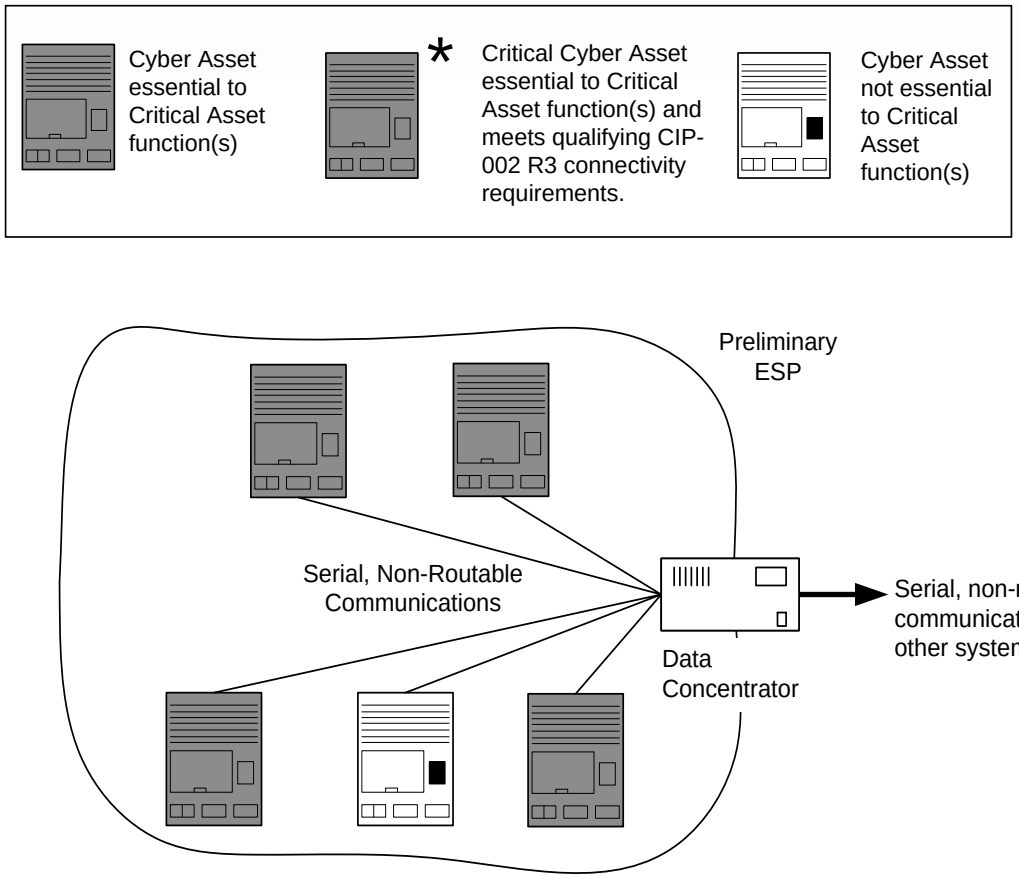
Essential and nonessential Cyber Assets on a LAN outside of a Control Center communicate with each other and with outside systems on a WAN or other LAN using a routable protocol. Essential Cyber Assets are Critical Cyber Assets per CIP-002 R3.1 based on preliminary ESP design. The fact that all the Cyber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





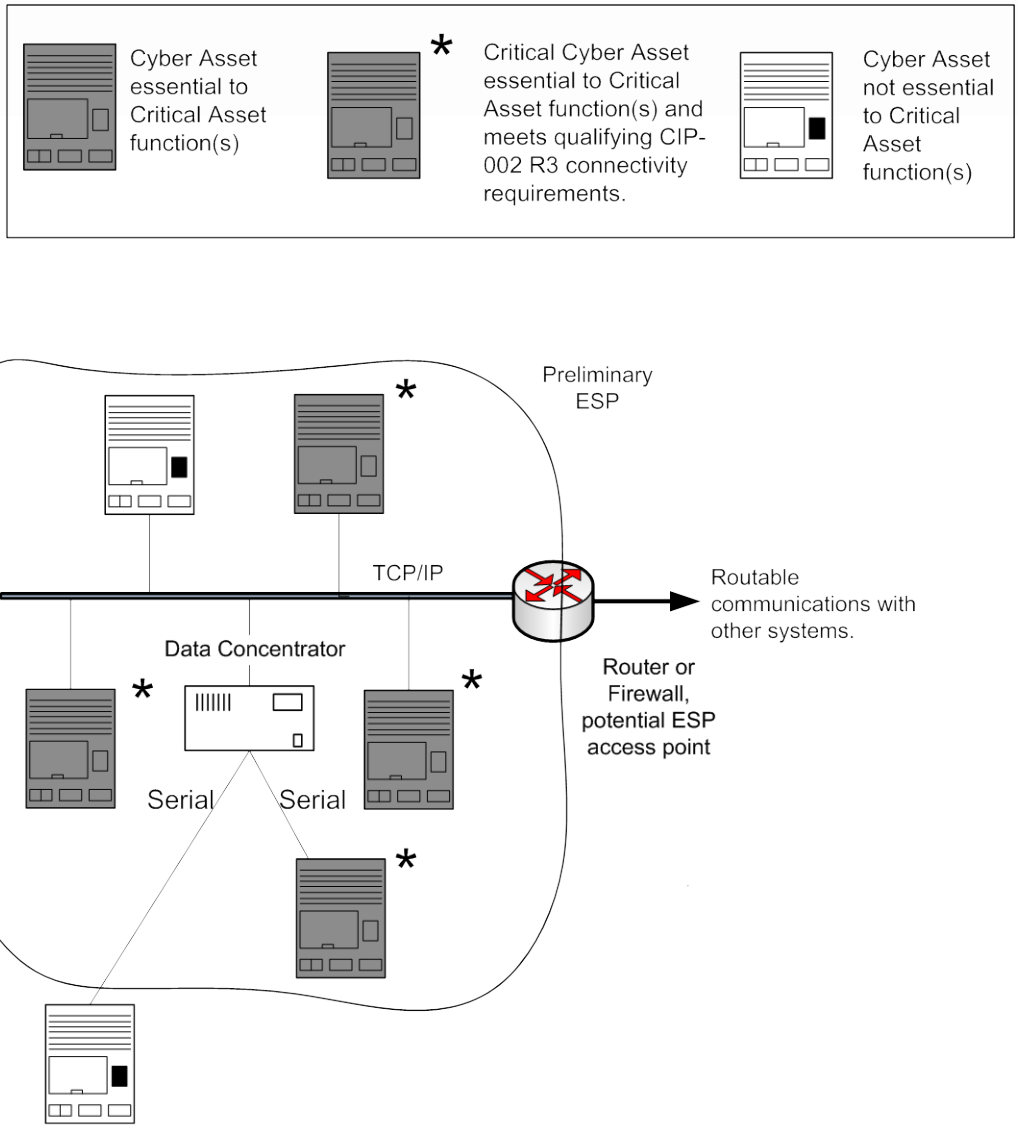
Drawing 5

Essential and nonessential Cyber Assets outside of a Control Center communicate to remote systems (e.g., SCADA) via a data concentrator that performs protocol conversion for communication outside the preliminary ESP using a routable protocol. The essential Cyber Assets shown are Critical Cyber Assets per CIP-002 R3.1, because they use a routable protocol to communicate with systems outside the preliminary ESP. Access to these essential Cyber Assets from outside the ESP using a routable protocol dictates the need for cyber security protection as prescribed by the CIP Standards. The nonessential Cyber Asset shown in the drawing is not a Critical Cyber Asset, so when the actual ESP is established this Cyber Asset is not required to be inside the ESP.



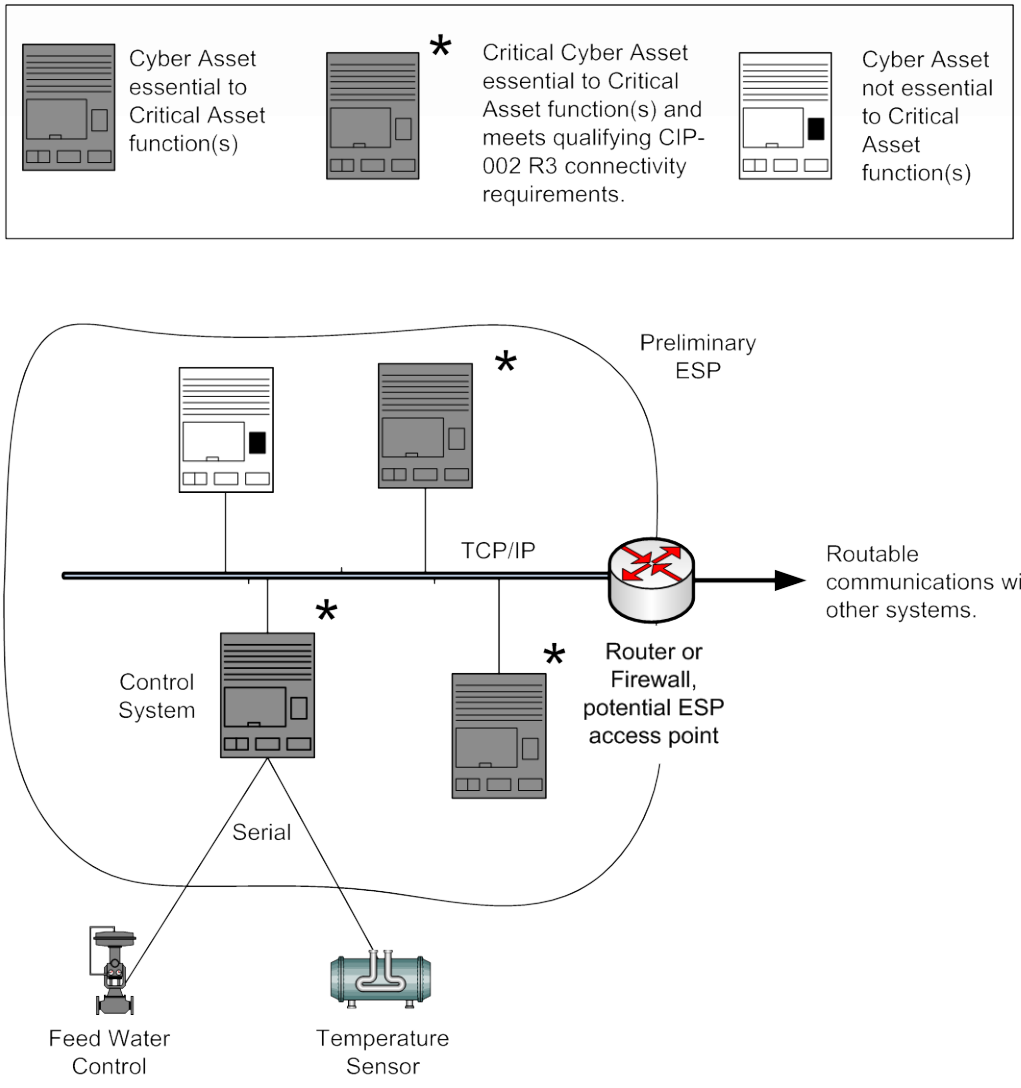
Drawing 6

Essential and nonessential Cyber Assets outside of a Control Center communicate to remote systems (e.g., SCADA) via a data concentrator that communicates with systems outside preliminary ESP using a non-routable protocol. The essential Cyber Assets shown do not use a routable protocol inside or outside of the preliminary ESP, do not meet the criterion of CIP-002 R3.1, and therefore, are not Critical Cyber Assets. Because there are no Critical Cyber Assets, no ESP is needed.



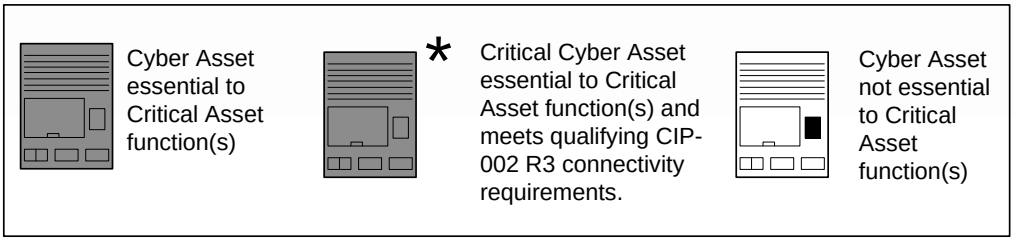
Drawing 7

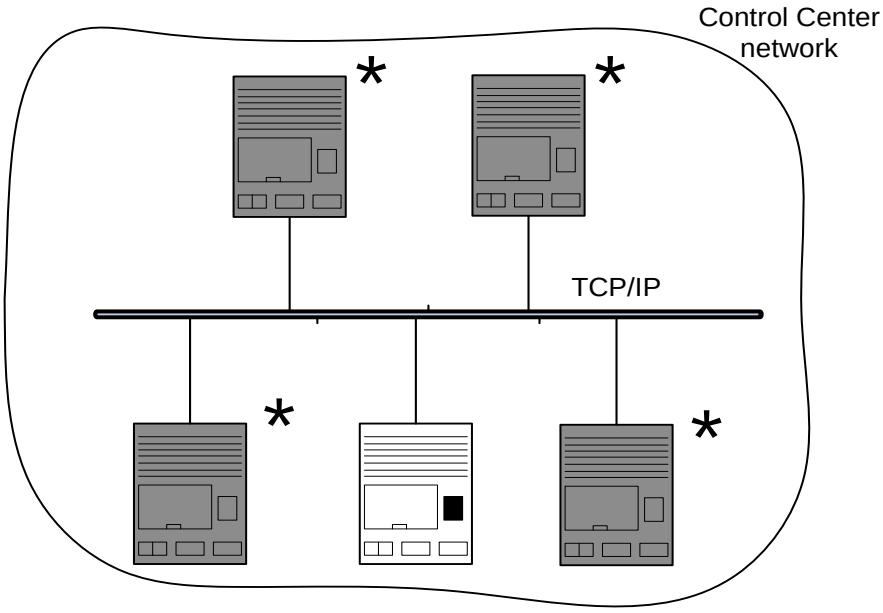
Essential and nonessential Cyber Assets on a LAN outside of a control center communicate with each other using a routable protocol. The essential Cyber Assets which have TCP/IP connectivity also communicate with systems outside the ESP using a routable protocol which qualifies them as Critical Cyber Assets. This includes the serially-connected essential Cyber Asset that is connected to the TCP/IP LAN via a data concentrator and connected inside the ESP to TCP/IP via a serial connection but communicates with systems outside the ESP using a routable protocol. The nonessential serially-connected Cyber Asset shown in the drawing is not a Critical Cyber Asset, so when the actual ESP is established this Cyber Asset is not required to be inside the ESP.



Drawing 8

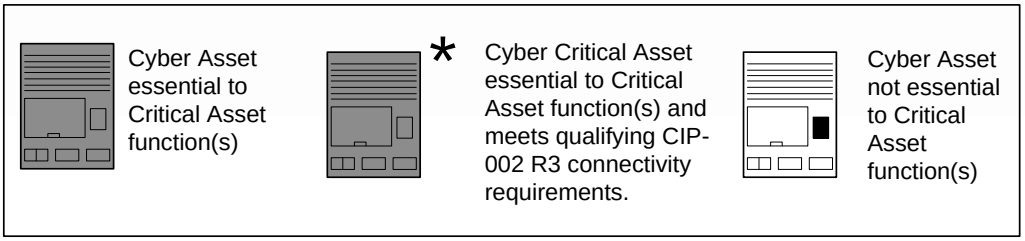
Essential and nonessential Cyber Assets on a LAN outside of a control center communicate with each other using a routable protocol. The essential Cyber Assets with TCP/IP connectivity communicate with systems outside the ESP using a routable protocol which qualifies them as Critical Cyber Assets. The two serially-connected Cyber Assets controlling feed water flow and monitoring temperature are not Critical Cyber Assets, even if they are essential, provided that they do not pass data directly to or receive commands directly from systems outside the ESP (i.e., the local control system that they are connected to communicates only processed data to systems outside the ESP.)

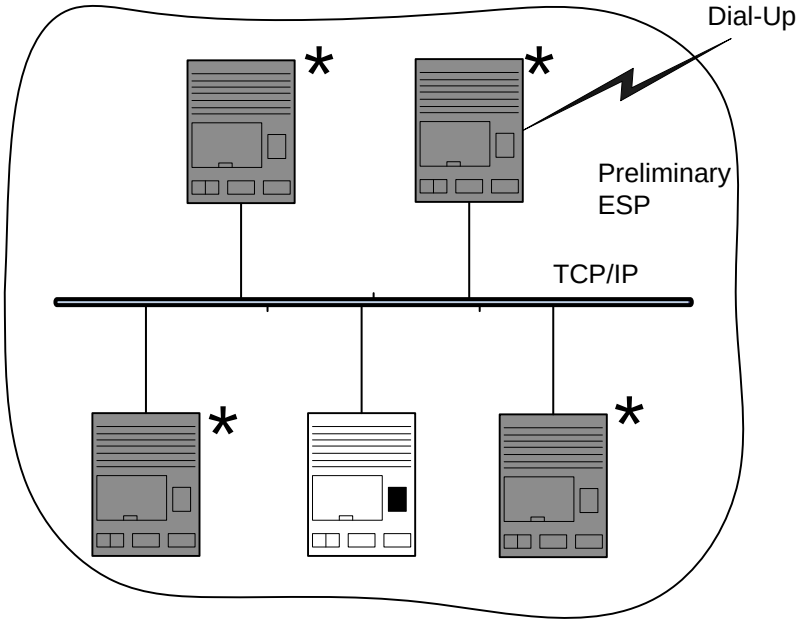




Drawing 9

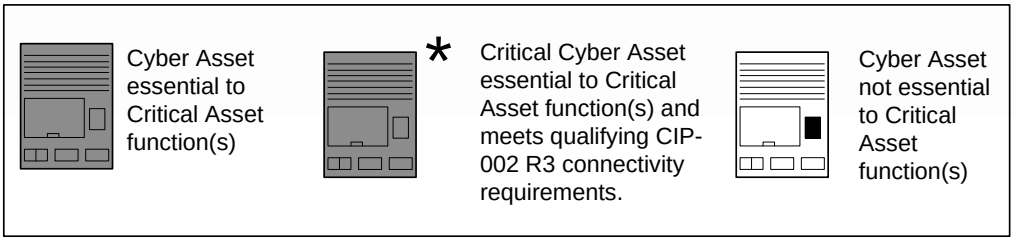
Essential and nonessential Cyber Assets on a LAN within a Control Center communicate with each other using a routable protocol. Essential Cyber Assets that use a routable protocol within a Control Center are Critical Cyber Assets per CIP-002-1 R3.2. Communication outside the Control Center is not a consideration for Critical Cyber Asset identification at the Control Center.

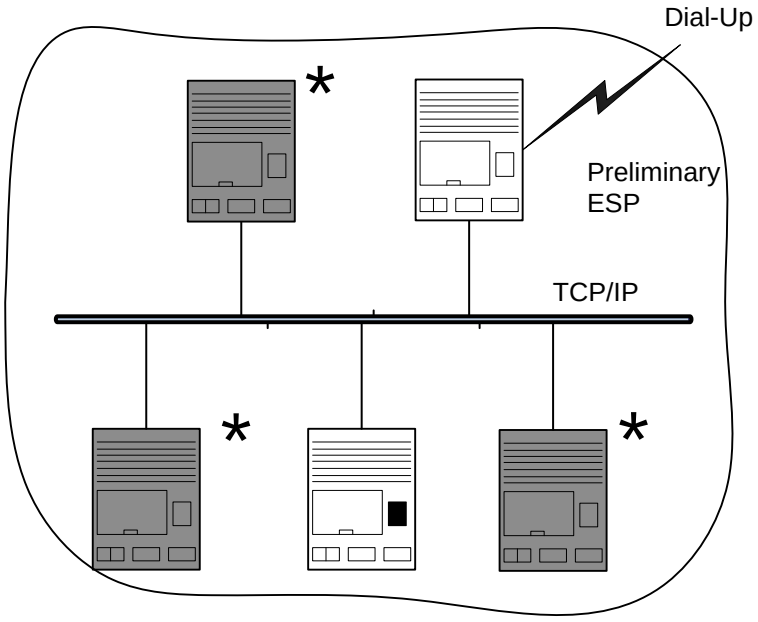




Drawing 10

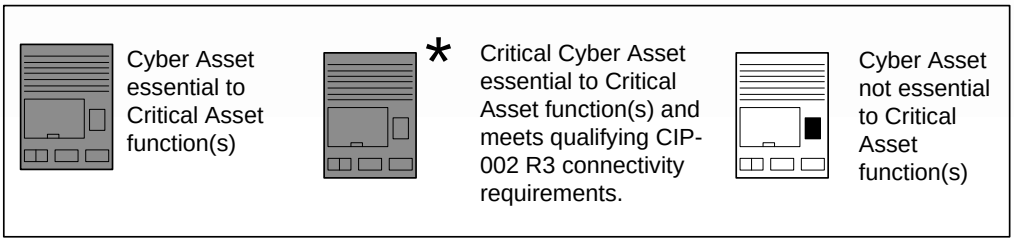
Essential and nonessential Cyber Assets on an autonomous LAN outside of a Control Center communicate with each other using a routable protocol. One essential Cyber Asset is dial-up-accessible and is therefore a Critical Cyber Asset per CIP-002 R3.3. It might be possible to gain access to this dial-up system and then to other Cyber Assets on the LAN, therefore all essential Cyber Assets shown should be identified as Critical Cyber Assets. If dial-up access is removed, none of these Cyber Assets meet the CIP-002 R3 connectivity criteria, and therefore, would not be Critical Cyber Assets.

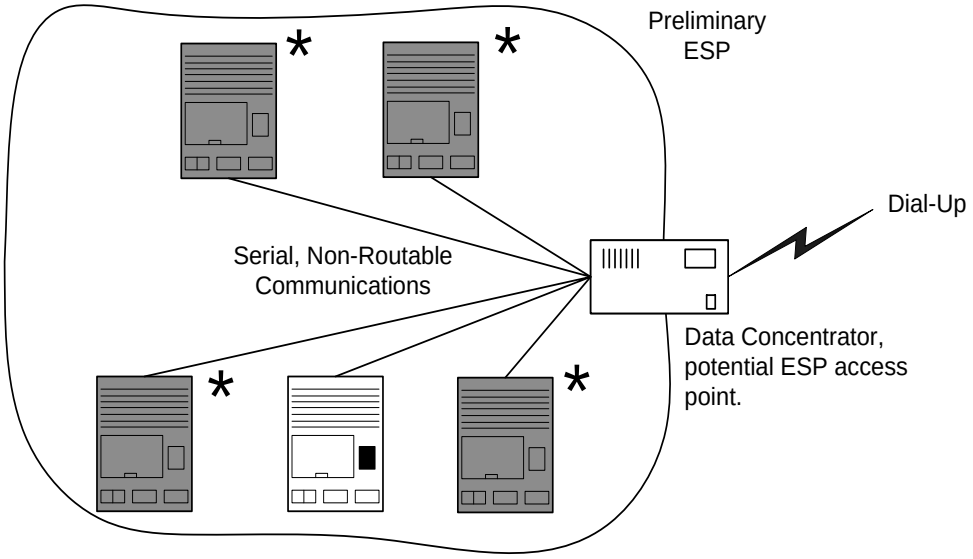




Drawing 11

Essential and nonessential Cyber Assets on an autonomous LAN outside of a Control Center communicate with each other using a routable protocol. One nonessential Cyber Asset is dial-up-accessible. It might be possible to gain access to this dial-up system and then to other Cyber Assets on the LAN, therefore all essential Cyber Assets shown should be identified as Critical Cyber Assets. If dial-up access is removed, none of these Cyber Assets meet the CIP-002 R3 connectivity criteria, and therefore, would not be Critical Cyber Assets





Drawing 12

Essential and nonessential Cyber Assets outside of a Control Center communicate with systems (e.g., SCADA) via a data concentrator that performs protocol conversion for communication with systems outside the preliminary ESP using a dial-up connection. The essential Cyber Assets shown do not use a routable protocol that communicates outside the ESP; however, they are connected via dial-up, therefore they meet the criterion of CIP-002 R3.3, and must be considered Critical Cyber Assets.

Attachment 2
Example Cyber Inventory List

Cyber Asset	Network Address	Application or Function	Associated Critical Asset	Used in supervisory or autonomous control impacting reliable operation of the Critical Asset?	Displays, transfers, or contains information relied on to make Real-time decisions impacting reliable operation of the Critical Asset?	Loss, Degradation or Compromise impacts the reliable operation of the Critical Asset?	Communicate with systems outside the ESP using a routable protocol?	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	Yes	Yes	Yes	No	Yes	No	YES
(Entity-specific identifier)	192.168.5.9	SCADA Supervisory Control – Backup Server	Primary Control Center	Yes	Yes	Yes	No	Yes	No	YES
(Entity-specific identifier)	192.168.5.10	State Estimator – App Server	Primary Control Center	No	Yes	Yes	No	Yes	No	YES
(Entity-specific identifier)	192.168.5.11	State Estimator – DB Server	Primary Control Center	No	No	Yes	No	Yes	No	YES
(Entity-specific identifier)	192.168.5.25	Print Server	Primary Control Center	No	No	No	No	Yes	No	NO

Confidential

Revision History:

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 3rd 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.
10/13/09	0.903	Results of October 13th 2009 RAWG online meeting.
10/19/09	0.904	Results of October 19th 2009 RAWG online meeting.
10/27/09	0.905	Results of October 27th 2009 RAWG online meeting.
11/03/09	0.906	Results of November 3rd 2009 RAWG online meeting.
11/10/09	0.907	Results of November 10th 2009 RAWG online meeting.
11/16/09	0.908	Results of November 16th 2009 RAWG online meeting.
11/23/09	0.909	Results of November 23rd 2009 RAWG online meeting.

11/24/09	0.910	Results of November 24th 2009 RAWG online meeting.
11/30/09	0.911	Results of November 30th 2009 RAWG online meeting.
1/18/10	0.912	Prepare for round of comments from industry
03/04/10	0.913	Results of March 4th 2010 RAWG online meeting.
03/15/10	0.914	Results of March 15th 2010 RAWG online meeting.
03/23/10	0.915	Results of March 23rd 2010 RAWG online meeting.
03/31/10	0.916	Results of March 31st 2010 RAWG online meeting.
04/07/10	0.917	Results of April 07st 2010 RAWG online meeting.
04/20/10	0.918	Results of April 20th 2010 RAWG online meeting.
04/27/10	0.919	Results of April 27th 2010 RAWG online meeting.
04/29/10	0.920	Results of April 29th 2010 RAWG online meeting.
05/06/10	0.921	Results of May 6th 2010 RAWG online meeting.
05/14/10	0.922	Results of edits made by email the week of May 10th.
5/21/10	0.923	Last edit during approval
6/17/10	1.0	Final Document – Approved by CIPC