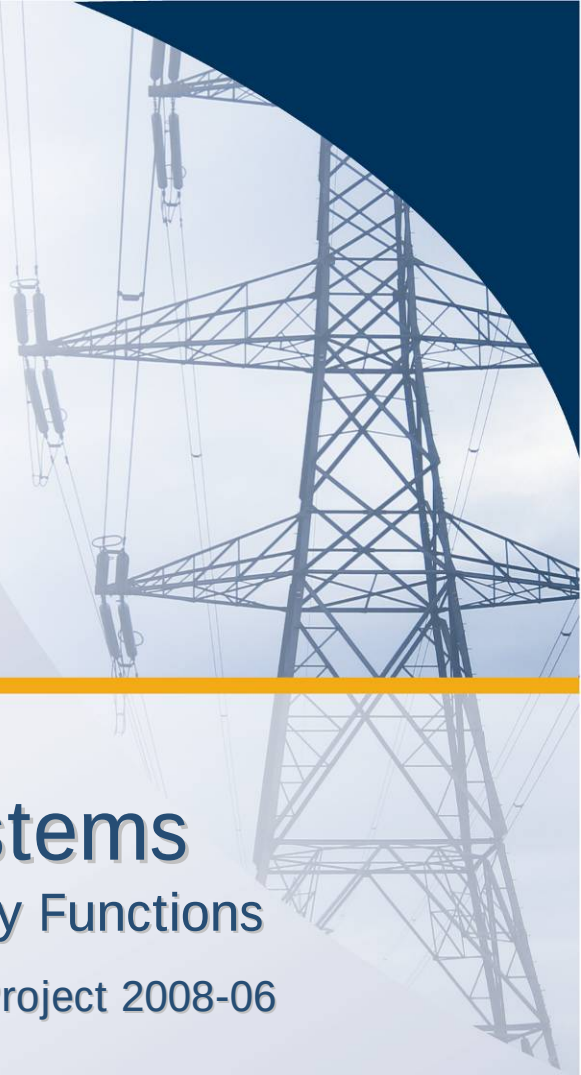
NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

Cyber Security Standards Drafting Team for Project 2008-06
Cyber Security Order 706

to ensure the reliability of the bulk power system

JULY 2009

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

TABLE OF CONTENTS

Categorizing Cyber Systems:

An Approach Based on Impact on BES Reliability Functions

A. EXECUTIVE SUMMARY

This paper, *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions*, proposes a broader and more comprehensive approach for providing appropriate and effective cyber security to protect the systems which support a reliable Bulk Electric System (BES).

The BES is viewed holistically in terms of reliability functions supporting an Adequate Level of Reliability, its supporting BES subsystems and cyber systems, which are categorized based on impact. This process results in a more uniform selection of appropriate security requirements and controls, which reduces risk to the BES caused by a Cyber Security Incident.

The methodology in the approach proposes a mapping of BES subsystems to pre-determined criteria into categories based on their impact on the reliability or operability of the BES. The categorization of BES cyber systems and their elements is based on an analysis of their impact, either directly or indirectly through the BES subsystems, on the BES functions they support. A rigorous analysis of the impact to the BES for any given cyber system results in a deterministically derived categorization of each cyber system.

In defining the cyber systems which constitute the target for protection, this paper considers issues associated with interconnected systems, systems associated with the computing infrastructure supporting these BES cyber systems and systems that are collaterally affected because of their proximity to BES cyber systems.

A crucial undertaking for the drafting team lies in developing these security controls in such a way as to mitigate risk while maximizing the value of the associated cyber security investment for the industry. To accomplish this objective, the drafting team seeks to develop a library of controls (requirements) appropriate to the degree and type of protection needed.

The development of these controls is outside the scope of this paper; the drafting team will seek further industry input in the development phase of the controls framework.

The concepts presented here are a paradigm shift, considering that cyber technology in support of reliability are *systems* intimately associated with the reliability functions that they support.

This paper deals with the identification and classification of BES assets and Cyber Systems. There are a number of other issues raised in FERC Order 706 concerning CIP-002-1 matters that are not addressed in this paper. The SDT will be soliciting industry feedback on those issues as part of the standards development process.

B. INTRODUCTION

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards aimed at preserving and enhancing the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability or operability** of this system. The overarching mission is preserving and enhancing the reliability of this system, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability or operability of these assets.

CIP-002 — Cyber Security — Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment." FERC's comments in its Order 706 approving the Cyber Security Standards as well as common perceptions and observations from various other commenters will all be considered as valuable input into this process.

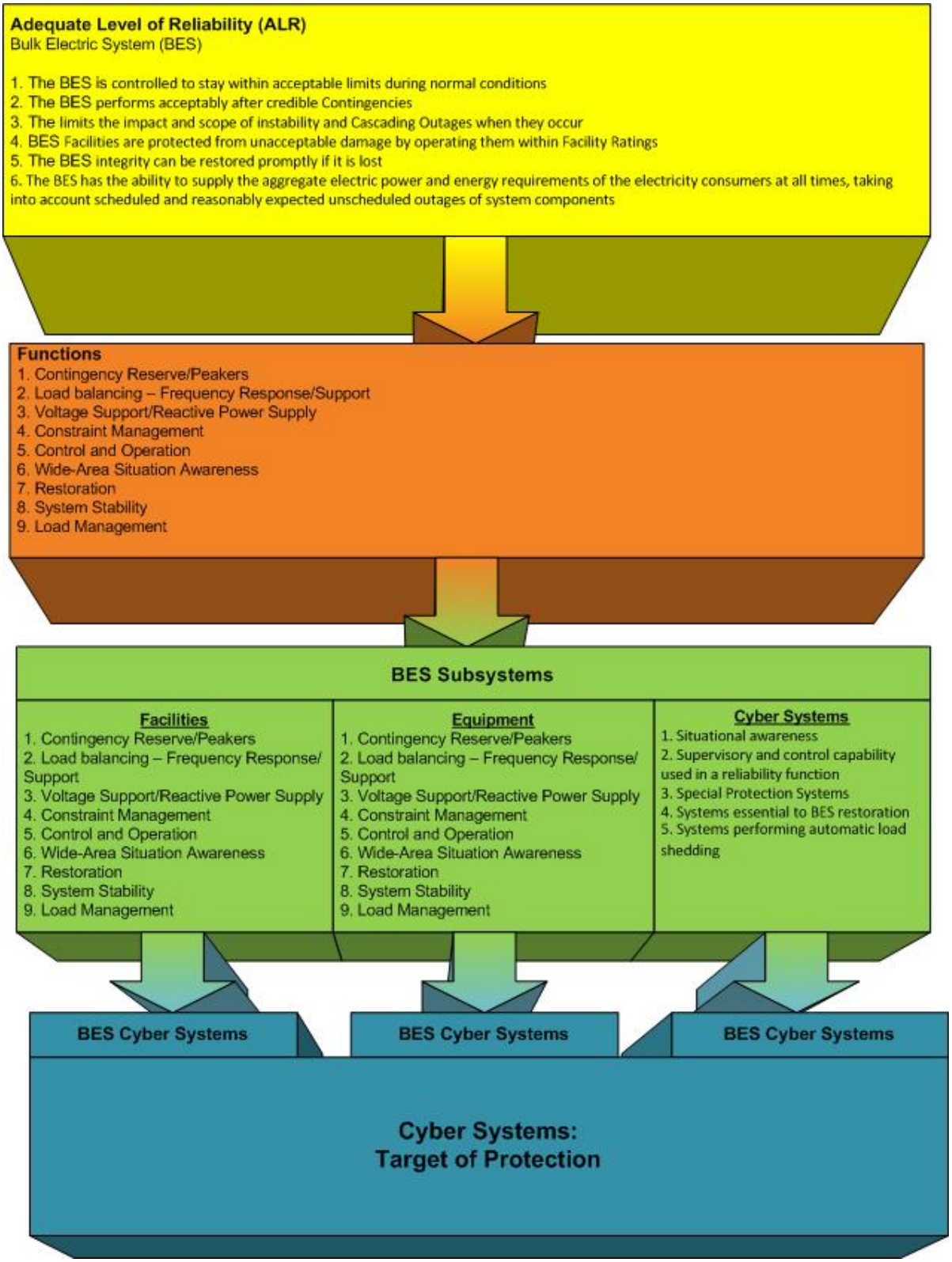
This paper describes an approach based on the concepts of NERC's definition of Adequate Level of Reliability (ALR) and the characteristics of the BES described therein that will achieve this ALR, namely:

1. The Bulk Electric System is controlled to stay within acceptable limits during normal conditions;
2. The Bulk Electric System performs acceptably after credible Contingencies;
3. The Bulk Electric System limits the impact and scope of instability and Cascading Outages when they occur;
4. The Bulk Electric System's Facilities are protected from unacceptable damage by operating them within Facility Ratings;
5. The Bulk Electric System's integrity can be restored promptly if it is lost; and
6. The Bulk Electric 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.

This proposed cyber system categorization approach relies on the identification of functions which are essential to achieving these characteristics and the BES subsystems which support these functions. These BES subsystems may be defined as facilities, equipment, or systems performing functions to ensure that the BES achieves an Adequate Level of Reliability.

The methodology proposes to identify all cyber systems which support the reliable operation of the BES; one must note that a cyber system can itself be a BES subsystem if it directly performs one or more of the identified functions and if compromised will impact that function.

Figure 1


Adequate Level of Reliability (ALR)
Bulk Electric System (BES)
1. The BES is controlled to stay within acceptable limits during normal conditions
2. The BES performs acceptably after credible Contingencies
3. The limits the impact and scope of instability and Cascading Outages when they occur
4. BES Facilities are protected from unacceptable damage by operating them within Facility Ratings
5. The BES integrity can be restored promptly if it is lost
6. The BES 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
Functions
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
BES Subsystems
Facilities
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/ Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
Equipment
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/ Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
Cyber Systems
1. Situational awareness
2. Supervisory and control capability used in a reliability function
3. Special Protection Systems
4. Systems essential to BES restoration
5. Systems performing automatic load shedding
BES Cyber Systems
BES Cyber Systems
BES Cyber Systems
Cyber Systems:
Target of Protection

Once BES subsystems and their cyber systems are identified, the methodology requires an analysis based on two major factors:

- A mapping of BES subsystems into categories based on pre-defined criteria which reflect their impact on the reliability or operability of the BES
- A categorization of their associated cyber systems and their elements based on their impact on the functions of the BES subsystems they support.

An analysis of any given cyber system results in a deterministically derived categorization of each cyber system based on its impact on the BES.

The scope of the CIP Cyber Security standards being considered excludes the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies, since they are regulated outside of NERC. Note that there may be facilities, equipment, or systems that may be in a nuclear facility associated with the BES that are outside of the regulatory realm of these nuclear regulatory organizations, and would therefore be regulated under these NERC CIP standards. It is also worth noting that the CIP Cyber Security Standards do not include those assets associated with BES planning activities UNLESS they also have a direct effect on the reliability or operability of the BES. There will, however, be cases where these types of BES planning and market function systems may be required to be protected under the CIP standards if they meet the protection requirements of the Cyber Security Standards (for example, if they impact a cyber system that is subject to the standards).

The concepts associated with an impact-based approach to determining the criticality of certain facilities, equipment, and systems are particularly well covered in the Draft Volume 1 of NERC's Security Guideline for the Electric Sector: Identifying Critical Assets. The development of this guidance document was in direct response to a directive by FERC in Order 706. An additional important concept in this approach is the inclusion of assets based on their functions in the operation of the BES. The SDT is currently engaged in an additional guidance document to address the identification of Critical Cyber Assets. The approach proposed by the Cyber Security Standard Drafting Team for the identification and classification of BES subsystems also draws upon the BES functions and asset identification as well as the criteria for Critical Assets sections of the guideline.

The ideas and approaches identified in this concept paper are well-grounded and draw on elements of principles already described in other related, publicly available information, such as the application of a Federal Information Processing Standards 199-like approach to classifying

cyber systems and the National Institute of Standards and Technology's framework for information security risk management, as well as internal SDT discussions on guiding principles used for the development of a cyber systems categorization model and comments and discussions with recognized industry experts from a variety of applicable domains.

The cyber system categorization approach outlined in this concept paper includes the consideration of NERC's mission, the essential functions necessary in achieving this mission, an impact-based methodology to map its BES subsystems into categories based on pre-defined criteria and the associated cyber systems engaged in the process, and finally the deterministic derivation of an overall impact-based categorization of the cyber systems, with the anticipated application of cyber security requirements commensurate with that categorization. This methodology parallels general approaches to risk management practices, which focus first on identifying key processes necessary for meeting high level objectives, then drilling down into supporting processes.

The relationship of cyber systems to BES reliability is deeper and more inter-related than it might appear on the surface. The readers of this concept paper are encouraged to use all of their experience as they review this paper, but should be prepared to have their assumptions challenged, as this represents a paradigm shift for experienced operating personnel. Consider that cyber technology in support of reliability is not just a piece of hardware or software or a communication circuit, but rather, a *system* intimately associated with the reliability functions that it supports. Cyber systems can have more subtle linkages in addition to the linkage caused by the interconnected bulk electric system.

This concept paper is focused on the identification and classification of BES assets and Cyber Systems. There are a number of other issues raised in FERC Order 706 dealing with CIP-002-1 matters that are not addressed in this paper. The SDT will be soliciting industry feedback on these issues as part of the standards development process.

C. BES RELIABILITY FUNCTIONS

A prerequisite to the start of the identification of BES Subsystems that affect the reliability or the operability of the BES is the identification of functions that support the characteristics of ALR. These functions may contribute to an adequate level of reliability in varying degrees, which would be considered through the impact assessment of the BES subsystem on the reliability or operability of the BES.

The following table provides an illustrative example of the BES Reliability Functions, the BES subsystem mapping criteria, together with sample BES subsystems and cyber systems that could be envisioned. The contents of this table are provided only as possible definitions and are not intended to be a final, comprehensive, and exhaustive list.

Table 1

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
Contingency Reserve/Peakers	Single resource or combined resources (sharing a common mode failure) whose output exceeds the Contingency Reserve • Unit capable of starting in 15 minutes or less Transmission facility or facilities, whose loss or compromise may result in the loss of resources identified for contingency reserves (those resources in the above bullet or it could be the loss of an import)	Generating unit(s) whose output exceeds the Contingency Reserve Transmission lines, busses and transformers associated with the such generation	Generation control system Real-time monitoring system used for operation Protective relay Station Automation System AGC Plant control room(s)
Load Balancing Frequency Response/Support	Single resource or combined resources (sharing a common mode failure) whose loss or compromise may result in under-frequency Transmission facility or facilities, whose loss or compromise may result in under-frequency	Generating Unit(s) Transmission lines, busses and transformers associated with such generation	Centrally controlled UFLS system EMS SCADA Generation control system Protective relay Plant control room(s)

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
Voltage Support/Reactive Power Supply	Single resource or combined resources (sharing a common mode failure) whose loss or compromised operation may result in: – Unacceptable system voltages – Voltage collapse – Not meeting Nuclear Plant Interface Requirements	Static VAr Compensator Capacitor bank(s) Synchronous Condenser(s) Generation Unit(s) Transmission lines, busses and transformers associated with the such generation	Automated Control System SCADA RTU Protective Relay
Constraint Management	Single resource or combined resources (sharing a common mode failure), transmission facilities or Special Protection Systems whose loss may reduce or eliminate the ability to manage to System Operating Limits or whose compromise could even be used to aggravate constraint loading.	Static VAr Compensator Capacitor bank(s) Synchronous Condenser(s) Generation Unit(s) Transmission lines, busses and transformers	EMS SCADA Automated Substation Control Protective Relays RTUs

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
Control and Operation	Primary and back-up Control Centers, and associated remote data acquisition systems, owned, operated, or employed by Balancing Authorities, Transmission Operators, Generation Operator or Reliability Coordinators that have been registered in the NERC registry Systems essential for reliable BES operation: Inter-utility data exchange Supervisory control or data acquisition Control centre functionality	RC, BA, and TOP Control Centers Generation Control Center	EMS SCADA AGC ICCP RTU
Situational Awareness	Systems essential for reliable BES operation: providing information used to make operational decisions regarding reliability or operability of the BES	– Status or alarm collection – Aggregation – Display functions of a primary or Back-up Control Center – Advanced Network Application (State estimation, Real-time contingency analysis)	– Status or alarm collection – Aggregation – Display functions of a primary or Back-up Control Center – Advanced Network Application (State estimation, Real-time contingency analysis)
Restoration	Generating units, including black-start units; transmission Elements identified in primary cranking paths (including Elements which may not be part of the BES):	Black Start generation unit(s) Reactors, Capacitors Load (distribution	Generation control system SCADA RTU

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
	– which are essential to the initial BES restoration	feeders) Transformers Transmission Lines	Protective Relays
System Stability	Generation resources, transmission facilities and Special Protection Systems whose loss or compromise may result in: – IROL violation – Voltage collapse (wide-spread) – Frequency collapse – Complete operational failure or shutdown of the transmission system – Separation or cascading outages that affect a wide-area spread are of the BES	Transmission lines impacting IROL(s) Generating Unit(s) supporting frequency (with large governor response)/voltage stability/supporting on constraint management on IROLs Capacitor bank(s) Static VAR compensator(s) Synchronous Condensers	Generation control system Associated control systems Protective relays
Load Management	Systems essential to load management whose loss or compromise may impact reliable BES operation: – Demand-Side Management Direct Control Load Management	Load control • Water heater, ac, etc. Interruptible loads DSM Systems Smart Grid	Load Management control system and associated cyber communications
Other	Specific use systems whose loss or compromise may impact the reliable BES operation	Dynamic Feeder Management System Support systems used to modify cyber systems	Dynamic Feeder Management System Support systems used to modify cyber systems

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
		(e.g., remote access, relay setting change) Dynamic Ratings monitoring Physical Security System	(e.g., remote access, relay setting change) Dynamic Ratings monitoring Physical Security System

D. IDENTIFICATION OF BES SUBSYSTEMS

The list of BES functions identified above is used to identify all BES Subsystems that support them. The inclusive list of these identified BES Subsystems constitute the overall scope for application of pre-defined criteria for their mapping to categories based on their impact on the reliability or operability of the BES, as defined by the characteristics of an ALR.

While many functions necessary to maintaining an ALR use specific BES elements or facilities, cyber systems may perform or support functions on a wide-area basis. These wide-area cyber systems may be associated with supporting a class of BES Subsystems in aggregate, or may not be associated with any specific BES asset, but directly perform a function necessary to maintain the ALR. Due to the wide-area Cyber System's direct impact on the operability or reliability of the BES, the wide-area Cyber System will be categorized both as a BES Subsystem, to capture the reliability impact, and as a Cyber System, to capture the cyber impact to the function. A centralized, automated, programmable area load shedding system is an example of a system that would be categorized both as a BES Subsystem and as a Cyber System.

Identical cyber systems may also be implemented in different environments, resulting in different impacts on the BES functions they support. For example, a control system in a small generating facility may have a different reliability impact on the BES than an identical control system operating a larger or several generating facilities.

E. IMPACT MAPPING OF BES SUBSYSTEMS

Identified BES subsystems are mapped into categories based on pre-defined criteria that reflect their impact on the reliability or operability of the BES; this mapping will be based on pre-defined criteria, in the functions they provide or support, which determines the level of that impact. As an example, a mapping process to categorize BES subsystems into High, Medium, and Low based on impact could be patterned after criteria used in categorizing bulk power events, such as NERC's Bulk Power System Event Classification Scale, which includes a graduated impact-scale based on: loss of transmission, generation or load; frequency or voltage deviation; BES system separation; and BES system stability. The categorization would also include impacts based on cyber systems, such as situational awareness or operational control.

The work in defining the detailed criteria and categorization levels for mapping of BES subsystems is underway by another Standards Drafting Team subgroup with expertise in BES planning and operating areas.

F. IDENTIFICATION OF BES CYBER SYSTEMS

Once the BES Subsystems have been mapped into the categories based on pre-defined criteria reflecting their impact on the BES, and all the essential functions performed by the BES Subsystems have been identified, the Responsible Entity uses this list to define those BES Cyber Systems that will support:

- The operation and control of these BES Subsystems

  Examples of these are HMI systems in Generating Stations and Transmission Substations, Generating Plant DCS systems, RTUs and PLCs with control and operation functions for BES elements, EMS systems providing control and operate functions for operators

- The monitoring and alerting functions for the reliability or operability of these BES Subsystems

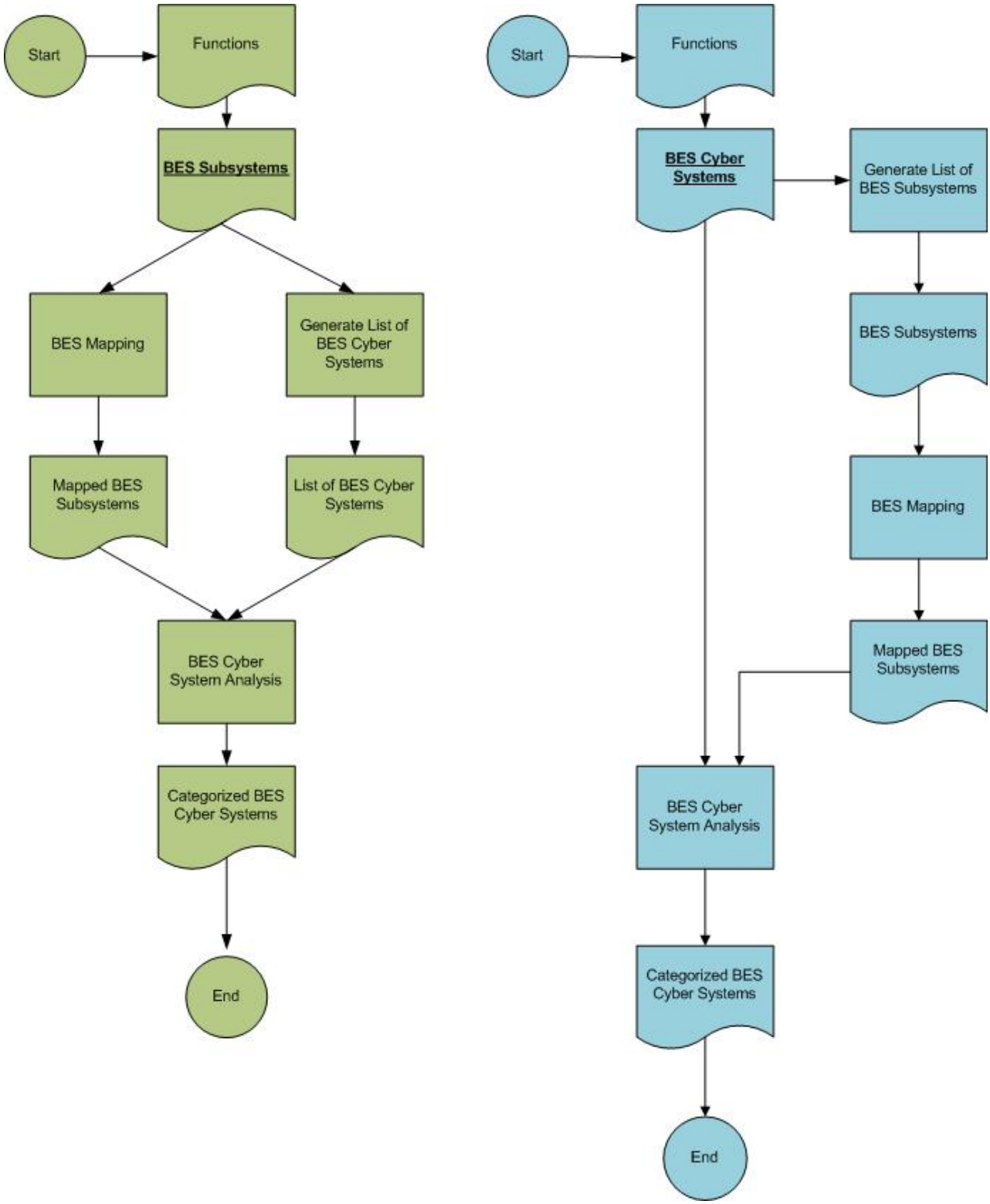
  Examples of these are RTUs providing remote metering functions, Dynamic Feeder Rating systems

- The data acquisition equipment and systems that support wide-area situation awareness for automated or operator assisted real-time reliable operation of these BES Subsystems

  Examples include Phasor Measurement Units when used in State Estimators for real-time operator assisted actions/alerts.

The approach described in this concept paper relies on initially identifying the BES subsystems, then mapping them to pre-defined criteria, and finally categorizing the associated BES cyber systems. Entities may choose to use an alternative approach of: inventorying all their BES cyber systems; analyzing them based on the criteria defined in BES impact mapping of the BES subsystems they support; and utilizing the categorization methodology described later. Both result in the set of categorized BES cyber systems for application of requirements or controls. In both approaches, the BES mapping process is required to determine the impact on the BES.

Figure 2


Start
Functions
BES Subsystems
BES Mapping
Generate List of BES Cyber Systems
Mapped BES Subsystems
List of BES Cyber Systems
BES Cyber System Analysis
Categorized BES Cyber Systems
End
Start
Functions
BES Cyber Systems
Generate List of BES Subsystems
BES Subsystems
BES Mapping
Mapped BES Subsystems
BES Cyber System Analysis
Categorized BES Cyber Systems
End

The focus of this impact categorization is on BES Cyber Systems since they directly support the reliability functions of the BES, but the process does not preclude consideration of other Cyber System components. Determining the full Target of Protection is an important step prior to applying security controls, and its impact categorization is inherited from the BES Cyber Systems within.

G. CATEGORIZATION OF CYBER SYSTEMS

The proposed criteria for the categorization of BES Cyber Systems are based on their impact on the functions of the BES Subsystems they support. For each BES Cyber System, a Responsible Entity determines the impact of the loss of confidentiality, integrity, and availability resulting from its loss or compromise to the functions of the BES Subsystem it supports. Categories of impact are defined as follows:

- **High** if the loss of confidentiality, integrity, or availability directly causes or contributes to the loss or compromise of the integrity or availability of the BES Functions it supports.
- **Medium** if the loss of confidentiality, integrity, or availability directly affects the BES Functions it supports, but is unlikely to lead to the loss or degradation of operational integrity or availability of the functions.
- **Low** if the loss of confidentiality, integrity, or availability would not be expected to affect the BES Functions it supports.

This methodology recognizes that a single Cyber System may support multiple BES function types and/or BES Subsystems as shown in Figure 3. For example, a SCADA system may provide automated generation control signals to a generator with minimal impact on the BES. However, the same SCADA system also provides control for substations on a high impact transmission line. As a result, the Responsible Entity would assign the final security categorization as *High* for the SCADA system.

This categorization approach makes two important advancements to ensuring a more complete and accurate assessment of Cyber System impact on the BES. First of all, the impact analysis requires a consideration of the functions of the BES Subsystem it supports. Secondly, the categorization ties directly to the security requirements of the Cyber System. As a result, the later security control selection should have its basis in reducing risk to the BES caused by a

Cyber Security Incident.

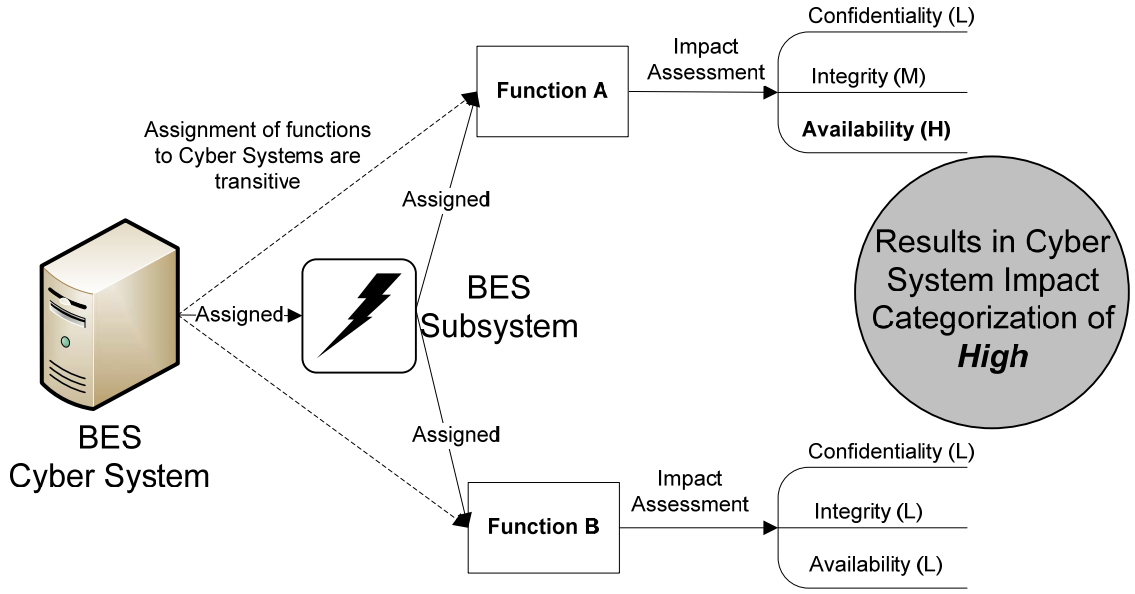


Figure 3: Cyber System Security Impact Categorization

H. FINAL CATEGORIZATION OF CYBER SYSTEMS BASED ON OVERALL IMPACT ON THE BES

The final categorization of each cyber system is determined by a matrix which has predetermined outcomes. The pre-determined categorization of the cyber system is based on both the impact mapping of the supported BES Subsystem and the impact of the cyber system on the BES function it supports.

This deterministic methodology will provide a more consistent approach and result than the looser requirement of a risk-based methodology included in CIP-002-1 and CIP-002-2. The approach is based on an impact based methodology and will provide for more uniform application of a methodology for categorizing cyber systems.

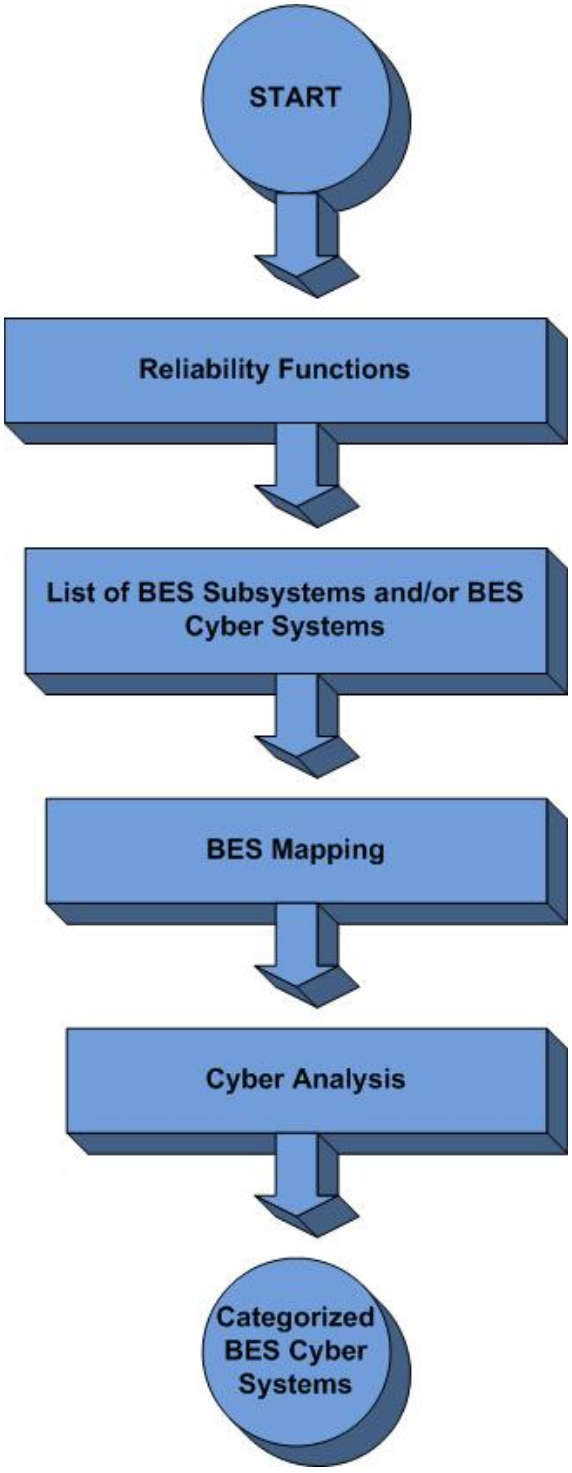
An example of the application of this approach in an evaluation matrix is shown below:

> **Note:** *Table 2 is a visual representation of what the categorization can look like, it's not the actual table.*

Table 2

Asset Impact -->	**High**	**Medium**	**Low**
Cyber Impact:			
High	H	H	H
Medium	H	M	M
Low	H	M	L

Figure 4


START
Reliability Functions
List of BES Subsystems and/or BES Cyber Systems
BES Mapping
Cyber Analysis
Categorized BES Cyber Systems

I. DEFINING THE TARGET OF PROTECTION

Up to this point, the process being laid out has focused on determining the impact that BES Cyber Systems have on the BES. The process now shifts to the Responsible Entity **protecting** the BES Cyber Systems; this begins with defining the set of both BES and non-BES Cyber Systems that must be protected to provide an adequate level of protection to the BES Cyber Systems. This resulting set of Cyber Systems is defined as the *Target of Protection*, to which a Responsible Entity would apply appropriate security controls.

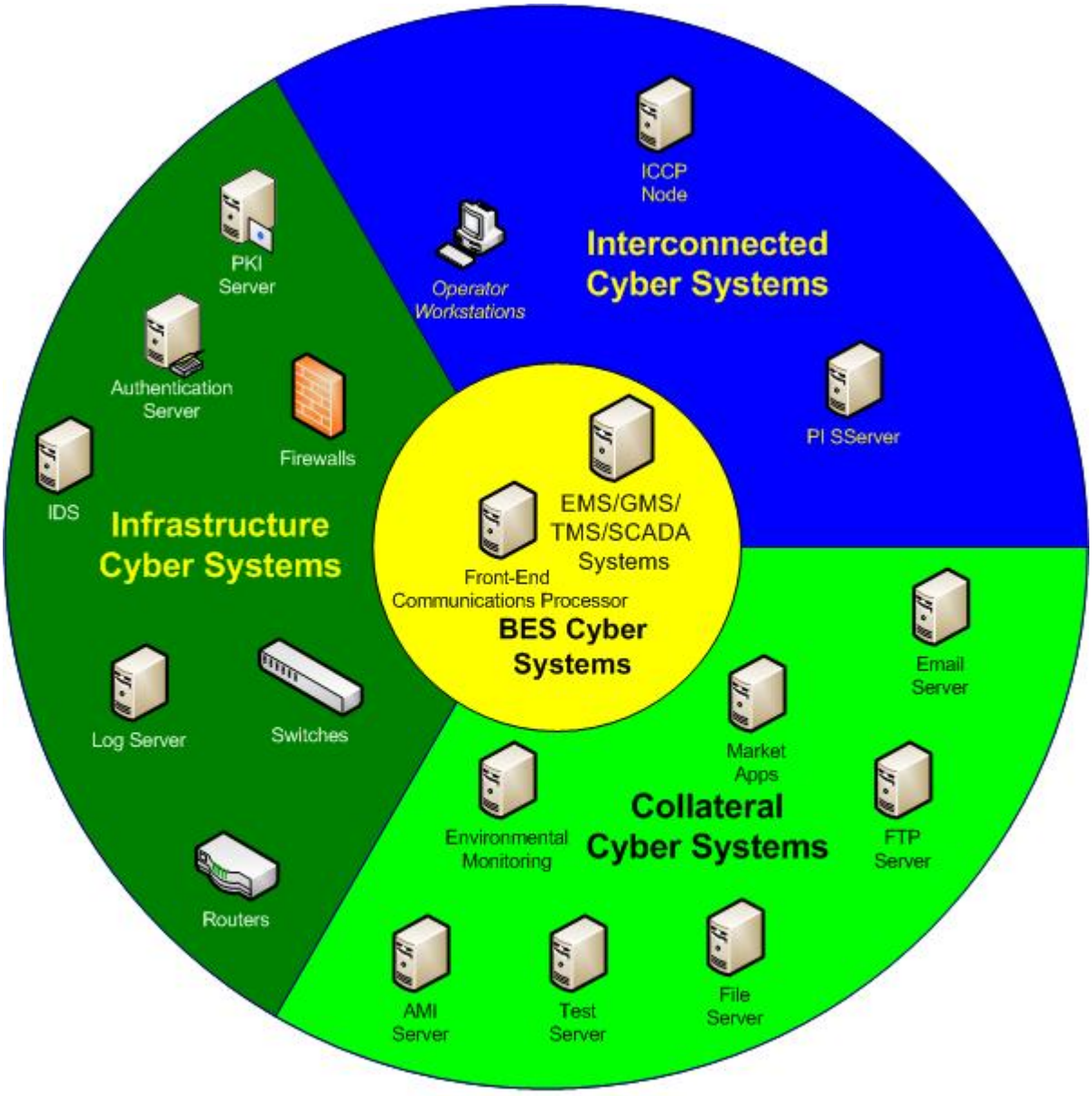
To form the Target of Protection, the Responsible Entity would start with the BES Cyber System and determine any additional *Interconnected Cyber Systems* supporting the mapped BES function(s). These Interconnected Cyber Systems may have involvement with the exchange and display of data but do not necessarily perform the BES function(s) themselves. Examples include historical data collectors, ICCP Nodes, Operations Support Workstations, etc. It is important to stress that these interconnected Cyber Systems may both exist outside of the traditional Electronic Security Perimeter and be operated external to a Responsible Entity. Those third-party interconnected Cyber Systems are discussed further in the next section.

In addition to the identified interconnected cyber systems, the Responsible Entity would also determine those Cyber Systems supporting the confidentiality, integrity, availability and non-repudiation requirements of the BES and Interconnected Cyber Systems. Examples of these may include routers, switches, firewalls, components involved in access-control and/or security monitoring, virtual server management, environmental control and/or monitoring systems.

A final class of Cyber Systems is incorporated within the Target of Protection only on the basis of their locality within a network segment or operating environment. The Responsible Entity can remove these *Collateral Cyber Systems* from the operating environment with no significant effect to the BES function, but an attacker could utilize its otherwise relaxed security posture to attack the function. As an example, an email server, while not supporting the BES function, may be located on the same network segment as the Interconnected or Infrastructure Cyber Systems. This introduces an unnecessary vulnerability and should be moved out of that network segment.

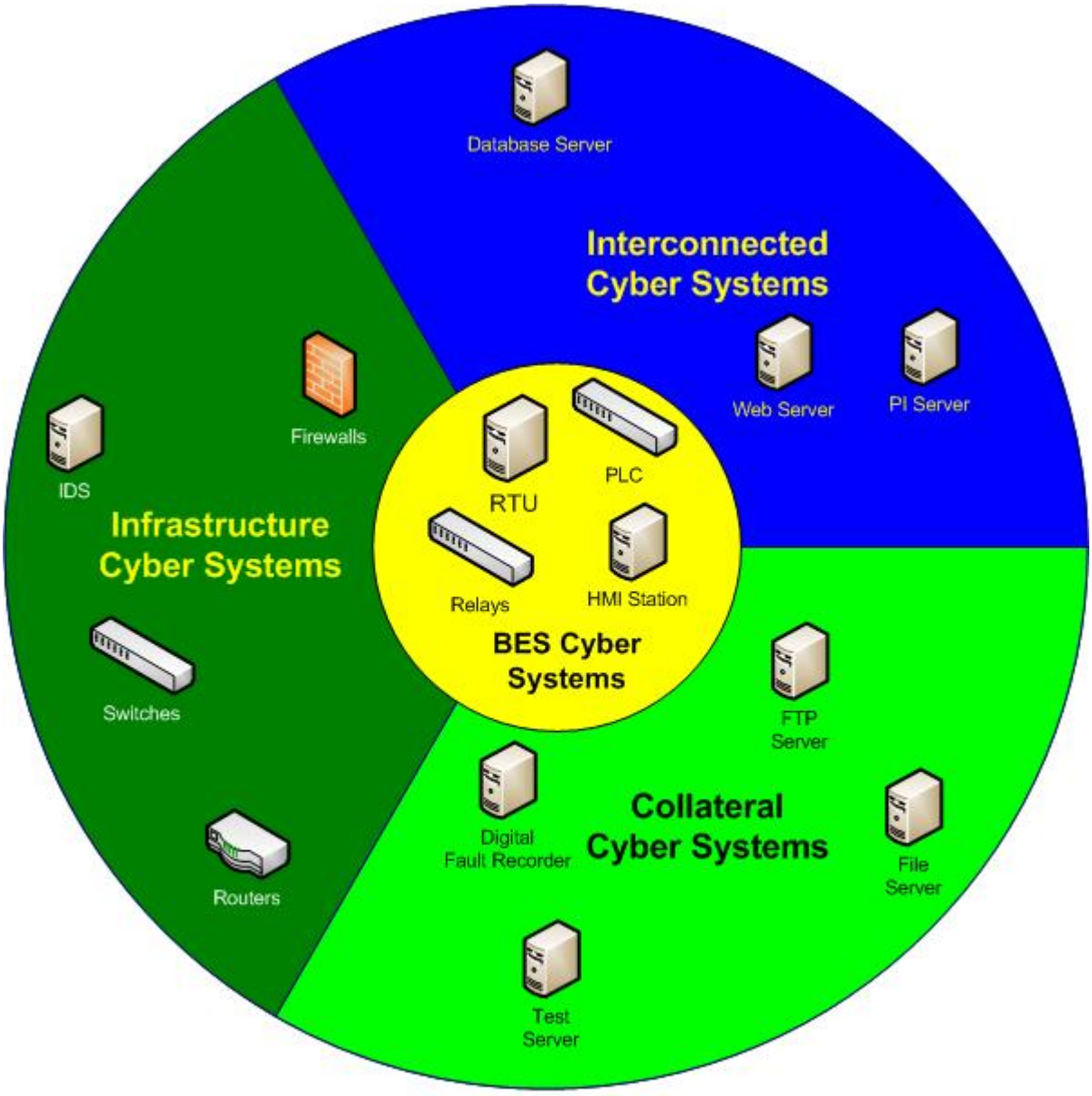
Examples of defining the Target of Protection are illustrated in the following diagrams. The systems in these figures are only specified for representation and may differ based on their functional role associated with the BES Cyber System.

Figure 5



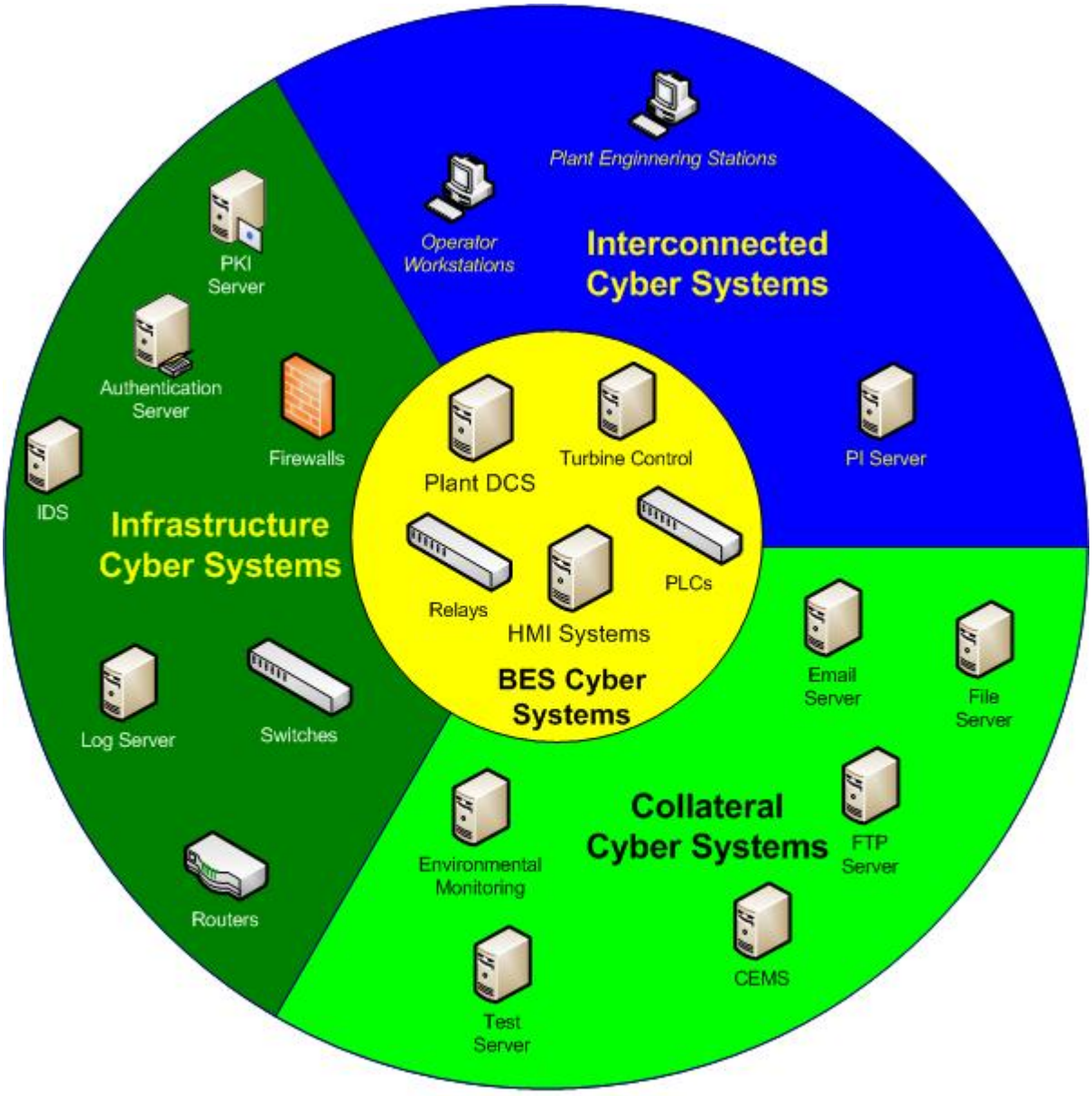
Target of Protection – Control Center

Figure 6



Target of Protection – Transmission Substations

Figure 7



Target of Protection – Generation

A Responsible Entity has flexibility in defining a Target of Protection to maximize efficiency in secure operations. They may choose the definition to include all Cyber Systems responsible for carrying out a single function or they may define it based on network proximity. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly would make the secure operation difficult to monitor and assess. To determine the Target of Protection, the Responsible Entity would take into account the operational environment and scope of management.

As an example, consider the following diagrams. A Responsible Entity may declare the entire SCADA cyber system to include supervisory control servers and field devices or multiple, similarly designed substation networks as a single Cyber System. This may make sense if they all lie under the same operational management. Or it may choose to define the few essential components in a substation network as the Cyber System.

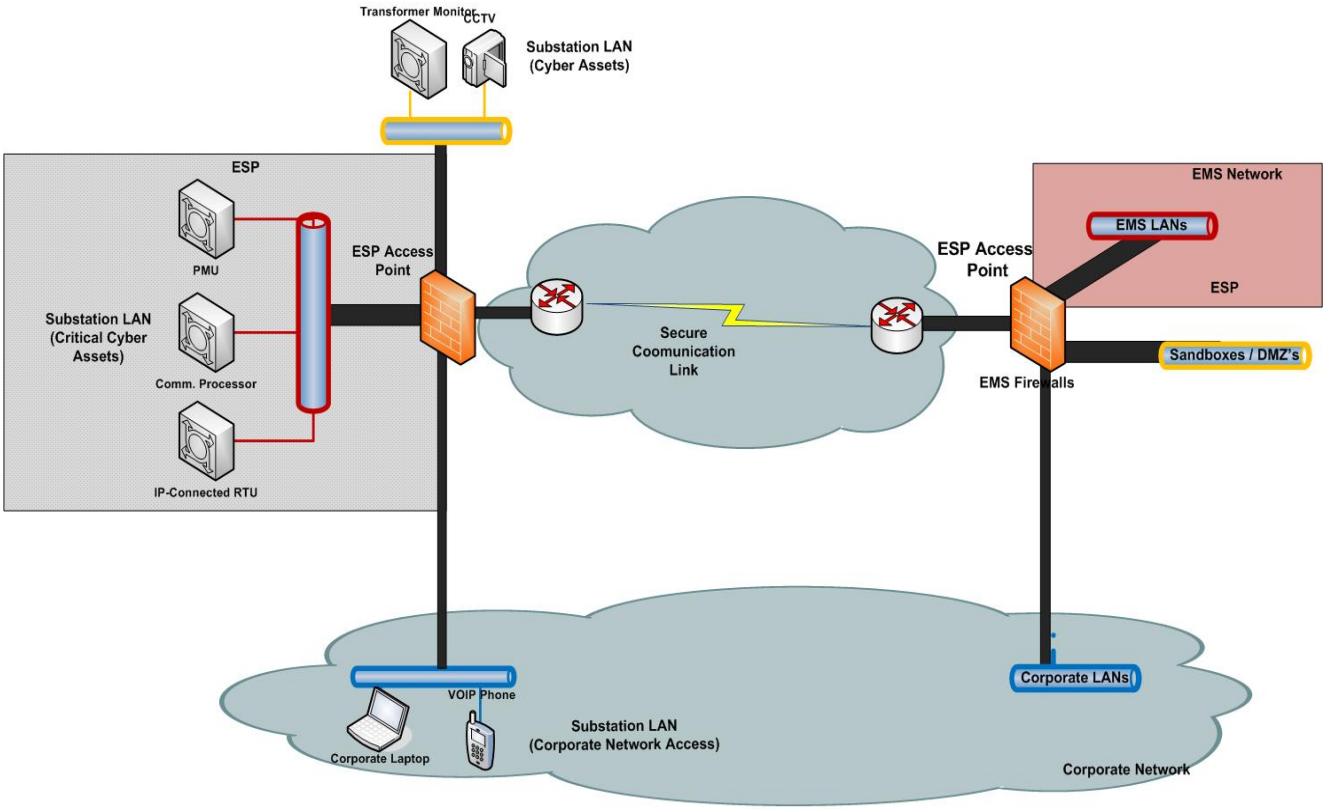


Figure 8 — SCADA and Substation Cyber System — Separate Security Perimeters

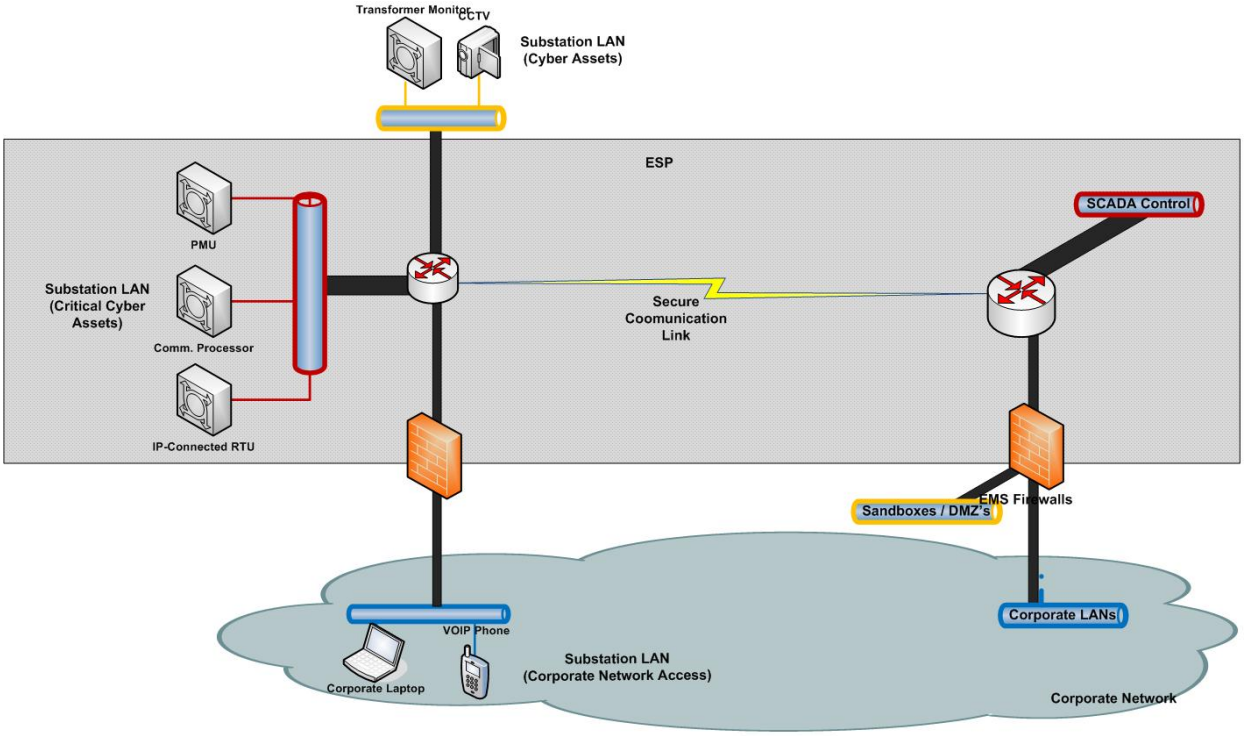


Figure 9 — SCADA and Substation Cyber System — Single Security Perimeter

J. EXTERNAL CYBER SYSTEMS

Cyber Systems performing functions of the BES exist within a complex network of interconnections and information exchange across multiple organizations. Just as a downstream fault could cause cascading power outages, so too, a compromise of one Cyber System could utilize a trusted path to impact multiple other Cyber Systems. Consequently, to achieve the desired protection level in the BES Cyber System, these external party dependencies cannot be ignored in establishing the Target of Protection.

As components of the Target of Protection cross organizational boundaries, the Responsible Entity with operational responsibility for the BES Cyber System should identify and manage the risk of these dependencies. This would include the identification of third party service providers operating within the Target of Protection, but it may also include a third party data connection outside of the traditional Electronic Security Perimeter.

As an example, if Utility Alpha categorizes one of its Cyber Systems as High and identifies an external interconnection with Company Beta as part of the Target of Protection, then Utility Alpha owns the risk associated with the interconnection and has the responsibility to mitigate the risk.

This approach ensures the standards consider the complex nature of Cyber Systems to protect the reliability or operability of the BES and assist organizations operating Cyber Systems downstream to understand their impact on the BES.

K. APPLYING SECURITY CONTROLS TO THE TARGET OF PROTECTION

At this point in the process, a Responsible Entity has assigned an impact category to a Cyber System and determined their Target of Protection. Now the remaining task involves mitigating the risk posed to the BES by applying an appropriate set of security controls and requirements to the Target of Protection. A crucial undertaking for the drafting team lies in developing these security controls in such a way as to mitigate risk while maximizing the value of the associated cyber security investment for the industry.

To accomplish this objective, the drafting team seeks to develop a library of controls (requirements) appropriate to the degree and type of protection needed. A part of this effort involves utilizing the impact categorization process. The underlying assumption for categorizing BES Cyber Systems is the need for differing levels of protection.

The application of security controls will consider the differences in contexts and characteristics in transmission substations, generating plants and control centers, their cyber equipment types and operating environments, and evaluate an approach to protect them without unduly requiring entities to invoke exception processes in the standards.

In the drafting of the controls and requirements, the drafting team will consider approaches to provide flexibility while ensuring adequate protection from dynamic and evolving threats and vulnerabilities. The drafting team will seek industry comments in the area of control specifications in future papers.

L. CONCLUSION

The approach proposed in this paper builds on work that the industry has already done in complying with the current standards, the guidance to be available soon in using a risk-based methodology for classifying BES Subsystems, the industry's experience and investments in current compliance programs, and a recognition that the reliability of the BES is based on an engineered system increasingly supported by cyber systems. It is an approach that represents a new paradigm and addresses many areas of the perceived or real deficiencies in the current CIP-002 standard. It seeks to ensure that all cyber systems related to the reliability or operability of the BES are required to implement a security posture commensurate to the level of criticality of the BES Subsystems they are supporting.

APPENDIX A: TERMS AND DEFINITIONS

Appendix A provides the defined terminology used throughout this concept paper. These terms are ordered here hierarchically to build upon each other and culminate to a definition of what the NERC Cyber Security Standards should seek to protect.

BES Subsystem	The set of BES assets necessary to perform or support a function or set of functions necessary to maintain an Adequate Level of Reliability in the Bulk Electric System. A BES Subsystem may be defined as a piece of equipment, a facility or system.
Cyber Asset [NERC Glossary]	Programmable electronic devices and communication networks including hardware, software, and data.
Cyber System	A discrete set of Cyber Assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (It is important to note the term system is used by itself in places throughout this paper and should not be considered interchangeable with Cyber System. A system performing a reliability function of the BES may be either electromechanical, manual or cyber in nature.)
BES Cyber System	A Cyber System directly supporting reliability functions of the BES. The term *BES* distinguishes the Cyber System from those which do not directly relate to a BES function for the purpose of simplifying the categorization process. Examples of *BES Cyber Systems* may include SCADA/EMS systems, generation DCS, RTU providing control, or HMI Workstations.
Interconnected Cyber Systems	Components necessary for BES *Cyber Systems* to perform their BES functions. These Cyber Systems may have involvement with the exchange and display of data but do not perform the BES functions themselves. Examples include historical data collectors, ICCP nodes or operations support workstations.
Infrastructure Support Cyber Systems	Components supporting the confidentiality, integrity, and availability of the BES and *Interconnected Cyber Systems*. Examples include routers, switches, firewalls, components involved in access-control and/or security monitoring, virtual server management, and environmental control and/or monitoring systems.

Collateral Cyber Systems	Other components included in the *Target of Protection* only on the basis of their locality within a network segment or operating environment.
Target of Protection	A Cyber System consisting of all components necessary to evaluate the desired level of resiliency in the BES functions the Cyber System provides and/or allows.