Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

NERC Cyber Security Standards Drafting Team for Order 706
06/15/2009 -Team

CATEGORIZING CYBER SYSTEMS: AN APPROACH BASED ON IMPACT ON BES RELIABILITY FUNCTIONS

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 supporting cyber systems, which are categorized based on impact. Third party oversight of the BES subsystem categorization ensures that the entire BES is adequately protected. 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 approach considers the major concerns expressed in FERC's Order 706.

The methodology in the approach proposes a categorization of BES subsystems based on their impact on the reliability or operability of the BES, and a parallel categorization of their associated cyber systems and their elements based on their impact on the BES subsystems they support. A rigorous merger of the two categorizations for any given cyber system results in a deterministically derived categorization of each cyber system essential to the function (essential cyber systems) based on its impact on the BES.

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 essential cyber systems and systems which are collaterally affected because of their proximity to essential 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.

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.

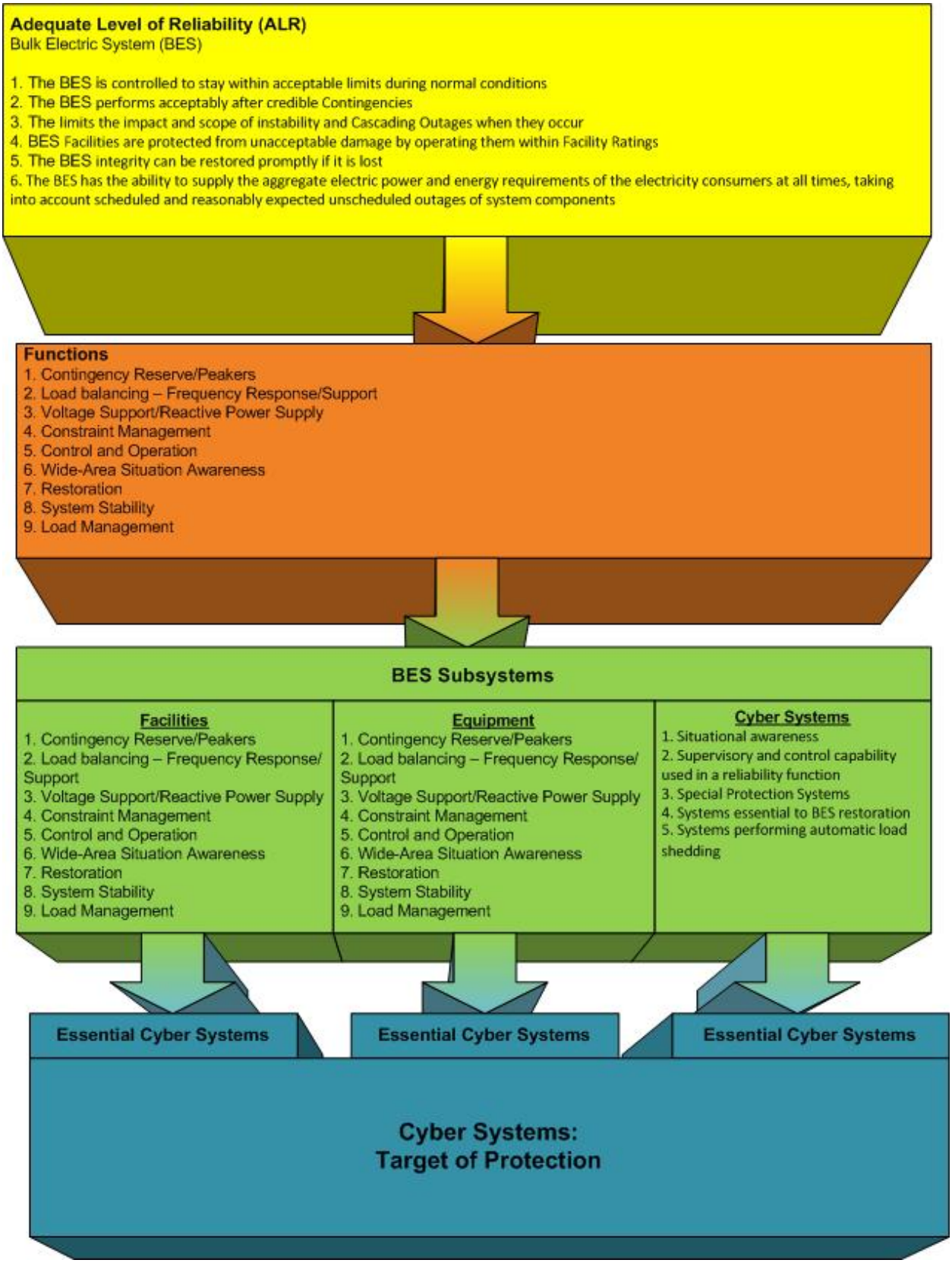
This paper describes an approach based on the concepts of NERC's definition of Adequate Level of Reliability (ALR) and the characteristics of the BES described therein that will achieve this ALR, namely:

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 essential to the reliable operation of these BES subsystems: 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.


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
Essential Cyber Systems
Essential Cyber Systems
Essential Cyber Systems
Cyber Systems:
Target of Protection

Once BES subsystems and their cyber systems are identified, the methodology proposes a two pronged categorization which results, on one side, in a categorization of BES subsystems based on their impact on the reliability or operability of the BES, and on the other, a categorization of their associated cyber systems and their elements based on their impact on the BES subsystems they support. A rigorous merger of the two categorizations for 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 exclude 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 which may be in a nuclear facility associated with the BES which 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 which 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 group 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 concepts and approach in this paper draw on elements of approaches already described in several presentations by members of the Cyber Security Standard Drafting Team. The presentations to the team members include the application of a FIPS199-like approach to classifying Cyber systems, NIST integration, a cyber systems based approach and discussions on

guiding principles used for development, as well as comments and discussions by other members of the drafting team.

This proposed cyber system categorization approach includes the consideration of NERC's mission, the essential functions necessary in achieving this mission, an impact based methodology to categorize its BES subsystems 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 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.

BES RELIABILITY FUNCTIONS

A pre-requisite to the start of the identification of BES Subsystems which affect the reliability or the operability of the BES is the identification of functions which 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 and operability of the BES.

Functions, subsystem criteria, together with sample BES subsystems and cyber systems, are provided for illustrative purposes, and are not intended to be a final, comprehensive, exhaustive list.

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 center
Load Balancing Frequency Response/Support	Single resource or combined resources (sharing a common mode failure) whose loss or compromise may result in underfrequency Transmission facility or facilities, whose loss or compromise may result in underfrequency	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 center
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	Static VAr Compensator Capacitor bank(s) Synchronous Condenser(s) Generation Unit(s)	Automated Control System SCADA RTU Protective Relay

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
	Interface Requirements	Transmission lines, busses and transformers associated with the such generation	
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 SCADA RTUs
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	SCADA EMS AGC ICCP RTU

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
Wide-area 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): – which are essential to the initial BES restoration	Black Start generation unit(s) Reactors, Capacitors Load (distribution feeders) Transformers Transmission Lines	Generation control system SCADA RTU Protective Relays
System Stability	Generation resources, transmission facilities and Special Protection Systems whose loss or compromise may result in: – IROL violation – Voltage collapse (wide-	Transmission lines impacting IROL(s) Generating Unit(s) supporting frequency (with large governor response)/voltage stability/supporting	Protective relays Generation control centers Associated control systems

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
	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	on constraint management on IROLs Capacitor bank(s) Static VAR compensator(s) Synchronous Condensers	
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 (eg. remote access, relay setting change) Dynamic Ratings monitoring Physical Security System	Dynamic Feeder Management System Support systems used to modify cyber systems (eg. remote access, relay setting change) Dynamic Ratings monitoring Physical Security System

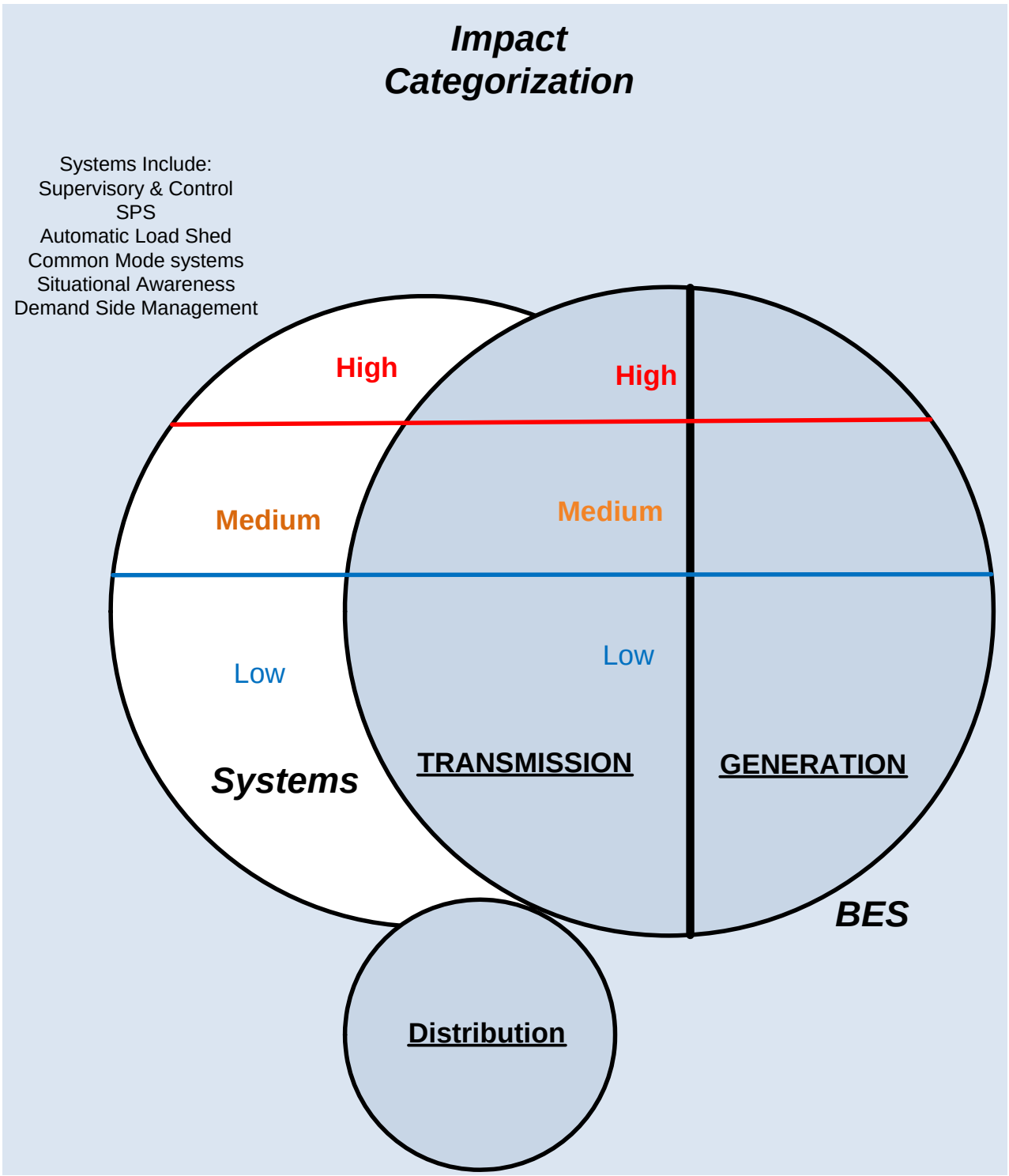
IDENTIFICATION OF BES SUBSYSTEMS

The functions above are then used to identify all BES Subsystems which support them. The inclusive list of these identified BES Subsystems constitute the overall scope for application of criteria for their categorization 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 that specific system. A centralized, automated, programmable area load shedding system is an example of a system which would be categorized both as a BES Subsystem and as a Cyber System.

In particular, the BES Subsystems must include facilities, equipment, and cyber systems that perform the following functions:

- Situational awareness
- Supervisory and control capability used in a reliability function
- Special Protection Systems
- Systems essential to BES restoration
- Systems performing automatic load shedding
- Other systems that may perform a function directly related to the reliability or operability of the BES.


Impact Categorization
Systems Include:
Supervisory & Control
SPS
Automatic Load Shed
Common Mode systems
Situational Awareness
Demand Side Management
High
High
Medium
Medium
Low
Low
Systems
TRANSMISSION
GENERATION
BES
Distribution

CATEGORIZATION OF BES SUBSYSTEMS

Identified BES subsystems are categorized based on their impact on the reliability and operability of the BES: this categorization will be based on criteria, in the functions they provide or support, which determine the level of that impact. For example, a broad categorization can be illustrated as follows:

The potential impact is **High** if the loss of or compromise of the BES Subsystem directly causes or contributes to BES instability, separation, or a cascading sequence of failures, or places the BES at an unacceptable risk of instability, separation, or cascading failures.

The potential impact is **Medium** if the loss or compromise of the BES Subsystem directly affects the electrical state or the capability of the BES, or the ability to effectively monitor and control the Bulk-Power System, but is unlikely to lead to BES instability, separation, or cascading failures.

The potential impact is **Low** if the loss or compromise of the BES Subsystem would not be expected to affect the electrical state or capability of the BES or the ability to effectively monitor and control the BES.

Work in defining the criteria and categorization levels is under way by a special Standards Drafting Team subgroup with expertise in BES planning and operating areas.

THIRD PARTY OVERSIGHT OF BES SUBSYSTEMS AND THEIR CATEGORIZATION

Oversight of the appropriate categorization of BES Subsystems is necessary to ensure that the Bulk Electric System is adequately protected by the CIP Standards. One approach to the oversight review function can be performed according to the following hierarchical structure:

- Entities performing the functions of Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Transmission Operator, Generator Owner, Generator Operator, and/or Load Serving Entity submit their categorized list of BES Subsystems to third party for review.
- Each Reliability Coordinator submits its categorized list of BES Subsystems to its Regional Entity for review.
- Each Regional Entity submits its categorized list of BES Subsystems to NERC for review.

- NERC has its categorized list of BES Subsystems reviewed by the Regional Entities.

The role of the third party reviewer is to take advantage of their wide-area perspective of the BES, and examine a Responsible Entity's list of categorized BES Subsystems, with the goal of ratifying the decisions of the Responsible Entity's BES Subsystem impact categorization. Based on their wide-area view and consistent with FERC Order 706, reviewers may increase, but not decrease the categorization of BES Subsystems. Additionally, reviewers may add, but not remove BES Subsystems from a Responsible Entity's list. A reviewer must provide written justification for any modifications that they enforce upon a Responsible Entity. Decisions about any modification must be justified with a statement as to why the reviewer believes the asset has been incorrectly categorized, and rationale for the new categorization level. The rationale must include the specific BES Functions that the reviewer believes will be impacted, and the reason that the new impact categorization is more appropriate than the current categorization.

The identification of the entity that will perform the third party review raises many issues.

In response to the NOPR originating FERC order 706 and in the final rule, two primary entities have been identified to perform the review of "Critical Assets": the Reliability Coordinator and the Regional Entity.[1] Of the 17 Reliability Coordinators in the NERC Compliance Registry, 12 are registered under multiple functions (i.e. BA, TOP, IA, TSP, TP, PC). These 12 RCs could not meet the FERC requirement for "external" review in order 706 for their other registered functions. As an example, Midwest ISO is registered as a RC, BA, PA, and TSP. Midwest ISO RC could not review the list of BES subsystems from the Midwest ISO BA while meeting the FERC requirement for an "external" review. Thus, a third party review of the third party review would be required.

While RCs clearly have the wide-area review that is needed to conduct a review of "Critical Asset" lists, they may lack the detailed knowledge of the BES that is necessary to thoroughly review BES subsystems. As an example, a circuit breaker may be identified as a BES subsystem. The RC may lack the detailed knowledge of the BES to know the criticality of the CB.

The Regional Entity serving as the third party reviewer brings its own issues as well. Historically, the Regional Entity generally has not had a wide area view of the reliability of the BES and its assets in that it does not operate the BES nor provide reliability services. While many but not all Regional Entities are developing Situational Awareness capabilities through the

[1]We are assuming that the portion of the Order 706 that applies to "external review of critical assets" will also apply to reviewing the categorization of BES subsystems.

Situation Awareness for FERC, NERC and Regional Entities (SAFNR) project, the Reliability Coordinator registered function, not the Regional Entity registered function, is responsible for regional situational awareness and response. As such, the Regional Entities may not uniformly have the staffing and expertise necessary to perform the third-party review of a registered entity's BES subsystems list. Additionally, the Regional Entity might find itself in a conflict of interest. In performing its Compliance Monitoring and Enforcement role, the Regional Entity is charged with auditing the CIP standards for compliance, including the determination of Critical Assets and Critical Cyber Assets under the current version of the standards. This will not change with the revision to the asset identification approach. It is probably not appropriate to require the auditing entity to provide assistance to the audited entity in the form of a third-party review outside of the audit process.

The oversight process will include an arbitration process for disputes that will follow a process modeled after that in the NERC Rules of Procedure (sections in Chapter 400). Once adjudicated, categorization decisions are final and binding.

IDENTIFICATION OF ESSENTIAL CYBER SYSTEMS

Once the categorized list of BES Subsystems has been defined, and all the essential functions performed by the BES Subsystems have been identified, the Responsible Entity uses this list to define those Essential Cyber Systems which 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 which 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 focus of this impact categorization is on Essential 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 Essential Cyber Systems within.

CATEGORIZATION OF CYBER SYSTEMS

The proposed criteria for the categorization of Essential Cyber Systems are based on their impact to the functions of the BES Subsystems they support. For each Essential 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 functions of the BES Subsystem it supports.
- **Medium** if the loss of confidentiality, integrity, or availability directly affects the functions of the BES Subsystem 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 functions of the BES Subsystem it supports.

This methodology recognizes that a single Cyber System may support multiple BES function types and/or BES Subsystems as shown in Figure 2. 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 to 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.

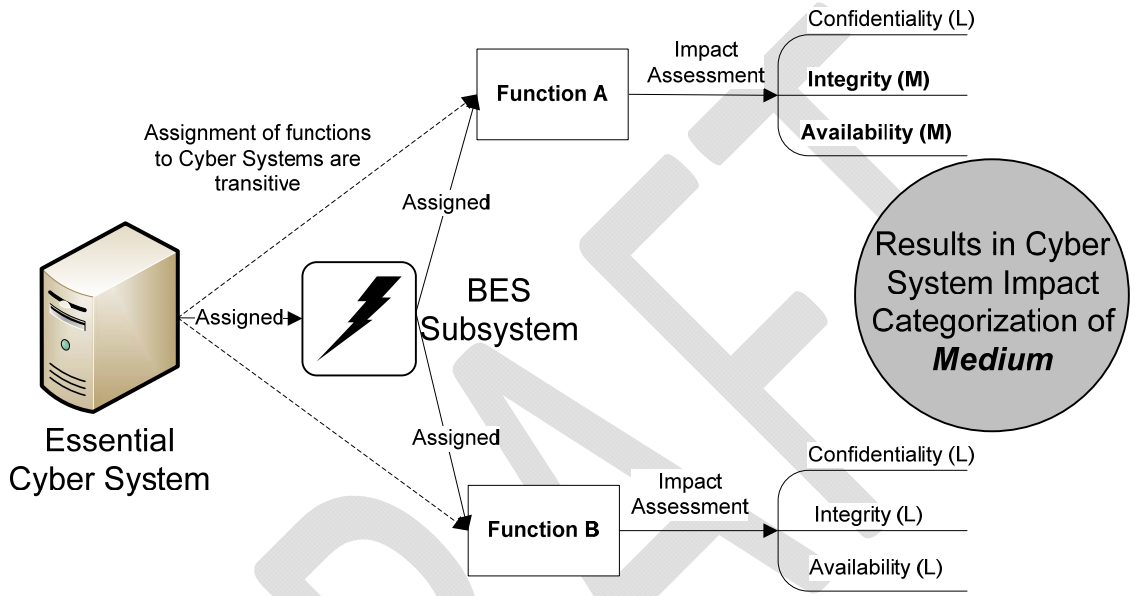
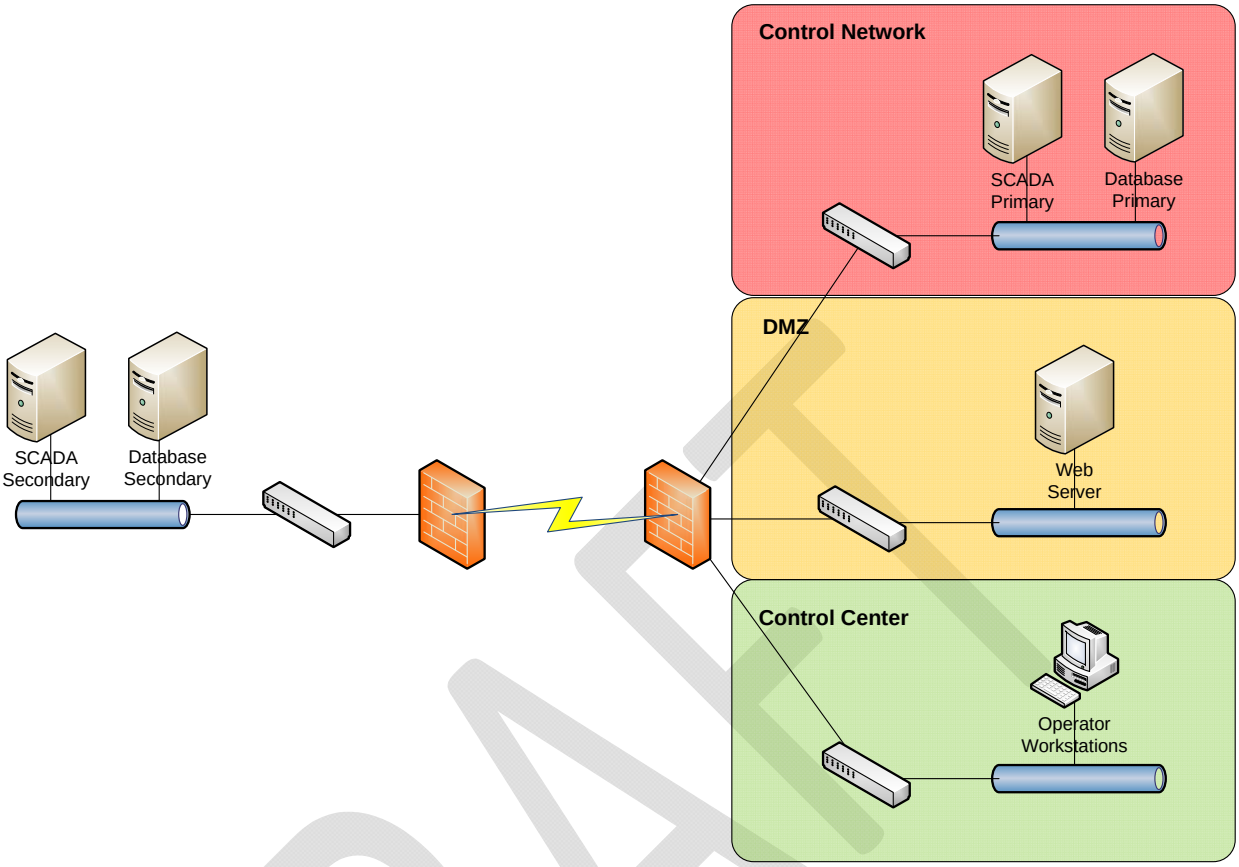


Figure 1: Cyber System Security Impact Categorization

CYBER SYSTEM INTERCONNECTIONS

Many Essential Cyber Systems exist within a complex network of interconnected Cyber Systems and exchange information necessary for the reliable operation of the BES. 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, the security protection level of the Essential Cyber System should reflect the level of risk associated with any interconnections.



Dependencies of an Essential Cyber System may be both ***internal*** and ***external*** to a Responsible Entity. The exercise of identifying the Target of Protection after Cyber System categorization addresses the ***internal*** dependencies. During this process, all Infrastructure Support Cyber Systems, internal Interconnected Cyber Systems, and Collateral Cyber Systems are identified. These may include network infrastructure, boundary protection components, access control and security monitoring components, etc.

EXTERNAL CYBER SYSTEM DEPENDENCIES

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 assurance level in the Essential Cyber System, these 3rd party dependencies cannot be ignored in establishing the Target of Protection.

As components of the Target of Protection cross organizational boundaries, the organization with operational responsibility of the Essential 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. Utility Alpha can accomplish this through appropriate Service Level or other appropriate contractual Agreements and then authorizing and monitoring the connection as part of its secure operation of the Cyber System.

In the case where Company Beta is also a registered functional entity in the BES, they have the additional responsibility to work with Utility Alpha to incorporate the interconnection when Company Beta performs their BES Cyber System categorization.

The nature of interconnected Cyber Systems across multiple organizations is complex, and any associated security requirements should be. A Responsible Entity should define, authorize and monitor these interconnections as part of its secure operation of the Cyber System.

This approach ensures the standards address the complex nature of Cyber Systems used in the reliability or operability of the BES and assist organizations operating Cyber Systems downstream to understand the impact that these Cyber Systems have to the BES.

FINAL CATEGORIZATION OF CYBER SYSTEM BASED ON OVERALL IMPACT ON THE BES

The final categorization of each cyber system is determined by the application of a matrix which has predetermined outcomes based on the supported BES Subsystem categorization and the categorization of the cyber system derived from its impact on the BES Subsystem it supports.

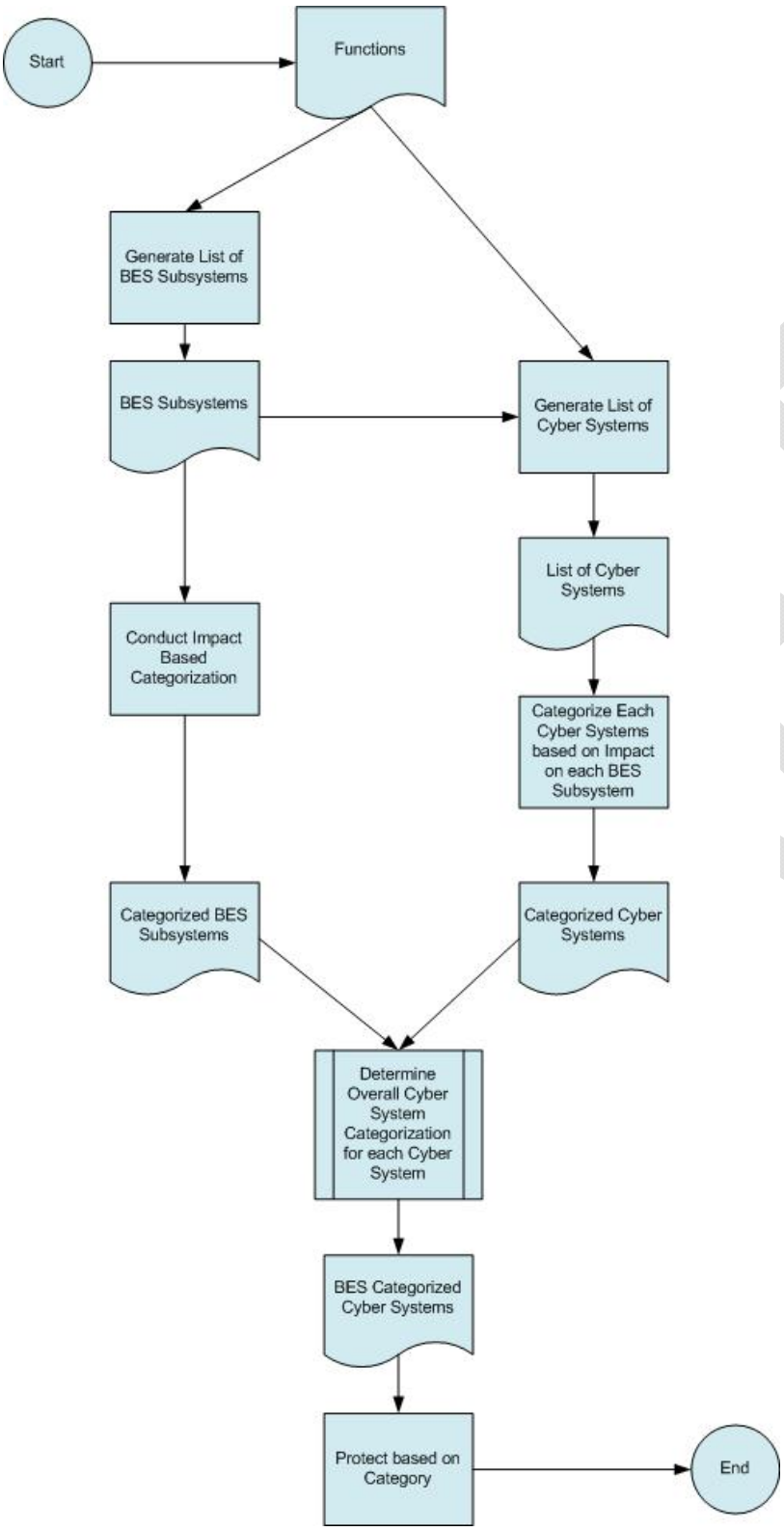
This deterministic methodology will provide a more consistent approach than the looser requirement of any risk-based methodology in CIP-002-1 and CIP-002-2. The approach is based

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:** *This table is a visual representation of what the categorization should look like, it's not the actual table.*

Asset Impact -->	High	Medium	Low
Cyber Impact:			
High	5	4	3
Medium	4	3	2
Low	3	2	1


Start
Functions
Generate List of BES Subsystems
BES Subsystems
Generate List of Cyber Systems
List of Cyber Systems
Conduct Impact Based Categorization
Categorize Each Cyber Systems based on Impact on each BES Subsystem
Categorized BES Subsystems
Categorized Cyber Systems
Determine Overall Cyber System Categorization for each Cyber System
BES Categorized Cyber Systems
Protect based on Category
End

DEFINING THE TARGET OF PROTECTION

Up to this point, the process being laid out has focused on determining the impact Essential Cyber Systems have on the BES. The process now shifts to the organization protecting the Essential Cyber Systems, and this begins with defining the set of Cyber Assets necessary to determine an adequate level of protection in the Essential Cyber System. This set of Cyber Assets is defined as the *Target of Protection*, to which an organization would apply appropriate security controls.

To form the Target of Protection, an organization would start with the Essential 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 an organization. Those third party interconnected Cyber Systems are discussed further in the next section.

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

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. An organization 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.

An example of defining the Target of Protection is illustrated in Figure 3. The systems in this figure are only specified for representation and may differ based on their functional role associated with the Essential Cyber System. Also, the radial distance of a Cyber System does not indicate its importance to the BES but rather the possibly sequential process of identification.

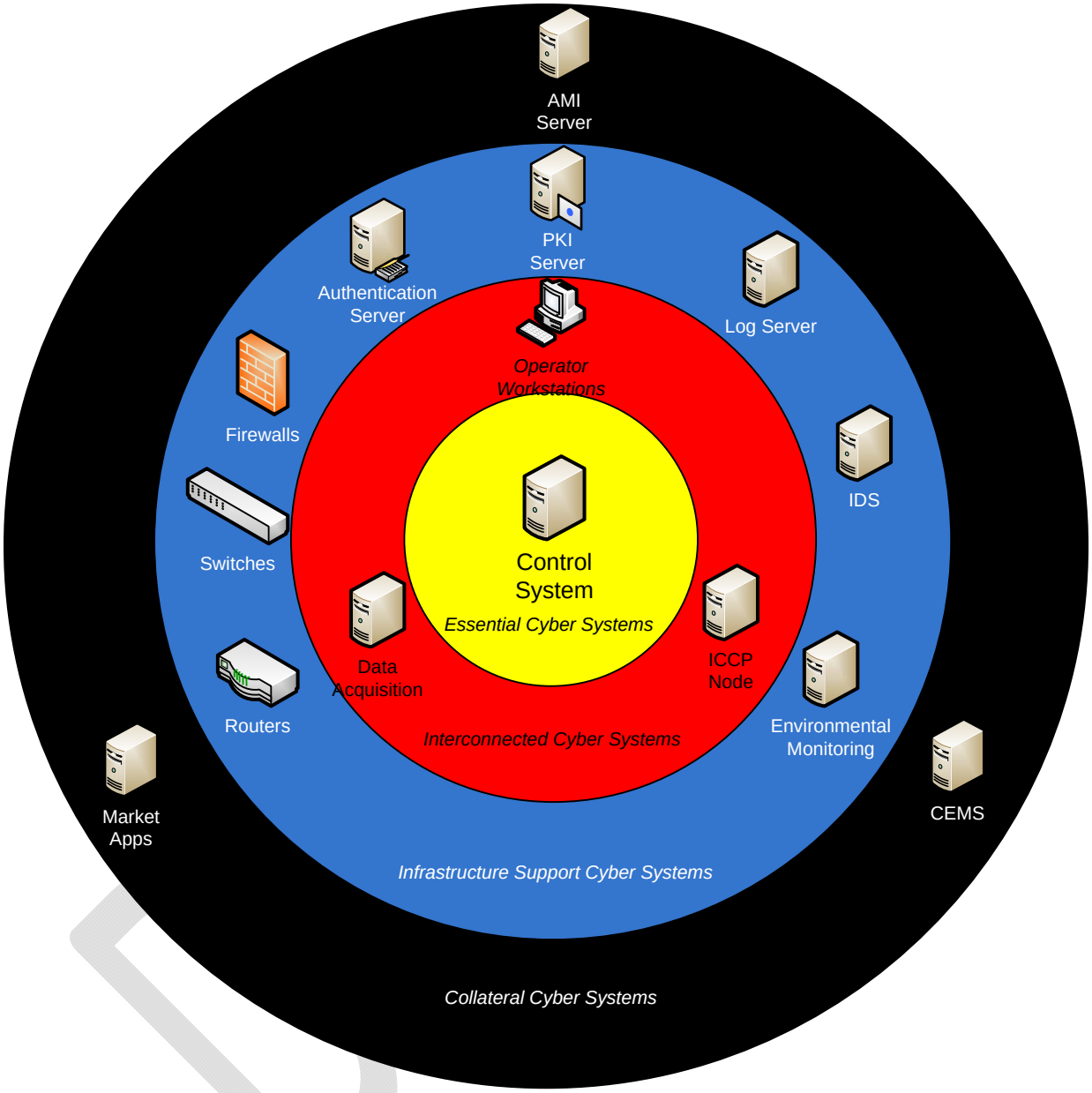


Figure 2: Target of Protection

APPLYING SECURITY CONTROLS TO THE TARGET OF PROTECTION

At this point in the process, an organization 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 Essential Cyber Systems is the need for differing levels of protection. The Standards can accommodate the levels of protection in a manner similar to NIST 800-53 Recommended Security Controls and the ISA99 Security Standards.

The Cyber Security Standard Drafting Team will review, change and augment the requirements in the current standards as necessary and appropriate based on an analysis of the catalog of controls in the NIST guidelines when mapped to the CIP requirements. It must be noted that the categorization resulting from the proposed CIP approach does not necessarily correspond to the categorization levels defined in the NIST guidelines. In particular, in the review of these standards, this paper proposes that consideration be made for the different general cyber system types and their capabilities. For example, the differences in characteristics of cyber systems built on general-purpose platforms from proprietary purpose-built systems will be considered: proprietary purpose-built systems may have vulnerabilities similar to general-purpose systems, and the preponderance of purpose-built systems and the implication on exception management, oversight and enforcement will be considered.

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

For example, limiting the requirement scope to specific components within the Target of Protection can provide one approach. For instance, certain network access control requirements might only apply to firewalls and malicious software protection might only apply to servers and workstations.

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.

CONCLUSION

The approach proposed in this paper builds on work which 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 incremental approach 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 reliable operation 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 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.)
Essential Cyber System	A Cyber System directly supporting reliability functions of the BES. The term *essential* 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 *Essential Cyber Systems* may include SCADA/EMS systems, generation DCS, RTU providing control, or HMI Workstations.
Interconnected Cyber Systems	Components necessary for *Essential 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 *Essential* 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.