

The logo for the North American Electric Reliability Corporation (NERC) features the acronym "NERC" in a large, bold, black sans-serif font. A horizontal blue bar is positioned directly beneath the letters.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Guidance for the Electric Sector: Categorizing Cyber Systems

A faint, light blue map of North America is visible in the background of the lower half of the page. The map shows the outlines of the United States and Canada.

to ensure
the reliability of the
bulk power system

December 2009

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

Table of Contents

Introduction	3
The Purpose of Categorizing BES Cyber Systems.....	3
Criteria for Impact Mapping of BES Subsystems.....	4
Acknowledging NIST’s Risk Management Framework.....	5
The role of this guidance.....	7
Categorizing BES Cyber Systems	7
Step 1: Performing a BES Subsystem Inventory.....	7
Step 2: Categorizing BES Subsystems	8
Step 3: Performing a BES Cyber System Inventory	8
Profiling BES Functions with Respect to Cyber Systems.....	8
Step 4: Perform an Impact Categorization for each BES Cyber System.....	9
Step 5: Monitoring for Changes to the System.....	10

Introduction

Critical infrastructure provides the essential services that underpin our society. Among the most important of the essential services is the Bulk Electric System (BES), which includes the capabilities of generation and transmission of electricity throughout North America. The industry, through NERC, has gone through the continuous refinement of the Cyber Security Standards since 2003 with the first mandatory set of standards approved by FERC on January 18, 2008 in FERC Order 706. This refinement has led to several revisions of the standards. As the standards have evolved, they had moved from an approach of “one size fits all,” to one that is better aligned with a strategy of risk management, with the goal of prioritizing the protection of Cyber Systems based on their potential impact on the BES and applying security controls appropriate to that potential impact.

The Purpose of Categorizing BES Cyber Systems

Having multiple impact categories for BES Cyber Systems will result in the application of more appropriate security controls across a broader spectrum of assets. To accomplish this, the NERC CIP Cyber Security Standards take a functions-based approach as a means to measure impact a particular Cyber System component has to the BES. Attachment 2 of CIP-002-4 identifies several functions as a set of activities that utilities perform to maintain BES reliability. BES Cyber Systems need to be “secure” – not for the sake of being secure; but to provide assurance (i.e., grounds for confidence) in the resiliency of these functions. The functions necessary to maintain BES reliability represent a path by which utilities can identify which of their Cyber Systems are essential to or can adversely impact the BES.

Ultimately, the impact-based categorization approach has the purpose of reducing risk to the performance of functions. Hazards to the Cyber System can have an impact to the functions being performed and the security constraints of the Cyber System should reflect this. For example, a generating unit designated as Reliability “must run” could imply a 24x7 availability constraint for the generation control system. Likewise, the selection of security controls should reflect the assurance needed in meeting this constraint. This relationship is shown in Figure 1. The degrees to which a Cyber System can impact the reliable operation of the BES establish the type and amount of security controls that are necessary.

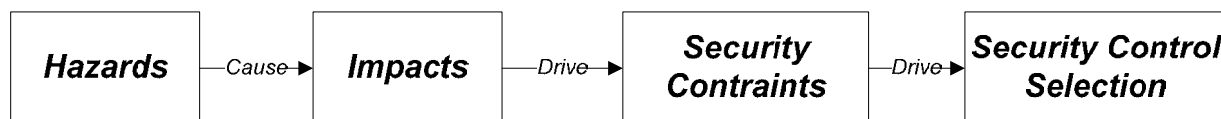


Figure 1: Connecting Avoidance of Hazards to selection of Security Controls

Criteria for Impact Mapping of BES Subsystems

Attachment 1 of CIP-002-4 lists categorization criteria which detail characteristics of BES Subsystems having the potential to impact the BES. The criteria have their basis in impact thresholds associated with BES functions and are patterned after criteria used in categorizing bulk power events. A **High** threshold indicates BES Subsystems, which if compromised or rendered unavailable, would significantly affect the integrity of BES system operations. A **Medium** threshold indicates BES Subsystems, which if compromised or rendered unavailable, would directly affect the capability of the BES. The **Low** category applies to all other BES Subsystems.

These thresholds are defined to provide a straightforward and objective path for a utility to determine the impact categorization of its BES Subsystems. The alignment of potential impacts to BES Subsystems enables a categorization of the inventory of assets relative to potential impact, resulting in a prioritized list of assets that must be protected to ensure the reliability of the BES.

The Cyber Systems which support the functions being performed by the BES Subsystem inherit the impact category. With this categorization of impact, it is possible to evaluate the BES Cyber Systems to determine where they fall on the scale in Figure 2. Consequently, industry resources can be more effectively used to apply the most protection on the smaller number of Cyber Systems with the highest potential impact.

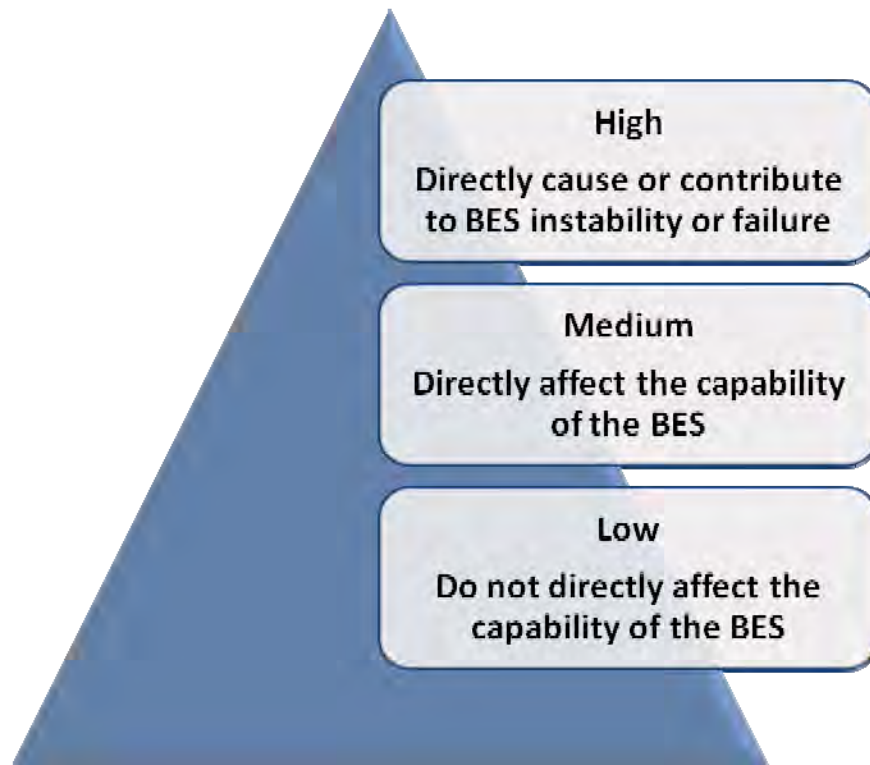


Figure 2: Categorization of BES Cyber Systems

Acknowledging NIST’s Risk Management Framework

The CIP-002-4 approach has considered various security risk management frameworks including the NIST Risk Management Framework as an approach to guide utilities in safeguarding the BES. There are many valuable lessons to be learned within the NIST Framework and a number of similarities between it and the NERC CIP Cyber Security Standards.

The NIST Framework involves a continuous process of six discrete steps to categorize and protect information systems. The NERC CIP Cyber Security Standards approach is similar in that it is a continuous process of separate steps for identifying Cyber Systems that support BES functions,

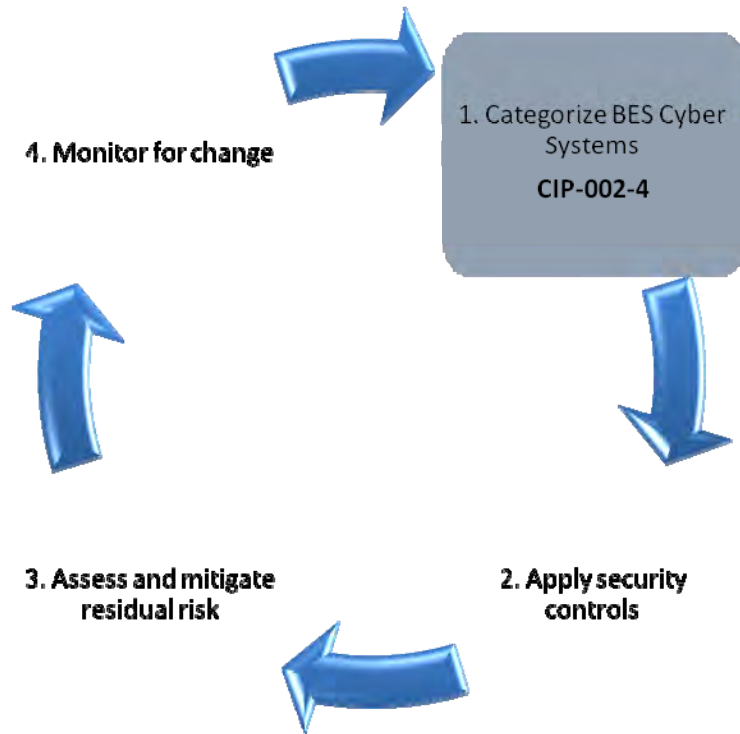


Figure 3: NERC Cyber Security Standards – Security Management Cycle

categorizes Cyber Systems based upon their potential impact to the functions, and assigns security controls based upon that categorization.

It is important to highlight differences between NERC’s and NIST’s approaches. At the root of these differences is the divergent responsibilities and goals. NIST is providing standards and guidance for U.S. Federal Agencies in managing risks to their information and systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to avoid in order to achieve their mission. NIST does not enjoy this benefit, as they are providing standards to almost two hundred different organizations, each with vastly different missions. The advantage that the NERC Standards enjoy enables a focus on a relatively small number of functions that need to be protected. This ultimately means that the NERC Standards can be more tailored and appropriate to the industry than a wholesale adoption of the NIST Risk Management Framework, as a higher degree of definition of

Cyber Systems and their potential impact to BES functions should yield better fidelity in selection of protection strategies, resulting in a more appropriate investment of resources by utilities.

The role of this guidance

This guidance document serves to assist NERC Registered Entities in categorizing their BES Cyber Systems based on their impact to the reliable operation of the Bulk Electric System.

Categorizing BES Cyber Systems

In this section, a five-step process is outlined to assist entities in categorizing their BES Cyber Systems. This is only one approach, and an entity may choose an alternate approach to complying with the requirements of CIP-002-4. However, this process attempts to build upon the investment utilities may have already made in complying with previous versions of the CIP Standards by utilizing the inventory and categorization of BES Subsystems to categorize their BES Cyber Systems.

Step 1: Performing a BES Subsystem Inventory

The categorization of BES Subsystems in steps 1 and 2 provides a measure of the impact its associated BES Cyber Systems have on the Bulk Electric System.

The inventory of BES Subsystems should include all Generation Subsystems, Transmission Subsystems, and Control Centers owned by the entity. The definition of a BES Subsystem is intentionally flexible to allow entities to evaluate their own particular power system design. For example, a multiple unit generation facility can be defined as one or more Generation Subsystems depending on the functions being performed and the operational and technical characteristics of the generating units.

The entity should consider any associated BES Cyber Systems when performing the inventory and defining boundaries of BES Subsystems. Although a full BES Cyber System inventory may not be available at this step in the process, the BES Cyber System will ultimately drive the final characterization of the BES Subsystem.

What is a BES Cyber System?

A BES Cyber System is defined in the NERC Glossary as “a Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.”

This definition includes all of the components necessary to ensure the protection of the reliability function(s) being performed. To determine these components, the Responsible Entity should consider the following:

1. Primary components – devices performing or having direct impact to the reliability function(s).
2. Interconnected components – servers and workstation components involved in the exchange and display of data associated with the reliability function(s) (e.g., historical data collectors, ICCP nodes, operations support workstations, etc.).
3. Infrastructure support components – devices supporting the confidentiality, integrity, and availability constraints of the BES Cyber System which may be defined by the selection of security controls (e.g., routers, switches, firewalls, access-control servers, security event monitoring servers, virtual server management, etc.)
4. Collateral components – devices included only on their location within a network segment that could be utilized to attack the supported function of the BES Cyber System.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System or they might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

The shared elements that an associated BES Cyber System can impact should be included as part of the BES Subsystem.

Step 2: Categorizing BES Subsystems

Identified BES Subsystems are then mapped into impact categories based on pre-defined criteria in Attachment 1 of CIP-002-4, which reflect their impact on the reliability and operability of the BES. The criteria represent impact thresholds based on the functions identified in Attachment 2 of CIP-002-4.

All BES Subsystems will have an assigned impact category. BES Subsystems that do not meet the High or Medium threshold criteria are by default categorized as Low impact.

Step 3: Performing a BES Cyber System Inventory

The inventory of BES Subsystems can be used as a starting point for identifying BES Cyber Systems. This process involves looking at each of the associated BES functions and determining which Cyber Systems are involved. Each BES Subsystem performs one or more functions of the BES. The identification of these functions provides the basis by which to identify, categorize, and protect BES Cyber Systems.

Profiling BES Functions with Respect to Cyber Systems

The exercise of profiling BES functions is a useful approach to determining BES Cyber Systems. BES functions are defined generically and each Responsible Entity will perform these differently using different components. The task of profiling BES functions involves describing how they are performed and the Cyber Systems that support or impact their performance. The description can be written in non-technical language and should be as specific as possible. This brings the generic function description to a level where the Responsible Entity can identify the function as processes within its operation. Table 1 shows an example profiling of the Reliability Function, Control, and Operation for an entity.

Reliability Function: Control & Operation	Control & Operation includes those activities, actions and conditions that provide monitoring and control of BES elements
Description	Relays and RTUs located at Company X substations provide the SCADA System with status and power flow data. If a protective relay trips at substation Y, then operations personnel are notified through the SCADA alarms or an automated after-hours call-out system. Operations personnel will then assess the condition and issue breaker control to reestablish power to the affected line.

Table 1: Profile of the Reliability Function Control & Operation

The profile can be further represented as a series of process steps that display the Cyber Systems involved for each step as shown in Figure 4.

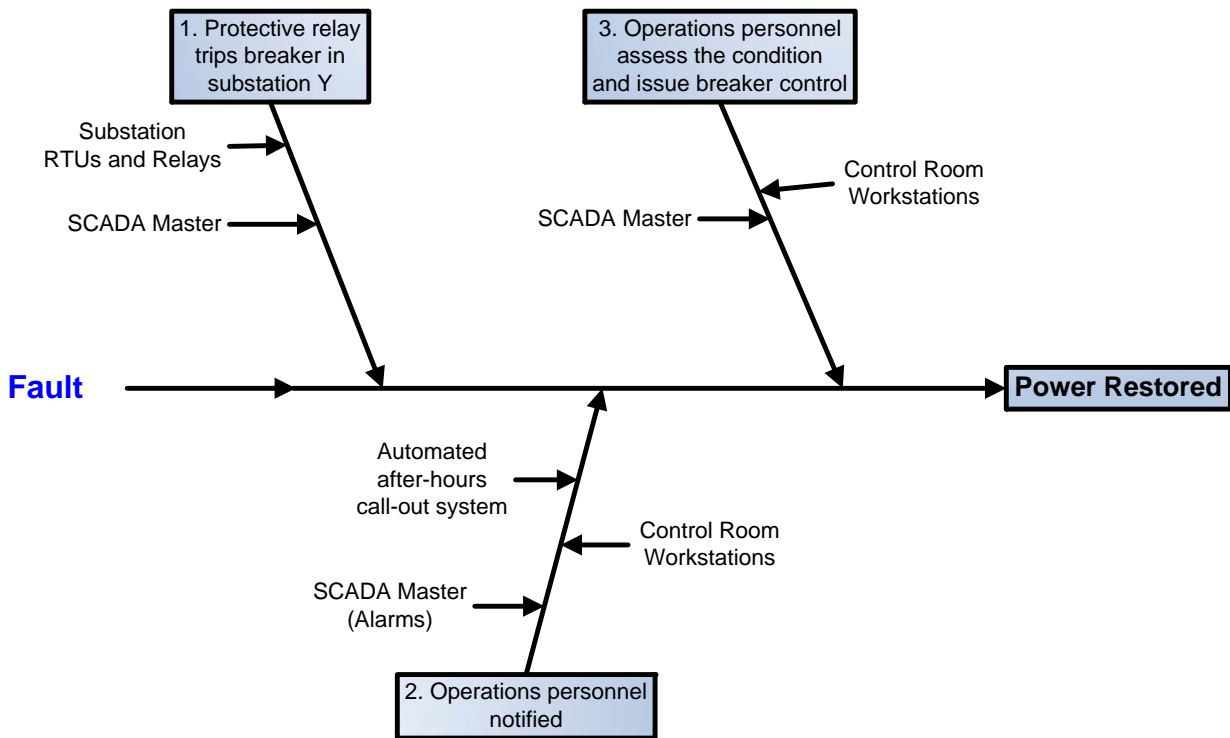


Figure 4: A sample fishbone diagram showing Cyber Systems involved in the function of Control & Operation

Step 4: Perform an Impact Categorization for each BES Cyber System

Using the Cyber System components identified in the previous step, BES Cyber System components can be identified as having the potential to adversely impact the BES function. The Responsible Entity should consider the impact to the Reliability Function given the loss, degradation, and compromise of the Cyber System component. For a complete assessment, each scenario of loss, degradation and compromise of the Cyber System component should be considered individually.

Loss of the BES Cyber System – Both BES Subsystems and BES Cyber Systems routinely go offline with no impact to the BES. However, the analysis should go beyond normal operating conditions to consider the impact of losing the Cyber System at an inopportune time and possibly for an extended period of time.

Degradation of the BES Cyber System – In this case, the BES Cyber System may still remain online but its performance is affected. This may occur in response to an unauthorized change in the system such as a defective upgrade or flood of network packets.

Compromise of the BES Cyber System – Unauthorized, unintended, or malicious use of the BES Cyber System. Specifically, the Responsible Entity should consider the following scenarios as applicable:

- Issuance of control commands to BES Subsystems
- Modification of configuration settings including operational parameters
- Modification of alarm limits
- Modification of collected or transmitted data

The result of this analysis determines the set of BES Cyber System components that have the capability of impacting the BES functions. The components are then grouped as a single or multiple, distinct BES Cyber Systems. Each BES Cyber System inherits the CIP-002 impact categorization (High, Medium, or Low) of the BES Subsystem through which the Reliability Function is being performed.

In the case where a BES Cyber System supports multiple BES Subsystems, then the BES Subsystem with the highest impact categorization is inherited. Table 2: Example Impact Categorization for a SCADA System demonstrates this concept for an example SCADA Cyber System associated with multiple BES Subsystems.

BES Subsystem	Associated Reliability Function(s)	BES Impact
Primary Control Center	Control & Operation	High
Hydro Plant #1	Balancing Load and Generation	Low
Coal Plant #1	Situational Awareness	Medium
Control Center at Company X	Inter-Entity Coordination and Communication	Low
Resultant Impact Categorization		High

Table 2: Example Impact Categorization for a SCADA System

Step 5: Monitoring for Changes to the System

Once a BES Cyber System has been assigned an initial impact categorization, processes should be in place to ensure this categorization continually reflects modifications to the electric system and operational processes of the BES Cyber System components. The following types of changes should be monitored as part of the process of BES Cyber System categorization.

1. Modifications to the BES Subsystems that result in a different impact mapping
2. Additions or modifications to the BES functions being performed by a BES Subsystem
3. Modifications to the Cyber System components performing the BES functions, which may result in the need to identify additional BES Cyber System components

To ensure these categories of changes are captured prior to deployment, an organization might include a quarterly review within their processes to capture any new or upcoming changes to the system.