Identifying BES Cyber Systems and BES Cyber Assets

Schneider Electric NERC CIP* assessment methodology

Solution at a glance

One of the most important and critical elements spanning all NERC CIP regulations is the identification of bulk electrical system (BES) Cyber Systems and associated BES Cyber Assets. These two crucial elements are at the core of NERC CIP compliance.

Schneider Electric has the resources, expertise and experience to help you identify NERC CIP assets. Our assessments follow a proven and repeatable methodology that:

- Classifies and lists assets consistently
- Assists in the collection and logging of supporting evidence for NERC CIP audits
- Solidifies NERC CIP compliance

NERC CIP risk assessment

The NERC CIP regulations require every entity to perform risk assessments and identify all basic electrical system (BES) Cyber Systems and associated BES Cyber Assets, as defined throughout the ten NERC CIP standards. These standards set forth the following specific regulations pertaining to cybersecurity.

- CIP-002 BES Cyber System Categorization
- CIP-003 Security Management Controls
- CIP-004 Personnel & Training
- CIP-005 Electronic Security Perimeters
- CIP-006 Physical Security of BES Cyber Systems
- CIP-007 System Security Management
- CIP-008 Incident Reporting and Response Planning

*North American Electric Reliability Corporation, Critical Infrastructure Protection

Identifying BES Cyber Systems and BES Cyber Assets

Schneider Electric NERC CIP assessment methodology

- CIP-009 Recovery Plans for BES Cyber Systems
- CIP-010 Configuration Change Management and Vulnerability Assessments
- CIP-011 Information Protection
- CIP-014 Physical Security

Asset identification and tracking

NERC CIP defines the term BES Cyber Asset in CIP-002.

BES Cyber Asset (BCA)
A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.

This definition appears to be fairly simple and straightforward. However, its interdependency with all other NERC CIP standards becomes quickly evident. The CIP-005 standard defines electronic security perimeters (ESP) as the logical border surrounding a network to which BES Cyber Assets are connected and for which access as well as all perimeter access points are controlled. The CIP-006 standard then defines the Physical Security Perimeter (PSP) as "the physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled."

Soon these simple objectives demand considerably more effort and expertise than many companies possess. These requirements don't simply apply to an entity's BES Cyber Systems and associated BES Cyber Assets within the Electronic Security Perimeters (ESP). They must address the systems that control and monitor both the ESPs and the Physical Security Perimeters (PSP) that protect them throughout the entire facility.

NERC CIP further requires that all information collected with regards to BES Cyber Assets be compiled into a list as outlined in CIP-002 and demonstrates that all assets have been validated. In addition, notes outlining the supporting evidence are to be collected and logged. This process must now be maintained for the complete lifecycle of the system. Failure to comply on any aspects of these standards can result in stiff penalties that range up to $1 million per day, per violation, depending on violation's severity.

Lifecycle management of BES Cyber Assets

The Schneider Electric cybersecurity team recognizes the challenges facing the industry to become NERC CIP compliant. We also understand that technology is the easy part. The real challenge lies in a repeatable methodology for lifecycle management of all BES Cyber Assets. To meet this challenge, we have designed a lifecycle management methodology that streamlines the process of defining BES Cyber Systems, BES Cyber Assets, reporting, and processing of audit records and other documentation required to demonstrate compliance with the NERC CIP standards.

The methodology applies the defined NERC CIP definitions to all assets identified. The result is a record of all assets and the evidence supporting the assignment.

Identifying BES Cyber Systems and BES Cyber Assets

Schneider Electric NERC CIP asset assessment methodology

The first phase of CIP-002 compliance must be a comprehensive risk-based assessment. The following steps should be taken to ensure that all BES Cyber Systems and associated BES Cyber Assets are identified:

Operational risk assessment
A list of all critical operational assets are identified. This includes assets such as process controls, environmental controls, alarms, safety and continuous power.

Network vulnerability assessment
A network vulnerability assessment accurately depicts the current security posture of cyber assets associated with critical infrastructure.

Gap analysis
A comprehensive risk assessment will identify and outline gaps to be reviewed. A gap analysis should be performed to evaluate current practices in accordance with policies and CIP requirements.

Security awareness and policy review
A general review of all policy documents and operational security awareness should be performed to assess the overall effectiveness in accordance with CIP requirements.

The CIP-002 R3 standard further qualifies Critical Cyber Assets (CCA) as those assets that meet any of the following qualifying connectivity requirements:

Methodology Features

- Repeatability of process
- Consistency in asset classification
- Listing of all assets
- Evidence reporting for NERC CIP audits
- Full NERC CIP compliance

Schneider Electric provides RSP workshops designed to get your assessment program jumpstarted in the right direction.

How can the Schneider Electric cybersecurity team help?

Understanding the NERC CIP regulations in their entirety is a large task. Having the expertise and ability to execute an effective assessment plan and then launch a comprehensive remediation program can seem virtually impossible. This is where the Schneider Electric cybersecurity team can help. Not only do we have the expertise and knowledge to help your facility become NERC CIP compliant, but we also understand that effective cybersecurity is a lifetime program. To manage this commitment, Schneider Electric has developed a cybersecurity lifecycle approach that can be applied at any stage, from an initial assessment to architecture and policy development as well as modernization and implementation right through to security management and optimization.

Schneider Electric

70 Mechanic Street
Foxborough, MA 02035 USA
+1 877 342 5173

schneider-electric.com/processautomation

Life Is On Schneider Electric