NERC CIP compliance
ABB Wireless

• Mature cyber posture that protects and accelerates a utility’s digital transformation with a defense-in-depth security strategy.
• Established technology leader, delivering cutting-edge security solutions.
NERC CIP compliance
ABB Wireless

This white paper outlines technical features of the ABB Wireless portfolio to help customers meet key NERC CIP compliance requirements.

Introduction

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) group mandates cyber security regulatory standards (CIP 002 through 014 NERC CIP Standards). The goal of these standards is to help protect bulk electric system owners, operators, and users in North America. NERC’s compliance program is designed to improve the reliability of the bulk power system.

ABB has a leadership role in the IEEE PES PSCC Cybersecurity Subcommittee developing technical standards and actively supports NERC CIP Committee activities. ABB Power Grids has over 100 years of utility operating experience and is a technology leader in providing products and comprehensive security solutions to electric utilities.

The purpose of this paper is to demonstrate the ABB Wireless Group’s commitment to supporting our customers in their efforts to become compliant or maintain compliance with NERC CIP requirements.

ABB has embedded cyber security in the design, development, maintenance, lifecycle management and communications processes.

ABB strives to continuously improve the security and robustness of our solutions and has integrated security testing as part of the development process. A dedicated, independent security test center has been established where ABB products are subject to security and robustness tests utilizing current state-of-the-art commercial and open source security testing tools. Tests include profiling, known vulnerability, denial of service and negative protocol tests.

NERC CIP is a performance-based standard, which means that only utilities and other end users can be NERC CIP compliant. No system, subsystem or product sold or delivered by ABB or other suppliers can be NERC CIP compliant. They can, however, include technical features that help support utilities or other end users in becoming NERC CIP compliant. Compliance to the NERC CIP standard, however, is ultimately the responsibility of the end user.

NERC CIP-005

Electronic Security Perimeter(s)

CIP-005 is focused on ensuring that the security of the bulk energy system is not compromised by unauthorized access to critical infrastructure and data. The definitions and descriptions below provide a high-level understanding of the requirements stated in CIP-005.

Note that no single networking device or security appliance satisfies all CIP-005 requirements.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP).

- The ESP defines a zone of protection around the BES Cyber System.
- Access into the ESP is controlled by an Electronic Access Point (EAP).
- The EAP should control both inbound and outbound traffic (firewall and role-based access control).

NERC CIP Standards

<table>
<thead>
<tr>
<th>NERC CIP Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-002 Critical Cyber Asset Identification</td>
</tr>
<tr>
<td>CIP-003 Security Management Controls</td>
</tr>
<tr>
<td>CIP-004 Personnel &amp; Training</td>
</tr>
<tr>
<td>CIP-005 Electronic Security Perimeter(s)</td>
</tr>
<tr>
<td>CIP-006 Physical Security of Critical Cyber Assets</td>
</tr>
<tr>
<td>CIP-007 Systems Security Management</td>
</tr>
<tr>
<td>CIP-008 Incident Reporting and Response Planning</td>
</tr>
<tr>
<td>CIP-009 Recovery Plans for Critical Cyber Assets</td>
</tr>
<tr>
<td>CIP-010 Configuration Change Management and Vulnerability Assessments</td>
</tr>
<tr>
<td>CIP-011 Information Protection</td>
</tr>
<tr>
<td>CIP-012 Communications between Control Centers</td>
</tr>
<tr>
<td>CIP-013 Supply Chain Risk Management</td>
</tr>
<tr>
<td>CIP-014 Physical Security</td>
</tr>
</tbody>
</table>

CIP-005-6: Cyber Security - Electronic Security Perimeter
### Remote Access Management

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. The ESP defines a zone of protection around the BES Cyber System.

1. There is a jump host, which is an intermediate device.
2. Remote access requires the intermediate device (ID) to provide multi-factor authentication.
3. Encryption is used to protect the data that is sent between the remote computer and the intermediate system.

---

### Supporting NERC CIP-005 requirements

The following table illustrates how the ABB Wireless solution provides the technical controls needed support the NERC CIP-005 requirements.

<table>
<thead>
<tr>
<th>Part</th>
<th>CIP-005-6: Cyber Security - Electronic Security Perimeter</th>
<th>Tropos &amp; Supros</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.</td>
<td>Tropos is one component of the ESP – providing a layer of defense in combination with other security appliances and tools.</td>
</tr>
<tr>
<td>1.2</td>
<td>All External/Remote Connectivity must be through an identified Electronic Access Point (EAP).</td>
<td>REQUIRED: Router can be accessed remotely only via the Web Interface. Remote connection to the web server on the router is via SSL/TLS (HTTPS) using certificate (PKI) authentication.</td>
</tr>
<tr>
<td>1.3</td>
<td>Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.</td>
<td>REQUIRED: Firewall rules on the router deny access by default except for HTTPS, ICMP DNS, DHCP, SSL/TLS, NTP, IKE/IPsec. Specific rules can be configured to allow other permitted connections. All unused protocols, ports and services will be disabled and enforced by the firewall on the router.</td>
</tr>
<tr>
<td>1.4</td>
<td>Where technically feasible, perform authentication when establishing Dialup Connectivity with applicable Cyber Assets.</td>
<td>REQUIRED: Where technically feasible, perform authentication when establishing Dialup Connectivity with applicable Cyber Assets. The Tropos router is a secure, reliable, scalable router utilizing several authentication methods including Radius for authorizing user access.</td>
</tr>
<tr>
<td>1.5</td>
<td>Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.</td>
<td>REQUIRED: Firewall rules consist of source and-or destination ports, source and-or destination IP addresses. Source and-or destination MAC addresses. Provisioning has an audit trail. Firewall hit counters and logging. Syslog for audits.</td>
</tr>
</tbody>
</table>

---

**Diagram Description**

- **Remote Access (SSH, HTTPS)**
- **DMZ**
- **ESP: Electronic Security Perimeter**
- **Tropos router**
- **Jump host or a bastion to access clients remotely.**
- **Apply firewall rules to allow remote access only via the jump host.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS (HTTPS) using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
- **Jump host or a bastion to access clients remotely.**
- **Remote connection to the web server on the router is via SSL/TLS using certificate (PKI) authentication.**
- **IPsec VPN with AES, SHA-2, 4096-bit RSA keys. IKEv2/IPsec.**
- **No CLI access via telnet or SSH.**
- **Router user authentication can be local or via RADIUS.**
- **No CLI access via telnet or SSH.**
- **WARNING: RADIUS accounting.**
NERC CIP-007-6

Systems Security Management

The following table illustrates how the ABB Wireless solution provides the technical controls needed support the NERC CIP-007-6 requirements.

<table>
<thead>
<tr>
<th>Part</th>
<th>CIP-007-6</th>
<th>Tropos</th>
</tr>
</thead>
</table>
| 1.1  | Table R1 – Ports and Services | • Firewall rules on the router deny access by default.  
• Specific rules can be configured to allow only permitted connections.  
• All unused protocols, ports and services will be disabled and enforced by the firewall on the router.  
• Firewall and VRF packet filtering rulesets to block and permit specific ports and services. |
| 1.2  |  | • Serial ports can be enabled from the Supros management platform.  
• The Ethernet ports can be administratively enabled or disabled from the Supros management platform. |

**Table R1 – Ports and Services**

A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

<table>
<thead>
<tr>
<th>Part</th>
<th>CIP-007-6</th>
<th>Tropos</th>
</tr>
</thead>
</table>
| 2.1  |  | • ABB Wireless provides efficient patch management as part of its security policy.  
• Security alerts are handled immediately by the software team.  
• In case of vulnerabilities, Tropos and Supros software patches are made available immediately with a vulnerability alert. |

**Table R2 – Security Patch Management**

Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1: Detected malicious code from Part 4.1; and 4.2.2: Detected failure of Part 4.1 event logging.

<table>
<thead>
<tr>
<th>Part</th>
<th>CIP-007-6</th>
<th>Tropos</th>
</tr>
</thead>
</table>
| 4.2  |  | • Tropos and Supros manage events and logging at the system level.  
• Detection and reporting of security-related events, for example: failed login attempts, denial of service attacks.  
• Audit trails of user access account access activity and configuration changes.  
• Monitoring and logging of unauthorized and unauthorized access attempts.  
• Automated alerts after a configurable number of unauthorized access attempts. |

**Table R4 – Security Event Monitoring**

Have a method(s) to enforce authentication of interactive user access, where technically feasible.

<table>
<thead>
<tr>
<th>Part</th>
<th>CIP-007-6</th>
<th>Tropos</th>
</tr>
</thead>
</table>
| 5.1-5.7 |  | • The Tropos router does not provide CLI access to the operating system or for configuration.  
• No SSH access is provided to the router itself.  
• Tropos recommends and utilizes best practices for passwords and user access, enforcement of strong passwords.  
• Detection and reporting of access-related events such as failed login attempts.  
• Tropos provides inherent security for access to the router itself and to the clients that are connected to it by utilizing several authentication methods to include Radius. |

**Table R5 – System Access Control**

NERC CIP-010-2

Configuration Change Management

The following table illustrates how the ABB Wireless solution provides the technical controls needed support the NERC CIP-010-2 requirements.

<table>
<thead>
<tr>
<th>Part</th>
<th>CIP-010-2</th>
<th>Tropos</th>
</tr>
</thead>
</table>
| 1.1  | Table R1 – Configuration Change Management | • All open-source applications are tracked.  
• All ports open by default are documented (standards ports for router operations at startup).  
• Security patches applied and bugs fixed are documented as part of software release notes. |
| 1.2  |  | • Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source. |

**Table R1 – Configuration Change Management**

Information Protection

The following table illustrates how the ABB Wireless solution provides the technical controls needed support the NERC CIP-011-2 requirements.

<table>
<thead>
<tr>
<th>Part</th>
<th>CIP-011-2</th>
<th>Tropos</th>
</tr>
</thead>
</table>
| 1.1  | Table R2 – BES Cyber Asset Reuse and Disposal | • ABB Wireless Router is assigned a serial number at time of manufacturing.  
• A hardware device certificate tied to the serial number is issued and placed on the router during manufacturing. This certificate will be part of the router for its entire operational lifetime. |
| 1.2  | Procedure(s) for protecting and securely handling BES Cyber System information, including storage, transit, and use. | • The router’s configuration can’t be exported from the router as a text file.  
• Configuration and monitoring data can be exported from Supros only via the northbound RESTAPIS.  
• External applications can extract data from Supros’ database via database APIs after authenticating to the database. |
| 2.2  |  | • Data encryption is done for data transmitted over the LAN (mesh encryption) as well as the WAN (IPsec). |

**Table R2 – BES Cyber Asset Reuse and Disposal**