NERC CIP Whitepaper
How Endian Solutions Can Help With Compliance

Introduction

Critical infrastructure is the backbone of any nations fundamental economic and societal well being. Like any business, in order to achieve improvements in efficiency and deliver new technologies critical infrastructure is increasingly becoming connected to the Internet. The power and utilities industry is perhaps the most important infrastructure component because without it people, government and business will potentially cease to exist. In recognition of these trends and potential threats, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) group created cyber security standards (CIP 002 through 009) to help protect Bulk Electric System owners, operators, and users in North America. To emphasize their importance, these standards will be audited and potentially large sanctions and fines will be assessed for those found in noncompliance.

NERC CIP Standards
IP-002 Critical Cyber Asset Identification
CIP-003 Security Management Controls
CIP-004 Personnel & Training
CIP-005 Electronic Security Perimeter(s)
CIP-006 Physical Security of Critical Cyber Assets
CIP-007 Systems Security Management
CIP-008 Incident Reporting and Response Planning
CIP-009 Recovery Plans for Critical Cyber Assets

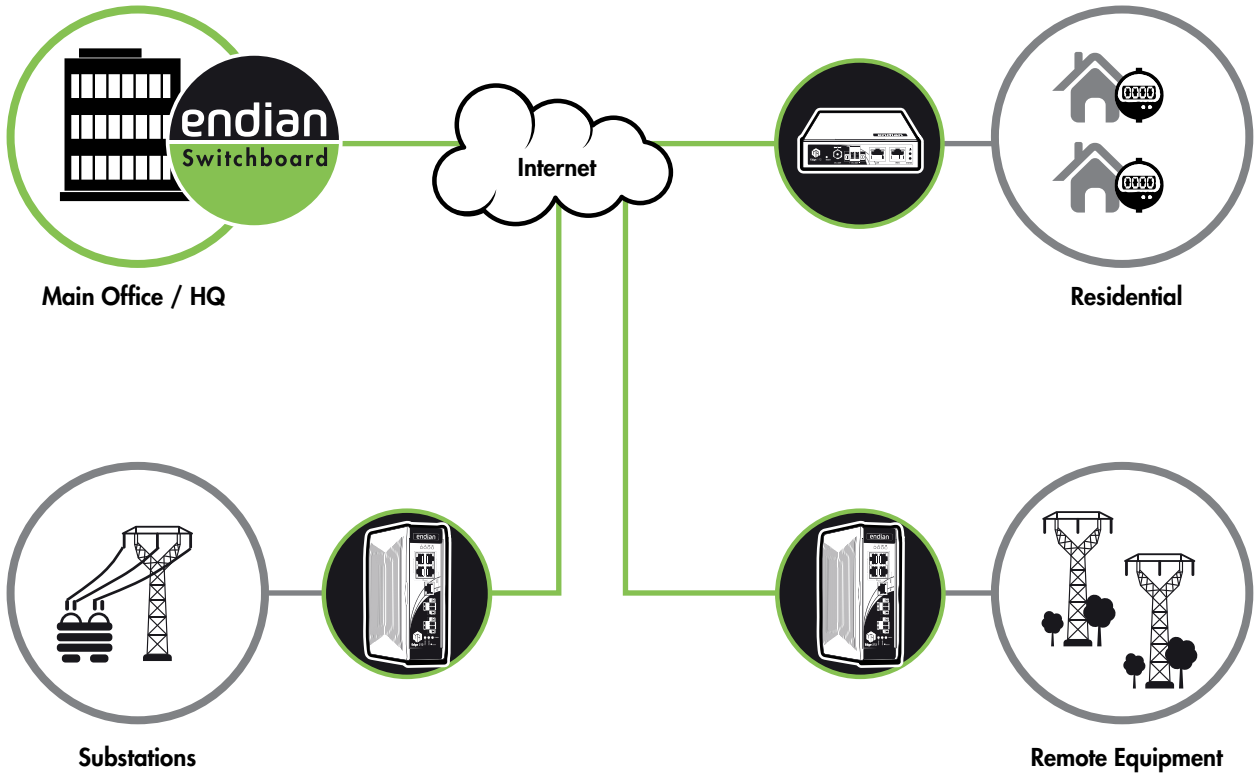
Security Challenges

There are numerous challenges for Bulk Electric System providers including maintaining the highest levels of reliability while managing and securing a geographically diverse set of equipment from potential threats both internally and externally from hackers, terrorists and even foreign countries. In addition, providers must also protect their backend infrastructure from external threats to prevent loss of customer or financial data as well as from their utility infrastructure all while allowing critical communications between those networks.

Endian Solution Set

Endian has created a complete end-to-end network security and connectivity solution set to help address the needs of critical infrastructure including Bulk Electric System providers. For all of the remote locations and or equipment substations, the Endian 4i Edge Industrial VPN Routers can protect and segregate the local networks while also facilitating redundant Internet connectivity. The products are available in multiple hardware versions with support for things like wide-temperature (-20° to 70°C), redundant 24V power, DIN rail mount, digital input/output ports and 3G cellular Internet modems. To securely connect and protect the infrastructure, the Endian Switchboard solution provides full Unified Threat Management (UTM) capabilities along with an advanced VPN technology stack that integrates seamlessly with our 4i Edge products. This complete solution stack can help to form a comprehensive security perimeter around your backend and utility infrastructure that enables role-based (and audit capable) access from users, vendors and third-party companies to your remote field equipment.

Endian Solution Set for Power/Utilities



Endian & NERC CIP Compliance

Regulatory standards and compliance are created around the idea that a framework of industry standard principles can advance regulatory objectives by creating minimum acceptable baselines that allow for entities to be held responsible for not complying. Put another way, there is no single product or solution that "solves" regulatory compliance but rather a set of products and solutions along with policies, procedures and training that when implemented and followed correctly can drastically mitigate the risk of compliance-related issues.

Endian and its products and solutions can address areas like your network security, network segmentation and isolation, network availability and redundancy, network access control (firewall), personnel access control (VPN and device authentication) and much more. In addition, Endian staff and their partners (distributors, resellers and service providers) can assist in the design and implementation of tools to help meet regulatory compliance.

The following table is an illustration of how Endian and it's partners, products and features can be utilized to help meet or exceed the relevant NERC CIP compliance standards.

CIP Standard	Req.	Description	Endian Solution
CIP-002	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter.	**4i / UTM:** Can be used to connect and protect the Electronic Security Perimeter while also securely encapsulating traffic in/out of the perimeter using VPN. **Partner:** Can assist in designing and providing products and services to use routable protocols (only).
CIP-002	R3.2	The Cyber Asset uses a routable protocol within a control center.	**4i / UTM:** Can be used to connect and protect within the control center while also securely encapsulating traffic in/ out of the control center using VPN. **Partner:** Can assist in designing and providing products and services to use routable protocols (only).
CIP-002	R3.3	The Cyber Asset is dial-up accessible.	**4i / UTM:** Can be used to facilitate secure dial-up or 3G/4G connectivity using firewall to limit access in/out and VPN to securely allow access over the dial-up or 3G/4G connection. **Partner:** Can assist in eliminating or designing secure dial-up products and solutions.
CIP-005	R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	**4i / UTM / Switchboard:** Can be used to establish the Electronic Security Perimeter using firewall and network segregation. Can also be used to secure out-of-band management and external communications devices like dial-up modems, 3G/4G modems, etc. Additionally using Endian VPN client ensures secure (encrypted) communications from external networks into the security perimeter. Switchboard and VPN features can provide highly secure and limit access to and inside the security perimeter to explicitly authorized devices for various users, groups and vendors.

CIP Standard	Req.	Description	Endian Solution
CIP-005	R1.2	For a dial-up accessible Critical Cyber Asset that uses a no routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	**See CIP-005, R1.1** **4i / UTM:** Can be used to secure individual access points for each dialup device or can protect and connect multiple dial-up devices while providing secure access in/out each of those devices.
CIP-005	R1.3	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	**4i / UTM / Switchboard:** Can be used as access points to establish secure (encrypted) communication links connecting one or more Electronic Security Perimeters using 4i and/ or UTM products combined with a centralized Switchboard solution. This solution will ensure you can define role-based (least) privilege access to the access points and any devices inside the security perimeter.
CIP-005	R1.4	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.	**4i / UTM / Switchboard:** Can be used to establish the Electronic Security Perimeter using firewall access control and provide network isolation/ segregation between critical and non-critical Cyber Assets. Switchboard can be used to logically create user and device groups that segregate critical and non-critical Cyber Assets for the purpose of remote user/vendor access.
CIP-005	R1.5	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	**4i / UTM / Switchboard:** Switchboard and UTM can be used to secure the network and remote access (authentication) of any Cyber Asset(s) presuming the proper network location and secure configuration (firewall, VPN, IPS, etc.).
CIP-005	R2.1	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	**4i / UTM:** Firewall is configured to deny all external access by default, only allow a minimum set of outbound communications and provide for zone-based access control between the internal networks. No remote access is enabled or allowed by default and must be explicitly defined by an administrator. **Switchboard:** Access to user/groups, devices and endpoints are denied by default and only allowed when explicitly defined by an administrator.

CIP Standard	Req.	Description	Endian Solution
CIP-005	R2.2	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	**See CIP-005, R2.1** **4i / UTM:** Use the firewall to explicitly define those ports and services that are required for operations and monitoring Cyber Assets. Use the VPN firewall to extend the same security policies to remote users. **Switchboard:** Define access only to required ports and services for a given set of Cyber Assets based on job role.
CIP-005	R2.3	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	**4i / UTM:** Can be used to secure individual access points for each dialup device or can protect and connect multiple dial-up devices while providing secure (encrypted) access in/out each of those devices using firewall and VPN. **Switchboard:** Can be used to manage and control remote (VPN) access to all Electronic Security Perimeter(s).
CIP-005	R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	**4i / UTM / Switchboard:** All products include SSL VPN functionality that utilized advanced encryption technology and is configured by default to require two-factor authentication (certificate plus valid username/password). VPN security can be increased by using PKI x.509 certificates that are unique for each user. SSL VPN solution can also be tied to existing Active Directory/LDAP infrastructure to enforce corporate user and password policies and to increase accuracy of user information (presuming it's kept up-to-date).
CIP-005	R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	**4i / UTM:** Can be used to send email or SMS alerts for access activity (login, logout, failed logins) including access to the 4i or UTM device (itself) and the remote SSL or IPsec VPN user access. **Switchboard:** Maintains complete audit log of user, device and endpoint activity which can be reviewed by authorized personnel on a set schedule.

CIP Standard	Req.	Description	Endian Solution
CIP-005	R4 R4.1-4.5	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually.	**Partner:** Can assist with asset and access point identification and performing cyber vulnerability assessment of the Electronic Security Perimeter.
CIP-005	R5.3	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	**4i / UTM / Switchboard:** Fully configurable in terms of log retention history and all logs are zipped and rotated on a set schedule. Logs can additionally be backed up manually or automatically on a set schedule and used to import onto a new device in the event of a failure. Logs can be exported in real-time to external log server(s) for data retention and correlation.
CIP-007	R2.1	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	**4i / UTM:** Use the firewall to explicitly define those ports and services that are required for emergency operations. Use the VPN firewall to extend the same security policies to remote users. **Switchboard:** Define access only to required ports and services for a given set of Cyber Assets based on job role.
CIP-007	R2.2	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	**See CIP-007, R2.1**
CIP-007	R4.1	The Responsible Entity shall document and implement antivirus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	**UTM:** Can be used to provide network anti-virus inspection for HTTP, HTTPS, FTP, SMTP, and POP3 traffic. Can also utilize malware prevention using the DNS system. Can utilize the IPS system to perform deep-packet inspection and identify viruses and malware as well. **4i:** Can be used to provide malware prevention using the DNS system. Can utilize the IPS system to perform deep-packet inspection and identify viruses and malware as well.

CIP Standard	Req.	Description	Endian Solution
CIP-007	R4.2	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	**4i / UTM:** All anti-virus, malware and IPS engines can be configured to check and update their signatures on a set schedule.
CIP-007	R5.1	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	**4i / UTM / Switchboard:** Can be used to define VPN remote access with rolebased (least) privilege access to the access points and any devices inside the security perimeter. Switchboard can provide complete audit logging capability in terms of users, devices and endpoint activity. Additionally Switchboard can add individual user authentication layer to devices and applications that have shared accounts or do not require authentication.
CIP-007	R5.2	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	**4i / UTM / Switchboard:** Initial configuration wizard forces user to set new passwords with minimum standards for system access. System access activity is logged and can be setup to send email or SMS notifications for each event. Additionally Switchboard can add individual user authentication layer to devices and applications that have shared accounts or do not require authentication.
CIP-007	R5.3	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible: • Each password shall be a minimum of six characters • Each password shall consist of a combination of alpha, numeric, and "special" characters • Each password shall be changed at least annually, or more frequently based on risk	**4i / UTM / Switchboard:** System and VPN user accounts must have passwords of six characters or greater and utilize alpha, numeric and "special" characters. For VPN user accounts, you can utilize Active Directory/LDAP infrastructure to enforce corporate user and password policies.

CIP Standard	Req.	Description	Endian Solution
CIP-007	R6.2 R6.3 R6.4	**R6.2** The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents. **R6.3** The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP- 008-3. **R6.4** The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	**4i / UTM / Switchboard:** System and VPN user accounts must have passwords of six characters or greater and utilize alpha, numeric and "special" characters. For VPN user accounts, you can utilize Active Directory/LDAP infrastructure to enforce corporate user and password policies.

Within this table are references to Endian products, features, and services (provided by Endian and it's partner channel). The legend below itemizes which Endian products belong to a given reference.

Products	Model	Webpage
4i	• 4i Edge 112 • 4i Edge 313 • 4i Edge 515	http://www.endian.com/products/4i/
UTM	• Mini 25 • Mini 25 WIFI • Mercury 50 • Mercury 100 • Macro 250/500 • Macro 1000/2500	http://www.endian.com/products/utm/
Switchboard	Switchboard Module & Connect Client App (installable in any UTM Mercury/ Software/Virtual 50 or higher)	http://www.endian.com/products/connect/
Partner	Can use an authorized Endian Industrial partner to assist in the design or other service oriented needs of the standard	

Endian International
Tel: +39 0471 631 763
E-mail: sales@endian.com

Endian US
Tel:+1 832 775 8795
E-mail: us@endian.com

Endian Italia
Tel: +39 0471 631 763
E-mail: italy@endian.com

Endian Japan
Tel:+81 3 680 651 86
E-mail: japan@endian.com

Endian Deutschland
Tel: +49 (0) 8106 30750 - 13
E-mail: germany@endian.com

Endian Turkey
Mobile +90 216 222 2933
E-mail: turkey@endian.com