COOPER Power Systems

Energy Automation Solutions

TECHNICAL NOTE

Meeting NERC CIP requirements with Cooper Power Systems IED Integration and Automation Solutions

To address the growing concern about the vulnerability of the bulk power system, the North American Electric Reliability Council (NERC) has issued the NERC CIP-002-1 to CIP-009-1 Cyber Security Standards. Utilities are now under a strict timeline to implement measures to address the vulnerabilities in their critical cyber assets.

This document describes the security features of **Cooper Power Systems SMP Gateway** and **IED Manager Suite** applications. It also describes how these solutions can provide utilities with a secure, NERC CIP-compliant, solution to integrate their substation devices.

In this document

cybectec

Quebec City
730 Commercial Street
Suite 200
Saint-Jean-Chrysostome, Quebec
Canada G6Z 2C5
Phone: 418-834-0009
Fax: 514-227-5256

Montreal
1290 St. Denis Street
Suite 400
Montreal, Quebec
Canada H2X 3J7
Phone: 514-845-6195
Fax: 514-227-5256

www.cybectec.com

2009/03/11

Introduction

One of the key benefits of IED integration is providing enterprise level users with access to substation devices for data retrieval and remote maintenance. However, providing access to devices connected to the substation network can constitute an unacceptable security risk if it is not done properly.

The Energy Automation Solutions division of Cooper Power Systems has invested considerable effort to provide utilities with solutions that help them put their substation data to use while meeting NERC CIP requirements, both at the substation and enterprise level.

The key component at the substation level is the **SMP Gateway**. This third generation data concentrator provides all the features required to implement a NERC CIP-compliant electronic perimeter that provides a secure single point of access to all substation devices. Its advanced security features allow it to integrate legacy IEDs, with little or no security, in a modern IED integration system.

At the enterprise level, **Yukon IED Manager Suite** provides utilities with the tools necessary to securely communicate with substation IEDs and to meet NERC CIP security management requirements.

SMP Gateway security features

SMP Gateway retrieves data from substation devices and makes it available to SCADA and to enterprise level applications. It also provides remote maintenance access to connected IEDs using its secure Passthrough function. The SMP Gateway supports both modern and legacy devices, using standard and proprietary protocols. It provides a secure single point of access to all substation devices, acting as NERC CIP-compliant electronic perimeter that protects connected devices, including those with little or no security.

The **SMP Gateway** implements the following security features that ensure that all connected devices can be accessed in a NERC CIP-compliant manner –

- **Authentication and authorization** — The SMP Gateway includes a built-in security server that authenticates each user via a user name and a password. Strong passwords, individual user accounts, user groups, and detailed group permissions are used to protect critical system functions from unauthorized access. All access attempts are logged, and accounts are locked out in the event of multiple failed access attempts. Alternatively, it can be used with the **IED Manager Suite Security Server** to implement a global security and simplify management of multiple users and SMP Gateways.
- **Network security** — The SMP Gateway is protected by a built-in firewall. All TCP/IP ports are blocked, except those required for control center communication and SMP Gateway status monitoring and management. All communication between the SMP Gateway and the SMP Tools is secured through the use of TLS (successor to "Secure Sockets Layer" or SSL).
- **Secure remote maintenance access** – The SMP Gateway provides remote users with the capability to securely use a terminal application or native vendor tool as if they were connected directly to the IEDs maintenance port.

- **Monitoring and locking of remote connections** — Control centers can control and monitor usage of the modem and remote maintenance access (passthrough) services; access is restricted to authorized users only; all successful and unsuccessful access attempts are logged locally, or to a standard Syslog server.
- **Integrity checking** — All SMP Gateway software and firmware components are signed in order to ensure their authenticity and integrity. The integrity of executable files is continuously monitored to prevent execution of unauthorized code.

Authentication and authorization

SMP Gateway authentication and authorization functions are used to control maintenance access to the gateway and to connected devices.

SMP Gateway provides the following authentication and authorization features —

- Support for distributed and centralized authentication. The default security model is distributed authentication, where each gateway has its own security server and performs its own authentication. Alternatively, the **Security Server**, part of **IED Manager Suite**, can also be used to maintain a global list of users and permissions and offer centralized authorization. This security model is described further on.
- Authentication by user name and a strong password. The maximum user name is 20 characters and the maximum password length is 64 characters. Password complexity can be enabled, requiring a combination of three of the following: upper case alphabetic, lower case alphabetic, numbers or punctuation.
- User accounts are locked after a predetermined number of failed login attempts to prevent password cracking and unauthorized access. Locked accounts can be unlocked by the administrator, or automatically after a configurable delay. Internal data points can be used to report failed login attempts and account lockout to SCADA, and can be used to trigger an intrusion detection function.
- Comprehensive authorization mechanism based on user groups and privileges –
  - There are predefined user groups. However, you can add new groups, or rename or suppress existing groups to suit your specific requirements.
  - You assign each user to one or more user groups.
  - You decide which predefined privileges to assign to each group. A privilege consists of a number of activities, and each activity is authorized individually. The predefined privileges include:
    - Security management — Update security database: users, groups, and privileges; unlock user accounts; access to Security and Firewall logs.
    - System management — Update firmware, software, license and components; configure redundancy, VPN, RAS, and SNMP; console access.
    - Configuration — Read or update the SMP Gateway configuration file.
    - Diagnostic — Use the SMP Gateway diagnostics tools: SMP Log, SMP Trace and SMP Stats.
    - Device maintenance — Use the SMP Gateway to remotely connect to an IED via passthrough connections.

  - Monitoring —Access the SMP Gateway internal real-time database through the internal web server.
  - Operation — Perform control operations, inhibit data points, and force operations on data points using the web-based commissioning tool.
  - Remote access — Obtain remote access via dialup or the network.
- All authentication and all activities, whether accepted or refused, are recorded in the security log. If technically possible, information about the PC connecting to the SMP Gateway is also recorded: IP address, Windows login user name, and machine name. All events can also be logged to a Syslog server.
- User accounts, groups, and privileges are edited centrally, using the **SMP Manager** tool.
- The SMP Gateway security database is encrypted using AES 128-bit encryption. Security information is never directly visible in clear form.
- Access to the security and firewall logs requires the Security Management permission.

Network security

The SMP Gateway ensures network security via a built-in firewall, the use of the Transport Layer Security (TLS) protocol, and a built-in VPN.

Firewall

- By default, all network ports are blocked, except for the management port (TCP 6650), the HTTPS web server port (TCP 443), and the legacy status server port (UDP 23). A firewall rule can be defined to restrict access through these ports.
- Ports are opened dynamically for the SNTP, SNMP, and redundancy functions. Access can be limited to specific IP addresses.
- TCP/IP ports used by slave protocols for SCADA, EMS or control centers, are automatically unblocked by the configuration tool. You can limit access to specific IP addresses.
- Simplified one-click management of CoDeSys Soft PLC Workbench, Visual T&D, SNMP and ICMP PING.
- Custom firewall rules can be defined for specific requirements.
- All blocked accesses are recorded in the firewall log.

Transport Layer Security (TLS)

To prevent identity spoofing, data tampering and information disclosure, the SMP Tools use the Transport Layer Security (TLS) protocol (successor to “Secure Sockets Layer” or SSL). Each SMP Gateway has a built-in certificate used to secure the communication channel.

The built-in web server uses the Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) protocol.

VPN

The SMP Gateway provides a built-in VPN to secure the connection to the **Visual T&D** application, third party applications such as the CoDeSys Soft PLC Workbench, or control centers, ensuring confidentiality and data integrity.

- The VPN uses Microsoft PPTP (Point-to-Point Tunneling Protocol) technology. Handshaking is done with MS-CHAPv2, and encryption is 128-bit MPPE (Microsoft Point-to-Point Encryption). PPTP does not require the implementation of a certificate server.
- The SMP Manager tool can be used to manage VPN connections; VPN connections can also be established manually, outside of SMP Manager.

Secure remote maintenance access

The SMP Gateway **Passthrough** function provides remote users with the capability to securely use a terminal application or native vendor tool as if they were connected directly to the IED maintenance port.

The **SMP Connect** application runs on the user PC and acts as port redirector. It captures all data from the application and forwards it to the SMP Gateway over a secure TLS channel. The SMP Gateway then forwards the data to the target device.

The Passthrough function can be used with serial and TCP/IP devices. Usage is limited to authenticated users with the correct permissions and can be monitored and controlled by SCADA.

The Passthrough function acts as a secure proxy and does not bridge traffic from the substation network to the enterprise network. Only preconfigured Passthrough connections can be activated.

Monitoring and locking remote connections

The SMP Gateway can monitor and lock connections to the internal modem. It can also monitor and lock passthrough connections.

Modem connections

- Modem accesses can be monitored by a control center, through a logical binary input data point.
- Modem accesses can be locked by a control center, through a logical binary output data point or through a RAS Manager command.
- Control centers can interrupt active modem connections.
- Lock settings are preserved between SMP Gateway restarts.

Passthrough connections

- Passthrough connections can be monitored and locked individually by a control center, through a logical binary input data point.
- An active passthrough connection can be interrupted by a control center.
- The startup lock settings can be specified via the configuration tool.

Integrity checking

Standard virus detection software is not designed to be used on devices running embedded software such as the SMP Gateway. Virus detection only works with known threats and needs to be updated regularly.

The SMP Gateway thus provides the following integrity checking functions to protect against viruses and other forms of malware —

- All SMP Gateway executable files (firmware and software) are signed by Cooper Power systems. Only signed executable files can be loaded onto the SMP Gateway.
- The integrity of all executable files on the SMP Gateway is continuously monitored in the background. This feature automatically detects any change resulting from hardware or software failure, or tampering.
- If an invalid executable file is detected, the SMP Gateway records the name of the file in the security log, and puts itself into a safe mode in which it interrupts all communication with devices and control centers.

Yukon IED Manager Suite

Yukon IED Manager Suite is a family of software applications that bridge the gap between the substation and the enterprise. They provide users with a single, enterprise-level, point of access to substation data and substation devices.

SMP Gateway and **Yukon IED Manager Suite** work in tandem, providing utilities with a comprehensive communications infrastructure and a powerful set of tools to manage their IEDs, simplifying the implementation of NERC CIP management procedures.

The following applications provide are part of Yukon IED Manager Suite (IMS) –

- **IMS Security Server** provides centralized authentication and authorization services.
- **IMS Passthrough Manager** provides corporate users with a single point of access to substation devices, for maintenance and engineering purposes.
- **IMS Event Manager** automatically retrieves event files from protection relays, notifies the appropriate users by email or pager, and provides access to event data through a web-based interface.
- **IMS Configuration Manager** provides centralized configuration management services for SMP Gateways and connected devices.

Security Server

The **IMS Security Server** provides centralized authentication and authorization services for all IMS applications. It also offers a centralized security model where access to SMP Gateways can be managed globally instead of individually.

In the default SMP Gateway security model, each gateway implements its own security server and performs its own authentication. System administrators use the **SMP Manager** application to define users, groups and permissions. Administrators copy the encrypted security database to each individual SMP Gateway.

When the centralized security model is implemented, user credentials are validated by the **Security Server** instead of being validated by individual SMP Gateways.

- The Security Server manages a database of IMS and SMP Gateway users.
- The Security Server can authenticate users from its database, or it can tie into the existing corporate security infrastructure, such as Microsoft Active Directory.
- Connecting to Active Directory ensures that access to Cooper Power Systems products is subject to the same security policies as all other enterprise applications: single user account and password for all applications, password complexity, two-factor authentication, etc.
- System administrators use the Security Server to assign permissions according to the previously described groups and permissions model. Permissions can be assigned to individual users, IMS groups, or Active Directory groups.
- SMP Tools and IMS applications validate the user's credentials with the Security Server to determine access permissions.
- For valid users, the Security Server returns an encrypted and signed message that contains the user name and permissions. Client applications and tools

forward this message to the IMS application server or SMP Gateway which decrypts the message and enables the appropriate functions.

- The authenticity of the messages exchanged between the Security Server and SMP Gateway is ensured by a shared private key. The physically secure central server uses the shared key to encrypt messages. The SMP Gateway uses the key to decrypt the message. The SMP Tools cannot decrypt these messages.

Once an SMP Gateway is configured for centralized security, the internal security server and authentication database is no longer used, except in emergency situations. Local "rescue" accounts provide access if contact with the central Security Server is lost.

Security Server provides centralized authentication and access management for all SMP Gateways, without having to implement Active Directory or Domain-based security at the substation level.

Passthrough Manager

IMS Passthrough Manager is an enterprise-level application that provides corporate users with secure remote access to substation devices. With Passthrough Manager, users can remotely perform configuration and maintenance operations on substation IEDs, using a terminal emulator program or native vendor tool.

Passthrough Manager is a client/server application. The **Passthrough Client** application can be installed on individual desktops or on a shared application server. The Passthrough Client forwards data from the native vendor tool to the **Passthrough Server** using a secure TLS connection. The Passthrough Server forwards the data to the remote device directly, through an SMP Gateway, or through a SEL 20xx gateway, using serial or TCP/IP connections.

Passthrough Manager offers the following security features –

- Isolate client applications from the substation devices. Only the Passthrough Server needs access to the substation devices, it can be installed in a DMZ.
- Secure all data exchanges between the Passthrough Client, Passthrough Server and SMP Gateway using TLS.
- Set access permissions by device, by user or by group.
- Show users only the devices to which they have access.
- Maintain a log of all accesses.
- Maintain a detailed log of all operations performed on a device.
- Automatically perform device login and hide device passwords from users, when technically feasible. Users no longer need to know device passwords.
- Filter commands to prevent users from performing unauthorized functions such as changing device passwords, when technically feasible.

Event Manager

IMS Event Manager is an enterprise-level application that automatically retrieves event files from protective relays, notifies the proper users and sends the data file along with the notification. Users can then analyze the fault data and eventually restore service more rapidly.

With Event Manager, protection engineers no longer need to connect to devices to analyze fault data. Event data is attached to the notification email, or available through a web browser.

The application offers the following features –

- Retrieve event from devices directly, through an SMP Gateway, or through a SEL 20xx gateway, using serial or TCP/IP connections.
- Retrieve events on demand or on a scheduled basis.
- When used with an SMP Gateway, events can be "pushed up" and retrieved immediately instead of waiting for the scheduled poll or a manual poll.
- Event notifications are sent automatically to the appropriate users by email or pager.
- Event data is stored in an industry-standard SQL Server database.
- Event data can be viewed using a web browser, converted to COMTRADE format, and analyzed using native vendor tools.
- Users only see data for the devices to which they have access.

Configuration Manager

IMS Configuration Manager is an enterprise-level application that manages a database of configuration files for all SMP Gateways and supported substation-level devices. On demand, or on a scheduled basis, Configuration Manager retrieves the current configuration of registered devices, compares it to the baseline version, and notifies the system administrator of any change.

Configuration Manager provides the following features to assist utilities in meeting NERC CIP requirements –

- Store device configuration files
- Track software versions, settings, patches and service packs for all managed SMP Gateways and devices
- Detect configuration changes and track change history
- Retrieve device configuration files for system recovery

Conformity to NERC CIP requirements

The following table summarizes how **SMP Gateway** and **Yukon IED Manager Suite** help utilities meet NERC CIP requirements.

NERC CIP	SMP Gateway IED Manager Suite
CIP-002-2 Critical Cyber Asset Identification	
R3. Critical Cyber Asset Identification *The Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset*	**IED Manager Suite** can manage the inventory of all gateways and substation-level devices accessible directly or through gateways.
CIP–003–2 Security Management Controls	
R4. Information Protection *The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.*	**IED Manager Suite** provides strong passwords, individual user accounts, user groups, and detailed group permissions to protect critical information from unauthorized access.
R5. Access Control *The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.*	**IED Manager Suite** assigns device access per individual user, or per group. Users only see devices to which they have access. With Auto-login, users do not need to know device passwords. Command filtering prevents unauthorized users from operating remote devices or changing device settings. Detailed reports identify accessible devices and permissions for each user.
R6. Change Control and Configuration Management *The Responsible Entity shall establish and document a process of change control and configuration management…*	The **IMS Configuration Manager** module maintains a database of all configuration files and tracks all configuration changes for each managed SMP Gateway and IED. Configuration Manager automatically detects configuration changes and notifies administrators.
CIP–004–2 Personnel and Training	
R4. Access *The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.* *R4.2. The Responsible Entity shall revoke such access to Critical Cyber*	**IED Manager Suite** provides centralized management of access rights for all applications, SMP Gateways and managed IEDs. When the **Security Server** module is tied-in to the corporate Active Directory, administrators can revoke access to all applications and devices with a single operation.

Assets within 24 hours for personnel terminated for cause…	Without Active Directory, system administrators can easily control access to IMS applications, SMP Gateways and substation IEDs on a per user basis. IMS Security Manager module provides system administrators the capability to easily update the security database of each individual SMP Gateway.
CIP–005–2 Electronic Security Perimeter(s)	
R1. Electronic Security Perimeter *The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter.*	**SMP Gateway** performs all the functions required by NERC CIP for an electronic perimeter.
R2. Electronic Access Controls R2.1. *…shall use an access control model … such that explicit access permissions must be specified.*	The **SMP Gateway** security limits access to authenticated users, for authorized operations only. **IMS Passthrough Manager** controls enterprise-level access to IEDs. Authenticated users can only see the devices to which they have access, and can only perform authorized operations.
R2.2. *…shall enable only ports and services required for operations and for monitoring…*	By default, the **SMP Gateway**'s built-in firewall block all network ports, except for the management port (TCP 6650), the HTTPS web server port (TCP 443), and the legacy status server port (UDP 23). A firewall rule can be defined to restrict access through these ports. The configuration tool unblocks only those ports required to connect to control centers, and to implement services such as SNMP and NTP, when they are used. Access can be limited to specific IP addresses. All serial ports are disabled unless configured to communicate with IEDs or control centers.
R2.3. *…shall maintain and implement a procedure for securing dial-up access to the Electronic Security Perimeter(s).*	By default, the **SMP Gateway**'s modem is disabled. Usage of the modem must be configured, and can be controlled by a SCADA interlock.
R2.4. *…shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party…*	The **SMP Gateway** security limits access to authenticated users, for authorized operations only. **IMS Passthrough Manager** limits access to authorized users only.
R2.6. *Appropriate Use Banner — … electronic access control devices shall display an appropriate use banner upon interactive access attempts…*	All **SMP Tools** and **IED Manager Suite** tools display a user-configurable appropriate use banner when they are launched.
R3. Monitoring Electronic Access R3.1. *For dial-up accessible Critical Cyber Assets … shall implement and*	The **SMP Gateway** implements internal data points that SCADA can monitor to detect modem and passthrough usage.

document monitoring process(es) …	All accesses are logged in the internal security log.
R3.2. *…shall detect and alert for attempts at or actual unauthorized accesses…*	The **SMP Gateway** security automatically locks out user accounts after a preset number of failed access attempts. Internal data points can be used to report failed login attempts and the locked-out state of the gateway. This information can trigger an alarm at SCADA, trigger an Intrusion Detection System (IDS), or be forwarded to a Managed Security Service (MSS).
R5. Documentation Review and Maintenance R5.1. *… shall ensure that all documentation … reflect current configurations and processes…*	**IMS Configuration Manager** tracks all version and change information for each device.
R5.3. *…shall retain electronic access logs for at least ninety calendar days.*	The **SMP Gateway** maintains a log of all accesses and can be configured to publish the information to a Syslog server. System administrators can use the **SMP Log** application to manually retrieve and store the log contents. **IMS Passthrough Manager** logs all accesses to IEDs and can be configured to publish the information to a Syslog server. Passthrough Manager also logs all data exchanged between the user and the IED.
CIP–007–2 Systems Security Management	
R3. Security Patch Management *…shall establish and document a security patch management program…*	**IMS Configuration Manager** tracks software versions, settings, patches and service packs for all managed devices.
R4. Malicious Software Prevention *…shall use anti-virus software and other malicious software ("malware") prevention tools…*	Only files signed by Cooper Power Systems can be loaded on the **SMP Gateway**. The **SMP Gateway** integrity checking function continuously scans all executable files and shuts down the gateway if file contents are modified by hardware or software failure, or by tampering.
R5. Account Management R5.1.2. *…shall establish methods, processes, and procedures that generate logs … of individual user account access activity…*	The **SMP Gateway** maintains a log of all accesses, and can publish this information to a Syslog server. System administrators can use the **SMP Log** application to manually retrieve and store the log contents.
R5.2. *…shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges…*	**IED Manager Suite** and **SMP Gateway** implement individual user accounts, user groups, and detailed group permissions. **IMS Passthrough Manager** performs Auto-login and hides device passwords from users.

R5.3. *…shall require and use passwords, subject to …* *R5.3.1. Each password shall be a minimum of six characters.* *R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.* *R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.*	The **SMP Gateway** built-in security server supports user names of up to 20 characters, and password length of up to 64 characters. Password complexity can be enabled, requiring a combination of three of the following: upper case alphabetic, lower case alphabetic, numbers or punctuation. **IMS Security Server** provides centralized account management and it can tie-in to the existing corporate Active Directory. It extends corporate security policies to substation devices, without the complexity of implementing domain-based security at the substation level.
R6. Security Status Monitoring *…shall ensure that all Cyber Assets … implement automated tools or organizational process controls to monitor system events that are related to cyber security…*	The **SMP Gateway** manages logical data points that can be used to report security events such as failed login attempts and the locked-out state of the gateway. This information can trigger an alarm at SCADA, trigger an Intrusion Detection System (IDS), or be forwarded to a Managed Security Service (MSS). **IMS** logs every user access and security event and can be configured to publish the information to a Syslog server.
CIP–009–1 Recovery Plans for Critical Cyber Assets	
R4. Backup and Restore *…shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets…*	**IMS Configuration Manager** stores all the configuration files required to restore all **SMP Gateways** and managed devices.