

Securing Critical Cyber Assets with Cooper Power Systems Products

2008/11/25



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

Contents

Figures	i
1. Introduction	3
1.1 Modernizing the Process Network.....	3
1.2 Mandatory Security.....	4
1.3 NERC CIP Requirements.....	4
1.4 Strategies for Meeting NERC CIP Requirements.....	5
1.4.1 Access Restricted to SCADA Only	5
1.4.2 Substation-Level Access Control.....	6
1.4.3 Enterprise-Level Access Control	8
1.4.4 The Best of Both Worlds: Substation- and Enterprise-Level Access Control	10
2. About Cooper Power Systems Substation Solutions and IED Manager Suite	11
2.1 Yukon IED Manager Suite (IMS)	12
2.2 Cooper Power Systems Substation Solutions	13
2.3 Technical Overview.....	13
3. Contact us	14
Appendix A - Web Page References	15

Figures

Figure 1 – Access Restricted to SCADA	6
Figure 2 – Substation-Based Security	7
Figure 3 – Enterprise-level security	9
Figure 4 – Substation- and Enterprise-level Security Implemented Together	10
Figure 5 – Cybectec security solution diagram	11

1. Introduction

With NERC CIP standards becoming mandatory in the United States, the question of security has gone from a concern to a priority. For engineering teams involved with substation automation and integration projects, NERC CIP is often seen as a complication. For IT professionals, NERC CIP is another set of electronic security levels to implement.

Cooper Power Systems' Cybectec product line can help utilities meet NERC CIP standards without compromising access to their IEDs or complicating the IT infrastructure.

This document is aimed at utilities' engineering and IT teams. It is intended to help them understand the different strategies that are available to secure their substation equipment in a NERC-compliant manner.

For more information on meeting NERC CIP standards, do not hesitate to contact us at: <http://www.cooperpower.com/CustomerService/contact.cfm>.

1.1 Modernizing the Process Network

In recent years, many utilities have started using WAN technologies with the goal of upgrading their communications infrastructure and providing an improved data path between the substation and the enterprise.

Modern communications technology between the substation and the enterprise provides utilities with numerous benefits:

- SCADA can now benefit from the additional operational data being produced by modern protective relays, and the numerous IEDs being installed.
- Additional control centers such as DMS, EMS and OMS can now directly access data produced by substation devices.
- Engineering and maintenance groups can now remotely access substation devices to retrieve equipment monitoring data or modify device settings.

Before the September 11 events, very few utilities were concerned by the security of their substation process network. The concern for security was further increased with the August 2003 blackout. While it was not caused by a security incident, it provided a vivid demonstration of the vulnerability of the power grid and prompted regulatory bodies to tighten utilities' margin for error when it comes to protecting their networks.

1.2 Mandatory Security

The traditional SCADA system has always been considered secure because it used proprietary technology and communicated using dedicated telephone lines. With the growing use of standard IT technology in the process network, the “security by obscurity” approach can no longer be considered valid.

The North American Energy Reliability Corporation (NERC) reacted to the growing vulnerability of control systems by setting the Critical Infrastructure Protection (CIP) standards. Utilities must now (Q2 2007) begin the work required to comply with these standards, and be auditably compliant by Q2 2010.

1.3 NERC CIP Requirements

A complete description of the NERC CIP requirements is beyond the scope of this document. However, these requirements can be summed up quite easily:

- Utilities must identify all critical assets – control centers, transmission substations, generation resources, systems and facilities critical to system restoration, and load shedding systems capable of shedding 300 MW or more.
- Utilities must identify critical cyber assets. Critical assets that communicate using a routable protocol or a dialup modem are considered to be critical cyber assets.
- All personnel that can operate critical cyber assets needs to be security screened.
- All critical cyber assets must be enclosed within a secure physical perimeter.
- All critical cyber assets must be enclosed within a secure “electronic perimeter” that limits access to authorized users only, blocks all unnecessary ports and services, and provides complete logging and monitoring services.
- Utilities must be able to restrict access to previously authorized users quickly and efficiently.

Utilities must now also document:

- Who has access to which critical cyber asset.
- All changes to hardware and software components of their critical cyber assets.

NERC CIP applies to all utilities that possess critical assets. Even if they do not, they still need to provide an inventory of all their assets and demonstrate that none are critical cyber assets.

All substation IEDs that are accessible using a TCP/IP network or a dialup modem can be considered critical cyber assets.

For more information on NERC CIP standards, visit [NERC's](#) web site.

For more information on how our Solutions help customers comply with NERC CIP standards, request the document “Meeting NERC requirements with Cybectec Solutions” from sales@cybectec.com.

1.4 Strategies for Meeting NERC CIP Requirements

All security solutions offered in the market today can be divided in three conceptual categories:

- Access to substation data is restricted to SCADA only
- Substation-level access control
- Enterprise-level access control

1.4.1 Access Restricted to SCADA Only

This basic model grants access to the SCADA master only. This model usually relies on the organization’s IT department to secure the link to the substation, using industry best practices. For example, a set of routers that only allows communications from a specific source. Often, TCP/IP is not used. Instead frame relay access devices (FRAD) are used to transport serial data between substation devices and SCADA.

No other user or system can access the substation remotely. There is no other access point to the substation devices. Communication is limited to SCADA protocols such as DNP3, Modbus, etc.

As long as no remote IED access is provided, the typical SCADA/RTU system can be considered substantially NERC CIP compliant. The corporate WAN uses the remote access bridge (such as a FRAD) to create the required electronic perimeter and protect substation devices. User authentication and access logging are implemented at the SCADA level.

This is the simplest solution to secure access to substation equipment and data. However, its shortcoming is that it limits the amount of data that is available. Since most SCADA systems will only poll operational data from substation equipment, most non-operational data remains unused. Moreover, engineering and maintenance teams may not have access to the SCADA system, and the SCADA itself may not provide the data those groups require.

No remote maintenance access is permitted. Maintenance on the IEDs must be performed locally.

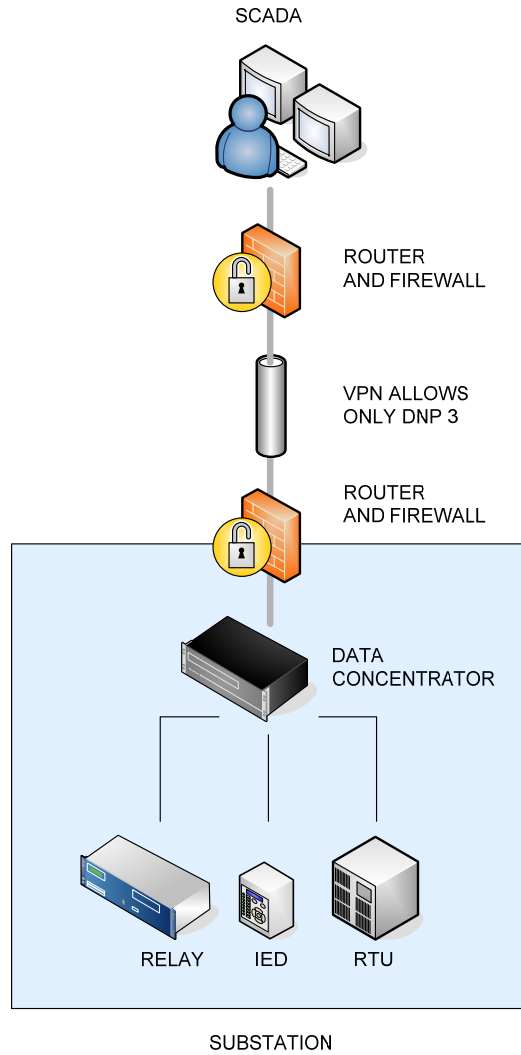


Figure 1 – Access Restricted to SCADA

1.4.2 Substation-Level Access Control

Providing secure remote access to substation devices for engineering and maintenance is much more challenging than just allowing SCADA to access substation equipment. In this case, the access points themselves must provide a NERC CIP-compliant electronic perimeter.

Substation-level access control places the function of authenticating users and keeping access logs in a substation gateway, data concentrator or security appliance. This type of solution usually uses the gateway or data concentrator as the single point of access to substation equipment and data.

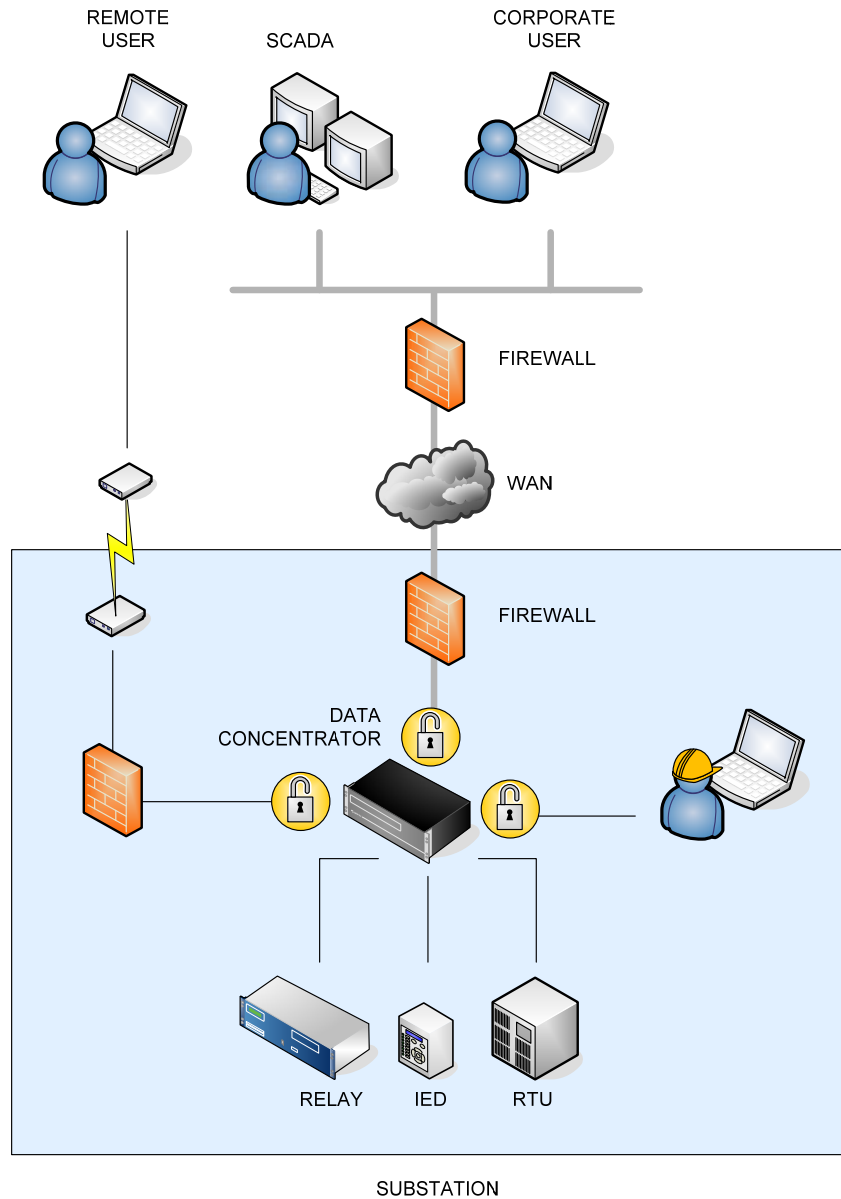


Figure 2 – Substation-Based Security

A important benefit of this security strategy is that it does not rely on a remote server or the corporate WAN to be present to provide user authentication. If the corporate link is not active, local users and remote users using other communication links (such as dialup) can still access substation equipment.

Implementing access controls at the substation-level introduces a number of challenges:

- Each gateway device must have its own security database that must be managed individually. Removing access to a user requires that each security database be updated. Ideally, this process should be automated.
- Each gateway device must maintain its own access logs. These logs must be retrieved and consolidated.
- Firewall rules must be configured to allow access from each possible remote computer.

Note that with some vendor solutions, the gateway device requires a permanent connection to a corporate security server to provide authentication. This reduces availability of the substation devices and does not provide the same benefits as having a completely local authentication mechanism.

1.4.3 Enterprise-Level Access Control

To solve the challenge of managing distributed systems and alleviate the reporting tasks, many vendors use an enterprise-level server to provide secure passthrough access to substation devices. The server ties in to the corporate security infrastructure to provide user authentication, leveraging existing security servers, such as RSA SecurID, to provide two-factor authentication.

Often, an application server such as CITRIX is used to host native vendor tools and simplify the management of client workstations.

Centralized access control means centralized user and device management, a valuable time-saver for IED network administrators. Also, this strategy allows the automation of several NERC CIP-required reports.

A shortcoming of this strategy is that local maintenance and configuration depends on the corporate network being present at the substation. For example, a local technician must go through the central passthrough server on the corporate network to access the device that may be physically in front of him or her. If the link to the corporate server is down, there can be no local access to substation devices.

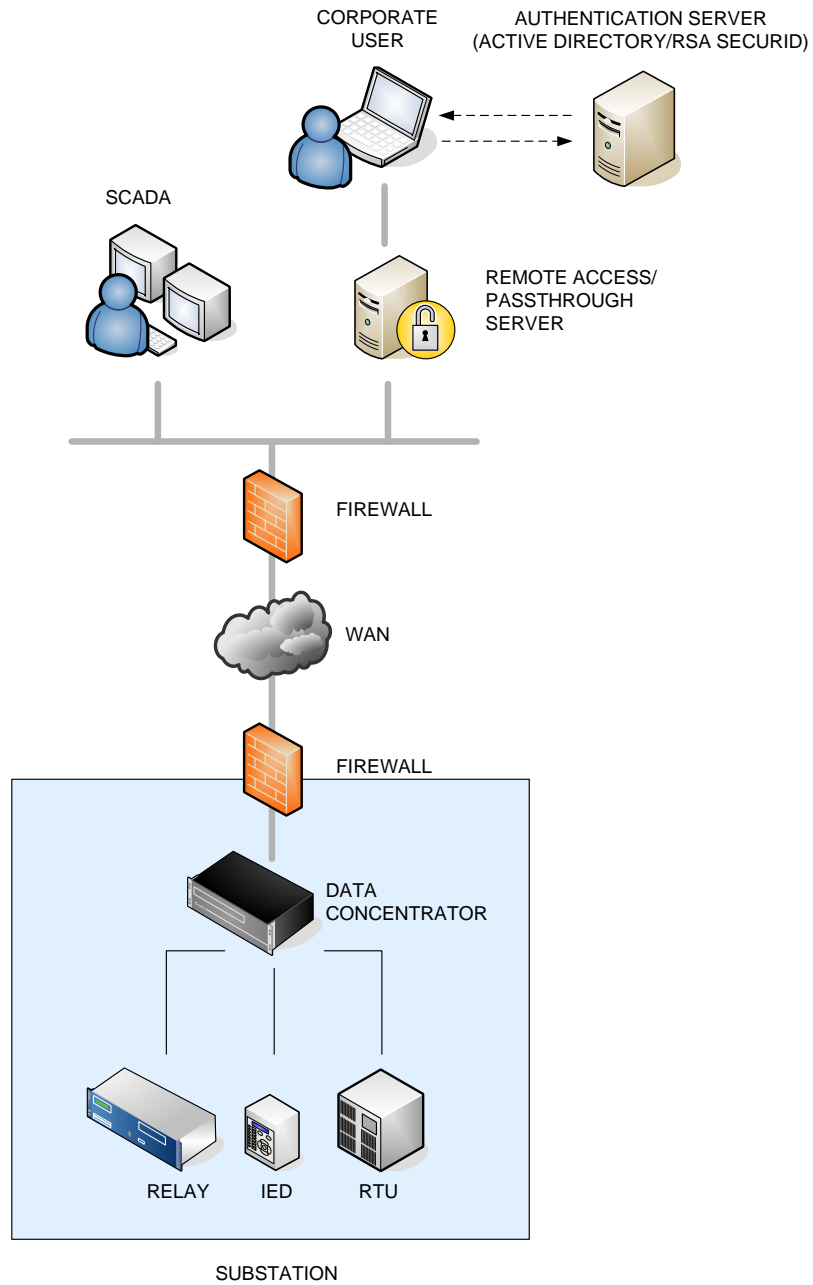


Figure 3 – Enterprise-level security

1.4.4 The Best of Both Worlds: Substation- and Enterprise-Level Access Control

One way to compensate for the shortcomings of the two previous security strategies is to implement centralized security, with local security available if the link to the security server is down. This ensures that substation devices and data remains secured and available to authorized users at all times.

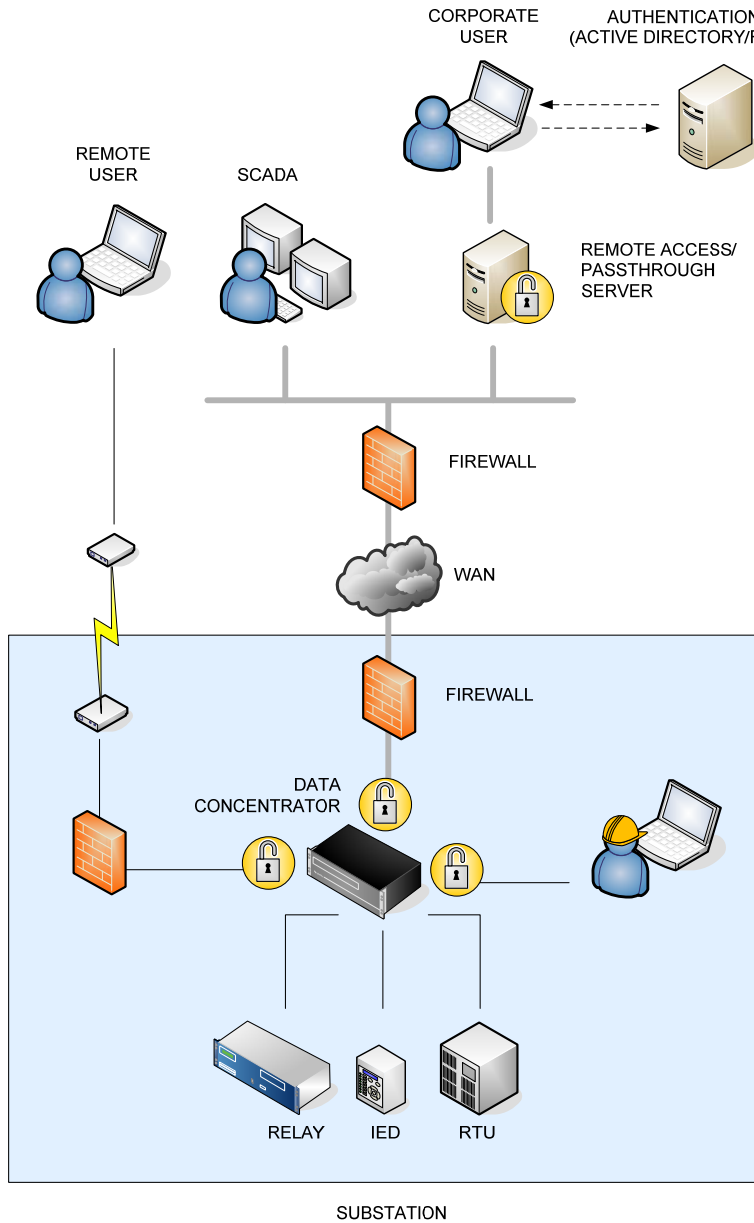


Figure 4 – Substation and Enterprise-level Security Implemented Together

2. About Cooper Power Systems Substation Solutions and IED Manager Suite

Cooper Power Systems Substation Solutions and IED Manager Suite help utilities integrate IEDs into a cohesive, automated whole, providing complete, enterprise-wide access to operational and non-operational substation data in a highly secure environment. These solutions work in tandem, allowing utilities to build a comprehensive communications infrastructure that is secure, fully integrated, delivers maximum reliability, and improves service quality.

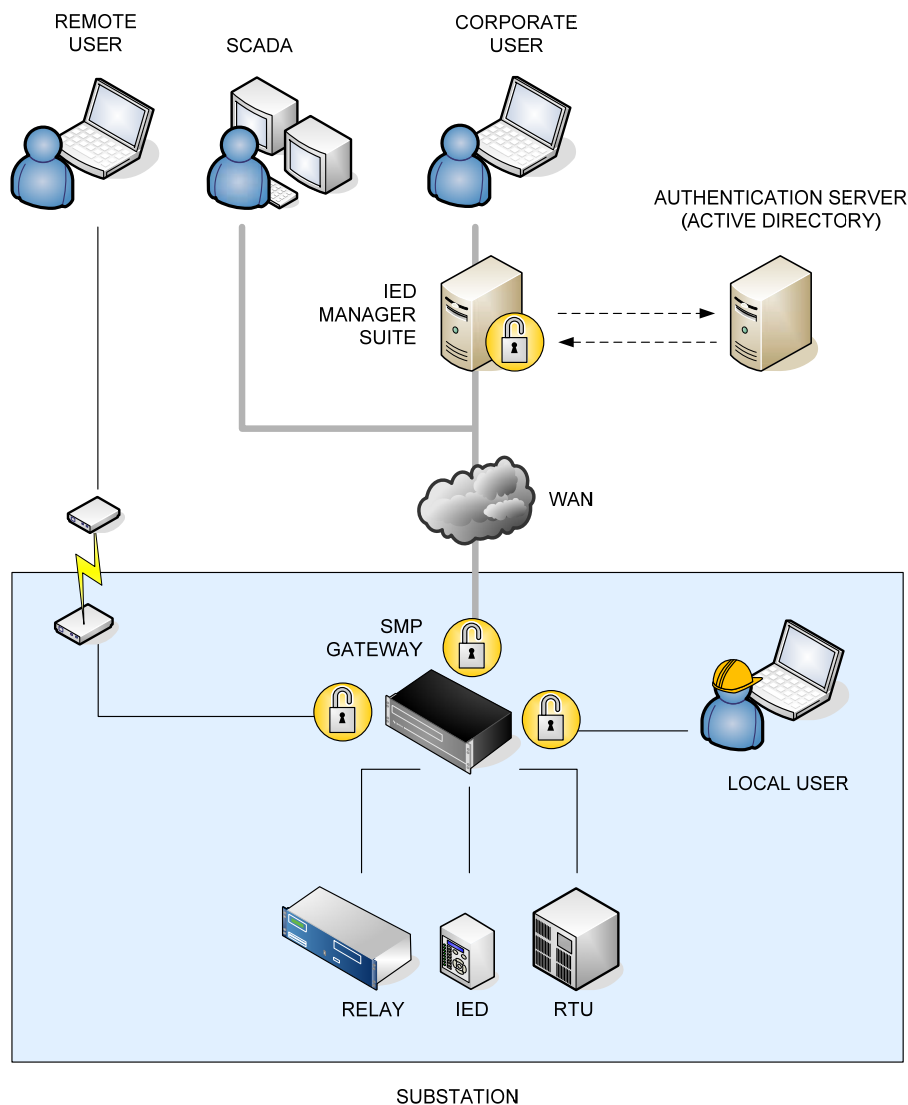


Figure 5 – Cooper Power Systems security solution diagram

Cooper Power Systems' security solution is twofold: substation and enterprise. The modules of the Yukon IED Manager Suite (IMS) are installed at the corporate level and the Cybectec SMP Gateways are installed at the substation level.

At the enterprise level, IMS is a software suite that performs centralized authentication, event retrieval, user and IED management, and ensures users within the corporate LAN access remote devices securely. The Passthrough Manager supports SEL 20xx gateways, direct IED connections and SMP Gateways.

At the substation level, SMP Gateway product line provides the NERC CIP-compliant, secure, single access point to substation devices and data. SMP Gateways feature secure access control and logging capabilities locally. They can also connect to IMS for centralized authentication, enhanced logging and reporting.

All those products are compliant with applicable NERC CIP standards. For a detailed list of our Solutions for NERC CIP standards, request "Meeting NERC Requirements with Cybectec Solutions" from sales@cybectec.com.

2.1 Yukon IED Manager Suite (IMS)

IED Manager Suite is a software suite that links corporate users to devices in the substation. Cooper Power Systems' security solution uses the Security Server, Passthrough Manager and Configuration Manager.

While competitors simply provide a secure passthrough solution, IMS also provides automated event and data retrieval features. IMS make substation data available to all authorized corporate users, from a secure, central location within the corporate network. Instead of having each user connect individually to IEDs, they can retrieve the data already extracted from the IED by the IMS server.

Cybectec Enterprise Gateway retrieves real-time data from substation gateways and devices. It is then available to enterprise systems through the **OPC Data Bridge** and **OSIsoft PI Data Bridge** software modules.

Passthrough Manager establishes a transparent connection between a client application and a remote IED, through an SMP Gateway, a SEL 203x gateway, or a direct IP connection. It provides a central point of access and password management for IEDs.

Configuration Manager provides a centralized location to manage the inventory, configuration change history, backup and restore IED configuration and passwords of IEDs and SMP Gateways installed in the field.

Security Server connects to the client's existing corporate security infrastructure and provides centralized authentication and authorization services for all products. Permissions can be assigned to corporate accounts for single-login access to all substation and enterprise solutions.

2.2 Cooper Power Systems Substation Solutions

In the substation, the SMP Gateway already features NERC CIP-compliant security: local user accounts with definable permissions, access logs and account lockout upon multiple failed attempts, a VPN, SSL, firewall and constant file integrity monitoring.

Coupled with IED Manager Suite, the SMP Gateway also supports centralized authentication via the Security Server.

Hence, the SMP Gateway becomes the secure single-point of access to substation data for all users, local or remote.

2.3 Technical Overview

SCADA systems usually have their own secure connection to the SMP Gateway and substation devices. The design goal of IED Manager Suite is to provide corporate users with a secure enterprise level single point of access to substation devices, separate from the SCADA data path.

The Passthrough Manager is the single access point for engineering and maintenance applications. This IMS module truly isolates IED and SMP Gateways from the users by automatically managing access codes and device passwords.

Communication encryption is guaranteed from client to IMS servers, and from the servers to the SMP Gateway. Encryption is provided by Windows CE PPTP VPN server using a 128-bit key and RC4 algorithm. An SSL solution is currently being developed to increase encryption strength and provide encryption for SCADA protocols.

Just like the Passthrough Manager at the enterprise level, the SMP Gateway acts as the single access point to data and devices at the substation level. It includes NERC CIP-compliant local authentication, in the event that the link to the corporate network is down, and hence central authentication is not available.

SMP Gateways use the Windows CE industrial operating system. This rugged operating system is ideal for high-availability systems and is virtually immune to cyber-attacks. For increased protection, SMP Gateways will only run components signed by Cooper Power Systems.

Our substation solutions also feature local and centralized logging via the syslog protocol.

Unlike its competition, Cooper Power Systems does not rely on third-parties to provide a complete, NERC CIP-compliant enterprise and substation security solution.

3. Contact us

Cooper Power Systems Substation Solutions and IED Manager Suite can help utilities secure their power network, improve reliability, reduce outage duration and optimize asset utilization.

For more information on how our Solutions help customers comply with NERC CIP standards, request the document "Meeting NERC requirements with Cybectec Solutions" from sales@cybectec.com.

Appendix A - Web Page References

NERC CIP Standards

<http://www.nerc.com/page.php?cid=2%7C20>

Cooper Power Systems

Substation Gateway

<http://www.cooperpowereas.com/Products/SMPGateway/SMPGateway.cfm>

Enterprise Solutions

<http://www.cooperpowereas.com/Products/IEDManagerSuite/IEDManagerSuite.cfm>

<http://www.cooperpowereas.com/Products/NERC-CIP/Security.cfm>