Communications Technologies and Practices to Satisfy NERC Critical Infrastructure Protection (CIP)

Tim Tibbals and David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
5th Annual Clemson University Power Systems Conference
Clemson, South Carolina
March 14–17, 2006

Originally presented at the
7th Annual Western Power Delivery Automation Conference, May 2005,
under the title “Substation Communication Techniques to Satisfy
NERC Urgent Action Standard 1200”

COMMUNICATIONS TECHNOLOGIES AND PRACTICES TO SATISFY NERC CRITICAL INFRASTRUCTURE PROTECTION (CIP)

Tim Tibbals and David Dolezilek
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

ABSTRACT

Events of the last several years, such as 9/11 and the East Coast blackout of August 2003, have brought about heightened awareness of the importance and vulnerability of critical infrastructure assets in North America and the world. Many organizations have worked to provide guidance to those responsible for these critical infrastructure assets, to increase security and reliability from both a physical and electronic access perspective. This paper addresses the new North American Reliability Council (NERC) Critical Infrastructure Protection (CIP) requirements, which have replaced the guidelines in the previous NERC Standards 1200 and 1300 on cybersecurity.

This paper is a tutorial on how to deploy Intelligent Electronic Devices (IEDs) and communications and security technology to satisfy each applicable section of the NERC CIP and reduce the chances of electronic intrusion. Through use of the information in this paper, each entity can begin the process of satisfying internal responsibilities to proactively improve security and strengthen their security posture. These steps include the following:

- Understand communications installations and assess security vulnerabilities.
- Create and maintain a cybersecurity policy to reduce security vulnerabilities.
- Stop all unnecessary communications and block all unnecessary connections.
- Encrypt all remote communications.
- Pass all remote communications through a communications processor that filters all communications, prevents the introduction of malicious software, prevents the use of "backdoor passwords," and controls the use of EAPs automatically and in response to commanded control. Use this communications processor to detect, alarm, stop, and lock out illegitimate communication.
- Choose IEDs that provide communications access warnings for every communications port.
- Create security administrator console with visibility and control of security features.
- Create an early warning system using integrated new and in-service I/O processors and IEDs for substations, control centers, and engineering access workstations.
- Create an engineering access method to collect and view diagnostics and data logs.
- Appropriately authenticate all access via passwords, etc.
- Place all PCs on secure LANs and configure appropriate NIST security.

INTRODUCTION

The mission of the North American Electric Reliability Council (NERC) is to ensure that the bulk electric system in North America is reliable, adequate, and secure. NERC operates successfully as a voluntary organization, relying on reciprocity, peer pressure, and the mutual self-interest of all those involved. Through this voluntary approach, NERC has helped to make the North American bulk electric system the most reliable in the world. Because of its leading role developing an interim and permanent cybersecurity standard, NERC will likely influence other standards and other industry bodies representing related industries (such as water/wastewater, gas, and all industrial processes) including:

- Instrumentation, Systems, and Automation Society (ISA SP-99)
- National Institute of Standards and Technology (NIST)
  - Process Control Security Requirements Forum (PCSRF)
- International Electrotechnical Committee (IEC)
  - Working Groups including WG 15, WG 65C
- American National Standards Institute (ANSI)
- Institute of Electrical and Electronic Engineers (IEEE), various technical standards
- International Standards Organization (ISO), ISO 17799, BS 7799, BS 7799-2
- International Council on Large Electric Systems (CIGRE)
- Chemical Industry Data Exchange (CIDX)
- Regulatory (Food bioterrorism, 21CFR 11)
- Government (Department of Homeland Security, Department of Energy, etc.)

NERC has historically developed standards applicable only to control areas. However, the council recently changed from regulating control areas to a Functional Model [2], which makes the standards applicable to all entities performing functions within the bulk electric system. Therefore, NERC *Standards CIP-002 through CIP-009 — Cyber Security* [8] explicitly requires compliance by each of the following entities:

- Generator owners
- Generator operators
- Transmission service providers
- Transmission owners
- Transmission operators
- Load-serving entities
- Reliability coordinator
- Balancing authorities
- Interchange authorities
- Regional reliability organizations
- NERC

Because the purpose of NERC *Standards CIP-002 through CIP-009 — Cyber Security* is to ensure that the bulk electric system in North America is reliable, adequate, and secure, it is clear that each entity interconnected to those listed above should maintain an independent level of security, as well as manage the self-certification and compliance of partners with whom the utility interconnects. These other entities include, but are not limited to, providers of the following:

- Power distribution
- Gas
- Water
- Wastewater
- Telecommunications
- Cable
- Purchasing selling entities
- Planning
- Internet
- Pipelines
- Railroad
- Industrial processes

NERC *Urgent Action Standard 1200 – Cyber Security*, initially authored in 2004, evolved the NERC *Cyber Security Standard 1300* [5], and finally became a permanent suite of standards referred to as NERC *Standards CIP-002 through CIP-009 — Cyber Security*. The NERC CIP standards represent significant work by the drafting team to ensure consistency across the suite of cybersecurity standards to ensure that levels of noncompliance are auditable and correctly matched to requirements, to clarify the requirements, and to eliminate redundancy between the standards.

Terms and Definitions Used in the Suite of Standards

> ***Critical Assets.*** *Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.*
>
> ***Cyber Assets.*** *Programmable electronic devices and communication networks including hardware, software, and data.*
>
> ***Critical Cyber Assets.*** *Cyber Assets essential to the reliable operation of Critical Assets.*
>
> ***Cyber Security Incident.*** *Any malicious act or suspicious event that:*
>
> - *Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,*
> - *Disrupts, or was an attempt to disrupt, the operation of a Critival Cyber Asset.*
>
> ***Electronic Security Perimeter.*** *The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.*
>
> ***Physical Security Perimeter.*** *The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.*

ROADMAPS TO COMPLIANCE

The next section of this paper addresses each section of the NERC *Standards CIP-002 through CIP-009 — Cyber Security* by providing a excerpts of the standard (in italics), summary interpretation of these requirements and a list of positive actions to take toward compliance and certification of substation communications. This paper does not address other components of a comprehensive cybersecurity procedure. This suite of standards, NERC *Standards CIP-002 through CIP-009 — Cyber Security*, includes:

Standard CIP-002-1 Critical Cyber Asset Identification
Standard CIP-003-1 Security Management Controls
Standard CIP-004-1 Personnel and Training
Standard CIP-005-1 Electronic Security Perimeter(s)
Standard CIP-006-1 Physical Security
Standard CIP-007-1 Systems Security Management
Standard CIP-008-1 Incident Reporting and Response Planning
Standard CIP-009-1 Recovery Plans for Critical Cyber Assets

The NERC *Standards CIP-002 through CIP-009 — Cyber Security* documents the requirements to demonstrate due diligence in creating and executing a cybersecurity plan as follows.

> *Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.*

STANDARD CIP-002-1 CRITICAL CYBER ASSET IDENTIFICATION

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange.

The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- *The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,*
- *The Cyber Asset uses a routable protocol within a Control Center; or,*
- *The Cyber Asset is dial-up accessible.*

For all entities, assets falling under this standard would be those for which the loss or compromise of the cyber assets would adversely impact the reliable operation of utility system assets. In general, a comprehensive list includes all computing systems, communications equipment, and intelligent electronic devices (IEDs) in use by the entity.

Call to Action

1. Document risk-based assessment methodology.
2. List critical assets.
3. List critical cyber assets.
4. Maintain records of annual approvals of the above stated lists.

STANDARD CIP-003-1 SECURITY MANAGEMENT CONTROLS

Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.

Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

Each entity should create, document, and maintain a cybersecurity policy, and assign a member of senior management the responsibility for leading and managing the entity's cybersecurity program. This person would authorize any deviation or exception from the requirements of this standard. Justification for any such deviation or exemption should be documented.

The cybersecurity policy needs to be comprehensive and satisfy all needs of the entity. With respect to the substation communications policy (a subset of the cybersecurity policy) personnel at each entity should identify and understand existing practices as well as proposed changes.

Communications connections are categorized as constant, such as SCADA and ad hoc engineering access that is activated on demand.

> *Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.*

Each entity should identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information.

Each entity should classify information related to critical cyber assets to aid personnel in determining the relative sensitivity of information, what information can be disclosed to unauthenticated personnel, and what information should not be disclosed outside of the entity without proper authorization.

Each entity must identify the information access limitations related to critical cyber assets according to classification level.

> *Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.*
>
> *Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.*

Call to Action

5. Document existing procedures and proposed changes as part of a comprehensive cybersecurity policy.
6. Document assignment of, and changes to, the responsible entity's leadership.
7. Document exceptions to the existing procedures and proposed changes.
8. Document the responsible entity's information protection program.
9. Review available technology and best practices to identify necessary modifications, such as bump-in-the-wire encryption.
10. Document existing connections and methods of communication to, from, and within the substation, pole-top IEDs, SCADA center, and engineering workstations. Identify connections as constant or ad hoc.
11. Document the responsible entity's change control and configuration management plans.

STANDARD CIP-004-1 PERSONNEL AND TRAINING

> *Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.*
>
> *Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis.*
>
> *Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted* physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> *Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access.*
>
> *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.*

Each entity should identify and document all personnel, including contractors and service vendors, granted electronic or physical access to critical cyber assets. The responsible entity should conduct background screening of personnel consistent with the degree of access they are granted, in accordance with federal, state, provincial, and local laws.

Each entity should train personnel commensurate with their access to critical cyber assets as well as document associated training plans. The training should address, at a minimum: the cybersecurity policy, physical and electronic access controls to critical cyber assets, the release of critical cyber asset information, potential threat incident reporting, and action plans and procedures to recover or re-establish critical cyber assets following a cybersecurity incident.

Training should be conducted upon initial employment and reviewed annually. The training should include, but is not limited to:

- Company cybersecurity policy
- Physical and electronic access controls to critical cyber assets
- Procedures for release of critical cyber-asset information
- Potential threat incident reporting
- Action plans and procedures to recover or reestablish critical cyber assets following a cybersecurity incident.

Call to Action

12. Implement and document a security awareness and reinforcement plan pertaining to the security policy.
13. Implement and document a training plan pertaining to the security policy.

14. As part of the cybersecurity policy, document existing procedures for identifying and documenting personnel.
15. Design a personnel risk assessment program and perform personnel risk assessment of all personnel who have authorized cyber or unescorted physical access to critical cyber assets.
16. Document lists of personnel with access rights as well as revocation of such rights.
17. Assign a security administrator responsible for monitoring security information.

STANDARD CIP-005-1 ELECTRONIC SECURITY PERIMETER(S)

> *Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.*
>
> *Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).*

Each entity should create, document, and maintain a description of each of its electronic security perimeters and verify that all critical cyber assets are within this perimeter. NERC describes an Electronic Security Perimeter as the logical border surrounding a network or group of subnetworks, referred to as the "secure network," to which the critical cyber assets are connected, and for which access is controlled. These secure networks are so called because the entity manages each device and connection and allows only trusted communications. Electronic security perimeters must be documented for each secure network that can communicate with another secure network.

These secure networks include, but are not limited to, the following:

- SCADA control centers
- EMS control centers
- Backup control center consoles
- Metering system consoles
- System administrator consoles
- Generation facilities
- Substations
- Pole-top IEDs
- Engineering access consoles
- Mobile engineering access laptops

Public and private communications channels used to connect secure networks together are referred to as Wide Area Networks (WANs). These include leased line and dial-up telephone, radio, frame relay, and virtual private network (VPN) links. In rare instances, secure networks are directly connected together by a dedicated end-to-end physical connection. We can consider WANs to be insecure because an entity relies on other communications service providers and utility personnel do not know or manage the devices and connections used. The devices that connect a secure network to a WAN, and vice versa, are Electronic Access Points (EAPs). EAPs include analog and digital modems, wireless modems, and routers. Transceivers, which serve as EAPs, manage direct connections. Figure 1 illustrates some examples of secure networks requiring electronic security perimeters. Unseen in this simplified drawing are encryption transceivers between the EAP and the secure network within each electronic security perimeter. Each rectangle in Figure 1 represents a unique collection of critical cyber assets for which one would need an electronic security perimeter.

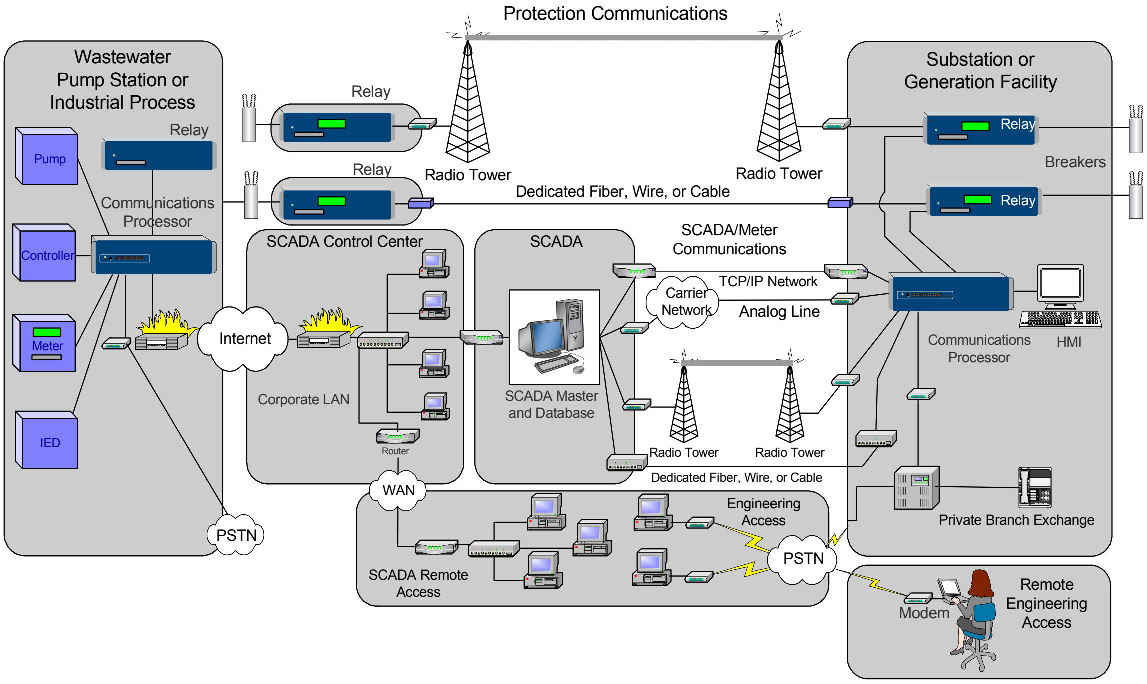
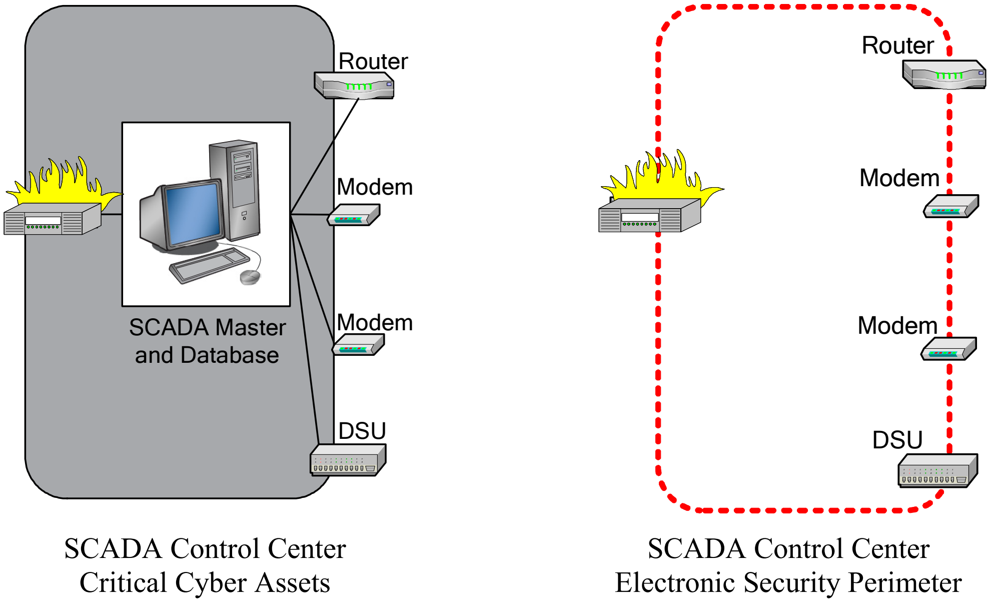


Figure 1 Communications Infrastructure Illustration

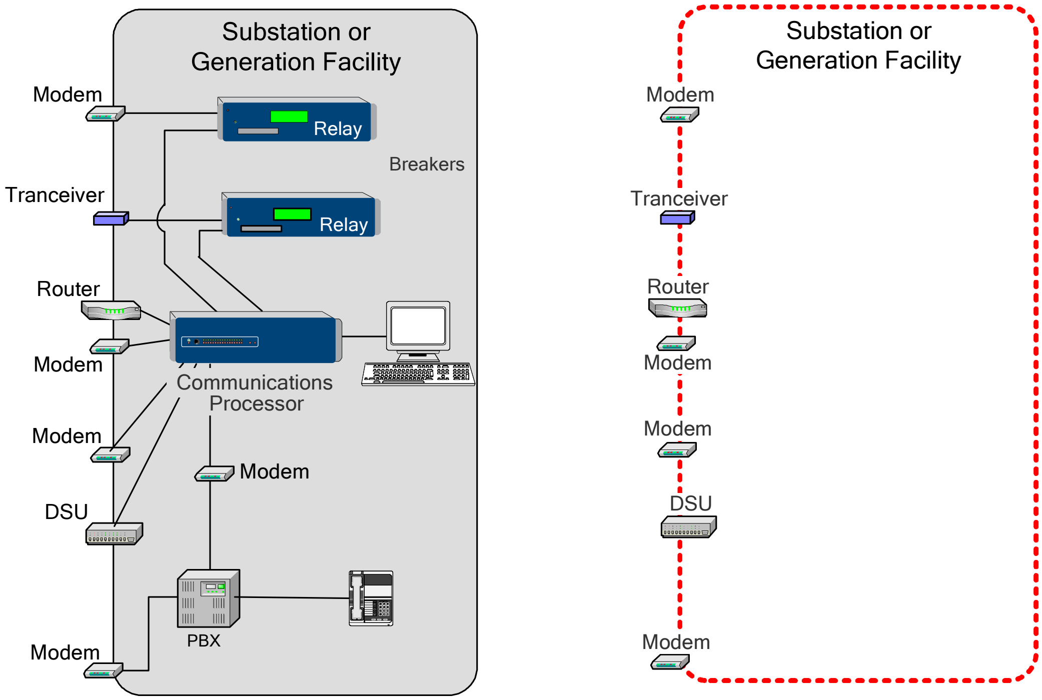
In practice, a security perimeter comprises the collection of all EAPs that permit access to the secure network. By visually connecting these devices together, as in the following figures, we can define an electronic security perimeter. Figure 2, Figure 3, Figure 4, and Figure 5 illustrate four examples of secure networks and their corresponding electronic security perimeters.



SCADA Control Center
Critical Cyber Assets

SCADA Control Center
Electronic Security Perimeter

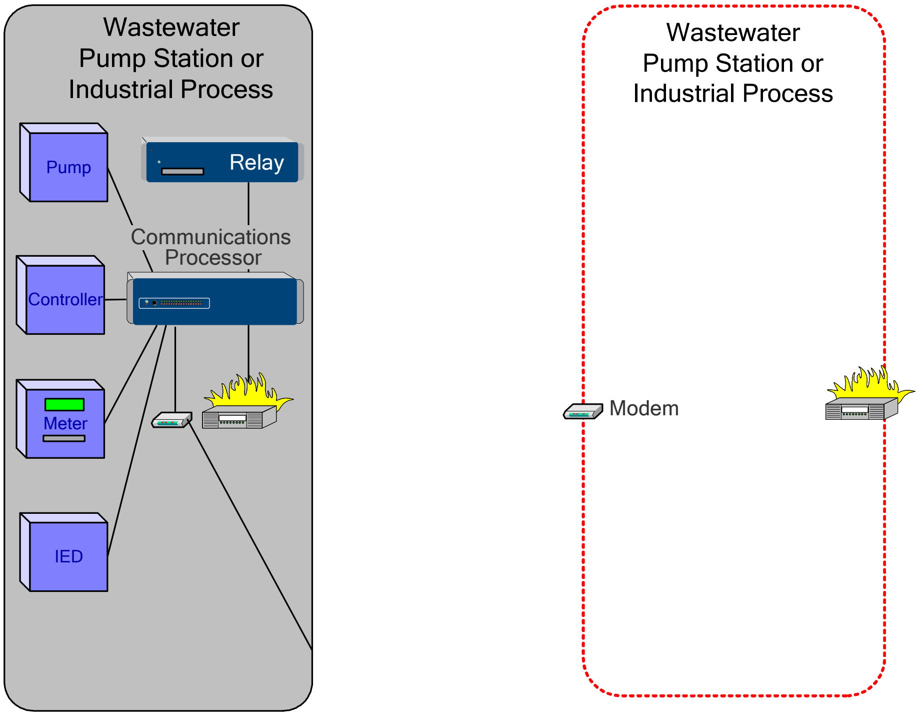
Figure 2 SCADA Control Center Example



Electrical Substation
Critical Cyber Assets

Electrical Substation
Electronic Security Perimeter

Figure 3 Electrical Substation Example



Industrial Substation
Critical Cyber Assets

Industrial Substation
Electronic Security Perimeter

Figure 4 Industrial Substation Example

Modem
Modem

Remote Engineering Access
Critical Cyber Assets

Remote Engineering Access
Electronic Security Perimeter

Figure 5 Remote Engineering Access Example

Complete documentation of each security perimeter includes an illustration of the perimeter, which you would create by visually connecting the EAPs, a complete list of the EAPs, and a complete list of all interconnected critical cyber assets in each secure network.

Electronic Access Controls

> *Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).*

Electronic access controls manage which, when, and under what conditions processes and people can connect to each device on each secure network. In the substation, communications processors manage communications that pass through the EAPs. The communications processor can be a function within a computing platform or a function within a stand-alone communications device. EAPs and communications processors act together to perform electronic access controls of communication connections to the secure network. Communications processors work together with features within the critical cyber assets to perform electronic access control of the critical cyber assets themselves.

Each entity should create, document, and maintain a description of the electronic access controls and their implementation for each critical cyber asset including EAPs, encryption devices, communications processors, IEDs and computing platforms associated with each electronic security perimeter.

As described in the *Security Guideline: Securing Remote Access to Electronic Control and Protection Systems* section of the NERC *Security Guidelines for the Electricity Sector* [6], NERC suggests using encryption when traversing unsecured networks to gain remote access. Other recent studies recommend using encryption whenever traversing unsecured networks including SCADA and control system communications. Therefore, an encryption device should be installed at every EAP.

The communications processor or function must control each EAP to permit or deny electronic access automatically, or in response to a commanded control from a system administrator or control system. It is common practice today to accomplish this control through use of output contacts to disable the EAP, interrupt power to the EAP, or interrupt the communications path between the EAP and the communications processor.

When using Ethernet LANs in the substation, SCADA and engineering access should be separated. The communications processor should support two unique Ethernet connections to two different EAPs, one for SCADA and one for engineering access. The communications processor Ethernet connection to SCADA should be set to permit only SCADA connections and disable unused SCADA protocols and all engineering access protocols. The communications processor

Ethernet connection to engineering access should be set to only allow engineering access connections and disable all SCADA connections.

Substation Devices Control the EAP

Application settings control access to devices connected to the EAP. Through the use of such settings, users perform commanded control to enable or disable connections based on verification need. The following example shows how to set a communications processor to enable and disable the passage of communications from an EAP through the communications processor and to a connected device.

Example: Control Logic Setting

NOCONN = !16:RB14

This equation turns access on and off. When 16:RB14 is set to a 1, the NOT (!) symbol inverts and NOCONN = 0. When NOCONN = 0, access to the EIA-232 pass-through connection is enabled.

Once a connection to an EAP is enabled, the communications processor manages connections directly to the cyber assets by enabling and disabling pass-through connections.

Simple Settings Eliminate Intrusion Through Otherwise Unused Connections

Unneeded communications ports on critical cyber assets should be configured so that they are unused or unusable.

Multiple protocol options exist on the serial port of many IEDs. By enabling a special purpose protocol on these ports, such as peer-to-peer or SCADA, you can prevent unintended connections to these ports from gaining immediate access.

Example: Port Communications Settings for Port 8 to Be Unused

PORT:8

DEVICE = U (Unused)

Example: Port Communications Settings for Port 1 to Be Set to SCADA Protocol

PORT:1

PROTO = DNP

A potential hacker will not know what protocol, if any, the port is configured to support, and is, therefore, prevented from using the port.

All local and remote ad hoc connections should prompt a security banner when initiated and perform an automatic time-out.

Disable All Backdoor Passwords

All default security settings should be changed and hard-coded backdoor passwords eliminated where possible. For existing devices with backdoor passwords, secure network components must automatically detect the use of the backdoor passwords and terminate communications. The following example shows how to set a communications processor to detect a known backdoor password and terminate pass-through communications.

Example: Port Communications Detect Backdoor Password and Suspend Communications

PORT:14

CMD1 = “Vendor#1_Backdoor_Password”

NOCONN = 14:CMD1

When the backdoor password for Vendor #1 IEDs passes through the communications processor, the command bit CMD1 is set to a 1. Pass-through communications is disabled by setting NOCONN = 14:CMD1, which has changed status to 1.

Strong Passwords Prevent Unwanted Intrusion

Each critical cyber asset shall support a multilevel password system with the capability of supporting industry-defined strong passwords. Various access levels allow small groups of specialized employees within geographic regions to share passwords on groups of IEDs. Use of this method compartmentalizes similar employees, provides access to only those functions that these employees require, simplifies the password change management process, and keeps IEDs from becoming unnecessarily complex and expensive. A multilevel password method that supports a minimum of three levels is described below:

Connect Only. Lowest access level, provides only asset identification.

Read Only. One level higher than Connect Only, provides viewing of asset parameters and information.

Beyond Read Only. Any level with more features than Read Only. This category provides various combinations of control abilities, extended data acquisition, data clearing and/or entry, and configuration manipulation.

Suspicious failed attempts to enter passwords will cause termination of the access and/or communications connection as warranted. There must be some means for logging this activity.

Innovative Features Prevent Misuse of Commands Passed “In the Clear”

For communications processors that allow engineering access “in the clear” or unencrypted, passwords should be combined with settings that obscure the functionality of the communications connections or add another level of security. These obscurity settings change the methods of interaction between the communications processor and the user. These methods are now different from the default methods; these methods are unique and known only to the utility. Other settings will prevent the communications processor from functioning, even with correct passwords, until the devices receive an additional permissive. This permissive is a non-default command that enables the functionality of the communications processor. The permissive command sequence is user definable and is either static (the same command each time) or dynamic (a different command each time). This permissive is a non-standard function that the utility creates through the use of logic. As such, it is not a standard documented feature, and any possible assailant would have no knowledge of the existence of this permissive or the corresponding command sequence.

Use a callback function to perform all ad hoc connections for backup control center connections. After the initial call, the connection shall be terminated and a new connection shall be automatically established to a known valid remote secure network. A security administrator should enable all ad hoc connections via remote control and there should be automatic inactivity timeouts to prevent unauthorized use of connections accidentally left open.

Security of Computers in Substations

The present state of PC security technology requires that computers or networks not be connected directly to the WAN via the EAP. Instead, all communication should pass from the EAP through a communications processor and then on to the computer. This connection method prevents unauthorized access and transmission of malicious code. Future computer developments will be necessary to enable the computers to manage these issues for themselves.

When it is necessary to connect the computer or network directly to the EAP for engineering access, the system administrator should manage the EAP via controls from the communications processor, as previously described. In this way, the communications processor protects the computer and network until the exact moment that the WAN connection is needed. This is a poor second alternative because, although the computer is protected while the EAP is disconnected, the computer remains threatened by the introduction of malicious code through the direct connection.

When it is necessary to connect the computer or network directly to the EAP for SCADA, all other types of communication, including engineering access and other SCADA protocols, must be disabled on the computer. The National Institute of Standards and Technology (NIST) has produced *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist* [7]. The main goal of the document is to recommend and explain tested, secure settings for Windows® XP workstations. These settings are organized into groups or templates that are applied according to computer usage. The following are the four categories or classes of security settings NIST defines.

SOHO. SOHO describes small, informal standalone computer installations that are used for business purposes.

Enterprise. Enterprises are typically managed environments that are very structured in terms of hardware and software configurations.

High Security. A high-security environment is one that is at high risk of attack or data exposure.

Legacy. A legacy environment contains older systems or applications that use outdated communications mechanisms. Other machines operating in a legacy environment may need less restrictive security settings before these machines can communicate with legacy systems and applications.

The high-security configuration is recommended for computers used in the substation.

Actively and Continually Monitor Electronic Access

> *Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.*

Each entity should monitor electronic access to critical cyber assets 24 hours a day, 7 days a week. Monitoring consists of detecting, monitoring, and recording access activity as well as creating alerts or alarms as appropriate.

Add alarm outputs from electronic access points, encryption devices, computing platforms, communications processors, and other IEDs to existing instrumentation and control (I&C) systems within the utility where possible. Also implement the ability to control these devices. If it is not possible to do this with the existing I&C system, it will be necessary to create a stand-alone system to perform security, data acquisition, and control.

Electronic access includes both remote users connecting through EAPs and local users connecting via operator interface or local computer connection. Monitored connections include, but are not limited to, the following:

- Ad hoc and on-demand connections through any EAP
- Ad hoc and on-demand connections through the communications processor to any connected critical cyber asset
- Ad hoc and on-demand connections through rogue, previously unknown electronic connections to any critical cyber asset
  - Secretly installed and unknown EAP
  - Secretly installed and unknown connections between a known EAP and a critical cyber asset

Electronic access monitoring includes displaying, reporting, and recording present status and change of status of physical and electronic security indications. It also includes storage and/or remote access to diagnostics and data logs.

Early Warning System

Early warning systems quickly present information to the security administrator via visible and audible indication and direct telephone contact.

Use a security console to make these data available to the security administrator. This console can stand alone or be incorporated into the display of a SCADA system.

The present status of the physical and electronic security indications are best displayed through the use of methods similar to those used for SCADA and HMI displays. Figure 6 illustrates a security one-line display of the present status of substation security indications.

In addition to status displays, use visual and audible annunciators and event messenger devices to quickly alert individuals about pertinent changes in security status. Automatic event messenger devices communicate security warnings directly to the security administrator via telephone in case the displays and annunciators are not being monitored.

Security Data Logs and Diagnostics

When time-stamped, the security activity change-of-state records create a sequence-of-events (SOE) or sequential event record (SER). The aggregate of these time-stamped activity records provides an activity log of what security activities took place, when, and in what order. Other diagnostics and data logs are stored in the individual IEDs and are retrieved via engineering access methods. The security administrator should review logged data within the IEDs for evidence of invalid access, alarms, system diagnostics and failures. Design the security administrator console to support remote engineering access.

Security Status Indications

Monitored electronic access statuses include at a minimum, but are not limited to, the following for each computing platform, IED, communications processor, and electronic access point device:

- Device power up detection
  - This may indicate inappropriate access during power failure
- Device health, failure, alarms

- Device activation status
- Device operational status
  - Device may be healthy but disabled for maintenance
- Device indication that new settings have been saved
- Detection of ad hoc or on-demand connections into each device through EAP
  - Successful navigation of password access
  - Unsuccessful attempt to navigate password access
- Detection of ad hoc or on-demand connections into each device through local computer connection
  - Successful navigation of password access
  - Unsuccessful attempt to navigate password access
- Detection of ad hoc or on-demand connections into each device through local communications processor connection
  - Successful navigation of password access
  - Unsuccessful attempt to navigate password access
- Detection of ad hoc or on-demand connections into each device through local user interface
  - Successful navigation of password access
  - Unsuccessful attempt to navigate password access
- Jurisdictional permissive change detection
  - Which entity has responsibility for control
- Operational permissive change detection
  - Is the device configured to permit operation of apparatus
    - Normal
    - Blocked due to maintenance
    - Blocked due to electronic data (interlock) from another device
    - Blocked due to security perimeter violation
- Communications path status between EAP and communications processor
- Communications path status between communications processor and computing platform or IED
  - Enabled/disabled
  - Locked as a result of security perimeter violation

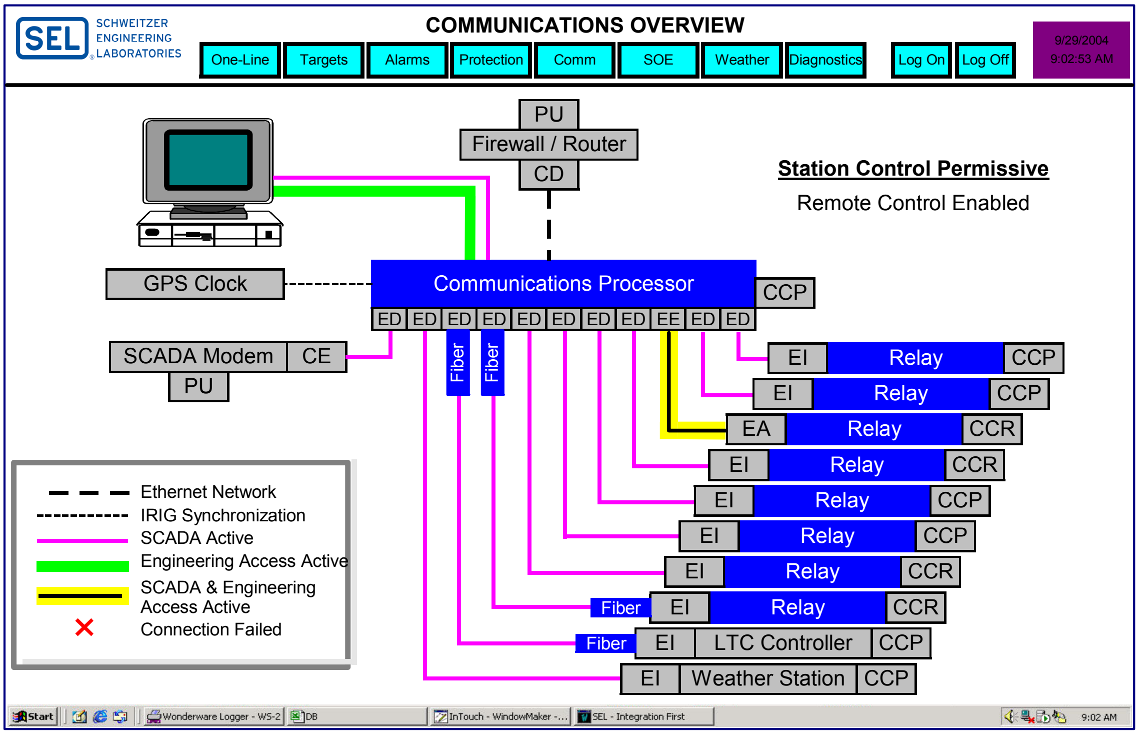
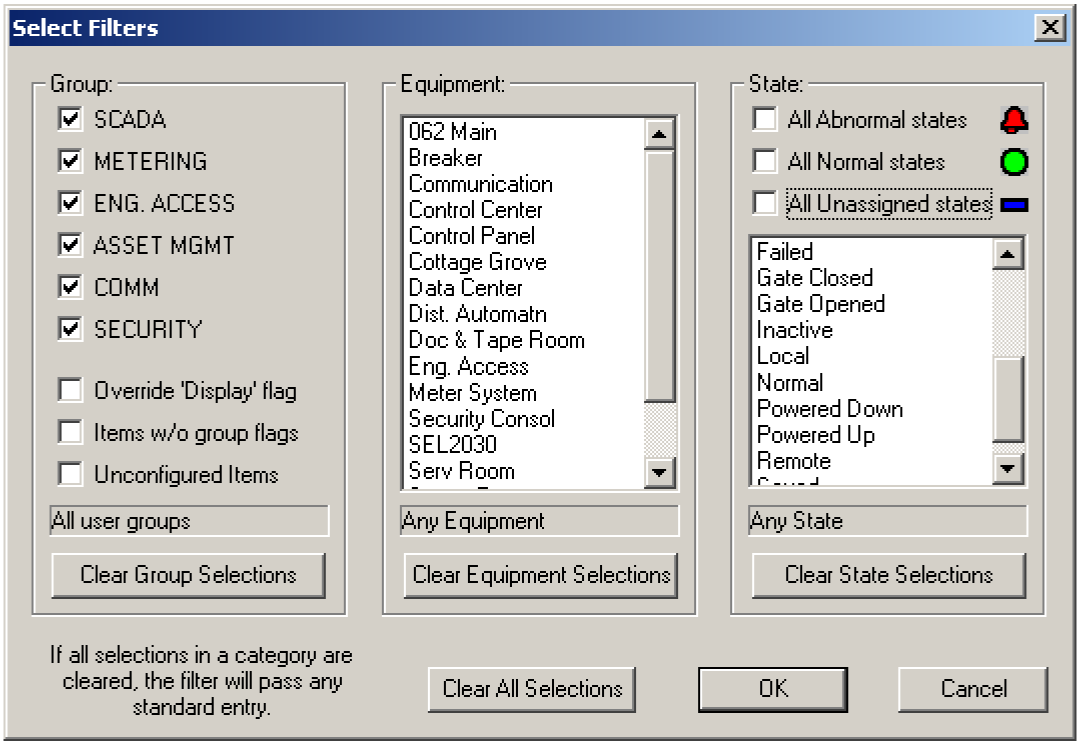


Figure 6 Security Overview Screen

In Figure 6, the communications and security status are abbreviated as follows.

- On relay or IED
  - EI – IED commanded control enabled, level two engineering access inactive
  - EA – IED commanded control enabled, level two engineering access active
  - CCP – IED commanded control permitted
  - CCR – IED commanded control restricted
- On communications processor
  - ED – communications processor to IED commanded control enabled, communications processor to IED engineering access disabled
  - EE – communications processor to IED commanded control enabled, communications processor to IED engineering access enabled
  - CCP – communications processor commanded control permitted
  - CCR – communications processor commanded control restricted
- On EAP – Modem or router
  - PU – powered up
  - PD – powered down
  - CE – connection enabled
  - CD – connection disabled

For implementation of a single SER system that records time-stamped activity for power system data as well as security data, the application needs to have the ability to filter and direct SER to appropriate information consumers within the entity. Figure 7 illustrates an example SER configuration interface. This interface supports creating filter groups that, among other groups, supports collection of security SER data and direction of these data to a security console. Figure 8 illustrates physical access SER, Figure 9 illustrates electronic access SER, and Figure 10 illustrates combined physical and electronic access SER for a security event.



Select Filters

Group:

- ☑ SCADA
- ☑ METERING
- ☑ ENG. ACCESS
- ☑ ASSET MGMT
- ☑ COMM
- ☑ SECURITY
- □ Override 'Display' flag
- □ Items w/o group flags
- □ Unconfigured Items

All user groups

Equipment:

062 Main
Breaker
Communication
Control Center
Control Panel
Cottage Grove
Data Center
Dist. Automatn
Doc & Tape Room
Eng. Access
Meter System
Security Consol
SEL2030
Serv Room

Any Equipment

State:

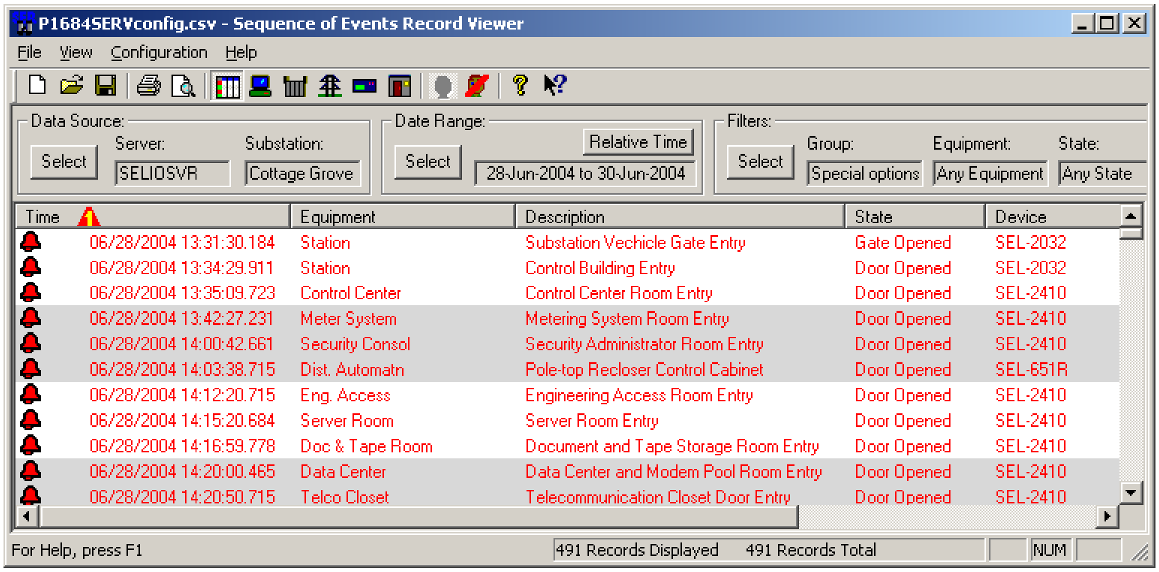
- □ All Abnormal states
- □ All Normal states
- □ All Unassigned states

Failed
Gate Closed
Gate Opened
Inactive
Local
Normal
Powered Down
Powered Up
Remote

Any State

If all selections in a category are cleared, the filter will pass any standard entry.

Figure 7 Example SER Configuration Interface



P1684SERVconfig.csv - Sequence of Events Record Viewer
File View Configuration Help

Data Source: Server: SELIOSVR Substation: Cottage Grove

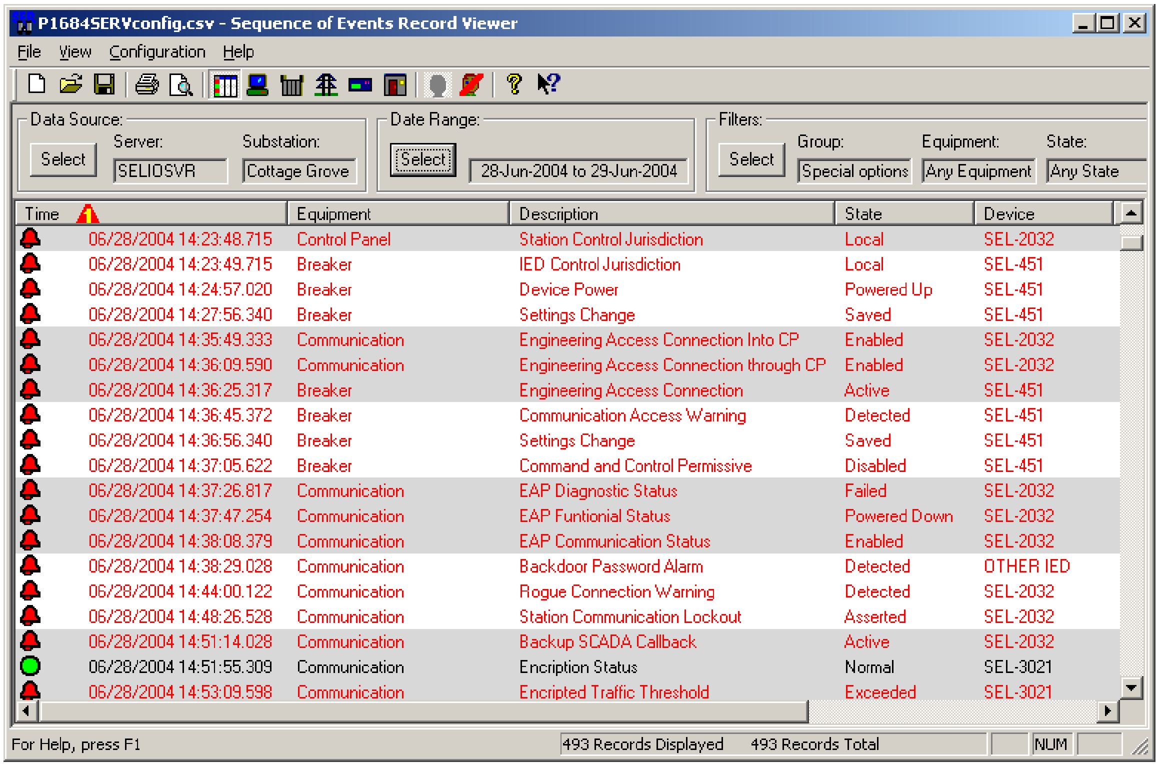
Date Range: Relative Time 28-Jun-2004 to 30-Jun-2004

Filters: Group: Special options Equipment: Any Equipment State: Any State

Time	Equipment	Description	State	Device
06/28/2004 13:31:30.184	Station	Substation Vechicle Gate Entry	Gate Opened	SEL-2032
06/28/2004 13:34:29.911	Station	Control Building Entry	Door Opened	SEL-2032
06/28/2004 13:35:09.723	Control Center	Control Center Room Entry	Door Opened	SEL-2410
06/28/2004 13:42:27.231	Meter System	Metering System Room Entry	Door Opened	SEL-2410
06/28/2004 14:00:42.661	Security Consol	Security Administrator Room Entry	Door Opened	SEL-2410
06/28/2004 14:03:38.715	Dist. Automatn	Pole-top Recloser Control Cabinet	Door Opened	SEL-651R
06/28/2004 14:12:20.715	Eng. Access	Engineering Access Room Entry	Door Opened	SEL-2410
06/28/2004 14:15:20.684	Server Room	Server Room Entry	Door Opened	SEL-2410
06/28/2004 14:16:59.778	Doc & Tape Room	Document and Tape Storage Room Entry	Door Opened	SEL-2410
06/28/2004 14:20:00.465	Data Center	Data Center and Modem Pool Room Entry	Door Opened	SEL-2410
06/28/2004 14:20:50.715	Telco Closet	Telecommunication Closet Door Entry	Door Opened	SEL-2410

For Help, press F1 491 Records Displayed 491 Records Total NUM

Figure 8 Physical Access Security SER Display Example



P1684SERVconfig.csv - Sequence of Events Record Viewer

Data Source: Server: SELIOSVR Substation: Cottage Grove

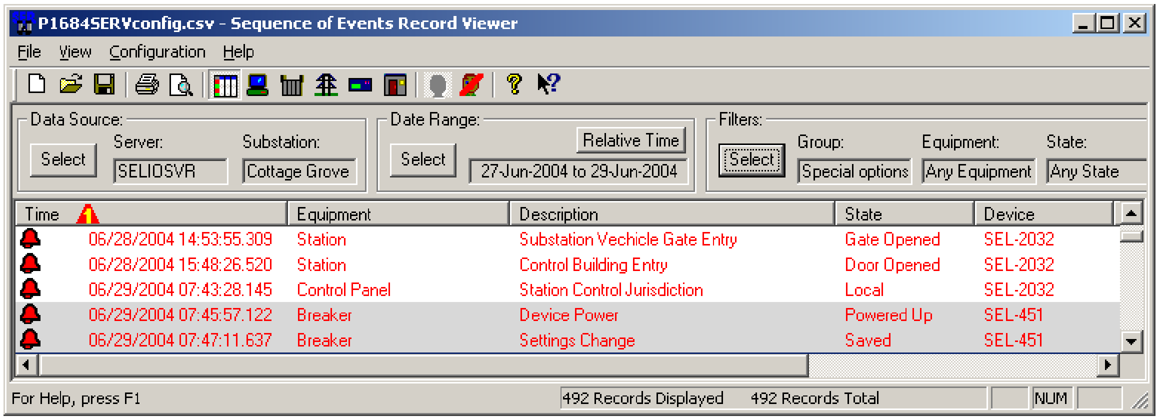
Date Range: 28-Jun-2004 to 29-Jun-2004

Filters: Group: Special options Equipment: Any Equipment State: Any State

	Time	Equipment	Description	State	Device
🔔	06/28/2004 14:23:48.715	Control Panel	Station Control Jurisdiction	Local	SEL-2032
🔔	06/28/2004 14:23:49.715	Breaker	IED Control Jurisdiction	Local	SEL-451
🔔	06/28/2004 14:24:57.020	Breaker	Device Power	Powered Up	SEL-451
🔔	06/28/2004 14:27:56.340	Breaker	Settings Change	Saved	SEL-451
🔔	06/28/2004 14:35:49.333	Communication	Engineering Access Connection Into CP	Enabled	SEL-2032
🔔	06/28/2004 14:36:09.590	Communication	Engineering Access Connection through CP	Enabled	SEL-2032
🔔	06/28/2004 14:36:25.317	Breaker	Engineering Access Connection	Active	SEL-451
🔔	06/28/2004 14:36:45.372	Breaker	Communication Access Warning	Detected	SEL-451
🔔	06/28/2004 14:36:56.340	Breaker	Settings Change	Saved	SEL-451
🔔	06/28/2004 14:37:05.622	Breaker	Command and Control Permissive	Disabled	SEL-451
🔔	06/28/2004 14:37:26.817	Communication	EAP Diagnostic Status	Failed	SEL-2032
🔔	06/28/2004 14:37:47.254	Communication	EAP Funtionial Status	Powered Down	SEL-2032
🔔	06/28/2004 14:38:08.379	Communication	EAP Communication Status	Enabled	SEL-2032
🔔	06/28/2004 14:38:29.028	Communication	Backdoor Password Alarm	Detected	OTHER IED
🔔	06/28/2004 14:44:00.122	Communication	Rogue Connection Warning	Detected	SEL-2032
🔔	06/28/2004 14:48:26.528	Communication	Station Communication Lockout	Asserted	SEL-2032
🔔	06/28/2004 14:51:14.028	Communication	Backup SCADA Callback	Active	SEL-2032
🟢	06/28/2004 14:51:55.309	Communication	Encription Status	Normal	SEL-3021
🔔	06/28/2004 14:53:09.598	Communication	Encripted Traffic Threshold	Exceeded	SEL-3021

For Help, press F1 493 Records Displayed 493 Records Total NUM

Figure 9 Electronic Access Security SER Display Example



P1684SERVconfig.csv - Sequence of Events Record Viewer

Data Source: Server: SELIOSVR Substation: Cottage Grove

Date Range: 27-Jun-2004 to 29-Jun-2004

Filters: Group: Special options Equipment: Any Equipment State: Any State

	Time	Equipment	Description	State	Device
🔔	06/28/2004 14:53:55.309	Station	Substation Vechicle Gate Entry	Gate Opened	SEL-2032
🔔	06/28/2004 15:48:26.520	Station	Control Building Entry	Door Opened	SEL-2032
🔔	06/29/2004 07:43:28.145	Control Panel	Station Control Jurisdiction	Local	SEL-2032
🔔	06/29/2004 07:45:57.122	Breaker	Device Power	Powered Up	SEL-451
🔔	06/29/2004 07:47:11.637	Breaker	Settings Change	Saved	SEL-451

For Help, press F1 492 Records Displayed 492 Records Total NUM

Figure 10 Combined Physical and Electronic Access Security SER Display Example

Examination of the combination of physical and electronic monitoring in Figure 10 reveals that someone entered a locked gate, entered the locked control house, rotated a control handle to change jurisdiction from remote to local, and turned off the power to a relay. It cannot be determined what physical changes were made to the relay or its installation, but new settings were saved into the relay when power was restored.

> *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.*
>
> *Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.*

Call to Action

18. Add encryption to communications connections into each SCADA control center, engineering access workstation, pole-top IED, and substation.
19. Add a communications processor or function to each communications connection into a substation.
20. Implement control of each substation EAP via the communications processor.
21. Disable all unused IED communications ports.
22. Implement call-back in the communications processor for backup SCADA.
23. Implement time-outs in the communications processor for pass-through communication.
24. Implement strong, multilevel passwords in all IEDs; change default passwords.
25. Place all PCs on secure LANs, and configure appropriate NIST security.
26. Use existing or newly installed I/O processors and/or communications processors to monitor electronic security indicators in SCADA control centers, engineering access workstations, pole-top installations, and substations.
27. Create an "Early Warning System."
    a. Establish a security administrator console to display the present state and history of physical and electronic security indicators.
    b. Create visual and audible annunciators, as necessary, in SCADA control centers, engineering workstation locations, and substations.
    c. Install event messengers in the substation.
28. Document each electronic perimeter including those for SCADA centers, engineering access workstations, substations, and pole-top IEDs.
29. Document existing organizational processes and technical and procedural mechanisms for control of electronic access points (EAPs) of each electronic perimeter.
30. Install and document a system, or features of another existing system, to create security data logs and diagnostics. These may be available and stored within the IEDs.
31. Install and document a security console for viewing, collection, and analysis of security data logs and diagnostics; archive these logs and diagnostics.
32. Add remote engineering access to the security console for remote and archival viewing of logs.
33. Document a process and method to review "Security Data Logs and Diagnostics."
34. Create an annual assessment process to verify and validate security of all EAPs for each electronic security perimeter.
35. Continually update and maintain cyber vulnerability assessment of each EAP.
36. Continually update and maintain all documentation associated with the electronic security perimeter as required by Standard CIP-005-01.

STANDARD CIP-006-1 PHYSICAL SECURITY

> *Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.*
>
> *Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s).*

Each entity should create, document, and maintain a description of the physical security perimeters protecting each of its critical cyber assets, all physical access points to each perimeter, and verification that all critical cyber assets are within this perimeter.

NERC describes a physical security perimeter as the physical border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which critical cyber assets are housed and for which access is controlled. By this description, physical security perimeters are, in fact, the physical boundaries encompassing the electronic security perimeters.

> *Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week.*

Each entity should identify, document, and implement physical access controls for access to critical cyber assets within each physical security perimeter. This requires that the entity control passage through physical access points into the perimeter as well as additional physical controls within the perimeter.

The physical access points into each perimeter must be controlled by the appropriate lock strategy. Remote security perimeters must be, at a minimum, controlled with physical keys that you would provide to a select few with a need to enter. Monitor entrance to high-traffic, centralized areas, such as control rooms, through such authenticated access devices as electronic locks, card readers, and badge entry.

Use multifactor (two or more) electronic authentication. Factors include something “you know” (e.g., passwords, destination IP address and/or telephone number, GPS location) or something “you have” (e.g., token, digital certificate). These will make access more difficult for unauthorized users and will identify authorized remote access users. Further, logical perimeters within a larger perimeter, such as server room and telecommunications closets within the control center, or control buildings within a substation should be locked separately through the use of physical keys or electronic authentication with a more restricted distribution.

> *Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008.*

Each entity should monitor physical access to critical cyber assets 24 hours a day, 7 days a week. Monitoring consists of detecting access and creating alerts or alarms as appropriate.

Use an I/O processor and/or communications processor within each physical security perimeter to collect, record, and report all physical security activity. Where possible, add this monitoring to existing instrumentation and control systems in substations. Add this monitoring to substations, SCADA control centers, and engineering access workstation physical perimeters via I/O processors that monitor physical access through gates, doors, windows, etc. Each record should include, at a minimum, the name of the instrumenting device, the name of the detected activity, and the time of activity with accuracy to the millisecond.

Perform physical access monitoring for access points into physical security perimeters and for specialized perimeters within physical security perimeters, which include, but are not limited to, the following:

- Substation control house
- System administrator console location
- Engineering access console locations
- Storage location of mobile engineering access laptops
- Server rooms
- Media and tape storage locations
- Data centers and modem pools locations
- Telecommunications closets
- Jurisdiction control handles
- Operational status control handles

> *Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s)*
>
> *Access Log Retention — The responsible entity shall retain physical 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.*

Creation and retention of physical access logs should be treated similarly to the creation and retention of electronic access logs.

> *Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems function properly.*

Call to Action

37. As part of the cybersecurity policy, document physical security perimeters for SCADA control centers, engineering access workstations, pole-top IEDs, and substations.
38. As part of the cybersecurity policy, document existing methods, including lock and authentication procedures, for controlling access to physical perimeters around SCADA control centers, engineering access workstations, pole-top IEDs, and substations.
39. Use existing or newly installed I/O processors and/or communications processors to monitor physical access through gates, doors, windows, etc., into substations, SCADA control centers, and engineering access workstation locations.
40. As part of the cybersecurity policy, document methods for monitoring access to physical security perimeters around SCADA control centers, engineering access workstations, pole-top IEDs, and substations.
41. As part of the cybersecurity policy, document methods for logging access to physical security perimeters around SCADA control centers, engineering access workstations, pole-top IEDs, and substations.
42. Create a maintenance and testing program to ensure that all physical security systems function properly.

Standard CIP-007-1 Systems Security Management

> *Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).*

> *Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.*

Each entity should establish and document test procedures and acceptance criteria to ensure that critical cyber assets, which are installed or modified, comply with the security requirements in this standard. Test procedures should require that testing and acceptance be conducted in an isolated test environment.

> *Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.*
>
> *Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).*
>
> *Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).*

Communications into a SCADA control center, engineering access workstation, or pole-top IED must pass through an EAP and an encryption device. Communications into a substation should pass, in order, through an EAP, encryption device and communications processor. Communications processors prohibit the introduction and redistribution of malicious software programs including, but not limited to, the following:

Viruses. Pieces of computer software that can partially or fully attach to files or applications and cause a device to perform an otherwise unintended and possibly malicious action.

Worms. Programs that self-replicate across networks. These programs affect system performance by using processing and memory.

Trojan Horses. Nonreplicating programs that masquerade as benign applications in order to capture information about a system or enable a communications port that can then be exploited. These programs can also infect a device with viruses.

Hoaxes. E-mails that claim a new virus, worm, or Trojan horse has been created. Hoaxes do not impact machines but do use network bandwidth and reduce employee efficiency.

The communications processor design should prohibit the malicious targeting of its own application programs and files that include, but are not limited to, the following:

Master Boot Record. Resides in the Master Boot Sector and contains hard drive organization

Partition Table. Resides in the Master Boot Sector and contains a pointer to a built-in operating system boot program

BIOS. Contains information on computer configuration

Command Files (*.com)

Executable Files (*.exe)

TSR (Terminate Stay Resident) Programs

Communications processor designs that prohibit the malicious targeting of their own application programs and files do so through methods that include, but are not limited to, the following:

- Use of product designs that do not have a master boot record, partition table, BIOS, etc.
- Use of product designs that support a single embedded firmware program (nonvolatile memory resident), and do not support multiple programs and program swapping.
- Use of EPROM (Erasable Program Read-Only Memory) chips to store a single embedded program. Firmware in these products can only be changed if the EPROM devices are physically replaced.
- Use of flash memory to store a single boot program and embedded firmware. Firmware in these products can only be upgraded with a specially formatted S-record, or other similarly formatted, file.
  - S-record files include a checksum per line; infected files would be detected during the download process, and an error message similar to "Invalid File" would appear.

> *Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.*

Each entity should establish and document systems management policies and procedures for configuring and securing critical cyber assets. These policies should address, at a minimum, the following:

- Use of effective password management that periodically requires changing of passwords, including default passwords for newly installed equipment
- Authorization and periodic review of computer accounts and access rights
- Disabling of unauthorized, invalidated, expired, or unused computer accounts and physical access rights
- Disabling of unused network services and ports
- Secure dial-up modem connections
- Firewall management
- Intrusion detection processes
  - Monitoring
  - Recording
  - Visual and audible alarming
  - Event messaging via telephony
  - Root cause analysis
  - Control system response and automatic communications lockdown procedures
- Security patch management
- Installation and update of anti-virus software
- Retention and review of operator logs, application logs, and intrusion detection logs; and identification of vulnerabilities and responses

> *Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.*

Standard CIP-005-1 lists additional recommendations:

> *Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.*
>
> *Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually.*
>
> *Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.*

Call to Action

43. Implement and document test procedures and acceptance criteria to ensure that critical cyber assets, installation, and/or modification complies with the security requirements.
44. Implement and document a process to protect information pertaining to critical cyber assets.
45. Implement and document management policies and procedures for configuring and securing critical cyber assets.
46. Implement and document procedures for disposal or redeployment of cyber assets within the electronic security perimeter.
47. Establish an annual cyber vulnerability assessment process.
48. Continually update and maintain cyber vulnerability assessment of each cyber asset.
49. As part of the cybersecurity policy, document methods for logging access to cyber assets.
50. As part of the cybersecurity policy, document methods for security patch management.
51. As part of the cybersecurity policy, document methods for malicious software prevention.
52. As part of the cybersecurity policy, document methods for account management.
53. As part of the cybersecurity policy, document methods for security status monitoring.
54. Review and update all documentation specified in Standard CIP-007-1 annually.

Standard CIP-008-1 Incident Reporting and Response Planning

> *Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.*
>
> *Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan.*
>
> *Cyber Security Incident Documentation — The Responsible Entity shall keep relevant*
>
> *documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.*

Each entity should define and document electronic incident response actions, including roles and responsibilities assigned by individual or job function.

Though no longer required in Standard CIP-008, it was formerly required in NERC *Cyber Security Standard 1300* that each entity should define and document physical incident response actions, including roles and responsibilities assigned by individual or job function.

Each entity should require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure.

Call to Action

55. Implement and document an electronic incident response action plan.
56. Implement and document a physical incident response action plan.

STANDARD CIP-009-1 RECOVERY PLANS FOR CRITICAL CYBER ASSETS

> *Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.*
>
> *Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets.*

Each entity should create and document action plans and procedures to recover or re-establish critical cyber assets following a cybersecurity incident. Each responsible entity shall exercise these plans via drill at least annually. The plans and procedures shall define actions as well as roles and responsibilities by individual or job function.

Call to Action

57. Implement and document an incident recovery action plan.

SUMMARY

A prudent design based on the recommendations in this paper will secure cyber assets and meet the intent of NERC *Standards CIP-002 through CIP-009 — Cyber Security*.

Through use of the information in this paper, each entity can begin the process to satisfy internal responsibilities to proactively improve security. These steps include the following:

- Understand communications installations and assess security vulnerabilities.
- Create and maintain a cybersecurity policy to reduce security vulnerabilities.
- Stop all unnecessary communications and block all unnecessary connections.
- Encrypt all remote communications.
- Pass all remote communications through a communications processor that filters all communications, prevents the introduction of malicious software, prevents the use of “backdoor passwords,” and controls the use of EAPs automatically and in response to commanded control. Use this communications processor to detect, alarm, stop, and lock out illegitimate communication.
- Choose IEDs that provide communications access warnings for every communications port.
- Create security administrator console with visibility and control of security features.
- Create an early warning system using integrated new and in-service I/O processors and IEDs for substations, control centers, and engineering access workstations.
- Create an engineering access method to collect and view diagnostics and data logs.
- Appropriately authenticate all access via passwords, etc.
- Place all PCs on secure LANs and configure appropriate NIST security.

REFERENCES

[1] George W. Bush, *National Strategy for Homeland Security*, Office of Homeland Security, July 16, 2002.

[2] NERC *Reliability Functional Model*, February 10, 2004.

[3] NERC *Urgent Action Standard 1200 – Cyber Security*, August 13, 2003.

[4] NERC *Implementation Plan – Renewal of Urgent Action Cyber Security Standard*, June 2, 2004.

[5] NERC *Cyber Security Standard 1300*, anticipated August 2005.

[6] NERC *Security Guidelines for the Electricity Sector, Version 1.0*, June 14, 2002.

[7] NIST Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist (Draft)*, June 2004.

[8] NERC *Standards CIP-002 through CIP-009* — Cyber Security *(Draft 3)*, January 16, 2006.

BIOGRAPHY

Timothy P. Tibbals received his BSEE from the Gonzaga University in Spokane Washington in 1989. After graduation, he joined Schweitzer Engineering Laboratories, Inc. as an Applications Engineer performing system studies and relay testing. He has also worked as a Development Engineer and has been part of the development team for many of the communication features and functions of SEL products. He subsequently worked as an Application Engineer for protection, integration and automation products assisting customers through product training, seminars and phone support. He served as the Supervisor for Automation Services in SEL's Systems and Services Division for several years before returning to the R&D division where he presently serves as the Lead Product Engineer for the Automation and Communications Engineering products. He is a member of the IEEE and has authored numerous application guides and papers related to automation and communications.

David J. Dolezilek received his BSEE from Montana State University in 1987 and is now the Technology Director of Schweitzer Engineering Laboratories. He is an electrical engineer with management and development experience in electric power protection, integration and automation, communications, control systems, and SCADA and EMS design and implementation. He is the author of numerous technical papers and continues to research and write about innovative design and implementation affecting our industry. Dolezilek has earned a patent and participates in numerous working groups and technical committees. He is a member of the IEEE, the IEEE Reliability Society, Cigre WG 35.16, and the International Electrotechnical Commission (IEC) Technical Committee 57 tasked with global standardization of communications networks and systems in substations.

20060128
TP6202-01