Methods for Securing Substation Relay Communications

David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
59th Annual Georgia Tech Protective Relaying Conference
Atlanta, Georgia
April 27–29, 2005

Originally presented at the
31st Annual Western Protective Relay Conference, October 2004

METHODS FOR SECURING SUBSTATION RELAY COMMUNICATIONS

David Dolezilek
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

ABSTRACT

Discussion of practical and useful security designs include:

- Often unused security features in substation devices from all vendors
- Detection, alarming, blocking of and automatic reaction to unauthorized access
- Control, monitoring and logging of communication status, permissives and active connections
- Robust lockout of unwanted connections including third party “back door” access and passwords
- Efficient serial encryption

At the heart of both the value and the vulnerability of power substation communication is the ability to remotely access control and protection equipment. These communication methods are becoming increasingly important to the engineering and operations staff of utilities, yet they leave systems vulnerable to electronic intrusion. Electronic intruders randomly or maliciously operating circuit breakers, reclosers, and switchgear, would have disastrous consequences on the safety and reliability of our electric power systems.

Needs to communicate with protection and control devices include:

- Engineering access, remote configuration management, settings verification
- Local and remote collection of historical and diagnostic information
- Testing

In light of communication vulnerabilities, the need for effective procedures and techniques to reduce the chances of electronic intrusion is increasingly evident. This paper is a tutorial on how to deploy several very effective communication security methods within new and existing substations. These methods, often already available but unused in substation devices, provide secure connections using traditional in-service modems, secure use of new, less secure WAN communication technologies, and secure access, via connection permissives, regardless of the type of communication methods used.

This paper discusses practical examples for several proven methods.

- Encryption
- Secure password methods
- IED and communications processor security settings
- Monitoring security parameters

INTRODUCTION

The multiple security features that are already available in substation communication devices are combined into many different security schemes with different characteristics and strengths. Some simple features virtually eliminate hacking, while others reduce the visibility of substation points of contact. This paper discusses the concepts of available features and applications but intentionally does not specify enough detail to permit circumvention. Using settings, passwords, and permissives, robust LAN security measures manage security elements of substation communication systems including:

- Control of devices that provide remote access
- Control of communication connections between remote communication devices and substation communication devices
- Control of communication connections between substation communication devices and IEDs
- Control of communication messages between remote communication devices and substation communication devices
- Control of communication messages between substation communication devices and IEDs
- Control of permission for commands and access
- Detection of access
- Monitoring of active communications
- Lock out of invalid communications
- Prevention of abuse during a system breach using system reconfiguration

COMMUNICATIONS INFRASTRUCTURE

Making communication connections between integrated IEDs creates a trusted, physically distinct local area network (LAN). LANs are created from copper, fiber, and/or wireless media connected in a star or multidrop fashion. LANs are created from EIA-232, EIA-485, Ethernet, and/or various other connections supporting one or many protocols. Hybrid LANs are made from collections of all of these components such that the IEDs interact with one another as if they were all directly connected locally to one another. One or two integrated devices on a pole top comprise a small LAN. Large LANs are created by directly connecting, or bridging, one or more physically separate LANs together using trusted connections. They may cover a wide area, but they are still simply large LANs. A wide area network (WAN) is a variable, unpredictable, and untrusted communication infrastructure that, because of these characteristics, is often drawn as a cloud. WANs move messages from one LAN to one or more other LANs. Although some WANS are more predictable than others, WANS are considered untrusted because of the unknown characteristics, components, and communication paths. Therefore, WANS must be secured. The point at which a LAN is connected to a WAN is called an access point.

The purpose of the LAN is threefold and can be summarized as follows.

- Move sensor measurements and information created from these data among IEDs
- Move information between IEDs and the LAN communications processor
- Move information between IEDs and the LAN communications processor to users across the WAN

Information moves within the LAN and across the WAN via two methods commonly referred to as SCADA (supervisory control and data acquisition) and engineering access. SCADA conversations support many types of systems such as SCADA, EMS (energy management system), distribution automation, and so forth, and involve constant messaging between a control center and the LAN to acquire present values for predefined data and to perform control. Engineering access conversations are on-demand data acquisition and LAN administration connections between a user or automated process and a LAN device, to support virtual terminal type connections and file transfer.

The design of the IEDs and communication products traditionally used to build substation LANs protects them from receiving viruses. Devices built with closed embedded operating systems, such as protective relays, other IEDs and some communications processors, remain virus free because they do not accept, store, or execute third party programs. They only accept specific firmware, only run this firmware after it passes verification, and can only be manipulated by settings. HMIs and communication products based on a PC architecture are susceptible to viruses and must be protected accordingly.

A communications processor is a device, or a function within a device, that, in addition to other tasks, manages communications on a LAN. Some vendors provide devices actually called Communications Processors, while others provide some of the same functionality in other devices such as RTUs, PLCs, or PC-based software applications. RTUs, PLCs, or PC-based solutions often connect to the SCADA access point and require a second device, such as a port switch, to connect to the engineering access WAN access point. They all have various features sets and support some or all of the methods discussed in this paper. For the remainder of this paper, communications processor will refer to a single device, or collection of devices, providing multiple SCADA and engineering access connections to the WAN.

WAN access point devices need to work well in concert with the communications processor; however, it is generally accepted that they should not be built into the communications processor. The communications processor performs many other functions as part of the LAN, including monitoring, automation, and substation SCADA. When physically separate, maintenance, upgrade, and replacement of the WAN access point device will not affect the LAN. Communication devices such as the following control WAN access points:

- Telephone modems connected to leased line or dial-up telephone access
- Wireless modems and radios
- Channel (CSU) and data service unit (DSU)
- VPN
- Firewall
- Router

Communications Processor

Integrated LANs are comprised of IEDs connected to each other and to one or more communications processors in various configurations. The communications processor acts as the central point of contact and collects and concentrates data for use by remote applications, such as SCADA and EMS, and local applications, such as a human machine interface (HMI). The communications processor also receives and disperses control commands from these remote applications. The communications processor is a single point of contact for remote engineers and system administrators to contact the IEDs via engineering access communications for the purposes of retrieving data, performing control, and performing diagnosis and analysis.

Access Data Through Multiple Paths

It is necessary to use a communications processor that supports multiple access points to the same information. In this way, once sound security practices are in place, only one communication system needs to be installed, maintained, and upgraded. This reduces expense and the complexity of maintaining and upgrading many duplicate systems. Unique security methods and features can be assigned within the communications processor to each type of user. Minimizing the number of LAN devices needed to support the access points to the substation reduces the chances that access points will not be upgraded or maintained. Further, using a single multifunctional device reduces the amount of training and spare parts expense.

The communications processor permits multiple simultaneous engineering access connections to multiple IEDs, simultaneous with multiple SCADA, EMS and HMI connections, etc. Although multiple paths exist for data access in the communications processor, only one engineering access connection to each IED is active at a time. The communications processor locks out all access to the IED port except the initial engineering access connection, to prevent spoofing or hostile takeover of an established connection. The connection returns to the lowest access level, "connect only," after a predetermined period of time of inactivity or immediately after a termination command is issued. Thus the connection is inaccessible without passwords, even if the WAN access point remains active. The communications processor only permits one settings change session at a time. This prevents an inappropriate and undetected settings change from being performed simultaneously with a valid settings session.

Overviews of typical LAN and WAN access communication infrastructures are shown in Figure 1 and Figure 2.

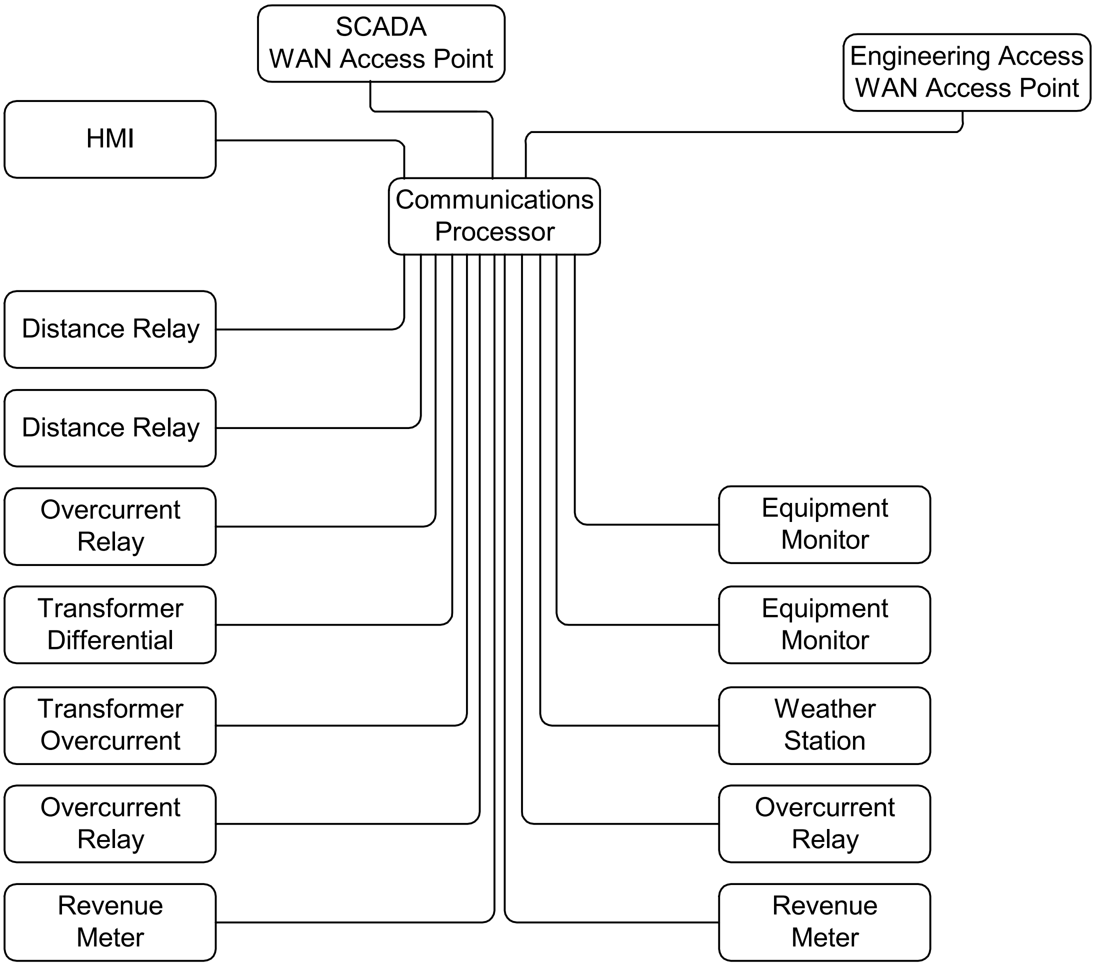


Figure 1 Typical Singe-Tier Substation LAN Diagram

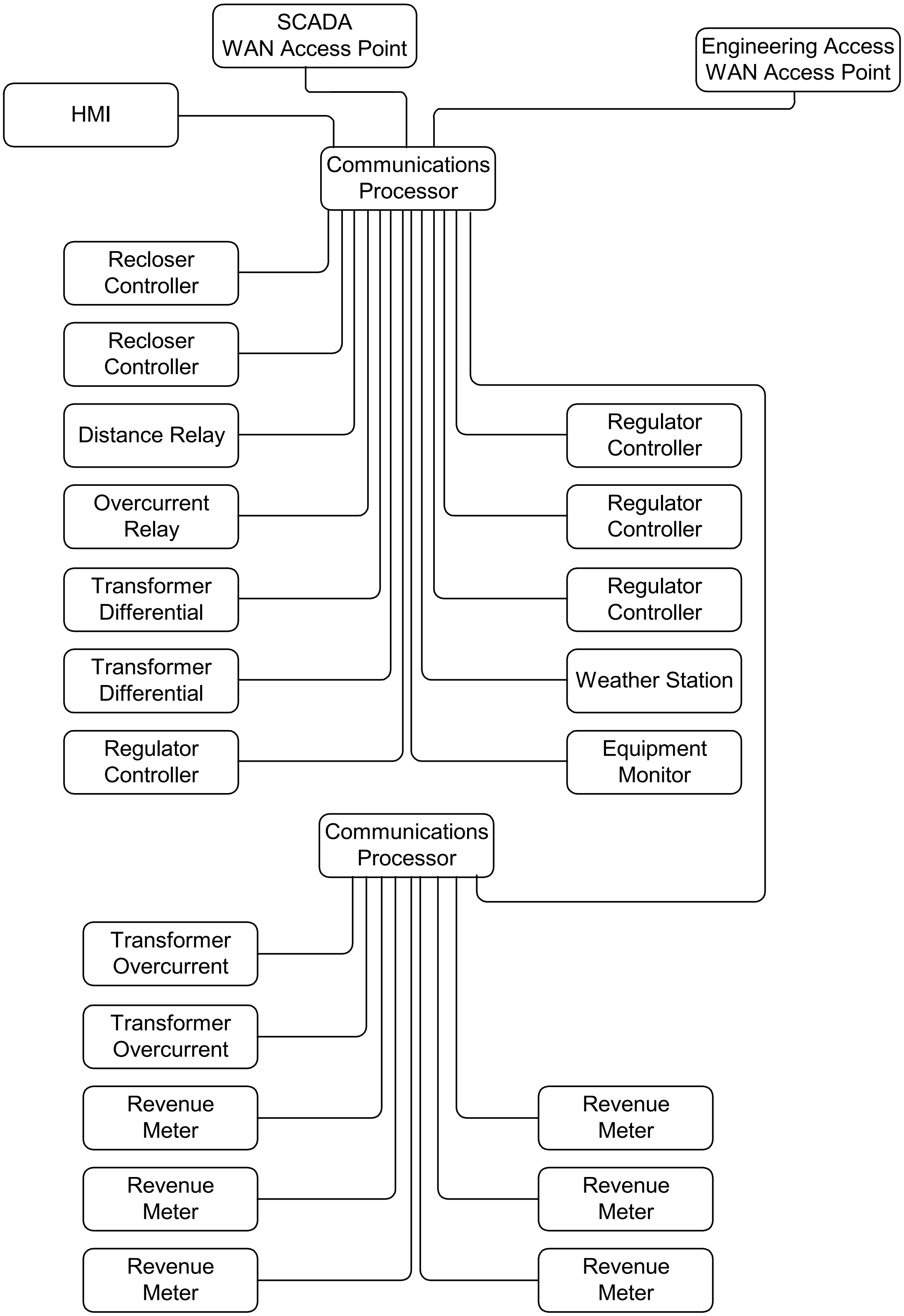


Figure 2 Typical Two-Tier Substation LAN Diagram

LAN Communication Management—Monitor, Control, and Report

LAN communication management includes both information security and connection management. Connection management controls who is allowed to connect, and when and under what conditions. Information security protects the data created within the LAN and mediates which data and commands are injected into the LAN. LAN communication management is accomplished via passwords and permissives.

LAN communication management prevents accidental connection by authorized users, connections by unauthorized persons or processes, and connections by persons who have knowledge of authorization techniques but do not have permission for access. The latter two scenarios are commonly referred to as hacking.

LAN Information Security

Information security refers to methods employed to ensure Confidentiality, Integrity, and Authentication (CIA) of information at rest and in transit. By virtue of their data processing, LANs provide integrity and authentication of LAN data passing through local connections and WAN access points, as well as messages received through WAN access points. By managing connections, WAN access points provide confidentiality of information in transit through untrusted WANs. They also provide integrity and authentication of communication channels passing messages between WAN access points. However, they cannot verify integrity and authentication of the message contents; this must be done on the LAN.

Individual WAN and LAN security practices need to remain confidential by nature, however an outline of elements of a successful security plan is included in the summary for reference.

Dynamic LAN Connection Management

LAN connection management monitors the status of connections and requested connections, enables appropriate connections to occur, and reports the status of all connections. The status of LAN port connection parameters and actual connections is sent to control center applications and the engineering access administrator. The existence of appropriate connections and the termination of inappropriate connections are controlled through connection management in the communications processor. LAN connection management controls access to connections that have successfully passed through WAN access points as well as local connections.

WAN access point devices are disabled until they are needed for legitimate access, thus reducing their visibility to persons or processes searching to find and compromise access points.

“The front panels of IEDs offer various types of HMI functionality and provide methods of interacting directly with an individual device on the LAN. The operator control and auxiliary SCADA pushbuttons on the IEDs are disabled by default. The remote system administrator or local operator must enable the IED front panels before they can be used. Automated processes also enable the front panels for control when the primary control interface is out of service.”

Pre-Emptive LAN Connection Management

Probably the most important and most often overlooked element of LAN connection management is the prohibiting of physical access. In addition to securing the physical building that houses the LAN, an IED on the LAN is configured to monitor and alarm when a door or window is opened. Communication ports on the front panel of IEDs are convenient as maintenance ports and are highly visible. However, they also represent a LAN or IED access point. Control panel or equipment rack doors, which in the past were considered an optional expense, are installed with locks to prevent access. Communication ports on the rear of the IEDs represent the additional threat that because they are not immediately visible, it is easier for an unauthorized wireless WAN access point, such as a radio, to be connected covertly. Control panel or equipment rack doors and end panels eliminate access to these rear communication ports.

Unneeded communication ports on the communications processor are configured to be unused so that they do not support any connection. Unused communication ports on the rear of the IED are configured to support a protocol that does not allow remote SCADA or engineering access such as a deterministic high-speed peer-to-peer protocol. The communications processor has factory default settings with all of the ports set to unused for security.

Encryption Adds Confidentiality to Data Acquisition and Control

Encryption protects data links against the unwanted results of intrusion. It does not prevent the intrusion, but rather, renders the intrusion less useful. The use of encryption makes data and control traffic confidential and authenticates the class of user as one familiar with the chosen encryption techniques. Dedicated encryption devices ensure authorization because each will only work in concert with others that have matching encryption keys. To be effective in substation communications, these devices must support multidrop and point-to-point links and protocols. Further, they should be configured and monitored through encrypted links as well. Encryption protects passwords and other data that would otherwise be easily intercepted.

Ferc and Nerc have created network perimeter requirements that can be satisfied by the correct encryption devices and NIST has approved the Federal Information Processing Standard (FIPS 197) that recommend the appropriate encryption to be used. The most important consideration for relay and substation communications is to choose a product with very low latency for the time-sensitive communication requirements. In other words, choose a product that does not cause inappropriate delay in communications as it processes, encrypts or decrypts, and then passes on the data.

There are a few commercial off-the-shelf (COTS) products available that provide strong cryptographic functions, including encryption and authentication. The easiest to install, and least intrusive to the present physical connections, provide the ability to protect traffic with a “bump-in-the-wire” solution. Such devices can simply be placed on either end of an existing communications link. They then secure the data on the link while, ideally, appearing transparent to the existing system.

Strong Passwords Provide Authorization of Data Acquisition and Control

Strong password protection is your best defense against all forms of unauthorized access. A good password not only protects a specific device against accidental and unauthorized settings, but also safeguards the integrated system and helps ensure the reliable operation of a substation or SCADA system. However, if your password is disabled, easily guessed, or cracked, or if the substation devices have secret vendor “back door” passwords, intruders can easily disable your system. Vendor “back door” passwords are secret access codes installed by some other vendors to simplify access or bypass traditional password access. Intruders can also use your system to distribute false data and sabotage other interconnected systems within your company and worldwide across the Internet. Strong passwords are virtually impossible to guess and may take thousands of hours to crack. Ill-chosen passwords may be guessed or cracked in just a few minutes. Hence, it is extremely important to maintain the security of your system by using strong passwords in communications processors, IEDs, and WAN access points devices.

A multilevel password system provides security against unauthorized access. This system allows you to give personnel access only to those functions they require. Though many different levels of access are used to differentiate users and processes, the most essential levels are as follows.

- "Connect only"—lowest access level, provides only IED identification.
- "Read only"—one level higher than "connect only," provides viewing of IED parameters and information.
- "More than read only"—any level higher than "read only." This category of access levels provides various combinations of control abilities, extended data acquisition, data clearing and/or entry, and configuration manipulation.

Many devices are shipped with default passwords. Change default passwords to private passwords at installation. Failure to change each default password to a private password may allow unauthorized access.

Used properly, passwords provide good protection against unauthorized access. Make sure you choose strong passwords and record them in a secure location. A guideline for creating strong passwords is included in the summary for reference.

Communications Processor Requires Strong Passwords Compliant With Federal Standards

The communications processor manages SCADA access to LAN data and control and passes through remote engineering access to the IEDs. Because the communications processor mediates all remote connections to the LAN, its password scheme is designed to meet or exceed all of the requirements of the DOE, Department of Energy, Password Guide (DOE G 205.3-1).

Permissives Prevent Unwanted Control, Data Access and Re-Configuration

Permissives are logical representations of one operator or process giving permission to another operator or process. Operators or processes use jurisdictional and operational permissives to manage authority over control or information access of the entire LAN or individual IEDs. Permissives apply to an individual action for a set period of time, or remain enabled until reset. They provide security of communications as well as protection of personnel. Some permissives, also known as tags, prevent remote and unwanted control while work is being performed in the substation. Other permissives prevent operation of apparatus under maintenance and unintended operations of in-service apparatus during communications or SCADA testing and commissioning. Still other permissives prevent users from creating an engineering access connection without first gaining approval from a SCADA operator or communications system administrator.

Some examples of frequently used permissives include:

- Enable remote versus local control of substation
- Enable remote versus local control of individual apparatus
- Enable engineering access to communications processor
- Enable engineering access through communications processor to connected IED
- Dynamically enable each remote control command to verify authenticity

The communications processor grants permission based on time of day, day of the week, or a specific event, such as a physical or logical change of state. The physical change of state is detected from a control handle or switch used to enable engineering access, remote control, or other permissive. The logical change of state is created as a database element that represents the state of the physical contact or is modified in response to a process calculation in the communications processor or receipt of a command from a remote location. Commands from remote locations are received via SCADA protocols or ASCII engineering access messages. Both are implemented as straightforward commands and/or encrypted commands or sequences. In each case a time out period is associated with the access enable.

The communications processor and the IEDs implement permissions, which function separately from the security features in WAN access point devices. They perform an additional robust level of information security and connection management that is not affected if the WAN access point devices fail or are compromised.

Create Access Warnings and Monitor Those Created In IEDs

Substation IEDs create access warnings based on several conditions. These warnings are communicated to other devices and users via digital communications protocols and/or physical contact outputs. IED access warnings pulse, rather than latch, the output contact so that they are differentiated from IED failure alarms. Access warnings are also created as logical elements in the IEDs that are monitoring the contact outputs so that they are manifest as physical and logical indications. Access warnings indicate that a user or process has accessed an IED via a communication connection at a level beyond "read only," capable of performing control or modification, or has failed trying for access. Any of the following conditions can cause an IED access warning.

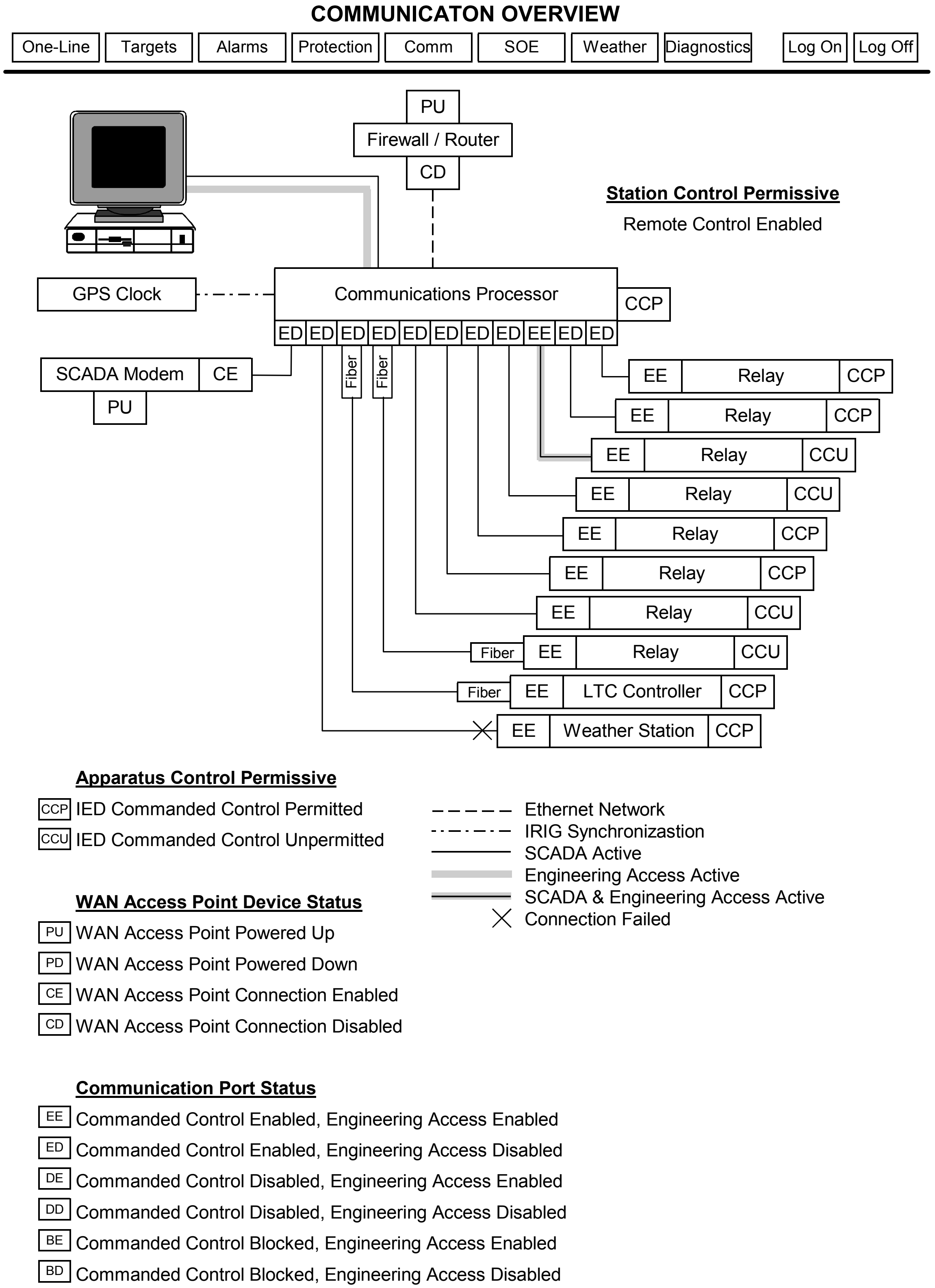
- Successful entry of password with sufficient authority to move beyond read only functionality via any communication port.
- Successful save of modified settings via any communication port or front panel. This also requires first reaching the appropriate password level.
- Unsuccessful password entry monitored as three consecutive incorrect password attempts via any communication port.

Therefore, the communications processor detects any connection to the substation IED, regardless of the communication port used. This will detect connection by a user or process communicating through the remote engineering access point, as well as local access directly connected to the IED or via an unauthorized and unknown wireless communication path covertly added to avoid detection. The communications processor also creates its own access warnings in response to any of the above conditions within the communications processor as well as:

- Successful change of a password via any communication port.

Report Status and Warnings About LAN Communications

As mentioned previously, IED access beyond "read only" is immediately and automatically detected in IEDs that support access warning. Also, the communications processor detects engineering access connections at each communication port connected to an IED. Therefore, in the unlikely event that an unauthorized connection passes through access point security AND passes through the password access of the communications processor, it will be detected. Notification of this access warning is sent to SCADA, EMS, and the engineering access administrator. Using these applications, operators view the status of communication permissives and actual access via communication overview screens such as the one pictured in Figure 3.



Apparatus Control Permissive

CCP IED Commanded Control Permitted
CCU IED Commanded Control Unpermitted

– – – – – Ethernet Network
- · — · — · IRIG Synchronizastion
——— SCADA Active
▬ Engineering Access Active
═ SCADA & Engineering Access Active
✕ Connection Failed

WAN Access Point Device Status

PU WAN Access Point Powered Up
PD WAN Access Point Powered Down
CE WAN Access Point Connection Enabled
CD WAN Access Point Connection Disabled

Communication Port Status

EE Commanded Control Enabled, Engineering Access Enabled
ED Commanded Control Enabled, Engineering Access Disabled
DE Commanded Control Disabled, Engineering Access Enabled
DD Commanded Control Disabled, Engineering Access Disabled
BE Commanded Control Blocked, Engineering Access Enabled
BD Commanded Control Blocked, Engineering Access Disabled

Figure 3 Communications One-Line Screen

Log, Alarm, Terminate and Lockout Illegitimate Communications

Operations and management information from substation IEDs, including access warning information, is collected from the IEDs via digital communications, as well as physical contact status, by the communications processor. The communications processor also creates its own access warning information. The communications processor sends predetermined messages or initiates control actions when illegitimate access is detected. Messages are sent directly to appointed personnel as text pager or telephone messages, voice annunciator telephone messages, or email. Audible alarms, flashing lights, and dedicated alarm dialers are also initiated as necessary.

The communications processor logs messages to a local printer. In addition to security monitoring messages, the communications processor is configured to log selected operational information including control actions, diagnostic status messages, short event reports, and demand meter data.

The communications processor also logs messages internally for diagnostic purposes. As it does so, it removes all passwords that it receives, so that they are not visible.

Most importantly, the communications processor immediately terminates and locks out each invalid access point connection until it is diagnosed and reinstated by the administrator.

Verify LAN Configuration Frequently And After Known Communication Access

The communications processor supports a simple command to verify the IEDs on the LAN and their status. Using the same command, system administrators verify that no new IEDs or WAN access points have been added and that ports intended to be disabled remain set to unused. We strongly recommend using this procedure after each visit and settings change made by employees and contractors.

Monitor Security Logs Created By SER

Sequential Event Recording (SER) applications monitor input contacts and elements of logical and arithmetic equations to timestamp their Change of State (COS). Communications processors then create and queue an SER message for each occurrence detected, as well as for each SER message received from IEDs in the substation. The processors store these messages and forward them to appropriate hosts for alarming and monitoring.

The SER is configured to monitor status, health, and performance of the power system as well as monitor communications access and security including the following records.

- IED or communications processor powered up
- New settings saved into IED or communications processor
- IED or communications processor access warning
- IED or communications processor jurisdictional permissive
- IED or communications processor operational permissive
- Communications processor has activated/deactivated WAN access point device
- Communications processor has enabled/disabled communications with WAN access point device
- Communications processor detected failure or warning of WAN access point device

- Communications processor has locked/unlocked IED communication port
- Communications processor detects that dynamic or static trigger is set/reset

Mitigating Access Threats to the LAN Control System

LAN communications provide the messaging between integrated IEDs acting as a control system. The messages come from operators or other IEDs and on the LAN or through the WAN access points. Messages through the WAN access points are in the form of a SCADA protocol or engineering access connection. Some WAN access points are available only on demand, such as dial-up telephone, while others, such as leased-line telephone, intranet, and internet access are constantly available.

Hackers must first learn the contact information such as the telephone number or internet protocol (IP) address of the access point device. This information can be found in utility documentation or learned from an employee. Another method is to randomly attempt various telephone numbers and IP addresses until access to a system is found and recorded. This method may or may not reveal the system identity.

SCADA Access Threats—Predictable Methods

SCADA connections are often open constantly. If the application permits, users can limit the visibility of these connections by allowing connections only during infrequent report by exception and commanded control actions. For access via a SCADA protocol, the hacker must learn the characteristics of the protocol and how to spoof or interact with it. SCADA protocol training, documentation, and test tools are widely available to help users implement and diagnose SCADA installations. These same products can be used by hackers to learn system characteristics. Some SCADA protocols consistently use the same message or sequence to perform control. In this case, the hacker can simply record a command sequence for a specific control action and inject it into the LAN at a later time. Without understanding the protocol, the hacker can still fool the LAN into believing that the command is legitimate without ever deciphering it. However, for this to be harmful the hacker will need to observe and record the specific sequence to perform a malicious control.

SCADA connections are threatened by protocol standardization, consistency, and availability of training and tools that make the hacker's job easier. Development of standardization and availability of training and tools are also useful to legitimate implementation of SCADA connections. A following section describes how the communications processor is used to thwart illegitimate control via SCADA connections.

All output contacts unused in the control strategy design, both on the communications processor and IEDs, are left at the factory default setting "disabled" so that they cannot be used. In this fashion, extra or spare outputs cannot be manipulated to perform unwanted control.

Engineering Access Threats—Full Time Access

If the WAN access point is being used for engineering access, it is essentially a connection that is capable of supporting data acquisition, control, LAN administration, IED maintenance, and collection and manipulation of settings. Operators as well as engineers, technicians, and system administrators use these connections as backup SCADA links. Engineering access connections differ from SCADA in that they are used less frequently and that the user must understand and use IED specific protocols and message sequence and syntax.

However, when WAN access points are constantly active regardless of whether they are in use, as is common practice, they are visible for discovery by hackers. Therefore, the LAN disables access points until legitimate use is needed. This reduces the window of opportunity for illegitimate detection of contact information AND illegitimate use. Permission for legitimate use is gained via a unique contact method or granted by a system operator or administrator via a control command. A following section describes how the communications processor is used to thwart illegitimate use of engineering access connections.

Security Strength via Combined WAN Access Point and LAN Management

LAN Management Of WAN Access Points—Monitor, Control, and Lockout

Regardless of the WAN access point communication device chosen or the strength of its security measures, security features of the communications processor reduce visibility and susceptibility to attack. The communications processor is configured to disable connection to, or operation of, the WAN access point unless permitted by a user or process. The communications processor grants permission based on time of day, day of the week, or a specific event, such as a physical or logical change of state. The physical change of state is determined by monitoring inputs such as control handles or switches used to enable engineering access. The logical change of state is detected in response to a process calculation in the communications processor or receipt of a command from a remote location. Remote source permission is granted in response to a command from SCADA, EMS, engineering access administrator, or other designated source. These commands are accepted through SCADA protocols or engineering access connections. In each case a time-out period is associated with the access enable.

The communications processor uses local contact inputs to monitor the state and health of IEDs as well as the WAN access point devices. The communications processor uses output contacts to physically manipulate, and command messaging to digitally manipulate, WAN access point devices, as well as IEDs and power system apparatus, based on calculations, remote commands, or time comparisons. Using this powerful capability the communications processor performs adaptive control schemes, automatic responses to alarms, and direct control of WAN access point devices.

The communications processor manages the WAN access point devices so that they are available only when needed for legitimate use, reducing their visibility to persons or processes attempting to hack the system.

- Contact outputs are used to provide or disrupt power to WAN access point devices.
- Contact outputs are used to complete or disrupt communications channels between the substation communications processor and WAN access point devices.
- Modems are disabled via command messages from the communications processor and remain unusable as WAN access points until enabled by other command messages from the communications processor.

Using the LAN communications processor in such a fashion will disable attacks via secret vendor “back door” access methods. By preventing any unwanted connections, the communications processor prevents communications with the IED and thus prevents the use of these secret methods. Care must be taken when manually or automatically allowing connection access because once granted, the remote user can send legitimate and/or “back door” passwords.

LAN Management Of Engineering Access And SCADA—Configuration And Control

In addition to manipulating the WAN access point devices, the communications processor detects and manages connections made to each communication port. As commands to grant permission are received, the connection status of the ports is changed so that remote administrators see the change in permission and the status of connection activity. The communications processor gives remote administrators the ability to grant engineering access to each communication connection in the LAN independently for security and safety. This prevents unauthorized connections but also prevents unintended operation by validating that the user is connected to the appropriate IED.

Although settings cannot be changed in the communications processor until the user has gained access more secure than “read only,” the settings are also prevented from being visible at the “read only” level. Automatic help messages in the communications processor are disabled so that this function is only available to knowledgeable users who request it specifically.

LAN Control System Management—Configuration And Control

The LAN SCADA system performs an additional level of authorization of commands that have passed through WAN access point CIA measures. Care is taken to create appropriate settings in each communications processor (several connected together for large LANs) and the IEDs to limit or eliminate commanded control via SCADA protocols and/or engineering access.

Settings Prevent Unwanted SCADA Connections Within The LAN

Ports in the communications processor have factory default settings preventing them from being WAN access point ports and should remain at these settings until needed. Also, within the communications processor and IEDs, settings are used to permanently enable or disable response to control commands received via SCADA or engineering access. Default factory settings prohibit control and should be maintained for read-only IEDs and communications processor ports. Therefore, even if the connection is enabled and active, appropriate settings will disable control commands. The control command disable feature is settable at the communications processor WAN access point port, at the communications processor IED port, and at the IED. Once control settings are enabled, other security measures apply.

The communications processor is configured to obscure information about the availability, quantity, and address of SCADA control points over primary and backup SCADA links. The factory default setting conceals the status of control points and should remain this way unless the SCADA master needs this information. If control point status is made visible, eavesdrop monitoring of the SCADA channel communications or a direct SCADA poll command will reveal the existence and quantity of control commands available via the SCADA protocol.

Backup SCADA links are configured to perform “dial back” regardless of the connection media. Using this feature, a backup SCADA link accepts a request for connection via the WAN access point and then disconnects. The communications processor then initiates contact to the WAN using predefined backup SCADA link contact information. This guarantees that contact is made only with a legitimate destination across the untrusted WAN.

Dynamic Processing and Triggers Prevent Unwanted SCADA Commands Within the LAN

Select-before-operate (SBO) in SCADA protocols was developed to prohibit poor communication media from creating an incorrect but actionable SCADA command. SBO no longer works to actually select the appropriate control in the IED. Instead, SBO requires that two corresponding messages be received in a defined period of time before the control command is considered valid, essentially acting as a trigger. The first message triggers the control; the second message actuates the control. The time-out period between receipt of messages makes it more difficult, but not impossible, to inject a rogue command sequence.

The communications processor implements additional SCADA trigger strategies using conventional SCADA protocol commands. Use of a dynamic trigger calculation prevents the command sequence from being consistent and prevents observed control command sequences from being reusable. A trigger calculation method at the remote control center determines which message or sequence of messages is sent as a trigger, followed by the command. Corresponding calculation in the communications processor verifies validity of the trigger and authorizes the associated command for execution. Dynamic SCADA trigger calculations work within the parameters of the SCADA protocol to provide messaging inconsistency and authorization of a received message. These triggers work identically for any SCADA protocol, WAN design, or LAN design.

The communications processor implements engineering access trigger strategies in the same dynamic fashion as the SCADA triggers or as static triggers. Engineering access connections are less frequent and therefore less prone to observation. They are also often freeform and less predictable than SCADA conversations. Although passwords and command sequences could be recorded and played back, it is not likely that the appropriate sequence would be observed. Therefore, it is often adequate to design a static engineering access trigger. Triggers are developed with the same abilities and security as strong passwords. The communications processor makes the engineering access port connected to the WAN access point device unusable until the trigger is received.

The communications processor also has the ability to dynamically block all control to an IED should an alarm or warning warrant it. Using this feature, even if all settings, permissives, and triggers are in place, the communications processor can dynamically lock out a communication port from sending a control message.

Dynamic processing of permissives and triggers in the communications processor disables intrusion from remote sites and local access. Dynamic processing of permissives and triggers in the IED disables intrusion from remote sites, local access via the communications processor, and direct connection to an IED communication port.

Robust LAN Security Management Stronger Than WAN Security

As explained previously, all of the following situations must coexist for a legitimate or rogue SCADA or engineering access command to pass through the communications processor and operate an IED. The entire feature set can be used, or any combination.

- Command passes through WAN CIA security
- Communications processor has activated WAN access point device
- Communications processor has enabled communications with WAN access point device
- Communications processor has not detected failure or warning of WAN access point device

- Communications processor has not detected access warning or received one from the intended IED
- Communications processor detects that station control jurisdictional permission is granted
- Communications processor verifies that command message meets protocol criteria
- Communications processor is configured to accept control messages
- Communications processor is configured to send control messages to IED
- Communications processor has not blocked commanded control through IED communication port
- Communications processor detects that IED control jurisdictional permission is granted
- IED is configured to accept control messages
- Communications processor detects that dynamic or static trigger is set
- Communications processor detects that IED control operational permission is granted
- IED detects that control jurisdictional and operational permission is granted

RE-CONFIGURE POWER SYSTEM PARAMETERS WHEN BREACH IS DETECTED

Change IED Setting Groups to Prevent Abuse and Malicious Operation

Many substation IEDs, such as relays, have multiple independent setting groups. Each setting group has complete protection, automation, and control equations. These groups allow a single command to quickly and completely reconfigure a device using alternate groups of settings stored in the device. Thus the IEDs are reconfigured without sending settings through the network. Only one setting group is active at a time. Multiple unique setting groups are designed to perform adaptive management of the power system in response to observed or commanded changes. Several of the setting groups work in a coordinated fashion with other IEDs in several typical power system configurations. One or more setting groups work in a coordinated or stand alone configuration in the atypical instance of a security breach.

Communications processors use the time of day, day of the week, or a specific event, such as a relay alarm output, to switch relay setting groups. In the event of an actual or suspected security breach, the communications processor automatically issues relay settings group changes, or issues them in response to an operator command. The settings group change incorporates complete protection, automation, and control settings designed to protect and secure power system assets during a suspected security breach. Settings are returned to normal through another subsequent settings group change initiated after the breach is terminated and the WAN and LAN are re-secured.

SUMMARY

Combining the many security features that are already available in substation communication devices virtually eliminates hacking, while also severely limiting visibility of substation points of contact. Using settings, passwords and permissives, robust LAN security measures manage WAN access point devices and security elements of applications within the substation including:

- Protection, automation, control, testing
- Substation SCADA, operator interface, HMI

- Connection to control center SCADA and EMS
- Local and remote asset monitoring and management
- Remote configuration management
- Remote engineering access

Network Security Plan Outline

An organization can develop a single, all-encompassing policy, or a suite of policies. At the minimum, policies should contain company positions regarding;

- Viruses and antivirus software—What the corporate standard is and how to protect company computer assets.
- How end-user access is granted to the work network or control systems—How operator and access levels are requested and granted to operators.
- Physical security and physical protection of perimeter gates, access control systems and alarms, protection of computer and server assets in controlled-access facilities.
- Operating System Security Standards should define the standardized setup of workstations, servers, relays, and network equipment.
- A Process for controlling laptops or rogue computers being installed in the network or substation should be included.
- Remote Access and Wireless Communications Policies—Defines the method of entering the network from a remote location. Clearly state whether this is allowed and under what circumstances.
- A New Employee process that briefs the employee on their rights and responsibilities under the security policy and the consequences of violating the policy.
- Departing Employee Procedures—How physical access, relay access, and password changes are handled when an employee leaves the organization.
- Who is authorized to make changes to the topology of the control and Ethernet network and to change security permissions on directories and files
- Password Complexity Policy—This would set the standards for the required complexity of passwords, including nondictionary words, password length, and the inclusion of special characters and numbers.
- Backups and Recovery of Files—Makes clear how tapes should be stored and the processes for backing up, securing, performing restoration from tape as well as the retention of the media.
- Vendor or Visitor Policy—Defines the processes for vendors or visitors within facilities.
- Employee Email and Internet Acceptable Use Policy—Make sure that employees are very familiar with this document.
- Who can audit—This helps define responsibilities for measuring how the security is applied within the organization.
- How often are audits or security checks performed?—daily, weekly, monthly, annual.

Creating Strong Passwords

Strong passwords consist of a minimum of six characters, with at least one special character or digit and mixed-case sensitivity, but do not form a name, date, acronym, or word. Passwords formed in this manner are less susceptible to password guessing and automated attacks. Examples of valid, distinct strong passwords include:

Ot3579 A24.68 Ih2dcs 4u-Iwg Ic-4.7

An easy way to create strong passwords is to take the first letter of each word in a memorable phrase and insert a nonalpha character somewhere in the resulting password. For example, the phrase "I love to ride my horse, Blue" can be used to form and remember the password Il2rmhB, which is difficult to crack because it cannot be pronounced and it is not meaningful. Similarly, the phrase "The Palouse has four beautiful seasons" can be used to create the password tPh4bs, which is simple and easy to remember because of the sentence from which it is formed.

Passwords compliant with DOE guidelines for length and character set are recommended for port switch devices that act as a single point of contact for all substation IEDs. DOE G 205.3-1 Security Guide recommends a 12-character length password that includes case sensitive letters, digits and special characters.

Guidelines for Creating and Maintaining Strong Passwords

The following are simple guidelines to bear in mind while creating and managing your passwords:

- Default passwords shipped with factory devices and application software should always be changed upon installation.
- Passwords should be known only by individuals with authorized access to the devices being installed or updated.
- Passwords should be kept in a secure location that is not easily found or viewed.
- Passwords should be at least six characters long.
- Passwords should contain both upper- and lower-case characters.
- Passwords should contain at least one non-alpha character (i.e., a number or punctuation mark).
- Passwords should not form a common word, date, name, or acronym.
- Passwords should be changed periodically and whenever the security of your password is compromised through personnel turnover, strife, intrusion, or threat.
- When possible, implement two levels of password protected access control–one for viewing settings and another for changing settings.
- On integrated systems, implement multitiered password protection, with one set of passwords for accessing relays and another set for accessing controllers and SCADA systems.

REFERENCES

[1] David Dolezilek, Kevin Carson, Kevin Leech, and Kevin Streett, "Secure SCADA and Engineering Access Communications: A Case Study of Private and Public Communication Link Security," Proceedings of the 5th Annual Western Power Delivery Automation Conference, Spokane, WA, April 1–3, 2003.

BIOGRAPHY

David J. Dolezilek received his BSEE from Montana State University in 1987. In addition to independent control system project consulting, he worked for the State of California, Department of Water Resources, and the Montana Power Company before joining Schweitzer Engineering Laboratories, Inc. in 1996 as a system integration project engineer. In 1998 Dolezilek became Engineering Manager of Research and Development in SEL's Automation and Communications Engineering group. He became the Automation Technology Manager in 2000, to research and design automated systems. In 2003, Dolezilek was promoted to Sales and Customer Service Technology Director at SEL. He continues to research and write technical papers about innovative design and implementation affecting our industry, as well as participate in working groups and technical committees. He is the author of numerous technical papers and 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 communication networks and systems in substations.

20040929
TP6182