Secure SCADA and Engineering Access Communications: A Case Study of Private and Public Communications Link Security

David Dolezilek, Kevin Carson, and Kevin Leech
Schweitzer Engineering Laboratories, Inc.

Kevin Streett
Overton Power District No. 5

Presented at the
DistribuTECH Conference
Orlando, Florida
January 20–22, 2004

Originally presented at the
5th Annual Western Power Delivery Automation Conference, April 2003

SECURE SCADA AND ENGINEERING ACCESS COMMUNICATIONS: A CASE STUDY OF PRIVATE AND PUBLIC COMMUNICATIONS LINK SECURITY

David Dolezilek, Kevin Carson, and Kevin Leech
Schweitzer Engineering Laboratories, Inc.
Pullman, Washington USA

Kevin Streett
Overton Power District No. 5
Overton, Nevada USA

ABSTRACT

Methods detailed in this paper provide an understanding of how to implement a secure substation information system. Overton Power District Number 5 (OPD5) recently installed a state-of-the-art area communications system that dramatically improved secure information access. Commercial Off-the-Shelf (COTS) products were combined with sound engineering practices and methods to secure engineering and business information over a combination of private and public communication links. This case study focuses on decisions, design, and methods affecting the successful implementation and subsequent use of secure local area network (LAN) and wide area network (WAN) communications at OPD5.

Multivendor protection, control, and monitoring IEDs in the substation are integrated with workstations in the substation and at several control and dispatch centers. This collection of equipment performs many simultaneous applications, including the following:

- Protection, automation, control, and testing
- Substation SCADA, operator interface, and HMI
- Control center SCADA and EMS
- Asset monitoring and management
- Remote configuration management
- Engineering access
- Remote data collection and analysis

Information security refers to methods employed to assure the privacy of data and information; the integrity of data and commands received into substation and control centers; and authentication of the source of received data and commands.

This paper describes a real-world implementation of one-way key encryption, key management in action, encryption strength, and performance issues in practice. The system provides comprehensive, multilayered security integration. Access security features of protection, automation, and communication IEDs, SCADA configuration, and communication security products are combined to securely move data, information, and control. The resulting communication infrastructure includes copper, fiber, and wireless serial and Ethernet connections, as well as Virtual Private Networks (VPNs), to provide operations teams with secure access to system data. Locations for data access include general offices, substations, homes of on-call technical staff, and the system integration contractor laboratory. This system gives the contractor the ability to respond to OPD5 requests for technical support and further system development, as well as the ability to perform analysis from remote locations that can be established anywhere in the world.

IN THE BEGINNING

In 1997, Overton Power District Number 5 (OPD5) decided they needed a Supervisory Control and Data Acquisition (SCADA) system. To begin the process of looking for a system, OPD5 sent a Request for Proposal to six engineering firms. Armed with the data contained in the responses, OPD5 sent people to conferences and neighboring utilities during 1998 and 1999.

While visiting neighboring utilities prior to deciding on what they wanted for a SCADA system, OPD5 gained knowledge about the systems that utilities were installing. In one instance, an expensive system that had not been in operation very long was replaced with a completely new system. Replacing the system was less costly than upgrading the proprietary system and its closed communication design. Another utility system was replaced three times in a 10-year span for the same reason.

Based upon what OPD5 witnessed at other utilities, they did not want a proprietary solution. The only solution they would consider had to have an open architecture and allow for easy future expansion. The open architecture would also provide vendor independence and utilize Commercial Off-the-Shelf (COTS) devices from vendors with name recognition in the marketplace. An open system would allow any integrator to work on and support devices from different manufacturers.

OPD5 wanted a system design that would allow each product and engineering service to be available from more than one source.

CHOOSING A WIDE AREA COMMUNICATIONS SOLUTION

All of the worldwide research and development going into the use of Ethernet in many industries encouraged OPD5 to design their solution to use Ethernet. Ethernet was viewed as progressive, while frame relay and other technologies that OPD5 had considered were seen as regressive. OPD5, like other utilities, is comfortable with using Ethernet in the office environment.

The system also had to be capable of providing information to several users. Metering information needed to be available to the billing department, and usage data had to be available to the planning department. The system also needed to support automatic report generation via COTS databases and spreadsheet software.

In 1997, OPD5 had only dial-up telephone communications. Even this was not available in all substations. No other communications media existed; therefore, though a new communications strategy was designed and created to meet technical requirements, the initial primary criterion was availability.

As part of the program to add a new control system, OPD5 was interested in creating secure business and SCADA communications to network data among several substations, dispatch centers, business centers, and remote operator consoles. The staff of the joint engineering, operations, and maintenance department is very small. Therefore, the ability to quickly, simply, and intuitively move data and commands was paramount. Also, many service calls are performed after hours by staff from home, so the system was required to support remote operator interfaces installed in personal residences. OPD5 wanted to create access to all these data, yet provide secure communications to protect the power system and the information.

During the 1998 Western Protective Relay Conference, OPD5 Operations Supervisor Kevin Streett wandered next door to the regional computer trade show being held in the same building.

While visiting a booth, he was introduced to the concept of using Digital Subscription Line (DSL) telephone service to create business office networks. He learned about using it over existing telephone infrastructures to create distributed business networks made secure with the appropriate precautions. It also looked attractive for connecting to home offices and could be used with mobile media.

Mr. Streett investigated using DSL to support the dual network purposes of business systems and SCADA at his business offices, control offices and substations, and employee residences.

NEW COMMUNICATIONS TECHNOLOGY ON EXISTING INFRASTRUCTURE

Back in Nevada, Mr. Streett began discussions with the local telephone service provider. Though they had considered adding DSL services, they were not planning on adding them to the areas serving the OPD5 substations. Kevin asked if this was possible, and soon OPD5 began negotiations with the telephone service provider. OPD5 was able to gain the necessary connectivity to most locations by committing to purchasing ongoing DSL service.

DSL was proven to be a fine solution for the needs mentioned earlier. It was implemented relatively inexpensively without significant new infrastructure and OPD5 merged their business and SCADA data traffic onto the same network.

BUSINESS SYSTEM AND SCADA NETWORKS ARE MISSION CRITICAL

For OPD5, as with most utilities, the robustness of the business system is of primary importance. Security constraints for the business system were more demanding than even the mission critical SCADA system. As with other utilities, the harsh reality is that failure of the SCADA system is inconvenient, but personnel can be dispatched to manually operate the power system. The electronic business system cannot be manually operated and its failure prevents revenue collection and cash flow, which can be catastrophic to the utility.

OPD5 documented two simple, but imperative, criteria for measuring network performance:

1. Availability
2. Security

The small utility needed their business system to be capable of performing customer billing every Thursday morning and employee payroll every Friday. Furthermore, in light of the new accessibility of these data and examples of network intrusion of other utilities, OPD5 wanted to eliminate the risk of customers manipulating billing and usage records.

The security measures implemented by OPD5 met the needs of both the business and SCADA systems.

CHOOSING AN INTEGRATED IED SOLUTION FOR PROTECTION, MONITORING, AND CONTROL

The chosen control system is made from integrating Intelligent Electronic Devices (IEDs) in the substation, rather than investing in a parallel SCADA system. New SCADA dispatch workstations were designed for multiple control stations [1].

IEDs in the substations communicate via serial connections to SEL-2030 Communications Processors. The SEL-2030 Communications Processors applied in transmission and distribution class substations are set to concentrate required IED data and provide specific control functions. They are physically located in station control buildings or mounted in outdoor enclosures.

Figure 1 illustrates a point-to-point "star" topology that is applied to achieve fast, efficient, and robust transmission of measurement data and control actions. Figure 2 illustrates a two-tier star topology that supports virtually any number of IEDs by adding additional SEL-2030 Communication Processors.

Cost-effective Modbus® RTU protocol is used between the SEL-2030 Communications Processors and the control centers. A second separate transparent link to the SEL-2030 Communications Processors provides engineering access to connected IEDs. This link allows engineers to communicate directly with the IEDs through the SEL-2030 Communications Processor from anywhere on the network—local or remote. Once the connection is established, the SEL-2030 Communications Processor becomes "transparent" and passes data to and from the IEDs.

Communications between the Overton office and the service center in Mesquite are via Overton's own T1 line. OPD5 relies on the Moapa Valley Telephone Company to deliver high-speed Asynchronous Digital Subscriber Line (ADSL) connectivity between the Overton office, the Internet, Sandhills substation, Tortoise substation, Logandale substation, and a system operator's house.

Overton substation is connected to the Overton office via single-mode fiber-optic cable. Glendale substation is connected to Tortoise substation via single-mode fiber-optic cable and Moapa substation is connected to Tortoise substation via multimode fiber-optic cable. In Mesquite, wireless Ethernet is used between Bunkerville substation and Pulsipher substation. Direct multimode fiber connects Painted Hills transmission and distribution substations to the Mesquite office. Mesquite substation is connected to the Mesquite office via single-mode fiber-optic cable. Single-mode fiber-optic cable connects Pulsipher substation to Mesquite substation.

The addition of Ethernet to each station supports portable human machine interface (HMI) and engineering access workstations. Laptop computers, when connected to the substation Ethernet network, provide local substation HMI functionality, visibility, access of the regional SCADA dispatch displays, and visibility and access of any HMI screen in any substation throughout the system. Engineering access (via transparent connections) is provided to all local IEDs, as well as any other IED in any other substation. These same HMI and engineering access capabilities are provided via various permanent workstations throughout the system.

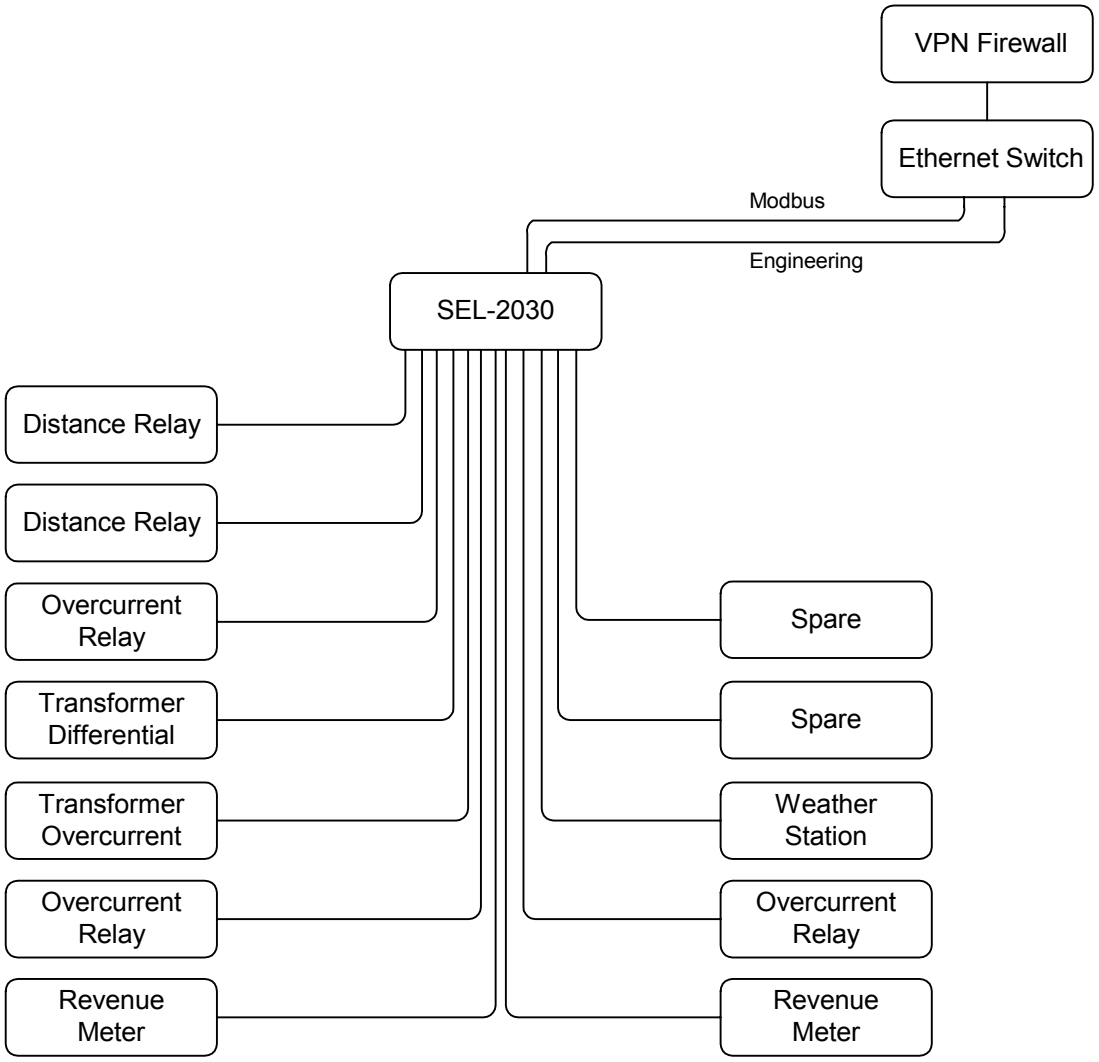

Figure 1 Typical Single-Tier Substation Communications Diagram

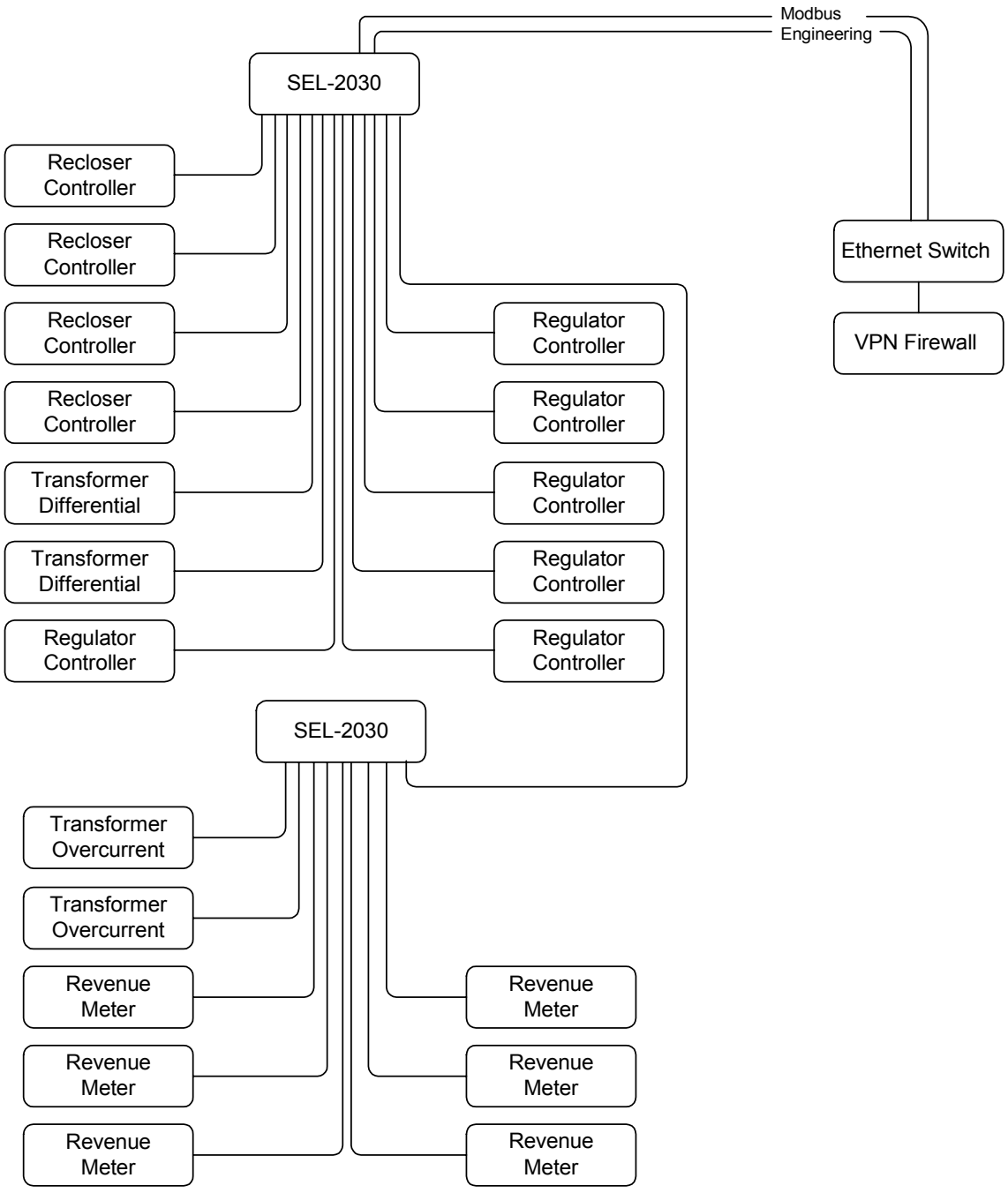

Figure 2 Typical Two-Tier Substation Communications Diagram

Wonderware® Manufacturing Management Information System FactorySuite™ 2000 was chosen to provide HMIs and data management. The Wonderware software used in the project included InTouch® HMI, IndustrialSQL Server™ database, and ActiveFactory™ client. Updates to Wonderware applications are automatically deployed using Wonderware's Network Application Development tools. This approach helps ensure timely and efficient upgrades to the HMI drivers and data management tools. One "View Node" application fits all present and future HMI installations. This simplifies the process of maintaining and adding functionality to the HMI system.

The OPD5 SCADA solution will evolve with technology, but did not require a large capital investment. The system provides data collection, data archiving, and remote operation.

NEW TECHNOLOGY PROVIDES NEW DATA ACCESS AND SECURITY CONCERNS

OPD5 became interested in providing these newly collected data to the appropriate employees to allow better and timelier management of the power system. They began exploring uses for their new innovative HMI applications to disseminate power system information and provide employees with web access.

This new access meant even more security concerns. They did not want employees to have the ability to willingly or accidentally manipulate the power system without authority. Nor did they want possible future disgruntled employees or former employees to have access to manipulate the system or steal information. Furthermore, adding web interfaces meant Internet connections and all of the associated security concerns.

The LAN and WAN communications of the final design are depicted in Figure 3.

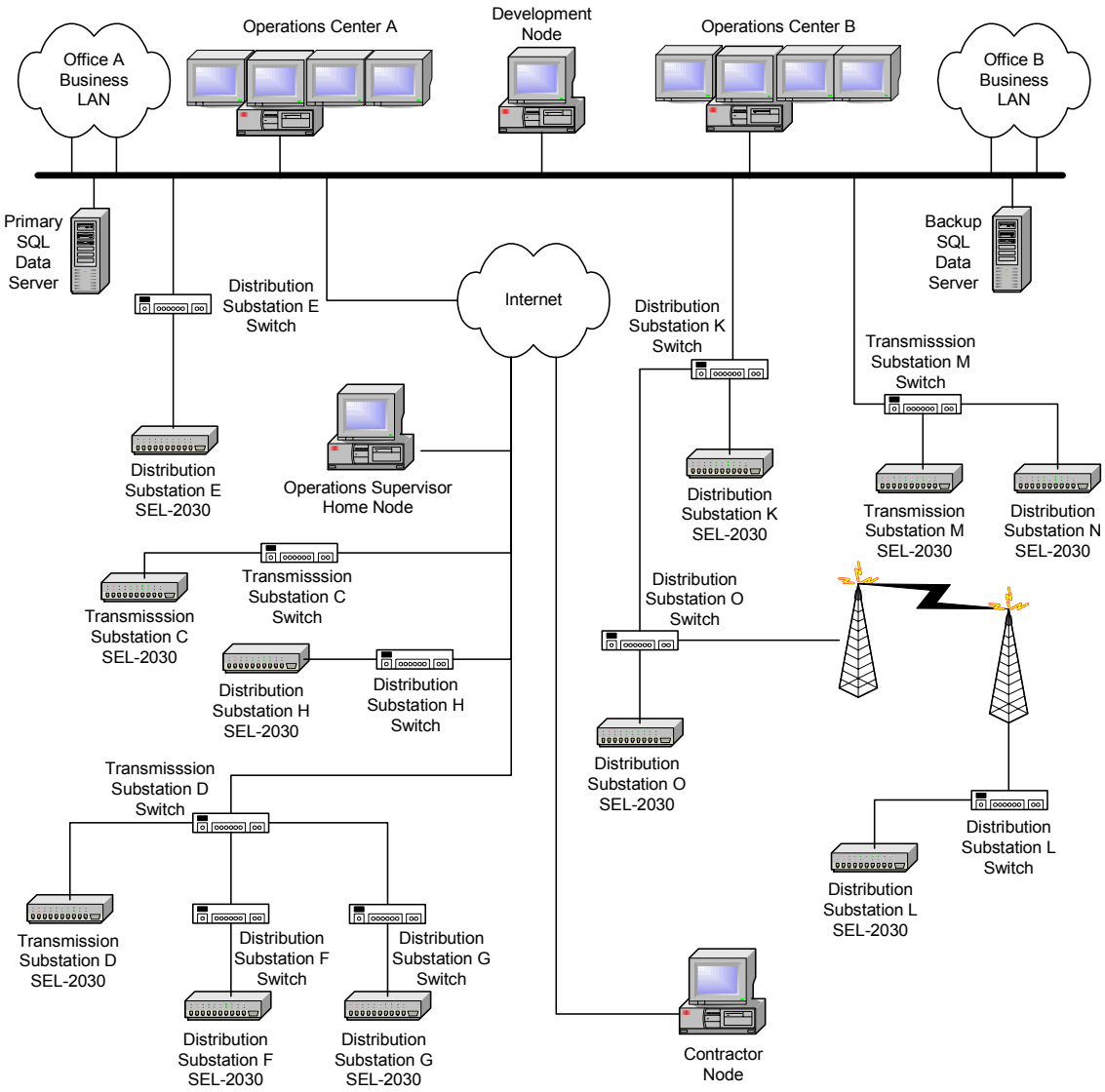

Figure 3 LAN and WAN Communications of the Final Design

ACCESS SECURITY

Information security refers to the methods employed to assure the privacy of substation data and information, the integrity of data and commands received into the substation, and authentication of the source of received data and commands. Two categories of access security include 1) prevention of access by persons who are attempting unauthorized electronic intrusion into the communications system, and 2) prevention of legitimate user access without permission.

The ubiquity and convenience of Ethernet has led to the expansion of Ethernet IP-based networks in utility environments. As with many utilities, OPD5 chose a hybrid design that relies heavily on proven, robust, direct-connect serial links merged with Ethernet to provide LAN and WAN solutions. The economies of Internet Protocol (IP) Networks via Ethernet provide the capabilities to link utility networks at a fraction of the cost of traditional network designs. Unfortunately, IP,

as designed, has no native security mechanisms. Therefore, the transit of IP packets across untrusted WANs (such as the Internet) must be protected with security and encryption techniques.

The SEL relays and SEL-2030 Communications Processors in the integrated system design provide unparalleled LAN information security through passwords, permissives, and monitoring and control strategies. These features are available over traditional copper or fiber communications cables and wireless connections, as well as Ethernet.

Communications products connecting the substation integration and automation systems and business systems to the outside world handle WAN information security. Some connections are secured via direct connection methods; others are secured through data encryption and source authentication.

WAN NETWORK SECURITY AND PROCESSES

OPD5 chose to use IP security protocol (IPSec) to perform encryption. IPSec offers a rich variety of options for exchanging and securing keys and different levels of encryption strength and keying. The role of IPSec is to shroud the data in a secure form for transport across unsecured (insecure) networks. Many strong encryption formats are available. The equipment chosen by OPD5 can be upgraded via firmware as new encryption formats and enhancements are available in the future.

IPSec itself is actually a security framework of methods that provide Confidentiality, Integrity, and Authentication (CIA). Each LAN is a subnetwork, or subnet, secure by virtue of being physically separate from WAN connections. The OPD5 design provides CIA coverage between any two endpoints on different subnets in the system. These subnets are often connected by untrusted WAN connections. The confidentiality of the data encryption is provided by the difficulty of factoring very large prime numbers. In order for IPSec to do its job, a security relationship must be established between two endpoint peers capable of building an encrypted tunnel across the WAN. Many things have to happen in order for this relationship to be successful. Once completed, the encrypted tunnel “virtually” connects the two endpoints as if they were on the same LAN or subnet, thus creating a virtual private network (VPN).

The VPN endpoints we used are firewalls. Firewalls are devices that, by default, allow communications between secure internal networks and unsecured external networks. By default, they also block all traffic from external sources that are not part of a conversation initiated from inside to outside. In this sense, they are “stateful” in that they track the state of connections involved in the TCP-IP conversation and timeout and close those openings that may be left open after the conversation is finished.

The ongoing security policies at OPD5 are a key part of their security strength. The policies are unique to the OPD5 environment and confidential; however, the elements of a successful security plan are outlined.

NETWORK SECURITY PLAN OUTLINE

An organization can develop a single, all-encompassing policy or a suite of policies. At the minimum, the policy should include company positions regarding the following issues:

- **Viruses and antivirus software:** Establish the corporate standard and specify how to protect company computer assets.

- **Operator and end user access:** Explain how end user access is granted to the network or control systems and how operator and access levels are requested and granted to operators.
- **Physical security and physical protection of perimeter gates, access control systems and alarms:** Describe the systems in place to protect computer and server assets in controlled access facilities.
- **Operating system security standards:** Define the standardized setup of workstations, servers, relays, and network equipment.
- **Remote computers:** Establish a process for controlling laptops or rogue computers being installed on the network or substation.
- **Remote access and wireless communications policies:** Define the method of entering the network from a remote location. Clearly state if this is allowed and if so, under what circumstances.
- **New employee orientation:** Develop 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:** Specify how physical access, relay access, and password changes are handled when an employee leaves the organization.
- **Administration:** Designate 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:** Set the standards for the required complexity of passwords, including nondictionary words, password length, and the inclusion of special characters and numbers.
- **Backup and recovery of files:** Make clear how tapes should be stored and the processes for backing up tapes, securing tapes, and performing restoration from tape, as well as the retention of the media.
- **Vendor or visitor policy:** Define the procedure for allowing visitors and vendors to access the physical sites or network.
- **Employee Email and Internet acceptable use policy:** Ensure employees are very familiar with the company's definition of reasonable use of company Email and Internet resources.
- **Audits:** Determine who performs audits and define responsibilities for measuring how the security is applied within the organization. Specify how often audits or security checks should be performed—daily, weekly, monthly, yearly.

These policies should be put into practice as well-understood processes. A primer on creating security policies can be found at the following URL:

http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf

DATA CONFIDENTIALITY, INTEGRITY, AND AUTHENTICITY

Using CIA coverage, OPD5 data are protected from malicious outsiders by firewalls and access control and authorization as defined in the security policies. The confidentiality of the data is ensured by the encryption technology. Integrity is provided by the shared secrets between the two trusted endpoints and the identity mechanisms used to validate the authenticity of the peer. Authentication is provided to end users by secure logon to Windows® 2000 Active Directory

domains and by the complex negotiations of session secret keys that last for a defined number of seconds or amount of data transmitted and then are changed.

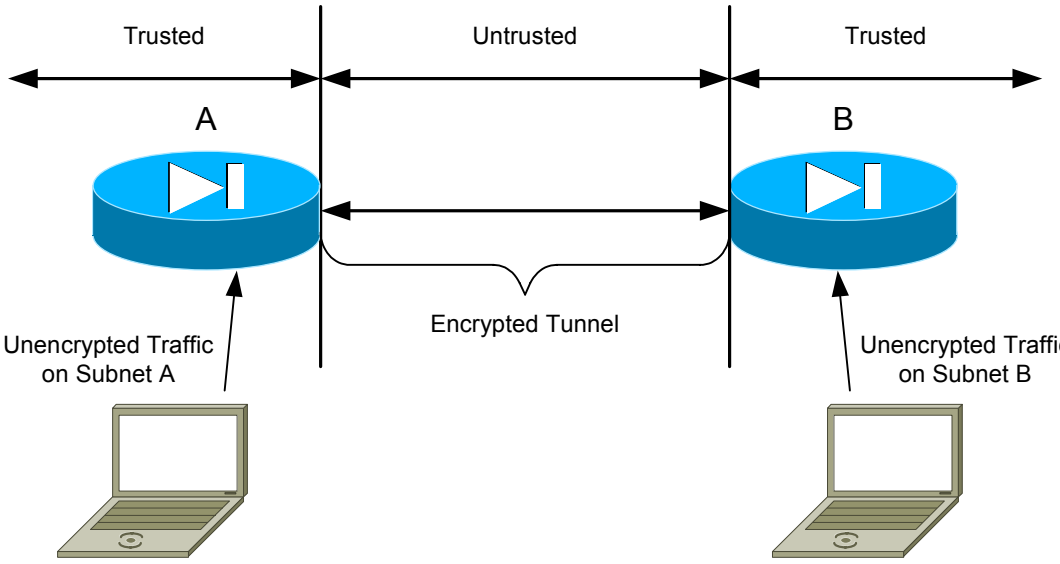

Figure 4 Encrypting Firewalls

IPSec includes mechanisms for providing enhanced IP transit, including Encapsulation Security Protocol (ESP) and Authentication Header (AH). OPD5 chose to use ESP because of its ability to enfold the entire message (or datagram) being sent in a secure wrapper. Furthermore, the method includes the real internal source IP address in the original IP header as seen in Figure 5. This is important because the encapsulation of the actual originating IP address inside of the encrypted wrapper hides important information from a potential hacker and makes the connection more secure.

When the packet reaches the peer firewall on the other side of the tunnel, the firewall terminates the IPsec tunnel on its outside interface, strips off the outer IP header, and reveals the actual private IP address to which the packet is being sent. The firewall passes the packet along via its private interface and it reaches its intended destination. No one between the two peer endpoints can ascertain the true originating or receiving IP addresses.

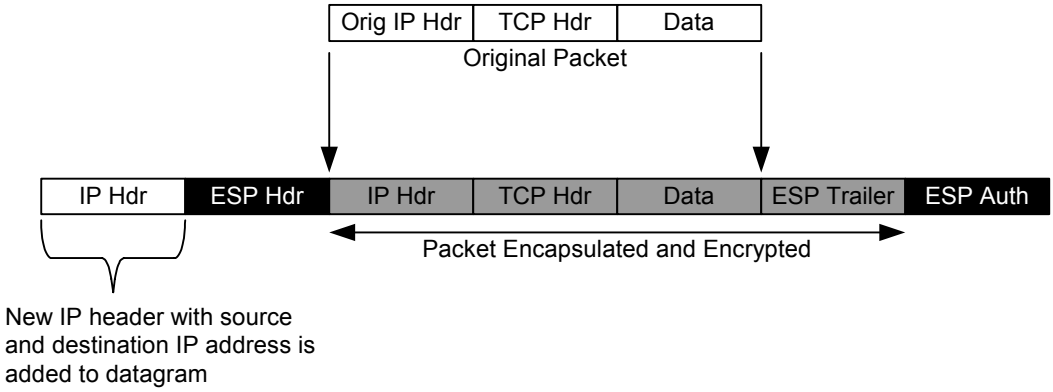

Figure 5 Changes to the IP Packet Using ESP in Tunnel Mode

In order for the virtual private network (VPN) endpoints to build their secure tunnels, a process called the Internet Key Exchange must occur. Matching security policies on OPD5 WAN connection endpoints assure that a security trust relationship can be built so that key negotiation can occur in a secure fashion. The Internet Key Exchange process is illustrated in Figure 6.

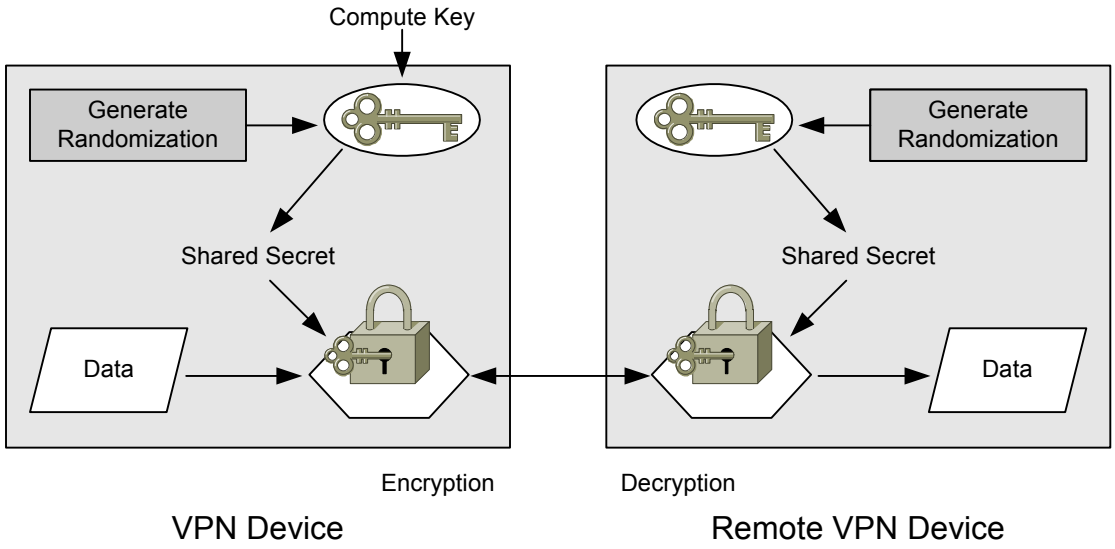

Figure 6 Internet Key Exchange Process

The addition of system and security event logging provides another level of protection and brings all the information from geographically dispersed sites to one logging console.

OPD5 uses a Windows 2000 domain for authentication and security of computer and user accounts. A domain is a logical grouping of computers, users, printers, and services in a common security framework. The OPD5 domain services logons for end users of the system and printer, file services, and files on the network drives. As these services are accessed, event records are logged in an event record database. This security database is accessible from anywhere in the network by the computer system administrator. The responsible administrator can tell who has logged on and for how long, what objects or files were accessed, and if there seems to be a security problem, such as locked out accounts or records of failed logon events.

CONCLUSION

The installed combined SCADA/business system communications network meets and exceeds the expectations and requirements of OPD5 management. The system is highly adaptable for the addition of new substations and new functionality for engineering and business purposes. The adaptability is made possible by readily available software application tools and a flexible communications architecture that uses COTS equipment. The security infrastructure was created with best engineering practices to be robust, yet also open, to allow each product and engineering service to be available from more than one source.

The role of security policies and well-defined processes cannot be understated. Periodic maintenance upgrades, password changes, and security audits and improvements are keys in the cycle of continuous security review.

The continuous improvements brought about by the new SCADA/EMS system help ensure that OPD5 will remain a technically and financially secure power provider for many years to come.

REFERENCES

[1] Kevin Streett (OPD); Kevin Leech (SEL), and Greg Rauch (SEL). "Power Delivery System Integration and Automation at Overton Power District No. 5, Overton, Nevada," Western Power Delivery Automation Conference, 2002.

RESOURCES

Michele D. Guel, The SANS Institute, "A Short Primer for Developing Security Policies," http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf

Andrew Mason, Cisco® Secure Virtual Private Networks, Cisco Press, 2001.

BIOGRAPHIES

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 was promoted to 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.

Kevin Carson studied graphic design and graduated with a BFA in 1981 from Washington State University. Working in the early years of CAD and computer graphics systems, he developed an interest in computer systems and networks and sought additional knowledge and training. During this time he worked on software development projects that included work for IBM, Lotus Development, and Microsoft. He also managed a technical support department, became an IT Department Director and built large-scale networks. In 1997, he received a Masters of Public Administration from the University of Idaho and joined SEL from the public sector in 1999. After 18 years of experience in the field, he is a Cisco Certified Network Associate (CCNA) and a Microsoft Certified Professional (MCP). Kevin worked as a Network Engineer until 2001. He is currently the Data and IS Security Manager for SEL.

Kevin Leech received his BSEE from the University of Wyoming in 1994. He worked for CME Engineers as a Design Engineer. In 1998, he joined SEL as a System Integration Engineer. He is now an Integration Application Engineer. His experience includes process automation and control, substation automation and integration, human machine interfaces, radio telemetry, SCADA, PLCs, programming and start up of PLC and HMI systems, control panel design, and lighting system design. He is a member of IEEE.

Kevin Streett majored in Construction Management at Boise State University. Prior to joining Overton Power District No. 5 in 1986, he worked as a construction foreman and supervisor in the U.S. and overseas, building substations, transmission lines, and distribution systems. He is presently Operations Supervisor at OPD5, responsible for substation construction and maintenance, metering, and operations.

20031031 • TP6148