Cybersecurity as Part of Modern Substations

Dwight Anderson and Garrett Leischner
Schweitzer Engineering Laboratories, Inc.

Presented at the
7th Annual Clemson University Power Systems Conference
Clemson, South Carolina
March 11–14, 2008

Cybersecurity as Part of Modern Substations

Dwight Anderson and Garrett Leischner, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Modern substation integrated systems deliver information to a wide range of users in near real time and also automate a number of tasks that streamline operations and performance. Often these new performance advantages come with an additional cost, cybersecurity. Every month there are reports of threats and attacks from hackers, disgruntled employees, and terrorists attempting to breach and/or corrupt sensitive control systems of power utilities. Fortunately, adding countermeasures to improve cybersecurity is relatively straightforward and is frequently present in the feature sets of equipment already in service. This paper shows and encourages integration and automation engineers to take straightforward steps to enhance the security of a modern substation.**

I. Introduction

There is a lot of interest in securing the electric power infrastructure. Increasing awareness of cybersecurity and the imminent deadlines by the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards are causing a heightened sense of urgency throughout the industry. Compounding the sense of urgency are many well-meaning "technical experts" who are urging an almost knee-jerk reaction from modern substation owners, creating a circus-like environment. This paper presents practical techniques that help mitigate potential vulnerabilities in the electric power infrastructure for little or no additional cost.

Many of us have had negative personal experiences, including identity theft, phishing, denial of service, computer viruses, and credit card fraud. Corporations and utilities have similar experiences and concerns. Magazines, newspapers, and television contain alarming reports of the many threats from hackers, disgruntled employees, terrorists, and countries with sophisticated information warfare plans and capabilities. These threats are as real as the ones we may have personally experienced.

Given the rapidly changing world of technology and the relatively new recognition of the importance of cybersecurity, it often seems as if there is no clear focus on the responsibility for security. Does it belong with the information service people, SCADA personnel, protection engineers, customers, suppliers, or government? The responsibility belongs to all of us who work for and with utilities. It has to because modern power systems use so many different kinds of electronic instruments and so many different means of communications and access for such a wide variety of purposes. No one entity can thoroughly cover cybersecurity. This responsibility comes in many forms, from documentation and implementation of policy, standards, and procedures to application of proven techniques to secure a substation's infrastructure, as will be discussed in this paper.

II. Generate Policy, Standards, and Procedures

Generation of a security policy is the most critical underpinning for a modern utility. Once written, the security policy leads to standards and procedures, which produce a security baseline of guidelines and a set of instructions. This step is essential to achieve the goals to secure a modern substation and must not be circumvented. It is one of the reasons a security policy is one of the cornerstones to the NERC CIP requirements.

Many vendors claim that if you purchase their product, it enables you to comply with the NERC CIP requirements. Some companies even go so far as to list the NERC CIP requirements and how their technology enables compliance. After much discussion regarding the NERC CIP requirements, the authors of the requirements clearly state, there is not a vendor or single product that will enable a substation utility to become compliant. A device can only aid in compliance once a policy, standard, or procedure is created, defining what mitigation technique a company is going to undertake in response to an identified threat or requirement, such as the NERC CIP requirements. The NERC CIP requirements are about policy, standards, and procedures that lead to security:

> "The Responsible Entity shall comply with the following requirements of Standard CIP-003:
>
> R1. 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. The Responsible Entity shall, at minimum, ensure the following:
>
> R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
>
> R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets" [1].

The policy must be as unique as the company creating it; no "one-size-fits-all" policy exists. A company's policy should contain such subjects as classification of substation data, access control measures, and remote engineering access. The policy must spell out acceptable-use constraints and privacy. It should also be short, not exceeding two or three pages.

There are a number of good sources of information and examples regarding security policy, starting with The SANS Security Policy Project [2].

Also available is the National Institute of Standards and Technology (NIST) Special Publications (800 Series) reports [3]. This series focuses on the policy, procedures, and guidelines for computer security, as well as collaborative activities with industry, government, and academic organizations. For example, the SP 800-12 Chapter 5 [4] provides specific policy requirements for computer security useful for a modern utility's security policy.

NIST and SANS provide insight into the purpose and design of a security policy for a modern substation. Most recently, the NIST SP 800-82 [5] and SP 800-53 [6] provide updated guidance to assess and implement security in industrial control systems (ICS).

Another good reference is the *IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security* [7], which provides a good overview of the security problem with general recommendations.

Also consider *Information Security Policies Made Easy* [8]. This is a valuable resource for those seeking practical templates, advice, and instructions that help generate very clear and compelling security policies.

III. Conduct Risk Analysis

The next step, after establishing policy, standards, and procedures, is to conduct a risk assessment and analysis of the substation. Part of the NERC CIP requirements is to determine and identify the critical cyber assets that may be part of the bulk power infrastructure. Part of any thorough security assessment includes determining risks associated with these critical assets.

There are two methods of risk assessment regarding security: qualitative and quantitative. Both methods yield important data that make up a risk assessment and, when used congruently, provide an optimum of security measures. We recommend applying both methods. For example, a team can qualitatively list all the possible scenarios of attack vectors, either physical or electronic, for a modern substation, then quantitatively assess and assign these scenarios a value of low, medium, or high, relating to likelihood and impact of attack. The qualitative process needs review on a yearly basis to identify technological shifts that could lead to significant changes in the outcome of an assessment.

A number of reference materials provide detailed examples of each type of assessment. One is the *Official (ISC)*$^{2®}$ *Guide to the CISSP*® *CBK*® (Certified Information Systems Security Professional Common Body of Knowledge) [9]. It uses the quantitative annual loss expectancy (ALE) to determine how much a utility should spend on countermeasures that mitigate risk for a critical asset. The ALE is equal to the single loss expectancy (SLE) or the total asset value (AV) times the percentage exposure factor (EF), stated as:

$$\text{SLE} = \text{AV}\ (\$) \bullet \text{EF}\ (\%) \qquad (1)$$

The exposure factor is the percentage of asset loss if a potential threat were to be successful. The ALE is the product of the SLE and the annualized rate of occurrence (ARO) given as a percentage.

For example, if a substation's total assets are worth $2.5 M and the threat analysis determines that one out of every five years an attack would occur against this asset and result in $1 M in damage, the ARO is 1/5 or 20%, with an SLE of $1 M • 20% yielding an ALE of $50 K. In this example, a utility can justify spending $50 K or more in countermeasures to protect that asset from the threat.

There are other alternatives to risk mitigation. A company could choose to accept the risk and be "self-insured." It might choose to transfer the risk, for example, purchasing an insurance policy and transferring the risk of an attack. Unfortunately, risk is accepted, reduced, transferred, or avoided, but never completely eliminated. Also the NERC CIP standards and associated penalties do not allow for risk transference. However, as seen in Fig. 1, a modest investment in effective security measures provides a very large reduction in the potential remediation costs.

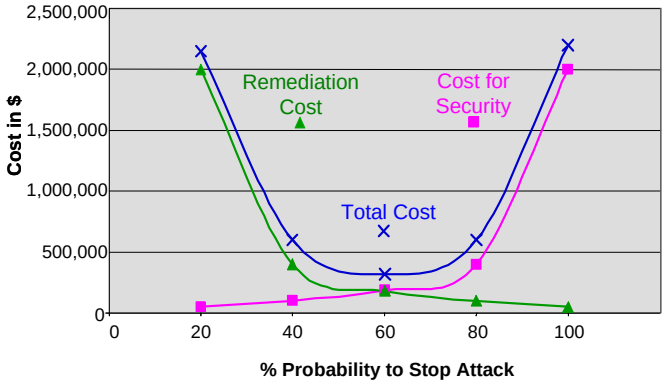

Fig. 1. Economic Model: Modest Investment Provides Great Benefit

IV. Identify and Map All Communications Pathways To and From a Substation

The first step to mitigate risks is to identify and visually inspect all communications paths via a network diagram and walking tour of the network. Because this knowledge may be found throughout a company, a team should be made up from various departments, such as research and development, manufacturing, information technology, legal, human resources, and facilities. The goal for each team member is to look at the substations and systems and contribute his or her view of potential vulnerabilities. A second pair of eyes viewing the substation and communications makes overlooking a vulnerability less likely. After analyzing their network diagram and conducting a visual walk of the network communications links, one company discovered a fiber-optic line that was exposed and open to access for a very long distance. Even an accidental cut would have taken down a large part of the SCADA system with the potential to cause a great deal of damage. It is important to identify all interconnections and bridges between systems, identifying SCADA links, engineering access, even maintenance. Take time to identify and visually inspect wireless, Internet, telephone line, or dedicated fiber connections.

A. *Internet Vulnerabilities*

There is a misconception that a substation must have an Internet connection to be a target. This is not true, for example, an inadvertent interconnection was made from a third-party vendor who connected their computer to install a patch on an "isolated" frame relay network. The network became connected to the Internet because the third-party vendor's computer had a broadband Internet wireless card installed. A similar scenario introduced the "Slammer" virus into a industrial plant. The virus originally came from the Internet, and then being network-aware, it propagated via a T-1 line and saturated the plant's networks with traffic. There was no connection to the Internet and the intranet of the company was isolated. The company met the NERC CIP requirements regarding routable protocol, but it was still susceptible to this type of threat.

Unfortunately hackers tend to use an "island hopping" approach to infiltrate a network. They begin with a vulnerable perimeter server (firewall, web server, internal modem, etc.) and use the compromised perimeter computer to launch a fresh attack on vulnerable devices on a "private" network (not publicly addressable). The typical corporate local area network (LAN) activities, like email or web surfing, can lead to direct compromise of a computer on the "private" network. This leads to viruses, trojan horses, backdoors, and logic bombs that can spread to SCADA computers. In some cases, this type of threat may lead to rogue access points that allow intruders access.

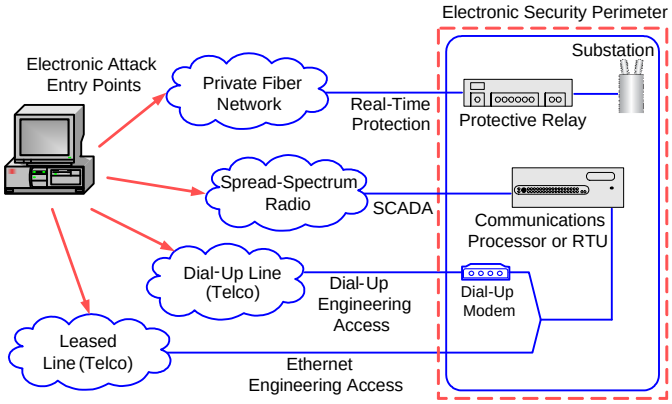

Fig. 2. Typical Modern Substation Network

Lack of network segmentation and filtering is one of the largest and most obvious problems in utility networks. The drive to include web portals for telemetry, measurement, and metering information can also create conduits between systems. As more and more systems use web front ends, it is important for them to comply to security policy, including up-to-date patching. Just because HTTP (Hypertext Transfer Protocol) processes are on an embedded system does not infer that they conform to the security standards your policy requires.

It is very important to note that any network connection over public communications infrastructure is vulnerable to electronic intrusion and other malicious intent. The Internet is clearly the most dangerous of public networks, but any network connection that is remotely accessible by a malicious individual is a potential security risk.

B. *Dial-Up Vulnerabilities*

The dial-up infrastructure of the public telephone system allows any-point to any-point connections, just like the Internet. "Security through obscurity" is not a valid method to protect the resources that connect to the Public Switched Telephone Network (PSTN). Because the PSTN is an open network, an attacker does not need to take over any switchgear or computers at the phone company to perform an attack. This network is a low-effort, low-risk attack vector. Most dial-up modems provide little or no access control mechanisms, and those that do often implement simple passwords that do not conform to the NERC CIP password requirements. Even when passwords provide electronic access control mechanisms, there are no intrusion detection mechanisms, or access logs; therefore, this type of access control provides little likelihood of deterring or, more importantly, detecting a password-guessing attack.

Some companies look at spread-spectrum radio technology to provide security, but its design is primarily for noise immunity and bandwidth sharing, not security. An attacker can ascertain the spreading sequence and modulation technique with sophisticated spectrum analyzers. Spread-spectrum sequences are not designed for security. Often they are short and relatively easy to reverse engineer when using real-time computational power in conjunction with high-speed scanning signal intelligence.

Reference [10] describes the practice of spreading codes publicly so that companies can build compatible equipment and users' computer systems can more easily associate with access points. In theory, an attacker cannot reconstruct (despread) the signal without knowledge of the exact spreading sequence used to spread out the signal during modulation. However, many spread-spectrum radios are designed in similar fashion to the 802.11 hopping pattern [10] and use the same pseudo noise code. Because of this, often the radios can receive and demodulate each other's signal.

C. *Fiber-Optic Vulnerabilities*

Fiber optics is a common communications medium that many presume to be secure, but if a person can acquire physical access to the fiber, it is easy to compromise. Fiber optics is just as vulnerable to hackers as a wired or wireless network.

Reference [11] reports the following:

> "There have been few public reports of fiber hacks: In 2000, three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany. In 2003, an illegal eavesdropping device was discovered hooked into Verizon's optical network; it was believed someone was trying to access the quarterly statement of a mutual fund company prior to its release—information that could have been worth millions. International incidents include optical taps found on police networks in the Netherlands and Germany, and on the networks of pharmaceutical giants in the United Kingdom and France."

The noise margin for fiber is larger than the insertion loss of a tap. This makes such taps difficult, if not impossible, to detect. Such taps have sold for under $1,000 on Internet auctions.

V. Use and Manage Strong Passwords

Passwords still form an important layer of security. All security experts agree that strong password protection is still the best defense against electronic intrusion and other forms of unauthorized access. Regardless of what other authentication mechanisms are used, a good password not only protects your equipment against unauthorized settings but also safeguards the integrated system and helps ensure the reliable operation of a substation or SCADA system. If a password is disabled, easily guessed, or cracked, intruders can not only shut down a system, they can also use the system to distribute false data and sabotage other interconnected systems within a company and worldwide across the Internet. A well-formed, strong password is virtually impossible to guess and may take thousands of hours to crack, whereas an ill-chosen password is crackable in just a few seconds. It is extremely important to maintain the security of a system by using strong passwords in protective relays, controllers, and remote access points to your SCADA systems.

Hackers have access to prebuilt, automated password attack programs like John The Ripper, Brutus, and LC4, and dictionaries that contain thousands of common passwords, including street slang, common spouse and pet names, foreign words, and popular culture terms and names. As a result, passwords are immensely strengthened if they are not existing words.

Strong passwords consist of at least six characters, have at least one special character or digit, use mixed-case sensitivity, and do not form a name, date, acronym, or word. Examples of valid, distinct strong passwords include:

Ot35f7~~ A24.68!s #Ih2dcs4 @4u-Iw2g

Modern substation protective relays and communications processors should support strong passwords. These products allow the user to program passwords made up of any of 90 characters (uppercase letters, lowercase letters, numbers, and nonalphanumeric characters). In addition, all these devices support a password length of at least six characters. Some newer devices and communications processors support password lengths of up to 12 characters. Table I shows a comparison of the password strengths supported by power protection devices made by different vendors.

The NERC CIP requirements of CIP-007 [13] state the following:

> "R5.3 At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
>
> R5.3.1 Each password shall be a minimum of six characters.
>
> R5.3.2 Each password shall consist of a combination of alpha, numeric, and 'special' characters.
>
> R5.3.3 Each password shall be changed at least annually, or more frequently based on risk."

TABLE I
PASSWORD STRENGTH COMPARISON IN PROTECTIVE RELAYS FROM DIFFERENT VENDORS [12]

	#Char, Length	Combinations	Time Required for Brute Force*
Vendor 1	90, 6	537 B	18 Years
Vendor 2	10, 10	11 B	201 Days
Vendor 3	10, 6	1 M	17 Minutes
Vendor 4	26, 4	475 K	5 Minutes
Vendor 5	14, 4	41 K	27 Seconds
Vendor 6	2, 3	14	4 Milliseconds

* This is the amount of time required to transmit all possible, maximum-length passwords in a continuous stream over a 57,600 bps serial line (assuming a 10-bit serial format).

It is important to note that some devices shown in Table I do not conform to the minimum password security length required by the NERC CIP requirements.

The six-character password with the support of 90 characters (Vendor 1) provides over 537 billion unique password values. If an attacker were to send every possible six-character password in a continuous stream using a fast 57,600 bps serial line, it would take almost 18 years to transmit all of the passwords! In reality, it would take more than 18 years to attempt to log into a substation relay using all possible passwords. This is because the relay must transmit the password prompt and other feedback strings between password attempts, and it takes time to process each password attempt. If you choose a strong password value and protect it with link encryption, you can make it virtually impossible for an attacker to compromise the password-based authentication mechanisms in a modern substation device.

A. Use Multilevel Password Support in Communications Processors and Relays

Communications processors and all protective relays in the modern substation should support multilevel password-authentication schemes (see Table II).

TABLE II
SUMMARY OF MULTILEVEL PASSWORD-AUTHENTICATION MECHANISM IN MODERN SUBSTATION DEVICES

Access Level	User Privileges	Authentication Requirements
0	View Device Identification Strings	N/A
1	View Settings	Level 1 Password
2	View and Change Settings	Level 1 and Level 2 Passwords
BREAKER (Protective Relays Only)	Operate Breakers	Level 1 and Breaker Level Password

This multilevel password authentication scheme provides a much stronger access-control mechanism than single-level password authentication for the following reasons:

- An attacker must compromise two independent passwords to reach Level 2 or BREAKER Level access.
- The system administrator can grant limited, read-only access to devices or to a group of users without giving them the ability to change critical device settings or operate control points.

The multilevel password scheme makes it much more difficult for an attacker to gain an access level with a high enough privilege to cause significant system damage. If we assume that the goal of a malicious cyberattack is to change device settings or to operate critical control points, then the multilevel password scheme doubles the difficulty of carrying out a successful attack using password-guessing techniques, such as a dictionary or brute force attack. This is because an attacker has to successfully guess the Level 1 password before beginning an attack on the Level 2 password.

The modern substation with multilevel password mechanisms also provides a system administrator with more control over the privileges granted to a given user. It is important to limit the dissemination of critical passwords as much as possible. The multilevel password authentication scheme outlined previously allows you to grant a group of users the ability to view device settings and status, download event reports, or check metering data without simultaneously granting them the ability to perform potentially damaging actions.

B. Time-Outs and Channel Disconnects Slow Password-Guessing Attacks

The modern substation's protective systems should also temporarily lock out the communications port in the event of three failed password-entry attempts. The lockout period of one minute on substation equipment effectively limits the rate of a password-guessing attack to less than three password attempts per minute. This functionality increases the effective strength of the password-based authentication scheme on a substation communications processor and protective relay. In addition, whenever the substation device locks out the remote communications port, it should also disconnect any current engineering access sessions by forcing the modem to hang up or by terminating the Telnet connection. This action further reduces the effectiveness of a password-guessing attack by forcing the attacker to redial the local modem or reestablish the Telnet connection every three failed password attempts.

The modern substation device should provide a port timeout setting that also logs off the user. The timeout setting disconnects after a set amount of inactivity. This forces all stale authenticated login sessions to terminate and not be available as an attack vector, namely preventing an attacker from inheriting the login privileges of a previous user.

C. Encrypt and Authenticate Communications

Unfortunately, capturing and dissecting Transmission Control Protocol/Internet Protocol (TCP/IP) frames over Ethernet is a relatively simple process using freely available tools from the Internet. These programs capture and dissect frames and now even feature decoding of popular automation protocols such as Modbus® and Distributed Network Protocol (DNP). Captures of serial information are just as easy to acquire and uncomplicated to decode and interpret. The tools work with wireless links, and information is readily available from the airwaves without having to tap a physical communications line. The hacker simply has to be within range of the signal. Fig. 3 and Fig. 4 illustrate the process of capturing a plaintext Telnet login dialog.

Using network switches instead of hubs can help to mitigate the risk of Ethernet sniffing, but any shared media is subject to the risk of data interception. This illustration further demonstrates the necessity of using encryption to secure links, especially over untrusted communications links.

Modern substation security should include the use of devices that secure byte-oriented data packets, such as those found on Modbus or DNP SCADA networks, with encryption and/or authentication algorithms. Authentication of the data packets ensures the data are from a trusted source and not modified *en route*. Encryption not only adds greater security but also provides privacy or confidentiality of the data. This is especially important if the data find their way onto publicly accessible networks, such as radios, telephone, or routable protocol infrastructures. These security devices do not interfere with data flow on control and/or monitoring systems, but ensure confidentiality, authentication, and integrity of the transmitted data. The modern substation may achieve this over a LAN through tunneling the traffic through a Virtual Private Network (VPN) based on Internet Protocol Security (IPsec) or Secure Sockets Layer (SSL), where the VPN separates and protects the traffic from the underlying infrastructure it is traversing.

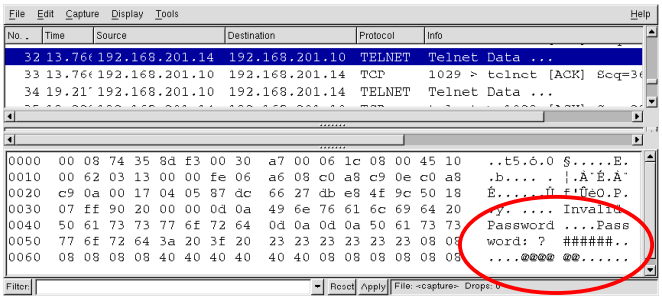

Fig. 3. Password Prompt From the IED

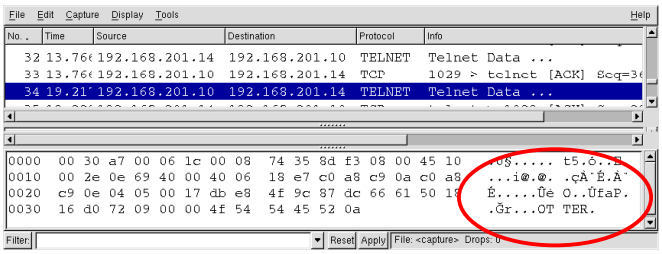

Fig. 4. Password Returning to the IED

VI. Secure Dial-Up Remote Access Points

To secure existing dial-up or remote engineering access, use a serial encryption and authentication device in line with the existing computer/modem/radio/fiber communications links. These types of devices provide data confidentiality and integrity, as well as prevent unauthorized access with session authentication. Using these types of devices protects the data that travel across a PSTN. The devices seen in Fig. 5 are protecting a remote access link.

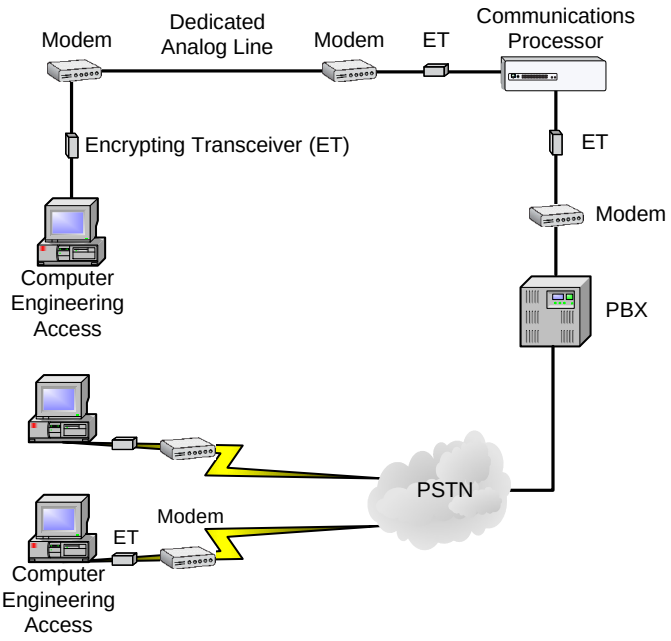

Fig. 5. Adding Serial Encrypting Transceivers Provides Data Security

VII. Secure TCP/IP Links

More computing platforms are finding their way into the modern substation. Fortunately there is a great deal of software and documentation about securing this type of communications link. A modern substation computer combined with Windows® 2000 Active Directory Domain, for example, can encrypt communications to compliant hosts (other computers and Windows 2000, Windows XP, or 2003 servers) with relatively few configuration selections. Also there are similar offerings for Linux-based computer systems. Once again the goal of encryption and authentication is to secure routable protocols that make their way into a substation network connection as required by the NERC CIP requirements.

With a slightly more involved configuration, a Windows-based system can communicate securely using IPsec encryption with hosts that are not part of their own domain or if a domain controller is not present [14].

A variety of special-purpose encryption and authentication devices for TCP/IP communications protocols provide confidentiality, integrity, and authentication services for utility communications. Depending upon the feature sets, these devices vary in cost and complexity of use. Encryption devices may operate as termination endpoints for VPN tunnels or they can simply provide transport services for TCP/IP packets. The most common architecture is point-to-point. It is also possible to aggregate many VPN tunnels at a single point of concentration.

VIII. Practice Need to Know and Compartmentalize Information

Modern substation procedures should include a formal process of "need to know" and compartmentalization of information. It is important to limit access to system details only to those who need it. Consider keeping system documentation safe and secure. To do so, utility security management should consider using access models such as discretionary access control (DAC) or mandatory access control (MAC). More information about these models is in [9].

In DAC, the owner determines who can obtain and access data. The owner of the data determines and provides the access rights and permissions for who can read, write, or modify the information.

In MAC, the policy and system defines who can access or modify information. The military uses MAC as a means to secure highly sensitive data, such as classified information. In a MAC system, subjects and objects have sensitivity labels that specify a level of trust. In order to access an object, the subject must have a sensitivity level equal to or higher than the label of the object.

Both DAC and MAC may seem cumbersome and too controlling; however, they are well-proven security management tools that align well with the NERC CIP requirements for security management controls.

CIP-003 Cyber Security — Security Management Controls [13] states:

> "R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
>
> R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
>
> R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access."

IX. Monitor the Security Status of Electronic Access Points

It is extremely important to detect potential electronic attacks and react to them as quickly as possible. Strong electronic access controls make it exceedingly difficult for an attacker to compromise your electronic devices, but they do not make it impossible. If you give attackers unlimited time to probe your critical systems for vulnerabilities, then they may eventually succeed in exploiting a weak point in your defenses. A way to combat this is to put technologies in place that allow you to monitor and create log entries of electronic connections. It is then important to view the log files on a regular basis to identify suspicious activity and receive timely

notification of a possible attack. Many substation products contain very effective electronic monitoring and alarming technologies that will allow you to detect and react to electronic attacks.

A. Dedicated Alarm Contacts

It is important for modern substation IEDs to have a dedicated alarm contact that will pulse in response to an event occuring, for example:

- Whenever there are three failed login attempts in a short time period.
- Whenever a user attains a level that settings may change.
- Whenever a user saves a new settings configuration to the device.

In these cases, routing the current status of the alarm bit through SCADA back to a central office alarm panel and log file allows a modern substation owner to detect potential password-guessing attacks or to detect unauthorized access or settings changes in the device.

B. Sequence of Events Records

In addition, operators can program devices to automatically send a time-stamped Sequence of Events (SOE) record in response to a change in status. They can also use SOEs to monitor changes in the internal logic bits in the device, including the alarm bit, the digital inputs, and the results of user-programmed logic equations. The event-reporting mechanism in modern devices is extremely flexible. Logic equations can be used to generate an SOE report for a wide variety of conditions. Fig. 6 shows a collection of SOE records from such a device as an example of securing a modern substation.

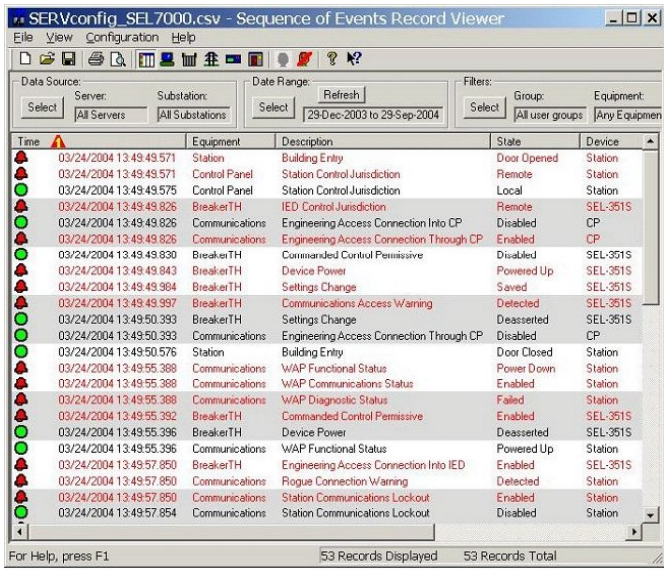

Fig. 6. Sequence of Events Records Collected From Various Devices

In this example, there are event records that indicate user access, physical perimeter breaches, enabling and disabling of remote breaker control, and many more valuable status indicators. The SOE mechanism, coupled with the robust logic programming capabilities in modern substation devices, provides the ability to monitor almost any event of interest. It is then possible to consolidate and monitor these event notifications from a central location and to react as necessary.

C. Monitoring Via Remote SCADA Links

Controlling and monitoring the communications status points via the remote SCADA link allows a substation owner the ability to control and monitor engineering access permissions from a central control center. An HMI Communications Overview screen, as pictured in Fig. 7, gives remote administrators the ability to grant engineering access to each serial or Ethernet connection independently for security and safety. This prevents unauthorized connections and validates that a user is appropriately connected to an IED. You can use the same procedure to manage and monitor remote breaker control in all relays connected to the communications processor.

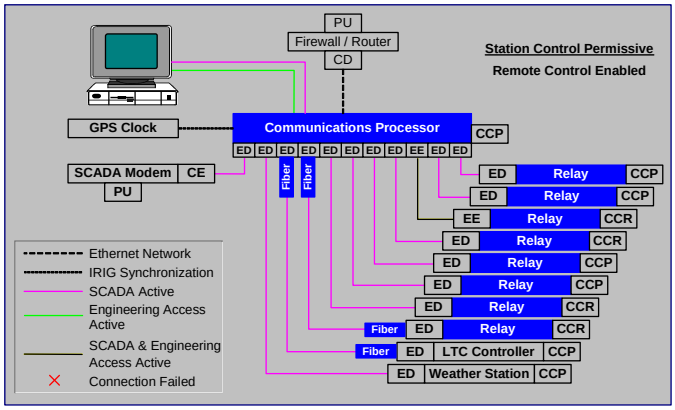

Fig. 7. HMI Screen Showing Status of Substation Communications and Control Status [15], [16]

D. Automated Event Messenger and Email Transceiver

Finally, enhancing the monitoring of the system by using an automated event messenger that delivers real-time alarm and event notification to the personnel via a telephone call allows the modern substation manager to react quickly to the situation. The event messenger turns the contents of the text into a computer-generated voice message that will inform the recipient of the nature of the detected event. The substation event messenger receives a text message and automatically dials a preconfigured telephone number to notify the recipient of the event or SOE report. The event messenger is connected to land line or cellular telephone connections or SMS (short message service) interfaces for text messaging. This method supports any text string so that it can be customized with personnel names, equipment names, geographical information, and instructions. The event messenger saves the message so that it can be called back for confirmation or repeat of the message. These same text strings are also, or alternately, sent via email directly to one or more recipients. An Ethernet transceiver captures the message and sends it to a predefined email recipient or mail group.

X. Conclusions

The technologies used for implementing critical SCADA, real-time protection, and engineering access communications links to a modern substation are susceptible to attack. In this paper, we have provided cost models, techniques, and methodologies that you can apply to secure critical communications links. Though you can never completely remove the possibility of attack, you can greatly reduce the probability of a successful attack and the severity of resulting effects by applying the suggestions outlined in this paper. These steps will greatly improve the overall security of your communications to and from a modern substation.

To summarize, here are the general steps to secure a modern substation:

- Generate unique policy, standards and processes.
- Conduct a risk analysis based on qualitative and quantitative assessments.
- Identify and map all communications pathways to and from the substation.
- Use and manage strong passwords.
- Secure all access points to protect from attacks.
- Practice "need to know" security and compartmentalize information.
- Monitor security status of critical electronic access points.

XI. References

[1] *Standard CIP–003–Cyber Security—Security Management Controls*, North American Electric Reliability Corporation, June 2006 [Online]. Available: ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-003-1.pdf

[2] *The SANS Security Policy Project*, SANS Institute [Online]. Available: http://www.sans.org/resources/policies/

[3] *NIST Special Publications (800 series)*, National Institute of Standards and Technology [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html

[4] *An Introduction to Computer Security: The NIST Handbook*, National Institute of Standards and Technology Special Publication 800-12, Oct. 1995, pp. 33-44 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

[5] *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology Special Publication 800-82 DRAFT, Sep. 2007 [Online]. Available: http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf

[6] *Recommended Security Controls for Federal Information Systems*, National Institute of Standards and Technology Special Publication 800-53 Rev. 1, Dec 2006 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf

[7] *IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE Standard 1402-2000, 2000.

[8] C. C. Wood, *Information Security Policies Made Easy, Version 10*, Houston, Texas: Information Shield, 2005.

[9] H. F. Tipton and K. Henry, *Official (ISC)^2 Guide to the CISSP CBK*, Boca Raton, Florida: Auerbach Publications, 2007.

[10] *Supplement to IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, IEEE Standard 802.11B, 2000.

[11] S. K., Miller (2006, Nov. 15). Fiber Optic Networks Vulnerable to Attack. *Information Security Magazine*. Available: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1230106,00.html

[12] P. Oman, "Using Passwords to Secure Relays, Controllers, and SCADA Systems From Unauthorized Access," SEL Application Guide Vol. VI, No. AG2001-05, May 17, 2001.

[13] *Standard CIP–007–1—Cyber Security—Systems Security Management*, North American Electric Reliability Corporation, June 2006, p. 3 [Online]. Available: ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-007-1.pdf

[14] E. Cole, *SANS Security Essentials, Version 2.6*, SANS Institute, October 2006.

[15] D. Dolezilek and T. Tibbals, "Communications Technologies and Practices to Satisfy NERC Critical Infrastructure Protection (CIP)," Proceedings of the 5th Annual Power Systems Conference, Clemson, SC, March 2006.

[16] D. Dolezilek, "Methods for Securing Substation LAN Communications," Proceedings of the 5th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2003.

XII. Biographies

Dwight Anderson received his Bachelor's degree in Electrical Engineering from Steven's Institute of Technology. He is now the security product manager for Schweitzer Engineering Laboratories, Inc. in Pullman, Washington. Prior to joining SEL in 2005, he worked twenty years for Hewlett-Packard as an aerospace and defense business development manager and systems engineer working on projects ranging from electronic warfare countermeasures to SCADA system programming. He recently became a member of the FBI InfraGard forum regarding the exchange of information related to critical infrastructure protection. He has received his Global Information Assurance Certification Security Essentials Certification (GSEC) for IT managers and security professionals. He has published a number of technical articles and most recently published an article in the UTC Journal regarding the effect to SCADA channel bandwidth when adding encryption.

Garrett Leischner is a product engineer with Schweitzer Engineering Laboratories, Inc. Automation Integration and Engineering Division, where he manages the Rugged Computing Platform. Prior to joining SEL, he worked for Cray, Inc. Garrett received his BA in Business from Western Washington University in 2003, and his MS in Computer Engineering from the University of Idaho in 2006. He is an active member of the IEEE Computer Society, Association for Computing Machinery, and the Software Engineering Institute, and has several patents pending. During his time at SEL, he has co-authored several technical papers and instructional courses.

20071214 • TP6310-01