Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions

Paul Oman, Edmund O. Schweitzer, III, and Jeff Roberts
Schweitzer Engineering Laboratories, Inc.

Presented at the
InterNational Electrical Testing Association 2002 Technical Conference
New Orleans, Louisiana
March 24–27, 2002

Originally presented at the
3rd Annual Western Power Delivery Automation Conference, April 2001

SAFEGUARDING IEDS, SUBSTATIONS, AND SCADA SYSTEMS AGAINST ELECTRONIC INTRUSIONS

Paul Oman, Edmund O. Schweitzer, III, and Jeff Roberts
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

ABSTRACT

United States agencies involved with national security are concerned about the vulnerability of the North American electric power grid to electronic intrusions, commonly known as cyber attacks. Several studies have identified changing socio-economic conditions that increase the probability of an electronic, computer-based attack being launched against a utility or substation, causing regional and possibly even widespread power outage. Increased domestic and international terrorism throughout North America, industry deregulation causing instability in the electric power utility job market, the shift to open protocols and interconnected computer networks, and the growing population of computer literate people with abundant and widely available hacker tools are factors contributing to this rising threat. The problem is compounded by industry's shift from discrete, manual substation control to increased reliance on automated, integrated networks of IEDs, controllers, and SCADA systems.

In this paper we identify and discuss technologies and procedures for safeguarding IEDs, PLCs, substation controllers, and networked SCADA systems against electronic intrusions. We show how technologies for access restrictions, audit logs, authentication, encryption, nonrepudiation, modem and network security, and network topologies can reduce vulnerability and increase survivability of integrated solutions for protection, metering, and SCADA. We discuss mitigating actions to reduce legal liability and outline training needs for increased awareness in the electric power industry. By creating the means to prevent, or at least to detect and survive, electronic attacks, we can ensure the continued safety and reliability of the electric power infrastructure.

INTRODUCTION

The White House and agencies concerned with national security are now aware of the risk of electronic intrusions, also known as cyber-attacks, and the subsequent vulnerability of the North American electric power grid. The IEEE standard governing substation security [1] defines *electronic intrusions* as:

> "Entry into the substation via telephone lines or other electronic-based media for the manipulation or disturbance of electronic devices. These devices include digital relays, fault recorders, equipment diagnostic packages, automation equipment, computers, PLC, and communication interfaces."

Studies commissioned by the White House, FBI, and North American Electric Reliability Council (NERC) have identified several socio-economic factors that increase the probability of an electronic, computer-based attack being launched against a utility or substation, causing regional and possibly even widespread power outage [1, 2, 3, 4]. Contributing factors to this rising threat include increased domestic and international terrorism throughout North America, industry deregulation causing instability in the electric power utility job market, the shift to open protocols and interconnected computer networks, and a growing population of computer literate people

with an abundance of widely available hacker tools. The industry's shift from discrete, manual substation control to the increasing reliance on automated, integrated networks of IEDs, controllers, and SCADA systems compounds the problem and may amplify the damages from malicious electronic intrusions unless these attacks are prevented or, at least, detected and isolated. A complete discussion of the documented concerns on electric power system intrusions can be found in Oman, et al. [5].

Motivations for electronic attacks against electric power systems may follow the same patterns seen in attacks on Internet E-commerce sites. They can be categorized into five broad groups:

1. **Hackers** are computer users who access unauthorized systems *simply because they can*. The relatively benign hacker is motivated by curiosity or the challenge of exploration, without overt malicious intent. Others are malicious with the intent of gaining notoriety or causing damage.

2. **Espionage** is the act of gaining industrial or political advantage by information gathering through both legal and illegal means. Much espionage gathers information through publicly available resources such as web pages, product descriptions, and promotional literature. Other espionage activities include insider access, theft, and illegal surveillance to acquire confidential information.

3. **Sabotage** is usually rooted in desires for personal, economic, or political gain caused through the destruction of your competitor's assets, organizational structure, and/or market share. "Hactivism" is an emerging form of sabotage where hackers deface or damage corporate Information Technology (IT) assets in the name of some radical cause.

4. **Electronic Theft** is the theft of credit and/or personal identity information, frequently stored in corporate IT systems, that can be used in subsequent fraudulent schemes. Losses in the U.S. alone are estimated to be billions of dollars.

5. **Vandalism** is the destruction of property value without personal gain, as distinct from sabotage because it is typically haphazard, random, and relatively localized.

Emergency services and infrastructure are not immune to these attacks. In a case in California, a hospital was electronically harassed over a two year period by a hacker who blocked incoming emergency 911 calls, connected outgoing calls to incorrect locations, and placed bogus emergency calls [6]. Further, because of the interrelated nature of infrastructure and utility services, an attack on one service can disable other services. In Massachusetts, for example, a hacker's attack on the phone system not only shut down phone services (including emergency 911 calls), but disabled the local airport control tower, weather service, radio transmitters, and runway lights [7]. Fortunately, there have been no documented instances of electronic intrusions causing outages or damage to the electric power grid, but there have been cases where individuals and radical groups have targeted electric power and telecommunications utilities:

- In several instances worldwide, hackers have attacked electric utility IT systems looking for credit information [2].
- At an undisclosed U.S. location, a radical environmental group was caught hacking into an electric utility IT system [2].
- In another unspecified U.S. location, hackers subverted an electric power company server in order to play games, consuming 95 percent of the server's resources and denying access to legitimate users [8].
- In Texas, a disgruntled ex-employee of an electric utility posted a note in a hacker journal that his knowledge of the system could be used to shut down the regional power grid [2].

Unfortunately, it is not clear whether electronic attacks on the electric power grid have not occurred or have simply not been reported. In their *Electric Power Risk Assessment* report the National Security Telecommunications Advisory Committee (NSTAC) cited findings that only 25 percent of electric power utilities use electronic intrusion detection systems and that less than 17 percent would report an intrusion incident [2]. Consequently, reports from the White House, FBI, NSTAC, NERC, and IEEE conclude that remotely accessible IEDs, controllers, and SCADA systems–and more importantly, substations controlled by those devices–are vulnerable to electronic attack [1, 2, 3, 4]. This vulnerability was recently brought to the public's attention by a PBS special on hackers, where one of the interviewees admitted that electric power control systems were certainly vulnerable [9]. Physical intruders have randomly and/or maliciously pushed buttons and operated circuit breakers, reclosers, and switches [1], so we must presume that electronic intruders would do the same. Because of the nature of the systems controlled by electronic substation IEDs, misuse of those devices could have disastrous consequences.

In this paper we identify and discuss technologies, procedural mechanisms, and personnel issues useful in safeguarding IEDs, PLCs, substation controllers, and networked SCADA systems against malicious electronic intrusions. We show how technologies for access restrictions, audit logs, authentication, encryption, modem and network security, and network topologies can be combined to reduce vulnerability and increase survivability of integrated solutions for protection, metering, and SCADA. We discuss mitigating actions to reduce legal liability for intrusions, and we reference training needs for increased awareness in the electric power industry for creating the means to prevent (or detect and survive) electronic attacks.

THREATS AND RISKS

As with all infrastructures, threats to electric power systems have existed for as long as the technology has been used to support that way of life. But these threats are not static or unchanging. We should assume that as the infrastructure technology changes, so do the threats and risks associated with supporting that service.

Threats

Following is a list of potential threats to the North American power grid as identified by White House subcommittees, NIST, and the IEEE [1, 2, 3, 6]:

- Natural Disasters and Events
- Accidental Physical Damage
- Physical Maintenance and Infrastructure Deterioration
- Terrorism and Sabotage
- Vandalism
- Blunders, Errors, and Omissions
- Threats to Personal Privacy
- Disgruntled Employees and Ex-employees
- Malicious Hackers
- Recreational Hackers
- Hacktivists
- Malicious Code and Viruses
- Information Warfare
- Foreign (state sponsored) Intelligence Gathering
- Industrial and Foreign Espionage
- Insiders and Associates
- Fraud and Theft
- Economic Conditions
- Labor Conflicts
- Civil/Political Unrest
- Curiosity and Ignorance
- Use of Adjacent Property
- Joint-Use Facilities
- Aesthetics

Risks

In recent years several factors in North America have combined to increase the risk of electronic attack on electric power services. These threats involve changing social, political, and technological issues:

1. The expanded use of public protocols to interconnect protective equipment and SCADA systems (e.g. TCP/IP and UCA over Ethernet LANs/WANs).
2. Increased dial-in and network access to remote sites through public communication services (e.g., public phones, Internet).
3. Instability in the electric power utility job market, creating disgruntled employees and ex-employees, caused by deregulation and mergers.
4. Increased competition for electricity generation and T&D services creating pressure to downsize, streamline, automate and cut costs, also causing disgruntled employees and ex-employees.
5. Instability in the electric power service, caused by deregulation and increased competition, creating disgruntled customers.
6. Increased public access to transmission system data mandated by FERC 888/889.
7. Increased terrorism worldwide and increased foreign government-sponsored terrorism and information warfare targeted against North America.
8. Rapid growth of a computer-literate population and widespread dissemination of hacker tools.
9. Increased electronic theft, recreational hacking, and hacktivism (i.e., the destruction of electronic assets for a political or socioeconomic cause).

Evidence of the increasing threat against electric power systems can be seen in the recent attack on an electric power company's information servers. Although it was not a malicious attack, the "game-playing" activities of the intruders consumed 95 percent of the available computing resources of the servers, so the utility's legitimate users could not access their own systems. Two disturbing aspects about this incident are the recognition that a segment of our society views these attacks as games, and that law enforcement authorities have little chance in identifying or prosecuting culprits. The attitude of many people that hacking is a relatively benign game is evident in most, if not all, hacker web sites and email postings. The "us-versus-them" attitude can be seen in the following excerpt from a hacker news article posted after the power company's servers had been hacked [10]:

> "The network in question was stupidly configured for anonymous FTP login with read and write privileges, pretty much a welcome mat for anyone in cyberspace…The incident occurred because hopelessly incompetent network administrators essentially left the door open, the lights on, and set out milk and cookies for their anonymous guests…with no access control whatsoever in place, there isn't any digital 'No Trespassing' sign in evidence."

Detection and Culpability

The fact that law enforcement agencies have little chance in establishing blame and successfully prosecuting is evident in the staggering losses already incurred by U.S. commerce (estimated at $45 billion in 1999) and the exponentially increasing caseload of the FBI's computer crime division [11, 12]. The number of open cases is growing far faster than the FBI can begin to

investigate them. The problem is exacerbated by lack of funds, trained personnel, and the U.S. economy's rush to provide Internet services [12, 13].

Figure 1, adapted from an anti-terrorism infrastructure threat matrix [14], contains an electric power system threat mode analysis contrasting type of attack (physical vs. electronic) against the target of the attack (physical vs. electronic). Physical attacks are the nominal terrorist activities, while electronic attacks refer to computer-based intrusions for purposes of sabotage. In the same manner, physical targets are your equipment and hard assets, while electronic targets are digital assets like data, information and control systems, and equipment settings.

		Attack Target	
		Physical	Electronic
Attack Method	Physical	Physical theft/sabotage of generation, T&D, or protection equipment. **(A)**	Physical theft/sabotage of information, data, or intellectual property. **(B)**
	Electronic	Electronic sabotage of equipment causing malfunction, system degradation, and/or loss of service. **(C)**	Electronic theft/sabotage of information, data, or intellectual property. **(D)**

Figure 1 Physical vs. Electronic Threat Mode Analysis

The matrix cells in Figure 1, labeled A through D, have varying degrees of difficulty when it comes to detection and establishing culpability. Cell A, the most prevalent means of attack on the most common targets today, is normally the easiest to detect and also the easiest to gather evidence for culpability and prosecution. Similarly, Cell B represents the physical destruction or theft of digital assets, which is similar to A, but slightly more difficult for establishing culpability and prosecution. The most difficult aspect of legal cases involving loss of digital assets is establishing the value of the stolen/damaged property. Cells C and D, however, represent the electronic sabotage of physical equipment and digital assets, respectively. These cells represent cases that are extremely difficult when it comes to establishing culpability and pursuing effective prosecution. With a physical attack you have physical evidence of who the attacker is, but with an electronic attack it is trivial to obfuscate the attack path and attacker identity. Likewise, with a physical attack you usually have immediate and obvious damage that can be detected and fixed. But with an electronic attack you may have theft without damage, or subtle setting changes that do nothing more than cause system deterioration over time. In either case it is much harder to detect the intrusion because there is no physical damage to observe. Finally, note that the most insidious form of electronic attack–a coordinated many-on-many attack–is also the hardest to diagnose and establish culpability. A few individuals determined to disrupt power services could launch a coordinated attack on electric power systems, using the same techniques that crippled U.S. E-commerce sites in February 2000.

VULNERABILITIES

The increased use of computer-based systems for electric power control and protection has created a parallel between the vulnerabilities of the power grid and those seen in complex

computer networks. IEEE Standard 1402-2000, *Guide for Electric Power Substation Physical and Electronic Security*, states [1]:

> "The introduction of computer systems with online access to substation information is significant in that substation relay protection, control, and data collection systems may be exposed to the same vulnerabilities as all other computer systems. As the use of computer equipment within the substation environment increases, the need for security systems to prevent electronic intrusions may become even more important."

Fortunately, the vulnerabilities of computer networks are well known and documented, and the myriad of techniques and procedures used to protect computer systems can be adapted to safeguard electric power systems against electronic intrusions. All remote electronic access points to power systems control and protection equipment are vulnerabilities. That is, wherever dial-in or network access points exist, they can be exploited by electronic intruders. Figure 2 shows vulnerable electronic access points in a hypothetical substation configuration.

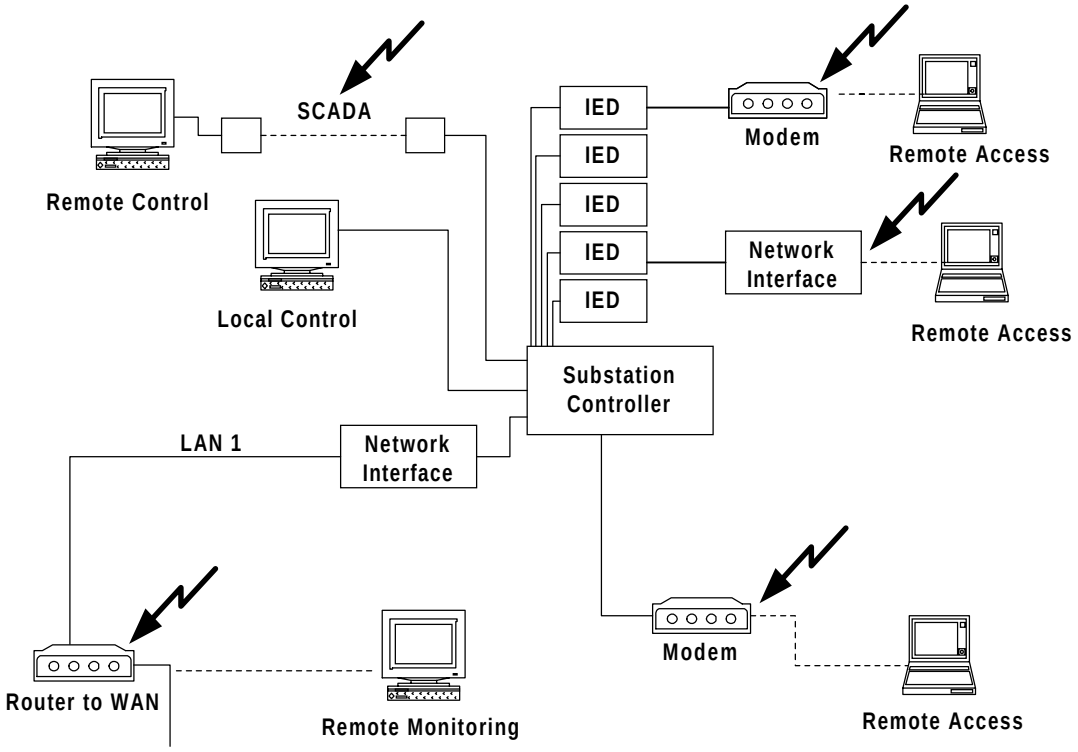

Figure 2 Electronic Intrusion Vulnerabilities

It is clear from Figure 2 that multiple vulnerabilities exist when implementing remote access to IEDs, controllers, and SCADA systems. What is not obvious is the different nature of the risk involved with each point of access. For example, an electronic intruder who gains access to a communications processor with control over a multitude of IEDs is much more threatening than the intruder who hacks into a single IED. Likewise, the hacker who gains control over a SCADA system can do far more damage–and more widespread damage–than the person who intrudes into a substation controller. Table 1 shows a listing of the vulnerabilities and risks involved in remote access to protective equipment (e.g., IEDs, PLCs, reclosers) and SCADA equipment. For simplicity, RTUs and communications processors are treated as components of a SCADA system.

Table 1 Equipment Vulnerability Matrix

Equipment	Vulnerable Point of Access	Risk
Protective devices w/o remote access (e.g. relays, IEDs, PLCs, reclosers)	• Local access to protective devices • Local access to protection settings	• Protective equipment accidentally or deliberately damaged • Protection settings accidentally or deliberately altered
Protective devices with remote phone access	• Electronic access to protective devices via modem or codec • Electronic access to protection settings	• Dial-in number accessible via social engineering or automated modem scan • Access control circumvented by password attack • Protection settings accidentally or deliberately altered
Protective devices with remote network access	• Electronic access to protective devices via system port or network address • Electronic access to protection settings • Electronic access to data packets • Equipment vulnerable to Denial of Service (DOS) attacks	• Network address accessible via social engineering or automated network port/IP scan • Access control circumvented by password attack • Protection settings accidentally or deliberately altered • Data packets visible on the network • Equipment inaccessible, and possibly non-functional, during DOS attacks
SCADA equipment with remote access via private network	• Physical access to SCADA system • Electronic access to subordinate protection equipment • Electronic access to protection settings	• SCADA system accidentally or deliberately damaged • SCADA functions accidentally or deliberately altered • Protection settings accidentally or deliberately altered
SCADA equipment with remote phone access	• Electronic access to SCADA system via modem or codec • Electronic access to subordinate protection equipment • Electronic access to protection settings	• Dial-in number accessible via social engineering or automated modem scan • Access control circumvented by password attack • SCADA functions accidentally or deliberately altered • Protection settings accidentally or deliberately altered
SCADA equipment with remote network access	• Electronic access to SCADA system via system port or network address • Electronic access to control and data packets • Electronic access to subordinate protection equipment • Electronic access to protection settings • SCADA vulnerable to DOS attacks	• Network address accessible via social engineering or automated network port/IP scan • Access control circumvented by password attack • SCADA functions accidentally or deliberately altered • Protection settings accidentally or deliberately altered • Control and data packets visible through a network sniffer • SCADA inaccessible, and possibly non-functional, during DOS attacks

ATTACKS AND CONSEQUENCES

Attack Scenarios

Electronic attacks concentrate on system vulnerabilities, and attack characteristics are based on the characteristics of the vulnerability being exploited. Following are six example attack scenarios showing how insiders and outsiders could exploit the vulnerabilities listed in the previous section.

Attack Scenario #1: Using insider information, a disgruntled employee or ex-employee, with a grudge against a generation facility or T&D provider accesses protective equipment (either physically or electronically) and changes settings such that the equipment either (a) fails to operate when it should, causing bus, line, or transformer damage, or (b) operates when it shouldn't, causing service interruption.

Attack Scenario #2: Using a war-dialer (a program to control a modem for automated attacks), a disgruntled customer scans hundreds of phone numbers above and below the utility's publicly available phone numbers, looking for answering modems. When a connection is found, multiple returns, question marks, "HELP," and "HELLO" are entered to probe the connection and look for clues as to the kind of connection. Once a login dialog is acquired the intruder uses *social engineering* to determine login information, or launches a *dictionary-based* or *brute-force* password attack. When the connection is complete, the intruder is "inside" the IED, controller, or SCADA system. Data can then be altered or destroyed, communications can be blocked or rerouted, and settings can be changed deliberately or randomly. The state of the equipment and service is in jeopardy.

Attack Scenario #3: A disgruntled customer or ex-employee uses a port scan or ping-sweep program to identify active system ports and/or network IP addresses belonging to a public utility. When an active connection is found, multiple returns, question marks, "HELP," "HELLO," and "LOGIN" are entered to probe the connection and look for clues as to the kind of connection. Once a login dialog is acquired the intruder uses insider information, social engineering, or a password attack to gain access to the system. Once again, all data, communications, and settings are vulnerable, so equipment and service is jeopardized.

Attack Scenario #4: An employee with access to computer information services is duped into installing or running a computer "game" or otherwise seemingly innocuous application by a friend, ex-employee, supervisor, vendor, or virtually anyone with legitimate connections to the employee's company. The installed computer application contains a Trojan horse program that opens a backdoor into the computer network. The inventor of the Trojan horse program, automatically notified that the backdoor is open, gains access to the system to retrieve and exploit inside information enabling him or her to access SCADA systems and protective equipment. The computer information system (e.g., control commands and metering data) and all systems subordinate to it are now in jeopardy.

Attack Scenario #5: An employee, inside service provider, or vendor representative with privileged information is approached by an unscrupulous competitor or foreign agent. The employee is bribed or duped into sabotaging systems and settings or creating access mechanisms the agent could use for subsequent activities that jeopardize equipment and services.

Attack Scenario #6: An unscrupulous competitor, foreign agent, or network service provider uses public information and social engineering to obtain network traffic patterns for TCP/IP packets moving between supervisory stations and remote protective equipment or metering

equipment. A network analyzer or "sniffer" is attached to the network line to show the content of all data packets between the supervisory and remote equipment. The unencrypted data packets contain control and settings information that can be used in subsequent attacks on either the SCADA system or the protective equipment.

Results and Consequences

As implausible as these attack scenarios seem, the computer network and telecommunications industries have already experienced these types of attacks, so it is probable that the electric power utilities will experience similar intrusions. Dictionary and brute-force password cracking programs are fast enough to attempt tens of thousands of passwords in just a few hours over a fast phone line or a slow network connection [5, 15]. Over fast network connections, and when encrypted passwords can be downloaded to a dedicated machine, millions of password combinations can be tried in a matter of hours. Using these techniques, if an electronic intruder gained access to substation control or protective systems, the intruder could then:

- Shut down the substation or any portion of the subsystem controlled by the compromised device, either immediately or in a delayed manner.
- Change protection device settings to degrade reliability of the device and, subsequently, the electric service provided by the substation.
- Gather control and protection settings information that could be used in a subsequent attack.
- Change or perturb the data in such a manner as to degrade electric service or cause loss of service.
- Plant malicious code that could later trigger a delayed or coordinated attack.

Further, if an electronic intruder gained access to an electric utility SCADA system, the intruder could then do all of the above, plus:

- Shut down the regional service controlled by that SCADA system, either immediately or in a delayed manner.
- Steal or alter metering data gathered by the SCADA system.
- Use the SCADA system as a backdoor into the corporate IT system to obtain customer credit and personal identity information commonly used in electronic theft.

Network Topology Influences Risk

The communications system shown in Figure 3 illustrates how system topology defines your system vulnerabilities and dictates your concerns for security risks. In this example system, we show a single network line (L_1) from a data communications packet switch to the Internet service provider, with access to outside lines ($L_2 \ldots L_n$). The purpose of the packet switch is to route data packets and filter out undesired access attempts (e.g., a firewall), thereby controlling access to each of the internal hubs. Each hub in turn is connected to protection equipment and SCADA devices, like IEDs and a substation controller/PC.

The data packet switch shown in Figure 3 protects the subnets by controlling access to each hub. This means that the devices connected to Hub_1 are isolated from the devices on other hubs.

Security isolation between the devices connected within a hub does not exist because the bus topology allows all devices to have access to all data packets within a hub subnet. Hence, if you connect a modem or network interface with an outside line to any of the devices within a hub isolated subnet, you have compromised the security of the entire subnet. For example, anyone gaining access to the Hub_1 PC can listen to and monitor all data packets within the hub. Allowing external connections in this manner eliminates the controlled isolation provided by the data communication packet switch.

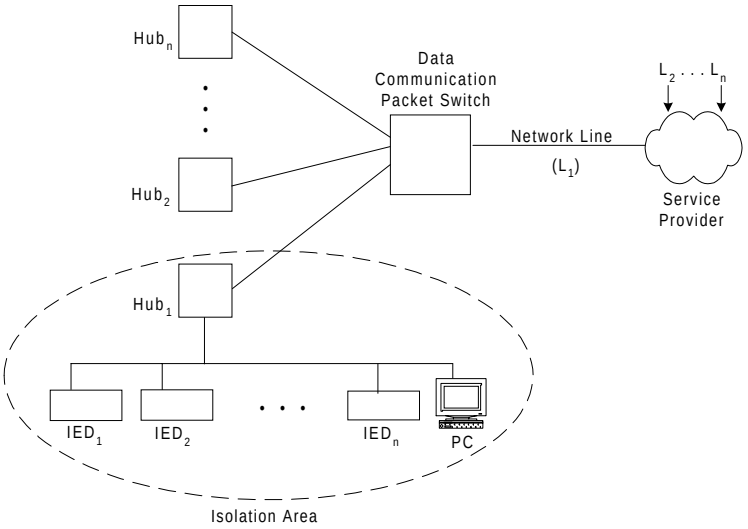

Figure 3 Isolated Subnets Increase Security

In the system shown in Figure 3, the data communications packet switch provided security for each of the hub subnets subordinate to it, but it did nothing to address the security of the data being transmitted to and from the network service provider. We still must consider data security transmittal over public telephone and Ethernet networks (e.g., the Internet). Figure 4 illustrates one common means by which someone with malicious intent can gain access to your unprotected substation data and information. The goal is to communicate information from the substation to the User's office. The communications path must pass through the switching network in the local phone company's central switching office. Electronic intrusions against telephone switching centers can be traced back over 20 years and are as common today as hacker attacks against corporate IT systems. If someone gains access to the phone company network switching computer, it is then a relatively easy task to listen to, or reroute, the data traffic on any public phone line. In a similar manner, a successful hacker attack on an Internet Service Provider (ISP) gives the intruder access to all the data packets flowing into and out of that ISP.

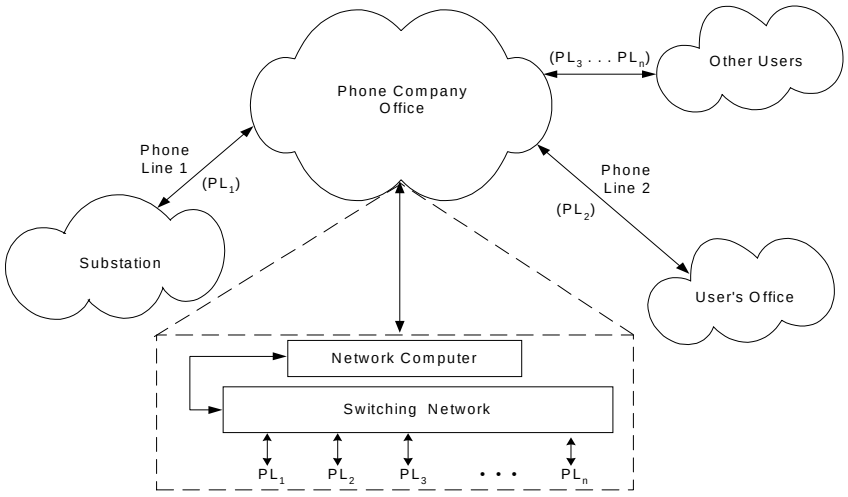

Figure 4 Tapping Phone Communication By Hacking Telephone Switchgear

MITIGATION

Modern configurations of electric power control systems and protection devices are essentially systems of distributed intelligent devices resembling networked computing systems. Typical ways to manage computer intrusions involve authentication of communicating partners, securing the connection between sites, encrypting the data communication between sites, and identification and remediation of intrusions if and when they penetrate the network. Fortunately, there are several techniques and processes that can be used to safeguard IEDs, PLCs, RTUs, controllers, communications processors, SCADA systems, and virtually every type of programmable digital device used in electric power systems control and protection. The cornerstone to all network security is access restriction and user authentication. Beyond that we are concerned with safeguarding the communication packets from prying eyes, via encryption, and verification of packet transmission and reception (nonrepudiation). Table 2 contains a synopsis of technologies to safeguard network equipment, ordered by increasing cost and/or complexity.

Access restriction should be both physical and electronic. Physical access restriction is commonplace and will not be discussed here. Electronic access restriction is easily implemented via password or Personal Identification Number (PIN) keyed to systems, individual computers, digital devices, databases or database records. If there is a one-to-many mapping between password or PIN and users, such that a whole group of users have the same password or PIN, then you have implemented a simple access restriction technique.

User authentication occurs when there is a one-to-one mapping between the user and his or her authentication mechanism. For example, entering a unique Password or PIN in order to gain access to the system, device, database, or data record being protected allows the protection system to authenticate that person as a legitimate user. There are three factors of user authentication mechanisms–knowledge, physical, and biological–which are commonly referred to as the (1) “What you know,” (2) “What you have,” and (3) “What you are” factors. A password or PIN falls in the first factor, a SmartCard or similar device falls in the second factor, and fingerprints or other biologic characteristics fall in the third factor.

The strength of your user authentication is a function of the number of factors used in the authentication process. For years, single-factor authentication was considered “adequate” for

computing systems, but with increased E-commerce and the corresponding increase in electronic theft, many systems are now using two-factor and even three-factor authentication. Two-factor authentication requires authentication mechanisms from two vectors, and three-factor authentication requires authentication in all three vectors. Two-factor authentication is common in E-commerce (your credit card and PIN, for example), and three-factor authentication is often used for access to critical military and proprietary systems (e.g., a Password, SmartCard, and fingerprint).

Table 2 Equipment Mitigation Tools and Techniques

Tool/Process	Purpose	Cost	Scalable?–Programmable?	Ease of Use
Device-based passwords/Pins	Access control	NA	Via custom programming.	Use and programming trivial.
Password generators	Software that generates strong passwords	Free–low cost	Via custom programming	Trivial to use; nontrivial to program.
Audit logs	Record device or system access	NA	Via system features or custom programming	Trivial to use; nontrivial to program.
ID devices	Hardware authentication	$2–$100 per unit; > $1000 for network servers	Via server license & host platform.	Trivial to use; nontrivial to program.
Biometrics	Strong single-factor ID, or two-factor ID	$200–$1000	Via custom programming on host.	Trivial to use; nontrivial to program.
Modem key/lock	Secure modem connections	$150 per pair	Any number of keys per lock; key codes are user selectable.	Use and programming trivial.
Secure modems	A. Programmable Secure Modem B. Encrypting Modems	$250–$600 each	A. Programmable user accounts that validate incoming calls. B. Handshaking security that works only in pairs.	Trivial to use; programming difficulty varies.
Virtual Private Network (VPN) devices	Hardware network security	~$2000 pair	Only work in pairs	Use and programming nontrivial
Firewalls	A. Software network filter B. Hardware network gates	A. Free–$5000+ B. $1200–$26000	NA	Use and programming nontrivial
Intrusion Detection Systems (IDS)	System anomaly and/or intrusion signature detection	Free– $50000	Few are scalable	Use and programming nontrivial
Public Key Infrastructure (PKI)	Authentication and secure network communications	Free– $10000	Inherently scalable	Use and programming nontrivial

Audit logs are used to record instances of valid and invalid user authentication and session termination (among other things), so that a record of activity exists for every system access, or attempt at system access. Audit logs are indispensable when diagnosing and prosecuting cases of electronic intrusion.

ID devices are (usually) electromagnetic mechanisms that furnish authentication information from the physical ("What you have") vector. For example, credit and debit cards, SmartCards, magnetic strips, barcodes, and embedded ID chips are all electromagnetic ID devices. One major advantage of using an ID device to augment user passwords or PINs is that the automated authentication via random keycode may only be valid for a short period of time before a new keycode is generated. "Use-once" keycodes change periodically and are not valid for very long past the original transmission, so keycodes transmitted across the network cannot be captured by persons listening in on the line and reused at a later time.

Biometrics are authentication measures or mechanisms that fall into the third authentication vector, "What you are." Fingerprints are the most commonly used. Fingerprinting devices are now available for less than $200, complete with software systems to create and maintain a database of users' fingerprints. Retinal eye scans, voice prints, face recognition systems, and other biological measurements are also used for multifactor authentication. Application limitations are usually based on cost and/or complexity.

Secure modems come in a variety of types and complexities. Simplest are modem key/lock combinations that work in pairs to ensure that all communication is conducted between similarly configured pairs (or groups) of modem devices. An authenticated connection is established by the keyed handshaking that occurs when the connection is established; data transmission is not encrypted beyond the normal compression needed for high-speed modem communication. Next are programmable modems with on-board security features that enable creation of user accounts, complete with assigned passwords and dial-out phone numbers. Again, security is limited to authentication upon initial connections, and data packets are not encrypted. Finally, secure encrypting modems have recently been introduced with embedded, secret keys that only work between pairs (or groups) of similarly configured modems. Encrypting modems use both secure authentication and secure data transmission, to safeguard against eavesdropping on public phone lines.

Encryption safeguards the communicated data packet while in transit from source to destination, so that prying eyes cannot read it. Unencrypted data communications over phone or network lines are susceptible to phone taps and network sniffers, respectively. For example, a TCP/IP packet or UCA packet transmitted raw (unencrypted) is visible to anyone on the network running a network analyzer in promiscuous mode or someone who spoofs (pretends to be) the destination address. Fortunately, both TCP/IP and UCA permit encrypted data packets. Unfortunately, few electric power service providers are using this capability.

Encryption techniques can be grouped into three broad categories: a) secret key algorithms known only to the transmitter and receiver, b) private keys used in symmetric public encryption algorithms, and c) public/private key pairs used in asymmetric public encryption algorithms. Secret key encryption is typically based on reversible hashing or ciphering algorithms. Symmetric encryption uses a private key to encrypt the message using a public encryption method so that anyone knowing your private key can decipher the message. The Data Encryption Standard (DES) is a commonly used symmetric encryption technique. Asymmetric public encryption, like the popular RSA algorithm, uses two keys, one public and one private, so that anything encrypted with your private key can be deciphered with your public key. Similarly, anything encrypted with someone else's public key can only be deciphered with that person's private key. Private keys cannot be derived from the public key, so two-way secure communication is possible.

For point-to-point secure communication you obtain the recipient's public key, encrypt your message and, because the message can only be deciphered via the recipients private key, you can

transmit it over public lines. Alternatively, for secure multipoint broadcasts you can encrypt your outgoing message with your private key and broadcast it to all holders of your public key. Anyone knowing your public key can decipher your broadcast, so restricted distribution of your public key provides convenient multipoint communication, without jeopardizing your secure point-to-point encryption.

Public Key Infrastructure (PKI) provides a means of issuing and revoking public keys and public key certificates via a Certificate Authority (CA) responsible for verifying the correct ownership of public keys. PKI enables authentication, encryption, and nonrepudiation services via asymmetric public key cryptography. A lengthy discussion of PKI public key encryption is beyond the scope of this paper, but there are many excellent papers and books describing the subject [16]. Through appropriate use of cryptography and cryptographic algorithms, it is possible to achieve private communications with improved assurance of communicating partner identity, and nonrepudiation technology to verify the message was transmitted and received correctly. However, designers of integrated substation solutions and SCADA systems may find that PKI solutions are too slow for supervisory control and power system protection. Single key (i.e., hash algorithms) may be needed in time critical applications, leaving PKI for advisory and informational applications over the public network.

Network Topology is a crucial factor in determining the security of your network accessible IEDs and your SCADA and IT systems. Star network topologies with point-to-point home-run lines and no modem connections or public network gateways are the most secure and reliable. Ring topologies suffer from the "one-down, all-down" single point of failure vulnerability, and bus topologies are insecure because all devices have access to all data packets on the bus. Unfortunately, Ethernet, the most widely used LAN technology, is a bus topology that permits any device connected to the hub to "see" the data packets meant for all other devices. Fortunately, Ethernet standards exist for star topologies (i.e., IEEE 802.3) and when devices are connected to a switch, rather than a hub, the packet switch ensures that each device only receives the data that was specifically addressed to it.

Firewalls are often used to defend a site against external network intrusions. A firewall is a protected gateway that stands between the resources requiring protection and the "outside." Firewalls create segmented networks with restricted access into and between segments. By setting up layers of segmented, restricted subnets, even when a hacker penetrates one layer they only have access to the data and systems within that segment. A firewall can be implemented via a router that filters out undesired traffic, or through more complicated combinations of hardware and software solutions.

To be effective, a firewall must guard *all* access to the internal network, including modem connections and remote network access. Internet Protocol Security (IPSec) and Virtual Private Networks (VPNs) are closely allied technologies that provide the means to protect communications between physically distant sites. IPSec uses encryption to safeguard data and embed authentication information in TCP/IP packets.

A **Virtual Private Network** (VPN) combines IPSec technology and firewalls to form a point-to-point secure, encrypted connection over public networks, so that from a privacy standpoint it appears to be a single internal network. This is often referred to as "tunneling." By encapsulating data packets within other protocols that permit encryption and allow point-to-point addressing, you can send secure packets from one firewall to another, across a public network. VPNs can be implemented via either software or hardware. VPN boxes are hardware devices that transmit and receive secured, encrypted network packets from similarly configured routers.

An **Intrusion Detection System** (IDS) can be a useful way to identify both internal misuse and external attackers attempting to gain internal access. The intent is to determine if insiders or external users are misusing the system. There are two types of IDS: signature detection systems and anomaly detection systems. Intrusions often have attack signatures (similar to virus signatures) that are patterns associated with misuse of the system. Signature detection systems match known, observable intrusion characteristics against a database of intrusion profiles and, based on sensitivity settings, determine if a match is likely. The goal is to recognize the attack signature as it unfolds and shut off the attack or notify the system administrator that an attack is occurring. Anomaly detection compares ongoing system behavior against a profile of normal system behavior and warns when anomalous behavior is occurring. For example, an IDS might notice unusually high activity during the middle of the night, or overseas external users with a high volume of disk I/O. When abnormal activity occurs the IDS may shut it down and/or inform the system operator.

Both types of IDS have different advantages and disadvantages, but they both have the same common problem which is setting the sensitivity [17]. Too sensitive a setting generates false positive warnings, or false alarms when there is no intrusion. In essence the IDS cries wolf which distracts and overburdens your systems staff who must respond to each warning as if it were an actual intrusion. Too insensitive a setting generates false negatives, or misdiagnosed, actual intrusions. These are actual intrusions that have gone unnoticed.

RECOMMENDATIONS AND CONCLUSIONS

Once familiar with electronic intrusion techniques and countermeasures, electric power generation and T&D utilities can assess their vulnerabilities and take steps to mitigate their risks. Government agencies suggest that there is a certain degree of urgency in "hardening" our infrastructures against electronic attacks, so this issue does need to be addressed in a timely fashion. The White House report on critical infrastructure protection [3] recommended three immediate steps to secure network-based infrastructure:

> "We suggest consideration of these immediate actions prior to the completion of a formal risk assessment: (1) Isolate critical control systems from insecure networks by disconnection or adequate firewalls, (2) Adopt best practices for password control and protection, or install modern authentication mechanisms, and (3) Provide for individual accountability through protected action logs or the equivalent."

As shown in the previous section, a variety of tools and techniques are available to mitigate risk associated with electronic intrusions into computer-based networks controlling electric power generation, transmission, and distribution. Recommendations for securing IEDs, communications controllers, and computer based SCADA and IT systems were compiled from the literature and are summarized below:

- Use passwords, PINs, data access restrictions, and other means of user authentication to guard against unauthorized access to protective equipment and SCADA systems. Match the strength of your user authentication to the criticality of the data being protected. Two-factor, and even three-factor, authentication may be appropriate for access to critical SCADA systems.
- For single-factor authentication, passwords are better than PINS because the increased permutations of characters makes them harder to crack. Use strong passwords of six or more characters with mixed case and special characters. Do not use common words, acronyms, or personal information like birthdays and names that can be cracked.

- Change passwords periodically (e.g., monthly or quarterly) and change them immediately after instances of contractor installation and maintenance, after suspected intrusions, and when personnel turnover or strife increases insider risk.
- Use different passwords in differing locales, equipment, and systems; do not be tempted by single sign-on ease of use. Ensure that passwords are issued and controlled locally, and not widely distributed.
- Teach password security and monitor compliance; use password generators and in-house password crackers to eliminate weak passwords.
- Issue alarm contacts for access, password, and settings events. Monitor alarms for intrusion detection and to verify device functionality. Automate alarm responses with preprogrammed disconnects, auto-dial warnings, and increasing audio and visual alarms.
- Log alarms and suspicious activity (e.g., failed password attempts) in nonvolatile storage. Scan audit logs and files regularly.
- Use private communications lines when possible to limit public eavesdropping and potential intrusions. When using public lines encrypt access and control information such as passwords.
- Implement access hierarchies with different levels of permission for viewing and setting devices. Use segmented network topologies and/or star topologies to increase survivability and avoid "one down, all down" vulnerabilities.
- Secure SCADA and IT systems with virus scanners, firewalls, and intrusion detection systems.
- When communicating over the Internet, use VPN or PKI technology to authenticate partners and secure data packets.
- Keep communications systems design and network access information private.
- Use "warning banners" to discourage electronic intrusions and enable electronic monitoring and trespass prosecution.
- Use secure dial-back, encrypting, or authenticating modems or modem-keys.
- Terminate interactive sessions after long periods of inactivity and ensure that open ports are properly closed so the next user does not inherit unauthorized access privileges.
- Limit the number of failed attempts to enter a password, then disconnect and time-out the communications line after a set limit.

We have called attention to the increasing risk the electric power industry faces from computer-based electronic intrusions and attacks. Attack scenarios, based on similar incidents in the computer and telecommunications industries, are presented to describe how the attacks may unfold and show the negative consequences to electric power system protection and SCADA systems. Fortunately, there are many tools and techniques, with a wide range of pricing and complexity, that can help safeguard your IEDs, PLCs, communications processors, and SCADA systems. The electric power industry can implement the lessons learned by the computer and telecommunications industries and stop electronic intrusions before the safety and reliability of the electric power grid are compromised [18, 19].

REFERENCES

[1] IEEE Power Engineering Society, *IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE, New York, NY, April 4, 2000.

[2] National Security Telecommunications Advisory Committee Information Assurance Task Force, Electric Power Risk Assessment, March 1997: http://www.ncs.gov/n5_hp/Reports/EPRA/electric.html.

[3] The White House Office of the Press Secretary, White House Communications on Critical Infrastructure Protection, October 22, 1997: http://www.julieryan.com/Infrastructure/IPdoc.html.

[4] U.S. Federal Bureau of Investigation, National Infrastructure Protection Center, 2000: http://www.nipc.gov.

[5] P. Oman, E. Schweitzer, and D. Frincke, "Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems," 27th Annual Western Protective Relay Conference, Paper #4, (October 23–26, Spokane, WA), 2000: http://www.selinc.com.

[6] U.S. National Institute of Standards and Technology, *Introduction to Computer Security*: *The NIST Handbook*, NIST, Dept. of Commerce, July 20, 1994.

[7] CNN, "Teen Hacker Faces Federal Charges," March 19, 1998: http://www.compugraf.com.br/hackers.html.

[8] R. Lemos, "Power Play–Electric Company Hacked," *ZDNet News*, December 14, 2000: http://www.zdii.com.

[9] Frontline, "Hackers," a *PBS* special report, aired Thursday, February 15, 2001.

[10] T. Greene, "FBI Hacker Sleuths Hint at Power-Grid Disaster," *The Register*, December 17, 2000: http://www.theregister.co.uk.

[11] B. Sullivan, "NetEspionage Costs Firms Millions," *MSNBC*, September 12, 2000: http://www.zdnet.com/zdnn/stories/news/0,4586,2626931,00.html.

[12] R. O'Conner, "Cracker Jacked," *ZDNet News*, November 5, 2000: http://www.zdii.com.

[13] T. Hansen, "Utilities and Internet Security," *Utility Automation*, October 2000, pp. 18–19.

[14] AFCEA, "Internet-Based Attack Risk Distracts Organizations From Internal Trouble," *SIGNAL*, August 2000, pp. 25-28.

[15] U.S. Department of Defense, *Department of Defense Password Management Guideline*, CSC-STD-002-85, DOD Computer Security Center, Fort Meade, MD 20755, April 12, 1985.

[16] W. Stallings, *Cryptography and Network Security*, Prentice Hall, New York, NY, 1999.

[17] S. Kent, "On the Trail of Intrusions into Information Systems," *IEEE Spectrum*, Vol. 37, (12), December 2000, pp. 52–56.

[18] M. Amin, "Toward Self-Healing Infrastructure Systems," *IEEE Computer*, Vol 33(8), August 2000, pp. 44–53.

[19] A. Jones, "The Challenge of Building Survivable Information Intensive Systems," *IEEE Computer*, Vol 33(8), August 2000, pp. 39–43.

BIOGRAPHIES

Dr. Paul W. Oman is a Senior Research Engineer at Schweitzer Engineering Laboratories in Pullman, WA. Prior to joining SEL he was Professor and Chair of Computer Science at the University of Idaho and was awarded the distinction of *Hewlett-Packard Engineering Chair* during his last seven years there. Dr. Oman has published over 100 papers and technical reports on software engineering topics. He is a past editor of *IEEE Computer* and *IEEE Software* journals. He has a Ph.D. in computer science from Oregon State University, serves as a Senior Member in the IEEE, and is active in the IEEE Computer Society and the ACM.

Dr. Edmund O. Schweitzer, III received his Bachelor's degree and his Master's in electrical engineering from Purdue University, and received his Ph.D. degree from Washington State University, with a dissertation on digital protective relaying. Dr. Schweitzer continued his research in digital protective relaying while serving on the electrical engineering faculties of Ohio University and Washington State University. In 1982, Dr. Schweitzer founded Schweitzer Engineering Laboratories, in Pullman, Washington, to develop and manufacture digital protective relays and related products and services. Dr. Schweitzer is recognized as a pioneer in digital protection, and holds the grade of Fellow of the Institute of Electrical and Electronic Engineers (IEEE), a title bestowed on less than one percent of IEEE members. He has written dozens of technical papers in the areas of distance relay design, filtering for protective relays, protective relay reliability and testing, fault locating on overhead lines, induction motor protection, directional element design, dynamics of overcurrent elements, and the sensitivity of protective relays. Dr. Schweitzer holds more than twenty patents pertaining to electric power system protection, metering, monitoring, and control.

Jeff Roberts received his BSEE from Washington State University in 1985. He worked for Pacific Gas and Electric as a Relay Protection Engineer for over three years. In 1988, he joined Schweitzer Engineering Laboratories, Inc. as an Application Engineer. He now serves as the Research Engineering Manager. He has written many papers in the areas of distance element design, sensitivity of distance and directional elements, directional element design, and analysis of event report data. Mr. Roberts has delivered papers at the Western Protective Relay Conference, Texas A&M University, Georgia Tech, Monterrey Symposium on Electric Systems Protection, and the South African Conference on Power System Protection. He holds 19 patents, with several others pending, and is a Senior Member of the IEEE.

SCADA data and using this to detect intrusions. Furthermore, Ernstâ€™s pruning tech-. nique does not allow invariants that are usually true, e.g. 99% of the time. 5.3 Support for the State Estimator in Electricity Networks. A lot of research has been carried out on the development of state estimation and. the extension of it to include topology errors. This includes the work by Clements on.Â been done on intrusion detection in SCADA systems. 6. Experiments. Using a load flow program,5 real and reactive power flow measurements for a six. bus network were calculated for total system loads varying over the annual cycle. given with the specification of the IEEE 24 bus test network [16]. This provided 8736. Oman, P., Schweitzer, E., Roberts, J.: Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions, available at: http://tesla.selinc.com/techpprs.htm. 14. Pereira, J.C., Saraiva, J.T., Miranda, V.C., Antonio, S.L., Clements, K.A.: Comparison of Approaches to Identify Topology Errors in the Scope of State Estimation Studies.Â Bigham J., Gamez D., Lu N. (2003) Safeguarding SCADA Systems with Anomaly Detection. In: Gorodetsky V., Popyack L., Skormin V. (eds) Computer Network Security. MMM-ACNS 2003. In general, SA and other control systems do not have logging functions to identify who is attempting to obtain access to these systems. Efforts are underway in the commercial arena and with the National Laboratories to develop intrusion detection capabilities for control systems. Summary. In summary, the art of detecting intrusions into substation control and diagnostic systems is still in its infancy. Until dependable automatic tools are developed, system owners will have to place their major efforts in two areas: Preventing intrusions from occurring, and. Recovering from them when they occur