Cyber Security Issues for Protective Relays

C1 Working Group Members of Power System Relaying Committee

Solveig Ward (chair); Jim O'Brien (co-chair), Bob Beresh, Gabriel Benmouyal, Dennis Holstein, John T. Tengdin, Ken Fodero, Mark Simon, Matt Carden, Murty V.V.S. Yalla, Tim Tibbals, Veselin Skendzic, Scott Mix, Richard Young, Tarlochan Sidhu, Stan Klein, Joe Weiss, Alex Apostolov, Dac-Phuoc Bui, Sam Sciacca, Joe Weiss, Craig Preuss, Steven Hodder

Abstract—**This report covers issues concerning the security of electronic communication paths to protective relays.**

It is the goal of this paper to present the reader with some background material and discussions by which they can become more aware of the concerns associated with electronic communications in the power industry.

Index Terms—**cyber security, protective relaying, relay, relaying communications.**

I. Introduction

THIS report is focusing on communications with protective relays. However, with the multifunction character of microprocessor relays, these devices might also provide services for and therefore will be accessed by other groups in the power utility.

A. Devices

In addition to the relays themselves, devices used to access relays such as substation computers, switches, routers as well as Local Area Network security are discussed.

The discussions in the report are not limited to transmission relaying equipment in substations. The concerns and recommendations can be equally valid for distribution substations and distributed relaying devices such as pole mounted reclosers.

II. Background

Over time words tend to change meaning as culture and perceptions change and new ideologies are adapted. The word "security" has in the past conjured up images of comfort, the physical protection offered by family and friends, stable financial prospects, and peace of mind. However in recent years our image of the word security has changed into something more likely to do with locks and gates, portable alarm devices, missile defense systems, and space shields. Change has also occurred in terms of the use of the word with respect to the area of computers - what is commonly known as cyber security. Security was not an issue of concern when computers were in their infancy and the Internet's predecessor, ARPANET, was developed for use by the scientific and academic community. However computers are no longer the technical amusement of a select group with trusted network access to any and all, but are now a commonplace and integral part of everyday life in our society and, unfortunately, now subject to frequent malicious attacks and electronic vandalism.

Initially when computers became networked electronic information in the form of data and applications was commonly exchanged via the use of FTP, or file transfer protocol. A user could typically log into a computer site using their email address and the password "anonymous" and be greeted with a "welcome" message. The guest would then have easy access to desired information, including oftentimes system files. Soon this technology became subversively exploited and the industry was told not to expect to prosecute violators when an open door and a welcome mat were laid out for common use. Security gradually took on a new meaning as the hosts of computer data sites became increasingly aware of issues surrounding the vulnerability and protection of their information and networks. Today it is not uncommon to have networked computer sites visited and attacked on a regular basis (1000's of times per day) by subversive forces for reasons ranging from espionage, extortion, "cyber protests", revenge, and sport. Not only are computer sites vulnerable to direct and focused attack, but they are also vulnerable to indirect, or indiscriminate, attacks from viruses, worms and Trojan horses.

As technology has increased, the use of computers and network access has also increased. Computers, or microprocessor-based devices with computing capability, are now commonly used for control and automation functions in addition to traditional data archival and processing. Computers preside over a plethora of daily activities from financial, manufacturing, scientific, and safety-rated issues. Millions of computers are connected to the Internet and now form a vast interconnection of devices used by corporations, individual, and government agencies. As can be imagined with this convenient and widespread use, the opportunity for misuse has also burgeoned.

Technological misuse and/or abuse has become a serious concern in all areas where computers are used and networked. The ability of seditious individuals to disrupt the national power supply, discharge harmful chemicals or waste into the environment, or upset production facilities, has become an unwelcome verity. Not only are there financial and safety concerns associated with this, but also issues relating to legal liability where individuals or corporations can be sued for mismanagement of technological resources. Other issues arising from compromised computing facilities are loss of customer confidence, information confidentiality, and the ability to conduct business. Computer security has now become the focus of national consideration.

The electric power industry, as the rest of society, has been taking advantage of the tremendous power provided by computer and microprocessor-based technology. Protection and control equipment, SCADA, remote control and monitoring, and many other applications are routinely implemented with this technology. Recent experience has shown that security related issues must be addressed by the power industry. Government regulation will soon legislate the need for proactive measures to be taken in terms of securing the computer network infrastructure within the power grid. The electrical supply is too important to be left in a state of vulnerability and neglect.

III. Data Access Needs for Protection Engineers

Utility personnel require remote access to the protection, control, and monitoring devices located in substations scattered throughout the system. This access is required to: continuously assess the health of the system; recognize developing problems that may adversely affect the ability of the system to remain operational; identify the location of faults and failures to facilitate the dispatch of repair crews; analyze the operation of protective devices to ensure correctness and maintain coordination to prevent cascading outages; identify possible improvements to protective schemes; verify the accuracy of system models to facilitate planning studies. Some of the devices for which access is needed are:

- Microprocessor-based protective relays
- Digital fault recorders
- Dynamic disturbance monitors
- Phasor measurement units
- Power system stabilizers
- Geo-magnetically-induced current monitors
- Remote terminal units (RTU) of system control and data acquisition (SCADA) systems
- Substation Computers
- Data Historians
- SCADA systems
- Security systems (fire, intrusion, etc.)

The level of access required depends on job function. System control operators need to know what happened and where (breaker status changes, system element loading, relay target data and fault locations, intrusion alarms, etc.) Protection engineers typically need to read the stored data (relay, fault recorder, and disturbance monitor event records and setting records) in order to analyze system disturbances, support operations personnel, coordinate protection schemes, and ensure compliance with NERC standards. Protection Engineers can also make settings changes as required due to changes in system configuration. Field relay technicians need read/write access to all levels of the devices in order to apply the settings determined by the protection engineers and set up the devices for proper operation and communication with those that need access.

Access needs to be available within the substation and corporate offices. A limited number of personnel will require full access at non-company locations. The expectation of round the clock analysis capabilities and the quantity of data available often requires access via the Internet. A dial up connection may also be used for less demanding requirements. Access to the corporate “Data” network via the Internet raises the highest level of concern for cybersecurity.

A. Relay Access and Settings Considerations

Relays are critical to the power system. The settings in a relay determines the response (or non-response) of the device and incorrect settings may have serious effect on the power system operation.

Typically, relay settings are allowed to be changed by Protection Personnel only, but the multi-function nature of microprocessor relays have extended use of protection devices to other groups as well. A modern relay may replace a traditional RTU and provide metering data and control functions for opening and closing breakers and other switches. A relay may also be connected to a substation computer that performs automation and control functions.

The multi-function nature of the relay device may generate the need to extend ‘setting-change-privileges’ to others than protection engineers which creates an added challenge for the protection engineer to track, document and verify relay settings.

Modern relay designs recognize the need for increased access to the device and provide some means to help the relay engineer with regards to setting changes. Some examples are:

- Passwords. Most relays have the ability of password protection for settings changes.
- A relay log for setting changes, and to issue an alarm when a setting change has been made.
- Multiple levels of access, with different passwords for each level. Typically, there is a read-only level that may be accessed by a larger number of users while the higher level for setting changes can be accessed by the relay engineer only.
- A relay with multiple settings groups where a switch to another per-verified group may be allowed by non-relay personnel, while change of individual parameters is not.

While procedures for access restriction to the substation are well established, the increased remote access to microprocessor relays is less regulated.

Typically, a utility utilizes the extended capability of microprocessor relays to provide status, control and metering functions to a station RTU via a serial communication link. This functionality has replaced traditional analog transducer and hard-wired alarm connections to a central station RTU in all new installations and many retrofit locations. Any settings required for these extended functions should be communicated to the protection engineer during the schematic and/or relay setting development phase. The automation engineer may also initiate setting changes through the protection engineer if only changes associated with automation are required. Ultimately, the protection engineer should be the individual responsible for all protective relay settings and documentation – the automation engineer works through the protection engineer to implement necessary automation settings.

Preferably, relay access passwords should be established that allow view-only user access to automation engineers (and maintenance personnel, system operators…). A second, more secure level in which setting changes may be made should be reserved for relay engineers and test technicians. Testing contractors may utilize temporary passwords to complete necessary setting changes and testing.

Relays have settings that can be generally grouped into the following categories: protection, communication (usually related to integration and automation, not teleprotection), and security. Utilities may have processes in place that dictate if any relay setting has changed, including the communication and security settings, the relay must be re-commissioned. This re-commissioning policy can be benficial when relay communication settings are changed. With the deployment of protective relays on substation LANs using IEC 61850, it is possible that communication settings could be changed (such as IP address) that would adversely impact the protective functions of the relay. This re-commissioning policy may adversely impact the procedures put in place for securing relays, where relay passwords must be changed under certain situations (employee leaving, contractors leaving, password aging, etc). In these situations where relay passwords must be changed, requiring a re-commissioning of all relays where the password(s) are changed can quickly become impractical because there may be hundreds or thousands of passwords to change, and in some cases, re-programming of devices that include passwords in the retrieval of SCADA data from relays.

Relay re-commissioning after a settings change should include a careful review of how communication and security settings impact overall device integration and security policies. This review should include not only relay engineers, but automation engineers and security professionals as well. For example, relays that do not perform protective functions over a LAN and are polled using DNP over the LAN may only require a quick point check to confirm that polling has been re-established after a communication settings change; relays that do not perform protective functions over a LAN and are polled using DNP do not require re-commissioning after a password change. It is possible that the relay setting change process may drive the technological solution for the security process, or vice-versa.

Further discussion of setting considerations is found in a report prepared by the PSRC group C3: “Processes, Issues, Trends and Quality Control of Relay Settings”.

IV. Communications Media

There is a large variety of communications routes for access of devices in substations. The physical media can be Point-to-Point (telephone lines), Microwave, and higher bandwidth transport (T1, SONET or Ethernet).

A. Typical Point-to-Point Communications Media

- POTS (Plain Old Telephone Service) dial-up via phone line – The most common medium used to access relays remotely is dial-up phone lines. A standard voice line run into the substation provides the path. Modems are required to interface the phone line with the IEDs. Line switchers typically allow one phone line to be switched and used for relay access, meter access, phone conversations, etc.
- Leased line – Leased lines are typically used for SCADA connection. They are dedicated lines that are connected 24 hours a day, 7 days a week. They allow constant data acquisition and control capability of substation equipment.
- Wire-less – Wire-less communication (cellular phones) is a technology that is useful in the substation environment. It can be less expensive than a hard phone line due to the protection required by Telcos on a phone line run into a substation to limit ground potential rise. The cost is based on actual usage (minutes used). Usability may be limited by cellular coverage in the area but that is continually improving.
- Radio – 900 MHz radio is another medium used by utilities. These radios can either be licensed or unlicensed depending on the frequency selected. The unlicensed installations have a lower installed cost but there is no protection from interference by other users.

B. Microwave

Microwave is a high frequency radio signal that is transmitted though the atmosphere. Common frequency bands are 2 GHz, 4 GHz, 6 GHz, 10 GHz, 18 GHz, and 23 GHz. Transmitted signals at these frequencies require a direct line of site path, and accurate antenna alignment. The federal Communications Commission (FCC Parts 21, and 94) controls operation and frequency allocations.

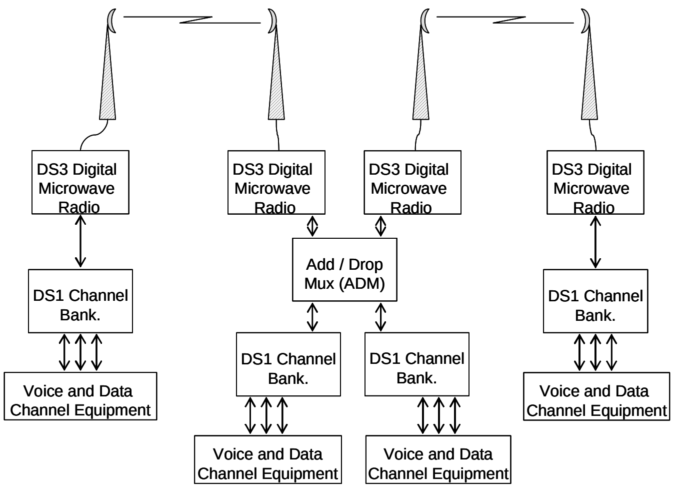
DS3 Digital Microwave Radio
DS3 Digital Microwave Radio
DS3 Digital Microwave Radio
DS3 Digital Microwave Radio
Add / Drop Mux (ADM)
DS1 Channel Bank.
DS1 Channel Bank.
DS1 Channel Bank.
DS1 Channel Bank.
Voice and Data Channel Equipment
Voice and Data Channel Equipment
Voice and Data Channel Equipment
Voice and Data Channel Equipment

Figure 1. Microwave System

In digital microwave systems the data modems, required in an analog system, are replaced by digital channel banks. These channel banks can be combined to form a multiplexed system as shown in Figure 1. The channel banks convert analog voice, and data inputs into a digital format using Pulse Code Modulation (PCM). The digital channel bank combines 24 voice channels into a standard 1.544 Mbps DS-1 signal. The DS-1 level is further multiplexed into DS-3 before transmitted over the radio link.

C. T1, SONET and Ethernet Transport Layer

Many substations are served by T1, SONET or Ethernet access equipment to provide a communications path to the substation device.

T1 is a term for a digital carrier facility used to transmit a DS-1 formatted digital signal at 1.544 megabits per second. T1 was developed by AT&T in 1957 and implemented in the early 1960’s to support long-haul pulse-code modulation (PCM) voice transmission. The primary innovation of T1 was to introduce “digitized” voice and to create a network fully capable of digitally representing what was, up until then, a fully analog telephone system.

T1 is used for a wide variety of voice and data applications. They are embedded in the network distribution architecture as a convenient means of reducing cable pair counts by carrying 24 voice channels in one 4-wire circuit. T1 multiplexers today are also used to provide DS0 “access” to higher order ‘transport’ multiplexers such as ‘SONET’.

SONET (Synchronous Optical NETwork) is the American National Standards standard for synchronous data transmission on optical media.

Some of the most common SONET (and SDH) applications include transport for all voice services, internet access, frame relay access, ATM transport, cellular/PCS cell site transport, inter-office trunking, private backbone networks, metropolitan area networks and more. SONET operates today as the backbone for most, if not all, interoffice trunking as well as trans-national, and trans-continental communications.

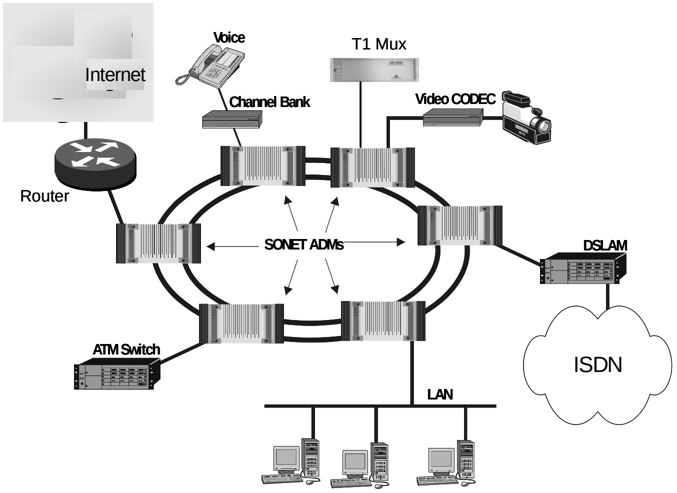

Figure 2. Telecommunications Network

IP Communications (Ethernet) is growing as a substation access technology. The transport is often over a SONET layer, but Ethernet LANs are also used.

The communications network can be privately owned by the utility, or leased from a carrier. A Local Area Network (LAN) can have its own dedicated communications links or exist as a VLAN (virtual local area network) where the transport layer is shared with other, unrelated traffic.

The LAN or VLAN may interconnect with a Wide Area Network (WAN) that carries corporate traffic and/or is a public transportation network.

D. Communications Media Cyber Security Concerns

Electronic eavesdropping can be achieved in all communications media by intercepting or tapping into communication signals. Dial-up phone lines are especially vulnerable as the device connected to it can be directly accessed through the public telephone network. Any security needs to be handled by the device itself. Leased phone lines are more likely to suffer from denial of service rather than interception due to the highly specialized and often proprietary data they carry.

Eavesdropping in Local Area Networks (LAN) and Wide Area Networks (WAN) is called sniffing. A sniffer is a program that accepts and opens network packets that are not addressed to your equipment.

Wireless eavesdropping and sniffing can occur on virtually all commonly used wireless networks including, radio, satellite, and microwave transmissions.

V. Communications Systems

Communication to the substation device can be point-to-point, over a Local Area Network (LAN), Virtual Local Area Network (VLAN), or Wide Area Network (WAN). The type of communications system is not directly related to the communication media as various media can be deployed within one network.

A. Internet

Technologies have been developed that allow Internet access to substation devices. Each device is assigned a unique Internet address and is connected to a LAN in the substation and on to the Internet. Web browser software can be used to communicate with the devices.

Cyber Security in the Substation can be addressed at both the Data link and Network layers of the OSI model. The addressing mechanism at the Data link layer is the Mac address which is predefined by the manufacturer of the Ethernet enabled communications equipment. At the Network Layer the IP address is used.

The network should be secured at both layers. Each communications device used on the network has specific vulnerabilities and in most cases features to deal with them. Many of these features need to be configured.

Security design within the network is paramount in the process of securing the network. While securing the network the following features should be considered.

1) Security at the Data Link Layer

The Data link layer is commonly called layer 2. At this layer switches are the most prevalent communications equipment used. Many different features are available on the switches that can impact the Security on the network.

2) Management Security

Switches have their own security to protect against intrusion or unauthorized configuration. Switches should be configured with passwords and secrets which are unique and follow strong password standards. SSL or SSH should be used when configuring switches to prevent sniffing these passwords.

3) Port Security

Individual ports on the switch can be secured using several methods. In the simplest form they may be enabled or disabled. It is recommended unused ports be disabled. Each port may be further secured using MAC based security, 802.1x or VLAN filtering.

4) MAC Security

When MAC based security is used each port on the switch can be configured to allow communications only from one specific MAC address. With this method of security, only the IED's intended to communicate on any given port (or a hacker spoofing an IED’s MAC address) can do so.

5) 802.1x

With this technology devices are forced to authenticate with a predefined user name / password before they gain access to the network. 802.1x clients are required on the IED in order to make this effective. Most windows clients available today have integrated 802.1x clients. The authentication is usually done by a third party entity, such as a RADIUS server.

6) VLAN Security

When VLAN based security is used, all traffic entering the network comprises (or is assigned) IEEE 802.1Q “tagged” frames, with each tag’s “VID” field identifying a specific VLAN. Un-trusted sources are assigned (on ingress) an appropriate VID to guarantee the isolation of such sources from the traffic assigned to other VID’s.

B. Security at the Network Layer

The Network layer is commonly called Layer 3. At the Network layer many devices can be used to secure the network. The devices commonly used at this layer are Routers, Firewalls and Intrusion detection devices. Some Security appliances are available that offer all three functions in one box.

1) Management Security

Routers / Firewalls / Intrusion detection devices have their own security to protect against intrusion or unauthorized configuration. These devices should be configured with passwords and secrets which are unique and follow strong password standards. SSL or SSH should be used when configuring these devices to prevent sniffing these passwords.

2) IP Filtering

Filtering can be done by Routers and Firewalls. Filtering can be used to deny access to the Substation network from unauthorized IP networks. In order to use this feature effectively the IP address space within the entire Utility should be assigned effectively.

3) Port / Socket Filtering

Filtering can be done at the Port / Socket layer. Ports / Sockets are used to identify traffic by type. These can be services such as FTP, HTTP or Telnet. Many organizations prohibit some of these services on the Substation LAN by policy.

4) Anomaly Detection

Intrusion Detection devices can be used to look for network anomalies. This is done by comparing traffic against a known database of signatures which identify traffic patterns which are known to present network vulnerabilities. When an anomaly is detected on the network the network administrator is notified. The network administrator will generally take action by configuring filters on the Routers or Firewalls.

5) Encryption

Encryption can be used on the LAN to secure traffic against unauthorized access. This can be done for Routers, Firewalls and some IED’s. Several different types of Encryption algorithms are commonly available. These include DES, 3DES or AES. 3DES is the most common. AES is a newer standard which offers a higher level of security.

VI. Relay Pilot Channels

Pilot protection schemes and SCADA control schemes are similar in that either system can potentially initiate breaker tripping. The communications channels and equipment requirements for pilot protection schemes differ from those used for SCADA in the following ways:

- They are predominantly operated on private, closed, and deterministic networks.
- Signal transmission and reception must have known and minimal delays.
- With the exception of direct transfer trip schemes, most pilot protection schemes qualify received messages with locally measured quantities.

The most widely used pilot protection system is directional comparison. Major reasons for this wide acceptance are the low channel requirements (i.e., lower data rate, small message sizes, etc.) and the inherent redundancy and backup of directional comparison systems. Although the channel bandwidth requirements are less than those of current differential schemes, the communication channel data integrity requirements are significant. We may classify directional comparison pilot protection systems as blocking or transfer trip. This classification corresponds to the way the local relay uses remote terminal information to generate the tripping signal.

A current differential system is another popular pilot protection scheme. Such schemes compare the magnitude and/or phase of the currents from all terminals. This means that current differential schemes require a reliable, high-capacity communications channel. When communication fails, the differential protection portion of these schemes must be blocked from operating. Today, many current differential schemes use redundant communications to handle the loss of a single channel.

All pilot schemes are characterized by the need for a reliable communications channel between the line-end devices. It is not necessary to extend or network the connections to any other devices. In practice, the majority of these communications channels are deployed on wholly owned (i.e., not leased from a telecomm provider) media such as fiber or the power line itself. Because of this, most real-time protection communications have very limited exposure to potential electronic attack.

Assuming that attackers are able to access the communications media (either electronically or physically), they could potentially execute the following general attacks:

- Denial of Service (DOS): Cause a break in the normal transmission of real-time protection messages.
- Traffic Manipulation (TM): Intercept legitimate traffic and/or inject malicious traffic on the line.

The effect of a DOS or TM attack depends upon the type of protection scheme. Table I shows the action and results for the various schemes.

TABLE I – EFFECT OF ATTACK ON PILOT RELAYING

Scheme	**DOS**		**TM**	
	Action	**Result**	**Action**	**Result**
Blocking	Block any Block Trip Signal	Out-of-section fault overtrip	Cause a standing Block Trip Signal	Time-delayed trip for in-section faults
Permissive	Block Permissive Trip Signal	Time-delayed trip of in-section faults	Cause a standing Permissive Trip Signal	Overtrip for out-of-section faults
DTT	Block DTT Signal	No trip	Send DTT Signal	False trip
87L	Disrupt communications	No trip	Alter or delay transmitted date	False trip

The blocking and permissive trip protection schemes provide high immunity to any potential attack damage (it is simply not possible to cause a severe mis-operation through manipulation of the communications channel). For the direct transfer trip (DTT) scheme, we can eliminate the possibility of tripping the local breaker with local supervision. Examples of local supervision are overcurrent, undervoltage, power, and rate-of-change elements. Finally, for current differential (87L) protection schemes, you can eliminate the loss of line protection resulting from channel failure (either accidental or deliberate) with effective backup communications and protection schemes.

Current differential schemes are extremely dependent upon communications: a DOS attack on a line current differential scheme does disable the primary, 87L protection on the line. However, many schemes include true hot-standby 87L communications and directional comparison protective schemes in the same device. Thus, in the event of an attack, the complete scheme would disable one of the 87L schemes and alarm, yet line protection would remain intact. It is possible, however, to initiate a false trip for DTT (without supervision) and 87L protection schemes with a TM attack. This may not be a cause for concern because of the limited exposure of most real-time protection communications.

The limited risks outlined above may warrant additional electronic security if the communications channels used to implement pilot protection schemes are not “sufficiently” secure. Such a decision can only be made by weighing the potential costs of an inadvertent breaker trip versus the risk of electronic attack.

VII. RAMIFICATIONS OF SECURITY

A number of issues are of serious concern with respect to power system security. In a society where companies and individuals increasingly succumb to litigation for reasons of negligence and lack of due diligence, one must ask, “What is the implication of not doing something” as well as of doing something?” Cyber security is no different, and as it relates to protection and control, can involve serious considerations with respect to the following areas:

- Legal
- Financial
- Safety
- Government Regulation
- Environmental

It is not the intention of this report to overreact to potential implications of a poorly designed security policy (or lack of a security policy) but to mention some issues that should be considered in giving cyber security due respect and attention.

Many people take for granted the safe and reliable operation of the power system and do not fully comprehend the amount of sophisticated equipment that is used in protecting the operation of the power system. With the proliferation of high-speed networks and the increased dependency on communications, there is serious potential for subversion on the reliable operation of the power system. For example, in one case a disgruntled employee who was dismissed from his job was able to use a remote communication link to activate a SCADA system in a local waste water treatment plant and cause effluent to discharge in the neighborhood. This network intrusion occurred numerous times before the culprit was apprehended. In another instance, hackers successfully infiltrated the computer system for the Salt River Project. The listing of examples can, unfortunately, be continued to some length. This list considers some of the possible ramifications arising from a cyber intrusion and is not intended to be exhaustive.

A. *Legal*

- What are the legal and financial implications of losing customer account information due to a negligent or laissé

faire attitude towards data protection? Can personal customer credit information be compromised? Can a list of customers be used to form a target list of new clients for a competitor? What is the effect on customer confidence and good will?
- Can correct utility operation be vindicated if there is loss or corruption of operational data (event records, oscillography) arising from a breach in cyber security? Can private technical information, such as relay settings, system operating conditions, etc., be used to implicate a utility for negligence in the operation of their system?
- What are the implications of a possible intrusion and the subsequent need for equipment to be quarantined in order to perform legal or forensic analysis of the equipment operation and data?

B. Financial

- What is the implication of the loss of customer loyalty and good will in the event of a publicized intrusion? If customers have a choice, will they go elsewhere?
- What are the financial implications of loss or damage to equipment arising from unauthorized remote access?
- What is the cost of importing power to replace lost generation in the event that networks or computers supporting station control are compromised?
- What are the financial implications of having to detect and restore settings or data that may have been altered?

C. Safety issues to public and employees

- What effect will an intrusion have on the safe operation of the power system? Could an intruder tamper with critical controls and cause equipment to operate incorrectly without system operator supervision?
- Could people be injured or property damaged as a result of unauthorized access to control or protection functions and settings?
- What are the implications for life support and emergency functions such as hospitals and health care facilities if the operation of the power system is impacted by unauthorized access to networks and computers?

D. Government regulation

- What are the implications with respect to disregard of government legislation should a system be compromised?
- Could national security be affected in the event of an intrusion and subsequent (mis)operation of the power system?

E. Environmental issues – re spills and contamination

- What are the implications of an intruder causing environmental damage? (Note, this could be air, water, radioactive, waste, etc.)

In summary, cyber security must not be treated carelessly as the implications are significant and can be devastating for the stability of the company and economy. A thorough investigation into the vulnerability of the system and implications of an intrusion needs to be weighed.

VIII. Security Threats and Vulnerabilities

A. Threats

In evaluating the security threat to substation equipment, it is apparent that numerous people have physical contact with various devices within the substation. These individuals include employees, contractors, vendors, manufacturers, etc. Of particular concern is the fact that the typical substation environment can provide a means to compromise the power system with a low probability being detected or apprehended. This low perceived probability of detection creates opportunities to compromise the operation of the power system which could be attractive for a number of reasons, including:

- Job dissatisfaction
- Economic gain
- Competitor discrediting
- Job security
- Blackmail
- Sport
- Terrorism/Political

The following list provides some examples of possible security threats that may exist in a substation (not to be considered all inclusive).

- A substation automation contractor, with access to the substation, recognizes the station has equipment from a competitor and seeks to discredit that competitor's system by modification of the system configuration.
- An employee concerned about future employment changes all passwords throughout the system so that only they can access the system.
- A third party provider/consumer of power with some authorization to the station arranges to have metering data improperly scaled to support compromised revenue meters.
- An authorized person is approached by a third party who offers financial reward for the point mapping, address, and password of the automation system.
- The vendor of the original system has left behind a back-door which is unknown to the owner and can be used to change the configuration and performance of the system.

It is also important to consider the inadvertent compromise of an IED or automation system by authorized personnel who do not intend to degrade or affect its performance, but through some action on their part, do indeed compromise the device. Examples include:

- The use of an outdated or incompatible configuration software version which results in a corruption of the substation device settings.
- The use/download of an incorrect configuration which results in incorrect settings.
- Errors in entering settings/configuration data or errors in the engineering development of settings/configuration

which compromise the performance of the system.

The intentional and unintentional compromises of the power system are areas of concern for the NERC Cyber Security-Critical Cyber Assets and require addressing in any comprehensive cyber security program.

1) *Threat Sources*

In recent years, information security attack technology has become increasingly sophisticated. Attacks have become automated, so that specialized expertise is not necessarily required to perform them. Many attacks install "root kits" on the victim systems which are usually designed to enable the intruder to re-enter the system at will, to prevent the system administrator from discovering the attack, and to destroy any remaining evidence of the attack when the intruder is finished.

Threats may be caused by inadvertent actions of authorized persons as well as malicious actions of authorized and unauthorized persons. Some of the threat sources to consider include:

- Natural disasters and equipment failure
- Well-intentioned employees who make inadvertent errors, use poor judgment, or are inadequately trained
- Employees with criminal intent to profit or to damage others by the misappropriation of utility resources
- Disgruntled employees or ex-employees who cause damage to satisfy a grudge
- Hobbyist intruders who gain pleasure from unauthorized access to utility information systems (sport)
- Criminal activity by both individuals and organizations directed against the utility, its employees, customers, suppliers, or others
- Terrorists
- Competing organizations searching for proprietary information of the utility, its suppliers, or customers
- Unscrupulous participants in the markets for electric power or derivatives
- Software providers who, in attempting to protect their intellectual property rights, create vulnerabilities or threaten to disable the software in contractual disputes

In general, threats are directed towards information held by the utility, but the target of the threat may be an entity other than the utility, such as an employee, customer, or supplier. For example, reading residential electric use at frequent intervals can provide intruders information on when a residence is unoccupied. Also, the utility may store data on employees or customers that affects their privacy.

B. Vulnerabilities

This section summarizes a number of categories of vulnerability source and attack methods. These are organized into the following groupings:

- Security gaps in computer software (Table III)
- Vulnerabilities related to communications links and networking software (Table IV)
- System Administration issues (Table V)
- Vulnerabilities based on user personnel (Table VI)
- Miscellaneous and unusual methods (Table VII)

TABLE II – SOFTWARE SECURITY VULNERABILITIES

Category	***Example***
Logic errors	Failure to check input data validity
Test and debug features left in production code	Bypassing login protection for debugging purposes
User convenience features	Automated execution of scripts in email and download programs
Incorrect configuration of security permissions and privileges	Factory default settings not changed
Deliberate sabotage, logic bombs	Code embedded in a program that is triggered by some event and causes a disruption to occur
Deliberate vulnerabilities built into proprietary software for contract enforcement purposes (UCITA "Self-Help")	Backdoors built into software to prevent use after alleged violation of contract terms
Maintainer convenience features (backdoors)	Access that bypasses normal protections - typically intended for debugging or troubleshooting purposes

TABLE III – NETWORK SECURITY VULNERABILITIES

Category	***Example***
Communications channel penetration	Access via microwave antenna sidelobe
Network sniffing	Interception of network traffic to look for specific information, such as passwords.
Keyboard sniffing	Hiding captured keyboard data for later retrieval
Hijacking	Takeover of a user session after authentication
Spoofing and playback	Imitation of a legitimate user by capturing and re-sending legitimate messages
Man-in-the-Middle attacks	Eavesdrop, alter messages, or hijack
Codebreaking	Breaking encryption routines
Denial-of-Service attacks	Prevent legitimate use by causing extreme network congestion

Category	***Example***
Internet-related attacks	Take advantage of Internet service vulnerabilities

TABLE IV – SYSTEM ADMINISTRATION VULNERABILITIES

Category	***Example***
System administration	Significant security role of system administrator • Account and access control setup • Software installation/removal privileges • Corporate policy enforcement • System monitoring and auditing • Maintain backups • Responding to intrusions • Most operating systems install insecurely

TABLE V – PERSONNEL RELATED VULNERABILITIES

Category	***Example***
Password Guessing	• No password used at all • Setting password the same as the user ID • Using own, family, or pet names • Using hobby or entertainment terms • Using organizational or project terms • Automatic checking of visible (but encrypted) password files against dictionaries
Social Engineering (Con games)	• Repair • Emergency • Security • Name dropping and sweet talk • Marketing survey for relevant information

TABLE VI - MISCELLANEOUS AND UNUSUAL VULNERABILITIES

Category	***Example***
Viruses and Worms	Self-propagating, malicious programs and code
Trojan Horse	A malicious program that appears benign and useful
Open Codes	Messages hidden in innocuous-looking material
Electromagnetic Emanations	Signals that disclose internal device processing
Covert Channels	Insiders sending out data by unusual means
Aggregation of Unprotected Information	Enough non-sensitive data may reveal sensitive
Physical vulnerability	Allows theft or alteration of equipment
Hidden Files	Means of concealing root kit files
Telephone-based	Diverting dialups at telephone switch
War dialer attacks	Automatically dial consecutive phone numbers and listen for modem connections then attempt to break into the connected device
Postscript Fax Machines	Backdoor network access

1) Communication Protocols and Associated Vulnerabilities

The power industry has focused almost exclusively on deploying equipment that can keep the power system reliable. Until recently, communications and information flows have been considered of peripheral importance. However, increasingly the Information Infrastructure that supports the protection, monitoring, and control of the power system has come to be pivotal to the reliability of the power system.

Communication protocols are one of the most critical parts of power system operations. They are responsible for retrieving information from field equipment and sending control commands. Despite their key importance, these communication protocols have rarely incorporated any deliberate security measures. Since these protocols were very specialized, “Security by Obscurity” has been the primary approach. No one would have thought that there was even a need for security. However, security by obscurity is no longer a valid mode of operation. In particular, the electricity market is pressuring participants to gain any edge on security that they can. A small amount of information can turn a losing bid into a winning bid – or withholding that information from your competitor can make their winning bid into a losing bid. And the desire to disrupt power system operations can stem from the simple teenager bravado to competitive game-playing in the electrical marketplace to actual terrorism.

It is not only the market forces that are making security a crucial operating practice, but the sheer complexity of operating a power system has increased over the years which makes equipment failures and operational mistakes more likely and their impact greater in scope and cost. In addition, older, less known and obsolete communications protocols are being replaced by standardized, well-documented protocols that are more susceptible to hackers and industrial spies.

The International Electrotechnical Commission (IEC) Technical Council (TC) 57 Power Systems Management and Associated Information Exchange is responsible for developing international standards for power system data communications protocols. Its scope is "To prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. Power systems management comprises control within control centers, substations, and individual pieces of primary equipment including telecontrol and interfaces to equipment, systems, and databases, which may be outside the scope of TC 57. The special conditions in a high voltage environment have to be taken into consideration."

IEC TC57 has developed three widely accepted protocols, and has been the source of a fourth:

- IEC 60870-5, which is widely used outside of the USA, for SCADA system to RTU data communications. It is used both in serial links and over networks.
- DNP 3.0, which was derived from IEC 60870-5, is in use in the USA and many other countries for SCADA system to RTU data communications.
- IEC 60870-6 (also known as TASE.2 or ICCP) which is used internationally for communications between control centers and often for communications between SCADA systems and other engineering systems within control centers.
- IEC 61850 which is used for protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control center, and other power industry operational functions. It is designed to meet the fast response times of protective relaying, for sampling of measured values, and monitoring/control of substation equipment.

These international standards account for close to 90% of the data communications protocols in newly implemented and upgraded power industry SCADA systems, substation automation, and protection equipment. (Modbus and Fieldbus as well as other proprietary protocols are still used in older systems and in other industries.)

By 1997, IEC TC57 recognized that security would be necessary for these four protocols. It therefore established a temporary working group to study the issues relating to security. This working group published a Technical Report (IEC 62210) on the security requirements of substations. One of the recommendations of the Technical Report was to form a working group to develop security standards for the IEC TC57 protocols and their derivatives (i.e. DNP 3.0). Therefore, IEC TC57 WG15 was formed in 1999, and has undertaken this work. The WG15 title is "Power system control and associated communications - Data and communication security" and its scope and purpose are to "Undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Undertake the development of standards and/or technical reports on end-to-end security issues."

The scope of the work of WG15 is to develop standards that increase the informational security assurance aspects of the protocols specified within TC57. As part of this work, concrete and implementable standards are intended to be developed. These standards are intended to be specified, as needed, by utilities and implemented by responding vendors. WG15 is committed to develop relevant standards that increase the overall informational security assurance aspects of utility infrastructures.

The justification for this work was that safety, security, and reliability have always been important issues in the design and operation of systems in the power industry, and cyber security is becoming increasingly important in this industry as it relies more and more on an information infrastructure. The deregulated market has imposed new threats as knowledge of assets of a competitor and the operation of their system can be beneficial and acquisition of such information is a possible reality. Since 9/11 the additional threat of terrorism has become more visible.

The final sentence in the scope/purpose statement is very important. It was recognized that the addition of just simple encryption of the protocols, for instance by adding "bump-in-the-wire" encryption boxes or even virtual private network (VPN) technologies would not be adequate for many situations. Security is an "end-to-end" requirement to ensure authenticated access to sensitive power system equipment, reliable and timely information on equipment functioning and failures, backup of critical systems, and audit capabilities that permit reconstruction of crucial events.

This work is to be published by the IEC as IEC 62351, Parts 1-7:

- IEC 62351-1: Introduction
  This first part of the standard covers the background on security for power system operations, and introductory information on the series of IEC 62351 security standards.
- IEC 62351-2: Glossary of Terms
  This part will include the definition of terms and acronyms used in the IEC 62351 standards. These definitions will be based on existing security and communications industry standard definitions as much as possible, given that security terms are widely used in other industries as well as in the power system industry.
- IEC 62351-3: Profiles Including TCP/IP
  IEC 62351-3 provides security for any profile that includes TCP/IP, including IEC 60870-6 TASE.2, IEC

61850 ACSI over TCP/IP, and IEC 60870-5-104. Rather than re-inventing the wheel, it specifies the use of Transport Level Security (TLS) which is commonly used over the Internet for secure interactions, covering authentication, confidentiality, and integrity. This part describes the parameters and settings for TLS that should be used for utility operations.

- IEC 62351-4: Security for Profiles That Include MMS
  IEC 62351-4 provides security for profiles that include the Manufacturing Message specification (MMS) (ISO 9506), including TASE.2 (ICCP) and IEC 61850. It primarily works with TLS to configure and make use of its security measures, in particular, authentication (the two entities interacting with each other are who they say they are). It also allows both secure and non-secure communications to be used simultaneously, so that not all systems need to be upgraded with the security measures at the same time.
- IEC 62351-5: Security for IEC 60870-5 and Derivatives
  IEC 62351-5 provides different solutions for the serial version (primarily IEC 60870-5-101, as well as parts 102 and 103) and for the networked versions (IEC 60870-5-104 and DNP 3.0). Specifically, the networked versions that run over TCP/IP can utilize the security measures described in IEC 62351-3, which includes confidentiality and integrity provided by TLS encryption. Therefore, the only additional requirement is authentication. The serial version is usually used with communications media that can only support low bit rates or with field equipment that is compute-constrained. Therefore, TLS would be too compute intense and/or communications-intense to use in these environments. Therefore, the only security measures provided for the serial version include some authentication mechanisms which address spoofing, replay, modification, and some denial of service attacks, but do not attempt to address eavesdropping, traffic analysis, or repudiation that require encryption. These encryption-based security measures could be provided by alternate methods, such as VPNs or “bump-in-the-wire” technologies, depending upon the capabilities of the communications and equipment involved.
- IEC 62351-6: Security for IEC 61850 Peer-to-Peer Profiles
  IEC 61850 contains three protocols that are peer-to-peer multicast datagrams on a substation LAN and are not routable. The messages need to be transmitted within 4 milliseconds and so that encryption or other security measures which affect transmission rates are not acceptable. Therefore, authentication is the only security measure included, so IEC 62351-6 provides a mechanism that involves minimal compute requirements to digitally sign these messages.
- IEC 62351-7 – Management Information Bases for Network and System Management
  This part will define Management Information Bases (MIBs) that are specific for the power industry to handle network and system management through SNMP-based capabilities. These will support communications network integrity, system and application health, Intrusion Detection Systems (IDS), and other security/network management requirements that are unique to power system operations.

The technology industry has developed two network management technologies: Simple Network Management Protocol (SNMP) for the Internet-based functions (standardized by the IETF), and Common Management Information Protocol (CMIP) as an ISO standard. In each of these technologies, Management Information Base objects must be specified representing the state of different equipment, applications, and systems. Although some MIB objects are generic enough for typical network equipment to be used by the power industry, many specialized MIB objects will need to be developed to represent some of the very specialized equipment and special environments found in power system operations.

IX. Mitigation

A. Defense in depth

Power system operations pose many security challenges that are different from most other industries. For instance, most security measures were developed to counter hackers on the Internet. The Internet environment is vastly different from the power system operations environment. Therefore, in the security industry there is typically a lack of understanding of the security requirements and the potential impact of security measures on the communication requirements of power system operations. In particular, the security services and technologies have been developed primarily for industries that do not have many of the strict performance and reliability requirements that are needed by power system operations.

For instance:

- Preventing an authorized dispatcher from accessing power system substation controls could have more serious consequences than preventing an authorized customer from accessing his banking account. Therefore, denial-of-service is far more important than in many typical Internet transactions.
- Many communication channels used in the power industry are narrowband, thus not permitting some of the overhead needed for certain security measures, such as encryption and key exchanges.
- Most systems and equipment are located in wide-spread, unmanned, remote sites with no access to the Internet. This makes key management and some other security measures difficult to implement.
- Many systems are connected by multi-drop communication channels, so normal network security measures cannot work.

- Although wireless communications are becoming widely used for many applications, utilities will need to be very careful where they implement these wireless technologies, partly because of the noisy electrical environment of substations, and partly because of the very rapid and extremely reliable response required by some applications.

B. LAN / IP Security

Because of the large variety of communication methods and performance characteristics, as well as because no single security measure can counter all types of threats, it is expected that multiple layers of security measures will be implemented. For instance, VPNs only secure the transport level protocols, but do not secure the application level protocols, so that additional security measures, such as IEC 62351-4, provide the application level security, possibly running over VPNs. In addition, role-based access passwords, intrusion detection, access control lists, locked doors, and other security measures are necessary to provide additional levels of security. It is clear that authentication plays a large role in many security measures. In fact, for most power system operations, authentication of control actions is far more important that "hiding" the data through encryption.

As connection to the Internet is (should not be) a factor, since power system operations should be well-protected by isolation and/or firewalls, some of the common threats are less critical, while others are more critical. Although importance of specific threats can vary greatly depending upon the assets being secured, some of the more critical threats are:

- Indiscretions by personnel – employees stick their passwords on their computer monitors or leave doors unlocked.
- Bypass controls – employees turn off security measures, do not change default passwords, or everyone uses the same password to access all substation equipment. Or a software application is assumed to be in a secure environment, so does not authenticate its actions.
- Authorization violation – someone undertakes actions for which they are not authorized, sometimes because of careless enforcement of authorization rules, or due to masquerade, theft, or other illegal means.
- Man-in-the-middle – a gateway, data server, communications channel, or other non-end equipment is compromised, so the data which is supposed to flow through this middle equipment is read or modified before it is sent on its way.
- Resource exhaustion – equipment is inadvertently (or deliberately) overloaded and cannot therefore perform its functions. Or a certificate expires and prevents access to equipment. This denial of service can seriously impact a power system operator trying to control the power system.

C. Procedural Security

1) Communications Network Management: Monitoring the Networks and Protocols:

- Detecting network equipment permanent failures
- Detecting network equipment temporary failures and/or resets
- Detecting network equipment failovers to backup equipment or communication paths
- Detecting the status of backup or spare equipment
- Detecting communication protocol version and status
- Detecting mis-matches of differing protocol versions and capabilities
- Detecting tampered/malformed protocol messages
- Detecting inadequately synchronized time clocks across networks
- Detecting resource exhaustion forms of Denial of Service (DOS) attacks
- Detecting buffer overflow DOS attacks
- Detecting physical access disruption
- Detecting invalid network access
- Detecting invalid application object access/operation
- Ability to detect coordinated attacks across multiple systems
- Collecting statistical information from network equipment; determining average message delivery times, slowest, fastest, etc. and counting number of messages, size of messages
- Providing audit logs and records

2) Communications Network Management: Controlling the Networks:

- Manual issuing of on/off commands to network equipment
- Manual issuing of switching commands to network equipment
- Setting parameters and sequences for automated network actions
- Automated actions in response to events, such as reconfiguration of the communications network upon equipment failure

3) System Management: Monitoring Intelligent Electronic Devices (IEDs)

- Numbers and times of all stops and starts of systems, controllers, and applications
- Status of each application and/or software module: stopped, suspended, running, not responding, inadequate or inconsistent input, errors in outputs, error state, etc.
- Status of all network connections to an IED, including numbers and times of temporary and permanent failures
- Status of any "keep-alive" heartbeats, including any missed heartbeats
- Status of backup or failover mechanisms, such as numbers and times these mechanisms were unavailable
- Status of data reporting: normal, not able to keep up with requests, missing data, etc.

- Status of access: numbers, times, and types of unauthorized attempts to access data or issue controls
- Anomalies in data access (e.g. individual request when normally reported periodically)

4) System Management: Control Actions within Intelligent Electronic Devices (IEDs):

- Start or stop reporting
- Restart IED
- Kill and/or restart application
- Re-establish connection to another IED
- Shut down another IED
- Provide event log of information events
- Change password
- Change backup or failover options
- Providing audit logs and records

D. Password and Key Management

The following discussions are an extract from FIPS PUB 112, Appendix A.

1) Password Usage

a) Introduction

This appendix contains background information, a discussion of the factors specified in the Password Usage Standard and the rationale for the minimum criteria specified in the Standard. It also provides guidance in selecting parameters of password systems based on increasing security requirements. Examples of three password systems meeting increasing levels of security requirements are included.

b) Background

Passwords are the most common method of personal identification used in conjunction with remote terminals to deter unauthorized access to computer systems and networks. The effectiveness of passwords has often been questioned, primarily because they can be easily forgotten or given to another person. However, passwords can provide reasonable deterrence to unauthorized access if properly handled by people authorized to use them and if properly stored and processed in the password verification system. Within its Computer Security and Risk Management Program, the Institute for Computer Sciences and Technology of the National Bureau of Standards developed this Standard for secure password usage to assure reasonable handling, storage and processing of passwords.

Shortly after issuing FIPS PUB 48, NIST published Special Publication 500-9, The Use of Passwords for Controlled Access to Computer Resources. This publication considered the generation of passwords and their effective application to the problem of controlling access to computer resources. Following analysis and use of this document, a project was initiated to establish a fundamental performance standard for the use of passwords and a guideline on how to use this Standard to achieve the degree of protection that passwords were intended to provide.

The Password Usage Standard was developed within the Computer Security and Risk Management Program of the Institute for Computer Sciences and Technology with considerable assistance from representatives of Federal organizations and private industry. In 1980, NIST developed and distributed a draft Password Usage Standard to government and industry representatives for comments and then held a workshop to discuss the benefits and impact of the draft Standard. The draft Standard identified 10 factors to be considered in the implementation of password systems and quantified security criteria in a hierarchical manner for each of the 10 factors. It also proposed five levels of security and specified minimum criteria for each level. The workshop participants felt that the 10 factors were useful in structuring the design of password systems, but that the proposed five levels were unworkable as a basis of a password Standard. As a result of the workshop recommendations, the Standard was revised to specify minimum criteria for the factors of a password system. An Appendix was drafted which provided guidelines for achieving higher levels of security. This revised Standard and the draft guidelines were published for public comment and for agency comment in July, 1981. The received comments were used in revising the proposed Standard and draft guidelines in preparing the published Standard and guidelines.

c) Factors

Ten factors of an automated password system are specified in the Standard. These factors constitute the fundamental elements which must be considered, specified and controlled when designing and operating a password system. The rationale for the factors and for the minimum acceptable criteria for the factors specified in the Standard are provided in the following discussion. Guidance on how to meet the minimum criteria and reasons for exceeding the minimum criteria are also provided.

d) Composition

A password is a sequence of characters obtained by a selection or generation process from a set of acceptable passwords. A good password system has a very large set of acceptable passwords in order to prevent an unauthorized person (or intruder) from determining a valid password in some way other than learning it from an authorized person (i.e., owner). The set of acceptable passwords should be large enough to assure protection against searching and testing threats to the password system (and hence the data or resources that it protects) commensurate with the value of the data or resources that are being protected. The set of acceptable passwords must be such that it can be specified easily, that acceptable passwords can be generated or selected easily, that a valid password can be remembered, can be stored reasonably, and can be entered easily. Composition is defined as the set of characters which may comprise a valid password.

The composition of a password depends in part on the device from which the password is going to be entered. It also depends on how and where the password is going to be stored and how the stored password will be compared with the entered password. Federal Information Processing Standards Publication 1-2 (FIPS PUB 1-2) incorporates the American

Standard Code for Information Interchange (ASCII) which specifies a set of characters for interchanging information between computers. Federal Information Processing Standards Publication 1-2 (FIPS PUB 1-2) defines several proper subsets of this set to be used for special applications. The 95-character graphics subset specified in FIPS PUB 1-2 is the set from which the System Manager and Security Officer should select the acceptable composition for a particular system. While backspaces can be used effectively to mask printed passwords, several comments on the draft guidelines described the special use of backspace in many computer systems and recommended that it not be allowed.

The minimum composition contains 10 characters because some systems (e.g., financial transaction systems) use a 10-digit PIN PAD (Personal Identification Number entry device) for entering the password which is called a PIN. The PIN PAD looks very similar to the keyboard of a push button telephone. Some systems being developed use the push button telephone for data entry and retrieval. Users of these systems stated their desire to use the Standard. A better composition contains 16 characters which includes the 10 digits plus (A, B, C, D, E, F). This set can represent hexadecimal characters, each of which is a four-bit (binary digit) code. For example, 16 hexadecimal characters are used to represent a Data Encryption Standard key (see FIPS PUB 46) which can be used as a personal key in a cryptographic system. Many passwords are composed only of the 26 lower case letters (a-z) or the 26 upper case letters (A-Z). However, using either of these sets often encourages the selection of a person's initials, name, nickname, relative, hometown, or common word easily associated with the person. Even allowing all possible 4-letter, 5-letter or 6-letter English words greatly restricts the number of passwords when compared to all possible passwords of length range 4-6 with the same composition. Totally alphabetic password composition should be discouraged. The best password composition is the 95-character graphic set as specified in FIPS PUB 1-2.

e) Length

Length is closely associated with composition in assessing the potential security of a password system against an intruder willing to try exhaustively all possible passwords. The length of a password provides bounds on the potential security of a system. A length of exactly 1 reduces the potential number of valid passwords to the number of characters in the acceptable composition set. A length of 2 squares this number; a length of 3 cubes this number; a composition of 10 and a length of exactly 4 provides for 10- (read 10 raised to the fourth power) or 10,000 possible passwords. PINs are typically four digits because of low security requirements, for ease of remembering by a large customer base and for speed and accuracy of entry. A PIN verification system generally prevents a person from quickly trying all 10,000 possible PIN's for a particular valid financial account in order to find the valid PIN. If the trial and error process can be automated, even on a small home computer, the valid PIN can be found in a few minutes. Having a length range of 4-6 increases the possible number of PIN's to 1,110,000 (106+105+104).

If all other factors are temporarily ignored, the security provided by a password is directly proportional to the allowed length of the password. In other words, longer passwords are more secure. However, other factors cannot be ignored in practical password systems. Long passwords take longer to enter, have more chance of error when being entered, and are generally more difficult to remember (the latter may not be true unless the password consists of random characters). Sixteen random hexadecimal characters are very difficult to remember and are very difficult to enter quickly and accurately. For this reason, DES keys are usually not personal passwords and vice versa. However, long passphrases can be transformed to virtual passwords of exactly 64 bits (or 56 bits with the other 8 bits recomputed to be parity bits). Long passphrases can be easy to remember but still take longer to enter.

The length range should include a number of lengths, probably from 5-8 characters, and the composition should be a large set so that a high level of security can be provided easily.

A passphrase is an understandable sequence of words (sentence, sentence segment, phrase) that can be transformed and stored as 64 bits, and which is used as a password. A passphrase is generally easy to remember by the owner of the passphrase, and hence is allowed on some systems because of this characteristic. Since the number of distinct possibilities of understandable passphrases is considerably smaller than for a random sequence of characters of the same length, a longer passphrase is preferable to a shorter one. For example, the number of understandable 64-character long passphrases composed using the 27-character set A-Z and space, is considerably less than 2764, which is the number of possibilities if the characters are selected randomly.

A passphrase may be used that is equivalent to a password as specified in the Standard. A passphrase may be transformed into a virtual password by using a transformation such as a hashing function or a cryptographic function. These functions should compute a value using the entire passphrase as input such that any change in the passphrase should result in a different computed value (within some probability). The value that is computed is the virtual password and must be 64 bits as specified in the Standard. This allows all password systems to allocate a maximum of 64 bits for storing each password, and therefore allows up to 264 possible passwords (many thousands of years of security against exhaustive searching attacks). Such a passphrase thus provides the benefits of being easily remembered at the added cost of additional time to enter the longer passphrase and the time needed to compute the virtual password. The Data Encryption Standard (FIPS PUB 46) and the cipher block chaining mode specified in the DES Modes of Operation Standard (FIPS PUB 81) are suggested as the transformation.

f) Lifetime

The security provided by a password depends on its composition, its length, and its protection from disclosure and substitution. The risk associated with an undetected compromise of a password can be minimized by frequent change. If a password has been compromised in some way and if a new password is created that is totally independent of the old password, then the continued risk associated with the old password is reduced to zero. Passwords thus should be changed on a periodic basis and must be changed whenever their compromise is suspected or confirmed.

The useful lifetime of a password depends on several variables, including:

- The cost of replacing a password
- The risk associated with compromise
- The risk associated with distribution
- The probability of "guessing" a password
- The number of times the password has been used
- The work of finding a password using exhaustive trial and error methods

Password systems should have the capability of replacing the password quickly, initiated either by the user or the Security Officer. Passwords should be changed voluntarily by the owner whenever compromise is suspected and should be changed periodically with a maximum interval selected by the Security Officer. The interval may be a period of time or depend on a number of uses. The password system itself should have automated features which enforce the change schedule and all the security criteria for the installation. The system should check that the new password is not the same as the previous password. Very sensitive applications may require that a new password not be the same as any of the previous two, three, ..., N passwords. Such a system requires storage for N passwords for each user. It should not be a requirement of a system that the password for each user be unique. Having a new password rejected for this reason confirms that another user has the password.

g) Source

Passwords should be selected at random from the acceptable set of passwords by either the owner or the password generator. However, this guidance may not be possible in all cases and may not be desirable in some cases. The Security Officer often selects a password for a new user of a system. This can be used for the first access to the system. The system may then require that the user replace this password which the Security Officer may know with a password that only the user knows. Passwords that are created or selected by a user should be checked by the automated password system as meeting all of the criteria of the password system. Passwords that do not meet all the criteria should be rejected by the automated password system. A record that an attempt to select an unacceptable password may be made by some automated systems but is not required by the Standard.

If passwords are generated by the system, the method of generation should not be predictable. Commonly used random number generators that are available in computer systems for statistical purposes should be avoided because the sequence of random numbers that they generate are predictable. The DES algorithm, together with a non-deterministic parameter such as the least significant bits of a high resolution computer system clock may be used. The results of a random generator are then combined with password selection rules to obtain a password which meets mandatory and desirable criteria.

h) Ownership

A personal password should be individually owned rather than owned in common by a group of individuals in order to provide individual accountability within a computer system. This is desirable even though a group of people all have common access privileges to the same resources or data. Individual ownership of personal passwords is required because:

- It can establish individual accountability for the determination of who accessed what resources and for what purposes
- It can establish illicit use of a password or loss of a password
- It can be used for an audit trail of the activities of a user
- It avoids the need to change the password of an entire group when a single member of the group leaves or loses authorization privileges

i) Distribution

A password must be transported from the owner to the authentication system if selected by a user, from the authentication system to the owner if generated by the password system or from the Security Officer to both the owner and the authentication system if generated by the Security Officer. The initial password is often distributed in a different manner than subsequent replacement passwords. The initial password is generally created and issued directly, either orally or in writing, during the meeting at which a user is initially authorized use of the computer system or access to a set of data. This may be a one- time password which must be changed after the initial access request is granted. Changing of a password by a user generally requires that the user supply the old password and then the replacement password. The replacement is checked for meeting the security requirements of the system, checked that it is different than the old password, and then entered into the storage location of the old password. An audit record should be made of the replacement, containing the date and time of the change, but not the new password. Forgotten passwords should be replaced and a new password issued in a manner similar to, if not identical with, issuance of the initial password.

Passwords that are distributed in writing should be contained in a sealed envelope marked "To be opened by addressee only." Delivery may be by courier, internal 'mail, or by U.S. Mail. Instructions to the user should be to:

- Destroy the written password after memorizing it; or
- Return the written password to the Security Officer after signing the receipt for the password and after sealing it in the return mailer.

- Use the password as soon as possible and, if the password can be changed by the user, change the password.

Some systems distribute passwords in a sealed mailer that has been printed by a computer. The mailer is designed so that it cannot be resealed once it is open. The password is printed only on the inside of the mailer on the second page using carbon paper attached to the back of the mailer's front page. The instructions say to remove the front of the mailer, which shows the name of, 'the intended recipient, to destroy the front and save the password (in a protected place readily accessible only to the intended recipient). The part of the mailer that has the password has no other identification which would associate the password with either the system or the owner. Thus, anyone finding a lost password would usually not be able to use it. While not as desirable as memorizing the password and destroying the distribution medium, this system is useful when passwords are not routinely used and would be written in a location which-is more easily associated with the owner.

When distributed by a secure mailer, a receipt for the password may be validated by positive response or on an exception basis. When password distribution is done on an unscheduled basis, a positive response is required. When passwords are distributed regularly, the user should be expecting a new password and should report any failure to obtain a new password. In either case, a record must be kept of the fact that a new password was issued.

There may be a transition period in which it is uncertain if the old password is valid or if the new password is valid. Some systems may allow either password to be valid during the transition period. This means that both passwords must be stored and compared with an entered password. Some systems may have no transition period (e.g., a password becomes valid at 8:06 P.M. exactly) and record attempts at using the old password in an audit file. A report of such attempts should be sent securely to the password owner as notification that usage of an old password was attempted. The owner can verify that the use was an accidental rather than an unauthorized use of an old password by an intruder.

j) Storage

Passwords should be stored in the authentication system in a manner which minimizes their exposure to disclosure or unauthorized replacement. Several methods have been used to protect passwords in storage. Most systems have a password file that can be legitimately read only by the "LOGON" program. The file is protected by a file access mechanism which checks a protection bit in a file access table. Only the privileged LOGON program has access to read the file and only the password program has access to write the file. Some systems separate the password file from the authorized user file. An index file is used to provide the correspondence between the user and the user's password. Some systems encrypt the passwords, either reversibly (two-way) or irreversibly (one-way) using a Data Ecrypting Key (DEK) or the password itself as a key. Of course, any key (e.g., a Data Encrypting Key) retained in storage would also need protection by encryption using a Key Encrypting Key (KEK). The type of protection provided to the passwords should be commensurate with the protection desired for the system or data and hence a protection system should be used to provide the desired protection.

One-way encryption of passwords is allowed in the Standard when encryption is used for stored password protection. One-way encryption systems transform the password in such a way that the original password can not be recovered. This protects the original password from everyone, including the Security Officer and the systems programmers. When a user is logging onto such a system, the password that is entered by the user is one-way encrypted and compared in encrypted form with the stored encrypted password. The same encryption method and key must be used to encrypt the valid password before storage and to encrypt the entered password before comparison.

Two-way encryption of passwords is also allowed in the Standard. Given the correct key, the original password may be determined from the encrypted password. A user entered password may be compared with the decrypted stored password (which was encrypted), or the user's password may be encrypted and compared with the stored password as is done with one way encrypted passwords.

k) Entry

Entry of a password into an automated authentication system in a secure manner is often a difficult task. An observer often is able to detect part or all of a password while the user is entering the password. Typing keyboards are the typical entry device. A user that is not a trained typist often enters the password with one finger. A long, random password that is difficult to enter may be more vulnerable to observation than a short easily entered password. The Standard specifies that a password shall be entered by a user in such a manner that the password will not be revealed to anyone observing the entry process. The following discussion provides some techniques which the user may find useful in achieving this goal and which the computer systems operation staff may find useful in assisting the user.

The computer terminal, keyboard, push-buttons, or password entry device should provide a means for minimizing the exposure of the password during entry. The password should not be printed on the terminal during the entry process. If the keyboard and the terminal display or printer are directly coupled, then the password should be masked by obliterating (understriking) the space where the password is going to be printed. The password may be masked further by overstriking the area after password entry. Computer generated masks used during password entry to disguise the entered password should not always be the same. In any case no printed or displayed copy of the password should exist after password entry.

CRT terminals which use half-duplex communications may present a problem because the password overwrites the understriking and remains visible on the display. The display should be immediately cleared by the password entry program after password entry in such systems. Users should be instructed to manually clear the display following password entry if the screen cannot be cleared by the password entry program.

When submitted as a part of a remote entry batch processing request, the password should be added to the request at the last possible moment and physically protected. Batch processing requests submitted in punched cards should have the password card added by the user just prior to submission. The computer operations staff should maintain the card decks in a protected area and should remove and destroy the password card after the deck has been read by the system. The password should never be printed on any output media. One-time passwords that are distributed to the owner in the form of a password list and sequentially used for sequential batch processing requests may be used. The Standard requires that such lists be physically protected by the owner.

Users should be allowed more than one attempt to enter a password correctly in order to allow for inadvertent errors. However, there should be a maximum number of trials allowed for a password to be entered correctly. A maximum of three (3) attempts is considered adequate for typical users of a computer system. The system should also prevent rapid retries when a password is entered incorrectly. Several seconds should elapse before another password is requested. This prevents an automated, high speed, trial-and-error attack on the password system. A security record should be maintained of the fact that incorrect passwords were entered but the incorrect password should not be kept in the record. A security alarm should be generated if:

- The maximum number of allowed password retries is exceeded;
- The maximum number of allowed failed logons from one terminal is exceeded;
- The maximum number of allowed failed logons for a time period is exceeded.

These parameters must be set according to the sensitivity of the data being protected, the profile of the typical system user and the policy of the organization. Some organizations will be willing to set the parameters high to prevent customer dissatisfaction while other organizations will set the parameters low to prevent security compromises. Terminals should be disabled and users should be denied service if these parameters are exceeded. The Security Officer should be the only one who can enable the terminal and restore the service of the user following these events.

The system should inform the user, following a successful LOGON procedure, of the last successful access by the user and of any unsuccessful intervening access attempts. This will aid in uncovering any unauthorized accesses or attempted accesses which may have occurred between successful accesses. The user can do several actions to prevent an observer from learning the password by watching the password entry process. First, entry of the password can be practiced so that it can be quickly entered using several fingers. Second, the body can be used to prevent the observer from seeing the keys being pressed during password entry. Third, the user can request that a guest not watch the password entry process. Fourth, the user can perform the password entry prior to demonstrating use of the system.

l) Transmission

Passwords are typically used to authenticate the identity of a user attempting to gain access to a shared computer system or network from a terminal. In order to be authenticated, the password is typically transmitted from the terminal to the computer via the communication line between the terminal and the computer. Unless the communication line is physically protected or encrypted, the password is vulnerable to disclosure. Most communication lines between terminals and computers are not afforded this protection at present. Therefore, users should be aware that their passwords can very easily be disclosed via passive wiretapping.

Computer systems can also be easily spoofed. This can occur if an intruder has inserted an active wiretap between a terminal and the computer. The active wiretap can replace one user's password with another user's password, even if the passwords are encrypted at the terminal. Spoofing occurs when the system is fooled into "believing" one user is at the terminal when another user is actually there. Reverse spoofing occurs when a user is fooled into believing that communication is with the intended computer when another computer is there. In the latter case, an authorized user can be spoofed into providing the valid user's password by simulating the "LOGON" request of the intended computer. After the password is obtained, the intruder that is controlling the spoofing computer informs the user that the requested service is temporarily unavailable. During this exchange the intruder has obtained a valid password without the user's knowledge.

These threats can be prevented by one of two encryption methods. First, the communication line between the terminal and the computer can be protected by encryption devices which use a secret key (e.g., a Data Encrypting Key) for encrypting all communication between the terminal and the computer. Transmitted passwords are thus protected from disclosure. In addition each transmission can be numbered so that a previous transmission cannot replace a later transmission (.i.e., a previously used valid password cannot be saved and used to replace an invalid password, even if both are encrypted). Passwords are thus protected to the same degree as the data as specified in the Standard.

Alternatively, the password can be used as the encryption key or as part of the encryption key. Suppose a user enters a password to be used as an encryption key at the terminal (i.e., never transmitted to the computer) and the user's password is retrieved from the computer's memory and used as the encryption key at the computer (i.e., never transmitted to the terminal). Then the terminal and the computer are mutually authenticated if normal communication can occur using the encryption and decryption processes at the terminal and computer, both using the password as the key (or a part of the key). This alternative is also allowed in the Standard.

In order to prevent compromise of the level of security provided by the cryptographic mechanism, the Standard specifies that personal passwords that are used as keys as described above be selected at random from the set of all possible encryption keys used by the cryptographic process. It also specifies that passwords that are used as Data Encrypting Keys should not also be used as Key Encrypting Keys, and vice versa. This is to minimize any possibility of attempting to recover the key (and hence the password) through cryptanalytic techniques.

(a) Authentication Period

Interactive "sessions" between a user and a computer via a remote terminal often last several hours. While security policy should state that a terminal that is "logged onto" a computer should never be left unattended by the user that is "logged onto" the computer, in practice this often occurs. Many systems have a feature which automatically logs a user off the system if the terminal has been inactive for some period of time. This is to prevent someone who encounters an unattended terminal from using it. Some access control systems require that a user be re-authenticated on a periodic basis in addition to the initial authentication process. These systems often antagonize the user if the authentication frequency is set too high. The message that the authentication process must be performed again often comes in the middle of the work that a user is performing. If this work happens to be a large printout of final text of a paper to be published, the user is rightfully upset. For this reason the Standard did not specify a minimum re-authentication period. Re-authentication should only be required to satisfy high security requirements, and then only requested if the terminal has been inactive for a period of time. This should prevent the authentication process from occurring in the middle of some important work.

m) Examples of Password Systems

The following examples of password systems which satisfy various security requirements are provided as assistance to Security Officers and System Managers. Determination of the parameters for each of the 10 factors discussed above will permit the preparation of the Password Standard Compliance Document. These examples should not be considered as the only selection of the parameters for the 10 password system factors.

(1) Password System for Low Protection Requirements

A hypothetical password system might have the following parameters for the 10 factors which will both satisfy the Standard and satisfy requirements for protection which are considered to be minimal. The example is similar to that found in many retail, customer initiated financial transaction systems in which the maximum liability of the customer is $50 and the maximum liability of the bank is limited by the number of transactions allowed per day. This example is also typical of many government-owned, government-leased computer systems in which no sensitive applications are performed. Small scientific systems, special purpose systems and systems not making critical automated decisions may fall in this category. Systems which have limited financial liability and those which require only accountability and control of computer usage and costs may also be considered in this category.

- Length Range: 4-6
- Composition: Digits (0-9)
- Lifetime: l year
- Source: User
- Ownership: Individual (personal password); group (access passwords)
- Distribution: Unmarked envelope in U.S. Mail
- Storage: Central computer on-line storage as plaintext
- Entry: Non-printing "PIN-PAD"
- Transmission: Plaintext
- Authentication Period: Each transaction

(2) Password System for Medium Protection Requirements

Government systems which process limited "sensitive" applications may fall in this category. These are applications which process data leading to or directly related to monetary payments or process data subject to the Privacy Act of 1974. Agency management may determine that additional applications should be designated as sensitive. Computer systems that are subject to fraud, theft, erroneous payments or other loss of sensitive information may also fall into this category. Government systems which make payments (e.g., Social Security, Treasury), keep inventories (e.g., Armed Forces), and process personal information (e.g., Internal Revenue, Service, Department of Education) would be examples of systems which would have requirements of this nature and probably would be satisfied by this type of password system.

- Length Range: 4-8
- Composition: U.C. Letters (A-Z), L.C. Letters (a-z), and digits (0-9)
- Lifetime: 6 months
- Source: System generated and user selected
- Ownership: Individual
- Distribution: Terminal and special mailer
- Storage: Encrypted passwords
- Entry: Non-printing keyboard and masked-printing keyboard
- Transmission: Cleartext
- Authentication Period: Login and after 10 minutes of terminal inactivity.

(3) Password System for High Protection Requirements

Computer systems which process information of a sensitive nature and which rely on passwords to provide personal identification may have high protection requirements that could be satisfied by a password system for personal identification having these characteristics.

Systems having high protection requirement's may include those which have unusually high potential for fraud or theft, have a high economic benefit to a system intruder, and have a substantial impact on safety or the well being of the society. Some computer systems of the Department of Defense or the Federal Reserve Communication System may fall into this category. Systems having very high security requirements may require methods of personal identification which are based on physical characteristics of a person (signature, voice, fingerprint) or on a combination of something unique that the person has (e.g., badge, ID card) and something unique that the person knows (i.e., a password). A risk analysis should be performed for each government owned or leased computer system to determine its security requirements and then a personal identification system should be selected which best satisfies these requirements.

- Length Range: 6-8
- Composition: Full 95 character set
- Lifetime: One month
- Source: Automated password generator within the authentication system
- Ownership: Individual
- Distribution: Registered mall, receipt required; personal delivery, affidavit required
- Storage: Encrypted passwords
- Entry: Non-printing keyboards
- Transmission: Encrypted communication with message numbering
- Authentication Period: Login and after 5 minutes of terminal inactivity.

E. Configuration and Change Control Management

Utilities should have strict procedures and processes in place to control configuration and changes. Access to make changes must be restricted to authorized personnel through the use of change level passwords that aren't common knowledge or factory defaults. Routinely changing passwords for security is a costly and time consuming process but it is highly recommended and should be considered. Access controls or encryption devices in the communication path will be required by regulatory bodies in the future.

Contractors and vendors should never be given the ongoing operating password. Passwords should be changed to a temporary one prior to giving contractors or vendors access to the relays. The passwords should then be changed back or to new ones after the contractors or vendors have completed their work.

F. Protection of IED Maintenance Ports

It is well recognized that the dial-up equipment installed to allow remote access to protective relay IED, now protected only by seldom changed passwords, is an undesirable (even unacceptable) vulnerability. One retrofit solution is to install a cryptographic module between the auto-answer modem and the IED whose access is to be protected. Such a module, when used with appropriate hardware/software at the initiating site, would provide authenticated and authorized remote access to the maintenance port, and encryption of the ensuing traffic to thwart eavesdropping. Proof of concept modules to perform this function were demonstrated at two utilities (DTE Energy and Peoples Energy) in 2005 under DoE NETL Project M63SNL34. Functional requirements for these modules and their key management are described in Report AGA 12 Part 1, developed by an industry panel of experts including strong representation from the electric utility industry

G. Physical Security

Unattended facilities like substations are common elements in the electric industry. Substations contain many of the fundamental critical assets necessary for the transmission and distribution of electric power to customers. Transformers, breakers, busses, switches, capacitor banks, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Intelligent Electronic Devices (IEDs), and communication systems can reside within the confines of the substation. The compromise of any one of these elements can impact the integrity of the electric grid, depending on the amount and type of load being served by this substation at the time of the incident.

While the substation is in many ways the “neuron” of the electrical network allowing effective monitoring and control of electric energy in that particular area of the network, they are attended for very short periods of time. Unlike control centers and most power plants that are staffed around the clock, there is typically no staffing, limited or no roving security patrols, and roofed structures are typically designed to protect electronic equipment and switch gear. Typically, substations out number power plants 30:1 and can be located in a downtown setting or in the most remote of rural areas. While most critical substations will logically be located in or near major load centers, interregional ties located in remote substations may be just as critical for interconnection purposes.

Substations are located in urban, suburban, rural, and industrial/commercial sites and the effectiveness of security methods differs greatly from site to site. Because of the diversity in substation size, location, and criticality, each substation should be assessed and classified. In general, more rigorous security measures should be applied to the more critical substations. While all substations are a critical element in the transmission and distribution of electric energy, not all substations are equally critical to North American electric grid reliability.

This guideline is intended to provide suggestions when considering the physical security at critical substations with a focus on practical methods using existing technology and proven processes. All of the security methods discussed here can be applied to existing substations, whether they are critical or not.

Physical security typically comprises five distinct elements, or systems:

- Delay/Deterrence

- Detection
- Assessment
- Communication
- Response

General Guidelines:

The details included below can generally be implemented with currently available technology.

- Fencing, gates, and other barriers to restrict access to the facility for both safety and security purposes;
- Limiting access to authorized persons through measures such as unique keying systems, "smart locks," access card systems, or the use of security personnel;
- Access control measures to identify and process all personnel, visitors, vendors, and contractors, (i.e., photo ids, visitors passes, contractor ids) to be displayed while in the substation;
- Alarm systems to monitor entry into substation grounds;
- Perimeter alarm systems to monitor forced intrusion into and surveillance of the substation;
- Alarms, CCTV, and other security systems reporting to an attended central security station that can then be evaluated and entity personnel or law enforcement authorities dispatched to investigate a potential problem;
- Guards (special events or targeted substations);
- Vehicle barriers;
- Adequate lighting;
- Signage;
- A comprehensive security awareness program.

Specific Guidelines:

- Each entity should have a security policy or procedures in place to manage and control access into and out of critical substations. These policies should clearly state what practices are prohibited, which ones are allowed, and what is expected of all personnel with access to the substation. The substation security policies should clearly define roles, responsibilities, and procedures for access and should be part of an overall critical infrastructure protection policy.
- The physical security perimeters at each substation should be clearly identified. All physical access points through each perimeter should be identified and documented. Most substations typically have at least two physical security perimeters such as the fence and the control house building. All access points through the substation fences and substation control houses should be identified.
- Physical access controls should be implemented at each identified perimeter access point. All access into and out of critical substations should be recorded and maintained for a period of time consistent with NERC standards. At minimum, these records should indicate the name of person(s) entering the substation, their business purpose, their entity affiliation, time in, and time out.
- Access into and out of critical substations should be monitored with authorization procedures. Substation access may be authorized by the system or security operator if not performed by electronic means such as a card reader where authorization is predetermined. Even if card readers are in place, it is recommended that personnel entering the substation contact the system or security operator so that the station can be tagged as "attended" in the event of an incident.
- Records that identify all entity, contractor, vendor and service personnel that have unescorted access privileges to substations should be identified and documented. While most entity personnel will have unescorted access to all substations, contractors and vendors should only have unescorted access to substations they have contractual business in.
- All contractors and vendors with critical substation access privileges should be required to pass a background screening before being issued an entity-provided contractor ID badge. Only those contractors with entity-issued ID badges should be granted unescorted substation access. Even in these circumstances, an entity employee with unescorted access to the substation should confirm and monitor the contractor's activity while in the substation appropriately.
- A substation incident response program should be established that at a minimum would provide a rapid assessment of events in the substation in order to differentiate normal electromechanical failures from malicious acts. If malicious activity is evident, the priority should be to notify law enforcement and return the substation to normal functionality while preserving forensic evidence where possible.
- Entities should avoid dual use of critical substation grounds for non-critical functions where possible. That is, eliminate or restrict the use of the substation secure area for non-critical activities such as equipment storage, non-critical asset storage, contractor staging, and personal vehicle parking. If dual use is unavoidable, the entity should consider the establishment of another physical security perimeter that excludes the non-critical activities from the substation secure area, or the entire area should conform to this security guideline.

H. *Remote Access*

Guideline Detail:

- Policies and procedures governing use and installation of Remote Access for Electronic Control and Protection Systems, including identifying responsible parties, should be established. These should be reviewed periodically and updated as required.
- Remote Access should only be enabled when required, approved, and authenticated.
- Multi-factor (two or more) authentication should be used. Factors include something "you know" (for example: passwords, destination IP address and/or telephone number), something "you have" (for example: token, digital certificate), something "you are" (for example:

biometrics). Other factors may include: source IP address and/or telephone number, GPS location. These will make access more difficult for unauthorized users and will help to ensure identity of authorized Remote Access users.

- Automatically lock accounts or access paths after a preset number of consecutive invalid password attempts. Consider automatically unlocking the account or access path after a pre-determined period of time or by other methods to ensure safe and reliable system operations.
- Encryption should be used when traversing unsecured networks to gain Remote Access. This will help ensure confidentiality and integrity of any information transfer.
- Approved Remote Access authorization lists should be established. These lists should be reviewed periodically and updated as required.
- Change or delete any default passwords or User IDs. Consider using meaningful but non-descriptive IDs.
- All Remote Access enabling hardware and software should be approved and installed in accordance with Policy. The location and specification of Remote Access enabling hardware and software should be documented and maintained in a controlled manner. Periodic audits should be conducted to ensure compliance.
- Remote Access connections should be logged. Logs should be periodically reviewed.
- Consider risk to the process when allowing Remote Access and specifying hardware and software.
- Policy considerations for Remote Access modems:
- Change default settings as appropriate:
- Set dial-out modems to not auto answer.
- Increase ring count before answer.
- Utilize inactivity timeout if available.
- Change passwords periodically.
- Use callback whenever possible.
- Require authentication before connection.
- Make maximum use of available security features.

Exceptions:

- This security guideline does not pertain to real time transfer of data and control commands.
- This security guideline does not address the integrity or confidentiality of the data on the device or of communications to the device.
- This security guideline does not address measures to preserve the availability of the device (i.e., measures to protect against denial of service attacks).
- There may be some legacy Electronic Control and Protection Systems for which it is technically or economically infeasible to apply all of the specifics contained in this security guideline.

X. Intrusion Detection Systems (IDS)

Although a strong perimeter defense is vital to securing a control/monitoring network and all its access points, studies show that up to 70% of attacks are internally initiated. Thus, an intrusion detection system (IDS) that looks only at external intrusion attempts is clearly not adequate. The encryption modules described above should include intrusion detection capability for both internal and external attempts to guess passwords or bypass the authentication/authorization functions. Upon detection of an intrusion attempt, the IDS function may shut down further communications through that link or may log the event and report the incident via existing communication links or via an alarm point on an existing SCADA system. Such reporting should ideally go to the person responsible for investigating intrusion attempts, and not to the SCADA operators.

XI. Recovery/Remediation from a Cyber Attack

In the event that a cyber attack is discovered on a relay, it is critical to make a full assessment of the situation as quickly as possible due to the following:

- The incident is unlikely to be an isolated incident
- Left unmitigated, more attacks may occur

Recovery and remediation will require the user to determine five things regarding the attack: Who, What, Where, When, and Why. Depending on the security features of the device and administrative procedures in effect, it may not be possible to determine all of these parameters. In such cases, consideration should be given to upgrading relay technology and installation/maintenance procedures to provide a better analysis of the attack. Without understanding the Who, What, Where, When and Why, it will be very difficult to develop an effective remedial plan to prevent attacks in the future.

- ▪ Who

The source of the attack needs to be identified to determine how to best prevent future attacks of this nature. If the source is an outside agency without authorized access (direct, or remote) to the relay, technical solutions will be the primary remediation. If, on the other hand, the source is determined to be someone with authorized access to the relay (employee, contractor or authorized third party) procedures such as modification of password policies, background checks, restrictions on laptop/configuration software use may be the key. It is strongly recommended that individual passwords or some other mechanism be employed to determine (or at least or narrow down the list) of who the attacker is. If the technology is not available to determine Who from the device itself, frequently the other parameters, when determined, will provide some insight to the attacker’s identity.

Of paramount concern will be the situation where the attacker is identified as an employee, contractor or authorized third party. In such case, the user will need to consider any other sites that the attacker had access to and inspect for other similar activity.

- ▪ What

What the attack was, or in other words, the nature of the attack, needs to be thoroughly analyzed. The type of attack will have a major impact on the recovery and remediation of the attack. For example:

- o If data theft (e.g., configuration upload) has occurred, the user must consider if passwords have been compromised. Personnel will typically reuse passwords for similar applications and the compromising of those passwords creates a larger issue within the user's environment. Recovery in this instance may include the wholesale change of all protective relay and configuration software passwords.

- If settings have been changed to render faulty operation, the user should look to similar devices to see if changes have been made there as well.

Also, the nature of the change may provide a clue to the source. Subtle changes, such as raising/lowering target values may indicate a person with specific knowledge about the user's facilities and perhaps access to the device's configuration software. Badly corrupted configurations or blindly operated points which are easily detected may suggest an outside hacker.

- Where

Where the attack took place is a two-fold question; where in terms of the location of the asset (e.g., substation location) and where in the substation (which relay(s), communications processors, dialers, et. al).

Identifying the substation itself may be important if the attack is determined to be from a threat with access to the station. If the threat is traced to a contractor, for example, all stations in which the contractor had access will need to be evaluated for the possibility that they too have been attacked. Attacks which are limited to a geographical area will similarly help to identify which personnel may be involved.

The other aspect is which relays or other devices in the protective relaying scheme have been attacked. Important to determine are the brand, model, firmware version of the device attacked to provide further clues on both the nature of the attack and the probability of widespread attack elsewhere on the system. Benefits of this information include:

- Gaps in security for various products can be brought to the vendor's attention for technical remediation.
- Vulnerable devices can be removed from the system or restricted in access by procedural means.
- Inspection of other substations can be more easily facilitated if the user knows where to look (which relays) and what to look for.

- When

When the attack took place can be an important tool in determining WHO. Knowing when can allow the user to correlate the attack with authorized personnel movement and work shifts, vendor and contractor site activities, hacker activity (e.g. attacks occurring from another time zone).

The attacks may also be correlated to other activities and procedures such as the installation of new firmware, password changes, employment changes, labor disputes/negotiations, activities, (internally and externally), communication system changes.

- Why

Though not a technical issue per se, WHY an attack took place is an important step in the prevention of future attacks. Hackers and outside agents attack for gratification and to further their causes, and little be done other than to harden assets from a technical nature and assist law enforcement with the apprehension of those responsible. But attacks generated by disgruntled employees, contractors, or vendors are the most difficult to detect/prevent and consideration must be given to preventing situations which would cause someone to seek redress through this method. Correlation of such attacks to cause can be useful in the prevention of future attacks. Users can and should monitor the temperament of any personnel (internal, contractors, vendors, system integrators) who could launch such an attack and address concerns before they lead to cyber attacks, or escalate security measures in the event that confrontation is expected.

XII. Technology on the horizon

There are currently several standards organizations such as IEEE and ISA addressing control system cyber security standards and several reputable companies developing products to help in this arena. Forthcoming standards will address recommended practices including graded approaches to retrofitting existing SCADA systems.

XIII. Recommendations

- Establish a broad corporate security policy based on its recommendations, tailored to the needs of protective relay systems
- Assess existing communications channels for vulnerabilities to intrusion
- Implement and enforce policies re computer usage, remote access control, with frequent auditing of systems and policies. Emphasize that security is not a part time ad hoc function. Have certain people in the utility be accountable for security (not IT, or not IT only)
- Where appropriate, add policies, procedures and hardware (cryptographic modules) to vulnerable communications channels and access ports.
- Monitor logs – see what is happening to the equipment/system
- Monitor traffic – who is getting access
- Maintain and monitor a list of authorized personnel who have password or authenticated access

The following section discusses selected aspects of the various means of protecting systems. These means include:

- Physical protection ("guards and gates"). This is always a consideration. Where possible, physical protection should always be provided. Many attacks are simplified by physical access to equipment. However, in electric power systems there are numerous situations under which physical protection is difficult or impossible, including equipment located on customer premises or in small, remote substations.
- Isolation. This is the traditional means of information security protection. For communications, it has

sometimes been called "air gap security." Isolation usually requires physical protection, with both physical and electronic access limited to a small group of trusted individuals.

- Access control. This is the mediation of access by security functionality within the system. Isolation can be considered a very coarse form of access control, and finer-grained access control is usually required even in isolated systems to prevent inadvertent errors and to provide protection if one of the trusted individuals is compromised.
- Logging and auditing. Logging security-relevant activity and auditing the logs can be used as a means of detecting and deterring malicious activity. In some cases, it is inadvisable to prevent access, such as in emergencies where arrangement of proper access authorization may be difficult. However, malicious activity can be deterred by logging emergency activity and auditing the logs for suspicious situations. Intrusion detection can be regarded as a form of real-time auditing.
- Encryption. This technology has many important uses in protective systems.
- "Security Through Obscurity" is not a valid protection. The notion that obscure technology is protective is a common misconception that is frequently attacked by security experts. Indeed, a fundamental principle in encryption systems is due to Kerckhoffs who stated in 1883 that a system should remain secure even when the adversary has all the information about its operation other than secrets such as passwords and encryption keys.

The following sections discuss various forms of access control and other security functions.

A. Role-Based Access Control (RBAC)

Role Based Access Control essentially implements the separation of duty approach that has long been taken by businesses in protecting the integrity of their business processes and critical data. Interest in RBAC arose as a result of an evaluation of information security technology, which at one time was focused on the confidentiality needs associated with military and diplomatic matters. Recognition that business (and some government) applications are more focused on the need for integrity resulted both in the development of the Common Criteria for Information Security Evaluation (ISO 15408) and research attention to RBAC. Indeed, one of the first examples of a Protection Profile prepared and published using the Common Criteria was a specification for evaluating RBAC.

The description of RBAC presented here is based on a proposed standard for RBAC prepared by NIST (available at http://csrc.nist.gov/rbac/). Under the proposed standard, RBAC deals with the elements of Users, Roles, Objects, Operations, and Permissions. A user is a person, but can be extended to a process. A role is a job function within the context of an organization. A user may be assigned multiple roles and a role may be occupied by multiple users, although the relationship between users and roles may be limited by constraints. Objects and operations depend on the system context. For example, in a DBMS an object may be a table and an operation may be a select or update. A permission is the approval to perform the operation on the object.

Core RBAC requires the capabilities to manage assignment of users to roles and manage assignment of permissions to roles. It requires that a user be able to assume multiple simultaneous roles. The proposed standard describes this as capturing the functionality of group permissions in current operating systems.

Hierarchical RBAC introduces role hierarchies, with senior roles in the hierarchy inheriting the permissions of their juniors and users assigned to senior roles being assigned as well to the associated junior roles. Constrained RBAC introduces separation of duty relationships, which are static or dynamic constraints on the roles to which a user can be simultaneously assigned. An example of a static constraint is that a billing clerk is never allowed to also be an accounts receivable clerk. An example of a dynamic relationship is that the originator of a document is never also allowed to be the approver of the same document, but may approve other documents.

B. Discretionary Access Control (DAC)

Discretionary Access Control is the traditional "user-group-other/read-write-execute" type of control traditionally found in operating systems and DBMS's. It is also the kind of control provided by access control lists. Under DAC, the owner of the data or file essentially has discretion to provide access to whoever the owner determines should have access. The system enforces the owner's access decision, but does not otherwise enforce constraints on access to the data. DAC is one means of enforcing Need-to-Know, where it is assumed that the security structure and policies are such that the "owner" of data knows who has need-to-know.

C. Mandatory Access Control (MAC)

In the traditional definition of Mandatory Access Control, objects (e.g., data) and subjects (e.g., users, devices) are given sensitivity labels according to a hierarchy. The label is part of the access control associated with the subject or object. Security policies govern the access and movement of objects by subjects. The most well-known MAC security policy is the "Bell LaPadula Security Model" that prohibits a subject having a lower level sensitivity label from reading an object having a higher sensitivity label and also prohibits a subject having a higher level sensitivity label from writing an object to a subject (e.g., a user directory or a printer) having a lower sensitivity label. The policy is often summarized as "No read up, no write down" and is enforced by the operating system.

There is a new, broader definition of MAC growing out of research at the US National Security Agency (NSA). This approach views MAC as comprising any security policy where the definition of the policy logic and the assignment of security attributes is tightly controlled by a system security policy administrator. Ten years of NSA research, combined with a goal of transferring the resulting technology, led to the development of Security-Enhanced Linux. (SE-Linux). This is one of the most important new concepts for improvement of Linux security (and indeed for advancement of operating system security in general). The requirements for SE-Linux are discussed in a paper "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments" by Peter A. Loscocco, Stephen D. Smalley, and others, published in Proceedings of the 21st National Information Systems Security Conference, pages 303-314, October 1998 (available at http://www.nsa.gov/selinux/inevit-abs.html).

SE Linux combines RBAC with another security method known as Type Enforcement. The traditional Multi Level Security sensitivity labels can also be implemented using these methods. These security methods are used in conjunction with a set of user defined policies. The RBAC and Type Enforcement create a large number of categorizations including object classes, domains, types, and roles. For example, object classes include processes, files, directories, character device, block device, socket, and numerous other system elements. Within each object class there may be a number of types. For example, there may be a type associated with a specific operating system function, such as creation of the system log. User defined policies could even extend types to specific user functions, such as sending commands to substation devices. Users and processes are also assigned roles, such as ordinary user, system administrator, dispatcher, maintainer, purchasing agent, financial auditor, and other organization related categories. Sensitivity labels can be optionally used to identify data according to categories of consequences resulting from unauthorized disclosure, alteration, destruction, or denial of use.

In SE Linux, all accesses and transitions among objects of various types and users of various roles are governed by permissions defined by policy rules and enforced by a reference monitor that is part of the operating system kernel. The permissions are much more fine grained than in current Linux systems. For example, existing Linux systems define permissions of read, write, and execute but SE Linux permissions may also include create, get attributes, set attributes, create hard link, lock/unlock, mount, unmount, and others. SE-Linux can also be configured to eliminate the concept of a "superuser," common in many operating systems, who is privileged for all system capabilities.

A project is ongoing to provide support in Linux kernel for loadable kernel modules that can implement a variety of security improvements and security hardened versions now offered as kernel patches. Security-Enhanced Linux is one of the security modules expected to be included. SE Linux software, documentation, and related publications are available for download from the NSA web site.

D. Authentication

Authentication is the process of determining that the user is authentic, i.e., that the user is who the user claims to be. This is done by receiving information about the user and comparing the received information to a stored version of the information for the authentic user. Up to three factors may be used:

- Something the user knows, such as a password
- Something the user has, such as a device or smartcard, usually identified by some kind of encrypted information. Some devices automatically change the information periodically in synchronism with other software or devices in the authentication system.
- Something the user is, essentially data regarding a biometric characteristic of the user, such as a fingerprint or eyeball pattern, generally stored in some encryption protected format.

There are numerous ways in which an authentication system can be attacked and compromised. These include various means of tricking a user into revealing a password, various strategies for guessing passwords and validating the accuracy of the guesses, and various methods of capturing passwords (or other authentication information) as it moves in the system. There are also ways in which an authentication system can be bypassed, essentially involving attacks on the security of the overall system.

E. Captured User Approaches

A captured user approach involves "capturing" or "jailing" the user to prevent any access to capabilities that a malicious user could exploit to engage in unauthorized activities on the system. For example, this would generally involve sending the user from system login directly into a menu system from which the user can't escape. Sending the user into the menu system generally involves a function that is automatically executed upon startup of a computer or upon user login. However, there are a wide variety of system functions that must be blocked to ensure that the user remains captured.

In general, the capturing fails if a user is able to access a system prompt, or also in the case of interpreted languages an interpreter prompt, that enables access to commands that can be used for performing functions that support disallowed activity. Among other things, this may mean that the user must be prevented from starting the system or logging in without going through the auto-execute function that starts the menu system. It means that functions that can stop a process and return to the system prompt (such as Control-C or Control-Z on some systems) must be disabled. It means that any exception that could result in a crash leading to a language interpreter prompt must be handled and returned instead to the menu system. It is best if functionality not needed by a legitimate user is not present on the system.

Captured user approaches are good for purposes such as specialized kiosk-type terminals having well-defined, limited uses. Also, any user accessing a web page is essentially a captured user of the system containing the web server.

F. Encryption

Encryption is another important security protection used in both stand-alone systems and networks. Encryption modifies a file or message so it can not be read without reversing the modifications using another piece of information called an encryption key (often shortened to key). The modifications usually involve substituting characters for those in the message or transposing (rearranging) the locations of either the original message characters or the substituted characters. The key provides data needed for controlling the substitutions and transpositions. The calculations are performed according to an encryption algorithm. Sometimes, for user convenience, the encryption key is generated from a password as part of the algorithm.

Encryption technology can be used for a variety of purposes. Examples include encryption of messages sent over communication lines, encryption of passwords stored on a computer, exchange of encryption-based information to authenticate user identity, creation of encryption-based checksums (called hashes) to verify the integrity of transmitted data, and use of encryption technology to digitally sign documents. There are a variety of methods for digital signature, all relying on encryption for verifying that a document originated from a particular source. Most of these methods use public key concepts that are discussed in the next section.

1) Key management and public key cryptography

Management of the encryption keys is a major issue in managing an encryption system, and tends to drive the technology of encryption systems. It is also a major source of vulnerability exploited in code-breaking.

The most convenient system is one in which the key is automatically generated from a short password used over and over again. The password can be the same for all users or different for different groups of users. However, this system is also less secure. The more often the password is used, the greater is the opportunity for compromise. There are also the issues of choosing the passwords themselves, deciding how often they should be changed, and securely providing this information to all the users.

A common practice in key management is to use a hierarchy of keys having various lifetimes. The higher level keys in the hierarchy are used only for the purpose of exchanging lower level keys. The lowest level key in the hierarchy is called the session key and is used only for encrypting a limited number of messages.

Another problem in key management occurs when the sender and recipient have not been able to prearrange a key or password. This situation can be expected to occur often in electronic commerce. One solution is to use a trusted third-party with whom both sender and receiver have already prearranged keys. Another solution is known as public key cryptography. This solution uses a pair of related mathematical functions, one of which is easy to calculate and the other of which is very difficult. One pair of such functions is multiplication and factoring. It is easy to multiply large numbers but very difficult to factor a large number into its prime components.

The approach offered by these solutions is to provide two keys, one a public key that is published and made available to potential senders and the other a private key that is kept secret by the owner. A message encrypted using the public key can be decrypted only with the private key and vice versa.

Public key cryptography is often used as a means of facilitating key management and as an adjunct to other systems of encryption. For this purpose, the public key cryptography is used for exchanging session keys in the other encryption system. Public key cryptography is also used as a means of digital signature. A signature encrypted with a user’s private key can be verified using the associated public key.

The most secure encryption method -- called the one-time pad – was developed in 1917 for use in World War I and uses a key that is completely random and is as long as the message to be sent. Only two physical copies of the key exist, one for the message sender and the other for the message recipient. The key is used once and then destroyed. The problem with this type of system is that enough key material to handle all messages has to be prepared and securely distributed to every sender and every recipient. The material has to be securely stored and destroyed after use. If a sender and recipient run out of key material, they cannot send and receive messages until fresh key material arrives at both locations. This system is very secure -- theoretically unbreakable if the key is derived from a random physical process -- but very inconvenient. However the system becomes subject to codebreaking if the key material is used more than once, e.g., if a message must be sent and there is no fresh key material available.

In a layered communications protocol system there is a tradeoff in the placement of the encryption in the protocol stack. Placement near the application layer allows the encryption to be tailored to the importance of the data and ensures that only the application itself actually sees the unencrypted data. However, this placement also exposes information about message flows such as date, time, addressee, message length, and (if the protocol system has a capability for priority transmission) other information such as the urgency of the message. Placement close to the physical layer can conceal message flow information but also exposes the information within the node outside the using application. Placement in both locations provides better protection but creates a more complex system.

Even with successful encryption an eavesdropper can still obtain information by watching a data stream. The technique for doing so is called “traffic analysis” and was also developed during World War I. It involves watching the patterns of message activity and correlating these patterns with the observable operational situation. When a pattern repeats, it can be inferred that the corresponding operational situation is occurring. Defeating traffic analysis requires that communications channel activity be modified to avoid patterns, such as by keeping channels active with dummy traffic in the absence of actual message traffic, or by taking other steps to avoid allowing patterns to be correlated with operational conditions.

XIV. Conclusions

One issue is how to decide what needs to be secured within a security policy. Some contend that every asset needs to be secured. However, this approach makes security deployment/adoption costly and could prevent entities from even attempting to deploy security. Therefore, all assets do not need to be secured, although all assets could be secured. However, all assets should be analyzed in regards to the need of security.

Protection and securing of networked communications, intelligent equipment, and the data and information vital to the operation of the future energy system is one of the key drivers behind developing an industry-level architecture. Cyber security faces substantial challenges both institutional and technical from the following major trends:

- Need for greater levels of integration with a variety of business entities
- Increased use of open systems based infrastructures that will comprise the future energy system
- The need for appropriate integration of existing or “legacy” systems with future systems
- Growing sophistication and complexity of integrated distributed computing systems
- Growing sophistication and threats from hostile communities

Security must be planned and designed into systems from the start. Security functions are integral to the designs of systems. Planning for security, in advance of deployment, will provide a more complete and cost effective solution. Additionally, advanced planning will ensure that security services are supportable (may be cost prohibitive to retrofit into non-planned environments. This means that security needs to be addressed at all levels of the architecture.

Security is an ever evolving process and is not static. It takes continual work and education to help the security processes keep up with the demands that will be placed on the systems. Security will continue to be a race between corporate security policies/security infrastructure and hostile entities. The security processes and systems will continue to evolve in the future. By definition there are no communication connected systems that are 100% secure. There will be always be residual risks that must be taken into account and managed. Thus, in order to maintain security, constant vigilance and monitoring are needed as well as adaptation to changes in the overall environment.

Security assessment is the process of assessing assets for their security requirements, based on probable risks of attack, liability related to successful attacks, and costs for ameliorating the risks and liabilities. The recommendations stemming from the security requirements analysis leads to the creation of security policies, the procurement of security related products and services, and the implementation of security procedures.

Security re-assessment is required periodically. The re-evaluation period needs to be prescribed for periodic review via policy. However, the policy needs to continuously evaluate the technological and political changes that may require immediate re-assessment.

Security policy generation is the process of creating policies on managing, implementing, and deploying security within a Security Domain. The recommendations produced by security assessment are reviewed, and policies are developed to ensure that the security recommendations are implemented and maintained over time.

Security deployment is a combination of purchasing and installing security products and services as well as the implementation of the security policies and procedures developed during the security policy process. As part of the deployment aspect of the Security Policies, management procedures need to be implemented that allow intrusion detection and audit capabilities, to name a few.

Security Training on security threats, security technologies, corporate and legal policies that impact security, Security measures analysis is a periodic, and best practices is needed. It is this training in the security process that will allow the security infrastructure to evolve.

Security audit is the process responsible for the detection of security attacks, detection of security breaches, and the performance assessment of the installed security infrastructure. However, the concept of an audit is typically applied to postevent/incursion. The Security Domain model, as with active security infrastructures, requires constant monitoring. Thus the audit process needs to be enhanced.

When attempting to evaluate the security process on an enterprise basis, it is impossible to account for all of the business entities, politics, and technological choices that could be chosen by the various entities that aggregate into the enterprise. Thus to discuss security on an enterprise level is often a daunting task that may never come to closure. In order to simplify the discussion, allow for various entities to control their own resources and to enable the discussion to focus on the important aspects.

XV. Appendix – NERC Cyber Security Standards

NERC Standards CIP-002-1 through CIP-009-1 were approved in May, 2006. The purpose of the standard is “To reduce the risk to the reliability of the bulk electric system from any compromise of critical cyber assets (computers, software and communication networks) that support these systems.

Table VII

Requirement	Implication for Relays

Requirement	Implication for Relays
CIP002 R1 and R2 require responsible entities to identify their critical assets using methodology based on risk assessment.	The methodology must consider substations and “special protection systems” that support reliable operation of the bulk power system and systems/facilities critical to automatic load shedding of 300 MW or more.
CIP002 R3 requires identification of critical cyber assets, defined as being essential to operation of critical assets.	Relays would be included if related to critical assets.
CIP003 R1 and R2 require a cyber security policy with senior management leadership covering all cyber critical assets.	Relays identified under CIP002 would be covered under the policy.
CIP003 R4 and R5 require a program to identify, classify, and protect information associated with cyber critical assets and to provide access control to that information.	Relays identified under CIP002 would be covered under the program.
CIP003 R6 requires a configuration management program to control any changes in hardware or software associated with cyber critical assets	Relays identified under CIP002 would be included in this configuration management and change control.
CIP004 R1, R2, and R3 require cyber security awareness training, cyber security policy/procedure/access training, and personnel risk assessment (i.e., a background investigation and clearance process) for all personnel having physical or cyber access to critical assets.	Personnel having physical or cyber access to critical relays would be included.
CIP004 R4 requires revocation (within specified time periods) of cyber access to critical cyber assets when personnel no longer require access.	For relays, this would require either individual log-ins or systems to change common passwords on all relays accessed by a revoked individual.
CIP005 R1 and R2 require establishment of electronic security perimeters covering all cyber critical assets and access controls at all points of entry to those perimeters.	Relays are included, if identified as cyber critical.
CIP005 R3 and R4 require electronic monitoring and logging of security perimeters, and annual vulnerability assessment of cyber critical assets.	Relays are included, if identified as cyber critical.
CIP006 requires physical security for all cyber critical assets	Relays are included, if identified as cyber critical.
CIP007 places a number of detailed requirements, including test procedures for security-relevant software changes, disabling of unneeded ports and services, management of security patches, malware prevention, access authentication and account management, control of shared accounts and privileges, password construction, security event monitoring, and others.	Relays are included, if identified as cyber critical.
CIP008 requires a cyber security incident response plan	The plan would have to include incidents affecting relays, if identified as cyber critical.
CIP009 requires a recovery plan for cyber critical assets.	Cyber critical relays would have to be included in recovery plans.

XVI. References

[1] NETL Project M63SNL34 “Cyber Security for Utility Operations” Final report of this project is available from DoE Office of Energy Assurance or from Sandia National Laboratories

[2] AGA 12 Part 1 “Cryptographic Protection of SCADA Communications Part 1 Background, Policies and Test Plan” available from Gas Technology Institute

[3] Security Guidelines for the Electricity Sector. Version 1.0 June 14, 2002

[4] PSRC C3 Processes, Issues, Trends and Quality Control of Relay Settings

[5] Pilot Protection Communications Channel Requirement, S. Ward et. al., Georgia Tech, May 2003

[6] Electronic Security of Real-Time Protection and SCADA Communications. Allen Risley, et al. Schweitzer Engineering Laboratories, Inc. WPDAC, April 2003

[7] Shea, Dana, “Critical Infrastructure: Control Systems and the Terrorist Threat” Updated February 21, 2003, Report For Congress, Order Code RL31534

[8] IEC TC57 WG15 Security Standards – White paper by Xanthus Consulting International

[9] NERC – Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems. Version 1.0. Effective Date: June 10, 2003

[10] FIPS_PUB_112–AppendixA http://www.itl.nist.gov/fipspubs/fip112.htm

[11] Role Based Access, a proposed standard for RBAC prepared by NIST, available at http://csrc.nist.gov/rbac/

[12] The requirements for SE-Linux are discussed in a paper “The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments” by Peter A. Loscocco, Stephen D. Smalley, and others, published in Proceedings of the 21st National Information Systems Security Conference, pages 303-314, October 1998, available at http://www.nsa.gov/selinux/inevit-abs.html)

[13] SE Linux software, documentation, and related publications are available for download from the NSA web site (http://www.nsa.gov/selinux/)