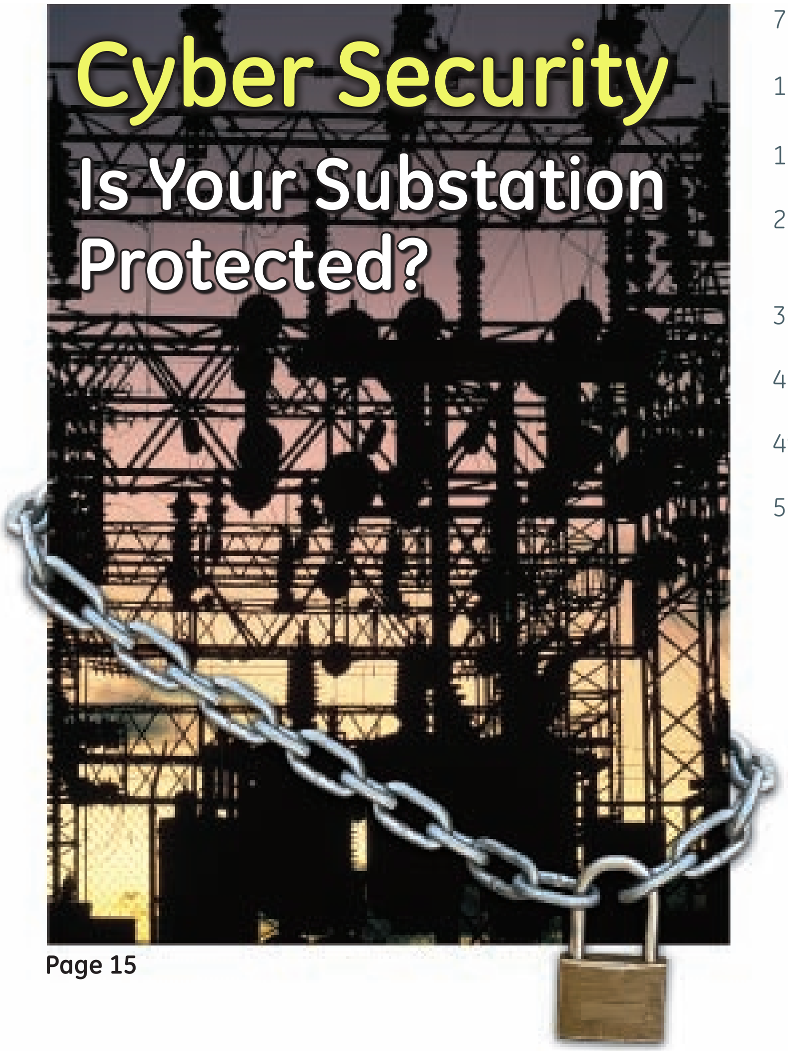
Engineering Quicktip - Enhancing Your Systems Security pg 81

Protection & Control Journal

May 2008

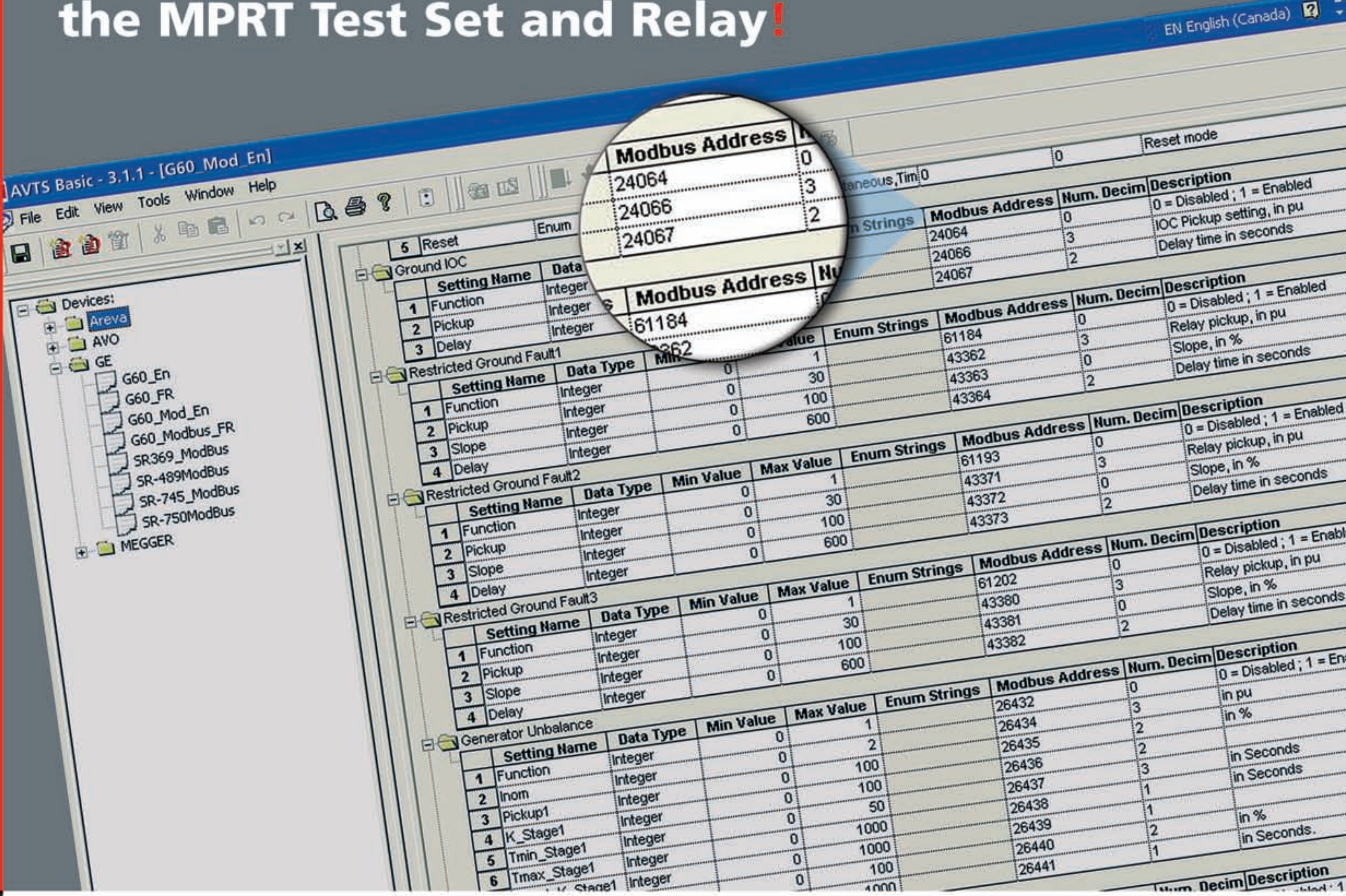


Page 15

Digital Energy
Multilin

www.GEMultilin.com

$19.95 USD



EN English (Canada)
AVTS Basic - 3.1.1 - [G60_Mod_En]
File
Edit
View
Tools
Window
Help
Devices:
Areva
AVO
GE
G60_En
G60_FR
G60_Mod_En
G60_Modbus_FR
SR369_ModBus
SR-489ModBus
SR-745_ModBus
SR-750ModBus
MEGGER
Modbus Address
24064
24066
24067
Modbus Address
61184

Megger MPRT 8430

Protection & Control Journal

Protection & Control Journal
December 2007
In-depth Analysis: Capacitor Bank Protection
D90Plus
C70
Multilin
www.GEMultilin.com

Stay Current

Get your FREE subscription today

To receive future publications of the Protection & Control Journal, sign up at:
www.GEMultilin.com/journal

Advertising Opportunities

Learn more about how to reach today's protection and control professionals.
www.GEMultilin.com/journal

Submit Articles

To submit articles to be considered for inclusion in a future issue of this journal email:
gemultilin@ge.com

The Protection and Control Journal is a unique publication that presents power system protection and control engineers with a compilation of relevant and valuable documents. GE Multilin grants permission to educators and academic libraries to photocopy articles from this journal for classroom purposes. There is no charge to educators and academic libraries provided that they give credit to the Protection & Control Journal and GE Multilin. Others must request reprint permission from GE Multilin.

The Protection & Control Journal is published by GE Multilin, 215 Anderson Avenue, Markham, Ontario, Canada, L6E 1B3. All rights reserved. GE and ⓖ are trademarks of the General Electric Company.

ISSN 1718-3189

Protection & Control Journal

May 2008

Contents

Inside the Cyber Security Perimeter
What you need to know to be protected
15

Richard Hunt
Application Engineer

Editorial

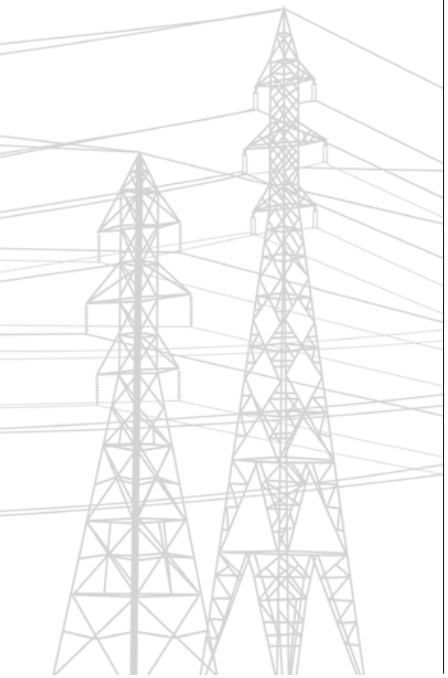
The Need for Security in Today's Electrical Infrastructure

Hackers. Phishing. Identify theft. Keyboard loggers. Computer viruses. Spyware. Denial of service. All terms we have become familiar with, as we've increased our use of the Internet for communications, shopping, and finance. Criminals and vandals have used widespread access to the Internet to steal or destroy our personal data and even identity. Spyware scanners. Virus scanners. 128-bit encryption. Passwords. More terms we wish we didn't have to become familiar with, as we try to keep our data and communications secure.

Now think about your electrical infrastructure and your expectations for high continuity of electrical service. By counting the large number of appliances and equipment that need electricity to run, it's not difficult to appreciate our reliance on electrical power and the incredible value placed on keeping electrical grids strong. Electric utilities have also increased their reliance on the Internet and communications networks to provide the basic control infrastructure to operate the electrical grid. The widespread use of communications increases the possibility of an individual or group maliciously attacking our electrical infrastructure. And the risks are great. During a recent event in the United States, over half a million customers lost electric service. 38 substations, 26 transmission lines, and 2 power generators all went off line, due to an operator mistakenly shutting off part of the protection system during routine testing. So imagine what a coordinated attack on the system could do.

The North American Electric Reliability Corporation (NERC), the electric utilities, and suppliers to the electric utility industry, have recognized the possibility of "cyber" attacks on the electrical grid. NERC has established the Critical Infrastructure Protection Committee (CIP) to address the challenges in cyber security. NERC, through the CIP, has issued 9 standards governing the protection of cyber assets: protecting those pieces of the grid that could be directly impacted by incorrect control via communications.

The standards issued by NERC are regulatory standards that set performance requirements, but do not set technical requirements. Both utilities and suppliers to utilities are scrambling to determine what the actual technical requirements are for cyber asset protection. Does cyber asset protection mean simply setting strong passwords? Establishing private communications networks that are physically separate? Eliminating the use of the Internet and Ethernet-based communications? The communications infrastructure of electric utilities is in place to provide reliable control of the electric grid during normal, and abnormal, operating conditions. So more importantly, will implementing cyber asset protection impact the operations, and therefore the reliability, of the electric grid?



This issue of the Protection & Control Journal focuses on the topic of cyber asset protection, commonly known as cyber security. The technical whitepapers in this issue don't answer all of the questions concerning the implementation of cyber security. They do, however, illustrate the various threats to electrical infrastructure security, bring clarity to the requirements and expectation of regulatory bodies, and provide recommendations and solutions for maintaining a robust security system. Hopefully, the information in these papers will help guide more informed decisions in implementing cyber asset protection systems and procedures.

VIRELEC LTD.

From Concept to Commissioning

Virelec has delivered systems for many utilities and industrials across Canada and in the USA. Let our team of knowledgeable professionals help you with your P&C or SCADA project.

Protection, Control and SCADA Systems

Virelec is an experienced supplier to the industry, offering engineering design, procurement, panel manufacture, system integration, testing and site commissioning.

System Engineering

In addition to detailed protection design, Virelec offers power system load flow, short circuit and relay co-ordination studies.

Drop-in Control Houses

Virelec offers this new method of delivering P&C systems. The complete building envelope containing panels, AC/DC distribution, batteries and auxiliaries is cabled, tested and pre-commissioned at Virelec's factory ready for field equipment cabling.

IED Engineering and Support

Integrating modern IED's into a system requires highly specialist skill sets. Virelec's experienced team offers relay setting and programming, IED and network configuration as well as site commissioning.

Call us at 905-569-8030
E-mail: info@virelec.com
Virelec Ltd., Mississauga, Ontario

NERC Critical Infrastructure Protection: Cyber Asset Protection

Rich Hunt
GE Digital Energy, Multilin

1. Introduction

The NERC Critical Infrastructure Protection Committee (CIPC) specifically develops procedural standards related to the protection of the cyber assets within an electric utility. NERC standard CIP-002-1 Critical Cyber Asset Identification requires the identification of critical assets such as control centers, bulk transmission substations, generation resources, load shedding schemes, and special protection systems, and the cyber assets essential to the operation of these critical assets. NERC standard CIP-005-1 Electronic Security Perimeter requires procedures for access request and authorization for communicating to these critical cyber assets, and CIP-007-1 Systems Security Management requires procedures, such as passwords and password management, be in place to prevent unauthorized access to critical cyber assets.

NERC standards are procedural standards, they define the "What" and "Why", but do not define "How" to implement proper protection of critical cyber assets. As utilities look to implement protection of critical cyber assets, they will look to the suppliers of various cyber assets, such as protective relays, communications equipment, and SCADA systems, to help define and provide solutions for their individual products. In addition, there has been some recent publicity over possible cyber attacks on the utility network, including one specific test (known as the "Aurora test") where a simulated hacker attack was able to take over the protection and control system of a generator, and physically destroy the generator. CIPC therefore decided to include some equipment suppliers in their discussion around cyber asset protection. A vendor panel discussion was held during the CIPC meeting in December 2007, and included GE Digital Energy among the participants.

The focus of this panel session was the vendor response to a list of questions suggested by utility members of CIPC. Many of the questions directly mentioned the publicized test of the simulated attach on a generator. However, these questions really addressed the basic of cyber asset protection. The questions can be loosely grouped into 3 categories:

- "What should we (the utilities) be concerned about?"
- "What are you (suppliers) doing to help us?"
- "What standards are you trying to meet?"

The rest of this article describes the GE Digital Energy responses to some of these questions.

2. What should utilities be concerned about?

There were several questions from the CIPC members that look for input on suppliers as to the actual cyber asset protection risks that utilities should be concerned about.

If you had to list 5 simple steps for utilities to take to greatly mitigate the Aurora-type vulnerabilities, what would they be?

Implement a security process. Successful security is always procedure driven. Successful procedures always require successful management. The NERC CIP standards directly address this, as they look for documentation on how security procedures are implemented across the utility, as well as the assessment and training of personnel. Without a process, and the management to follow the process, the other steps in security are meaningless.

Identify what needs to be protected. The CIP standards directly describe critical assets, such as generators and bulk transmission substations. A specific asset, such as a generating station, consists of many systems, including the primary generator protection, the excitation system, governor control, primary unit transformer protection, and auxiliary power system. The risks and vulnerabilities of each of these systems must be identified. Each of these subsystems must be addressed in a cyber asset protection plan.

Design for security. The simpler a process, the more reliable the process is. Part of making security procedures simpler is to engineer systems with security in mind from the start. Using a private communications network between sites, such as a SONET network or secure digital radio, prevents public access to your network, greatly reducing exposure and risk. Controlling access to this system, both through authorization and physical control of access points also simplifies security implementation, as does isolating key control networks from public communications networks.

Operate securely. Procedures and design are only as good as the actual operations behind them. Potential cyber attacks are events as significant as regular operational events. Operators must identify and respond to possible cyber attacks. In addition, the monitoring of access to the system, even down to the device level, is necessary. For example, the EnerVista Viewpoint Maintenance software can retrieve a complete security history for GE Multilin relays.

Take simple steps now. Creating security procedures, identifying what needs to be protected, designing for security, and training personnel all take some thought and time to implement. There are simple steps that can be taken immediately. The most basic step is to enable and set passwords in devices that support passwords.

3. What are the top 5 things that a utility should be worried about, and how does Aurora stack up in that top 5?

The Aurora test was an experiment intended to visually make the point that there are threats to the power system. The actions to take, however, are to secure your power system (and generating stations) against the risks based on how your system actually operates. In general, the biggest risks can be seen as:

Malicious physical attack. The electric infrastructure is hard to physically secure and easy to damage. An attack can easily be coordinated across a wide geographic area, targeting difficult to replace transmission assets. Many of these assets, such as large power transformers, and a long mean time to repair, long lead time for replacement, and are custom-designed for each application. The risk is a long-term degradation of the power system.

Unintentional operational mistakes. Employees with authorized access can unintentionally cause events. For example, loading a relay settings file into the incorrect relay can possibly cause protection trips. Good procedures and good system design will help reduce the possibility of operational mistakes, but not all scenarios can be identified or protected against.

Intentional harmful actions by employees. The utility industry has always had examples of disgruntled employees intentionally damaging equipment and the system. This is difficult to protect against, as employees have intimate knowledge of system design and operations, as well as authorized access. The only defense against this is appropriate, attentive management of employees.

Coordinated cyber attacks. The Aurora attack is simply an example of a cyber attack on the power system. Coordinated cyber attacks are difficult to coordinate, and it is possible to detect and defeat these kinds of attacks. There will be evidence of impending attacks, as there must be attempts to locate key assets to attack. However, generating stations are typically more secure against such attacks, due to already implemented security procedures mechanical protection devices, and the presence of human operators at the plant.

4. What is GE Digital Energy doing to help utilities?

The next group of questions directly address how equipment suppliers are helping utilities to address the NERC CIP standards. These questions can be loosely broken down into a couple of basic questions:

- What are you doing to improve or implement security in existing, installed devices, including legacy devices?
- What tools are you developing to help utilities with security management?

Some examples of questions posed by CIPC members to the vendor panel members regarding the Aurora attack are:

There is an Aurora mitigation plan. What are your plans and timeframes for each of the measures that involve you? We want to know what you will do to help mitigate these issues in the installed base of your equipment.

What are you going to do in future firmware upgrades to improve security in the installed base... rather than provide add on products or 'bump in the wire' products or other 'bolt on' solutions.

What are you doing to help companies meet CIP standards and still keep their systems under warranty for both legacy and new systems for patching. Is software "patching" an option for a firmware based device.

[We] have determined the best approach for our substation control IEDs is to use [non-routable] serial communication. Will all of the functions provided via IP communication be available using serial communications? Will serial interfaces continue to be provided for the foreseeable future?

These four questions all relate to support for installed products (modern and legacy) as well as for future installations. The Aurora mitigation plan has many specific requirements, which are simply good security practices. GE Digital Energy already meets much of the requirements of this plan, or is in the process of implementing solutions. These include local and remote passwords in devices, separate passwords for control and setting access, the ability to block access for configuration changes, logging of access to devices, and security audit tools to retrieve access logs. GE Multilin blocks access to all settings in protective relays, not just subsets of settings. Blocking access to all settings reduces the likelihood of unauthorized breaker control, as well as the possibility of malicious setpoint changes.

Fully implementing security measures, especially on installed products, will require firmware updates. GE Digital Energy treats firmware as a product. Each release is a complete, rigorously tested product, using only 1 file to load into an IED. This ensures complete, correct operation of the IED. Patching carries too many risks for incompatibilities and unintentional backdoor access or software hooks to exploit. GE Digital Energy solutions tend to be highly integrated, and we do not promote stand-alone or add-on devices such as communications processors or encryption units.

The challenge is actually updating equipment in the field. This is a time consuming process, and does involve operational risks during the process. Loading new firmware into a line protection relay, for example, typically requires an outage, and a few days of basic protection testing after the new firmware is in place. GE Digital Energy is committed work with customers to help identify which products need to be upgraded, and how best to manage this process. It is important to remember that it may not be possible to upgrade many legacy products due to the performance limitations of processors and hardware.

The question about serial interfaces raises some interesting points. GE Digital Energy will continue to support serial interfaces in our devices as long as there is a market need. Our serial interfaces provide the same access to settings, control, and data that the Ethernet interfaces do. However, the market is moving toward Ethernet due to the advantages of bandwidth, speed, and network availability and redundancy.

Also, serial interfaces are not inherently secure, and in fact, don't address security in any way. Security comes by restricting access to the serial network through other devices. Therefore, security of serial communications and Ethernet communications share the same principles. The best method is to engineer the communications networks with security in mind. Best practices can include:

- Keeping the engineering data access path separate from the SCADA/DCS path.
- Requiring two-step authentication to allow access to change settings, such as explicit permission from system operators.
- Using encrypted communications.
- Controlling physical access to the network, including the use of private networks such as SONET networks between sites.

Independent of the type of communications infrastructure, and the capabilities of installed products, the best solution would be to secure the trunk communications network first. In conjunction, secure installed devices as much as is possible based on their criticality, especially by enabling and using access controls. This greatly reduces the risk of the majority of cyber attack scenarios. This process also is relatively simple, inexpensive, and quick to implement. Going forward, for new projects, security features must be one of the criterion for selecting specific products.

5. Are any of the venders developing software that will assist in dealing with CIP requirements?

The CIP standards had been in development for quite a while before approval. Are your current devices fully compliant with the applicable technical requirements of CIP-005 and CIP-007, especially with respect to access control, monitoring/alerting and logging?

Both of these questions relate to tools to assist utilities in addressing parts of the CIP requirements for monitoring, intrusion detection, and security audit information, and the first one has several interpretations.

Security monitoring tools and intrusion detection tools for the overall communications network are commercially available from information technology suppliers. However, the use of commercial IT tools must be carefully considered as many of these tools assume a large communications bandwidth, and that the data being transmitted is not especially time critical. The communications network, however, is designed to control the power system reliably by issuing time critical controls, often over a network with very limited bandwidth. Security monitoring tools can not disrupt these flow of operational data, or the purpose of the control system, which is reliable operation of the power system, is compromised.

GE Digital Energy does have software tools that can generate and retrieve security audit trail information from a number of our products to facilitate reporting requirements. EnerVista Viewpoint Maintenance automatically retrieves the security log database from protective relays, and automatically generates reports on this database. This information includes changes made to settings, when the changes were made, and the MAC address of the computer that downloaded the settings changes to the relay. This functionality currently exists in a number of GE Multilin protective relays and the software to download and generate audit reports is already commercially available.

6. What standards are you trying to meet?

NERC is a regulatory body, that sets procedural requirements, but NERC is not a standards creating body that sets technical performance requirements. The challenge for electric utilities is to set the technical performance requirements for cyber asset protection in the absence of standards. These next few questions are driving towards how suppliers will be active in standards development.

What are you doing to help companies meet CIP standards and still keep their systems under warranty for both legacy and new systems for: system access and change management – must be controlled much more rigorously than in most companies today? What support is there for centralized authentication and authorization, multi-factor authentication, and access/activity logging? What support is there for configuration management, configuration auditing and change roll-back? How will the system allow autonomous operation in the event that a centralized service (e.g., authorization, logging) is unavailable?

At what point do you feel that 'Certified & Secure by Design' will be available? The real issue is one of complexity & the lack of a "Security Certification" for hardware or an "Underwriters Laboratory" type framework is one of the reasons we see such confusion in the application of security practice & pending compliance.

There are many methods of implementing access and authorization, including centralized authorization, to networks. For example, SONET networks using JungleMux have 3 different ways a user can access the network, all of which have been secured. There is access via the IP network, the optical network, and local serial interface access. All of these methods of access may be available, and all can require a two-step authentication process. So reliability of the cyber security system is very high. The goal of a system that permits access to relays and other IEDs is similar: requiring a two-step authentication process, while the system is highly available to permit the access.

For any type of system to work, there must be an open (non-proprietary), standards-based solution to support this type of access. It quickly becomes unmanageable for vendors, such as GE Digital Energy, and utilities, to have to work towards a variety of different solutions caused by unique interpretations of NERC CIP standards. GE Digital Energy will participate in any such standards development, but this process must be driven by the industry-at-large to be successful.

The concept of Certified and Secure by Design implies there are documented standards that can be designed and tested towards. Such standards must address how passwords are implemented, how authorization is performed, how security audit information is logged, and how these criterions must be met. The CIP standards, as they currently exist, are not precise enough to define what compliance really means. The industry must develop technical performance standards to define compliance, and to define the testing protocols that prove and document compliance. Once again, GE Digital Energy is continually working with NERC, and utilities, and is actively participating in the standards development process, we will ensure our products will comply with these requirements and standards.

7. Conclusions

The electric utility industry is being driven towards implementing cyber asset protection. There is much discussion about what should be done, and how to do it. GE Digital Energy believes that cyber asset protection is essential, and is working to ensure that our products form a sound base for any cyber security plan.

The key to cyber asset protection is more procedural than technical, and requires the identification of critical assets to protect, engineering the control system with security as a key component, operating the system securely, and taking immediate steps to use the existing security capability of products.

GE Digital Energy products already support a wide range of security functions, including:

- Establishment of secure, private communications networks using SONET or digital radio.
- Advanced access control and monitoring, intrusion detection and auditing in our GE Multilin protective relays.
  - Strong passwords, with separate passwords for Local and Remote access to settings and controls.
  - Dual-Permission Access Control to prevent unauthorized setting changes.
  - Access level annunciation and unauthorized access alarms.
  - Security audit logs to keep track of setting changes and commands performed in the relay.
- Secure SONET maintenance access via NERC CIP Security modules in the firmware and VistaNet software for the Lentronics JungleMUX products.
- Advanced network security suite, including SNMP and SYSLOG, in GE MDS wireless technology and products.

For more information, go to www.GEDigitalEnergy.com or contact your local representative.

0319-v6

NERC CIP Security Standards: What you need to know to comply

Arturo Herrera
GE Digital Energy, MDS

Our nations' electric systems are the foundation for the operation of every other critical infrastructure, business and organization. Our potable water supply, businesses, schools, hospitals and others all operate based on the reliability of the power grid.

In July 2006, NERC's Critical Infrastructure Protection (CIP) standards went into effect with CIP compliance audits slated to begin in 2007. According to NERC, the intent of the CIP Cyber Security Standards is "to ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric Systems."

The standards outline specific requirements to protect access to communications devices and networks that use routable protocols, such as TCP/IP. When non-routable serial protocols, which are typically used in SCADA, are transported over IP—a common practice—they must then adhere to the same requirements of routable protocols.

There is an additional note of interest for utility companies not required to follow these new standards. According to a recent report completed by the Utilities Telecom Council (UTC), "...even if a utility does not fall under the standards, many other utilities are obliged to comply, and those companies will have to be comfortable with the security of their dealings with other utilities..."

UTC and other industry experts expect the standards eventually to have wider acceptance than NERC's current authority.

There are eight different CIP standards covering everything from Security Management Controls and Critical Cyber Assets, to Incident Reporting and Recovery Plans. Each one of the eight standards defines a series of specific requirements.

CIP-002-1: Critical Cyber Asset Identification

CIP-003-1: Security Management Controls

CIP-004-1: Personnel and Training

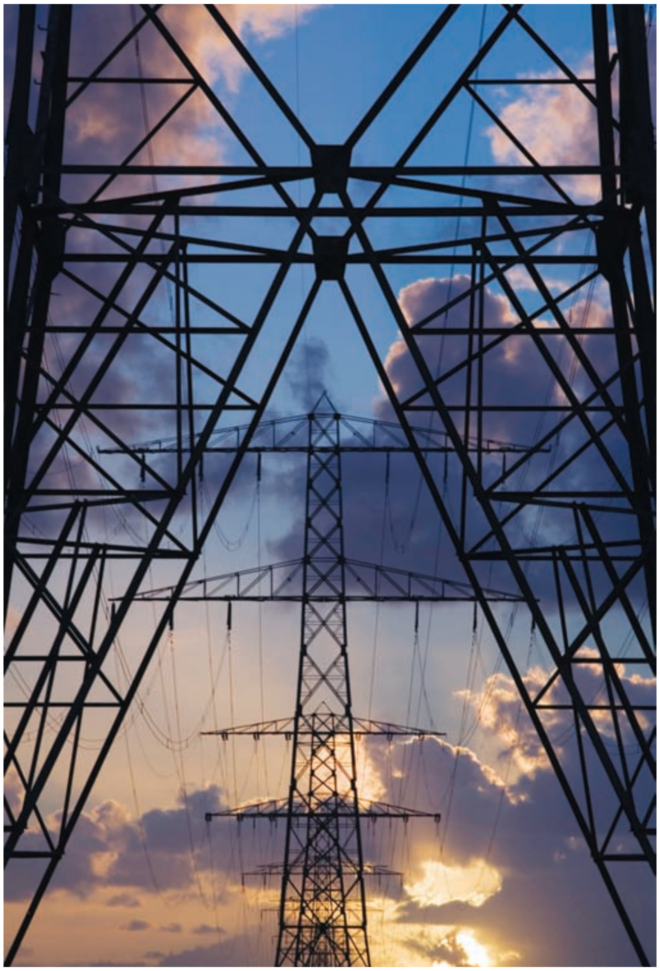
CIP-005-1: Electronic Security Perimeter

CIP-006-1: Physical Security of Critical Cyber Assets

CIP-007-1: Systems Security Management

CIP-008-1: Incident Reporting and Response Planning

CIP-009-1: Recovery Plans for Critical Cyber Assets



While the previously-referenced standards are to be considered as a group, this paper focuses on CIP-005 and CIP-007 and how these standards relate specifically to wireless communications.

SCADA/EMS systems were designed for reliability, not for security. Engineering, operations and IT departments must work in partnership to secure the power grid, and awareness and compliance are necessary to make this happen.

Creating a policy to use available cyber security technology by deploying, enabling, and configuring the tools and features provided as part of the equipment, as well as monitoring on a regular basis, are all necessary.

Best Practices for Wireless

In addition to using the security mechanisms already available in most communications systems, there are five specific practices that can be taken in order to comply with the NERC/CIP standards.

Authentication

802.1x is a framework for authentication and key management that was originally developed for wired LANs. It is a standard and industry accepted authentication tool, and it defines several protocols, including EAP, TLS, TTLS, MD5, and PEAP.

Authentication means that traffic does not flow until the authentication server validates the identity of the Access Point (AP) and the remote. This is done through the use of digital certificates that are created with the serial number of the radio used as the "Common Name" parameter.

The standard authentication mechanism is typically used on a PC or laptop computer. However, in industrial applications the device is not often a PC and a user is not present, but rather an unmanned stand-alone PLC or RTU. Until now, most PLCs were not equipped to implement the authentication mechanisms described above.

Encryption with Key Rotation

AES-128 Encryption

- FIPS PUB 192
- Eliminate data captures for man-in-the-middle or replay attacks of serial protocols

Automatic Key Rotation

- Eliminate key management risk

Separate Traffic by Function

TCP/IP technology supports the isolation of different types of traffic from another, even when they may be traveling on the same physical media. VLAN tagging (802.1q) allows traffic that uses the same infrastructure, wire or radio, to be virtually independent. VLAN tagging was created to limit broadcast storms, but is increasingly being used as a security barrier for unauthorized traffic.

VLAN tagging means that payload or serial data is transported over one specific VLAN and management traffic is transported over a separate VLAN. Personnel working on management tasks are thus prevented from accessing payload data.

Filter Traffic at Entry Port

Quality of Service (QoS) contains traffic to manageable levels. Using MAC address filtering limits traffic to known Ethernet addresses, and firewalls limit traffic to known IP addresses and ports.

Event Logging

Events, especially those critical in nature, must be logged in a non-volatile memory and time-stamped. This allows later analysis in the event of an issue or problem.

Event Reporting

The right network management tool enables the use of alarm monitoring. SNMP management reports suspect activity and minimize the risk of management break-in by reviewing event log files.

Existing IT technology can help protect the electronic security perimeter. Authentication, VLAN tagging, AES encryption, SSH or HTTPS secure access, Firewall and other filters all work together to secure the integrity of your communications and the reliability of your network.

Switch Your Frame of Mind

Reduce substation communication costs by up to 70%

A breakthrough in networking hardware that can reduce up to 70% of your total communications costs, the Multilin UR Switch Module is a fully managed, embedded Ethernet switch for the Universal Relay (UR) family. This advanced, 6-port Ethernet Switch eliminates the need for external, rack-mounted switches and significantly reduces the total costs associated with hardware, installation, wiring and troubleshooting, required for today's traditional substation communication architectures.

For a mere $200 more*, when compared to the cost of selecting the redundant Ethernet option on a UR, the Multilin UR Switch Module delivers full station management, monitoring, and control functionality, with complete communications redundancy.

* USD List Price

UR Ethernet Switch Module

Digital Energy
Multilin

GE Multilin
www.GEMultilin.com/URSwitch
gemultilin@ge.com

Worldwide	North America	Europe/MiddleEast/Africa
Tel: 905-294-6222	Tel: 1-800-547-8629	Tel: +34 94 485 88 00

Inside the Cyber-Security Perimeter

Steven Hodder
GE Digital Energy, Multilin

Dave McGinn
GE Digital Energy, Multilin

Dale Finney
GE Digital Energy, Multilin

1. Introduction

A common strategy for the provision of cyber security for electrical power transmission substations is to establish a single cyber security perimeter that includes all vulnerable devices in the station. This cyber security perimeter equipment is located inside the station's physical security perimeter to protect it from physical attack. A concern regarding this strategy is that it provides little or no cyber security against someone inside the physical perimeter. Proposals have been made to instead make each relay independently cyber secure, to limit access from inside the station to the internal unsecured LAN, and so on. However, anyone with malicious intent who has breached the physical security perimeter has numerous alternatives to cyber attack. Plugging this internal cyber hole would therefore result in little overall security improvement, and would present significant difficulties in comparison to a station wide-defence.

However, a cyber security concern that should draw more attention is security against employee errors. Such security would be invaluable in guarding against employees going about their assigned duties with no malicious intent, that through taking short-cuts or thorough unintentional error, negatively affect electric grid reliability. Many of the forms of cyber security discussed in the literature are ineffective against such undesired outcomes, as the employees are legitimately operating inside the cyber security perimeter. LAN-based protection and control systems can exacerbate this kind of problem, by making it easier to be working on a relay other than the intended one, or to incompletely block or restore a protection system.

This paper discusses the provision of cyber security at the relay level, and explores means to integrate security effective against employee error. Regulatory requirements are considered. Various sources of security threat are evaluated, and the value of the different security approaches against these sources is considered.

2. Security Overview

In order to discuss security in the context of protective relaying, it is first necessary to be able to break down, quantify and categorize security issues according to their risk and impact. Also, the impact of new technologies deployed in protection and control system within substations needs to be examined, with the intention of looking for vulnerabilities where a lack of suitable cyber security may have an undesired effect due to intentional or accidental user actions.

2.1 Security Risks

The nature of power systems and how they are constructed tends to make them a target for physical attacks:

- Assets (stations, towers) tend to be located away from densely populated areas, so there is very low risk of being seen by passers by.
- Utilities have undergone significant consolidation in past years, both in an attempt to reduce operating costs and also due to workforce attrition with the end result being most facilities are unmanned. Also, it is not common practice to provide 24 hour manned security at most stations.

Most large power apparatus (circuit breakers, transformers) are long lead time items, and transmission towers take a fairly long time to reconstruct. The physical destruction of these assets would not only result in potentially widespread outages, the repair/replacement time would make the duration of these outages unacceptably long.

This is not to say that there is not the potential for electronic-based attacks on key electricity assets, but the potential risks are greater and impacts are lower for an intentional, malicious electronic attack versus a corresponding physical attack. However, an internal security breach, caused by an inadvertent action of an internal user is far more likely.

2.2 Categorization of Threats

In evaluating the effectiveness of a security system, one should review the challenges that it might face. These may originate from two different source categories, either outside of or inside of the cyber-security perimeter that the utility community appears to be moving towards.

Sources from outside of the perimeter fall into many sub-categories.

Foreign Terrorists – With today's worldwide communications, it is quite conceivable for a foreign terrorist, bent on causing ruin to a western economy, to attempt to gain access to the computer assets of electric utilities. Once in, it is not difficult to cause major disruptions to electricity supply. Not only could geographically widespread blackouts be produced, taking many hours to recover from, but also damage to major equipment such as generators could result, taking weeks or months to recover from. It should not be assumed that foreign terrorists are unable to accomplish much with sophisticated modern protection and control equipment. They have a proven ability to acquire or develop the skills necessary for a complex operation. Such attacks would likely not produce the immediately visible impact that a physical attack would produce.

Domestic Terrorists – Domestic terrorists have opportunities and challenges similar to those of foreign terrorists, but being "in country", have the additional opportunity of attacking the physical perimeter. The strength of physical intrusion barriers is typically low, and in un-staffed rural transmission locations the response time to intrusion alarms is long. It would therefore seem less likely that domestic terrorists would attack the electronic cyber security barriers, or that having breached the physical security perimeter, that they would then mount a cyber attack rather than a direct physical assault.

Industrial Espionage – With open electricity markets, there is tremendous economic potential in having information not publicly available regarding the status of generators across the area, information that can be obtained from protection and control systems once the electronic security perimeter is breached. With this inside information, unscrupulous market participants can adjust their bids so as to control the market. Unlike previous categories, industrial spies would prefer that their intrusions go undetected in the long term, and so they would be unlikely to intentionally cause system disturbances or equipment damage with their cyber activities.

Hackers – There are people who will challenge security systems just because they are there. These people are more typically individuals, each acting independently, and thus not the same threat as a group with vast resources focused on a particular target. However, hacker communities exist that share techniques and other information that may be used by other more focused, malicious groups.

The above-mentioned threat categories originate from outside the electronic security perimeter, and for the most part can be countered with current cyber-security measures and technologies available in the computer networking industry. However, there is another category of threat that may not be receiving the attention it deserves relative to the threats previously discussed. In particular, threats posed by people who have been intentionally given legitimate electronic access to the system, and are inside the electronic security perimeter.

Disgruntled Employees – a conceivable source of attack is a utility worker whose normal job duties require access to the protected cyber assets, and who for some reason has decided to cause malicious harm or embarrassment to the employer, its customers, or to colleagues.

Employees can be a difficult challenge to security. They generally are well aware of the vulnerabilities of the power system, and have been given some degree of access in order that they can perform their intended functions. The limits to their access requirements are difficult to forecast – in an emergency the unforeseen often arises. As a result, access rights are often set wide with much attention paid to preparing for the unexpected.

This category could also include dismissed employees and employees involved in a labour dispute. An appropriate password management system could implement a policy that quickly removes the access privileges of this class of employees, and thereby promptly places them outside the electronic security perimeter. However, it should be kept in mind that such password management is effective only where it can be reliably implemented and there is foreknowledge of risk; there are many situations where is not possible to foresee the problem or not politically acceptable to take pre-emptive action.

Regular Employees – A threat category that deserves a much higher proportion of the attention the industry is giving to system compromise is that presented by regular employees going about their assigned duties, with no intention of causing any harm.

Such employees frequently make mistakes or take shortcuts that directly affect the security of the electric power system, most commonly by inadvertently tripping major generation or transmission assets. Comparatively little attention has been paid recently by the electric utility community as a whole to securing against the regular employee threat.

Typical mistakes and shortcuts a regular employ might make include:

- Isolating one subsystem for modification or test, and then inadvertently working on a neighboring system that has not been isolated.
- Isolating a subsystem and then inadvertently doing a test outside of the isolation boundary.
- Incompletely isolating a system so that a test results in some unplanned action.
- Isolating a subsystem to safely perform some job, then failing to completely remove the isolation when the job is finished.
- Making changes and then failing to properly verify that the change has been correctly executed.
- Making changes to facilitate some test activity, and then either forgetting to undo these changes when the work is complete, or undoing them incorrectly.
- Making changes that through error or inadvertence compromise the isolation of the system being worked on.
- Removing isolation before a subsystem that had been worked on completely resets.
- Installing a "backdoor" bypassing security to facilitate maintenance access.

While history has shown that the impact to power system security from regular employees is much less than intentional attacks potentially could be, history has also shown that regular employees cause incidents with an overwhelmingly higher frequency. Security risk can be defined as the cost of a security-related incident multiplied by the probability of that incident occurring. Using this definition to qualitatively compare the risk from regular employees to other threat classes, it can be seen that the comparison is between a very high cost multiplied a very low probability for a intentional incident against a low cost multiplied a high probability for an unintentional incident. As none of the values of these factors is known with any degree of certainty, the risks of each could very well be similar, so the effort expended on each should be similar.

Microprocessor technology presents a fantastic opportunity to greatly reduce the frequency in which this kind of security breach occurs. Unfortunately, the present momentum of security enhancements seems to be solely focused on defeating potential intruders and preventing regular employees from working outside of their discipline.

2.3 Effect of New Technologies

An additional incentive for expending more effort on securing against the threat posed by mishaps is the changing technology employed by protection and control systems. Over the long period of time previous technologies have been deployed, the design of the facilities and the work methods used have been tuned to provide relatively safe and secure means to perform the various activities needed. However, it appears that the future belongs to so-called station bus and process bus technologies. These communications network-based technologies present their own unique opportunities for commissioning and maintenance activities to affect the security of the power system.

Previous technologies provided many physical barriers to making the mistakes outlined earlier in this paper. For the most part, hardware is dedicated to particular and easily conceptualized functions. The hardware for different functions is located in physically separate locations. For instance, the protection relays for a line usually are on a panel or rack of their own. The protection relays for other power system elements, the RTU, the local control, the DFR, etc. are located elsewhere. The physical separation provides a barrier against worker activity affecting other equipment or functions. Re-testing following a change is limited to the equipment on that panel. Utilities often adopt a practice where temporary visual or physical barriers such as caution tape or plastic film are required to be installed masking off neighboring equipment prior to work. This forces focus on correctly identifying the equipment to be worked on while installing these barriers, and facilitates returning to the correct equipment after attention is temporarily diverted. Typically utilities provide all the test switches necessary to completely block the protection on the same panel as the relays, so that the worker can easily see that if all are open then the protection may be tested safely, and if all are closed the protection is restored. While these and other devices can lessen the security impact to tolerable levels, they are far from perfect.

Figure 1.
Security within new technology

With future technologies, many of the physical mechanisms used successfully with previous technologies become irrelevant. Physical separation is not provided to the same degree: an IED may protect multiple elements, and may in addition implement the RTU function, local control, DFR and more. If one is revising an RTU setting in an IED, there is a valid concern that the protection could be inadvertently affected. Is it then necessary to re-test the protection? A Merging Unit may supply data to three or more IEDs. If a change is made to a merging unit, is it necessary to take all three IEDs out of service and re-test them? Using caution tape to mask off neighboring equipment will have no value if access to the relay is via a LAN that could equally provide connectivity to another relay in the station. The worker may not even be at the station; changes may be initiated from a remote engineering office, in which case there is the concern whether a change or test is even to a relay at the correct station. FT type blocking switches are of course unusable on GOOSE trip signals. Equivalent blocking could be provided with the IED configurable logic, but can these be trusted when a new and therefore untested configuration is downloaded to the IED?

These future technologies can however provide other means to achieve or even surpass the security provided with previous technologies, provided these means are fully thought out and carefully implemented. For instance the IEDs and/or their setup programs could be designed such that setting modification or test initiation is permitted only after two different people have authorized the activity, a technique that in other industries is referred to as double custody. The immutable base firmware can be designed to implement independently of user settings virtual devices that completely and securely block the relay, and provide positive indication of the relay's blocked/unblocked state. Many activities may be disallowed by the IED when it is not blocked. Features may be provided that prevent the blocking being removed should doing so directly result in control action such as tripping. Even better, features may be implemented that remove the requirement for workers to access the system at all for many activities.

3. Standards Overview

World events over the past years have placed increasing focus on critical public infrastructures, like public works (water/waste water) and bulk electricity systems, and the importance of their security and availability. The events of September 11th, 2001 opened a whole new dimension of concerns for public infrastructure – no longer was interruption of these key systems solely the result of unexpected equipment failures or natural occurrences, but also intentional and malicious acts of human beings. Widespread power system outages, like the August 2003 Northeast blackout, heightened awareness of the necessity of a reliable bulk power system, and the ramifications that result when the power system is unexpectedly unavailable for long periods.

There are a number of standards, both officially published as well as in draft that deal with the issue of security of so-called electronic assets considered critical to the safe and reliable operation of bulk electricity systems. There are also a number of key industry working groups addressing issues related to cyber security for electric utilities

3.1 NERC Critical Infrastructure Protection (CIP)

NERC Critical Infrastructure Protection standards outline the security requirements for Critical Cyber Assets. Critical Cyber Assets are essentially any programmable electronic devices or communication networks that if damaged or otherwise made unavailable may impact the safe and reliable operation of the associated bulk electricity system[1]. Access to these Critical Cyber Assets is broken down into both the physical security of the installation housing these assets, as well as the electronic access (i.e. communications) to these assets.

NERC CIP is broken down into the following sections:

CIP Standard		Scope	Technical/Procedural /Documentation
CIP-002	Critical Cyber Assets	Identification & enumeration of critical cyber assets	D
CIP-003	Security Management Controls	Development of cyber security policy, including auditing	D
CIP-004	Personnel & Training	People authorized to access critical assets must be trained on security policy, having deeper background checks	P
CIP-005	Electronic Security	Electronic Security Perimeter and Electronic Access Controls	T,P
CIP-006	Physical Security	Physical security and access controls around Critical Assets	T,P
CIP-007	Systems Security Management	Security controls to detect/ deter/prevent compromise of Critical Cyber Assets	T,P
CIP-008	Incident Reporting	Identification, classification and reporting of Cyber Security incidents	P
CIP-009	Recovery Plans	Restoration of Critical Cyber Assets following compromise of the asset(s)	P

Table 1.
NERC Critical Infrastructure Protection Standards CIP-002 through CIP-009

In the above table, the focus of each section can be classified as Documentation, Technical or Procedural. Documentation refers to exercises in identifying or enumerating key pieces of information related to critical cyber assets. Sections with a Technical focus deal with actual functionality of devices and technologies within secure cyber assets. Procedural sections speak to organizational and process requirements for utilities and how personnel deal with and access secure cyber assets.

3.2 IEEE Power Engineering Society (PES)

Following the release of the NERC CIP standards, and the certification of NERC as electricity reliability organization for North America by the Federal Energy Regulatory Commission there has been a significant amount of activity from several Subcommittees within the IEEE PES.

Power System Relaying Committee (PSRC)

The Power System Relaying Committee Working Group C1 is developing a report covering issues related to cyber security for electronic communications access for protective relays. The document is intended to educate those individuals implementing or using electronic communications to access protective relays.

Power System Substations Committee (PSCC)

The Power System Substations Committee Working Group C1 is currently finalizing Standard P1686: Standard for Substation IED Cyber Security Standards. This standard defines the functions and features needed to accommodate critical infrastructure protection programs. In particular, it outlines the security requirements for access, configuration, upgrading and data retrieval for substation IEDs (including RTUs) and presents a compliance table for users to include in RFI/RFP documents.

Power System Communications Committee (PSCC)

The purpose of the PSCC Security Assessment Working Group has been established to develop methods for utilities to assess information security risks. These efforts will be closely coordinated with the on-going work on security standards for power system communications in other standards activities.

3.3 IEC Technical Committee (TC) 57

IEC TC57 WG15 has been commissioned to recommend or supply standardized security enhancements as needed to other TC57 WGs, to secure the information exchange for tele-control applications through enhancements to the IEC TC57 protocols including IEC 60870-5 and its derivatives (e.g. DNP), IEC 60870-6 TASE.2 (a.k.a. ICCP), and IEC 61850.

4. Authentication

Authentication is the process by which the identities of the parties involved in a transaction are verified by some trusted source or mechanism, and to establish which privileges those parties have within the transaction. In the context of protective relaying, the real goal of authentication is two-fold:

1. Verify the identity of the user who will be accessing the protective relay in question, and to define what features and functions they will be allowed to access or execute.
2. Verify the identity of the end relay that the user wishes to access and work with.

Authentication is a typical function of life in modern society. Examples of user authentication in day-to-day life include logging in to a computer network at the office, accessing voicemail messages and banking via an ATM. All of these examples feature the same two-step identification: the user must provide both a “name” (login ID, voicemail box, ATM card) and a secret piece of information or “key” (password, PIN) that is associated with the name given that proves the individual requesting access must be the true individual.

Typically, the process of authentication involves establishing a session, where the two parties exchange identification credentials and create a trusted communications channel between them. A key feature of most sessions is the inclusion of an expiry time that requires the parties to re-establish their credentials in order to resume communications. This prevents potentially malicious parties from using an old set of credentials to initiate communication sessions by posing as a trusted party.

Authentication mechanisms can be very simple, as the user ID/password schemes above, or they may be very complex, multi-realm distributed authentication schemes such as Kerberos.

A simple analogy to describe Kerberos is riding on most public transit systems. The first step in the authentication process is to provide a set of valid credentials, in this case a transit pass and photo ID. This validates that the rider is (1) who they claim to be and (2) that they have a valid fare to ride the system. Once inside the system, a transfer can be obtained that allows the rider to go between different routes (say from a subway to a bus) without having to provide all of the initial credentials each time. The transfer normally includes a time stamp that invalidates the transfer after a preset time and forces the rider to “re-authenticate” to re-enter the transit system and prevents other users from riding the transit system using a discarded transfer.

4.1 Authentication for Power System Protective Relaying

The Requirements for an Authentication Mechanism

Authentication, as defined previously, is any mechanism for ensuring that the parties involved in a communication transaction are identified correctly. In the case of protective relaying, this would predominantly be engineering or maintenance staff accessing IEDs to load or update settings, commission or re-verify protection or download diagnostic information. It is therefore necessary, for the reasons discussed in previously, to absolutely verify both the identity of the person who wishes to access the IED and the correct IED has been accessed. Again, for the purposes of this discussion it is assumed that the individual requiring authentication is already within the electronic security perimeter of a given station.

Authentication is typically done by comparing information sent by one party against information generated internally by the other party, using some secret information based on an agreed upon algorithm. The secret information would not be easily discernable by an outside party by altering the information sent via the communications link based on an agreed upon algorithm.

Any authentication mechanism within protective relays must meet the following requirements and constraints:

- Any authentication algorithm running within the IED must not impact the fundamental performance of protection elements, logic execution and high-speed, time critical, communications (e.g. IEC61850 GOOSE).
- The addition of any authentication algorithms must be tested to ensure that the above requirement is not violated. This test must be done on an IED with the maximum feature set configured and running, with the injection of meaningful signals including AC quantities, contact inputs and communications messages a must. Tests should be run both in the steady state as well as for typical fault cases with performance verified for each case.

- The authentication mechanism must prevent an unauthorized user from using historical data to decode the secret information used in the authentication mechanism, or from using past authentication credentials to masquerade as a valid user to gain access to the IED.

- The authentication mechanism should not only use key secret information about the user to be authenticated, but ideally information for both the user and the given IED to generate a set of credentials for the transaction.

- The IED configuration and access software should require these credentials to be valid for the given IED before allowing the user to connect to the device. Credentials that are not valid for the desired IED should prevent the user from connecting to the device.

- The IED should keep track of the credential information used for each access session. The information should allow forensic examination of the individuals that accessed the IED based on the credentials.

It is possible to use the basic principles of cryptography to take key pieces of information and use simple cryptographic algorithms to generate these secure credentials for authentication. While the algorithms and keys themselves may not be as strong as those typically found in the world of computer security, additional strength can be obtained by the relative obscurity of the IED secret information used in the creation of credentials.

4.2 IED Passwords for Security and Authentication

Passwords for Security

Many standards mandate the use of "strong" passwords within IEDs as an absolute requirement for security. These strong passwords are usually defined as having at least 8 characters, with a mix of upper case letters, lower case letters, numbers and special characters. While this mandate makes sense at first glance, there are a number of issues that need to be considered before simply assuming that strong passwords will be the panacea for security issues.

- Strong passwords, by their very nature, must not be easily associated with any human discernable information to prevent compromise via dictionary attacks or so-called social engineering attacks. This also means that the password is not easily remembered by the human beings that are required to use it, the end result of which is that the password will likely be written down somewhere thus violating a fundamental rule of password security.

- Passwords, strong or otherwise, should be unique for each IED within a given station. In a small distribution station there may be only a few IEDs but in a large transmission station there may be hundreds of individual IEDs and therefore potentially hundreds of individual passwords. Even if the passwords were not strong, it is unlikely that any human being would remember every password and therefore the result is again passwords being written down.

Password management also presents a number of issues.

- In order for passwords to be truly a mechanism for security, they should be changed periodically or in the event of staff turnover. This proves to be a significant challenge to execute in a real-world utility. As an example for calculation, say a given utility has a total of 100 critical stations, and an average of 100 IEDs in each of these critical stations. Assume that the average time to drive between any two stations is 2 hours and that each password change takes 10 minutes, including the time to actually change the password plus fill out the required documentation. Also, assume that one full-time employee (FTE) is defined as 1920 hours/year (40 hours/week, 48 weeks/year). The total time required for password management is 1865 hours/year, or 0.97 FTE. In other words, one employee would do nothing for the entire year, year after year, but drive between stations and change passwords. This is assuming there is only one password to change, but the reality is there are often multiple passwords within IEDs, and therefore the amount of labour involved in password management increases accordingly.

- The solution to the above issue would seem to be somewhat alleviated through the use of remote password management, however there are a number of issues with this strategy. The loss of communications between a remote site and the password management system renders the system ineffective. Additionally, any system used for remote password management must be at least as secure as the system where the passwords are to be managed. A compromise of the remote password management system could result in the compromise of all of the IEDs managed by the system, potentially making it impossible for any legitimate users from accessing the IEDs.

4.3 Passwords for Intrusion Detection

Often, the strength of passwords within protection IEDs is a source of debate and specification games. One could argue the perceived strength of one password paradigm versus another and the absolute superiority of one over the other. In reality, regardless of the password paradigm chosen, having relatively strong passwords does have certain advantages, particularly in terms of improving the probability of Intrusion Detection (ID) systems detecting unauthorized access attempts from internal and external hackers attempting brute force attacks (e.g. dictionary attacks).

As the number of password permutations is increased, eventually the point is reached where the increase in security does not justify the increased difficulty of use. Calculation of the probability that a time-limited attack is defeated is illuminating. Consider the following three password paradigms:

	Type 1	Type 2	Type 3
Password Length:	6	8	10
Characters:	10 (Digits Only)	70 (Alphanumeric)	10 (Digits Only)
Number of Permutations:	1×10^{6}	5.8×10^{14}	1×10^{10}
Time/Attempt:	60 seconds		
Attack Duration:	1 month		
Probability Attack Defeated:	95%	99.999999994%	99.9996%

Table 2.
Examples of password paradigms

In the table above, the assumption is that the attacker tries passwords in some sequence that avoids repetition. The Time/Attempt is chosen to ensure that any invalid password monitoring functions within the target IED will not be asserted. Some IEDs implement a function to detect a certain number of invalid password attempts within a given time window. This function will typically generate an alarm event that can be passed to a SCADA or Network Management System and may even close the affected communications port for a given time, thus increasing the amount of time needed to break the IED password.

Again referring to the table above, the attacker is limited to the maximum time duration shown to prosecute the attack. A hacker must open a communications port continuously during the attack. The risk is that this open communication port to the outside world may be detected as suspicious by an ID system. The best result for the hacker is that the port is closed and access is no longer available; the worst result is the communications are traced back to the origin and the hacker is caught.

In the above example, it would appear obvious from first glance at the number of permutations that Type 2 is the best password mechanism, with Type 3 being a distant second and Type 1 apparently completely useless. Often individuals will state this to be the case, however before judging the suitability of these password models, one must consider the whole system and process for accessing IEDs, including in the context of ID systems. Looking at the probability that an attack is defeated, it can be seem that the advantage of Type 2 over Type 3 is a negligible 0.0006%, and that even the simple Type 1 scheme gives pretty good security.

4.4 Passwords for IED Authentication

A different perspective on passwords would be to look at them as an authentication mechanism not to identify the human user, but rather authenticate the identity of the end IED that is to be accessed. The rationale behind this is simple: a user may be able to access any IED within a station via a local substation network such that the user may not even be in front of, or potentially in the same building as the protection to be worked on. Without clear authentication of the end IED to be accessed, it is quite possible that the user may inadvertently connect with an IED other than the intended one. The result may be maintenance actions performed on the wrong protection leading to unexpected power system outages, or settings being loaded on to the incorrect relay potentially causing either a failure to trip or overtripping.

By assigning unique passwords to each device, a level of protection against this type of security breach can be obtained. In order to have unexpected or undesired outcomes from relay setting and maintenance, the user must not only connect to the incorrect device but also provide the password for the same incorrect device. Inadvertently connecting to the wrong device and providing the password for the correct device will generate an error that forces the user to closely examine the connection they are attempting.

5. Encryption

Encryption, by contrast, is a set of mathematical algorithms that are used to encode information to be transmitted over communications media so that the information is unusable except for those parties involved in the transaction. There are two methods of providing encryption: symmetric (private key) and asymmetric (public key). This is done to ensure confidentiality and integrity of the data transmitted.

Symmetric encryption uses a common secret key that both encrypts and decrypts the information to be transmitted securely over an insecure communications link. The secret key can only be used to decrypt the information if an associated secret (i.e. a password) is provided by each key owner.

The risk in symmetric encryption is that the key used for decryption must be transmitted over a potentially insecure link, making it possible to hijack the key during transmission creating what is known as a "man-in-the-middle" attack.

Asymmetric encryption, on the other hand, uses two separate cryptographic keys – one that is freely distributed and one that is kept secret. The public key is always used to encrypt the data and the private key is always used for decryption. The strength of asymmetric encryption lies in the fact that the public key can be easily generated when the private key is known, but it is computationally impractical to derive the private key by only knowing the public key.

The major disadvantage of public key encryption is that the private key must be securely stored and backed up, preferably in several locations. This is necessary as the private key (the actual electronic file) can never be recreated – if it is lost then a new private key must be created and a new public key derived and distributed.

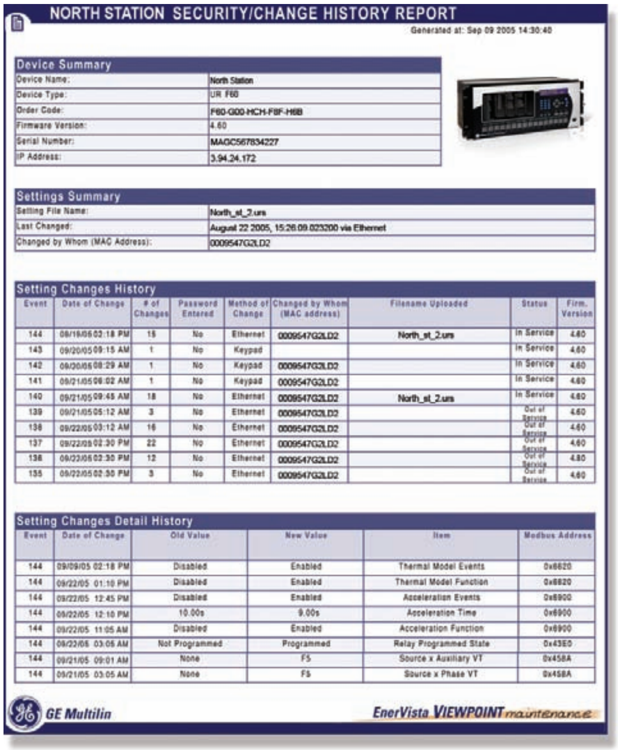
Real-time encryption and decryption of all communications between a user and an IED is not likely practical due to performance constraints, and within the electronic security perimeter its necessity is arguable.

6. Security Audit Trail

A sound security policy will minimize the possibility of unwanted access to the IED. Even so, it is necessary to plan for the unexpected. NERC CIP-003 mandates that electric utilities must have a process for managing changes in critical cyber assets, including hardware and software changes. In the case of power system protective relay IEDs, an electronic log within the IED that is dedicated to storage of security events is an essential tool for detecting configuration changes and an aid in the post-mortem analysis of a breach or recording the results of a penetration test. The following events should be time-stamped and logged:

- Attempted and failed access
- Password change
- Download of settings
- Download of firmware
- Deletion of a record (sequence of events, etc.)
- Security log retrieval
- Time and date change
- Factory service access
- IED out-of-service / IED-in-test
- IED powered down / IED powered up

Access to this log should be restricted with a separate password required for retrieval. It should not be possible to delete the log under any circumstances even through a firmware upgrade.



NORTH STATION SECURITY/CHANGE HISTORY REPORT

Generated at: Sep 09 2005 14:30:40

Device Summary	
Device Name:	North Station
Device Type:	UR F60
Order Code:	F60-G00-HCH-F8F-H6B
Firmware Version:	4.60
Serial Number:	MAGC567834227
IP Address:	3.94.24.172

Settings Summary	
Setting File Name:	North_st_2.urs
Last Changed:	August 22 2005, 15:26:09.023200 via Ethernet
Changed by Whom (MAC Address):	0009547G2LD2

Setting Changes History

Event	Date of Change	# of Changes	Password Entered	Method of Change	Changed by Whom (MAC address)	Filename Uploaded	Status	Firm. Version
144	09/19/05 02:18 PM	15	No	Ethernet	0009547G2LD2	North_st_2.urs	In Service	4.60
143	09/20/05 09:15 AM	1	No	Keypad			In Service	4.60
142	09/20/05 08:29 AM	1	No	Keypad	0009547G2LD2		In Service	4.60
141	09/21/05 06:02 AM	1	No	Keypad	0009547G2LD2		In Service	4.60
140	09/21/05 09:45 AM	18	No	Ethernet	0009547G2LD2	North_st_2.urs	In Service	4.60
139	09/21/05 05:12 AM	3	No	Ethernet	0009547G2LD2		Out of Service	4.60
138	09/22/05 03:12 AM	16	No	Ethernet	0009547G2LD2		Out of Service	4.60
137	09/22/05 02:30 PM	22	No	Ethernet	0009547G2LD2		Out of Service	4.60
136	09/22/05 02:30 PM	12	No	Ethernet	0009547G2LD2		Out of Service	4.80
135	09/22/05 02:30 PM	3	No	Ethernet	0009547G2LD2		Out of Service	4.60

Setting Changes Detail History

Event	Date of Change	Old Value	New Value	Item	Modbus Address
144	09/09/05 02:18 PM	Disabled	Enabled	Thermal Model Events	0x6620
144	09/22/05 01:10 PM	Disabled	Enabled	Thermal Model Function	0x6820
144	09/22/05 12:45 PM	Disabled	Enabled	Acceleration Events	0x6900
144	09/22/05 12:10 PM	10.00s	9.00s	Acceleration Time	0x6900
144	09/22/05 11:05 AM	Disabled	Enabled	Acceleration Function	0x6900
144	09/22/05 03:05 AM	Not Programmed	Programmed	Relay Programmed State	0x43E0
144	09/21/05 09:01 AM	None	F5	Source x Auxiliary VT	0x458A
144	09/21/05 03:05 AM	None	F5	Source x Phase VT	0x458A

Figure 2.
Security audit trail's found in software such as GE Multilin's Viewpoint Maintenance, can automatically track the details of settings changes to your relays.

7. Permission from a Controlling Authority

It is a common practice among utilities today that work is carried out in the substation only with the permission of a controlling authority, and usually work is scheduled and approved weeks in advance. Even so, events can arise in the power system at the last minute such as a forced outage of a transmission line that can make the approved work an unacceptable risk. The controlling authority is the sole entity with the required information on the overall status of the power system needed to make such assessments at the time the work commences.

Under a typical scenario, a maintenance person arrives at the substation. He notifies the system operator, usually by telephone, of his arrival and requests permission to carry out some activity on a particular system, nowadays taking the form of a multifunction IED. The activity can involve removing the IED from service. The activity can also require some actions by the system operator such as opening a particular breaker or taking a particular line out-of-service. During the maintenance period the system operator may inhibit alarms or status associated with the IED under maintenance. The IED itself may provide some indications to the operator of its operational state (out-of-service, critical failure, etc.) although this is often not the case with older systems. On completion of the task, the maintenance person will contact the operator to indicate that the system has been restored to service.

A serious exposure arises when the maintenance person, through negligence or inexperience, carries out his activity on the wrong system. The consequences of such a mistake can result in an element of the power system being left unprotected. Alternatively, it can result in an unexpected false trip of a system element that is currently in-service. Such events have been known to result in the loss of the entire substation (e.g. a station is fed from two lines – one line is removed from service for maintenance – the maintenance personnel mistakenly initiate a test trip on the line that remains in-service). Finally, the IED may be configured with the wrong settings, resulting in a subsequent failure-to-trip or false trip. The problem becomes more likely in the case that IEDs may be controlled or configured over a substation LAN allowing access to any IED in the substation. Requiring unique passwords for each IED in the substation could mitigate this problem.

A proposed improvement to this solution is to place the IED access control function under SCADA supervision. Such a scheme can be readily implemented in modern IEDs. A command from SCADA opens a time-window within the IED wherein passwords are accepted and access to the IED is granted. Outside this window, access to the IED is rejected, regardless if the correct access password is provided. The window would expire after a fixed period of time (say 8 hours). Under such a scenario, the maintenance person informs the operator of the device to be accessed. The operator sends a command to the IED via SCADA. All other IEDs in the substation reject any access attempts. Access to the wrong IED would require both the operator and the maintenance person to make the same mistake. A failure of SCADA would prevent password access to any of the IEDs in the substation, however, in this instance, arguably the primary concern should be the timely restoration of the SCADA system.

Importantly, this solution also provides an additional layer of security against malicious attacks. The SCADA system typically utilizes a secure, dedicated communications network which is unlikely to be compromised by an external hacker or accidentally through misadventure of internal personnel. It is also highly improbable that a hacker would initiate an attack on a particular IED at the same time that maintenance is occurring.

8. Processor Prioritization within IEDs

Microprocessor-based protective relays can be considered as highly specialized embedded systems, optimized for the execution of specific tasks, primarily to run power system protection algorithms and associated programmable scheme logic with high speed and determinism. This often forces other services, including non-critical communications to run at lower priorities than the main protection tasks. Many factors must be balanced, including processor clock speed (related to heat dissipation), processing margin and available data memory. The way this balancing of processor priority is done in older technology relays, can result in limitations to advanced communications functions such as secure session management and data encryption.

This is not to say that certain key concepts from the realm of security, including authentication and cryptography, can not be applied to the existing installed base of protection IEDs.

8.1 Restrictions on Traditional Authentication Mechanisms

Often, it is assumed that use of industry standard security mechanisms are either impractical, or impossible to implement in protective relaying IEDs. This in the sense of certain mechanisms, for example strong encryption of communications messages, may impose too great a demand on microprocessors resulting in degraded system performance. One could argue that new IED technology may render some of these arguments obsolete. However, the present state of most utilities is that there are hundreds, even thousands, of protection IEDs based on old technology. Therefore, these processing concerns may still apply. It is not practical, both in terms of economics and timely execution, to assume that existing protection IEDs would be swapped out immediately should a new technology be available tomorrow, next month or next year.

It is possible to provide reasonably good security and authentication in protective relaying IEDs without necessarily trying to apply existing technologies and mechanisms from the computer security world-at-large. Rather, the underlying principles and paradigms for these mechanisms should be examined and then a new set of technologies and mechanisms developed that can be applied to current and future protective relay technologies without requiring significant hardware upgrades or change-outs of existing IED installations.

9. Conclusions

All power systems are potentially vulnerable to compromise, both physical and electronic, resulting in undesired effects on power system stability and reliability. Potential activities may originate from either internal or external sources, and may occur due to malicious intent from unauthorized individuals or an inadvertent action on the part of legitimate users. Security from external electronic threats outside of the electronic security perimeter can be achieved using current computer security technologies but a separate mechanism is needed to prevent legitimate users from accidentally compromise protection systems. While the world's most advanced authentication and encryption technology is not likely to be applied to all IEDs, the basic principles of the protection IED can be adapted to significantly help prevent power system disruption caused by legitimate user misadventure.

10. References

[1] NERC Critical Infrastructure Protection Standards CIP-002 through CIP-009.

0325-v6

unmatched...

D90 Plus - Line Distance Protection System

True Sub-cycle Distance Protection
Dedicated Disturbance Recording
Advanced Automation Engine
Integrated Digital Annunciator
Local Color HMI
Comprehensive Communications
IEC61850 Compliant

The most advanced line distance protection system in the market, GE Multilin's **D90**Plus delivers maximum performance, flexibility and functionality. Designed as a true multifunction device, the **D90**Plus eliminates the need for external devices reducing system complexity, commissioning time and capital costs.

Featuring advanced automation and control, dedicated digital fault recording, comprehensive communications including IEC61850, and an extensive local HMI, the **D90**Plus represents the next benchmark in protective relaying.

Digital Energy
Multilin

GE Multilin
www.GEMultilin.com/D90Plus
gemultilin@ge.com

Worldwide
Tel: 905-294-6222

North America
Tel: 1-800-547-8629

Europe/MiddleEast/Africa
Tel: +34 94 485 88 00

Application Considerations in System Integrity Protection Schemes (SIPS)

Vahid Madani
Pacific Gas & Electric Co.

Damir Novosel
Quanta Technology

Miroslave Begovic
Georgia Institute of Technology

Mark Adamiak
GE Digital Energy, Multilin

1. Abstract

This paper describes some of the critical engineering, design, and applications of the latest technology for the implementation of System Integrity Protection Schemes (SIPS). Applicability of the advanced analytical techniques for various types of SIPS applications on the basis of modern technology is also addressed. An overview is presented of traditional scheme requirements leading to the SIPS of the future. A new survey is described in the paper, which should provide valuable information about power industry trends and experiences in SIPS.

Keywords: Power system protection, emergency control, industry practice, SIPS.

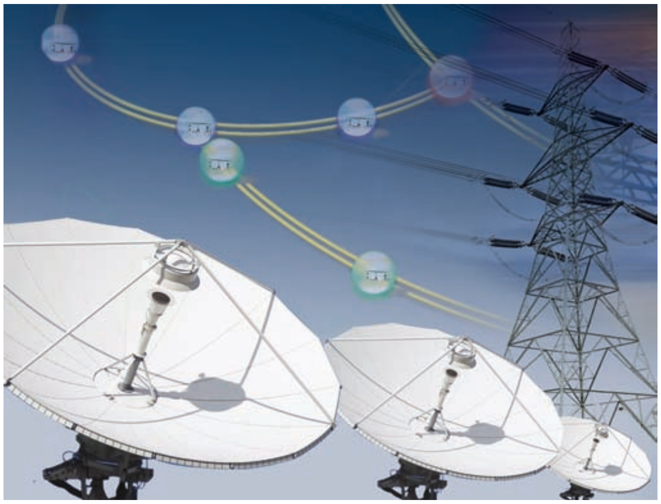
2. Introduction

The electric power grid is the "pivot point" that balances the generation and load. Maintaining the integrity of this pivot point is imperative for the effective operation of interconnected power systems. As such, the balance of power is only as reliable as the weakest pivot point in the system.

When a major disturbance occurs, protection and control actions are required to stop the power system degradation, restore the system to a normal state, and minimize the impact of the disturbance [1]. Control center operators must deal with a very complex situation and rely on heuristic solutions and policies [1], [2].

Local protection systems arrest the propagation of the fast-developing emergencies through automatic actions. Local protection systems, however, are not able to address the entire power system, which may be affected by the disturbance.

The trend in power system planning utilizes tight operating margins, with less redundancy in the grid. At the same time, addition of non-utility generators and independent power producers, an interchange increase in a growing competitive environment and introduction of fast control devices make the power system more complex to operate. This changing environment highlights the need for automated systems with advanced monitoring and intuitive interface tools to enable real-time operator interactions. On the other hand, the advanced measurement devices and communication technology in wide-area monitoring and controls, FACTS devices (better operational and stability control), and new analytical and heuristic procedures provide better ways to detect and control an impending system collapse [3], [4], [5], [6].



Advanced detection and control strategies through the concept of System Integrity Protection Schemes (SIPS) offer a cohesive management of the disturbances. SIPS is a concept of using system information from local as well as relevant remote sites and sending this information to a processing location to counteract propagation of the major disturbances in the power system. With the increased availability of advanced computer, communication and measurement technologies, more "intelligent" equipment can be used at the local level to improve the overall response. Traditional contingency dependant / event based systems could be enhanced to include power system response based algorithms with proper local supervisions for security.

Decentralized subsystems that can make local decisions based on local measurements (system-wide data and emergency control policies) and/or send pre-processed information to higher hierarchical levels are an economical solution to the problem [7]. A major component of the SIPS is the ability to receive remote measurement information and commands via the data communication system and to send selected local information to the SCADA centre. This information should reflect the prevailing state of the power system.

This paper describes how SIPS help manage system disturbances and prevent blackouts. The design and architecture of a SIPS is addressed. The paper also discusses an effort underway to gather best practices and operational experiences globally [8].

3. Blackouts - Cause and Effect

Reviewing examples of 1996 and 2003 system blackouts worldwide [9-10] reveal some similar patterns among such disturbances. Some common causes include:

- Pre-existing conditions, such as generator/line maintenance, heavy loading.
- Tripping lines due to faults and/or protection actions resulting in heavy overloads on other lines. Protection and control misoperation or unnecessary actions, which may contribute to disturbance propagation.
- Insufficient voltage (reactive power) support.
- Inadequate right-of-way maintenance.
- Insufficient alarms or monitoring to inform operators of equipment malfunctions.
- Inability of operators to respond to impending disturbances or to prevent further propagation of the disturbance and problems with EMS/SCADA systems to provide only important information when required.
- Inadequate planning/operation studies.
- Automated actions are not available/initiated to prevent further overloading of the lines, arrest voltage decline and/or initiate automatic and pre-planned separation of the power system.

While it is not realistically possible to completely eliminate blackouts (unless very large investments are made that would make the price of electricity unreasonable for end users) the above shows that by taking some reasonably cost-effective measures, occurrence of the blackouts could be reduced. We are focusing in this paper on the last of those issues, implementation of automated actions, the purpose of which is to prevent an imminent blackout, or at least arrest its propagation and mitigate some of its undesired consequences.

4. Technology for Modern Protection

SCADA/EMS system capability has greatly improved in the last few years, due to improved communication facilities and enhanced data handling capabilities. Improved EMS/SCADA systems require the ability to filter, display, and analyze only critical information and to increase availability of critical functions to 99.99% or better. Critical alarm monitoring systems must be maintained in top operating condition, and newer alarm analysis technologies should be deployed to detect and prevent the spread of major disturbances.

Modern technology, such as phasor measurement units (PMUs) and high bandwidth and high-speed communication networks, can provide time-synchronized measurements from all over the grid [1]. Based on those measurements, improved, faster and more accurate state estimators can be developed. In addition, advanced algorithms and calculation programs that assist the operator can also be included in the SCADA system, such as “faster than real-time simulations” to calculate power transfer margins based on various contingencies.

Development of system integrity protection schemes can help manage system disturbances and prevent blackouts. Those wide area protection schemes are based on pre-planned, automatic and corrective actions, implemented on the basis of system studies, with the goal to restore acceptable system performance. Although SIPS schemes can help increase the transfer limits, their primary goal is to improve security of the power system.

As system conditions change, it is necessary to perform studies and review protection designs on a regular basis to prevent protection misoperation. In addition, as protection systems are designed to be either more dependable (emphasis on making sure that protection acts when it should) or more secure (protection does not misoperate), designers can increase the security of protection design in the areas vulnerable to blackouts. As an example, transmission line pilot protection could be migrated to Permissive Overreach Transfer Trip scheme (POTT), which is more secure, compared to the more dependable Directional Comparison Blocking (DCB) scheme.

As hidden failures have been identified to be the significant contributors to blackouts [9], adequate testing of not only individual relays, but also overall relay applications, is crucial to reveal the potential failures. As system protection is generally intended to operate for rare events, and at the same time to mitigate a large number of potential disturbance conditions, a well developed automated testing plan which verifies inputs, logic, and output, is critical for proper maintenance of the scheme.

5. SIPS: Design and Architectures

The SIPS encompasses Special Protection Schemes (SPS), Remedial Action Schemes (RAS), as well as additional schemes such as, but not limited to, Underfrequency (UF), undervoltage (UV), out-of-step (OOS), etc., Figure 1.

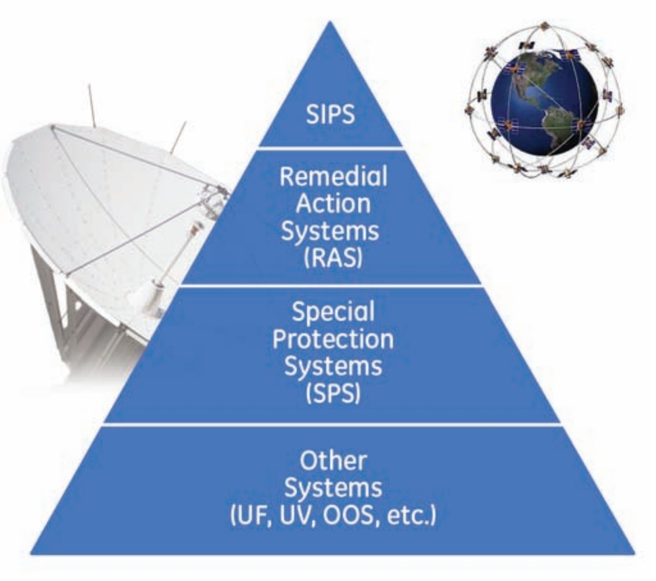

SIPS
Remedial Action Systems (RAS)
Special Protection Systems (SPS)
Other Systems (UF, UV, OOS, etc.)

Figure 1.
SIPS, A Set of Automatic, Synchronized, and Coordinated Counter Measures

SIPS are installed to protect the integrity of the power system or its strategic portions. A SIPS is applied to the overall power system or a strategic part of it in order to preserve system stability, maintain overall system connectivity, and/or to avoid serious equipment damage during major events. Therefore, the SIPS may require multiple detection and actuation devices and communication facilities. Figure 2 shows SIPS classification.

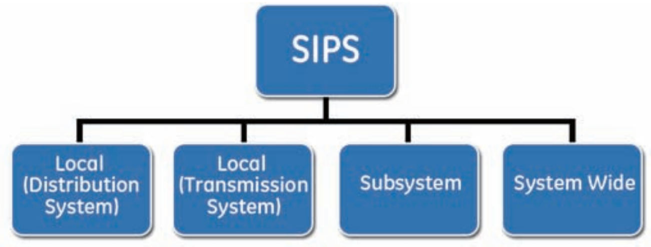


Figure 2.
SIPS Classification

SIPS classifications have been defined through a collective global industry effort by members of the IEEE and CIGRE [8]. Below is a summary.

Local (Distribution System) – SIPS equipment is usually simple, with a dedicated function. All sensing, decision-making and control devices are typically located within one distribution substation. Operation of this type of SIPS generally affects only a very limited portion of the distribution system such as a radial feeder or small network.

Local (Transmission System) - All sensing, decision-making and control devices are typically located within one transmission substation. Operation of this type of SIPS generally affects only a single small power company, or portion of a larger utility, with limited impact on neighboring interconnected systems. This category includes SIPS with impact on generating facilities.

Subsystem - The operation of this type of SIPS has a significant impact on a large geographic area consisting of more than one utility, transmission system owner or generating facility. SIPS of this type are more complex, involving sensing of multiple power system parameters and states. Information can be collected both locally and from remote locations. Decision-making and logic functions are typically performed at one location. Telecommunications facilities are generally needed both to collect information and to initiate remote corrective actions.

System wide - SIPS of this type are the most complex and involve multiple levels of arming and decision making and communications. These types of schemes collect local and telemetry data from multiple locations and can initiate multi-level corrective actions consistent with real-time power system requirements. These schemes typically have multi-level logic for different types and layers of power system contingencies or outage scenarios. Operation of a SIPS of this type has a significant impact on an entire interconnected system.

Failure of the SIPS to operate when required, or its undesired or unintentional operation will also impact balanced power system operation. Therefore, design of the SIPS may involve redundancy or some backup functions, and depending on the operational security requirements, may involve some form of voting or vetoing (fail-safe) based on the intended design.

The scheme architecture can be described by the physical location of the sensing, decision making, and control devices that make up the scheme and the extent of impact the SIPS has on the electrical system. SIPS are classified into two main types of architectures: flat and hierarchical.

Flat Architecture - the measurement and operating elements of the SIPS are typically in the same location. The decision and corrective action may need a communication link to collect remote information and/or to initiate actions.

Hierarchical Architecture - There are several steps involved in the SIPS corrective action. For example, local measurement, or a series of predetermined parameters at several locations are transmitted to multiple control locations. Depending on the intent of the scheme, immediate action can be taken and further analysis performed. The scheme purpose will drive the logic, design, and actions. Typical logic involves use of operating nomograms, state estimation and contingency analysis.

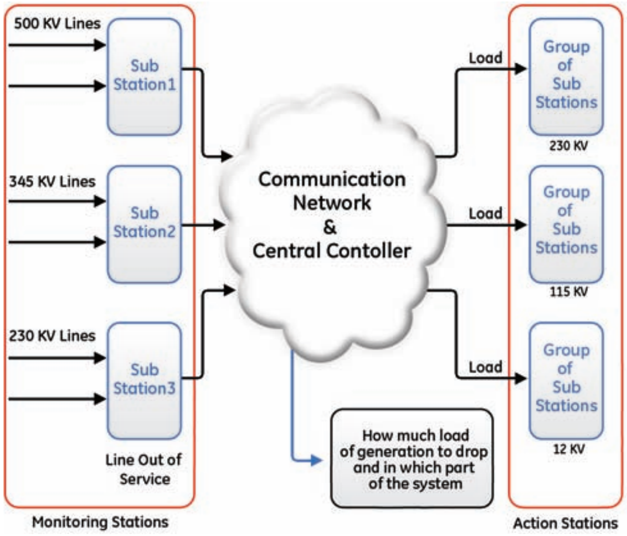


Figure 3.
System protection terminal [12]

The design should address all standard requirements for protection terminals [13], [14]. The terminal is connected to the substation control system. For time tagging applications, a GPS-based synchronization function is needed, Figures 1 and 3. The system protection terminal possesses a high-speed communication interface to transfer data between the terminal databases, which contain all updated measurements and binary signals recorded in that specific substation. The conventional substation control system is used for the input and output interfaces with the power system. The decision-making logic contains all the algorithms and configured logic necessary to derive appropriate output control signals, such as circuit-breaker trip, AVR-boosting, and tap-changer action, to be performed in that substation. The input data to the decision-making logic is taken from the continuously monitored data, stored in the database. A low speed communication interface for SCADA communication and operator interface should also be available as an enhancement for the SCADA state estimator. Actions ordered from SCADA/EMS functions, such as optimal power flow, emergency load control, etc., could be activated via the system protection terminal. The power system operator should also have access to the terminal, for supervision, maintenance, update, parameter setting, change of setting groups, disturbance recorder data collection, etc.

For local schemes, where monitoring and decision stations are within close proximity, there may still be a need for use of high-speed communication. Details of an extremely high speed vetoing scheme involving major generation and coordination against various types of protection schemes including out-of-step protection has been described in [13].

6. SIPS or RAS Application Definitions

The types of SIPS applications may vary based on the topology of the power grid. There may also be different views on the acceptability of the type of the application. For example, use of SIPS for generation shedding to balance grid performance may be viewed as unacceptable for certain levels of contingency in one network but a common practice in another interconnected grid. Consider power systems with limited transmission corridors where building a redundant and diverse interconnection outlet for a generating facility may not be physically practical or economically feasible to address variety of technically possible outlet outages. In such conditions, the generator owner may accept a certain level of risk so long as it can be demonstrated that such SIPS does not result in an unacceptable level of security for to other parts of the grid.

Table 1 shows the types of wide-are disturbances likely to occur in two different types of interconnected power grids, namely meshed network vs. an interconnected transmission system of narrow corridors consisting of extensive generation tied to the interconnection.

System Configuration	Densely meshed power system with dispersed generation and load		Lightly meshed transmission systems with localized generation and load	
Events	Located in a large interconnection	Not interconnected or by far the largest partner	Located in a large interconnection	Not interconnected or far the largest partner
Overloads	**	**	*	*
Frequency instability	*	**	*	**
Voltage instability	*	*	**	**
Transient angle instability	*	*	**	**
Small signal stability	*	*	*	*

Table 1.
Types of Wide-Area Events on two Different Interconnected Transmission Systems

The characteristics of the power system influencing the types of mitigation methods have been described in a variety of literature [15-19]. The mitigation measure to maintain grid integrity are described in a document under development by a collaborative effort of IEEE, CIGRE, and EPRI [8]. Below is a summary listing of the types:

- Generator Rejection
- Load Rejection
- Under-Frequency Load Shedding
- Under-Voltage Load Shedding
- Adaptive Load Mitigation
- Out-of-Step Tripping
- Voltage Instability Advance Warning Scheme
- Angular Stability Advance Warning Scheme
- Overload Mitigation
- Congestion Mitigation
- System Separation
- Shunt Capacitor Switching
- Tap-Changer Control
- SVC/STATCOM Control
- Turbine Valve Control
- HVDC Controls
- Power System Stabilizer Control
- Discrete Excitation
- Dynamic Breaking
- Generator Runback
- Bypassing Series Capacitor
- Black-Start or Gas-Turbine Start-Up
- AGC Actions
- Busbar Splitting

7. SIPS or RAS: Industry Experience

In August of 1996, a seminal article [20] was published as a result of the activity of the joint Working Group of IEEE and CIGRE, the purpose of which was to investigate the special protection schemes then in existence worldwide and to report about various aspects of their designs, functional specifications, reliability, cost and operating experience. The report encompassed over 100 schemes from all over the world and provided a wealth of information on the direction the industry was taking in coping with ever larger disturbances.

In 2004, the System Protection Subcommittee of the IEEE Power System Relaying Committee started an initiative to update the industry experience on RAS, SPS and SIPS by creating and widely disseminating a new survey, which would attempt to attract as wide a response from the industry worldwide as the original report did. The authors of this paper are amongst the many industry recognized members that have generated a survey of industry experiences [16]. After considerable effort to incorporate in the framework of the new survey most of the advances which have occurred in the last decade, coupled by design considerations for natural calamity phenomenon such as tsunami or hurricanes, or seismic events, the revised survey has been completed and has distributed globally to professional audience with an intention to solicit as wide a response.

8. Structure of the Survey

The survey is divided into two parts: Part 1 identifies the "Purpose" of the scheme with subsections of "Type" and "Operational Experience" - For that part, a series of questions are repeated for each type of scheme which is reported.

Part 2 concerns Engineering, Design, Implementation, technology, and other related sections such as cyber security Considerations. This series of questions are asked only one time. The respondents are asked to answer those questions based on most common practice in their companies.

The survey also asks respondents to identify the system integrity protection schemes that exist on their systems, the design and implementation, and the operation experience as applicable. Results of the survey are expected to assist the respondents in:

- The application, design, implementation, operation, and maintenance of new and next generation SIPS.
- Understanding feasible alternatives applied to extending transmission system ratings without adding new transmission facilities.
- Applicability of delayed enhancement of transmission networks to the respondent's system.
- Providing reasonable countermeasures to slow and/or stop cascading outages caused by extreme contingencies (safety net).

The survey is intended for power system professionals involved in the Planning, Design, and Operation of SIPS. Specific skill required to complete the survey include, protection, telecommunication and system planning. The survey is distributed through CIGRE, IEEE, and EPRI. Among the questions found in Part II of the survey are the following issues:

- System Studies Done Prior to Deploying the SIPS
    - Planning criteria
    - Types of planning studies
    - Real-time operational studies
    - Protection and control coordination studies
- Coordination with other Protection and Control systems
- Types of protective relaying technology used
- Existence of standards for SIPS applications
- Hardware Description and Outage Detection
    - Outage detection Method
    - Questions on use of programmable logic controllers
- Scheme Architecture
    - Objective: decision making
    - Redundancy needs/implementation - Both telecommunication and hardware
    - Redundancy philosophy
    - Questions on use of the voting schemes
    - Questions about control: event based, or response based
    - Questions on Breaker Failure
    - Performance requirements:
        - Throughput timing: entire scheme
        - Throughput timing of the controller
- Data acquisition and related tools
    - Measured Quantities
    - Time synchronization requirements
    - Use of SMART SIPS / Intelligent SIPS
    - Blocking (by the scheme) of any automatic reclosing
    - Restoration Issues and Planned Mechanisms
- Communication, Networking, and Data Exchange
    - Architecture of the communication
    - Communication medium and protocols
    - Information about shared communication (with other applications)
    - Impact of communication failure on reliability index and availability
    - Cyber security implementation and protection features
    - Operability of the scheme with a communication channel failure
    - Control Area Visibility
- Arming methodology
- Implementation issues
    - Multi-functionality of the scheme
    - Design: Centralized or Distributed Architecture
    - Availability of event reconstruction or system playback capability
    - Description of event records and their availability within the organization
- Testing Considerations
    - Testing procedure
    - Periodicity of testing
    - Maintenance issues
- Cost Considerations
    - Approximate cost
    - System information (infrastructure)

The survey is currently being disseminated and responses are being collected. When sufficiently large sample of responses is received, a report will be compiled which is expected to answer many questions about current industry practices, regional differences in system protection philosophy and experience with such designs.

9. Conclusions

The paper describes some of the critical design considerations and applications of latest technology for SIPS. Applicability of the advanced analytical techniques for various types of SIPS applications on the basis of modern technology is also addressed as part of the overview. An overview is presented of traditional scheme requirements leading to the SIPS of the future. In the light of fast changing operating conditions in power systems (ever smaller security margins and transmission capacity, aging infrastructure, etc.) and quickly changing enabling technologies for power system control and protection, the industry landscape is changing quickly and adapting to the conditions imposed by new business practices. The new survey should provide valuable information to industry practitioners and researchers alike about the trends and experiences in system protection. The readers are encouraged to assist the authors in disseminating the survey across the globe for maximum impact.

10. References

[1] D. Novosel, M. Begovic, V. Madani, "Shedding Light on Blackouts", IEEE PES Power & Energy, January / February 2004.

[2] K. Walve, "Modelling of Power System Components at Severe Disturbances", CIGRE paper 38-17, 1986, Paris, France.

[3] V. Madani, D. Novosel, A. Apostolov, S. Corsi, "Innovative Solutions for Preventing Wide Area Disturbance Propagation - Protection and Control Coordination Impact and Other Considerations In Cascading Disturbances ", International Institute for Research and Education in Power Systems Symposium Proceedings, August 2004.

[4] "Wide Area Protection and Emergency Control", Working Group C-6, System Protection Subcommittee, IEEE PES Power System Relaying Committee, January 2003.

[5] V. Madani "Understanding and Preventing Cascading Failures in Power Systems", National Science Foundation, October 2005.

[6] P. Kundur, Power System Stability and Control, McGraw-Hill, 1994.

[7] K. Vu, M. Begovic, D. Novosel and M. Saha, "Use of Local Measurements to Estimate Voltage-Stability Margin," Power Industry Computer Applications Conference (PICA), May 1997.

[8] "Global Industry Experiences with System Integrity Protection Schemes" – Survey of Industry practices – IEEE PES Power System Relaying Committee - Work in progress.

[9] Union for the Coordination of Transmission of Electricity (UCTE), Press Release, September 29, www.ucte.com.

[10] FERC, U.S./Canada Power Outage Task Force, "Initial Blackout Timeline," Press Release, September 12, 2003, www.ferc.gov.

[11] WECC, Coordinated Off-Nominal Frequency Load Shedding and Restoration Plan, November, 1997 and 2004.

[12] V. Madani, M. Adamiak, Engineering and Implementation of Wide Area Special Protection Schemes; Clemson, March 2008.

[13] V. Madani, M. Adamiak; et al. "High-Speed Control Scheme to Prevent Instability of a Large Multi-Unit Power Plant", Georgia Tech Protective Relaying Conference; May 2007.

[14] M. Begovic, V. Madani, D. Novosel, "System Integrity Protection Schemes (SIPS)", International Institute for Research and Education in Power Systems Proceedings, August 2007.

[15] S.H. Horowitz and A.G. Phadke, "Boosting Immunity to Blackouts," Power & Energy Magazine, September/October 2003.

[16] I. Dobson, J. Chen, J. Thorp, B. Carreras, D. Newman, "Examining Criticality of Blackouts in Power System Models with Cascading Outages", Proc. 35th Hawaii International Conference on System Science, Hawaii, January 2002.

[17] "Guide for the Application of Protective Relays Used for Abnormal Frequency Load Shedding and Restoration", IEEE PES PC37.117 System Protection Subcommittee, May 2004.

[18] CIGRE WG38.02.19, D. Karlson, et al., System protection schemes in power, June 2001.

[19] WECC Voltage Stability Methodology – May 1998 and May 2004.

[20] "Industry Experience with Special Protection Schemes" IEEE/CIGRE Special Report, P. Anderson, B.K. LeReverend, IEEE Transactions on Power Systems, Vol. 11, No. 3, Aug. 1996, pp. 1166-1179.

0319-v3

ESAC

ELECTRICAL & SYSTEMS ADVANCED CONTROL INC.

Providing turn-key tailored integrated solutions using the latest technology in standard products to specifically suit your needs. Our friendly staff work with you from functional specification and establishing budgets to technical design, system development, site implementation and training; to ensure system performance.

ESAC offers services that will broaden your system's capabilities and increase the operations effectiveness with potential for growth in your organization. With an expanding client base, ESAC is equipped to fulfill your needs.

Electrical & Process Systems

- Load flow, short circuit and protection coordination
- SLD, AC/DC, CWD and IED drawings
- IED, RTU and PLC programming
- Protection and automation models

Software & Graphic Systems

- Communications, Historian and Web Interfaces
- HMI screens, databases and system manuals
- Custom software for user interfaces
- Database and graphic models

Technical Services

- CSA Panel Shop
- Site investigations, maintenance and testing
- System retrofits and upgrades
- Training and support programs
- Strategic alliance partnering
- Project technical management
- Detailed conceptual design and budget reports

Distribution Automation

- Fault localization, auto sectionalizing and restoration
- Distribution generation, voltage and VAR control

Projects Administration

- Commercial contracts, project life cycle and scheduling
- Materials processing, assessments, operations and reporting

Systems at Your Fingertips
Integrated Protection, Control and Metering

Visit our website or contact us for further information
www.esac.com   (519) 686-6722

142.2 A
10.8 MW
8.09 Mvar
565.7 A
11.713 MW
7.949 Mvar
SYSTEM GENERATION

Powered by
etap iSUB

Tieline Controls in Microgrid Applications

M. Adamiak
GE Digital Energy, Multilin

S.Bose,
GE Global Research,

Y.Liu,
GE Global Research,

K.Bahei-Eldin
GE Global Research,

J.deBedout
GE Global Research,

1. Introduction

As electric distribution technology moves into the next century, many trends are becoming apparent that will change the requirements of energy delivery. These changes are being driven from both the demand side where higher energy availability and efficiency are desired, and from the supply side where the integration of distributed generation and peak-shaving technologies must be accommodated. Distribution systems possessing distributed generation and controllable loads with the ability to operate in both grid-connected and standalone modes are an important class of the so-called Microgrid power system (Figure 1).

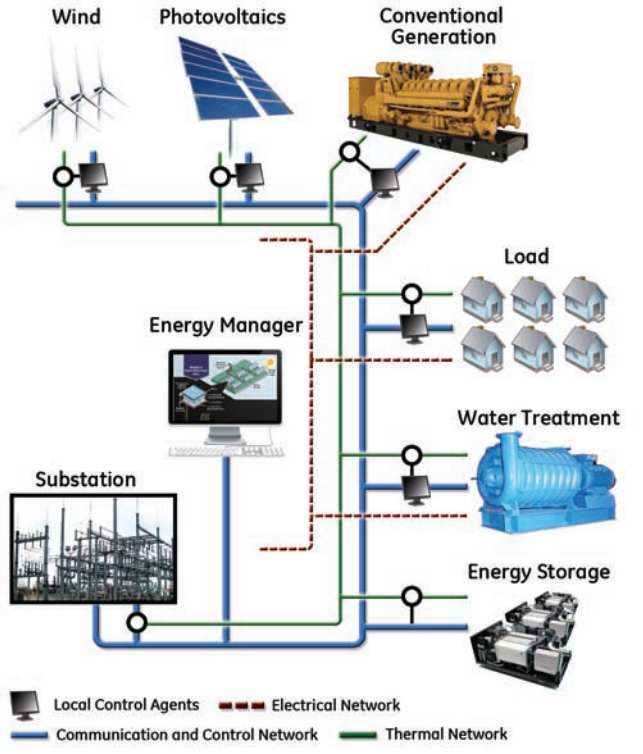


Figure 1.
Microgrid power system

This class of Microgrid strives for optimized operation of the aggregated distribution system by coordinating the distributed generation and load resources - not only when connected to the main grid but also in a stand-alone mode. In either mode of operation, advanced local controls, energy management and protection technologies are required for robustness and reliability.

While the energy management optimization objective function can be tailored to the needs of each application, in general the overall objective is to optimize operating performance and cost in the normally grid-connected mode, while ensuring that the system is capable of meeting the performance requirements in stand-alone mode. One very appealing technology for grid connected operation is tieline controls, which will regulate the active and reactive power flow between the Microgrid and the bulk grid at the point of interconnection. These controls essentially allow the Microgrid to behave as an aggregated power entity that can be made dispatchable by the utility. Particularly beneficial to the utility is the fact that this feature can be designed to compensate for intermittency associated with renewable energy resources such as wind energy and solar energy, essentially pushing the management burden inside the Microgrid. This paper reviews the overall architecture of the Microgrid concept, and presents details associated with the tieline control features.

2. Microgrid Concept and Architecture

A report by Navigant Consulting [1] prepared for DOE's Office of Electricity Delivery and Energy Reliability identifies four classes of Microgrids:

Single Facility Microgrids

These Microgrids include installations such as industrial and commercial buildings, residential buildings, and hospitals, with loads typically under 2 MW. These systems typically have low inertia and require backup generation for off-grid operation. Microgrids for these applications will be designed to have improved power availability and quality, and a subset of them, such as hospitals, will require a seamless transition between grid-connected and island operation.

Multiple Facility Microgrids

This category includes Microgrids spanning multiple buildings or structures, with loads typically ranging between 2 and 5 MW. Examples include campuses (medical, academic, municipal, etc), military bases, industrial and commercial complexes, and building residential developments. As with single facility Microgrids, the design of multiple facility Microgrids will be driven by the need for high availability as well as improved power quality.

Feeder Microgrids

The feeder Microgrid will manage the generation and/or load of all entities within a distribution feeder – which can encompass 5-10MW. These Microgrids may incorporate smaller Microgrids – single or multiple facility – within them. The appeal of these Microgrids is the potential to realize regional improvements in availability, offered by the ability of the Microgrid to separate from the bulk grid during grid disturbances and service it's internal loads. Utilities, municipal utilities and coops are seen as future owners/operators of these Microgrids.

Substation Microgrids

The substation Microgrid will manage the generation and/or load of all entities connected to a distribution substation – which can encompass 5-10+MW. It will likely include some generation directly at the substation, as well as distributed generation and Microgrids included at the feeder and facility level. The appeal is again the potential to realize improvements in availability, offered by the ability of the Microgrid to separate from the bulk grid during disturbances and service its internal loads.

All of these Microgrid categories will benefit from the ability to control the dynamic exchange of power between the Microgrid and the bulk grid over the interconnecting tieline(s).

3. Tieline Control Design

A "tieline" refers to the feeder connection between the Microgrid and bulk grid. Tieline controls can be designed to manage the feeder power flow and voltage at the point of interconnection (POI) to meet the needs of the system operator. Control is implemented by coordinating the assets of the Microgrid, allowing the collection of these assets to appear as one aggregated dispatchable producing or consuming entity connected to the bulk grid. This section outlines the reactive and active power controls required for this capability.

Microgrid Reactive Power Control (M-VAR)

The primary functions of M-VAR are voltage regulation and power factor control at the tieline. Capabilities include voltage setpoint, steady state voltage response, and transient VAR response.

The M-VAR controller can receive either an external remote reactive power command or a voltage command from the system operator. The closed loop control issues reference VAR commands over the communication channel to each Microgrid controllable asset controller. The local controls [2] ultimately are responsible for regulating the VARs locally in each component. The controller compares the VAR output at the tieline or point of interconnection (POI) and adjusts the M-VAR command to obtain the desired system voltage. M-VAR control has two modes of operation: voltage regulated and VAR regulated (Figure 2). The voltage Vpoi refers to the measured line-to-line RMS value. Qpoi is to the total reactive power measured at the POI.

In the voltage regulation mode, the voltage error is compensated by a proportional-integral (PI) controller to produce a total reactive power demand. After subtracting the shunt reactive power, provided by the shunt capacitors (if any), the total reactive power command, Qttl,net, for the controllable asset in the Microgrid is obtained.

In the VAR regulation mode, the error between the Q reference and the Q measurement at the POI is regulated by a PI regulator. By adding the desired voltage feed forward, it provides a voltage reference to the voltage regulation loop. The total reactive power command is applied to the dispatch reference selection function to generate a reactive power command for each individual available controllable asset.

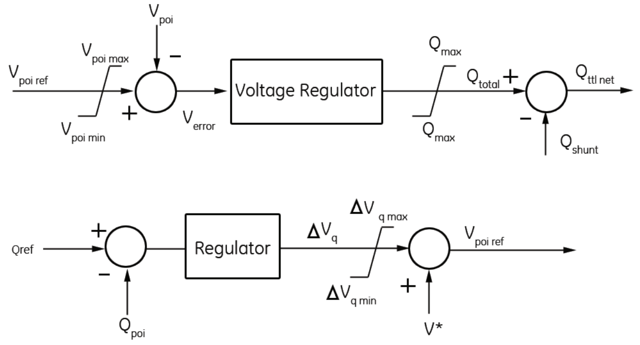


Figure 2.
M-VAR Block Diagram

Microgrid Active Power Control (M-APC)

The primary function of M-APC is to control steady-state and transient active power flow at the tieline. The objectives of the M-APC include:

- Enforcing power limits at the point of interconnection (POI)
- Enforcing ramp-rate limits at the POI
- Responding to system frequency excursions

These three functions are represented graphically in the block diagram in Figure 3. The parallel control loops for power limit, ramp rate limit and frequency limit will not be activated if all the operating conditions are within allowable limits. However, if any one of the controls is triggered, an adjustment command ***P is generated with the intent to bring the system back to the normal operating condition. A priority is given to each parallel control loop with power limit control having highest priority and ramp rate limit control having the lowest. The total adjustment command ***P is passed to the dispatch reference selection function, which allocates the ***P among the available controllable assets based on their participation factor assigned by the optimal dispatch control. The individual adjustment is added to the P set point from the optimal dispatch control to provide the final command to the controlled assets.

Power Limit Control.

Power limit control permits the system operator to assign a limit on the amount of active power that can be exported or imported from the grid. Power import and export are represented as negative and positive power, respectively, at the POI in the control.

Power Frequency Control.

Power frequency control is designed to support the grid frequency at the POI by adjusting active power. The inputs to the controller are the frequency and active power measured at the POI. The control law determines the power order in response to frequency excursions as specified by the system operator. A typical control law will require increased power output when frequency dips below nominal and decreased power output for increased frequency. The final output DPpr is fed to the prioritization function.

Ramp Rate Limit Control.

It is anticipated that system operators will require ramp rate control of tieline power. This control will operate by adjusting the power output of Microgrid assets to compensate for the variable nature of Microgrid loads and generation. Two rate limits are specified for both increasing and decreasing power flow. The first applies to the maximum ramp rate averaged over one minute, and the second applies to the maximum ramp rate averaged over ten minutes. The ramp rate limit calculation is designed to meet these ramp rate limits, without unnecessarily penalizing.

Microgrid Energy Production.

Power is measured at the POI and passed through washout filters to determine the average ramp rates. The measured ramp rates are then compared with the ramp rate limits. The resulting error signals are compared and the most limiting is selected.

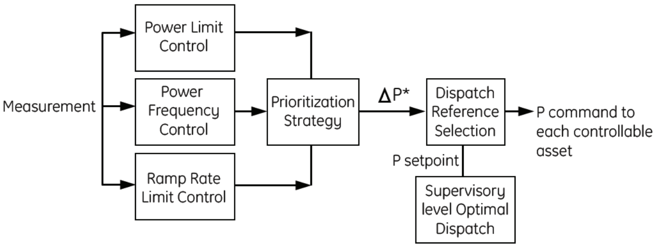


Figure 3.
M-APC Block Diagram

M-APC Regulator.

The error signals generated by power limit, ramp rate limit, and power frequency feed a prioritization block that selects a single error signal for control. This error signal is the input to a common M-APC regulator. The output of this regulator is a Microgrid power adjustment signal that is distributed to the controllable assets of the Microgrid.

4. Case Study Results on Tieline Controls

Case Study 1: Municipal Campus Microgrid

This case study examines a comprehensive and integrated solution to the challenge of providing reliable energy for a multi-facility Microgrid.

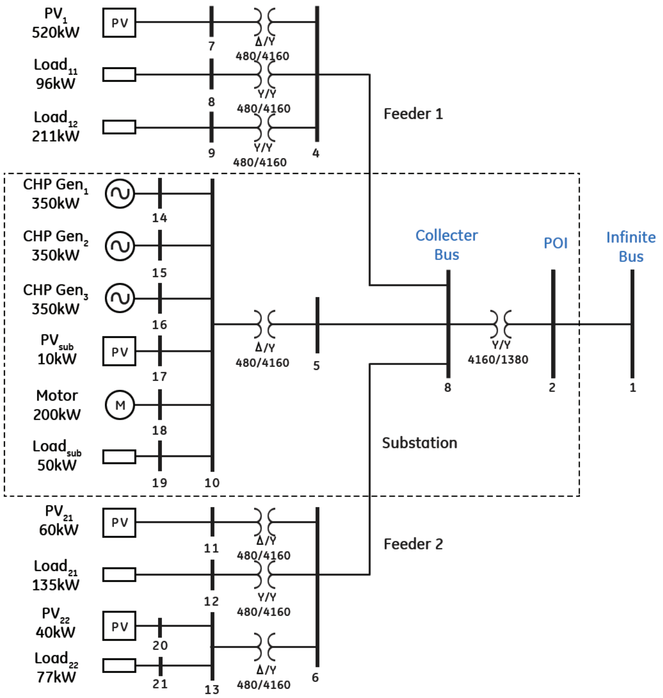


Figure 4.
Municipal Campus Microgrid

Figure 4 shows the municipal campus network considered in this example. Feeder one includes 100kW of critical loads and 200kW of noncritical loads and an aggregated solar PV system of 500kW. Feeder two includes two PV systems rated at 60kW and 40kW respectively, and two loads at 135kW and 80kW. The substation houses three 350kW engine gensets, a 10kW solar PV system, a 250 KW operating load, and a 250kW motor load representing a chiller for CHP. The standard loads are modeled as P and Q controlled impedance loads, while the motor load is modeled as an induction motor. The solar PV system is modeled as a PV module with a DC/AC converter in d-q form. The PV array in the substation is modeled with VAR control capability. The power flow in the network is solved using a traditional load flow solution, which assumes balanced (positive sequence only) conditions. Since gensets 2 and 3 are a peaker unit and a backup unit respectively, in the test cases they are both offline. Only genset 1 and the small PV at the substation are considered controllable assets. The supervisory control includes the dispatch control as well as the tieline control (M-VAR and M-APC). The goal for this case study is to analyze the control performance for tieline controls.

Impact of Voltage Disturbance

The utility grid voltage is subject to variations that are usually within +/- 5% depending mainly on the voltage level, utility system operation and design practices. The simulation shown in Figure 5 illustrates some of the performance characteristics of the M-VAR control. M-VAR has two modes of operation: voltage regulated and VAR regulated. In this case, the system was operating under voltage control. That is, the MVAR modifies reactive power of controllable sources in order to maintain the POI voltage at its setpoint. The test consists of a 1% voltage step change at the "Infinite Bus" in Figure 4. Results are presented in Figure 5.

Shown in Figure 5 are the disturbance and variations at the POI. The transient voltage variation at the POI is relatively small. The reactive power variation at the POI is a result of the operation of the M-VAR. The active power at the POI varies due to the voltage variations inside the Microgrid. The reactive power commands to genset 1 and the PV at the substation are modified. The response time of the system is on the order of 15 seconds. This response is relatively slow compared to typical response times of excitation controls, avoiding undesirable interactions with other controls.

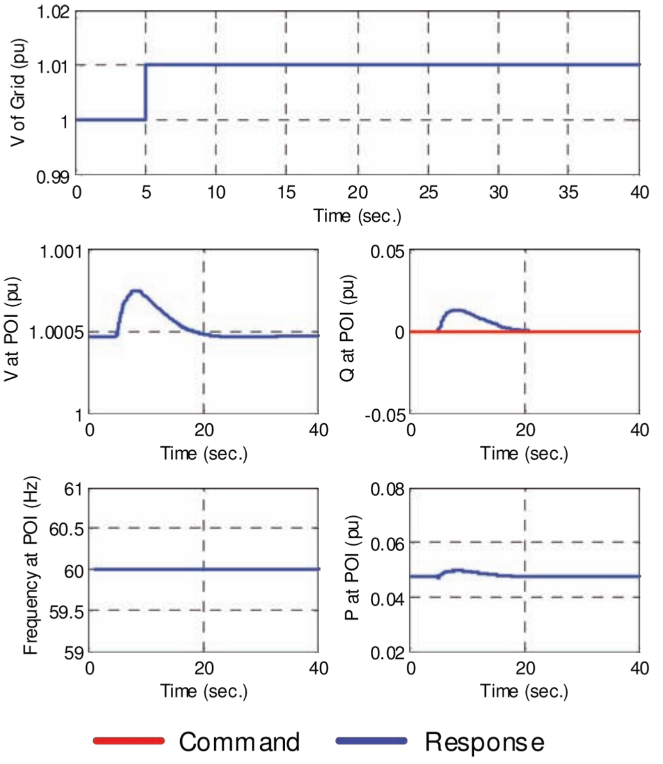


Figure 5.
Response at POI to +1% grid voltage change

Impact of Reactive Power Command Change

To maintain voltages throughout a distribution system, a utility may send reactive power commands from the control center. A Microgrid that can meet such commands supports the system operation and provides a potential market service opportunity. The simulation shown in Figure 6 illustrates the response of the M-VAR under reactive power control to an increase in reactive power command of 0.01pu (10MW base). Figure 6 presents the simulation results.

Shown in Figure 6 are magnitudes at the POI. The reactive power at the POI follows the command with a 15 second response time. The reactive power change causes an increase in the voltage at the POI and inside the Microgrid, while the impact on frequency is negligible. The test results show that the controls are able to respond to this command and supply the requested reactive power at the POI by allocating it amongst the controllable generation sources. In this case, the VAR dispatchable assets are engine genset 1 and the PV at the substation.

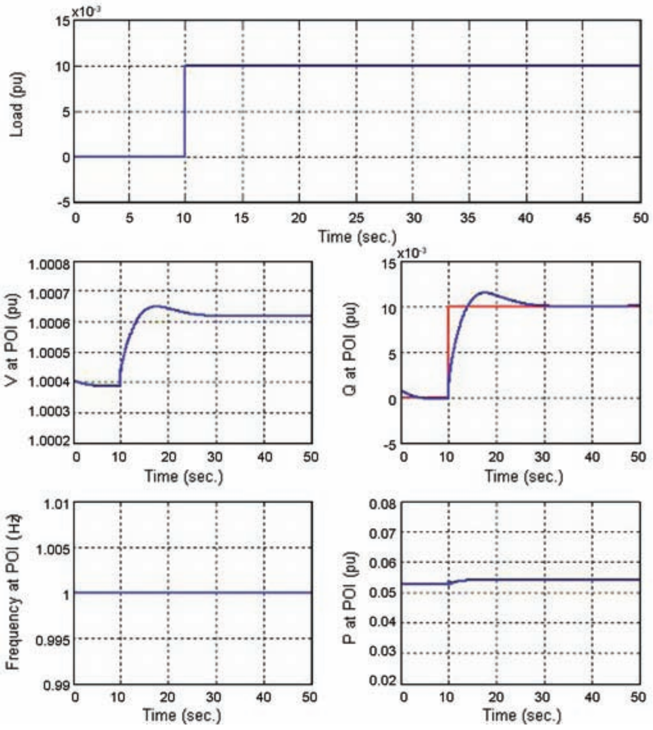


Figure 6.
Response at POI to +0.01 pu Q command change

Impact of Load Changes

The total load in the Microgrid is subject to demand changes. The system should adapt to load changes to not exceed operational limits at the POI, such as power export/import limits or power ramp rate limits. The examples in this section show M-APC control under 2 scenarios:

1. A load change that exceeds the power import limit, triggering the power limit control
2. A load change causing power at the POI to ramp at a rate that exceeds the ramp rate limit, triggering the power ramp rate limit control

Power Import/Export Limit.

In this example 750kW of load is ramped up in 4 seconds. The results are presented in Figure 7. This load change causes the power import to violate the import limit at the POI. The M-APC operates to increase the power from the controllable generators to bring the active power at the POI back within limits. Genset 1 is the controllable active power source in service. The governor response of Genset 1 is significantly faster than the M-APC and the power output and the command almost coincide. The M-APC control was not set to operate on active power rate limitation at the POI in this example. M-VAR is in reactive power control mode and operates to compensate for the reactive power changes at the POI. Due to the load change, the system moved to a new steady state with lower voltage at the POI while maintaining the commanded Q (0 pu).

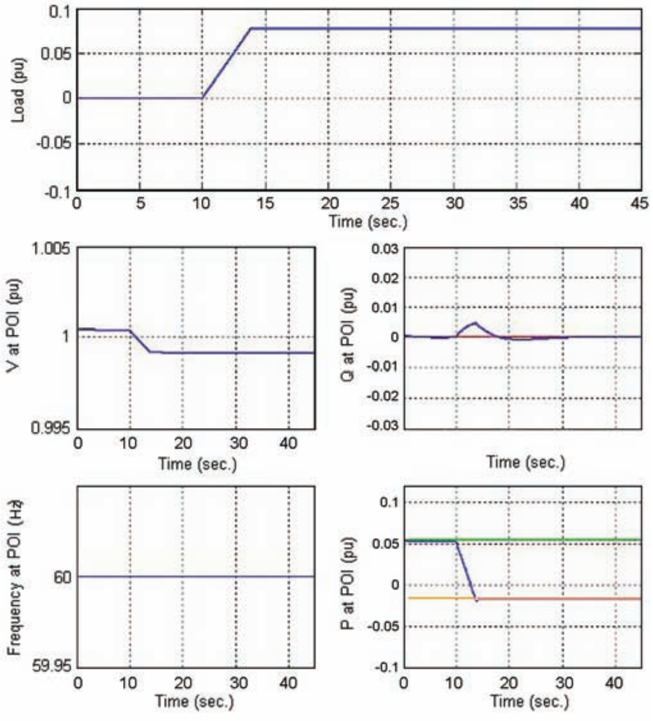


Figure 7.
Response at POI to load change (750kW) – Power Limit Control

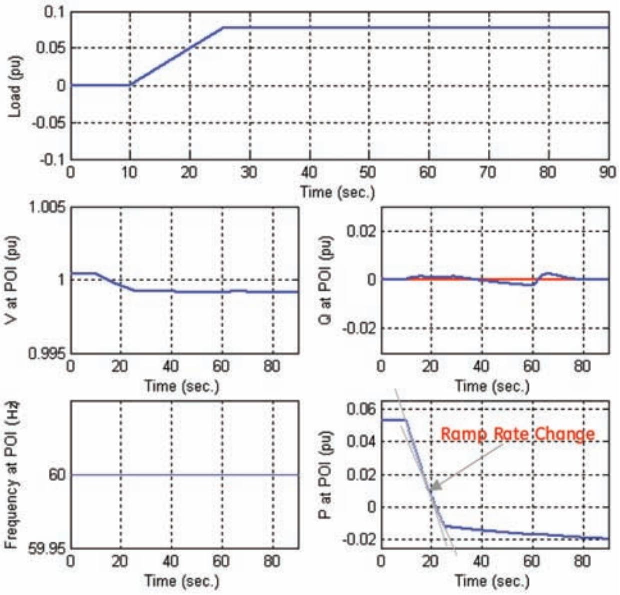


Figure 8.
Response at POI to Load change 50kW) – Power Ramp Rate Control

Ramp Rate Limit.

In this example (Figure 8), the M-APC is set to limit the ramp rate of active power at the POI. A 750 kW load is picked up in 15 seconds at the rate of 3MW/min, exceeding the 600kW/min limit at the POI. The M-APC control increases the active power output of the controllable generator to reduce the Microgrid active power rate of change. With this method of control, the Microgrid requires less active power support compared to a Microgrid without MAPC. Due to the load change, the system moved to a new steady state with lower voltage at the POI while maintaining the commanded Q (0 pu). The delta P command is dispatched to the only active power controllable generation, Genset 1.

Case Study 2: Island Microgrid

This second case study evaluates a potential Microgrid on an island (in the geographical sense). The model includes a 34.5KV line from a switching station to the Microgrid location. The network configuration is shown in Figure 9 as a single-line diagram. The model is tested with the tieline control concepts discussed in the previous section. The model includes:

- A model of a conventional run-of-river hydro generator of 500kW.
- A 15MW wind farm model represented by aggregating 10 x 1.5MW wind turbines.
- A conventional load modeled as a P & Q controlled impedance load.
- The tieline controls, which include M-VAR and M-APC controls.

To test extreme cases, load variation sizes and power import/export limits and ramp rate limits are assumed.

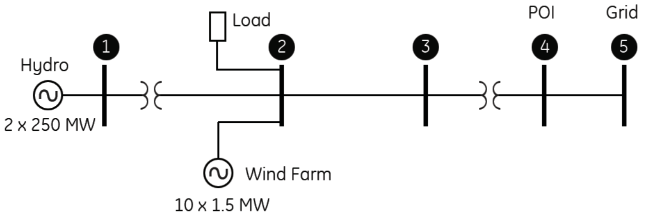


Figure 9.
Network Diagram for Case Study 2

Impact of Voltage Disturbance

A 1% voltage disturbance/step at the grid is applied at time t=30 seconds. This case is used to test the voltage regulation capability of the tieline control. Without a tieline controller, the voltage at the POI follows the disturbances and the effect of this disturbance is seen in the reactive and active powers at the POI as well as in all the wind and hydro assets (Figure 10).

M-VAR control will compensate for the voltage change at the grid side by dispatching VARs inside the Microgrid, so that the voltage at the POI will return to the setpoint after a short transient. The M-VAR control adjusts system reactive power to regulate voltage by commanding more VARs, allocating them among the wind and hydro. Figure 11 shows the results of a voltage disturbance at the grid, with M-VAR control and including wind variability. To show a clear response, a 2% grid voltage disturbance/step is applied in the variable wind case. Due to the variability of the wind, the control reaction in the test result is more difficult to discern, but it is clear that Q at the POI returns to its original average value. The test result shows that in the test time window, the ~30% power variation from wind causes about 0.5% of voltage fluctuation at the POI with the control.

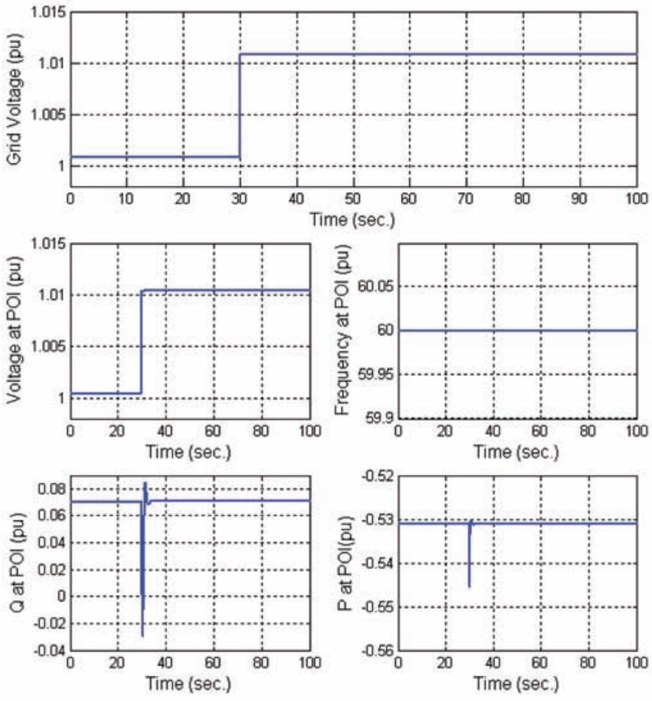


Figure 10.

Response to 1% grid voltage change – no Tieline Control, no wind variation

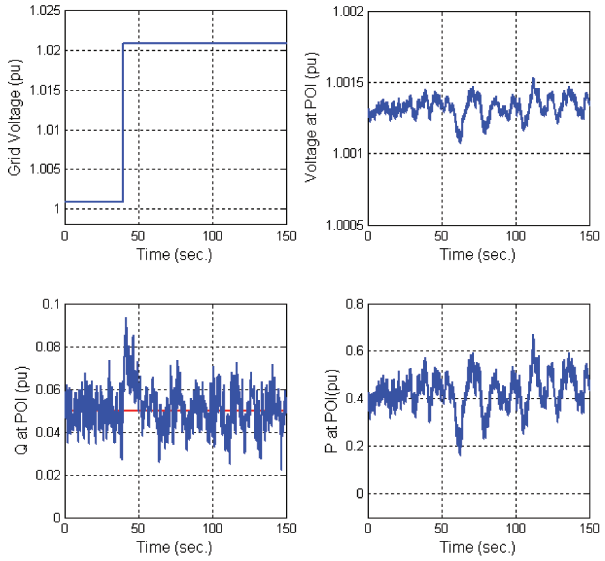


Figure 11.

Response to 2% grid voltage change with Tieline Control and wind variation

Impact of Reactive Power Command Change

Response to a reactive power commands would enable the Microgrid to provide VAR/Voltage regulation services. This test case is triggered by a Q command step change from an initial 500kVAR export to 0kVAR export at the POI. The test was performed under constant as well as time variable wind speed conditions. The results (Figure 12) show the system responds promptly and maintains voltage stability at the POI. The simulation results with wind variability (Figure 13) show clear reactive power response but no apparent voltage or active power changes.

Impact of Load Changes

Normally, the grid would cast a limit on how much power the Microgrid can import or export, as well as how fast the change can be. This capability ensures good grid citizenship. In this example, two scenarios are tested by a load change: active power import/export limit control and active power ramp rate control. In the first load change case (Figure 14), the load is ramped down from 10MW (1.0 pu) to 3.5MW (0.35 pu).

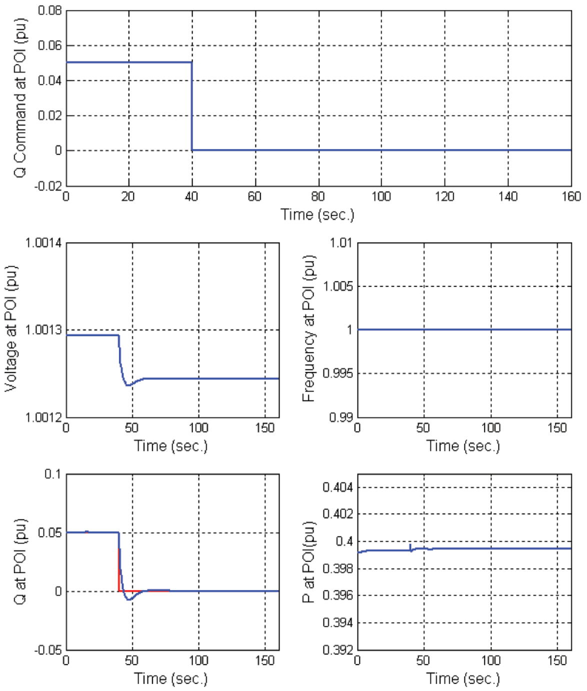


Figure 12.

Response to Q command change - no wind variability

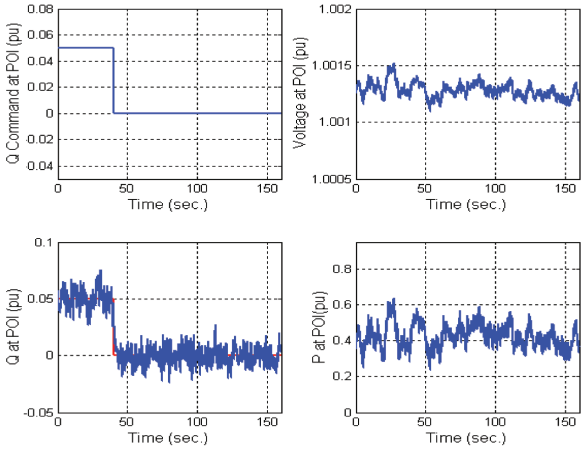


Figure 13.

Response to Q command change -wind variability

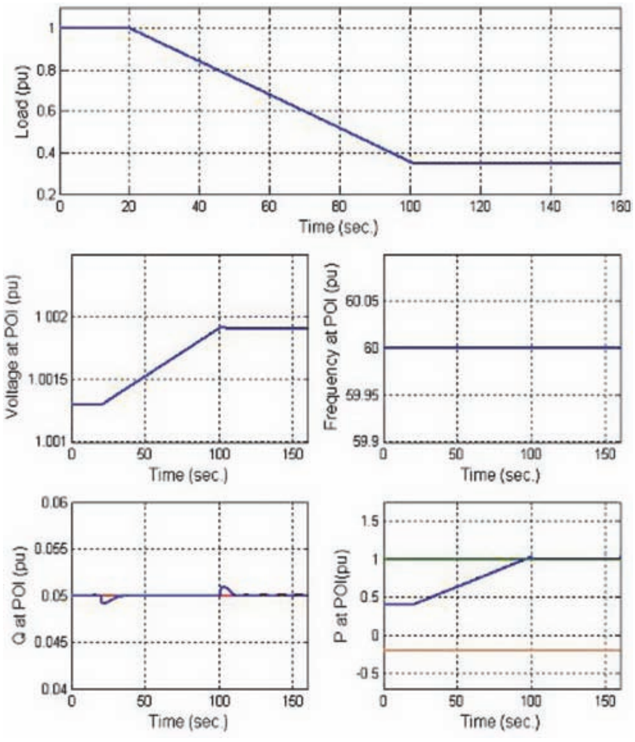


Figure 14.
Response to load change – Power Limit Control, no wind variation

The low load condition causes the power export to exceed a preset limit. As shown in the Figure, the violation triggers the M-APC, which controls the active power export so as not to exceed the limit by reducing the wind and hydro production.

Figure 15 shows the same test scenario with wind variation. The results show that meeting the power limit requirement with the fluctuation of the wind forces the hydro to be cycled more than 20%-30% of its capacity in a short time. This is not a desirable feature. An energy storage device may be able to take over some of the fluctuation and reduce the cycling of the hydro.

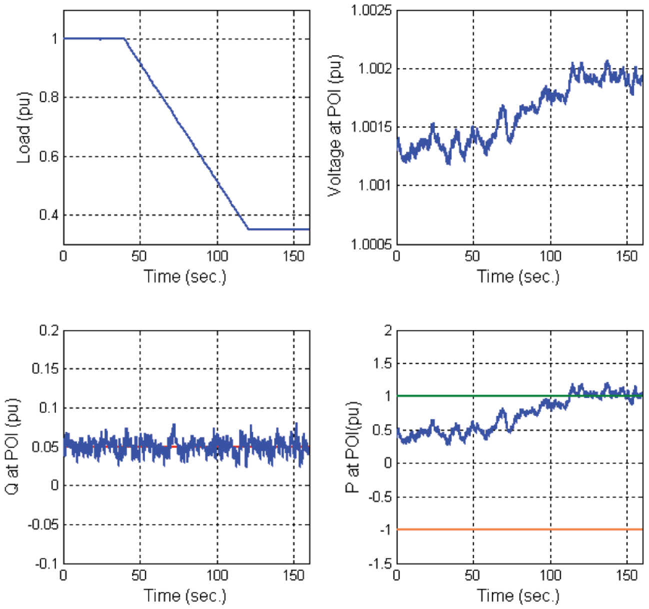


Figure 15.
Response to load change – Power Limit Control, wind variation

Another load change example has the load ramped down from an initial 19MW to 6MW at a rate of 0.2 MW/sec (Figure 16). A steady wind example is shown. This causes a violation of the active power 1-minute ramp rate limit (0.1 MW/sec).

As shown in Figure 16, the ramp rate of the active power at the POI is controlled to a slower rate of change when the ramp rate limit is exceeded. The ramp rate control of M-APC limits the ramp rate by adjusting the power from each generation source. The power reduction is dispatched among the wind and hydro assets.

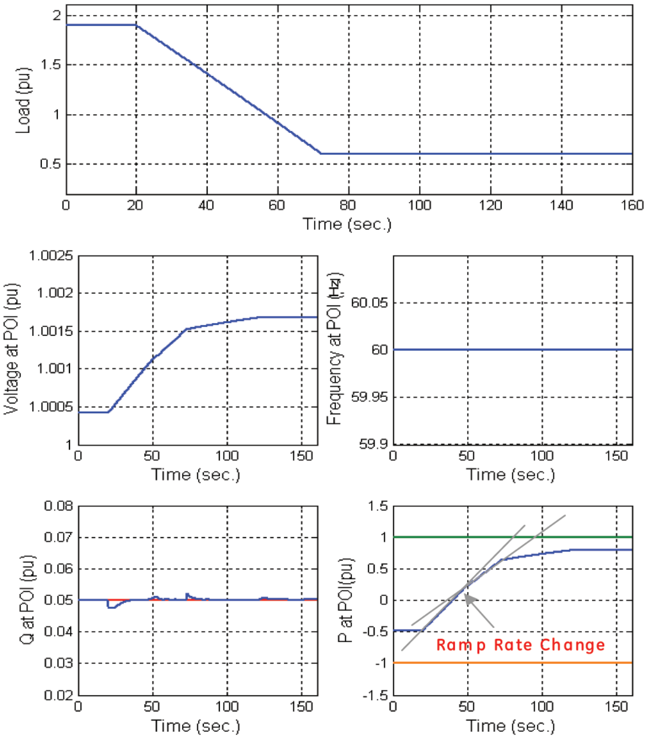


Figure 16.
Response to load change – Power Ramp Rate Control, no wind variation

5. Lab Demonstration

GE is working to identify a suitable centralized control hardware platform for Microgrid applications. Current lab testing employs a hardware-in-the-loop simulation of supervisory and tieline controls to validate their functionality. Figure 17 shows the layout for the laboratory setup. The setup includes four components:

- Single board computer (SBC) rack with QNX real-time operating system (RTOS), +/- 10V analog input and output cards.
- RT-LAB software coupled with generation and load asset models for the Microgrid.
- Supervisory controls developed using Simulink and linked with an OLE for Process Control (OPC) interface.
- GE Universal Relay (UR). The GE UR family [3] is a new generation of modular relays built on a common platform. The UR features high performance protection and communications.

RT-LAB software is used in conjunction with Simulink's Real-Time Workshop to compile the generation and load asset models into C code that can then be downloaded to the single board computer rack. These models consists of two generators and five loads that can be connected or disconnected to the system and a bus network that is connected to the grid. This model also includes drivers to interface with the digital-to-analog (D/A) and analog-to-digital (A/D) cards connected to the rack. The A/D card receives the active and reactive power commands for each generator from the UR as a voltage that is then scaled to the appropriate per unit value via a gain multiplier. The D/A card sends the scaled power and reactive power output of each generator, the reactive and active power at POI and the POI voltage and frequency to the UR.

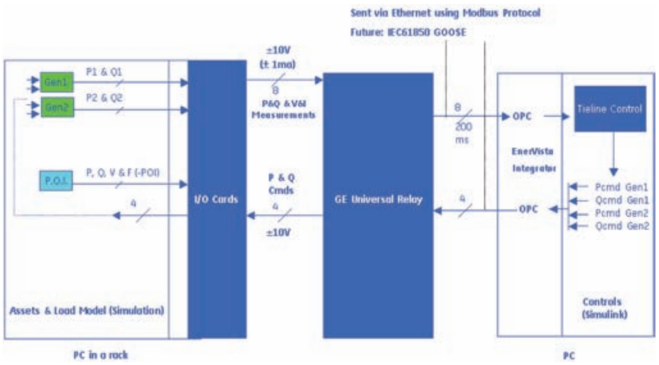


Figure 17.
Lab Setup Block Diagram

The UR is the hardware interface between the supervisory controls and generators. The analog measurements from the generators and POI are sent via Ethernet and IEC 61850 GOOSE/OPC to the supervisory controls in Simulink. The supervisory controls recalculate the active and reactive power commands for each generator based on the current state of the generators and the POI. The new commands are then sent to the UR where they are scaled to a voltage that represents the analog value of the commands. The voltage is sensed by the SBC rack's analog input card and the generators adjust their output accordingly.

Lab Testing Results

The lab test shown in this section utilizes the electrical model developed for the Municipal Campus Microgrid described earlier and represented by Figure 4. This test case examines the system response after disconnecting a load from the Microgrid. The maximum connected Microgrid load is equal to 770 kW. The goal of the test is to confirm the functionality of the supervisory controls after the controls and generators have been separated into separate subsystems that interface with analog and OPC signals. In the test, a 0.03pu load is disconnected from the Microgrid. The results of the test are shown in Figure 18.

The generator responds to the active power command and behaves as expected. The M-APC increases the power from the controllable generator (Gen1) to keep the active power at the POI within the defined limit. The power flow at the POI indicates that power is now exported to the grid after the load is disconnected.

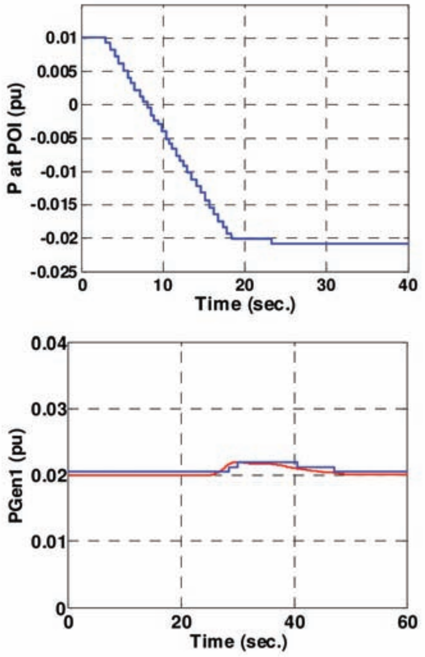


Figure 18.
Response to 30 kW load step change

6. Conclusions

This paper presents details on an important Microgrid control feature: tieline controls. These controls essentially coordinate the response of the several distributed energy resources within the Microgrid, such as generation, energy storage, or controllable loads, to make the response of the aggregate system at the point of interconnection to the grid resemble one single dispatchable entity. As such, the Microgrid can become a better citizen to the grid, managing its power exchange with the grid, and supporting voltage at the point of interconnection. One interesting benefit of this technology is that it can be designed to compensate for intermittency associated with renewable energy resources such as wind energy and solar energy, pushing the intermittency management burden inside the Microgrid, thereby potentially allowing for an increased penetration of these renewable energy resources. The dynamic response of the tieline control active and reactive power compensation elements were illustrated in several simulations, as well as in a hardware-in-the-loop simulation environment.

7. References

[1] Navigant Consulting Inc., "Final Report Microgrids Research Assessment for the US Department of Energy's Office of Electricity Delivery and Energy Reliability and the California Energy Commission's Public Interest Energy Research Program", May 2006.

[2] Nicholas W. Miller, Einar V. Larsen, and Jason M. MacDowell, "Advanced Control of Wind Turbine-Generators to Improve Power System Dynamic Performance", 11th International Conference on Harmonics and Quality of Power, 2004.

[3] Brochure for N60 Network Stability and Synchrophasor Measurement System: http://www.geindustrial.com/cwc

0314-v2

Security Aspects Of Communications To Substations

Mark Adamiak
GE Digital Energy, Multilin

Herb Falk
SISCO

1. Abstract

The security of data and information transmitted either point to point or through network access that utilizes an Internet or intranet infrastructure has recently become a major concern to all. The data communication industry, however, has been cognizant of the issues and has been quite active in determining the various "attack" modes and creating mechanisms to address potential weaknesses. In particular, the Internet has driven such innovations such as Secure Socket Layer (SSL), Internet Protocol Security (IPSec), and Virtual Private Network (VPN).

SSL encryption and authentication can be used between a remote site and the user's browser to ensure that the data is secure. SSL is used by the online banking industry to insure secure transfer of data & information. A hard token with a rolling password provides an extra measure of security for critical applications with control.

The VPN security appliance encrypts the data to create a "virtual tunnel" between the substation equipment and a specific company's PC. This technology is very useful for protecting serial data streams. Firewalls can be used to prevent external access to the data source.

This paper reviews the general issues of secure communications (including recently released NERC guidelines) and addresses the solutions to providing secure substation network connections on the Internet or an intranet. It will also review existing work in progress that deals with utility-to-utility and utility-to-substation communication security.

2. Introduction

The rapid migration of the digital society into the utility enterprise has resulted in the establishment of communication interfaces with most utility protection, control, and monitoring devices. This rapid and pervasive penetration of communications has raised many concerns as to the security and integrity of the data being communicated and the consequences of inadvertent access. The tools and general knowledge to potentially "attack" utility systems are readily available. The utility industry, to date, has been mostly immune from cyber attacks as most communications occur on private networks and through the "security through obscurity" principle, however, most utility security departments are demanding more security.

Over the past several years, several surveys and studies have been conducted in order to determine the communication and informational security concerns of the global utility industry. The results are primarily based on information provided by utilities located within the United States or from the United States Department of Energy. The Electric Power Research Institute (EPRI) has commissioned several such studies, and the major concerns prior to 911 are quite similar to the concerns for post 911. The top ten security concerns are:

1. Bypassing Controls

System flaws or security weaknesses that are intentionally attacked.

2. Integrity Violation

Information is created or modified by an unauthorized entity.

3. Authorization Violation

An entity authorized to use a system for one purpose that uses it for another unauthorized purpose.

4. Indiscretion

An authorized person discloses restricted information to a non-authorized entity.

5. Intercept/Alter

A communication packet is intercepted, modified, and then forwarded as if the modified packet were the original. This is a typical man-in-the-middle scenario.

6. Illegitimate Use

An action, control, or information retrieval is performed by an individual authorized for one action, but an action is completed for which the individual is not authorized.

7. Information Leakage

An unauthorized entity acquires restricted information. Typically this term is for non-eavesdropping acquisition of the information (e.g., through other means of disclosure).

8. Spoof/Masquerade

An attack against a communication dialog in which the attacker attempts to assume the identity of one of the communicating partners.

9. Denial of service (Availability)

Action(s) that prevent any part of an information system from functioning in accordance with its intended purpose. Usually flooding a system with messages to prevent it from servicing normal and legitimate requests. A PING attack, where the server is bombarded with requests for a simple echo command, can result in a denial of service.

10. Eavesdropping

An attack against the security of a communication in which the attacker attempts to "overhear" the communication – similar to wire tapping.

As with any type of attack, typically, a defense can be found to defeat the attack. Table 1 summarizes the security concerns discussed above and lists the defenses that are typically implemented to mitigate these concerns.

Concern Ranking	Concerns	
	Threat	Possible Counter-Measures
1	Bypassing Controls	Utility Policies, Strong Peer Authentication
2	Integrity Violation	Encryption, Message Authentication
3	Authorization Violation	Strong Peer Authentication, Privilege Levels
4	Indiscretion	Utility Policies
5	Intercept/Alter	Encryption, Message Authentication
6	Illegitimate Use	Utility Policies, Privilege Levels
7	Information Leakage	Encryption
8	Spoof/Masquerade	Strong Peer Authentication, Message Authentication
9	Availability (e.g. Denial of Service)	Appropriate Resource Management and fixing buffer issues.
10	Eavesdropping (e.g. Data Confidentiality)	Encryption

Table1.
Top ten utility communication and informational security concerns

Some details of these defenses are offered here:

3. Encryption

Encryption is the process of applying a "cipher" algorithm to input information, typically called "plaintext", that results in encrypted output data, typically called "ciphertext". The cipher algorithm scrambles the data based on a secret "key" that is exchanged between the communicating parties. There are numerous cipher implementations, however, the more common implementations are the Data Encryption Standard (DES), Triple DES or 3DES, and the Advanced Encryption Standard (AES). 3DES is quite well known due to its use in the Secure Sockets Layer protocol (see SSL description below). Basic DES uses a 56-bit key to encrypt the data. The basic encryption process is shown in Figure 1. The encryption process takes 8 bytes (64 bits) of data and splits it into two 32-bit pieces referred to al L0 and R0. The input 56-bit key is then broken into sixteen 48-bit keys.

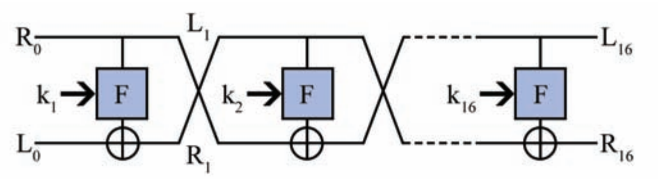


Figure 1.
Data Encryption Standard (DES) Implementation

The data (R0 and L0) and key 1 is fed into the input of the cipher. The R0 data is fed into the function F and is operated on by key k1. The output of F is exclusive ored with the L0 data. The out of this operation becomes L1 and R0 becomes R1. This process is then repeated 16 times – once with each of the 48-bit keys that had been created. The result of this process is the encrypted data. Note that in 3DES, this process is repeated three times with three different keys. Since available computer power makes a 56 key somewhat decipherable (it actually has been cracked), the usual implementation is a triple implementation of encryption known as 3DES which, to date, has not been cracked. In this implementation, the key is 168 bits long and the above process is repeated three times with the three different 56 bit keys.

4. Secret Keys

Similar to physical security, cyber security is implemented by placing a digital "lock" on the secured information. To open the lock, one must have the appropriate "key". The security key system is based on a series of linked public/private key pairs. In one type of encryption algorithm, data that has been encrypted with one's public key can only be decrypted with the paired private key and visa-versa. There are a number of algorithms for sharing public keys (you never share your private key) and for creating new shared secret keys. 3DES requires that each party know the same "secret" so the key exchange algorithm goes about securely creating a shared secret. Just to make things more difficult for attackers, new keys are typically re-negotiated every 1 to 3 minutes.

5. Authentication

Authentication is the security process that validates the identity of a communicating party. In the simplest implementation, this takes the form of a static password. Passwords can be easily compromised through indiscretion as discussed above and typically do not address "who" is entering the password. A variant of the static password is the rolling password as provided on a hard token. The hard token has a programmed sequence where the password changes every 1-minute. Many business enterprises use this technology for remote access to corporate networks.

Another variant of authentication is known as "strong authentication". In this implementation, authentication is provided by a "digital signature" which is an encrypted value provided by the entity requesting authentication that can only be decoded by the "public" key of the signature's owner.

6. Non-Repudiation

A security service that prevents a party from falsely denying that it was the source of data that is did indeed create.

7. Security Implementations

The above tools are typically integrated together at create a "total" security solution. The first of these solutions is known as a "Virtual Private Network" or VPN. VPN creates a secure "tunnel" between two networks (Figure 2). The tunnel is established through the use of the Internet Key Exchange to establish secret keys between the ends of the communication tunnel. Once the keys are established, data is encrypted at one end of the tunnel, sent through the tunnel in the network, decrypted at the receiving end of the tunnel and sent into the remote end network. For added security, keys between the ends are periodically re-negotiated (for example, every 3 minutes) to add greater security to the connection.

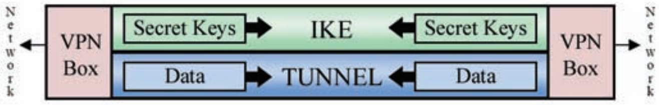


Figure 2.
VPN Tunnel

A second implementation that incorporates the above tools is known as Secure Sockets Layer (SSL 3.0)/ Transport Layer Security (TLS). These implementations are similar to VPN technologies in that the both use a key exchange and similar encryption technology to VPN. The primary difference is that SSL/TLS are implemented at the transport layer of the communication profile (Figure 3).

SSL/TLS Profile
Applications
Transport Layer Security (TLS)
Transmission Control Protocol
Internet Protocol
Transport (Ethernet)

VPN Profile
Tranmission Control Protocol
Internet Protocol Security (IPSec)
Transport (Ethernet)

Figure 3.
TLS and VPN Communication Profile Comparison

A third technology often employed for security is the firewall. As the name implies, a firewall is a go/no-go portal through with all data must pass in order to enter or exit a network. There are three basic techniques used to filter data through a firewall, namely, packer filtering, application gateway, and a stateful inspection.

A packet filter is the simplest form of firewall. A packet filter firewall will compare any IP packet that attempts to traverse the firewall against its Access Control List (ACL). If the packet is allowed, it is sent through. If not, the packet filter can either silently drop the packet (DENY) or send back an error response indicating "REJECT". Packet filters only look at five things: the source and destination IP addresses, the source and destination ports, and the protocol (UDP, TCP, and so on). These tests are very fast because each packet contains all the data (in the packet headers) necessary to make its determination. Due to its simplicity and speed, a packet filter can be enabled on your routers, eliminating the need for a dedicated firewall.

One problem with packet filters is that they generally do not look deeply enough into the packet to have any idea what is actually being sent in the packet. Though you might have configured a packet filter to allow inbound access to port 25, the Simple Mail Transfer Protocol (SMTP) port, a packet filter would never know if some other protocol was used on that port. For example, a user on one system might run his Secure Shell (SSH – another secure communication protocol) application on that port, knowing that the traffic would be allowed by the packet filter, and would be able to communicate through the firewall against policy.

A second and more thorough filter is an application gateway. An application gateway goes one step beyond a packet filter. Instead of simply checking the IP parameters, it actually looks at the application layer data. Individual application gateways are often called proxies, such as an SMTP (Simple Mail Transport Protocol) proxy that understands the SMTP protocol. These proxies inspect the data that is being sent and verify that the specified protocol is being used correctly. Given the creation of an SMTP application gateway, the proxy would need to keep track of the state of the connection: Has the client sent a HELO/ELHO request? Has it sent a MAIL FROM before attempting to send a DATA request? As long as the protocol is obeyed, the proxy will shuttle the commands from the client to the server.

Since application gateway must understand the protocol and process both sides of the conversation, it is a much more CPU-intensive process than a simple packet filter. However, this also lends itself to a greater element of security. You will not be able to run the previously described SSH-over-port-25 trick when an application gateway is in the way because it will realize that SMTP is not in use. Additionally, because an application gateway understands the protocols in use, it is able to support tricky protocols such as FTP that create random data channels for each file transfer. As it reads the FTP command channel, it will see (and rewrite, if necessary) the data channel declaration and allow the specified port to traverse the firewall only until the data transfer is complete.

Often there is a protocol that is not directly understood by your application gateway but that must be allowed to traverse the firewall. SSH (Secure Shell) and HTTPS (Hyper Text Transfer Protocol Secure) are two simple examples. Because they are encrypted end to end, an application gateway cannot read the traffic actually being sent. In these cases, there is usually a way to configure your firewall to allow the appropriate packets to be sent without interference by the firewall. This configuration is often called a plug.

The third filter technique often employed in firewalls is called stateful inspection. Stateful inspection firewalls are a middle ground between application gateways and packet filters. Rather than truly reading the whole dialog between client and server, a stateful inspection firewall will read only the amount necessary to determine how it should behave.

8. Industry Efforts

The International Electotechnical Commission (IEC) Technical Committee (TC) 57 Working Group (WG) 15 (e.g. IEC TC57 WG15) was formed to address security concerns for communication protocols for which IEC TC57 was the standards forming and maintenance body. The EPRI report was submitted to WG15 as base research for use in the evaluation, in additional to the NIST Common Criteria (ISO/IEC 15408), of the security issues regarding the Inter Control Center Protocol ICCP/IEC 60870-6-TASE.2, IEC 60870-5 (and its sibling DNP), UCA/IEC 61850, and DMS/IEC 61134, and others.

WG15 was tasked with analyzing the threats, potential risks, and to recommend security work item proposals, as required, to secure the TC57 protocols. Additionally, WG15 represents the core competency for security of TC57 and is to assist in the creation of the security mechanisms for the relevant protocols.

WG15 began its task prior to 911. It determined that the highest risk protocol was ICCP/IEC 80870-6-TASE.2 since it is wide scale deployment for 60-80% of utility control centers within the United States and the percentage of deployment worldwide is increasing dramatically. Additionally, the ICCP/TASE.2 protocol is used to convey control, generation schedules, and financially sensitive SCADA information. These factors, plus the perception of control centers being exposed to cyber attacks made the securing of ICCP/TASE.2 the highest WG15 work priority.

It is worthwhile to note that several of the countermeasures listed in Table 1 involve the utility developing appropriate policies and software/equipment vendors implementing appropriate access privilege levels. These issues are clearly outside the scope of WG15, however, this does not minimize their importance. Part of the scope of WG15 was to determine recommended security communication topologies and how to achieve Strong Peer Authentication, Encryption, and Message Authentication across those topologies. Another dimension to the TASE.2 work was knowledge that UCA/IEC 61850 and DMS/IEC 61134 specified similar protocols for use (being ISO 9506/MMS or a derivative). Therefore, one of the design objectives of WG15 became to develop common security specifications for these three protocols when possible. Such work would allow securing of communications between control centers, control centers to meters, control centers to substations, and internally to a substation.

The communication topologies addressed were the use of microwave, frame relay, internet, dial-up, and other wireless media (including satellite). In general, the use of well understood security technologies was found desirable. The OSI Reference Model clearly indicates that encryption is a Presentation function (e.g. transforms local representation into encrypted information) and is not an Application Protocol function. However, Strong Peer Authentication can only be accomplished at the Application level. Additionally, Message Authentication needs to be accomplished at the Transport or Network layer (Figure 4).

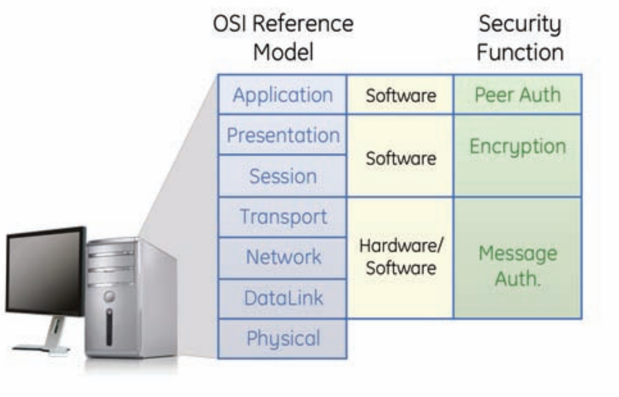


Figure 4.
Possible Security Solutions

Both TASE.2 and UCA/61850 make use of standard networking technologies (e.g. TCP/IP) and therefore there are potential hardware (e.g. VPN and Firewall) solutions that can provide Encryption and Message Authentication functions. However, there are software solutions that can also provide this capability. WG15 recommended a solution that allowed combination of hardware/ software solutions to exist in order to accommodate different trust levels (e.g. Internet vs. Intranet). In this regard, WG15 has recommended that TASE.2 be secured through the use of SSL/TLS (Transport Layer Software) that provides encryption and message authentication. Additionally, WG15 has recommended that backward compatibility with non-secure implementations needs to be provided (e.g. no SSL/TLS) and that the use of SSL/TLS needs to be a configuration issue. These recommendations result in the following capabilities at the transport level:

- The ability to use VPN/Firewall technology to provide secure tunnels between implementations that are not using SSL/TLS and thereby providing a "secure" environment for non-secure TASE.2/61850 transport connections.
- The ability to use VPN/Firewall technology in conjunction with "secure" TASE.2/61850 transport connections (e.g. SSL/ TLS).
- The ability to use the "secure" TASE.2/61850 transport connection solely.

These combinations allow maximum deployment flexibility by a utility so that issues of cost and performance may be addressed as appropriate.

The graph in Figure 5 attempts to illustrate that the probability of a successful attack increases with time if security methods are not changed. In the case of encryption, the longer a single key/ algorithm is in use, the higher the likelihood that the encryption will be cracked.

Therefore, WG15 has recommended a minimum key re-negotiation period based upon time and number of packets, whichever occurs first. This mechanism is specified as part of a "secure-profile". This capability may not be available in all VPN/Firewall implementations.

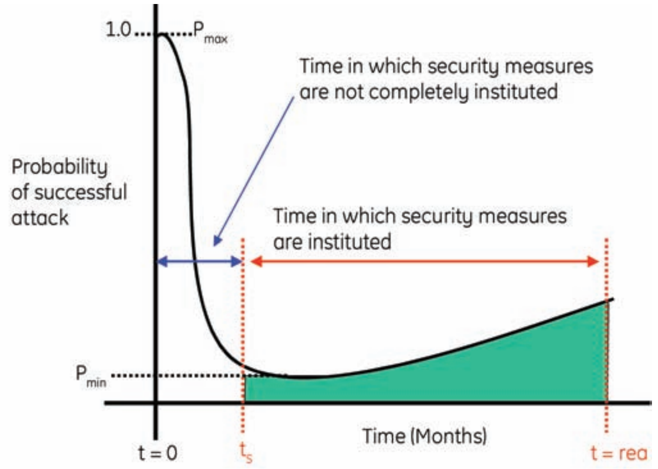


Figure 5.

WG15 has also rejected certain SSL/TLS supported cipher suites since the suites do not offer what is perceived to be enough protection. Additionally, it has mandated a set of cipher suites that must be supported thereby allowing interoperability to be achieved. One of the cipher suites that is mandated is AES, thereby allowing some performance concerns to be addressed.

The Strong Peer Authentication, recommended by WG15, supports the use of certificates and username/passwords. Both formats are digitally signed and sealed so that a replay of the connection sequence will not result in a connection.

WG15 has recommended that the end application (e.g. TASE.2/61850) must allow for the configuration of multiple combinations of incoming connections:

- NON SECURE: Neither transport encryption or application authentication is to be used. This provides backward compatibility and would need to be used over a VPN if any security is desired.
- AUTHENTICATED: Only application authentication is to be used.
- SECURE: Both transport and Application level security is to be used.

The current status of the WG15 work is that IEC TC57 WG07 (the group responsible for TASE.2) is in the process of evaluating the recommendations to become a Technical Report specifying how to secure TASE.2. It is expected that this decision will be positive since three vendors are already implementing the recommendations and since WG07 comments have already been addressed in the current recommendations. In addition to the WG07 recommendations, WG15 has created a similar work item to address the similar issues and solutions for UCA/61850.

9. Securing Remote Access to Electronic Control and Protection Systems

In January of 2003, the North American Electric Reliability Council released a draft guideline for securing access to Electronic Control and Protection Systems (ECPS). The guideline is aimed at communications to electronic relays, substation automation and control systems, power plant control systems, energy management systems, SCADA, and Programmable Logic Controllers where the remote connection is anything other than a direct connection. A summary of the guidelines are as follows:

1. Establish policies and procedures governing the use of remote access to ECPS systems including identifying responsible parties. Periodic review and updates should be schedules.
2. Remote Access should only be enabled when required, approved, and authenticated.
3. Multi-factor authentication (2 or more factors) should be used. Factors include passwords, phone numbers, IP addresses, biometrics, GPS location, etc.
4. Automatically lock account access after a preset number of consecutive invalid password attempts.
5. Encryption should be used when traversing unsecured networks.
6. Approved Remote Access authorization lists should be established and periodically reviewed.
7. DO NOT use default passwords. Use meaningful but non-descriptive passwords.
8. All remote access hardware and software should be approved and installed per policy.
9. Remote access connections should be logged (and periodically reviewed).
10. Consider the risk to the process when allowing remote access.

10. Security Architectures

Given the above tools and security guidelines, there are several security architectures that can be developed. Two of these are suggested below.

First, there is the architecture where a secure VPN tunnel is created from the utility headquarters network into the substation network (Figure 6). This architecture implements a single secure point of entrance into the substation and does not burden the existing hardware with encryption/decryption overhead. The drawback to this implementation is that there are still authorization issues to address. This could partially be addressed through the addition of a firewall in series with the VPN tunnel. The firewall would only allow authorized computers to pass requests through the firewall. Ultimately, the IED will need to provide authentication of a user.

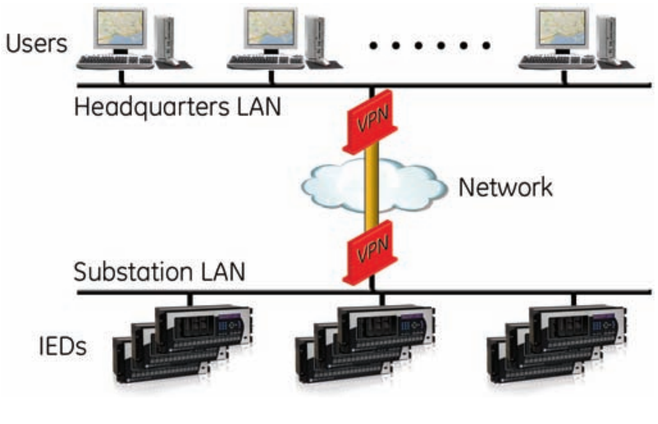


Figure 6.
Secure Substation Architecture via VPN

The second architecture, which results from the IEC WG15 recommendations, is an SSL/TLS based solution. In this implementation, TLS/SSL is inserted as the presentation layer of the client-server protocols. In the case of a UCA implementation, the resulting protocol profile is shown in Figure 7.

Standardization of such architectures will be required in the future in order to facilitate inter-operability. Work is underway to develop such an Integrated Energy and Communications System Architecture (IECSA) that will detail implementations from the energy traders to the thermostat (see reference 6).

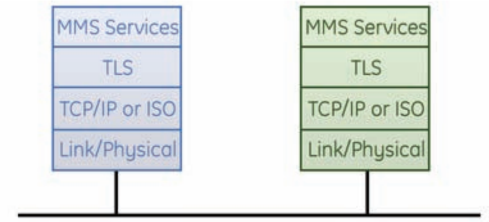


Figure 7.
Secure Communications Architecture between UCA Based Client and Server

11. Conclusions

Security in all forms is becoming a requirement in our society. Communication security concerns have been identified by EPRI, NERC and others and can be addressed with available software and procedures. The industry has responded with recommendations of application of TLS/SSL and VPN in the utility communication infrastructure. Although these software solutions are strong and effective security tools, they are only part of the total equation. True security requires many such tools and a comprehensive plan to employ them.

12. References

[1]. SSL and TLS Essentials – Securing the Web, Stephen A. Thomas, Wiley Computer Publishing, 2000.

[2]. VPN Fundamentals, Chuck Semeria, Juniper Networks, Sunnyvale, CA., Part # 200012-001 3/01.

[3]. Security Guidelines for the Electricity Sector; Securing Access to Electronic Control and Protection Systems, North American Electric Reliability Council; version .3, January 15, 2003.

[4]. ICCP (TASE.2) Security Enhancements Volume 1, EPRI, Palo Alto, CA, 2002. 1001642.

[5]. 3DES and Encryption, Kenneth Castelino; http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html

[6]. Integrated Energy and Communications System Architecture; www.IECSA.org

Test CT's and PT's

INSTRUMENT TRANSFORMER TEST SYSTEMS

FEATURES:

- Test CT's and PT's at High Accuracy for all IEC and ANSI classes
- Easy to Use, High Speed Fully Automatic
- Prints RCF and Phase Data
- Stores Test Programs for Easy Recall
- All Solid State
- Low Cost

"The world's best test systems"

Model CT-4000 for Current Transformers

Model PT-3000 for Potential Transformers

Model CTPT for CT's and PT's

CALL FOR LITERATURE
OR DEMONSTRATION

OPTIMIZED DEVICES, INC.

220 Marble Ave. Pleasantville, New York 10570
Phone: 914-769-6100 Fax: 914-769-6102 Email: sales@optdev.com

Practical Considerations for Security

Steven Hodder
GE Digital Energy, Multilin

1. Introduction

This paper has been prepared to outline some practical security strategies for protection & control engineers that can be adopted quickly and considerations when designing and implementing communications access to protection and control systems. The intention of this paper is not to provide a detailed explanation of NERC Critical Infrastructure Protection (CIP) standards, as this is discussed in several already-published works. Nor is the intent to provide a detailed treatise on the finer details in configuring the various facets of network security.

2. Drivers for Cyber Security

A number of world events in recent years has put critical infrastructure in the spotlight, and highlighted the need to adequately protect these systems from intentional and accidental interruption.

- The attacks on September 11th, 2001 changed the way North Americans viewed terrorism – the world became a very scary, dangerous place. A great deal of concern arose over the safety of key infrastructure in North America, including gas pipelines, transportation, water and electricity against similar terrorist attacks.
- The August 14th, 2003 Northeast blackout, along with several other high-profile outages, heightened awareness of the importance of the bulk electrical system, and provided a powerful illustration of the financial and societal impacts of a large-scale interruption of the electrical infrastructure.

The increased public and governmental concern over the safety, security and availability of critical infrastructure lead to the creation of a number of regulations regarding the identification, prioritization and protection of critical infrastructure .

3. What's all this "CIP" Stuff, Anyhow?

The North American Electric Reliability Corporation (NERC) has developed eight Critical Infrastructure Protection (CIP) standards (CIP-002 to CIP-009), covering the identification, protection, management, incident reporting and recovery for critical electronic systems for the bulk electrical system.

CIP-002	Critical Cyber Assets	Identification & enumeration of Critical Cyber Assets
CIP-003	Security Management Controls	Development of cyber security policy (incl. Auditing)
CIP-004	Personnel & Training	Background checks, regular training on security policy
CIP-005	Electronic Security	Electronic Security Perimeter & Access Controls
CIP-006	Physical Security	Physical Security Perimeter & Access Controls
CIP-007	Systems Security Management	Controls to Detect/Deter/Prevent Compromise
CIP-008	Incident Reporting	Incident Identification, Classification & Reporting
CIP-009	Recovery Plans	Restoration of Critical Cyber Assets once compromised

It is important to note that all of the above NERC standards are procedural in nature – they describe the 'What' and the 'Why', but they do not, other than in general terms, describe the 'How'. The end result is often

4. Cyber Security: Exactly What is it?

According to NERC CIP standards, so-called Critical Cyber Assets (CCAs) are defined as:

Critical Cyber Assets: any programmable electronic devices or communication networks that if damaged or otherwise made unavailable may impact the safe and reliable operation of the associated bulk electricity system.

The impact of this definition is fairly far-reaching in the world of Protection & Control. Effectively, this definition applies to protective relays and RTUs, local and remote HMI computers, and the communications infrastructure that connects them where remote access using routable protocols is used. The communications networks involved may include (but of course, not be limited to) local so-called Station Bus LANs as well as IEC 61850 Process Bus LANs where actively switched networks are involved.

So what exactly does this mean to the average Protection & Control engineer? What has changed to make the handling of P&C systems different from what was historically done? The principle answer to this question is simple: access.

Historically, electromechanical and static relays did not offer any digital communications interfaces and consequently there were no means to access and modify these devices remotely. Any changes, including removing protection from service, required staff to be physically present within the station, standing directly in front of the device(s) involved. There was no operational (i.e. real-time values) or non-operational (i.e. historical, SOE, fault record) data within the protection devices so there was no driver to communicate with these relays.

With the introduction of digital relays, particularly more modern micro-processor based relays, there is an ever-increasing demand to provide communications access to these devices. Modern digital relays can provide real-time values and control for SCADA applications, non-operational data for fault and system disturbance analysis and the ability to interrogate (and potentially change) settings remotely via advanced communications protocols and interfaces. Therein lies the issue – remote access, if incorrectly provisioned and secured, may present a channel for malicious or unintentional disruptions to be caused on the power system.

Let us consider a very simple system as shown in Figure 1.

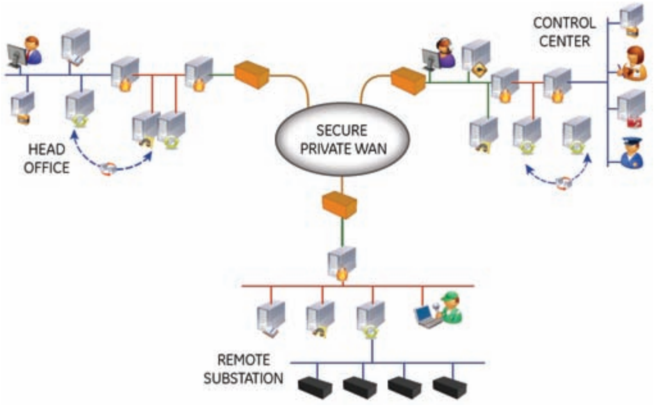


Figure 1.
Simple system with remote access

Here we have a single substation being accessed remotely from two separate locations: a Head Office location and a Control/ Operating center. Each location has different users each with different user requirements. Access is provided via a secure private LAN (such as SONET or VPN).

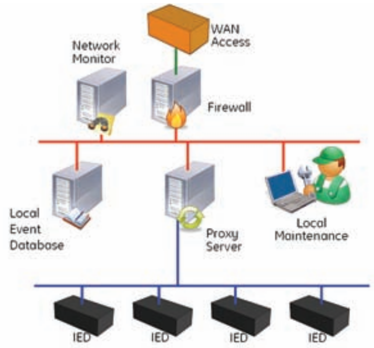


Figure 2.
Remote Substation

The Remote Substation consists of the following functions:

- A single point of access to the outside world (WAN Access), providing connections to external users. This WAN access may be channels within a SONET multiplexer or a VPN connection to an external network.
- A Firewall function that provides additional filtering of traffic between the external world and the secure network within the station.
- A Network Traffic Monitor, that examines network traffic generated locally and entering from the external network
- A Proxy Server, that mirrors the data generated and functions provided by the IEDs to the outside world to external users.
- A Local Event Server that automatically gathers events from all of the devices within the network, including relays and the Network Monitor, stores them locally and also provides for automated transfer to centralized event databases.

While these functions are shown as individual functions, often several may be merged into a single network appliance. For example, VPN access, firewall functions and network traffic monitoring may be involved into a single network appliance. Similarly, the event log and proxy server may be merged into a single device on the network.

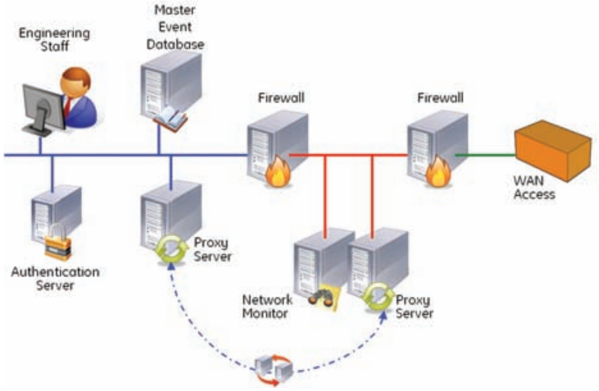


Figure 3.
Head Office

The Head Office system shares several functions with the Remote Substation, and adds several new functions.

- Two firewalls are set-up back-to-back, creating a specialized network known as a Demilitarized Zone (DMZ). This architecture is extremely common in the IT world where access is provided to common resources for both internal/ secure and external/insecure networks.
- Two proxy servers are provided, one within the DMZ and one residing on the office network. Data is mirrored on the proxy residing on the office network from the proxy residing in the DMZ and users on the office network access data on the local office network proxy only. Similarly, data is mirrored onto a Centralized Event Database for user access.
- The process of data mirroring is provided completely autonomously between the proxy servers (both at head office and at remote substations) with no human access required using Machine-to-Machine (M2M) transfer.

- A network monitor is provided within the DMZ to detect unauthorized traffic. If unexpected traffic on the DMZ is detected, then alarms/logs are generated. In general the only expected traffic on the DMZ will be:
  - M2M data coming from remote proxy servers destined for the DMZ proxy via the External Network firewall.
  - M2M data coming from DMZ proxy server destined for the office proxy and central event database via the Internal Network firewall.
  - Administrative traffic on the DMZ for configuration & monitoring of the network resources including the traffic monitor.
- A centralized Authentication Server allows users to prove their identity against the centralized user management database in order to gain access to the proxy and centralized event database.

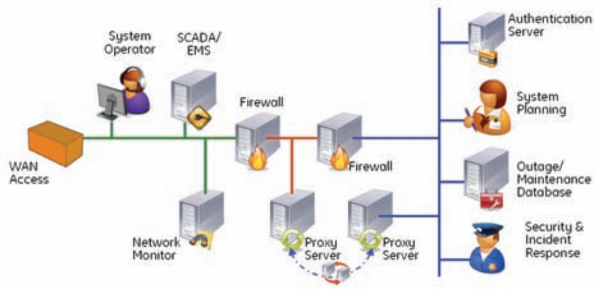


Figure 4.
Control Center

Finally, the control center again shares several functions with the Remote Substation and Head Office systems, with some new additions.

- The Primary Energy Management System (EMS) or SCADA system is provided in a dedicated, secured network connected to the secure WAN.
- Security and Incident Response, acting on incidents detected by the various network monitoring systems to detect and remediate unauthorized network access.

5. Cyber Security: Zones of Protection

Perhaps the best way to introduce cyber security is to provide an analogy to concepts that P&C engineers are already familiar with: zones of protection. In the power system, we provision protection for primary power system apparatus in zones encircling each power system element we wish to protect. Each zone is typically bound by measurement devices (current transformers) and there are isolators (circuit breakers) within the zone, typically just inside the measurement devices, to disconnect the primary apparatus from the rest of the power system in the event of a fault. So far, so good – but how does this relate to cyber security?

An analogy can be drawn between power system protection and the provisioning of zones of protection, and network system protection.

6. Defence-In-Depth

In the realm of cyber security, it is often common to refer to the concept of Defence-in-Depth, and perhaps the best way to describe this concept is to relate it back to the previous discussion on zones of protection.

We have within each network monitoring functions that monitor the flow of data from one system or device to another. These network monitors detect unusual network traffic patterns and generate signals in the event of illicit network access. These monitoring functions are often referred to as Intrusion Detection Systems (IDS) and are analogous to instrument transformers and protective relaying used to detect abnormal power system conditions.

The next step in the protection is to isolate devices or networks that are generating the illicit traffic based on signals from the IDS. The actions taken may include throttling down or turning off network ports, blocking access from specific addresses or forcing a reconfiguration of certain network resources to “hide” from external parties. These functions are commonly referred to as Intrusion Prevention Systems (IPS) and are analogous to the isolators (circuit breakers) in the power system used to isolate faulted portions of the power system to protect the remaining system.

If we take our overall simplified system shown in Figure 1, then consider the “zones of protection” shown in the following figures, beginning with the Remote Substation. There are a number of individual zones of protection for each location.

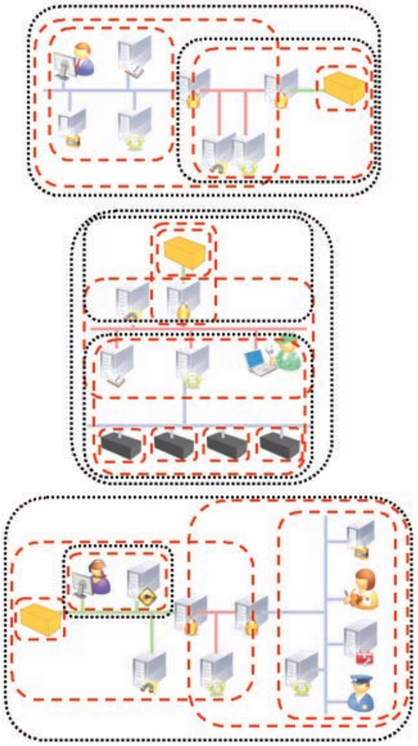


Figure 5.
Electronic Security Perimeters

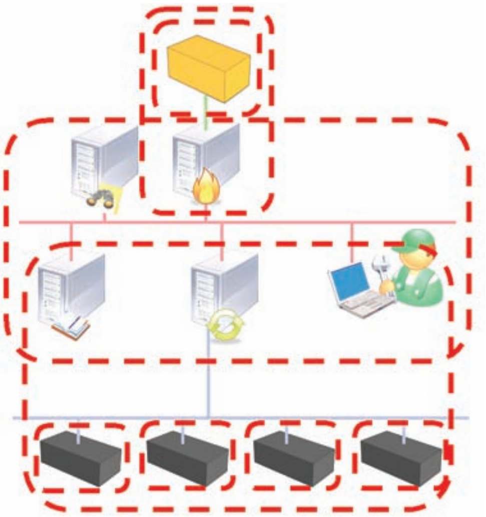


Figure 6.
Remote Substations ESPs

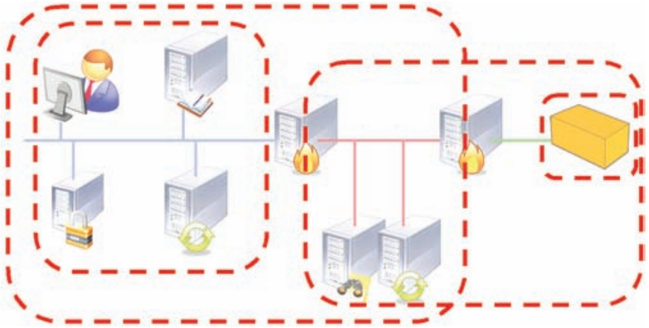


Figure 7.
Head Office ESPs

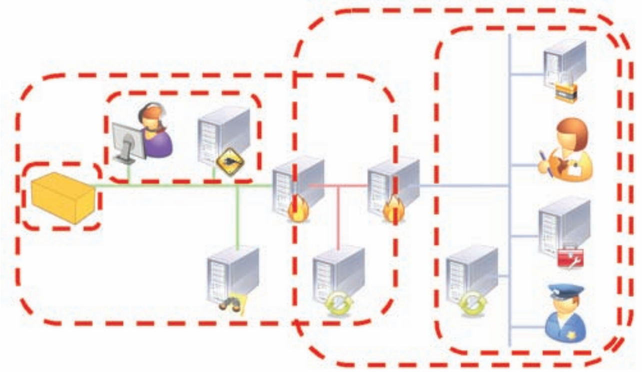


Figure 8.
Control Center ESPs

In each case, the system has overlapping "zones of electronic security", bounded by so-called Electronic Security Perimeters (ESPs). The concept of Defence-in-Depth refers to architectures that overlay several zones of protection. As can be seen, the overlapping of ESPs is very similar to the concept of overlapping zones of protection in protective relaying.

This Defence-in-Depth is an extremely key concept. Much like protective relaying, where occasionally blind spots exist, there are situations where complete security can not be provided within a single given device – however this does not mean that the device itself is unusable because it is insecure. It simply means that the electronic security "blind-spot" must be addressed by a higher-order network system.

In reality, it is advantageous in critical P&C systems to provide a significant portion of the security functionality in higher order network systems. Once commissioned, it is often impractical or risky to make changes to the in-service protective relaying. However, security is a very organic process that is constantly evolving. Users are frequently added or removed as staffing changes. New vulnerabilities are identified daily and fixes to address these vulnerabilities are released as frequently. Rather than making these continuous changes to critical P&C systems, these changes are made to higher order systems leaving P&C devices alone to perform their purpose.

7. Final Thoughts and Comments

This paper has presented some high-level concepts and discussions on the concepts of security in the context of P&C systems. It is not intended to be prescriptive to users, but rather raise issues for consideration and discussion when developing and providing security to comply with NERC CIP requirements.

Some final thoughts for consideration on the topic of security:

- The single largest threat to electricity infrastructure will likely be a direct physical attack on key generation and transmission assets. These assets are prime targets because:
    - They are large, easily identifiable targets that are typically located in remote areas (NIMBY principle) and in general, transmission stations are largely unmanned and poorly monitored (if monitored at all). This makes them ideal low-risk targets for malicious physical attacks.
    - The destruction and loss of key transmission infrastructure has an immediate and long-lasting impact on the bulk power system. Even if the fleet of generation remains completely in tact, insufficient transmission capacity will bottleneck or strand this generation capacity rendering it partially or completely unusable. Generation requires transmission infrastructure; electricity cannot be sent via courier.
    - Large power apparatus have extremely long lead times with very few vendors globally. This, coupled with the lack of common industry-wide specifications for key transmission assets like power transformers means there is a limited set of universal spares so that a physical attack will have an immediate, and long-lasting effect, on the power system.

- Secure remote access and security at the network layer is a well-understood issue within the general telecommunications industry at large. There exist a number of broadly accepted and thoroughly tested technology solutions for secure remote access, encryption, authentication, intrusion detection and prevention. Therefore, it is not advisable to "reinvent the wheel" when securing remote access, but rather judiciously apply existing best practices from the network communications industry.

- While adopting and implementing a solution, it is important to keep in mind the requirements of all users, not just one particular group. Different users will have different requirements and a security solution should not prevent legitimate users from having necessary access. Conversely, the business needs for remote access for each user group should be reviewed and justified – is direct remote access fundamentally required or can the data be provided by other means? Can data be mirrored securely to allow users to perform their necessary functions?

- To the maximum extent possible, critical protection, control and automation traffic should be carried over dedicated communication systems that are under direct administration of the controlling authority.

    - For example, within a generating station the control and automation network may be provisioned over a dedicated internal SONET network with user access only within the plant control room. While this may be an expensive option, it will also likely be the most secure method of providing access. In engineering, there is no such thing as a shortage, only a shortage at a price.

- Where connections between critical/secure and non-critical/less secure networks is made, multiple layers of security should be provided according to industry best practices.

    - De-Militarized Zones (DMZs)

    - Firewalls

    - Proxy Servers, including M2M (Machine-to-Machine) Proxies

- Advanced digital relays have a number of security features in the latest versions of firmware, including local and remote user passwords, remote user access supervision and security logging. It is recommended that users:

    - As part of CCA identification, include the specific version of relay firmware installed. Compare the firmware versions as-installed against the latest firmware version available, particularly with respect to new security features. Where needed, develop deployment plans to upgrade the firmware in those relays, starting with those CCAs that are designated as highly critical.

    - Enable and use existing security features within digital relays, particularly where these features have been disabled or left with default values:

        - Change passwords from defaults

        - Provide separate access passwords for local and remote access

        - Force the use of additional access controls for setting access

    - Provide routine auditing of changes to relay settings and commands executed through the relay. Where possible, invest in infrastructure to automate the collection, concatenation, reporting and archiving of security event data.

- Ensure that security-related alarms and events are communicated as part of a security monitoring system and included in the relay SOE record, and that the records for each relay SOE is downloaded automatically and mirrored in a central database to prevent loss of security event information.

    - Alarms should include excessive invalid password attempts made to the relay, local relay setting access granted, remote relay setting access granted.

        - Integrate alarms with outage and/or maintenance scheduling systems to detect if setting access is granted to a relay but no outage or work has been scheduled.

    - Develop expert algorithms to digest and analyze relay event data to look for patterns in events.

        - Crosschecking with maintenance scheduling and outage management systems/databases.

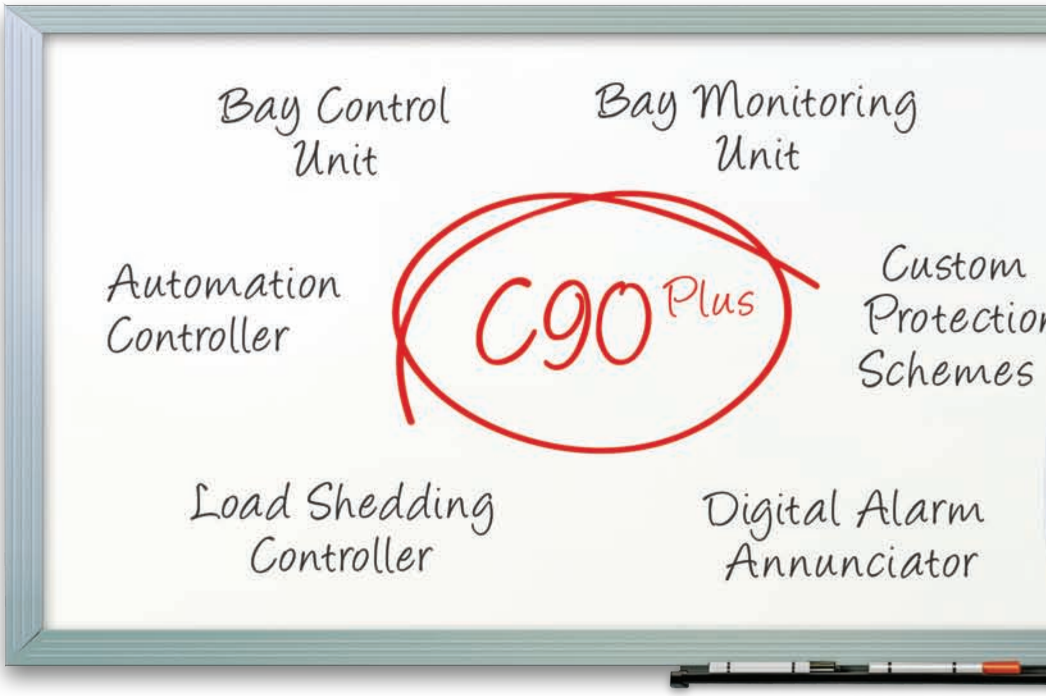
        - Crosschecking with standard network monitoring applications and logs (traffic pattern analysis, anomalous network traffic detection).

- There is no "magic bullet" for cyber security – security is as much an organizational/procedural activity as it is a single technology solution. The only way to provide true security is to implement Defence-in-Depth security.

8. References

[1] Homeland Security Presidential Directive/Hspd-7: Critical Infrastructure Identification, Prioiritization, and Protection.

[2] A Shortage of Engineers: A Novel. R. Grossbach. St. Martins Press 2001.


Bay Control Unit
Bay Monitoring Unit
Automation Controller
C90 Plus
Custom Protection Schemes
Load Shedding Controller
Digital Alarm Annunciator

Multilin C90Plus Controller

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, 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.**

1. Introduction

HIS 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.

2. 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.

3. 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 ofpassword 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".

4. 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.

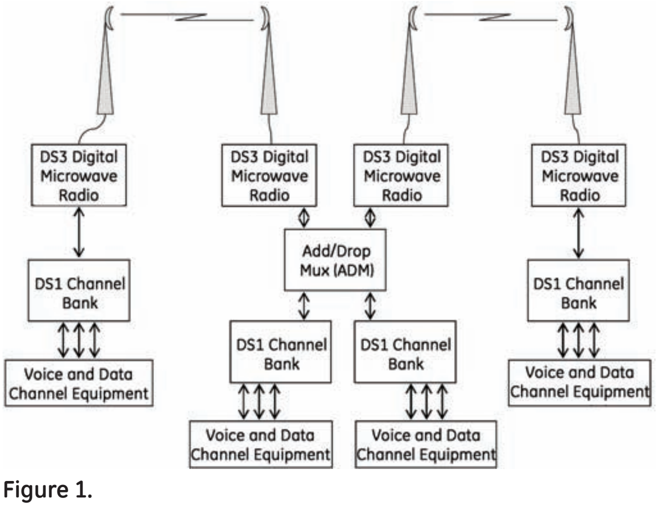

DS3 Digital Microwave Radio
DS3 Digital Microwave Radio
DS3 Digital Microwave Radio
DS3 Digital Microwave Radio
Add/Drop Mux (ADM)
DS1 Channel Bank
DS1 Channel Bank
DS1 Channel Bank
DS1 Channel Bank
Voice and Data Channel Equipment
Voice and Data Channel Equipment
Voice and Data Channel Equipment
Voice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

Figure 1.
Microwave Systems

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.

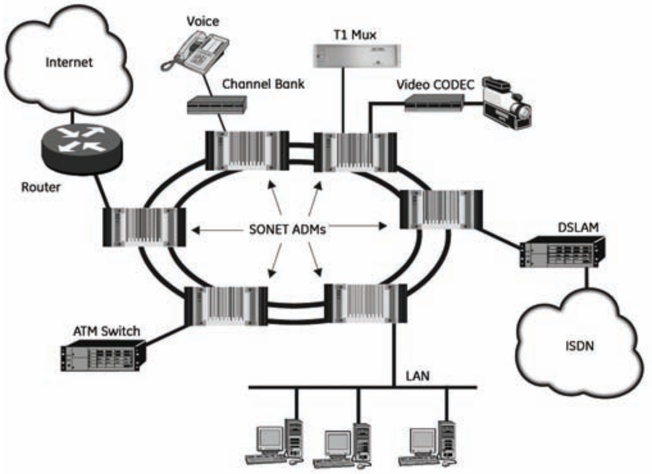


Figure 2.
Telecommunications Network

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.

5. 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.

6. 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 realtime 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.

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
Transient angle instability	Disrupt communications	No trip	Alter or delay transmitted date	False trip

Table 1.
Effect of attach on pilot relaying

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.

7. 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.

8. 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 backdoor 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)

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 2.
Software 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
Internet-related attacks	Take advantage of Internet service vulnerabilities

Table 3.
Network security 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 4.
System Administration 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 5.
Personal related 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

Table 6.
Miscellaneous and unusual vulnerabilities

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 endto-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-topeer 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.

9. 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 nondeterministic 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 (twoway) 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. Reauthentication 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.

10. 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.

11. 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:

  - 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.

12. 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.

13. 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 "usergroup- 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/inevitabs.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.

14. 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 reevaluation 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.

15. 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.

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.

Table 7.

16. 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–Appendix A

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:

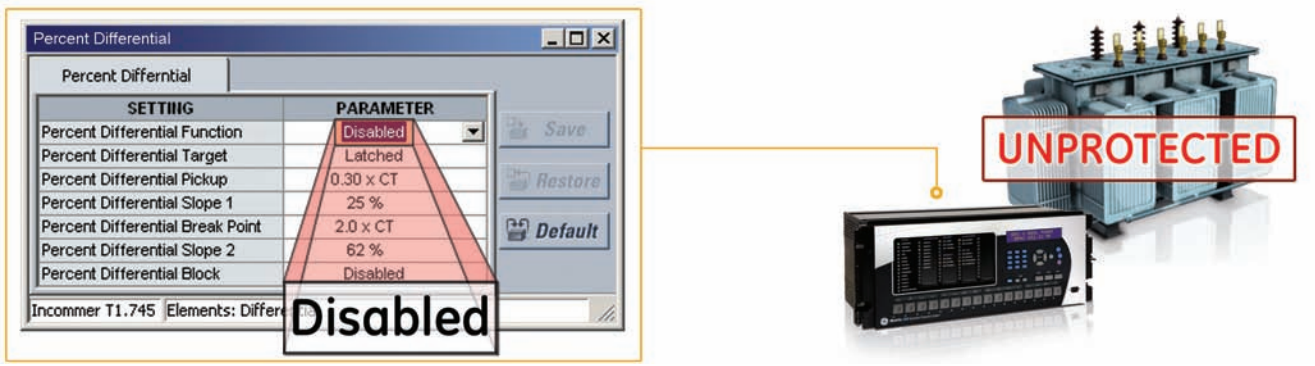
http://www.nsa.gov/selinux/inevit-abs.html)

[13] SE Linux software, documentation, and related publications are available for download from the NSA web site:

(http://www.nsa.gov/selinux/)

Engineering Quick Tip: Enhancing your Systems Security

With the proliferation of microprocessor-based protective relays with advanced communications capabilities, one area of growing concern is the security of protection and control systems. Often when security threats are discussed, conversation typically runs to people with intent to cause harm or interrupt processes. Overlooked are the actions of legitimate workers who have simply made mistakes during their work, even though the overall outcomes are the same.



Percent Differential

Percent Differntial

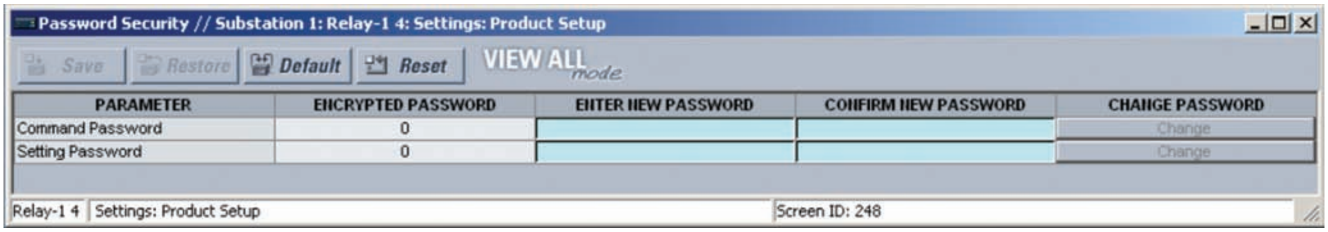
SETTING	PARAMETER
Percent Differential Function	Disabled
Percent Differential Target	Latched
Percent Differential Pickup	0.30 x CT
Percent Differential Slope 1	25 %
Percent Differential Break Point	2.0 x CT
Percent Differential Slope 2	62 %
Percent Differential Block	Disabled

Incommer T1.745 | Elements: Differ

Figure 1.
A simple settings change to disable a protective element can leave system equipment unprotected

There are a number of security features included in GE Multilin protection device that will help protect against intentional or inadvertent changes in device configuration.

Password Protection



Password Security // Substation 1: Relay-1 4: Settings: Product Setup

PARAMETER	ENCRYPTED PASSWORD	ENTER NEW PASSWORD	CONFIRM NEW PASSWORD	CHANGE PASSWORD
Command Password	0			Change
Setting Password	0			Change

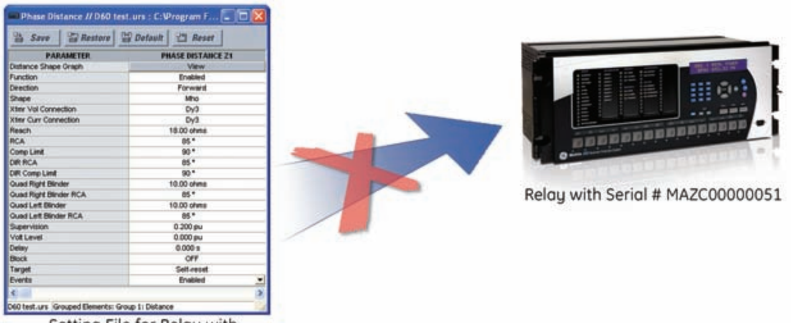
Relay-1 4 | Settings: Product Setup | Screen ID: 248

Password protection requires users to enter a password before they are allowed to perform a number of tasks, such as change a devices configuration, perform system commands, or clear historical information. Different levels of password security allows for flexibility in your security, with options such as local and remote passwords, as well as passwords for configuration changes and issuing system commands.

Serial Number Locking

The serial number locking function found in EnerVista Setup programs ensures that settings files can only be sent to a specific device. By locking a settings file to a specific device serial number, you are ensuring you never load protection settings into the wrong device.

In addition to the security features designed to avoid undesired configuration changes, GE Multilin EnerVista Setup and Viewpoint Maintenance software packages offer tools for identifying and tracking changes in device settings.



Phase Distance // D60 test.urs : C:\Program F...

PARAMETER	PHASE DISTANCE Z1
Distance Shape Graph	View
Function	Enabled
Direction	Forward
Shape	Mho
Xtmr Vol Connection	Dy3
Xtmr Curr Connection	Dy3
Reach	18.00 ohms
RCA	85 °
Comp Limit	90 °
DIR RCA	85 °
DIR Comp Limit	90 °
Quad Right Blinder	10.00 ohms
Quad Right Blinder RCA	85 °
Quad Left Blinder	10.00 ohms
Quad Left Blinder RCA	85 °
Supervision	0.200 pu
Volt Level	0.000 pu
Delay	0.000 s
Block	OFF
Target	Self-reset
Events	Enabled

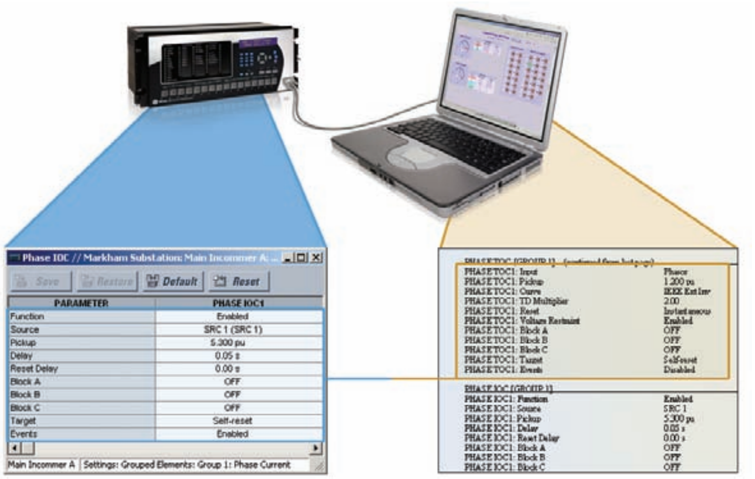
D60 test.urs | Grouped Elements: Group 1: Distance

Setting File for Relay with Serial # MAZC05000186

Relay with Serial # MAZC00000051

Compare Settings Files

GE Multilin's Enervista Setup programs allows you to compare the settings that are programmed in a relay with a file stored on your computer. This can be done while the relay is online and protecting the system, requiring no down time at all. When completed, a report will be generated outlining any settings in the relay which do not match the settings programmed in the file.



Phase IOC // Markham Substation: Main Incommer A: ...

PARAMETER	PHASE IOC1
Function	Enabled
Source	SRC 1 (SRC 1)
Pickup	5.300 pu
Delay	0.05 s
Reset Delay	0.00 s
Block A	OFF
Block B	OFF
Block C	OFF
Target	Self-reset
Events	Enabled

Main Incommer A | Settings: Grouped Elements: Group 1: Phase Current

PHASE TOC (GROUP 1) (continued from last page)

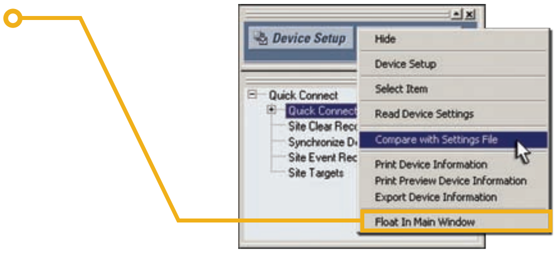
PHASE TOC1: Input	Phasor
PHASE TOC1: Pickup	1.200 pu
PHASE TOC1: Curve	IEEE Ext Inv
PHASE TOC1: TD Multiplier	2.00
PHASE TOC1: Reset	Instantaneous
PHASE TOC1: Voltage Restraint	Enabled
PHASE TOC1: Block A	OFF
PHASE TOC1: Block B	OFF
PHASE TOC1: Block C	OFF
PHASE TOC1: Target	Self-reset
PHASE TOC1: Events	Disabled

PHASE IOC (GROUP 1)

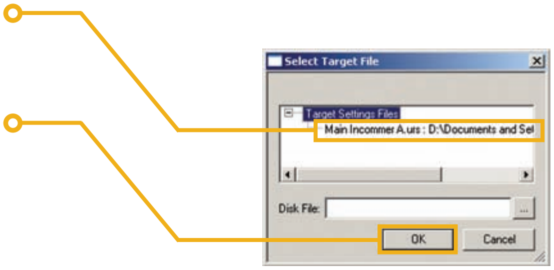
PHASE IOC1: Function	Enabled
PHASE IOC1: Source	SRC 1
PHASE IOC1: Pickup	5.300 pu
PHASE IOC1: Delay	0.05 s
PHASE IOC1: Reset Delay	0.00 s
PHASE IOC1: Block A	OFF
PHASE IOC1: Block B	OFF
PHASE IOC1: Block C	OFF

To perform a settings file comparison simply use the following procedure:

1. In the Online Window of the EnerVista setup program, Right Click on the name of the relay and select Compare Settings File



2. A window will open asking you to select which file you wish to use for the comparison. Select your file, and then OK.

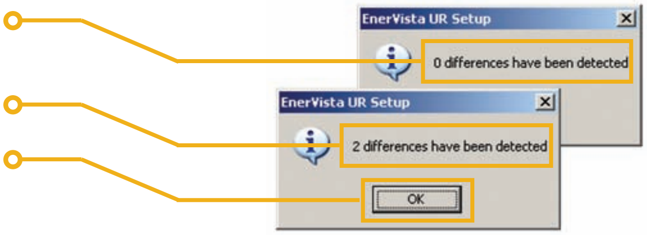


Select Target File

If the relay's programming matches all settings in the saved file, a message will be displayed indicating that no differences were found.

If the relay's programming does not match the settings in the saved file, a message will be displayed indicating the number of settings that are not the same.

Selecting OK will generate a report of all mismatched settings



EnerVista UR Setup

0 differences have been detected

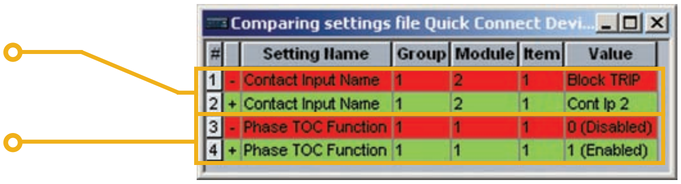
EnerVista UR Setup

2 differences have been detected

Setting Difference Examples

Example 1: Relay settings have Contact Input 2 named as Black TRIP. The settings files has the contact named Cont IP 2.

Example 2: Relay settings has the phase time Overcurrent (TOC) Disabled. The settings file has the TOC function Enabled



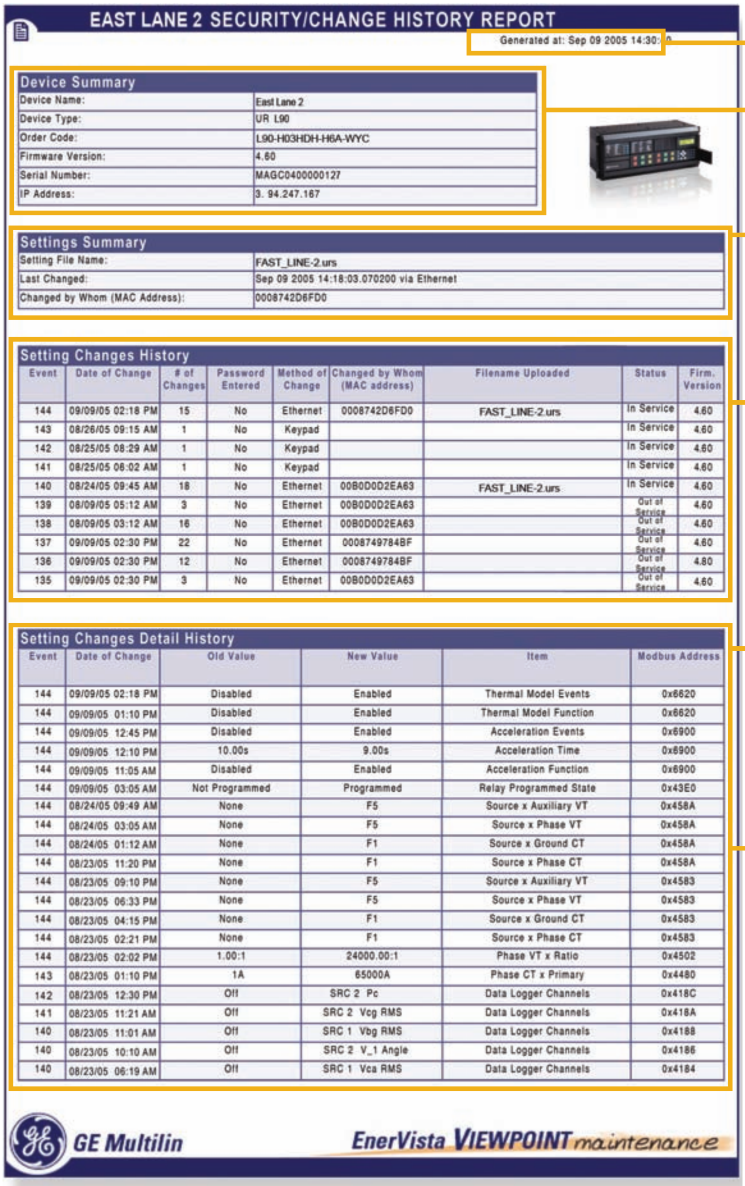
Comparing settings file Quick Connect Devi...

#		Setting Name	Group	Module	Item	Value
1	-	Contact Input Name	1	2	1	Block TRIP
2	+	Contact Input Name	1	2	1	Cont Ip 2
3	-	Phase TOC Function	1	1	1	0 (Disabled)
4	+	Phase TOC Function	1	1	1	1 (Enabled)

Settings Security Audit Trail

The *Viewpoint Maintenance* software package provides an easy to use Security Audit Trail. This report will outline when a device's settings were changed, who made the changes, as well as the specific settings and values which have been altered.

VIEWPOINT maintenance



EAST LANE 2 SECURITY/CHANGE HISTORY REPORT

Generated at: Sep 09 2005 14:30:[illegible]

Device Summary	
Device Name:	East Lane 2
Device Type:	UR L90
Order Code:	L90-H03HDH-H6A-WYC
Firmware Version:	4.60
Serial Number:	MAGC0400000127
IP Address:	3. 94.247.167

Settings Summary	
Setting File Name:	FAST_LINE-2.urs
Last Changed:	Sep 09 2005 14:18:03.070200 via Ethernet
Changed by Whom (MAC Address):	0008742D6FD0

Setting Changes History

Event	Date of Change	# of Changes	Password Entered	Method of Change	Changed by Whom (MAC address)	Filename Uploaded	Status	Firm. Version
144	09/09/05 02:18 PM	15	No	Ethernet	0008742D6FD0	FAST_LINE-2.urs	In Service	4.60
143	08/26/05 09:15 AM	1	No	Keypad			In Service	4.60
142	08/25/05 08:29 AM	1	No	Keypad			In Service	4.60
141	08/25/05 06:02 AM	1	No	Keypad			In Service	4.60
140	08/24/05 09:45 AM	18	No	Ethernet	00B0D0D2EA63	FAST_LINE-2.urs	In Service	4.60
139	08/09/05 05:12 AM	3	No	Ethernet	00B0D0D2EA63		Out of Service	4.60
138	08/09/05 03:12 AM	16	No	Ethernet	00B0D0D2EA63		Out of Service	4.60
137	09/09/05 02:30 PM	22	No	Ethernet	0008749784BF		Out of Service	4.60
136	09/09/05 02:30 PM	12	No	Ethernet	0008749784BF		Out of Service	4.80
135	09/09/05 02:30 PM	3	No	Ethernet	00B0D0D2EA63		Out of Service	4.60

Setting Changes Detail History

Event	Date of Change	Old Value	New Value	Item	Modbus Address
144	09/09/05 02:18 PM	Disabled	Enabled	Thermal Model Events	0x6620
144	09/09/05 01:10 PM	Disabled	Enabled	Thermal Model Function	0x6620
144	09/09/05 12:45 PM	Disabled	Enabled	Acceleration Events	0x6900
144	09/09/05 12:10 PM	10.00s	9.00s	Acceleration Time	0x6900
144	09/09/05 11:05 AM	Disabled	Enabled	Acceleration Function	0x6900
144	09/09/05 03:05 AM	Not Programmed	Programmed	Relay Programmed State	0x43E0
144	08/24/05 09:49 AM	None	F5	Source x Auxiliary VT	0x458A
144	08/24/05 03:05 AM	None	F5	Source x Phase VT	0x458A
144	08/24/05 01:12 AM	None	F1	Source x Ground CT	0x458A
144	08/23/05 11:20 PM	None	F1	Source x Phase CT	0x458A
144	08/23/05 09:10 PM	None	F5	Source x Auxiliary VT	0x4583
144	08/23/05 06:33 PM	None	F5	Source x Phase VT	0x4583
144	08/23/05 04:15 PM	None	F1	Source x Ground CT	0x4583
144	08/23/05 02:21 PM	None	F1	Source x Phase CT	0x4583
144	08/23/05 02:02 PM	1.00:1	24000.00:1	Phase VT x Ratio	0x4502
143	08/23/05 01:10 PM	1A	65000A	Phase CT x Primary	0x4480
142	08/23/05 12:30 PM	Off	SRC 2 Pc	Data Logger Channels	0x418C
141	08/23/05 11:21 AM	Off	SRC 2 Vcg RMS	Data Logger Channels	0x418A
140	08/23/05 11:01 AM	Off	SRC 1 Vbg RMS	Data Logger Channels	0x4188
140	08/23/05 10:10 AM	Off	SRC 2 V_1 Angle	Data Logger Channels	0x4186
140	08/23/05 06:19 AM	Off	SRC 1 Vca RMS	Data Logger Channels	0x4184

GE Multilin

EnerVista VIEWPOINT maintenance

Date and Time that the Security Report was generated

Description of the GE Multilin Relay

- Equipment Name
- Relay Model and Firmware version
- Relay Serial Number

Summary of the last time the configuration was changed

- Name of setting file
- Who loaded the file
- When the file was loaded

History of the last 10 occurrences the configuration was changed

- Date and time of the configuration change
- Number of setting changes at this time
- Method used to change the relay settings
- MAC address of the computer sending settings
- Name of the setting file sent to the relay
- The relay status after the setting changes

Detailed description of all changes made to the relays configuration

- Date and time of the configuration change
- Description of the setting that was changed
- Setting value before change was made
- Setting value after change was made

Convenient File Format

- On-line and off-line copies
- Easily zip these reports with other pertinent Files such as setting files and fault reports to share with engineers

Figure 2.

1. Open Viewpoint Maintenance and select Security Report.

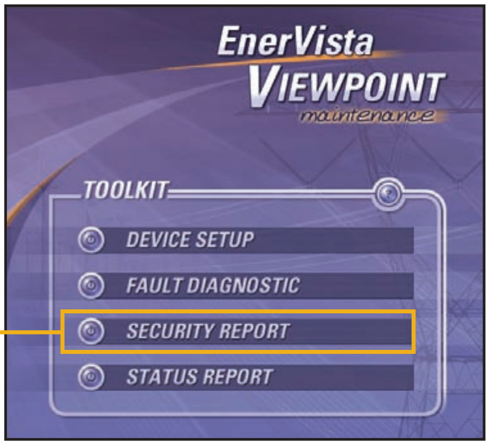
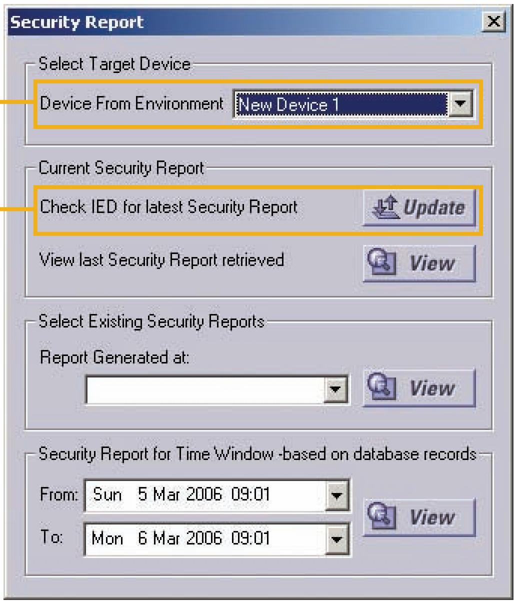


Figure 3.

2. Select the device you wish to create the Security Report for.

   Note:
   If the device is not seen in the drop down menu, it will need to be configured under the Device Setup menu of Viewpoint Maintenance.

3. Select the *Check IED for latest Security Report* button to perform the settings verification.


Security Report

Select Target Device
Device From Environment: New Device 1

Current Security Report
Check IED for latest Security Report — Update
View last Security Report retrieved — View

Select Existing Security Reports
Report Generated at: — View

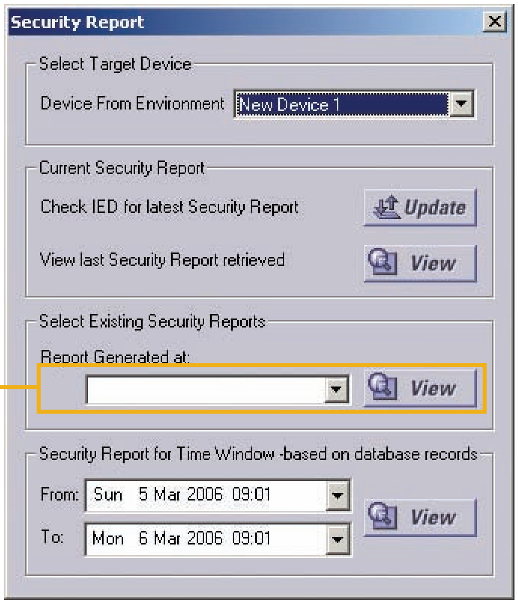
Security Report for Time Window -based on database records
From: Sun 5 Mar 2006 09:01
To: Mon 6 Mar 2006 09:01
View

Figure 4.

Note:
When performing security reports for relays that do not store the Security Audit Trail internally a security report will not be generated the first time the program is run. The settings will be saved from the relay, and these settings will be used as the baseline for any future reports.

4. To view Security Reports that were previously generated, select the date that the report was created from the Select Existing Security Reports drop down menu

To download a no charge 15 day trial of Viewpoint Maintenance visit www.GEMultilin.com/Enervista


Security Report

Select Target Device
Device From Environment: New Device 1

Current Security Report
Check IED for latest Security Report — Update
View last Security Report retrieved — View

Select Existing Security Reports
Report Generated at: — View

Security Report for Time Window -based on database records
From: Sun 5 Mar 2006 09:01
To: Mon 6 Mar 2006 09:01
View

Figure 5.

Industry Innovations

Featured Innovation

Unparalleled Control

C90^{Plus} - Controller
GE Multilin
www.GEMultilin.com/C90Plus

GE Multilin's new C90Plus - Controller - the most advanced substation hardened controller in the market. C90Plus features true convergence of multiple functions, including advanced automation logic engine, bay protection & control, high accuracy digital fault recording, comprehensive communications and local HMI capabilities. .

Protective Relay Test System

MPRT
Megger
www.megger.com

The MPRT is designed to perform routine testing of protective relays used in the operation of electric utilities, power plants and heavy industrials, and eliminates the complexity of relay testing.

- The MPRT System consists of a 'Power Box', the TouchView Interface™, and AVTS Software
- Unique new TouchView Interface (TVI) simplifies the manual testing of complex relays
- Ultra flexible output design provides up to four-phase voltage and current or eight-phase current
- User specified configuration. Every system is made to order based on specific customer needs.

Transient Voltage Surge Suppressors TVSS

TVSS
GE Power Quality
www.GEDigitalEnergy.com/pq

GE Power Quality's New lineup of Transient Voltage Surge Suppressors (TVSS) feature a patented Thermally Protected Metal Oxide Varistor (TPMOV®) technology, an advancement that includes a safety feature that shuts down the TVSS to prevent overheating and ensures compliancy with UL 1449 2nd Edition requirements for all TVSS products. Ideally suited for use in demanding and sensitive commercial and industrial environments, all GE TVSS products are UL Listed and bear the UL mark.

The CMC 256 Just Got Even Better

CMC 256plus
Omicron
www.omicronusa.com

The CMC 256plus is the right choice if high precision is required. This device is not only an excellent protection test set for all protection generations (from IEC 61850 IEDs to high-burden, electromechanical relays - in single-phase mode) but also a universal calibrator. The CMC 256plus supersedes the well-known CMC 256-6 test set.

Industry Innovations

Fully Managed Embedded Ethernet Switch

Universal Relay Ethernet Switch Module
GE Multilin
www.GEMultilin.com/URSwitch

The UR Switch Module simplifies Ethernet networking in Substations and Industrial environments and can save users as much as 70% of the entire cost associated with installing Ethernet networks. For only $200 USD (List) more than the price of a 100Mbps redundant Ethernet CPU, the switch module eliminates the need for using external Ethernet switches to create fault tolerant protective relaying networks.

Multi-Functional Partial Discharge Investigation Tool

UltraTEV Plus+™
ea Technology
www.eatechnology.com/NewProducts.asp

The new UltraTEV Plus+™ combines all the functionality of the UltraTEV Detector™, with many new features for investigating and understanding Partial Discharge (PD) activity in MV and HV switchgear in greater detail. Ultrasonic emissions are displayed as decibel readings as well as being converted into audible signals, which can be heard through the headphones supplied. TEV signals appear on the menu-driven colour LCD screen as numerical values, a bar graph, and as a green - amber - red indication.

Wireless Distributed Generation Transfer Trip

DGT - Distributed Generation Trip Control
GE Multilin
www.GEMultilin.com/DGT

GE Mulitlin unveils the new DGT – Distributed Generation Trip Control solution for enabling fast and secure disconnect of renewable energy generators from the electrical power grid. Designed to wirelessly transmit high-speed trip signals, this new device not only transfer trips a Distributed Generator in the event of a faulted grid, but also relays a status confirmation back to the Utility after the DG has been disconnected.

Overhead Cable Management Solution

Mega Snake™
Snake Tray
www.snaketray.com

Mega Snake is our new high capacity cable tray for overhead applications. Mega Snake's unique design can convey thousands of cables for large cable runs. The Snake Rail™, a built-in suspension system, requires no brackets and allows for random placement of the hanging rod system. The Snake Rail ™ can also seamlessly interface with other size Snake Trays as well as patch panels, strain relief and fiber optic pass over devices.

Industry Innovations

Compact LV Motor Protection and Control

MM200
GE Multilin
www.GEMultilin.com/MM200

Designed for low voltage motor applications in industrial facilities, the GE Multilin MM300 Motor Manager provides complete motor protection and automation in a compact form-factor. Providing advanced motor protection, the MM300 also incorporates advanced real-time and historic diagnostic capabilities, providing key system data that can be used to diagnose potential motor and process problems to ensure process operation and optimization. The MM300 is fully supported by the EnerVista suite of software tools, including Viewpoint Maintenance with single-click reporting of fault and motor diagnostic data and relay maintenance summary reports.

Thermal Imaging cameras

Fluke TiR Thermal Imager
Fluke
http://us.fluke.com

The Fluke TiR Thermal Imaging cameras are the perfect imagers for building envelope, restoration and remediation, inspection and roofing applications. See things both ways—infrared and visual (visible light) images fused together communicating critical information faster and easier—traditional infrared images are no longer enough. IR-Fusion, a patent-pending technology that simultaneously captures a digital photo in addition to the infrared image and fuses it together taking the mystery out of IR image analysis. IR-Fusion is standard on TiR models.

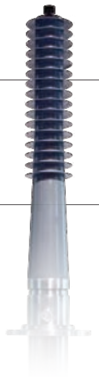
High Performance UPS

Digital Energy™ LP-33U Series 10-60kVA UPS
GE Power Quality
www.geindustrial.com/pq

The new high-performance Digital Energy™ LP-33U Series 10-60kVA Uninterruptible Power Supply (UPS) from GE Power Quality delivers reliable power protection, an industry-leading 97 percent system efficiency and proven Redundant Parallel Architecture™ (RPA™) to owners and operators of e-commerce applications, mobile networks, corporate internet sites, medical equipment, banking systems, ePay and networked IT structures

Solid Insulation Hybrid Bushings

ECI 115/145kV Hybrid Bushings
ECI Group
www.eci-co.com



Tested to ANSI standards, the ECI 115/145 kV bushing is a cycloaliphatic/silicone hybrid product, providing excellent insulation, combined with the durability and performance only polymers can offer. The design features and characteristics of bushings provide many benefits and advantages over traditional OIP (Oil Impregnated Paper) porcelain bushings.

Upcoming Events

UTC | May 4 - 7 | Orlando, Florida, United States

The Utilities Telecom Council 2008 Conference and Exposition will target issues involved in core transport technologies. These systems form the backbone of critical infrastructure communication, but look quite different from one utility to the next. As these systems evolve, utility telecom professionals are faced with the challenge to upgrade, while continuing to meet the fundamentals – ensuring the safety and reliability of core utility services.

Single Creek Resort
www.utc.org/events/upcoming

GE Multilin, GE Lentronics, & GE MDS Tradeshow Booth

- Visit GE at booth #909

Georgia Tech FDAC & PRC | May 19 - 23 | Atlanta, Georgia, United States

Join GE Multilin for two ½ day complimentary seminars; Distribution Substation Protection Examples and Generator Protection Fundamentals. These seminars are free and are beneficial to plant engineers, consulting engineers and utility personnel. Lunch is included.

For participants maintaining a P.E. license, a course certificate with PDHs will be issued confirming your participation in the seminar.

Atlanta Renaissance Hotel Downtown
www.pe.gatech.edu

GE Multilin Presentations at the 11th Annual Fault & Disturbance Analysis Conference

- Monday, May 19th: 9:15 am - Synchrophasor and High-Speed Oscillography Analysis of an Industrial Facility Islanding Test
  Mark Adamiak, Michael Schiefen, Gary Schauerman
- Tuesday, May 20th 8:35 am - Impact of CT Error on Protective Relays – Case Studies and Analysis

GE Multilin Seminar at the 62nd Annual Georgia Tech Protective Relay Conference

- Distribution Substation Protection Examples
  Location: Atlanta Renaissance Hotel Downtown – Ballroom B
  Time: 8:00 am to 11:45 am
- Generator Protection Fundamentals
  Location: Atlanta Renaissance Hotel Downtown – Ballroom B
  Time: 12:30 pm to 5:00 pm

GE Multilin Papers to be Presented at the 62nd Annual Georgia Tech Protective Relay Conference

- Fundamentals of Distance Protection
- Re-strike and Breaker Failure Conditions for Circuit Breakers Connecting Capacitor Banks
- Design and Implementation of an Industrial Facility Islanding and Load Shed System
- Detection of Incipient Faults in Underground Medium Voltage Cables
- Fast and Secure Numerical Breaker Failure Protection
- CT Failure Detection for Differential Protection Applications
- Application of Digital Radio for Distribution Pilot Protection and Other Applications

Upcoming Events

Railway Systems Suppliers Inc.

May 20 - 22

Orlando, Florida, United States

Railway Systems Suppliers, Inc. is a trade association serving the communication and signal segment of the rail transportation industry. Their primary effort each year is to organize and manage a trade show for their members to exhibit their products and services

Gaylord Texan Resort & Convention Center
www.RSSI.org

GE MDS Tradeshow Booth

- Visit GE MDS at booth #1103

AWWA ACE

June 8 - 12

Atlanta, Georgia, United States

Nowhere else can you see up-close the innovations of more than 500 exhibiting companies and organizations in all aspects of the water industry. ACE 2008 offers expert insight and provides a hands-on understanding of the latest products and technologies.

The ACE08 Exposition is the perfect complement to the annual conference's professional program. From pipes to valves, meters to hydrants, engineering services to tank-related companies, membrane filtration systems to laboratory equipment, and security to wastewater—if it relates to water in any way it will be at ACE 2008

Georgia World Congress Center
www.awwa.org

GE MDS Tradeshow Booth

- Visit GE MDS at Booth #1642

Global Petroleum Show 2008

June 10 - 12

Calgary, Alberta, Canada

2008 will mark the 20th Global Petroleum Show as the most significant petroleum event anywhere in the world. Since its inception in 1968, the event has grown to be renowned for first-rate presentation of the latest in technology in the fields of onshore and offshore exploration, production and transportation.

Stampede Park
www.petroleumshow.com/globalpetroleum

GE MDS Tradeshow Booth

- Visit GE MDS at Booth #1609

Upcoming Events

IEEE Pulp & Paper Conference | June 22-27 | Seattle, Washington, United States

The Conference Technical Program will provide paper industry Electrical Engineers valuable knowledge that can be applied to daily mill responsibilities encompassing:

- Changes in electrical engineering, maintenance and safety practices, standards and codes.
- Learning about equipment upgrades in other plants, and hearing about the projects that worked and the ones that didn't.
- Acquiring skills in generator and motor protection, determining relay settings and troubleshooting failures.
- Discovering how to justify electrical upgrades with an emphasis on reliability.
- Networking with other attendees that are extremely knowledgeable and actively working every day in the industry to make it better, safer and more competitive.

Grand Hyatt Seattle
www.pulppaper.org

GE Multilin Tradeshow Booth

- Visit GE Multilin at booth #1

IMSA Public Safety | July 17 - 23 | Phoenix, Arizona, United States

The International Municipal Signal Association (IMSA) is dedicated to providing quality certification programs for the safe installation, operation and maintenance of public safety systems; delivering value to it's members by providing the latest information and education in the industry.

Sheraton Wild Horse Pass Resort
www.imsasafety.org/

GE MDS Tradeshow Booth

- Visit GE MDS at Booth #513

APCO International | August 3 - 7 | Kansas City, Missouri, United States

APCO International is the world's largest organization dedicated to public safety communications. The International Municipal Signal Association (IMSA) is dedicated to providing quality certification programs for the safe installation, operation and maintenance of public safety systems; delivering value to it's members by providing the latest information and education in the industry

Kansas City Convention Center
www.apco2008.org

GE MDS Tradeshow Booth

- Visit GE MDS at Booth #2131

Upcoming Events

CIGRÉ	August 24 - 29	Paris, France

CIGRÉ is a permanent, non-governmental and non-profit making international association, which was founded in 1921 in France. Issues related to planning and operation of power systems, design, construction, maintenance and disposal of HV equipment and plants, protection of electrical systems, telecontrol and telecommunication equipment and data management are at the core of CIGRÉ's mission. Electricity markets, regulation and environment are also within the field of concern of CIGRÉ.

Palais des Congrès
www.cigre.org

GE Multilin Tradeshow Stand

- Visit GE Multilin at stand #46

ASGMT	September 8	Houston, Texas, United States

The School is the largest gas measurement school in the United States devoted to natural gas measurement, pressure regulation, flow control, and other measurement related arenas. The purpose of the School, the sponsoring associations, and the operating companies within the petroleum and natural gas industry, is to provide instruction on technical subjects for people in the industry.

Mariott House Westchase
www.ASGMT.com

IEEE IAS PCIC	September 22 - 24	Cincinnati, Ohio, United States

The PCIC provides an international forum for the exchange of electrical applications technology related to the petroleum and chemical industry. The PCIC annual conference is rotated across North American locations of industry strength to attract national and international participation. User, manufacturer, consultant, and contractor participation is encouraged to strengthen the conference technical base

Cincinnati Hilton Hotel
www.ieee-pcic.org

GE Multilin Papers to be Presented

- Cost Efficient Applications of Bus Transfer Schemes Utilizing Microprocessor Base Relaying Technology
- Safety First: The Detection of Downed Conductors and Arcing on Overhead Distribution Lines

Drive More Spend Less

Best Protection
Best Communications
Lowest Price

Designed for low voltage motors in process and control applications, the Multilin MM200 Low Voltage Motor Management System delivers superior protection, control and comprehensive communications for maximum ease-of-use and process continuity at the lowest price. Utilizing the Multilin motor thermal model perfected over the last 25 years, GE's Multilin MM200 provides truly optimized protection. With the ability to simultaneously communicate using Modbus RTU and either DeviceNet or Profibus DP protocols, the Multilin MM200 ensures direct control and easy access to information across common network architectures.

With its rugged, compact design that fits into common NEMA and IEC Motor Control Centers, the Multilin MM200 is ideally suited for low voltage motors found in oil & gas, mining & minerals, pulp & paper, food & beverage, pharmaceuticals, cement, forest products, water / waste water, and packaging applications.

MM200 Motor Management System

Digital Energy
Multilin

GE Multilin
www.GEMultilin.com/mm200
gemultilin@ge.com

Worldwide
Tel: 905-294-6222

North America
Tel: 1-800-547-8629

Europe/MiddleEast/Africa
Tel: +34 94 485 88 00

Protection & Control Journal

Content Index

Articles

Trade Shows/Conferences

Product Listings

Advertiser Listings

Wireless DG Trip Control

DGT
Distributed Generation Trip Control

Disconnect DG from the grid... Fast, Wireless, and Cost-effective

From the industry leader in protection and control, GE's Multilin DGT is revolutionary and innovative Distributed Generation disconnect solution that provides high-speed, cost-effective, wireless, reliable and secure trip control. Extremely resistant to interference, the DGT- Distributed Generation Trip Control can transfer trip signals in as fast as 28 milliseconds over a 30 mile range with up to 7 Distributed Generation sites and provides status confirmation to the Utility Substation after a trip operation has been performed.

From wind to solar to other traditional types of generation, customers trust Multilin to deliver safe and dependable Protection & Control solutions for Distributed Generation Systems.

For more information please visit www.gemultilin.com/dgt

Digital Energy
Multilin

GE Multilin
www.GEMultilin.com/dgt
gemultilin@ge.com

Worldwide
Tel: 905-294-6222

North America
Tel: 1-800-547-8629

Europe/MiddleEast/Africa
Tel: +34 94 485 88 00

Advanced Training

GE Multilin 2008 Course Calendar

Comprehensive Training Solutions for
Protection, Control and Automation

SCHEDULED COURSES IN NORTH AMERICA

Courses for 2008	Tuition*	CEU Credits	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
Fundamentals of Modern Protective Relaying	$2,400	2.8	21-24			21-24			21-24		15-18		17-20	
Power System Communications	$1,800			7-8		1-2		5-6	10-11			9-10		
Introduction to the IEC61850 Protocol	$1,800	2.1		4-6				16-18				6-8		
Distribution Protection Principles & Relaying	$1,800	2.1			3-5						3-5			
Motor Protection Principles & Relaying	$1,800	2.1			11-13				7-9			1-3		2-4
UR Platform	$1,800	2.1		18-20		8-10		2-4		18-20			3-5	
UR Advanced Applications	$3,000	3.5					12-16					27-31		
Enervista Viewpoint Monitoring	$600				14		2				19		6	

All North American courses are located in Markham, Ontario, Canada unless otherwise stated

*Tuition quoted in US dollars

SCHEDULED COURSES IN EUROPE

Courses for 2008	Tuition*	CEU Credits	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
UR Advanced Applications	$2,400	2.8		11-15			12-16				22-26		10-14	
UR Platform	$1,800	2.1		6-8			7-9				17-19		5-7	
Distribution Protection Principles & Relaying	$1,800	2.1			3-5				9-11					
Fundamentals of Modern Protective Relaying	$2,400	2.8						2-5						15-18
Motor Management Relays	$1,800	2.1			10-14				14-16					
F650 Platform	$1,800	2.1				14-16		16-18				6-8		3-5
Introduction to the IEC61850 Protocol	$1,800	2.1				17-18						9-10		

All European courses are located in Bilbao, Spain unless otherwise stated

*Tuition quoted in US dollars

Course dates are subject to change. Please visit our website at **www.GEMultilin.com/training** for the most up-to-date schedule.

/ ANALOG INP
2
3
6
7