

A Survivable System Analysis for the Communications Infrastructure used by the Electric Power Grid

John Waite, *Student, University of Idaho*, Donghui Yang, *Student, University of Idaho*,
and John Hall, *Student, University of Idaho*

Abstract—The electric power industry depends upon the security and reliability of its power substations. These substations are generally planned with good physical security and redundancy in mind. These substations must communicate with outside sources and relay data from systems such as the SCADA. Remote access control to the substations is increasing and with that increase is an increase in the vulnerability to a cyber attack. A survivability systems analysis (SSA) can help to define the critical systems and defense strategies for those systems. For each critical system a series of attacks, the current state of defense and a recommendation for better defense is proposed in the areas of resistance, recognition, and recovery.

Index Terms—Survivability, Survivable System Assessment, Electric Power Grid, Substation Security.

I. INTRODUCTION

THE electric power grid is made up of many components. Substations are one of the most prominent and critical of these components. They are critical because they control power transmission. They are vulnerable for many reasons. For example, substations tend to be unoccupied. [7] states the following causes of substation intrusions: economic, location, aesthetics, labor conflicts, use of adjacent property curiosity and ignorance, civil/political unrest, joint-use facilities, natural and/or catastrophic disasters. Substations are vulnerable to several different sorts of attacks. This document will focus on electronic [7] attacks. These are attacks on the communication systems used within a substation and those that allow the substation to communicate with outside systems.

Substations typically consist of three major types of components. These components communicate among themselves to maintain power services. The lowest level devices are Intelligent Electronic Devices (IEDs). Each of these devices is responsible for one basic function. For example, an IED may control a protective breaker or a recloser. These systems typically have deterministic embedded functionality to try to correct most simple problems. External connections may be made directly to some IEDs through an outside connection. This connection will typically be made using a modem connected using RS-232. These IEDs will also communicate with a substation controller. This controller is typically responsible for coordinating these devices. Historically a wide variety of protocols were used for this communication, such as Modbus,

DNP, UCA, Modem, FieldBus, RS481, and many other proprietary protocols [16], [20]. However, the default communication protocol for most modern systems is Ethernet. The substation controller will then communicate with a Supervisory Control and Data Acquisition (SCADA) system. Historically this connection was typically RS-232 (EIA232), but EIA 485, UCA, ControlNet, WAP, WEP, FieldBus, ICCP, IEC 60870-5-101, DNP3, Modbus, Conitel, and many other proprietary protocols [16], [4] were also used. Typically modern devices handle this communication with Ethernet. The SCADA system is responsible for a higher level storage and analysis of the data coming from the various devices. If the substation controller reports a problem that could not be corrected, the local SCADA system will attempt to determine a higher level approach to fixing the problem. If the local SCADA system cannot fix the problem, it will send an alert to a centralized system. These alerts and other data are typically sent over either a leased line, or a long haul ethernet line, or even wireless or satellite communications. Typically each distribution company will maintain their own higher level command centers. These command centers look for long-term trends in the data and for alarms that need additional corrections. These centers typically send commands back to the SCADA systems within substations, but may also communicate directly to the substation controller or to an IED. These communications are done using the communications paths listed above.

As power substation systems in nowadays more and more rely on SCADA system, the security of SCADA data and control system itself and the reliability of the communication system out of or into SCADA system become critical to the reliable operation of power substation system. With the ever increasing intrusions happened on computer systems and the high impact of failure in power station system, power grid system especially power substation system become a potential target of computer intrusions. In this paper, we uses the Survivable Network Analysis (SNA) to analysis the proposed power substation system. A couple of resources including literatures are used to build a general power station constructure as the case of this analysis. Usage scenarios are analysed for essential services and assets, intrusion scenarios are explored to identify the compromisable network components, based on the this work, 3 rs are analysed for the intrusion scenario that targets the essetnail and compromisable components. The resulted analysis help improve the security and reliability current power substation communication system.

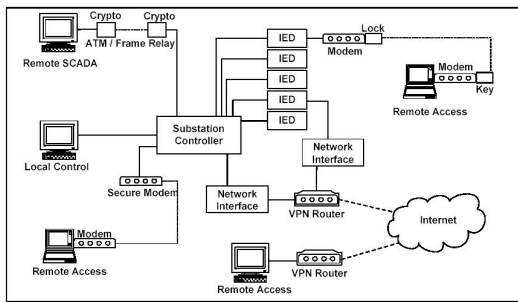


Figure 2: Securing Communications

Fig. 1. Power Substation Architecture [18]

II. ANALYSIS

Since we do not have a real customer to work with, we got the information for our usage scenarios from the literature, product specifications, and some online sources. We will use this information to identify usage scenarios. As a team we will identify the services offered by the electric power systems. We will assign a set of the usage scenarios to each team member to research and write up in more detail. This phase will include research to become familiar with the protocols and products currently offered for use in power systems. By the end of these steps, we had the architecture for a power substation as shown below.

III. NORMAL USAGE SCENARIOS

A. NUS1-Automatic SCADA Response

Under normal operation in a substation, the SCADA system supervises system operation. The SCADA system typically communicates directly to the substation controller. This communication may use a variety of protocols. The SCADA system will rely on this communication channel to get the current status information from the substation controller. Part of this supervision involves responses generated by the local SCADA system. When the SCADA system detects a problem, it tries to correct the problem by sending a command to the substation controller. This automatic response relies on the same communication path.

B. NUS2-Remotely Initiated SCADA Response

When the local SCADA system is unable to correct a local problem, it sends a notification to a centralized corporate system. This system is typically in the company's regional command center. The regional supervisory system will send response commands back to the local SCADA system. These remotely initiated responses are communicated back to the local SCADA system using a variety of communication protocols. However, most of these communication paths are implemented using ethernet or leased telecommunication lines.

C. NUS3-Automated SCADA Remote Reporting

The SCADA system prepares its data and sends it out via various methods to a general repository or other reporting mechanism. The SCADA system constantly collects data from

the various devices attached to the substation and deals with most of the minor variations in voltage, phase, and current automatically. As many vendors desire to view that data in order to perform more detailed analysis SCADA systems are being used to send this data as a reporting mechanism. The values of various measurements are compiled into a report and this report is sent to some repository. This can be a database, web server, or other receiving media. The transmission of the data can happen in any of a number of ways. It can be obtained by remote dialing in to an attached modem, direct transmission over private lines, sent directly over company LAN, wirelessly broadcast, or any other form of communication. As the SCADA system itself does not retain the values the reporting system is ongoing. This reporting can be used to help identify errors, problems, or inefficiencies in the substation. Occasionally there are problems in the transmission of power for which the SCADA system is inadequate to deal with. The correct responses have either not been implemented, or the problem is recurrent and can't be dealt with by the SCADA system. In this case the SCADA system prepares and transmits an alert to some kind of reporting authority. The report is sent so that engineers can review the data and possibly deal with the situation remotely.

D. NUS4-Local SCADA Reporting

The SCADA system's data is capable of being viewed by accessing a local terminal. While being viewed any alarms will be sent to the terminal for the engineer to deal with.

E. NUS5-Poll SCADA Data

As SCADA systems provide both diagnostic data and production data to the operators, when there is a fault occurs, operator could retrieve diagnostic data such as the characteristic data of protective relay saved when the fault happened. Or operator wants to review how many alarms were set in the system within a few days. Some of the SCADA system records the activities of the operators, in these systems, when fault happens, operators can access SCADA data and find out what happened. SCADA systems also collect production data such as voltage, current etc. Managers would want to know how the power is used and retrieve this data. This kind of data request can be done with local access to the SCADA system as well remote control through proprietary network or Ethernet.

F. NUS6-Read Current Settings From a Local Intelligent Electronic Device (IED)

IEDs are simple electronic devices that control some limited device. For example, an IED in a power substation will typically control a breaker or a recloser. These intelligent devices contain settings that control how the device behaves. For example, an IED that controls a breaker will have settings that determine the sensitivity of that breaker. An engineer in a substation is able to access these settings. Typically, these IEDs may be connected to the substation controller using a variety of protocols. RS-232 and Ethernet are the dominant protocols used for these communications. These communication paths allow the engineer to query the device to get its current settings.

G. NUS7-Read Current Settings From a Remote IED

Some IEDs support connecting communication devices directly. While a variety of communication devices may be used, typically modems are connected using RS-232. These communication devices allow an engineer working remotely to connect to an IED and determine its current settings. While this may seem redundant since most of this information would be available from the local SCADA system, such communication paths are common. They are necessary in simple substations that do not have a SCADA system. They are also useful for troubleshooting or verifying a SCADA system. They can also be used to analyze the device directly. They are also useful where low level control of devices is needed.

H. NUS8-Control IED Settings From a Remote Site

Users from offsite may access the IED devices via electronic communication and change/alter settings on the device directly. A user may need to access an IED directly in order to perform maintenance or to implement a change in the operational settings on the device. Access to the IED devices can be obtained either directly, by dialing into an attached modem, connecting over serial line, or other form of communication, or through the substation controllers themselves. Access through the substation controllers will give the user to make changes to settings or control all IED devices attached to the system while direct access will only allow the changing of a single device.

I. NUS9-Manage IED Settings Locally

Users may access the IED devices from local terminals and control settings or make changes to operations of the device. Local terminals will be attached to the substation control system and can allow access to the controls of an IED. The connection is usually direct via serial or other cable.

J. NUS10-Maintain Software

In the substation, there is supporting software on SCADA server, substation controller, IED and local monitor. SCADA system uses some interface software to support data retrieval and sharing, and database management system to store collected data, alarms and reports. There is also terminal software to support SCADA local operation. On substation controller, there are supporting software for collecting data from IEDs and sending control command to IEDs. On IED controllers, there are software to control devices such as protection relays, breakers and so on. These software especially SCADA system supporting software may need to be updated due to the requirement of operator and the increasing of data volume. As far as I know, this update should be done local for secure.

K. NUS11-Reset Software

While the software used in a substation has an impressive track record for reliability, especially when compared to other commercially available software systems, these software systems do occasionally fail. When this happens, it is necessary

to reset the software. While this may be as simple an activity as locally rebooting the server, some systems also have means to remotely trigger the reset. These systems allow a remote engineer using the communication paths normally used for SCADA control to trigger a reboot. This communication path may use a variety of protocols, but typically uses an ethernet, or leased telecommunication line.

L. NUS12-Bringing a Substation Online

In bringing a station online, the communication systems are attached to the physical devices and connected to a terminal unit for testing. Each device is tested for its ability to read information, and to set/control the device itself. After settings are in place, the devices are connected to outside connections. These connections come in the form of modems, wireless, LAN, dedicated lines, etc. Each of these communication devices is configured to allow access within the substation and to the correct control device. After the connections are made and tested, any other security devices are implemented and tested. (some security devices will be the same devices as used for communication ie. Encrypting modems, etc.)

M. NUS13-Bringing a Substation Online

In bringing a station online, the internal devices are connected to local control computers (RTU's) and tested. Each device attached is checked for availability of access on the local terminal and the ability to control settings.

N. NUS14-Bringing a Substation Offline for Repair

Cut off all the communication paths out/in substation. Test substation controller and IED for reliability and performance.

O. NUS15-Reading Substation Controller Settings Remotely

The substation controller combines the information from all the IEDs in a power station. The substation controller may trigger an alarm if a power control function is operating outside tolerances. Many modern substation controllers allow reading these tolerances remotely. While a variety of communication protocols may be used, these communication paths are typically ethernet or leased telecommunication lines.

P. NUS16-Modify Substation Controller Settings Remotely

The substation controller combines the information from all the IEDs in a power station. The substation controller may trigger an alarm if a power control function is operating outside tolerances. Many modern substation controllers allow settings these tolerances remotely. While a variety of communication protocols may be used, these communication paths are typically ethernet or leased telecommunication lines.

Q. NUS17-Access SCADA Settings Remotely

SCADA systems typically run on UNIX systems. Many of these systems allow accessing their settings remotely. Some SCADA systems support this using XWindows or even a Web Browser. This is typically done over an ethernet based local network.

R. *NUS18-Set SCADA Settings Locally*

SCADA systems typically run on UNIX systems. Configuring these systems locally is typically done through a local terminal. However, some installations may use a simple terminal or laptop running XWindows (or a Web Browser on some recent products) for configuration. This is typically done over an ethernet based local network.

S. *NUS19-Remotely Control SCADA Settings*

SCADA systems are complex with many configuration parameters. Often, engineers need to modify these settings from a remote location. This configuration is typically done over an ethernet, leased line, or even modem connection. The configuration are typically done using proprietary protocols. However, some systems use XWindows and some even use Web Browsers.

IV. SERVICES

- 1) Automatic SCADA Control (commands in)
- 2) Constant SCADA Communication (data and alarms out)
- 3) Access (SCADA) Data (pull data)
- 4) Access IED Settings (read)
- 5) Access IED Settings (set / control)
- 6) Maintain Software (update)
- 7) Maintain Software (reset)
- 8) Bring Substation Online
- 9) Bring Substation Offline (for repair)
- 10) Access Substation Controller Settings (read)
- 11) Access Substation Controller Settings (set / control)
- 12) Access SCADA Settings (read)
- 13) Access SCADA Settings (set / control)
- 14) Fault Alarm

V. CRITICAL ASSET SELECTION

A. *Local SCADA system*

B. Communication channel between Local SCADA and outside central reporting system

C. Communication channel between Local SCADA and Substation Controller

D. Communication channel between Substation Controller and IEDs

E. Communication path into IEDs from remote site.

VI. ATTACK SCENARIOS

A. *IUS1-Ping Sweep to Find IPs of Private Power Station Controllers*

An attacker determines the IP address of the publicly available cooperate servers. The attacker then tries pinging other addresses within the same class to try to locate substation devices. This attack may be done with a variety of tools. A popular attack tool that includes ping sweep functionality is the port scanner nMap. With this tool, the attacker can learn which IP addresses are used. The attacker can then perform a port scan to try to identify power station controllers. (And other critical devices.)

B. *IUS2-Wardial to Find Modems Used in Power Substations*

An attacker uses a script to control a modem to try a wide range of phone numbers. This allows the attacker to build a list of phone numbers of modems attached inside the substation.

C. *IUS3-Denial of Service Attack on Modem Used for Remote IED Access*

An attacker discovers the phone number of a modem connected to an IED. He constantly dial the same number so the modem is kept busy answering his call and no authorized operators can access the IED through the modem.

D. *IUS4-Brute Force or Dictionary Attack on Password of IED*

The attacker locates the phone number for a modem connected to an IED. The attacker then tries passwords either at random or from a dictionary of common passwords. The attacker redials each time the connection is dropped due to login timeouts. The effectiveness of this attack varies greatly based on the number of possible passwords allowed by the device, and the complexity of the password used.

E. *IUS5-Denial of Service Attack on Modem Used for Substation Controller*

Once the existence of a communication device within the substation is confirmed, either by wardialing, scanning, or other means, a hacker can direct large amounts of traffic into that communication channel making it impossible for legitimate use to occur. This can make it very difficult to impossible to access or control the device in any way.

F. *IUS6-Tap into Fixed LAN Line to Eavesdrop on Substation Traffic*

An attacker taps into LAN line to eavesdrop on substation traffic. The attacker can get any substation information that operators request from the substation controller and any control/reset information operators send through LAN. This information can be sold to competition utility company or save for later attack on substation controller or IEDs.

G. *IUS7-Tap into Fixed LAN Line to Spoof Legitimate Traffic*

A SCADA system connected by a fixed LAN to a corporate system will constantly send status messages. In general, there are "all clear" messages and "alarm" messages. In this attack, the attacker gains physical access to the communication wire connecting the substation to the corporate system. The attacker separates this wire and inserts a communication device between the two halves. This device allows the attacker to pretend to be the SCADA system and send "all clear" messages to the corporate system.

H. *IUS8-Hack into Telecommunication to Eavesdrop or Spoof Traffic on a Leased LAN Line*

A hacker may hack into the telecommunication system in order to eavesdrop the line. Once some other method of attack works, the hacker can listen to all traffic on the line and possibly use it maliciously. The hacker may be able to introduce false messages into the communication line which can disrupt service or damage equipment.

I. IUS9-Cut a Fixed LAN to Perform a Physical Denial of Service

An attacker physically access substation and cut communication lines. Any communication through the line is cut off, information can not be retrieved and substation controller can not be instructed through this communication path.

J. IUS10-Use Control of Fixed LAN to Hack into Substation Controller

An attacker physically accesses a fixed LAN communication line. The attacker then connects a communication device onto the line. The attacker then generates attacks (such as are well known in the field of network security) directed at a substation controller. The intent of the attack may be to perform a denial of service, or it may be to gain access so settings may be modified.

K. IUS11-Gain Physical Access to Substation Controller and Hook into Substation Controller to Change Settings

A hacker may attempt to break through the physical security in order to access the computing resources or communication lines within the substation. The hacker can access the terminal directly and if able to successfully login disrupt service in some way. The hacker may also put their own hardware in place to act as a back door for future attacks.

L. IUS12-Ping Sweep to Find Route to Substation Controller

An attacker uses port scanner or ping sweep tool to scan the IP addresses close to a known IP address of the utility company to find out which one is alive.

M. IUS13-Gain Access to Remote Substation Controller Monitoring Computer

Summaries of the SCADA data from substations is collected at corporate sites. Typically a computer in this command room displays the status of the substations. An attacker could gain access to this monitoring computer and disrupt its operation, for example by installing software that showed that there were no problems at any substation.

N. IUS14-Install Virus, Worm, Trojan, or Logic Bomb on Remote Substation Controller Monitoring Computer

An attacker may, after breaking into the system, plant malicious code into the software which can cause problems. It may be that the malicious code immediately takes affect and performs some kind of disruptive action, or may provide ways to attack the station at a future time.

O. IUS15-Accidentally or Maliciously Send Incorrect Settings to Substation Controller. (Insider)

An operator accidentally or maliciously send incorrect settings to substation controller through local control or from remote site. This can degrade substation reliability or even shut down part or all the substation.

P. IUS16-Gain Physical Access to Substation Controller and Hook Into IED to Change Settings

An attacker who can get into a substation may connect directly to an IED, for example, by using a laptop. The attacker could then modify the settings of the IED. These new settings may either allow the equipment to operate in an unsafe way, or to operate in an overly conservative way.

Q. IUS17-Burn Out Recloser by Maliciously Causing Breaker to Open at Incorrect Times

An attacker who has gained access may attempt to cause physical damage to equipment within the substation by causing breakers and reclosers to operate continuously or repeatedly.

R. IUS18-Coordinated Attack on Substations

Some SCADA systems and some IEDs allow setting events at a given time. An attacker could hack into the SCADA system or into an IED using another attack listed above. The system could then be configured to behave undesirably at a given time. The attack could be repeated on multiple substations.

S. IUS19-Gain Physical Access and Disconnect IED Control From Substation Controller

An attacker who has gained physical access to a substation could physically disrupt the communication between IEDs and the substation controller. This attack could be done by simply cutting the wires connecting these devices.

T. IUS20-Crash IED Remotely Over Modem or Network Interface

An attacker may attempt to maliciously affect an IED over the communication interface by either changing settings or causing the IED to stop functioning. This attack can be carried out over the modem or network interface.

U. IUS21-Gain Physical Access and Locally Control Substation Controller

An attacker physically access substation controller and send command to IEDs. This could be disable protective relay, set threshold for breaker to be higer, so breaker won't break when the flow-by power is too high and all the devices are burned.

V. IUS22-Gain Physical Access and Disable Connection from Substation Controller to SCADA System

An attacker who has gained physical access to a substation could physically disrupt the communication between the substation controller and the SCADA system. This attack could be done by simply cutting the wires connecting these systems.

W. IUS23-Remotely Crash Substation Controller

An attacker may attempt to cause a disruption of the substation controller. This may be attempted by any of the attacking scenarios discussed. The disruption could take down the entire substation and any access into the substation controller has the potential to do this attack.

X. IUS24-Denial of Service Substation SCADA System

An attacker keeps sending out data requesting or control packages to the SCADA system and occupies all the resource so SCADA system can not serve other authorized SCADA operations.

Y. IUS25-Overload Remote SCADA Controller

An attacker who can gain access to any of the communication lines connecting the SCADA systems in substations to the corporate SCADA controller could perform a denial of service attack on the corporate controller. The attack could be performed by sending a large number of "all clear" or "alarm" messages.

Z. IUS26-Hack into SCADA Control or Data Lines and Eavesdrop

An attacker may attempt to hack their way into the SCADA control/data lines. The attacker could then eavesdrop on the lines and listen to, record, and spoof traffic over the line. This attack could also give control of the SCADA system to the attacker and cause misreporting of data and damage to the system.

. IUS27-Hack into SCADA Control or Data Lines and Falsify Data or Send Harmful Commands

An attacker gains access to SCADA system and modifies the production data, deletes alarms, change reports or send harmful commands to substation controller to maliciously reset IEDs.

. IUS28-Cut SCADA Transmission Line

An attacker that has physical access to the communication line connecting the SCADA system in a substation to the corporate system could disrupt that line. For example an attacker may cut the communication line.

- 4) Communication channel between Substation Controller and IEDs
- 5) Communication path into IEDs and substation controllers from remote site.

The survivability analysis focuses on the essential services and assets that these components provide in fulfilling the mission objectives of the system.

VIII. RESISTANCE, RECOGNITION AND RECOVERY ANALYSIS

Analysis of three R's resulted in the Survivability Map. This process starts by matching each intrusion scenario trace to the softspot components. For each R, first the current components or implementations are checked, because of the lack of real substation data, assumptions are made according to literature reading. If there is the current component or mechanism are unable to guarantee the R, then recommendations are proposed.

VII. SOFTSPOT ANALYSIS

A. Comprisable Components

- 1) SCADA data and control system
- 2) SCADA transmission line (out)
- 3) Transmission line between SCADA and IED
- 4) Power Station Controller
- 5) Modems to controller or IED
- 6) Remote substation monitoring computer

B. Softspot Component Identification

Softspot components are those components that are both essential and compromisable. Previous analysis shows that following components are both essential and compromisable:

- 1) Substation SCADA system
- 2) Communication channel between Local SCADA and outside central reporting system
- 3) Communication channel between Local SCADA and Substation Controller

TABLE I
SURVIVABILITY MAP

Intrusion Scenario	Resistance Strategy	Recognition Strategy	Recovery Strategy
IUS1 Ping sweep to find IPs of private power station controllers.	Current: Install a Corporate Firewall	Current: None	Current: None
	Recommended: Configure the firewall to not grant access to any unnecessary packets.	Recommended: Install an Intrusion Detection System (IDS) to monitor for these probes.	Recommended: Update firewall ruleset as necessary.
IUS2 Wardial to find modems used in power substations.	Current: None	Current: Phone service provider monitoring, looking for patterns of sequential calls.	Current: None needed.
	Recommended: Tone lock modems, modems which drop the signal unless a predetermined tone is sent immediately upon connection.	Recommended: None	Recommended: If attack is successful through phone lines, it may be possible to change phone numbers used.
IUS3 Denial of service attack on modem used for remote IED access.	Current: None	Current: Obvious, modem's number will continuously be busy.	Current: None
	Recommended: Callback modems may help.	Recommended: Same	Recommended: Arrange an emergency override with the telecommunication company.
IUS4 Brute force/ dictionary attack on password of IED.	Current: Passwords	Current: None	Current: None
	Recommended: Only use equipment that allows complex passwords. Choose difficult passwords. Employ good password management techniques.	Recommended: Monitor all failed and successful logons.	Recommended: Change the password. Verify that all good password management techniques are followed.
IUS5 Denial of service attack on modem used for substation controller.	Current: None	Current: None	Current: None
	Recommended: Tone lock modems, immediately drop connections which do not use the correct signal	Recommended: Program modem to keep track of failed connection attempts per minute.	Recommended: After a predetermined number of failed logins per minute, disable connection to the device for a length of time.
IUS6 Tap into fixed LAN line to eavesdrop on substation traffic.	Current: None	Current: None	Current: None
	Recommended: Use IPSec (with encryption) to make eavesdrop more difficult.	Recommended: None- It is difficult and expensive to detect eavesdropping.	Recommended: Change encryption keys.
IUS7 Tap into fixed LAN line to spoof legitimate traffic.	Current: None	Current: None	Current: manually restore all the settings changed by spoofed traffic.
	Recommended: Encryption of all traffic, and authentication via IPSec. Update encryption keys at reasonable intervals.	Recommended: Add digital signatures such as offered by IPSec to traffic. Install an intrusion detection system to look for abnormal communications.	Recommended: Keep a copy of current setting each time before change setting so in case of emergency, setting can be easily restored. Establish a secure means of updating the keys used for authentication. Reestablish secure communications.
IUS8 Hack into telecommunication to eavesdrop or spoof traffic on a leased line LAN.	Current: corporate firewalls	Current: none	Current: manually restore all the settings changed by spoofed traffic.
	Recommended: Encryption of all traffic, and authentication via IPSec. Update encryption keys at reasonable intervals.	Recommended: Add digital signatures such as offered by IPSec to traffic. Install an IDS to look for abnormal communications.	Recommended: Keep a copy of current setting each time before change setting so in case of emergency, setting can be easily restored. Establish a secure means of updating the keys used for authentication. Reestablish secure communications.
IUS9 Cut a fixed LAN to perform a physical denial of service.	Current: None	Current: None - obvious.	Current: Repair the damaged line.
	Recommended: In especially critical installations, install a secondary independent communication line. (For example, a satellite connection.)	Recommended: Same	Recommended: Above, and switch to secondary communication method.

TABLE II
SURVIVABILITY MAP

Intrusion Scenario	Resistance Strategy	Recognition Strategy	Recovery Strategy
IUS10 Use control of fixed LAN to hack into substation controller.	Current: None	Current: None	Current: None
	Recommended: Encryption of all traffic, and authentication via IPSec. Update encryption keys at reasonable intervals.	Recommended: Add digital signatures such as offered by IPSec to traffic. Install an IDS to look for abnormal communications.	Recommended: Verify current substation configuration. Change passwords. Change encryption keys.
IUS11 Gain physical access to substation controller and hook into substation controller to change settings.	Current: all physical security measures	Current: None	Current: Engineers check settings to insure nothing was changed.
	Recommended: Secure login at substation, hard passwords	Recommended: Log failed login attempts and lock terminal after predetermined number. Contact HQ to verify physical access.	Recommended: Above, plus passwords which have been broken be changed, evaluation of physical security.
IUS12 Ping sweep to find route to substation controller.	Current: Corporate firewall.	Current: None	Current: None
	Recommended: Install an IDS. Disallow all packets at the firewall that are not necessary. Isolate the network connecting the substation to the corporate office from the corporate network.	Recommended: Install an IDS to monitor for such anomalous behavior.	Recommended: Verify that all security mechanisms are in place and functioning.
IUS13 Gain access to remote substation controller monitoring computer.	Current: Physical security of monitoring computer. Corporate firewall.	Current: None	Current: None
	Recommended: Verify that any communication devices connected to monitoring computer will not answer uninitiated calls. Improve the physical security of this computer.	Recommended: Install an IDS to look for network attacks on this computer. Install a tool such as Tripwire to monitor changes to the system.	Recommended: Keep a backup image of the correct configuration of the server so the computer can be restored if compromised. Isolate the monitoring computer from the corporate network.
IUS14 Install virus/worm/trojan/logic bomb etc on remote substation controller monitoring computer.	Current: Anti-Virus software.	Current: None	Current: Manually clean up computer
	Recommended: Continued use of antivirus and implementation of an IDS to monitor computer use. Restrict the right to install software on monitoring computer.	Recommended: Continued use of anti-virus software. Monitor the intrusion detection system. Install a file comparison system such as Tripwire.	Recommended: Anti-virus system automatically delete detected virus. Intrusion detection tool automatically quarantine trojan code. Keep a backup of critical settings and programs. Reinstall as necessary. Consider having a drop-in replacement system available.
IUS15 Accidentally or maliciously send incorrect settings to substation controller. (Insider)	Current: None	Current: None	Current: Could not find any.
	Recommended: Each time ask for confirmation before update the setting, works only for accidentally send incorrect setting. Use authentication schemes so a user can be held accountable for changes they made. Use difficult passwords.	Recommended: Install an anomaly based IDS.	Recommended: Save settings each time before update, so system can roll back to previous settings. Disable the user's account who made the change. Investigate the incident to determine if the change was made maliciously.
IUS16 Gain physical access to substation controller and hook into IED to change settings.	Current: Physical security.	Current: None.	Current: Reconnect the broken communication path. Improve physical security.
	Recommended: Generate an alarm if any communication paths inside the substation are disrupted. Improve the authentication mechanism in the IED. If the IED is particularly critical, allow a secondary communication path.	Recommended: Keep track of communication times with all substation components. Try to contact any device that has not sent a notification in the expected time frame.	Recommended: switch to use the secondary communication path. Automatically notify authorities of the break-in.

TABLE III
SURVIVABILITY MAP

Intrusion Scenario	Resistance Strategy	Recognition Strategy	Recovery Strategy
IUS17 Burn out recloser by maliciously causing breaker to open at incorrect times.	Current: None	Current: Log open/close operations	Current: Replace re-closer if not working.
	Recommended: Set to default state after predetermined number of open/close operations per minute/hour/day	Recommended: Send open/close data to SCADA system and to corporate HQ as a warning.	Recommended: Preemptively replace re-closer as it nears end-of-life.
IUS18 * Coordinated shut-down/ attack on substations	Current: None	Current: None	Current: None
	Recommended: Use difficult passwords. Examine the use of devices that allow for delayed actions.	Recommended: Install a corporation wide IDS to look for anomalies that may indicate any type of coordinated attack is occurring.	Recommended: At the first sign of a coordinated attack, lock down systems that have not yet been compromised.
IUS19 Gain physical access and disconnect IED control from substation controller.	Current: Physical Security.	Current: None	Current: Reconnect the broken communication path. Improve physical security.
	Recommended: Generate an alarm if any communication paths inside the substation are disrupted. Improve the authentication mechanism in the IED. If the IED is particularly critical, allow a secondary communication path.	Recommended: Keep track of communication times with all substation components. Try to contact any device that has not sent a notification in the expected time frame.	Recommended: Switch to use the secondary communication path. Automatically notify authorities of the break-in.
IUS20 Crash IED remotely over modem or network interface.	Current: None	Current: None	Current: Manually reboot IED device.
	Recommended: Improve modem or network security. If using modems, use encrypting modems or install modem locks to make it more difficult for an attacker to connect. If using a network interface, use IPSec based security (with encryption and signatures) to make it more difficult for an attacker to connect.	Recommended: If IED is crashed, cause the substation controller to detect the lack of communication and alert the SCADA system. Install a watchdog device to detect a failure in an IED.	Recommended: When the watchdog device detects a failure in an IED, automatically trigger a reset.
IUS21 Gain physical access and locally control substation controller.	Current: Physical security.	Current: Physical mechanisms.	Current: Manually restore settings.
	Recommended: Require strong passwords for all local accesses. If the substation is particularly critical, employ multiple authentication factors.	Recommended: Install an IDS to look for abnormal accesses.	Recommended: Keep a copy of current setting each time before change setting so in case of emergency, setting can be easily restored. Update passwords.
IUS22 Gain physical access and disable connection from substation controller to SCADA system.	Current: None	Current: None	Current: Reconnect the broken communication path. Improve physical security.
	Recommended: Generate an alarm if any communication paths inside the substation are disrupted. Improve the authentication mechanism in the substation controller. If the substation controller is particularly critical, allow a secondary communication path.	Recommended: Keep track of communication times with all substation components. Try to contact any device that has not sent a notification in the expected time frame.	Recommended: Switch to use the secondary communication path. Automatically notify authorities of the break-in.
IUS23 Remotely crash substation controller.	Current: None	Current: None	Current: Manual reboot.
	Recommended: Antivirus, IPSec.	Recommended: Install an IDS to detect early probes for weaknesses.	Recommended: Reboot, bring systems online gradually. Update encryption keys.
IUS24 * Denial of service substation SCADA system.	Current: None.	Current: None. Often denial of service attacks are obvious.	Current: None
	Recommended: Use IPSec to disallow most abnormal traffic from reaching the SCADA system. In particularly critical substations, employ a second independent communication channel.	Recommended: Use an IDS to detect unusual requests.	Recommended: Update encryption keys. Switch to secondary communication channel.

TABLE IV
SURVIVABILITY MAP

Intrusion Scenario	Resistance Strategy	Recognition Strategy	Recovery Strategy
IUS25 * Overload remote SCADA controller.	Current: None	Current: None- obvious?	Current: None.
	Recommended: Use IPSec to disallow most abnormal traffic from reaching the remote SCADA controller. Use a star based communication system so the disruptive communication will only affect one communication channel. Use multiple independent communication channels to each substation.	Recommended: Install an IDS to detect when unusual requests are made of the SCADA controller.	Recommended: Switch to a secondary communication channel. Update the encryption keys.
IUS26 Hack into SCADA control/data lines and eavesdrop.	Current: None	Current: None	Current: None
	Recommended: Use IPSec (with cryptography) for communication	Recommended: None - Eavesdropping is difficult and costly to detect.	Recommended: Periodic changing of cryptographic keys.
IUS27 * Hack into SCADA control/data and falsify data or send harmful commands.	Current: None	Current: None	Current: None
	Recommended: Use IPSec (encryption and authentication) to secure communications channels to and from the SCADA device.	Recommended: Install an IDS to monitor for unusual data trends or unusual commands. Compare data from multiple substations.	Recommended: Change encryption keys. Increase the sensitivity of the IDS.
IUS28 Cut SCADA transmission line.	Current: None	Current: None	Current: None
	Recommended: In particularly critical substations, employ a second independent communication channel.	Recommended: Use an IDS to detect unusual requests. At the corporate system, keep track of when each SCADA system last checked in.	Recommended: Update encryption keys. Switch to secondary communication channel.

IX. CONCLUSION

Power substations are a critical part of the electronic power infrastructure. With the increasing use of remote control of SCADA and other substation control systems, security weaknesses have been introduced. While making it easier for engineers to finely tune the performance and respond to possible problems, this communication has introduced the problems which are inherent in any kind of network. Attacks on these resources can take many forms and can limit the ability of the station to perform its critical functionalities. A look into the security problems has shown us that the ability of the SCADA system to communicate with and respond to the input of engineers is critical to the function of a substation. Communication from the SCADA system to report the status of the substation helps to maintain a survivable powergrid. The ability of the SCADA to receive updates to settings and parameters helps it to respond quickly to problems it otherwise might not be able to fix. By identifying the critical portions of the system and analyzing their ability to resist, recognize and recover from attacks, we show that they can be made more survivable. The proposed changes to the current system all involve currently used technologies in network security. We would propose that where possible these changes be implemented in order to enhance the security of the power substations which are located through out all of North America.

REFERENCES

- [1] S. Brown, "Applying Internet Technology to Utility SCADA Systems," *Utility Automation*, Vol. 5(5), September 2000, pp. 25-26.
- [2] Taylor Carol, Axel Krings and Jim Alves-Foss, "Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening", *Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism, (SACT)*, Washington DC, November 21, 2002.
- [3] D. Dolezilek, L. M. Ayers, Using Dynamic Real-Time Substation Information to Reinvent Asset Management, Schweitzer Engineering Labs Technical Report, 2001, available online at: <http://www.selinc.com/techpprs.htm>.
- [4] Foxboro, The Foxboro Company, 2003, available at <http://www.foxboro.com/scada/power/technical.htm>.
- [5] T. Godard, R. Kelley, B. Fesmire, "Metering Automation: Beyond AMR," *Utility Automation*, Vol. 7(5), September 2000, pp. 35-42.
- [6] N. Grudin and I. Roytelman, "Heading Off Emergencies in large Electric Grids," *IEEE Spectrum*, Vol. 34(4), April 1997, pp. 42-47.
- [7] Exerpts from IEEE Power Endigeering Society, IEEE Guide for Electric Power Substation Physical and Electronic Security, IEEE, Inc., New York, NY, April 4, 2000.
- [8] ITT Industries, Flygt, March 2001. available from www.ittflygt.ca/Site/En/controls/fmc/44639.PDF.
- [9] A. Jones, "The Challenge of Building Survivable Information-Intensive Systems," *IEEE Computer*, Vol. 33(8), August 2000, pp. 39-43.
- [10] LEM Instruments Inc., QWave Light, available from www.lem.com/inet/products.nsf/.
- [11] Conte de Leon, Daniel, Jim Alves-Foss, Axel Krings, and Paul Oman, "Modeling Complex Control Systems to Identify Remotely Accessible Devices Vulnerable to Cyber Attack", accepted, *ACM Workshop on Scientific Aspects of Cyber Terrorism, (SACT)*, Washington DC, November 21, 2002.
- [12] Locamation® Control Systems, Product Guide, available from www.locamation.com/locam01/04_SubstationAutomation/Download/ProductGuide.pdf.
- [13] T. Longstaff, C. Chittister, R. Pethia, and Y. James, "Are We Forgetting the Risks of Information Technology?," *IEEE Computer*, Vol. 33(12), December 2000, pp. 43-51.
- [14] NERC web site. Available at www.nerc.com.
- [15] P. Oman, E. Schweitzer, D. Frincke, "Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems," Paper 4, 27th Annual Western Protective Relay conference, (Oct. 23-26, Spokane, WA), 2000, available from www.selinc.com/techpprs.htm.
- [16] Exerpts from P. Oman, et al., Industrial Applications of Information Security to Protect the Electric Power Infrastructure, a grant proposal funded by the NIST Critical Infrastructure Protection Program, National Institute of Standards and Technology, U.S. Dept. of Comericy, 2001
- [17] P. Oman, E. Schweitzer, and J. Roberty, Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusion, published as "Protecting the Grid from Cyber Attack," in *Utility Automation*, Part I (Nov./Dec. 2001, pp. 16-22) and Part II (Jan./Feb. 2002, pp. 25-32), available from www.selinc.com/techpprs.htm
- [18] P. Oman, Low-Cost Authentication Devices for Secure Modem and Network Connections, Schweitzer Engineering Labs Application Guide AG2001-10, 2001, available from www.selind.com/ag7.htm.
- [19] A. Riskey, C. Marlow, P. Oman, D. Dolezilek, Securing SEL Ethernet Products With VPN Technology, Schweitzer Engineering Labs Application Guide AG2002-05, 2002, available from www.selinc.com/ag7.htm.
- [20] SixNet, SiteTRAK™ Remote Site Manager, available from www.sixnetio.com/htmlhelps/datashts/sitetrak.pdf.