COMMUNICATION VULNERABILITIES AND MITIGATIONS IN WIND POWER SCADA SYSTEMS

American Wind Energy Association WINDPOWER 2003 Conference
Austin, Texas
SESSION 3B – TECHNOLOGY PERFORMANCE PART 1
MAY 19, 2003, 2-3:20 PM

William F. Young, Jason E. Stamp and John D. Dillinger
Networked Systems Survivability and Assurance Department
Sandia National Laboratories
P.O. Box 5800, MS 0785
Albuquerque, New Mexico 87185-0785

Mark A. Rumsey
Wind Energy Technology Department
Sandia National Laboratories
P.O. Box 5800, MS 0708
Albuquerque, New Mexico 87185-0708
http://www.sandia.gov/
http://www.sandia.gov/iorta/
http://www.sandia.gov/wind/

Abstract

This paper focuses on securing wind power Supervisory Control And Data Acquisition (SCADA) systems that utilize commercial-off-the-shelf Information Technology (IT). The use of IT within SCADA systems provides the benefits of low implementation cost and ease of interoperability, but introduces the potential for new security vulnerabilities. To address these new vulnerabilities in wind power SCADA systems, we apply lessons learned from our SCADA assessment activities, design and implementation experience in secure communication systems, and knowledge of wind power operations. We present a SCADA security policy framework and provide two IT "best practices" examples. We also list several typical SCADA/IT vulnerabilities. To provide further reading into the many facets of securing SCADA/IT, an extensive list of references has been provided.

Acronyms

CD	Compact Disk	IEC	International Electrotechnical Commission
COTS	Commercial Off The Shelf		
DHCP	Dynamic Host Configuration Protocol	IEEE	Institute of Electrical and Electronics Engineers
DMZ	Demilitarized Zone		
DVD	Digital Versatile Disk	IP	Internet Protocol
FTP	File Transport Protocol	IPSec	Internet Protocol Security
HTTP	Hypertext Transfer Protocol	ISO	Independent System Operator
HTTPS	Hypertext Transfer Protocol Secure	IT	Information Technology
		LAN	Local Area Network

MAC	Media Access Control
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PC	Personal Computer
PLC	Programmable Logic Controller
PSS	Physical Security System
POTS	Plain Old Telephone Service
RF	Radio Frequency
RTU	Remote Terminal Unit
SANS	System Administration, Networking and Security
SCADA	Supervisory Control And Data Acquisition
SSH	Secure Shell
SSID	Service Set Identifier
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy

Introduction

The strategically distributed nature of wind power presents unique challenges. Generation is not centralized, generally remote, sometimes offshore, and often covers large geographic areas. These factors usually require a variety of networked interconnections and telecommunication technologies for monitoring and controlling wind power electric generating facilities utilizing SCADA technology. Compromising a SCADA system can lead to a number of undesirable consequences, such as disruption of operations, asset availability, asset misconfiguration (circuit protection), loss of data and confidentiality, loss of consumer confidence, or unsafe conditions. Since current SCADA systems utilize IT, wind turbine/farm designers, purchasers, and providers should incorporate current IT "best practices" in securing SCADA systems.

This paper discusses a strategy for securing wind power SCADA systems. A well-developed security policy serves as the center point of our approach. This security policy guides the integration of technology and the development of security procedures. The SCADA vulnerabilities listed in this document are attributable to the lack of a well-developed and meticulously practiced security policy. Even though this paper focuses on the wind power industry, our security strategy applies to any SCADA system.

The main body of the paper proceeds as follows. The **Wind Power SCADA Systems** section provides examples of current technology and communication architectures used in wind power SCADA systems. Next, we introduce the framework for a SCADA security policy and provide two examples on how the policy relates to practical implementation in the **Security Approaches** section. Third, the **SCADA Vulnerabilities** section contains a list of some potential vulnerabilities in wind power SCADA systems to help designers, administrators, and operators identify potential problems in their own systems. Finally, the **Security References** section indicates where additional security information is available.

Wind Power SCADA Systems

The utilization of COTS IT represents the current trend in SCADA system implementation. COTS IT includes operating systems such as Windows, UNIX, or Linux, and common network devices like Ethernet routers, switches, and hubs. Wireless specific COTS technology includes

the use of IEEE 802.11 and Bluetooth™ standards. While the usage of COTS IT does provide some significant benefits such as low implementation cost and ease of interoperability with other information systems, a SCADA system inherits a variety of security vulnerabilities when incorporating COTS IT. Wind power SCADA systems can be made secure, however, due to the ever changing IT environment, maintaining sustainable security must be considered an ongoing process. In Figure 1, we depict an example SCADA system configuration used to monitor and control wind power electric generation.

The six items in Figure 1 instrumental to SCADA security are (1) the use of wireless bridges to communicate with wind turbines, (2) the connection of a wireless bridge to Ethernet hub/switch, (3) the connection between the SCADA control center Ethernet switch/router and 3rd party and administrative networks through a firewall, (4) modems attached to the main SCADA control center server and the wind farm server, (5) the Internet connection to the substation, and (6) the connection to non-SCADA types of data, e.g. PSS data. These particular features are extremely important when one tries to assess the vulnerability of a SCADA system, and when designing mitigations. Vulnerabilities related to these specific aspects of the system are listed in the **SCADA Vulnerabilities** section, Table 4.

The different types of connection media in Figure 1 include fiber optic, copper wire twisted pair, and two wireless technologies, microwave and bridged wireless (e.g. IEEE 802.11 in bridging mode). Wireless LAN configurations (i.e. wireless clients and access points), and direct wireless interfacing to the RTU/PLCs via IEEE 802.11 or Bluetooth™ are not shown to minimize the complexity of Figure 1, but represent emerging technologies present in some SCADA systems.

Security Approaches

SCADA security begins with policy. In this section, we describe the framework of a security policy. We describe some important aspects in developing this policy, such as data characterization and definition of the SCADA perimeter. In addition, we provide a generic policy framework to assist in the policy creation. After the policy framework, we provide detailed implementation considerations in two specific areas, connections to other systems and wireless bridging.

SCADA System Characterization

Policy depends on system characterization. The definition of data types is the first step. Data types are based on where and how the data is used, and which personnel need access to that data. Typical data types include SCADA monitor, SCADA control, SCADA historical, maintenance, prototype testing, network administration, engineering, and non-SCADA data for physical security monitoring (e.g. PSS). The next step is the identification of data flows, which are determined by the personnel and applications using the data, and include details such as source, destination, storage locations, and communication paths. Identification of data flows helps determine the appropriate type and placement of security mechanisms. For example, in Figure 1, the PSS data could flow through the Ethernet hub/switch in the remote control center, over the Internet, to the administrative network, through the Ethernet switch/router, and to the SCADA server. Figure 1 also depicts two firewalls in this path, which may not be present in an actual system, or may provide inadequate data filtering and network protection.

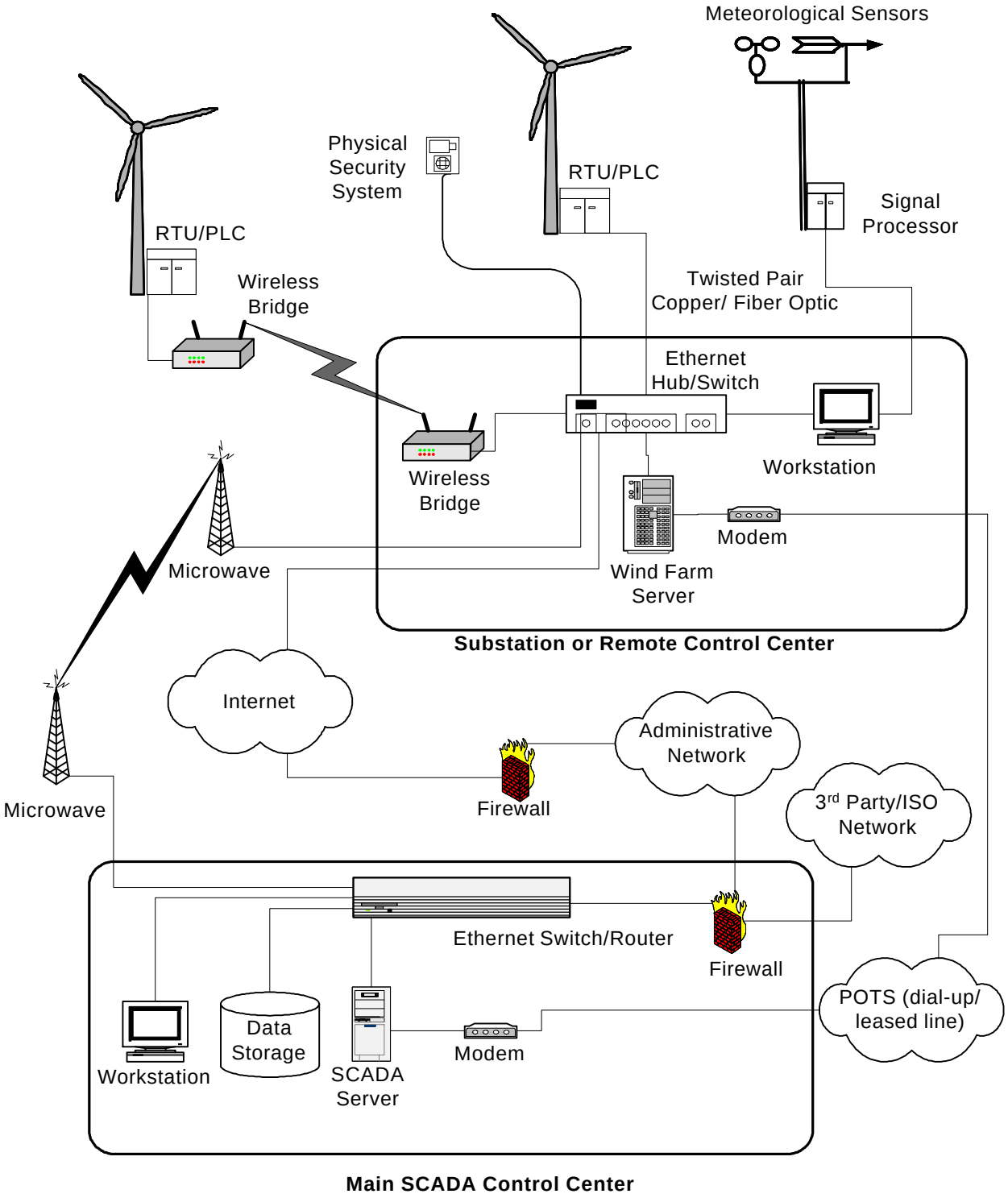

Figure 1 EXAMPLE SCADA SYSTEM FOR WIND POWER ELECTRIC GENERATION

In addition to data characterization, a perimeter of the SCADA system must be defined to ensure the security design covers all critical elements and does not negatively impact other systems, such as an administrative network. In Figure 1, obvious boundaries to the SCADA system occur at the interface between the firewall and the administrative and 3rd party networks. Less obvious boundaries occur where the wireless bridges and the microwave antennae interface with the atmosphere. Controlling RF access is impractical, if not impossible.

Generic SCADA Security Policy

Figure 2 depicts our SCADA Security Policy Framework™ [1]. Important features include the hierarchal structure of the policy framework, which allows the development of detailed utility specific sub-policies to support generic higher-level policies. It is our experience that this hierarchal structure improves the policy creation process by providing traceability while partitioning the problem into manageable pieces.

The "SCADA System Security Policy" represents the complete document. At the first level, eight boxes represent primary categories within the policy, which we consider applicable to any utility. The levels below the boxes provide additional detail on the specific elements within those eight boxes. For example, under the category of "SCADA Network Security Policy" the second level of detail consists of "LAN Policy" and "Perimeter Policy." Elements of the "Perimeter Policy" at the third level include "Intranet Access Policy," "Remote Access Policy," and "External Networks/3rd Party Access Policy."

The security policy framework in Figure 2 provides varying degrees of coverage at the three levels. At the first level, the eight boxes are intended to provide complete coverage. The first level breakdown attempts to delineate the overall SCADA policy in an intuitive and useful manner. While a utility is not restricted to this specific delineation, the breadth of coverage should be equivalent to the first level in Figure 2. The second and third levels are not comprehensive as shown in Figure 2, with the rectangles representing sample elements.

At the second level, rectangles, we depict some of the sub-policies supporting the initial eight. The details at this level are site specific, and must be developed for a particular SCADA system. For example under the "SCADA Network Security Policy," the diagram only includes "LAN Policy" and "Perimeter Policy." This might suffice for a simple SCADA network, consisting of only a LAN segment, but a larger network may utilize WANs. In this case a "WAN Policy" would also be an element at the second level. Table 1 provides examples of security items addressed in the "SCADA Network Security Policy," with the corresponding level in the policy hierarchy. Three sources that contain textual examples of security policy content are listed in the ***Security Policy*** part of the **Security References** section.

The third level in Figure 2, grayed rectangles, includes a finer granularity than the second level policies. As in the case of the second level, the elements depicted in Figure 2 serve as examples for guiding the security policy development of a particular utility. Descriptions at this level are the narrowest in scope of the three levels. Note: the bold-bordered rectangles represent items covered in the ***Implementation and Technology Considerations*** section.

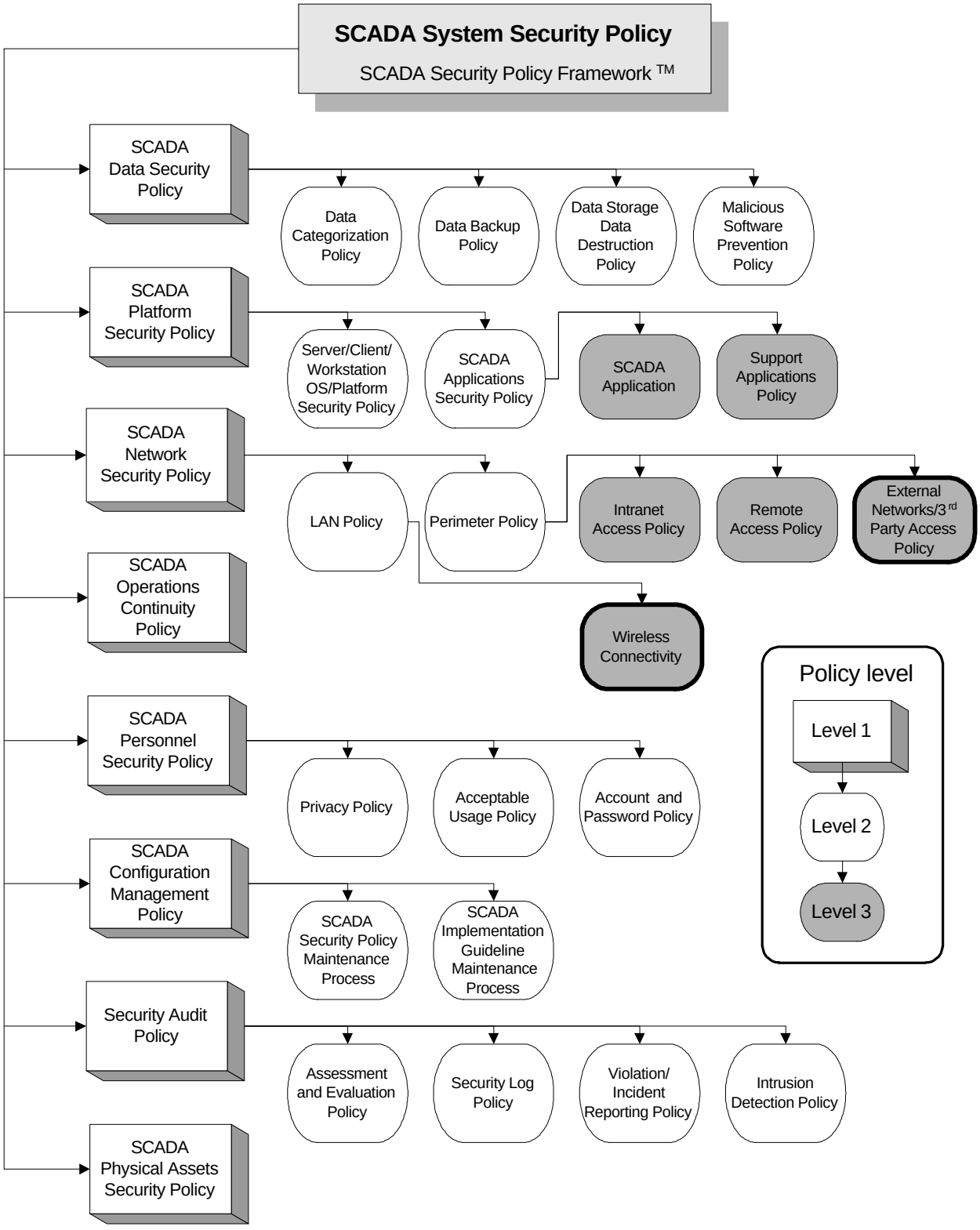

Figure 2 SCADA SECURITY POLICY FRAMEWORK™

Table 1 ITEMS COVERED IN AN EXAMPLE LAN SECURITY POLICY

SCADA Network Security Policy (Level 1)
LAN Policy (Level 2)
o Implement private IP address space for SCADA o Hardware and software will be installed on the SCADA system after authorized by configuration management and malicious software policies. o Data can traverse trusted internal SCADA networks unencrypted. o What is allowed: SCADA operations o What is not allowed: Internet/Surfing, Personal Software, Email
Wireless Connectivity (Level 3)
o Wireless LANs are not allowed as part of the SCADA network (i.e. no clients and access points). o Wireless bridging is allowed. o Strong encryption must be applied to SCADA data traversing wireless links. o Strong authentication between the Control Center and remotes should be applied. o Address and protocol filtering must be applied at all wireless interfaces.

Several important system aspects to consider when creating a security policy include the breadth of coverage, level of detail, traceability, and consistency with available technology and operating procedure. Developers should consider these aspects when creating a SCADA security policy; otherwise the policy will lead to an ineffective implementation of security mechanisms, processes, and procedures. A poorly developed security policy can adversely affect normal operations, or generate a false sense of security. Careful development of a security policy is vital to achieving robust and maintainable security. It is important to remember site-specific operations will affect the specific details of the security policy, so a policy written for one SCADA system will probably not directly apply to another system. However, major similarities between sections of the policies are likely.

Implementation and Technology Considerations

A well-developed security policy, outlined in the previous section, provides implementation guidance and selection criterion for technology, in order to reduce the security risk in a SCADA system. In order to demonstrate how the security policy relates to the system architecture and to the configuration of devices, we address two particular security implementation challenges: (1) connection to 3rd party and administrative networks and (2) bridged wireless communications.

Connections to External Networks

An external network is any network that is not part of the SCADA system. Examples include interfaces to the utility's administrative network and 3rd Party connections, either to other SCADA systems for information transfer or mutual control or to ISOs to facilitate power trading and grid management. Often, interfaces to external systems assume that the outside network can be trusted, which means that SCADA security is dependent on one or more organizations. These interfaces must either be eliminated (if possible) or be replaced with secure data flow mechanisms, and the SCADA system must be insulated from the potential effects of unauthentic data from the external network. The data that must be transferred should be pushed from the

SCADA network to the external network in a secure fashion. No machine residing on the SCADA network may connect directly to the business network.

Utilities often connect their SCADA systems to their business systems to facilitate the transfer and viewing of data collected by the SCADA. The data can have billing, warranty, maintenance, or other significant purpose, and may be required or requested at regular short intervals. Because of the differences in administration possible between the utility business network and the SCADA network, and the enhanced criticality of the SCADA network relative to the business network, it is important this connection be made secure. Specifically, the SCADA network must treat the business system as an untrusted network.

There are two effective ways to implement a secure connection for the purpose of data transfer from the SCADA network to external networks. The first and easiest method is through shared computer storage media (e.g. floppy disk, CD, DVD). The second method involves securely connecting the SCADA network to intermediate platforms, which service requests from clients on enterprise networks to effectively create a one-way data connection. Figure 3 illustrates a method to secure connections to enterprise networks.

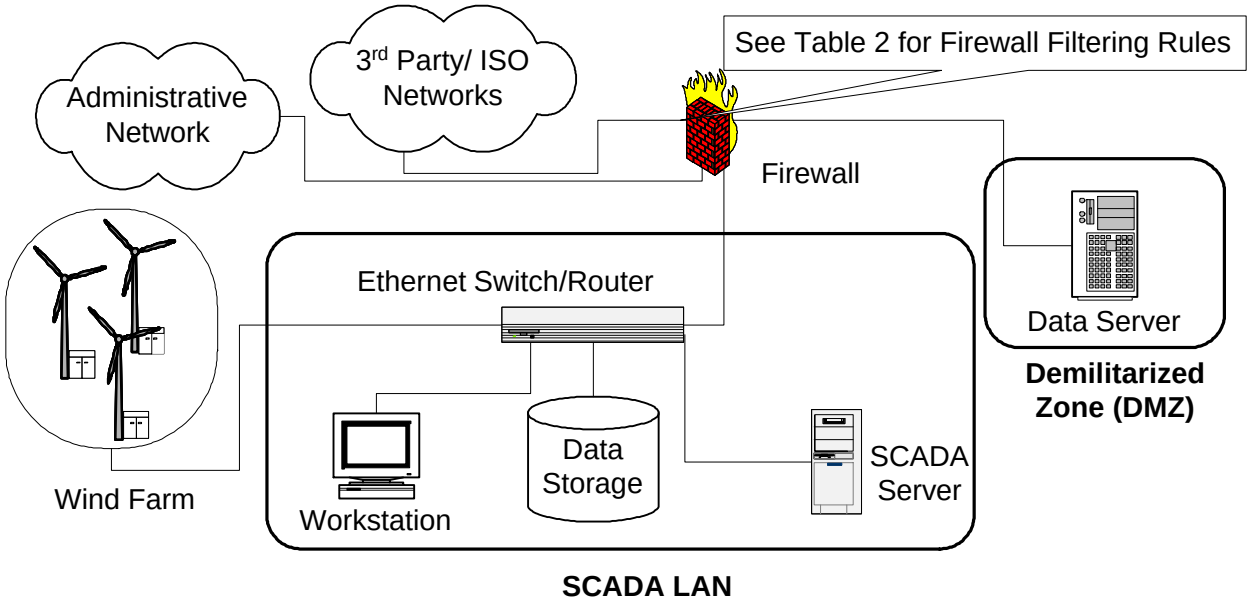

Figure 3 CONNECTIONS TO OTHER NETWORKS VIA A DMZ

The recommended system consists of a data server located in a DMZ behind a firewall. Carefully configured routers might be used instead of firewalls since filtering rules can provide adequate protection, although a firewall is recommended. The effectiveness of this solution will degrade drastically if the firewalls permit any traffic that is not required for this connection.

The data server platform in the DMZ acts as a repository for SCADA data that has been pushed onto it via connections initiated from the SCADA network. The DMZ data server allows data to

be read from its repository only by platforms on the external network. In this configuration, no machine that can initiate a connection to the SCADA network is visible to the external network. The firewall implements the configuration rules listed in Table 2.

Table 2 FIREWALL CONFIGURATION RULES

Connection Path	Firewall Configuration Rules
SCADA network to DMZ	Connections may be initiated from the SCADA network to a specific port or ports on the DMZ data server only.
External network to DMZ	Connections may be initiated from addresses on the external network to a specific port or ports on the DMZ data server only.
DMZ to SCADA network or external network	Connections may not be initiated from the DMZ to any other network. Only externally initiated data connections either to the external or SCADA networks are permitted.
External network to/from SCADA network	No direct connections allowed.

SCADA network administrators should manage the firewall in coordination with the external network so that security is achieved while meeting business objectives. Also, the firewall needs to be physically and logically secure (e.g. no telnet, FTP, SNMP, etc.). The data server in the DMZ should be configured as a bastion host, allowing only the required file services, and the rules above will require optimization for each particular implementation. A bastion host is the only computer allowed to be addressed directly from the external network and is designed to screen the rest of the SCADA network from security exposure.

Bridged Wireless Communications

Wireless technology offers an inexpensive and flexible communication solution for SCADA systems. [2] However, wireless technology also presents significant security challenges. Modern SCADA systems can utilize wireless technology in a variety of locations, such as wireless LANs in the control network, wireless interfacing to the RTU/PLCs, and wireless connectivity between remote sites or LAN segments (commonly referred to as wireless bridging). The bridged wireless link shown in Figure 1 depicts a common instance of wireless communication. We will address only wireless bridging in this section, focusing on IEEE 802.11 technology since it provides an increasingly popular means of communication. (Bluetooth™ is not intended for bridging type connections.)

Securing wireless links in a network is a very difficult problem due to the amount of device management traffic needed between wireless devices to establish and maintain the communication channel. This communication channel supports the transfer of user data (SCADA control, monitoring, historical, administrative, etc.). The security of this channel relies on a combination of security mechanisms and device configurations. In Figure 4, we show a VPN tunnel between the wind turbine and substation. The VPN could also be used between the remote substation and the main SCADA control center.

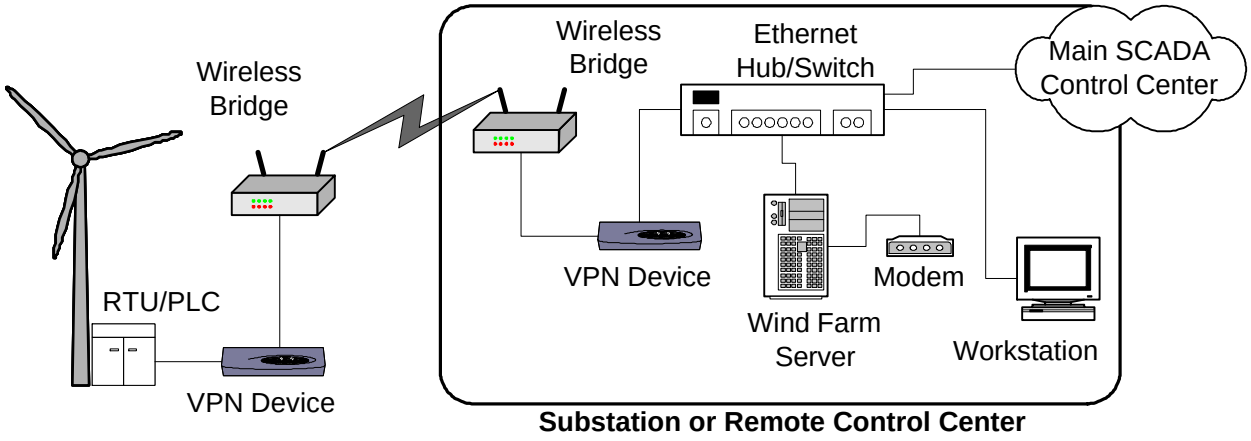

Figure 4 WIRELESS BRIDGE NETWORK WITH VPN DEVICES

The VPN devices encrypt/decrypt the user data that traverses the wireless link, and create a protected tunnel for the user data. These devices should only allow connections with other authorized VPN devices on the network, and should not support any additional network services, such as telnet and SNMP. Devices implementing IPSec offer a strong cryptographic solution for the creation of this VPN. In addition to utilizing VPN devices, the wireless bridges must be configured securely to prevent unauthorized or malicious users from accessing the network. Current security methods available on most IEEE 802.11 wireless devices operated in bridging mode are not robust (e.g. WEP without dynamic key updates). While the encrypted tunnel depicted in Figure 4 protects the user data, the device management traffic between the wireless bridges is not protected because this data exists outside of the encrypted tunnel.

Securing the wireless bridges and the VPN devices is important to the overall security of this communication path. Wireless bridges offer a range of security features, such as MAC filtering, administrator password protection, and the ability to disable unnecessary services. Currently, many wireless network devices provide limited, if any, security protocols (e.g. SSH), for protecting the device management traffic. We provide guidelines to securing or hardening the wireless bridges in Table 3.

Additional filtering can be applied at the Ethernet switches/routers to provide a level of redundancy in case of a misconfiguration or a security failure in either the VPN devices or the filtering at the wireless bridges. If the VPN devices encapsulate the data, the Ethernet switches/routers, which reside outside of the encrypted tunnel, can filter the unencrypted data flow based on original source and destination addresses. However, the total series of filters must not introduce a delay in the data flow that adversely impacts the SCADA operations.

As manufactures of wireless devices begin to deploy IEEE 802.11i, the emerging IEEE wireless security standard, a VPN security solution will likely not be necessary. However, suggestions such as filtering MAC addresses, still provide some level of security backup, and are worthwhile to include in the overall system design. In addition, legacy wireless devices will likely not support IEEE 802.11i. The physical security of the devices is important because physical access

allows the attacker to either bypass or disable most, if not all, of the security mechanisms. Remotes sites, as in most wind power applications, are often difficult to secure, and thus a Security Policy that includes monitoring of traffic flows, particularity between sites, will help efforts to identify and isolate the problem. Finally, some denial-of-service vulnerabilities, such as RF interference, still exist if all the previously mentioned security mechanisms are utilized.

Table 3 GUIDELINES FOR SECURING WIRELESS BRIDGES

Access Control/ Filtering

- ⇒ Allow only MAC address of bridges used in the network to communicate
- ⇒ If possible, restrict IP ports to only those used by the encrypted tunnel

Wireless Device Management

- ⇒ If possible, use a secure interface to manage the device, such as HTTPS or SSH
- ⇒ Disable FTP and/or TFTP
- ⇒ Disable SNMP
- ⇒ Disable telnet
- ⇒ Disable the HTTP interface (via a console interface) upon completion of device configuration. (This assumes a web browser is used to configure the device.)

Note: Services enabled for device configuration should be disabled during normal operations.

Device Configuring

- ⇒ Change the SSID from the default to something non-obvious
- ⇒ Disable beaconing from the bridges (Manually load the SSID in allowed bridges.)
- ⇒ Assign IP addresses statically, and disable DHCP

Event Logging

- ⇒ Log important events such as account logins, packets dropped due to filtering, etc.
- ⇒ Review logs on a regular basis, as established by the Security Audit Policy

Note: Make sure items logged are not excessive or impact SCADA operations.

Physical Security

- ⇒ Provide two layers of physical protection, such as a locked building and a locked equipment cabinet.

SCADA Vulnerabilities

Cyber security engineering is expensive. However, the presence of vulnerabilities requires it. In this section we list vulnerabilities we typically see in SCADA systems. The order in the list of vulnerabilities does not reflect a priority in terms of likelihood of occurrence or severity of impact. Typical vulnerabilities in SCADA systems are listed in Table 4. The vulnerabilities are grouped in the categories (1) policy/procedure/configuration management, (2) system, (3) network, and (4) platform to assist in determining how to provide the best mitigation strategy. A given SCADA system usually only exhibits a subset of the list in Table 4, but may also have some unique system specific vulnerabilities.

Table 4 TYPICAL VULNERABILITIES IN SCADA SYSTEMS

Policy/Procedure/Configuration Management

- ⇒ The SCADA system has no specific documented security policy or security plan.
- ⇒ There is no formal configuration management and no official documented procedures. Hence, there are neither formal requirements, nor a consistent approach of configuration management.
- ⇒ There is neither formal security training nor official documented security procedures.

System

- ⇒ Sensitivity levels for SCADA data are not established, making it impractical to identify which communication links to secure, databases requiring protection, etc.
- ⇒ No security perimeter has been defined for the existing system that defines access points to the system that should be secured.
- ⇒ Physical security alarms reside on the SCADA system; hence, a failure in the SCADA system affects the integrity of the physical security.
- ⇒ Critical monitoring and control paths are not identified, in order to determine necessary redundancy or contingency plans.

Network

- ⇒ Dial-up access exists on individual workstations within the SCADA network.
- ⇒ The dial-up access into the SCADA network utilizes shared passwords and shared accounts.
- ⇒ Administrative and SCADA networks utilize the same IP subnet. (This removes the possibility to implement extranets, data diodes, filtering, etc.)
- ⇒ Inadequate data protection exists as the SCADA data traverse other networks, both as data is transferred to other SCADA segments and as the data is sent to servers on the administrative network. The data is used for a variety of purposes, including public display and engineering efforts.
- ⇒ Wireless bridging used without strong mutual authentication and/or data integrity protection on supported data flows.
- ⇒ Wireless LAN technology used in the SCADA network without strong authentication and/or data protection between clients and access points.
- ⇒ There is inadequate physical protection of network equipment.
- ⇒ There is no security monitoring on the SCADA network.

Platform

- ⇒ Default OS configurations are utilized, which enables insecure and unnecessary services.
- ⇒ There is no regular virus checking.
- ⇒ A PC is allowed connection to both the SCADA network and the Internet.
- ⇒ There are no time limit, character length, or character type requirements for the passwords.
- ⇒ OS security patches are not maintained as part of a formal procedure of process.

As pointed out in the beginning of the paper, we are focused on system level vulnerabilities, not point security problems, such as physical security or a particular protocol like WEP or SNMP. A well-developed security policy balances operational performance and security requirements, and

is necessary for sustained security. This security policy also guides the integration of technology and the development of security procedures. Again we iterate all the SCADA vulnerabilities discussed in this document are attributable to the lack of a well-developed and meticulously practiced security policy.

Security References

Several documents we reference in this section provide insights into system level security ([3], [4], and [5]). However, detailed SCADA-specific security documentation is limited. Since SCADA systems utilize IT infrastructure and corresponding architectures, security solutions from the IT community often apply to the new SCADA environment. This section lists some useful texts in the areas of (1) security policies, (2) network security (both wireless and wired), and (3) platform security. Additional sources are available and we are not endorsing these texts and documents as better than others available. We are merely seeking to provide the reader with an initial and reasonably comprehensive coverage of the important aspects of information security applicable to modern SCADA systems. Also, see [6] and [7] for real-world cryptography applications. Note: Users of these references must be aware they are solely responsible for undesirable impacts on systems implementing any of these recommendations.

Security Policy

These texts provide much more textual detail on cyber security policies. The additional detail should be used in conjunction with the framework in Figure 2 to create a security policy. Note: *Information Security Policies Made Easy* should be used as example text to facilitate the creation of a security policy, and should not be copied directly.

1. *Information Security: Protecting the Global Enterprise*, Donald L. Pipkin: May 2000.
2. *e-Commerce Security -- Enterprise Best Practices.* Published by the Information Systems Audit and Control Foundation. www.isaca.org. 2000. Deloitte & Touche,
3. *Information Security Policies Made Easy*, Charles Cresson Wood, 9th Edition. http://www.netiq.com/products/pub/ispme.asp.

Network Security

The following texts provide guidance on how to create a secure network, and contain discussions on threats, network device configurations, cryptographic solutions, and secure network architectures. Although some coverage of security polices and platform security is provided, the primary focus is on the networking technology.

1. *Designing Network Security*, Merike Kaeo. [7]
2. *Wireless Security End to End™*, Brian Carter and Russell Shumway, © 2002, Wiley Publishing, Inc.

Platform Security

Along with network devices, the configuration for operating systems used in SCADA systems holds the greatest opportunity for both insecure implementations and corresponding vulnerabilities. These vulnerabilities can include unnecessary network services, shared accounts and/or weak passwords, insufficient logging, etc.

Following are references to several documents that include checklists and specific recommendations to harden operating systems. However, administrators must be aware that invoking any checklist without clear requirements and a relevant policy will eventually lead to security failure. A security policy must be in place for staff to design and implement a successful and enduring security program.

1. *60-Minute Network Security Guide (First Steps Towards a Secure Network Environment)*, National Security Agency: October 2001. http://nsa1.www.conxion.com/support/download.htm
2. *Hackers Beware: Defending Your Network from the Wiley Hacker*, Eric Cole: (Hackers Beware is an authorized text of the SANS Institute), August 2001.

Additional Cyber and Wind Power SCADA Security Resources

1. NIST Computer Security Resource Center. http://csrc.nist.gov
2. System Administration, Networking, and Security (SANS) homepage. http://www.sans.org
3. IEC 61850 (Communication networks and systems in substations) http://www.scc-online.de/; http://www.nettedautomation.com/index.html
4. IEC 61400-25 (Communication standard for control and monitoring of wind turbine plants) http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=2199

Conclusion

The generation of electricity from wind power is quickly becoming a viable electric utility option; these systems require robust and secure SCADA systems. Since modern SCADA systems utilize IT infrastructure and corresponding architectures, as well as COTS IT technology, wind turbine/farm designers, purchasers, and providers should incorporate current IT "best practices" in securing SCADA systems.

Security of these SCADA systems requires a comprehensive approach, not simply the application of security technology. The starting point is the creation of a SCADA specific security policy, based on data characterization and an established SCADA perimeter. A well-developed policy will guide technology selection and implementation. An effective policy balances operational performance and security requirements. Wind power SCADA systems can be made secure, however, due to the ever changing IT environment, maintaining sustainable security is an ongoing process.

Acknowledgements

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000. This paper is declared a work of the U. S. Government and is not subject to copyright protection in the United States.

References

[1] Trademark of Sandia National Laboratories.

[2] *Wireless Solutions For Supervisory Control Systems*, Thomas L. Frobase, ***Pipeline & Gas Journa***l, March 2001.
http://www.oildompublishing.com/PGJ/pgj_archive/March01/wireless.pdf

[3] *SCADA Security Strategy*, Jonathan Pollet, PlantData Technologies, August, 2002.
http://www.plantdata.com/SCADA%20Security%20Strategy.pdf

[4] *Protecting SCADA and the Vital Energy Infrastructure*, Vigilinx Digital Security Solutions.
http://www.packetnexus.com/docs/secdos/50722_White_Paper-SCADA.pdf

[5] *IT Security for Industrial Control Systems*, Joe Falco, Keith Stouffer, Albert Wavering, and Frederick Proctor, National Institute of Standards and Technology.
http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf

[6] *Designing Network Security*, Merike Kaeo, © 1999 Macmillan Technical Publishing, Inc.

[7] *A Survey of 802.11a Wireless Security Threats and Security Mechanisms*, Colonel Donald J. Welch, Ph.D. and Major Scott D. Lathrop, A Technical Report to the Army G6.
http://www.itoc.usma.edu/Documents/ITOC_TR-2003-101_(G6).pdf