System Threats and Vulnerabilities

An EMS and SCADA Security System Overview

by Thomas Kropp

©COMSTOCK

1540-7977/06/$20.00©2006 IEEE

THE GOVERNMENT, THE PRESS, AND INDUSTRY HAVE EXPRESSED CONCERN regarding the security of the information networks used to communicate with supervisory control and data acquisition (SCADA) and distributed control systems (DCS) applications (which are referred to as *SCADA applications* in this article). Much of the discussion has dealt with encryption techniques and the timing issues associated with the real-time aspects of these types of systems. Other initiatives to enhance the protocols for the overlaying communication networks continue to be addressed. Additional studies also include user and data verification and authentication strategies. Many of these initiatives require the adoption of new standards before any type of global solutions can be implemented.

While planning for the future is important, we cannot forget that today's installations have vulnerabilities through commonly deployed communication channels. These vulnerabilities are escalating due to the increased adoption of open system concepts within specific vendor SCADA solutions, the use of the Internet as a communications channel, and the increased integration of common TCP/IP protocol-based corporate communication networks with SCADA applications. This trend is amplified by the increasing need to link real-time data generated by SCADA applications with business systems to complement the decision-making activities and optimize the day-to-day business processes of the company.

To compound our problems, it is becoming easier to break into computer systems due to the increased availability of common hacker tools on the Internet, and the technical knowledge required to impact significant damage to underlying application systems is decreasing. This scenario, in recognition of the increased use of TCP/IP network-based communications in the SCADA architectures, spells danger for these highly critical applications. When we recognize the availability of technical information regarding the proprietary design of SCADA applications on the Internet, we further appreciate the vulnerabilities to these applications.

There are literally thousands of threats, from viruses to password-cracking algorithms, which can be employed to exploit vulnerabilities in the corporate network and common application systems. Derivatives of these threats are generated daily in the hacker communities. When it comes to securing critical SCADA applications and their associated databases, it is essential that threats generated by these types of individuals be addressed completely, both from a corporate network and SCADA control system network source perspective.

The good news is that countermeasures are available using today's technology that are capable of mitigating many of the risks associated with these kinds of threats. The purpose of this article is to present a high-level view of the security concerns for SCADA and control systems.

Terminology

A *threat* is a person, thing, event, or idea which poses some danger to an asset and/or organization in terms of that asset's confidentiality, integrity, availability, or legitimate use. An *attack* is an actual realization of a threat. *Safeguards* are physical controls, mechanisms, policies, or procedures that protect assets from threats. *Vulnerabilities* are weaknesses in a safeguard or the absence of a safeguard. *Risk* is a measure of the probability of a successful attack and the consequences of that successful attack. Therefore, high risk implies both a high probability of a successful attack and significant consequences of a successful attack. *Countermeasures* are those actions which can be taken to avoid or minimize the risk of attacks.

From a utility operations standpoint, the term *information* is used to include not only data that can be viewed by humans but also to data that is used as input to applications and output from applications, some of which can control other applications. In utility operations, these controllable applications can directly affect the electric power grid.

History

Before deregulation, electric power utilities operated information networks for both business and operational functions. Deregulation has resulted in the distribution of information functions

from what was a vertically integrated company of generation, transmission, and distribution assets. This has directly impacted the operation of the data networks and their security. Under the regulated model, it was clear that the responsibility for assuring stable grid operation and secure communications was the responsibility of the integrated utility. After deregulation, there is a separation of control from the utility with more responsibility consolidated in control areas. This has required an increase in the need for computer systems to control the energy flow and an increase in the transmission of grid reliability and market data. Utilities now interconnect to multiple agencies for data exchange and power system coordination. The power system scheduling function is a major driver for authentication and nonrepudiation of market actions and grid operations; see Figure 1.

Systems deployed prior to deregulation were designed to be efficient and possessed minimal processing power, relatively small memory capacity, and unsecured communications capabilities. These were very adequate designs for the times, and, indeed, many are still performing as intended. These systems were designed, however, without considerations for security, and their processors, memory, and communications capabilities do not readily allow for the addition of security as a retrofit functionality.

Modern Trends

Several trends have led to an environment in which the security of SCADA systems has become more critical. The main trends are

1) the use of common operating systems, such as Microsoft Windows and Unix, in SCADA and control systems platforms
2) the increased use of TCP/IP communications
3) the demand from corporate users for operational data on a near-real-time basis.

This article will not attempt to address each of these in depth, but it is important to understand the ramifications of these trends.

Common Operating Systems

The use of common operating systems enables efficiencies for both the vendor and for the end user. The vendor no longer needs to develop proprietary operating systems for their equipment, and the end user can now maintain the same operating system for both corporate and operational systems. The downside to this is that operational systems built on common operating systems inherit all of the same vulnerabilities as their corporate brethren. For example, if malware is released that attacks Windows or Linux systems, then operational systems built on Windows or Linux are also vulnerable to that malware.

The situation is complicated because many of the commonly used techniques to protect corporate workstations are difficult to apply to operational systems. Patch management, for example, is problematic for at least two reasons.

1) Installation of patches often requires systems to be restarted, which may not be an option for a critical control system.

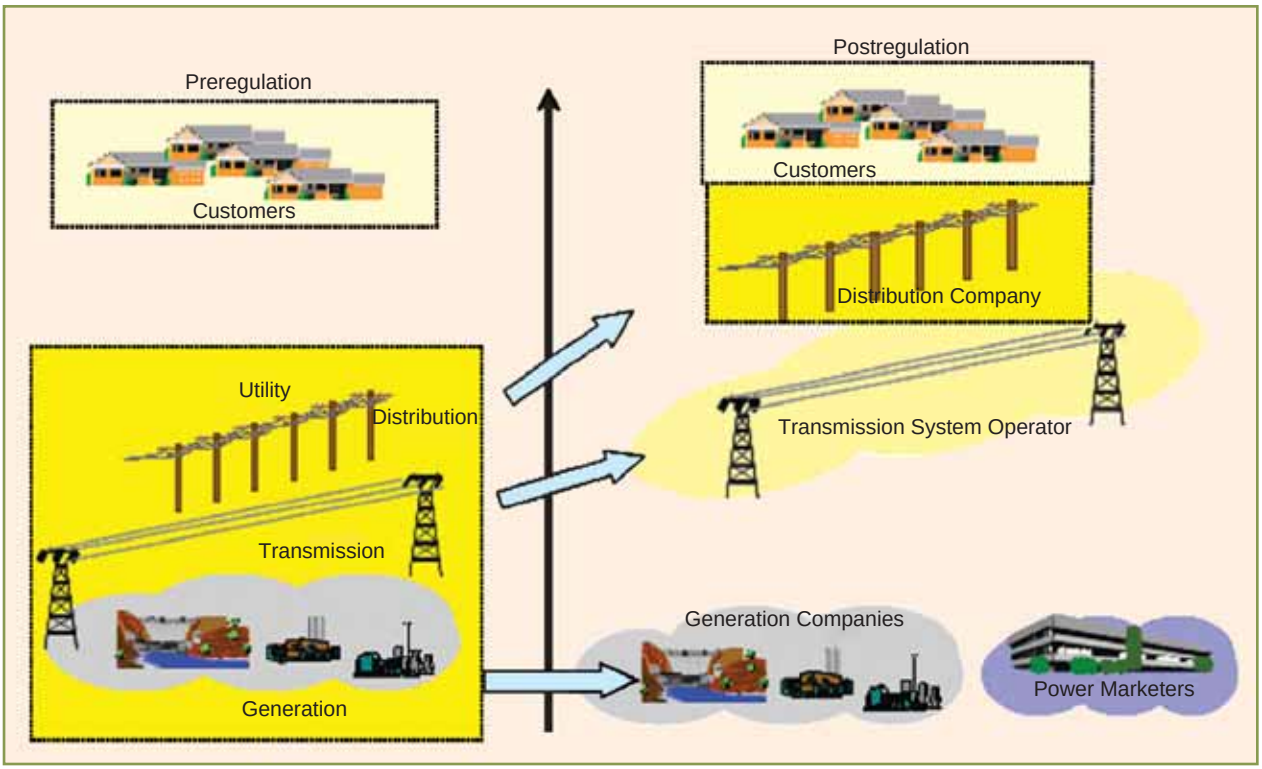

figure 1. Then and now.

2) Patches may cause critical control applications to fail and, hence, cannot be applied until thorough testing is performed by the control application vendor and the end user. This adds significantly to the time required to apply the patch and leaves a large window of vulnerability for potential intruders (attacks against known vulnerabilities are typically released within a few days of a vulnerability being discovered).

Another technique used to protect corporate systems is to deploy antivirus and intrusion detection tools. While these can be applied to operational systems, they provide unique challenges, primarily due to the computational resources required to analyze files for viruses and to update signatures for these tools. For example, virus signatures are typically updated daily. The update process has a significant impact on operational systems, delaying their response while the update is in progress.

Use of TCP/IP

TCP/IP allows a much richer communications environment than serial communications protocols do. As with common operating systems, it also provides commonality with the communications protocols used in the corporate network. This allows economies of scale in support of these communication networks. It also opens the operational networks to the same vulnerabilities as the corporate networks and, in particular, enables attacks from the Internet. The same problems noted in the section on common operating systems apply to TCP/IP.

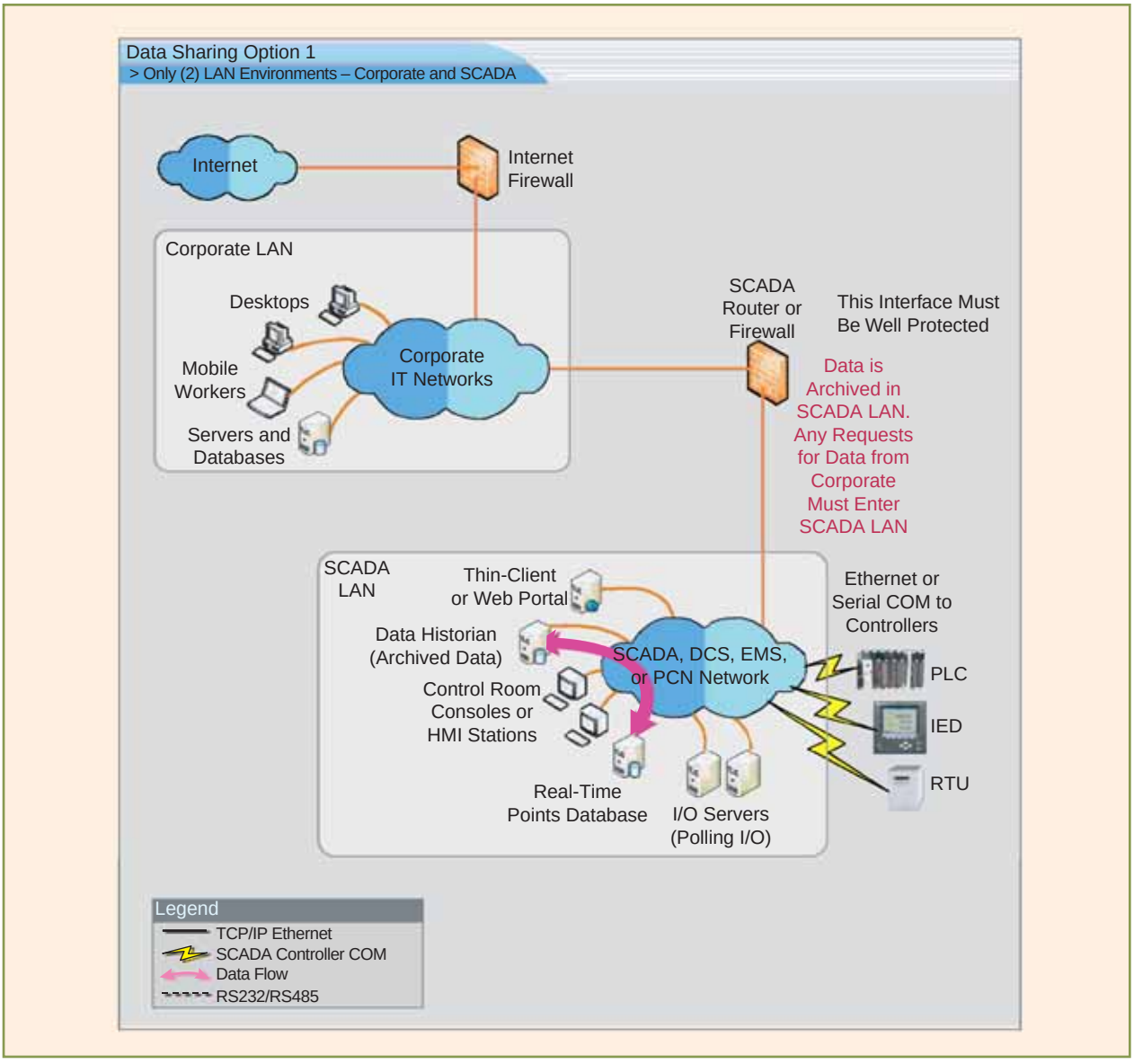

figure 2. Corporate-operational network connections.

Corporate Demand for Near-Real-Time Data

In many utilities, business requirements have driven the need to connect business and operational networks to provide near-real-time access to operational data. It is not a trivial exercise to configure the interface between operational and business networks so that appropriate access is facilitated while unauthorized access is denied. All connections should be thoroughly validated as meeting a genuine business need. See Figure 2.

Threats

Threats to the correct functioning of the electric power system come from both natural and human causes. Human causes come from a variety of sources, ranging from novices who are experimenting with intrusion techniques to malicious activities of criminals or extranational, covert operatives. Criminal activities include attempts by competitors to obtain sensitive business information as well as the activities of criminal organizations. One of the concerns among security experts is that an attack upon the SCADA or control system communications network could be coupled with a physical attack to maximize damage to the electric power grid.

Threats appear to be increasing as international relations become more fragile. It is well known that several nations have or are developing cyberwarfare capabilities. The exact dimension of the threat from nations is not specifically known outside of government agencies, but the threat is admitted to exist.

Criminal organizations regularly attack commercial enterprises, often in an effort to extort money from a company in payment for not causing damage to either that company's network, business, or customer base. These organizations are becoming more sophisticated and, being international in scope, provide a difficult challenge for law enforcement to contain.

Mitigations

Of course, all is not bad news. The past few years have seen an increase in the level of interest in security for SCADA and control system communications both within the U.S. government and within the electric power industry.

The U.S. Department of Energy has created the National SCADA Testbed which includes Idaho National Laboratory (INL), Pacific Northwest National Laboratory (PNL), Sandia National Laboratory (SNL), and NIST. Work done by these laboratories includes development of retrofit solutions, testing of vendor products, validation of encryption techniques and algorithms, vulnerability assessments for industry, and assessment of threats to SCADA and control system communications.

Homeland Security Advanced Research Projects Agency (HS-ARPA) has funded several innovative technology development efforts over the past few years. These efforts have the potential to yield new and effective tools to help secure SCADA and control systems for the electric power sector as well as for other sectors such as gas and oil, water, and transportation.

Individual companies and industry research organizations have also been active. Two examples are the American Gas Association (AGA) and the Electric Power Research Institute (EPRI). AGA has developed a specification for retrofit security of SCADA and control system communications; this is scheduled for testing at PNL in the near future. EPRI maintains several programs to provide member companies with security solutions for operational systems.

The North American Energy Reliability Council (NERC) Critical Infrastructure Protection Committee (CIPC) develops security standards and guidelines for the electric power industry. Formal CIPC representation is determined by the NERC regions, but meetings can be observed by any qualified industry member.

Standards for future solutions are being developed in several arenas, including, but not limited to, the International Electrotechnical Commission (IEC), the Instrumentation, Systems, and Automation Society (ISA), and, of course, the IEEE.

Summary

SCADA and control systems are subject today to vulnerabilities that did not exist prior to deregulation. This is due to a variety of factors, including business needs brought on by deregulation and a movement toward using common operating systems and networking protocols for SCADA and control systems. The rise of organized criminal activity on the Internet and of national, covert, cyberoperations has compounded the threat.

However, both the U.S. government and industry, sometimes in partnership and sometimes independently, are working to mitigate these vulnerabilities and provide the means to secure our infrastructure.

For Further Reading

"NERC security guidelines for the electricity sector," [Online]. Available: http://www.esisac.com/library-guidelines.htm

"A reference model for control and automation systems in electric power," Sandia Nat. Lab., SAND2005-1001C, Oct. 2005 [Online]. Available: http://www.sandia.gov

"Framework for SCADA security policy," Sandia Nat. Lab., SAND2005-1002, Oct. 2005 [Online]. Available: http://www.sandia.gov

AGA-12 Specification [Online]. Available: http://www.gtiservices.org/security/aga12_wkgdoc_homepg.shtml

"Guideline for securing control system & corporate network interfaces," EPRI, Rep. 1010714, 2005 [Online]. Available: http://www.epri.com

"Supervisory control and data acquisition (SCADA) systems security guide," EPRI, Rep. 1002604, 2004 [Online]. Available: http://www.epri.com

Biography

Thomas Kropp is a security infrastructure project manager within the security program area at the Electric Power Research Institute. He received a B.S. in mathematics at Santa Clara University, California, and an M.A. in mathematics at the University of California at Davis.