

The U.S. House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations
and the Census

Hearing on Telecommunications and SCADA:
Secure links or Open Portals to the Security of the Nation's
Critical Infrastructure?

March 30, 2004

Statement Submitted for the Record
By
Gerald S. Freese, Director of Information Security
American Electric Power

**THE INTERDEPENDENCIES BETWEEN SUPERVISORY CONTROL AND
DATA ACQUISITION (SCADA) SYSTEMS and TELECOMMUNICATIONS
FUNCTIONS IN THE ENERGY INDUSTRY**

Introduction

Critical Infrastructure is built and operates on a framework of critical interdependencies. The energy industry, which either enables or supports every other critical infrastructure entity, is equally reliant on several of those same entities for its own viability. This statement will center on critical infrastructure protection as an "inclusive" concept – in this instance focusing on the interdependencies between energy Supervisory Control and Data Acquisition (SCADA) systems and the Telecommunications functions that support them. SCADA and Telecommunications are two areas where we must integrate cross-sector functional strategies into current and future infrastructure protection initiatives.

Functions of SCADA in Relation to Telecommunications Systems

SCADA is the "nervous system" of the power grid. It controls and coordinates multiple geographically separated, complex operational functions in power generation, transmission and distribution. It also concurrently monitors this operational environment by acquiring and processing vital electronic and physical system data. Telecommunications represents the intricate network of nerve pathways that connects these operational assets, providing the means by which to deliver the control instructions and update system status. These updates occur every .5 to 2 seconds from every Remote Terminal Unit (RTU) engaged in

the transmission and distribution of power. The data rely on the telecommunications infrastructure to ensure their uninterrupted transfer to Control Centers that analyze the data. These updates, through operator interface or automated commands associated with 140 individual control centers together maintain the balanced flow of electricity across the three interconnects that comprise the North American grid. Without these telecommunications pathways, the SCADA “nervous system” is isolated from essential information exchange and effectively ceases to function.

SCADA and Telecommunications Vulnerabilities Not Mutually Exclusive

Energy utilities use a number of communications media to connect various SCADA system components. This array of private microwave and fiber networks, wireless radio and increasingly the public networks are all inextricably tied to SCADA operations and are either potential pathways of attacks, the ultimate victims of attacks or both. This array of private microwave and fiber networks, wireless radio and public networks, including cellular are all inextricably tied to SCADA operations and are either potential pathways of attacks, the ultimate victims of attacks or both. We have to keep in mind that Telecommunications is vulnerable in its role as a transport medium. It is subject to attacks such as “man in the middle,” where transmissions are intercepted and altered, redirected or destroyed. Also, many power plants and substations use modems, vulnerable to a number of intrusion exploits, to manage equipment such as breakers, relays and switches over telephone lines. Telecommunications is also vulnerable in its network interface role, where telecom device exploits or network malicious code can create denial of service or buffer overflow conditions, effectively disabling operational data exchange with critical SCADA components. The key point is that SCADA and Telecommunications vulnerabilities are not mutually exclusive. The impact of successful exploits cuts across the “inclusive” interdependency model.

Compounding the SCADA/Telecommunications vulnerability issue is the move toward a centralized, more “open system” model with distributed computing and communications environments. This model is moving away from less vulnerable mainframe technology and private communications networks in favor of common technology sets and public telecom providers. These factors increase susceptibility of SCADA and Telecommunications resources to multiple electronic attack vectors from virtually anywhere in the world. In addition, this move to standardized, common technology enables a parallel and proportionate growth in an attacker’s knowledge base and significantly increases control system and communications exploitability. Ultimately routine attacks designed to impact targets as common as all Internet connected computers will have a greater likelihood of disrupting critical SCADA communication paths.

Critical SCADA and Telecommunications infrastructures are “open books”

There is no mystery or obscurity associated with SCADA communications, configurations or protocols. One example that supports that premise centers on infrastructure development in Pakistan. SCADA and supporting telecom infrastructures there closely parallel the U.S. model. This is because their systems were designed and built with assistance of U.S. energy companies, using much of the same open technology, obtained through many of the same vendors. Also, analysis of computers recovered in Afghanistan showed that terrorists were engaged in research on software and programming instructions for distributed control and SCADA systems. These examples plus the vast amount of data on energy SCADA and Telecommunications available through open sources such as electric industry publications, FERC filings and on the Internet strongly support the assumption that there are few if any SCADA or Telecom system unknowns and no geographic constraints on specific knowledge factors. Add the growing ubiquity of common open systems technology and the increasing ranks of the computer-skilled to the equation and it is clear there is no logical basis for discounting the possibility of cyber attacks against targeted telecommunications and SCADA systems or components.

Electronic attacks against the energy and telecommunications infrastructures are less a question of “Can it be done?” than “How will it be done, to what extent, and what are the expected impacts?” The U.S. Canadian Task Force investigation following the August 14, 2003 blackout concluded in its interim report that the outage across a large portion of the U.S. and Canada was not caused by malicious cyber events. Notwithstanding that finding, if we review the interim report and substitute some well-known forms of intentional attack as the cause of the initial line malfunction, we can see that an internal or external intrusion could result in the same net result. An attack via the network, access through an unprotected modem into a data concentrator, remote access software vulnerability exploits or even a wireless network based intrusion could have resulted in a similar, and in these scenarios, hostile blackout condition. A successful undetected and coordinated attack against multiple vulnerable systems and networks over the Internet or through the phone systems could redirect processes, manipulate data and equipment and eventually disrupt service across entire regions.

Factors Contributing to Vulnerability of SCADA

In a number of companies, SCADA networks are not properly segmented from corporate networks. In others, access controls, firewall protection and intrusion detection are inadequately deployed. These factors increase their vulnerability to either incidental or directed malicious code attacks via the Internet, third parties or remote connections. Once malicious code enters the SCADA network, propagation methods can effectively initiate denial of service attacks against communications interfaces and disable control communications. In all of these

instances, telecommunications is at once the enabler and the target of these disruptive attacks, but only to the extent that it is operating without the benefit of appropriate and effective protective measures.

Conclusion

SCADA systems and Telecommunications provide critical services and are inseparable in their functional roles throughout the U.S. critical infrastructure. Their continued effectiveness and their joint improvement and evolution depend on CI organizations taking responsibility for securing these networks and systems – decreasing the numbers of vulnerabilities, increasing reliability and protecting the infrastructure that provides essential services to the country.

American Electric Power appreciates the opportunity to provide this information to the Subcommittee. We would be pleased to provide any additional information the Subcommittee may require for its deliberations.