SCADA Security: Challenges and Solutions

June 2011 / White paper

by Metin Ozturk, Philip Aubin

Make the most of your energy

Schneider Electric

Summary

Executive summary

This paper presents the case for improving security to SCADA systems. It examines the factors that have contributed to the growing vulnerability of control systems, and presents new standards designed to protect critical infrastructure including the use of encryption and authentication for SCADA systems.

Protecting Critical Infrastructure Includes Secure SCADA

Supervisory Control and Data Acquisition (SCADA) systems are typically used for monitoring and controlling geographically remote operations. In relative obscurity, these extensive control systems perform behind-the-scenes, collecting sensor measurements and operational data from the field, processing and displaying this information, and relaying control commands to local or remote equipment. Although SCADA systems are employed around the world in numerous industries, the average citizen is unaware of their critical importance. However, this is quickly changing as more information about the cyber vulnerabilities of utility SCADA systems is publicly available.

There is good reason why SCADA systems are getting the attention of hostile governments and competitors, terrorist groups, disgruntled employees, and other malicious intruders—they offer the huge potential to acquire confidential data and disrupt operations.

SCADA systems control some of the most vital infrastructure in industrial and energy sectors, from oil and gas pipelines to nuclear facilities to water treatment plants. Critical infrastructure is defined as the physical and IT assets, networks and services that if disrupted or destroyed would have a serious impact on the health, security, or economic well-being of citizens and the efficient functioning of a country's government.[1] One does not have to look far for examples of disruptions that have cost organizations time, resources, and possibly lives. Added to this is the fact that many SCADA systems are vulnerable. It is therefore imperative that system security and risk mitigation be at the forefront of the minds of all SCADA system users.

1 Myriam Dunn, "Critical Infrastructures: Vulnerabilities, Threats, Responses", CSS Analyses in Security Policy, Vol. 2, No. 16, June 2007. Typically, each country has their own definition of Critical Infrastructure. For more information on the 17 U.S. sectors visit http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

The Growing Vulnerability of Control Systems

Historically, security concerns over control systems were limited to physical attacks. SCADA system operators rationalized that if the management consoles were adequately isolated and only authorized personnel had access to the network, the system was intrinsically secure. There was little risk of tampering since few people had technical expertise of the system and the data communication paths remained isolated.

SCADA has been hidden behind its cloak of obscurity for the past four decades, with information technology managers convinced that these systems would never be accessed through corporate networks or from remote access points. The modern SCADA system has evolved significantly. Utility companies recognize the lower costs, easier accessibility, and improved efficiency gained through connecting their TCP/IP networks to their SCADA systems. These next generation systems, integrated with corporate networks and the Internet, face many challenges in their quest to becoming secure.

Several factors have contributed to the growing vulnerability of control systems, including:

1) The networking of control systems—Enterprises have increased connectivity through the integration of their control systems and enterprise networks. Breaches in enterprise security can arise if appropriate security controls are not put in place for both networks.

2) Insecure remote connections—Access links such as dial-up modems and wireless communications are used for remote diagnostics, maintenance, and examination of system status. If encryption or authentication mechanisms are not utilized, the integrity of the transmitted information is vulnerable.

3) Standardized technologies—Organizations are transitioning to standardized technologies, such as Microsoft's Windows, in order to reduce costs and improve system scalability and performance. The result is more people armed with the knowledge and tools able to attack a system, and an increase in the number of systems vulnerable to an attack.

4) Availability of technical information—Public information about infrastructures and control systems is readily available to potential hackers and intruders. Design and maintenance documents and technical standards for a critical system can all be found on the internet, greatly jeopardizing overall security.[2]

With so much riding on SCADA systems, it should come as no surprise that shortly after September 11, 2001, government officials found evidence of terrorist groups visiting websites that offer software and programming instructions for the digital equipment that run power, water, transport and communications grids. Furthermore, it has since been proven that the inner controls of critical infrastructure systems have been the target of cyber attacks. For example, in 2006 a water filtration plant near Harrisburg, Pennsylvania had its security system hacked. Malicious software that had the capability of disrupting the water treatment operations was planted from an outside source into the computer system.[3]

2 United States General Accounting Office, "Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems", GAO-04-354, March 2004.

3 Philip Leggiere, "Infrastructure Security, Securing SCADA", HSToday, www.hstoday.us, September 2008.

Most recently to shake the cyber security world was the "Stuxnet" malware, discovered in June 2010. On Nov 29, 2010, Iran's president Mahmound Ahmadinejad publicly disclosed that the Stuxnet cyber-threat had affected his country's uranium enrichment efforts. It is believed that the code was designed to sabotage nuclear plants, specifically targeting an individual company's configuration software and control devices. This intelligent worm was primarily spread via USB sticks but was found to also infect systems through network shares and SQL databases. According to Symantec, the worm would search for specific models of frequency converter drives made by two firms. Once the worm found the right configuration, it sabotaged operations by introducing subtle changes to the speed of the frequency drives over several weeks, while displaying normal readings to maintain its stealth.

The Stuxnet malware began infecting systems in January 2009 and reports indicate that more than 100,000 computer systems have been infected worldwide. Historic data from the early days of the attack showed that 58.85% of infections occurred in Iran, 18.22% occurred in Indonesia, and 8.31% occurred in India.[4] Although no serious damage was caused to any utility sectors, this sophisticated malware highlights the risks modern SCADA systems face with respect to connectivity, insecure remote connections, standardized technologies, and readily available technical information. Cyber security is a topic for utility experts and manufacturers that can no longer be ignored.[5]

4 Jarrad Shearer, "W32.Stuxnet", Symantec, www.symantec.com, September 17, 2010.

5 For control system security program information and incident reporting, visit Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at www.ics-cert.org.

Proactive Cyber Security is Smart Business

Ensuring cyber security in control systems may at first seem like a daunting task as it requires a commitment from the entire organization. Upper management needs to recognize the numerous benefits of a secure SCADA system. These advantages include ensuring system uptime, reliability and availability. Implementing good cyber security is smart business because a secure system is a trusted system, and customer retention and loyalty is built around trust. Vendors, system integrators, IT and control engineers all share in the responsibility.

There are many resources available now to help critical infrastructure SCADA systems enhance their security. For example, the standard ISA99 - Industrial Automation and Control Systems Security, establishes best practices, technical reports, and related information to define procedures for implementing and assessing electronically secure systems. Compliance with this standard can improve manufacturing and control system electronic security, help identify and address vulnerabilities, and reduce the risk of compromised confidential information and system degradation.[6]

Government regulations also exist and continue to evolve with the goal of securing critical infrastructure industries. The most ambitious for influencing government policy is the non-profit North American Electric Reliability Corporation (NERC) – Critical Infrastructure Protection (CIP) standard. Known as NERC-CIP, this standard has its roots in the Electricity Modernization Act which is part of the US Energy Policy Act of 2005. Within the Energy Policy Act of 2005, there is a section which dictates that the NERC-CIP standard requires all power plants and electric utility facilities to develop new cyber security systems and procedures in accordance with a 3-year implementation plan. There are eight different CIP standards covering everything from Security Management Control and Critical Cyber Assets, to Incident Reporting and Recovery Plans. Each one of the eight standards defines a series of specific requirements. The standards are:

- CIP-002-1: Critical Cyber Asset Identification
- CIP-003-1: Security Management Controls
- CIP-004-1: Personnel and Training
- CIP-005-1: Electronic Security Perimeter
- CIP-006-1: Physical Security of Critical Cyber Assets
- CIP-007-1: Systems Security Management
- CIP-008-1: Incident Reporting and Response Planning
- CIP-009-1: Recovery Plans for Critical Cyber Assets

Now that we're seeing congressional action and government penalties for non-compliance, SCADA cyber security is being taken more seriously.[7]

6 The International Society of Automation, "ISA99, Industrial Automation and Control System Security", http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821.

7 Philip Leggiere, "Infrastructure Security, Securing SCADA", HSToday, www.hstoday.us, September 2008.

Encryption and Authentication

In order to meet CIP-005-1 and CIP-007-1 standards, encryption and authentication are critical elements in a comprehensive cyber security solution. Typical SCADA security measures consist of physically securing the hardware and transmission media, and employing common cyber security defenses such as password protection and anti-virus utilities. Communication security measures are harder to enforce since modern day hackers can easily identify confidential phone numbers, decode proprietary protocols, and bypass firewalls and gateways. Encryption and authentication are highly effective methods to reduce some of these cyber threats to SCADA communications.

There are two open standards for SCADA communications available on the market today that were developed to provide security through encryption and authentication:

- IEEE6189 suite—Also known as AGA 12 incorporated in IEEE 1711, these standards secure SCADA equipment communication.

- IEC62351 suite—Secure Authentication for DNP3 communication is based on this standard.

Encryption is the act of manipulating information until it appears almost meaningless to the casual observer. Decryption is the process that takes place to restore an encrypted message back to its previous readable state.

In a typical SCADA system, messages are sent using a given protocol format, such as MODBUS or DNP3. Anyone who can see the messages being transmitted can decode them and see what information is being transferred from device to device. On an encrypted SCADA communication system, messages are transformed into a seemingly garbled sequence of bytes. Short messages are stuffed with extra random data to make it difficult to estimate the size or type of the messages being transmitted. A casual observer can determine little more than the fact that a message has been sent from one device to another. Encryption makes spying on and tampering with SCADA networks much more difficult.

Like many forms of physical or electronic security, encryption uses a key. This type of key is a secret sequence of data that determines how the information being sent between devices is obscured (encrypted). Keeping this key secure is a fundamental part of SCADA security. It is therefore important to reiterate that employing a diverse range of security measures will always prove more effective. The other layers of security, like physical locks, operating procedures, and separately secured corporate and SCADA networks are necessary to protect encryption keys, and the system as a whole.

Authentication is the process by which one part of a SCADA system proves its identity to another. A SCADA device receiving a critical message, such as a command to perform controls or respond with data, can challenge the sending device's identity. The sending device must then provide the challenge response. If the receiving device is satisfied with the challenge response then it will act on the original command.

Like encryption, authentication requires the communicating SCADA devices to have a mutually know secret key. Whereas encryption uses its key to transform entire messages into an encrypted data stream, authentication challenges and challenge responses use their key to create special digital signatures. The mathematics used in authentication is similar to that of encryption, but a smaller amount of data needs to be manipulated. This means that authentication is computationally far cheaper than encryption and typically uses the structure of the original SCADA protocol for better communication efficiency. Authentication prevents malicious parties from controlling a secured SCADA device, but it will not stop them from intercepting messages and reading their content.

Achieving Your Secure SCADA with Schneider Electric

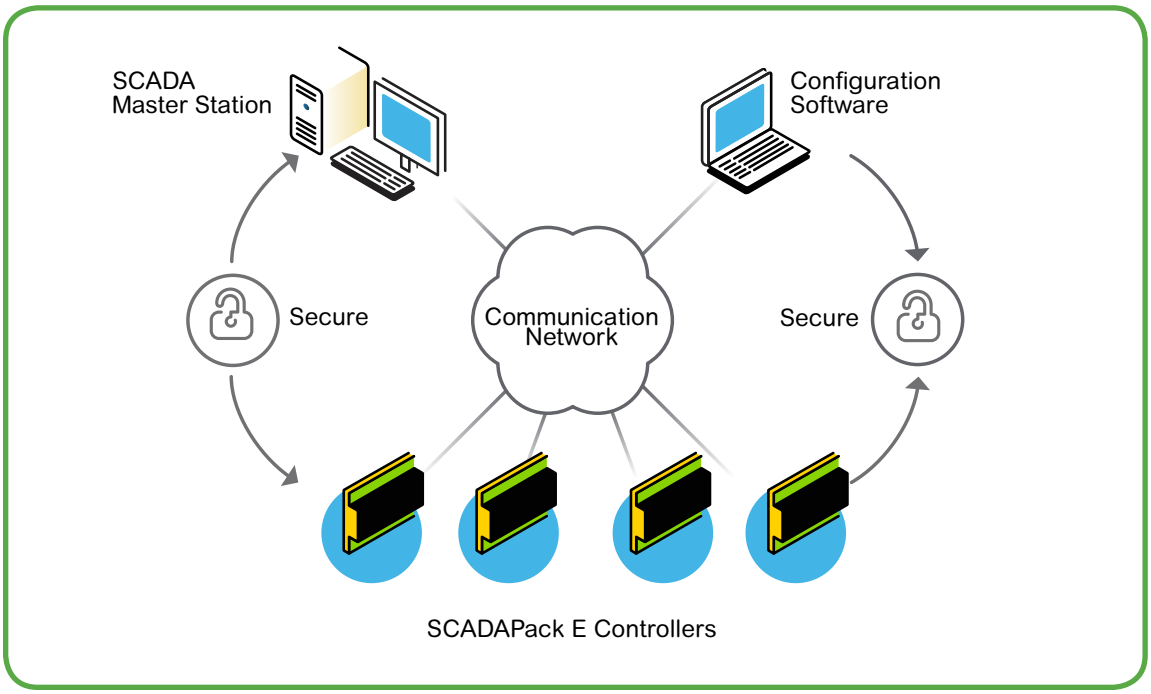
As described above, government is mandating the deployment of security technology for SCADA systems in some utility sectors, while for the moment leaving others free to choose whether they deploy security or not. With the growing vulnerabilities of control systems and the potential for harm and civil disruption in a breached critical infrastructure system, SCADA users are advised to formulate and deploy a security plan that meets their individual and immediate needs. Even within a security mandate there is scope for choice about how to implement the security system: authentication or encryption, or both.

Schneider Electric's SCADAPack E controllers provide both IEEE6189 message encryption and DNP3 secure authentication. As well, the E controllers now provide DNP3 communications to the latest DNP3-2009 standard. A new user-friendly security administrator is available for managing DNP3 secure authentication and AGA12 encryption security and is multi-group aware so it can be used to manage security configurations for multiple controllers in a system.

The SCADAPack E Configurator software further enhances system security as it cooperates with the E controllers to authorize configuration software installation, authorize users, and prevent system manipulation. This technology addresses the vulnerable security gap that commonly exists between control devices and their management software.

This powerful line of programmable logic controllers with remote terminal unit functionality is designed specifically for telemetry and remote SCADA water and wastewater applications. With improving overall system visibility and security at its core, E controllers maintain no holes in data even when communication links go down and allow end users peace of mind in their system data's integrity for billable applications or critical operations.

In 2011, we will see utilities take a more proactive approach to protecting their SCADA infrastructure with the adoption of encryption and authentication technologies to meet compliance standards and avoid the monetary fines and reputational damage that a security breach can cause.



Schneider Electric

Telemetry & Remote SCADA Solutions
48 Steacie Drive, Kanata, Ontario K2K 2A9 Canada
Direct Worldwide: 1 (613) 591-1943
Fax: 1 (613) 591-1022
Toll Free within North America: 1 (888) 267-2232
http://www.schneider-electric.com

This document has been printed on recycled paper

Document Number M01012-32

April 2011 tk