Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security for Critical Infrastructure SCADA Systems

This paper provides a non-technical overview of critical infrastructure Supervisory Control and Data Acquisition (SCADA) security. It gives a background on SCADA systems and the history of critical infrastructure concern. The SCADA security threats, incidents and vulnerabilities are examined along with issues that impede security advances. Finally the broad range of security initiatives is discussed and observations and recommendations are made. Supervisory Control and Data Acquisition Systems Supervisory Control and D...

Copyright SANS Institute
Author Retains Full Rights

AD

Security for Critical Infrastructure SCADA Systems

Andrew Hildick-Smith

GSEC Practical Assignment
Version 1.4c, Option 1
February 23, 2005

© SANS Institute 2000 - 2005 Author retains full rights.

Abstract

Supervisory Control and Data Acquisition (SCADA) systems and other similar control systems are widely used by utilities and industries that are considered critical to the functioning of countries around the world. Early in the history of SCADA systems the equipment and software was fairly obscure and network exposure to the world was limited. Over time a combination of factors drove vendors to adopting standard IT platforms and SCADA system owners to interconnect their systems to other networks. These changes plus other conditions have produced SCADA systems that are more vulnerable to attack.

This paper provides a non-technical overview of critical infrastructure SCADA security. It gives a background on SCADA systems and the history of critical infrastructure concern. The SCADA security threats, incidents and vulnerabilities are examined along with issues that impede security advances. Finally the broad range of security initiatives is discussed and observations and recommendations are made.

Supervisory Control and Data Acquisition Systems

Supervisory Control and Data Acquisition (SCADA) systems provide automated control and remote human monitoring of real world processes. SCADA systems can be used to improve quality and efficiencies in processes such as beer brewing and snow making for ski resorts, but are traditionally used by utilities and industries in the areas of oil and natural gas, electric power, rail transportation, water and wastewater. [It is estimated that there are 3 million SCADA systems in use.] SCADA systems provide near real time monitoring and control with time delays ranging between fractions of seconds to minutes. Depending on the size and sophistication, SCADA systems can cost from tens of thousands of dollars to tens of millions of dollars.

Typically SCADA systems include the following components:

1. Instruments in the field or in a facility that sense conditions such as pH, temperature, pressure, power level and flow rate.

2. Operating equipment such as pumps, valves, conveyors and substation breakers that can be controlled by energizing actuators or relays.

3. Local processors that communicate with the site's instruments and operating equipment. These local processors can have some or all or the following roles:

    a. Collecting instrument data
    b. Turning on and off operating equipment based on internal programmed logic or based on remote commands sent by human operators or computers

© SANS Institute 2000 - 2005 Author retains full rights.

c. Translating protocols so different controllers, instruments and equipment can communicate, and
d. Identifying alarm conditions

Local processors go by several different names including Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED) and Process Automation Controller (PAC). A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment.

4. Short range communications between the local processors and the instruments and operating equipment. These relatively short cables or wireless connections carry analog and discrete signals using electrical characteristics such as voltage and current, or using other established industrial communications protocols.

5. Host computers that act as the central point of monitoring and control. The host computer is where a human operator can supervise the process, receive alarms, review data and exercise control. In some cases the host computer has logic programmed into it to provide control over the local processors. In other cases it is just an interface between the human operator and the local processors. Other roles for the host computer are storing the database and generating reports. The host computer may be known as the Master Terminal Unit (MTU), the SCADA Server, or a personal computer (PC) with Human Machine Interface (HMI) software. The host computer hardware is often but not necessarily a standard PC.

6. Long range communications between the local processors and host computers. This communication typically covers miles using methods such as leased phone lines, satellite, microwave, cellular packet data, and frame relay.

SCADA is just one implementation of process control systems (PCS). Another common method is Distributed Control Systems (DCS). SCADA systems are typically spread over miles of distance and sometimes have their programmed control functions in the central host computer, whereas DCS systems are usually installed within single large facilities with the local processor providing the control logic. At this point in time the distinctions between the two have largely blurred as each has adopted the strengths of the other. SCADA systems are often linked to related enterprise systems such as Energy Management Systems (EMS), Distribution Management Systems (DMS), Manufacturing Execution Systems (MES) and Substation Automation (SA). In this paper I focus on SCADA systems but the discussion of security issues is applicable to DCS systems and other varieties of control systems.

© SANS Institute 2000 - 2005 Author retains full rights.

Critical Infrastructure Concern

In the 1997 a report was released by the President's Commission on Critical Infrastructure Protection. It was a very important foundation and the beginning of a series of high profile United States Government documents recognizing the country's reliance on increasingly vulnerable, interconnected physical and cyber infrastructures.

Less than a year later, in 1998, The White House acknowledged the work of the Commission and released an important policy document known as the Presidential Decision Directive 63 (PDD63). This directive defined critical infrastructure as "those physical and cyber-based systems essential to the minimum operations of the economy and government." It defined critical infrastructure as including: telecommunications, energy, banking and finance, transportation, water systems and emergency services. It had the ambitious goal of protecting the nation's critical infrastructure by 2003. Significantly, the PDD63 established the principle elements that frame the current efforts to protect critical infrastructure SCADA systems:

- The importance of a public-private partnership for success in reducing vulnerabilities,

- Lead federal agencies that act as liaisons for each infrastructure sector. A partial list of the lead agencies included: the Environmental Protection Agency (EPA) for water supply and wastewater, the Transportation Department for rail and pipelines, and the Energy Department for electric power and oil and gas production,

- Interagency and inter-industry coordination groups including the Critical Infrastructure Coordination Group and the National Infrastructure Assurance Council,

- A warning and information sharing system through the creation of the National Infrastructure Protection Center,

- Industry specific information sharing systems known as Information Sharing and Analysis Centers (ISACs), and

- A requirement for the National Infrastructure Assurance Plan to establish milestones for sector based vulnerability analyses and remedial plans.

Less than two months after the September 11, 2001 attacks the USA Patriot Act was passed. The last section of the law covers critical infrastructure and is known as the Critical Infrastructure Protection Act of 2001. It states, as does PDD63, that any disruption of critical infrastructure must be infrequent and "minimally detrimental" to the nation. It recognized the existing National

© SANS Institute 2000 - 2005 Author retains full rights.

Infrastructure Simulation and Analysis Center (NISAC) as the advanced technical resource for research on critical infrastructure protection and provided funding.

In the following year the Homeland Security Act of 2002 created the Department of Homeland Security (DHS) and carried out numerous consolidations. One of these consolidations established the Director of Information Analysis and Infrastructure Protection (IAIP), which became responsible for cyber and critical infrastructure protection.

In 2003, the President released The National Strategy to Secure Cyberspace. This document was addressed to the American public with the intention of expanding the effort and broadening participation. The bulk of the strategy lays out cyberspace security priorities to establish a response system, a threat and vulnerability reduction program, an awareness and training program, and national and international cooperation. Within the threat and vulnerability section it states that, "Securing DCS/SCADA is a national priority."

Security Threats

SCADA systems have evolved from exotic hardware and software in the 1970's, to systems that can include standard PCs and operating systems, TCP/IP communications and Internet access. The threat exposure has increased further by the common practice of linking SCADA networks to business networks.

Intentional security threats to SCADA systems can be grouped as follows:

1. Malware – Like any IT system, SCADA systems are potentially vulnerable to viruses, worms, trojans and spyware. For the purposes of this characterization I define the malware threat as an undirected attack that has no "interest" in SCADA systems. It could impact the system by corrupting data, overwhelming communications, installing back doors or key stroke loggers.

2. Insider – The disgruntled worker who knows the system can be one of the largest threats. The insider may be motivated to damage or disrupt the SCADA system or the utility's physical system. An insider may also attempt to illicitly gain higher privileges for convenience sake. Bored or inquisitive Operators may inadvertently create problems. [SCADA engineers may make errors that bring down the system.]

3. Hacker – Here the individual is an outsider who may be interested in probing, intruding, or controlling a system because of the challenge. Another possibility is modifying data related to rate generation. While not an incident, one example of hacker interest was a presentation at the 2003 Brumcon meeting titled "Water Management Systems Using Packet Radio" The talk apparently discussed radio systems used by the British

© SANS Institute 2000 - 2005 Author retains full rights.

water utilities, how to monitor un-encrypted traffic and create denial of service attacks.

4. Terrorist – This is the threat that distinguishes critical infrastructure systems from most IT systems. A terrorist is likely to want to either disable the SCADA system to disrupt monitoring and control capability, take control of the SCADA system to feed false values to the operators or to use the control system to degrade service or possibly damage the physical critical infrastructure system. Based on evidence collected in Afghanistan, Al Qaeda had a "high level of interest" in DCS and SCADA devices. In addition to interest, Al Qaeda presumably has appropriately skilled members, for example it was also reported that Khalid Sheikh Mohammed, their arrested operations chief, was an engineering student in North Carolina who later worked in the water industry in the Middle East.

Fortunately for the critical infrastructure industries that principally use SCADA for their control systems, two of the common threat motivations are not relevant. One is the lack of economic incentives such as credit cards or financial accounts that inspire many cyber crimes. The other is the absence of proprietary recipes and formulas that can inspire corporate espionage.

Documented Incidents

There are a number of documented security incidents where critical infrastructure control systems were adversely impacted. The British Columbia Institute of Technology (BCIT) keeps a database of accidental and intentional cyber incidents that affect control systems. As of 2004 they had cataloged 34 incidents. Extrapolating from their 2003 data of 10 incidents and the estimated level of underreporting of traditional business crime, they concluded that there are at least 100 industrial cyber incidents a year. Using the cyber crime underreporting number estimated by the Computer Security Institute and the FBI for 2002, the extrapolated annual number of industrial cyber incidents may be closer to 25. The BCIT data shows an increasing trend of incidents perpetrated by outsiders, with 31% being responsible during the 1980 – 2000 period and 70% being responsible during the 2001 – 2003 period. Records of actual incidents include examples of each of the security threat categories except for the terrorist threat.

The Davis-Besse nuclear plant in Ohio had been off line for almost a year when the SQL Slammer worm was released in January, 2003 and infected and disabled their Safety Parameter Display System for five hours and their Plant Process Computer for six hours. Both monitoring systems had analog backups that were not affected. The worm reached the systems through a remote contractor link to the corporate network which in turn was connected to the process network.

© SANS Institute 2000 - 2005 Author retains full rights.

On August 20, 2003, CSX, the railroad corporation, halted passenger and freight train traffic in response to a worm infection. While the worm did not get into their signal system, it did infect the telecommunications network that supported both their signal system and dispatch system. Service was affected in 23 states.

One of the most commonly cited incidents used to illustrate the vulnerability of critical infrastructure SCADA systems is that of "insider" Vitek Boden who gained access into the controls of the sewer system of Australia's Maroochy Shire Council. The following information on the incident was described in the documentation of his appeals case. Mr. Boden was convicted of twenty-six counts of unauthorized access to the Council's SCADA system computers and causing intentional damage. Prior to the incident Mr. Boden was the onsite supervisor for a contractor installing a SCADA system for a sewer system with 150 pumping stations. The system included a local processor at each pumping station that could communicate using data radios with other pumping stations and a central host computer. After two years of working on the project, the job was basically done. Mr. Boden resigned from his firm and asked the client about employment. He was told he would not be hired. Later that month the Council's sewer pumping stations began experiencing apparent malfunctions. Over time it became clear that the problem was not system failures but rather intentional disruptions. Problems included alarms being turned off, loss of communications, pumps not activating at appropriate times and the release of raw sewage. Mr. Boden did this from his car using a laptop computer, a data radio from his former employer and one of their local processors. He received a prison sentence of two years. It was estimated that he released nearly 264,000 gallons of sewerage.

In the spring of 2001 the California Independent System Operator, the organization that manages the electric grid in California, was remotely hacked. While the hackers did not gain access to the active SCADA system, they did have access to the network for 17 days. The intent of the hackers and whether they were in fact merely hackers was not known.

Vulnerabilities and Associated Impediments to Change

Opinions vary on how difficult it is for an outsider to access control systems. Some articles describe it as "extremely difficult", while others say it "requires very little knowledge". In the same way that critical infrastructure SCADA systems have common and unique threats compared with traditional IT systems, they also have shared and additional vulnerabilities. The following is a description of SCADA system vulnerabilities with an emphasis on those that are either unique to SCADA systems or are exacerbated by SCADA system peculiarities:

1. Staff Experience – SCADA system staff are familiar with keeping control systems running. The normal goals of reliability and availability can

© SANS Institute 2000 - 2005 Author retains full rights.

initially feel in conflict with security efforts. With a bent for engineering and technical solutions to problems, the important role of developing security policies can be a foreign concept to typical SCADA staff. Furthermore SCADA staff may not be receptive to IT staff recommendations.

2. Operating System Vulnerabilities – The whole host of normal IT operating system vulnerabilities are present in SCADA systems. The difference from an IT shop is that patching may be performed less rigorously. The SCADA system operator has a running system that is expect to perform without interruptions. A test bed is unusual and reports of patch induced problems that cause systems to crash or take severe performance hits creates reluctance.

3. Authentication – It is not uncommon for SCADA systems to have shared passwords. This creates convenience for the staff but eliminates any sense of authentication and accountability. In some cases moving to two-factor authentication is limited by work conditions that may impede iris scans or fingerprint scans because of dirty hands or the wearing of safety goggles. Confidentiality of authentication is often compromised by the use of clear text transmissions.

4. Remote access – Because of the economics of staffing control centers around the clock it is not uncommon for SCADA systems to be configured with remote access. This can include dial-up access or VPN access over the Internet. In one interview of 50 water utilities in 1997 and 1998, a total of 60% reported that they could control their systems from a dial-up line.

5. Interconnections – The more connections the more exposure and vulnerability a SCADA system has. The deregulation of the electric power industry has increased interconnections between systems. Economic and enterprise pressures often result in internal connections between the SCADA network and the business network. As recently as 2003, a security conscious SCADA consultant publicly promoted combining networks for the sake of simplifying network administration and enhancing security.

6. Monitoring and Defenses – The use of Intrusion Detection Software (IDS) is not common. Firewalls and antivirus software is not universal. Given staff cut backs and drives for higher efficiency there is often little time to review logs. The potential for zero-day worms is always present.

7. Wireless – SCADA systems often use microwave, data radios and cellular packet services for communications. Depending on the implementation, these forms of communication can be vulnerable to certain types of attacks. Recently at least one utility adopted 802.11 wireless for their control system. Their consultant acknowledged that the

© SANS Institute 2000 - 2005 Author retains full rights.

implemented security measures would not stop a determined hacker.

8. Remote Processors – Certain classes of remote processors have recognized security vulnerabilities. Here the difficulty is two fold. First the computation power and memory resources of the processors are modest and not suitable for security upgrades. Secondly, once they are installed they typically stay in place for ten years or more. The result is vulnerable equipment that stays vulnerable for a long time.

9. SCADA Software – The SCADA application software has modest security features and other design weaknesses.

10. Public Information – It is not unusual for SCADA system owners to have published papers on the design of their system at a time when security was not a priority. This can expose system vulnerabilities. It is also fairly common for consultants or contractors to advertise their experience and reveal information about past clients.

11. Physical security – SCADA systems are usually distributed over large distances with multiple unstaffed locations. The physical protection of SCADA devices becomes important. But because pin tumbler locks, master keys and cylinder locks all have reported weaknesses it is important to be realistic about the level of protection they provide. In some cases economics and vendor promotion have brought closed circuit TV and intrusion contacts into the SCADA system. While convenient and cost effective, this weakens the reinforcing nature of separate physical security and SCADA systems.

SCADA Security Initiatives

Numerous SCADA security initiatives have been undertaken to address the vulnerable nature of SCADA systems. Valuable contributions have been made by all of the stakeholders in improving SCADA security: system owners, vendors, consultants, academic institutions, National Labs, independent associations and bodies, and government organizations.

SCADA system owners bear the ultimate responsibility for protecting what they manage. They have participated in vulnerability assessments, have made improvements and continue to do so. Through vulnerability assessments and responding to research questions, they also provide the information that gives direction for other stakeholders.

The vendors in the SCADA world are working on securing their products. They are aware of the market value and competitive advantage of secure products. If they do a good job and produce products that are demonstrated, through independent testing, to be secure and that are easy to upgrade to, they may even shorten the typical SCADA system lifecycle and reap extra gains. On the

© SANS Institute 2000 - 2005 Author retains full rights.

down side, in theory, they could face legal suits for providing knowingly insecure products, should their component be the primary factor contributing to a severe SCADA attack. Of the industrial cyber incidents documented by BCIT, five were self-reported to have cost over $1 million.

SCADA consultants are also driven by economics and an interest in helping solving an important problem. They contribute to the security cause by providing expert services to clients, publishing papers and making presentations that educate and heighten awareness of system owners, and conducting funded research that advances the state of the art. The sophistication of consultant advice is variable so hopefully firms with less knowledge will partner with IT security firms to provide rigorous recommendations and designs. Consultants are also acting as instructors in the handful of SCADA security classes that are being offered.

Academic institutions are similar to the consultants in that they raise awareness and advance the field of SCADA security. They also play the unique role of educating students who may become the future experts in the field. [BCIT, Univ. Illinois]

The Department of Energy's National Laboratories in the United States were created for nuclear energy and related research and development. Some of these labs now support advanced research on SCADA security. The Idaho National Laboratory in conjunction with the Sandia National Laboratory have created the National SCADA Test Bed in a setting that includes a functioning power grid and synergistic cyber and wireless test beds. The Sandia National Laboratory has The Center for SCADA Security, where they participate in research, training, red teams and standards development. One of their past projects was the development of the Risk Assessment Methodology for water utilities (RAM-W). A current project is the creation of a SCADA security guide book for the SCADA user. Sandia staff have emphasized the vital importance of the administrative side of security, what they call "security governance", for the long term success of security efforts by each system owner. They recommend concerted effort on the sequential development and application of an IT control framework, a security policy, a security plan, implementation guidance and security enforcement consisting of configuration management and auditing.

There are many independent associations and organizations engaged in SCADA and PCS security work. They represent a large part of the effort towards bolstering SCADA security. They are both industry specific and broad based in interest. They can be grouped into two populations, Information Sharing and Analysis Centers (ISACs) and Standards Bodies.

ISACs were encouraged under PDD63 and have been established for the Electricity Sector, Energy (oil & gas), Surface Transportation (rail) and Water (water and wastewater). They are independent organizations with members from their industrial sector. They maintain confidential information and provide early warning and analysis of threats and vulnerabilities.

© SANS Institute 2000 - 2005 Author retains full rights.

The other class of independent organizations can be loosely called Standards Bodies. Examples of these include: the Instrumentation, Systems and Automation Society (ISA), the American Gas Association (AGA), the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Council (NERC). While outside of the industries included in this paper, the Chemical Industry Data Exchange (CIDX) is another body that is actively working on cyber security including process control.

The ISA, through its SP99 standards committee has published two technical reports that are directed to cyber security of manufacturing and control systems. The first document, "Security Technologies for Manufacturing and Control Systems", acts as a primer on computer security technology. It examines different topics such as biometric authentication, host-based firewalls and virtual private networks and describes the vulnerability that the technology addresses, the typical deployment, known weaknesses, how it fits into the control systems environment, future directions and recommendations. The second technical report, "Integrating Electronic Security into the Manufacturing and Control Systems Environment" gives guidance on developing a security program. Both documents are sold for approximately $100.

The AGA has focused on communications encryption. The first document in a future series, "Cryptographic Protection of SCADA Communications, Part 1: Background, Polices and Test Plan", provides background on the need to protect SCADA communications, a guide to defining security goals, and cryptographic requirements. Their second document, still early in its development, will address retrofitting serial communications with encryption.

NIST through its Process Control Security Requirements Forum (PCSRF) is developing security requirements using the ISO Common Criteria for vendors and integrators. Their first document is, "System Protection Profile – Industrial Control Systems". They are in the early stages of working on a comparable document for SCADA systems.

NERC has established cyber security standards that it holds it members to. "Urgent Action Standard 1200 – Cyber Security" lays out security requirements, measures for compliance, compliance monitoring through self-certification, levels of non-compliance and sanctions. Depending on the level of non-compliance, financial penalties are established. Their next document, "Cyber Security Standards", is still a draft. It covers: critical cyber assets, security management controls, personnel and training, electronic security, physical security, systems security management and incident reporting and response planning.

Government organizations represent the public part of the public-private partnership. They have established critical infrastructure protection centers, provided research funding, overseen industry groups as regulators and most recently attempted an overall coordination of process control security.

© SANS Institute 2000 - 2005 Author retains full rights.

Federal, foreign and state governments have created offices of critical infrastructure protection that typically act as clearing houses to disseminate relevant information, although some take a more active role of incident response. In the United States there is the Directorate of Information Analysis and Infrastructure Protection (IAIP) within the DHS. The IAIP took over and consolidated the National Infrastructure Protection Center and the National Infrastructure Assurance Office, both of which were created by PDD63. In England there is the National Infrastructure Security Co-ordination Centre that aims to "minimize the risk to the CNI (Critical National Infrastructure) from electronic attack." In February 2005, the Canadian government announced the formation of the Canadian Cyber Incident Response Centre with a focus on critical infrastructure. New York State even has its own Office of Cyber Security & Critical Infrastructure Coordination.

Given the relatively primitive state of SCADA hardware and software security, research funding is needed to help move SCADA security. In 2004, DHS provided grants of up to $100K to 11 small businesses to do research projects involving SCADA security. Several of the topics involved IDS and encryption. The EPA has also supported research. In the fall of 2004 the EPA granted the Water Environment Research Foundation $250K towards work on "Security Measures for Computerized and Automated Systems", which WERF subsequently awarded along with some of their own funds to a consultant. This work is designed to "provide guidance to water and wastewater utilities on how to secure and protect automated systems." As part of this project the consultant has recently distributed a beta security self-assessment tool to a sample of utilities. The Interagency Technical Support Working Group has provided $87K of funding to a university to test SCADA communication protocol vulnerabilities and $881K to an institute to develop a retrofit table encryption module. Finally, the National Center for Advanced Secure Systems Research has funded a university to develop a way of authenticating data signals without full encryption.

Research work has paid off in the development of Modbus / TCP and DNP 3.0 attack signatures for the Intrusion Detection Software (IDS), Snort. Another useful tool, the protocol analyzer, Ethereal, supports the following SCADA and PCS protocols: BACnet Virtual Link Control, Common Industrial Protocol, EtherNet / IP (Industrial Protocol), Modbus / TCP, PROFINET and Distributed Network Protocol 3.0. While not complete, work has also begun on creating a SCADA Honey Pot to simulate a SCADA or DCS network.

The Department of Homeland Security has recently sponsored the creation of a new group called the Process Control Systems Forum (PCSF). It has the ambitious aim of facilitating and coordinating all work in the field of process control security. Its focus is on the future and to "accelerate the implementation of more secure Process Control System (PCS) and Supervisory Control and Data Acquisition (SCADA) systems." In order not to compete with existing organizations it has proposed active roles and interfaces with other groups and individuals from those groups including: the PCSRF, Department of Energy's

© SANS Institute 2000 - 2005 Author retains full rights.

National SCADA Test Bed, EPA, INEEL, Sandia National Laboratory and Argonne National Laboratory. One encouraging sign is PCSF's effort to include international bodies through the stated plan of having meetings alternate between American sites and foreign sites. PCSF is still in its infancy having had its formational meeting in February 2005 and planning to have its first Forum meeting in May 2005.

Observations and Recommendations

It is a difficult situation with high stakes. Most SCADA systems have all the vulnerabilities of IT systems plus a plethora of their own software and hardware weaknesses. The transition to secure SCADA systems will require two transformations. SCADA vendors will need to replace their existing products with ones that are secure. SCADA system owners will need to undergo a culture change that places security priorities on par with operational priorities.

The following support is needed in order to promote and accelerate the successful transformation of vendors:

1. SCADA system owners need to become vocal in demanding secure products.

2. Vendors must understand that security may be a make-or-break factor for their enterprise. They should pursue both product replacement and interim product retrofits.

3. Government organizations need to continue to fund SCADA security research.

4. Protection Profiles such as those planned by the PCSRF need to be developed.

5. Once products are prototyped, access to the National SCADA Test Bed provides a valuable proving ground and potential credentials for marketing.

The following support is needed in order to promote and accelerate the successful transformation of SCADA owners:

1. With infrequent incidents the risk of inaction may seem small. Owners need appropriate motivation. This could come from a government funded awareness blitz. Perhaps it could follow the format of the 2004 Microsoft Security Summit that toured 20 cities. Experts could debunk naive assumptions, instill some fear and provide stepped guidance documents with common language. Alternatively, all the industry sectors could adopt the accountability and proactive requirements that NERC has.

© SANS Institute 2000 - 2005 Author retains full rights.

2. The continued development of standards and guidance documents such as those produced by ISA, Sandia, NERC and CIDX. Ideally there would be a single document that ties everything together.

3. The continued development of retrofitting efforts such as AGA's.

4. To do it properly SCADA security is a full time job. Advice to create a dedicated security staff position within the SCADA group is understandable. Perhaps a better approach would be to dedicate half of the time of two existing staff members. That way the knowledge would be distributed between two people who could help each other out over tough spots.

5. Tight budgets and staffing characterize most companies. It may be worth considering government grant programs to help with the transition to the next generation of protects and systems.

The environment that we have now for correcting SCADA security problems was essentially established in 1998 by PDD63. It set the framework that is both beneficial and detrimental to progress. Understandably PDD63 reinforced sector compartmentalization to keep industries in familiar settings with their government regulator as liaison and their own trusted ISACs. However, the result is multiple groups addressing their own standards and guidelines. This has fragmented the security effort and probably led to some waste and uncertainty. Compounding the problem is the unfortunate variety of names for similar devices such as PLC, RTU, IED, etc. This reinforces the sense of difference and masks the fact that all SCADA and PCS systems are essentially the same. Perhaps the newly formed PCSF will help bridge the divide.

SCADA security is a rich topic. Assuming the government funded SCADA security research results are published, valuable future work on this topic could analyze or build on recent findings. For example one project might examine the Snort rules for Modbus / TCP and DNP 3.0 and then develop public source rules for another industrial protocol. Another project could focus on SCADA encryption efforts and the difficulties imposed by tight latency requirements. A third project could compare item-by-item the existing SCADA owner guidance documents and either identify one that is universally acceptable or propose how to make one.

© SANS Institute 2000 - 2005 Author retains full rights.

List of References

"AFI Intelligence Briefing." Richard Bennett Media. 28 Jun. 2002. 17 Feb. 2005 <http:/www.milnet.com/afi/AFI-Research-0628.htm>.

American Gas Association. Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan, Draft 4. AGA Report No. 12. 1 Nov. 2004. 22 Feb 2005 <http://www.gtiservices.org/security/AGA12Draft4r1.pdf>.

Byres, Eric P., J. Lowe. "The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems." 4 Oct. 2004. 20 Feb. 2005 <http://www.tswg.gov/tswg/ip/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf>.

The Center for SCADA Security. Home page. 21 Feb. 2005 <http://www.sandia.gov/scada/home.htm>.

"CSX Blames Virus for Delays". Washington Post. 20 Aug. 2003: E05. 12 Feb. 2003 <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A23020-2003Aug20&notFound=true>.

"Cyber War!" Frontline. PBS. WGBH. 24 Apr. 2003. 19 Feb. 2005 <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/alqaeda.html>.

Datz, Todd. "Out of Control." CSO Magazine. Aug. 2004. 20 Feb 2005 <http://www.csoonline.com/read/080104/control.html>.

DePoy, Jennifer. Telephone interview. 22 Feb. 2005.

"F-Secure Corporation's Data Security Summary for 2003, The Year of the Worm." F-Secure Corporation. December 2003. 24 Jan. 2005 <http://www.f-secure.com/2003/>.

"Ethereal Frequently Asked Questions." Ethereal. 13 Feb. 2005 <http://www.ethereal.com/faq.html>.

Evers, Joris. "Microsoft Pulls Patch That Crashes NT 4.0." ComputerWorld 4 Feb. 2003. 5 Feb. 2005 <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,78171,00.html>.

Evers, Joris, P. Roberts. "Microsoft Fixing Patch That Can Slow Windows XP." Network World Fusion 24 Apr. 2003. 5 Feb. 05 <http://www.nwfusion.com/news/2003/0424micropulls.html>.

© SANS Institute 2000 - 2005 Author retains full rights.

Ezell, Captain Barry C. “Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply.” Diss. University of Virginia, May 1998. 15 Feb 2005 <http://www.riskinfo.com/cyberisk/Watersupply/SCADA-thesis.html>.

“Frequently Asked Questions (FAQs).” Process Control Systems Forum. 11 Feb. 2005 <https://www.pcsforum.org/faqs.php>.

Fussell, Ellen. “Security Breaches Are Real.” InTech 1 Mar. 2004. 12 Feb. 2005 <http://www.isa.org/Template.cfm?Section=InTech&template=/ContentManagement/ContentDisplay.cfm&ContentID=34074>.

Gellman, Barton. “Cyber-Attacks by Al Qaeda Feared.” Washington Post 27 Jun. 2002. 12 Feb. 2005 <http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26>.

“Government of Canada Announces Cyber Security Initiatives.” Public Safety and Emergency Preparedness Canada. 12 Feb. 2005 <http://www.psepc.gc.ca/publications/news/2005/20050202_e.asp>.

Harrold, Dave. “Get Safe: Prepare for Security Intrusion”. Control Engineering. March 2003. 20 Feb. 2005 < http://www.manufacturing.net/ctl/article/CA283196>.

Homeland Security Act of 2002. H.R. 5005. 23 Jan. 2002. 19 Feb. 2005 <http://www.dhs.gov/interweb/assetlibrary/hr_5005_enr.pdf>.

“INEEL’s SCADA Test Bed.” Idaho National Engineering and Environmental Laboratory. 21 Feb. 2005 <http://www.inel.gov/nationalsecurity/factsheets/scada_test_bed.pdf>.

The Instrumentation, Systems and Automation Society. Security Technologies for Manufacturing and Control Systems. Technical Report ISA-TR99.00.01-2004. 11 Mar. 2004.

“ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment (Downloadable)”. Promotional sales page. ISA. 22 Feb. 2005 <http://www.isa.org/Template.cfm?Section=Standards1 &template=/Ecommerce/ProductDisplay.cfm&ProductID=7380>.

Jones, Jennifer. “Models of Mayhem.” Federal Computer Week. 30 Sep. 2002. 21 Feb. 2005 < http://www.fcw.com/supplements/homeland/2002/sup3/hom-models-09-30-02.asp>.

Lemos, Robert. “E-Terrorisim, Safety: Assessing the Infrastructure Risk.” 26

© SANS Institute 2000 - 2005 Author retains full rights.

Aug. 2002. 20 Feb. 2005 <http://news.com.com/2009-1001-954780.html>.

Loughnane, Michael, et. al. EPA Needs to Determine What Barriers Prevent Water Systems from Securing Known Supervisory Control and Data Acquisition (SCADA) Vulnerabilities. Report 2005-P-00002. EPA Office of Inspector General. 6 Jan. 2005. 21 Feb. 2005. <http://www.epa.gov/oig/reports/2005/20050106-2005-P-00002.pdf>.

National Infrastructure Security Co-ordination Centre. Home page. 17 Feb. 2005 <http://www.niscc.gov.uk/niscc/index-en.html>.

"NCASSR Project: SCADA Protocol Authentication Project." National Center for Advanced Secure Systems Research. 21 Feb. 2005 <http://www.ncassr.org/projects/scada.html>.

New York State Office of Cyber Security & Critical Infrastructure Coordination. Home page. 27 Jan. 2005 <http://www.cscic.state.ny.us/>.

North American Electric Reliability Council. Cyber Security Standards. Draft 17 Jan. 2005. 22 Feb. 2005 < ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_CIP_002-009_Jan_24_2005.pdf>.

North American Electric Reliability Council. Urgent Action Standard 1200 – Cyber Security. 13 Aug. 2003. 22 Feb. 2005 <ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Urgent_Action_Standard_1200_Cyber_Security.pdf>.

Peterson, Dale. "Modbus TCP." SCADA Security 31 May 2004. 13 Feb. 2005 <http://www.digitalbond.com/SCADA_Blog/2004/05/modbus-tcp.html>.

Peterson, Dale. "Snort Rules for DNP3." SCADA Security 7 Nov. 2004. 13 Feb. 2005 <http://www.digitalbond.com/SCADA_Blog/2004/11/snort-rules-for-dnp3.html>.

Pothamsetty, Venkat, M. Franz. "SCADA HoneyNet Project: Building Honeypots for Industrial Networks." 13 Feb. 2005 <http://scadahoneynet.sourceforge.net/>.

Poulsen, Kevin. "Slammer Worm Crashed Ohio Nuke Plant Network." SecurityFocus News. 19 Aug. 2003. 24 Jan. 2005 <http://www.securityfocus.com/news/6767>.

President's Commission on Critical Infrastructure Protection. Critical Foundations – Protecting America's Infrastructures 13 Oct. 1997. 19 Feb 2005 <http://www.tsa.gov/public/interweb/assetlibrary/Infrastructure.pdf>.

© SANS Institute 2000 - 2005 Author retains full rights.

The Process Control Security Requirements Form (PCSRF). Home page. 22 Feb. 2005 <http://www.isd.mel.nist.gov/projects/processcontrol/>.

"Process Control Systems Forum Formational Meeting." Process Control Systems Forum 9 Feb. 2005. 11 Feb. 2005 <https://www.pcsforum.org/events/form_mtg/formMtg.pdf>.

"Project Database Search." Water Environment Research Foundation. 22 Feb. 2005 <http://www.werf.org/research/search/index.cfm?fuseaction=projectinfo&index=933>.

"Recent Contract Awards." Technical Support Working Group. 22 Feb. 2005 <http://www.tswg.gov/tswg/contracts/contracts.htm>.

"Return of the Fed Guy." Brum2600. 4 Oct. 2003. 13 Feb. 2005 <http://www.brum2600.net/brumcon3/>.

R v Boden. QCA 164. Supreme Court of Queensland. Queensland Court. 10 May 2002. 12 Feb. 2005 <http://www.courts.qld.gov.au/qjudgment/qca%202002/qca02-164.pdf>.

Sarkar, Dibya. "DHS Funds Control Systems Research." Federal Computer Week. 23 Apr. 2004. 22 Feb. 2005 < http://www.fcw.com/fcw/articles/2004/0419/web-scada-04-19-04.asp>.

"SBIR Past Awards." Homeland Security Advanced Research Projects Agency. <http://www.hsarpasbir.com/SBIRAwards41.asp>.

Stamp, Jason et al. "Sustainable Security for Infrastructure SCADA." Sandia Corporation. 2003. 21 Feb. 2005 <http://www.sandia.gov/scada/documents/SustainableSecurity.pdf>.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. Pub. L. 107-56. 26. Oct. 2001. Stat. 115.272. 19 Feb. 2005 <http://news.findlaw.com/cnn/docs/terrorism/hr3162.pdf>.

Verton, Dan. "California Hack Points to Possible IT Surveillance Threat." ComputerWorld. 12 Jun. 2001. 19 Feb 2005 < http://www.computerworld.com/industrytopics/energy/story/0,10801,61313,00.html>.

"We Have Your Water Supply, and Printers' – Brumcon Report." The Register 20 Oct. 2003. 13 Feb. 2005 <http://www.theregister.co.uk/2003/10/20/we_have_your_water_supply/>.

Weiss, Joseph M. "Control Systems Cyber Security – Maintaining the Reliability of the Critical Infrastructure." Testimony before the US House of

© SANS Institute 2000 - 2005 Author retains full rights.

Representatives subcommittee. 30 Mar. 2004. 13 Feb. 2005 <http://www.utc.org/file_depot/0-10000000/0-10000/1013/conman/Joseph+Weiss+of+KEMA+Testimony+03-30-04.pdf>.

The White House. The National Strategy to Secure Cyberspace. Feb. 2003. 19 Feb. 2005 <http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf>.

The White House. Presidential Decision Directive/NSC-63. 22 May 1998. 18 Jan. 2005 <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

Willoughby, Mark. "Panel: Authentication has a Long Way to Go at Industrial Sites." Computerworld. 3 Jun. 2003. 20 Feb. 2005 <www.computerworld.com/securitytopics/security/story/0,10801,81764,00.html?nas=SEC-81764>.

"The World Market Study of SCADA, Energy Management Systems and Distribution Management Systems in Electrical Utilities: 2003-2005." Marketing announcement. Newton-Evans Research Company Jun. 2003. 13 Feb 2005 <http://newton-evans.com/reports/2003-2005_SCADA_EMS_DMS_Brochure1.pdf>.

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced