12-1-2008

A Holistic SCADA Security Standard for the Australian Context

Christopher Beggs
Sinclair Knight Merz Pty Ltd

DOI: 10.4225/75/57a824b8aa0d9
9th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 1st December, 2008

A Holistic SCADA Security Standard for the Australian Context

Christopher Beggs
Sinclair Knight Merz Pty Ltd
Email: cbeggs@skm.com.au

Abstract

Supervisory Control and Data Acquisition (SCADA) systems which control Australia's critical infrastructure are currently demonstrating signs of vulnerabilities as they are being interconnected to corporate networks, essentially exposing them to malicious threats. This paper discusses the vulnerabilities associated with SCADA systems, as well as discussing various SCADA standards and initiatives that have been developed in recent years to mitigate such threats. The paper presents the requirement for a holistic SCADA security standard that is practical and feasible for each SCADA industry sector.

Keywords SCADA, Vulnerability, Critical Infrastructure, Standards

INTRODUCTION

SCADA systems are currently facing vulnerabilities as they are becoming more increasingly connected to the Internet. This has caused organisations to develop security measures in order to secure their SCADA systems from internal and external security threats. SCADA systems are used for remote monitoring and control in the delivery of essential service products such as electricity, natural gas, water, waste treatment and transportation. They enable remote monitoring and control of a variety of industrial devices as diverse as water and gas pumps, track switches and traffic signals (IT Security Expert Advisory Group, 2005).

SCADA networks provide great efficiency to industry sectors that run critical infrastructure; however they also present a security risk. They were initially designed to provide functionality including performance, reliability, flexibility and control. Presently, SCADA systems are vulnerable to disruption of service, process re-direction or manipulation of operational data that could result in public safety concerns (US Department of Energy, 2002). These systems have become a concern to utilities within the industrial sector as they are playing a crucial role in their performance, reliability and productivity. However, this dependence has exposed these infrastructures to new threats of cyber-attack. This suggests that there is a need and a requirement for a holistic SCADA security standard in order to address the current vulnerabilities associated with SCADA systems. This standard needs to be practical and useful and shall provide organisations with comprehensive set of security guidelines that is systematic and fluid and that is easily adaptable to each SCADA industry sector.

SCADA SYSTEMS OVERVIEW

SCADA systems are primarily software tool kits for building industrial control systems. These systems are often used for remote monitoring and sending commands to valves and switches. For example, they can be found in water utilities and oil pipelines where they monitor flow rates and pressures. Based on the data that these systems provide, computer programs or operators at a central control centre balance the flow of material using industrial control systems to activate valves and regulators. These systems are vulnerable to implantation of faulty data and to remote access through dial up modems used for maintenance (Shea, 2003).

SCADA security risks have intensified since the development of Information Communication Technologies (ICTs) and the growth of terrorist organisations. Currently, SCADA systems are vulnerable to insiders, terrorists and malicious hackers. These risks and vulnerabilities have arisen because of system development on open based communications standards like Ethernet Communications and web enabled screens. SCADA software companies have embraced the Transmission Control Protocol and Internet Protocol (TCP/IP) and Ethernet communications as a common channel transfer information and data and to improve integration across multiple systems. However, these developments have exposed the industrial sector to common Internet vulnerabilities within communication protocols, which increase the risk of attack (Pollet, 2002). It is important to acknowledge that many of these protocols designed for SCADA can be easily attacked as they were not designed with

security in mind. Some of the existing SCADA hardware uses electronic chips that do not even have the computing power to encrypt the transmission for security (Mays, 2004).

Also, many old legacy SCADA systems are not compliant with new security technologies such as advanced encryption and intrusion detection devices. This is one of the reasons why SCADA vulnerabilities are appearing in critical infrastructure systems, but more importantly, highlights that SCADA systems were not originally designed to be used on open networks such as the Internet.

Public exposure of SCADA manuals and documents has also added to this risk of attack. Pollet (2002, p.1) claims that over 90% of major SCADA and automation vendors have all their manuals and specifications available online. Subsequently, Pollet argues that we are now at a time "when the technical knowledge and motivation are beginning to meet." Hacker communities now have the knowledge, tool sets and abilities to conduct destruction via a computer and it is possible that at some stage they could be approached by terrorists to engage in cyber crime, including cyber-terrorism, for an appropriate amount of money. This over exposure is obviously making SCADA systems more vulnerable to attack as hacking groups or terrorist groups can study and understand these systems and their weaknesses.

Many of Australia's critical infrastructures are controlled by industrial control systems. These systems can include distributed control systems (DCS) and programmable logic controllers (PLC) as well as SCADA systems. DCS are process control systems where hardware and software components are often provided by a single vendor. These process control systems are commonly deployed in a single manufacturing or production complex, and perform a higher level of internal data processing. DCS generally provide processed information to or a series of commands from a control center. For example, within a chemical plant a DCS might simultaneously monitor the temperature of a series of reactors and control the rate at which reactants were mixed together, while performing real time process optimisation and reporting the progress of the reaction. PLCs are devices used to automate monitoring and control of industrial plants and are generally used within a manufacturing plant (Shea, 2003).

All of these industrial control systems DCS, PLC and SCADA systems are employed in many of Australia's critical infrastructures. They were previously viewed as secure systems which protected remote locations from being physically broken into and damaged. For example, the establishment of remote control systems in dams was believed to protect against the unlawful release of the dammed water, as no hand operable valves and switches were accessible (Shea 2003). However, industrial control systems such as SCADA systems are becoming linked to corporate computer systems, potentially making them vulnerable to cyber-attack through the Internet (Shea, 2003).

COMMON VULNERABILITIES AND THREATS IN SCADA SYSTEMS

A recent assessment conducted by the Fink et al. (2006), part of the US National SCADA Test Bed (NSTB) a program created by the US Department of Energy to identify key vulnerabilities within control systems such as SCADA was carried out in 2006. The program involved the Idaho National Laboratory (INL) who is part of the NSTB to perform security reviews and assessments on a range of different sized controls systems including large SCADA systems with complex networks. The study involved over ten assessments which identified categories of vulnerabilities these are discussed below in Table 1.1

Table 1.1 SCADA Vulnerabilities Identified from NSTB Assessment

Category	**Description**
Clear Text Communications	Clear text (unencrypted) communications were observed in the network traffic (through packet sniffing). The clear text revealed user names and passwords which might permit replay attacks or simplify the process for reverse engineering of the data protocol. In some cases, clear text communications were observed between the control system network and the external corporate network segments.
Account Management	Privileged accounts were found with default or easily guessed user names and passwords; hard coded usernames and passwords were defined in documentation or extracted from binary executables or configuration files; password protection policies were weak.
Weak or No Authentication	Little or no authentication of host to host communications, increasing the vulnerability of the system to impersonation, replay, or man in the middle attacks.
Coding Practices	Disassembly or de-compilation of executable code revealed potentially unsafe coding styles (particularly with respect to string handling and buffer management); applications vulnerable to crashing on deliberately malicious input.
Unused Services	Services with known vulnerabilities were running on hosts; need for the service was not apparent in the system architecture.
Network Addressing	Network address resolution protocols (DNS, etc) were exploitable by spoofing or other bypassing schemes.
Scripting and Interface Programming	Batch files and other script files (Perl, etc) could be exploited with malicious input or other techniques.
Un-patched Components	Software modules were not current versions and contained known exploitable vulnerabilities that were required by the configuration.
Web Servers and Clients	Web servers were not securely configured, allowing directory traversal or file modification.
Perimeter Protection	Connections initiated from outside the SCADA perimeter; firewalls had unnecessary open ports; access control lists were mis-configured.
Enumeration	Web servers and other networks services revealed version information that could be use by an attacker.

(Fink et al. 2006)

These vulnerabilities discovered by Fink et al. and the NSTB program in 2006 indicate the dangers that control systems such as SCADA are currently facing since the convergence of these systems with Internet. Other studies recently carried out on SCADA systems of large water utilities found other common similar vulnerabilities like NSTB program which included:

- Operator station logged on all the time even when the operator is not present at the work station, thereby restricting the authentication process;
- Physical access to the SCADA equipment was relatively easy;
- Unprotected SCADA network access from remote locations via Digital Subscriber Lines (DSL) and/ or dial up modem lines;
- Insecure wireless access points on the network;
- Most of the SCADA networks directly or indirectly connected to the Internet;
- No Firewall installed or the firewall configuration or weak or unverified;
- System event logs not monitored;
- Intrusion Detection Systems not used;
- Operating and SCADA system software patches not routinely applied;
- Network and router configuration insecure; passwords not changed from manufacturer's default.

(Mays, 2004, p.5.8)

These vulnerabilities have been the cause of many security issues associated with ICT. Some of these issues are noted below:

- Increasing reliance on public telecommunications networks to link previously separate SCADA systems is making them more accessible to electronic attacks;
- Increasing use of published open standards and protocols in particular, Internet technologies, expose SCADA systems to Internet vulnerabilities;
- The interconnection of SCADA systems with corporate networks may make then accessible to undesirable entities;
- Lack of mechanisms in many SCADA systems which provide confidentiality of communications means that intercepted communications may be easily read;
- Lack of authentication in many SCADA systems may result in a system user's identity not being accurately confirmed.

(IT Security Expert Advisory Group, 2005)

The lack of security design and configuration with these systems seems to be a trend with the vulnerabilities identified within this discussion. These issues need to be considered when designing and configuring controls systems networks and need to be addressed in order to reduce control system vulnerabilities. The studies discussed above demonstrate further the need for new standards for SCADA protection.

OVERSEAS SCADA STANDARDS

There have been a number of SCADA standards that have been developed and released throughout the world in recent years in order to address SCADA vulnerabilities. In 1999, the Gas Technology Institute (GTI) was awarded a contract by the Technical Support Working Group to identify encryption algorithms that would protect gas SCADA systems from cyber-attack. GTI discovered an approach that was to incorporate Digital Encryption Standard (DES) and Public Key Encryption (PKI) and the Diffie-Hillman number generating algorithm as a suite of algorithms to protect SCADA units. At the time, it was found that these algorithms could be used but at a very high cost. GTI demonstrated this work, but few gas utilities were interested as they did not want to include security in their SCADA systems (Mays, 2004). Since September 11 2001, this has changed and most utilities are now interested in using these standards to protect their SCADA networks and have started to explore the integration process of using such technologies on their SCADA systems. However, many organisations using old legacy SCADA systems have found difficulties in applying such technologies because of the overhead processing time on low bandwidth serial communications, causing sluggish real time control and acquisition which has been a problem when trying to secure legacy SCADA systems with inadequate technologies.

Likewise, other initiatives that have been formulated to improve SCADA systems security have been developed by the National Institute of Standards and Technology (NIST) who have an ongoing initiative to improve critical infrastructure protection (CIP) by developing standards for process control security. They have established a process control security requirement forum for users of process control systems such as SCADA (Mays, 2004). NIST has launched a System Protection Profile for Industrial Control Systems addressing information system security certification and accreditation for federal governments. In 2007, NIST developed another Guide to Industrial Control Systems Security (SP 800-82) which provides guidance in establishing secure industrial control systems (NIST, 2007). This guide provides a comprehensive detailed assessment on securing SCADA systems for the industrial sector. The guidelines suggested can be used by organisations as best practice when designing and configuring control system networks such as SCADA.

Another measure initiated to improve security within SCADA systems is the development of the Instrumentation Systems and Automation Society (ISA) which is developing a standard ISA-SP99 for Manufacturing and Control Systems Security. The SP99 establishes standards, recommends practices, and provides technical reports and related information that will define procedures for implementing electronically secure manufacturing and control system practices as well as assessing security performance (Mays, 2004).

Also, in 2005, the National Infrastructure Security Coordination Centre (NISCC) in the UK developed a Good Practice Guide for process control and SCADA security with specific information on firewall deployment, and managing SCADA security risks (NISCC, 2005). This standard has been developed to promote effective SCADA security risk management and firewall deployment.

The present author would also like to recognise and summarise other standards that are currently available for SCADA security. Below are just some of the many SCADA standards that are currently available.

- NIST Systems Protection Profile Critical Infrastructure Process Control Systems (SPP-CIPS);
- NIST SPP Industrial Control Systems (SPP-ICS);
- Common Criteria ISO/IEC 15408 Version 2.1 to 3.1;
- ISO/IEC 27002:2006 Information Technology Security Techniques and Code of Practice for Information Security Management Standard;
- NERC Critical Infrastructure Protection (CIP) Reliability Standard CIP-002-CIP-009;
- DOD Instruction 8500.2 Information Assurance Implementation;
- Sans Top 20.

(USCERT, 2008)

There is a plethora of SCADA standards overseas that can be currently used within the SCADA industry. At this stage it is not possible to critique every standard but in order to determine which standard should be used can be very challenging and complex for many organisations. The extent of how useful these standards are for organisations is still questionable as vulnerabilities are continually appearing within SCADA systems. This suggests that the amount of information and complexity within these standards makes it challenging for organisations to determine what standards to follow and hence why there is need and a requirement for holistic SCADA standards that address SCADA security for each sector.

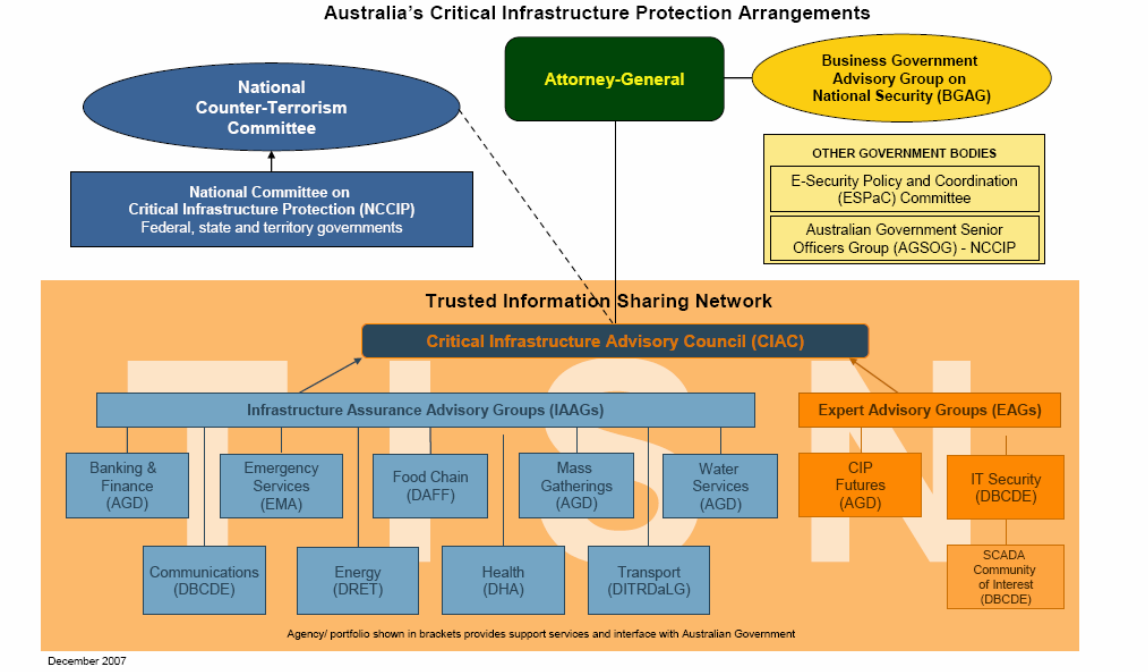
Below the Australian SCADA context is discussed with a proposed holistic SCADA security standard that can be easily adopted by organisations that own SCADA assets.

AUSTRALIAN SCADA INITIATIVES AND STANDARDS

In comparison to the overseas SCADA context there has been a limited amount of Australian SCADA security standards been made available to Australian SCADA asset owners in order to address SCADA security vulnerabilities. Alternatively, there have been various initiatives that have been developed by the Australian government to assist SCADA asset owners and operators.

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) is Australia's critical infrastructure information sharing network that intends to allow the owners and operators of critical infrastructure to share information on important issues relating to business continuity, consequence management, information system attacks and vulnerabilities, e-crime, protection of key sites from attack or sabotage, chemical, biological and radiological threats to water and food supplies and the identification and protection of offshore and maritime assets (Schneider, 2003). This network has a specific focus on SCADA and has several critical infrastructure advisory councils, including an IT security expert advisory board and the SCADA community of interest that focuses on strategies and methods to reduce SCADA vulnerability and threats. Figure 1.1 demonstrates how TISN focuses on protecting Australia's critical infrastructure. In terms of how effective TISN is a key agency in SCADA critical infrastructure protection is still questionable as vulnerabilities and weaknesses are still appearing in Australian SCADA systems (TISN, 2007a).

Figure 1.1 TISN and Australia's Critical Infrastructure Protection Arrangements



(TISN, 2007a)

In 2005, an Australian initiative was developed to reduce vulnerabilities in Australian SCADA systems because of the lack of commitment from the private sector. The Computer Network Vulnerability Assessment Program (CNVA) has been developed to support the work of the Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection. The Program aims to enhance the level of protection of Australia's critical infrastructure by working with critical infrastructure owners and operators to identify major vulnerabilities in SCADA systems and test those systems' ability to resist exploitation (TISN, 2006). The Program provides dollar for dollar funding to help owners and operators of critical infrastructure to:

- identify major vulnerabilities within ICT systems, dependencies between networks, and to test the ability of systems to resist exploitation;
- examine the security implications of planned changes to an information technology infrastructure;
- assess associated physical and personnel security issues.

The CNVA Program also provides assurances to organisations that the IT infrastructure and associated policies and processes that are in place are appropriate for their current environment. It also provides an opportunity for government and business to develop strategies to ensure that critical services continue to be delivered under a variety of conditions and circumstances (TISN, 2006).

Also, another initiative developed by the Australian government is GovCERT which provide plans and policies to protect Australia from a severe information based attack (SCADA). Its main focus is to integrate policy and plans together in order to prepare and protect the national information infrastructure from a cyber based attack or possible cyber-terrorism.

GovCERT is responsible for:

- liaising with CERTs from foreign government;
- coordinating enquiries from foreign governments about cyber-security issues affecting Australian businesses, including critical infrastructure owners and operators;
- coordinating the Australian Government's policy for the National Information Infrastructure on how to prepare for, respond to and recover from computer emergencies, and
- managing the Australian Government's Computer Network Vulnerability Assessment Program, which provides cash grants to critical infrastructure owners and operators to undertake security assessments of their IT systems and networks.

(TISN, 2007b)

GovCERT plays a role in coordinating SCADA related actives and provides various initiatives to assist with SCADA protection. This suggests that the effectiveness and usefulness of GovCERT is hard to assess, but believes they are providing some assistance in order to address SCADA security issues.

Another initiative set up by the Australian government is the SCADA portal which provides an online, community-based environment that facilitates collaboration between government organisations, academic institutions and owners and operators of critical infrastructure (TISN, 2007c). The portal has recently been initiated in 2007 by the Australian government and TISN and is another strategy in place to improve SCADA security by encouraging owners of critical infrastructure to collaborate. The present author can't assess how widely and effective this portal is currently being used as this is still in early stages of development

Lastly, the SCADA Risk Management Framework (RMF) was developed in 2006 to assist organisations in managing SCADA risks. The framework is a generic high-level document that provides a cross-sector approach to identifying and assessing risks for owners and operators of SCADA systems. The Risk Management Framework can be tailored to suit a particular sector or organisation and also contains advice on how information security risks can be simplified and presented to senior management (TISN, 2007d). This framework is a measure that has been developed recently by the Australian government to manage SCADA security threats. The framework can be used effectively in order to conduct SCADA security risk assessments and workshops as well as assisting organisations in ranking SCADA security risks.

Additional Australian Government Shortcomings for SCADA

The Australian government and private sector have developed an information sharing network to improve SCADA security with the initiatives and standards mentioned above. It is unclear how effective these agencies and measures are working in order to reduce the vulnerability of high risk targets such as SCADA. These agencies and measures discussed provide an insight into the main response to SCADA security within Australia. These measures are only working to a certain extent in defending organisations assets from cyber-attack, because threats and vulnerabilities are still appearing in critical information systems such as SCADA as mentioned above. For example, in 2008, Australia joined the US, the UK, Canada and New Zealand in the international cyber-exercise Cyber Storm II, held in March 2008. Around 55 organisations from the Australian Government, state and territory governments, the IT industry and private sector members of the Trusted Information Sharing Network took part in the Australian leg of the exercise (TISN, 2008b). The exercise did not

extend to real attacks on any security infrastructure. It did, however, operate on the premise that the 'adversary' could successfully overwhelm an organisation's cyber-defences and it was these successful attacks that made up the scenarios. What was then tested was the organisation's ability to respond to and recover from attacks (TISN, 2008b).

This exercise demonstrates that the Australian Government perceives a threat of an information based attack such as cyber-terrorism against their critical infrastructure systems. These simulation exercises are identifying system vulnerabilities to improve SCADA system security from potential threats such as hackers and possibly even cyber-terrorists.

Such cases highlight the need for additional measures to improve the cyber-security of SCADA systems. The measures discussed above promote a public and private partnership model to enhance SCADA security within both sectors. The author suggests that specific SCADA initiatives such as TISN, GovCERT, the SCADA Risk Framework and the SCADA portal are useful contributions that have been set up by the Australian government in order to improve SCADA security. Since the development of such initiatives the SCADA community and the increase in SCADA security awareness has given the ability for key decision makers to integrate SCADA security into their overall business strategy. Public and private owners of critical SCADA utilities are now more widely involved in using such initiatives to improve their overall security and performance.

These initiatives developed by the government have made some contribution in order to protect organisations from cyber attack. The extent of whether these standards and measures are adequate is still questionable as SCADA vulnerabilities and cases such as Cyber-Storm 2 suggest that continued and ongoing improvement and collaboration are necessary in order to achieve sustainability in this area and to maintain best industry security practice and standards.

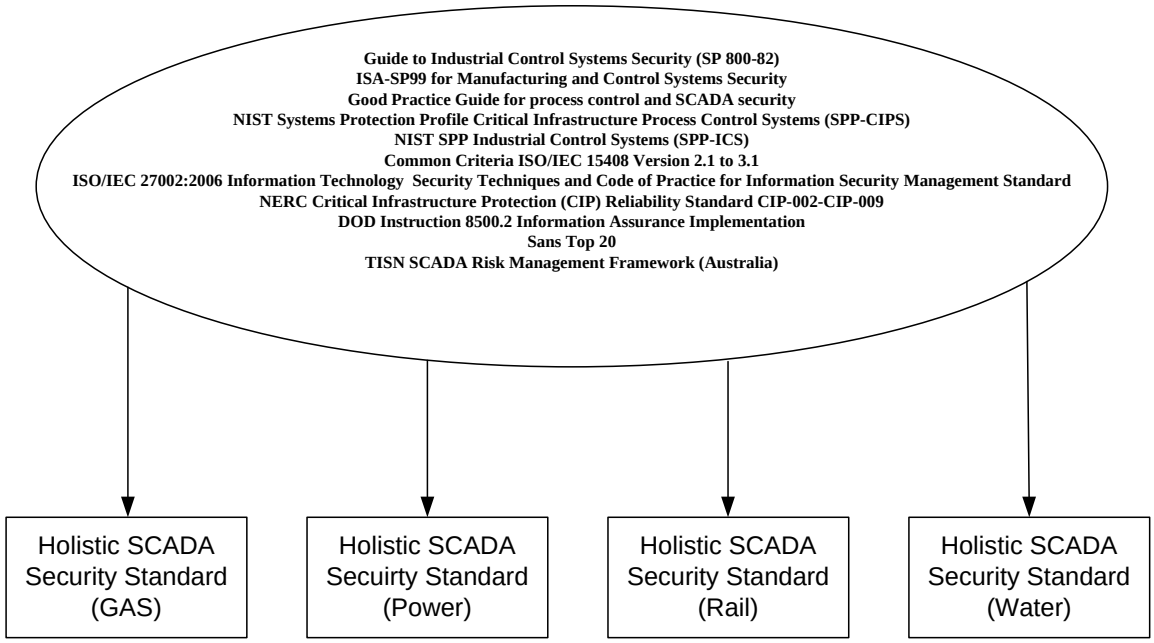
With so many SCADA standards currently available for organisations overseas can make it difficult in determining which standard should be used within each individual SCADA sector. Below discusses the requirement for a holistic SCADA standard for each critical infrastructure sector that could be applied and used within the Australian context.

A PROPOSED REQUIREMENT FOR HOLISTIC SCADA STANDARDS FOR MULTIPLE SECTORS

In order to achieve success in this challenging and complex environment action must be taken to implement a public and private sector relationship SCADA model that works across many specific industries. The present author suggests that a holistic SCADA framework and standard could be developed that addresses different sectors with specific aspects for SCADA security. At present there are various SCADA standards that are being used including standards discussed above such as, NIST 2007, NERC, ISO, TISN SCADA Risk Framework and others. Although some of th**e**se standards do focus on certain sectors they don't necessarily provide a comprehensive or holistic SCADA security approach. Also, there are so many different SCADA standards that their usefulness and practicality can be limited according to which SCADA sector the organisation belongs too. For example, SCADA systems in the rail sector are ultimately different from those systems used in the water sector. There are also different regulation guidelines and rules for each individual infrastructure and hence why specific SCADA frameworks would be deemed significant and necessary according to each individual sector. It is suggested that each standard must cover all aspects of SCADA security in relation to each industry, but with some commonalities.

In terms of practicality and feasibility it would be necessary to have one holistic SCADA standard for each critical infrastructure sector, rather than having a plethora of SCADA standards for all cross sectors. Ultimately, SCADA assets owners and operators need to be able to follow and adopt a process that suits their own needs and requirements as well as acquiring a methodology that is viable and effective. Below is a sample of the proposed holistic SCADA standards concept for each sector.

Figure 2.1 Proposed Holistic SCADA Standards for Each Sector (Examples)



Although the present author is proposing one SCADA security standard for each sector the amount of standards has effectively been minimised providing a single standard approach for each sector. Each standard would ultimately have similarities but may also provide specific details or amendments according to each individual sector. The proposed concept provides a process that is comprehensive, fluid and easily adoptable for many organisations. The use and practicality of holistic standards that are sector specific with similar commonalities is an attractive option that many organisations could simply follow. Current standards available don't meet this requirement although they do offer some assistance in specific areas for SCADA security. The concept of providing an "all in one holistic SCADA security standard approach" would be a viable option for an organisation to adopt to assist with SCADA security that is specific to there own sector. The proposed concept will ultimately address various concerns within industry and provides a systematic process that is practical for each SCADA environment. Figure 2.1 is only a representation of some of the possible sectors that it could be applied to and by no means is a complete or exhaustive list. The proposed concept could be driven by industry with the assistance of various standards committees such as "Standards Australia (2008)" in order to create an effective SCADA security solution. The significance of using holistic standards for SCADA protection would enable organisations to follow a consistent process that is adopted by all industry sectors.

CONCLUSION:

SCADA system vulnerabilities discovered by the NSTB program and the Cyber Storm 2 exercise in 2008 have suggested the dangers that control systems such as SCADA are currently facing since the convergence of these systems with Internet. Various SCADA initiatives and SCADA standards have been developed in recent years both overseas and within Australia in order to address SCADA security issues. These standards maybe limited in providing organisations with effective and easy to follow guidelines for securing SCADA systems. This paper has proposed a holistic SCADA security standard that is sector specific and that provides organisations with a process that can be implemented relatively easily. Further research is needed in developing a holistic SCADA standard that is industry specific and widely accepted, ultimately providing an even greater contribution to the SCADA security community.

REFERENCES

IT Security Expert Advisory Group, (2005) Supervisory Control and Data Acquisition-SCADA Security Advice for CEOs, URL http://www.tisn.gov.au, Accessed 7 November 2005.

Fink, Raymond, Spencer, David, and Wells, Rita, (2006) Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems Control, URL http://www.inl.gov/scada/publications/d/nstb_lessons_learned_from_cyber_security_assessments.pdf, Accessed 10 September 2008.

Mays, L. (2004) *Water Supply System Security*, McGraw-Hill, New York.

NISCC, (2005) Good Practice Guide of Firewall Development for SCADA and Process Control Networks, URL http://www.cpni.gov.uk/Docs/re-20050223-00157.pdf , Accessed 17 June 2008

NIST, (2007) Guide to Industrial Control Systems Security, URL http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf , Accessed 17 June 2008.

Pollet, J. (2002) Developing a Solid SCADA Security Strategy, *Sensors for Industry Conferences USA*, 2nd ISA/IEEE, 19-21 Nov, 2002, pp.148-156.

US CERT, (2008), Control Systems Documents, URL http://www.us-cert.gov/control_systems/csdocuments.html#docs , Accessed August 24 2008.

US Department of Energy, (2002) 21 Steps to Improve SCADA networks, URL http://www.counterterrorismtraining.gov , Accessed 12 April 2007.

Shea, D. (2003), Critical Infrastructure: Control Systems and the Terrorist Threat, *Congressional Research Services*, URL http://www.fas.org/irp/crs/RL31534.pdf , Accessed 1 June 2008.

Schneider, A. (2003), Parliamentary Joint Committee on the Australian Crime Commission - Inquiry into Cyber crime, *Attorneys General Department*, URL http://www.aph.gov.au/Senate/committee/acc_ctte/cybercrime/submissions/sub21.doc , Accessed 24 August 2008.

Standards Australia, (2008) URL http://www.standards.org.au/, Accessed 13 September 2008.

TISN, (2006) CIP Newsletter, *Vol 3 March* URL http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~Newsletter+March+06.pdf/$file/Newsletter+March+06.pdf , Accessed 10 September 2008.

TISN, (2007a) Australia's Critical Infrastructure Protection Arrangements, URL http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~TISN+diagram+v.2+Dec+07.pdf/$file/TISN+diagram+v.2+Dec+07.pdf , Accessed 24 August 2008.

TISN (2007b), GovCERT, URL http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~GovCERT.au+October+2007.PDF/$file/GovCERT.au+October+2007.PDF , Accessed 24 August 2008.

TISN (2007c), SCADA Portal, URL http://www.scadacoi.com.au, Accessed 12 September 2008.

TISN (2007d), SCADA Risk Management Framework, URL http://www.tisn.gov.au/agd/www/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EA

A)~SCADA+Generic+RMF+V2.0.pdf/$file/SCADA+Generic+RMF+V2.0.pdf , Accessed 24 August 2008.

TISN (2008b), "CIP Newsletter July 2008" URL http://ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(C7C220BBE2D77410637AB17935C2BD2E)~CIPNewsletterVol5No2.pdf/$file/CIPNewsletterVol5No2.pdf, Accessed 2 October 2008.

COPYRIGHT