



Trusted Information  
Sharing Network

for Critical Infrastructure Protection

Supervisory Control and Data Acquisition

# **SCADA SECURITY**

**– ADVICE FOR CEOs**



January 2005

## EXECUTIVE SUMMARY

---

Supervisory Control and Data Acquisition (SCADA) systems are used for remote monitoring and control in the delivery of essential services/products such as electricity, natural gas, water, waste treatment and transportation. This makes SCADA systems an integral part of a nation's critical infrastructure. They are also crucial to the continuity of business. This paper identifies emerging electronic threats to the security of SCADA systems and some issues you should be aware of to protect your SCADA systems.

### What are the security issues with SCADA systems?

Traditionally SCADA systems were designed around reliability and safety. Security was not a consideration. However, security of these systems is increasingly becoming an issue due to:

- 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 to corporate networks may make them accessible to undesirable entities;
- lack of mechanisms in many SCADA systems to provide confidentiality of communications means that intercepted communications may be easily read; and
- lack of authentication in many SCADA systems may result in a system user's identity not being accurately confirmed.

### Where do the threats come from?

Threats to SCADA may come not only in the form of *terrorism*, but from *general internet threats* (e.g. *worms and viruses*), *recreational hackers*, *errors resulting from training programs* or even *disgruntled employees*.

**DISCLAIMER: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. The document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.**

**What questions should you ask your Chief Information Officer (CIO) to ensure that your SCADA security is robust?**

- What processes are in place to identify security risks from cyber incidents in our SCADA system?
- What strategies have been put in place to manage these risks?
- How regularly are vulnerability assessments undertaken of our SCADA system?
- How well do the IT and the Engineering departments communicate?
- What assessments are undertaken of the training needs of our IT personnel involved with SCADA security?
- What measures have been put in place to ensure that our network design takes account of SCADA security?

## INTRODUCTION

---

If you are a Chief Executive Officer (CEO) of a utility, transport or broadcasting company your organisation uses Supervisory Control and Data Acquisition (SCADA) systems.

SCADA systems are a crucial part of a nation's critical infrastructure. They are also crucial to the continuity of your business. Therefore you need to think about how to secure your systems in the advent of an electronic attack.

This paper is provided to you as independent advice from the Trusted Information Sharing Network\* and is designed to make you aware of some of the security issues associated with SCADA networks. It does not discuss the technical aspects of SCADA security. Rather, its objective is to outline in broad terms issues that you should be aware of in relation to SCADA security. The paper concludes with some questions that you might ask your Chief Information Officer (CIO) regarding the security of your organisation's SCADA operations.

The integration of SCADA systems with technologies such as the Internet and wireless means that security is an important issue for these systems. While physical security has always been a priority for such systems, the new threat is that of cyber or electronic attacks. Such attacks can come from a host of sources ranging from recreational hackers to terrorists, disgruntled employees or contractors. The ever increasing extortion attempts on on-line gambling systems are a case in point.

**An Australian example of what can happen in the event of a SCADA electronic attack is discussed on page 7 along with a case study of an Internet based threat to a SCADA system.**

***Some issues for CEOs to think about:***

- ***Consider the ramifications of your SCADA system going 'down' or false commands given to your infrastructure due to a cyber attack. Consider also the effect it might have on both your bottom line and your reputation for service delivery.***
- ***Is your SCADA security system robust enough to counter an electronic attack or at least minimise its effects?***
- ***Is your SCADA system controlled in-house or is it outsourced which makes system oversight challenging?***

## What is SCADA?

Many industrial measurement, monitoring and control systems use SCADA, especially electricity and natural gas utilities, water and sewerage utilities, railroads, communications and other critical infrastructure sectors. It enables remote monitoring and control of a variety of industrial devices as diverse as water and gas pumps, track switches and traffic signals.

## SCADA Security

The majority of SCADA systems have useful lifetimes ranging from 15 to 30 years. In most instances the underlying protocols were designed without modern security requirements in mind. The rapid advance of technology and the changing business environment is driving change in SCADA network architecture, introducing new vulnerabilities to legacy systems. The current push towards greater efficiency, consolidated production platforms and larger companies with smaller staffing levels is leading to changes in SCADA systems which are raising many questions about security. In summary, these involve:

- an increasing reliance on public telecommunications networks to link previously separate SCADA systems;
- increasing use of published open standards and protocols, in particular Internet technologies; and
- the interconnection of SCADA systems to other business networks to enhance the amount, detail and timeliness of information available to management.

## Issues that you should be aware of

There are a number of issues that you need to be aware of when considering SCADA security. Some of these include:

- **Commodity infrastructure:** The changes in SCADA systems have exposed them to vulnerabilities that may not have existed before. For example, the switch from using leased telecommunications lines to public infrastructure ie. public CDMA and GSM networks, the use of commodity computers running commodity software and the change from proprietary to open standards have meant that vulnerabilities have been introduced into SCADA systems.
- **Network Architecture:** Effective network design which provides the appropriate amount of segmentation between the Internet, the company's corporate network, and the SCADA network is critical to risk management in modern SCADA systems. Network architecture weaknesses can increase the risk from Internet and other sources of intrusion.
- **Confidentiality:** Generally, there are no mechanisms in SCADA to provide confidentiality of communications. If lower level protocols do not provide this confidentiality then SCADA transactions are communicated "in the clear" meaning that intercepted communications may be easily read.

- **Authentication:** Many SCADA systems give little regard to security, often lacking the memory and bandwidth for sophisticated password or authentication systems. As a result there is no mechanism to determine a system user's identity or what that user is authorized to access. This allows for the injection of false requests or replies into the SCADA system.
- **Lack of session structure<sup>1</sup>:** SCADA systems often lack a session structure which, when combined with the lack of authentication, allow the injection of erroneous or rogue requests or replies into the system without any prior knowledge of what has gone on before.

### Where does the threat come from?

Electronic attacks on SCADA systems could come from a number of different sources. Following are some examples of threat sources, however, these have not been ranked in any order:

- **insider attack** from employees or ex-employees who are disgruntled or for any other reason are a possible security threat;
- **organised crime** may be driven by financial incentive to penetrate SCADA systems;
- **genuine mistakes** made as a result of lack of training, carelessness or an oversight;
- **terrorists** who may be seeking to add electronic attack to their existing capabilities;
- **generic Internet threats** such as worms, trojans and viruses that infect systems on the Internet can also affect SCADA systems when they use the same software and protocols. This may not be the result of a deliberate attack, SCADA systems may be infected merely because they can be.
- **recreational hackers, crackers and virus writers** motivated primarily by the challenge and a fascination with technology;
- **script kiddies** who are primarily untrained and yet have hostile or thrill-seeking intentions towards almost anything connected to the Internet;
- **activists** conducting publicity-seeking attacks; and
- **corporate attackers** that spy on competitors to gain a competitive advantage.

---

<sup>1</sup> A session in a networking sense is a group of commands and responses that together achieve a particular aim. At any point in the session, only certain commands are allowable and all others will result in an error. The SCADA protocols do not contain the concept of a session. Each command exists in isolation, any command is acceptable at any time.

### **Maroochy Shire Council (Maroochy Water Services)**

In April 2000 an ex employee of Hunter Watertech, a supplier of Maroochy Water Services' remote control and telemetry equipment, was arrested for illegally accessing the Council's sewerage management system. During March and April 2000 this person made 46 successful intrusions into the sewerage management system. It is alleged that he was vying for a contract position with Maroochy Water Services to correct faults in the system, faults that were later attributed to his own illegal activities.

After resigning from his position at Hunter Watertech, and later being refused a new position with Maroochy Water Services, he began a sabotage campaign against the sewerage management system. To gain access to the system he used:

- a stolen laptop from Hunter Watertech;
- control management software;
- commercial radio equipment; and
- a knowledge of the water management system gained from his employment at Hunter Watertech.

Each time he gained access to the system, the laptop assumed the functions of a pumping station and was able to access nodes governing the control of the sewerage system operations. While in control of the system he caused numerous pump station shutdowns resulting in millions of litres of raw sewage spilling into local parks and rivers including the grounds of a 5 star resort. He was later found guilty on 30 charges including computer hacking, theft and causing significant environmental damage and was fined and sentenced to two years jail in 2001.

The unauthorised intrusions resulted in direct costs of \$13,000 in clean up costs for the sewage spilt and \$176,000 in extra monitoring and security of the system. It also resulted in an extensive and costly in-house investigation, extensive media activity, and a loss of Maroochy Water Service's reputation over a five month period.

### **SQL Slammer Worm**

On the 25th of January 2003 an Internet based worm was released onto the world. The spread of this worm across the Internet was prolific. Compromised systems generated considerable network traffic, effectively denying service to all other network users. It became known as the SQL Slammer worm or Slammer for short.

Slammer exploited a vulnerability in a Microsoft database product and SCADA systems that utilised this product were potentially vulnerable to the worm. At the Davis-Besse nuclear power plant in Ohio USA, worm activity on the Process Control Network blocked SCADA traffic causing the operators to lose some degree of control of the system. As a consequence, the plant's Safety Parameter Display System and Plant Process Computer were downed for four hours, fifty minutes and six hours, nine minutes respectively.

**Some questions that you might ask your CIO regarding the security of your SCADA system**

- **What processes are in place to identify security risks from cyber incidents in our SCADA system?**

Considering the potential for security risks associated with SCADA systems, it is important that there is a framework in place to identify possible risks for existing and new SCADA systems. As SCADA systems are becoming increasingly interconnected with the Internet and corporate networks they are also becoming more exposed to Internet security threats and network vulnerabilities.

- **What strategies have been put in place to manage these risks?**

It is crucial for SCADA managers to put in place appropriate risk management strategies. Such strategies might include regular vulnerability assessments of SCADA systems, processes for patch management and configuration management, communication between engineering and IT departments, staff training, appropriate network architecture etc.

- **How regularly are vulnerability assessments undertaken of our SCADA system?**

While the identification of risks is important, equally important is the need for regular assessments of the vulnerabilities in your SCADA system. Many organisations fail to do this. In addition to assessing operational systems, assessments should also be undertaken of corporate networks, web servers, and customer management systems to reveal unintended gaps in security, including unknown links between public and private networks, and firewall configuration problems.

- **How well do the IT and the Engineering departments communicate?**

SCADA systems are traditionally engineering systems which are now deploying new technologies. It has been found that vulnerabilities can arise from a lack of communication between the IT and engineering departments. In many organisations the engineering and IT departments do not communicate on SCADA security matters. Is this the case in your organisation? These two areas need to work closely together to ensure that SCADA systems have appropriate security arrangements.

- **What assessments are undertaken of the training needs of our IT personnel involved with SCADA security?**

New security threats mean new security responses. These may require skills usually not found in process control personnel. Considering that SCADA systems are integral to your business processes, have you budgeted for appropriate education and training? Is time allocated for this? This applies at both the executive level as well as at the information systems and network management levels since it is likely that IT employees' earlier education and training did not include many of the security issues that are now faced by SCADA systems.

- **What measures have been put in place to ensure that our network design takes account of SCADA security?**

While firewalls, Intrusion Detection Systems, and Virtual Private Networks can all help protect networks from malicious attacks, improper configuration and/or product selection can seriously hamper the effectiveness of a security position. Your network design should provide segmentation between the Internet, the company's corporate network and your SCADA network to avoid any SCADA system compromise through the corporate network or the Internet. Network architecture should be robust and sufficiently adaptable to counter existing and new threats.

**Note:**

This paper has been prepared by the IT Security Expert Advisory Group (ITSEAG)\* For more information on the ITSEAG's work on SCADA security, please contact the Secretariat in the Department of Communications, Information Technology and the Arts on (02) 6271 1426 or SCADA@dcita.gov.au

*\* ITSEAG is part of the Trusted Information Sharing Network for critical infrastructure protection (TISN) which enables the owners and operators of critical infrastructure to share information on important issues. It is made up of a number of sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAG), and the Critical Infrastructure Advisory Council (CIAC - which is the peak body of TISN and oversees the IAAGs and the EAGs). One of the expert advisory groups within the TISN framework is the ITSEAG which provides advice to the CIAC and the sector-based IAAGs on IT issues as they relate to critical infrastructure protection. The ITSEAG is made up of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field. More information on TISN can be sought from <http://www.tisn.gov.au>*