2006

# A Security Architecture for SCADA Networks

Jill Slay
*University of South Australia*, jill.slay@unisa.edu.au

Michael Miller
*University of South Australia*

# A Security Architecture for SCADA Networks

Dr Jill Slay
Michael Miller
University of South Australia

School of Computer and Information Science
University of South Australia
Mawson Lakes, South Australia
Email: jill.slay@unisa.edu.au

## Abstract

*Supervisory Control and Data Acquisition (SCADA) networks are control and monitoring systems that are a major feature of the critical infrastructure of most developed nations. In recent years, these systems have become "open" by connecting them to corporate networks to allow access to real time data and process control from an office PC. This paper focuses mainly on the new risks which have been introduced by connecting SCADA networks to corporate networks, and proposes a security architecture which aims to minimise the security risks in SCADA networks.*

**Keywords**

SCADA, corporate network security, security architecture

## INTRODUCTION

Utility companies are becoming increasingly worried about "hackers" gaining access to their monitoring and control systems. A common system used for monitoring and control is a SCADA system. SCADA networks have the majority share of the automated control market. Graham (2004) estimated that by 2006, the market for SCADA systems in the electric power industry would reach approximately $1.7 billion. This represents a large interest in ensuring that these systems are secure from attacks that result in financial loss.

Originally SCADA networks were built on proprietary protocols and were implemented as stand alone networks. This deterred possible intrusion as there is no remote access and there is an "unknown" factor created by the use of proprietary protocols. In recent years these networks are no longer stand alone and corporate needs have resulted in the SCADA network being connected to a company's internal network, allowing for remote access to system. These networks are now also being built on common technologies such as Windows, Ethernet and Web Services.

Many business drivers are responsible for the need for remote access to the SCADA network. For example, senior staff may want the ability to view real time data on power output levels, or a supervisor may want to be able to monitor the network via their PC. However, by introducing non proprietary protocols and software, the "unknown" factor (accomplished by the use of proprietary protocols) has been eliminated. All common and commercially available SCADA technologies are widely published on the internet and the security flaws of these common technologies can be researched by any potential attacker.

## WHAT IS A SCADA SYSTEM?

A SCADA system is used for gathering real time data, controlling processes and monitoring equipment from remote locations in automated systems. They can be used to automate processes such as:

- Electricity power generation, transmission and distribution.
- Oil and gas refining and pipeline management.
- Water treatment and distribution.
- Chemical production and processing.
- Railroads and mass transit.

Although SCADA is most popular in large automation networks for utility companies, these systems can be used for almost any automated process. Any company using assembly lines, such as a bottling factory, can also benefit from a SCADA system. Entire plants can be automated, making manufacturing more efficient and reliable.

A SCADA network is essentially a collection of servers, clients and field devices connected together by a communication network. The process control and logic is controlled by master servers. The information used by the servers is collected via controllers/sensors. The clients are interfaces used by users to interact with the system. Servers are generally located in the main plant/station. They communicate with the controllers which can be located inside the plant or at remote locations. Programmable Logic Controllers (PLC) are placed onsite wherever equipment needs to be monitored or controlled. Essentially, a SCADA network can be very large and cover a hundreds of kilometres, especially in the case of utility plants where controllers need to be placed along power lines or gas pipelines.

The size and complexity of a SCADA network varies depending on the process that it controls, and also the size of the utility/business which runs it. The task will primarily affect the size and sophistication of the SCADA network. A typical electrical utility could have up to 50,000 data collection points in its network (Fernandez 2005), whilst a simple bottling factory may only require one server and a small number of PLC's. Large companies are more likely to have extra connections and features on their network.

A larger SCADA network will generally include (NCS 2004):

- More than one server in the control system area.
- A HMI, Human Machine Interface, for engineers to interact with the system.
- A large number of PLC's (up to hundreds of kilometres away from the main plant).
- Remote connections for engineers, contractors or third party entities.
- A communications network for the devices to communicate over.

## THE NEED TO SECURE SCADA SYSTEMS

Much research has identified the SCADA networks as a potential "weak" point in a power utilities networks. SCADA systems are responsible for controlling and monitoring many of our power plants. If these systems have security flaws, then they become a potential target to attackers. Gaining control of a system can lead to the entire plant being shut down. According to Sandia National Laboratories, SCADA systems are used by 270 utilities in the U.S. This amounts to eighty percent of the nation's power (Fernandez 2005). This makes SCADA systems the most common system for controlling and monitoring utility plants. With so many plants using SCADA, this makes it vitally important to secure these systems from attackers.

Fernandez *et al* (2005) has given strong reasons for the need to secure the SCADA systems which control the critical utility infrastructures such as power, oil, gas and water. The authors emphasise the potential risks by looking at the financial loss caused by recent major blackouts across the world. Not only do they identify financial risks, they point out other factors which are affected by blackouts. For example, on the 25 August 2003, in the United States, more than 100 power plants were shut down. This led to 50 million people in the U.S. and Canada being affected. More importantly though, it lead to the closure of 10 major airports and also shut down the New York subway system. The loss of critical infrastructure such as Airports is a major risk which emphasises the need to protect the SCADA systems, especially if the cause is cyber terrorism.

Oman (2000) attributes the recent concerns to mainly be generated by political means. One of the factors identified is the recent increase in international and domestic terrorist activity against North America. There have been recommendations and documents developed by various U.S. government agencies. This emphasises that the government, in this time of terrorist threat, understands the importance of securing utilities that are crucial to the infrastructure of their country. The focus of his paper is on gaining remote access to the substations located at various points in the network and provides an example of how an "open" SCADA network can be penetrated by a potential intruder.

National Communication Systems (2004) have identified that if a SCADA network is interconnected with the corporate network, then it is exposed to the same risks as those experienced in an attack on a conventional network. Companies may be under the false impression that a SCADA network is safe and lies on a separate network. However, once these networks are interconnected, then any attacker who breaches the corporate network has the ability to get at any device on the network, especially the SCADA system.

## THREATS TO SCADA NETWORKS

Byres *et al* (2004) discuss a threat that is very likely to affect SCADA networks. The authors recognise that attacks from hackers directly are not the only threat. In January 2003, the Slammer Worm managed to infiltrate an Ohio nuclear power plant and several other power utilities. This research discusses how the Slammer Worm managed to infiltrate the various SCADA systems in at least four different ways. These are:

- A power plant's process computer and safety parameter display via a contractor's T1 line.
- A power SCADA system via a VPN.
- A petroleum control system via a laptop.
- A paper machine's HMI via a dial-up modem.

These infiltration points demonstrate that many SCADA networks are being connected to the internet without consideration of security. Once connected to the corporate network, a SCADA network is also vulnerable to worms and viruses which circulate the internet.

Some attack examples and exploitations using the communications protocols in SCADA are given in KatipamulaIet al (2004). The attacks are based on the ICCP protocol for communication. Oman (2000), GAO (2004), and Dzung (2004) all give example attacks and likely threats to a SCADA networks. The attacks take advantage of the lack of security mechanisms protecting SCADA networks. Symantec (2005) give a vulnerability matrix discussing the various vulnerabilities associated with an insecure SCADA network. The attack types discussed are external attacks which take advantage of insecure remote connections.

## RESEARCH ON SECURITY MECHANISMS AND POLICIES FOR SCADA NETWORKS

Symantec (2005) discuss the importance and use of firewalls to protect the network. The research uses firewalls to firstly protect the corporate and SCADA client terminals from the internet. Then another firewall is used where there is a connection to the actual SCADA network. The use of firewalls is crucial to develop strong security architecture. However it is more likely to be multiple connections into the SCADA network, therefore it may be difficult to control incoming traffic through only one firewall. The amount and type of these connections would be discovered in initial security audits and assessments.

Peterson (2004) introduces and discusses the use of an Intrusion Detection Systems as a method of strengthening the security of a network. The author presents the advantages and disadvantages of using a traditional IDS device. The most important point of this study is that the author discusses the need for SCADA specific security devices. The specialised nature of these networks makes traditional security mechanism not as effective in this environment.

An NCS (2003) paper focuses how to identify possible security flaws in the SCADA network. Through evaluations, audits, surveys and strengthening identified "weak" points, the network security can be strengthened and protected against possible intrusions. The authors concentrate on the problem from an administrative prospective. They focus on developing policies, conducting security audits, ongoing assessments, and developing documentation about the network. Identifying the problem and performing risk assessments is the first stage in securing the SCADA network. Before implementing any form of security, an understanding of the current configuration of the network is vital. Stamp (2003) looks at the SCADA security problem from a long term point of view. The authors realise the fact that IT security is not static, but continually changing due to the nature of IT technology. The focus is placed on management, administration, policies and plans.

## PROTOCOLS IN SCADA NETWORKS

Katipamula *et al*(2004) discuss SCADA security at the protocol level. Many other papers focus on a higher levels of security than those which are the focus of this study. The paper discusses the Inter-Control Centre Communication Protocol, ICCP, used for communication in SCADA networks. Some attacks and exploitations of the protocol are given in the paper. ICCP is a very common protocol used in SCADA networks.

Graham (2004) gives a detailed look at the role of security at the protocol level and suggests some security mechanisms/practises that can be used to help secure networks at the protocol level. This paper focuses on the Distributed Network Protocol, DNP3, but the results apply to any protocol which has been built on top of TCP/IP. Therefore the ICCP protocol could be secured in a similar way, which is the protocol that the research will focus on.

Dzung (2004) discusses security and vulnerabilities of a variety of protocols used in SCADA networks. It includes ICCP which will be the protocol focused upon in this paper. The discussion of attacks and security at

the protocol level is an important factor in researching SCADA security. A secure solution would require security to be discussed as a whole. Implementing security at the protocol level will only strengthen and support other security mechanisms in the network.

Our literature review has found that there is an increased awareness in the problems associated with SCADA security. Many researchers have identified the potential problem and the need to address the issue. The contributing factors have been well documented:

- Moving away from a completely isolated, stand alone SCADA network.
- Implementing the SCADA networks on top of commercial software and common protocols.
- Increased political awareness of the problem due to recent terrorism events.

## SECURITY VULNERABILITIES

The main problem with protecting SCADA networks is that there are many routes that an attacker can exploit. Protecting against a large number of entry points increases the complexity of the final security architecture. Some attack routes include:

- Attacks originating from the corporate network.
- Attacks that gain access to the corporate network, then onto the SCADA network.
- Attacks that directly access the network.
- Attacks that gain access to the network via a remote connection (ie a contractor's laptop or a connection for a corporate partner).

### Virus, Worms and Trojans

Virus, worms and Trojans are a major security threat to SCADA. Their risk greatly increases when security mechanisms are not present. This gives the virus, worm or Trojan direct access to the SCADA network once it has gained access via the corporate network or a remote connection. The only part of the network that can become infected is the server/control applications. These machines are generally PC's with an operating system, such as Windows. The PLC's and other devices cannot be directly infected as they are not running an operating system like Windows. One effect of this type of attack is that it disrupts the network by creating extra traffic that is not normally found on the network. As a SCADA network is performance dependent, the extra traffic degrades the effectiveness of the network. The resources and bandwidth of the network are consumed, slowing down or restricting the normal SCADA traffic that travels through the network. This in effect becomes a Denial of Service attack. The server(s) and field devices are no longer able to communicate with each other at the rate needed.

### Gaining Unauthorised Access to the SCADA Application

Gaining unauthorised access is possibly one of the most dangerous attacks on a SCADA networks. Once the attacker has access to the system there are many possibilities in which attack can proceed. This form of attack is most likely going to be taken out by insiders, or disgruntled employees, who can easily access the SCADA application. An external attacker can also be a source, but not all SCADA systems, or implementations, have a means in which to gain remote access to the application. Therefore, attackers who can gain access to the actual machines in the company are the most likely source of this attack.

There are a variety of actions that can be taken once the attack has access to the application. The attacker has the capabilities to start/stop the processes in the plant. Depending on the process being controlled, the effects of these changes will vary. With access to the application the attacker has a chance to disable alarms in the system to hide their malicious actions. Plant operators will not be able to identify the attack occurring immediately without the alarms that are normally triggered. On their consoles/interfaces it would appear that the overall state of the plant is normal.

### Denial-of-Service

A Denial-of-Service, DoS, attack can be made on a SCADA network. This form of attack attempts to disrupt of the availability of services, processes or devices on the network. The simplest form of this attack is to block or delay communications between devices on the network. This result can be achieved by:

- Intercepting communications.
- Creating excess traffic on the network to consume the available bandwidth.

A DoS attack will disable, or slow down, the ability of devices to communicate on the network. The direct results of this will vary depending on the process being controlled. In some cases, a DoS, may be more of a nuisance to company rather than creating a serious situation or problem. For example, in a time critical operation, where the control system must close a valve on a pump, the results could be rather damaging. If this valve was part of a dam, then this may lead to some form of overflow, possibly resulting in environmental damage.

**Eavesdropping**

Eavesdropping is a problem with nearly all communication networks. SCADA networks are also vulnerable to eavesdropping. The method in which capturing network traffic will vary depending on the communication medium deployed for the network. A network deployed using wireless communication, will arguably result in the easiest interception of packets. Any attacker armed with suitable equipment can quite easily capture and inspect packets from the network.

The information embedded in the packets is generally not encrypted. Therefore, the attacker can read the encoded information in plain text. However, understanding the information being passed between devices is more difficult. Due to the specialised nature of the network, eavesdropping may not be as serious as in a traditional network. Most traffic on the network is the passing of data values collected in the field. Without a detailed understanding of the process being controlled, it may be quite hard to relate them with useful information (Graham 2004). An attacker with the right knowledge could quite potentially monitor traffic and extract useful information from the packets.

**Spoofing**

Spoofing involves the attacker impersonating a valid device on the network, and potentially sending commands to field devices. There is little security and validation involved in sending commands, making it possible to send false commands to a PLC.

If the attacker gains the ability to send commands to a device on the network, they can potentially (GAO 2004):

- Shut down devices.
- Cause equipment to overload and become damaged or unusable.
- Cause environmental damage opening a malicious valve.
- Send false information back to the servers to disguise the attack.

This form of attack could quite possibly be the biggest threat to a SCADA network. This attack can lead to environmental and financial damage.

**Insecure Remote Connections**

A common vulnerability in a SCADA network involves insecure remote connections into the network. Most commonly these are unprotected dial-up modems to allow remote access to a substation. Remote access allows operators to easily perform:

- Diagnostics on the substation.
- Maintenance on the substation.
- Monitoring of system status.

In many cases, the dial-up modems have no authentication or other security mechanisms in place at all. This gives the attacker an easy access point into the SCADA network.

## A PROPOSED SECURITY ARCHITECTURE

The security architecture proposed here aims to strengthen the overall security of the network. Its goal is to prevent, or mitigate, the number of successful attacks on a SCADA network. It comprises a combination of security mechanisms, policies and guidelines, and IT security concepts to help create a secure SCADA network.

Enforcing a security policy on employees is just as important the security mechanisms protecting the network. Techniques such as social engineering can compromise even the strongest network security. Employees need to be aware of the risks involved and should be made to conform to security guidelines and policies. The goals are the security architecture includes:

- Minimise/prevents attacks from compromising the network.
- Minimise any overheads that inhibit the SCADA network from functioning at full capacity.

- Provide a defence in depth approach to strengthen overall network security.

The proposed architecture creates a boundary between the SCADA network and the outside world. Originally SCADA networks were not at risk due to the fact that they were isolated but current business demands mean it is not possible to completely isolate the SCADA network. Therefore, any external connections need to be protected and monitored.

The main security mechanisms have been implemented at the boundary of the network where there is a security gateway. This gateway includes a firewall, an IDS and an anti virus mechanism. The three mechanisms provide three layers of security that suspicious traffic must pass through. Incoming traffic must:

- Pass the rules configured in the firewall.
- Pass the anti virus software/hardware.
- Not raise the alarm of the IDS.

**Firewalls**

Firewall(s) are important in creating a more secure SCADA network. The firewalls used in the security architecture aim to create distinct boundaries between the different network types.

The proposed firewall architecture is a DMZ approach. The architecture aims to create distinct zones which separate private sections from less secure sections of the network. In the case of the proposed architecture, the DMZ should contain any shared servers/resources between the corporate network and the SCADA network. Some servers/resources that may be found in the DMZ can include:

- Data historian servers that hold the data collected in the SCADA network.
- Wireless AP for engineers, contractors or third party entities.

A DMZ allows corporate partners to get access to the information they require (from a data historian), without gaining direct access to the SCADA network. This helps to reduce the risk of an attack on the network originating from the corporate partner's connection. This approach aims to restrict or minimise the direct access from the corporate network and the SCADA network. Placing the insecure or shared resources in the DMZ ensures that at the very least, suspicious or dangerous traffic, must at least cross the firewall before entering the SCADA network. The use of a DMZ may not be needed in the case of simpler SCADA networks. If there are no shared resources, then a single barrier between the corporate and SCADA network is only needed. The firewall configuration needs to be customised to suit the needs of each different SCADA network. Every network varies, as well as the needs of the company that runs the network. Qualified personnel should be used to deploy and configure the firewall. A poorly configured firewall will not perform the task needed to help secure the SCADA network.

**Intrusion Detection Systems**

An IDS should be implemented to enhance the security of the SCADA network. This mechanism should be deployed at the perimeter of the SCADA network. The goal of the IDS would be to monitor inbound and outbound traffic between the SCADA and corporate network, and not interfere with communications between devices on the SCADA network. Introducing an IDS would increase the overhead associated with communications on a network. A SCADA network is performance dependent, therefore any unnecessary overheads would degrade the performance of the system. Traditional IDS mechanisms have no knowledge of SCADA applications and protocols. So an attack on the SCADA control application using the Modbus protocol would not be detected. The benefits of using an IDS for a SCADA network would be to stop attacks that use common protocols or target applications. To effectively use an IDS in a SCADA environment, the application and protocol intelligence needs to be incorporated. The most dangerous attackers, such as a cyber terrorist or disgruntled employee, have detailed knowledge of SCADA networks. Their attacks would most likely be more sophisticated and SCADA specific.

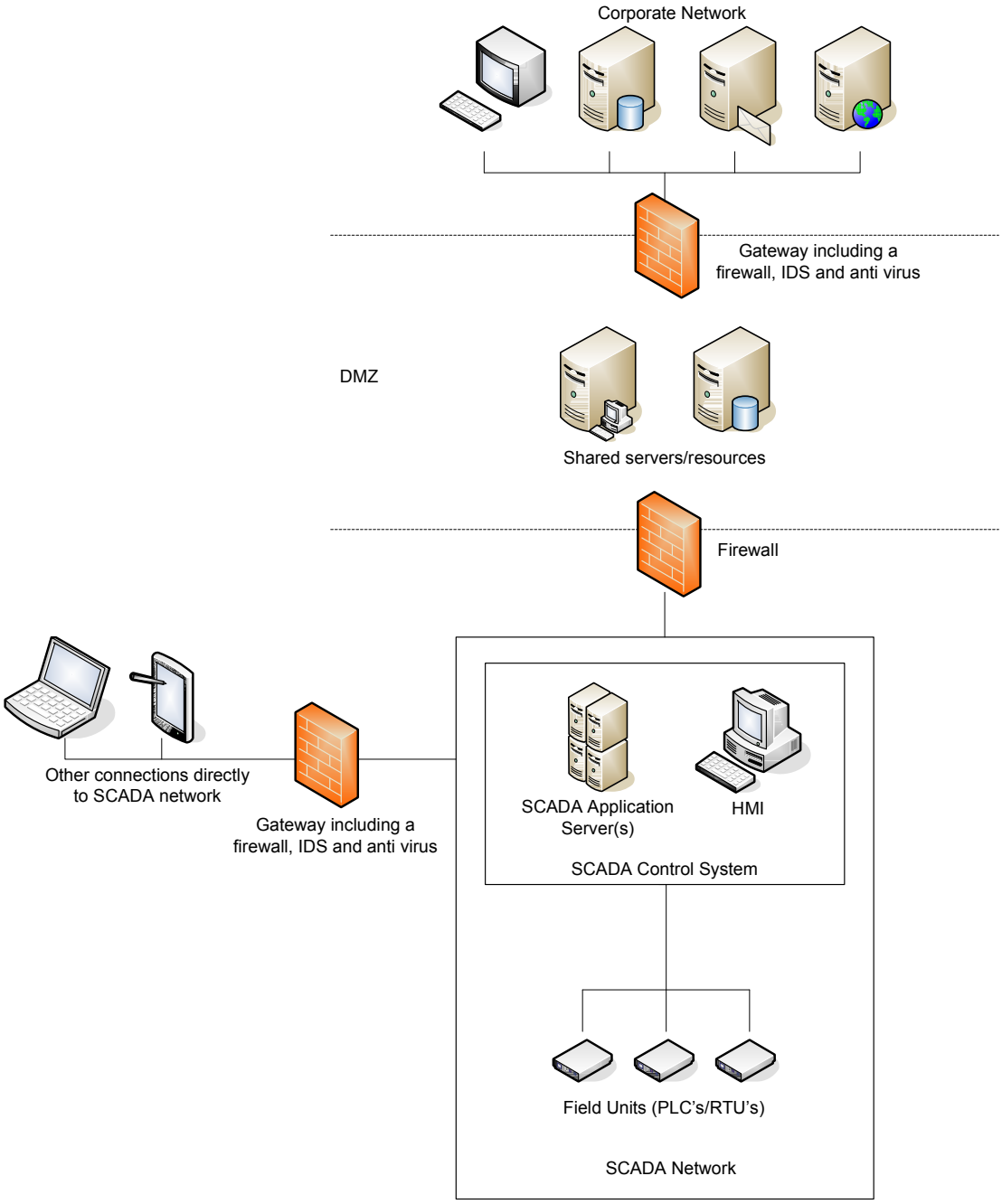


Figure 1: Proposed security architecture

**Anti Virus Solution on the SCADA Network**

A network based anti virus solution has been proposed at the perimeter of the SCADA network and no host based anti virus software on the servers. This is due to the extra overheads associated with using anti virus software/hardware. SCADA networks are dependent on communicating with in real time, and at very high speeds for time critical tasks. Anti virus software running on the servers would degrade the performance of the SCADA system. Implementing the anti virus technologies at the perimeter would stop viruses before they enter the network. By stopping viruses at the entry points, then the only way to bypass the security mechanisms would be to infect the servers directly. To add another layer to the anti virus solution, host based anti virus software should be enforced upon all contractors, or third party devices, accessing the network. These devices generally have direct access to the SCADA network. A virus originating on contractor's laptop can easily spread to the SCADA network if proper security considerations are not taken.

**Enhancing Security at the Protocol Level**

A large portion of SCADA network insecurity comes from the vulnerabilities at the protocol level. Very little to no security has been built into the communication protocols utilised in SCADA networks. Without redesigning, or modifying, the protocols, security can only be added on top of the protocol. This adds extra overhead to the communications between devices.

Many protocols are able to be embedded in TCP/IP packets, giving them the ability to be transmitted over traditional network medium. This results in SCADA systems having the possibility to utilise Internet technology (Graham 2004). The protocols embedded in TCP/IP are compatible with security technologies such as IPSec, SSL/TLS or VPN. These technologies would increase the security of SCADA networks at the protocol level.

Graham (2004) proposed that the most beneficial protocol security mechanism would be a SSL/TLS solution. The advantages of using SSL/TLS include:

- SSL/TLS covers most security components needed at the protocol level.
- The implementation would be fast, cost effective and simple.
- Can be used for any protocol that uses TCP/IP.

The problem with implementing this type of security on top is the extra overheads introduced. SCADA systems rely on high performance; therefore any extra overheads could potentially slow down the entire network, or result in some time critical tasks not functioning correctly. This sort of technologies would only provide a short term improvement in protocol security. However, in the long term, the most robust and SCADA specific security solution would involve the protocols themselves being enhanced. Research needs to be carried out into creating a fast, secure and reliable communication protocol. This could be done by enhancing or modifying the existing protocols, or starting with a completely new protocol to ensure security is included from the very start of its development.

**Securing Remote Connections**

The first step to securing the remote connections should be to evaluate all external connections. Identify the connections that are necessary, and then disconnect as many connections as possible without disrupting the running of the plant. External connections provide an entry point into the system, therefore having a few as possible will reduce the risk of attack on the network. (NCS 2003). The remaining connections should be evaluated using penetration testing and vulnerability assessments. This should help identify what sort of risks the connection will be exposed to (NCS, 2003). The remote connections should be made to pass through the gateway security setup in the architecture. This will help to detect suspicious traffic, and possibly block it, before it can enter the SCADA network. However, this may not always be possible, depending on the size and complexity of the network.

## DISCUSSION AND CONCLUSION

This theoretical research has found that there are many mechanisms available to companies to secure their networks. The use of firewalls, anti virus and IDS's will deter, detect or prevent a range of attacks and this has been proven in their implementation on traditional networks. SCADA networks, whilst being similar to traditional networks, are still a specialised type of network. They require specific knowledge by the attacker to make an effective attack. This reason may limit the effectiveness of the security mechanisms proposed by the research. They are intended for traditional networks, to stop normal network attacks. Without the knowledge of SCADA communication protocols built into these mechanisms, their effectiveness will be decreased, providing holes in the security architecture. The architecture proposed has been created by investigating current research into the area and applying traditional network security techniques in an attempt to increase the security of a SCADA network.

SCADA networks control the nation's critical resources, making them a target for terrorism. Recently seized terrorist computers, with control systems information on them, reinforce the current problem. An effective attack on these networks can potentially cause much harm financially, environmentally or even to the public.

Continuing research is vital to provide robust and effective security solutions for SCADA networks. Research will lead to security mechanisms being developed that have the knowledge of SCADA protocols and attack signatures. These mechanisms will provide a much more effective way of securing a network. Until the SCADA systems themselves become fairly secure, security will need to be built around the networks. The biggest increase in security will come when the SCADA systems are developed from the ground up with security in place. Authentication, encryption and other principles are essential in creating a more secure application. If this were to occur, then other security mechanisms will help compliment the overall security of the network.

Management and engineers responsible for SCADA networks are generally unaware of the security problems, despite recent research and publicity. Many utility companies are still under the impression that their systems are secure. Engineers are responsible for deploying and maintaining SCADA systems, whilst network security comes from an IT background. The gap between these two disciplines needs to be bridged to recognise and identify the vulnerabilities in these SCADA networks. Broader awareness and the sharing of good practice on SCADA security between utility companies themselves is a key step in beginning to secure the nation's critical resources.

## REFERENCES

Byres, E & Lowe, J, 2004, 'The Myths and Facts behind Cyber Security Risks for Industrial Control Systems', PA Consulting Group.

Dzung, D., Naedele., M, Von Hoff, T. & Crevatin, M, 2004, 'Security for Industrial Communication Systems', Proceedings of the IEEE, 2005, vol. 93, pp. 1152-1177.

Fernandez, J.D. & Fernandez, A.E. 2005, 'SCADA Systems: Vulnerabilities and Remediation', *Journal of Computing Sciences in Colleges*, vol. 20, issue 4, pp. 160-168.

GAO 2004 'Critical Infrastructure Protection – Challenges in Securing Control Systems', United States General Accounting Office, viewed 15 March 2005, <http://www.gao.gov/new.items/d04140t.pdf>.

Graham, J. & Patel, S, 2004, 'Security Considerations in SCADA Communication Protocols', Intelligent Systems Research Laboratory, viewed 20 June 2005, <http://www.louisville.edu/speed/cecs/facilities/ISLab/tech%20papers/ISRL-04-01.pdf>.

Katipamula, S., Hadley, M. & McKenna, T 2004, 'Evaluation of Symantec Security Products in an AREVA T&D-Implemented SCADA Environment using ICCP Communication Servers', Battelle Pacific Northwest Division, viewed 15 July 2005, <http://enterprisesecurity.symantec.com/Content/displaypdf.cfm?PDFID=804>.

NCS, 2004, 'Technical Information Bulletin 04-1', National Communications System, viewed 9 March 2005, <http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf>.

NCS, 2003, '21 Steps to Improve Cyber Security of SCADA Networks', National Communications System, viewed 10 March 2005, <http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf>.

Oman, P., Schweitzer, E. & Frincke, D 2000, 'Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems', CiteSeer, viewed 16 March 2005, <http://citeseer.ist.psu.edu/oman00concerns.html>.

Riptech, 2001, 'Understanding SCADA System Security Vulnerabilities', viewed 8 March 2005,

<www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf>.

Stamp, J, Campbell, P, DePoy, J, Dillinger, J, & Young, W 2003, 'Sustainable Security for Infrastructure SCADA', Sandia National Laboratories, viewed 16 March 2005, <www.tswg.gov/tswg/ip/SustainableSecurity.pdf>.

Symantec, 2004, 'Understanding SCADA System Security Vulnerabilities', Symantec.

## COPYRIGHT