

# CitectSCADA

## SECURING AN INTEGRATED SCADA SYSTEM

### Network Security & SCADA Systems Whitepaper

**Technical Paper**  
**April 2007**

Presented by:

**Scott Wooldridge**  
**Managing Director of Oceania**  
**Citect**

## **Abstract**

This paper discusses some of the options available to companies concerned with the threat of cyber attack on their critical infrastructure, who as part of their process of tightening up security, wish to prevent unauthorized network access to SCADA systems that monitor and control critical infrastructure.

## **About the Author**

Scott Wooldridge holds an MBA degree in addition to degrees in electrical engineering and mechanical engineering. He has over 15 years experience providing production improvement engineering, IT, project management and consultancy services to a variety of industrial, process, food and mining customers, including: Rio Tinto, BHP Billiton, ALCOA, PG & E, Mitsubishi, Caterpillar and GM. Scott now serves as Managing Director of Oceania, and previously acted as the Vice President Vice President of Sales for the Americas, Citect.

## **About Citect**

Citect is a leading, global provider of industrial and facilities automation, real-time intelligence and next generation manufacturing execution systems (MES). Leveraging open technologies, CitectHMI/SCADA, Ampla and CitectFacilities connect to multiple plant and business systems. Its products are complemented by Professional Services, Global Customer Support and Educational Services. Citect solutions are installed in over 80 countries and implemented in numerous industries: mining, metals, food and beverage, manufacturing, facilities, water, gas pipelines, power distribution and pharmaceuticals. Headquartered in Sydney Australia, Citect has representation in Oceania, Southeast Asia, China and Japan, North and South America, Europe, Africa and the Middle East.

[www.citect.com/support](http://www.citect.com/support)

## **Contact**

[customerservice@citect.com](mailto:customerservice@citect.com)

## **Contents**

Overview.....	3
Protecting Your SCADA Network.....	4
Further Security Measures.....	5
Network and Operating Environment Security.....	8
Special Considerations for Wireless Networks .....	10
References (in alphabetical order).....	11

## Overview

In recent years, utility companies have undergone great changes in the way they run their businesses. The pressure to increase profits and reduce expenses has them integrating their SCADA systems with their business networks to streamline operations. The popularity of the Internet has customers requesting online access to their accounts as well as online bill payment, further increasing network exposure. In addition, utility companies have reduced costs by leveraging the Internet to facilitate core business operations such as outage management and procurement.

The August 2003 mass power outage heightened public concern about the possibility of an intentional outage. As a result North American Electric Reliability Council (NERC) created the Urgent Action Standard 1200. The purpose of this action was to ensure all entities responsible for the reliability of the bulk electric systems in North America identify and protect critical cyber assets that control or could impact the reliability of bulk electric systems. In 2004, NERC issued a continuation and update of Standard 1200 that remains mandatory for control areas and reliability coordinators. All control areas and reliability coordinators must complete and submit the appropriate regional self-certification renewal form(s) indicating their degree of compliance or non-compliance with the cyber security standard requirements during the first quarter of 2005.

In addition, global terrorism has the public and media concerned about the security of public utility companies' critical infrastructure and their SCADA systems. Despite the public fears, there is no reason for utility companies to shun the immense benefits resulting from the integration of SCADA systems and the advantages of the Internet. The threat may be real, but the measures to protect SCADA systems are, fortunately, relatively easy.

Perhaps the greatest danger to utility companies is the lack of awareness of the need for greater security. Many public and private companies controlling vital public utilities like gas, power and water, never thought they would be the target of cyber attacks and now must implement measures to improve network security. While many utility companies perform regular risk assessments of their SCADA systems, too many do not. They have become dependent on their tightly integrated digital information systems without fully understanding the potential impact of a cyber attack.

SCADA systems were traditionally "walled off" from other systems operating independently from the network. Prior to the awareness of possible attacks, this seemed to provide all the protection the SCADA system needed. They were largely proprietary systems with such limited access and esoteric coding that very few people would have the ability to access them to launch an attack. Over time, however, they became integrated into the larger company network as a means to leverage their valuable data and increase plant efficiency. Therefore, the reality is their security is now often only as strong as the security of the network.

## Protecting Your SCADA Network

The first step towards securing SCADA systems is creating a written security policy, an essential component in protecting the corporate network. Failure to have a policy in place exposes the company to attacks, revenue loss and legal action. A security policy should also be a living document, not a static policy created once and shelved. The management team needs to draw very clear and understandable objectives, goals, rules and formal procedures to define the overall position and architecture of the plan. Key personnel such as senior management, IT department, human resources and the legal department all should be included in the plan. It should also cover the following key components:

- Roles and responsibilities of those affected by the policy
- Actions, activities and processes that are allowed and those that are not allowed
- Consequences of non-compliance

### ***Vulnerability Assessment***

A key aspect of preparing a written security policy is to perform a vulnerability assessment prior to completing the written policy. A vulnerability assessment is designed to identify both the potential risks associated with the different aspects of the SCADA-related IT infrastructure and the priority of the different aspects of the infrastructure. This would typically be presented in a hierarchical manner, which in turn sets the priority to address security concerns and the level of related funding associated with each area of vulnerability.

For example, within a typical SCADA environment, key items and the related hierarchy could be as follows:

- Operational Availability of Operator Stations
- Accuracy of Real-Time Data
- Protection of System Configuration Data
- Interconnection to Business Networks
- Availability of Historical Data
- Availability of Casual User Stations

A vulnerability assessment also acts as a mechanism to identify holes or flaws in the understanding of how a system is architected and where threats against the system may originate.

To successfully complete a vulnerability assessment, a physical audit of all the computer and networking equipment, associated software and network routings needs to be performed. A clear and accurate network diagram should be used to present a detailed depiction of the infrastructure following the audit.

After defining the hierarchy and auditing the different system components, the next section highlights the areas of vulnerability need to be addressed, as they relate to each component, as part of the assessment process.

## Further Security Measures

As previously mentioned, SCADA networks were once separate from other networks and physical penetration of the system was needed to perpetuate an attack. As corporate networks became electronically linked via the Internet or wireless technology, physical access was no longer necessary for a cyber attack. One solution is to isolate the SCADA network; however, this is not a practical solution for budget-minded operations that require monitoring plants and remote terminal units (RTU) from distant locations. Therefore, security measures need to be taken to protect the network, and some common security mechanisms apply to virtually all SCADA networks, which have any form of wide area (WAN) or Internet-based access requirements. The core elements are:

- Network Design
- Firewalls
- Virtual Private Networks (VPN)
- IP Security (IPSec) and
- Demilitarized Zones (DMZs)

### ***Network Design – Keep It Simple***

Simple networks are at less risk than more complex, interconnected networks. Keep the network simple and, more importantly, well documented from the beginning.

A key factor in ensuring a secure network is the number of contact points. These should be limited as far as possible. While firewalls have secured access from the Internet, many existing control systems have modems installed to allow remote users access to the system for debugging.

These modems are often connected directly to controllers in the substations. The access point, if required, should be through a single point that is password protected and where user action logging can be achieved.

### ***Firewalls***

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from outside users. A firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network, so that no incoming request can get directly at private network resources.

In packet switched networks such as the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks to which it is connected. A router is

located at any gateway (where one network meets another), including each point of presence on the Internet. A router is often included as part of a network switch. It is imperative to utilize a secured firewall between the corporate network and the Internet. As the single point of traffic into and out of a corporate network, a firewall can be effectively monitored and secured. It is important to have at least one firewall and router separating the network from external networks not in the company's dominion.

On larger sites the control system needs to be protected from attack within the SCADA network. Implementing an additional firewall between the corporate and SCADA network can achieve this aim and is highly recommended.

### ***Virtual Private Network (VPN)***

One of the main security issues facing more complex networks today is remote access. VPN is a secured way of connecting to remote SCADA networks. With a Virtual Private Network (VPN), all data paths are secret to a certain extent, yet open to a limited group of persons, such as employees of a supplier company. A VPN is basically a group of computers that interact as if they are on their own private network regardless of the actual structure of the physical network (e.g., the Internet, local LAN, wireless LAN, etc) upon which they actually exist. For example, there are a number of systems that allow the creation of networks using the Internet as the medium for transporting data. These systems use encryption and other security measures to ensure only authorized users access the network and data cannot be intercepted. Based on the existing public network infrastructure and incorporating data encryption and tunneling techniques, it provides a high level of data security. Typically a VPN server will be installed either as part of the firewall or as a separate machine to which external users will authenticate before gaining access to the SCADA networks.

### ***IP Security (IPsec)***

IP Security (IPsec) is a set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets at the IP layer. IPsec has been deployed widely to implement VPNs.

IPsec can be deployed within a network to provide computer-level authentication, as well as data encryption. IPsec can be used to create a VPN connection between the two remote networks using the highly secured Layer Two Tunneling Protocol with Internet Protocol security (L2TP/IPSec). IPsec supports two encryption modes: Transport and Tunnel. The Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet.

For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/ Oakley), which allows the receiver to obtain

a public key and authenticate the sender using digital certificates.

It is important during the selection process of network hardware such as routers, switches and gateways to consider the inclusion of support for IPsec security as part of the devices to enable the support of secure VPN connections.

***Demilitarized Zones (DMZ)***

Demilitarized Zones (DMZ) are a buffer between a trusted network (SCADA network) and the corporate network or Internet, separated through additional firewalls and routers, which provide an extra layer of security against cyber attacks. Utilizing DMZ buffers is becoming an increasingly common method to segregate business applications from the SCADA network and is a highly recommended additional security measure.

## **Network and Operating Environment Security**

It should also be understood when dealing with the SCADA infrastructure that there are commonalities and differences between SCADA-related IT security and IT security focused on typical business systems. For example, in a business systems environment, access to the server is typically the key focus. Whereas in a SCADA environment, the access focus is at the operator console level. This difference produces both alternate network topologies to provide the necessary availability as well as a different focus on what elements of the SCADA system would be of highest priority to safeguard against security breaches.

### ***Authentication and Authorization***

Authentication is the software process of identifying a user who is authorized to access the SCADA system. Authorization is the process of defining access permissions on the SCADA system and allowing users with permissions to access respective areas of the system. Authentication and authorization are the mechanisms for single point of control for identifying and allowing only authorized users to access the SCADA system, thereby ensuring a high level of control over the system's security.

To provide effective authentication the system must require each user to enter a unique user name and password. A shared user name implies a lack of responsibility for the protection of the password and the actions completed by that user.

Users must be able to be created, edited and deleted within the system while the system is active to ensure that individual passwords can be maintained. In addition it is highly recommended that password aging is implemented. Password aging ensures that operators change their passwords over a controlled time period, such as every week, month or so on.

To provide authorization, the system must be able to control access to every component of the control system. The system must not provide a "back door" with which to bypass the levels of authentication specified in the application.

### ***Secured Data Storage and Communication***

Critical data pertaining to a SCADA system must be securely persisted and communicated. It is recommended that critical data like a password be stored using an encryption algorithm. Similarly, remote login processes should use VPNs or encryption to communicate the user name and password over the network. Critical data like user name and password must be persisted in a secured data repository and access rights monitored and managed using secured mechanisms like Windows authentication and role based security.

### ***Intrusion Detection***

Firewalls and other simple boundary devices currently available lack some degree of intelligence when it comes to observing, recognizing and identifying attack signatures that may be present in the traffic they monitor and the log files they collect. This deficiency explains why intrusion detection systems, (IDS) are becoming increasingly important in helping to maintain network security.

In a nutshell, an IDS is a specialized tool that knows how to read and interpret the contents of log files from routers, firewalls, servers and other network devices. Furthermore, an IDS often stores a database of known attack signatures and can compare patterns of activity,

traffic or behavior it identifies in the logs it's monitoring against those signatures so it can recognize when a close match between a signature and current or recent behavior occurs.

There are various types of IDS monitoring approaches:

- *Network-based IDS characteristics:* Network-based IDSs can monitor an entire, large network with only a few well-situated nodes or devices and impose little overhead on a network.
- *Host-based IDS characteristics:* Host-based IDS can analyze activities on the host it monitors at a high level of detail. It can often determine which processes and/or users are involved in malicious activities.
- *Application-based IDS characteristics:* An application-based IDS concentrates on events occurring within some specific application. They often detect attacks through analysis of application log files and can usually identify many types of attack or suspicious activity.

In practice, most commercial environments use some combination of network- and host- and/or application-based IDS systems to observe what's happening on the network while also monitoring key hosts and applications more closely.

### ***Regulating Physical Access to the SCADA Network***

Physical access to your network should be closely monitored:

1. Use built-in Microsoft Windows features such as NTFS to require user authentication when perusing network shares.
2. Do not allow anyone that does not belong to your organization to connect to your network Ethernet or have physical access to your IT server room.
3. Monitor your network regularly for activity that may be suspicious and note the IP addresses when running sniffing software or hardware on the network.
4. Ensure that there are no foreign IP addresses on the list. If you find a foreign IP address, trace route to the IP address. Once you locate where this foreign IP address originates from you can take action. If you are unsure physically disconnect the segment where the potential intruder may be on the network.

## Special Considerations for Wireless Networks

The two most common ways of gaining unauthorized access to a wireless network are by using an unauthorized wireless client, such as a laptop or PDA, or by creating a clone of a wireless access point. If no measures have been taken to secure the wireless network then either of these methods can provide full access to the wireless network.

Many commercial wireless networks are available, these range in price, complexity and level of security provided.

When implementing a wireless network a number of standard security measures can be taken to minimize the chance of an attacker gaining access to the wireless network.

- Approved clients – The access points in the wireless network contains a configurable list of all MAC addresses of the clients that are authorized to gain access to the wireless network. A client not listed in an access point will not gain access to the wireless network.
- Server Set ID (SSID) – This is an identification string that can be configured on all clients and access points in your wireless network. Any client or access point participating on the wireless network must have the same SSID configured. We recommend that SSIDs are not broadcast. We also recommend against enabling 'ad-hoc' connections.
- Wired Equivalent Privacy (WEP) – we recommend that customers do not rely on WEP only security for their wireless networks. WEP security has been shown to be insecure and relatively easy to break.
- We recommend the use of WPA-2 (or at minimum WPA) security protocol, in addition to AES-CCMP or equivalent encryption
- For authentication protocols, our recommendations include EAP-TTLS and EAP-MSCHAPV2, but this may vary depending on the network and client infrastructure in place. Customers should also consider a RADIUS server for authentication against network logins in addition to wireless gateway connections.
- A VLAN solution, splitting wireless and other networks may also be applicable.

VPN (described earlier) was developed to provide secure connections through the Internet to internal corporate networks. A VPN simplistically creates a secure tunnel through open networks such as the Internet or a wireless network. Data transmitted through the tunnel is encrypted on the client and then decrypted and validated in a VPN gateway inside of the wireless access point. Another advantage with using a VPN is that a single solution provides security both for the wireless and wired network and the maintenance cost is lower.

## References (in alphabetical order)

- The Instrumentation, Systems and Automation Society (ISA). 2004.
- Integrating Electronic Security into the Manufacturing and Control Systems Environment.
- North American Electric Reliability Council (NERC). 2004. Implementation Plan – Renewal of Urgent