SCADA Systems Security

Arjun Venkatraman

arjun.dhanush@gmail.com

1. Abstract

The purpose of this paper is to define what SCADA systems are and their application in modern industry and infrastructure, to elucidate the reasons for rising concern over the security of these systems, to analyze the fundamental vulnerabilities and to put forth recommendations for the implementation of security in these systems.

2. Introduction:

Supervisory Control and Data Acquisition systems are basically Process Control Systems (PCS), specifically designed to automate systems such as traffic control, power grid management, waste processing etc.

3. Application

Control systems are used at all levels of manufacturing and industrial processing. A manufacturing plant that employs robotic arms will have a control system to direct robotic arms and conveyor belts on the shop floor. It may use that same system for packaging the finished product and tracking inventory. It may also use a control system to monitor its distribution network. A chemical company will use control systems to monitor tank levels and to ensure that ingredients are mixed in the proper proportions. A Las Vegas casino will use control systems to direct the spray from water fountains in coordination with the lights and music. Control systems are also used in the drilling and refining of oil and natural gas. They are used in the distribution of water and electricity by utility companies, and in the collection of wastewater and sewage. Virtually every sector of the economy employs control systems at all levels.

The term "supervisory control and data acquisition" (SCADA), however, is generally accepted to mean the systems that control the distribution of critical infrastructure public utilities (water, sewer, electricity, and oil and gas).

SCADA systems are still to come into widespread infrastructural use in India. In this country they are being used primarily for automation in industrial production, and to some extent for specialized process control. Ranbaxy Labs[1] and Voltas[2] are two of the companies in India using SCADA systems for process control.

However, they are increasingly common in the US, UK, Australia to name a few countries, where they are used in the control of infrastructural systems such as power, water and waste management, traffic control etc. The economy and infrastructure of these countries is increasingly dependant on SCADA systems.

4. Implementation: How do they work? [3]

SCADA systems are primarily control systems. A typical control system consists of one or more remote terminal units (RTU) connected to a variety of sensors and actuators, and relaying information to a master station. Figure 1 illustrates this generic, three tiered approach to control system design. Figure 2 shows a typical RTU.

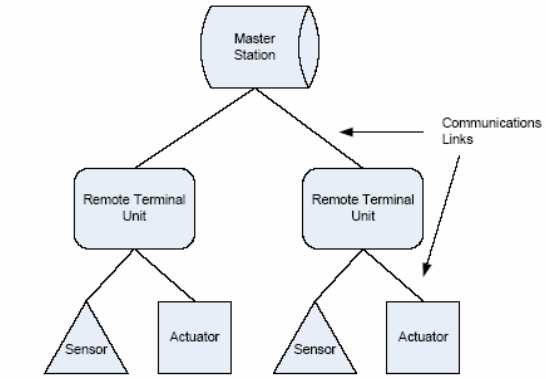

Figure 1: A typical 3-tiered approach to SCADA systems

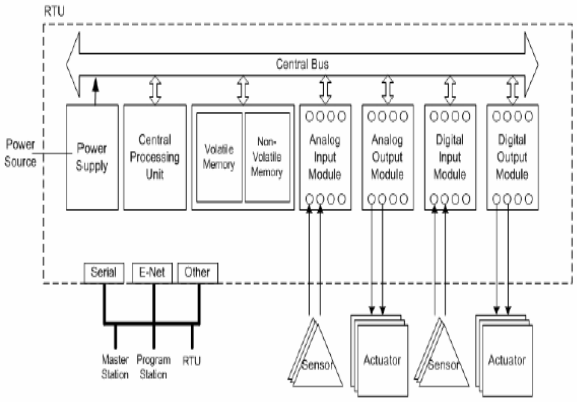

Figure 2: A generic representation of an RTU

4.1 Sensors and Actuators

The philosophy behind control systems can be summed up by the phrase "If you can measure it, you can control it." Sensors perform measurement, and actuators perform control. Sensors get

the data (supervision and data acquisition) and actuators perform actions dependent on this data (control). The processing and determination of what action to take, is done by the master control system (i.e. SCADA).

4.2 Remote Terminal Units (RTUs)

4.2.1 Programmable Logic Controllers

Advances in CPUs and the programming capabilities of RTUs have allowed for more sophisticated monitoring and control. Applications that had previously been programmed at the central master station can now be programmed at the RTU.

These modern RTUs typically use a ladder-logic approach to programming due to its similarity to standard electrical circuits. A RTU that employs this ladder logic programming is called a Programmable Logic Controller (PLC). PLCs are quickly becoming the standard in control systems.

4.2.2 Analog Input and Output Modules

The configuration of sensors and actuators determines the quantity and type of inputs and outputs on a PLC or RTU; depending on the model and manufacturer, modules can be designed solely for input, output, digital, analog, or any combination.

An analog input module has a number of interfaces. Typical analog input modules have 8, 16, or 32 inputs.

Analog output modules take digital values from the CPU and convert them to analog representations, which are then sent to the actuators. An output module usually has 8, 16 or 32 outputs, and typically offers 8 or 12 bits of resolution.

4.2.3 Digital Input and Output Modules

Digital input modules typically are used to indicate status and alarm signals.

A specialized digital input module is used for counting pulses of voltage or current, rather than for strictly indicating "open" or "closed." This functionality, however, can also be implemented using standard input modules and functions found in the ladder-logic programming language of the PLC.

4.3 Master Station

Master stations have two main functions:

• Periodically obtain data from RTUs/PLCs (and other master or sub-master stations)

• Control remote devices through the operator station

Master stations consist of one or more personal computers (PC), which, although they can function in a multi-purpose mode (email, word processing, etc), are configured to be dedicated to

master station duties. These duties include trending, alarm handling, logging and archiving, report generation, and facilitation of automation. These duties may be distributed across multiple PCs, either standalone or networked.

4.4 Communications interfaces

Modern RTUs and PLCs (Programmable Logic Controllers) offer a wide variety of communications means, either built in directly or through a module. The following list represents a variety of transmission methods supported:

- RS-232/RS-442/RS-485
- Dialup telephone lines
- Dedicated telephone lines
- Microwave
- Satellite
- X.25
- Ethernet
- 802.11a/b/g
- Radio (VHF, UHF, etc) [2]

4.5 Design and Implementation Protocols

In SCADA Systems, the three major categories of protocols involve the specifications for design and manufacture of sensors and actuators, specifications for RTUs, and the specifications for communications between components of a control system.

These can be segregated into three levels for a functional representation as shown in Figure 3 below.

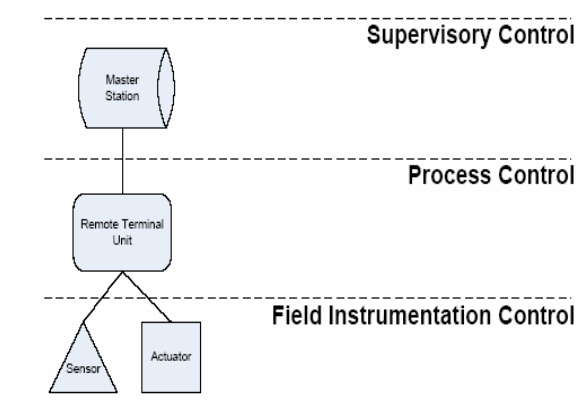

Figure 3: Segregation of the functions of a SCADA system, into a functional representation

These can further be split into nine operational and management components as shown in the table below (Figure 4):

Name	Operation Functions	Management Functions
Mission	X	X
Application Criticality	X	X
Data Sensitivity	X	X
Operating Environment	X	X
System Interfaces	X	X
Communications Requirements	X	X
Hardware	X	
Software	X	
Users and Personnel Action		X

Figure 4: Nine-component approach to analyzing operational and functional requirements of a SCADA system

4.5.1 Mission

The mission defines the reason for the existence of the particular SCADA system under study. In any organization, business systems dictate policy and procedures relevant to the control and monitoring of the process; conceptually, these reside above the Master Station. Similarly, the sensors and actuators directly act upon the physical objects we have been calling the "process." A boundary will normally be defined for components of a SCADA system with similar functional or geographic characteristics.

4.5.2 Application Criticality

Since SCADA systems typically support vital distribution systems, an assessment of the criticality of that system will provide direction on its design and implementation, as well as the type of security measures to apply. Several questions must be answered:

• Are the processes our system is monitoring of a nature that failure of the monitor functions will cause serious harm to the organization's mission?

• Are the processes our system is controlling of a nature that failure of the control functions will cause serious harm to the organization's mission?

• What type and level of failure of our system is acceptable?

• Are the individual components in our system critical to the overall success of the system?

• What type and level of failure of the components is acceptable?

4.5.3 Data Sensitivity

SCADA systems, as noted, typically control critical systems. The question of whether the data processed by the system is sensitive and subject to compromise or loss, must be examined in order to determine how best to protect it. Several questions that should be answered include:

• Is the data returned by the process of a sensitive nature such that loss, modification or compromise of the data, either intentional or unintentional, will cause serious harm to the organization's mission?

• Are the instructions transmitted to the process of a sensitive nature such that loss, modification or compromise of the instructions, either intentional or unintentional, will cause serious harm to the organization's mission?

• What type and amount of system data loss, modification or compromise is acceptable?

• Is the data retained or transmitted by the individual components subject to loss, modification or compromise, either intentionally or unintentionally, to a degree that the system will be affected?

• What level of component data loss, modification or compromise is acceptable?

4.5.4 Operating Environment

SCADA system hardware components are designed for industrial environments, and thus offer robust features for operation in austere environments. These features, however, do not address the management related concerns of security professionals such as data protection and controlled access to components. Understanding how a SCADA system is designed requires understanding the environment it operates in, both for operations functions and management functions. Some questions that should be answered include:

• What environmental factors will affect the process, either negatively or positively?

• What environmental factors will affect the system components, either negatively or positively?

• What is an acceptable level of interference by environmental factors?

• How should these factors be mitigated?

4.5.5 System Interfaces

A complex system will likely have many interfaces, each of which may become an avenue of attack. All interfaces must be closely examined and evaluated in order to understand how it must be protected, both system wide and at the individual components.

Some questions that should be answered include:

• What interfaces exist for data to flow out of the system?

• What interfaces exist for instructions to flow into the system?

• What level of access is required to the feedback data returned by the process? Who requires access to the data?

• What level of access is required to send instructions to carry out commands against the process? Who requires the capability to transmit instructions to the process?

• What protections exist or can be applied to minimize the exposure of vulnerable interfaces by the system?
• What interfaces exist on the components for data or instructions to flow into or out of the component?
• What interfaces exist within the components for data or instructions to flow between components?
• What protections exist or can be applied to minimize the exposure of vulnerable interfaces by the components?

4.5.6 Communications Requirements

Since SCADA systems are designed for reliability, availability and data integrity, extra consideration must be given to confidentiality and authentication. Other issues to consider include protocols employed, types of interfaces required, hardware configuration, and budget. Some questions to answer include:
• What degree of reliability is required?
• What degree of availability is required?
• What degree of data integrity is required?
• What degree of confidentiality is required?
• What overhead and latency in transmission is acceptable?
• What is the environment the communications links must traverse?

The communication requirements are of particular importance to the analysis of security of these systems. Some of the protocols used in SCADA communication are

IEC 60870

IEC 60870 was defined primarily for the telecommunications of electrical system and control information and its data structures are geared to that application. It is the favored standard in the United States for electrical power grid SCADA systems, but is not as popular in Europe.

DNP3

The second protocol specifically designed for SCADA communications is the Distributed Network protocol Version 3 (DNP3). Also created for the electrical industry, it has been adapted by other industry sectors and is the leading protocol employed in Europe for most SCADA applications.

HDLC

Several other SCADA standards exist, primarily High Level Data Link Control (HDLC) and Modbus. HDLC, defined by ISO for point-to-point and multi-point links, is also known as Synchronous Data Link Control (SDLC) and Advanced Data Communication Control Procedure

(ADCCP). It is a bit-based protocol, the precursor to Ethernet, and is rapidly being replaced by DNP3, Industrial Ethernet2, and TCP/IP.

Modbus

Modbus is a relatively slow protocol that does not define interfaces, thus allowing users to choose between EIA-232, EIA-422, EIA-485 or 20mA current loop.

While slow, it is widely accepted and has become a *de-facto* standard--a recent survey indicated that 40% of industrial communication applications use Modbus.

Profibus

Profibus is a German standard that defines three types: Field Message Specification (FMS) for use in general data acquisition systems, Decentralized Peripherals (DP) for use when fast communication is required, and Process Automation (PA) for use when highly reliable and safe communication is required.

Foundation Fieldbus

Foundation Fieldbus is an extension to the 4-20mA standard to take advantage of digital technologies.

UCA

The Utility Communications Architecture (UCA) is a new initiative from the Electric Power Research Institute (EPRI) designed for the electrical industry. It is more than just a protocol definition; it is a comprehensive set of standards designed to allow "plug and play" integration into systems, allowing manufacturers to design off-the-shelf compliant devices. IEEE assumed the UCA standards process in 1999 and has developed extensions for the water industry. Other industries are also examining UCA for suitability.

4.5.7 Hardware and Software (Operational Functions)

When discussing operational functions of a SCADA system, the hardware and software to be used must also be evaluated. In the context of standard SCADA systems, reliability, stability and safety are primary concerns. Adding a security perspective introduces the concept of assurance, or ensuring that the hardware and software have minimal exploitable flaws. Questions to answer include:

• What degree of reliability should the system have with respect to software and hardware?

• What degree of assurance should the system have with respect to software and hardware?

• What degree of reliability do the components require in order to effectively satisfy the system's mission?

• What degree of assurance do the components require?

• Has the hardware been tested for reliability, safety, assurance, stability?

• Has the software undergone a formal documented software development process?

• Have the software and hardware formally analyzed or evaluated by a trusted third party?
• What is the configuration management and lifecycle maintenance process for the software, and the firmware update process for the hardware?
• What maintenance is required for the hardware?

4.5.8 Users and Personnel Actions (Management Functions)

When discussing management functions, the users of the system and its components must also be evaluated. In addition, the automated decision-making that is programmed into the system must be evaluated in the same terms. Some questions to answer include:
• Are the users cleared for all functions of the system? Which functions require clearance?
• What degree of automation of decision-making is required before human intervention is required?
• What training do the users receive?
• What are the different roles required for operating the system?

5. Security Concerns: Why is security of these systems increasingly important?

SCADA systems are not designed with security in mind; rather the priority of developers has been reliability, availability, and speed. This does not mean they cannot be secured, however. If we can understand a particular system's features, functions and capabilities, we can address its limitations.

No inherent security is provided in these systems, since security is not a direct concern when the efficiency of the system is under consideration.

This situation is acceptable as long as the systems are isolated from the outside world.

However in recent times, more and more of these systems are being exposed to open access, in order to promote inter-system communication and interaction.

Two recent trends raising concerns are,

a) Definition of standard interfaces and communication protocols in support of cross-vendor compatibility and modularity

b) Connection of nodes in a SCADA system to open networks such as the Internet.

While these phenomena have definitely brought about an increase in the efficiency of these systems, they have also caused them to inherit all the problems of common, networked information systems. The security of information, both against corruption and misuse, is now an increasing concern for these systems.

This concern for security becomes even more magnified when these systems are deployed in key positions, where they are heavily depended upon for critical operations.

Leaving such key positions unsecured, invites attacks from a number of increasingly dangerous sources, ranging from low-level pranksters to terrorists.

In fact a number of recently seized al Qaeda laptops have revealed the existence of exactly such a danger. Data from these computers reveals that al Qaeda has in fact obtained large amounts of information regarding the infrastructural control systems of the United States, and could well be planning an attack.

In fact, a recent Washington Post[4] article quoted Richard Clarke, advisor, Information Security to the President of the United States as saying, "You will be hacked. What's more, you deserve to be hacked." This was said to industry leaders, whom Clarke accused of spending more on coffee than on information security.

Concern regarding the systems controlling critical operations also increased in the United States after teams of mock intruders from the Energy Department formulated eight different scenarios for an attack on the power grid of the country, all of which work.

When considering the possibility of e-terrorism, what is most fearsome is the fact that if ever an attack was carried out consisting of both physical and electronic components, the result as a whole could be more devastating than the individual components alone.

"The thing that keeps me awake at night is [the thought of] a physical attack on a U.S. infrastructure...combined with a cyber-attack which disrupts the ability of first responders to access 911 systems," says Ron Dick, former head of the FBI's National Infrastructure Protection Center.

6. Analysis of the vulnerabilities of SCADA systems [5]

To assist in determining optimal mitigation strategies, the vulnerabilities are grouped in the categories of

1 1 Data,
2 2 Security Administration,
3 3 Architecture,
4 4 Network, and
5 5 Platforms

Any given control system will usually exhibit a subset of these vulnerabilities, but may also have some unique additional problems.

6.1 Data

Sensitivity levels for control system data are usually not established. An essential characteristic of secure information systems is the identification and classification of data into categories of similar sensitivity. Absence of these fundamental distinctions makes it impractical and fruitless to identify where security precautions are appropriate (for example, which communication links to secure, databases requiring protection, etc).

6.2 Security Administration

Security administration is notoriously lax in the case of control systems, usually the result of poor legacy environment.

The need to manage and administer security is usually overlooked, resulting in informal practices and inefficient management. As experience has proved, any system, which does not have well founded management and administrative policies, will eventually show vulnerabilities. This is the case with control systems as well.

6.3 Architecture

Architecturally, many control systems include centralized data storage and control. This results in the creation of a single-point-of failure.

Occasionally, physical damage to infrastructure assets may be possible through permissible operation of control equipment. An effective control hierarchy would preclude this possibility.

In addition to the above, many implementations of control systems have integrated in-house emergency services such as fire alarms etc, into the control system itself. In view of the pathetic condition of the security of these systems, thoughtless addition of these services into the system adds to the complexity and further increases the vulnerability.

6.4 Networks

Vulnerabilities in control system networks depend on the type of system. Legacy implementations rely on proprietary protocols and low-bandwidth data channels. While there are fewer opportunities for disruptive behavior compared to newer networks, which closely resemble modern TCP/IP systems, problems are inherent because of the technology's age. Security is lamentable. This is due to the fact that these systems were designed in a time when error checking and integrity validation had not gained their present importance. In addition to this, accounting and logging are usually non-existent, making it impossible to find the basis and reason for vulnerabilities. Configuration passwords are often simple and may be limited in effectiveness by the device itself. Wireless links are not secured. Networking equipment in these systems, particularly when physical access is presumed, is acutely vulnerable to attack. Systems

with contemporary technologies like Ethernet, routers, and firewalls have vulnerabilities that are more publicized than the vulnerabilities in the older networks.
Little or no network restriction is implemented within the perimeter of the network, allowing 'telnet hopping' from innocuous network devices to sensitive utility equipment.
Two other factors contribute significantly to the vulnerability of control systems:

1) 1) The blind trust in the capability of PCS links to faithfully transmit data. The geographically sparse PCS network generally forces links of considerable span. These needs are filled by either cabled or wireless connections, which may be exclusively used by the PCS or shared. Shared links are more economically sensible, but many times the PCS systems at either end of the link are not adequately shielded from other entities using it. Furthermore, unsecured information on wireless and shared links is susceptible to eavesdropping or manipulation, and even long or unprotected unshared cable links may be vulnerable to a significant degree. E.g. if the master station and RTU have no security mechanism between them, an attacker could direct a malicious signal via the master station to the RTU and vice versa. Recently a California based security firm, involved in vulnerability assessment of critical infrastructure systems, proved just this sort of vulnerability by accessing a remote substation of a large southwester United States utility company. They did this using a directional antenna and a wireless laptop from a vehicle parked in the vicinity of the substation[6].

2) The connections between the PCS and external networks. An external network is any network that is not part of the PCS. Examples include interfaces to an administrative (non-automation) network or connections to other PCS systems for information transfer or mutual control. Often, interfaces to external systems assume that the outside network can be trusted, which leaves PCS security dependent on one or more organizations. This includes backdoor network access for strategic partners or IT consultants, which are not secured by adequate firewall measures, command logging or privilege control.
With the world moving towards outsourcing, and strategic partnerships, security implementation suffers due to the absence of a common standard. Designers frequently omit to secure the backdoors left by them for easy tuning of a system, resulting in disaster at a later stage.
Dial-up modem access is unencrypted, with a general lack of authentication practices.
The data transfer that takes place over telephone lines, or wireless networks is usually either unencrypted, or encrypted with a weak algorithm, which does not take much effort to crack. The primary reason for this is a requirement to save time/resources on encryption.
However, the result is that the signals can be easily analyzed and if so wished, modified by an attacker.

7. Case Studies and Scenarios:

Below are listed some of the known attacks, and possible scenarios, which exploit the vulnerabilities in SCADA systems

7.1 Australian sewage release

In March-April 2000, Vitek Boden, a disgruntled employee, accessed the sewage management system of Maroochy Shire on the Sunshine Coast, Queensland, Australia and released large amounts of sewage into public areas. What Boden did, was to gain access to the system, and alter data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way. The central computer was unable to exercise proper control and, at great inconvenience and expense, technicians had to be mobilized throughout the system to correct faults at affected pumping stations.

It is true that Boden had access to inside knowledge about the system, and access to proprietary software, by virtue of being an ex-employee of the firm, which provided the telemetry equipment to the Maroochy Shire administration. However, vulnerabilities in the system also contributed to the breach of security.

For one, the system did not use adequate wireless protection measures, making it vulnerable at the network level. Also, a strong security policy would have revoked credentials to the designers of the system after it was deployed.

7.2 Slammer Worm

In January 2003, a Slammer worm bypassed the corporate network firewall disabling a safety monitoring system for nearly five hours and the “Plant Process Computer” for nearly six hours at the Ohio Davis-Besse nuclear power plant operated by FirstEnergy Corp. A Davis-Besse contractor who had logged into an unsecured network had spread the worm into the internal corporate network via one of several unclearly documented backdoor connections to deliver the Slammer worm. The point to be noted is that the Slammer worm exploits a vulnerability in the MS SQL Server 2000. This implies that vulnerabilities in the platform or the operating environment are in fact, inherited by the SCADA system.

8. Security Recommendations: How may security be implemented?

Computer security in the present context deals mainly with information stored on systems, or information in transit. This is not adequate for the protection of infrastructural systems such as SCADA networks

Traditional information assurance does not adequately protect against cyber attacks on SCADA control systems in which the countermeasures used may compromise the safety or operability of the SCADA control systems. The United States Federal Government has begun to lead in the protection of critical infrastructure but it will rest in the hands of the commercial industries to develop and implement an enterprise assurance policy to improve the SCADA control systems security posture. Several steps can be taken to assist in the improvement of the implementation and management of policies and procedures.
Some of these are:

8.1 Implement Common Criteria evaluations on SCADA control systems.

As standards and technology continued to change, the United States and Europe began working on standards for a common evaluation criteria for information security. The various evaluation criteria projects begun by the United States and Europe merged into a single International Common Criteria project ISO/IEC 15408 with the intent to standardize methods for evaluating information systems security. SCADA control systems products should be included and evaluated based on the Common Criteria standards to ensure the implementation of SCADA products does not compromise the security or safety of the critical infrastructure.

8.2 Adopt "best practices" and procedures.

Most of the vulnerabilities of computer systems are well known and documented.
Adopting "best practices" (i.e. implementing secured network devices and operating systems, and patch management) and procedures (i.e. backups) will allow administrators to protect systems not only from the cyber threats, but also normal system failures

8.3 Isolate & harden SCADA networks.

Isolation of SCADA networks to a closed-loop network with limited & highly restrictive access from physical and electronic outside sources would help in mitigating the threat to them.
If the connection of a SCADA network to the Internet or another open network is essential, appropriate buffers and checks should be placed between the layers.
Segmented network topologies could increase the level of restrictive access and survivability.
Utilization of authentication mechanisms such as passwords, tokens and biometrics could guard against unauthorized access.
Enabling strong encryption for all data communications would further minimize the risk of a security breach.

Vulnerability and threat assessments should be performed regularly on current and newly implemented systems.
Risk assessments should be conducted on each interconnection between the SCADA and corporate enterprise network.
All unnecessary networks should be disconnected, especially if an open pathway to the Internet is formed.
Unnecessary services that are not required to support the operation of the SCADA control systems should be removed or disabled.
Firewalls and intrusion detection systems should be implemented, to not only prevent entries but also monitor unintentional security breaches on the SCADA and corporate enterprise network.
Detailed network knowledge should be restricted.
Communicating IP addresses and DNS names is unnecessary and can be costly if in the wrong hands. Implementing single-sign-on procedures (via an administrative management portal) will pass authorized users to the command prompt of a device without knowledge of the IP address or password.
Removing all 'open' ports/backdoors for third party access would reduce the risk arising from the possibility of a simple port scan resulting in the discovery of a vulnerability by an attacker.
Limiting access privileges on a device and port level is advisable. There is no reason for PBX maintenance staff to access a data center database or for IT consultants to access all network devices.
Implementing a virtual private network (VPN) for administrative channel access and partitioning dependent upon privileges provides additional levels of security.

8.4 Provide Leadership, Accountability and Law Enforcement support.

An effective security policy requires the backing and commitment from senior management. Provide for individual accountability through protected system logs or the equivalent. Perform audits, site surveys and penetration tests to ensure the security effectiveness. Increase support for law enforcement to track malicious access and software, including support for additional R&D for forensic tools and technologies.

8.5 Establish enterprise security policy through a life-cycle risk management process.

Combining the Common Criteria evaluations and an enterprise assurance policy on all SCADA control systems and interconnections of the computer systems could greatly minimize risk by ensuring that the security of one system is not undermined by vulnerabilities of other systems

connected to it. Standardizing a process that will minimize the risks associated across the shared network infrastructure and computer systems includes activities to:
Develop a methodology for identifying critical infrastructure assets and evaluate security requirements.
Perform vulnerabilities threat assessment.
Develop regular security monitoring and warning process.
Develop and plan for a response and remediation process against potential vulnerabilities and further incidents.

8.6 Establish a configuration management program.

Define a configuration management methodology, model, and application that can be used during the design, implementation, and operation of the SCADA systems. Evaluate the integration of custom developed software, hardware, and firmware to ensure that the integration into the system design complies with the system security architecture and the integrity of each product is maintained. Assess the impact, risk, and resource requirements associated with changes, and then implement changes effectively and efficiently.
The lowest cost is not the most efficient for use for critical SCADA applications.

8.7 Establish an Enterprise Assurance Awareness Program.

Provide support on wider awareness of the importance and need for security, promoting the understanding of security vulnerabilities and corrective measures, and in facilitating greater awareness for the SCADA network. Awareness relies upon reaching broad audiences with attractive packaging techniques.

8.8 Develop Continuity Plans.

Develop disaster recovery plans to ensure the safe and continued operation of the SCADA network caused by unexpected and undesirable occurrences or contingencies that interrupt the normal SCADA operations.

9. Conclusion:

In summation, it is easy to observe that SCADA technology holds a lot of promise for the future. The economic and performance advantages of this type of system are definitely attractive. However, since the vulnerabilities of current implementations are in proportion to the advantages, it is essential that measures be taken to mitigate the risk to current systems and to ensure that future systems are designed with sound policies and design.

We in India stand a lot to gain from such systems, and having the foreknowledge of the possible risks can take adequate measures to ensure our continued safety and prosperity.

In the words of Master Sun Tzu from “The Art of War”:
Those who are first on the battlefield, and await the opponents are at ease; those who are last, and head into battle are worn out.

10. References

1) 1) **“Citect Used on FDA Validated Process to Monitor Reactor Profiles Ranbaxy Labs”**
K. Subramaniam, Managing Director, Masibus Process Instruments Pvt. Ltd.

2) 2) **“VSCADA”** © - Voltas Supervisory Control and Data Acquisition, http://www.voltasacnr.com/default.html

3) 3) Implementation details based on:
“An Architectural Framework for Describing Supervisory Control and Data Acquisition (SCADA) Systems”
Michael P. Ward, US Naval Postgraduate School, September 2004

4) 4) **“Cyber-Attacks by Al Qaeda Feared”**
Barton Gellman, Washington Post, June 27, 2002; Page A01

5) 5) Vulnerability analysis based on:
“Common Vulnerabilities in Critical Infrastructure Control Systems”
Stamp, Dillinger, Young, DePoy, Sandia National Laboratories, May 2003.

6) 6) **“SCADA vs. the hackers”**
Alan S. Brown, American Society of Mechanical Engineers, http://www.memagazine.org/backissues/dec02/features/scadavs/

7) 7) Security recommendations based on:
“SCADA Systems Security”
Michael A. Young, SANS Institute, February 2004