Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

SCADA Information Security Management Guide

by

MAMOS, Jakub

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Associate Professor, MISSM

SCADA Information Security Management Guide

by

MAMOS, Jakub

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Associate Professor, MISSM

Reviews Committee:

Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

SCADA Information Security Management Guide

Jakub Mamos

1 Introduction

Supervisory Control and Data Acquisition (SCADA) systems within the corporate environment are changing into information systems. As such, they also are becoming information assets within the organization and, therefore, they need to be protected appropriately, possibly via existing IT standards and strategies.

There appears to be support for this approach as shown in the following excerpts:

- Modern SCADA, or even SCADA in modern times, must be addressed and managed in a style appropriate for a critical IT system [1].
- SCADA infrastructure should also employ a “ring of defence” as well as an IT control framework, SCADA security policy, security plan, and implementation guidance. These should be based on industry standards such as COBIT and ISO 17799 [2].

This paper will show that employing an information security management practice standard, specifically the ISO/IEC 17799:2005 and supplementing it with SCADA-specific existing information where necessary, to provide insight into specific requirements and limitations of process control systems can indeed provide a meaningful guide for IT security staff in developing a security management guide for SCADA systems.

This approach will provide assurance for business continuity, minimal business risk, and maximum return on investments and business opportunities as determined by executive direction and security management practice as it will create a consistent benchmark for an organization and its entities/business partners to communicate and establish information security controls and requirements for SCADA systems.

By employing this approach, the following goals can be achieved:

- Creation of the guide document that can used to bring together existing SCADA security information (academic research, industry standards, best practice document) into one body of knowledge
- Utilization of such document as a starting point by IT security managers and IT auditors tasked with identifying, deploying and auditing security management practice for the SCADA systems
- Identification and gap analysis in regards to SCADA systems security management in the organization

This research will take each of the relevant sections (omitting scope, terms and definitions, and structure sections) from the ISO/IEC 17799:2005 and match them with the corresponding SCADA security information (research papers, best practice documents, industry relevant drafts documents, standards etc), when possible and/or necessary. Additionally, a table will summarize the sources of SCADA security information matched to each of the sections of the ISO/IEC 17799:2005.

1.1 SCADA overview

Supervisory Control and Data Acquisition (SCADA) refers to systems that are used to monitor and control industrial processes in water supply systems, electric power generation, transmission and distribution, gas and oil pipelines, and others.

A SCADA system includes input/output signal hardware, controllers, human machine interface (HMI), networks, communication, database and software.

In the Supervisory Control component, SCADA usually encompasses a central system that monitors and controls a complete site or a system spread out geographically over networks for alarms and processing data status. Depending on the response received from these sites and their devices, appropriate supervisory type of commands can be then delivered back.

The main control mechanisms are performed automatically by a Remote Terminal Unit (RTU) or by a Programmable Logic Controller (PLC). Host control functions are restricted to basic site over-ride or supervisory level capability. This means that while PLC will usually control day-to-day operations, the SCADA system has a built-in ability to allow an operator to override the controls when necessary. A simple SCADA system overview is shown in the Figure 1 SCADA SYSTEM.

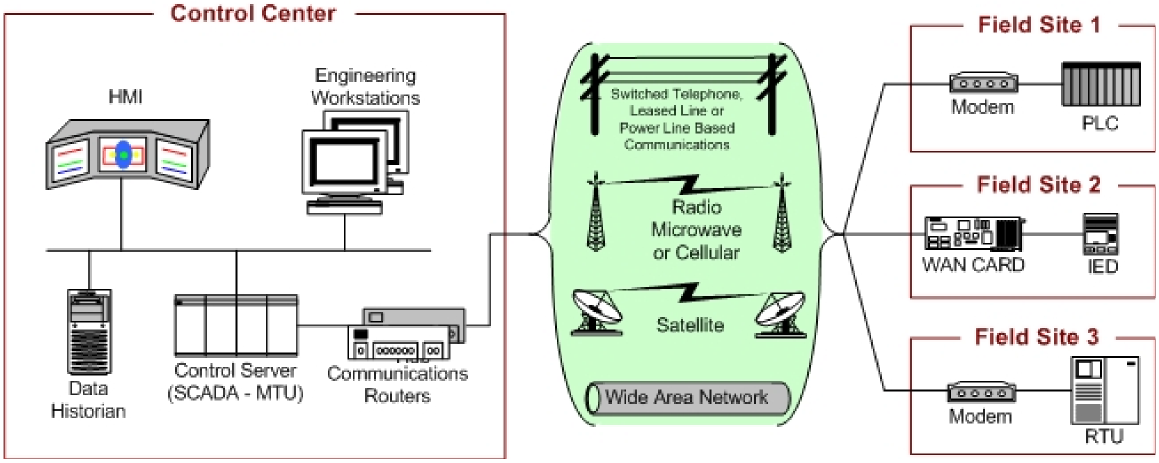

Figure 1 SCADA SYSTEM [4]

The Data Acquisition part of SCADA begins at the RTU or PLC level and can include meter readings and equipment status information that are communicated to SCADA in defined intervals. After the data is collected, it is compiled and formatted to be available for the operator to make supervisory decisions that may be required to adjust or over-ride normal (PLC) controls. Data may also be collected in a data collection system, often referred to as a data historian, that allows the collected data to be further analyzed and provide the business with information derived from such analysis.

1.2 SCADA security

The initial requirements for SCADA were driven primarily by the concern for performance, reliability and safety. These requirements were coupled with vendor specific hardware optimized for the specific environment, utilizing proprietary communication protocols and generally employing solutions that were isolated in their own environment, without any connection to the business information systems. Due to that uniqueness and lack of connectivity, early SCADA deployments minimized the need for security other than physically securing the access to the devices and operation locations.

With the proliferation of information technology, there has been a shift in using IP enabled devices and protocols and increased reliance on such solutions in SCADA networks. Such solutions are usually deployed to deliver more efficient management, better utilization of an organization's resources, and a business' need for the data provided by the SCADA systems, however, this increased interconnectivity and technical solution "homogenization" of the environment has been identified (NISCC Good Practice Guide Process Control and SCADA Security [5]) as the reason for increased exposure of the previously isolated systems to new threats that they are not equipped to deal with.

An additional overview of the SCADA security history and the threats and attacks against them can be found in the Securing SCADA Systems by Ronald L. Krutz [3]. The material in this book can provide useful references for the IT security professionals trying to gain the understanding of the SCADA and its specific requirements in regards to the information security. This book also makes an argument that the existing IT expertise combined with the understanding of SCADA-specific requirements can be useful to securely manage the SCADA systems.

> A number of conventional IT security controls can be applied to SCADA systems if the specific needs of these systems are taken into account. Government, industrial organizations, and standards groups have identified the need for additional research and development into SCADA system security and are developing guidelines for protecting SCADA systems from cyberattacks [3].

1.3 Introduction and overview of the 17799:2005

> Information security is achieved by implementing a suitable set of controls, including policies, processes, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes [6].

ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

- risk management;
- security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management; and
- compliance.

ISO/IEC 17799:2005, is the latest version of the ISO standard of good practice for information security management. The ISO 17799 started as a code of practice published by the UK Department of Trade and Industry, which was released as a British Standard (BS) 7799 by the British Standard Institute (BSI) in 1995. After a period of international consideration and review, BS 7799 was adopted by ISO and was released as ISO 17799 in December 2000 and then revised and reissued in June 2005 as the ISO/IEC 17799:2005. According to the International

Organization for Standardization (www.iso.org), an international body responsible for the ISO standards, ISO/IEC 17799:2005 is going to be renamed into the ISO 27002 sometime in 2007 moving it into line with the other ISO 27000 series standards listed below:

- ISO/IEC 27000 (a standard vocabulary for the Information Security Management Systems (ISMS) standards) - unpublished;
- ISO/IEC 27001 (the certification standard against which organizations' ISMS may be certified) - published in 2005;
- ISO/IEC 27002 (the proposed new name for ISO 17799) due to be renamed in 2007;
- ISO/IEC 27003 (new ISMS implementation guide) - unpublished;
- ISO/IEC 27004 (standard for information security measurement and metrics) - unpublished;
- ISO/IEC 27005 (standard for risk management) – unpublished;
- ISO/IEC 27006 (guide to the certification/registration process) - unpublished;
- ISO/IEC 27007 (guideline for auditing information security management systems) - unpublished;
- ISO/IEC 27799 (guidance on ISO 17799 in the healthcare industry) - unpublished.

The ISO/IEC 17799:2005 provides a comprehensive outline for developing organization of the security management practice. The ISO/IEC 17799:2005 will be used in the course of this research to provide the key areas and concepts needed to be addressed in developing the security management practice for SCADA systems. This approach will be enhanced by SCADA specific security research that will populate areas outlined by the ISO/IEC 17799:2005 as needed. Derived from this research will be key points/findings that should provide specific context for an organization when addressing security management of the SCADA systems under its control.

2 Risk Assessment (ISO 17799:2005 Sec. 4)

Risk assessment should identify, quantify and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing these risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems [6].

Existing SCADA security information:

Organizations must consider the potential consequences resulting from an incident on an ICS[1]. Well-defined policy and procedures lead to mitigation techniques designed to thwart incidents and manage the risk to eliminate or minimize the consequences. The degradation of the physical plant, economic status, or national confidence could justify mitigation. For an ICS, a very important aspect of the risk assessment is to determine the value of the data that is flowing from the control network to the corporate network. In instances where pricing decisions are determined from this data, the data could have a very high value. The fiscal justification for mitigation has to be derived by the cost benefit compared to the effects of the consequence. However, it is not possible to define

[1] In the NIST 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, ICS (Industrial Control System) is used to describe both SCADA (Supervisory Control and Data Acquisition), and distributed control systems (DCS). The authors of the NIST 800-82 state that, unless the specific distinction is made, the term ICS applies universally to both types of systems (SCADA and ICS).

> a one-size-fits-all set of security requirements. A very high level of security may be achievable but undesirable in many situations because of the loss of functionality and other associated costs. A well-thought-out security implementation is a balance of risk versus cost. In some situations the risk may be safety, health, or environment-related rather than purely economic. The risk may result in an unrecoverable consequence rather than a temporary financial setback [4].

The NISCC *Good Practice Guide Process Control and SCADA Security [5]* provides the "Principles of Good Practice" that divides the Risk Assessment process into **Assessing Business Risk** and **Undertaking Ongoing Assessment of Business Risk**.

Assessing Business Risk is divided into the following:

- Understanding the system – formal inventory audit and evaluation of SCADA systems. This process should include capturing and documenting answers to questions such as: what systems exist, what is their respective role, what are the business and safety criticalities, what are the locations of the systems, who are the owners and custodians of the systems and how do the systems interact with the rest of the infrastructure. The formal inventory of the systems should also drive the requirement of putting these systems under the formal change management process within the organization.
- Understanding the threats – formal identification of the threats facing the SCADA systems. The threats need to be identified and documented. They can typically include some or all of the following: unauthorized access (both accidental and malicious), denial of service, loss of data, etc.
- Understanding the impacts – identification of the potential impacts of the realized threats to the SCADA systems. Examples of the impacts can include loss of reputation, violation of the regulatory requirements, financial loss, etc. If the SCADA systems are a part of the critical infrastructure or provide services that affect human life and safety, the identification process of the potential impact should include that information.
- Understanding the vulnerabilities – assessing the vulnerabilities affecting SCADA systems. This can be done via a review of the environment and the existing safeguards.

Undertaking Ongoing Assessment of Business Risk Principle in the NISCC document states that the organization should proactively monitor and identify changes to its SCADA systems as they will drive the re-evaluation of the business risks and possible need to improve the existing safeguards [5].

3 Security Policy (ISO 17799:2005 Sec. 5)

This section describes the objective for the security policy within the organization as follows:

> To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
>
> Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization [6].

Existing SCADA security information:

> Security policy for SCADA administration translates the desired security and reliability control objectives for the overall business into enforceable direction and behaviour for the staff to ensure secure SCADA design, implementation and operation [3].
>
> Consistent security policy alignment throughout the plant is required. Control system operators and engineers are usually very interested and capable of doing a good job securing the control systems, but they often lack a direction from senior management. As a result, a quality of the security efforts (such as anti-virus management) can vary widely, putting even well-secured systems in jeopardy. Site-wide security policies for the control process area must be developed [7].

The following framework shown in the Figure 2 SCADA security policy framework developed by Dominique Kilman and Jason Stamp from Sandia National Laboratories [8], addresses SCADA security policy set in a systematic way based on practical research into such systems and their requirements and as such, is meant to provide a map of the areas that need to be considered by the organization when undertaking development of the security policy set for the organization. It can be tailored to specific needs and expanded as the new areas emerge. The framework can be also utilised as a starting point for an organization to identify existing documents and then have them used to populate appropriate areas in the framework.

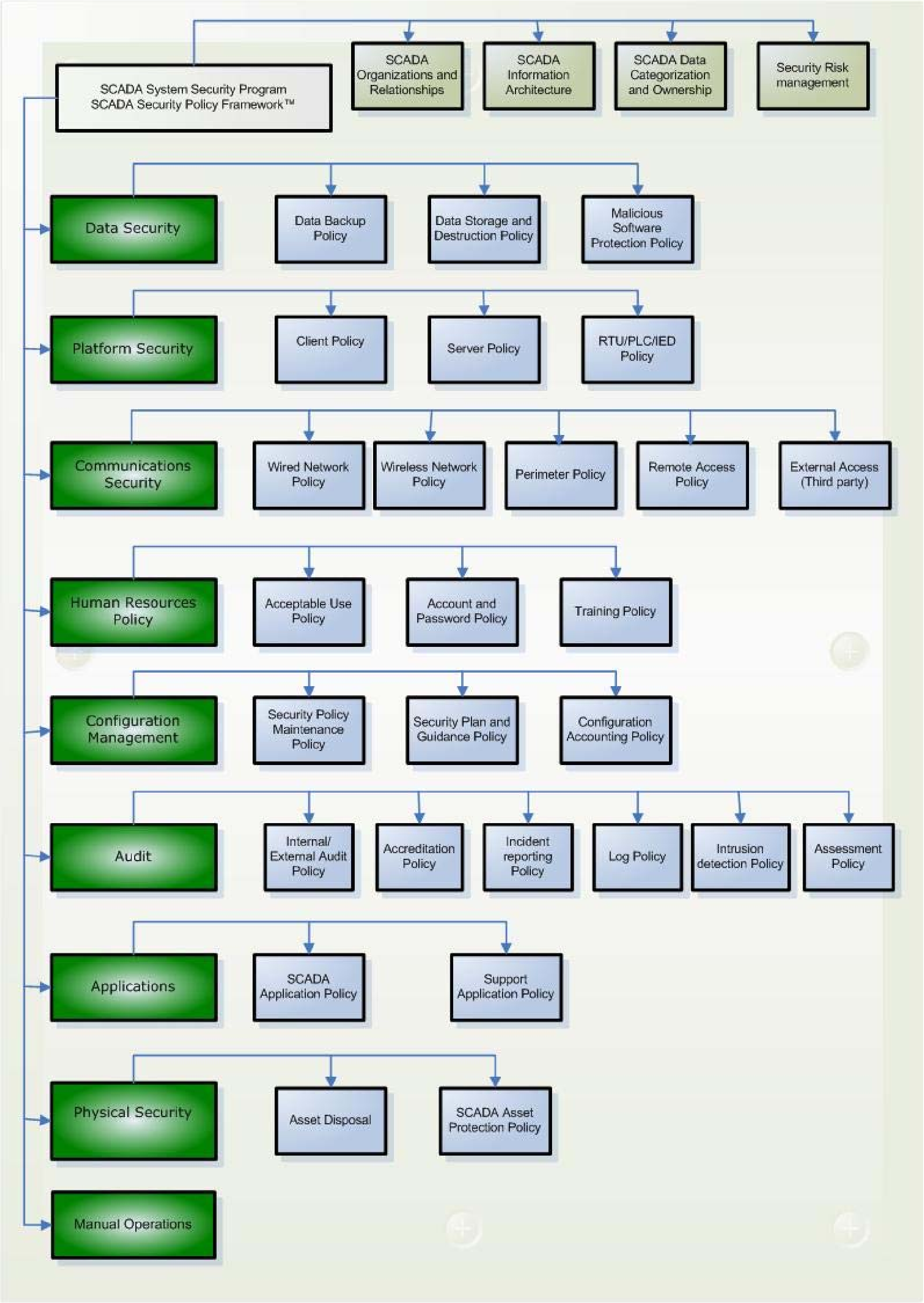
SCADA System Security Program
SCADA Security Policy Framework™
SCADA Organizations and Relationships
SCADA Information Architecture
SCADA Data Categorization and Ownership
Security Risk management
Data Security
Data Backup Policy
Data Storage and Destruction Policy
Malicious Software Protection Policy
Platform Security
Client Policy
Server Policy
RTU/PLC/IED Policy
Communications Security
Wired Network Policy
Wireless Network Policy
Perimeter Policy
Remote Access Policy
External Access (Third party)
Human Resources Policy
Acceptable Use Policy
Account and Password Policy
Training Policy
Configuration Management
Security Policy Maintenance Policy
Security Plan and Guidance Policy
Configuration Accounting Policy
Audit
Internal/ External Audit Policy
Accreditation Policy
Incident reporting Policy
Log Policy
Intrusion detection Policy
Assessment Policy
Applications
SCADA Application Policy
Support Application Policy
Physical Security
Asset Disposal
SCADA Asset Protection Policy
Manual Operations

Figure 2 SCADA Security Policy Framework

SCADA SYSTEM SECURITY PROGRAM
Introduction to the target system, context for the rest of the Policy Set, definition of the SCADA operations within the organization.

DATA SECURITY POLICY
Description of the treatment of the data categories and their requirements (as defined in the Security Program).

PLATFORM SECURITY POLICY
Identification of the secure configuration defaults required for SCADA systems.

COMMUNICATION SECURITY POLICY
Identification of the paths used by data travelling the network, segments of the network within the environment related to SCADA, external connections and protection mechanisms employed for different security zones.

HUMAN RESOURCES POLICY
Identification of the job requirements (e.g., citizenship, educational) and hiring policy for SCADA personnel (e.g., background checks including security clearances).

AUDIT POLICY
Definition of the scope of the auditing and assessment activities; identification of the person/role/position responsible for the scheduling and reviewing the audit/assessment results.

APPLICATION POLICY
Identification of applications used by the SCADA systems and description of the security measures used when deploying, configuring and using such applications, to provide assurance for the security needs of SCADA systems; detailed description of the program-level access, training and test/development requirements.

PHYSICAL SECURITY POLICY
Identification and description of the security mechanisms used to protect SCADA systems from physical damage, unauthorised physical access and destruction. Specification for control and monitoring of the above mechanisms.

MANUAL OPERATION POLICY
Detailed description of the manual processes and procedures (e.g., backup, chain of command, periodic inspections, training, disaster recovery) that need to be implemented when the day-to–day automated processes get interrupted.

4 Organization of Information Security (ISO 17799:2005 Sec. 6)

This area of the ISO/IEC 17799:2005 deals with information security governance mechanisms including internal organization and external parties.

4.1 Internal organization

The organization should have a management framework for information security with senior management providing direction and support for it. Some of the key points include a roles and responsibilities definition for the information security function, cooperation and coordination activities of all relevant functions in the organization in support of the information security; proper authorisation of the IT facilities; appropriate confidentiality agreements; in place contacts with relevant authorities (e.g., law enforcement), information partners, and special interest groups. Finally there should be provisions in place to independently review the in place structures.

Existing SCADA research seems to validate the approach stated above at least in regards to the roles and responsibilities and coordination and cooperation from the other functions within the organization as stated below:

> It is essential for a cross-functional cyber security team to share their varied domain knowledge and experience to evaluate and mitigate risk in the ICS. At a minimum, the cyber security team should consist of a member of the organization’s IT staff, a control engineer, security subject matter experts, and a member of the management staff. Security knowledge and skills should include network architecture and design, security processes and practices, and secure infrastructure design and operation. For continuity and completeness, the cyber security team should also include the control system vendor(s). The cyber security team should report directly to site management or the company’s CIO/CSO, who in turn, accepts complete responsibility and accountability for the cyber security of the corporate and ICS networks. Management level accountability will help ensure an ongoing commitment to cyber security efforts [4].

It would be prudent in any effort to evaluate security management practice of SCADA systems to address the proper authorisation of the IT facilities, confidentiality agreements, contacts with relevant authorities (e.g., law enforcement, regulatory organizations) and special interest groups.

4.2 External parties

This section of the ISO/IEC 17799:2005 identifies the idea of protecting the information security practice by not allowing it to be compromised by the introduction of third party products, services and contractual relationships. It also identifies the need to assess the risks and mitigate them where the third parties are concerned.

The document that best addresses the issues connected to the third parties in the SCADA environment is the NISCC *Good Practice Guide Process Control and SCADA Security [5]*. This best practice document addresses the topic of third parties within its section 7.3. That section is divided into the three subsections that deal with managing the risks from the vendors, support organizations and supply chain. Each of these three subsections lists an extensive number of principles that can be applied to assure the appropriate protection of business assets by not allowing their compromise by the third parties.

5 Asset Management (ISO 17799:2005 Sec. 7)

This section of the standard deals with the organization's understanding of its information assets and their management. The subsections deal with the responsibility for assets where the need for accountability, ownership and the inventory of the information assets needs to be clearly stated and managed. The other subsection involves the classification of the information according to its need for security protection and appropriate labelling.

Even though it would appear that this area of the standard is omitted in the existing SCADA security research, it is very evident that it would be important to address information assets within the SCADA systems in a holistic manner. Some of the examples for the SCADA assets that need to be managed as part of the information security practice include information produced by the SCADA systems in the data acquisition cycle, technical manuals, blue prints, specific procedures, etc. This section proves the benefit of taking the ISO/IEC 17799:2005 to provide a clear framework for managing SCADA systems as an information asset.

6 Human Resources (ISO 17799:2005 Sec. 8)

This section includes three subsections for managing the human resources security requirements.

The Prior to Employment subsection deals with defining and documenting the processes such as pre-employment screening (background checks, interview process) and clearly communicating hiring policies, job descriptions, terms and conditions of employment and legal rights and responsibilities of employees or contractors. The possible additional requirements for SCADA systems might require an enhanced level of background checks (security clearances) for personnel in contact with the SCADA systems that are part of the critical infrastructure.

The During the Employment subsection deals with detailed expected and required behaviour of the organization's employees, contractors and visitors. This includes documented processes for acknowledgement and adherence to management approved security policies and procedures of the organization, provision for appropriate security awareness training and regular updates in organizational policies and procedures as pertaining to employees and contractor job function and disciplinary process dealing with violations. It is important that the document set mentioned above be clearly defined and available to all employees and contractors through a number of clearly defined means such as an employee handbook or an intranet web site.

Termination or Change of Employment outlines the need for defining and documenting the following:

- responsibilities for performing an employment termination or change of employment,
- ensuring that employees, contractors and third party users surrender all of the organization's assets in their possession upon termination of their employment, contract or agreement, and
- removing access rights of all employees, contractors and third party users to information and information processing facilities upon termination or adjusting them upon change.

This section is self evident in its importance with the existing research supporting this type of approach to managing the SCADA personnel throughout their tenure with the organization. NIST 800-82 [4] document suggests that staff members that have access to SCADA systems should be evaluated even more closely than their non-SCADA counterparts in the organization, possibly requiring government-issued security clearances.

7 Physical and Environmental Security (ISO 17799:2005 Sec. 9)

This section deals with the physical protection for the assets against malicious or accidental damage or loss, overheating, loss of main power, etc. This section is divided into the secure areas and equipment security subsections dealing with the need for layered physical controls to protect sensitive facilities from unauthorized access and protection against physical damage, fire, flood, theft, etc., both on and off-site respectively.

Historically, the area of physical and environmental security has been very well understood and addressed in the SCADA environments mostly because it is directly related to the safety of humans and equipment.

> The physical protection of the cyber components and data associated with the ICS must be addressed as part of the overall security of a plant. Security at many ICS facilities is

> intimately tied to plant safety. A primary goal is to keep people out of hazardous situations without preventing them from doing their job or carrying out emergency procedures.
>
> Gaining physical access to a control room or control system components often implies gaining logical access to the process control system as well. Likewise, having logical access to systems such as main servers and control room computers allows an adversary to exercise control over the physical process. […] In addressing the security needs of the system and data, it is important to consider environmental factors. For example, if a site is dusty, systems should be placed in a filtered environment. This is particularly important if the dust is likely to be conductive or magnetic, as in the case of sites that process coal or iron. If vibration is likely to be a problem, systems should be mounted on rubber bushings to prevent disk crashes and wiring connection problems. In addition, the environments containing systems and media (e.g., backup tapes, floppy disks) should have stable temperature and humidity. An alarm to the process control system should be generated when environmental specifications such as temperature and humidity are exceeded [4].

Given this level of understanding of physical and environmental security factors in SCADA environments, the challenge in establishing the security management practice might be present mostly in documenting the policies and procedures associated with the controls in place.

8 Communications and Operations Management (ISO 17799:2005 Sec. 10)

This section of the ISO/IEC 17799:2005 describes security controls for systems and network management. Some of the subsections are very obvious and self explanatory (Operational procedures and responsibilities, system planning and acceptance, third party service delivery management, exchange of information, back-up) and can be addressed by developing appropriate processes and documentation and implementing them. The other subsections are listed and addressed below.

8.1 Protection against malicious and mobile code

This subsection addresses the need for anti-malware controls in the information system environment as expressed by the following objective statement:

> To protect the integrity of software and information.
>
> Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code.
>
> Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code [6].

There is a long standing concern in the SCADA community about the impact of the commonly used enterprise class anti-virus solutions on the systems that are part of the SCADA environments. The issue is examined in detail in the *Using Anti-virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts* draft document released in 2006 [9]. The document provides a good collection of background information on ICS and anti-virus software, implementation guidance (gathered from the SCADA end users of such solutions) and “good practices” with a focus on minimizing performance impacts and methodology for developing custom performance test procedures for assessing SCADA systems for any performance impacts associated with anti-virus software practices.

8.2 Network security management

This subsection describes the controls needed for secure network management, network security monitoring and network services such as firewalls and private network communications. The objectives for this subsection state:

> To ensure the protection of information in networks and the protection of the supporting infrastructure.
>
> The secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection.
>
> Additional controls may also be required to protect sensitive information passing over public networks [6].

There is a wealth of SCADA-specific security research in this area. One of the outstanding sources providing guidance for the network services security in the SCADA environment is *The IAONA Handbook for Network Security – Draft/RFC v0.[10]*. This document provides an overview of the security concepts and network services in relation to the SCADA environments. Another excellent source for SCADA specific research in this area is the *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks [11]*. This paper summarizes firewall architectures, designs, deployment and management practices commonly deployed in SCADA networks. Additionally, it provides analysis of these elements and scores of their effectiveness.

8.3 Media handling

This subsection deals with protection of the documents and computer media containing data, system information, etc. It addresses the handling, transportation, storage and disposal of backup media, documents, voice and other recordings, test data, etc., and the procedures that define these procedures. It lists the objective as:

> To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities. Media should be controlled and physically protected [6].

Some SCADA specific guidance in this areas can be drawn from the section 6.2.7 of NIST as shown below:

> Media assets include removable media and devices such floppy disks, CDs, DVDs and USB memory sticks, as well as printed reports and documents. Physical security controls should address specific requirements for the safe maintenance of these assets and provide specific guidance for transporting, handling, and erasing or destroying these assets. Security requirements could include safe storage from loss, fire, theft, unintentional distribution, or environmental damage [4].

8.4 Monitoring

For this subsection, the ISO/IEC 17799:2005 states the following:.

> Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified. An organization should comply with all relevant legal requirements

> applicable to its monitoring and logging activities. System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model [6].

Existing SCADA security information:

> Diligent use of auditing and log management tools can provide valuable assistance in maintaining and proving the integrity of the ICS from installation through the system life cycle. The value of these tools in this environment can be calculated by the effort required to re-qualify or otherwise re-test the ICS where the integrity due to attack, accident, or error is in question. The system should provide reliable, synchronized time stamps in support of the audit tools.
>
> Monitoring of sensors, logs, IDS, antivirus, patch management, policy management software, and other security mechanisms should be done on a real-time basis where feasible. A first-line monitoring service would receive alarms, do rapid initial problem determination and take action to alert appropriate facility personnel to intervene.
>
> System auditing utilities should be incorporated into new and existing ICS projects. These tools can provide tangible records of evidence and system integrity. Additionally, active log management utilities may actually flag an attack or event in progress and provide location and tracing information to help respond to the incident.
>
> There should be a method for tracing all console activities to a user, either manually (e.g., control room sign in) or automatic (e.g., login at the application and/or OS layer). Policies and procedures for what is logged, how the logs are stored (or printed), how they are protected, who has access to the logs and how/when are they reviewed should be developed. These policies and procedures will vary with the ICS application and platform. Legacy systems typically employ printer loggers, which are reviewed by administrative, operational, and security staff. Logs maintained by the ICS application may be stored at various locations and may or may not be encrypted [4].

Other relevant information from the SCADA research is provided by Dale Peterson in his *Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks* [12] paper. Here the author outlines the approaches to the monitoring the SCADA network environments. This topic is taken step further by Matthew Franz and Venkat Pothamsetty in the *ModbusFW Deep Packet Inspection for Industrial Ethernet* [13]. Here the authors go into more technical detail by looking at possible development and implementation of the filtering devices that are suited for the specific needs of the industrial control network traffic.

8.5 Electronic commerce services

This subsection provides guidance on security management controls for the e-commerce and it would most likely not be applicable to the SCADA environments.

9 Access Control (ISO 17799:2005 Sec. 11)

The objective in this section of the standard is stated as follows:

> To control access to information.
>
> Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements [6].

The subsections of the main section deal with documenting, managing and controlling of the user access via authentication and authorization to all of the information assets of the organization.

Some of the specific items are user access management, user responsibilities, network, operating system and application access controls as well as remote access to the resources.

Existing SCADA security information:

- Company-wide policies: Developing short, simple, and easy to follow guidelines for every employee is pertinent for any security strategy to be successful. A key to successful implementation is posting the policies where they can be easily accessed and read by everyone.
- Two levels of authentication: No employee should be allowed access to the SCADA network unless there is a separate login account that resides on a separate network, and requires two levels of authentication. This can be accomplished through an assigned user id and password along with either an RSA SecurID access token that changes every minute, a biometrics mechanism, a smart card, or through other separate physical access type devices.
- Password modification: It should be mandatory that passwords change at least once every 90 days, and that they are at least eight characters, including numbers, letters, and a special character that would be hard to guess. Passwords representing family names, events, pets, dictionary words, passwords that are the same as the user id, and the like, should be disallowed.
- Remote access: If remote access is to be allowed, only operators and managers who must control this information should have access. Remote access should be done through a company-supplied laptop that has VPN encryption installed on the machine, and if possible, dial-back modems should be setup [14].

The above can be taken as a sample more than a guideline, especially in regards to the specific settings and technical implementations. For more detailed ,guidance on implementing appropriate access control mechanisms for SCADA environments is provided in section 6.2 of the NIST 800-82 [4].

10 Information Systems Acquisition, Development and Maintenance (ISO 17799:2005 Sec. 12)

This section of the standard outlines the necessity for information security to be taken into account in the processes for specifying, building/acquiring, testing and implementing systems as the security functionality should be implemented based on a risk analysis that determines security requirements based on an assessment of threats, vulnerabilities and impacts.

The SCADA world has made significant progress in recent years to provide the guidance on addressing some of these areas. Specifically the SCADA and Control Systems Procurement Project has provided the community with the *Cyber Security Procurement Language for Control Systems [15]* document (currently at draft version 1.5) that summarizes security principles to be considered when designing and procuring control systems components. This document also provides specific examples to be used in such situations.

Another excellent document to address this section is NIST's *System Protection Profile - Industrial Control Systems [16]* document that provides a very detailed basis for installing security retrofits or upgrading existing ones as well as the design of new systems.

The Cryptographic Controls subsection of the Information Systems Acquisition, Development and Maintenance section identifies the need for a cryptography policy that should be defined and include roles and responsibilities, digital signatures, non-repudiation, management of keys and digital certificates, etc. The existing SCADA security research supports the notion that protecting the confidentiality of data by using encryption mechanisms is important and should be addressed. The most notable is the effort by the American Gas Association to develop a standard, AGA-12, *Cryptographic Protection of SCADA Communications* [17], to protect SCADA communication links from a variety of active and passive attacks. Some of the material addressed by this effort might provide useful inputs into understanding the complexity and challenges present in this domain as well as provide insights into developing meaningful approach to managing cryptographic controls in the SCADA environment.

10.1 Technical vulnerability management

This subsection focuses on the technical vulnerabilities and processes around their management. The objective of this subsection is formulated as follows:

> To reduce risks resulting from exploitation of published technical vulnerabilities.
>
> Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use [6].

Existing SCADA security information very much supports the approach presented in the ISO/IEC 17799:2005 as shown in this segment from the NISCC *Good Practice Guide Process Control and SCADA Security:*

> Implement processes for deployment of security patches to process control systems.
>
> - These processes should be supported by audit and deployment tools.
> - The processes should make allowance for vendor certification of patches, testing of patches prior to deployment and a staged deployment process to minimize the risk of disruption from the change.
> - Where security patching is not possible or practical, alternative appropriate protection measures should be considered [5].

11 Information Security Incident Management (ISO 17799:2005 Sec. 13)

This section deals with information security events, incidents and weaknesses and the way they should be reported and managed. The following two subsections with their objectives show the items that need to be accounted for when managing the information security. They are as follows:

11.1 Reporting in information security events and weaknesses

> To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
>
> Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of

organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact [6].

11.2 Management of information security incidents and improvements

To ensure a consistent and effective approach is applied to the management of information security incidents.

Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents. Where evidence is required, it should be collected to ensure compliance with legal requirements [6].

Existing SCADA security related information provides a number of good sources for addressing the information security incident management as outlined in the two subsections above. Among them, the third instalment of the NISCC Good Practice Guide Process Control and SCADA Security[18] comes to the forefront. This document outlines and describes the principles for the information security incident management and then provides detailed guidance for the organizational considerations when implementing them. The principles used in this document are as follows:

- Create a Process Control Security Response Team (PCSRT) to respond to security incidents.
- Ensure that appropriate incident response and business continuity plans are in operation for all process control systems.
- Ensure that all electronic security plans are regularly maintained, rehearsed and tested.
- Establish an early warning system that notifies appropriate personnel of security alerts and incidents.
- Establish processes and procedures to monitor, assess and initiate responses to security alerts and incidents. Possible responses may include: increase vigilance, isolate system, apply patches, or mobilize the Process Control Security Response Team.
- Ensure all process control security incidents are formally reported and reviewed.
- Lessons learned should be fed back to improve plans and update policy and standards [18].

Additionally, the Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security [4] provides the following items that should be included in the incident response planning for the SCADA system:

Classification of Incidents. This item stresses the importance of categorizing the possible incidents that might occur in the SCADA environments. This provides for identification and classification of possible incidents in regards to their potential impact and likelihood. This allows for a development of clear response for each potential incident.

Response Actions. This item draws on the previous one by identifying and documenting the specific responses that can be used to address specific incidents. Having a plan documenting the types of incidents and the response to each type will provide clear guidance during the time of the incident when clarity and decisiveness is most needed. Such a plan should also include templates to be used for communication, reports and note taking during the time of the incident.

Recovery Actions. The results of the intrusion might be minor or could cause many problems in the ICS. Prior analysis should be conducted to determine the sensitivity of the physical system being controlled to failure modes in the ICS. In each case, step-by-step recovery actions should be documented so that the system can be returned to normal operations as quickly and safely as possible.

The NIST document also states the importance of the review, approval and a "buy-in" from the various stakeholders including operations, management, organized labor, legal, and safety in the preparation of the incident response plan.

Yet another document that provides relevant information in relation to SCADA systems in this area is the "Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems" [19]. Some of that information includes clearly defined characteristics for categories for vulnerabilities and mitigation strategies.

12 Business Continuity Management (ISO 17799:2005 Sec. 14)

The objective for this section of the ISO/IEC 17799:2005 is stated as follows:

> To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities. The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organization. Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available [6].

Existing SCADA security information supports the approach presented by the ISO/IEC 17799:2005. Here, the Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security has an exhaustive quote on managing the BCP in the SCADA environments:

> For the purposes of ICS cyber security, it is recommended that long-term outages (disaster recovery) and short-term outages (operational recovery) should be considered [in the BCP]. Because some of potential interruptions involve man-made events, it is

> also important to work collaboratively with the physical security organization to understand the relative risks of these events and the physical security countermeasures that are in place to prevent them. It is also important for the physical security organization to understand which areas of a production site house data acquisition and control systems that might have higher-level risks. Before creating a business continuity plan (BCP) to deal with potential outages, it is important to specify the recovery objectives for the various systems and subsystems involved based on typical business needs. There are two distinct types of objectives: system recovery and data recovery. System recovery involves the recovery of all communication links and processing capabilities, and it is usually specified in terms of a Recovery Time Objective (RTO). This is defined as the time required to recover all communication links and processing capabilities. Data recovery involves the recovery of data describing production or product conditions in the past and is usually specified in terms of a Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated [4].

It is clear that the point expressed in the ISO objective is something that applies to the SCADA environments and should be addressed. SCADA systems are part of the business operations and they do need to have their BCP developed, documented and implemented. Such plans should be a subset of the overall BCP for an organization.

13 Compliance (ISO 17799:2005 Sec. 15)

The first part of this section deals with the compliance with the legal requirements, internal policies and standards. This section can only be addressed with the understanding of the specific legal regulations and legislations as related to the function and jurisdiction of the specific SCADA environment. That understanding and the following guidance as to what specific legal requirements might be impacting the security management practice of the SCADA environment in this area should be delivered from the organization’s legal department.

The next subsection of the Compliance section addresses the need for the compliance with the security policies and standards as well as the technical compliance and it is stated as follows:

> The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls [6].

The need for compliance with the internal security policies and standards is driven by the organization’s approach to mitigating business risks. The understanding of what industry standards might be applicable to the specific SCADA environment will have to be developed and appropriate steps taken to ensure that this compliance is achieved.

The final note on these two subsections is to state that most of the industry standards regulations in the SCADA environment will most likely incorporate objectives that are related to having a sound security management practice in place. Implementing the security management practice prior to having to comply with a standard such as the North American Electric Reliability Corporation (NERC) Reliability Standards [20] will allow the organization to achieve this compliance much faster as well as provide due diligence in the process.

13.1 Information systems audit considerations

This subsection stresses the importance and the need for the controlled management of the technical audit process. This is expressed as the following objective:

> To maximize the effectiveness of and to minimize interference to/from the information systems audit process. There should be controls to safeguard operational systems and audit tools during information systems audits. Protection is also required to safeguard the integrity and prevent misuse of audit tools [6].

Existing SCADA security information supports the above approach as illustrated by the following quote:

> Auditing is a critical step for the enforcement of the procedural and technical security measures (controls or control practices) in the system. The existence of an effective auditing program that contributes meaningfully to SCADA security meets requirements for security enforcement in the security policy and plans. Requirements for the necessary detail and repetition of the audits must be adequate to ensure compliance with the security controls but below the threshold of nuisance. Auditing may be performed internally or externally, with some mixture of both an optimal solution [4].

14 Conclusion

It is important to understand that an information security management practice is essential in order to sufficiently meet the security and business objectives of an organization by providing the assurance that its assets are protected in order to maintain legal compliance, competitiveness, profitability and commercial image. Since SCADA systems are business assets, establishing and maintaining the security management practice to ensure their protection needs to be undertaken as a necessary business practice.

In employing ISO/IEC 17799:2005, and possibly the ISO 27002 in the future, it is possible to establish a clear set of information security objectives, standards and processes for an organization with SCADA systems. This step can done by:

- identifying the areas that need to be addressed by the organization and then developing and implementing the appropriate processes or,
- consciously deciding not to address a specific area as it: might not apply, or may be addressed by existing controls employed by the organization, or it might not be applicable to the SCADA system in place.

When the specific areas are identified as needing to be addressed, the direction provided by the ISO/IEC 17799:2005 should be combined with the existing information (industry best practices, academic research, standards and regulations) and expertise that might exist in the organization already. This approach should provide an organization with a clear path to achieving information security in the SCADA environment.

The approach shown here can be used effectively in developing a security management practice for SCADA systems, however, the SCADA world has been slow in adopting this view. The notion that SCADA systems can be classified as information systems and business assets and their security management practice developed accordingly is still resisted as shown in the following quote:

> ICSs have many characteristics that differ from traditional Internet-based information processing systems, including different risks and priorities. Some of these include significant risk to the health and safety of human lives, serious damage to the environment, and financial issues such as production losses, negative impact to a nation's economy, and compromise of proprietary information. ICSs have different performance and reliability requirements and use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency can sometimes conflict with security in the design and operation of control systems (e.g., requiring password authentication and authorization should not hamper emergency actions for ICSs.) [4].

This statement shows that there is still a disconnect and misunderstanding between the traditional SCADA world and how it perceives the capabilities of the information technology systems. The arguments stated in the quote above can be easily refuted: "significant risk to the health and safety of human lives" - hospitals with patient and drug information, "financial issues" – banking sector and their systems, "negative impact to nation's economy" - stock markets. However, it is also important to note that the importance of looking at SCADA security from a management and a process level is more evident today than it was even a few years ago. The documents like the NISCC series of Good Practice Guide for SCADA systems and even the NIST 800-82 Special Publication draft are the examples of the new found holistic approach.

The present day situation requires that security management be addressed to sufficiently meet the security and business objectives of an organization by providing the assurance that its assets are protected in order to maintain legal compliance, competitiveness, profitability and commercial image. The approach recommended in this paper can lead to that goal. Additionally, it can provide the benefit of having the same underlying standard within an organization for all of its security management practice (if the ISO/IEC 17799:2005 has been chosen for that purpose).

Standardizing the security management practice for SCADA systems will be the definite future trend. In taking this approach, the business organization (which is ultimately the owner of the SCADA systems in the enterprise) will ensure that information security is being achieved by both being efficient and cost effective and ensuring that that technical issues and differences are addressed.

BIBLIOGRAPHY

1. Stamp Jason, et al., Sustainable Security for Infrastructure SCADA Sandia National Laboratory. URL: http://www.tswg.gov/tswg/ip/SustainableSecurity.pdf

2. Haji, F.; Lindsay, L.; Shaowen Song *Practical security strategy for SCADA automation systems and networks* Electrical and Computer Engineering, 2005. Canadian Conference on Volume , Issue , 1-4 May 2005 Page(s): 172 – 178

3. Krutz Ronald L. (Nov 2005) *Securing SCADA Systems* Wiley Press

4. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, Special Publication 800-82 INITIAL PUBLIC DRAFT. URL: http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf

5. NISCC Good Practice Guide Process Control and SCADA Security. URL: http://www.cpni.gov.uk/docs/re-20051025-00940.pdf

6. International Standard ISO/IEC 17799:2005 Information technology — Security techniques — Code of practice for information security management.

7. Creery, A.; Byres, E.J., *Industrial Cybersecurity for power system and SCADA networks* Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual Volume , Issue , 12-14 Sept. 2005 Page(s): 303 – 309

8. Kilman D., Stamp J., Framework for SCADA Security Policy Sandia National Laboratories. URL: http://www.sandia.gov/scada/documents/sand_2005_1002C.pdf

9. Falco, Joe, et al., Using Anti-virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts, 2006, Draft Document. URL: http://www.isd.mel.nist.gov/projects/processcontrol/AV_Guide_PCSF_Draft_Release_20060530.pdf

10. *The IAONA Handbook for Network Security – Draft/RFC v0.4*, Industrial Automation Open Networking Association (IAONA), Magdeburg, Germany, 2003 URL: http://www.innominate.de/images/stories/documents/publikationen/2003/public_iaona-security.pdf

11. NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, National Infrastructure Security Coordination Centre, London, 2005 URL: http://www.cpni.gov.uk/docs/re-20050223-00157.pdf

12. Peterson D., Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks, ISA, 2004, URL: http://www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=35311

13. Franz M., Pothamsetty V., ModbusFW Deep Packet Inspection for Industrial Ethernet, Critical Infrastructure Assurance Group, Cisco Systems, 2004, URL: http://www.threatmind.net/papers/franz-niscc-modbusfw-may04.pdf.

14. Fernandez J., Fernandez A., SCADA SYSTEMS: VULNERABILITIES AND REMEDIATION, Journal of Computing Sciences in Colleges Volume 20 , Issue 4 (April 2005)

15. Cyber Security Procurement Language for Control Systems URL: http://www.msisac.org/scada/documents/16nov06-scada-procurement_.pdf

16. System Protection Profile - Industrial Control Systems URL: http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.pdf

17. Cryptographic Protection of SCADA Communications URL : http://intelligrid.info/IntelliGrid_Architecture/New_Technologies/Tech_AGA-12_Cryptographic_Protection_of_SCADA_Communications_Gene.htm

18. NISCC Good Practice Guide Process Control and SCADA Security Guide 3. Establish response capabilities. URL: http://www.cpni.gov.uk/docs/re-20061107-00755.pdf

19. Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems US Department of Energy September 2006 URL: http://www.oe.energy.gov/DocumentsandMedia/Composite_Report_1-22-07.pdf

20. NERC Reliability Standards URL: http://www.nerc.com/~filez/standards/Reliability_Standards_Regulatory_Approved.html

21. Ralston P., Graham J., and Patel S.,. Literature Review of Security and Risk Assessment of SCADA and DCS Systems Intelligent Systems Research Laboratory, Technical Report TR-ISRL-06-01 Dept. of Computer Engineering and Computer Science July 2006 URL: http://louisville.edu/speed/cecs/facilities/ISLab/tech%20papers/ISRL-TR-06-01.pdf

22. Duggan, David, *Penetration Testing of Industrial Control Systems*, Report SAND2005-2846P, Sandia National Laboratories, 2005, URL: http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf

ANNEX

Standard Section Number	Section Title		Existing SCADA Information Sources
4	**Risk Assessment and Treatment**		NISCC *Good Practice Guide Process Control and SCADA Security [5]* Sandia National Laboratories *Sustainable Security for Infrastructure [1]* "Literature Review of Security and Risk Assessment of SCADA and DCS Systems" *[21]*
5	**Security Policy**		Sandia National Laboratories *Framework for SCADA Security Policy [8]* NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]*
5.1	*Information security policy*		
6	**Organization of information security**		Sandia National Laboratories *Sustainable Security for Infrastructure [1]* NISCC *Good Practice Guide Process Control and SCADA Security [5]*
6	*Internal Organization*		
6.2	*External Parties*		
7	**Asset Management**		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]*
7.1	*Responsibility for assets*		
7.2	*Information classification*		
8	**Human resources security**		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]* NISCC *Good Practice Guide Process Control and SCADA Security [5]*
8.1	*Prior to employment*		
8.2	*During employment*		
8.3	*Termination or change of employment*		
9	**Physical and Environmental Security**		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]* *Practical security strategy for SCADA automation systems and*
9.1	*Secure Areas*		
9.2	*Equipment Security*		

			networks [2]
10	**Communications and Operations Management**		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]* NISCC *Good Practice Guide Process Control and SCADA Security [5]*
10.1	*Operational Procedures and responsibilities*		
10.2	*Third party service delivery management*		
10.3	*System planning and acceptance*		
10.4	*Protection against malicious and mobile code*		*Using Anti-virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts [9]*
10.5	*Backup*		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]*
10.6	*Network Security Management*		NISCC *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks [11]*
10.7	*Media handling*		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]*
10.8	*Exchange of Information*		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]* NISCC *Good Practice Guide Process Control and SCADA Security [5]*
10.9	*Electronic Commerce Services*		This section would most likely not be applicable to security management practice for SCADA systems.
10.10	*Monitoring*		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]* Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks [12] Modbus FW Deep Pocket Inspection [13]

			The IONA Handbook for Network Security [10]
11	**Access Control**		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]* NISCC *Good Practice Guide Process Control and SCADA Security [5]* SCADA Systems: Vulnerabilities and Remediation [14] NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks [11]
11.1	*Business Requirement for Access Control*		
11.2	*User Access Management*		
11.3	*User Responsibilities*		
11.4	*Network Access Control*		
11.5	*Operating system access control*		
11.6	*Application and Information Access Control*		
11.7	*Mobile Computing and teleworking*		
12	**Information systems acquisition, development and maintenance**		SCADA and Control Systems Procurement Project *Cyber Security Procurement Language for Control Systems [15]*
12.1	*Security requirements of information systems*		
12.2	*Correct processing in applications*		
12.3	*Cryptographic controls*		AGA-12, *Cryptographic Protection of SCADA Communications [17]*
12.4	*Security of system files*		SCADA and Control Systems Procurement Project *Cyber Security Procurement Language for Control Systems [15]*
12.5	*Security in development and support processes*		SCADA and Control Systems Procurement Project *Cyber Security Procurement Language for Control Systems [15]*
12.6	*Technical Vulnerability Management*		*Practical security strategy for SCADA automation systems and networks*[2]
13	**Information security incident management**		NISCC *Third Instalment in the Good Practice Guide Process Control and SCADA Security [18]* Sandia National Laboratories *Sustainable Security for Infrastructure [1]* US DoE Lessons Learned from Cyber Security Assessments of SCADA and Energy Management[19]
13.1	*Reporting information security events and weaknesses*		
13.2	*Management of information security incidents and improvements*		
14	**Business Continuity Management**		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]*
14.1	*Information security aspects of business continuity management*		

15	**Compliance**		NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. [4]*
15.1	*Compliance with legal requirements*		Depending on the jurisdiction and the industry.
15.2	*Compliance with security policies and standards, and technical compliance*		Depending on the industry and the organization.
15.3	*Information Systems audit considerations*		Sandia National Laboratories *Penetration Testing of Industrial Control Systems[22]*