INL/CON-06-01317
PREPRINT

Process Control System Cyber Security Standards – an Overview

52nd International Instrumentation Symposium

Robert P. Evans

May 2006

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Process Control System Cyber Security Standards – An Overview

Robert P. Evans, PhD
Idaho National Laboratory

KEY WORDS:

Process Control System, Cyber Security, Standards

ABSTRACT

The use of cyber security standards can greatly assist in the protection of process control systems by providing guidelines and requirements for the implementation of computer-controlled systems. These standards are most effective when the engineers and operators, using the standards, understand what each standard addresses. This paper provides an overview of several standards that deal with the cyber security of process measurements and control systems.

INTRODUCTION

One of the first things a company needs to do when implementing a cyber security program is establish a cyber security policy. This will be the foundation of all cyber security efforts in the future. This policy should be founded on sound principles and practices, the kind that are found in industry standards.

Much of the industry of the United States is dependent on the use of computers for their operation both in information technology (IT) and control systems. These systems are at risk due to increasing cyber intrusions that impact normal operations. Data from the United States Computer Emergency Readiness Team (U.S. CERT) intrusion tracking site show a near-exponential increase in cyber attacks on IT systems over the last decade [1], and there is a growing body of evidence suggesting that attacks against the control systems of utilities and other critical infrastructures are also increasing [2]. This recognition of control system vulnerability to cyber attacks was emphasized by the President's Commission on Critical Infrastructure Protection. [3]

Industry is responding with an interest in how to address cyber threats to their critical control systems. The application of common, proven methods for vulnerability reduction, documented and shared in industry standards and guidelines, can be an important part of a strategy for achieving such reductions at an acceptable cost. This paper presents a description of several documents, consisting of standards, technical reports, and guidelines, relating to the cyber security. The goal of this paper is to assist users of control systems, especially those not familiar with cyber security standards, in providing an increased understanding of cyber security standards that influence the security of process control systems.

ADDRESSING THE PROBLEM

Although the primary focus of this paper is on process control systems, several standards that apply to IT systems are also included because they are considered benchmarks in the area of cyber security. While not written specifically for process control systems, they provide a starting point for developing organization guidance. They offer guidelines and voluntary directions for cyber security management and

provide a high level, general description of the areas currently considered important when initiating, implementing or maintaining information security in an organization. [4]

Electronic intrusions are coming from both inside and outside of companies. [5] Although many of the statistics referenced here deal primarily with IT systems, it would appear that attacks against control systems are increasing proportionally. These intrusions come in the form of innocent mistakes by an operator, inappropriate testing by internal organizations, use of inappropriate security policies, attacks by disgruntled employees or former employees, viruses, and from external attackers. Vulnerability of the control system to the external attacks has increased with increased external connections and with the increased use of commercial off the shelf technologies, for which exploits already exist.

Many businesses, as they have become aware of the problems, have begun to respond to these security threats because of increased potential liability and threat of regulatory compliance. Much of the problem can be reduced by application of security principles and practices contained in the cyber security standards. Because of differences in systems, it is important to use the appropriate standards. They can assist in understanding vulnerabilities in a system, help identify specific system problems, and suggest solutions. For these standards to be of benefit, it is necessary to understand something of what each addresses.

This document provides a reference at a point in time. Cyber security standards are evolving at a very fast pace and hence it is necessary for the user to stay current on what standards exist and their current status. This paper only presents a brief overview of some of the standards that exist, with an emphasis on those standards that address control system cyber security.

STANDARDS

A few standards, relevant to control systems in addition to three IT-focused standards, are reviewed. Several of these are standards, some still in draft form, others are reports or guidelines. It is recognized that this is not a complete list of standards that deal with cyber security or even control system security, but this study can help identify those standards that might be of benefit to an organization that uses process control systems.

The following sections present a brief description of the standards and their current status (as of January 2006). Table 1 provides a summary of the various standards addressed in this paper. A more detailed analysis of the relationship of the requirements, presented in some of these standards, is contained in two reports: A Summary of Control System Security Standards Activities in the Energy Sector [6] and Comparison Study of Industrial Control System Standards against the Control Systems Protection Framework Cyber-Security Requirements [7].

There is some uncertainty with the actual status of some of these documents. A given document may be referred to as a standard in one reference and a report in another. This may be due in part to the various levels of standards. Informative standards provide goals that would assist in securing a system and suggested ways to meet these goals, but do not contain specific requirements, therefore they are much the same as a report. On the other hand, Normative standards contain specific requirements that must be followed. Therefore there is probably more difference between Normative and Informative standards than between Informative standards and reports or guidelines. These designations are not critical to the application of the principles contained in the documents. Although every effort has been made to determine the actual designation by the issuing organization, in some cases there may still be some confusion.

Table 1. Cyber security standards.

Organization	Number	Name	Focus	Sector	Status
AGA(1)	AGA 12-1	Cryptographic Protection of SCADA Communications	Encryption	Energy - Gas	Report Not released
API(2)	API 1164	Pipeline SCADA Security	Control System	Energy – Oil and Gas	Standard Released 09/2004
CIDX(3)	Version 2.0	Guidance for Addressing Cybersecurity in the Chemical Sector	Control System	Chemical	Guidelines Released 05/2005
IEC(4)	IEC 62351	Data and Communications Security	Communications		Standard Not released
IEEE(5)	IEEE 1402	IEEE Guide for Electric Power Substation Physical and Electronic Security	Physical and Control System	Energy - Electrical	Standard Released 01/30/2000
ISA(6)	SP99.00.01	Manufacturing and Control Systems Security; Concepts, Models and Terminology	Control System Cyber security	Cross Sector	Standard Not released
ISA(6)	SP99.00.02	Establishing a Manufacturing and Control Systems Security Program	Control System Cyber security	Cross Sector	Standard Not released
ISA(6)	TR99.00.01	Security Technologies for Manufacturing and Control Systems	Control System Cyber security	Cross Sector	Technical Report Released 10/2004
ISA(6)	TR99.00.02	Integrating Electronic Security into the Manufacturing and Control Systems Environment	Control System Cyber security	Cross Sector	Technical Report Released 10/2004
ISO(7)	ISO/IEC 17799	Information technology – Security techniques – Code of practice for information security management	Information Technology	Cross Sector	Standard Released 06/15/2005
ISO(7)	ISO/IEC 27001	Information technology – Security techniques – Information security management systems - Requirements	Information Technology	Cross Sector	Standard Released 10/15/2005
NERC(8)	NERC 1200	Cyber Security	Control System	Energy - Electrical	Standard Released 08/13/2003
NERC(8)	NERC CIP-002 through 009	Cyber Security	Control System	Energy - Electrical	Standard Not released
NERC(8)	NERC Security Guidelines	Security Guidelines for the Electricity Sector	Control System	Energy - Electrical	Guidelines Released 06/14/2002
NIST(9)	SPP-ICS	System Protection Profile – Industrial Control Systems	Control System	Cross Sector	SPP Released 05/26/2004
NIST(9)	SP800-53	Recommended Security Controls for Federal Information Systems	Information Technology	Cross Sector	Guidelines Released 02/2005
NIST(9)	SP800-82	Guide for SCADA and ICS Security	Control System	Cross Sector	Guidelines Not released

1 AGA – American Gas Association
2 API - American Petroleum Institute
3 CIDX - Chemical Industry Data Exchange
4 IEC - International Electrotechnical Commission
5 IEEE - Institute of Electrical and Electronic Engineers
6 ISA – Instrumentation, Systems, and Automation Society
7 ISO - International Organization for Standardization
8 NERC - North American Electric Reliability Council
9 NIST - National Institute of Standards and Technology

AGA 12 – Cryptographic Protection for SCADA Communications General Recommendations

Scope: When completed, American Gas Association (AGA) Report No. 12 [8, 9] will consist of a series of documents recommending practices designed to protect Supervisory Control and Data Acquisition (SCADA) communications against cyber attacks by focusing on securing the communication link between the field devices and the control servers in the control center. [10] It will define one part of a strategy to protect gas, water, wastewater, and electric utility SCADA systems from cyber attack by specifying a means of encrypting the serial data before they are transmitted through vulnerable media such as radio or telephone lines. [11] Part 1. "Background, Policies & Test Plan," will address the background, security policy fundamentals, and a test plan that generally apply to all areas of cryptographic protection of SCADA systems while Part 2. "Retrofit Link Encryption for Asynchronous Serial Communications," will focus on retrofit link encryption for asynchronous serial communications. It will contain the functional requirements and detailed technical specifications for AGA-12-compliant retrofit devices.

Status:
Report
Not released - There are currently two parts of the standard, both in draft: Part 1 is in the final stage of balloting and Part 2 is in first draft. Additional parts are also planned.

API 1164 – Pipeline SCADA Security

Scope: American Petroleum Institute (API) 1164 [12] is a SCADA security standard that provides guidance to the operators of oil, gas and liquid pipeline systems for managing SCADA system integrity and security. It is specifically designed to provide the operators with a description of industry practices in SCADA security and to provide the framework needed to develop sound security practices within the operator's individual companies. It addresses access control, communication security (including encryption), information distribution classification, physical issues (including disaster recovery and business continuity plans), operating systems, network design, data interchange between enterprise and third-party support/customers, management systems, and field devices configuration and local access. [13] Although the standard does address physical security, the primary thrust of this document is cyber security and access control.

Status:
Standard - Informative
Released – First Edition, September 2004

CIDX - Guidance for Addressing Cybersecurity in the Chemical Sector, version 2.0

Scope: The Chemical Industry Data Exchange (CIDX) *Guidance for Addressing Cybersecurity in the Chemical Sector,* [14] describes in detail the key elements of a cyber security management system (CSMS) applicable to manufacturing and control systems, business IT systems, and value chain systems in the chemical sector. It includes references to the Security Code, which provides cyber requirements and management practices for the chemical industry, as well as to other international and domestic cyber security guidelines and standards. It provides best practices and guidance to include in corporate policies, procedures, and practices. Actions for the protection of control systems and information for increasing awareness of the problems, are presented. It attempts to provide practical guidance by first identifying the base-level set of functions key to a CSMS, followed by additional guidance known to be employed by some companies in the chemical sector. [14]

Status:
Guidelines
Released – Version 2.1, May 2005

IEC 62351 - Data and Communication Security

Scope: International Electrotechnical Commission (IEC) 62351 [15], when released, will be a multipart standard developed by the International Electrotechnical Commission. It will address information security for the control of power systems. There are currently seven parts planned, of which one is in draft. Part 1 of the standard will provide the background on security for power system operations and an introduction to the remaining parts of the standard, primarily to introduce the reader to various aspects of information security as applied to power system operations. [15] Part 2 will contain definitions of terms and acronyms. Parts 3 through 6 will cover security requirements for various protocols, while Part 7 will address network and system management. [16]

Status:

Standard - Informative

Not released - Parts 1, 3, 4, 5, and 6 were submitted as Committee Drafts (CDs) in May 2005. Comments from National Committees on the CDs were received and responded to during the last meeting of WG15 in September. Parts 3, 4, and 6 have been updated and will then be submitted for CDV (Committee Draft Vote). Part 5 is being updated. Parts 2 and 7 are moving forward. [16] The current status of each of the parts can be found at Reference [17].

IEEE 1402-2000 – IEEE Guide for Electric Power Substation Physical and Electronic Security

Scope: Institute of Electrical and Electronic Engineers (IEEE) *Guide for Electric Power Substation Physical and Electronic Security,* IEEE 1402-2000, [18] is a standard sponsored by the Power Engineering Society/Substations of IEEE. This standard identifies and discusses security issues related to human intrusion at electric power supply substations. Various methods and techniques that are being used to mitigate both physical and electronic intrusions are also presented. [18] Although IEEE 1402 is primarily concerned with physical security, it also mentions defense against electronic intrusions. [19]

Status:

Standard – Informative

Approved – January 30, 2000

ISA SP99.00.01 - Manufacturing and Control Systems Security – Concepts, Models and Terminology

Scope: The Instrumentation, Systems, and Automation Society (ISA) SP99.00.01 [20], when released, will address the basic concepts, models, and terminology that form the basis for the other standards in the series but will not address guidance in establishing a cyber security program. It will be the first in a series of standards that address the subject of Manufacturing and Control System security.

Status:

Standard - Normative

Not released. Part 1 is currently in draft stage with first ballot scheduled for the first part of 2006.

ISA SP99.00.02 - Manufacturing and Control Systems Security – Establishing a Manufacturing and Control Systems Security Program

Scope: ISA SP99.00.02 [21] will focus on establishing a security program for manufacturing and control systems. It will provide practical guidance and direction on how to establish a business case for a security program and how to design a security program, tailored to a company's individual needs. This standard will cover cyber security for manufacturing and control systems as it applies, in the broadest possible sense, encompassing all types of manufacturing plants and facilities, as well as other processing operations such as utilities (i.e., electric, gas and water), pipelines and transportation systems or other industries which use automated or remotely controlled vehicles. It will be based on function, not industry, type of control or other limited views. Specifically, Manufacturing and Control Systems include all systems that can affect or influence the safe, secure and reliable operation of an industrial process.

Status:
Standard - Normative
Part 2 is not released. It is currently in draft stage with first ballot scheduled for the latter part of 2006.

ANSI/ISA TR99.00.01-2004 - Security Technologies for Manufacturing and Control Systems

Scope: ISA Technical Report TR99.00.01 [22] provides an evaluation and assessment of several categories of electronic security technologies and tools that apply to the Manufacturing and Control Systems environment, including development, implementation, operations, maintenance, engineering and other user services. It discusses specific types of applications within each category, the vulnerabilities addressed by each type, suggestions for deployment, and known strengths and weaknesses, as well as some forms of mitigation for the mentioned risks. It does not make recommendations of one technology over others, but provides recommendations and guidance for using the technologies, as well as information to consider when developing a site or corporate security program and plan. It also provides guidance to manufacturers, vendors, and security practitioners and end-user companies on the technological options for securing these systems against electronic (cyber) attack.

Status:
Technical Report
Approved 10 October 2004

ANSI/ISA-TR99.00.02-2004 - Integrating Electronic Security into the Manufacturing and Control Systems Environment

Scope: ISA Technical Report TR99.00.02 [23] provides a framework for developing an electronic security program and a recommended organization and structure for a security plan. It focuses on the planning, developing, and implementing activities involved with a comprehensive program for integrating security into the Manufacturing and Control Systems environment. It also gives detailed information about the minimum elements to include and guidance on broad policy goals and objectives in areas ranging from risk analysis to management of change and compliance auditing. It also provides guidance for auditing a system against the defined electronic security policy to determine security breaches or vulnerabilities, and assists in verifying compliance with security policies and procedures. It includes guidance on using metrics to measure progress, identify potential pitfalls, and potentially modify the audit procedure.

Status:
Technical Report
Approved 10 October 2004
When ISA SP99.00.02 is released, this technical report will be inactivated.

ISO/IEC 17799 – Information Technology – Code of practice for information security management

Scope: International Organization for Standardization (ISO)/IEC-17799:2005 [24] establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this standard provide general guidance on the commonly accepted goals of information security management. [24] It offers guidelines and voluntary directions for information security management and is meant to provide a high level, general description of the areas currently considered important when initiating, implementing or maintaining information security in an organization. [25]

The control objectives presented in this standard are intended to be implemented to meet the requirements identified by a risk assessment. It my also serve as a practical guideline for developing

organizational security standards and effective security management practices and to help build confidence in inter-organizational activities. [24] It is organized into twelve major sections, each covering a different topic, including risk assessment and treatment, security policy, physical and environmental security, asset management, etc.

Status:

Standard - Informative

Released: 15 June 2005

ISO/IEC 27001 - Information technology – Security techniques – Information security management systems – Requirements

Scope: The basic objective of ISO/IEC 27001 [26] is to help establish and maintain an effective information security management system, using a continual improvement approach. [27] It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organization's overall business risks. It specifies the requirements for the implementation of security controls customized to the needs of individual organizations. [26] Although the standard contains both informative and normative sections, the standard is intended to provide normative requirements based on ISO/IEC 17799:2005.

Status:

Standard - Normative

Released: 15 October 2005

NERC 1200 – Urgent Action Standard 1200 – Cyber Security

Scope: North American Electric Reliability Council (NERC), developed the "Urgent Action Cyber Security Standard" (NERC 1200) [28] to establish a set of defined security requirements related to the energy industry and to reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets. [28, 29] NERC 1200 applies to existing entities (such as control areas, transmission owners and operators, and generation owners and operators) performing various electric system functions. [30] NERC 1200 addresses cyber security policy, critical cyber assets, electronic and physical security perimeter, access controls, monitoring of access, the protection of information, training systems management, test procedures, response to incidents, and plans for recovery following an incident. It was developed as temporary standard for a one-year period, to be replaced by Cyber Security Standards, CIP-002-1 through CIP-009-1. It has since received extensions until August, 2006.

Status:

Standard - Normative

Adopted 13 August 2003

This standard will be inactivated when the CIP series Cyber Security Standards are released.

NERC CIP – Cyber Security

Scope: The NERC CIP (Critical Infrastructure Protection) series, CIP-002-1 through CIP-009-1, [31] will establish standards in eight key areas, designed to protect not only power plants but all other aspects of electric utility operations and assets as well. This standard will include provisions for identifying critical cyber assets, developing security management controls, implementing training, identifying and implementing perimeter security, implementing a physical security program for the protection of critical cyber assets, protecting assets and information within the perimeter, conducting incident reporting and response planning, and crafting and implementing recovery plans. This standard will cover the same basic areas covered by the NERC 1200 Standard. [32] It will include audit measures and levels of non-compliance that will be tied to penalties. [33]

Status:
Standard - Normative
Not released - The committee has decided that a ballot on the revised draft 3 would be held in February 2006 with expected effective date of June 2006. [34]

NERC Security Guidelines for the Electricity Sector

Scope: The "NERC Security Guidelines for the Electrical Sector" [35] describe general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric infrastructure systems. [36] They address both physical and cyber security, providing a minimum baseline for secure cyber access control across the electric sector. These guidelines focus on vulnerability and risk assessment, emergency plans, continuity of business process, communications, physical security, cyber-risk management, cyber-access control, cyber-IT firewalls, employment background screening, protecting potentially sensitive information, securing remote access to electronic control and protection systems, threat and incident reporting, patch management, and control system-business electronic connectivity. Their purpose is to provide recommendations to effectively and reliably secure control system networks and thereby enhances the security and reliability of the bulk electric system infrastructure. [35] These guidelines are advisory in nature. [36]

Status:
Guidelines
Released - June 14, 2002

SPP-ICS - System Protection Profile for Industrial Control Systems

Scope: The System Protection Profile (SPP) for Industrial Control Systems (ICS) [37], prepared for NIST (National Institute of Standards and Technology), addresses security requirements needed throughout an industrial control system's lifecycle for an entire industrial control system, including design, implementation, configuration, maintenance, and decommissioning. It covers requirements for operating policies and procedures, information technology based system components, interfaces and interoperability between system components, and the physical environment and protection of the system. [37] It also includes security concepts such as defense in-depth, or layered security, extending from industrial process sensors and programmable logic controllers up through the factory control and enterprise business hierarchy to the Internet. [38] It deals with industrial control systems such as SCADA systems, distributed control systems, and programmable logic controllers. Requirements for components of the control system, such as industrial controller authentication and sensor authentication, also are outlined. SPP-ICS is a baseline document that states necessary industrial security requirements at an implementation-independent level. System integrators and end-users can apply SPP-ICS to specify security functional requirements to procure new systems while vendors can use it to demonstrate assurance that their products meet these security requirements. [39]

Status:
System Protection Profile
Released May 26, 2004

SP800-53 Recommended Security Controls for Federal Information Systems

Scope: NIST Special Publication (SP)800-53, Recommended Security Controls for Federal Information Systems, [40] provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. These guidelines address the selection and specification of security controls, recommendations for minimum security controls, development of assessment methods and procedures for determining security effectiveness, and promote a dynamic catalog of security controls to meet changing requirements. [40] SP800-53 outlines

the management, operational, and technical safeguards necessary to comply with the Federal Information Security Management Act. [41]

Status:
Guidelines
Released February 2005

SP800-82 Guide for SCADA and ICS Security

Scope: NIST SP 800-82, will provide guidance for establishing secure SCADA and Industrial Control Systems while presenting an overview of typical topologies to facilitate the understanding of industrial control systems. It will also identify typical vulnerabilities, threats and consequences while providing guidance on security deployment including administrative, physical and technical countermeasures to mitigate the associated risks. [42]

Status:
Guidelines
Not released - A Subject Matter Expert draft of SP800-82 is expected shortly [43].

CONCLUSIONS

Cyber security standards can assist in providing increased security to computer-controlled systems by supplying an understanding of areas of concern and how they can be addressed. There are many aspects that come into play when considering the protection of a control system, both physical and cyber.

This paper reviews several cyber security standards used in control system cyber security. A review of these standards shows both distinct differences as well as areas of overlap in the coverage by the standards. Therefore, a careful examination of the standards should be made before using any given standard.

This paper provides a high-level examination of several standards related to process control system cyber security, and may be used as a first step towards identifying the control system standards that should be applied in protecting a process control system. It is recommended that those developing control system cyber security programs continue exploration of the existing standards as they are in a constant state of flux due to the changing level of attack and the changing security environment.

REFERENCES

1 CERT/CC Statistics 1988-2004, www.cert.org/stats/cert_stats.html

2 Poulsen, Kevin, "Shifting Cyber Threats Menace Factory Floors," *Security Focus Printable NEWS* 9671, October 7, 2004, http://www.security focus.com/ printable/news/9671

3 Report to Congressional Requesters, *Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems*, GAO-04-0354, March 2004.

4 International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, Frequently Asked Questions, What is ISO/IEC 17799:2000?, November 2002, http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pd

5 CSI/FBI *Computer Crime and Security Survey*, Computer Security Institute, 600 Harrison St., San Francisco, CA, 94107, 2003.

6 A Summary of Control System Security Standards Activities in the Energy Sector, National SCADA Test Bed, October 2005, https://www.pcsforum.org/news/NSTB%20Security%20Standards%20Report.pdf

7 Comparison Study of Industrial Control System Standards against the Control Systems Protection Framework Cyber-Security Requirements, Version 3.2, Control Systems Security Center – Standards Awareness Team, INL/EXT-05-00831, September 2005

8 AGA Report No. 12, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan, Draft 5, American Gas Association, April 2005

9 AGA Report No. 12, Cryptographic Protection of SCADA Communications, Part 2: Retrofit Link Encryption for Asynchronous Serial Communications, American Gas Association, Draft 29 November 2005.

10 AGA 12 Working Document Collaboration Area -*Welcome to your AGA 12 Cryptographically Protected SCADA Communications Working Document Collaboration Area,* http://www.gtiservices.org/security/aga12_wkgdoc_homepg.shtml

11 Cryptographic Protection of SCADA Communicatons, http://www.gtiservices.org/security/report/scope.shtml

12 Pipeline SCADA Security, API Standard 1164, American Petroleum Institute, Washington, DC, First Edition, September, 2004.

13 Fisher. R, July 29, 2004*,* "Supervisory Control and Data Acquisition (SCADA) Systems White Paper," prepared by Argonne National Laboratory for DPO.

14 Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1, Chemical Industry Data Exchange, May 2005, http://www.cidx.org/

15 IEC 62351-1: Data and Communication Security, Introduction and Overview, April, 2005.

16 Frances Cleveland, IEC TC57 Security Standards for the Power System's Information Infrastructure – Beyond Simple Encryption, https://www.pcsforum.org/library/files/1129579675-White_Paper_on_Security_Standards_in_IEC_TC57_ver_5.pdf

17 IEC, Working documents for TC 88, http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea1112.p&committee=88&class=&refno=&type=&date=

18 IEEE Standard 1402-2000, IEEE Guide for Electric Power Substation Physical and Electronic Security. The Institute of Electrical and Electronics Engineers, Inc., ISBN 0-7381-1960-1, New York, NY, April 2000.

19 Dacfey Dzung, Martin Naedele, Thomas P. Van Hoff, and Mario Crevatin, Security for Industrial Communication Systems, Proceedings of the IEEE, Vol. 93, No. 6, June 2005, http://eleit.stlib.gd.cn/jszc/Ieee%20new/0506/06.pdf]

20 ISA SP99.00.01 Manufacturing and Control Systems Security – Concepts, Models and Terminology, Draft 2, Edit 3, ISBN: 1-55617-975-8, Instrumentation, Systems and Automation Society, Research Triangle Park, NC, October 2005

21 ISA SP99.00.02 Manufacturing and Control Systems Security – Establishing a Manufacturing and Control System Security Program, Draft 1, Edit 5, ISBN: 1-55617-976-6, Instrumentation, Systems and Automation Society, Research Triangle Park, NC, October 2005

22 ANSI/ISA TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems, ISBN: 1-55617-886-7, Instrumentation, Systems and Automation Society, Research Triangle Park, NC, October 2004

23 ANSI/ISA TR99.00.02-2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment, ISBN: 1-55617-889-1, Instrumentation, Systems and Automation Society, Research Triangle Park, NC, October 2004

24 International Standard ISO/IEC 17799:2005, Information Technology – Security techniques – *Code of practice for information security management*, International Standards Organization, Geneva, Switzerland, 15 June 2005

25 International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, Frequently Asked Questions, What is ISO/IEC 17799:2000?, November 2002, http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pd
26 International Standard ISO/IEC 27001, Information Technology – Security techniques – Information security management systems - Requirements, International Standards Organization, Geneva, Switzerland, 15 October 2005
27 Welcome to ISO 27001 Online... Dedicated to the ISO 27001 Security Management Standard, http://www.27001-online.com/
28 NERC, Urgent Action Standard 1200 Cyber Security, ftp://ftp.nerc.com/pub/sys/all_updl/standards/Urgent-Req-CyberStnd-3-3121.pdf
29 NERC, "NERC Approves Extension of Urgent Action Cyber Security Standard," *NERC News*, September 8, 2004, http://www.nerc.com/~filez/nercnews/news-0804c.html
30 Breakwater Security, "Key Energy and Utility Security Questions, What is the NERC 1200 Urgent Action Cyber Security Standard?," Breakwater Security Associates, http://www.breakwatersecurity.com/energy/key_questions.html?id=2
31 NERC Standard CIP-002-1 through CIP-009-1, Cyber Security – Draft 3, North American Electric Reliability Council, http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html
32 Joseph Lindstrom and Gary Sevounts, Inside the NERC CIP Standards, Symantec Corporation, SEP 11, 2005, http://ses.symantec.com/industry/power/article.cfm?articleid=5980
33 NERC CIP, Digital Bond, A Network Security Practice, September 2005, http://www.digitalbond.com/SCADA_security/NERC.htm
34 Bugh, Larry, Cyber Security Standards, Draft Meeting Minutes of the Critical Infrastructure Protection Committee, North American Electric Reliability Council, St. Petersburg, Florida, December 8-9, 2005. ftp://www.nerc.com/pub/sys/all_updl/cip/CIPC_draft_min120805.pdf
35 Security Guidelines for the Electricity Sector Version 1.0, North American Electric Reliability Council, Princeton, NJ, June 14, 2002
36 NERC, "Security Guidelines for the Electricity Sector, Overview, Version 1.0," http://www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf
37 System Protection Profile – Industrial Control Systems, Version 1.0, National Institute of Standards and Technology, 14 April 2004.
38 Willoughby, Mark, "Information Security News: New security standards to strengthen SCADA," *InfoSec News*, 22 Nov 2004, http://www.computerworld.com/securitytopics/security/story/0,10801,97606,00.html]
39 "NIST's process control forum helps networks prevent cyber attacks," *Control Engineering,* November 1, 2004, http://www.manufacturing.net/ctl/article/CA478475]
40 SP800-53, NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.
41 Greenemeier, Larry, Security Compliance An Issue For Government And Businesses, InformationWeek, Business Technology Network, Sept. 19, 2005, http://informationweek.com/story/showArticle.jhtml?articleID=170704644
42 Stouffer, Keith, NIST Industrial Control System Security Activities, Information Security and Privacy Advisory Board (ISPAB) Meeting, Rockville, MD, September 14, 2005, http://csrc.nist.gov/ispab/2005-09/ISPAB-KStouffer.pdf
43 Stouffer, Keith, personal communication to Robert Evans, 9 January 2006.