INEEL/EXT-04-02462
Revision 0

Control Systems Security and Test Center

A Comparison of Oil and Gas Segment Cyber Security Standards

Prepared by the Idaho National Engineering and Environmental Laboratory

November 3, 2004

Homeland Security

INEEL/EXT-04-02462

A Comparison of Oil and Gas Segment Cyber Security Standards

November 3, 2004

Control Systems Security and Test Center
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-99ID13727

ABSTRACT

This report presents a review and comparison (commonality and differences) of two oil and gas segment cyber security standards and an internationally recognized information security standard. The comparison identifies security areas that are covered by each standard and reveals where the standards differ in emphasis. By identifying differences in the standards the user can evaluate which standard best meets their needs. For this report, only standards applicable to the oil and gas segment were reviewed.

CONTENTS

TABLES

ACRONYMS

AGA	American Gas Association
API	American Petroleum Institute
HSPD	Homeland Security Presidential Directive
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
SCADA	Supervisory Control and Data Acquisition

A Comparison of Oil and Gas Segment Cyber Security Standards

1. INTRODUCTION

This report compares two security standards developed for oil and gas critical infrastructures with a widely recognized information security international standard. The Idaho National Engineering and Environmental Laboratory coordinated with the Department of Energy's Critical Infrastructure Security Standards Working Group and academic partners at the University of Idaho to produce this report.

"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security."[1]

These critical infrastructures are composed of public and private institutions. Cyberspace is their "nervous system—the control system of our country."[2]

"Cyberattacks come in two forms: one against data, the other on control systems. The first type attempts to steal or corrupt data and deny services. The vast majority of Internet and other computer attacks have fallen into this category, such as credit-card number theft, Web site vandalism and the occasional major denial-of-service assault."[3]

"Control-system attacks attempt to disable or take power over operations used to maintain physical infrastructure, such as distributed control systems that regulate water supplies, electrical transmission networks and railroads. While remote access to many control systems have previously required an attacker to dial in with a modem, these operations are increasingly using the Internet to transmit data or are connected to a company's local network—a system protected with firewalls that, in some cases, could be penetrated."[3]

Cyber security standards, when followed, can provide increased security to control systems. There are distinct differences in the topics considered by the two current standards (American Gas Association [AGA] Report No. 12, and American Petroleum Institute [API] 1164) within the Oil and Gas segment. The task of this report is to promote an understanding of the security requirements, and application of the appropriate control system security standards and guidelines for that area of concern.

This report compares the two cyber security standards developed for the oil and gas critical infrastructures, using International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17799 standard as a comparison. ISO/IEC 17799 was established as a Cyber Security Standard in 1995. The standard was finally issued in 2000. Later standards were designed on the footings of ISO/IEC 17799. Although there are other standards that address control system cyber security, they all use ISO/IEC 17799 as the base of starting point for cyber security standards.

2. PROBLEM

Much of the critical infrastructure in the United States is at risk due to increasing cyber intrusions that may impact normal operations. Critical oil and gas infrastructures depend on control systems for their operation. The President of the United States issued Homeland Security Presidential Directive (HSPD)–7 on December 17, 2003, which stated in part, "it is the policy of the United States to enhance the protection of our Nation's critical infrastructure."[4] In addition, HSPD-7 states "The Department and Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms." The HSPD-7 directs that the Department of Commerce, in coordination with the Department of Homeland Security, will work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act to ensure the timely availability of industrial products, materials, and services to meet homeland security requirements.

Physical and cyber attacks are increasing against the control systems used in our critical infrastructures.[5] Physical attacks are very visible to the public and industry. There is usually property damage or personal injury involved with the physical attack and the news media will publicize the event. Cyber attacks, on the other hand, are not as easily identified and many companies do not report the events or publicize their cyber vulnerabilities. Many of the cyber attacks go unnoticed or may go unnoticed for long periods of time. However, the resources and tools for cyber attacks are becoming more commonplace and readily available. AGA's Natural Gas Security Committee, in partnership with the Interstate Natural Gas Association of America's Security Task Group, developed security guidelines for the industry that were submitted in June 2002 to the Department of Transportation's Office of Pipeline Safety. The "Security Guidelines for the Natural Gas Industry" were also submitted to the Department of Energy. The report provides an approach for vulnerability assessment, a critical facility definition, detection/deterrent methods, response and recovery, cyber security, and relevant operational standards.[5] Many companies under the oil and gas infrastructure are now reviewing practices and security of Supervisory Control and Data Acquisition (SCADA)/controls system. Under the discussions, participation, and guidance through standards committee activities companies are tightening the physical and cyber access to the SCADA/Control systems to limited operating and contract personnel. AGA 12 Report and API-1164 SCADA Security standards are now actively being discussed within the petroleum and natural gas industry.

Electronic intrusions and attacks may come from inside or outside a company. From within, intrusions may be innocent mistakes made by an operator, or deliberate attacks by disgruntled employees. Externally, intrusions come from former employees, computer viruses, and from hostile external attackers. Many companies have Internet connections to the control system to enable management, engineering, and others to monitor processes and progress. Vulnerability to the intrusions and attacks has increased with access to the control systems through the Internet. HSPD-7 states, "While it is not possible to protect or eliminate the vulnerability of all critical infrastructure … strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur."[4] Cyber intrusions are costly to industries, and many could be prevented by applying cyber security standards.[a]

a. A similar study considered standards in the electrical industries

2.1 Applying Standards to the Solve the Problem

Cyber security standards can be used to help identify problems and reduce the vulnerabilities in a control system. By knowing the problems and vulnerabilities, standards can be applied to control systems and to minimize the risk of intrusion. This report presents a comparison of some of the oil and gas segment cyber security standards. Implementing the proper standard for a particular industry's application can reduce vulnerabilities in control systems. For the oil and gas segment, this document helps identify which standard most closely matches the pipeline sector's cyber security needs.

3. STANDARDS

This section provides a brief description of an international information security standard and the two oil and gas segment security standards used in this study. Table 1 shows the major sections of each standard. This study can help identify the similarities and differences between standards, which can contribute to selecting the best security practices and help strengthen sections of the standards in future revisions.

1. **ISO/IEC 17799**. ISO/IEC 17799, First edition 2000-12-01, standard titled "Information Technology – Code of Practice for Information Security Management," gives recommendations for information security management. It is high level, broad in scope, conceptual in nature and intended to provide a basis for an organization to develop its own organizational security standards and security management practices.[7]

   The standard states: "This code of practice may be regarded as a starting point in developing organization specific guidance. Not all of the guidance and controls in the code of practice may be applicable. Furthermore, additional control not included in this document may be required."[8]

   ISO/IEC 17799 is a widely recognized, comprehensive information security standard. It is organized into ten major sections or topics. The sections are listed in Table 1, along with the major sections from the other standards covered in this report. Although it was not written specifically for the oil and gas sector, ISO/IEC 17799 offers guidelines and voluntary directions for information security management and is meant to provide a general description of the areas considered important when initiating, implementing, or maintaining information security in an organization. It addresses the topics in terms of policies and general good practices but does not provide definitive details or "how-to's."[9]

2. **API 1164**. American Petroleum Institute (API) Standard 1164, First edition September 2004. API represents more than 400 members involved in oil and natural gas industry.[10] Oil and natural gas utilities are part of the nation's critical infrastructure. They rely on SCADA systems to control their operations.

   The objective of API 1164 is to provide "a means to improve the security of the pipeline SCADA operation by:

   - Listing the processes used to identify and analyze the SCADA system vulnerabilities to unauthorized attacks
   - Providing a comprehensive list of practices to harden the core architecture
   - Providing examples of industry best practices."[11]

   "This standard on SCADA security provides guidance to the operators of oil and gas liquid pipeline systems for managing SCADA system integrity and security. The use of this document … should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA system."[12]

   This standard is targeted at small to medium pipeline operators with limited Information Technology security resources. While the recommendations are not as comprehensive as those in ISO/IEC 17799, they are applicable to any SCADA system and their implementation could significantly improve the cyber security of a SCADA system. The two appendices in the

specification add a significant amount of detail. Appendix A is a checklist to be used as a guide when reviewing the cyber security of SCADA systems. Appendix B is an example of a SCADA Control System Security Plan. It is intended to be used when developing an operator specific SCADA security plan. The example plan is not all-inclusive or intended to cover all possible vulnerabilities but it is a useful starting point.

3. **AGA-12**. American Gas Association (AGA) "Cryptographic Protection of SCADA Communications General Recommendations" Draft 3, AGA Report No. 12 dated August 14, 2004. The AGA represents 192 local utilities that deliver natural gas to homes, businesses, and industries throughout the United States. AGA member companies account for roughly 83 percent of all natural gas delivered by the nation's local natural gas distribution companies. The AGA "encourages and assists members in sharing information designed to achieve operational excellence by improving their security, safety, reliability, efficiency, and environmental and other performance."[13]

   Natural gas utilities are part of the nation's critical infrastructure. They rely on SCADA systems to control their operations. The AGA asked the Gas Technology Institute to research encryption methods that could lead to a standard industry encryption system for both new and existing SCADA systems.[14]

   AGA 12 is the first of an expected series of documents recommending practices designed to protect SCADA communications against cyber attacks. It is the product of a cooperative effort by AGA and the Gas Technology Institute in coordination with associations representing the gas, water, and electric industries; manufacturers; SCADA operators; U.S. Government Agencies (National Institute of Standards and Technology and Department of Transportation); and security experts.[14] The intent of the recommended practices is "to provide confidential SCADA communications that are known to be unaltered by potential attackers and that can be authenticated as having originated from valid authorized users."[16]

   The AGA 12 series of documents focus on securing the communications link between field devices and the control servers or control center. AGA 12 "contains the background, security policy fundamentals, and a test plan that apply generally to all areas of cryptographic protection of SCADA systems." Planned addendums to AGA 12 are expected to address cryptographic key management, and protection of data at rest. Additional planned documents in the AGA 12 series include:

   AGA 12-1: Retrofit link encryption for asynchronous serial communications of SCADA systems
   AGA 12-2: Protection of IP-based, networked SCADA systems
   AGA 12-3: Protection embedded in SCADA components.[16]

   AGA 12 Draft 3 contains a number of informative sections as well as normative (required) sections. The major normative sections are listed in Table 1. Major informative sections include: SCADA fundamentals, Cryptography fundamentals, Challenges in applying cryptography to SCADA communications, and Classes of attacks against SCADA systems. As mentioned above, the main body of AGA 12 focuses on securing the communications link between field devices and the control servers or control center using encryption. However, Annex F provides a discussion on security practice fundamentals. Annex H provides a Cryptographic system test plan.

Table 1. Major security sections in oil and gas segment standards.

ISO/IEC 17799 Information Technology- Code of Practice for Information Security Management	API 1164 Pipeline SCADA Security	AGA Report No. 12 Draft 3 August 14, 2004 Cryptographic Protection of SCADA Communications General Recommendations
82 pages	60 pages	110 pages
Security Policy	Access Control	Steps to define security goals
Organizational Security	Communication	Cryptographic system requirements
Asset Classification and Control	Information Distribution	
Personnel Security	Physical	
Physical and Environmental Security	Network Design and Data Interchange	
Communications and Operations Management	Management System	
Access Control	Appendix A (SCADA System Security Checklist) • Application and Database • Authentication • Change and Problem Management • Computer, Telephone, and Network Usage • Contractors, Vendors, Consultants, and Third Party • Information Classification and Application Criticality • Information Retention/Archive/Backup • Network Connectivity • Personnel Security • Physical Security • System Security Audit and Review	Annex F Security Practice Fundamentals • Recommendations for staffing an InfoSec team • Awareness of security assurance • Recommendations for writing security policies • Recommendations for performing assessment and analysis • Auditing
Systems Development and Maintenance	Appendix B (Example) SCADA/Control System Security Plan • Identification and Documentation • Risk Analysis • Preventive Action • Oversight • Security Management	Annex H Cryptographic System Test Plan • Test requirements and evaluation criteria • Interoperability testing • Special test setup requirements • Test reports • Test Architecture and environment
Business Continuity Management		
Compliance		

4. DISCUSSION - COMPARISON OF STANDARDS

The three standards considered in this report provide recommendations for information/control system security management for use by those responsible for initiating, implementing, or maintaining security in their organization. In addition, SCADA manufacturers should consider using the AGA 12 series of documents (when they become available) as a step to ensure their product offerings comply with an open standard for SCADA communications encryption.

Appendix A compares the three standards considered in this report. By examining Appendix A, it is possible to see which section of a particular standard addresses which recommendation. This comparison of the security standards was performed by identifying similar recommendations within the three standards.

The standards were examined and the recommendations that were stated in the standard were noted. International Standard ISO/IEC 17799 was used as the baseline because it is the starting point for other cyber security standards. Since all of the standards do not address the same recommendations, it is recognized that there will be areas where there are no comparisons. For example, AGA 12 is geared more toward encryption for the purpose of authenticating data transfer within the (SCADA) control system network, while the API 1164 focus is on pipeline control system security by listing the processes used to identify and analyze the SCADA system vulnerabilities, providing a comprehensive list of practices to harden the core architecture, and providing examples of industry best practices. The ISO/IEC standard considers the network, operating system, and application separately, and looks at recommendations such as passwords for each of these individually. This leads to difficulty in comparing standards and leaves the comparison open to personal interpretation.

5. CONCLUSIONS

This report reviews and compares the recommendations for three security standards used in the oil and gas segment of the energy sector. There are distinct differences in the topics considered by these standards. Therefore, a careful examination of this comparison, and of the standards presented here, should be made before attempting to use any given standard.

Cyber security standards can provide increased security to control systems by giving an understanding of areas of concern and how they can be addressed.

6. REFERENCES

1. Residential Decision Directive 63 (PDD-63) May 22, 1998
http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

2. The National Strategy to Secure Cyberspace February 2003, page vii
http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

3. Emos, Robert, "Cyberterrorism: The real risk", CNET News.com, August 27, 2002
http://news.zdnet.co.uk/internet/0,39020369,2121358,00.htm

4. Homeland Security Presidential Directive/Hspd-7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003
http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html

5. Infrastructure Security in the Natural Gas Industry Activities & Programs Since 9/11 - Security Guidelines
http://www.aga.org/Template.cfm?Section=News&template=/ContentManagement/ContentDisplay.cfm&ContentID=8504

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

7. Information Security Management: Understanding ISO-17799, Tom Carlson, CISSP,
http://www.ins.com/downloads/whitepapers/ins_white_paper_info_security_iso_17799_1101.pdf

8. ISO/IEC 17799:2000, "Information Technology -- Code of Practice for Information Security Management", Page xi.
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3

9. International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management Frequently Asked Questions.
http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf

10. About API. http://api-ec.api.org/aboutapi/index.cfm?bitmask=001010000000000000

11. API Standard 1164, Pipeline SCADA Security First Edition, September 2004, page 1. http://api-ep.api.org/filelibrary/1164PA.pdf

12. API Standard 1164, Pipeline SCADA Security First Edition, September 2004, page iii. http://api-ep.api.org/filelibrary/1164PA.pdf

13. About AGA.
http://www.aga.org/Content/NavigationMenu/Membership_Services/About_AGA/About_AGA.htm

14. "Industry SCADA Encryption Standard in the Works," American Gas Association,
http://www.aga.org/Content/ContentGroups/American_Gas_Magazine1/November_2002/Industry_SCADA_Encryption_Standard_in_the_Works.htm

15. AGA Report No. 12. Cryptographic Protection of SCADA Communications: General Recommendations. Draft 3, August 14, 2004. Page ii. http://www.gtiservices.org/security/AGA12Draft3r6.pdf

16. AGA Report No. 12. Cryptographic Protection of SCADA Communications: General Recommendations. Draft 3, August 14, 2004. Page 1. http://www.gtiservices.org/security/AGA12Draft3r6.pdf

Appendix A

Security Standards Comparison

Appendix A

Security Standards Comparison

	ISO/IEC 17799	API 1164	AGA Report No. 12 Draft 3 August 14, 2004
SECURITY POLICY	3	1.1, 7.1	3, F.2
Information security policy.	3.1		3.1, F.2
Information security policy document.	3.1.1	2.3, 2.6, 7.2	3.1, F.2, F.3
Review and evaluation of information security policy.	3.1.2	B.4.2, B.5.1.5	3.4, F.2
VULNERABILITY AND RISK ASSESSMENT			
Vulnerability and risk assessment.			
Conduct a risk assessment.	7.1.1, 7.1.5, 7.2.5, 7.2.6, 9.4.3, 9.7.2.1, 10.2, 10.3.1, 10.3.2, 11.1.2	2.1, 5.1.1-2, B.2	3.2, F.4
Three layer analysis			F.4.1
Security architecture analysis			F.4.2
Successive compromise analysis			F.4.3
Quantitative risk analysis			F.4.4.1
Qualitative risk analysis			F.4.4.2
Risk management process.		B.2	3.2, 3.3, 3.4, F
Mitigation program.		5.1.2, B.2.3	3.4, F.3, F.5
Equipment backup		5.1.2, B.2.3.5, B.3.5.1	
General considerations for conducting a risk and vulnerability assessment.		5.1.2, B.2	2.4, 3.2, 3.3, F.4
ORGANIZATIONAL SECURITY	4	B.5	
Information security infrastructure.	4.1	B.5, B.5.1	3.1, F.2
Management information security forum.	4.1.1	B.5.1.5	3.1
Information security coordination (within the organization).	4.1.2	B.5.1.5	3.1, F
Allocation of information security responsibilities (for assets and processes including leadership and management).	4.1.3	B.5.1	F.1
Authorization process for new information processing facilities.	4.1.4		
Specialist information security advice.	4.1.5		
Cooperation between (external) organizations.	4.1.6		

	ISO/IEC 17799	API 1164	AGA Report No. 12 Draft 3 August 14, 2004
Restrict exchanges of sensitive information.	4.1.6	B.5.2	
Respond to disclosures of sensitive information.			
Independent review of information security.	4.1.7		
Staffing an InfoSec team		B.5.1	F.1
Security of third party access.	4.2	2.2.2, 6.2.2, B.3.4, B.3.4.2	2.1.1
Identification of risks from third party access.	4.2.1	2.2.2	2.1.1
Types of access (physical or logical).	4.2.1.1	2.1, 2.2.1-2, 2.3, 2.5	2.1.1
Reasons for access.	4.2.1.2	6.2.3	
On-site contractors.	4.2.1.3	5.1.1	
Security requirements in third party contracts.	4.2.2		
Outsourcing.	4.3		
Security requirements in outsourcing contracts.	4.3.1		
ASSET CLASSIFICATION AND CONTROL	5		
Accountability for assets.	5.1		
Inventory of assets.	5.1.1	B.1	
Information classification.	5.2	4.1	
Classification guidelines.	5.2.1	4.1	
Information labeling and handling.	5.2.2	4.1.5	
PERSONNEL SECURITY	6		
Security in job definition and resourcing.	6.1		F.2
Including security in job responsibilities.	6.1.1		3.1
Personnel (background) screening and policy.	6.1.2	4.1.4, 5.1.1	F.2
Confidentiality agreements.	6.1.3	4.1.4	F.1
Terms and conditions of employment.	6.1.4		
Identify personnel granted physical or electronic access.		2.2, 2.2.1, 2.6	
Department employees and contractors		2.6	
Job responsibilities			
User training.	6.2		F.2
Information security education, training, and awareness.	6.2.1	7.1, B.5.2, B.5.2.4	F.2
Responding to security incidents and malfunctions.	6.3	7.2	F.3
Reporting security threats, incidents, and weaknesses.	6.3.1, 6.3.2	7.2	

	ISO/IEC 17799	API 1164	AGA Report No. 12 Draft 3 August 14, 2004
Timely reporting.	6.3.1		
Information to report.			
Incident reporting mechanisms.	6.3.1		
Reporting software malfunction.	6.3.3		
Learning from incidents.	6.3.4		
Disciplinary process.	6.3.5		
PHYSICAL AND ENVIRONMENTAL SECURITY	7	5	F.2
Secure areas.	7.1	5.1.2, 7.2	F.2
Physical security perimeter.	7.1.1	5.1.2	
Monitoring physical access.	7.1.1	5.1.2	
Physical entry controls.	7.1.2	5, 5.1.2	
Securing offices, rooms, and facilities.	7.1.3	5, 5.1.2	
Working in secure areas.	7.1.4		
Isolated delivery and loading areas.	7.1.5		
Intruder detection	7.1.3.e	5.1.1	F.2
Equipment security.	7.2	5.1	
Equipment siting and protection.	7.2.1	5.1.2	
Power supplies.	7.2.2	5.1.1	
Cabling security.	7.2.3	5.1.1	
Equipment maintenance.	7.2.4	5.1.1	
Security of equipment off-premises.	7.2.5	7.4	
Secure disposal or re-use of equipment.	7.2.6		
Utility security		4.1.1	
Port security		3.1.2, 3.3.1, 4.1.1	
General controls (information and information processing facilities).	7.3		
Clear desk and clear screen policy.	7.3.1		
Removal of property	7.3.2		
COMMUNICATIONS AND OPERATIONS MANAGEMENT	8	3	F.2
Operational procedures and responsibilities.	8.1		F.2
Documented operating procedures.	8.1.1		F.2

	ISO/IEC 17799	API 1164	AGA Report No. 12 Draft 3 August 14, 2004
Operational change control.	8.1.2	3.3.1, 7.2, B.3.1	
Incident management procedures.	8.1.3		
Segregation of duties.	8.1.4		
Separation of development and operational facilities.	8.1.5		
External facilities management.	8.1.6		
Testing and documentation procedure		5.1.2	
System planning and acceptance.	8.2		
Capacity planning.	8.2.1		
System acceptance.	8.2.2		
Protection against malicious software.	8.3		F.2
Controls against malicious software.	8.3.1	3.2.2-3, 3.3.3, 7.2	
Vulnerability assessment (controlled penetration testing)		B.3.4	4.3
Housekeeping.	8.4		
Information back-up.	8.4.1	B.3.5.1	
Operator logs.	8.4.2		
Fault logging.	8.4.3		
Network management.	8.5		F.2
Network controls.	8.5.1	3.1, 6.1	
Media handling and security.	8.6		F.2
Management of removable computer media.	8.6.1		F.2
Disposal of media.	8.6.2, 7.2.6		F.2
Information handling procedures.	8.6.3	B.5.2	F.2
Information protection.		B.5.2.1-3	
Security of system documentation.	8.6.4	B.5.2.1	
File Transfer Protocol		2.4	
Information distribution		B.5.2	
Exchanges of information and software.	8.7		
Information and software exchange agreements.	8.7.1		
Security of media in transit.	8.7.2		
Electronic commerce security.	8.7.3		

	ISO/IEC 17799	API 1164	AGA Report No. 12 Draft 3 August 14, 2004
Security of electronic mail: security risks and policy on electronic mail.	8.7.4, 8.7.4.1, 8.7.4.2		
Security of electronic office systems.	8.7.5		
Publicly available systems.	8.7.6		
Other forms of information exchange.	8.7.7		
Remote functions		2.4	
Availability		3.3	
ACCESS CONTROL	9	2, B.3.6.2	
Business requirements for access control.	9.1		
Access control policy.	9.1.1	2.1	
Policy and business requirements.	9.1.1.1	2.2	
Access control rules.	9.1.1.2	7.2	
User access management.	9.2		F.2
User registration.	9.2.1	2.2, 2.6	
Privilege management.	9.2.2	2.2.1	
Authentication (field devices).		7.4	
User password management.	9.2.3	2.2.1-2, 2.3	
Review of user access rights.	9.2.4		
User responsibilities.	9.3		F.2
Password use.	9.3.1		
Unattended user equipment (protection).	9.3.2	7.4	
Network access control.	9.4	B.3.4	F.2
Policy on use of network services.	9.4.1		
Enforced path.	9.4.2		
Securing remote access.		3.1.3, 3.3.2, 6.2.2, 7.4	
User authentication for external connections.	9.4.3	3.3.2, B.3.4.2	
Connections between SCADA systems		6.2.1, B.3.3	
Connections to the internet		6.2.3, B.3.3	
VPN Access		6.2.4	
Node authentication.	9.4.4		
Remote diagnostic port protection.	9.4.5	3.1.2	
Segregation in networks (firewalls).	9.4.6	3.2.2, 6.1.2, 6.2.2-3, B.3.4, B.3.5.1	F.2

	ISO/IEC 17799	API 1164	AGA Report No. 12 Draft 3 August 14, 2004
Demilitarized zone (DMZ)		6.1.1, B.3.3, B.3.4	
Disconnect unnecessary connections to the SCADA network		B.3.3	
Network connection control.	9.4.7	B.3.3	
Network routing control.	9.4.8	3.3.3	
Security of network services (description of services security attributes).	9.4.9		
Embedded passwords		2.3	
Operating system access control.	9.5		F.2
Automatic terminal identification.	9.5.1		
Terminal log-on procedures.	9.5.2		
User identification and authentication.	9.5.3	2.2.2	
Password management system.	9.5.4	2.3	
Use of system utilities.	9.5.5	2.4	
Duress alarm to safeguard users.	9.5.6		
Terminal time-out.	9.5.7	2.2.2	4.2.2.1
Limitation of connection time.	9.5.8		
Application access control.	9.6		
Information access restriction.	9.6.1		
Sensitive system isolation.	9.6.2		
Monitoring system access and use.	9.7		F.2
Event logging.	9.7.1		
Monitoring system use/access.	9.7.2	3.1.2	4.2.2.1
Procedures (for monitoring use including intrusion detection systems) and areas of risk.	9.7.2.1	7.2, B.3.2, B.3.4	4.4.3
Review results of monitoring activities based on risk factors.	9.7.2.2		4.4.3
Logging and reviewing events (emphasis on review).	9.7.2.3	7.2, B.3.2, B.5.1.3	4.4.3
Clock synchronization.	9.7.3		
Mobile computing and teleworking considerations.	9.8, 9.8.1, 9.8.2		
Field Device Access			
Device access		2.5, 7.4	
Authentication		7.4	4.1.2, 4.2.1, 4.2.2.1

	ISO/IEC 17799	API 1164	AGA Report No. 12 Draft 3 August 14, 2004
Electronic protection		7.4	
Physical security		7.4	4.1.2
SYSTEMS DEVELOPMENT AND MAINTENANCE	10		F
Security requirements of systems.	10.1	2, 2.1	
Security requirements analysis and specification.	10.1.1		
Security in application systems.	10.2		
Input data validation.	10.2.1		
Control of internal processing.	10.2.2		
Areas of risk.	10.2.2.1		
Checks and controls.	10.2.2.2		
Message authentication.	10.2.3		4
Output data validation.	10.2.4		
Cryptographic controls.	10.3		4
Policy on the use of cryptographic controls.	10.3.1		4
Encryption.	10.3.2	3.1.1	
Digital signatures considerations.	10.3.3		4.1.3.3
Non-repudiation services.	10.3.4		
SCADA Cryptographic system component requirements			4.2
Management components			4.2.1
Cryptographic module components			4.2.2, 4.2.2.1
SCADA Communication channel encryption components			4.2.2.2
Maintenance communication channel protection components			4.2.2.3
Environmental and power supply requirements			4.2.3
Quality requirements			4.2.4
SCADA Interoperability			4.2.4.1
Scalability			4.2.4.2
Reliability			4.2.4.3
Availability			4.2.4.4
Maintainability			4.2.4.5
Flexibility and expandability			4.2.4.6

	ISO/IEC 17799	API 1164	AGA Report No. 12 Draft 3 August 14, 2004
SCADA Cryptographic system performance requirements			4.3
SCADA system response time			4.3.1
Cryptographic interoperability			4.3.2
SCADA Cryptographic system design goals			4.4
Key management (SCADA)			4.4.1
External communication interfaces to the SCADA system			4.4.2
Control center communication interface			4.4.2.1
Local SCADA master communication interface			4.4.2.2
RTU communication interface			4.4.2.3
Intrusion detection and forensics			4.4.3
Key management.	10.3.5		4.4.1
Protection of cryptographic keys.	10.3.5.1		4.1.3.1
Standards, procedures, and methods.	10.3.5.2		4.1.3.1
Security of system files.	10.4		
Control of operational software.	10.4.1		
Protection of system test data.	10.4.2		
Access control to program source library.	10.4.3		
Security in development and support processes.	10.5		
Change control procedures.	10.5.1	B.3.1	
Technical review of operating system changes.	10.5.2	5.1.2	
Restrictions on changes to software packages.	10.5.3		
Covert channels and Trojan code considerations.	10.5.4		
Outsourced software development considerations.	10.5.5		
Security patch management.			
BUSINESS CONTINUITY MANAGEMENT	11	5.1.2	
Aspects of business continuity management.	11.1	5.1.2	
Business continuity management process.	11.1.1	5.1.2	
Business continuity and impact analysis.	11.1.2	5.1.2	
Writing and implementing continuity plans.	11.1.3	5.1.2, B.2.3.5	
Business continuity planning framework (consistency of plans).	11.1.4		
Testing, maintaining, and re-assessing business continuity plans.	11.1.5, 11.1.5.1-11.1.5.2	B.2.3.5	

	ISO/IEC 17799	API 1164	AGA Report No. 12 Draft 3 August 14, 2004
COMPLIANCE	12		4.1
SCADA System Compliance Requirements			4.1
Compliance with Standard			4.1.1
NIST FIPS Publication 140-1 and 140-2 compliance			4.1.2
Cryptography compliance			4.1.3
Cryptographic hardware compliance			4.1.3.1
Cryptographic software compliance			4.1.3.2
Cryptographic algorithm compliance			4.1.3.3
Compliance certification			4.1.4
Compliance monitoring process (compliance with standard).			
Compliance with legal requirements.	12.1		
Identification of applicable legislation.	12.1.1		
Intellectual property rights: copyright, software copyright.	12.1.2, 12.1.2.1-12.1.2.2		
Safeguarding of organizational records.	12.1.3		
Data protection and privacy of personal information.	12.1.4		
Prevention of misuse of information processing facilities.	12.1.5		
Regulation of cryptographic controls.	12.1.6		
Collection of evidence: rules for evidence, admissibility of evidence, quality of evidence.	12.1.7, 12.1.7.1-12.1.7.3		
Reviews of security policy and technical compliance.	12.2		F.2
Compliance with security policy (auditing).	12.2.1	B.4.1-2	F.2, F.5
Technical compliance checking.	12.2.2	B.4.1-2	F.4
System audit considerations.	12.3		F.2, F.5
System audit controls.	12.3.1		
Protection of system audit tools.	12.3.2		
Preliminary action auditing			F.5.1
Post-implementation auditing			F.5.2
Recursive auditing			F.5.3
CRYPTOGRAPHIC SYSTEM TEST PLAN			H
SCADA SYSTEM SECURITY CHECKLIST		A	

Appendix B

SCADA Control System Security Plan

Appendix B

SCADA Control System Security Plan