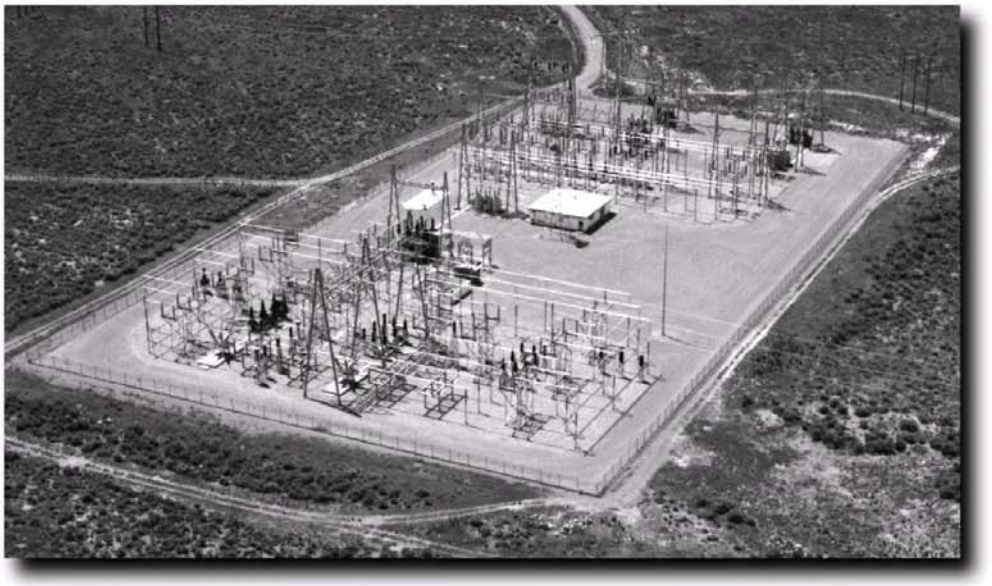
INL/EXT-05-00656
Revision 0

Department of Energy

A Comparison of Cross-Sector Cyber Security Standards

Prepared by Idaho National Laboratory



September 9, 2005

INL/EXT-05-00656

A Comparison of Cross-Sector Cyber Security Standards

September 9, 2005

Idaho National Laboratory
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Energy, Office of
Electricity Delivery and Energy Reliability
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

A Comparison of Cross-Sector Cyber Security Standards

INL/EXT-05-00656

September, 2005

Approved by:

Robert P. Evans
INL Staff Engineer

9-9-2005
Date

Robert C. Hill
INL Project Manager
National SCADA Test Bed Program

9/9/05
Date

Julio G. Rodriguez
INL Program Lead, SCADA
and Power Systems

9/12/05
Date

ABSTRACT

This report presents a review and comparison (commonality and differences) of three cross-sector cyber security standards and an internationally recognized information technology standard. The comparison identifies the security areas 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 cross-sector standards were reviewed.

CONTENTS

TABLES

ACRONYMS

BPCS	Basic Process Control System
DCS	Distributed Control Systems
HSPD	Homeland Security Presidential Directive
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
INL	Idaho National Laboratory
ISA	Instrumentation, Systems, and Automation Society
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
PCSRF	Process Control Security Requirements Forum
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System
SPP	System Protection Profile
STOE	System Target of Evaluation

A Comparison of Cross-Sector Cyber Security Standards

1. INTRODUCTION

This report compares three cross-sector cyber security documents developed for critical infrastructures to a widely recognized information security international standard (International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17799). The Idaho National Laboratory (INL) 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. Although these three documents are not standards, they do provide sound guidance in providing cyber security to control systems in the industry.

"Critical infrastructures rely upon physical and cyber-based systems for their daily operations. 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]

"Cyber attacks may target data or 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]

These cyber security measures, whether in the form of standards, guidelines, best practices, or technical reports (hereafter broadly referred to as standards), when followed, can provide increased security to control systems. There are distinct differences in the topics considered by the three documents (National Institute of Standards and Technology [NIST] Process Control Security Requirements Forum [PCSRF] Industrial Control Systems [ICS] System Protection

Profile [SPP], Instrumentation, Systems, and Automation Society [ISA] Technical Report 99-1 [TR99-01], and ISA Technical Report 99-2 [TR99-02]) considered in this report. There are also differences in the format. The ICS-SPP is written in the Common Criteria format and is Normative in nature, while the ISA Technical Reports are written in plain text and are informative in nature. The objective of this report is to promote an understanding of cyber security issues and promote identification and use of the applicable control system security standards and guidelines for specific areas of concern.

This report compares the three cyber security standards developed for the protection of critical infrastructures, using ISO/IEC 17799 standard as a comparison. ISO/IEC 17799 was established as a Cyber Security Standard in 1995 and finally issued in 2000. Although there are other standards that address control system cyber security, many use ISO/IEC 17799 as the base, or starting point, for cyber security standards.

2. PROBLEM

Much of the critical infrastructure in the United States may be at risk due to increasing cyber intrusions that can impact normal operations. Many of the critical infrastructure sectors 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 may go unnoticed for long periods of time. Further, resources and tools for cyber attacks are becoming more commonplace and readily available. In order to combat these intrusions, both ISA and NIST have documented cyber security measures.

Electronic intrusions and attacks may come from both inside and 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 can be costly to industries, and many can be thwarted by the proper application of cyber security standards.[a]

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 three cyber security standards developed for industrial control systems. Because there are differences in these standards, a careful examination of this comparison and the standards should be made, based on individual needs, before applying this information.

a. A similar study considered standards in the electrical industries.

Implementing the proper standard for a particular industry's application can reduce vulnerabilities in control systems.

3. STANDARDS

This section provides a brief description of an international information security standard and the three other 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. Care should be taken in applying this information, as there are differences in the emphases of each of the standards.

3.1 ISO/IEC 17799. Information Technology – Code of Practice for Information Security Management

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.[6]

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."[7]

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-tos."[8]

3.2 NIST PCSRF – Security Capabilities Profile for Industrial Control Systems

The Process Control Securities Requirements Forum (PCSRF) has prepared a System Protection Profile (SPP) to formally state security requirements associated with industrial control systems (ICS). This document discusses security issues and capabilities relevant to those regarded as components of the national critical information infrastructure. The document defines security capabilities that would exist in electronic programmable components that comprise an industrial control system.[9]

The document directs users to review the "Common Criteria" document for further guidance in securing control systems. The SPP has been written in such a way that it may be used as the basis for preparing a System Security Target for a specific ICS, or it may be used as

the basis for a more detailed SPP for a sub-class of ICS, such as a Supervisory Control and Data Acquisition System (SCADA).

3.3 ISA SP99 – Manufacturing and Control System Security Standard

The focus of the ISA-SP99 committee is to improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and provide criteria for procuring and implementing secure control systems. To date, the committee has issued two technical reports dealing with control system security.[10]

The ISA TR99 technical reports incorporate a great deal of information from other security standards and publications and add information specific to control systems. These technical reports are useful for identifying issues to consider and security options. They are not standards with well defined requirements that can be tested, certified, or included in proposals.[11]

3.3.1 ISA-TR99.00.01-2004 - Security Technologies of Manufacturing and Control Systems

The ISA Technical Report, "Security Technologies of Manufacturing and Control Systems" (TR99-01) provides recommendations and guidance for effectively using electronic security technology and developing a site or corporate security program and plan for the manufacturing and control systems environment.

ISA TR99-01 provides an evaluation and assessment of current types 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 provides guidance to manufacturers, vendors, and security practitioners at end-user companies on the technological options for securing these systems against cyber attack. It deals with analyzing technologies and determining applicability to securing the manufacturing and control systems environment.

It also provides a current assessment of security tools and technologies that apply to the manufacturing and control systems environment and describes several categories of security technologies, the types of products available in those categories, the pros and cons of using those products in the manufacturing and control systems environment relative to expected threats and known vulnerabilities, along with preliminary recommendations and guidance for using those security technologies.[12]

3.3.2 ISA-TR99.00.02-2004 - Integrating Electronic Security into the Manufacturing and Control System Environment

ISA Technical Report, "Integrating Electronic Security into the Manufacturing and Control System Environment," (TR99-02) provides recommendations and guidance for effectively using electronic security technology and developing a site or corporate security program and plan for the manufacturing and control systems environment. It provides a framework for developing an

electronic security program and a recommended organization and structure for the security plan. Detailed information is provided about the minimum elements to include and where specific information should be included in the program.

The concept of manufacturing and control systems cyber security, as addressed in TR99-02, is applied in the broadest practical sense, encompassing all types of plants, facilities, and systems in all industries. Included are hardware and software systems such as Distributed Control Systems (DCSs); Programmable Logic Controllers (PLCs), and Supervisory Control and Data Acquisition (SCADA) systems. The technical report also addresses networked electronic sensing and monitoring and diagnostic systems associated internal, human, network, or machine interfaces and Basic Process Control System (BPCS), Safety Instrumented System (SIS), and associated systems.[13]

Table 1. Major sections in cross-sector developed cyber security standards.

ISO/IEC 17799 Information Technology- Code of Practice for Information Security Management	**NIST PCSRF** System Protection Profile – Industrial Control System – SPP-ICS	**ISA-TR99.00.01-2004** Security Technologies of Manufacturing and Control Systems	**ISA-TR99.00.02-2004** Integrating Electronic Security into the Manufacturing and Control System Environment
82 pages	151 pages	80 pages	87 pages
Security Policy	STOE (System Target of Evaluation) Description	Authentication and Authorization Technologies	Developing a Security Program
Organizational Security	STOE Security Environment	Filtering/Blocking/ Access Control Technologies	Define Risk Goals
Asset Classification and Control	Risks	Encryption Technologies and Data Validation	Assess and Define Existing System
Personnel Security	Security Objectives	Audit, Measurement, Monitoring, and Detection Tools	Conduct Risk Assessment and Gap Analysis
Physical and Environmental Security	IT (Information Technology) Security Requirements	Computer Software	Design of Select Countermeasures
Network Design and Data Interchange	SPP Application Notes	Physical Security Controls	Procure or Build Countermeasures
Communications and Operations Management	Rational		Define Component Test Plans
Access Control			Test Countermeasures
Systems Development and Maintenance			Define Integrated Test Plan
Business Continuity Management			Perform Preinstallation Test Plan
Compliance			Define System Validation Test Plan
			Perform Validation Test on Installed System
			Finalize Operational Security Measures
			Routine Security Reporting and Analysis
			Periodic Audit and Compliance Measures
			Reevaluate Security Countermeasures
			Work with Suppliers and Consultants
			Participate in Industry Forums and Development Programs

4. DISCUSSION – COMPARISON OF STANDARDS

The 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.

The Appendix compares the standards considered in this report. By examining the Appendix, 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 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, the ICS-SPP is written as a normative specification in the "Common Criteria" format. It primarily addresses system components. The ISA Technical Reports are informative in nature and are addressed to securing systems. The ISO/IEC standard considers the network, operating system, and application separately, and addresses recommendations such as passwords for each of these individually. This required the author's judgment in defining areas of comparison.

5. CONCLUSIONS

This report reviews and compares the recommendations provided in three cross-sector cyber security standards to ISO/IEC 17799. There are distinct differences in the topics considered by these standards. Through a careful examination of this comparison, and of the standards presented here, this report can be used to help identify and reduce the vulnerabilities in a control system. By knowing the vulnerabilities, standards can be applied to control systems to minimize the risk of intrusion.

Cyber security standards can provide increased security to control systems by giving an understanding of areas of concern and how they can be addressed. Although the three standards that were compared to the international information security standard were developed specifically for industries using manufacturing and control systems, they may be applied to other critical infrastructure segments or sectors. By comparing and sharing standards information across sectors, all sectors may benefit.

6. REFERENCES

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

7. 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

8. 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

9. Process Control Security Requirements Forum (PCSRF),
http://www.isd.mel.nist.gov/projects/processcontrol/

10. ISA web page, www.isa.org

11. ISA SP99, http://www.digitalbond.com/SCADA_security/SP99.htm

12. ANSI/ISA-TR99.00.01-2004, "Security Technologies for Manufacturing and Control Systems,"
http://www.isa.org/Template.cfm?Section=Products3&template=/Ecommerce/ProductDisplay.cfm&ProductID=7372

13. ANSI/ISA-TR99.00.02-2004, "Integrating Electronic Security into the Manufacturing and Control Systems Environment,"
http://www.isa.org/Template.cfm?Section=Products3&template=/Ecommerce/ProductDisplay.cfm&ProductID=7380

Appendix A

Security Standards Comparison

Appendix

Security Standards Comparison

Requirement	ISO/IEC 17799	ICS-SPP	TR99-01	TR99-02
SECURITY POLICY	3	2, 7.1.2.3		6
Information security policy.	3.1	2.2	7.1.3, 7.1.6, 8.4, 9.1.3	
Information security policy document.	3.1.1	2.3 (Table 2)		6.3, 6.4
Review and evaluation of information security policy.	3.1.2	3.1; Table 3		6.6.10
VULNERABILITY AND RISK ASSESSMENT		3, 4, 7, and 8		6.6.5, 9
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	3.2.1.2; 4; and Tables 5, 6, 8, 10, 7.2.1.3, 7.3.2	8.5.1	9.1
Three layer analysis.		7.1.2.1		
Security architecture analysis.		3.2.1.2.1, Table 5, 7.1.2		9.1.3
Successive compromise analysis.				9.1.3
Quantitative risk analysis.		4		9.1.3
Qualitative risk analysis.		7.2.1.3.1		9.1.3
Risk management process.		7.2.1		10.1
Mitigation program.		2.3 (Table 2)		10.1.1
Equipment backup.		2.2 (Table 1); 2.3 (Table 2)		
General considerations for conducting a risk and vulnerability assessment.		4.1 (Table 10); 6.2.9, 7.2.1.3, 7.3.1.3		
ORGANIZATIONAL SECURITY	4	2.2, 3.3; Table 9, 5.1 Table 11, 6.1.16,		6
Information security infrastructure.	4.1	5.1; Table 11		6
Management information security forum.	4.1.1			6.1
Information security coordination (within the organization).	4.1.2	5.1; Table 11		6.3.1

Requirement	ISO/IEC 17799	ICS-SPP	TR99-01	TR99-02
Allocation of information security responsibilities (for assets and processes including leadership and management).	4.1.3			6.3.1
Authorization process for new information processing facilities.	4.1.4			6.1
Specialist information security advice.	4.1.5			
Cooperation between (external) organizations.	4.1.6			6.6.3
Respond to disclosures of sensitive information.				
Independent review of information security.	4.1.7			
Staffing an InfoSec team.				6.3.1
Security of third party access.	4.2			6.6.8.2.7
Identification of risks from third party access.	4.2.1	2.2		7
Types of access (physical or logical).	4.2.1.1	3.1, 5.1 Table 11		
Reasons for access.	4.2.1.2			
On-site contractors.	4.2.1.3			
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	3.2.1.3; Table 7; 7.3.1.2		6.4
Accountability for assets.	5.1	7.3.1.2		6.4, 8
Inventory of assets.	5.1.1	7.3.1.2	10.1.6	9.1.1, 9.1.2
Information classification.	5.2		10.2	9.1.2.1
Classification guidelines.	5.2.1			9.1.3
Information labeling and handling.	5.2.2			6.6.8.4
PERSONNEL SECURITY	6		10.2	
Security in job definition and resourcing.	6.1	3.3, Table 9	10.2	6.1
Including security in job responsibilities.	6.1.1		10.2.1	
Personnel (background) screening and policy.	6.1.2		10.2	
Confidentiality agreements.	6.1.3			
Terms and conditions of employment.	6.1.4		10.2.1	
Identify personnel granted physical or electronic access.		6.1.6, 6.1.7	3	
Job responsibilities.			10.2	
User training.	6.2	3.3, Table 9; 6.2.3, 6.2.5	10.2	4

Requirement	ISO/IEC 17799	ICS-SPP	TR99-01	TR99-02
Information security education, training, and awareness.	6.2.1	3.3, Table 9; 6.2, Table 13; 6.2.3	10.2.1	4, 6.4
Responding to security incidents and malfunctions.	6.3	6.1.21		18.13
Incident reporting mechanisms.	6.3.1			
Reporting software malfunction.	6.3.3			
Learning from incidents.	6.3.4			18.12
PHYSICAL AND ENVIRONMENTAL SECURITY	7	6.1.20	9.1.4, 10	6.6.4, 6.6.8.3
Secure areas.	7.1		5.2.6	
Physical security perimeter.	7.1.1		7.4.2, 10.1.2, 10.1.4, 10.1.6	6.2.2, 6.6.8.3
Monitoring physical access.	7.1.1	6.1.21	10.1.1, 10.1.3, 10.1.5	6.6.4
Physical entry controls.	7.1.2	6.1.11	10.1.6	6.6.4
Securing offices, rooms, and facilities.	7.1.3	6.1.20	10.1.2	
Working in secure areas.	7.1.4			
Isolated delivery and loading areas.	7.1.5			
Intruder detection.	7.1.3.e	6.1.11	8.3, 10.1.1	
Equipment security.	7.2	6.1.14, 7.3.1.2	10.1.2	6.6.8.2.6, 6.6.8.3
Equipment siting and protection.	7.2.1		10.1.2	
Power supplies.	7.2.2			6.7.1
Cabling security.	7.2.3			6.7.1
Equipment maintenance.	7.2.4		10.2.2	
Security of equipment off-premises.	7.2.5			
Secure disposal or re-use of equipment.	7.2.6			6.6.8.4
Utility security.				8.2.1
Port security.				Annex A
General controls (information and information processing facilities).	7.3			
Clear desk and clear screen policy.	7.3.1		10.1.6	
Removal of property.	7.3.2			
COMMUNICATIONS AND OPERATIONS MANAGEMENT	8	6.1.18, 6.1.19		6.6.8.4
Operational procedures and responsibilities.	8.1			6.6.8.4
Documented operating procedures.	8.1.1		8.3.3?	

Requirement	ISO/IEC 17799	ICS-SPP	TR99-01	TR99-02
Operational change control.	8.1.2		5.1.1?, 6.1.4?	
Incident management procedures.	8.1.3		8.1, 10.2.1	
Segregation of duties.	8.1.4			
Separation of development and operational facilities.	8.1.5			12.1
External facilities management.	8.1.6			
Testing and documentation procedure.			8.3.3	
System planning and acceptance.	8.2			6.6.8.4
Capacity planning.	8.2.1			
System acceptance.	8.2.2			
Protection against malicious software.	8.3		8.2	6.6.8.4
Operating status monitoring.			8.5.2	
Housekeeping.	8.4			6.6.8.4
Information back-up.	8.4.1			
Operator logs.	8.4.2			
Fault logging.	8.4.3			
Network management.	8.5		5.2.2, 8.5.2	6.6.8.1, 6.6.8.4
Network controls.	8.5.1			
Media handling and security.	8.6		10.1.2, 10.2	6.6.8.4
Management of removable computer media.	8.6.1		10.1.2	6.6.8.4
Disposal of media.	8.6.2, 7.2.6		10.1.2, 10.1.6	6.6.8.4
Information handling procedures.	8.6.3		10.1.2	6.6.8.4
Information protection.			10.1.2	
Security of system documentation.	8.6.4			6.6.8.4
File Transfer Protocol.			3.1, 6.1	
Information distribution.			5.3.3	
Exchanges of information and software.	8.7			6.6.8.4
Information and software exchange agreements.	8.7.1			
Security of media in transit.	8.7.2			
Electronic commerce security.	8.7.3			
Security of electronic mail: security risks and policy on electronic mail.	8.7.4, 8.7.4.1, 8.7.4.2		6.1.4, 9.1.4	
Security of electronic office systems.	8.7.5			
Publicly available systems.	8.7.6			

Requirement	ISO/IEC 17799	ICS-SPP	TR99-01	TR99-02
Other forms of information exchange.	8.7.7			
ACCESS CONTROL	9	6.1.1, 6.1.7	6	6.6.8.2
Business requirements for access control.	9.1	6.1.7	8.2.4, 10.1.6, 10.2.1	
Access control policy.	9.1.1	6.1.7	5.1	
Policy and business requirements.	9.1.1.1	6.1.7		
Access control rules.	9.1.1.2	6.1.1, 6.1.7		
User access management.	9.2	6.1.1	5.1.1	6.6.8.2.1
User registration.	9.2.1	6.1.1		6.6.8.2.1
Privilege management.	9.2.2	6.1.1	5.1.1	6.6.8.2.1
Authentication (field devices).			5	
User password management.	9.2.3	6.1.2	5.2.6	
Review of user access rights.	9.2.4			
User responsibilities.	9.3	6.1, Table 12		6.6.8.2.2
Password use.	9.3.1	6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6		6.6.8.2.2
Unattended user equipment (protection).	9.3.2	6.1.5		6.6.8.2.2
Network access control.	9.4		5	6.6.8.2.3
Policy on use of network services.	9.4.1			6.6.8.2.3
Enforced path.	9.4.2			6.6.8.2.3
Securing remote access.		6.1.22, 6.1.23, 6.1.24	9.1.3	
User authentication for external connections.	9.4.3	6.1.22, 6.1.23, 6.1.24		6.6.8.2.3
Connections to the internet.			7.1.1, 7.1.4	6.6.8.2.7
VPN Access.			7.4.2	Annex A
Node authentication.	9.4.4			
Remote diagnostic port protection.	9.4.5			
Segregation in networks (firewalls).	9.4.6	6.1.9		
Network connection control.	9.4.7			
Network routing control.	9.4.8			
Electronic access controls.			6.1	
Operating system access control.	9.5	6, 6.1.1-6.1.6	5.2.4, 6.2.4, 6.3.5	6.6.8.2.4
Automatic terminal identification.	9.5.1	6.1.1		6.6.8.2.4
Terminal log-on procedures.	9.5.2	6.1.1		6.6.8.2.4

Requirement	ISO/IEC 17799	ICS-SPP	TR99-01	TR99-02
User identification and authentication.	9.5.3	6.1.1		6.6.8.2.4
Password management system.	9.5.4	6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6	5	6.6.8.2.4
Use of system utilities.	9.5.5		5.8	6.6.8.2.4
Duress alarm to safeguard users.	9.5.6			6.6.8.2.4
Terminal time-out.	9.5.7			6.6.8.2.4
Limitation of connection time.	9.5.8			6.6.8.2.4
Application access control.	9.6			6.6.8.2.5
Information access restriction.	9.6.1			6.6.8.2.5
Sensitive system isolation.	9.6.2			6.6.8.2.5
Monitoring system access and use.	9.7		3.1, 5.5.3, 6.1, 6.2, 8	6.6.8.2.6
Event logging.	9.7.1	6.1.21		6.6.8.2.6
Monitoring system use/access.	9.7.2	6.1.21	8.1	6.6.8.2.6
Procedures (for monitoring use including intrusion detection systems) and areas of risk.	9.7.2.1	7.2, 7.2.1		
Review results of monitoring activities based on risk factors.	9.7.2.2	8.1, 8.1.1	8.1	
Logging and reviewing events (emphasis on review).	9.7.2.3		8.2, 8.3	
Clock synchronization.	9.7.3			
Mobile computing and teleworking considerations.	9.8, 9.8.1, 9.8.2		5.3.2, 7.4.2, 9.1.3	6.6.8.2.7
Field Device Access			9.2.2	6.6.8.1
Authentication.			5.7	
Physical security.			10.1.2	
SYSTEMS DEVELOPMENT AND MAINTENANCE	10	6, 6.1 Table 12		6.6.9
Systems management policies and procedures.				4
New systems and significant changes to existing systems must use information security test procedures.				6.6.9, 6.7, 18.3
Security in application systems.	10.2		9	6.5
Input data validation.	10.2.1			
Control of internal processing.	10.2.2			
Areas of risk.	10.2.2.1		9.1.3, 9.2.3, 9.3.3	
Checks and controls.	10.2.2.2			

Requirement	ISO/IEC 17799	ICS-SPP	TR99-01	TR99-02
Message authentication.	10.2.3			
Output data validation.	10.2.4			
Cryptographic controls.	10.3		7	
Policy on the use of cryptographic controls.	10.3.1		7.1, 7.2, 7.3, 7.4	Annex A
Encryption.	10.3.2		7	10.2.3
Digital signatures considerations.	10.3.3		7.2	
Non-repudiation services.	10.3.4		7.2.4	
SCADA Cryptographic system component requirements.			7.2	
Management components.			7.2	
Cryptographic module components.			7.1, 7.2	
SCADA Communication channel encryption components.			7.1, 7.2	
SCADA Cryptographic system design goals.			7.4	
Key management.	10.3.5		7.1	
Protection of cryptographic keys.	10.3.5.1		7.1.6	
Standards, procedures, and methods.	10.3.5.2			
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		9	6.6.9
Change control procedures.	10.5.1			18.3
Technical review of operating system changes.	10.5.2			
Restrictions on changes to software packages.	10.5.3			
Outsourced software development considerations.	10.5.5			
Security patch management.			9.1.4	12.1
BUSINESS CONTINUITY MANAGEMENT	11	3.3, Table 9, 5.1 Table 11		
Aspects of business continuity management.	11.1	5.1 Table 11		
Business continuity management process.	11.1.1	5.1 Table 11		
Business continuity and impact analysis.	11.1.2	5.1 Table 11		
Writing and implementing continuity plans.	11.1.3	5.1 Table 11		
Business continuity planning framework (consistency of plans).	11.1.4	5.1 Table 11		
Testing, maintaining, and re-assessing business continuity plans.	11.1.5, 11.1.5.1-11.1.5.2	5.1 Table 11		

Requirement	ISO/IEC 17799	ICS-SPP	TR99-01	TR99-02
COMPLIANCE	12			
SCADA System Compliance Requirements.		1.2, 7.1		18.7
Compliance monitoring process (compliance with standard).				20
				8.2.1
Compliance with legal requirements.	12.1		8.2.4	
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	5.1 Table 11		
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	5.1 Table 11	6.1.6	6.6.8
Compliance with security policy (auditing).	12.2.1	5.1 Table 11	6.1.6	18.15.1
Technical compliance checking.	12.2.2	5.1 Table 11		18
System audit considerations.	12.3	6.1.10, 6.1.12, 6.1.13	8	20
System audit controls.	12.3.1			
Protection of system audit tools.	12.3.2		8.1	
Post-implementation auditing.			8.2, 8.3, 8.4, 8.5	
Recursive auditing.			8.2, 8.3, 8.4, 8.5	