



Contents

About the Author	vii
Acknowledgments	xvii
Introduction	xix
Chapter 1 What Is a SCADA System?	1
History of Critical Infrastructure Directives	1
SCADA System Evolution, Definitions, and Basic Architecture	3
SCADA Evolution	5
SCADA Definition	6
SCADA System Architecture	7
SCADA Applications	10
SCADA System Security Issues Overview	16
SCADA and IT Convergence	16
Conventional IT Security and Relevant SCADA Issues	17
Redundancy as a Component of SCADA Security	20
SCADA System Desirable Properties	20
Summary	22
Chapter 2 SCADA Systems in the Critical Infrastructure	23
Employment of SCADA Systems	23
Petroleum Refining	23
The Basic Refining Process	24
Possible Attack Consequences	26
Nuclear Power Generation	26
The Boiling Water Reactor	27
The Pressurized Water Reactor	28
Possible Attack Consequences	29

	Conventional Electric Power Generation	30
	Petroleum Wellhead Pump Control	32
	Water Purification System	34
	Crane Control	36
	SCADA in the Corporation	37
	Chemical Plant	38
	Benzene Production	38
	Embedded Systems	40
	Why We Should Worry about These Operations	40
	Summary	41
Chapter 3	The Evolution of SCADA Protocols	43
	Evolution of SCADA Protocols	43
	Background Technologies of the SCADA Protocols	44
	Overview of the OSI Model	44
	Overview of the TCP/IP Model	48
	SCADA Protocols	50
	The MODBUS Model	50
	The DNP3 Protocol	52
	UCA 2.0 and IEC61850 Standards	53
	Controller Area Network	54
	Control and Information Protocol	55
	DeviceNet	56
	ControlNet	57
	EtherNet/IP	57
	FFB	59
	Profibus	61
	The Security Implications of the SCADA Protocols	63
	Firewalls	63
	Packet-Filtering Firewalls	63
	Stateful Inspection Firewalls	65
	Proxy Firewalls	65
	Demilitarized Zone	65
	Single Firewall DMZ	66
	Dual Firewall DMZ	66
	General Firewall Rules for Different Services	66
	Virtual Private Networks	69
	Summary	71
Chapter 4	SCADA Vulnerabilities and Attacks	73
	The Myth of SCADA Invulnerability	73
	SCADA Risk Components	76
	Managing Risk	78
	Risk Management Components	79
	Assessing the Risk	79
	Mitigating the Risk	80

	SCADA Threats and Attack Routes	81
	Threats	81
	SCADA Attack Routes	82
	Typical Attacker Privilege Goals	83
	SCADA Honeynet Project	85
	Honeypots	85
	Honeynet Project	86
	SCADA Honeynet	86
	Summary	87
Chapter 5	SCADA Security Methods and Techniques	89
	SCADA Security Mechanisms	89
	Improving Cybersecurity of SCADA Networks	90
	Implementing Security Improvements	96
	SCADA Intrusion Detection Systems	97
	Types of Intrusion Detection Systems	98
	Network-Based and Host-Based IDS	98
	Signature-Based and Anomaly-Based IDS	99
	Active-Response IDS	99
	Passive-Response IDS	100
	Processing of IDS Data	100
	Vulnerability Scanning and Analysis	100
	SCADA Audit Logs	102
	Security Awareness	106
	Summary	108
Chapter 6	SCADA Security Standards and Reference Documents	109
	ISO/IEC 17799:2005 and BS 7799-2:2002	110
	ISO/IEC 1779:2005	111
	BS 7799-2:2002	112
	ISA-TR99.00.01-2004, <i>Security Technologies for Manufacturing and Control Systems</i>	113
	ISA-TR99.00.02-2004, <i>Integrating Electronic Security into the Manufacturing and Control Systems Environment</i>	114
	GAO-04-140T, <i>Critical Infrastructure Protection, Challenges in Securing Control Systems</i>	115
	NIST, <i>System Protection Profile for Industrial Control Systems (SPP ICS)</i>	117
	Federal Information Processing Standards Publication (FIPS Pub) 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i> , February 2004	117
	Additional Useful NIST Special Publications	119
	NIST Special Publication 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i>	119

	NIST Special Publication 800-53, <i>Recommended Security Controls for Federal Information Systems</i>	120
	NIST Special Publication 800-53A, <i>Guide for Assessing the Security Controls in Federal Information Systems</i>	121
	Summary	122
Chapter 7	SCADA Security Management Implementation Issues and Guidelines	123
	Management Impressions of SCADA Security	123
	SCADA Culture	124
	Unique Characteristics and Requirements of SCADA Systems	125
	Limitations of Current Technologies	126
	Guidance for Management in SCADA Security Investment	127
	Information-System Security Engineering	127
	Discover Information Protection Needs	128
	Define System Security Requirements	128
	Design System Security Architecture	128
	Develop Detailed Security Design	129
	Implement System Security	129
	Common Criteria Protection Profiles	130
	Defense-in-Depth	130
	People	131
	Technology	131
	Operations	132
	Defense-in-Depth Strategy	132
	The NIST SP 800-14, <i>Generally Accepted Principles and Practices for Securing Information Technology Systems</i>	134
	NIST Special Publication 800-26, <i>Security Self-Assessment Guide for Information Technology Systems</i>	136
	Summary	137
Chapter 8	Where We Stand Today	139
	The Status Today	139
	Human Issues	140
	Weakness of Standard Security Approaches	142
	The Oil and Gas Industry	142
	API Standard 1164	143
	AGA Report Number 12	144
	Interdependencies	144
	Rail System Security	145
	Port Security	146
	Legislation	148
	Threats to Seaports	148
	Countermeasures	149
	Conventional Countermeasures	149
	Advanced Countermeasures	150
	Security Controls That Can Be Put in Place Now	151
	Summary	152

Appendix A Acronyms and Abbreviations	153
Appendix B System Protection Profile – Industrial Control Systems	157
Appendix C Bibliography	195
Index	201

