Chapter 3 of: Industrial Automation and Control System Security Principles: Protecting the Critical Infrastructure,

Second Edition

Ronald L. Krutz, PhD, PE

Industrial Automation and Control System Security Principles:

Protecting the Critical Infrastructure, Second Edition





Industrial Automation and Control System Security Principles: Protecting the Critical Infrastructure Second Edition

By Ronald L. Krutz, PhD, PE



Notice

The information presented in this publication is for the general education of the reader. Because neither the author nor the publisher has any control over the use of the information by the reader, both the author and the publisher disclaim any and all liability of any kind arising out of such use. The reader is expected to exercise sound professional judgment in using any of the information presented in a particular application.

Additionally, neither the author nor the publisher has investigated or considered the effect of any patents on the ability of the reader to use any of the information in a particular application. The reader is responsible for reviewing any possible patents that may affect any particular use of the information presented.

Any references to commercial products in the work are cited as examples only. Neither the author nor the publisher endorses any referenced commercial product. Any trademarks or tradenames referenced belong to the respective owner of the mark or name. Neither the author nor the publisher makes any representation regarding the availability of any referenced commercial product at any time. The manufacturer's instructions on the use of any commercial product must be followed at all times, even if in conflict with the information in this publication.

Copyright © 2017 International Society of Automation (ISA) All rights reserved.

Printed in the United States of America. 1098765432

ISBN: 978-1-941546-82-6

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

ISA 67 T. W. Alexander Drive P.O. Box 12277 Research Triangle Park, NC 27709

Library of Congress Cataloging-in-Publication Data in process

3

Industrial Automation and Control System Culture versus IT Paradigms

Some of the basic principles of information system security were presented in Chapter 2 as a prelude to selectively and properly applying them to securing industrial automation and control systems. As a prerequisite to this adaptation, it is important to examine the differences in culture, requirements, and operational issues between automation and control systems and IT systems. Critical areas that have to be addressed include safety, real-time demands, maintenance, productivity, training, and personnel mindsets. These topics and related subject areas are discussed in this chapter to help the reader better understand how to apply security principles to automation and control systems without negatively impacting their primary mission and in full acknowledgement of their special requirements.

Differences in Culture, Philosophy, and Requirements

The major advances in securing computer systems and networks have come through the information system technology route, with origins in computer science and software engineering. The principal players are IT system administrators, systems analysts, database administrators, software engineers, network administrators, chief information officers (CIOs), and so on. On the other hand, a large number of the personnel populating the industrial automation and control system field come from engineering backgrounds, with training in such areas as electrical engineering, chemical engineering, mechanical engineering, systems engineering, and control engineering. The motivation, requirements, and focus of each of the groups are, in many instances, largely divergent, with some overlapping common areas. For example, software quality and process improvement methods widely used in the IT environment are often foreign to control engineers and in fact may be viewed as cumbersome in implementing SCADA and process control algorithms. In addition, the performance of a process in a plant is critical, and inadequate performance in production areas can result in huge financial losses, equipment damage, and personnel injuries. These severe consequences of operational errors are not usually a common occurrence in IT facilities. Similarly, safety is a critical concern in a production environment, and control system malfunctions can result in fires or explosions in some instances. Thus, in a production environment, safety and performance usually take precedence over information security, which is not the case in an IT system.

Some of the major differences between IT and industrial automation and control system requirements are listed in Table 3-1.

Issue	IT Systems	Industrial Automation and Control Systems
Application of encryption	Advanced encryption systems used.	Encryption used sometimes or not at all. Delays caused by encryption software are a consideration.
Degree of employment of patch management	Implementation of software patches performed routinely under formal procedures.	Installation of software patches usually done infrequently, with deliberation, and with involvement of vendors. The impact of software patches should be tested off- line to ensure no harmful effects are introduced into the process or plant. In some instances, adding patches can produce some dangerous consequences.
Degree of vulnerability testing	Penetration testing by ethical hackers is widely used to expose vulnerabilities.	Penetration testing must be conducted sparingly and at appropriate times in order not to inadvertently cause malfunctions in monitoring and control systems.

 Table 3-1. Comparison between IT and Industrial Control and

 Automation Systems Issues

Automation Syste	ms Issues	
Employment and impact of security software	Antivirus software is effective and commonly used to scan for malware.	Antivirus software can be used but issues, such as delays due to scanning and processing and lack of spare computing cycles, might cause problems in plant systems.
Employment of change management	Change management is used extensively to document and confirm system changes.	Change management is employed inconsistently and sporadically in many organizations. Changes might also result in hazardous situations.
Impact of equipment upgrades	Equipment modifications, upgrades, and replacements occur almost continuously in various parts of organizations.	Many legacy systems in use with few changes over periods of many years.
Level of security awareness training	Awareness training is actively conducted in accordance with security policy.	Security awareness training is conducted sporadically and inconsistently in many cases.
Tolerance to data loss	Recovery from data loss can usually be accomplished from backups without severe consequences in most situations.	Loss of data can result in loss of product, unsafe conditions, and disruption of plant operations.
Tolerance to loss of availability	Recovery follows standard procedures and unless availability is lost for extended periods of time, effects are not disastrous. However, availability is critical and can affect mission objectives.	Systems should be designed with resiliency; however many are not, particularly legacy systems. Loss of availability can have serious consequences, including safety of personnel and equipment.
Tolerance to loss of confidentiality	Depending on the data involved, the consequences might be minimal or extremely harmful, such as the loss of trade secrets, personnel data, credit card numbers, and health information.	Consequences not usually severe.
Tolerance to loss of integrity	Consequences can range from minimal to extremely harmful if critical data has been altered and is acted on as being valid.	Consequences can be very severe because, in many instances, critical decisions are made based on data assumed to be correct.

Table 3-1. Comparison between IT and Industrial Control and

68

Tolerance to system delays	In most cases, delays might be considered a nuisance, but can be tolerated.	In situations where critical control decisions are based on deterministic response times, delays might result in serious or dangerous consequences.
Use of auditing	Based on organizational polices, internal and external audits are normally conducted and provide detective controls for breaches of information system security.	Audits of a systems' security posture are conducted irregularly and are a function of the particular organization and regulatory requirements.
System performance	Performance can be suboptimal at times.	Proper performance is critical.
Safety	Safety is critical, particularly that of personnel.	Safety is critical, particularly that of personnel.

Table 3-1. Comparison between IT and Industrial Control andAutomation Systems Issues

Figure 3-1 summarizes the important issues listed in Table 3-1 and emphasizes some of the common areas between IT and automation and control systems.

The lesson to be learned from these comparisons is that traditional information system security knowledge and methods provide a solid basis for addressing industrial automation and control system security, albeit with deliberate, appropriate, and intelligent modifications required to address the unique characteristics of automation and control systems.

One important starting point in incorporating these modifications is education. In general, most universities and certification programs addressing computer and network security have been heavily focused on IT security. Automation and control systems, which are typically sitting on isolated networks and are relatively few in number compared to IT systems, have not been considered to be interesting targets. With the advent of the terrorism threat, this situation is no longer the case. In addition, SCADA and plant process control systems are now being connected to large networks and the Internet.

The Certified Information System Security Professional (CISSP) and related certifications do not address the security of industrial automation and control



Figure 3-1. IT and Automation and Control System Issue Comparisons

systems. Organizations, such as ISA, have addressed this problem and are filling a critical need. NIST has generated special publications that directly address industrial automation and control systems. However, it is important that security training related to the control of production lines, industrial processes, electrical transmission and distribution, pipelines, chemical plants, and so on moves to the fore in universities, technical institutes, and certification organizations.

To understand how to adapt IT security methods to industrial automation and control system security, threats to the latter have to be identified and understood. One impediment to full disclosure of threats realized is the fact that a majority of affected facilities are privately owned, and these organizations are reluctant to publicize security breaches that could negatively affect their reputation and value.

Organizations also need incentives to invest in upgrading their automation and control infrastructure. Many existing installations have been in place for 10 or 20 years, and investments in security have to compete with other compelling initiatives in an organization.

Considerations in Adapting IT Security Methods to Industrial Automation and Control Systems

In order to secure an IACS, there are specific issues that have to be addressed that take into account the differences between IT systems and IACSs. These issues include the following:

- Accountability, authorization, and computer forensics have not matured and have not been implemented widely in IACSs as compared to IT systems.
- Ethernet to serial line paths provide a means of injecting malicious commands into a control network.
- Excessive checking, encryption, monitoring, and so on can interfere with the deterministic nature of process control systems.
- In many IACS environments, control engineers have multiple responsibilities that, in many instances, violate the security principle of separation of duties.
- Installing patches and upgrades in process control systems can lead to serious and sometimes dangerous situations in production facilities.
- Life-cycle design disciplines common in the IT field are not widely used in industrial automation and control systems.

- Maintenance hooks and trap doors installed in automation and control systems for remote maintenance can be easy entry points to modify critical software and firmware with negative consequences.
- Many IACS vendors combine safety mechanisms with security mechanisms, leading to single points of failure and less resiliency than separating these two functions logically and physically.
- Many manufacturing facilities and SCADA installations house legacy systems with outdated technology, minimal memory and computing power, and little thought to security.
- Port scanning of automation and control systems can result in blockages and lack of system availability.
- Remote access into automation and control systems via older modems or newer wireless devices poses a serious threat to security.
- There is a trend to apply protocols used for IT systems to industrial control and automation systems because of their wide availability, their lower cost, and the existence of trained personnel. However, in most instances, these protocols were not designed for deterministic process control systems, and they are vulnerable to many existing attacks.
- There is heavy reliance on suppliers who provide modified software and hardware for IACSs, resulting in nonstandard implementations that are difficult to maintain without support from these suppliers.
- Weak authentication mechanisms in many SCADA systems and networked plant control systems leave them vulnerable to attack.

A variety of additional items must be considered when discussing comparisons between IT and industrial automation and control systems. The concepts related to risk management and the means to protect industrial automation and control systems will be discussed in detail in Chapters 5 and 6, respectively. However, it is important to now examine some related critical subject areas to provide a basis for developing more specific security solutions.

Threats

Threats to IT and industrial automation and control systems come from different sources, with different motivations. It is important to understand these threat sources and their characteristics in order to counter any malicious activities on their part. NIST SP 800-30¹ summarizes the various types of threat sources and some of their driving factors, as shown in Table 3-2. Table 3-3, also from NIST SP 800-30, provides a listing of some general threat sources, including environmental ones, which can also cause disruptions to industrial automation and control systems.

The categories of terrorists, industrial espionage, and insiders are of particular interest in connection with industrial automation and control systems. Traditionally, insider threats have been considered one of the most dangerous because they give insiders the ability to bypass protective measures. However, external threats are increasing and are also of grave concern, particularly relating to our nation's critical infrastructure and resource processing plants. In addition, threats to automation systems can materialize from environmental and structural sources, as illustrated in the next section.

Sensitivity of Industrial Automation and Control Systems to Upgrades and Modifications

One area that is not usually considered when discussing the relative sensitivities of IT systems and industrial automation and control systems is the effects of equipment upgrades and modifications. A particularly relevant example concerns the consequences of converting analog controls to digital controls. Digital systems transfer information via pulses, which inherently generate high frequency electromagnetic radiation that can interfere with control system operations. An article in the journal *Interference Technology*² describes the electromagnetic radiation environment in a nuclear plant that was being changed from analog to digital controls. The authors obtained measurement data in the range of 100 Hz to 6 GHz in instances before and after the conversion.

Table 3-2. Threats and Motivations for Attackers

Source: NIST SP 800-30 (2012)

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	 Hacking Social engineering System intrusion, break-ins Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	 Computer crime (e.g., cyber stalking) Fraudulent act (e.g., replay, impersonation, interception) Information bribery Spoofing System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	 Bomb/terrorism Information warfare System attack (e.g., distributed denial of service) System penetration System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	 Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	 Assault on an employee Blackmail Browsing of proprietary information Computer abuse Fraud and theft Information bribery Input of falsified, computed data Interception Malicious code (e.g., virus, logic bomb, Trojan horse) Sale of personal information System bugs System intrusion System sabotage Unauthorized system access

The testing followed guidelines in U.S. Nuclear Regulatory Commission Regulatory Guide, NUREG 1.180,³ and Electric Power Research Institute (EPRI) document TR-102023-2004.⁴ In the tests, antennas were installed next to three cabinets housing control electronics, and radiation emission measurements were taken from the analog and digital control installations. Some of the results obtained are summarized in Table 3-4, showing frequencies at which peak amplitudes occur at antennas 1 and 2.

Table 3-3. Listing of General Threat Sources

Source: NIST SP 800-30 (2012)

Type of Threat Source	Description	Characteristics
Adversarial Individual Outsider Insider Trusted insider Privileged insider Group Ad hoc Established Organization Nation-state 	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, intent, targeting
 Accidental Ordinary user Privileged user/ administrator 	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects
Structural IT Equipment Storage Processing Communications Display Sensor Controller Environmental controls Temperature/humidity controls Power supply Software Operating system Networking General-purpose application Mission-specific application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters.	Range of effects

Table 3-3. Listing of General Threat Sources

Source: NIST SP 800-30 (2012)

Environmental	Natural disasters and failures of critical	Range of effects
 Natural or man-made 	infrastructures on which the organization	
disaster	depends, but which are outside the control	
Fire	of the organization.	
 Flood/tsunami 		
 Windstorm/tornado 	NOTE: Natural and man-made disasters	
Hurricane	can also be characterized in terms of their	
 Earthquake 	severity and/or duration. However,	
Bombing	because the threat source and the threat	
Overrun	event are strongly identified, severity and	
• Unusual natural event (e.g.,	duration can be included in the description	
sunspots)	of the threat event (e.g., Category 5	
Infrastructure failure/outage	hurricane causes extensive damage to the	
 Telecommunications 	facilities housing mission-critical systems,	
 Electrical power 	making those systems unavailable for	
	three weeks).	

Table 3-4. Radiation Emission Measurements

Source: Keebler and Berger (2011)

	Analo	g Measurement	Digital Measurement	
Antenna [–]	Frequency	Significant Peak Amplitudes (dBµV/m)	Frequency	Significant Peak Amplitudes (dBµV/m)
1	1.34 MHz	99.2	468 MHz	71.6
1	928 MHz	76.6	826 MHz	94.5
1			928 MHz	113.5
1			1.35 GHz	49.9
1			1.88 GHz	50.5
1			1.92 GHz	53.4
1			2.41 GHz	76.3
1			2.46 GHz	54.4
1			5.82 GHz	60.6
2	1.04 MHz	99.3	2 MHz	84
2	4.55 MHz	88.5	10 MHz	80
2			1 GHz	109
2			1.17 GHz	48.8
2			1.92 GHz	48.9
2			2.42 GHz	57.7
2			5.82 GHz	50.9

This data is plotted in Figures 3-2 and 3-3 for antennas 1 and 2, respectively. Note that the digital electronics generate more peak radiation generally and more at high frequencies compared to the analog equipment. These peak emissions have the potential to interfere with control system signals and cause malfunctions if proper shielding and isolation are not applied.

The sample electromagnetic emanations collected illustrate the necessity to ensure electromagnetic compliance (EMC) when equipment upgrades are made to plant control systems. These actions will serve to protect against interruptions of control systems' operation due to electromagnetic emissions from digital systems.



Figure 3-2. Analog and Digital Radiation Emissions Received at Antenna 1

IT and Industrial Automation and Control Systems Comparisons from a Standards Perspective

Valuable insight into the contrasts and similarities between IT systems security focus areas and those of industrial automation and control systems can be obtained from an example using standards that represent each of the areas. In this example, ISO/IEC 27002, *Code of Practice for Information Security Management*,⁵ will be used to represent IT systems security areas of emphasis while ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems*



Figure 3-3. Analog and Digital Radiation Emissions Received at Antenna 2

*Security Program,*⁶ will be used to illustrate the major concerns of automation and control system security.

In each document, there are common areas addressed by both standards and other areas addressed by one standard and not the other. Figure 3-4 summarizes the main characteristics of each standard and identifies common areas addressed by both, as well as topics that are addressed mainly by one document and not the other.

Figure 3-4 shows that topics, such as change management, email security, access control policies, digital signatures, compliance, and business continuity planning are among the areas considered critical for IT systems that are not emphasized in automation and control system standards. Conversely, for automation and control systems, the significant domains not covered include security architecture analysis, quantitative and qualitative analysis, information security management, and information security testing. Areas of common emphasis include information security policy, risk assessment, training, media physical security, remote access, event logging, and protection against malware.



Figure 3-4. Standards Comparison Example of IT versus IACSs Important Security

79

Summary

Understanding the requirements of industrial automation and control systems security and how they relate to IT systems requires a mapping of these requirements onto the emerging technologies being employed in the control of production processes, as well as the critical infrastructure (represented primarily by the electrical generation and distribution grid). The advances in capability and sophistication of industrial automation and control systems require a tailored approach to security. Some of the factors pushing the industrial automation and control systems security envelope include:

- The Smart Grid
- Advanced cryptography and key management applications
- Advanced PLCs and PACs
- Advanced protective relaying
- Advanced wireless networks
- Alarm processing
- Availability of real-time energy information
- Multisphere security among IT, transportation, and power systems
- Redundancy in networks, equipment, and sensors
- Fiber communication
- Use of GPS tracking

Chapter 4 will investigate the technical evolution taking place in elements of the critical infrastructure and in key production facilities to identify the important risk factors and areas of maximum potential impact in the event of an attack.

Review Questions for Chapter 3

- 3.1 Which of the following statements is generally TRUE regarding an industrial automation and control system?
 - A. Installation of software patches can be performed routinely and frequently.
 - B. Encryption of data can sometimes lead to problematic delays.
 - C. Penetration testing can be conducted routinely and frequently.
 - D. Confidentiality is a key concern in automation systems as opposed to integrity and availability.
- 3.2 In both IT and automation and control systems, which of the following is the primary concern in the event of an emergency or malicious event?
 - A. Equipment safety
 - B. Preservation of documentation
 - C. Personnel safety
 - D. Facility protection
- 3.3 Which of the following statements is FALSE?
 - A. Flash drives and other portable memory devices can be sources of malware injections into control systems.
 - B. Maintenance hooks and trap doors installed in automation and control systems for remote maintenance can be easy entry points to modify critical software and firmware with negative consequences.
 - C. In many control system environments, control engineers, in general, do not have multiple responsibilities, such that the security principle of separation of duties is not normally violated.
 - D. Many facilities house legacy systems with outdated technology, minimal memory and computing power, and little thought to security.

- 3.4 Which of the following actions is the most likely to result in blockages and lack of system availability in automation and control systems?
 - A. Remote access
 - B. Life-cycle design
 - C. Accountability
 - D. Port scanning
- 3.5 Which threat source is motivated by revenge, ego, and dissatisfaction?
 - A. Insider
 - B. Espionage
 - C. Criminal
 - D. Hacker
- 3.6 What is a source of a possible disruption of control system functions that is not normally considered?
 - A. Changes from digital to analog systems
 - B. Upgrades from analog to digital systems
 - C. Malware
 - D. Attacks
- 3.7 In general, what distinguishes analog control equipment from digital control equipment?
 - A. Analog controls generate more high-frequency peak voltages than digital controls.
 - B. Digital controls generate more high-frequency peak voltages than analog controls.
 - C. Analog controls generate essentially the same number of high-frequency peak voltages as digital controls.
 - D. Digital controls generate essentially the same number of high-frequency peak voltages as analog controls.

- 3.8 Which of the following is more likely to be performed in an IT environment than in an automation and control system environment?
 - A. Security architecture analysis
 - B. Information security testing
 - C. Quantitative risk analysis
 - D. Change management
- 3.9 Which of the following is more likely to be performed in an IT environment than in an automation and control system environment?
 - A. Security architecture analysis
 - B. Information security testing
 - C. Quantitative risk analysis
 - D. Change management
- 3.10 Which of the following threat sources is motivated by economic exploitation and competitive advantage, and uses social engineering?
 - A. Insider
 - B. Terrorist
 - C. Industrial espionage
 - D. Computer criminal
- 3.11 What is a detective control that is more frequently applied in IT systems than in control and automation systems?
 - A. Firewall
 - B. Separation of duties
 - C. Biometrics
 - D. Auditing

- 3.12 Which of the following is NOT a usual reason for an organization's reluctance to disclose successful attacks against it?
 - A. Hope the attack will harm competitors
 - B. Embarrassment
 - C. Effect on reputation
 - D. Possible loss of customers
- 3.13 Which of the following can lead to a single point of failure in an industrial automation and control system?
 - A. Separation of duties
 - B. Disk redundancy
 - C. Combination of safety and security mechanisms
 - D. Use of authentication with identification
- 3.14 What is a typical characteristic of industrial automation and control systems?
 - A. Have excess computing cycles
 - B. Have limited extra computing cycles
 - C. Have excess memory
 - D. Computational speed is not an issue
- 3.15 What is a typical characteristic of an automation and control system supplier?
 - A. Usually ensures maintenance hooks are never left enabled without the customer's approval
 - B. Usually ensures default passwords are never duplicated from one customer to another
 - C. Usually provides unmodified off-the-shelf hardware and software
 - D. Usually provides modified hardware and software

References

- NIST SP 800-30. *Guide for Conducting Risk Assessments*. Revision 1. Washington, DC: NIST (National Institute of Standards and Technology), 2012.
- 2. Keebler, P., and S. Berger. "Going from Analog to Digital." *Interference Technology*, 2011 EMC Directory and Design Guide, 2011.
- U.S. Nuclear Regulatory Commission (NRC) Regulatory Guide NUREG 1.180. Guidelines for Evaluating Electronic and Radio Frequency Interference in Safety-Related Instrumentation and Control Systems. Revision 1. Washington, DC: U.S. Nuclear Regulatory Commission, 2003.
- 4. EPRI TR-102323-2004. *Guidelines for Electromagnetic Interference Testing in Power Plants*. Revision 3. Palo Alto, CA: EPRI (Electric Power Research Institute), 2004.
- ISO/IEC Standard 27002-2005. Information Technology Security Techniques – Code of Practices for Information Security Management. Geneva 20 – Switzerland: IEC (International Electrotechnical Commission) and ISO (International Organization for Standardization).
- 6. ANSI/ISA-62443-2-1 (99.02.01)-2009. Security for Industrial Automation and Control Systems – Part 2-1: Establishing an Industrial Automation and Control Systems Security Program. Research Triangle Park, NC: ISA (International Society of Automation).

About the Author

Ronald L. Krutz, PhD, PE, CISSP, ISSEP

Dr. Krutz is Chief Scientist for Security Risk Solutions, Inc. He has more than 30 years of experience in industrial automation and control systems, distributed computing systems, computer architectures, information assurance methodologies, and information security training. He has been a Senior Information Security Consultant at Lockheed Martin, BAE Systems, and REALTECH Systems Corporation, an Associate Director of the Carnegie Mellon Research Institute (CMRI), and a faculty member in the Carnegie Mellon University Department of Electrical and Computer Engineering. Dr. Krutz founded the CMRI Cyber Security Center and was founder and director of the CMRI Computer, Automation and Robotics Group. He was also a lead instructor for (ISC)² Inc. in its Certified Information Systems Security Professionals (CISSP) training seminars

He coauthored the CISSP Prep Guide for John Wiley and Sons and is coauthor of the Wiley Advanced CISSP Prep Guide; the CISSP Prep Guide, Gold Edition; the Security + Certification Guide; the CISM Prep Guide; the CISSP Prep Guide, Second Edition: Mastering CISSP and ISSEP (Information Systems Security Engineering Professional); the Network Security Bible; the CISSP and CAP (Certification and Accreditation Professional) Prep Guide, Platinum Edition: Mastering CISSP and CAP; the Certified Ethical Hacker (CEH) Prep Guide; Cloud Computing Security; and Web Commerce Security. He is also the author of Securing SCADA Systems and of three textbooks in the areas of microcomputer system design, computer interfacing, and computer architecture. Dr. Krutz has seven patents in the area of digital systems and has published more than 30 technical papers.

Dr. Krutz is also a Senior Fellow of the International Cyber Center of George Mason University.

Dr. Krutz holds BS, MS, and PhD degrees in Electrical and Computer Engineering, is a Registered Professional Engineer in Pennsylvania, and is a Senior Life Member of the IEEE.

Contents

bout the Author	. xiii
preword	xv
reface	. xix
hapter 1 Industrial Automation and Control System	1
Industrial Automation and Control Systems	····I
SCADA Systems	3
Distributed Control Systems	6
Safety Instrumented Systems	8
Industrial Automation and Control System Protocol Summary	10
The OSI Model	11
The TCP/IP Model	12
Object Linking and Embedding for Process Control	13
OPC Unified Architecture	14
Modbus/TCP Model	15
The Distributed Network Protocol	15
Utility Communications Architecture Version 2.0/IEC 61850	16
PROFIBUS	17
Controller Area Network	17
EtherNet/IP	17
openSAFETY Protocol.	18
Issues in Industrial Automation and Control Systems Security	19
Summary	20

	Review Questions for Chapter 1	21
	References	26
Chanter 2	Information System Coousity Technology	20
Chapter 2	Information System Security Technology	20 20
	Confidentiality	
	Availability	30
	Identification	30
	Authentication	
	Authorization	31
	Accountability	
	Auditing	
	Nonrepudiation	
	Related Terminology	
	Types and Classes of Attack	33
	Additional System Security Concepts	34
	Complete Mediation.	35
	Defense in Depth	35
	Economy of Mechanism	
	Fail-Safe	36
	Least Common Mechanism	36
	Least Privilege	36
	Leveraging Existing Components	36
	Open Design	
	Psychological Acceptability	37
	Separation of Duties	37
	Weakest Link	37
	Policies, Standards, Guidelines, and Procedures	
	Standards	
	Guidelines	
	Malizious Cada and Attacks	
	Viruses and Worms	
	Trojan Horso	30
	Logic Bomb	30
	Mobile Code	40
	Back Door	40
	Scanning	40
	Man-in-the-Middle	
	Social Engineering	
	Guessing Passwords	
	Denial of Service/Distributed Denial of Service	
	Replay	41

Firewalls 42 Packet-Filtering Firewall 42 Stateful Inspection 43 Application Firewall 44 Application-Proxy Gateway 44 Screened-Host Firewall 45 Dual-Homed Host Firewall 45 Screened-Subnet Firewalls 46 Cryptography 47 Symmetric Key Cryptography 47 Symmetric Key Cryptography 48 Digital Signatures 50 Attacks Against Cryptosystems 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary 56 Summary 56 Summary 56 Summary 56 Summary 56 Summary 55 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 57 Industrial Automation and Control Systems 70 Threats 72 IT and Industrial Automation and Control Systems 72 IT and Industrial	Firewalls Packet-Fili Stateful In Application Application Screened-J Dual-Hom Screened-S Cryptography Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	tering Firewall	42 42 43 44 45 45 45 45 46 47 47 48 50 52 53 56 56 57 63
Packet-Filtering Firewall 42 Stateful Inspection 43 Application Firewall 44 Application-Proxy Gateway. 44 Screened-Host Firewall 45 Dual-Homed Host Firewall 45 Screened-Subnet Firewalls 46 Cryptography. 47 Symmetric Key Cryptography. 47 Asymmetric Key Cryptography. 48 Digital Signatures 50 Attacks Against Cryptosystems. 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary. 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 55 Differences in Culture, Philosophy, and Requirements. 65 Considerations in Adapting IT Security Methods to 51 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 70 To and Industrial Automation and Control Systems 70 Compa	Packet-Filt Stateful In Application Screened-J Dual-Horr Screened-S Cryptography Symmetric Asymmetr Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Differences in Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tecl	tering Firewall	42 43 44 45 45 45 45 45 47 47 47 47 47 50 52 53 56 56 57 63
Stateful Inspection 43 Application Firewall 44 Application-Proxy Gateway 44 Screened-Host Firewall 45 Dual-Homed Host Firewall 45 Screened-Subnet Firewalls 46 Cryptography 47 Symmetric Key Cryptography 47 Asymmetric Key Cryptography 48 Digital Signatures 50 Attacks Against Cryptosystems 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 57 versus IT Paradigms 55 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 50 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 76 Comparisons for Ch	Stateful In Application Application Screened-J Dual-Hom Screened-S Cryptography Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	spection on Firewall	43 44 45 45 45 45 46 47 47 48 50 52 53 56 56 56 57 63
Application Firewall 44 Application Firewall 44 Screened-Host Firewall 45 Dual-Homed Host Firewall 45 Screened-Subnet Firewalls 46 Cryptography 47 Symmetric Key Cryptography 47 Asymmetric Key Cryptography 48 Digital Signatures 50 Attacks Against Cryptosystems 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary 56 Summary 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 56 versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 57 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Co	Application Application Screened-J Dual-Hom Screened-S Cryptography Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tech	on Firewall	44 45 45 45 46 47 47 47 48 50 52 53 56 56 56 57 63
Application-Proxy Gateway 44 Screened-Host Firewall 45 Dual-Homed Host Firewall 45 Screened-Subnet Firewalls 46 Cryptography 47 Symmetric Key Cryptography 47 Asymmetric Key Cryptography 47 Asymmetric Key Cryptography 48 Digital Signatures 50 Attacks Against Cryptosystems 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 65 versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 71 Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 79 Review Questions for Chapter 3 80 </th <th>Application Screened-J Dual-Hom Screened-S Cryptography Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tecl</th> <th>on-Proxy Gateway Host Firewall Ned Host Firewall Subnet Firewalls C Key Cryptography ric Key Cryptography. st Cryptosystems. Network Network Ckets Layer</th> <th> 44 45 45 46 47 47 48 50 52 53 56 56 56 57 63</th>	Application Screened-J Dual-Hom Screened-S Cryptography Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tecl	on-Proxy Gateway Host Firewall Ned Host Firewall Subnet Firewalls C Key Cryptography ric Key Cryptography. st Cryptosystems. Network Network Ckets Layer	44 45 45 46 47 47 48 50 52 53 56 56 56 57 63
Screened-Host Firewall 45 Dual-Homed Host Firewall 45 Screened-Subnet Firewalls 46 Cryptography 47 Symmetric Key Cryptography 47 Asymmetric Key Cryptography 47 Asymmetric Key Cryptography 48 Digital Signatures 50 Attacks Against Cryptosystems 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary 56 Summary 56 Summary 56 Screenes 63 Chapter 3 Industrial Automation and Control System Culture versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 70 Comparisons from a Standards Perspective <th>Screened-J Dual-Hom Screened-S Cryptography Symmetric Asymmetri Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems</th> <th>Host Firewall</th> <th> 45 45 46 47 47 48 50 52 53 56 56 56 57 63</th>	Screened-J Dual-Hom Screened-S Cryptography Symmetric Asymmetri Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	Host Firewall	45 45 46 47 47 48 50 52 53 56 56 56 57 63
Dual-Homed Host Firewall 45 Screened-Subnet Firewalls 46 Cryptography 47 Symmetric Key Cryptography 47 Asymmetric Key Cryptography 48 Digital Signatures 50 Attacks Against Cryptosystems 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 65 versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements. 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 70 Comparisons from a Standards Perspective 76 Summary 79 Review Questions for Chapter 3 80 <th>Dual-Horr Screened-S Cryptography Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems</th> <th>ned Host Firewall Subnet Firewalls c Key Cryptography ric Key Cryptography matures st Cryptosystems e Network ckets Layer ons for Chapter 2</th> <th> 45 46 47 47 48 50 52 53 56 56 56 57 63</th>	Dual-Horr Screened-S Cryptography Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	ned Host Firewall Subnet Firewalls c Key Cryptography ric Key Cryptography matures st Cryptosystems e Network ckets Layer ons for Chapter 2	45 46 47 47 48 50 52 53 56 56 56 57 63
Screened-Subnet Firewalls 46 Cryptography. 47 Symmetric Key Cryptography. 47 Asymmetric Key Cryptography. 48 Digital Signatures. 50 Attacks Against Cryptosystems. 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary. 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 55 Differences in Culture, Philosophy, and Requirements. 65 Considerations in Adapting IT Security Methods to 70 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 70 Comparisons from a Standards Perspective 76 Summary. 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evo	Screened-5 Cryptography Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tecl	Subnet Firewalls	46 47 47 48 50 52 53 56 56 56 57 63
Cryptography 47 Symmetric Key Cryptography 47 Asymmetric Key Cryptography 48 Digital Signatures 50 Attacks Against Cryptosystems 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary 56 Summary 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 65 Versus IT Paradigms 65 Considerations in Adapting IT Security Methods to 10 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 70 Threats 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting 85 IAC Systems 85 Important Technological Trends 85	Cryptography Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	c Key Cryptography ric Key Cryptography. matures. st Cryptosystems. Network ckets Layer ons for Chapter 2	47 47 48 50 52 53 56 56 56 57 63
Symmetric Key Cryptography. 47 Asymmetric Key Cryptography. 48 Digital Signatures. 50 Attacks Against Cryptosystems. 52 Virtual Private Network 53 IPsec. 56 Secure Sockets Layer 56 Summary. 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 65 Versus IT Paradigms 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 74 Comparisons from a Standards Perspective 76 Summary. 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85	Symmetric Asymmetric Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	c Key Cryptography ric Key Cryptography gnatures st Cryptosystems Network ckets Layer ons for Chapter 2	47 48 50 52 53 56 56 56 57 63
Asymmetric Key Cryptography. 48 Digital Signatures. 50 Attacks Against Cryptosystems. 52 Virtual Private Network 53 IPsec. 56 Secure Sockets Layer 56 Secure Sockets Layer 56 Summary. 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 65 Versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 70 Comparisons from a Standards Perspective 76 Summary. 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems.	Asymmeti Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tecl	ric Key Cryptography. gnatures. st Cryptosystems. Network. ckets Layer	48 50 52 53 56 56 56 57 63
Digital Signatures. 50 Attacks Against Cryptosystems. 52 Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary. 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 65 Versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Digital Sig Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	natures st Cryptosystems Network ckets Layer ons for Chapter 2	50 52 53 56 56 56 57 63
Attacks Against Cryptosystems. 52 Virtual Private Network 53 IPsec 53 IPsec 56 Secure Sockets Layer 56 Summary. 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements. 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems. 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 76 Summary. 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Attacks Agains Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tecl	st Cryptosystems. Network Ekets Layer	52 53 56 56 56 57 63
Virtual Private Network 53 IPsec 56 Secure Sockets Layer 56 Summary 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements. 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems. 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 70 Comparisons from a Standards Perspective 76 Summary 79 Review Questions for Chapter 3 80 References 80 References 81 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Energy	Virtual Private IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tech	Network	53 56 56 56 57 63
IPsec 56 Secure Sockets Layer 56 Secure Sockets Layer 56 Summary 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 65 versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 76 Summary 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	IPsec Secure Soc Summary Review Questi References Chapter 3 Industrial Autoversus IT Paradigms Differences in 0 Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	ckets Layer	56 56 56 57 63
Secure Sockets Layer 56 Summary 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 74 Comparisons from a Standards Perspective 76 Summary 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Ener	Secure Soc Summary Review Questi References Chapter 3 Industrial Auto versus IT Paradigms Differences in Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tecl	ons for Chapter 2	56 56 57 63
Summary 56 Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Chapter 3 Industrial Autoversus IT Paradigms Differences in Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	ons for Chapter 2	56 57 63
Review Questions for Chapter 2 57 References 63 Chapter 3 Industrial Automation and Control System Culture 65 versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 70 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 76 Summary 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Chapter 3 Industrial Autoversus IT Paradigms Differences in Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems	ons for Chapter 2	63
Chapter 3 Industrial Automation and Control System Culture 65 Versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 70 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 76 Comparisons from a Standards Perspective 76 Summary 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Chapter 3 Industrial Autoversus IT Paradigms Differences in Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industri Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems		63
Chapter 3 Industrial Automation and Control System Culture 65 versus IT Paradigms 65 Differences in Culture, Philosophy, and Requirements 65 Considerations in Adapting IT Security Methods to 65 Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 76 Summary. 79 Review Questions for A Standards Perspective 76 Summary. 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Chapter 3 Industrial Autoversus IT Paradigms Differences in Considerations Industrial Auto Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tecl	• • • • • • • • • • • • • • • • • • • •	
Industrial Automation and Control Systems 70 Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 76 Comparisons from a Standards Perspective 76 Summary 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Industrial Auto Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tecl	omation and Control System Culture Culture, Philosophy, and Requirements	65
Threats 71 Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 76 Summary 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Threats Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tech	omation and Control Systems	70
Sensitivity of Industrial Automation and Control Systems 72 IT and Industrial Automation and Control Systems 76 Comparisons from a Standards Perspective 76 Summary 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Sensitivity to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tech	· · · · · · · · · · · · · · · · · · ·	71
to Upgrades and Modifications	to Upgrad IT and Industr Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tech	of Industrial Automation and Control Systems	
IT and Industrial Automation and Control Systems Comparisons from a Standards Perspective	IT and Industry Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tech	es and Modifications	72
Comparisons from a Standards Perspective 76 Summary 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Comparisons f Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tech	ial Automation and Control Systems	
Summary 79 Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Summary Review Questi References Chapter 4 The Continuin IAC Systems Important Tech	rom a Standards Perspective	76
Review Questions for Chapter 3 80 References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Review Questi References Chapter 4 The Continuin IAC Systems Important Tech		79
References 84 Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	References Chapter 4 The Continuin IAC Systems	ons for Chapter 3	80
Chapter 4 The Continuing Technological Evolution Affecting IAC Systems 85 Important Technological Trends 85 Home Area Networks 86 Energy Storage 86	Chapter 4 The Continuin IAC Systems Important Tech		84
IAC Systems	Important Tecl		05
Home Area Networks	important feel	g Technological Evolution Affecting	05
Energy Storage		g Technological Evolution Affecting	00
$\frac{1}{2}$	Fnorm St	nological Trends	00 86
Analytics	Analytics	nological Trends	00 86
Cloud Computing 87	Cloud Cor	g Technological Evolution Affecting hnological Trends a Networks orage	00
Privacy 80	Privacy	nological Trends	
Social Networks 91	Social Net	nological Trends	89
	Mobile Te	nological Trends	

	Interoperability	
	The Smart Grid and Technological Trends	93
	The Bulk Generation Domain	
	The Transmission Domain	
	The Distribution Domain	
	The Operations Domain	
	The Service Provider Domain	
	The Markets Domain	
	The Customer Domain	
	Advanced Metering Infrastructure	
	Energy Storage and Management of Stored Energy	101
	Smart Grid Protocols	103
	Mapping of Emerging Technology Issues onto an	
	Example Automation System – The Smart Grid	105
	Summary	107
	Review Ouestions for Chapter 4	
	References	
Chapter 5	Risk Management for Industrial Automation and	

Control Sy	stems	115
·	Risk Management	115
	ANSI/ISA-62443-2-1 (99.02.01)-2009 Cyber Security	
	Management System	117
	Risk Analysis	118
	Addressing Risk	119
	Monitoring and Improving the CSMS	121
	NIST SP 800-39 Integrated Enterprise Risk Management	122
	NIST SP 800-37 Risk Management Framework	127
	Threats	128
	The Insider Threat	128
	Relevant IACS External Threats	128
	Summary	136
	Review Questions	136
	References	144
Chapter 6	IAC Systems Security Methodologies and Approaches Automation and Control System Security Standards	147
	and Guidelines	147
	NIST Special Publication 800-53, Revision 4, Recommended	
	Security Controls for Federal Information Systems	148
	Minimum Assurance Requirements – Low-Impact Systems	154
	Minimum Assurance Requirements – Moderate-Impact	
	Systems	155
	Minimum Assurance Requirements – High-Impact Systems .	156

	NIST Special Publication 800-82, Guide to Industrial	
	Control Systems Security	158
	Network Segmentation and Segregation	159
	ICS Security Controls.	161
	NIST 800-53 Control Families	164
	Appendix G – ICS Overlay	166
	ANSI/ISA-62443-1-1 (99.01.01)-2007, Security Technologies	
	for Industrial Automation and Control Systems	174
	Authentication and Authorization	175
	Filtering/Blocking/Access Control	176
	Encryption Technologies Data Validation	177
	Management, Audit, Measurement, Monitoring,	
	and Detection	178
	Industrial Automation and Control Systems	
	Computer Software	179
	Physical Security Controls	179
	Personnel Security Controls	180
	North American Electric Reliability Corporation,	
	Critical Infrastructure Protection Cyber Security Standards	180
	Department of Homeland Security, Catalog of Control	
	Systems Security: Recommendations for Standards Developers	192
	AMI System Security Requirements	194
	Identification (FID).	196
	Consolidation of Best Practices Controls for Industrial	
	Automation and Control Systems	197
	Summary	203
	Review Questions for Chapter 6	203
	References	215
Chapter 7	Industrial Automation and Control System Security Training	217
	Background	217
	Training Sources and Approaches	218
	Idaho National Laboratory	219
	Sandia National Laboratories	221
	International Society of Automation	221
	U.S. Computer Emergency Readiness Team	225
	SANS	227
	National Initiative for Cybersecurity Education	227
	National Security Agency and the Department of	
	Homeland Security National Centers of Academic Excellence.	229
	Training Support Guidelines	230
	NIST Special Publication 800-50	230
	NIST Special Publication 800-16	232
	Common Training Subjects	238
	Summary	239

	Review Questions for Chapter 7.	239		
	References			
Chanter 0	Industrial Automation and Control System Tranda			
Chapter 8	Industrial Automation and Control System Trends,	245		
Approache	Automation and Control System Trands	245		
	Popotration Testing of Industrial Automation and			
	Control Systems	250		
	Formal Methods Used to Quantify and Standardize			
	Important Concepts and Applications	252		
	ISCM Strateov	252		
	The Smart Grid Maturity Model (SGMM)	259		
	Automation Maturity Model	268		
	Future Smart Grid Issues and Automation Security Issues	269		
	Smart Grid Electromagnetic Radiation Issues	269		
	NIST 7628	271		
	Summary	273		
	Review Questions for Chapter 8	274		
	References	280		
Chapter 9	Emerging Approaches to Industrial Automation and			
Control Sy	stem Security			
	Internet of Things	281		
	Open Platform Communications Unified Architecture			
	Industry 4.0			
	Security and Privacy	285		
	OWASP IoT Security Categories			
	Big Data Analytics and the Industrial Internet of Things	289		
	Industrial Internet of Things			
	The NIST Cyber-Physical Systems (CPS) Framework	296		
	CPS and Cybersecurity	303		
	Critical Infrastructure Security			
	Framework Fundamentals	309		
	Framework Feedback	315		
	Software-Defined Elements.			
	Summary			
	Review Questions for Chapter 9.			
	References			
Appondix /	A Roview Questions and Answers	333		
Appendix E	3 ICS Supplemental Guidance for NIST SP 800-53			
Security Co	ontrols	409		
-				
Glossary and Acronyms				

Bibliography	 563
Index	