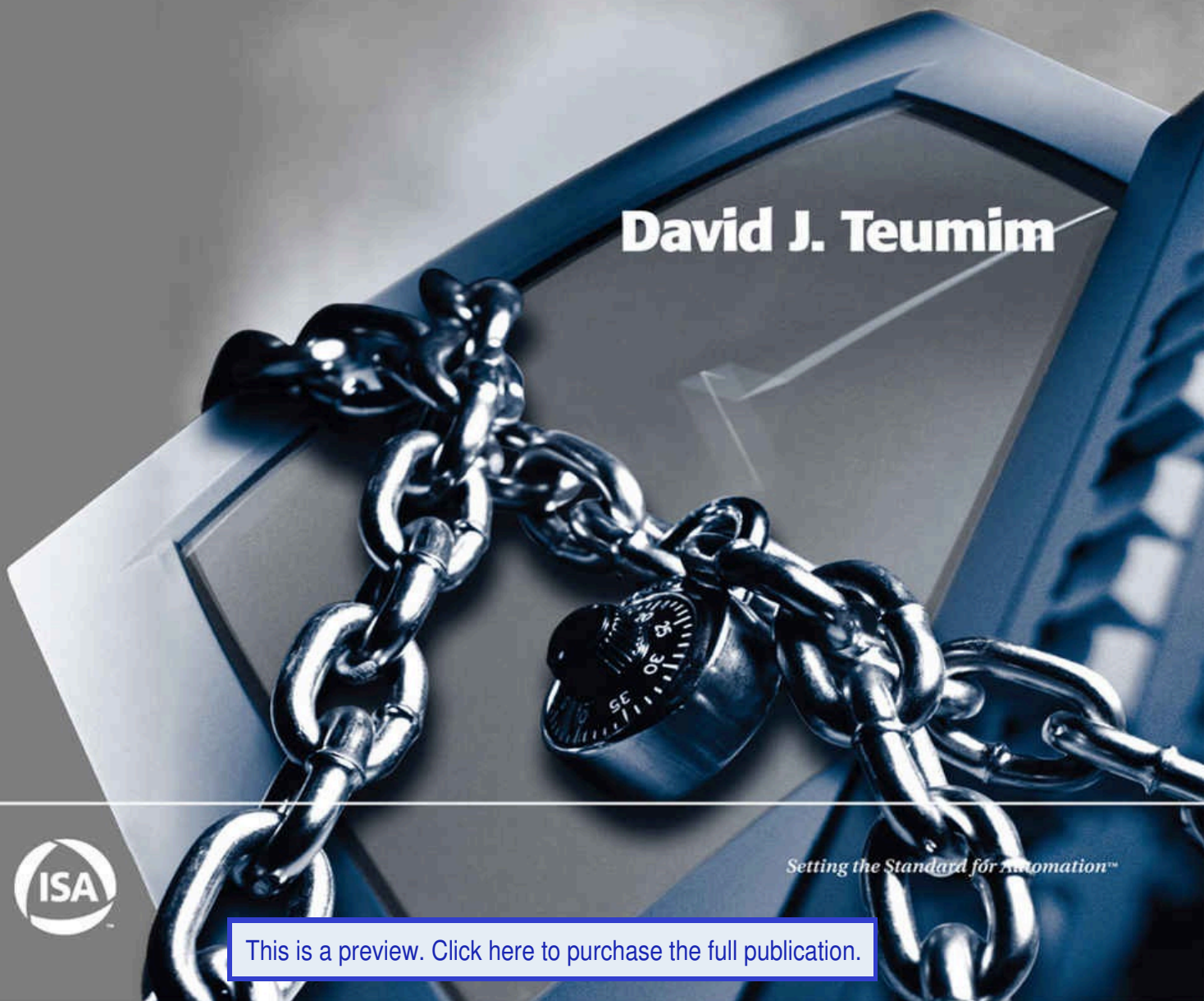
Industrial Network Security

2nd Edition



David J. Teumim

ISA

Setting the Standard for Automation™

Industrial Network Security

Second Edition

By David J. Teumim

ISA—The International Society of Automation

Printed in the United States of America.

10 9 8 7 6 5 4 3 2

ISBN 978-1-936007-07-3

ISA

67 Alexander Drive

P.O. Box 12277

Research Triangle Park, NC 27709

www.isa.org

Library of Congress Cataloging-in-Publication Data in process

Notice

professional judgment in using any of the information presented in a particular application.

Additionally, neither the author nor the publisher have 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 endorse 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 make any representation regarding the availability of any referenced commercial product at any time. The manufacturer's instructions on use of any commercial product must be followed at all times, even if in conflict with the information in this publication.

Acknowledgments

My appreciation is expressed for the people who helped and inspired me to write the second edition of this book.

Once again, my special thanks go to my ISA editor, Susan Colwell.

John Clem, from Sandia National Laboratories, contributed content on Red Teaming for the new Chapter 9, New Topics in Industrial Network Security.

My good friend from college, Andy Hagel, provided content and review for Chapter 3, COTS and Connectivity.

As with the first edition, Tom Good from DuPont and Dave Mills of Procter & Gamble provided content for Chapter 10.

Table of Contents

Preface

Chapter 1.0 Industrial Network Security

1.1 What Are Industrial Networks?

1.2 What Is Industrial Network Security?

1.3 The Big Picture: Critical Infrastructure Protection

1.4 The Challenge: “Open and Secure”

1.5 Who’s Working on What?

1.6 Federal Regulatory Authority

References

Chapter 2.0 A Security Backgrounder

2.1 Physical, Cyber, and Personnel Security

2.2 Risk Assessment and IT Cybersecurity

2.3 Risk Assessment for the Plant

2.4 Who’s Responsible for Industrial Network Security?

2.5 Tips for Making the Business Case to Upper Management

2.6 Making the Business Case with Data

References

Chapter 3.0 COTS and Connectivity

3.1 Use of COTS and Open Systems

3.2 Connectivity

3.3 What You Get that You Didn’t Bargain For

References

Chapter 4.0 Cybersecurity in a Nutshell

4.1 Security Is a Process

4.2 Basic Principles and Definitions

4.3 Basic Principles: Identification, Authentication, and Authorization

4.4 More Cyber Attack Case Histories

4.5 Risk Assessment and Risk Management Revisited

4.6 Cyber Threats
4.7 Vulnerabilities
4.8 A Common COTS Vulnerability: The Buffer Overflow
4.9 Attacker Tools and Techniques
4.10 Anatomy of the Slammer Worm
4.11 Who's Guarding Whom?
References

Chapter 5.0 Countermeasures

5.1 Balancing the Risk Equation with Countermeasures
5.2 The Effect of Countermeasure Use
5.3 Creating an Industrial Network Cyber Defense

Chapter 6.0 Cyberdefense Part I — Design and Planning

6.1 Defense in Layers
6.2 Access Control
6.3 Principle of Least Privilege
6.4 Network Separation
References

Chapter 7.0 Cyberdefense Part II — Technology

7.1 Guidance from ISA99 TR1
7.2 Firewalls and Boundary Protection
7.3 Intrusion Detection
7.4 Virus Control
7.5 Encryption Technologies
7.6 Virtual Private Networks (VPNs)
7.7 Authentication and Authorization Technologies
References

Chapter 8.0 Cyberdefense Part III — People, Policies, and Security Assurance

8.1 Management Actions and Responsibility
8.2 Writing Effective Security Documentation
8.3 Awareness and Training
8.4 Industrial Network Security Assurance Program: Security Checklists

8.5 Security Assurance: Audits

8.6 Adding in Physical Security

8.7 Adding in Personnel Security

References

Chapter 9.0 New Topics in Industrial Network Security

9.1 Red Teaming: Test Yourself Before Adversaries Test You

9.2 Different Types to Answer Different Questions

9.3 Red Teaming Industrial Networks – Caution, It's Not the Same!

9.4 System Security Demands Both Physical Security and Cybersecurity

9.5 The Transportation Connection: Passenger Rail and Cybersecurity

References

Chapter 10.0 Defending Industrial Networks—Case Histories

10.1 A Large Chemical Company

10.2 Another Company's Story—Procter & Gamble

Appendix A – Acronyms

About the Author

Preface

So much has happened since the first edition of *Industrial Network Security* was published in 1995. This area has gone "mainstream" in terms of public awareness of the importance of Industrial Networks to our critical infrastructure and the threat to them from hackers, cyberspies, and cyberterrorists.

For instance, the story "America's Growing Risk: Cyber Attack" is featured on the cover of the April 2009 *Popular Mechanics*. And one of the lead stories on the front page of the 8 April 2009 edition of *The Wall Street Journal* was "Electricity Grid in U.S. Penetrated By Spies." The story talked about how foreign powers had mapped the U.S. electrical grid and left behind some rogue programs that could be activated remotely to disrupt the grid.

The "Big R," Regulation, has reared its head in the electric power industry. The NERC-CIP control system cybersecurity standards for electric power generation and transmission entities are now mandated by the U.S. government.

Commercial-off-the-shelf (COTS) hardware and software, as described in Chapter 3, continues its move into Industrial Networks as legacy equipment is phased out. And other sectors, such as passenger rail, described through the writer's eyes in the new Chapter 9, are coming up to speed on Industrial Network Security as COTS become commonplace in that sector control systems.

Consistent with the first edition, an effort has been made to keep this book introductory and easy-to-read. As with the first edition, this edition is intended for the technical layman, manager, or automation engineer without a cybersecurity background. New cyber incidents and updated information have been added to the chapters without changing the original format.

1.0

Industrial Network Security

1.1 What Are Industrial Networks?

To define industrial network security, one first has to define industrial networks. For the purposes of this book, industrial networks are the instrumentation, control, and automation networks that exist within three industrial domains:

- *Chemical Processing* – The industrial networks in this domain are control systems that operate equipment in chemical plants, refineries, and other industries that involve continuous and batch processing, such as food and beverage, pharmaceutical, pulp and paper, and so on. Using terms from ANSI/ISA-84.00.01-2004 Part 1[6], industrial networks include the Basic Process Control System (BPCS) and the Safety Instrumented Systems (SIS) that provide safety backup.

- *Utilities* – These industrial networks serve distribution systems spread out over large geographic areas to provide essential services, such as water, wastewater, electric power, and natural gas, to the public and industry. Utility grids are usually monitored and controlled by Supervisory Control And Data Acquisition (SCADA) systems.

- *Discrete Manufacturing* – Industrial networks that serve plants that fabricate discrete objects ranging from autos to zippers.

The term Industrial Automation and Control Systems (IACS) is used by ISA in its committee name and in the recently issued standards and technical report series from the ISA99 Industrial Automation and Control Systems Security standards and technical committee (also, simply ISA99). This term is closely allied with the term *Industrial Networks*.

The standard, ANSI/ISA-99.00.01-2007-Security for *Industrial Automation and Control Systems, Part 1*[1], defines the term Industrial Automation and Control Systems to include "control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e., electricity, gas, and water), pipelines and petroleum production and distribution facilities, and other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets." This standard will be referred to as "ISA-99 Part 1" in the book.

The technical report ANSI/ISA-TR99.00.01-2007 *Security Technologies for Industrial Automation and Control Systems* [4] succeeds the 2004 version of the document referenced in the first edition of this book. This report will be referred to as "ISA-99 TR1." Note: At the time of this writing, Part 2 of the ISA-99 standard has just been approved. Part 2 is