Contents

Authors ix

Chapter 1 Introduction 1

Where This Book Starts and Stops 2

Our Audience 3

What Is an Industrial Control System? 6

Is Industrial Control System Security Different Than Regular IT Security? 8

Where Are ICS Used? 9

ICS Compared to Safety Instrumented Systems 14

What Has Changed in ICS That Raises New Concerns? 15

Naming, Functionality, and Components of Typical ICS/SCADA Systems 18

- Supervisory Control and Data Acquisition (SCADA) 19
- Remote Terminal Unit (RTU) 20
- Distributed Control System (DCS) 20
- Programmable Logic Controllers (PLCs) 20
- Human–Machine Interface (HMI) 21

Analogue versus IP Industrial Automation 22

Convergence 101: It Is Not Just Process Data Crowding onto IP 25

Convergence by Another Name 27

Taxonomy of Convergence 28

- Triple-Play Convergence 29
- Transparent Convergence 30
- Blue-Sky Convergence 31

The Business Drivers of IP Convergence 33

Cost Drivers 33
Competitive Drivers 36
Regulatory Drivers 37
The Conflicting Priorities of Convergence 38
ICS Security Architecture and Convergence 40
The Discussions to Follow in This Book 43
Endnotes 44

CHAPTER 2 THREATS TO ICS 45
Threats to ICS: How Security Requirements Are Different from ICS to IT 46
Threat Treatment in ICS and IT 53
Threats to ICS 54
Threat-To and Threat-From 57
The Most Serious Threat to ICS 59
Collateral Damage 60
Whatever Happened to the Old-Fashioned E-Mail Virus? 60
Money, Money, Money 62
The Fatally Curious, Naïve, and Gullible 62
Hi-Jacking Malware 64
No Room for Amateurs 68
Taxonomy of Hi-Jacking Malware and Botnets 68
Hi-Jacking Malware 101 69
Characteristics of a Bot (Zombie/Drone) 69
The Reproductive Cycle of Modern Malware 72
A Socks 4/Sock 5/HTTP Connect Proxy 76
SMTP Spam Engines 78
Porn Dialers 78
Conclusions on ICS Threats 79
Endnotes 80

CHAPTER 3 ICS VULNERABILITIES 81
ICS Vulnerability versus IT Vulnerabilities 82
Availability, Integrity, and Confidentiality 83
Purdue Enterprise Reference Architecture 89
PERA Levels 89
Levels 5 and 4: Enterprise Systems 89
Level 3: Operations Management 90
Level 2: Supervisory Control 90
Level 1: Local or Basic Control 91
Level 0: Process 91
An Ironic Comment on PERA 92
Data at Rest, Data in Use, Data in Motion 93
Distinguishing Business, Operational, and Technical Features of ICS 95

ICS Vulnerabilities 98
Management Vulnerabilities 99
Operational Vulnerabilities 100
Technical Vulnerabilities 105
Functional Vulnerabilities 106
ICS Technical Vulnerability Class Breakdown 111
Technical Vectors of Attack 113
IT Devices on the ICS Network 114
Interdependency with IT 115
Green Network Stacks 116
Protocol Inertia 116
Limited Processing Power and Memory Size 118
Storms/DOS of Various Forms 119
Fuzzing 120
MITM and Packet Injection 121
Summary 123
Endnotes 123

CHAPTER 4 RISK ASSESSMENT TECHNIQUES 125
Introduction 125
Contemporary ICS Security Analysis Techniques 126
North American Electricity Reliability Council (NERC) 126
National Institute of Standards and Technology (NIST) 128
Department of Homeland Security (DHS) ICS Risk Assessment Processes 129
INL National SCADA Test Bed Program (NSTB): Control System Security Assessment 130
INL Vulnerability Assessment Methodology 131
INL Metrics-Based Reporting for Risk Assessment 133
Ideal-Based Risk Assessment and Metrics 134
CCSP Cyber Security Evaluation Tool (CSET) 135
U.S. Department of Energy: Electricity Sector Cyber Security Risk Management Process Guideline 136
Evolving Risk Assessment Processes 137
Consequence Matrices 138
Safety Integrity Levels and Security Assurance Levels 140
Security Assurance Level 141
SAL-Based Assessments 144
SAL Workflow 145
Future of SAL 147
Overall Equipment Effectiveness (Assessment) 148
Security OEE 149
Putting OEE Metrics Together 152
Network-Centric Assessment 153
Network-Centric Compromise Indicators 155
Assessing Threat Agents, Force, and Velocity 155

Other Network Infrastructure That Can Be Used for Network-Centric Analysis and ICS Security 157
Network-Centric Assessment Caveats 159
Conclusion 160
Endnotes 161

CHAPTER 5 WHAT IS NEXT IN ICS SECURITY? 163
The Internet of Things 163
IPv6 164
There Is a New Internet Protocol in Town 164
In Brief: What Is IPv6? 164
What Does IPv6 Mean for My Business in General? 165
What Does the Switch to IPv6 Mean for the Security of My ICS Network? 166
What Will the Move to IPv6 Require, for IT and ICS? 167
ICS v6 Test Lab Designs 168
Stage 1 Test Environment: Introduce IPv6 169
Stage 2 Test Environment: Sense IPv6 170
Stage 3 Test Environment: Dual-Stack Testing 170
Stage 4 Test Environment 171
Stage 5 Test Environment 172
Dual Stacking 174
ICS and Cellular Wireless 176
Private Architecture and Cellular Wireless 176
v6 Security Testing Methodology for ICS Devices 180
IPv6 and ICS Sensors 182
Pros and Cons of IPv6 and Low-Power (Wireless) Devices 183
A Few Years Yet… 185
Endnotes 185

INDEX 187