

Contents

	Foreword	xv
	Preface	xix
	Authors	xxiii
	Acknowledgments	xxv
Chapter 1	What Is the Smart Grid, and Why Should We Care about Security?	1
	1.1 Definitions: The Traditional Power Grid	1
	1.2 Definitions: What's a Smart Grid?	3
	1.3 Why Do We Need a Smarter Grid?	7
	1.4 Smart Grid Risks	9
	1.5 Smart Grid Risks versus Benefits	12
	Endnotes	14
Chapter 2	The Smart Grid Evolution: Smart Grid Standards, Laws, and Industry Guidance	17
	2.1 Introduction	17
	2.2 Regulations, Smart Grid, and the Bulk Electric System	20
	2.3 Privacy Information Impacts on Smart Grid	24
	2.4 Security Standards	27
	2.5 Smart Grid Security Strategy	31
	2.6 Smart Grid Impacts	38
	2.7 Applying Security Control Frameworks to Smart Grid	41
	2.8 Managing the Overall Risk to Smart Grid	46
	Endnotes	49

Chapter 3	Smart Metering: The First Security Challenge	51
3.1	Introduction	51
3.2	The Cost of Smart Metering	52
3.3	Smart Metering Programs	53
3.3.1	The Smart Meter Architecture	57
3.3.2	In-Home Display	58
3.3.3	Smart Meters	59
3.3.4	Neighborhood Area Network	60
3.3.5	Smart Meter Collectors	61
3.3.6	Wide Area Network (WAN)	62
3.3.7	Utility Demilitarized Zone	64
3.3.8	Head End System	64
3.4	Smart Meter Authentication	64
3.5	Smart Metering Security	67
3.6	Smart Meter Vendor Management	67
3.7	Smart Meter Security Management	70
3.7.1	AMI Vulnerabilities	72
3.7.2	AMI Impacts	74
	Endnotes	76
Chapter 4	Home Area Networking: Giving Consumers Control or Opening a Pandora's Box?	79
4.1	Introduction	79
4.2	Elements of the Home Area Network	81
4.2.1	Energy Services Interface	83
4.2.2	Programmable Communicating Thermostat (PCT)	84
4.2.3	In-Home Display (IHD) and Energy Management System (EMS)	85
4.2.4	Load Control and Smart Appliance	86
4.2.5	HAN Nonelectric Meter	87
4.2.6	Plug-In Electric Vehicle (PEV) and Electric Vehicle Supply Equipment (EVSE)	87
4.2.7	Mobile HAN Devices	89
4.2.8	Other Devices	90

4.3	HAN Communications	91
4.4	HAN Commissioning, Registration, and Enrollment	92
4.5	Defense-in-Depth and Other Security Solutions	94
	Endnotes	96
Chapter 5	Distribution Automation: Moving from Legacy to Secure	99
5.1	Introduction	99
5.2	What Is the Distribution System?	100
5.3	Distribution System Architecture	102
5.3.1	Utility Field Sensors (Sensors)	103
5.3.2	Utility Distribution and Feeder Meters	103
5.3.3	Utility Field Controllers	104
5.3.4	Local Access Network (LAN)	104
5.3.5	Sensor/Meter Aggregator	105
5.3.6	Wide Area Network (WAN)	105
5.3.7	Data Center Access	106
5.3.8	Sensor Head-End	106
5.3.9	Meter Head-End	107
5.3.10	Distribution SCADA MTU	107
5.3.11	Back-Office Computational Platforms	107
5.3.12	Traditional Back-Office Applications	108
5.4	Definition of Distribution Automation	108
5.5	How Does Distribution Automation Work?	114
5.6	Distribution System Costs	118
5.7	What Is the Smart Grid Function of Distribution Automation?	118
5.8	The Importance of the Distribution System and Its Security Challenges	120
5.9	Securing the Distribution System	121
5.10	Distribution Management Systems	122
5.11	Standards, Inoperability, and Cyber Security	123
	Endnotes	126

Chapter 6	Transmission Automation: Can Utilities Work Together Securely?	129
6.1	Introduction	129
6.2	Transmission Infrastructure Costs	130
6.3	Transmission Infrastructure Functionality	131
6.4	Transmission Technology	135
6.4.1	Energy Management System	138
6.4.2	Map Board	138
6.4.3	Automatic Generation Control (AGC)	139
6.4.4	Supervisory Control	139
6.4.5	Contingency Reserve Management	139
6.4.6	Interchange Scheduling	140
6.4.7	SCADA Master Terminal Unit	141
6.4.8	SCADA Front-End Processor	141
6.5	Transmission Substations	142
6.5.1	Synchrophasors as IEDs	143
6.5.2	Relays as IEDs	144
6.5.3	Programmable Logic Controllers as IEDs	145
6.5.4	RTUs as IEDs	145
6.6	Smart Transmission Cyber Security	145
6.6.1	Control Center Cyber Security	147
6.6.2	Transmission Substation Cyber Security	151
6.7	Strategies for Securing the Transmission System	152
	Endnotes	154
Chapter 7	Distributed Generation and Micro-Grids: Can Distributed Systems Work Together?	157
7.1	Introduction	157
7.2	Major Generation Resources	158
7.3	Major Generation Costs	158
7.3.1	Nuclear Power	161
7.3.2	Coal Power	162
7.3.3	Gas Power	163
7.3.4	Hydroelectric Generation	163
7.3.5	Distributed Energy Resources (DERs)	164

7.4	Distributed Energy Resource Costs	165
7.4.1	Energy Generation Systems	165
7.4.2	Energy Storage Systems	167
7.4.3	DER Programs	169
7.5	DER Cyber Security	170
7.6	Micro-Grids	171
7.6.1	Micro-Grid Functions and Smart Grid Interaction	172
7.6.2	Cyber Security for Micro-Grids	173
7.6.3	Future of Micro-Grids	175
7.7	Distributed Control System	175
7.8	Smart Grid and Distributed Generation	176
7.9	Cyber Security and Distributed Generation	177
	Endnotes	180
Chapter 8	Operations and Outsourcing	185
8.1	Introduction	185
8.2	Design	186
8.3	Engineering	186
8.4	Communications	186
8.5	Information Technology (IT)	187
8.6	Planning	187
8.7	Grid Operations	189
8.8	Plant Operations	191
8.9	Substation Operations	192
8.10	Accounting	194
8.11	Marketing	194
8.12	Maintenance	195
8.13	Substation Maintenance	195
8.14	Generation Maintenance	196
8.15	Construction	197
8.16	Metering Support	197
8.17	Smart Grid Operations	199
8.17.1	Outsourcing	200

	8.17.2	Cyber Security Incident Response and Outsourcing	202
	8.17.3	Cyber Security Controls	205
		Endnotes	206
Chapter 9		Plug-In Electric Vehicles and Energy Storage: Now the Fun Really Begins	207
	9.1	Introduction	207
	9.2	Storage Technologies	208
	9.3	Measurement and Coordination	210
	9.4	What Makes Plug-In Electric Vehicles Unique?	211
	9.5	Plug-In Vehicle to Grid Logistics	212
	9.6	Grid to Plug-In Vehicle Logistics	214
	9.7	Energy Storage and Cyber Security	216
	9.8	The Future of Energy Storage	218
		Endnotes	218
Chapter 10		What about the Consumer?: Securing Relationships between the Utilities and Their Customers	221
	10.1	Introduction	221
	10.2	Electric Charging Stations	221
	10.3	Home Area Networks	222
	10.4	Distributed Generation	223
	10.5	Demand Response and the Consumer	223
	10.6	Consumer Health Risks of Smart Grid	224
	10.7	Consumer Protections	224
	10.8	Utility Protection from the Consumer	226
	10.9	Third-Party Service Providers	228
	10.10	Protecting Consumers from Themselves	232
		Endnotes	233
Chapter 11		Identifying and Recovering the Grid from a Cyber-Disaster	235
	11.1	Introduction	235
	11.2	Malicious Threats	236
	11.2.1	Malicious Threats in Control Systems	243

11.3	Nonmalicious Threats	246
11.4	Incident Identification	248
11.5	Incident Containment	248
11.6	Incident Eradication	250
11.7	Cyber-Disaster	251
11.7.1	Load-Shedding Events	253
11.7.2	Cyber-Disaster Response	254
11.7.3	Cyber-Disaster Recovery	255
	Endnotes	256
Chapter 12	Crystal Ball Time: Will We Have a Secure Grid and What Will It Take?	257
12.1	Introduction	257
12.2	Smart Meter Security	258
12.3	Home Area Networks	259
12.4	Head-End and Meter Data Management	259
12.5	Distribution System Security	261
12.6	Transmission Security and the Bulk Electric System	262
12.7	The Distribution System and NERC CIP	263
12.8	Identity and Key Management	265
12.9	Differential Power Analysis and Other Side Channel Attacks	267
12.10	Energy Theft and Market Manipulation	268
12.11	Privacy	269
12.12	Will the Smart Grid Be Secure?	269
	Endnotes	271
	Bibliography	273
	Index	281