Contents

Foreword xiii

Introduction xix

Chapter 1. Components of an Industrial Control System 1

1.1. Introduction 1
1.1.1. Definition: automated and cyber-physical systems 1
1.1.2. Definition: Information System (IS) 1
1.1.3. Definition: industrial IS or ICS 2
1.1.4. Definition: IT and OT system 4
1.1.5. Definition: SCADA 4
1.1.6. Definition: Distributed Control Systems (DCS) 5
1.1.7. Definition: Industrial Internet of Things (IIOT) 5
1.1.8. Different types of ICS 6
1.2. From the birth of the PLC to the SCADA system 6
1.3. Programmable logic controller (PLC) 8
1.4. RTU, master terminal unit and intelligent electronic device 12
1.5. Programmable Automation Controller 13
1.6. Industrial PC 13
1.7. Safety instrumented systems 13
1.8. Human–machine interface (HMI) 15
1.9. Historians 17
1.10. Programming and parameter setting stations 17
1.11. Industrial Internet of Things (IIoT) 18
1.12. Network equipment 19
1.12.1. Switch and hub 19
1.12.2. Router and gateway 20
1.12.3. Firewall 20
1.12.4. IoT gateway 20

1.13. Data processing platform 21
1.14. Lifecycle of an ICS 22

Chapter 2. Architecture and Communication in an Industrial Control System 25

2.1. Network architecture 25
2.1.1. Purdue model and CIM model 26
2.1.2. Architecture of the Industrial Internet of Things 29
2.2. Different types of communication networks 31
2.2.1. Topology 31
2.2.2. Types of networks 33
2.2.3. Virtual private network 34
2.2.4. OSI model 34
2.3. Transport networks 35
2.3.1. Ethernet. 35
2.3.2. Wi-Fi 36
2.3.3. The IEEE 802.15.1 (Bluetooth) standard 36
2.3.4. IEEE 802.15.4 networks 37
2.3.5. LPWAN networks 38
2.3.6. Cellular networks 38
2.4. Internet protocols 39
2.4.1. The Internet protocol 39
2.4.2. Transmission Control Protocol 39
2.4.3. Unified Datagram Protocol (UDP). 42
2.4.4. Address Resolution Protocol (ARP) 42
2.4.5. Internet Control Message Protocol (ICMP) 42
2.4.6. The IPv6 protocol. 43
2.5. Industrial protocols 43
2.5.1. Introduction 43
2.5.2. Modbus 45
2.5.3. Profibus and Profinet. 46
2.5.4. Actuator/sensor interface 47
2.5.5. Highway Addressable Remote Transducer 48
2.5.6. DNP3 and IEC 60870 48
2.5.7. The CAN bus 49
2.5.8. Ethernet/IP and Common Industrial Protocol (CIP) 49
2.5.9. OLE for Process Control (OPC) 51
2.5.10. Other protocols 52
2.6. IoT protocols 52
2.6.1. 6LowPAN 53
2.6.2. Message Queuing Telemetry Transport 53
2.6.3. CoAP 54
2.6.4. Other protocols 54

Chapter 3. IT Security 57

3.1. Security objectives 57
3.1.1. The AIC criteria. 57
3.1.2. The different levels of IT security 61
3.2. Differences between IT and OT systems 64
3.2.1. The functionalities 64
3.2.2. The technology 65
3.2.3. System lifecycle. 66
3.2.4. Security management 67
3.2.5. IT/OT convergence. 68
3.2.6. Summary 68
3.3. Risk components. 70
3.3.1. Asset and impact 70
3.3.2. Threats 71
3.3.3. Attacks 71
3.3.4. Vulnerabilities. 72
3.3.5. Definition of risk 73
3.3.6. Scenarios and impact. 74
3.3.7. Risk measurement 75
3.4. Risk analysis and treatment process 77
3.4.1. Principle 77
3.4.2. Acceptance of risk 79
3.4.3. Risk reduction 79
3.5. Principle of defense in depth. 80
3.6. IT security management 82
3.7. Risk treatment process 85
3.8. Governance and security policy for IT systems. 86
3.8.1. Governance 86
3.8.2. Security policy 87
3.9. Security management of industrial systems 88

Chapter 4. Threats and Attacks to ICS. 91

4.1. General principle of an attack 91
4.2. Sources of threats 95
4.3. Attack vectors 98
4.4. Main categories of malware 99
4.4.1. Virus/worms. 100
4.4.2. Trojan horse 100
4.4.3. Logical bomb 101
4.4.4. Rootkit 101
4.4.5. Spyware 101
4.4.6. Back doors 101

4.4.7. Botnet . . . 102
4.4.8. Ransomware . . . 103
4.5. Attacks on equipment and applications . . . 103
4.5.1. Buffer overflow and integer overflow . . . 103
4.5.2. Attack by brute force . . . 104
4.5.3. Attack via a zero day flaw . . . 105
4.5.4. Side-channel attacks . . . 105
4.5.5. Attacks specific to ICS equipment . . . 106
4.5.6. Attacks on IIoT systems . . . 107
4.6. Site attacks and via websites . . . 108
4.7. Network attacks . . . 109
4.7.1. Man-in-the-middle . . . 109
4.7.2. Denial of service . . . 110
4.7.3. Network and port scanning . . . 111
4.7.4. Replay attack . . . 112
4.8. Physical attacks . . . 112
4.9. Attacks using the human factor . . . 113
4.9.1. Social engineering . . . 113
4.9.2. Internal fraud . . . 114
4.10. History of attacks on ICS . . . 114
4.11. Some statistics . . . 119

Chapter 5. Vulnerabilities of ICS . . . 121

5.1. Introduction . . . 121
5.2. Generic approach to vulnerability research . . . 122
5.3. Attack surface . . . 124
5.4. Vulnerabilities of SCADA industrial systems . . . 126
5.5. Vulnerabilities of IoT industrial systems . . . 128
5.6. Systematic analysis of vulnerabilities . . . 130
5.7. Practical tools to analyze technical vulnerability . . . 136
5.7.1. Databases and information sources . . . 137
5.7.2. Pentest tools . . . 137
5.7.3. Search engines . . . 139

Chapter 6. Standards, Guides and Regulatory Aspects . . . 141

6.1. Introduction . . . 141
6.2. ISO 27000 family . . . 142
6.3. NIST framework and guides . . . 144
6.3.1. NIST Cyber Security Framework . . . 144
6.3.2. The guides . . . 145
6.4. Distribution and production of electrical energy . . . 148
6.4.1. NERC CIP . . . 148

6.4.2. IEC 62351 150
6.4.3. IEEE 1686 151
6.5. Nuclear industry 151
6.5.1. The IAEA technical guide. 151
6.5.2. IEC 62645 152
6.6. Transportation 153
6.6.1. Vehicles 153
6.6.2. Aeronautics 153
6.7. Other standards. 154
6.7.1. National Information Security Standards 154
6.7.2. Operating safety standards 154
6.8. ANSSI’s approach. 155
6.9. Good practices for securing industrial Internet of Things equipment . . 159
6.9.1. Trust base (root of trust) 160
6.9.2. Identity management (endpoint identity) 161
6.9.3. Secure boot 161
6.9.4. Cryptographic services. 161
6.9.5. Secure communications 162
6.9.6. Equipment configuration and management. 162
6.9.7. Activity dashboard and event management by a SIEM. 162
6.10. Legislative and regulatory aspects. 163

Chapter 7. The Approach Proposed by Standard 62443 167

7.1. Presentation. 167
7.2. IACS lifecycle and security stakeholders 169
7.3. Structure of the IEC 62443 standard 170
7.4. General idea of the proposed approach 172
7.5. Basics of the standard. 174
7.5.1. Fundamental requirements 174
7.5.2. Security Levels (SL) 177
7.5.3. Zones and conduits 180
7.5.4. Maturity level 182
7.5.5. Protection level 183
7.6. Risk analysis 184
7.6.1. General approach 185
7.6.2. Detailed risk analysis. 186
7.6.3. Determination of SL-T. 187
7.6.4. Countermeasures 188
7.7. Security management 189
7.8. Assessment of the level of protection 190
7.9. Implementation of the IEC 62443 standard 191

7.9.1. Certification 191
7.9.2. Service providers and integrators 192
7.9.3. IACS Operators 192

Chapter 8. Functional Safety and Cybersecurity 193

8.1. Introduction. 193
8.1.1. Components of operational safety 193
8.1.2. SIS and SIL levels 198
8.2. IEC 61508 standard and its derivatives 200
8.3. Alignment of safety and security 203
8.4. Risk analysis methods used in operational safety 204
8.4.1. Preliminary hazard analysis 204
8.4.2. Failure Mode and Effects Analysis 205
8.4.3. HAZOP. 207
8.4.4. Layer Of Protection Analysis 208
8.4.5. Fault trees and bowtie diagrams 210

Chapter 9. Risk Assessment Methods 213

9.1. Introduction. 213
9.2. General principle of a risk analysis 214
9.2.1. General information 214
9.2.2. Setting the context 217
9.2.3. Risk identification 218
9.2.4. Estimation of the level of risk 219
9.2.5. Risk assessment and treatment 219
9.2.6. Tailor-made approach and ICS 221
9.3. EBIOS method 221
9.3.1. Workshop 1: framing and security base. 222
9.3.2. Workshop 2: sources of risk 226
9.3.3. Workshop 3: study of strategic scenarios 227
9.3.4. Workshop 4: study of operational scenarios 229
9.3.5. Workshop 5: risk treatment 230
9.3.6. Implementation for ICS 233
9.4. Attack trees 234
9.5. Cyber PHA and cyber HAZOP 236
9.5.1. Principle 236
9.5.2. Cyber PHA. 239
9.5.3. Cyber HAZOP 243
9.6. Bowtie cyber diagram. 245
9.7. Risk analysis of IIoT systems 246

Chapter 10. Methods and Tools to Secure ICS 249

10.1. Identification of assets. 249
10.2. Architecture security. 253
10.2.1. Presentation 253
10.2.2. Secure architecture 254
10.2.3. Partitioning into zones 255
10.3. Firewall 257
10.4. Data diode 260
10.5. Intrusion detection system 261
10.5.1. Principle of operation. 261
10.5.2. Detection methods 264
10.5.3. Intrusion detection based on a process model 267
10.6. Security incident and event monitoring. 268
10.7. Secure element 270

Chapter 11. Implementation of the ICS Cybersecurity Management Approach 273

11.1. Introduction 273
11.1.1. Organization of the process 273
11.1.2. Technical, human and organizational aspects 275
11.1.3. Different levels of implementation and maturity. 275
11.2. Simplified process 276
11.3. Detailed approach 277
11.4. Inventory of assets 279
11.4.1. Mapping 279
11.4.2. Documentation management 279
11.5. Risk assessment 280
11.6. Governance and ISMS 281
11.6.1. Governance of the ICS and its enviroment 281
11.6.2. ISMS for ICS 281
11.7. Definition of the security policy and procedures 282
11.8. Securing human aspects. 283
11.9. Physical security 284
11.10. Network security 285
11.11. Securing exchanges by removable media. 285
11.12. Securing machines 285
11.12.1. Securing workstations and servers 285
11.12.2. Securing engineering stations 286
11.12.3. Securing PLCs 286
11.12.4. Securing IIoT equipment 287
11.12.5. Securing network equipment. 287
11.12.6. Antivirus 287

11.13. Data security and configuration 288
11.14. Securing logical accesses 289
11.15. Securing supplier and service provider interactions 290
11.16. Incident detection. 291
11.16.1. Logging and alerts 291
11.16.2. Intrusion detection system 291
11.16.3. Centralization of events (SIEM). 291
11.17. Security monitoring 291
11.17.1. Updating mapping and documentation. 291
11.17.2. Security patch management 291
11.17.3. Audit of the facility 292
11.18. Incident handling 292
11.19. Recovery 293
11.19.1. Backup. 293
11.19.2. Business continuity plan 294
11.20. Cybersecurity and lifecycle 294

Appendix 1 295

Appendix 2 303

Appendix 3 309

Appendix 4 329

Appendix 5 355

Appendix 6 361

List of acronyms and abbreviations 363

References 367

Index 377