# Table des matières

**Préface** . . . . . 1
Jean-Pierre HAUET

**Introduction** . . . . . 7

**Chapitre 1. Composants d'un système de commande industriel** . . 19

1.1. Introduction . . . . . 19
1.2. De la naissance du PLC au système SCADA . . . . . 25
1.3. Automate programmable ou PLC . . . . . 26
1.4. RTU, MTU et IED . . . . . 30
1.5. *Programmable Automation Controller* (PAC) . . . . . 31
1.6. *Industrial PC* . . . . . 31
1.7. Systèmes instrumentés de sécurité (SIS) . . . . . 31
1.8. Interface homme-machine . . . . . 33
1.9. Gestion des historiques . . . . . 34
1.10. Station de programmation et de paramétrage . . . . . 35
1.11. Objets connectés industriels (IIoT) . . . . . 35
1.12. Équipements réseau . . . . . 37
1.13. Plateforme de traitement de données . . . . . 39
1.14. Cycle de vie d'un ICS . . . . . 39

**Chapitre 2. Architecture et communication dans un système de commande industriel** . . . . . 43

2.1. Architecture du réseau . . . . . 43
2.2. Différents types de réseaux de communication . . . . . 49

2.3. Réseaux de transport . . . . . 53
2.4. Protocoles d'Internet . . . . . 57
2.5. Protocoles industriels . . . . . 61
2.6. Protocoles de l'IoT . . . . . 70

**Chapitre 3. Sécurité informatique** . . . . . 73

3.1. Objectifs de sécurité . . . . . 73
3.2. Différences entre les systèmes IT et OT . . . . . 79
3.3. Composantes du risque . . . . . 85
3.4. Démarche d'analyse et de traitement des risques . . . . . 92
3.5. Principe de défense en profondeur . . . . . 95
3.6. Management de la sécurité informatique . . . . . 96
3.7. Processus de traitement des risques . . . . . 100
3.8. Gouvernance et politique de sécurité des systèmes informatiques . . . . 101
3.9. Management de la sécurité des systèmes industriels . . . . . 102

**Chapitre 4. Menaces et attaques des ICS** . . . . . 105

4.1. Principe général d'une attaque . . . . . 105
4.2. Sources de menaces . . . . . 109
4.3. Vecteurs d'attaque . . . . . 112
4.4. Principales catégories de logiciels malveillants . . . . . 113
4.5. Attaques des équipements et des applications . . . . . 117
4.6. Attaques des sites et *via* les sites Web . . . . . 122
4.7. Attaques du réseau . . . . . 122
4.8. Attaques physiques . . . . . 125
4.9. Attaques utilisant le facteur humain . . . . . 126
4.10. Historique des attaques sur les ICS . . . . . 127
4.11. Quelques statistiques . . . . . 132

**Chapitre 5. Vulnérabilités des ICS** . . . . . 135

5.1. Introduction . . . . . 135
5.2. Démarche générique de recherche des vulnérabilités . . . . . 136
5.3. Surface d'attaque . . . . . 138
5.4. Vulnérabilités des systèmes industriels SCADA . . . . . 140
5.5. Vulnérabilités des systèmes industriels IoT . . . . . 142
5.6. Analyse systématique des vulnérabilités . . . . . 143
5.7. Outils pratiques pour analyser la vulnérabilité technique . . . . . 150

**Chapitre 6. Normes, guides et aspects réglementaires** . . . . . 155

6.1. Introduction . . . . . 155
6.2. Famille ISO 27000 . . . . . 156
6.3. *Framework* et guides NIST . . . . . 158
6.4. Distribution et production d'énergie électrique . . . . . 162
6.5. Industrie nucléaire . . . . . 164
6.6. Transports . . . . . 166
6.7. Autres normes . . . . . 167
6.8. Approche de l'ANSSI . . . . . 168
6.9. Bonnes pratiques de sécurisation des équipements IIoT . . . . . 172
6.10. Aspects législatifs et réglementaires . . . . . 176

**Chapitre 7. L'approche proposée par la norme 62443** . . . . . 179

7.1. Présentation . . . . . 179
7.2. Cycle de vie d'un IACS et parties prenantes de la sécurité . . . . . 181
7.3. Structure de la norme IEC 62443 . . . . . 182
7.4. Idée générale de l'approche proposée . . . . . 184
7.5. Notions de base de la norme . . . . . 186
7.6. Analyse des risques . . . . . 196
7.7. Management de la sécurité . . . . . 201
7.8. Évaluation du niveau de protection . . . . . 202
7.9. Mise en œuvre de la norme IEC 62443 . . . . . 203

**Chapitre 8. Sûreté de fonctionnement et cybersécurité** . . . . . 205

8.1. Introduction . . . . . 205
8.2. Norme IEC 61508 et ses dérivées . . . . . 212
8.3. Alignement de la sûreté et de la sécurité . . . . . 214
8.4. Méthodes d'analyse de risque utilisées en sûreté de fonctionnement . . . . . 216

**Chapitre 9. Méthodes d'évaluation des risques** . . . . . 223

9.1. Introduction . . . . . 223
9.2. Principe général d'une analyse de risque . . . . . 224
9.3. Méthode EBIOS . . . . . 231
9.4. Arbres d'attaque . . . . . 243
9.5. Cyber APR et Cyber HAZOP . . . . . 245
9.6. Cyber-diagramme nœud-papillon . . . . . 253
9.7. Analyse des risques des systèmes IIoT . . . . . 256

**Chapitre 10. Méthodes et outils de sécurisation des ICS** . . . . . 257

10.1. Identification des biens . . . . . 257
10.2. Sécurisation de l'architecture . . . . . 261
10.3. Pare-feu . . . . . 265
10.4. *Data-diode* . . . . . 268
10.5. Système de détection d'intrusion . . . . . 269
10.6. *Security Incident and Event Monitoring* (SIEM) . . . . . 276
10.7. *Secure Element* . . . . . 278

**Chapitre 11. Mise en œuvre de la démarche de gestion de la cybersécurité des ICS** . . . . . 281

11.1. Introduction . . . . . 281
11.2. Démarche simplifiée . . . . . 283
11.3. Démarche détaillée . . . . . 285
11.4. Inventaire des biens . . . . . 286
11.5. Évaluation du risque . . . . . 287
11.6. Gouvernance et SMSI . . . . . 288
11.7. Définition de la politique de sécurité et des procédures . . . . . 289
11.8. Sécurisation des aspects humains . . . . . 290
11.9. Sécurisation physique . . . . . 291
11.10. Sécurisation du réseau . . . . . 292
11.11. Sécurisation des échanges par médias amovibles . . . . . 292
11.12. Sécurisation des machines . . . . . 292
11.13. Sécurisation des données et configurations . . . . . 295
11.14. Sécurisation des accès logiques . . . . . 295
11.15. Sécurisation des interactions fournisseurs et prestataires . . . . . 296
11.16. Détection d'incident . . . . . 297
11.17. Surveillance de la sécurité . . . . . 297
11.18. Traitement des incidents . . . . . 298
11.19. Restauration . . . . . 299
11.20. Cybersécurité et cycle de vie . . . . . 300

**Annexe 1. Notions de cryptographie** . . . . . 301

**Annexe 2. *Blockchain* et sécurité de l'IIoT** . . . . . 309

**Annexe 3. Mesures de sécurité du NIST SP 800-82** . . . . . 315

**Annexe 4. Mesures de sécurité de l'ANSSI** . . . . . 327

**Annexe 5. Compléments sur la norme IEC 62433** . . . . . 349

**Annexe 6. Quelques outils** . . . . . 353

**Liste des sigles et abréviations** . . . . . 355

**Bibliographie** . . . . . 359

**Index** . . . . . 369