Contents

Foreword xi

Preface xiii

Acknowledgements xv

Preamble xvii

Part 1. Introduction – The Buzz about IoT and IoE 1

Chapter 1. Introduction 3

1.1. Definition of communicating- or connected Things 3
1.1.1. Connected Things – Communicating Things 3
1.1.2. Definition of the IoT 4
1.1.3. Internet of x 5

Chapter 2. The (Overly) Vast World of IoT 9

2.1. 2011–2016: the craze for the term “Connected Thing” 9
2.1.1. The catch-all 9
2.1.2. Fashion, buzz and “bubble” 10
2.1.3. “Hype” cycle for innovations 11
2.2. The true goal of this book 14

Chapter 3. Why a Connectable Thing? 15

3.1. Examples of connectable things 15
3.1.1. Home care for the elderly 16
3.1.2. In the automotive industry 19

Part 2. Constraints Surrounding an IoT Project 21

Chapter 4. Aspects to be Taken into Consideration 23

4.1. Aspects pertaining to the concrete realization of Connected Things 23
4.1.1. Financial and marketing aspects 24
4.1.2. Technical and industrial aspects 24
4.1.3. Regulatory and normative aspects 24
4.1.4. Security aspects 24
4.1.5. Cost aspects 24

Chapter 5. Financial and Marketing Aspects 27

5.1. Economic aspects 27
5.1.1. Saleable / buyable 27
5.2. Ergonomic aspects 29
5.2.1. Mechanical form and design vs ergonomics 29

Chapter 6. Technical and Industrial Aspects 31

6.1. Technical aspects 31
6.1.1. Life cycle of a new product 31
6.1.2. Techno-economic feasibility 32
6.1.3. Design 32
6.1.4. Industrialization, manufacturing process and quality assurance 32
6.2. Energy aspects 32
6.2.1. Power supply to the Thing 33
6.3. Industrial aspects. 39

Chapter 7. Regulatory and Normative Aspects 41

7.1. Regulatory aspects and recommendations 41
7.1.1. Radiofrequency regulations 42
7.2. Health-related recommendations 43
7.2.1. Exposure of the human body to electromagnetic fields 44
7.2.2. Specific Absorption Rate (SAR). 44
7.3. Societal regulations and individual freedoms (privacy) 45
7.3.1. The various data needing to be protected 45
7.3.2. Loi Informatique et Libertés 45
7.3.3. Mandate 436, PIA and RFID and IoT applications 46
7.3.4. GDPR – General Data Protection Regulation 49
7.3.5. Privacy by design 51
7.4. Environmental regulations and recycling 53
7.4.1. Electronic waste treatment 53

7.4.2. Regulation and organization of the chain 54
7.4.3. Labeling of electrical and electronic equipment 54
7.5. Normative aspects 55
7.5.1. ISO/AFNOR. 55
7.5.2. IEEE 56
7.5.3. ETSI 56

Chapter 8. Security Aspects 59

8.1. Security aspects 59
8.1.1. The weak links 60
8.1.2. Possible solutions 62
8.1.3. Definition and choice of security target. 63
8.1.4. Concepts of security levels applied in IoT 64
8.1.5. True security – the “Secure Element”. 67
8.1.6. Cryptography 70
8.1.7. Symmetric and asymmetric encryption 71
8.1.8. Consumer Things, IoT, security… and the Cloud 75
8.2. Judging the quality of security 80
8.3. Some thoughts about security, privacy and IoT. 81
8.4. Vulnerabilities and attacks in the IoT chain 82
8.4.1. Attacks on the software layer 83
8.4.2. Attacks on the board or Thing 84
8.4.3. Attacks on the integrated circuits 84
8.4.4. Security standards. 85

Part 3. Overall Architecture of the IoT Chain 87

Chapter 9. Communication Models in IoT 89

9.1. Communication models in IoT 89
9.1.1. OSI model 89
9.1.2. TCP/IP model 92
9.1.3. By way of conclusion. 98

Chapter 10. Overall Architecture of an IoT System 101

10.1. Overall architecture of a CT and IoT solution 101
10.1.1. Description of the complete chain 102
10.2. From a more technological point of view 102
10.2.1. Architecture and overview of an IoT chain 102
10.2.2. The “base station/gateway”. 106
10.2.3. The “Cloud” zone 109
10.2.4. The “User” zone 110
10.3. The very numerous protocols involved. 113

Part 4. Detailed Description of the IoT Chain 117

Part 4A. From the User (The Outside World) to the Thing 119

Chapter 11. From the Outside World to the Thing 121

11.1. Connection of the Thing to the outside world 121
11.1.1. Using sensors 121
11.1.2. Using wired connections 122
11.1.3. Using RF links 122
11.1.4. Very Short Range (<10 cm) 122
11.1.5. Short range SR Wide band (tens of meters) 124

Chapter 12. The Secure Connected Thing 127

12.1. Physical constitution of the Thing 127
12.1.1. Sensors 127
12.1.2. Local intelligence – microcontroller 128
12.1.3. Security (SE) 128

Part 4B. From the Thing to the Base Station 131

Chapter 13. Means of Communication to Access a Base Station 133

13.1. Possible network connectivity technologies 133
13.1.1. Local or ultra-local non-operated RF networks 135
13.1.2. Extended-deployment operated RF networks 136
13.1.3. Is there space for all these technologies? 136
13.2. Medium-range MR Wide-band (hundreds of meters) 136
13.2.1. Wi-Fi 137
13.3. Long-range (LR – tens of kilometers) 138
13.3.1. NB, UNB, WB, UWB, FHSS, DSSS and RF regulations 138
13.3.2. Regulators and regulations 140
13.3.3. RF bases 146
13.4. LTN – Low-Throughput Network 152
13.4.1. Long Range LR - LTN 153
13.4.2. LR LTN in (U)NB – SIGFOX 156
13.4.3. LR LTN in DSSS (spectrum spreading) – LoRa, from Semtech 167
13.4.4. A discussion of spectrum spreading – SS 169
13.4.5. LR WB 192
13.4.6. Operated LR WB networks 196

Part 4C. From the Base Station to the Server 203

Chapter 14. Network Access Layer – IP 205

14.1. IPv4 205
14.1.1. Operation 206
14.1.2. Services provided 206
14.1.3. Reliability 206
14.2. IPv6 207
14.2.1. Differences between IPv6 and IPv4 207
14.2.2. Problems of privacy and/or anonymity? 209
14.3. 6LoWPAN 209
14.3.1. Description of the technology 210
14.3.2. Integration of an IPv6 packet into an IEEE 802.15.4 frame 210
14.3.3. Autoconfiguration of an IP address 211
14.3.4. Network supervision and management 211
14.3.5. Constraints on “upper-layer” applications 211
14.3.6. Security 212
14.3.7. Routing 212

Chapter 15. The Server 215

15.1. Conventional functions of a server in IoT 216

Chapter 16. Transport and Messaging Protocols 219

16.1. Transport 219
16.1.1. Operation 220
16.1.2. Structure of a TCP segment 220
16.2. “IoT messaging” technologies 221
16.2.1. Main protocol parameters 221
16.3. Protocols 225
16.4. HTTP – HyperText Transfer Protocol 226
16.5. HTTP/2 227
16.6. MQTT – Message Queuing Telemetry Transport 227
16.6.1. Security in MQTT 229
16.7. CoAP – Constrained Application Protocol 229
16.8. XMPP 230
16.9. DDS – Data Distribution Service 231
16.10. AMQP – Advanced Message Queuing Protocol 232
16.11. SMQ 233
16.12. JMS – Java Messaging Service 233
16.13. Other protocols 234

16.14. The broker 234
16.14.1 Examples of possibilities 235
16.15. Programming languages 236
16.16. Operating systems 236

Part 4D. From the Cloud Server to the Various Users 237

Chapter 17. Cloud and Fog Computing 239

17.1. Cloud computing? 239
17.1.1. What is its mode of operation? 240
17.1.2. Advantages and benefits in IoT applications 240
17.1.3. Types of Cloud computing 241
17.1.4. Cloud products and services 241
17.2. Example: the PaaS platform AWS IoT 242
17.3. How security is managed 244
17.4. Fog computing? 245
17.5. Big data 246
17.6. Natural interfaces 247

Part 5. Concrete Realization of an IoT Solution Examples and Costs 249

Chapter 18. Examples of the Concrete Realization of Connected Things 251

18.1. Subject/application taken as an example 251
18.1.1. Architecture of the product: a communicating physical Thing 253
18.1.2. Mandatory steps in creating the Thing 255

Chapter 19. Cost Aspects 261

19.1. CAPEX and OPEX are in the same boat… 261
19.1.1. CAPEX 262
19.1.2. OPEX 273
19.1.3. Conclusions 275
19.1.4. Very important conclusions 276

Conclusion 279

Bibliography 281

Index 285