# Contents

**Foreword** . . . . . V

**Preface of the Editors** . . . . . VII

**1 The Market for Fieldbus and industrial Ethernet** . . . . . 1
*David Humphrey, Florian Güldner*

1.1 The Benefits of Being Connected . . . . . 2
1.2 The Market for industrial Ethernet Products . . . . . 3
1.3 Market Players . . . . . 4

**2 Trends in Factory Automation** . . . . . 9
*Michael Volz*

2.1 Growth Factors. . . . . 10
2.2 What Users are Demanding . . . . . 11
2.3 Focus on Engineering Cost . . . . . 11
2.4 Security Aspects . . . . . 12

**3 International Standardization** . . . . . 13
*Max Felser*

3.1 History of Fieldbus Standards . . . . . 13
3.1.1 The German-French Fieldbus War . . . . . 13
3.1.2 The International Fieldbus War . . . . . 14
3.1.3 The Compromise Solution . . . . . 14
3.1.4 Extensions with Ethernet . . . . . 16
3.1.5 Extensions with Wireless Systems . . . . . 16
3.2 Structure of Fieldbus Standards . . . . . 17
3.2.1 Definition of Fieldbuses . . . . . 17
3.2.2 Definition of Real-time Ethernet . . . . . 17
3.2.3 Installation Guidelines . . . . . 18
3.2.4 Reliability. . . . . 19
3.2.5 Definition of Protocol Families . . . . . 19
3.3 Summary . . . . . 21

**4 Fieldbuses: Status and Outlook** . . . 25
*Michael Volz*
4.1 Stability and Reliability as Success Factors . . . 26
4.2 Challenges for the Future . . . 26
4.3 Quality through Certification . . . 27

**5 CANopen** . . . 29
*Holger Zeltwanger*
5.1 Lower Communication Layers . . . 30
5.2 Higher Communication Layers . . . 32
5.3 Device and Application Profiles . . . 35
5.4 Summary . . . 40

**6 CC-Link** . . . 41
*John Browett, John Wozniak*
6.1 CC-Link Network Types . . . 42
6.2 CC-Link topology and communication speeds . . . 43
6.3 Data Transmission . . . 44
6.3.1 CC-Link Data Types . . . 44
6.3.2 Types of Stations . . . 45
6.3.3 Maximum Number of Devices . . . 45
6.3.4 Typical Scan Times . . . 45
6.4 How CC-Link Communicates . . . 48
6.4.1 CC-Link Transmission Processes . . . 48
6.4.2 CC-Link Memory Mapping . . . 50
6.5 Version 1.1 or Version 2.0 . . . 54
6.6 CC-Link Implementation . . . 55
6.7 Profiles . . . 55
6.8 CC-Link Safety . . . 57
6.9 Certification Testing . . . 57

**7 CIP: DeviceNet and ControlNet** . . . 59
*Viktor Schiffer*
7.1 Basic Elements of the Common Industrial Protocol (CIP) . . . 60
7.1.1 Object Orientation . . . 61
7.1.2 Basic Principles of CIP Communications . . . 62
7.1.3 Connections, Message Types . . . 63
7.1.4 Objects . . . 64
7.1.5 Device Profiles . . . 66
7.1.6 Configuration and Device Description . . . 67
7.1.7 Bridging and Routing . . . 68
7.1.8 Functional Safety (CIP Safety) . . . 69
7.1.9 Conformance Testing . . . 71

7.2 DeviceNet . . . 72
7.2.1 Communication Model . . . 72
7.2.2 System Concepts . . . 73
7.2.3 System Start-up . . . 74
7.2.4 Addressing Principles . . . 75
7.2.5 Supported Topologies . . . 75
7.2.6 Data Rates . . . 76
7.2.7 Installation . . . 76
7.2.8 Communication PLC – I/O . . . 77
7.2.9 Communication PLC – PLC . . . 79
7.2.10 Device Configuration and Integration . . . 80
7.2.11 Safety Support . . . 80
7.2.12 Profiles . . . 80
7.2.13 Diagnostics . . . 80
7.2.14 Device Replacement . . . 81
7.3 ControlNet . . . 81
7.3.1 Communication Model . . . 81
7.3.2 System Concepts . . . 82
7.3.3 Addressing Principles . . . 84
7.3.4 Supported Topologies . . . 84
7.3.5 Data Rates . . . 84
7.3.6 Installation . . . 84
7.3.7 Communication PLC – I/O . . . 86
7.3.8 Communication PLC – PLC . . . 86
7.3.9 Device Configuration and Integration . . . 87
7.3.10 Safety Support . . . 87
7.3.11 Profiles . . . 87
7.3.12 Diagnostics . . . 87
7.3.13 Device Replacement . . . 88

**8 INTERBUS** . . . 91
*Martin Müller*
8.1 Basic Specifications of the INTERBUS System . . . 91
8.1.1 The Ring System . . . 92
8.1.2 The INTERBUS Elements . . . 93
8.1.3 The INTERBUS Remote Bus . . . 94
8.2 Data Transmission in the INTERBUS System . . . 95
8.2.1 The Summation Frame Protocol . . . 95
8.2.2 Data Security in the INTERBUS System . . . 96
8.2.3 Hybrid Data Transmission . . . 96
8.3 INTERBUS Protocol Chips . . . 97
8.3.1 The IPMS4 Master Protocol Chip . . . 97
8.3.2 The Slave Protocol Chips . . . 97

8.4 INTERBUS Diagnostics . . . 99
8.4.1 Graded Diagnostic Concept . . . 99
8.4.2 Fiber Optic Diagnostics . . . 101
8.5 INTERBUS Safety . . . 103
8.5.1 Method of Operation . . . 103
8.5.2 Advantages for the User . . . 103
8.6 Conclusion . . . 105

**9 PROFIBUS** . . . 107
*Klaus-Peter Lindner*
9.1 Overview: PROFIBUS as Modular System . . . 107
9.2 Transmission Technology . . . 109
9.2.1 RS485 . . . 109
9.2.2 Optical Transmission . . . 110
9.2.3 MBP . . . 111
9.2.4 Troubleshooting . . . 112
9.3 Communication . . . 112
9.3.1 Performance Level DP-V0 . . . 113
9.3.2 Performance Level DP-V1 . . . 115
9.3.3 Performance Level DP-V2 . . . 116
9.3.4 Addressing with Slot and Index . . . 116
9.4 General Application Profiles . . . 117
9.4.1 PROFIsafe . . . 117
9.4.2 Redundancy . . . 119
9.5 Specific Application Profiles . . . 120
9.5.1 PROFIdrive . . . 120
9.5.2 Fluid Power . . . 121
9.5.3 Ident Systems . . . 121
9.5.4 PROFIBUS PA . . . 121
9.6 Device Management . . . 122
9.7 PROFIBUS Implementation . . . 123
9.8 Quality Assurance and Certification . . . 123
9.8.1 Test Procedure . . . 124

**10 Comparison of Fieldbus Systems** . . . 127
*Michael Volz*

**11 Industrial Ethernet: Status and Outlook** . . . . . **129**
*Michael Volz*

11.1 Real-time Behavior . . . . . 130
11.2 Connection between Office World and Control Technology . . . . . 131
11.3 Cabling Technology . . . . . 131
11.4 Outlook . . . . . 132

**12 CC-Link IE** . . . . . 133
*John Browett, John Wozniak*

12.1 CC-Link IE Control . . . . . 133
12.2 CC-Link IE Field . . . . . 134
12.2.1 CC-Link IE Field Topology . . . . . 134
12.2.2 CC-Link IE Field Data Types and Network Memory Allocation . . . . . 137
12.2.3 CC-Link IE Field Communication . . . . . 139
12.2.4 CC-Link IE Field Frame Structure . . . . . 144
12.2.5 Connection for Ethernet TCP/IP (UDP/IP) Devices . . . . . 145
12.2.6 CC-Link IE Field Implementation . . . . . 145
12.2.7 Profiles . . . . . 146
12.2.8 CC-Link Conformance Testing . . . . . 148
12.2.9 Main features of CC-Link IE Field . . . . . 148

**13 EtherCAT** . . . . . 149
*Oliver Fels*

13.1 Technology Principle . . . . . 150
13.1.1 Processing „on the fly“ . . . . . 150
13.1.2 Best Performance . . . . . 150
13.1.3 Migration from Classical Fieldbus to EtherCAT with Gateways . . . . . 151
13.1.4 Flexible Topology Including Redundancy Options . . . . . 152
13.1.5 Easy Diagnosis and Configuration . . . . . 154
13.1.6 Use of Standard Components . . . . . 154
13.2 The EtherCAT Device Protocol . . . . . 155
13.2.1 Cyclic Communication (Process Data) . . . . . 156
13.2.2 Acyclic Communication . . . . . 156
13.2.3 Synchronization with Distributed Clocks (DC) . . . . . 158
13.3 Integrated Functional Safety . . . . . 159
13.4 EtherCAT for Plant Automation . . . . . 162
13.5 Implementation Aspects . . . . . 165
13.5.1 Master Implementation . . . . . 165
13.5.2 Slave Implementation . . . . . 166
13.5.3 Monitoring Tools . . . . . 166
13.6 EtherCAT Technology Group . . . . . 167

**14 EtherNet/IP** . . . 171
*Viktor Schiffer*
14.1 Communication Model . . . 172
14.2 System Concepts . . . 172
14.3 Addressing Principles . . . 174
14.4 Supported Topologies . . . 174
14.5 Data Rates . . . 175
14.6 Installation . . . 175
14.7 Communication PLC – I/O . . . 176
14.8 Communication PLC – PLC . . . 177
14.9 Device Configuration and Integration . . . 177
14.10 Safety Support . . . 178
14.11 Profiles . . . 178
14.12 Diagnostics . . . 178
14.13 Device Replacement . . . 178
14.14 Fieldbus Integration . . . 179
14.15 Integration in Enterprise Networks . . . 179
14.16 Security . . . 180

**15 Modbus** . . . 183
*Michael Volz*
15.1 History of the Modbus Protocol . . . 183
15.2 The Modbus Protocol Suite . . . 184
15.3 Modbus TCP Overview . . . 184
15.3.1 Modbus Protocol Function Codes . . . 185
15.3.2 The Modbus application data unit (ADU) . . . 187
15.3.3 Modbus TCP Addressing Model . . . 188
15.3.4 Modbus TCP Data Model . . . 188
15.3.5 Modbus Protocol Transactions . . . 189
15.3.6 Modbus PDU and ADU Formats . . . 190
15.3.7 Modbus Exception Responses . . . 191
15.4 Mapping the Modbus Protocol on TCP/IP . . . 193
15.4.1 Modbus TCP Connection Management . . . 194
15.4.2 Use of TCP/IP Stack . . . 194
15.5 Configuration of Modbus TCP devices and systems . . . 196
15.6 Performance Aspects . . . 196
15.7 Modbus TCP Conformance Testing . . . 197
15.8 The Modbus Organization . . . 197

**16 POWERLINK** . . . 199
*Stefan Schönegger*
16.1 Data Exchange with POWERLINK . . . 200
16.1.1 Why Standard Ethernet cannot Achieve Hard Real-time Operation . . . 200

16.1.2 The POWERLINK Stack . . . 201
16.1.3 The POWERLINK Mechanism . . . 202
16.2 Functional Characteristics of POWERLINK . . . 203
16.2.1 Network Structure with POWERLINK: Free Selection of Topology . . . 203
16.2.2 Unique Addressing for each Node . . . 204
16.2.3 Hot Plugging . . . 204
16.2.4 Cross-traffic Increases Performance and Simplifies the System . . . 205
16.2.5 Redundant Networks with POWERLINK . . . 206
16.2.6 Diagnostics . . . 206
16.2.7 POWERLINK = CANopen over Ethernet . . . 207
16.3 Safety and Security . . . 207
16.3.1 Bus Independence . . . 208
16.3.2 openSAFETY Functionality . . . 209
16.3.3 Mechanisms for Error Detection and Prevention . . . 209
16.3.4 Structure of the openSAFETY Frame . . . 210
16.3.5 The openSAFETY Network . . . 210
16.3.6 Security . . . 211
16.4 Technical Implementation of the Master and Slaves . . . 211
16.4.1 Solutions for the POWERLINK Master . . . 212
16.4.2 Solutions for the POWERLINK Slave . . . 212
16.5 POWERLINK Open Source . . . 213
16.6 EPSG User Organization . . . 213

**17 PROFINET** . . . 215
*Jörg Freitag*
17.1 PROFINET at a Glance . . . 216
17.1.1 PROFINET Highlights . . . 217
17.1.2 PROFINET IO Device Classes . . . 217
17.1.3 Addressing in PROFINET IO . . . 218
17.2 PROFINET IO Basics . . . 219
17.2.1 Device Model . . . 219
17.2.2 Real-time Communication . . . 220
17.2.3 Data Communication . . . 221
17.2.4 Network Diagnostics in PROFINET . . . 222
17.2.5 System Engineering and GSD . . . 223
17.2.6 System Power-up . . . 223
17.2.7 Neighborhood Detection . . . 224
17.2.8 Fast Start-up . . . 224
17.3 IRT Communication in PROFINET IO . . . 225
17.3.1 IRT Control . . . 225
17.3.2 IRT Intervals . . . 226
17.4 PROFINET IO Controller and Device . . . 227

17.5 Conformance Classes (CC) . . . 227
17.6 Application Profiles for PROFINET IO . . . 228
17.6.1 Train Applications . . . 228
17.6.2 PROFIenergy . . . 228
17.7 Integration of Fieldbus Systems . . . 230
17.8 Network Installation . . . 230
17.8.1 PROFINET Cabling . . . 231
17.8.2 Plug Connectors for Data . . . 232
17.8.3 Plug Connectors for Power . . . 232
17.8.4 Network Components . . . 232
17.8.5 Redundancy . . . 232
17.8.6 Industrial Wireless . . . 233
17.9 PROFINET IO Certification . . . 234

**18 sercos** . . . 235
*Peter Lutz*
18.1 sercos I and II . . . 235
18.1.1 Topology . . . 236
18.1.2 Communication Method, Synchronization and Protocol Structure . . . 237
18.1.3 Standardized Data . . . 239
18.1.4 Implementation . . . 240
18.2 sercos III . . . 240
18.2.1 Topology and Installation . . . 240
18.2.2 Transmission Procedure . . . 241
18.2.3 Message Structure . . . 243
18.2.4 Ring Redundancy and Hot-Plugging . . . 243
18.2.5 Direct Cross Communication and Controller-to-Controller Communication (C2C) . . . 243
18.2.6 Synchronization . . . 244
18.2.7 CIP Safety on sercos . . . 245
18.2.8 Device Profiles . . . 246
18.3 Implementation of sercos III . . . 248
18.4 Summary . . . 249

**19 Comparison of Ethernet Systems** . . . 251
*Frithjof Klasen*
19.1 Performance Indicators . . . 251
19.2 Requirements . . . 252
19.3 Implementation Concept . . . 254
19.4 Selection Criteria . . . 256
19.5 Future Outlook . . . 258

**20 Wireless: Status and Outlook** . . . 259
*Lutz Rauchhaupt*
20.1 Wireless, Radio, or WLAN . . . 259
20.2 Requirements and Conditions of Radio-based Industrial Communication . . . 260
20.3 Cellular Network Systems. . . . 261
20.4 Wireless Local Area Networks (WLAN) . . . 263
20.5 Bluetooth . . . 265
20.6 WirelessHART . . . 266
20.7 Wireless Sensor/Actor Network for Factory Automation (WSAN-FA) . . . 267
20.8 Other Wireless Solutions . . . 268
20.9 Outlook . . . 269

**21 Connecting Networks** . . . 271
*Michael Volz*
21.1 Connection of Autonomous Plant Units having their Own PLCs . . . 271
21.2 Connection of Lower-level Plant Units without Own PLCs. . . . 273
21.3 Selection and Use Criteria . . . 273

**22 Security for Ethernet Systems** . . . 275
*Frithjof Klasen*
22.1 Industrial Ethernet Affects Security Solutions . . . 275
22.2 Challenges . . . 276
22.2.1 Organizational Challenges . . . 277
22.3 Differences to Business IT . . . 277
22.4 Technical Challenges . . . 278
22.5 Possible Solutions . . . 279
22.5.1 Security Objectives . . . 280
22.5.2 Threats and Risk Analysis . . . 280
22.5.3 Security – A Joint Project. . . . 280
22.6 The Solution: People, Processes, Technologies . . . 281

**23 Field Device Integration with FDI** . . . 283
*Daniel Großmann, Alexander Kaiser*
23.1 Current Situation in Device Integration. . . . 283
23.2 The Solution: Field Device Integration . . . 284
23.2.1 Benefits of EDDL . . . 284
23.2.2 Benefits of FDT . . . 284
23.3 Device Package – Representative for a Device . . . 285
23.3.1 Catalog (mandatory) . . . 285
23.3.2 EDD – Device Definition – DEF (mandatory, based on EDDL) . . . 286

23.3.3 EDD – User Interface Description – UID (mandatory, based on EDDL) . . . 286
23.3.4 EDD – Business Logic – BL (mandatory, based on EDDL and FDT) . . . 286
23.3.5 User Interface Plug-in – UIP (optional, based on FDT) . . . 286
23.3.6 Attachments (mandatory; optional – depending on protocol) . . . 287
23.4 The Basic Architecture . . . 287
23.4.1 System Architectures . . . 288
23.4.2 Topologies . . . 289
23.5 Aiming for a Uniform Approach through Harmonization . . . 291
23.6 FDI from an End User Perspective . . . 293
23.6.1 A Solution . . . 293
23.6.2 Safeguarding Investments . . . 294
23.6.3 Robustness . . . 294
23.6.4 Interoperability . . . 294
23.6.5 Uniformity . . . 295
23.6.6 Version Handling . . . 295
23.7 Summary . . . 295

**24 Implementation Criteria: Make or Buy?** . . . 297
*Volker Oestreich*
24.1 Market Situation . . . 297
24.2 Options for Implementation . . . 298
24.2.1 In-House Development of Communication Interfaces . . . 298
24.2.2 In-house Development with External Support . . . 298
24.2.3 Application of Modular Communication Modules . . . 299
24.3 The Right Decision: Assistance Offered . . . 299
24.3.1 Example: Tightening Controller . . . 301
24.3.2 Specified Boundary Conditions . . . 301
24.3.3 Results of the Calculation . . . 302
24.4 Conclusion . . . 303

**25 Flexible Interface Implementation** . . . 305
*Michael Volz*
25.1 Development Planning . . . 305
25.1.1 Consultation . . . 305
25.1.2 Implementation . . . 306
25.1.3 Development Environment . . . 306
25.1.4 Hardware/Software Design . . . 306
25.1.5 Certification . . . 306
25.1.6 Technology Support . . . 307

25.2 In-house Development or Development Partnership . . . . . 307
25.2.1 Implementation Options . . . . . 308
25.2.2 In-house Development of Communication Interfaces . . . . . 308
25.2.3 Customer-specific Solutions . . . . . 309
25.2.4 Ready-to-use Communication Modules . . . . . 309
25.2.5 External Bus Connection with a Protocol Converter . . . . . 310

**Organizations** . . . . . 312

**Authors** . . . . . 317

**Index** . . . . . 327