

Contents

Preface.....	xix
Author	xxi

Chapter 1 Data Communication.....	1
1.1 Introduction	1
1.2 Comparison between Digital and Analog Communication	1
1.3 Data Communication.....	2
1.3.1 Main Characteristics.....	3
1.4 Data Types	3
1.5 Data Transfer Characteristics	4
1.6 Data Flow Methods	5
1.7 Transmission Modes	6
1.7.1 Parallel.....	6
1.7.2 Serial.....	7
1.7.3 Asynchronous	7
1.7.4 Synchronous	9
1.7.5 Isochronous.....	9
1.8 Use of Modems.....	10
1.9 Power Spectral Density.....	11
1.10 Transmission Impairments	11
1.11 Data Rate and Bandwidth Relationship.....	12
1.12 Multiplexing	13
1.12.1 Introduction	13
1.12.2 Types.....	13
1.12.3 FDM	14
1.12.4 WDM.....	15
1.12.5 TDM	16
1.12.5.1 Synchronous TDM	16
1.12.5.2 Statistical TDM	17
1.12.6 Variable Data Rate.....	17
1.12.7 Multilevel Multiplexing	18
1.12.8 Multislot Multiplexing	18
1.12.9 Pulse Stuffing Multiplexing.....	19
1.13 Spread Spectrum	19
1.13.1 Introduction	20
1.13.2 FHSS	21

1.13.3 DSSS.....	23
1.13.4 Comparison between FHSS and DSSS	24
1.13.5 Advantages of Spread Spectrum.....	25
1.14 Data Coding.....	26
1.14.1 Introduction	27
1.14.2 Characteristics of a Line Code	27
1.14.3 Types.....	28
Chapter 2 Networking.....	29
2.1 Introduction	29
2.2 Characteristics	30
2.3 Connection Types.....	31
2.4 Data Communication Standards and Organizations...	31
2.5 Network Topology	34
2.5.1 Mesh	34
2.5.2 Star	35
2.5.3 Bus.....	35
2.5.4 Ring	36
2.5.5 Hybrid.....	37
2.6 Network Applications.....	38
2.7 Network Components	38
2.8 Classification of Networks.....	40
2.8.1 LANs	40
2.8.2 MANs	40
2.8.3 WANs	41
2.8.4 GANs.....	41
2.8.5 Building and Campus Backbone and Enterprise Network.....	41
2.9 Interconnection of Networks	41
Chapter 3 Network Models	45
3.1 Introduction	45
3.2 Three-Layer Model.....	45
3.3 OSI Model	47
3.3.1 Physical Layer.....	49
3.3.2 Data Link Layer.....	51
3.3.3 Network Layer	52
3.3.4 Transport Layer	53
3.3.5 Session Layer.....	54
3.3.6 Presentation Layer	55
3.3.7 Application Layer	56

3.4 TCP/IP Protocol Suite	56
3.4.1 Introduction	56
3.4.2 Protocol Architecture	57
3.4.2.1 TCP	58
3.4.2.2 UDP.....	62
3.4.2.3 IP	62
3.4.3 Operation.....	65
3.4.4 PDUs in Architecture	66
3.4.5 Addressing	66
3.4.5.1 Physical.....	66
3.4.5.2 Logical.....	66
3.4.5.3 Port	67
3.4.5.4 Specific	67
Chapter 4 Networks in Process Automation	69
4.1 Introduction	69
4.2 Communication Hierarchy in Factory Automation	69
4.3 I/O Bus Networks	71
4.3.1 Types.....	71
4.3.2 Network and Protocol Standards	73
4.3.3 Advantages	74
4.4 OSI Reference Model	75
4.5 Networking at I/O and Field Levels.....	77
4.6 Networking at Control Level	79
4.7 Networking at Enterprise/Management Level.....	79
Chapter 5 Fieldbuses	81
5.1 What Is a Fieldbus?.....	81
5.1.1 Evolution.....	81
5.1.2 Architectural Progress.....	82
5.1.3 Types	84
5.1.4 Expanded Network View.....	85
5.2 Topologies.....	88
5.2.1 Point-to-Point.....	88
5.2.2 Bus with Spurs.....	88
5.2.3 Tree (Chicken Foot)	89
5.2.4 Daisy Chain	89
5.2.5 Mixed Topology.....	90
5.3 Terminators.....	91
5.4 Fieldbus Benefits.....	91

Chapter 6	Highway Addressable Remote Transducer (HART)	93
6.1	Introduction	93
6.2	Evolution and Adaptation of HART Protocol.....	94
6.3	HART and Smart Devices.....	94
6.4	HART Encoding and Waveform	95
6.5	HART Character	95
6.6	Addressing.....	96
6.7	Arbitration	97
6.8	Communication Modes	97
6.9	HART Networks.....	98
6.10	Field Device Calibration.....	99
6.11	HART Communication Layers.....	100
6.11.1	Physical Layer.....	100
6.11.2	Data Link Layer.....	101
6.11.3	Application Layer	102
6.12	Installation and Guidelines for HART Networks ...	104
6.13	Device Descriptions.....	105
6.14	Application in Control Systems	105
6.15	Application in SCADA	106
6.16	Benefits	106

Chapter 7	Foundation Fieldbus	109
------------------	---------------------------	-----

7.1	Introduction	109
7.2	Definition and Features	109
7.3	Foundation Fieldbus Data Types	110
7.4	Architecture	110
7.5	Standards	111
7.6	H1 Benefits	111
7.7	HSE Benefits.....	112
7.7.1	Interoperability of Subsystems	112
7.7.2	Function Blocks	112
7.7.3	Control Backbone	112
7.7.4	Standard Ethernet	112
7.8	Communication Process	113
7.8.1	OSI Reference Model	113
7.8.2	PDU	114
7.8.3	Physical Layer.....	114
7.8.3.1	Manchester Coding	115
7.8.3.2	Signaling.....	115
7.8.4	Data Link Layer.....	116
7.8.4.1	Medium Access Control	117

7.8.4.2	Addresses	117
7.8.4.3	LAS and Device Types.....	117
7.8.5	Application Layer	122
7.8.5.1	FAS.....	122
7.8.5.2	FMS.....	124
7.9	Technology of Foundation Fieldbus.....	129
7.9.1	User Application Blocks	130
7.9.2	Resource Block	130
7.9.3	Function Block.....	130
7.9.3.1	Function Block Library	133
7.9.3.2	Function Block Scheduling	133
7.9.3.3	Application Clock Distribution.....	134
7.9.3.4	Macrocycle and Elementary Cycle	135
7.9.3.5	Device Address Assignment.....	135
7.9.3.6	Tag Service	136
7.9.4	Transducer Block	136
7.9.5	Support Objects	137
7.10	Linking and Scheduling of Blocks	138
7.11	Device Information.....	138
7.11.1	Device Description	139
7.11.2	Device Description Language	139
7.11.3	DD Tokenizer	139
7.11.4	DD Services	139
7.11.5	DD Hierarchy	140
7.11.6	Capabilities File	141
7.11.7	Device Identification	141
7.12	Redundancy	141
7.12.1	Host-Level Redundancy.....	142
7.12.1.1	Media Redundancy	142
7.12.1.2	Network Redundancy	143
7.12.1.3	Media and Network Redundancy	144
7.12.2	Sensor Redundancy	144
7.12.3	Transmitter Redundancy	144
7.13	HSE Device Types	145
7.14	System Configuration	146
7.14.1	System Design	146
7.14.2	Device Configuration	146
	Chapter 8 PROFIBUS	147
8.1	Introduction	147
8.2	PROFIBUS Family	147

Contents

8.3	Transmission Technology	149
8.4	Communication Protocols	149
8.5	Device Classes.....	151
8.6	PROFIBUS in Automation	152
8.7	OSI Model of PROFIBUS Protocol Stack	153
8.8	PROFIBUS-DP Characteristics	153
8.8.1	Version DP-V0	154
8.8.1.1	Diagnostic Functions	154
8.8.1.2	Synchronization and Freeze Mode	155
8.8.1.3	System Configuration	155
8.8.1.4	Time Monitors	155
8.8.1.5	Token-Passing Characteristics.....	156
8.8.2	Version DP-V1	156
8.8.2.1	Cyclic and Acyclic Communication	156
8.8.3	Version DP-V2	158
8.8.3.1	Slave-to-Slave Communication	158
8.8.3.2	Isochronous Mode	159
8.8.3.3	Clock Control	159
8.8.3.4	Upload and Download.....	159
8.8.3.5	HART on DP.....	159
8.8.3.6	Comparison between DP-V0, DP-V1, and DP-V2.....	159
8.8.4	Communication Profile.....	159
8.8.5	Physical Layer.....	160
8.8.5.1	Transmission Speed vs. Segment Length	161
8.8.6	Data Link Layer.....	162
8.8.7	DDLM and User Interface.....	163
8.8.8	State Diagram of Slave	164
8.8.9	Addressing with Slot and Index	165
8.9	PROFIBUS-PA Characteristics	166
8.9.1	Bus Access Method	167
8.9.2	Data Telegram	168
8.9.3	Device Profile	169
8.9.4	PA Block Model.....	170
8.9.4.1	Transducer Block	171
8.9.4.2	Physical Block	171
8.9.4.3	Function Block	172
8.9.4.4	Device Management Block.....	172
8.10	Network Configuration	175
8.11	Bus Monitor.....	176

Contents

8.12	Time Stamp	176
8.13	Redundancy	176
8.14	PROFIsafe	178
8.15	PROFIdrive.....	179
8.16	PROFINet	180
8.17	PROFIBUS International.....	182
8.18	Foundation Fieldbus and PROFIBUS—A Comparison.....	182
Chapter 9 MODBUS and MODBUS Plus.....		185
9.1	Introduction	185
9.2	Communication Stack	186
9.3	Network Architecture	187
9.4	Communication Transactions	187
9.4.1	Master-Slave and Broadcast Communication	188
9.4.2	Query–Response Cycle.....	189
9.4.2.1	Address Field.....	189
9.4.2.2	Function Field	189
9.4.2.3	Data Field	190
9.4.2.4	Error Check Field	190
9.5	Protocol Description: PDU and ADU	190
9.6	Transmission Modes	191
9.6.1	ASCII Mode	192
9.6.2	RTU Mode.....	192
9.7	Message Framing	192
9.7.1	ASCII Framing	193
9.7.2	RTU Framing	193
9.8	MODBUS TCP/IP	193
9.9	Introduction to MODBUS Plus.....	194
9.10	Message Frame	195
9.11	Networking MODBUS Plus.....	196
Chapter 10 CAN Bus		199
10.1	Introduction	199
10.2	Features	200
10.3	Types.....	200
10.3.1	Speed vs. Bus Length	200
10.4	CAN Frames.....	200
10.5	CAN Data Frame	202
10.6	CAN Arbitration.....	202

Contents

10.6.1 CAN Communication	204
10.7 Types of Errors	204
10.8 Error States	206
Chapter 11 DeviceNet.....	207
11.1 Introduction	207
11.2 Features	207
11.3 Object Model	208
11.4 Protocol Layers.....	208
11.5 Physical Layer.....	209
11.5.1 Data Rate	209
11.6 Data Link Layer.....	209
11.7 Application Layer	210
11.8 Power Supply and Cables	211
11.9 Error States.....	211
Chapter 12 AS-i	213
12.1 Introduction	213
12.2 Features	213
12.3 Different Versions.....	214
12.4 Topology	214
12.5 Protocol Layers.....	215
12.6 Physical Layer.....	215
12.7 Data Link Layer.....	215
12.8 Execution Control	216
12.9 Modulation Technique	217
Chapter 13 Seriplex	219
13.1 Introduction	219
13.2 Features	219
13.3 Physical Layer.....	220
13.4 Data Link Layer.....	220
13.5 Data Integrity.....	221
Chapter 14 Interbus-S	223
14.1 Introduction	223
14.2 Features	223
14.3 Operation	223
14.4 Topology	226
14.5 Protocol Structure.....	228

Contents

14.5.1 Physical Layer.....	228
14.5.2 Data Link Layer.....	228
14.5.3 Application Layer	230
Chapter 15 ControlNet	233
15.1 Introduction	233
15.2 Features	233
15.3 Producer–Consumer Model.....	234
15.4 ControlNet Media.....	235
15.5 Physical Layer.....	236
15.6 Data Link Layer.....	236
15.7 Network and Transport Layers	240
15.8 Presentation Layer	242
15.9 Application Layer	242
Chapter 16 Intrinsically Safe Fieldbus Systems.....	245
16.1 Introduction	245
16.2 Hazardous Area	245
16.3 Hazardous Area Classification	246
16.3.1 Division Classification System	246
16.3.2 Zone Classification System.....	246
16.4 Explosion Protection Types	246
16.5 Intrinsic Safety in Fieldbus Systems.....	248
16.6 Entity Concept	249
16.7 FISCO Model	250
16.8 Redundant FISCO Model	252
16.9 Multidrop FISCO Model	253
16.10 HPTC Model	254
16.11 Dart Model	255
16.12 Performance Summary	258
16.13 Conclusion	258
Chapter 17 Wiring, Installation, and Commissioning	259
17.1 Introduction	259
17.2 HART Wiring.....	261
17.2.1 Surge Protection	262
17.2.2 Device Commissioning	262
17.3 Building a Fieldbus Network	263
17.3.1 Multifieldbus Devices	265
17.3.2 Expanding the Network	265

Contents

17.3.2.1 NICs	266
17.3.2.2 Hubs.....	266
17.3.2.3 Repeaters	267
17.3.2.4 Switches.....	268
17.3.2.5 Bridges.....	269
17.3.2.6 Routers.....	270
17.3.2.7 Gateways	271
17.3.2.8 Routers vs. Gateways.....	271
17.4 Powering Fieldbus Devices.....	272
17.5 Shielding.....	273
17.6 Cables	274
17.7 Number of Spurs and Devices per Segment	275
17.8 Polarity	277
17.9 Segment Voltage and Current Calculations.....	277
17.10 Linking Device.....	280
17.11 Device Coupler	281
17.12 Communication Signals.....	283
17.13 Device Commissioning	286
17.13.1 Foundation Fieldbus Device Commissioning	286
17.13.2 PROFIBUS-PA Fieldbus Device Commissioning	287
17.14 Host Commissioning	287
17.15 Wiring and Addressing via Ethernet and IP.....	288
17.16 Ethernet	288
17.16.1 IEEE Ethernet Standards	288
17.16.2 Topologies	291
17.17 IP Basics	291
17.18 IP Commissioning	292
17.18.1 Subnet.....	293
17.19 Manual IP Configuration.....	293
17.20 Automatic IP Configuration.....	293
Chapter 18 Wireless Communication	295
18.1 Introduction	295
18.2 Wireless Communication	295
18.2.1 Wired vs. Wireless.....	298
18.2.2 ISM Band.....	298
18.2.3 Wireless Standards	301
18.2.3.1 WiFi.....	302
18.2.3.2 WiMax.....	302

Contents

18.2.3.3 Bluetooth	303
18.2.3.4 ZigBee	305
18.2.3.5 WHART	305
18.2.3.6 ISA100.11a.....	306
18.2.4 Media Access.....	306
18.2.5 Topology	307
18.3 Wireless Sensor Networks.....	309
18.3.1 Coexistence Issues.....	309
18.3.2 WSNs in Industrial Networks.....	311
18.3.3 Benefits of Industrial WSNs	313
Chapter 19 WirelessHART	315
19.1 Introduction	315
19.2 Key Features	316
19.3 WHART Network Architecture	317
19.4 Protocol Stack.....	318
19.4.1 Physical Layer.....	318
19.4.2 Data Link Layer.....	319
19.4.3 Network Layer	322
19.4.4 Transport Layer	323
19.4.5 Application Layer	324
19.5 Network Components	324
19.5.1 Network Manager	325
19.5.2 Security Manager	326
19.5.3 Gateway	326
19.5.4 Adapter	327
19.6 Addressing Control.....	327
19.6.1 Sample Interval.....	327
19.6.2 Latency and Jitter	329
19.7 Coexistence Techniques	329
19.7.1 Channel Hopping	330
19.7.2 DSSS.....	331
19.7.3 Low Power Transmission.....	332
19.7.4 Blacklisting and Channel Assessment	332
19.7.5 Spatial Diversity	332
19.8 Time-Synchronized Mesh Protocol (TSMP).....	332
19.9 Security.....	333
19.9.1 OSI Layer-Based Security in HART and WHART	333
19.9.2 End-to-End Security	334
19.9.3 NPDU	335

Contents	
19.9.3.1 Security Control Byte	335
19.9.3.2 Message Integrity Code (MIC)	336
19.9.3.3 AES-CCM	336
19.9.3.4 AES-CCM–CBC-MAC	337
19.10 Security Threats	338
19.10.1 Interference	338
19.10.2 Jamming	339
19.10.3 Sybil Attack	339
19.10.4 Collusion	339
19.10.5 Tampering	340
19.10.6 Spoofing	340
19.10.7 Exhaustion	340
19.10.8 DOS	340
19.10.9 Traffic Analysis	341
19.10.10 Wormhole	341
19.10.11 Selective Forwarding Attack	341
19.10.12 Desynchronization	342
19.10.13 Security Threats at Different Protocol Layers	343
19.11 Redundancy	343
19.11.1 Redundancy in WSN	343
19.11.2 Redundancy at Network Access Points	344
19.11.3 Redundancy at Gateway, Network Manager, and Security Manager	344
19.12 Security Keys in WHART	345
19.12.1 Join Key	346
19.12.2 Session Keys	347
19.12.3 Network Key	347
19.12.4 Handheld Key	347
19.12.5 Well-Known Key	348
19.13 Key Management	348
19.13.1 Key Generation	348
19.13.2 Key Storage	348
19.13.3 Key Distribution	349
19.13.4 Key Renewal	349
19.13.5 Key Revocation	349
19.13.6 Key Vetting	350
19.13.7 Shortcomings	350
19.14 WHART Network Formation	351
19.15 HART and WHART—A Comparison	352
19.16 HART and WHART—Integration	353

Contents	
Chapter 20 ISA100.11a.....	355
20.1 Introduction	355
20.2 Scope of ISA100	355
20.3 ISA100 Working Group	356
20.4 Features	357
20.5 Sensor Classes	359
20.6 System Configuration	359
20.7 Convergence between ISA100.11a and WHART	360
20.8 NAMUR Proposal	360
20.9 Architecture	361
20.9.1 Differences with WHART	363
20.9.2 Routing Ability of Devices	363
20.9.3 Subnet	364
20.9.4 Provisioning Device	364
20.9.5 Backbone Routers	364
20.9.6 Device Management Data Flow	365
20.9.7 System Management Architecture	366
20.9.8 System Management Application Process	366
20.10 Comparison between ISA100.11a and WHART Protocol Stacks	367
20.11 Physical Layer	368
20.12 Data Link Layer	369
20.12.1 Protocol Data Unit	369
20.12.2 Coexistence Issues in DLL	370
20.12.2.1 TDMA	370
20.12.2.2 Collision Avoidance	373
20.12.2.3 Frequency Diversity	373
20.12.2.4 Spectrum Management	374
20.12.3 Routing in DLL	374
20.12.4 Neighborhood Discovery	375
20.12.5 DLL Characteristics	375
20.13 Network Layer	376
20.13.1 Functionality	376
20.13.2 Header Formats	377
20.13.2.1 Basic	377
20.13.2.2 Contract Enabled	377
20.13.2.3 Full IPv6	378
20.13.3 Summary of Header Differences	378
20.13.4 6LoWPAN	379
20.13.5 Data Flow between Two Subnets	379
20.14 Transport Layer	380
20.14.1 Protocol Data Unit	380

20.14.2 Security	380
20.14.3 Session and Contract.....	381
20.15 Application Layer	381
20.15.1 Structure.....	381
20.15.2 Protocol Data Unit	381
20.15.3 Communication Model	382
20.15.4 Objects, Their Addressing, and Merits ..	382
20.15.5 Gateway.....	384
20.15.5.1 Gateway Service Access Point..	384
20.16 Keys in ISA100.11a.....	384
20.16.1 Joining by Symmetric Key—A Comparison between ISA100.11a and WHART.....	385
20.16.1.1 Protection of Join Messages	386
20.16.1.2 Key Agreement and Distribution.....	388
20.16.2 Asymmetric Keys.....	389
20.16.2.1 Asymmetric Key-Based Join Process	389
20.16.2.2 Key Agreement and Distribution.....	389
20.16.2.3 Security Policy	390
20.17 Provisioning Overview	391
20.17.1 Different Keys.....	391
20.17.2 Configuration Bits	392
20.17.3 Provisioning Data Flow between PD and DBP	392
20.17.4 Requirement for Joining.....	392
20.17.5 Differences in Provisioning between ISA11.11a and WHART	392
20.18 Data Delivery Reliability.....	396
20.19 Two-Layer Security	397
20.20 Communications in ISA100.11a.....	397
20.21 ISA100.11a and WHART—A Comparison	401
20.22 Conclusion	401
References	403
Index	407