1 Ein kurzer Überblick ... 13

2 PROFIBUS ... 15
2.1 Protokollvarianten bei PROFIBUS ... 15
2.2 PROFIBUS DP ... 16
2.3 PROFIBUS FMS ... 16
2.4 PROFIBUS PA ... 17
2.5 PROFIBUS-Schichten ... 17
2.5.1 Bitübertragungsschicht – Schicht 1 ... 17
2.5.2 Fieldbus Data Link – Schicht 2 ... 19
2.5.3 Anwendungsschicht – Schicht 7 ... 20
2.6 Bustopologien ... 21
2.6.1 RS485 ... 21
2.6.2 LWL ... 22
2.6.3 IEC 1158-2 (PROFIBUS PA) ... 22
2.7 Buszugriffssteuerung ... 22
2.7.1 Token-Bus-Verfahren (Token-Passing) ... 23
2.7.2 Master-Slave-Verfahren ... 24
2.8 Die Zukunft von PROFIBUS ... 24

3 AS-Interface ... 26
3.1 Übertragungstechnik ... 26
3.2 Buszugriffsverfahren ... 27
3.3 Weitere AS-i-Varianten ... 27
3.3.1 ASIsafe ... 27
3.3.2 AS-i Power24V ... 28
3.4 Eckdaten und Projektierung ... 28

4 CAN-Bus ... 30
4.1 Übertragungstechnik ... 30
4.2 Buszugriffsverfahren ... 30
4.3 Eckdaten ... 31

Bibliografische Informationen
http://d-nb.info/1063373247

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

5 Ethernet ... 32
5.1 Definition ... 32
5.2 Geschichte ... 33
5.3 Paketaufbau ... 34
5.4 MAC-Adresse ... 37
5.5 Zugriffsmechanismen ... 38
5.6 Shared Ethernet ... 39
5.6.1 CSMA/CD ... 39
5.6.2 Kollisionsdomäne ... 41
5.6.3 Netzwerktopologie bei Ethernet ... 41
5.7 Fast-Ethernet ... 41
5.8 Switched Ethernet ... 42
5.8.1 Switch versus Hub ... 42
5.8.2 Simplex, Half-Duplex und Full-Duplex ... 43
5.9 Weitere Funktionalitäten für Ethernet ... 43
5.9.1 Autonegotiation ... 43
5.9.2 Autosensing ... 44
5.9.3 Autocrossover ... 44
5.9.4 Power-over-Ethernet (PoE) ... 44
5.10 Weiterentwicklungen bei Ethernet ... 44

6 TCP/IP ... 46
6.1 Internet-Protokoll (IP) – Vermittlungsschicht ... 47
6.1.1 IP-Paketaufbau ... 47
6.1.2 IP-Adresse ... 49
6.1.3 Net-ID und Host-ID bei IP-Adressen ... 51
6.1.4 Spezielle IP-Adressen ... 54
6.1.5 IP-Adressvergabe ... 55
6.1.6 IP-Routing ... 56
6.1.7 IPv6 – Nachfolger von IPv4 ... 58
6.1.8 Beispiel für eine Netzwerkberechnung mit IPv4 ... 59
6.2 Weitere Protokolle der Schicht 3 ... 61
6.2.1 ARP ... 61
6.2.2 ICMP ... 61
6.3 Transportschicht ... 62
6.3.1 TCP ... 62
6.3.2 UDP ... 67
6.4 TCP/IP – kompletter Frameaufbau ... 68

7 WLAN ... 70
7.1 Frequenzen und Datendurchsatz ... 70
7.2 Shared Medium ... 71
7.2.1 CSMA/CA ... 72
7.2.2 Hidden Station Problem ... 72
7.2.3 RTS/CTS ... 73
7.2.4 Exposed Station Problem ... 73
7.3 Grundlegende Begriffe im WLAN ... 74
7.4 Betriebsmodi und Verfahren im WLAN ... 76
7.4.1 Infrastructure Mode ... 76
7.4.2 Extended Service Set ... 77
7.4.3 Wireless Distribution System ... 77
7.4.4 Wireless Mesh Network (WMN) ... 78
7.4.5 Roaming ... 78
7.5 DCF und PCF ... 79
7.5.1 Distributed Coordination Function ... 79
7.5.2 Point Coordination Function ... 80
7.6 Industrial Point Coordination Function ... 80
7.6.1 iPCF-Zyklus ... 81
7.6.2 Rapid Roaming ... 81
7.6.3 Industrial Point Coordination Function - MC ... 82
7.7 Ausblick ... 83

8 Mechanismen zur Steigerung der Verfügbarkeit eines Netzwerks ... 84
8.1 STP/RSTP ... 84
8.2 MRP ... 85
8.3 PRP ... 85

9 PROFINET ... 87
9.1 Vertikale Kommunikation erfordert Ethernet ... 87
9.2 PROFINET – ein umfassender Industrial Ethernet Standard ... 87
9.2.1 Netzwerk-Installation ... 88
9.2.2 IT-Standards & Security ... 88
9.2.3 PROFINET IO – die Einbindung dezentraler Feldgeräte ... 89
9.2.4 PROFINET in der Prozessindustrie ... 89
9.2.5 Real-Time-Kommunikation ... 90
9.2.6 Motion Control ... 91
9.2.7 Safety mit PROFIsafe ... 91
9.2.8 Verteilte Intelligenz ... 91

9.3 Funktionsweise von PROFINET ... 92
9.3.1 PROFINET – ein voll geswitchtes Industrial Ethernet ... 92
9.3.2 Kommunikationsarten im PROFINET – zyklisch und azyklisch ... 93
9.3.3 Echtzeit-Kommunikationskanal – Layer-2-optimiert ... 93
9.3.4 Priorisierung von Real-Time-Daten über 802.1Q ... 94
9.3.5 PROFINET IRT – Isochrone Real-Time-Kommunikation ... 95
9.4 Konfiguration von PROFINET IO ... 97
9.4.1 Planung, Installation und Inbetriebnahme ... 97
9.4.2 Strukturen eines PROFINET-Netzwerks ... 98
9.4.3 Komponenten eines PROFINET-Netzwerks ... 99
9.4.4 IO-Device – Gerätenamen- und Adressvergabe ... 100
9.4.5 Wechselmedien ... 102
9.4.6 Sendetakt von IO-Controller und Aktualisierungszeit von IO-Device ... 103
9.4.7 Beispiel: Konfiguration eines PROFINET-IO-Netzwerks mit STEP 7 V5.6 ... 103
9.5 MRP – fehlertolerante Kommunikation im PROFINET ... 108
9.5.1 MRP – ein intelligentes Redundanzkonzept ... 108
9.5.2 MRP – Funktionsweise ... 109
9.5.3 Konfigurationsregeln ... 111
9.5.4 Beispiel: Konfiguration eines MRP-Rings mit STEP 7 V5.6 ... 111
9.5.5 Beispiel: Konfiguration eines MRP-Rings mit TIA Portal V15 ... 115
9.5.6 MRPD – stoßfreie Umschaltung im PROFINET ... 117
9.6 Shared Device – geteilte Ressourcen im PROFINET ... 121
9.6.1 Shared Device – eine geschickte und flexible Teilung ... 121
9.6.2 Beispiel: Konfiguration eines Shared Device mit STEP 7 V5.6 ... 122
9.6.3 Beispiel: Konfiguration eines Shared Device mit TIA Portal V15 ... 127
9.6.4 MSI/MSO – Modulinternes Shared Input/Shared Output ... 132
9.6.5 Beispiel: Konfiguration eines MSI/MSO mit TIA Portal V15 ... 133
9.7 I-Device – effiziente Kommunikation im PROFINET ... 135
9.7.1 Wirkungsweise ... 135
9.7.2 Beispiel: Konfiguration eines I-Device mit STEP 7 V5.6 ... 136
9.7.3 Transferbereiche anlegen und im Anwenderprogramm nutzen ... 137
9.7.4 Beispiel: Konfiguration eines I-Device mit TIA Portal V15 ... 141

10 Industrial Security ... 144
10.1 IT-Security versus Industrial Security: Was ist anders? ... 144
10.1.1 Unterschiedliche Anforderungen in IT- und ICS-Umfeld ... 145
10.1.2 Unterschiedliche Prioritäten in IT- und ICS-Umfeld ... 146
10.2 Trends, Standards, Normen und Gremien ... 147
10.2.1 Trends, die Industrial Security notwendig machen ... 147

10.2.2 Normierungsgremien ... 148
10.2.3 Die Normenreihe IEC 62443/EN 62443 ... 149
10.3 Angriffstechniken und Täterprofile ... 150
10.3.1 Viren ... 150
10.3.2 Würmer ... 150
10.3.3 Trojaner ... 151
10.3.4 Ransomware ... 151
10.3.5 Denial-of-Service ... 151
10.3.6 Man-in-the-Middle ... 153
10.3.7 Sniffing ... 153
10.3.8 Spoofing ... 153
10.3.9 Social Engineering ... 154
10.3.10 Hacking ... 154
10.3.11 Scriptkiddie ... 155
10.3.12 Cyberterrorismus ... 156
10.3.13 Insider-Angriffe ... 156
10.3.14 Industriespionage ... 156
10.3.15 Industrial Security – die aktuelle Situation ... 156
10.4 Defense in Depth ... 157
10.5 Anlagensicherheit ... 159
10.5.1 Physische Sicherheit: Zugangsschutz ... 159
10.5.2 Physische Sicherheit: Umwelt ... 161
10.5.3 Organisatorische Sicherheit ... 161
10.6 Netzwerksicherheit ... 163
10.6.1 Zellenschutzkonzept ... 163
10.6.2 Firewall ... 165
10.6.3 Zugriffsbeschränkung ... 168
10.6.4 NAT/NAPT – für Serienmaschinen oder Serviceanwendungen ... 172
10.6.5 VPN (Virtual Private Network) ... 175
10.7 Systemintegrität ... 186
10.7.1 Produkte mit Basis-Security-Funktionen ... 186
10.7.2 Zugriffsschutz und Know-how-Schutz ... 187
10.7.3 Passwörter ... 188
10.7.4 Sichere und unsichere Protokolle ... 190
10.7.5 Absicherung von WLAN-Netzwerken ... 192
10.7.6 Updates – Sicherheit nach aktueller Bedrohungslage ... 193
10.7.7 Scanner und Whitelisting ... 194
10.7.8 Virenscanner, Intrusion-Detection-Systeme und Deep Packet Inspection ... 195

11 Security-Beispielkonfigurationen mit dem TIA Portal V15 198
11.1 SCALANCE S zum Zellenschutz als NAT Firewall Router 198
11.2 SCALANCE S zum Zellen- und Zugriffsschutz als benutzerspezifischer Firewall-Router 206
11.3 SCALANCE S zum Zellen- und Zugriffsschutz als VPN-Endpunkt mit benutzerspezifischer Firewall 213

12 Industrielle Netzwerke und Komponenten 226
12.1 Die Gerätefamilie SCALANCE 226
12.1.1 SCALANCE M 226
12.1.2 SCALANCE W 227
12.1.3 SCALANCE X 228
12.1.4 SCALANCE S 231
12.2 Aufbau und Struktur industrieller Netzwerke 232

13 Ausblick: Auf dem Weg zur Digital Connectivity 237
13.1 Anforderungen an die Kommunikationsnetze 238
13.2 OPC Unified Architecture 239
13.3 Time-Sensitive Networking (TSN) 239
13.4 Digital Connectivity: Das industrielle Internet der Dinge 242

Stichwortverzeichnis 244