
SIEMENS
Ricarda Koch, Ralph Lüftner
Kommunikationsnetze in der Automatisierungs-technik
Bussysteme, Netzwerkdesign und Sicherheit im industriellen Umfeld

Koch / Lüftner Kommunikationsnetze in der Automatisierungstechnik

Kommunikationsnetze in der Automatisierungstechnik

Bussysteme, Netzwerkdesign und Sicherheit im industriellen Umfeld

Von Ricarda Koch und Ralph Lüftner

Publicis Pixelpark

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Dr. Gerhard Seitfudem, gerhard.seitfudem@publicispixelpark.de
www.publicis.de/books

Danke an Markus Weinländer für die Inhalte zu Kapitel 13.

Print ISBN 978-3-89578-441-5
ePDF ISBN 978-3-89578-971-7
EPUB ISBN 978-3-89578-738-6

Herausgeber: Siemens Aktiengesellschaft, Berlin und München
Verlag: Publicis Pixelpark, Erlangen

Printed in Germany

Geleitwort

Die Automatisierung der Industrie ist ein Schlüsselelement, das zu höherer Fertigungsqualität bei niedrigeren Kosten geführt hat, und damit auch einen Beitrag zu Wettbewerbsfähigkeit und Wohlstand leistet. Mit dem Siegeszug der Simatic-Steuerungen, die seit über 60 Jahren in Fertigungsbetrieben und Prozessanlagen rund um den Globus im Einsatz sind, hat Siemens immer wieder wesentliche Impulse zur Weiterentwicklung von Automatisierungs-Konzepten gegeben.

Dabei geht es längst nicht mehr um die reine Automatisierung – inzwischen steht die intelligente Vernetzung von Sensoren und Aktoren, Steuerungskomponenten und HMI-Geräten, IT-Systemen und Software-Applikationen im Vordergrund. Die Anforderungen unterscheiden sich jedoch wesentlich von der Vernetzung im Office-Bereich: Während es dort vor allem vertikale Datenströme zwischen Servern und Endgeräten gibt und die sogenannte User Experience im Vordergrund steht, geht es bei der Automatisierung vor allem um horizontale Kommunikation zwischen den Komponenten sowie um die maximale Verfügbarkeit. Denn eines ist klar: Anlagenstillstände können leicht etliche Tausende Euro und mehr kosten.

Es braucht deshalb spezielle technische Systeme für die Kommunikation, die den besonderen Anforderungen Rechnung tragen. Und es braucht Menschen, die in der Lage sind, solche Systeme auszulegen, zu betreiben und zu warten – einfach deshalb, um die maximale Höchstleistung auch im praktischen Einsatz zu erreichen. Ein fundiertes, technisches Verständnis für die Wirkungsweise der unterschiedlichen Technologien – von einfachen drahtgebundenen Sensor-Interfaces bis zu Industrial Wireless LAN für die Steuerung autonomer, mobiler Systeme – ist unverzichtbar.

Besonders wichtig ist aber die Sicherheit der Systeme gegen Hackerangriffe. Oftmals stehen neben der reinen Anlagenverfügbarkeit auch erhebliche immaterielle Vermögenswerte auf dem Spiel, zum Beispiel Rezepturen oder anderes geistiges Eigentum. Ein umfassendes Sicherheitskonzept muss deshalb von Beginn an bei der Konzeption eines industriellen Kommunikationsnetzwerks vorgesehen werden. Und auch hier braucht es Mitarbeiter, die verstehen, wie die Systeme funktionieren und was sie konkret leisten können.

Allerdings ist die Entwicklung mit den verfügbaren Techniken noch lange nicht abgeschlossen. Die Digitalisierung stellt neue Anforderungen auch an die industrielle Kommunikation. Neue Strukturen in den Netzen, neue Übertragungstechnologien wie TSN oder 5G und neue Protokolle wie OPC UA sind in der Entstehung oder erobern Schritt für Schritt die Fabrikhallen. Das entstehende Konzept – Digital Connectivity – wird die Fabrik der Zukunft nachhaltig verändern.

Ich freue mich, dass mit Ricarda Koch und Ralph Lüftner zwei engagierte Experten unseres Hauses alle notwendigen Informationen zur industriellen Kommunikation in diesem Buch zusammengetragen haben und mit hoher Praxisrelevanz erläutern. Damit ist die Grundlage geschaffen, die verfügbaren Technologien noch erfolgreicher in Maschinen und Anlagen einzusetzen, um Flexibilität und Produktivität gleichermaßen deutlich zu verbessern. Allen Lesern wünsche ich eine gewinnbringende Lektüre!

Nürnberg, im Juli 2019

Herbert Wegmann
General Manager, Siemens Industrial Communication & Identification

Inhaltsverzeichnis

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

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

1 Ein kurzer Überblick

„Kommunikationsnetze in der Automatisierungstechnik“ – möchte man alle Kommunikationsarten, -protokolle und -medien beschreiben, die in der Automatisierungstechnik eingesetzt wurden bzw. aktuell eingesetzt werden, würde das den Umfang dieses Buches bei weitem sprengen. Aus diesem Grund werden im Folgenden nur die wichtigsten und am weitesten verbreiteten Bussysteme und Protokolle vorgestellt. Das Buch soll als Einführung in diese Kommunikationsmechanismen und als Nachschlagewerk dienen.

Den Anfang macht PROFIBUS, eines der Urgesteine der Feldbusse. Für einen ersten Überblick gehen wir zunächst auf die verschiedenen Ausprägungen und deren Unterschiede in den Schichten des ISO/OSI-Modells ein. Dann folgen die möglichen Bustopologien und die Erläuterung der Buszugriffssteuerung bei PROFIBUS.

Als nächstes werden zwei weitere Feldbusse kurz vorgestellt, die in der Automatisierung nicht wegzudenken sind: der einfache und robuste AS-i-Bus für die schnelle Anbindung kleiner IO-Geräte und der Bus der Automobilindustrie, der CAN-Bus.

Der Fokus des Buchs liegt auf den Grundlagen und Themen rund um Ethernet, PROFINET und Industrial Security. Daher machen diese Kapitel den größten Teil des Buchs aus. Die Verbreitung von Ethernet begann in den 90er Jahren, und seitdem hat sich viel getan. Zahlreiche neue Standards wurden verabschiedet und so das Protokoll immer weiterentwickelt, um den steigenden Anforderungen durch den Einsatz sowohl im privaten, als auch im industriellen Umfeld gerecht zu werden.

Zunächst wird auf die Historie und die Eigenschaften von Ethernet eingegangen. Die Idee zum Ethernet hatte Robert M. Metcalf. Jeder Teilnehmer an einem Netzwerk sollte danach gleichberechtigt auf das Busmedium zugreifen können. Um dies möglich zu machen, brauchte man eine Adressierung und ein Buszugriffsverfahren. Diese grundlegenden Eigenschaften finden wir auch heute in jedem Protokoll wieder, das wir tagtäglich benutzen. Daher ist es wichtig, diese Grundlagen und Eigenschaften zu verstehen, wenn man Netzwerke aufbauen, planen, betreiben und diagnostizieren können will.

Um Kommunikation über größere Distanzen zu ermöglichen, wurde nicht zuletzt das Internet erfunden. Das Ethernet ist eher beschränkt hinsichtlich seiner Ausdehnung und der möglichen Teilnehmer. Die Verknüpfung von verschiedenen Ethernet-Netzwerken wurde also notwendig und damit eine weitere Adressierungsart und zahlreiche Protokolle. Definiert sind die Grundlagen in zahlreichen Standards rund um TCP/IP.

Die folgenden zwei Kapitel stellen jeweils einen kleinen Ausflug in die Themen dar und legen keinen Wert auf Vollständigkeit. Die WLAN-Technologie ist vielseitig und hat sich in den letzten Jahren ebenso rasant weiterentwickelt wie Ethernet, das Thema wird hier kurz beleuchtet. Auf die Darstellung der Eigenschaften der ver-

schiedenen Funkstandards und Mechanismen wird in diesem Buch verzichtet. Auch das Kapitel zu den Mechanismen zur Steigerung der Verfügbarkeit eines Netzwerks soll lediglich einen kurzen Überblick verschaffen.

PROFINET als umfassender Industrial Ethernet Standard ist das nächste große Thema des Buchs. Nach einem grundlegenden Überblick über den Standard werden die Funktionsweise und Mechanismen dieses echtzeitfähigen Protokolls erläutert, bevor wir auf verschiedene Details des PROFINET-Standards, wie MRP, Shared Device und I-Device näher eingehen. Zudem kann man anhand der Beispielkonfigurationen die Umsetzung kleiner PROFINET-Netzwerke nachvollziehen und diese Beispiele gegebenenfalls als Orientierung für erste eigene praxisnahe Schritte nutzen.

Ethernet hat sich sowohl im privaten, als auch im Office- und im industriellen Umfeld etabliert. Dass die Risiken und Gefahren der stetig wachsenden Vernetzung mit Ethernet ebenso in allen dessen Umfeldern wirken, ist in den letzten Jahren deutlich geworden. Da Security inzwischen in allen Anwendungsfeldern hochrelevant ist, widmet sich das folgende Kapitel ausführlich diesem Thema. Angefangen von den verschiedenen Anforderungen nach Verfügbarkeit und Sicherheit, über die Standards und Normen, wird auf die verschiedenen Angriffstechniken und Täterprofile eingegangen und letztendlich wird das Security-Konzept Defense in Depth beleuchtet. Auch zu diesem Thema stellen wir Beispielkonfigurationen vor, die als Einblick in die Konfiguration von Firewalls und VPNs dienen sollen.

Den Abschluss des Buches bildet ein Kapitel, das einige Netzwerkkomponenten von Siemens kurz vorstellt.

2 PROFIBUS

Im Zuge der zunehmenden Dezentralisierung bei Automatisierungslösungen bestand schon bald der Bedarf für ein serielles Feldbussystem, das herstellerübergreifend eingesetzt werden kann – also ein standardisiertes und offenes Feldbussystem. Ein solches System bietet durch reduzierten Kabelaufwand auch eine deutliche Kostenersparnis. Um dieses Ziel zu erreichen, wurde 1987 von der deutschen Industrie das Verbundprojekt „PROFIBUS“ initiiert. Die erarbeiteten Standards wurden dann in der DIN EN 19245 beschrieben. Der internationale Durchbruch von PROFIBUS erfolgte schließlich 1996, als die nationale Feldbusnorm zum internationalen Standard EN 50170 avancierte. Der Name PROFIBUS ist dabei eine Abkürzung aus PROcess FIeld BUS.

2.1 Protokollvarianten bei PROFIBUS

Bild 2.1 zeigt die Protokollarchitektur des PROFIBUS. Bei PROFIBUS sind die Schichten 1 und 2 sowie ggf. die Schicht 7 des ISO/OSI-Modells realisiert. Zur Festlegung der zu benutzenden Leitungen und der Übertragungsprotokolle wurden für die Schichten 1 und 2 zum einen der US-Standard EIA RS485, zum anderen die inter-

	PROFIBUS DP	PROFIBUS FMS	PROFIBUS PA
	Profile für DP-Geräte	Profile für FMS-Geräte	Profile für PA-Geräte
	Grundfunktionen Erweiterte Funktionen		Grundfunktionen Erweiterte Funktionen
	DP User Interface Direct Data Link Mapper (DDLM)	Application Layer Interface (ALI)	DP User Interface Direct Data Link Mapper (DDLM)
Schicht 7	↓	Anwendungsschicht Fieldbus Message Specification (FMS)	↓
Schicht 3 bis 6	↓	Nicht ausgeprägt!	↓
Schicht 2	Datenübertragungs-schicht Fieldbus Data Link (FDL)	Datenübertragungs-schicht Fieldbus Data Link (FDL)	IEC-Interface
Schicht 1	RS485 / LWL	RS485 / LWL	IEC 1158-2

Bild 2.1 Protokollarchitektur bei PROFIBUS

nationalen Normen IEC 870-5-1 und EN 60870-5-1 herangezogen. Die DIN 19241 (Teil 1-39) und die Norm IEC 955 beschreiben das Buszugriffsverfahren und die Datenübertragungs- und Managementdienste. Die Management-Funktionen orientieren sich an der ISO/IEC 498-4. Aus Anwendersicht unterscheidet PROFIBUS drei Protokollvarianten: DP, FMS und PA.

2.2 PROFIBUS DP

PROFIBUS DP nutzt die Schichten 1 und 2 sowie das User Interface. Die übrigen Schichten des OSI-Modells (3 bis 7) sind nicht ausgeprägt. Aufgrund dieser schlanken Architektur kann eine schnelle Datenübertragung erreicht werden. Der Zugang zur Schicht 2 ist der Direct Data Link Mapper (DDLM). Im User Interface sind die nutzbaren Anwendungsfunktionen und das System- und Geräteverhalten der unterschiedlichen Gerätetypen definiert.

Da diese Protokollvariante eine sehr schnelle Datenübertragung ermöglicht, wird sie speziell für die Kommunikation zwischen Automatisierungsgeräten und deren dezentralen Peripheriegeräten (Sensoren und Aktoren) eingesetzt. Daher auch der Name, das „DP“ steht für Dezentrale Peripherie.

2.3 PROFIBUS FMS

PROFIBUS FMS nutzt zusätzlich zu den Schichten 1 und 2 auch die Schicht 7. Die Anwendungsschicht besteht aus der FMS (Fieldbus Message Specification) und dem LLI (Lower Layer Interface). Da die FMS das Anwendungsprotokoll enthält, übernimmt sie die Aufgabe, die Kommunikationsdienste zur Verfügung zu stellen. Das LLI ist für die Realisierung der unterschiedlichen Kommunikationsbeziehungen zuständig, wie den Verbindungsauf- und -abbau sowie die Verbindungsüberwachung, und bildet deshalb für die FMS einen geräteunabhängigen Zugang zur Schicht 2.

FMS wird für den Datenaustausch innerhalb der Zellebene (PC und SPS) genutzt. Mit ihr kann man objektorientierten Datenaustausch betreiben. D. h. alle übertragenen Daten werden herstellunabhängig mit genormten Kommunikationsobjekten übertragen. Die Übertragung der Daten erfolgt hierbei in geräteneutralen Strukturen. Im Endgerät werden diese dann wieder in die gerätespezifische Form konvertiert.

Da PROFIBUS DP und PROFIBUS FMS die gleiche Übertragungstechnik und ein einheitliches Buszugriffsverfahren verwenden, können beide Protokolle parallel auf demselben Kabel betrieben werden.

2.4 PROFIBUS PA

PROFIBUS PA nutzt zur Datenübertragung das erweiterte PROFIBUS DP-Protokoll. Zusätzlich verwendet es das PA-Profil, in dem das Geräteverhalten der Feldgeräte definiert wird. Durch Nutzung der Übertragungstechnik laut IEC 1158-2 kann bei PROFIBUS PA die Eigensicherheit und die Energieversorgung der Feldgeräte über den Bus ermöglicht werden. Mit Hilfe von Segmentkopplern können PROFIBUS PA-Geräte einfach in ein PROFIBUS DP-Netz integriert werden.

Aufgrund der genannten Eigenschaften ist PROFIBUS PA speziell für den Bereich der Prozessautomatisierung geeignet, daher der Name „PA“. Außerdem erlaubt es (auch in explosionsgefährdeten Bereichen) die Anbindung von Sensoren und Aktoren an eine gemeinsame Feldbusleitung.

2.5 PROFIBUS-Schichten

2.5.1 Bitübertragungsschicht – Schicht 1

... für DP/FMS (RS485)

Eine geschirmte und verdrillte 2-Draht-Leitung genügt der Schicht 1 des PROFIBUS zur symmetrischen Datenübertragung gemäß EIA RS485. Diese wird, je nach Profilausprägung, auch als H1 bzw. H2 bezeichnet. Die Übertragungsgeschwindigkeit liegt im Bereich von 9,6 kBit/s bis 12 MBit/s. Alle Geräte am Bus müssen dann die in diesem Bereich gewählte Baudrate benutzen.

Das RS485-Übertragungsverfahren des PROFIBUS basiert auf einer halbduplex, asynchronen, schlupffesten Synchronisierung. Die Daten werden dabei im NRZ-Code übertragen. NRZ steht für „Non Return to Zero“ und bedeutet, dass sich der Signalverlauf von Binär „0“ nach „1“ während der Bitübertragungsdauer nicht ändert (Bild 2.2).

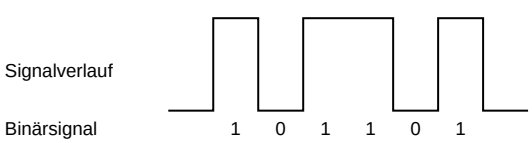

Bild 2.2 Signalverlauf bei NRZ

Anders als bei dem weiterentwickelten RZ-Code (Return-to-Zero) werden beim NRZ-Code Binärwerte mit zwei statt drei Pegelwerten über ein Medium übertragen, was bei einer längeren Folge von gesendeten „0“en oder „1“en zu keiner Pegeländerung führt. Ein Empfänger kann für diesen Zeitraum daher keinen Takt aus dem Signal zurückgewinnen.

Die maximal zulässige Leitungslänge eines PROFIBUS-Systems hängt direkt von der gewählten Baudrate ab (Tabelle 2.1). Innerhalb eines Segments dürfen 32 Teilnehmer betrieben werden.

Tabelle 2.1 PROFIBUS-Segmentlänge für unterschiedliche Baudraten

Baudrate (kbit/s)	9,6 19,2 45,45 93,75	187,5	500	1500	3000 6000 12000
Segmentlänge (m)	1200	1000	400	200	100

... für DP/FMS (LWL)

Eine weitere Übertragungsmöglichkeit auf Schicht 1 stellt die Verwendung von Lichtwellenleitern dar. Diese ist in der Richtlinie der PI (PROFIBUS & PROFINET International; regionale Gesellschaft in Deutschland: früher PNO = PROFIBUS Nutzer Organisation) „Optische Übertragungstechnik für PROFIBUS“ beschrieben. Durch den Einsatz von Lichtwellenleitern kann eine Ausdehnung der Segmentlänge von bis zu 15 km erreicht werden. Ein weiterer Vorteil der LWL-Technik ist, dass sie immun gegen elektromagnetische Störungen ist. Auch stellt die Verwendung von Lichtwellenleitern immer eine Potentialtrennung zwischen einzelnen Busteilnehmern sicher.

... für PA

Bei PROFIBUS PA wird die Schicht 1 durch die IEC 1158-2 festgelegt. Diese Technik ermöglicht die Eigensicherheit der Feldgeräte und deren Spannungsversorgung direkt über die Busleitung. In der PA-Variante verwendet man zur Datenübertragung ein bitsynchrones und manchestercodiertes Leitungsprotokoll mit gleichstromfreier Übertragung (oft auch H1 genannt). Die manchestercodierte Datenübertragung definiert für eine binäre „0“ den Flankenwechsel von „0“ nach „1“. Analog dazu wird die binäre „1“ als Flankenwechsel von „1“ nach „0“ dargestellt (Bild 2.3). Die Übertragungsgeschwindigkeit bei PROFIBUS PA ist auf 31,25 kBit/s fest eingestellt. Die Anzahl der maximalen Busteilnehmer innerhalb eines PA-Segments beträgt 32.

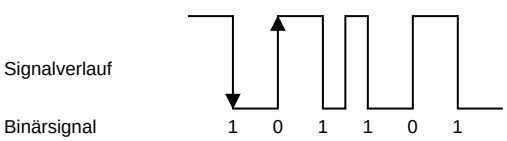

Bild 2.3 Datenübertragung (Manchester-II-Code)

2.5.2 Fieldbus Data Link – Schicht 2

Aufgabe der Schicht 2 im ISO/OSI-Modell ist die Buszugriffssteuerung, die Datensicherung und die Abwicklung der Übertragungsprotokolle und Telegramme. Bei PROFIBUS wird die Schicht 2 als FDL-Schicht (Fieldbus Data Link) bezeichnet.

Eine große Übertragungssicherheit wird durch die Telegrammformate der Schicht 2 erreicht. Dabei können bis zu drei gleichzeitig verfälschte Bits im Datentelegramm erkannt werden. Dies erfolgt durch die Verwendung von speziellen Start- und Endezeichen der Telegramme, durch eine schlupffeste Synchronisierung, Paritätsbit und Kontrollbyte, wie es in der IEC 870-5-1 beschrieben ist.

Folgende Fehler können erkannt werden:

- Zeichenformatfehler (Parität, Overrun, Framing-Error)
- Protokoll-Fehler
- Start- und End-Delimiter-Fehler
- Frame-Check-Byte-Fehler
- Telegrammlängen-Fehler

Sollte bei einem Telegramm ein solcher Fehler erkannt werden, wird dieses mindestens einmal wiederholt. Die Anzahl der Wiederholungen kann in der Schicht 2 anhand des Busparameters „Retry“ auf bis zu 8 Wiederholungen eingestellt werden.

Neben einer logischen Punkt-zu-Punkt-Datenübertragung ermöglicht die Schicht 2 auch eine Punkt-zu-Mehrpunkt-Übertragung (Point to Multipoint):

- Bei einer Broadcast-Kommunikation sendet ein aktiver Teilnehmer eine Nachricht an alle anderen Netzteilnehmer, wobei der Empfang der Nachricht nicht quittiert wird.
- Bei einer Multicast-Kommunikation sendet ein aktiver Netzwerkteilnehmer eine Nachricht an eine Gruppe von Empfängern. Auch hierbei erfolgt keine Quittierung der Nachricht.

Die in Schicht 2 verfügbaren Datendienste sind in Tabelle 2.2 aufgezeigt.

Tabelle 2.2 Verfügbare Datendienste in Schicht 2

Dienst	Funktion	DP	PA	FMS
SDA	Send Data with Acknowledge			×
SRD	Send and Request Data with reply	×	×	×
SDN	Send Data with No acknowledge	×	×	×
CSRD	Cyclic Send and Request Data wih reply			×

Die Dienste werden über die Dienstzugangspunkte (SAP, Service Access Points) der Schicht 2 von den übergeordneten Schichten aufgerufen. PROFIBUS FMS nutzt die SAPs zur Adressierung der logischen Kommunikationsverbindungen. Im Gegensatz dazu ist bei PROFIBUS PA bzw. DP jedem SAP eine genau festgelegte Funktion

zugeordnet. Die Teilnehmer einer Kommunikation können mehrere SAPs parallel verwenden. Dabei wird unterschieden zwischen Quell-Dienstzugangspunkt (SSAP = Source Service Access Point) und Ziel-Dienstzugangspunkt (DSAP = Destination Service Access Point).

2.5.3 Anwendungsschicht – Schicht 7

Durch die Schicht 7 werden die nutzbaren Kommunikationsdienste zur Verfügung gestellt. Bei PROFIBUS FMS besteht die Schicht 7 aus der FMS (Fieldbus Message Specification) und der LLI-Schnittstelle (Lower Layer Interface).

Um sicherzustellen, dass Geräte herstellerübergreifend dieselben Kommunikationsfunktionen bereitstellen, wurden durch die PI folgende FMS-Profile definiert:

- Kommunikation zwischen Controllern (3.002)
- Profil für Gebäudeautomation (3.011)
- Niederspannungsschaltgeräte (3.032)

Bei PROFIBUS DP wird die Schicht 7 nicht verwendet, DP nutzt lediglich Schicht 1 und Schicht 2. Die jeweils nutzbaren Funktionen sowie das System- und Geräteverhalten der unterschiedlichen DP-Gerätetypen werden durch das User Interface festgelegt.

Das PROFIBUS DP-Protokoll definiert nur, wie die Nutzdaten zwischen Partnern im Netz über den Bus übertragen werden. Die Bedeutung der übertragenen Nutzdaten wird hingegen durch die verwendeten DP-Profile festgelegt. In Tabelle 2.3 sind die verfügbaren PROFIBUS-Profile aufgelistet.

Tabelle 2.3 PROFIBUS-Profile

Profil	Inhalt	Nr.
Dosing / Weighing	Wäge- und Dosiersysteme	3.182a, 3.182 b, 3.182c
Encoder	Dreh-, Winkel- und Linear-Encoder	3.162
Fluid Power	Hydraulische Antriebe	3.112
HART on PROFIBUS	HART-Geräte	3.102
Ident Systems	Barcode-Leser, Transponder	3.142
LabDevices	Laborgeräte	2.412
Liquid Pumps	Flüssigkeitspumpen	2.422
Low Voltage Switchgear	Niederspannungsschaltgeräte	3.122
PA Devices	Geräte der Prozesstechnik	3.042
PROFIdrive	Drehzahlveränderbare elektrische Antriebe	3.172, 3.272
Remote I/O für die PA	Remote I/O-Geräte in der Prozessautomatisierung	3.132

Profil	Inhalt	Nr.
Remote I/O für die FA	Remote I/O-Geräte in der Fabrikautomatisierung	3.242
Robot / Numerical Controls	Roboter- und Positioniersteuerungen, Numerische Steuerungen	3.052
SEMI	Halbleiterherstellung	3.152
Identification & Maintenance	Identifikation und Internet-Zugriff auf gerätespezifische Informationen	3.502
IPar-Server	Gerätetausch	3.532
PROFIsafe	Sicherheitsgerichtete Geräte	3.192
Redundancy	Geräte mit redundanter Kommunikation	2.212
Time Stamp	Zeitgenaue Zuordnung bestimmter Ereignisse	3.522
Data Types	Datentyp-Definitionen, Programmiersprachen und Plattform-Aspekte	3.512
Diagnosis	Diagnose	3.522
Host Application	Host-Funktionen gegenüber Engineeringsystem	3.902

2.6 Bustopologien

Je nach Übertragungstechnik können bei PROFIBUS unterschiedliche Topologien (also Anordnungen der Leitungen und Geräte) realisiert werden. Im Folgenden sind die Übertragungstechniken und die entsprechenden Eigenschaften kurz aufgeführt.

2.6.1 RS485

Aus topologischer Sicht handelt es sich bei einem PROFIBUS-System um eine beidseitig aktiv abgeschlossene Linien-Busstruktur, auch als RS485-Bussegment bezeichnet. Pro Segment können 32 Teilnehmer angeschlossen werden.

Um die Anzahl der Teilnehmer zu erhöhen, müssen mehrere Bussegmente miteinander verschaltet werden. Zu deren Kopplung verwendet man Repeater (Leitungsverstärker). Dabei zählt jeder Repeater auch immer als eigenständiger Teilnehmer im Segment. Die Anzahl der Repeater, die man in Reihe schalten darf, ist abhängig vom Hersteller. Dies gilt auch für das Ausmaß der Erweiterung der Gesamtausdehnung.

Durch den Einsatz von Repeatern lassen sich so neben der Linien-Busstruktur auch Baum- und Sternstrukturen realisieren.

2.6.2 LWL

Größere Entfernungen können abhängig von der Übertragungsgeschwindigkeit mit Lichtwellenleitern (LWL) überbrückt werden. LWL-Leitungen sollten ebenfalls zum Einsatz kommen, wenn extreme EMV-Belastungen auf der Übertragungsstrecke auf die Datenleitungen einwirken, um so Störungen und Datenverlusten entgegenzuwirken.

Zusätzlich zu den schon bekannten Topologien (siehe Kapitel 2.6.1 „RS485“) ermöglicht die LWL-Technik den Aufbau von Ringstrukturen. Ringe sind eine Sonderform der Linien-Busstruktur, die eine hohe Verfügbarkeit des Netzes ermöglichen.

Wird eine LWL-Unterbrechung zwischen zwei Geräten im Ring erkannt, wird das Netz zu einer optischen Linie umkonfiguriert, so dass das gesamte Netz verfügbar bleibt. Fällt ein Gerät aus, so sind lediglich die an dieses Gerät direkt angeschlossenen Endgeräte nicht mehr verfügbar, der Rest des Netzes bleibt als Linienstruktur funktionsfähig.

Durch den Einsatz entsprechender Geräte können sowohl optische Einfaserringe als auch redundante Zweifaserringe realisiert werden. Bei Zweifaserringen ist zusätzlich eine Leitungsredundanz verfügbar, da hier die Punkt-zu-Punkt-Verbindungen zwischen zwei Geräten im Ring redundant ausgelegt werden.

2.6.3 IEC 1158-2 (PROFIBUS PA)

Auch bei PROFIBUS PA lassen sich Linien-, Baum- und Sternstrukturen realisieren, ebenso ist es möglich, einzelne Bussegmente redundant auszuführen. Dabei hängt die Anzahl der am Netz betreibbaren Busteilnehmer ab von der verwendeten Spannungsversorgung, der Stromaufnahme der einzelnen Busteilnehmer, den eingesetzten Buskabeln und der Ausdehnung des Bussystems. Wie bei DP gilt auch hier, dass je Bussegment maximal 32 Teilnehmer eingebunden werden dürfen. Die Kopplung zwischen PA und DP erfolgt über entsprechende Segmentkoppler und DP/PA-Links.

2.7 Buszugriffssteuerung

Es gibt zwei wesentliche Anforderungen aus der Verfahrens- und Fertigungstechnik an einen Feldbus bezüglich der Buszugriffsteuerung. Zum einen soll für die Kommunikation zwischen gleichberechtigten Automatisierungssystemen bzw. PCs sichergestellt werden, dass jeder Teilnehmer eines Netzwerks innerhalb eines definierten Zeitraums genügend Zeit erhält, um seine Kommunikationsaufgaben zu erfüllen. Zum anderen benötigt man einen schnellen Datenaustausch zwischen der dezentralen Prozessperipherie und dem zugehörigen Automatisierungssystem bzw. dem zugehörigen PC, und die Kommunikation soll mit einem geringen Protokollaufwand durchführbar sein.

PROFIBUS erfüllt diese Aufgaben durch seine hybrid aufgebaute Buszugriffssteuerung. Diese besteht aus zwei Teilen. Da ist auf der einen Seite ein dezentrales Token-Passing-Verfahren, das zwischen den aktiven Busteilnehmern, Master ge-

nannt, für die Zugriffssteuerung sorgt. Auf der anderen Seite gibt es dann noch ein zentrales Master-Slave-Verfahren, das den Datenaustausch zwischen den aktiven und den passiven Busteilnehmern regelt.

Mehrere Master in einem Netzwerk geben sich in einem Netzwerk nacheinander in der Reihenfolge der Teilnehmeradressen die Sendeberechtigung mit einem speziellen Telegramm, das Token genannt wird. Sobald ein aktiver Teilnehmer den Token erhält, übernimmt er die Rolle des Masters am Bus, und zwar solange er im Besitz des Tokens ist. Während dieser Zeit kommuniziert er mit anderen aktiven und passiven Teilnehmern. Eine Teilnehmeradressierung sorgt hierbei dafür, dass einzelne Geräte diskret angesprochen werden können. Jedem PROFIBUS-Teilnehmer muss innerhalb eines Bussystems eine busweit eindeutige Adresse zugewiesen sein. Der maximal nutzbare Adressbereich bei PROFIBUS geht von 0 bis 126. Somit ist klar, dass die maximale Teilnehmerzahl innerhalb eines Bussystems 127 beträgt.

Folgende Systemkonfigurationen sind innerhalb eines PROFIBUS-Netzwerks umsetzbar:

- Reines Master-Master-System (Token-Passing)
- Reines Master-Slave-System (Master-Slave)
- Kombination von Token-Passing und Master-Slave (Bild 2.4)

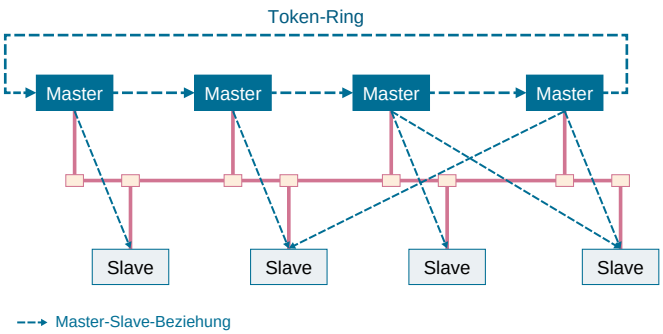

Bild 2.4 Kombination von Token-Passing und Master-Slave-Zugriffsverfahren

Dabei ist anzumerken, dass das Buszugriffsverfahren bei PROFIBUS unabhängig vom verwendeten Übertragungsmedium ist.

2.7.1 Token-Bus-Verfahren (Token-Passing)

Durch die aktiven Teilnehmer am PROFIBUS wird in numerisch aufsteigender Reihenfolge der Teilnehmeradressen ein logischer Token-Ring gebildet. Ein Token-Ring ist dabei eine organisatorische Aneinanderreihung von aktiven Busteilnehmern, die nach Ablauf einer einstellbaren Zeit das Token immer an die nächsthöhere Adresse weiterreichen. Dies geschieht mit speziellen Token-Telegrammen. Ist das Token beim Teilnehmer mit der höchsten Teilnehmeradresse im Ring, der

HSA (Highest Station Address), angelangt, gibt dieser das Token nach Zeitablauf an die Station mit der niedrigsten Adresse, der LSA (Lowest Station Address), weiter.

Die Zeit für einen Umlauf des Tokens wird auch als Token-Umlaufzeit bezeichnet. Bei der Projektierung eines Token-Rings wird die Token-Soll-Umlaufzeit TTRT (Target Token Rotation Time) als maximal erlaubte Zeit für einen Token-Umlauf definiert.

Die Buszugriffssteuerung der aktiven Teilnehmer richtet während der Initialisierungs- und Hochlaufphase den Token-Ring ein. Dazu ermittelt die Buszugriffssteuerung für die Tokenverwaltung selbstständig alle Adressen der aktiven Busteilnehmer. Jeder aktive Teilnehmer legt sich eine Tabelle mit diesen Adressen an. Diese Tabelle nennt man LAS (List of Active Stations). Zusätzlich trägt der Teilnehmer auch immer seine eigene Adresse ein. In dieser Tabelle gibt es zwei besonders wichtige Adressen:

- *PS (Previous Station)*
  Adresse der direkten Vorgängerstation, von der das Token empfangen wird
- *NS (Next Station)*
  Adresse der direkten Nachfolgestation, an die das Token weitergegeben wird

Ein weiterer Zweck der LAS ist es, während des Betriebs ausgefallene bzw. defekte aktive Teilnehmer aus dem Ring auszutragen oder auch neu hinzukommende Teilnehmer aufzunehmen, ohne dass es zu Störungen beim laufenden Datenaustausch kommt.

2.7.2 Master-Slave-Verfahren

Gibt es in einem Token-Ring nur einen aktiven Teilnehmer, aber mehrere passive Teilnehmer, spricht man von einem reinen Master-Slave-System.

Erhält ein Master beim Master-Slave-Verfahren den Token, kann er die Slaves (passive Teilnehmer) ansprechen, die ihm, dem Master, zugeordnet sind. Dabei geht die Kommunikation immer vom Master aus, er sendet Nachrichten an den bzw. die Slaves bzw. holt Daten von dem bzw. den Slaves ab. Man spricht hierbei auch von „Polling“.

Eine Standard-PROFIBUS DP-Buskonfiguration setzt typischerweise auf diesem Buszugriffsverfahren auf. Ein DP-Master (aktive Station) pollt in zyklischer Reihenfolge von den DP-Slaves (passive Stationen) die Daten.

2.8 Die Zukunft von PROFIBUS

Wie geht es weiter mit PROFIBUS? Seit Jahren ist immer wieder zu hören, dass Industrial Ethernet die Zukunft ist und PROFIBUS aussterben wird. Dieser Trend ist zwar sichtbar, jedoch ist der robuste PROFIBUS-Feldbus aus den industriellen Netzwerken noch längst nicht wegzudenken. Das wird auch dadurch verdeutlicht, dass in den letzten Jahren konstant ca. 150 Zertifikate jährlich durch die PI für PROFIBUS-Geräte vergeben wurden.

Mit dem Einfluss von Industrie 4.0 steigt zwar kontinuierlich die Zahl der zertifizierten PROFINET-Geräte (2016 über 500), und auch der Vormarsch von OPC UA und TSN wird eine Rolle beim Wandel der Netzwerkstrukturen haben. Wann allerdings Lösungen, wie sie bereits heute bei PROFIBUS bewährt sind, durch andere Busstrukturen und Techniken abgelöst werden, bleibt weiterhin abzuwarten.