西门子PLC通信网络解决方案及工程应用实例

XIMENZI PLC TONGXIN
WANGLUO JIEJUE FANGAN JI GONGCHENG YINGYONG SHILI

周志敏　纪爱华　等编著

机械工业出版社
CHINA MACHINE PRESS

西门子 PLC 通信网络解决方案及工程应用实例

周志敏　纪爱华　等编著

机 械 工 业 出 版 社

本书结合西门子 PLC 及 PROFIBUS 现场总线在国内的工程应用实践，全面系统地阐述了由西门子 PLC 构建的自动化控制系统的通信网络解决方案及工程应用实例。全书共分 5 章，在概述西门子 PLC 及 PROFIBUS 现场总线的基础上，系统地阐述了西门子 PLC 通信技术、西门子 PLC 基于 PROFIBUS 构成的控制系统、西门子 PLC 与变频器通信实例、西门子 PLC 基于现场总线的系统配置与组态实例等内容。本书在写作上把西门子 PLC 与 PROFIBUS 的基础理论知识与工程应用有机地结合，深入浅出地阐述了西门子 PLC 通信网络的解决方案及工程应用实例。

全书文字通俗易懂，重点突出，内容新颖实用，可供从事 PLC 控制系统通信网络设计及工程应用的工程技术人员和高等院校及职业技术学院的师生阅读参考。

图书在版编目（CIP）数据

西门子 PLC 通信网络解决方案及工程应用实例/周志敏等编著. —北京：机械工业出版社，2014.3

ISBN 978-7-111-46009-1

Ⅰ.①西… Ⅱ.①周… Ⅲ.①plc 技术-应用-通信网 Ⅳ.①TM571.6 ②TN915

中国版本图书馆 CIP 数据核字（2014）第 036580 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：林春泉 责任编辑：翟天睿 版式设计：常天培

责任校对：陈立辉 封面设计：路恩中 责任印制：李 洋

北京市四季青双青印刷厂印刷

2014 年 5 月第 1 版第 1 次印刷

184mm × 260mm · 13.25 印张 · 323 千字

标准书号：ISBN 978-7-111-46009-1

定价：39.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务 网络服务

社 服 务 中 心：（010）88361066 教 材 网：http://www.cmpedu.com

销 售 一 部：（010）68326294 机工官网：http://www.cmpbook.com

销 售 二 部：（010）88379649 机工官博：http://weibo.com/cmp1952

读者购书热线：（010）88379203 **封面无防伪标均为盗版**

前　言

近年来，随着工业自动化产业的高速发展，PLC 得以广泛应用。PLC 已成为工业自动化控制系统中的重要组成部分，其性能的优劣直接关系到整个控制系统的安全性和可靠性指标。随着信息技术的高速发展，工业自动化控制系统的结构已发生了深刻变革，信息交换的范围正从工厂的管理、控制迅速覆盖到现场设备的各个层次，并逐步形成了分布式网络集成自动化控制系统和以此为基础的企业信息化系统。

PROFIBUS 现场总线是顺应信息技术的发展趋势和工业控制系统的分散化、网络化、智能化要求而发展起来的新技术，目前，PROFIBUS 现场总线已成为自动化技术发展的驱动力，PROFIBUS 现场总线技术融合 PLC、DCS 技术构成的全集成自动化系统以及信息网络技术将是 21 世纪自动化技术发展的主流。为此，学习 PLC 通信网络技术是将 PLC 应用到自动化控制工程实践中所必须掌握的理论基础，同时也是保证由 PLC 构成的自动化控制系统具有高性能比和最佳性能指标的技术基础，还是确保 PLC 控制系统安全稳定运行所必需的。

本书在概述西门子 PLC 及 PROFIBUS 现场总线的基础上，系统地介绍由西门子 PLC 构建的自动化控制系统的通信网络配置及工程设计实例。本书在写作上尽量做到有针对性和实用性，力求做到通俗易懂和结合实际，使得从事西门子 PLC 控制系统通信网络配置及工程应用的工程技术人员从中获益，读者可以此为“桥梁”，系统全面地了解和掌握 PLC 控制系统网络配置和最新工程应用技术。

参加本书编写工作的有周志敏、纪爱华、周纪海、纪达奇、刘建秀、顾发娥、刘淑芬、纪和平、纪达安、陈爱华等，本书在写作过程中无论从资料的收集和技术信息交流上都得到了国内专业学者和同行及 PLC 生产厂商的大力支持，在此表示衷心的感谢。

由于时间短，水平有限，难免有错误之处，敬请读者批评指正。

编　者

目　录

前言

第 1 章　概述 …… 1

1.1　西门子 PLC 发展及产品区别 …… 1

1.1.1　西门子 PLC 发展历程及产品 …… 1

1.1.2　西门子 S7-200 与 S7-300/400 系列 PLC 的区别 …… 4

1.2　PROFIBUS 现场总线 …… 5

1.2.1　PROFIBUS 现场总线的发展与优点 … 5

1.2.2　PROFIBUS-DP 特性及规范 …… 12

1.2.3　PROFIBUS-FMS 特性及规范 …… 19

1.2.4　PROFIBUS-PA 特性及规范 …… 21

第 2 章　西门子 PLC 通信技术 …… 37

2.1　工业自动化通信技术 …… 37

2.1.1　工业通信系统 …… 37

2.1.2　通信互联技术 …… 39

2.1.3　PROFIBUS 传输技术 …… 45

2.2　PROFIBUS-DP 通信协议及行规 …… 52

2.2.1　PROFIBUS-DP 通信协议 …… 52

2.2.2　应用行规及特殊行规 …… 59

第 3 章　西门子 PLC 基于 PROFIBUS 构成的控制系统 …… 66

3.1　PROFIBUS 控制系统层次及配置 …… 66

3.1.1　PROFIBUS 控制系统层次及组成 …… 66

3.1.2　PROFIBUS 控制系统配置形式 …… 71

3.2　PROFIBUS 控制系统的设计 …… 78

3.2.1　PROFIBUS 单主站控制系统 …… 78

3.2.2　PROFIBUS-DP 主从控制系统 …… 84

3.2.3　PROFIBUS 控制系统设计实例 …… 90

3.2.4　在 STEP7 中组态 PROFINET 接口 … 97

第 4 章　西门子 PLC 与变频器通信实例 …… 104

实例 1　西门子 PLC 与三菱 FR 系列变频器通信 …… 104

实例 2　西门子 PLC 与 ACS800 变频器通信 …… 110

实例 3　西门子 PLC 与 Master 系列变频器通信 …… 115

实例 4　西门子 S7-300/400 系列 PLC 与 6SE70 变频器通信 …… 117

实例 5　西门子 S7-200 系列 PLC 基于 MODBUS 与 ABB 变频器通信 …… 121

实例 6　西门子 S7-300 系列 PLC 基于 PROFIBUS-DP 与 ABB 变频器通信 …… 127

实例 7　西门子 PLC 基于 TDS-PA01 与艾默生变频器通信 …… 131

实例 8　西门子 PLC 与收获变频器通信 …… 134

实例 9　西门子 PLC 与台达 C2000 系列变频器通信 …… 140

第 5 章　西门子 PLC 基于现场总线的系统配置与组态实例 …… 143

实例 1　CP342-5 作从站与 FC1（DP_SEND）、FC2（DP_RECV）的配置 …… 143

实例 2　CP342-5 作主站与 FC1（DP_SEND）、FC2（DP_RECV）的配置 …… 147

实例 3　PB-OEM4-PCI 作从站与 PROFIBUS 主站的连接与配置 …… 150

实例 4　S7-400 作主站基于 PROFIBUS-DP 连接 ET200M 的配置 …… 156

实例 5　S7-400 作主站基于 PROFIBUS 连接智能从站配置 …… 159

实例 6　PLC-PLC 之间基于 PROFIBUS 的通信配置 …… 168

实例 7　基于 PROFIBUS 建立 OPC 服务器与 S7PLC 的连接 …… 186

实例 8　主站与主站之间基于 PROFIBUS 的 FDL 通信配置 …… 199

参考文献 …… 206

第1章 概 述

1.1 西门子 PLC 发展及产品区别

1.1.1 西门子 PLC 发展历程及产品

1. 西门子 PLC 产品发展历程

德国西门子（SIEMENS）公司是欧洲最大的电子和电气设备制造商，SIMATIC 是西门子自动化系列产品品牌的统称，诞生于 1958 年，至今已有 50 多年的历史，涵盖了从 PLC、工业软件到 HMI，是全球自动化领导品牌。50 多年来，SIMATIC 的 PLC 系列产品从 S3 系列发展到 S7 系列，已经成为我国自动化用户最为信赖和熟知的品牌。西门子公司生产的 PLC 在我国的应用相当广泛，在冶金、化工、印刷等领域都有广泛的应用。西门子的 PLC 系列产品发展历程如下：

1）西门子公司的 PLC 产品 S3 系列是在 1975 年投放市场的，它实际上是带有简单操作接口的二进制控制器。

2）在 1979 年微处理器技术被应用到 PLC 中，研发出 S5 系列取代了 S3 系列，该系列产品广泛地使用了微处理器技术。

3）20 世纪 80 年代初，S5 系统进一步升级为 U 系列 PLC，较常用的机型有 S5-90U、95U、100U、115U、135U、155U。

4）S7 系列诞生于 1994 年 4 月，它具有更国际化、更高性能等级、安装空间更小、更良好的 Windows 用户界面等优势，其机型为 S7-200、300、400、1200。

西门子公司的 PLC 产品由最初的 S3 发展到如今的 S7，目前，S3、S5 系列 PLC 已逐步退出市场，停止生产，而 S7 系列 PLC 现已成为了西门子自动化系统的控制核心，TDC 系统沿用 SIMADYND 技术内核，是对 S7 系列产品的进一步升级，它是西门子自动化系统最尖端、功能最强的 PLC。

2. 西门子 PLC 的特点

（1）可靠性高，抗干扰能力强

高可靠性是电气控制设备的关键性能，西门子 PLC 采用现代大规模集成电路技术，采用严格的生产工艺制造，内部电路采取先进的抗干扰技术，具有很高的可靠性。S7 系列 PLC 的平均无故障时间高达 30 万 h，而使用冗余 CPU（西门子 PLC）的平均无故障工作时间则更长。就西门子 PLC 的机外电路来说，使用西门子 PLC 构成控制系统和同等规模的继电器系统相比，电气接线及开关接点已减少到数百甚至数千分之一，故障也就大大降低。此外，西门子 PLC 带有硬件故障自我检测功能，出现故障时可及时发出警报信息。在应用软件中，应用时还可以编入外围器件的故障自诊断程序，使系统中除西门子 PLC 以外的电路及设备也能获得故障自诊断保护。

（2）配套齐全，功能完善，适用性强

西门子 PLC 发展到今天，已经形成了大、中、小各种规模的系列化产品，可以适用于各种规模的工业控制场合。除了逻辑处理功能以外，现代 PLC 大多具有完善的数据运算能力，可用于各种数字控制领域。近年来 PLC 的功能单元大量涌现，使 PLC 渗透到位置控制、温度控制、CNC 等各种工业控制中。加上西门子 PLC 通信能力的增强及人机界面技术的发展，使用西门子 PLC 组成各种控制系统变得非常容易。

（3）易学易用，深受工程技术人员欢迎

西门子 PLC 作为通用的工业控制计算机，是面向工矿企业的工控设备。它接口容易，编程语言易于被工程技术人员接受。梯形图语言的图形符号与表达方式和继电器控制电路图相当接近，只用 PLC 的少量开关量逻辑控制指令就可以方便地实现继电器控制电路的功能。为不熟悉电子电路、不懂计算机原理和汇编语言的人使用计算机从事工业控制打开了方便之门。

（4）系统的设计、构建工作量小，维护方便，容易改造

西门子 PLC 用存储逻辑代替接线逻辑，大大减少了控制设备外部接线，使控制系统设计及构建的周期大为缩短，同时维护也变得容易起来。更重要的是使同一设备经过改变程序从而改变生产过程成为可能，这很适合多品种、小批量的生产场合。

（5）体积小，重量轻，能耗低

以超小型西门子 PLC 为例，新推出的产品底部尺寸小于 100mm，重量小于 150g，功耗仅数瓦。由于体积小很容易装入机械设备内部，因此是实现机电一体化的理想控制设备。

3. S7 系列 PLC 产品

西门子 S7 系列 PLC 具有体积小、速度快、标准化、具有网络通信能力、功能更强、可靠性更高等特点。S7 系列 PLC 产品可分为微型 PLC（如 S7-200），小规模高性能 PLC（如 S7-300）和中规模高性能的 PLC（如 S7-400）等。

（1）西门子 S7-200 系列 PLC

西门子 S7-200 系列 PLC 是超小型化的 PLC，适用于各行各业及各种场合中的自动检测、监测及控制。S7-200 系列 PLC 的强大功能使其无论单机运行，或连成网络都能实现复杂的控制功能。S7-200 系列 PLC 提供 4 个不同的基本型号与 8 种 CPU 可供选择使用。从 CPU 模块的功能来看，西门子 S7-200 系列 PLC 发展至今大致经历了两代，第一代产品的 CPU 模块为 CPU21X，主机都可进行扩展，它具有 4 种不同结构配置的 CPU：CPU212、CPU214、CPU215 和 CPU216；第二代产品的 CPU 模块为 CPU22X，是在 21 世纪初投放市场的，速度快，具有较强的通信能力，它具有 4 种不同结构配置的 CPU：CPU221、CPU222、CPU224 和 CPU226，除了 CPU221 之外，其他都可加扩展模块。

针对低性能要求的模块化小型控制系统，西门子 S7-200 系列 PLC 最多可有 7 个模块的扩展能力，在模块中集成背板总线的网络连接有 RS-485 通信接口和 PROFIBUS 两种，可通过编程器（PG）访问所有模块，是带有电源、CPU 和 I/O 的一体化单元设备。其中扩展模块（EM）有数字量输入（DI）模块（24VDC 和 120/230VDC）；数字量输出（DO）模块（24VDC 和继电器）；模拟量输入（AI）模块（电压、电流、电阻和热电偶）；模拟量输出（AO）模块（电压和电流）。

还有一个比较特殊的模块是通信处理器（CP），该模块的功能是可以把西门子 S7-200

系列 PLC 作为主站连接到 AS 接口（传感器和执行器接口），通过 AS 接口的从站可以控制多达 248 个设备，这样就可以显著地扩展西门子 S7-200 系列 PLC 的输入和输出点数。

（2）西门子 S7-300 系列 PLC

西门子 S7-300 系列 PLC 为模块化结构、易于实现分布式配置，并具有性价比高、电磁兼容性强、抗振动冲击性能好，使其广泛地应用于工业控制领域，成为一种既经济又切合实际的自动化解决方案。

西门子 S7-300 系列是模块化小型 PLC，能满足中等控制规模的要求。各模块之间可进行广泛组合构成不同要求的控制系统。与 S7-200 系列 PLC 相比，S7-300 系列 PLC 采用模块化结构，具备高速（0.6～0.1μs）的指令运算速度，用浮点数运算可以比较有效地实现更为复杂的算术运算，一个带标准用户接口的软件工具，可方便用户给所有模块进行参数赋值，方便的人机界面服务已经集成在西门子 S7-300 系列 PLC 的操作系统内，人机对话的编程要求大大减少。SIMATIC 人机界面（HMI）从 S7-300 系列 PLC 中取得数据，S7-300 系列 PLC 按用户指定的刷新速度传送这些数据。S7-300 的操作系统自动地处理数据的传送；CPU 智能化的诊断系统能连续监控系统的功能是否正常、记录错误和特殊系统事件（例如超时，模块更换等）；多级口令保护可以使用户高度、有效地保护其技术机密，防止未经允许的复制和修改；S7-300 系列 PLC 设有操作方式选择开关，操作方式选择开关像钥匙一样可以拔出，当钥匙拔出时，就不能改变操作方式，这样就可防止非法删除或改写用户程序。S7-300 系列 PLC 可通过编程软件（STEP7）的用户界面提供通信组态功能，这使得组态变得非常简单。S7-300 系列 PLC 具有多种不同的通信接口，并通过多种通信处理器来连接 AS-i 总线接口和工业以太网总线系统；串行通信处理器用来连接点到点的通信系统；多点接口（MPI）集成在 CPU 中，用于同时连接编程器、PC、人机界面及其他 SIMATIC S7/M7/C7 等自动化控制系统。

相比 S7-200 系列 PLC，S7-300 系列 PLC 针对的是中型系统，可以扩展多达 32 个模块，背板总线也在模块内集成，它的网络连接已比较成熟和流行，有 MPI、工业以太网，使通信和编程变得简单，选择性也比较多，并可借助工具进行组态和参数设置。

S7-300 系列 PLC 的模块除了信号模块（SM）和 S7-200 的 EM 模块同类型之外，它还有接口模块（IM）可用来进行多层组态，把总线从一层传到另一层；占位模块（DM）为没有设置参数的信号模块保留一个插槽或为以后安装的接口模块保留一个插槽；功能模块（FM）执行特殊功能，如计数、定位、闭环控制相当于对 CPU 功能的一个扩展或补充；通信处理器（CP）提供点对点连接、PROFIBUS 和工业以太网。

新一代的 S7-300 系列 CPU 与以前对应版本备件兼容，在性能方面提升了两倍或者更高。在内存方面，CPU314 从 96KB 扩展到 128KB，CPU315-2DP 从 128KB 扩展到 256KB，CPU315F-2DP 从 192KB 扩展到 384KB。此外，可以同时在线监控两个块，技术数据也趋于一致，I/O 过程映像区增大。同时，CPU315（F）-2DP 的 PROFIBUS 可以使用同步模式，并带有可以进行数据设置的路由。

新一代的 S7-300 系列 PLC 的 CPU 性能比现有的 312、314 和 315（F）-2DP 的 CPU 有了显著提升，例如，新一代 CPU 的用户程序执行速度是原来 CPU 的两倍或更高。位运算时间缩减到 50ns，字运算时间缩减到 90ns，定点和浮点数运算性能也有了较大的提升。

新一代 S7-300 系列 PLC 固件版本 V3.0 CPU 可以同时在线监控两个块，用户可以选择

在一个 PG 或 PC 上同时监视两个块，或在两个 PG 或 PC 上同时监控一个块。此外，还增加了在块状态中监视程序行数的功能，只有在 STEP 7V 5.4 SP5 中才有这个功能。

（3）西门子 S7-400 系列 PLC

S7-400 系列 PLC 采用模块化无风扇设计，可靠耐用，同时可以选用多种级别（功能逐步升级）的 CPU，并配有多种通用功能的模板，这使用户能根据需要组合成不同的控制系统。当控制系统规模扩大或升级时，只要适当地增加一些模板，便能使系统升级并充分满足需要。

西门子 S7-400 系列 PLC 所具有的模板扩展和配置功能使其能够按照不同的需求灵活组合，一个系统包括电源模板，中央处理器单元（CPU），各种信号模板（SM），通信模板（CP），功能模板（FM），接口模板（IM），西门子 S5 模板。

S7-400 系列同 S7-300 系列 PLC 的区别主要在于热启动（wrst）部分，其他基本一样。它还有一个外部的电池电源接口，当在线更换电池时可以向 RAM 提供后备电源。编程设备主要有 PG720/PG740/PG760（可以理解成装有编程软件的手提电脑），也可以直接用安装有 STEP7（西门子的编程软件）的 PC 来完成。实现通信（要编程首先要和 PLC 的 CPU 通信上）的主要接口有：

1）在 PC 上安装 CP5611 卡，其上面的 MPI 口可用电缆直接连接。

2）加装 PC 适配器，将 MPI 口转换成 RS-232 口后接到 PC 上。

3）在 PLC 上安装 CP343 卡使其具有以太网口。

（4）西门子 S7-1200 系列 PLC

西门子 S7-1200 系列 PLC 是低端的离散自动化系统和独立自动化系统中使用的小型控制器模块，S7-1200 系列 PLC 具有集成 PROFINET 接口、强大的集成工艺功能和灵活的可扩展性等特点，充分满足中小型自动化系统的需求。在研发过程中充分考虑了系统、控制器、人机界面和软件的无缝整合和高效协调的需求。S7-1200 系列 PLC 的问世，标志着西门子在原有系列的基础上拓展了产品的应用领域，代表了未来小型 PLC 的发展方向。

1.1.2 西门子 S7-200 与 S7-300/400 系列 PLC 的区别

西门子 S7-200 与 S7-300/400 系列 PLC 的主要区别是 PLC 的等级不同和模块差别，S7-200 系列 PLC 属于基础入门级，而 S7-300/400 系列 PLC 相对较高端。即 S7-200 系列 PLC 属于小型机，用于小型的电气控制系统中，着重于逻辑控制；S7-200 也是多功能机，将所有功能结合在一起，它的控制规模最大为 512 点，CPU 的运算处理速度不及中大型机快，小型机多为整体式，扩展模块最多可加 8 块，适用于小型设备，性价比高。

S7-300 系列 PLC 属于中型机，用于稍大系统，可实现复杂的工艺控制，如 PID、脉宽调制等；S7-400 系列 PLC 用于中大型控制系统，主要是实现冗余控制。中大型机结构是模块化的，最多可加 300 多块扩展模块，中大型机硬件较贵、成本高，但其运算处理速度快，有很强的通信功能，主要应用于中大型生产线。

1. 硬件区别

最主要的区别就是 S7-300/400 系列 PLC 为模块化结构，S7-200 系列 PLC 是整体式结构，CPU 模块、I/O 模块和电源模块都在一个模块内，称为 CPU 模块；而 S7-300/400 系列 PLC 的电源、I/O、CPU 都是独立模块。S7-200 系列 PLC 也可以扩展，只是 CPU 模块集成

了部分功能，一些小型系统不需要另外定制模块，S7-200 系列 PLC 的模块也有信号、通信、位控等模块。

S7-200 系列 PLC 对机架没有特定概念，称之为导轨。为了便于分散控制，S7-300/400 系列 PLC 的模块装在一根导轨上的，称之为一个机架，与中央机架对应的是扩展机架，机架还在软件里反映出来。

S7-200 系列 PLC 同一机架上的模块之间是通过模块正上方的数据接头联系的；而 S7-300/400 系列 PLC 则是通过在底部的 U 形总线连接器连接的。

S7-300/400 系列 PLC 的 I/O 输入是接在前连接器上，前连接器再接在信号模块上的，而不是 I/O 信号直接接在信号模块上，这样可以在更换信号模块时不用重新接线。S7-300/400 系列 PLC 的 CPU 带有 PROFIBUS（PROFIBUS 是一种国际化、开放式、不依赖于设备生产商的现场总线标准）接口。

2. 软件区别

S7-200 系列 PLC 使用 STEP7-Micro/WIN32 软件；S7-300/400 系列 PLC 使用的是 STEP7 软件，带有 Micro 和不带的区别是相当明显的。S7-200 系列 PLC 的编程语言有语句表（STL）、梯形图（LAD）、功能块图（FBD）三种；S7-300 系列 PLC 除了这 3 种外，还有结构化控制语言（SCL）和图形语言（S7graph），其中 SCL 就是一种高级语言，S7-300/400 系列 PLC 软件最大的特点就是提供了一些数据块来对应每一个功能块（Function Block，FB）。

1.2 PROFIBUS 现场总线

1.2.1 PROFIBUS 现场总线的发展与优点

1. PROFIBUS 现场总线的发展

PROFIBUS 是 Process Fieldbus 的简称，它是 1987 年由原联邦德国科技部集中了 13 家公司及 5 家研究所的力量按照 ISO/OSI 参考模型制定现场总线的德国国家标准。经过两年多的努力，完成了制定工作，于 1991 年 4 月在 DIN19245 中发表，正式成为德国现场总线的国家标准。后来，又通过投票成为欧洲标准 EN50170。

PROFIBUS 的历史应追溯到 1987 年，在德国开始的由政府支持的联合投资项目。在此投资的框架中，参加此项目的 21 个公司和研究院所通力合作拟定了一个战略性的现场总线项目。其目标是实现和建立一个比特串行现场总线，它的基本要求是现场设备接口的标准化。为此目的，ZVEI（德国电气和电子制造商协会）的相关成员公司同意支持用于工厂自动化和过程自动化的共性技术研究。

PROFIBUS 已成为国际化的开放现场总线标准，得到了众多生产厂家的支持，并和基金会现场总线一起成为现场总线的两大体系，在欧洲，PROFIBUS 拥有 40% 以上的市场份额，近年来，在北美和日本的发展情况也不错。由于得到 PLC 生产厂商的支持，加上基金会现场总线的标准迟迟得不到完善，PROFIBUS 将会有更大的发展空间。

PROFIBUS 是现场总线国际标准 IEC 61158 中的 Type-3，它是世界上应用最成功、市场占有率最高的现场总线技术。PROFIBUS 包括用于制造业自动化的 DP 和流程工业的 PA，它是唯一一种能在所有自动化应用领域使用的现场总线技术。作为国际现场总线标准之一的

PROFIBUS，在工业自动化、传动、化工等领域占据主导地位。除具有现场总线的普遍特点外，PROFIBUS 还有其独特的优点：

1）总线传输速度高，最高可达 12Mbit/s。

2）采用主从轮询方式，具有确定的传输响应时间，可应用于对时间要求苛刻的复杂控制系统中。

3）PROFIBUS 满足了从现场层到工厂管理层对网络的要求，应用面广、产品多样。尤其在传动行业，几乎所有著名厂商的产品都支持 PROFIBUS。

与其他现场总线系统相比，PROFIBUS 的最大优点在于具有稳定的国际标准 EN 50170 作保证，并经实际应用验证具有普遍性。目前已应用的领域包括加工制造、过程控制和楼宇自动化等。PROFIBUS 的开放性和不依赖于厂商通信的设想，已在 10 多万成功应用中得以实现。市场调查确认，在德国和欧洲市场中，PROFIBUS 占开放性工业现场总线系统的市场份额超过 40%。PROFIBUS 有国际著名自动化技术装备的生产厂商支持，它们都具有各自的技术优势并能提供广泛优质的新产品和技术服务。多种行规保证了不同厂家产品之间的通用性。在十多年的开发和应用实践过程中，PROFIBUS 以其技术的成熟性、完整性和应用的可靠性等多方面优秀的表现，使其在现场总线技术领域中成为国际市场的领导者。

对于制造业自动化和过程自动化的所有应用领域来说，PROFIBUS 是一个标准化的、开放的数字通信系统。PROFIBUS 协议是以国际标准 EN 50170 和 IEC 61158 为基础的，这一技术适合于替代离散和模拟的信号。PROFIBUS 的存在已超过 20 年，期间它不断地自我发展以跻身于世界市场的领先地位。由于具有一系列不同类型的协议、接口和行规，PROFIBUS 以其模块化设计为基础被确定为普遍的应用，同时它也超出了制造业自动化和过程自动化的要求。

PROFIBUS 凭借其在我国广泛的应用、测试技术本地化、国内企业广泛参与其技术的应用和推广等，2006 年 10 月，它被批准为中华人民共和国国家标准 GB/T 20540—2006，它是目前我国唯一的现场总线国家标准。

现场总线是 20 世纪 90 年代兴起的一种先进的工业控制技术，是目前自动化技术中的一个热点，备受国内外自动化设备制造商和用户的关注。现场总线是当今 3C 技术，即计算机（Computer）、通信（Communication）与控制（Control）技术发展汇聚成的结合点。它是一种数字通信协议，是用于仪表和控制器的一种开放、全数字化、双向、多站的通信系统，是控制技术、仪表技术和计算机网络技术相结合的产物。由于现场总线代表着自动化技术未来的发展方向，国外许多大公司相继推出了各自的现场总线标准。在众多的现场总线产品中，作为欧洲标准并已占据较大市场份额的 PROFIBUS 是很具有代表性的一种。

PROFIBUS 是目前国际上通用的现场总线标准之一，以其独特的技术特点、严格的认证规范、开放的标准、众多厂商的支持和不断发展的应用行规，已成为最重要的现场总线标准。符合 IEC 61158 国际标准——JB/T 10308.3—2001（中国标准 2001 年），PROFIBUS 协议包括 3 个主要部分：

1）PROFIBUS-DP。主站和从站之间采用轮询的通信方式，PROFIBUS-DP 用于分散外设间高速数据传输，适用于加工自动化领域、制造业自动化系统中单元级和现场级通信。

2）PROFIBUS-PA。电源和通信数据通过总线并行传输，PROFIBUS-PA 用于过程自动化的总线类型，服从 IEC 1158—2 标准，主要用于面向过程自动化系统中单元级和现场级

通信。

3）PROFIBUS-FMS：定义了主站和主站之间的通信模型，PROFIBUS-FMS 适用于纺织、楼宇自动化、PLC、低压开关等，主要用于自动化系统中系统级和车间级的过程数据交换。

PROFIBUS 支持主—从系统、纯主站系统、多主多从混合系统等几种传输方式，PROFIBUS 的传输速率为 9.6k ~ 12Mbit/s，最大传输距离在 9.6kbit/s 时为 1200m，在 12Mbit/s 时小于 200m，可采用中继器延长至 10km，传输介质为双绞线或者光缆，最多可挂接 127 个站点。

PROFIBUS 产品在世界市场上已被普遍接受，市场份额占欧洲首位，年增长率为 25%。目前支持 PROFIBUS 标准的产品超过 1500 种，分别来自国际上 250 多个生产厂商。在世界范围内已安装运行的 PROFIBUS 设备超过 200 万台，适用于过程自动化的 PROFIBUS-PA 仪表设备在多个国家的多个用户厂商投入现场运行。

1985 年组建了 PROFIBUS 国际支持中心；1989 年 12 月建立了 PROFIBUS 用户组织（PNO）。目前在世界各地相继组建了 20 个地区性的用户组织，企业会员近 650 家。1997 年 7 月组建了中国现场总线（PROFIBUS）专业委员会，并筹建现场总线 PROFIBUS 产品演示及认证的实验室。

2. PROFIBUS 技术特点

PROFIBUS 实际上是一种应用类的系统框架，其基本技术特点如下。

1）分为通用性自动化（FMS）、工厂自动化（DP）和过程控制自动化（PA）三个系列。

2）设备之间的通信采用主从方式；结构采用 OSI 参考模型中的物理、数据链路和应用三层结构。

3）标准采用 EN 50170；其接口标准为：PA 采用 IEC 1158-2，FMS 和 DP 采用 RS-485。

4）信号线可用设备电源线。

5）每条总线区段可连接 32 个设备，不同区段用中继器连接。

6）传输速率可在 9.6k ~ 12Mbit/s 间选择。

7）传输介质可以用金属双绞线或光纤。

8）提供通用的功能模块管理规范。

9）在一定范围内可实现互操作。

10）没有统一的设备描述语言和 DDL 支持。

11）提供系统通信管理软件（包括波形识别、速率识别和协议识别等功能）。

12）提供 244B 报文格式，提供通信接口故障安全模式（当 I/O 故障时输出全为零）。

PROFIBUS 是面向工厂自动化、过程自动化的一种国际性的现场总线标准，是一种具有广泛应用范围的、开放的数字通信系统，适用于快捷、时间要求严格和可靠性要求高的各种通信任务。

PROFIBUS 是基于分布式控制思想发展而来的，最初的设计构想是基于扩展 MAP/MMS 标准的思想，建立一个基于客户/服务器（Client/Server）结构的、面向对象的、适应工厂上下各层的工业通信系统。PROFIBUS 是国际性的、开放的现场总线标准，PROFIBUS 标准（EN 50170）是完整的、开放的、与制造商无关的、已经生效的，其保护了世界范围的用户和制造商的投资。采用 PROFIBUS 现场总线可节省硬件和安装费用，更容易组态（对所有设

备只需一套工具），更容易保养和维修，更容易且更快捷的系统启动，更大的制造灵活性，改进功能可减少故障时间，采用准确、可靠的数据诊断和可靠的数字传输技术。

3. PROFIBUS 现场总线系统的优点

（1）开放性

PROFIBUS 是一个完全开放的、与制造商无关的、无知识产权保护的现场总线标准，全球有超过 250 家公司，可以生产超过 2000 种支持 PROFIBUS 的系统和设备。PROFIBUS 的开放性保证了不同制造厂商产品的互联，例如西门子公司的 DCS 或 PLC 可以通过 PROFIBUS 连接第三方的远程 I/O、智能设备和仪表，这些连接只需要产品制造商提供相应的 GSD 文件或 EDD 文件，然后进行简单组态即可实现。目前国际知名的自动化系统制造商及仪表制造商，如西门子、ABB、EMERSON 等都可以提供丰富的支持 PROFIBUS 的产品。在电力行业知名的 DCS 制造商如：西门子、ABB、EMERSON、FOXBORO 等也都支持 PROFIBUS 现场总线，知名的 PLC 品牌，如西门子、MODICON、AB 的产品也都支持 PROFIBUS 总线。

（2）可靠性

PROFIBUS 现场总线安装运行节点数超过 1000 万个，大大高于其他现场总线系统。PROFIBUS 是 IEC 61158 的重要组成部分，并于 2001 年成为中国的行业标准 JB/T 10308.3—2001（与 GB 等效）。PROFIBUS 的可靠性表现在以下几个方面：

1）PROFIBUS 总线上的数据传输是完全基于数字信号实现的，这样可以大幅提高信号传输过程中的抗干扰能力。

2）采用 PROFIBUS 总线直接连接现场智能设备，可以大幅减少接线点，减少了由于接线不牢或接线不规范引起的故障。

3）PROFIBUS 可直接连接智能设备，减少了 A-D 转换的环节，提高了自动化系统的采集精度，为精确控制提供保障。

4）PROFIBUS 上各设备的连接非常简单，并可以通过专用剥线工具和 PROFIBUS 接头减少接线风险；同时 PROFIBUS 接头可以保证总线上任何一个节点设备故障不影响系统通信。

5）支持冗余总线系统，提高系统可靠性。

（3）灵活扩展

采用 PROFIBUS 总线结构的控制系统扩展非常方便灵活，主要表现在以下几个方面：

1）拓扑结构灵活，可以支持总线型、星形、树形、冗余环形等多种拓扑结构。

2）支持光纤和双绞线作为通信介质，采用多模光纤时，两个光电模块间的距离可达 3km，采用单模光纤时，两个光电模块间的距离可达 26km；采用双绞线不加中继的最远通信距离可达 1km，采用中继时最远可达 9km。

3）一条 PROFIBUS-DP 总线最多可以连接 123 个 DP 从站，所有满足 PROFIBUS-DP 通信规约的设备都可以连接到系统中。目前全球有超过 1200 家公司，生产超过 2000 种支持 PROFIBUS 的产品，因此具有很强的开放性和可扩展性。

4）网络拓扑灵活，单一总线系统和冗余总线系统间可无缝连接，PA 总线可以通过网络上任一点扩展，并能与其他网络和总线（PROFINET 和 AS-i）方便集成。

5）PROFIBUS 同时可以支持 PROFIsafe 协议，一条总线上既可以传输标准数字信号，也可以同时传输故障安全信号。

6）提供可用于危险领域的接口模块，可以支持在危险区域的应用。

（4）实时性

采用 PROFIBUS 总线的系统具有很高的实时性，这是由 PROFIBUS 总线系统的数据传输速率所决定的。PROFIBUS-DP 总线的传输速率可达 12Mbit/s，是目前通信速率最高的现场总线。PROFIBUS-DP 总线的响应时间可以按下面的公式进行计算：

$$t_{\text{Cycle\_ DP}} = [317 \times (N_{\text{Slaves}}) + 11 \times (N_{\text{Bytes}})] \times T_{\text{bit}} \tag{1-1}$$

式中，317 是一个常数，表示一个 DP 从站建立通信连接所需的数据位；N_{Slaves} 表示整个 PROFIBUS-DP 总线上的从站数量；N_{Bytes} 表示整个 PROFIBUS-DP 总线上传输的数据总数，单位为 B（字节）。

如果总线系统中还有 PA 总线，则 PA 总线的响应时间为

$$t_{\text{Cycle\_ PA-channel}} = [317 \times (N_{\text{Slaves}}) + 8 \times (N_{\text{Bytes}})] \times T_{\text{bit}} \tag{1-2}$$

整个 PROFIBUS-DP 系统的响应时间为

$$t_{\text{Cycle}} = t_{\text{Cycle\_ PA-channel}} + t_{\text{Cycle\_ DP}} + t_{\text{Acylic}} \tag{1-3}$$

从上面的公式可以看出，一个典型的通过 PA 总线连接的智能仪表的响应时间为 10ms，一个典型的通过 PA 总线连接的执行机构的响应时间为 15ms，一个 PROFIBUS-DP 从站的响应时间小于 0.3ms。因此可以确定 PROFIBUS 总线系统是一个实时的系统，大大优于其他总线系统。

4. PROFIBUS 协议结构

网络协议是指用于网络之间相互沟通、传输信息所要共同遵守的基础。网络协议有专用网络协议和非专用（标准）网络协议之别。现场总线通信协议基本遵照 ISO/OSI 参考模型，主要实现第 1（物理层）、2（数据链路层）、7（应用层）层功能。OSI 模型是建立在七层协议基础上，作为一个起始点以发展计算机通信标准的。每层都有一定等级功能，具有规定的高层或低层的接口，为其提供一定功能通信标准，但并不一定所有的层都需要。当与很好定义的程序模块连接时，该模块定义了数据意义及格式，OSI 模块将提供一个多卖主相互操作的高水平工具。一个典型的开放系统结构可以应用在工业和商业的控制系统上，所有的开放系统元件使用标准协议作为本系统语言，无需翻译，可以相互通信。

PROFIBUS 开始只有 PROFIBUS-DP 和 PROFIBUS-FMS，1994 年又推出了 PROFIBUS-PA，它引用了 IEC 标准的物理层（IEC 1158-2，1993 年通过），从而可以在有爆炸危险的区域（EX）内连接本征安全型，通过总线馈电的现场仪表，这使 PROFIBUS 更加完善。PROFIBUS 已于 1996 年 3 月 15 日被批准为欧洲标准 EN 50170 的第 2 卷。

PROFIBUS 同 FF 一样省略了 3～6 层，增加了用户层。PROFIBUS-DP 使用第 1 层、第 2 层和用户接口。PROFIBUS-FMS 分别对 1 层、2 层和 7 层加以定义，PROFIBUS-PA 的数据传输沿用 PROFIBUS-DP 的协议，只是在上层增加了描述现场设备行为的 PA 行规。它的总线访问方式为：主站之间通信采用令牌传输，主站和从站之间采用主从方式。PROFIBUS 可以采用总线型、树形、星形等网络拓扑，总线上最多可挂接 127 个站点。PROFIBUS 行规的制定为遵循 PROFIBUS 协议的设备之间的互操作奠定了基础。通过对设备指定符合 PROFIBUS 行规的过程参数、工作参数、厂家特定参数，设备之间就可以实现互操作。

PROFIBUS 协议结构如图 1-1 所示，物理层采用 EIA-RS-232、EIA-RS-422/RS-485 等协

议。由于在某些情况下，现场传感器、变送器要从现场总线“窃取”电能作为它们的工作电源，因此对总线上数字信号的强度（驱动能力）、传输速率、信噪比以及电缆尺寸、线路长度等都提出一定要求。

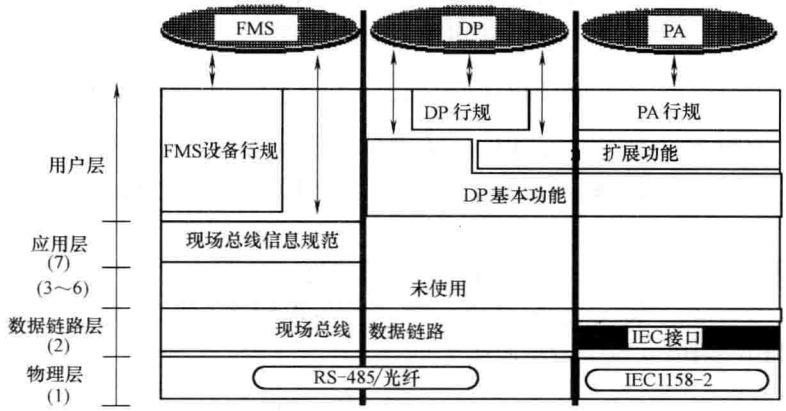

图 1-1　PROFIBUS 协议结构

考虑到数据链路层现场设备故障较多，更换频繁，所以数据链路层媒体访问控制多采用受控访问（包括轮询和令牌）协议，通常，各 PC、PLC 作为主站，传感器、变送器等作为从站。另外，必须支持点对点、点对多点和广播通信方式。

应用层解决的是应用什么样的高级语言（或过程控制语言）作为面向用户的编程（或组态）语言，其中包括设备名称、网络变量与配置（捆绑）关系，参数与功能调用及相关说明等，一般应具有符合 IEC 1131-3 标准的图形用户界面（GUI）。

（1）PROFIBUS-DP。DP 定义了第 1、2 层和用户接口，第 3～7 层未加描述。用户接口规定了用户和系统以及不同设备可调用的应用功能，并详细说明了各种不同 PROFIBUS-DP 设备的设备行为。典型的 PROFIBUS-DP 系统组成如图 1-2 所示。图 1-2 是一个由 3 个主站、7 个从站构成的 PROFIBUS 系统。3 个主站之间构成令牌逻辑环。当某主站得到令牌报文后，该主站可在一定时间内执行主站工作。在这段时间内，它可依照主—从通信关系表与所有从站通信，也可依照主—主通信关系表与所有主站通信。

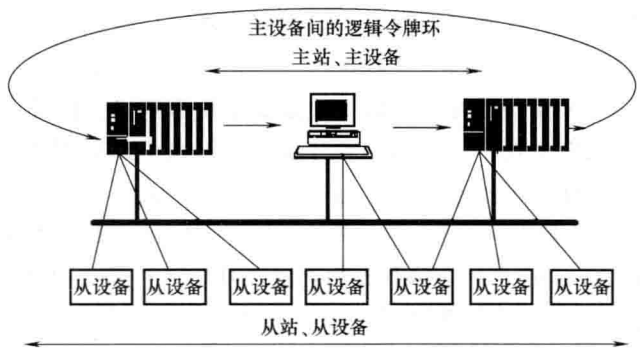

图 1-2　PROFIBUS-DP 系统组成

（2）PROFIBUS-FMS。FMS 定义了第 1、2、7 层，应用层包括现场总线信息规范（Fieldbus Message Specification，FMS）和低层接口（Lower Layer Interface，LLI）。FMS 包括了应用协议并向用户提供了可广泛选用的强有力的通信服务。LLI 协调不同的通信关系并提供不依赖设备的第 2 层访问接口，典型的 PROFIBUS-FMS 系统组成如图 1-3 所示。

（3）PROFIBUS-PA。PA 的数据传输采用扩展的 PROFIBUS-DP 协议。另外，PA 还描述

了现场设备行为的 PA 行规。根据 IEC 1158-2 标准，PA 的传输技术可确保其本征安全性，而且可通过总线给现场设备供电。使用连接器可在 DP 上扩展 PA 网络。典型的 PROFIBUS-PA 系统组成如图 1-4 所示。

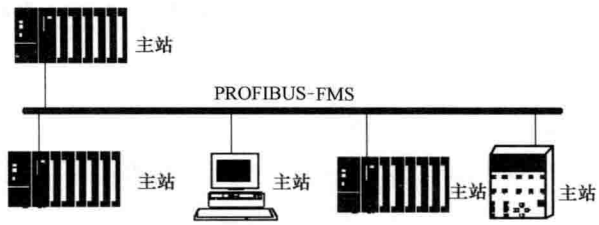

图 1-3 典型的 PROFIBUS-FMS 系统组成

PROFIBUS 具有模块化的设计，并提供通信技术、许多应用和系统行规，以及设备管理工具等。这样，PROFIBUS 在相当程度上覆盖了工厂自动化和过程自动化领域不同的和特殊应用的要求。从安装 PROFIBUS 系统的数量看，证明了对此现场总线技术的高度认可。从技术的观点看，PROFIBUS 系统结构的低层（通信）是基于 ISO/OSI 模型的。这里只给出了通信步骤的纯抽象描述，并未提供详细内容的实现。在第 7 层上面的应用行规Ⅰ和Ⅱ中，安排了制造商与用户之间基于特定设备应用所约定的规范。跨过若干层的模块系统如下：

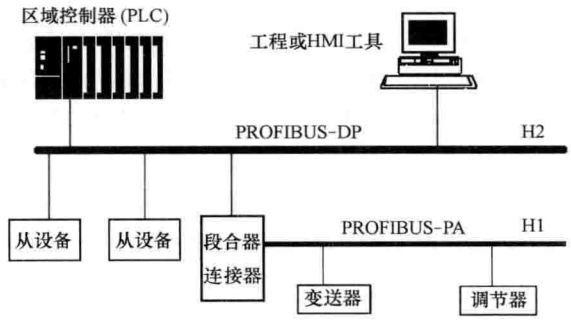

图 1-4 PROFIBUS-PA 系统组成

1）用于设备描述和集成的功能和工具（总称：集成技术）。

2）标准范围（接口，主站行规；总称：系统行规），它主要服务于统一的标准化系统的实现。

从用户的观点看 PROFIBUS 以不同典型应用的主要侧重点来表现自己，虽然未专门对它们进行定义，但频繁应用的结果证明它们是实用的。每一种主要侧重点是由“传输技术”、“通信协议”和“应用行规”中模块元素的典型结合（但没有特别的定义）产生的结果。

5. PROFIBUS 应用领域

PROFIBUS 是一种国际化、开放式、不依赖于生产商的现场总线标准，广泛应用于工业自动化。PROFIBUS 根据应用特点分为 PROFIBUS-DP、PROFIBUS-FMS、PROFIBUS-PA 三个兼容版本。其中 PROFIBUS-DP 是一种高速的（数据传输速率 9.6k ~ 12Mbit/s）、经济的设备级网络，主要用于现场控制器与分散 I/O 之间的通信，可满足交直流调速系统快速响应的时间要求；PROFIBUS-PA 采用 IEC 1158-2 标准，传输速率为 31.25kbit/s，并提供本征安全特性，适用于安全性要求较高及由总线供电的场合；PROFIBUS-FMS 主要解决车间级通信问题，完成中等传输速度的循环或非循环数据交换任务。

PROFIBUS 自 1997 年进入我国后，市场发展非常迅速。据 CPO 对北京周边 300 多家企业的调查结果显示，PROFIBUS 的市场占有率为 40% ~50%，而在全国市场至少有 30% ~40% 的占有率。有理由相信，随着自动化技术的进一步提高，PROFIBUS 技术会在国内有更进一步的推广应用。PROFIBUS 主要应用领域有：

1）制造业自动化：汽车制造（机器人、装配线、冲压线等）、造纸、纺织。

2）过程控制自动化：石化、制药、水泥、食品、啤酒。

3）电力：发电、输配电。

4）楼宇：空调、风机、照明。

5）铁路交通：信号系统。

PROFIBUS 由西门子公司提出并极力倡导，已先后成为德国国家标准 DIN 19245 和欧洲标准 EN 50170，是一种开放而独立的总线标准，在机械制造、工业过程控制、智能建筑中充当通信网络。PROFIBUS 由 PROFIBUS-PA、PROFIBUS-DP 和 PROFIBUS-FMS 三个系列组成。PROFIBUS-PA（Process Automation）用于过程自动化的低速数据传输，其基本特性同 FF 的 H1 总线，可以提供总线供电和本征安全，并得到了专用集成电路（ASIC）和软件的支持。PROFIBUS-DP 与 PROFIBUS-PA 兼容，基本特性同 FF 的 H2 总线，可实现高速传输，适用于分散的外部设备和自控设备之间的高速数据传输，用于连接 PROFIBUS-PA 和加工自动化。PROFIBUS-FMS 适用于一般自动化的中速数据传输，主要用于传感器、执行器、电气传动、PLC、纺织和楼宇自动化等。PROFIBUS-DP、PROFIBUS-PA 采用 RS-485 通信标准，传输速率为 9.6k ~ 12Mbit/s，传输距离为 100 ~ 1200m（与传输速率有关）。介质存取控制的基本方式为主站之间的令牌方式和主站与从站之间的主从方式，以及综合这两种方式的混合方式。PROFIBUS 是一种比较成熟的总线，在工程上的应用十分广泛。PROFIBUS 的应用范围如图 1-5 所示。

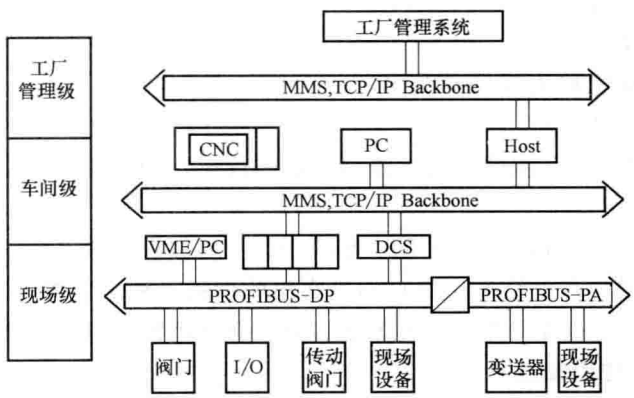

图 1-5 PROFIBUS 应用范围

1.2.2 PROFIBUS-DP 特性及规范

1. PROFIBUS-DP 特性

PROFIBUS-DP 是一种高速且优化的通信方案，主要用于实现现场级控制系统与分布式 I/O 及其他现场设备之间的通信，总线周期一般小于 10ms。主站（PLC 或 IPC 等）通过标准的专用电缆与分散的现场设备（远程 I/O、驱动器、阀门、智能传感器和下层网络等）进行通信，对整个 DP 网络进行管理和控制。PROFIBUS-DP 用于传感器和执行器级的高速数据传输，它以德国标准 DIN 1924 的第一部分为基础，根据其所需要达到的目标对通信功能加以扩充。

PROFIBUS-DP 使用第 1 层，第 2 层和用户接口。这种结构确保了数据传输的快速和有