第1章 现场总线技术概述

1.1 现场总线简介

1.1.1 现场总线的概念

随着科学技术的快速发展，过程控制领域在过去的两个世纪里发生了巨大的变革。150多年前出现的基于5～13ps（pneumatic signal，气动信号）气动信号标准的气动控制系统（Pneumatic Control System，PCS），标志着控制理论初步形成，但此时尚未有控制室的概念；20世纪50年代，随着基于0～10mA或4～20mA的电流模拟信号的模拟过程控制体系被提出并得到广泛的应用，标志了电气自动控制时代的到来，三大控制论的确立奠定了现代控制的基础，设立控制室、控制功能分离的模式也一直沿用至今；20世纪70年代，随着数字计算机的介入，产生了“集中控制”的中央控制计算机系统，而信号传输系统大部分依然沿用4～20mA的模拟信号，不久人们也发现了伴随着“集中控制”，该系统存在着易失控、可靠性低的缺点，并很快将其发展为分布式控制系统（Distributed Control System，DCS）；微处理器的普遍应用和计算机可靠性的提高，使分布式控制系统得到了广泛的应用，由多台计算机和一些智能仪表以及智能部件实现的分布式控制是其最主要的特征，而数字传输信号也在逐步取代模拟传输信号。随着微处理器的快速发展和广泛的应用，数字通信网络延伸到工业过程现场成为可能，产生了以微处理器为核心，使用集成电路代替常规电子线路，实施信息采集、显示、处理、传输以及优化控制等功能的智能设备。设备之间彼此通信、控制，在精度、可操作性以及可靠性、可维护性等都有更高的要求。由此，导致了现场总线的产生。

现场总线是连接智能现场设备和自动化系统的全数字、双向、多站的通信系统，主要解决工业现场的智能化仪器仪表、控制器、执行机构等现场设备间的数字通信以及这些现场控制设备和高级控制系统之间的信息传递问题；或者现场总线是安装在生产过程区域的现场设备/仪表与控制室内的自动控制装置/系统之间的一种串行数字式多点双向通信的数据总线，其中“生产过程”包括断续生产过程和连续生产过程两类；或者现场总线是以单个分散的数字化智能化的测量和控制设备作为网络节点用总线相连接实现相互交换信息共同完成自动控制功能的网络系统与控制系统。现场总线主要用于制造业、流程工业、交通、楼宇、电力等方面的自动化系统中。早在2003年，IEC61158 Edition 3即现场总线标准第3版正式成为国际标准，规定了10种类型的现场总线。这10种现场总线分别是：TS61158现场总线、ControlNet和Ethernet/IP现场总线、Profibus现场总线、P—NET现场总线、FF HSE现场总线、SwiftNet现场总线、World FIP现场总线、Interbus现场总线、FF H1现场总线、PROFInet现场总线，以及蓝牙和ZigBee无线现场总线等。

现场控制设备具有通信功能，便于构成工厂底层控制网络。通信标准的公开、一致，使系统具备开放性，设备间具有互可操作性。功能块与结构的规范化使相同功能的设备间具有互换性。控制功能下放到现场，使控制系统结构具备高度的分散性。

现场总线控制系统的体系结构如图 1－1 所示，最底层是 Infranet 控制网（即现场总线控制系统），各控制器节点下放分散到现场，构成一种彻底的分布式控制体系结构，网络拓扑结构任意（可为总线型、星型、环型等），通信介质不受限制（可用双绞线、电力线、光纤、无线、红外线等多种形式）。由图 1－1 可知，由现场总线控制系统形成的 Infranet 控制网很容易与 Intranet（企业内部局域网）和 Internet 全球信息网互联，构成一个完整的企业网络 3 级体系结构。

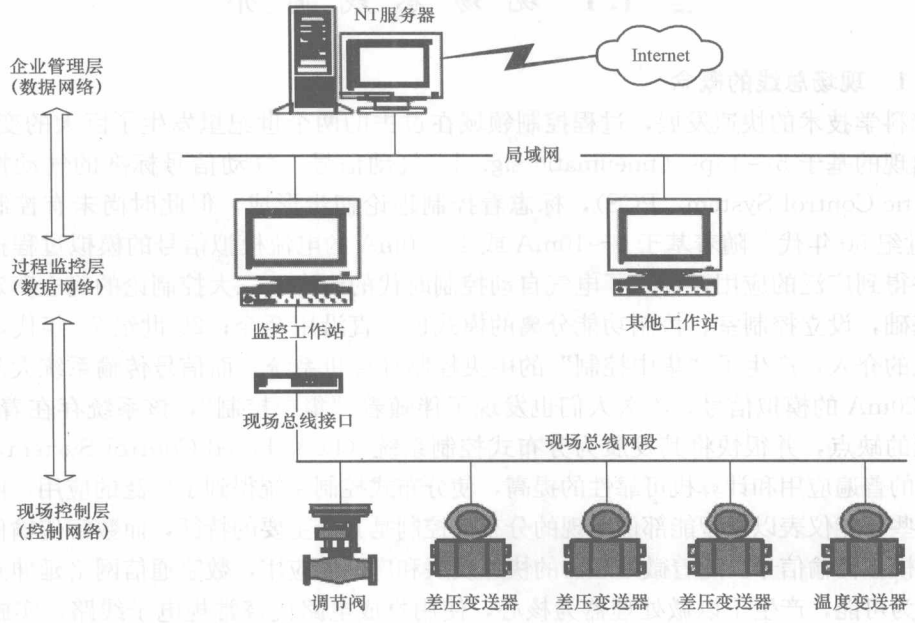

图 1－1　现场总线控制系统体系结构

当控制网络把智能仪器、设备连接在一起时，可提供一个经济、可靠、根据控制需要优化的灵活的联网平台。“The network is the computer（网络就是计算机）”，这一口号多年前由 Sun Microsystems 公司广为宣传，现在能应用于新的模式，即网络就是控制系统。现场总线技术使控制系统向着分散化、智能化、网络化方向发展，使控制技术与计算机及网络技术的结合更为紧密。基于开放通信协议标准的现场总线，为控制网络与信息网络的连接提供了方便，因而对控制网络与信息网络的集成起到了积极的促进作用。当传统的控制系统逐步走向现场总线控制网络的时候，便为构建完整信息基础结构（即 Infranet－Intranet－Internet 网络结构）、集成为一个协调统一的整体铺平了道路。一旦实现 Infranet 与 Intranet/Internet 互联，不仅可丰富网络的信息内容、更好地发挥数据信息和控制信息的综合优势，而且也是真正实现远程监控和综合自动化的坚实基础。

现场总线在自动化以及工业系统中的位置如图 1－2 所示。以工业现场控制中常用的 Profibus 总线为例，在设备级包括驱动器、输出/输出设备、传感器、变送器等现场设备，通过现场总线 Profibus 在现场总线级进行组网，系统轮询完整个系统所需的时间小于 100ms，然后通过 Profibus－FMS 现场管理总线连接服务器控制平台，对车间级的局域现场总线网络进行控制，最后通过 TCP/IP 协议进行以太网连接，组成工厂级别的区域控制系统。

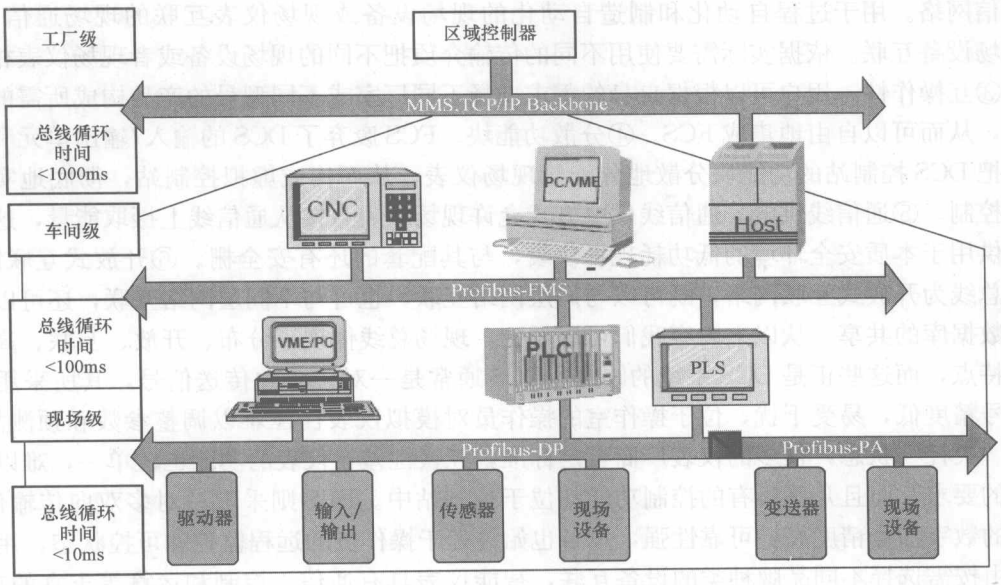

图 1-2 工业系统中现场总线的位置

传统方式现场级设备与控制器之间连接采用一对一的方式，即所谓I/O接线方式传递4～20mA交流信号或24V直流电压信号，典型的车间级现场总线的连接图如图1-3所示。

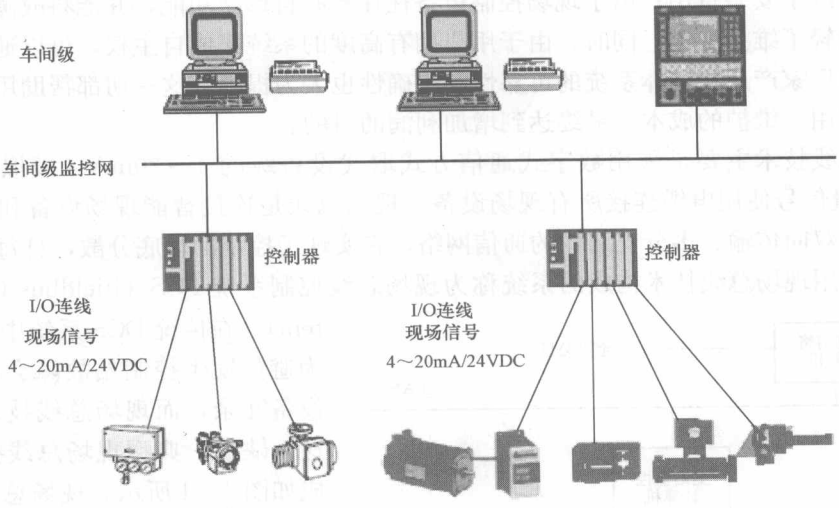

图 1-3 车间级现场总线的连接图

1.1.2 现场总线系统的特点

IEC（International Electrotechnical Commission，国际电工委员会）对现场总线（Fieldbus）的定义为：现场总线是一种应用于生产现场，在现场设备之间、现场设备和控制装置之间实行双向、串行、多节点的数字通信技术。不同的机构和不同的人可能对现场总线有着不同的定义，不过通常情况下，大家公认现场总线的本质体现在以下六个方面：①现

场通信网络。用于过程自动化和制造自动化的现场设备或现场仪表互联的现场通信网络。②现场设备互联。依据实际需要使用不同的传输介质把不同的现场设备或者现场仪表相互关联。③互操作性。用户可以根据自身的需求选择不同厂家或不同型号的产品构成所需的控制回路，从而可以自由地集成 FCS。④分散功能块。FCS 废弃了 DCS 的输入/输出单元和控制站，把 DCS 控制站的功能块分散地分配给现场仪表，从而构成虚拟控制站，彻底地实现了分散控制。⑤通信线供电。通信线供电方式允许现场仪表直接从通信线上摄取能量，这种方式提供用于本质安全环境的低功耗现场仪表，与其配套的还有安全栅。⑥开放式互联网络。现场总线为开放式互联网络，既可以与同层网络互联，也可与不同层网络互联，还可以实现网络数据库的共享。从以上内容我们可以看到，现场总线体现了分布、开放、互联、高可靠性的特点，而这些正是 DCS 系统的缺点。DCS 通常是一对一单独传送信号，其所采用的模拟信号精度低，易受干扰，位于操作室的操作员对模拟仪表往往难以调整参数和预测故障，处于“失控”状态，很多的仪表厂商自定标准，互换性差，仪表的功能也较单一，难以满足现代的要求，而且几乎所有的控制功能都位于控制站中。FCS 则采取一对多双向传输信号，采用的数字信号精度高、可靠性强，设备也始终处于操作员的远程监控和可控状态，用户可以自由按需选择不同品牌种类的设备互联，智能仪表具有通信、控制和运算等丰富的功能，而且控制功能分散到各个智能仪表中去。由此我们可以看到 FCS 相对于 DCS 的巨大进步。也正是由于 FCS 的以上特点使得其在设计、安装、投运到正常生产都具有很大的优越性：首先由于分散在前端的智能设备能执行较为复杂的任务，不再需要单独的控制器、计算单元等，节省了硬件投资和使用面积；FCS 的接线较为简单，而且一条传输线可以挂接多个设备，大大节约了安装费用；由于现场控制设备往往具有自诊断功能，并能将故障信息发送至控制室，减轻了维护工作；同时，由于用户拥有高度的系统集成自主权，可以通过比较灵活选择合适的厂家产品；整体系统的可靠性和准确性也大为提高。这一切都帮助用户实现了减低安装、使用、维护的成本，最终达到增加利润的目的。

现场总线技术主要是采用数字式通信方式取代设备级的 4～20mA（模拟量或者 24V DC）开关量信号使用电缆连接所有现场设备。现场总线是连接智能现场设备和自动化系统的数字式、双向传输、多分支结构的通信网络，它实现了控制的彻底分散，且每个回路的自治性好。采用现场总线技术构成的系统称为现场总线控制系统 FCS（Fieldbus Control System）。在传统 DCS 系统中，设计人员为避免发生控制站故障会设置复杂的设备冗余，而现场总线技术则克服了这一缺点。典型现场总线控制系统构成如图 1-4 所示。现场总线技术的优点具体表现在以下几个方面：

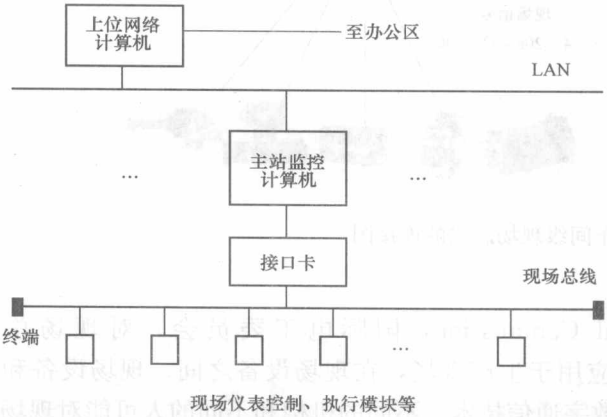

图 1-4 典型现场总线控制系统构成

（1）由于现场总线上传递的是全数字化信号，这样可以克服模拟通信方式由于传输、DPA 转换以及 APD 转换所带来的误差，可提高传送精度，抗干扰能力强，无须再采用抗干扰措施，因此降低了成本。

（2）现场总线可以进行双向通信，且一条现场总线信道可以连接多台智能仪表，因此可大大简化系统布线，可使工程周期缩短，安装费用降低，且维护容易。

（3）现场总线上所连接的各种智能设备不存在主从关系，它们在网络上的地位是等同的，因此与 DCS 相比使网络通信的可靠性得到了提高。

（4）现场总线通信方式可以传递现场仪表所测量的多种参数，且现场仪表之间还可以进行多对多的通信。

（5）现场总线正推进国际标准化，因此可以保证系统的互操作性，不同厂家的设备之间可以交换信息，因此在构造控制系统时，不必局限于购买一个厂家的产品，使控制系统构成的自由度增加，用户可以自由选择不同制造商提供的性能价格比最优的现场设备和现场仪表，系统和仪表的供应商将提供“即插即用”的产品。

（6）现场总线将功能分散地分配给现场仪表，许多变送器不仅具有信号变换、补偿功能，而且还带有 PID 控制和运算功能，这样可以将传统 DCS 系统变送器—控制器—执行器的三层结构简化为变送控制器—执行器的两层结构，从而可大大减少设备数量，而且使控制彻底分散，提高了系统的可靠性、自治性和灵活性。

（7）现场总线技术具有自诊断和纠错功能，因此可以进一步提高系统通信的可靠性，并可发现和排除一部分现场仪表故障。

（8）现场总线为开放式互联网络，所有技术和标准都是公开的，用户可以集成不同制造商的通信网络，还可方便地共享网络数据库。

（9）现场总线复杂的系统程序都由厂家来提供，用户所要开发的内容较少且比较简便，系统开发易学、易用、易维护。

现场总线对自动控制系统给自动化系统产生了很大的影响，传统的信号制将由 4～20mA 模拟信号制转换为双向数字通信的现场总线信号，自动控制系统的体系结构将由模拟与数字的分散型控制系统（DCS）转换为全数字现场总线控制系统（FCS），进而自动控制、系统的设计方法和安装调试方式也将发生重大的变化，现行的现场设备和仪表的产品结构将发生重大变革，现场总线把自动控制系统和设备带进了信息网络之中形成为企业信息网络的底层，从而为实现企业信息集成和企业综合自动化提供了可行的基础。

1.1.3 现场总线给用户带来的好处

现场总线使自控设备与系统步入了信息网络的行列，为其应用开拓了更为广阔的领域；一对双绞线上可挂接多个控制设备，便于节省安装费用；节省维护开销；提高了系统的可靠性；为用户提供了更为灵活的系统集成主动权。

从现场总线技术本身来分析，它有两个明显的发展趋势：一是寻求统一的现场总线国际标准；二是 Industrial Ethernet 走向工业控制网络统一、开放的 TCP/IP。Ethernet 是 20 多年来发展最成功的网络技术，过去一直认为，Ethernet 是为 IT 领域应用而开发的，它与工业网络在实时性、环境适应性、总线馈电等许多方面的要求存在差距，在工业自动化领域只能得到有限应用。事实上，这些问题正在迅速得到解决，国内对 EPA 技术（Ethernet for Process Automation）也取得了很大的进展。

随着 FF HSE 的成功开发以及 PROFInet 的推广应用，可以预见 Ethernet 技术将会十分迅速地进入工业控制系统的各级网络。

使用现场总线技术给用户带来的好处（使用现场总线从硬件、组装、工程上的节省见图

1-5)：使用现场总线节省硬件成本；设计组态安装调试简便；系统的安全可靠性好；减少故障停机时间；系统维护设备更换和系统扩充方便；用户对系统配置设备选型有最大的自主权；完善了企业信息系统为实现企业综合自动化提供了基础。

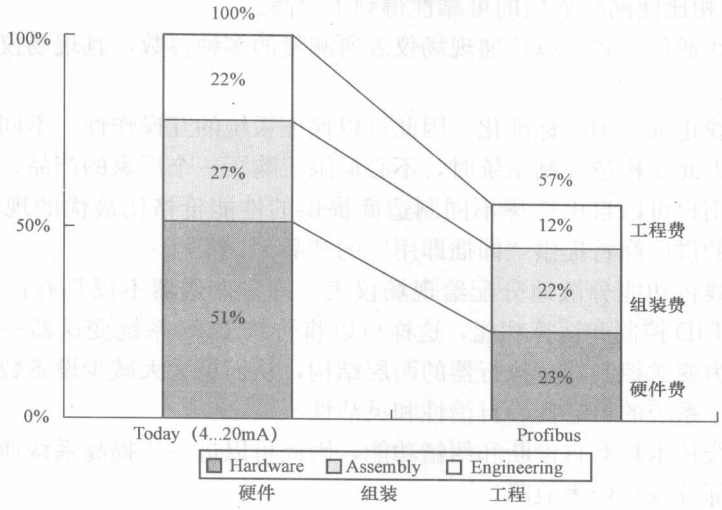

图 1-5 使用现场总线从硬件、组装、工程上的节省

1.1.4 主流现场总线简介

现场总线技术是控制、计算机、通信技术的交叉与集成，几乎涵盖了所有连续、离散工业领域，如过程自动化、制造加工自动化、楼宇自动化、家庭自动化等。它的出现和快速发展体现了控制领域对降低成本、提高可靠性、增强可维护性和提高数据采集的智能化的要求。现场总线技术的发展体现为两个方面：一个是低速现场总线领域的不断发展和完善；另一个是高速现场总线技术的发展。而目前现场总线产品主要是低速总线产品，应用于运行速率较低的领域，对网络的性能要求不是很高。从实际应用状况看，大多数现场总线，都能较好地实现速率要求较低的过程控制。因此，在速率要求较低的控制领域，谁都很难统一整个市场。就目前而言，由于 FF 基金会几乎集中了世界上主要自动化仪表制造商，其全球影响力日益增加，但其在中国市场营销力度似乎不足，市场份额不是很高；LonWorks 形成了全面的分工合作体系，在国内有一些实质性的进展，在楼宇自动化、家庭自动化、智能通信产品等方面，LonWorks 则具有独特的优势；在离散制造加工领域，由于行业应用的特点和历史原因，Profibus 和 CAN 在这一领域形成了自己的优势，具有较强的竞争力。国内厂商的规模相对较小，研发能力较差，更多的是依赖技术供应商的支持，比较容易受现场总线技术供应商（芯片制造商等）对国内的支持和市场推广力度的影响。而且，还有一个不可忽视的一点就是在构建自动化管理系统时，选择的上位机，比如组态软件对总线设备的支持程度，有些监控组态软件，比如紫金桥监控组态软件或者 InTouch 等对一些主流的总线设备（比如 LonWorks、Profibus、CAN 等）有着良好的支持，通过 DDE、OPC 或者直接连接等方式进行通信和采集数据。这样可以方便用户的选择，而一些组态软件则支持的种类较少，使用户选择的范围也随之减少。由于目前自动化技术从单机控制发展到工厂自动化 FA，发展到系统自动化。工厂自动化信息网络可分为以下三层结构：工厂管理级、车间监控级、现场

设备级，而现场总线是工厂底层设备之间的通信网络。

由于不同厂家纷纷推出了自己的现场总线控制系统，并规定了相应的标准，而现场总线的标准目前还没有统一起来，目前市场上出现的比较通用的现场总线系统有以下 11 种，下面对这些主流的现场总线做一简单介绍。

1. 基金会现场总线

现场总线基金会是国际公认的唯一不附属于某厂家的非商业化的国际标准化组织，其宗旨是制定单一的国际现场总线标准，它于 1994 年 9 月成立，国际上许多著名的仪表公司都加入了该组织。基金会现场总线（Foundation Fieldbus，FF）是以美国 Fisher－Rosemount 公司为首联合了横河、ABB、西门子、英维斯等 80 家公司制定的 ISP 协议和以 Honeywell 公司为首联合欧洲等地 150 余家公司制定的 WorldFIP 协议于 1994 年 9 月合并的。该总线在过程自动化领域得到了广泛的应用，具有良好的发展前景。基金会现场总线采用国际标准化组织 ISO 的开放系统互联 OSI 的简化模型（1、2、7 层），即物理层、数据链路层、应用层，另外增加了用户层。FF 提供了两种物理层标准 H1 和 H2。H1 为用于过程控制的低速总线，速率为 31.25kbit/s，传输距离为 200m（无屏蔽多芯电缆）、400m（无屏蔽多芯双绞线）和 1200m（屏蔽多芯双绞线）、1900m（屏蔽双绞线），由总线提供供电电源，每段节点数最多为 32 个，拓扑结构为总线型或树型，可支持总线供电和本质安全防爆环境。H2 为用于制造自动化的高速总线，传输速率为 1Mbit/s（750m）和 215Mbit/s（500m），传输媒介可以为屏蔽双绞线、同轴电缆、光纤和无线发射，协议符合 IEC1158－2 标准。FF 的物理媒介的传输信号采用曼彻斯特编码，每段最多可接 124 个节点，拓扑结构为总线型。H1 和 H2 之间通过网桥互联，目前已有多家公司生产 H1 低速总线的专用芯片，如 Honeywell、Yokogawa、National Semiconductor 等。

2. CAN

CAN（Controller Area Network，控制器局域网）协议是由德国 Bosch 公司为汽车的监测和控制而设计的，它广泛用于离散控制领域，得到了 Intel、Motorola、NEC 等公司的支持。目前它已逐步应用到其他工业部门的控制应用中，并已成为 ISO－11898 国际标准。CAN 的接口模块支持 8、16 位的 CPU，可做成 ISA 与 PCI 总线的插卡，也可置于温度、压力以及流量等物理量的变送器中，构成智能化仪表。CAN 支持多主工作方式，网络上任意节点可以在任意时刻主动向网络上其他节点发送信息，而不分主从，通信方式灵活，而且网络上的节点可以设定成不同的优先级，可以满足不同的实时要求。CAN 可以点对点、点对多点以及广播式发送或接收数据。CAN 协议分为两层：物理层和数据链路层。CAN 的信号传输采用短帧结构，传输时间短，具有自动关闭功能，具有较强的抗干扰能力。CAN 支持多主工作方式，并采用了非破坏性总线仲裁技术，通过设置优先级来避免冲突，通信最远距离为 10km（5kbit/s），通信速率最快可达到 1Mbit/s（40m），节点数目可达 110 个。CAN 采用 CRC 校验和其他纠错措施，保证了数据的可靠性，而且 CAN 节点在出现严重错误的情况下，还可自动切断它与总线的联系，可避免影响总线上其他节点的正常工作。CAN 的传输介质为普通双绞线或光纤，它链路比较简单，价格较低，芯片资源也很丰富，用户开发起来比较方便，因此获得了广泛应用。

3. LonWorks

LonWorks 由美国 Echelon 公司推出，并由 Motorola、Toshiba 公司共同倡导。它具有

统一性、开放性和互操作性。LonWorks 现场总线网络简称为 LON 网络，LON 网络的核心是 Neuron 芯片，它既能管理通信，又具有输入、输出能力，芯片内部含有三个 CPU，分别管理网络、介质访问和应用，芯片还附有固件，由固件实现通信协议和任务调度，用户不必将时间花在底层通信上，因此可以缩短开发时间。LON 网络采用的通信协议称为 LonTalk 协议，LonTalk 协议是遵循 OSI 七层参考模型的完整的七层协议，该协议对用户完全开放，而且任何制造商的产品都可以实现互操作，它支持多种通信媒介，包括双绞线、电力线、射频、红外线、同轴电缆和光纤等，LonTalk 协议支持检测 P 应答、自动重发、请求响应等消息服务类型，可以实现点到点、点到多点和广播式信息接收和发送方式。LON 网络在一个测控网络上的节点数最多可达到 32000 个，无论是哪一类节点，都含有用于控制和通信的 Neuron 芯片、用于连接一个或多个 IPO 设备的 IPO 接口，以及负责将节点连接上网的收发器，不同的通信媒介需要使用不同的收发器。

它采用 ISO/OSI 模型的全部七层通信协议，采用面向对象的设计方法，通过网络变量把网络通信设计简化为参数设置。支持双绞线、同轴电缆、光缆和红外线等多种通信介质，通信速率从 300bit/s 至 1.5Mbit/s 不等，直接通信距离可达 2700m（78kbit/s），被誉为通用控制网络。LonWorks 技术采用的 LonTalk 协议被封装到 Neuron（神经元）芯片中，并得以实现。采用 LonWorks 技术和神经元芯片的产品，被广泛应用在楼宇自动化、家庭自动化、保安系统、办公设备、交通运输、工业过程控制等行业。

Echelon 公司和其他一些公司提供了多种收发器产品，用户也可自行开发，对于双绞线来说，收发器支持总线和自由拓扑结构，对于不同的双绞线收发器，数据传输速率有 78kbit/s（500～2700m）和 1125Mbit/s（130m）两种，若采用其他通信媒介，则 Echelon 公司还可提供电力线收发器，Motorola 公司则可提供无线收发器，Echelon 公司还推出了不同的路由器产品，这些路由器可以连接不同的通信媒介或进行中继以延长数据传输距离。Echelon 公司又推出了 i. LON Internet 服务器，用户可以利用 i. LON 服务器将 LON 网络与 Internet 网连接在一起，这样就能够很方便地实现远程设备的连接，还可为不同企业共享同一网络中的信息资源提供标准的平台。

4. DeviceNet

DeviceNet 是一种低成本的通信连接也是一种简单的网络解决方案，有着开放的网络标准。DeviceNet 具有的直接互联性不仅改善了设备间的通信而且提供了相当重要的设备级阵地功能。DeviceNet 基于 CAN 技术，传输率为 125～500kbit/s，每个网络的最大节点为 64 个，其通信模式为：生产者/客户（Producer/Consumer），采用多信道广播信息发送方式。位于 DeviceNet 网络上的设备可以自由连接或断开，不影响网上的其他设备，而且其设备的安装布线成本也较低。DeviceNet 总线的组织结构是 Open DeviceNet Vendor Association（开放式设备网络供应商协会，简称“ODVA”）。

5. Profibus

Profibus 是以欧洲厂家和用户为主的过程自动化现场总线系统，是德国标准（DIN19245）和欧洲标准（EN50170）的现场总线标准。它是一种多主多从的令牌网络，目前它可提供三种模式，Profibus 由 Profibus－DP、Profibus－FMS、Profibus－PA 系列组成。Profibus－PA（H1，符合 IEC1158－2 标准），用于过程自动化，它是低速总线，可以提供总线供电和本质安全。网络中由耦合器连接和耦合两个不同的网段，耦合器还可起到供电

和隔爆作用。Profibus－DP（H2）可以和 Profibus－PA 兼容，实现分散外设间的高速数据传输，很多 PLC 支持该协议，用于连接 Profibus－PA 和加工自动化领域，Profibus－PA 和 Profibus－DP 段间通过耦合器相连，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。Profibus－FMS 用于一般自动化控制，支持多主处理，适用于纺织、楼宇自动化、可编程控制器、低压开关等。Profibus 是一种传输速率很高的现场总线，最高速率可达 12Mbit/s，是一种比较成熟的现场总线技术，Profibus 于 1999 年底成为国际标准 IEC 61158 中的一个组成部分。

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 下为 1200m，在 12Mbit/s 下为 200m，可采用中继器延长至 10km，传输介质为双绞线或光缆，最多可挂接 127 个站点。

6. HART

HART 是美国 Rosemount 公司推出的一种兼容 4～20mA 模拟信号和调控数字信号的现场总线协议，HART 协议参照 OSI 的模型标准，简化并引用其中的物理层、数据链路层和应用层制定而成。其特点是在现有模拟信号传输线上实现数字信号通信，属于模拟系统向数字系统转变的过渡产品。其通信模型采用物理层、数据链路层和应用层三层，支持点对点主从应答方式和多点广播方式。由于它采用模拟数字信号混合，难以开发通用的通信接口芯片。HART 能利用总线供电，可满足本质安全防爆的要求，并可用于由手持编程器与管理系统主机作为主设备的双主设备系统。它采用基于 Bell 202 通信标准的 FSK 技术，即在 4～20mA（DC）的模拟信号上叠加幅度为 0.5mA 的正弦调制波，逻辑 1 为 1200Hz，逻辑 0 为 2200Hz，波特率为 1200bit/s，由于所叠加的正弦信号平均值为 0，所以数字通信信号不会干扰 4～20mA 的模拟信号，因此可以做到在一根双绞线上 4～20mA 的模拟信号和数字信号同时传输。HART 通信可以有点对点或多点连接模式，但没有自诊断功能。用屏蔽双绞线单台设备距离为 3000m，多台设备互联距离为 1500m。由于目前 4～20mA 信号制的模拟设备还在大量使用，不可能一蹴而就地改为全数字信号的现场总线设备，因此 HART 作为一种 4～20mA 模拟信号与数字通信兼容的标准，国内外已有 70 多家企业采用了此协议。

7. CC－Link

CC－Link 是 Control & Communication Link（控制与通信链路系统）的缩写，CC－Link 为三菱电机公司开发的现场总线网络，它在实时性、分散控制与智能设备通信等方面都具有较好的功能性，它的通信速率较高，传送距离也较长，有 156kbit/s（1200m）、625kbit/s（600m）、215Mbit/s（200m）、5Mbit/s（150m）和 10Mbit/s（100m）等规格，使用 T 分支连接时，最大支线长度为 8m，此外，通过使用增幅器（T 形分支）或光纤增幅器，还可进一步延长传送距离，具有性能卓越、使用简单、应用广泛、节省成本等优点。该网络可与智能化设备进行通信，这些智能化设备包括显示设备、条形码读写器、测量设备以及计算机等，它具备自动在线恢复功能、待机主控功能、切断从站功能、确认链接状态功能以及测试和诊断功能，网络可靠性很高。三菱电机公司和合作生产厂家（包括日本电气株式会社、DIGITAL 电气公司等）开发出了许多 CC－Link 产品，包括专用电缆、CC－Link IPO 接口模块、可编程显示器、电磁阀、阀门终端、接口终端以及各种信号转换器、传感

器、控制器、调节器、网桥、适配器等，通过使用 CC－Link 接口板（PCI 总线）可将计算机连接到 CC－Link 系统上。CC－Link 的技术已完全公开，又具有丰富的支持产品，因此用户可以方便地选择最适用的产品，而且由于网络组网灵活，且可提供品种繁多、质量可靠的接口端子，配线也比较容易实现。

其不仅解决了工业现场配线复杂的问题，同时具有优异的抗噪性能和兼容性。CC－Link 是一个以设备层为主的网络，同时也可覆盖较高层次的控制层和较低层次的传感层。2005 年 7 月 CC－Link 被中国国家标准委员会批准为中国国家标准指导性技术文件。

8. WorldFIP

WorldFIP 的北美部分与 ISP 合并为 FF 以后，WorldFIP 的欧洲部分仍保持独立，总部设在法国。其在欧洲市场占有重要地位，特别是在法国占有率大约为 60%。WorldFIP 的特点是具有单一的总线结构来适用不同的应用领域的需求，而且没有任何网关或网桥，用软件的办法来解决高速和低速的衔接。WorldFIP 与 FF HSE 可以实现“透明连接”，并对 FF 的 H1 进行了技术拓展，如速率等。在与 IEC61158 第一类型的连接方面，WorldFIP 做得最好，走在了世界前列。

9. INTERBUS

INTERBUS 是德国 Phoenix 公司推出的较早的现场总线，2000 年 2 月成为国际标准 IEC61158 的一部分。INTERBUS 采用国际标准化组织 ISO 的开放系统互联 OSI 的简化模型（1、2、7 层），即物理层、数据链路层、应用层，具有强大的可靠性、可诊断性和易维护性。其采用集总帧型的数据环通信，具有低速度、高效率的特点，并严格保证了数据传输的同步性和周期性；该总线的实时性、抗干扰性和可维护性也非常出色。INTERBUS 广泛地应用到汽车、烟草、仓储、造纸、包装、食品等工业，成为国际现场总线的领先者。

此外，较有影响的现场总线还有丹麦公司 Process－Data A/S 提出的 P－Net，该总线主要应用于农业、林业、水利、食品等行业；SwiftNet 现场总线主要使用在航空航天等领域，还有一些其他的现场总线这里就不再赘述了。

10. 工业以太网

国际上形成的工业以太网技术的四大阵营，主要用于离散制造控制系统的是：Modbus－IDA 工业以太网、Ethernet/IP 工业以太网、PROFInet 工业以太网。主要用于过程控制系统的是：Foundation Fieldbus HSE 工业以太网。

工业以太网是作为办公室自动化领域衍生的工业网络协议，按习惯主要指 IEEE 802.3 协议，如果进一步采用 TCP/IP 协议族，则采用“以太网＋TCP/IP”来表示，其技术特点主要适合信息管理、信息处理系统，并在 IT 业得到了巨大的成功。在工厂管理级、车间监控级信息集成领域中，工业以太网已有不少成功的案例，在设备层对实时性没有严格要求场合也有许多应用。由于现场总线目前种类繁多，标准不一，很多人都希望以太网技术能介入设备低层，广泛取代现有的现场总线技术，施耐德公司以及台湾的 MOXA 公司等就是该想法的积极倡导者和实践者，目前已有一批工业级产品问世和实际应用。

11. 无线网络

随着通信技术的快速发展，短距离无线通信技术已经成为通信技术的一大热点。目前市

场上的焦点技术包括 ZigBee、Wi-Fi、3G/HSDPA、WiMAX、UWB、蓝牙等，其中 ZigBee 是一种具备低成本、近距离、低功耗、组网能力强等优点的无线互联标准，主要用于近距离无线连接，适合承载数据量小的工业现场控制、医疗设备控制、汽车自动化、农业自动化和消费类电子设备等。只要具有控制或者传感功能的现场仪表，在加入无线通信的功能后，再结合适当的网络拓扑机制，就能组成具有自动控制、传感以及监控等功能的电子设备网络系统。例如可以用于家庭看护监控、防盗入侵检测、家电网络自动化、工厂作业自动化、物流管理以及环境监测等。

ZigBee 名字来源于蜜蜂的通信方式，蜜蜂之间是通过 ZigZag 形状的舞蹈来相互交流信息，以便共享食物源的方向、距离和位置等信息。其标准是由 ZigBee 联盟与 IEEE 802.15.4 任务小组来共同制定的。其中，实体层、MAC 层、数据链路层，以及传输过程中的数据加密机制等发展由 IEEE 所主导。

ZigBee 与其他的短距离无线通信技术相比有不少优势，其对比如表 1-1 所示。

表 1-1　　ZigBee 与其他的短距离无线通信技术对比

种　类	ZigBee	蓝牙	Wi-Fi	移动通信	传统数传电台
单点覆盖距离	50～300m	10m	50m	可达几千米	可达 16 千米
网络扩展性	自动扩展	无	无	依赖现有网络覆盖	无
电池寿命	数年	数天	数小时	数天	数小时
复杂性	简单	复杂	非常复杂	复杂	复杂
传输速率	250kbit/s	1Mbit/s	1～11Mbit/s	38.4kbit/s	一般 19.2kbit/s
频段	868M～2.4GHz	2.4GHz	2.4GHz	0.8～1GHz	400M～2.4GHz
网络节点数	65000	8	50	无	
联网所需时间	仅 30ms	高达 10s	3s	数秒	
终端设备费用	低	低	高	较高	高
集成度和可靠性	高	高	一般	一般	低
使用成本	低	低	一般	高	高
安装使用难易度	非常简单	一般	难	一般	难

由表 1-1 不难总结 ZigBee 的如下优点：数据传输率低，10～250kbit/s，专注于低传输应用；功耗低，在低功耗待机模式下，两节普通 5 号电池可使用 6～24 个月；成本低，ZigBee 数据传输率低，协议简单，所以大大降低了成本；网络容量大，网络可容纳 65000 个设备；时延短，典型搜索设备时延为 30ms，休眠激活时延为 15ms，移动设备信道接入时延为 15ms；网络的自组织、自愈能力强，通信可靠；数据安全，ZigBee 提供了数据完整性检查和鉴权功能，采用 AES-128 加密算法（美国加密算法，是目前最好的文本加密算法之一），各种应用可灵活确定其安全属性；工作频段灵活，shoyng 频段为 2.4G、868MHz（欧洲）和 915MHz（美国），均为免执照（免费）的频段，而不同频段可使用的信道分别是 16、10、1 个。

12. 各种现场总线技术比较

几种常见的现场总线技术的比较如表 1-2 所示。

表 1-2 各种现场总线技术的比较

类别	FF	LonWorks	Profibus	CC-Link	HART	CAN
OSI	1，2，7	1～7	1，2，7	1，2，7	1，2，7	1，2
网络结构	总线或树型	总线或自由拓扑	总线	总线	总线	总线
通信媒介	双绞线、同轴电缆、光纤、无线电	双绞线、同轴电缆、无线电、电力线、红外光波	双绞线	双绞线、光纤、红外光波	双绞线	双绞线、同轴电缆、光纤
访问方式	单、多址、广播方式	单、多址、广播方式	单、多址、广播方式	广播方式	单、多址、广播方式	单、多址、广播方式
自诊断功能	有	有	有	有		有
最大通信速率	1Mbit/s	1.25Mbit/s	12Mbit/s	10Mbit/s	1200bit/s	1Mbit/s
网桥/路由器/中继器	有	有	有	有		
协议分析功能		有				
本质安全	可提供总线供电	可提供总线供电（电力线）	可提供总线供电			

现场总线技术的出现推动了整个控制技术的发展，目前现场总线技术的优越性正越来越受到全世界冶金、汽车、电力、机械制造以及楼宇自动化等领域技术人员和管理人员的重视。但在目前现场总线的标准还未完全统一，因此用户在选择现场总线技术时可以根据实际工程需要（现场条件、传输信号、传输速度、传输距离）以及造价、开发周期、开发难易程度等进行综合选择。在将来，现场总线技术会向着开放性、互操作性、支持多种通信媒介、网络结构灵活等方向发展。还需指出的是，现场总线系统的优越性主要体现在控制场合，而不是单纯的采集检测场合。

1.2 现场总线技术的标准化

1.2.1 HART 技术以及标准化

现代工业生产中存在着多种不同的主机和现场设备，为了获得稳定可靠的通信，完善的通信协议是必须的。HART 协议最初是由美国 Rosemount 公司开发，已应用了多年。HART 协议采用标准的 Bell202 频移键控信号以 1200bit/s 通信，使用 FSK 技术，在 4～20mA 信号过程量上叠加一个频率信号，成功地把模拟信号和数字信号同时双向通信，而不互相干扰，增加了远传数字通信的功能。HART 协议参照了国际标准化组织的开放系统互联模型，使用 OSI 标准的物理层、数据链路层、应用层。下面介绍 HART OSI 标准的各层内容。

HART 物理层规定了信号的传输方法、传输介质。采用 Bell202 标准的 FSK 频移键控信号，在低频的 4～20mA 模拟信号上叠加一个频率数字信号进行双向数字通信。数字信号的幅度为 0.5mA，数据传输率为 1200bit/s，1200Hz 代表逻辑“1”，2200Hz 代表逻辑“0”。数字信号波形如图 1-6 所示。

HART 数据链路层规定 HART 协议帧的格式，可寻址范围 0～15，“0”时处于 4～

20mA及数字信号点对点模式，现场仪表与两个数字通信主设备（也称为通信设备或主设备）之间采用特定的串行通信，主设备包括PC机或控制室系统和手持通信器。单站操作中，主变量（过程变量）可以以模拟形式输出，也可以以数字通信方式读出，以数字方式读出时，轮询地址始终为0。也就是说，单站模式时数字信号和4～20mA模拟信号同时有效。“1～15”处于全数字通信状态，工作在点对多点模式，通信模式有“问答”式、“突发”式（点对点、自动连续地发送信息）。按问答方式工作时的数据更新速率为2～3次/s，按突发方式工作时的数据更新速率为3～4次/s。

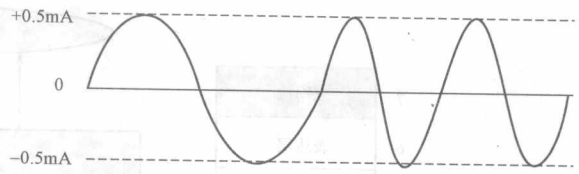

图1-6 数字信号波形

在本质安全要求下，只使用一个电源，至多能连接15台现场仪表，每个现场设备可有256个变量，每个信息最大可包含4个变量。这就是所谓的多点（多站）操作模式。这种工作方式尤其适用于远程监控，如管道系统和油罐储存场地。采用多点模式，4～20mA的模拟输出信号不再有效（输出设在4mA时功耗最小，主要是为变送器供电，各个现场装置并联连接），系统以数字通信方式依次读取并联到一对传输线上的多台现场仪表的测量值（或其他数据）。如果以这种方式构成控制系统，可以显著地降低现场布线的费用和减少主设备输入接口电路，这对于控制系统有重要价值。HART协议根据冗余检错码信息，采用自动重复请求发送机制，消除由于线路噪声或其他干扰引起的数据误码，实现数据无差错传送。能利用总线供电，可满足本质安全防爆要求。

HART协议的帧格式以8位为一个字节进行编码，对每个字节加上一个起始位、一个奇偶校验位和一个停止位以串行方式进行传输。通常采用UART（通用异步接收/发送器）来完成字节的传输。由于数据的有无和长短不恒定，所以HART数据的长度不能超过25个字节。一条消息包括源地址、目的地址和一个校验位。每一个应答消息中包括现场设备状态，用于确保持续通信的顺畅进行。数据位可有可无，视具体情况而定。一般每秒钟可以传输2～3条消息。

应用层：操作命令处于应用层，包括通用命令、普通命令和特殊命令。本部分由于涉及具体的命令操作，具体详细内容将在后续章节中介绍。

1.2.2 Profibus技术及标准化

Profibus技术是由Siemens公司等13家企业和5家研究机构联合开发，1989年批准为德国工业标准DIN 19245，1996年批准为欧洲标准EN50170 V.2（Profibus-FMS/-DP），1998年Profibus-PA批准纳入EN 50170 V.2。1999年Profibus成为国际标准IEC 61158的组成部分（Type Ⅲ），2001年批准成为JB/T 10308.3—2001。

ISO/OSI协议模型与Profibus协议模型的关系如图1-7所示，可见Profibus协议已经做了很大程度的简化。

Profibus协议详细的结构如图1-8所示。

1.2.3 Modbus总线技术以及标准化

Modbus是OSI模型第7层上的应用层报文传输协议，它在连接至不同类型总线或网络的设备之间提供客户机/服务器通信。自从出现工业串行链路的事实标准以来，Modbus使

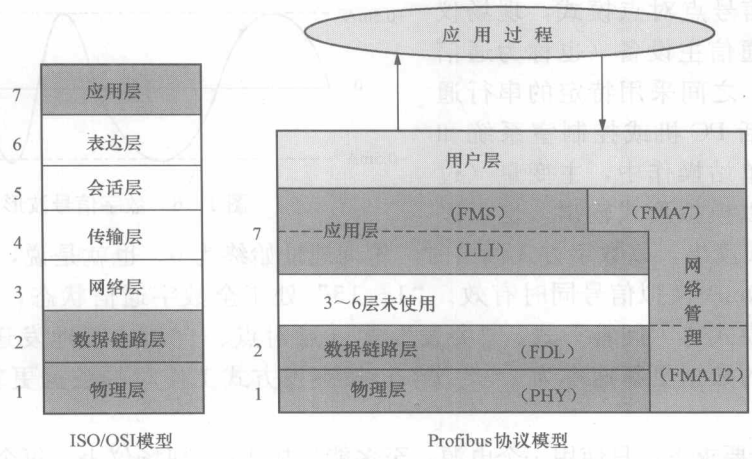

图 1-7 ISO/OSI 协议模型与 Profibus 协议模型的关系

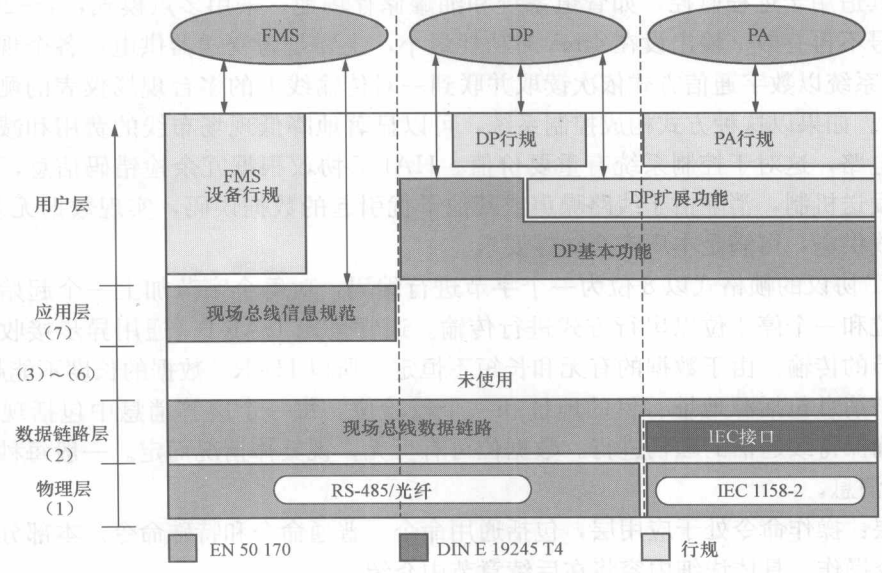

图 1-8 Profibus 协议结构

成千上万的自动化设备能够通信。目前，对 Modbus 结构的支持仍在不断增加。互联网组织能使 TCP/IP 栈上的保留系统端口 502 访问 Modbus。

Modbus 是一个请求/应答协议，并且提供功能码规定的服务。Modbus 功能码是 Modbus 请求/应答 PDU 的元素。Modbus 是一项应用层报文传输协议，用于在通过不同类型的总线或网络连接的设备之间的客户机/服务器通信。目前，使用下列情况实现 Modbus：以太网上的 TCP/IP；各种媒介（有线，如 EIA/TIA-232-E、EIA-422、EIA/TIA-485-A；光纤、无线等）上的异步串行传输。Modbus 通信协议栈如图 1-9 所示。

不熟悉 Modbus 的读者可能对一些缩略语不熟悉，下面简单列以下常用的术语。

ADU——应用数据单元；

HDLC——高级数据链路控制；

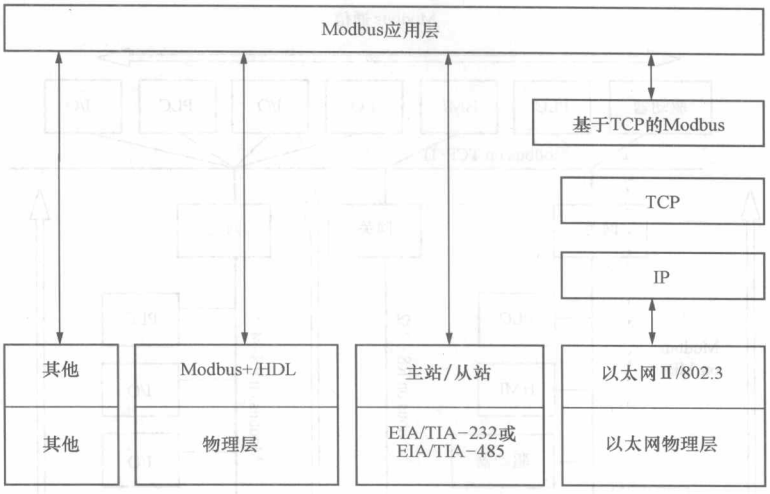

图 1-9 Modbus 通信协议栈

HMI——人机界面；

IETF——因特网工程工作组；

I/O——输入/输出设备；

IP——互联网协议；

MAC——介质访问控制；

MB Modbus——协议；

MBAP Modbus——协议；

PDU——协议数据单元；

PLC——可编程逻辑控制器；

TCP——传输控制协议。

Modbus 协议允许在各种网络体系结构内进行简单通信，Modbus 网络体系结构的实例如图 1-9 所示。

每种设备（PLC、HMI、控制面板、驱动程序、动作控制、输入/输出设备）都能使用 Modbus 协议来启动远程操作。在基于串行链路和以太 TCP/IP 网络的 Modbus 上可以进行相同通信。一些网关允许在几种使用 Modbus 协议的总线或网络之间进行通信。

Modbus 协议定义了一个与基础通信层无关的简单协议数据单元（PDU）。特定总线或网络上的 Modbus 协议映射能够在应用数据单元（ADU）上引入一些附加域。通用 Modbus 帧如图 1-11 所示。

启动 Modbus 事务处理的客户机创建 Modbus 应用数据单元。功能码向服务器指示将执行哪种操作。Modbus 协议建立了客户机启动的请求格式。用一个字节编码 Modbus 数据单元的功能码域。有效的码字范围是十进制 1～255（128～255 为异常响应保留）。当从客户机向服务器设备发送报文时，功能码域通知服务器执行哪种操作。向一些功能码加入子功能码来定义多项操作。从客户机向服务器设备发送的报文数据域包括附加信息，服务器使用这个信息执行功能码定义的操作。这个域还包括离散项目和寄存器地址、处理的项目数量以及域

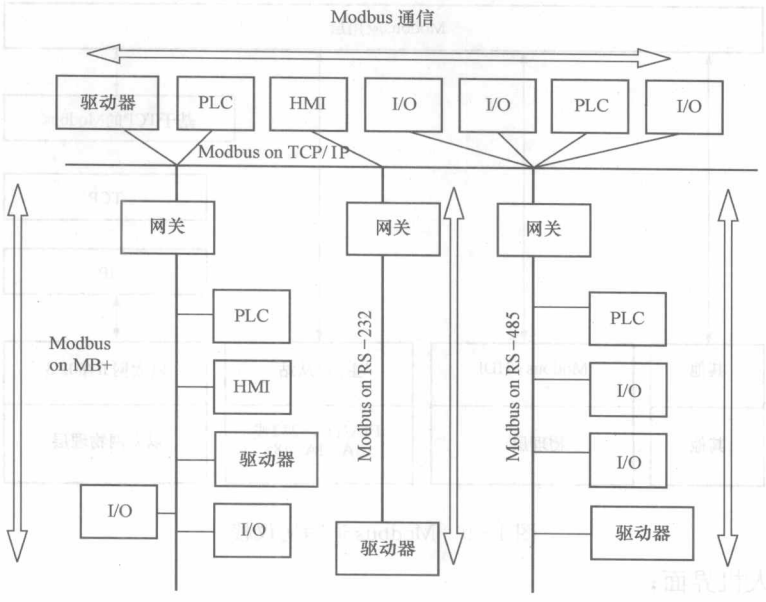

图 1-10 Modbus 网络体系结构的实例

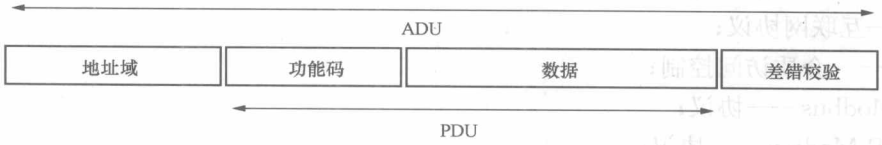

图 1-11 通用 Modbus 帧

中的实际数据字节数。在某种请求中，数据域可以是不存在的（0 长度），在此情况下服务器不需要任何附加信息。功能码仅说明操作。如果在一个正确接收的 Modbus ADU 中，不出现与请求 Modbus 功能有关的差错，那么服务器至客户机的响应数据域包括请求数据。如果出现与请求 Modbus 功能有关的差错，那么域包括一个异常码，服务器应用能够使用这个域确定下一个执行的操作。例如，客户机能够读一组离散量输出或输入的开/关状态，或者客户机能够读/写一组寄存器的数据内容。当服务器对客户机响应时，它使用功能码域来指示正常（无差错）响应或者出现某种差错（称为异常响应）。对于一个正常响应来说，服务器仅对原始功能码响应。正常响应的 Modbus 事务处理（无差错）如图 1-12 所示，异常响应的 Modbus 事务处理如图 1-13 所示。

对于异常响应，服务器返回一个与原始功能码等同的码，设置该原始功能码的最高有效位为逻辑 1。

串行链路上第一个 Modbus 执行的长度约束限制了 Modbus PDU 大小（最大 RS-485ADU=256 字节）。因此，对串行链路通信来说，Modbus PDU=256－服务器地址（1 字节）－CRC（2 字节）=253 字节。从而：RS-232 / RS-485 ADU=253 字节＋服务器地址（1 byte）＋CRC（2 字节）=256 字节。TCP Modbus ADU=249 字节＋MBAP（7 字节）=256 字节。Modbus 协议定义了三种 PDU。它们是：Modbus 请求 PDU，mb _ req _ pdu；Modbus 响应 PDU，mb _ rsp _ pdu；Modbus 异常响应 PDU，mb _ excep _ rsp _ pdu；

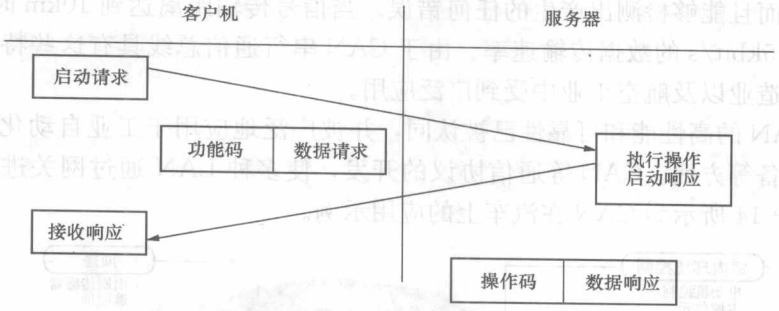

图 1-12 Modbus 事务处理（无差错）

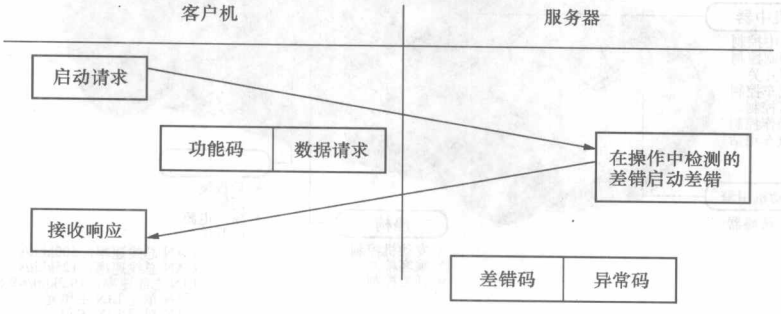

图 1-13 Modbus 事务处理（异常响应）

定义 mb _ req _ pdu 为 mb _ req _ pdu＝｛function _ code，request _ data｝，其中 function _ code，包括 1 个字节，是 Modbus 的功能码。request _ data－［n 个字节］，这个域与功能码有关，并且通常包括诸如可变参考量、变量、数据偏移量、子功能码等信息。

定义 mb _ rsp _ pdu 为 mb _ rsp _ pdu＝｛function _ code，response _ data｝，其中 function _ code－［1 个字节］Modbus 功能码。response _ data－［n 个字节］，这个域与功能码有关，并且通常包括诸如可变参考量、变量、数据偏移量、子功能码等信息。

定义 mb _ excep _ rsp _ pdu 为 mb _ excep _ rsp _ pdu＝｛ function _ code，request _ data｝，其中 function _ code－［1 个字节］Modbus 功能码＋0x80。

1.2.4 CAN 总线技术以及标准化

CAN 是 Controller Area Network 的缩写，即控制器局域网，是 ISO 国际标准化的串行通信协议。CAN－bus 是国际上应用最广泛的现场总线之一。起先，CAN－bus 被设计作为汽车环境中的微控制器通信，在车载各电子控制装置 ECU 之间交换信息，形成汽车电子控制网络。比如，发动机管理系统、变速箱控制器、仪表装备、电子主干系统中，均嵌入 CAN 控制装置。在当前的汽车产业中，出于对安全性、舒适性、方便性、低公害、低成本的要求，各种各样的电子控制系统被开发了出来。由于这些系统之间通信所用的数据类型及对可靠性的要求不尽相同，由多条总线构成的情况很多，线束的数量也随之增加。为适应“减少线束的数量”、“通过多个 LAN，进行大量数据的高速通信”的需要，1986 年德国电气商博世公司开发出面向汽车的 CAN 通信协议。此后，CAN 通过 ISO11898 及 ISO11519 进行了标准化，现在在欧洲已是汽车网络的标准协议。

CAN－bus 是一种多主方式的串行通信总线，基本设计规范要求有较高的位速率，高抗