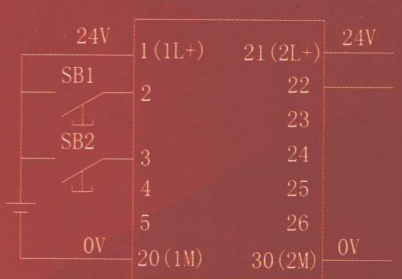
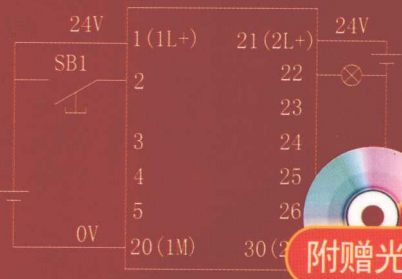
SIEMENS

西门子 PLC 工业通信网络应用案例精讲

向晓汉　陆 彬　编著





附赠光盘

化学工业出版社

SIEMENS

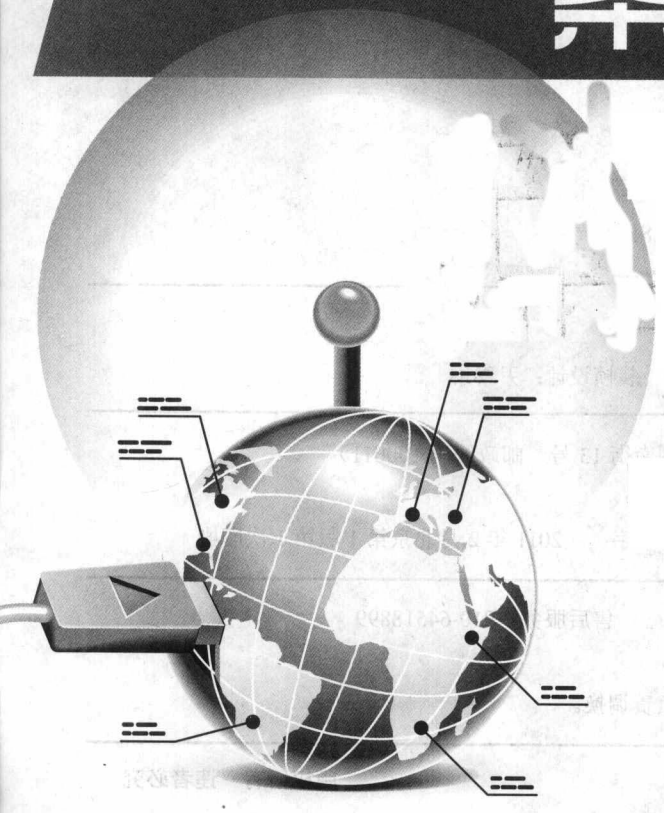
西门子 PLC 工业通信网络应用案例精讲

SIEMENS

西门子 PLC

工业通信网络应用案例精讲

向晓汉　陆 彬　编著



化学工业出版社

·北京·

图书在版编目(CIP)数据

西门子 PLC 工业通信网络应用案例精讲 / 向晓汉，陆彬编著.
北京：化学工业出版社，2011.2
ISBN 978-7-122-09965-5

Ⅰ. 西… Ⅱ. ①向… ②陆… Ⅲ.可编程序控制器-应用-通信网 Ⅳ. ①TP332.3②TN915

中国版本图书馆 CIP 数据核字（2010）第 228825 号

责任编辑：李军亮　　文字编辑：云　雷
责任校对：蒋　宇　　装帧设计：尹琳琳

出版发行：化学工业出版社（北京市东城区青年湖南街 13 号　邮政编码 100011）
印　　装：三河市延风印装厂
787mm×1092mm　1/16　印张 17¾　字数　430　千字　　2011 年 2 月北京第 1 版第 1 次印刷

购书咨询：010-64518888（传真：010-64519686）　售后服务：010-64518899
网　　址：http: // www. cip. com. cn
凡购买本书，如有缺损质量问题，本社销售中心负责调换。

定　　价：48.00 元

前　言

随着计算机技术的发展，以可编程序控制器、变频器调速和计算机通信等技术为主体的新型电气控制系统已经逐渐取代传统的继电器控制系统，并广泛应用于各行业。由于西门子PLC具有的卓越的性能，因此在电气控制领域占有非常大的市场份额，应用十分广泛。PLC通信和张力控制是PLC控制中公认的难点，对于那些刚入门的读者来说就更是如此，因此，为了使读者能更好地掌握西门子PLC在网络通信中的应用技术，我们在总结长期的教学经验和工程实践的基础上，联合相关企业人员，共同编写了本书。

我们在编写过程中，将一些生动的操作实例融入到实际中，以提高读者的学习兴趣。本书具有以下特点。

① 用实例引导读者学习。该书的内容全部用精选的例子讲解。例如，用实例说明现场总线通信的实现的全过程。

② 所有的实例都包含软硬件的配置方案图、接线图和程序，而且为确保程序的正确性，程序已经在PLC上运行通过。

③ 对于比较复杂的例子，随书光盘中有录像和程序源代码。如工业以太网通信的硬件组态较复杂，就配有录像和程序源代码，读者可以在出版社的网站上下载，便于读者学习。

④ 本书实用性较强，实例容易被读者进行工程移植。

本书第1、3、5、6章由无锡雷华科技有限公司的陆彬编写，第2、4、7、8章由无锡职业技术学院的向晓汉编写；本书由陆金荣高级工程师主审。另外，在编写过程中无锡职业技术学院机电教研室的教师提出了许多宝贵的意见，在此深表感谢！

由于编者水平有限，书中不妥之处在所难免，敬请读者批评指正。

编　者

目录

第1章 概 述

1.1 通信基础知识

PLC 的通信包括 PLC 之间的通信、PLC 与上位计算机之间的通信以及和其他智能设备之间的通信。PLC 之间通信的实质就是计算机的通信，使得众多的独立的控制任务构成一个控制工程整体，形成模块控制体系。PLC 与计算机连接组成网络，将 PLC 用于控制工业现场，计算机用于编程、显示和管理等任务，构成“集中管理、分散控制”的分布式控制系统（DCS）。

1.1.1 通信的基本概念

（1）串行通信与并行通信

串行通信和并行通信是两种不同的数据传输方式。

并行通信就是将一个 8 位数据（或 16 位、32 位）的每一个二进制位采用单独的导线进行传输，并将传送方和接收方进行并行连接，一个数据的各二进制位可以在同一时间内一次传送。例如，老式打印机的打印口和计算机的通信就是并行通信。并行通信的特点是一个周期里可以一次传输多位数据，其连线的电缆多，因此长距离传送时成本高。

串行通信就是通过一对导线将发送方与接收方进行连接，传输数据的每个二进制位，按照规定顺序在同一导线上依次发送与接收。例如，常用的优盘的 USB 接口就是串行通信。串行通信的特点是通信控制复杂，通信电缆少，因此与并行通信相比，成本低。串行通信是一种趋势，随着串行通信速率的提高，以往使用并行通信的场合，现在完全或部分被串行通信取代，如打印机的通信，现在基本被串行通信取代，再如个人计算机硬盘的数据通信，现在已经被串行通信取代。

（2）异步通信与同步通信

异步通信与同步通信也称为异步传送与同步传送，这是串行通信的两种基本信息传送方式。从用户的角度上说，两者最主要的区别在于通信方式的“帧”不同。

异步通信方式又称起止方式。它在发送字符时，要先发送起始位，然后是字符本身，最后是停止位，字符之后还可以加入奇偶校验位。异步通信方式具有硬件简单、成本低的特点，主要用于传输速率低于 19.2kbit/s 以下的数据通信。

同步通信方式在传递数据的同时，也传输时钟同步信号，并始终按照给定的时刻采集数据。其传输数据的效率高，硬件复杂，成本高，一般用于传输速率高于 20kbit/s 以上的数据通信。

（3）单工、双工与半双工

单工、双工与半双工是通信中描述数据传送方向的专用术语。

① 单工（Simplex） 指数据只能实现单向传送的通信方式，一般用于数据的输出，不可

以进行数据交换。

② 全双工（Full Simplex） 也称双工，指数据可以进行双向数据传送，同一时刻既能发送数据，也能接收数据。通常需要两对双绞线连接，通信线路成本高。例如，RS-422 就是“全双工”通信方式。

③ 半双工（Half Simplex） 指数据可以进行双向数据传送，同一时刻，只能发送数据或者接收数据。通常需要一对双绞线连接，与全双工相比，通信线路成本低。例如，RS-485 只用一对双绞线时就是“半双工”通信方式。

1.1.2 RS-485 标准串行接口

（1）RS-485 接口

RS-485 接口是在 RS-422 基础上发展起来的一种 EIA 标准串行接口，采用“平衡差分驱动”方式。RS-485 接口满足 RS-422 的全部技术规范，可以用于 RS-422 通信。RS-485 接口通常采用 9 针连接器。RS-485 接口的引脚功能参见表 1-1。

表 1-1 RS-485 接口的引脚功能

PLC 侧引脚	信 号 代 号	信 号 功 能
1	SG 或 GND	机壳接地
2	+24V 返回	逻辑地
3	RXD+或 TXD+	RS-485 的 B，数据发送/接收+端
4	+5V 返回	逻辑地
5	+5V	+5V
6	+24V	+24V
7	RXD－或 TXD－	RS-485 的 A，数据发送/接收－端
8	不适用	10 位协议选择（输入）

（2）西门子的 PLC 连线

西门子 PLC 的 PPI 通信、MPI 通信和 PROFIBUS-DP 现场总线通信的物理层都是 RS-485 通信，而且都是采用相同的通信线缆和专用网络接头。西门子提供两种网络接头，即标准网络接头和包括编程端口接头，可方便地将多台设备与网络连接，编程端口允许用户将编程站或 HMI 设备与网络连接，而不会干扰任何现有网络连接。编程端口接头通过编程端口传送所有来自 S7-200 CPU 的信号（包括电源针脚），这对于连接由 S7-200 CPU（例如 SIMATIC 文本显示）供电的设备尤其有用。标准网络接头的编程端口接头均有两套终端螺钉，用于连接输入和输出网络电缆。这两种接头还配有开关，可选择网络偏流和终端。图 1-1 显示了电缆接头的普通偏流和终端状况，将拨钮拨向一侧，电阻设置为“on”，而将拨钮拨向另一侧，则电阻设置为“off”，图中只显示了一个，若有多个也是这样设置。图 1-1 中拨钮在“off”一侧，因此终端电阻未接入电路。

【关键点】 西门子的专用 PROFIBUS 电缆中有两根线，一根为红色，上标有“B”，一根为绿色，上面标有“A”，这两根线只要与网络接头上相对应的“A”和“B”接线端子相连即可（如“A”线与“A”接线端相连）。网络接头直接插在 PLC 的 PORT 口上即可，不需要其他设备。注意：三菱的 FX 系列 PLC 的 RS-485 通信要加 RS-485 专用通信模块和终端电阻。

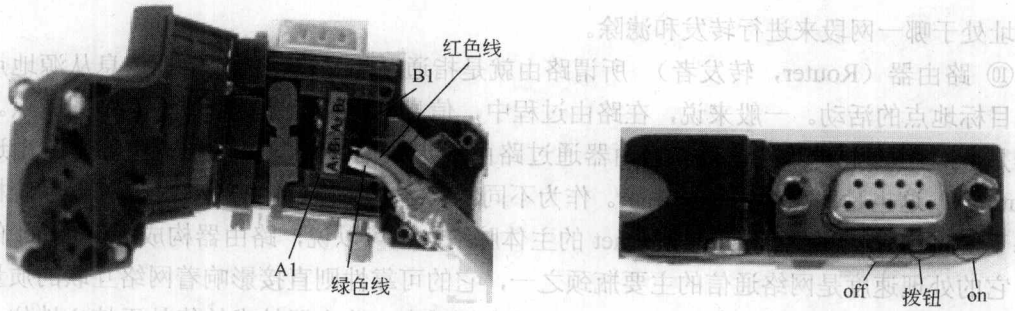


图 1-1　网络接头的终端电阻设置图

1.1.3　PLC 网络的术语解释

PLC 网络中的名词、术语很多，现将常用的予以介绍。

① 站（Station）　在 PLC 网络系统中，将可以进行数据通信、连接外部输入/输出的物理设备称为“站”。例如，由 PLC 组成的网络系统中，每台 PLC 可以是一个“站”。

② 主站（Master Station）　PLC 网络系统中进行数据链接的系统控制站，主站上设置了控制整个网络的参数，每个网络系统只有一个主站，主站号的固定为“0”，站号实际就是 PLC 在网络中的地址。

③ 从站（Slave Station）　PLC 网络系统中，除主站外，其他的站称为“从站”。

④ 远程设备站（Remote Device Station）　PLC 网络系统中，能同时处理二进制位、字的从站。

⑤ 本地站（Local Station）　PLC 网络系统中，带有 CPU 模块并可以与主站以及其他本地站进行循环传输的站。

⑥ 站数（Number of Station）　PLC 网络系统中，所有物理设备（站）所占用的“内存站数”的综合。

⑦ 网关（Gateway）　又称网间连接器、协议转换器。网关在传输层上以实现网络互联，是最复杂的网络互联设备，仅用于两个高层协议不同的网络互联。网关的结构和路由器类似，不同的是互联层。网关既可以用于广域网互联，也可以用于局域网互联。网关是一种充当转换重任的计算机系统或设备。在使用不同的通信协议、数据格式或语言，甚至体系结构完全不同的两种系统之间，网关是一个翻译器。例如 AS-I 网络的信息要传送到由西门子 S7-200 系列 PLC 组成的 PPI 网络，就要通过 CP243-2 通信模块进行转换，这个模块实际上就是网关。

⑧ 中继器（Repeater）　用于网络信号放大、调整的网络互联设备，能有效延长网络的连接长度。例如，以太网的正常传送距离是 500m，经过中继器放大后，可传输 2500m。由于存在损耗，在线路上传输的信号功率会逐渐衰减，衰减到一定程度时将造成信号失真，因此会导致接收错误。中继器就是为解决这一问题而设计的。它完成物理线路的连接，对衰减的信号进行放大，保持与原数据相同。一般情况下，中继器的两端连接的是相同的媒体，但有的中继器也可以完成不同媒体的转接工作。

⑨ 网桥（Bridge）　网桥将两个相似的网络连接起来，并对网络数据的流通进行管理。网桥的功能在延长网络跨度上类似于中继器，然而它能提供智能化连接服务，即根据帧的终

点地址处于哪一网段来进行转发和滤除。

⑩ 路由器（Router，转发者） 所谓路由就是指通过相互连接的网络把信息从源地点移动到目标地点的活动。一般来说，在路由过程中，信息至少会经过一个或多个中间节点。路由器是互联网的主要节点设备。路由器通过路由决定数据的转发。转发策略称为路由选择（Routing），这也是路由器名称的由来。作为不同网络之间互相连接的枢纽，路由器系统构成了基于 TCP/IP 的国际互联网络 Internet 的主体脉络，也可以说，路由器构成了 Internet 的骨架。它的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互联的质量。因此，在园区网、地区网乃至整个 Internet 研究领域中，路由器技术始终处于核心地位，其发展历程和方向，成为整个 Internet 研究的一个缩影。

⑪ 交换机（Switch） 交换机是一种基于 MAC 地址识别，能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC 地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

交换机通过直通式、存储转发和碎片隔离三种方式进行交换。

交换机的传输模式有全双工、半双工和全双工/半双工自适应。

1.1.4 OSI 参考模型

通信网络的核心是 OSI（OSI-Open System Interconnection，开放式系统互联）参考模型。为了理解网络的操作方法，为创建和实现网络标准、设备和网络互联规划提供了一个框架。1984 年，国际标准化组织（ISO），提出了开放式系统互联的七层模型，即 OSI 模型。该模型自下而上分为物理层、数据链接层、网络层、传输层、会话层、表示层和应用层。理解 OSI 参考模型比较难，但了解它，对掌握后续的以太网通信和 PROFIBUS 通信是很有帮助的。

OSI 的上三层通常称为应用层，用来处理用户接口、数据格式和应用程序的访问。下四层负责定义数据的物理传输介质和网络设备。OSI 参考模型定义了大多数协议栈共有的基本框架，如图 1-2 所示。

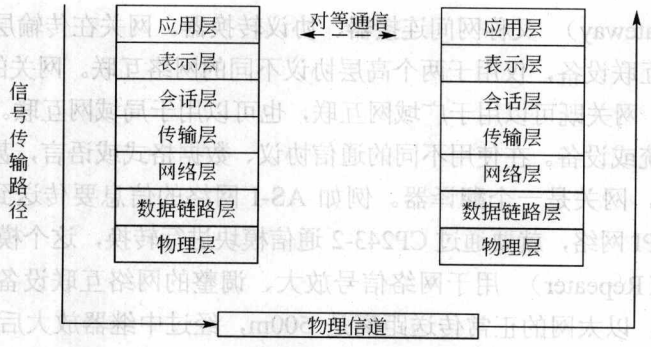


图 1-2 信息在 OSI 模型中的流动形式

① 物理层（Physical Layer） 定义了传输介质、连接器和信号发生器的类型，规定了物理连接的电气、机械功能特性，如电压、传输速率、传输距离等特性。典型的物理层设备有集线器（HUB）和中继器等。

② 数据链路层（Data Link Layer） 确定传输站点物理地址以及将消息传送到协议栈，

提供顺序控制和数据流向控制。该层可以继续分为两个子层：介质访问控制层（MAC，Medium Access Control）和逻辑链路层（LLC，Logical Link Control Layer），即层 2a 和 2b。其中 IEEE802.3（Ethernet，CSMA/CD）就是 MAC 层常用的通信标准。典型的数据链路层的设备有交换机和网桥等。

③ 网络层（Network Layer） 定义了设备间通过逻辑地址（IP-Internet Protocol 因特网协议地址）传输数据，连接位于不同广播域的设备，常用来组织路由。典型的网络层设备是路由器。

④ 传输层（Transport Layer） 建立会话连接，分配服务访问点（SAP-Service Access Point），允许数据进行可靠（TCP，Transmission Control Protocol，传输控制协议）或者不可靠（UDP，User Datagram Protocol，用户数据报协议）的传输。可以提供通信质量检测服务（QOS）。网关是互联网设备中最复杂的，它是传输层及以上层的设备。

⑤ 会话层（Session Layer） 负责建立、管理和终止表示层实体间通信会话，处理不同设备应用程序间的服务请求和响应。

⑥ 表示层（Presentation Layer） 提供多种编码用于应用层的数据转化服务。

⑦ 应用层（Application Layer） 定义用户及用户应用程序接口与协议对网络访问的切入点。目前各种应用版本较多，很难建立统一的标准。在工控领域常用的标准是 MMS（Multimedia Messaging Service 多媒体信息服务），用来描述制造业应用的服务和协议。

数据经过封装后通过物理介质传输到网络上，接收设备除去附加信息后，将数据上传到上层堆栈层。

各层的数据单位一般有各自特定的称呼。物理层的单位是比特（bit）；数据链路层的单位是帧（frame）；网络层的单位是分组（packet，有时也称包）；传输层的单位是数据报（datagram）或者段（segment）；会话层、表示层和应用层的单位是消息（message）。

1.2 SIMATIC NET 工业通信网络

SIMATIC NET 是西门子工业网络通信解决方案的统称。

1.2.1 工业通信网络结构

通常，企业的通信网络可分为三级：企业级、车间级和现场级，以下分别介绍。

（1）企业级通信网络

企业级通信网络用于企业的上层管理，为企业提供生产、管理和经营数据，通过数据化的方式优化企业资源，提高企业的管理水平。这个层中，IT 技术得到了广泛的应用，如 Internet 和 Intranet。

（2）车间级通信网络

车间级通信网络介于企业级和现场级之间。其主要功能是解决车间内各需要协调工作的不同工艺段之间的通信。车间级通信网络要求能传递大量的信息数据和少量控制信息，而且要求具备较强的实时性。这个层主要使用工业以太网。

（3）现场级通信网络

现场级通信网络处于工业网络的最底层，直接连接现场的各种设备，包括 I/O 设备、变

频与驱动、传感器和变送器等，由于连接的设备千差万别，因此所使用的通信方式也比较复杂。又由于现场级通信网络直接连接现场设备，网络上传递的主要是控制信号，因此，对网络的实时性和确定性有很高的要求。

SIMATIC NET 中，现场级通信网络中主要使用 PROFIBUS。同时 SIMATIC NET 也支持 AS-Interface、EIB 等总线技术。

1.2.2 通信网络技术说明

（1）MPI 通信

MPI（Multi-Point Interface，即多点接口）协议，用于小范围、少点数的现场级通信。MPI 是为 S7/M7/C7 系统提供接口，它设计用于编程设备的接口，也可用于在少数 CPU 间传递少量的数据。

（2）PROFIBUS 通信

PROFIBUS 符合国际标准 IEC61158，是目前国际上通用的现场总线中 8 大现场总线之一，并以独特的技术特点、严格的认证规范、开放的标准和众多的厂家支持，成为现场级通信网络的优秀解决方案，目前其全球网络节点已经突破 1000 万个。

从用户的角度看，PROFIBUS 提供三种通信协议类型：PROFIBUS-FMS、PROFIBUS-DP 和 PROFIBUS-PA。

① PROFIBUS-FMS（Fieldbus Message Specification，现场总线报文规范）主要用于系统级和车间级的不同供应商的自动化系统之间传输数据，处理单元级（PLC 和 PC）的多主站数据通信。

② PROFIBUS-DP（Decentralized Periphery，分布式外部设备）用于自动化系统中单元级控制设备与分布式 I/O（例如 ET 200）的通信。主站之间的通信为令牌方式，主站与从站之间为主从方式，以及这两种方式的混合。

③ PROFIBUS-PA（Process Automation，过程自动化）用于过程自动化的现场传感器和执行器的低速数据传输，使用扩展的 PROFIBUS-DP 协议。

（3）工业以太网

工业以太网符合 IEEE802.3 国际标准，是功能强大的区域和单元网络，是目前工控界最为流行的网络通信技术之一。

（4）点对点连接

严格地说，点对点（Point-to-Point）连接并不是网络通信。但点对点连接可以通过串口连接模块实现数据交换，应用比较广泛。

（5）AS-Interface

传感器/执行器接口用于自动化系统最底层的通信网络。它专门用来连接二进制的传感器和执行器，每个从站的最大数据量为 4bit。

第 2 章　西门子 PLC 的自由口通信

2.1　自由口通信概述

S7-200 的自由口通信是基于 RS-485 通信基础的半双工通信，西门子 S7-200 系列 PLC 拥有自由口通信功能，顾名思义，就是没有标准的通信协议，用户可以自己规定协议。第三方设备大多支持 RS-485 串口通信，西门子 S7-200 系列 PLC 可以通过自由口通信模式控制串口通信。最简单的使用案例就是只用发送指令（XMT）向打印机或者变频器等第三方设备发送信息。不管任何情况，都通过 S7-200 系列 PLC 编写程序实现。

自由口通信的核心就是发送（XMT）和接收（RCV）两条指令，以及相应的特殊寄存器控制。由于 S7-200 CPU 通信端口是 RS-485 半双工通信口，因此发送和接收不能同时处于激活状态。RS-485 半双工通信串行字符通信的格式可以包括一个起始位、7 或 8 位字符（数据字节）、一个奇/偶校验位（或者没有校验位）、一个停止位 。

自由口通信的波特率可以设置为 1200、2400、4800、9600、19200、38400、57600 或 115200。凡是符合这些格式的串行通信设备，理论上都可以和 S7-200 CPU 通信。自由口模式可以灵活应用。STEP7-Micro/WIN 的两个指令库（**USS** 和 **Modbus RTU**）就是使用自由口模式编程实现的。

S7-200 CPU 使用 SMB30（对于 Port0）和 SMB130（对于 Port1）定义通信口的工作模式，控制字节的定义如图 2-1 所示。

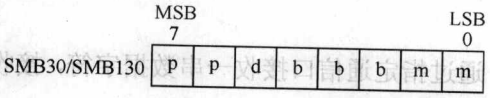


图 2-1　控制字节的定义

① 通信模式由控制字的最低的两位“mm”决定。

- mm=00：PPI 从站模式（默认这个数值）。
- mm=01：自由口模式 。
- mm=10：PPI 主站模式 。

所以，只要将 SMB30 或 SMB130 赋值为 2#01，即可将通信口设置为自由口模式。

② 控制位的“pp”是奇偶校验选择。

- pp=00：无校验。
- pp=01：偶校验。
- pp=10：无校验。
- pp=11：奇校验 。

③ 控制位的“d”是每个字符的位数。

- d=0：每个字符 8 位。

- d=1：每个字符 7 位。

④ 控制位的“bbb”是波特率选择。

- bbb=000： 38400bit/s。
- bbb=001： 19200bit/s。
- bbb=010： 9600bit/s。
- bbb=011： 4800bit/s。
- bbb=100： 2400bit/s。
- bbb=101： 1200bit/s。
- bbb=110： 115200bit/s。
- bbb=111： 57600bit/s。

（1）发送指令

以字节为单位，XMT 向指定通信口发送一串数据字符，要发送的字符以数据缓冲区指定，一次发送的字符最多为 255 个。

发送完成后，会产生一个中断事件，对于 Port0 口为中断事件 9，而对于 Port1 口为中断事件 26。当然也可以不通过中断，而通过监控 SM4.5（对于 Port0 口）或者 SM4.6（对于 Port1 口）的状态来判断发送是否完成，如果状态为 1，说明完成。XMT 指令缓冲区格式见表 2-1。

表 2-1 XMT 指令缓冲区格式

序 号	字节编号	内 容
1	*T*+0	发送字节的个数
2	*T*+1	数据字节
3	*T*+2	数据字节
⋮	⋮	⋮
256	*T*+255	数据字节

（2）接收指令

以字节为单位，RCV 通过指定通信口接收一串数据字符，接收的字符保存在指定的数据缓冲区，一次接收的字符最多为 255 个。

接收完成后，会产生一个中断事件，对于 Port0 口为中断事件 23，而对于 Port1 口为中断事件 24。当然也可以不通过中断，而通过监控 SMB86（对于 Port0 口）或者 SMB186（对于 Port1 口）的状态来判断发送是否完成，如果状态为非零，说明完成。SMB86 和 SMB186 含义见表 2-2，SMB87 和 SMB187 含义见表 2-3。

表 2-2 SMB86 和 SMB186 含义

对于 Port0 口	对于 Port1 口	控制字节各位的含义
SM86.0	SM186.0	为 1 说明奇偶校验错误而终止接收
SM86.1	SM186.1	为 1 说明接收字符超长而终止接收
SM86.2	SM186.2	为 1 说明接收超时而终止接收
SM86.3	SM186.3	为 0
SM86.4	SM186.4	为 0
SM86.5	SM186.5	为 1 说明是正常收到结束字符
SM86.6	SM186.6	为 1 说明输入参数错误或者缺少起始和终止条件而结束接收
SM86.7	SM186.7	为 1 说明用户通过禁止命令结束接收

表 2-3　SMB87 和 SMB187 含义

对于 Port0 口	对于 Port1 口	控制字节各位的含义
SM87.0	SM187.0	0
SM87.1	SM187.1	1 使用中断条件，0 不使用中断条件
SM87.2	SM187.2	1 使用 SM92 或者 SM192 时间段结束接收 0 不使用 SM92 或者 SM192 时间段结束接收
SM87.3	SM187.3	1 定时器是信息定时器，0 定时器是内部字符定时器
SM87.4	SM187.4	1 使用 SM90 或者 SM190 检测空闲状态 0 不使用 SM90 或者 SM190 检测空闲状态
SM87.5	SM187.5	1 使用 SM89 或者 SM189 终止符检测终止信息 0 不使用 SM89 或者 SM189 终止符检测终止信息
SM87.6	SM187.6	1 使用 SM88 或者 SM188 起始符检测起始信息 0 不使用 SM88 或者 SM188 起始符检测起始信息
SM87.7	SM187.7	1 禁止接收，0 允许接收

与自由口通信相关的其他重要特殊控制字/字节见表 2-4。

表 2-4　其他重要特殊控制字/字节

对于 Port0 口	对于 Port1 口	控制字节或者控制字的含义
SMB88	SMB188	信息字符的开始
SMB89	SMB189	信息字符的结束
SMW90	SMW190	空闲线时间段，按毫秒设定。空闲线时间用完后接收的第一个字符是新消息的开始
SMW92	SMW192	中间字符/消息定时器溢出值，按毫秒设定。如果超过这个时间段，则终止接收消息
SMW94	SMW194	要接收的最大字符数（1～255 字节）。此范围必须设置为期望的最大缓冲区大小，即使不使用字符计数消息终端

RCV 指令缓冲区格式见表 2-5。

表 2-5　RCV 指令缓冲区格式

序　号	字 节 编 号	内　容
1	*T*+0	接收字节的个数
2	*T*+1	起始字符（如果有）
3	*T*+2	数据字节
4	*T*+3	数据字节
⋮	⋮	⋮
256	*T*+255	结束字符（如果有）

2.2　S7-200 系列 PLC 之间的自由口通信

以下以两台 S7-200 CPU 之间的自由口通信为例介绍 S7-200 系列 PLC 之间的自由口通信的编程实施方法。

【例 2-1】 有两台设备，控制器都是 CPU 226CN，两者之间为自由口通信，实现设备 1 的 I0.0 启动设备 2 的电动机的星-三角启动控制，设备 1 的 I0.1 终止设备 2 的电动机的转动，反过来设备 2 的 I0.2 启动设备 1 电动机的星-三角启动控制，设备 2 的 I0.3 终止设备 1 的电动机的转动。

（1）主要软硬件配置

① 1 套 STEP7-Micro/WIN V4.0 SP7；

② 2 台 CPU 226CN；

③ 1 根 PROFIBUS 网络电缆（含 2 个网络总线连接器）；

④ 1 根 PC/PPI 电缆。

自由口通信硬件配置如图 2-2 所示，两台 CPU 的接线如图 2-3 所示。

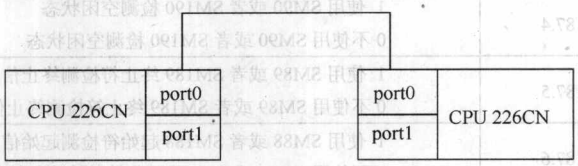


图 2-2 自由口通信硬件配置

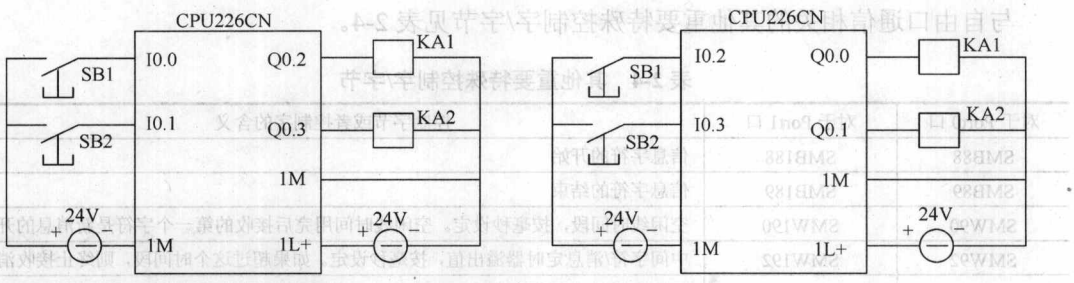


图 2-3 接线图

【关键点】 自由口通信的通信线缆最好使用 PROFIBUS 网络电缆和网络总线连接器，若要求不高，为了节省开支可购买市场上的 DB9 接插件，再将两个接插件的 3 和 8 角对连即可，如图 2-4 所示。

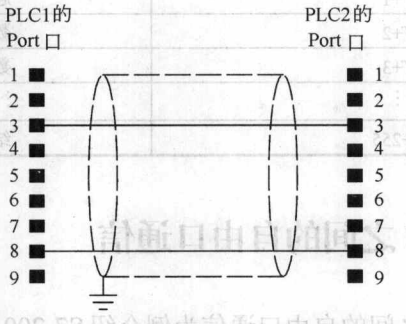


图 2-4 自由口通信连线的另一种方案

（2）编写设备 1 的程序

设备 1 的主程序如图 2-5 所示。

设备 1 的子程序 0 如图 2-6 所示。