普通高等教育“十二五”规划教材

西门子PLC编程及应用

XIMENZI PLC BIANCHENG JI YINGYONG

刘美俊　主编

机械工业出版社
CHINA MACHINE PRESS

普通高等教育“十二五”规划教材

西门子 PLC 编程及应用

主　编　刘美俊
副主编　邵利敏　曾立华
参　编　郝　雷　牛晓颖

机械工业出版社

前　言

可编程序控制器（PLC）是集计算机技术、现代控制技术、通信技术为一体的先进工业控制装置。它具有抗干扰能力强、编程简单方便、使用灵活、控制系统易于设计、通用性强、连网功能强等特点，在工业控制的各个领域获得了十分广泛的应用。PLC 在工程上的应用技术已成为工业自动化应用技术之一。

本书以西门子 S7-200 PLC 为主线，以 STEP7-Micro/WIN 4.0 编程系统为平台，系统介绍了 PLC 的硬件组成、编程技巧、通信组网以及应用实例等知识。新颖、实用、易读以及可操作是本书的编写宗旨，在讲解 PLC 理论的基础上，注重理论与工程实践相结合，把 PLC 控制系统工程设计思想、方法及其工程实例相融合，便于读者在学习过程中理论联系实际，较好地掌握 PLC 基础理论知识和工程应用技术。作者对全书的内容和结构进行了精心组织和安排：第 1 章介绍了 PLC 的基本概念；第 2 章介绍了 PLC 的硬件组成；第 3、4 章介绍了 PLC 的指令系统和程序语言；第 5 章介绍了数字量控制梯形图的一整套先进完整的设计方法，这些方法易学易用，可以节约大量的设计时间；第 6 章介绍了 PLC 的通信网络、USS 协议以及使用 USS 协议库控制 MicroMaster 变频器的设计方法；第 7 章讲解了 STEP 7-Micro/WIN 4.0 编程软件的安装、功能以及程序的调试运行，仿真软件的使用等；第 8 章介绍了 PLC 控制系统的设计方法、提高 PLC 控制系统可靠性的措施、节省 PLC 输入/输出点数的方法、模拟量控制、PID 闭环控制以及五个工程应用项目，每个项目给出了具体的硬件接线方法、程序清单与注释，便于初学者掌握开发 PLC 控制生产过程的基本方法。全书各章配有习题。

本书内容阐述循序渐进，深入本质，切中要害，结构合理严谨，概念准确，易读易懂。编写者具体分工为刘美俊负责第 3、8 章及第 5 章部分章节的编写并统稿；邵利敏、牛晓颖负责第 4、7 章的编写；曾立华负责第 1、6 章的编写；郝雷负责第 2 章以及第 5 章部分章节的编写。在编写过程中，作者借鉴和参考了 S7-200 PLC 的最新参考文献，在此谨向文献作者致以衷心的感谢。同时，本书获得了厦门理工学院教材出版基金资助。

由于作者水平有限，书中错误在所难免，恳请广大读者批评指正，联系邮箱：liumeijun@xmut.edu.cn。

作　者

目　录

第 1 章　可编程序控制器基础

1.1　可编程序控制器的基本概念与硬件结构

1.1.1　可编程序控制器的基本概念

可编程序控制器（PLC，Programmable Logic Controller）是在传统顺序控制器的基础上引入微电子技术、计算机技术、自动控制技术和通信技术等形成的新型工业控制装置。它具有控制能力强、可靠性高、配置灵活、编程简单等优点，是当代工业自动化技术领域中应用场合最多的工业控制装置之一，也被公认为是现代工业自动化的三大支柱（PLC、机器人、CAD/CAM）之一。

国际电工委员会（IEC）于 1987 年颁布了可编程序控制器标准草案第三稿，在草案中对可编程序控制器定义如下：可编程序控制器是一种数字运算操作的电子系统，专为在工业环境下应用而设计。它采用可编程序的存储器，在其内部存储、执行逻辑运算、顺序控制、定时、计数和算术运算等操作的指令，并通过数字式和模拟式的输入和输出，控制各种类型的机械或生产过程。可编程序控制器及其有关外部设备，都应按易于与工业系统连成一个整体、易于扩充其功能的原则设计。

定义强调了 PLC 应直接应用于工业环境，必须具有很强的抗干扰能力、广泛的适应能力和广阔的应用范围，这是区别于一般微机控制系统的重要特征；同时，也强调了 PLC 用软件方式实现的“可编程”与传统控制装置中通过硬件或硬接线的变更来改变程序的本质区别。

近年来，可编程序控制器发展很快，几乎每年都推出不少新系列产品，其功能也远远超出了上述定义的范围。

本书以西门子公司的 S7-200 系列小型 PLC 为主要讲授对象，可提供 4 个不同的基本型号的 8 种 CPU 供使用。S7-200 具有极高的可靠性、强大的通信能力和丰富的扩展模块，可以用编程软件中的梯形图、语句表和功能块图 3 种语言来编程。它的指令丰富、功能强，易于掌握，操作方便，集成有高速计数器、高速输出、PID 控制器和 RS-485 通信/编程接口，可以使用多种通信协议。例如，CPU224 最多可以扩展到 168 路数字量 I/O 点或 35 路模拟量 I/O 点。

1.1.2　可编程序控制器的硬件结构

PLC 是微机技术和继电器常规控制概念相结合的产物。从广义上讲，PLC 也是一种计算机系统，只不过它比一般计算机具有更强的、与工业过程相连接的 I/O 接口，具有更适用于控制要求的编程语言，具有更适应于工业环境的抗干扰性能。因此，PLC 是一种工业控制用的专用计算机，它的实际组成与一般微型计算机系统基本相同，由硬件系统和软件系统两大部分组成。

PLC 的类型种类繁多，功能和指令系统也不尽相同，但其结构和工作方式大同小异。硬件系统由主机、I/O 接口、电源、编程器、I/O 扩展接口和外部设备接口等主要部分构成，如图 1-1 所示。

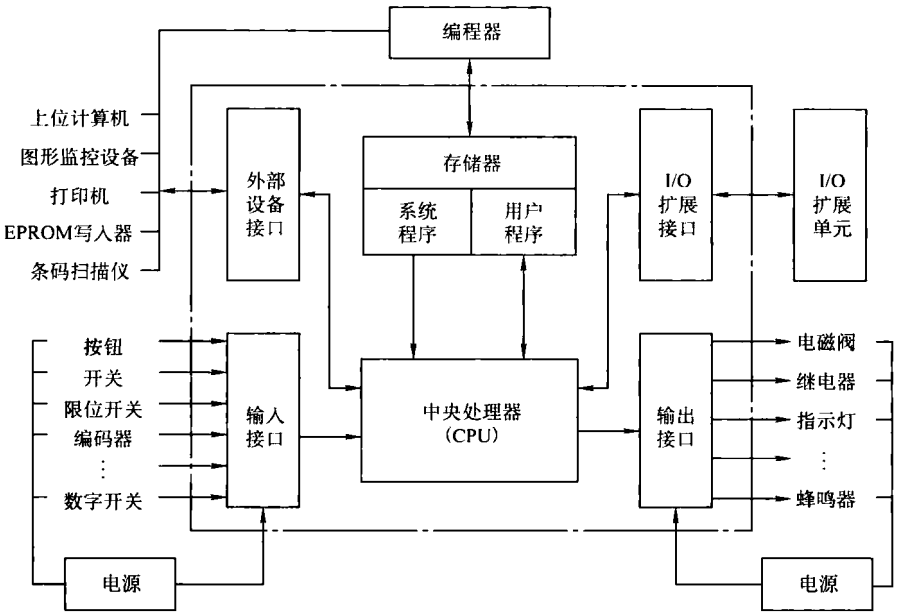

图 1-1 PLC 系统的基本结构

如果将 PLC 看作一个系统，外部的各种开关信号或模拟信号均为输入变量，它们经输入接口输入并寄存到 PLC 内部的数据寄存器中，而后按用户程序要求进行逻辑运算或数据处理，最后以输出变量形式送到输出接口，从而控制输出设备。

1. 主机

主机部分包括中央处理器（CPU）、系统程序存储器和用户程序及数据存储器。

CPU 是 PLC 的核心，起着总指挥的作用，它主要用来运行用户程序、监控输入/输出接口状态、做出逻辑判断和进行数据处理，即读入输入变量，完成用户指令规定的各种操作，将结果送到输出端，并响应外部设备（如打印机、条码扫描仪等）的请求以及进行各种内部诊断等。

PLC 的内部存储器有两类：一类是系统程序存储器，主要存放系统管理、监控程序和对用户程序作编译处理的程序，系统程序已由厂家固定，用户不能更改；另一类是用户程序及数据存储器，主要存放用户编制的应用程序及各种暂存数据和中间结果。

2. 输入/输出（I/O）接口

I/O 接口是系统的眼、耳、手、脚，是 PLC 与输入/输出设备连接的部件。输入接口用来接收和采集输入信号，开关量输入模块用来接收从按钮、选择开关、数字拨码开关、限位开关、接近开关、光电开关、压力继电器等传来的开关量输入信号；模拟量输入模块用来接收电位器、测速发电机、各种变送器提供的连续变化的模拟量电流电压信号。开关量输出模块用来控制接触器、电磁阀、电磁铁、指示灯、数字显示装置和报警装置等输出设备；模拟量输出模块用来控制调节阀、变频器等执行装置。

主机的工作电压一般是 5V，而 PLC 外部的输入/输出电路的电源电压较高，如 DC 24V 和 AC 220V。从外部引入的尖峰电压和干扰噪声可能损坏主机中的元器件，或使 PLC 不能正常工作。在 I/O 接口模块中，用光耦合器、光敏晶闸管、小型继电器等器件来隔离 PLC 内部电路和外部的 I/O 电路。I/O 接口除了传递信号外，还有电平转换与隔离的作用。

3. 电源

PLC 的电源是指为 CPU、存储器、I/O 接口等内部电子电路工作所配备的直流开关稳压电源，PLC 通常使用 AC 220V 或 DC 24V 工作电源。它的电源模块为其他各功能模块提供 DC 5V、DC 12V、DC 24V 等各种内部直流工作电源。一般情况下，许多 PLC 可以为输入电路和外部的传感器提供 DC 24V 的工作电源，但是驱动 PLC 负载的直流电源或交流电源一般由用户提供。

4. 编程器

编程器是编制、调试 PLC 用户程序的外部设备，是人机交互的窗口。通过编程器可以把用户程序输入到 RAM 中，或者对 RAM 中已有程序进行编辑；通过编程器还可以对 PLC 的工作状态进行监视和跟踪，对调试和试运行用户程序非常有用。

除手持编程器外，目前使用较多的是利用通信电缆将 PLC 和计算机连接，利用专用的工具软件进行编程或监控。

5. 输入/输出（I/O）扩展接口

I/O 扩展接口是 PLC 主机为了扩展输入/输出点数和类型的部件，输入/输出扩展单元、远程输入/输出扩展单元、智能输入/输出单元等都通过它与主机相连。I/O 扩展接口有并行接口、串行接口等多种形式。

6. 外部 I/O 接口

外设 I/O 接口是 PLC 主机实现人机对话、机机对话的通道。通过它，PLC 可以和编程器、彩色图形显示器、打印机等外部设备相连，也可以与其他 PLC 或上位机连接。外设 I/O 接口一般是 RS-232C、RS-422A、USB 等串行通信接口，该接口能够进行串行/并行数据转换、通信格式识别、数据传输出错检验、信号电平转换等。对于一些小型 PLC，外设 I/O 接口中还有与专用编程器连接的并行数据接口。

1.2　可编程序控制器的特点、主要功能及性能指标

1.2.1　可编程序控制器的特点

PLC 之所以能够迅速发展，除了工业自动化的客观需要外，还因为它具有许多独特的优点，主要有：

1. 可靠性高、抗干扰能力强

PLC 用程序来实现逻辑顺序和时序控制，最大限度地取代了传统继电器系统中的硬件电路，大大减少了机械触点和连线的数量，因触点接触不良造成的故障也大为减少。

可靠性是指 PLC 的平均无故障工作时间（Mean Time Between Failures，MTBF）。可靠性高、抗干扰能力强是 PLC 的重要特点之一，其 MTBF 可达几十万个小时，可以直接用于有强烈干扰的工业生产现场，PLC 已被公认为是可靠的工业控制设备之一。PLC 在硬件和软件方

面采取了多种措施，来提高其可靠性和抗干扰能力。

硬件方面，对所有的 I/O 接口电路均采用光电隔离，使工业现场的外电路与 PLC 内部电路之间在电气上隔离；各模块均采用屏蔽措施，以防止辐射干扰；采用性能优良的开关电源并对供电系统和各输入电路均采用多种形式的滤波，以消除或抑制高频干扰；采用模块式结构，一旦某一模块出现故障，可以迅速更换，从而尽可能地缩短系统的故障停机时间。

软件方面，PLC 具有良好的自诊断功能，一旦电源或其他软、硬件发生异常情况，CPU 立即采取有效措施，以防止故障扩大；PLC 设置了监视定时器（Watching Dog），如果循环执行时间超过了设置值，则表明程序进入了死循环，可以立即报警。

大型 PLC 还可以采用由双 CPU 构成冗余系统或由三 CPU 构成表决系统，使可靠性进一步提高。

2. 编程简单、使用方便

梯形图是可编程序控制器使用最多的编程语言，是面向生产、面向用户的编程语言，与电器控制电路图相似；梯形图形象、直观、简单、易学，广大工程技术人员很容易上手。当生产流程需要改变时，可现场改变程序，使用方便灵活。同时，PLC 编程器的操作和使用也很简单，这也是 PLC 获得普及和推广的原因之一。

3. 功能完善、通用性强

如今，PLC 不仅具有逻辑运算、定时、计数、顺序控制等功能，而且还具有 A/D 和 D/A 转换、数值运算、数据处理、PID 控制、通信连网等许多功能。同时，由于 PLC 产品的系列化、模块化，以及品种齐全的硬件装置，可以组成满足各种要求的控制系统。

4. 设计安装简单、维护方便

由于 PLC 用软件代替了传统电气控制系统的硬件，使控制柜的设计、安装、接线工作量大为减少，缩短了施工周期。PLC 的用户程序大部分可在实验室模拟调试，模拟调试好后再将 PLC 控制系统在生产现场进行安装、接线、调试，发现问题可通过修改程序加以解决。维修方面，由于 PLC 的故障率极低，维修工作量很小；而且，PLC 具有很强的自诊断功能，若出现故障，可根据 PLC 上指示或编程器上提供的故障信息，迅速查明原因，维修极为方便。

5. 体积小、质量轻、能耗低

由于 PLC 采用了集成电路，其结构紧凑、体积小、能耗低，因而是实现机电一体化的理想控制设备。目前 PLC 已普遍应用于 CNC 设备和机器人装置的控制器。

1.2.2 可编程序控制器的主要功能及性能指标

1. 可编程序控制器的主要功能

（1）逻辑控制功能

逻辑控制功能实际上就是位处理功能，是可编程序控制器的最基本的功能之一。PLC 设置有“与”、“或”、“非”等逻辑指令。利用这些指令，根据外部现场元件（开关、按钮或其他传感器）的状态，按照预定的逻辑进行运算处理后，将结果输出到现场的被控对象（电磁阀、接触器、继电器、指示灯等）。PLC 可以代替继电器进行开关控制，完成触点的串联、并联等各种连接。另外，在 PLC 中一个逻辑位的状态可以无限次地使用，逻辑关系的修改变更也十分方便。

（2）定时控制功能

PLC 中有许多可供用户使用的定时器，功能类似于继电器电路中的时间继电器。定时器的设置值（定时时间）可以在编程时设置，也可以在运行过程中根据需要进行修改，使用方便灵活。程序执行时，PLC 将根据用户指定的定时器指令对某个操作进行限制或延时控制，以满足生产工艺的要求。

（3）计数控制功能

PLC 为用户提供了很多计数器。计数器计到某一定值（设置值）时，产生一个状态信号，利用该状态信号实现对某个操作的计数控制。计数器的设置值可以在编程时设置，也可以在运行过程中根据需要进行修改。程序执行时，PLC 将根据用户用计数器指令指定的计数器对某个控制信号的状态改变次数（如某个开关的闭合次数）进行计数，以完成对某个工作过程的计数控制。

（4）步进控制功能

PLC 为用户提供了若干个状态器，可以实现由时间、计数或其他指定逻辑信号为转移条件的步进控制，即在一道工序完成以后，在转移条件满足时，自动进行下一道工序。大部分 PLC 都有专用的步进控制指令，应用步进控制指令编程十分方便。

（5）数据处理功能

大部分 PLC 都有数据处理功能，可以实现算术运算、数据比较、数据传送、数据移位、数制转换、译码编码等操作。现在一些新型的 PLC 数据处理功能更加齐全，可以完成开方、PID 运算、浮点运算等操作，还可以和 CRT、打印机连接，实现程序、数据的显示和打印。

（6）过程控制功能

有些 PLC 具有 A/D、D/A 转换功能，可以方便地完成对模拟量的控制和调节。

（7）通信连网功能

有些 PLC 采用通信技术，可以实现多台 PLC 之间的同位连接、PLC 与计算机之间的通信连接等。利用 PLC 之间的同位连接，可以把数十台 PLC 用同级或分级的方式连成网络，使各台 PLC 的 I/O 状态相互透明。采用 PLC 和计算机之间的通信连接，可用计算机为上位机，下面连接数十台 PLC 作为现场控制。目前 PLC 的连网和通信技术正趋于完善并迅速发展。

（8）监控功能

PLC 设置了较强的监控功能。操作人员利用编程器或监视器可对 PLC 的运行状态进行监视。利用编程器可以调整定时器、计数器的设置值和当前值，并根据需要改变 PLC 内部逻辑信号的状态及数据区的数据内容，为调试和维护提供了极大的方便。

（9）停电记忆功能

PLC 内部的部分存储器所使用的 RAM 设置了停电保持器件（如备用电池等），以保证断电后这部分存储器中的信息不会丢失。

（10）故障自诊断功能

PLC 可对系统组成、某些硬件状态及指令的合法性等进行自诊断，若发现异常情况，则发出报警信号并显示错误类型，如属于严重错误则自动终止运行。它的故障自诊断功能大大提高了 PLC 控制系统的安全性和可维护性。

2. PLC 的性能指标

PLC 的主要性能，一般可用以下 8 种指标表述。

（1）存储容量

PLC 的存储器由系统程序存储器、用户程序存储器和数据存储器三部分组成。PLC 存储容量通常指用户程序存储器和数据存储器容量之和，表征系统提供给用户的可用资源，是系统性能的重要技术指标。

（2）I/O 点数

I/O 点数是 PLC 可以接收的输入、输出信号的总和，是衡量 PLC 性能的重要指标。I/O 点数越多，外部可接的输入设备和输出设备就越多，控制规模就越大。

（3）扫描速度

扫描速度是指 PLC 执行用户程序的速度，一般以扫描 1KB 用户程序所需时间来表示，通常以 ms/KB 为单位。PLC 用户手册一般给出执行各条指令所用的时间，可以通过比较各种 PLC 执行相同的操作所用的时间，来衡量扫描速度的快慢。影响扫描速度的主要因素有用户程序的长度和 PLC 产品的类型，CPU 的类型、机器字长等直接影响 PLC 运算精度和运行速度。

（4）指令系统

指令系统指 PLC 所有指令的总和，PLC 具有基本指令和功能指令。指令的种类、数量也是衡量 PLC 性能的重要指标。PLC 的编程指令越多、软件功能越强，PLC 的处理能力和控制能力也越强，用户编程越简单、方便，越容易完成复杂的控制任务。

（5）内部元件的种类与数量

在编制 PLC 程序时，需要用到大量的内部元件来存放变量、中间结果、保持数据、定时计数、模块设置和各种标志位等信息，这些元件的种类与数量越多，表示 PLC 存储和处理各种信息的能力越强。

（6）特殊功能单元

特殊功能单元种类的多少与功能的强弱是衡量PLC产品的一个重要指标。近年来，各 PLC 厂商非常重视特殊功能单元的开发，特殊功能单元的种类日益增多、功能日益增强、控制功能日益扩大。

（7）可扩展能力

PLC 的可扩展能力包括 I/O 点数的扩展、存储容量的扩展、连网功能的扩展、各种功能模块的扩展等。在选择 PLC 时，经常需要考虑 PLC 的可扩展能力。

（8）通信能力

通信分为 PLC 之间的通信和 PLC 与其他设备之间的通信。通信主要涉及通信模块、通信接口、通信协议和通信指令等内容，PLC 的组网和通信能力也已成为衡量 PLC 产品水平的重要指标之一。

1.2.3 S7-200 PLC 概述

西门子公司较早地进行了 PLC 的研发和生产，欧洲第一台 PLC 就是由西门子公司在 1973 年研制成功的，此后，相继在 1975 年推出了 SIMATIC S3 系列 PLC，1979 年推出了 SIMATIC S5 系列 PLC，20 世纪末又推出了 SIMATIC S7 系列 PLC，SIMATIC 是西门子自动化系列产品品牌统称，来源于 SIEMENS + Automatic（西门子+自动化）。

西门子公司目前最新的 PLC 产品是 SIMATIC M7、C7 和 S7 三个系列。M7 系列 PLC 是嵌入式的高档机，用于解决对时间要求非常高的技术问题，它既可作为 CPU，也可作为功能

模块使用，目前国内引进比较少；C7 系列 PLC 往往在一个单元中集成一个 PLC 和一个控制操作面板（OP），由于 PLC 和 OP 同是 SIMATIC 系列产品，因此，C7 控制系统的扩展也很容易，并可简便地在 SIMATIC 自动化网络中进行集成；S7 系列又分为 S7-200、S7-300、S7-400 几个子系列，分别为小型、中型和大型 PLC，这个系列的 PLC 体积小、速度快、标准化高，具有网络通信能力，功能更强、可靠性更高。

S7-200 PLC 作为西门子 SIMATIC PLC 家族中的最小成员，以其超小的体积、灵活的配置、强大的内置功能，在诸多领域得到了广泛应用。它可以用于输入/输出点数较少的小型机械与设备的单机控制，也可以利用其较强的通信与网络功能，作为复杂系统的“子站”使用，构成 PLC 网络。

采用整体式固定 I/O 型（CPU221）与基本单元加扩展的结构，PLC 集 CPU、电源、输入/输出安装于一体，结构紧凑、安装简单。它的运算速度快，基本逻辑控制指令 0.22μs/条，可以实现高速控制；编程指令、编程元件较丰富，性价比高。

S7-200 PLC 均带有固定点数的高速计数输入与高速脉冲输出，输入/输出频率可以达到 20～100kHz。S7-200 PLC 带有 RS-485 串行通信接口，可以支持自由口通信（无协议通信）与 PPI（点到点通信）、MPI（多点通信）、PROFIBUS 现场总线通信。

S7-200 PLC 的用户程序存储在 EEPROM 中，最大数字量输入、输出映像区均为 128 点，最大模拟量输入、输出映像区均为 32 点；内部标志位（M 寄存器）为 256 位，其中掉电永久保存为 112 位，超级电容或电池保存为 256 位；256 个定时器中有 4 个 1ms 定时器，16 个 10ms 定时器，236 个 100ms 定时器；256 个计数器均能用超级电容或电池保存；顺序控制继电器为 256 点；布尔量运算执行速度为 0.37μs/指令；有 2 个 1ms 分辨率的定时中断，4 个硬件输入边沿中断，可选输入滤波时间为 0.25～12.8ms。

其中，CPU 221 无扩展功能，适于作小点数的微型控制器；CPU 222 有扩展功能；CPU 224 是具有较强控制功能的控制器；新型 CPU 224XP 集成有 2 路模拟量输入，1 路模拟量输出，有 2 个 RS-485 通信口，单相高速脉冲输出频率提高到 200kHz，2 相高速计数器频率提高到 100kHz，有 PID 自整定功能，这种新型 CPU 增强了 S7-200 在运动控制、过程控制、位置控制、数据监视和采集及通信方面的功能；CPU 226 适用于复杂的中小型控制系统，可扩展到 248 点数字量，有 2 个 RS-485 通信口。

S7-200 PLC 的 CPU 模块均集成有 1～2 个串行通信接口，它不仅可以连接外部设备、构成简单的网络，而且支持比较复杂的网络。利用 STEP 7-Micro/WIN 可方便快捷地构建和配置网络。PLC 的通信功能见表 1-1。

Modem 通信和以太网解决方案是最新推出的通信方式。现在的 PPI 通信的速率已升至 187.5kbit/s；自由口通信的速率升至 1.2～115.2kbit/s，去掉了原来的 300bit/s 和 600bit/s，增加了 57.6kbit/s 和 115.2kbit/s，速度更快，效率更高。在开放系统互联（OSI）七层模式通信结构的基础上，PPI、MPI、PROFIBUS-DP 这些通信协议可在一个令牌环网络上实现。通信结构依赖于特定的起始字符和停止字符，源和目地站地址，持久长度和数据校验和。如果使用相同的波特率，这些协议可以在同一个网络中同时运行而互不干扰。

除了 CPU 集成通信口外，S7-200 还可以通过通信扩展模块连接成更大的网络。S7-200 系列目前有两种通信扩展模块：PROFIBUS-DP 扩展从站模块（EM277）和 AS-i 接口扩展模块（CP243-2）。

表 1-1 S7-200 PLC 通信功能一览表

项目		功能				
		CPU221	CPU222	CPU224	CPU224XP	CPU226
接口类型		RS-485 串行通信接口				
接口数量		1			2	
波特率	PPI、DP/T	9.6kbit/s、19.2kbit/s、187.5kbit/s				
	无协议通信	1.2～115.2kbit/s				
通信距离	不使用中继器	50m				
	使用中继器	与波特率有关，187.5kbit/s 时为 1000m				
PLC 网络连接方式		PPI、MPI、PROFIBUS-DP、Ethernet（需要网络模块支持）				

1.2.4 S7-300/400 PLC 的概述

1. S7-300 PLC 的概述

S7-300 PLC 是模块化小型系统，能满足中等性能要求的应用，其模块化结构设计使得各种单独的模块之间可进行广泛组合以用于扩展。S7-300 PLC 产品的规格众多，而且在不断扩充中，产品性能主要通过不同的 CPU 模块进行区分，I/O 模块、电源模块、功能模块之间可通用。目前，S7-300 CPU 有标准型、紧凑型、故障安全型、技术功能型四种，前期产品还包括“户外型”等，同系列产品的性能与型号也有不同程度的变化。

（1）标准型

S7-300 系列标准型 CPU 包括 CPU312、CPU314、CPU315-2DP、CPU315-2PN/DP、CPU317-2DP、CPU317-2PN/DP、CPU319-3PN/DP 七种规格。标准型 CPU 均为模块式结构，CPU 无集成 I/O 点。CPU312 不可以连接扩展机架，主机架上的最大安装模块数为 8 个，每一模块的最大 I/O 点数为 32 点，因此，PLC 的最大输入/输出点数为 256 点。其余 CPU 均可以连接最多 3 个扩展机架，每一机架的安装模块数均为 8 个，连同主机架 PLC 的最大安装模块数为 32 个，因此，PLC 的最大输入/输出点数为 1024 点。

（2）紧凑型

S7-300 系列紧凑型 CPU 包括 CPU312C、CPU313C、CPU313C-2PtP、CPU313C-2DP、CPU314C-2PtP、CPU314C-2DP 六种规格。紧凑型 CPU 与标准型 CPU 的主要区别是 CPU 本身带有数量不等的集成 I/O 点，具有集成计数、脉冲输出等功能，当然，也可以根据需要进行扩展。

（3）故障安全型

S7-300 系列故障安全型 CPU 包括 CPU315F-2DP、CPU315F-2PN/DP、CPU317F-2DP、CPU317F-2PN/DP 四种规格。该系列 PLC 内部安装有经德国技术监督委员会认可的基本功能块与安全型 I/O 模块参数化工具，可以用于锅炉、索道以及对安全性要求极高的特殊控制场合，它可以在系统出现故障时立即进入安全状态或安全模式，以确保人身与设备的安全。

（4）技术功能型

S7-300 系列技术功能型 CPU 包括 CPU315T-2DP、CPU317T-2DP 两种规格，是一种专门用于运动控制的 PLC，最大可以控制 16 轴，可以控制轴定位，也可以实现简单的插补与同步

控制，还可以根据需要进行坐标位置、速度等控制。S7-300 系列 PLC 的主要功能特点如下：

1）运算速度快、PLC 循环周期短。0.1～0.6μs 的指令处理时间在中等到较低的性能要求范围内开辟了全新的应用领域。

2）编程能力强。可以用于复杂功能的编程与控制，支持多种编程语言。浮点数运算功能可有效地实现更为复杂的算术运算。

3）人机界面（HMI）。方便的人机界面服务已经集成在 S7-300 操作系统内，因此人机对话的编程要求大大减少。SIMATIC 人机界面（HMI）从 S7-300 中取得数据，S7-300 按用户指定的刷新速度传送这些数据。S7-300 操作系统自动地处理数据的传送。

4）诊断功能。CPU 的智能化的诊断系统连续监控系统的功能是否正常、记录错误和特殊系统事件（如超时、模块更换等）。

5）口令保护。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。

6）强大的通信功能。方便用户的 STEP 7 的用户界面提供了通信组态功能，这使得组态非常容易、简单。SIMATIC S7-300 具有多种不同的通信接口，多种通信处理器用来连接 AS-i 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、人机界面系统及其他 SIMATIC S7/M7/C7 等自动化控制系统。

CPU 支持下列通信类型：

过程通信：通过总线（AS-i 或 PRONBUS）对 I/O 模块周期寻址（过程映像交换）。

数据通信：在自动控制系统之间、人机界面（HMI）和几个自动化功能块间相互调用。

2. S7-400 的概述

SIMATIC S7-400 是用于中、高档性能范围的可编程序控制器。模块化及无风扇的设计、坚固耐用、容易扩展和广泛的通信能力、容易实现的分布式结构以及用户友好的操作，使 SIMATIC S7-400 成为中、高档性能控制领域中首选的理想解决方案。

SIMATIC S7-400 的应用领域包括通用机械工程、汽车工业、立体仓库、机床与工具、过程控制、控制技术与仪表、纺织机械、包装机械、控制设备制造、专用机械等。功能逐步升级的多种级别的 CPU，带有各种用户友好功能的种类齐全的功能模块，使用户能够构成最佳的解决方案，满足自动化的任务要求。当控制任务变得更加复杂时，任何时候控制系统都可以逐步升级，而不必过多的添加额外的模块。

从 PLC 用途与功能上分，S7-400 PLC 可以分为标准型（S7-400）、冗余型（S7-400H）、故障安全型（S7-400F/FH）三种基本类型，适用于不同的控制场合。

标准型是常用产品，适用于绝大多数对安全性能无特别严格要求的一般场合。冗余型用于对控制系统可靠性要求极高、不允许控制系统出现停机的控制场合，需要选用“冗余”型模块。所谓“冗余”系统，事实上是通过一套在系统正常工作时并不需要、完整的“多余”系统作为系统的备件（称为备用系统或待机系统），而且，备用系统始终处于待机状态（也称为“热待机”），只要工作控制系统发生故障，“备用系统”可以立即投入正常工作，并成为工作控制系统，以保证整个控制系统的连续、不间断运行。

S7-400 自动化系统采用模块化结构设计。它所具有的模块的扩展和配置功能使其能够按照每个不同的需求灵活组合。一个系统包括电源模块、中央处理器（CPU）、各种信号模块

（SM）、通信模块（CP）、功能模块（FM）、接口模块（IM）和 SIMATIC S5 模块。除了具有 S7-300 系列系统的功能外，S7-400 还具有如下的增强功能：

1）冗余设计的容错自动化系统。硬件冗余 CPU 同步速率更快，同步光缆最长可达 10km。

2）处理速度显著提高。CPU 处理速度比同型号其他机器整体提高 3～70 倍，417 型 CPU 最快高达 0.03μs/bit。执行复杂数学运算的速度最高提高到原来的 70 倍。工作内存加倍，最高达 20MB。S7 定时器和计数器个数提高 8 倍，达到 2048 个。

3）多 CPU 处理。在 S7-400 中央机架上，最多 4 个有多 CPU 处理能力的 CPU 同时运行。这些 CPU 自动地、同步地变换其运行模式，可以同步执行控制任务。使用多 CPU 中断（OB60）可以在相应的 CPU 中同步地响应一个事件。而且，由于工作方式的复杂，CPU 模块上的指示灯也很多。

4）扩展能力。中央机架能插入最多 6 块发送型的接口模块，每个模块有两个接口，每个接口可以连接 4 个扩展机架，最多能连接 21 个扩展机架。扩展机架中的接口模块只能安装在最右边的槽内。

5）诊断功能。诊断能力比 S7-300 强大，比如多达 8 个硬件中断功能，其他中断功能也比 S7-300 多。

6）CPU 通信性能显著增强。由于等时模式工作中循环周期更短，现场级通信连接性能有了显著提高，特别是与驱动装置的通信能力进一步增强，数据传输速率加倍，垂直集成通信及 PLC-PLC 的通信响应时间缩短一半。

1.3 可编程序控制器的工作原理与编程语言

1.3.1 可编程序控制器的工作方式

最初研制生产的 PLC 主要用于代替传统的由继电器、接触器构成的控制装置，但这两者的运行方式是不相同的：

1）继电器控制装置采用硬逻辑并行运行的方式，即如果这个继电器的线圈通电或断电，该继电器所有的触点（包括其常开或常闭触点）无论在继电器控制电路的哪个位置上都会立即同时动作。

2）PLC 的 CPU 则采用顺序逻辑扫描用户程序的运行方式，即如果一个输出线圈或逻辑线圈被接通或断开，该线圈的所有触点（包括其常开或常闭触点）不会立即动作，必须等扫描到该触点时才会动作。

为了消除二者之间由于运行方式不同而造成的差异，考虑到继电器控制装置各类触点的动作时间一般在 100ms 以上，而 PLC 扫描用户程序的时间一般均小于 100ms，因此，PLC 采用了一种不同于一般微型计算机的运行方式——扫描技术。这样在对于 I/O 响应要求不高的场合，PLC 与继电器控制装置在处理结果上就没有什么区别了。

PLC 控制任务的完成建立在硬件支持下，通过执行反映控制要求的用户程序来实现，其工作原理与计算机控制系统基本相同。

PLC 采用“顺序扫描，不断循环”的方式进行工作。运行时，CPU 根据用户按控制要求编制好并存于用户存储器中的程序，按指令步序号（或地址号）作周期性循环扫描，如无跳

转指令，则从第一条指令开始逐条顺序执行用户程序，直至程序结束，然后重新返回第一条指令，开始新一轮扫描。在每次扫描过程中，还要完成对输入信号的采样和对输出状态的刷新等工作。

1.3.2　可编程序控制器的扫描工作过程

当 PLC 投入运行后，其工作过程一般分为三个阶段，即输入采样、程序执行和输出刷新三个阶段。完成上述三个阶段称为一个扫描周期。在整个运行期间，PLC 的 CPU 以一定的扫描速度重复执行上述三个阶段，如图 1-2 所示。

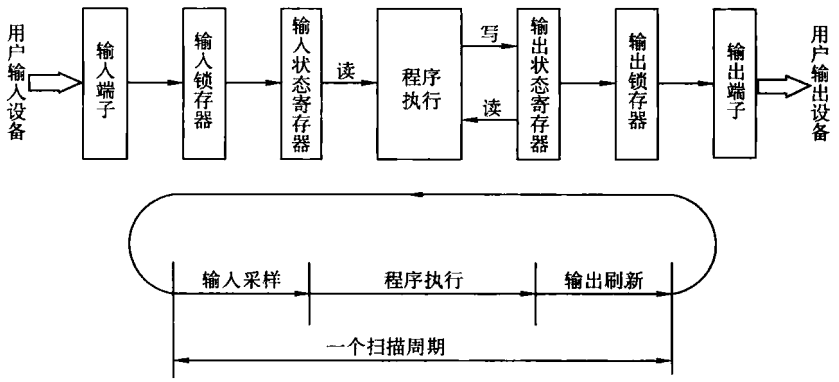

图 1-2　PLC 的扫描工作过程

1）输入采样阶段：首先以扫描方式按顺序读入所有暂存在输入锁存器中的输入端子的通断状态或输入数据，并将其存入（写入）各对应的输入状态寄存器中，即刷新输入。随即关闭输入端口，进入程序执行阶段。在程序执行阶段，即使输入状态有变化，输入状态寄存器也不会改变，只能等下一个扫描周期的输入采样阶段被读入。

2）程序执行阶段：按用户程序指令存放的先后顺序扫描执行每条指令，所需的执行条件可从输入状态寄存器和当前输出状态寄存器中读入，经相应的运算和处理后，其结果再写入输出状态寄存器中，输出状态寄存器中所有的内容随着程序的执行而改变。

在程序执行阶段，除输入映像寄存器外，各个元件映像寄存器的内容是随着程序的执行而不断变化的。

3）输出刷新阶段：当所有指令执行完毕后，输出状态寄存器的通断状态在输出刷新阶段送至输出锁存器中，并通过一定的方式（继电器、晶体管或晶闸管）输出，驱动相应输出设备工作。

在输出刷新阶段结束后，CPU 进入下一个扫描周期，重新执行输入采样，周而复始。

1.3.3　可编程序控制器的编程语言

PLC 编程时通常不直接采用微机的编程语言，而常常采用面向控制过程、面向问题的“自然语言”。

PLC 各厂家的编程语言、指令的条数和表达方式有较大区别。为电子技术制定全球性标准的世界性组织 IEC（国际电工委员会）于 1994 年 5 月公布了 PLC 标准（IEC 61131），其第