职 · 场 · 金 · 钥 · 匙

西门子 S7-200CN PLC 编程技术及工程应用

高正中　张仁彦　隋 涛　等编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

http://www.phei.com.cn

职场金钥匙

西门子 S7-200CN PLC 编程技术及工程应用

高正中　张仁彦　隋　涛　等编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书以学习可编程控制器（PLC）和工程实际应用 PLC 为出发点，以国内市场应用较为广泛的西门子 S7-200CN 系列 PLC 为例，按照基础篇、实践篇和应用篇进行应用讲解。第 1～3 章为基础篇部分，讲解 PLC 的工作原理、S7-200CN PLC 的硬件结构、数据格式、寻址方式及指令系统、STEP 7-Micro/WIN 编程软件的使用方法。第 4 章为实践篇，精编 14 个典型实例，介绍 S7-200CN PLC 的基本控制应用、编程方法。第 5～7 章为应用篇，第 5 章针对 PLC 控制系统工程设计步骤、设计方法和安装技术等进行讲解；第 6 章从实际工程设计出发，讲解应用设计实例和相关源程序的设计；第 7 章介绍 S7-200CN PLC 的通信技术，并针对应用较为广泛的 USS 协议、Modbus RTU 协议、工业以太网通信技术举例说明。

本书适合从事工业自动化控制的技术人员阅读，也可作为高等学校相关专业的教学用书。

图书在版编目（CIP）数据

西门子 S7-200CN PLC 编程技术及工程应用 / 高正中等编著. —北京：电子工业出版社，2010.1
（职场金钥匙）
ISBN 978-7-121-10055-0

Ⅰ. 西… Ⅱ. 高… Ⅲ. 可编程序控制器 Ⅳ. TM571.6

中国版本图书馆 CIP 数据核字（2009）第 225535 号

策划编辑：张 剑
责任编辑：刘真平
印 刷：涿州市京南印刷厂
装 订：涿州市桃园装订有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1 092 1/16 印张：21 字数：537.6 千字
印 次：2010 年 1 月第 1 次印刷
印 数：4 000 册 定价：38.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着社会生产力的发展，对现代生产制造业的自动化程度要求越来越高，可编程控制器（PLC）在其中发挥了重要的作用。本书介绍在国内应用广泛的西门子 S7-200CN 小型 PLC 的设计与应用。

本书第 1～3 章为基础篇，对 S7-200CN PLC 的基础知识进行详解，系统介绍西门子 S7-200CN PLC 的硬件结构模块、指令系统和编程环境——STEP 7-Micro/WIN 软件的使用方法；S7-200CN PLC 的数据结构和数据类型，重点介绍常用的指令及其用法。第 4 章是 S7-200CN PLC 的实践应用设计，精编 14 个应用实例进行讲解，以达到对 S7-200CN PLC 的指令系统学习掌握的目的。第 5～7 章为工程应用设计部分，讲解有关 S7-200CN PLC 系统在工业现场的实际应用系统设计。第 5 章讲解设计工业控制 PLC 系统的方法、步骤和应用技术；第 6 章讲解工程应用设计实例；第 7 章讲解 S7-200CN 的通信应用设计，主要介绍基于自由口应用的 USS 协议、Modbus RTU 协议的应用和工业以太网模块 CP243-1、GPRS 通信模块 MD720-3 的应用配置设计。实例经过简单的修改，可以在工程中应用移植，帮助工程设计人员尽快完成工程设计，节约设计时间。

本书的编写得到了西门子（中国）公司的大力支持，西门子公司的李士光先生对本书的编写提出了很好的建议和帮助。在本书编写过程中，山东科技大学信息与电气工程学院李世光高级工程师给予了大力支持，并提出了指导性的建议，在此一并表示衷心的感谢！

本书由山东科技大学的高正中、张仁彦、隋涛、张松梅和中国绿林工程技术有限公司（济南分部）的李长春共同编写。其中第 1、2 章由张仁彦编写，第 3 章由李长春编写，第 4 章由隋涛编写，第 5～7 章由高正中、张松梅、李长春编写。参加本书编写的还有管殿柱、宋一兵、李文秋、王献红、张轩等。另外，刘隆吉、孔凡雪、蔺相斌、张洪薇等参加了书中部分例程的调试编写工作。

由于时间仓促及作者水平有限，书中可能存在不妥或错漏之处，恳请读者指正。

编　著　者

目　录

第1章　可编程控制器系统概述

本章主要介绍可编程控制器的历史、定义、基本结构和程序执行过程等基本知识，同时简要介绍 S7-200CN 系列 PLC 的 I/O 模块。通过本章内容的学习，读者将对 PLC 有初步认识，为下面学习 PLC 程序和系统设计方法奠定基础。

本章重点

★ PLC 的基本结构
★ PLC 程序的执行过程
★ S7-200CN 系列 PLC 的 I/O 模块

1.1　PLC 的基本概念与基本结构

可编程控制器（Programmable Controller）是一种重要工业控制计算机，广泛应用于工业生产的各个领域。本节将主要介绍可编程控制器的基本概念和结构，并在此基础上介绍 PLC 的程序执行过程等内容。

1. PLC 的历史

可编程控制器是工业控制领域中自动化技术发展的产物。众所周知，工业生产过程中存在大量顺序控制和安全互锁逻辑控制，在 20 世纪 60 年代之前，这些功能是通过气动或电气控制系统实现的，相应的控制系统主要由继电器和计数器等构成。这种系统的主要缺点是体积大，接线复杂和可靠性差，特别是系统适应性差，不易维护和更改。上述缺点不但增加了生产成本，而且严重制约生产效率的进一步提高。为解决这一问题，美国通用汽车公司（GM）提出要设计一种新的系统来代替继电器系统，并于 1968 年向社会公开招标，同时给出了 10 条招标指标，即“通用十条”：

（1）编程方便，可现场修改和调试程序；
（2）维护方便，采用模块化结构；
（3）可靠性高于继电器控制系统；
（4）体积小于继电器控制装置；
（5）数据可直接送入管理计算机；
（6）成本可与继电器控制系统竞争；
（7）输入可以是 115V 交流电；
（8）输出为交流 115V，输出电流可达 2A 以上，能直接驱动电磁阀；
（9）扩展时，原系统只需作很小改动；
（10）用户程序存储器容量至少能扩展到 4KB。

1969 年美国数字设备公司（DEC）根据上述要求研制成功了 PDP-14 控制器，并在汽车自动装配线上成功使用。这种控制器主要用于顺序控制，并仅能进行逻辑运算，因此被称做可编程逻辑控制器（Programmable Logic Controller，PLC）。虽然早期的 PLC 只有简易的逻辑开/关功能，但是这种控制装置以集成电路和电子技术为基础，实现了电气控制的程序化，与继电器控制系统相比使用方便，体积小，易于维护和修改。

2. PLC 的定义

随着集成电路、计算机技术和电气控制技术的发展，可编程逻辑控制器 PLC 逐渐发展成以微处理器为核心的新型工业控制设备，是计算机家族中的一员。鉴于可编程逻辑控制器的功能越来越丰富（如具备高速通信网络和以梯形图方式编程等），早已不限于进行逻辑控制，美国电器制造商协会（NEMA）经过 4 年的调查，于 1980 年把它正式命名为可编程控制器（Programmable Controller，PC），但是为了与个人计算机（Personal Computer，PC）相区别，仍将可编程控制器简称为 PLC。

PLC 自诞生起就进入了快速发展阶段，国际电工委员会（IEC）分别于 1982 年 11 月、1985 年 1 月和 1987 年 2 月颁布了可编程控制器标准的草案第一稿、第二稿和第三稿，并在草案第三稿中将可编程控制器定义为："可编程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。它采用了可编程序的存储器，用来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。PLC 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。"作为一种应用于工业环境下的计算机，该定义强调了 PLC 应具有抗干扰性强，适应性好和应用范围广泛的特点，这正是工业控制计算机区别于一般微型计算机的重要特征。

目前，PLC 因其具有通用性强，使用方便，适应面广，可靠性高，抗干扰能力强，编程简单等特点，已成为工业控制领域中不可或缺的一种控制装置，具有广阔的市场。

3. PLC 的基本结构

作为计算机家族中的一员，PLC 的基本结构与一般的微型计算机系统类似，主要由中央处理器（CPU）、存储器、输入/输出设备组成，另外具有电源、A/D 和 D/A 等模块，其基本结构如图 1-1 所示。

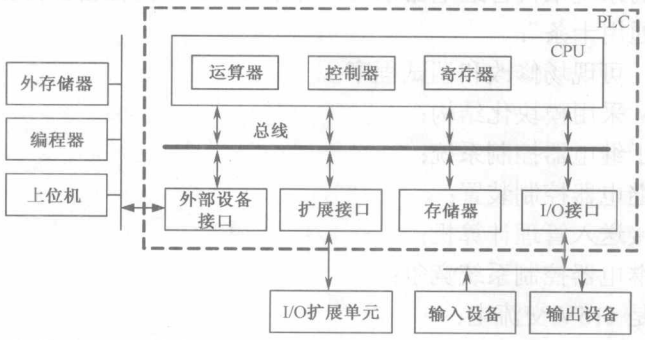

图 1-1　PLC 的基本结构

1）CPU　与所有微型计算机系统（如通用计算机系统和单片微型计算机系统）相同，CPU 是 PLC 的核心部件，主要包含运算器、控制器和寄存器。控制器控制 CPU 工作，由 CPU

读取指令、解释指令及执行指令。运算器用于进行算术、逻辑等运算，其工作由控制器控制完成。另外，CPU 内部还有一些寄存器参与运算，并存储运算的中间结果。CPU 可以是通用微处理器（如 8086、80286 和 80386 等）和单片机（如 8051 和 M6800）等。

CPU 按位数可分为 8 位、16 位和 32 位，通常小型 PLC 采用价格较低，通用性较好的 8 位和 16 位 CPU，中型 PLC 通常采用集成度高，运算速度快，可靠性更高的 16 位和 32 位 CPU，而大型 PLC 多采用灵活性强，速度快的高速 CPU。另外，小型 PLC 多采用单 CPU，而大型 PLC 多采用双 CPU 甚至多 CPU 系统，在多个 CPU 中往往有一个是位处理器，其他是字处理器，而位处理器的使用进一步提高了 PLC 的实时性。

2）存储器　存储器用于存放程序和数据。

按照读/写功能，存储器可分为两种：一是随机存储器 RAM（Random Access Memory），可读可写；二是只读存储器 ROM（Read Only Memory），只能读不能写。

按照存储功能，PLC 存储空间可划分为：系统程序存储区、系统 RAM 存储区和用户程序存储区。

（1）系统程序存储区：存放系统程序即所谓的系统软件（相当于计算机操作系统软件），是由 PLC 制造厂家编写的与 PLC 硬件有关的程序，和硬件一起决定了 PLC 的性能。它主要完成系统诊断，命令解释，提供 PLC 运行平台等功能，通常固化到 ROM 中，用户不能访问和修改。

（2）系统 RAM 存储区：存放 I/O 映像区及各类软设备，如逻辑线圈、数据寄存器、计时器、计数器、变址寄存器、累加器等。

（3）用户程序存储区：存放用户编制的程序，不同类型的 PLC，其存储容量各不相同。

3）I/O 模块　I/O 模块又称 I/O 单元，负责实现 I/O 信号的扩展，这些数据可以由被控对象通过 I/O 模块传送给 PLC，也可由 PLC 通过 I/O 模块传送给被控对象。在数据传输过程中，I/O 模块的作用是实现 PLC 与外部输入和输出设备间不同信号间的电平转换。

4）其他功能模块

（1）A/D、D/A 模块：A/D 模块主要用于将电压、电流、湿度和温度等模拟信号转换成 PLC 能够处理的数字量。D/A 模块与 A/D 模块的作用相反，其作用是把 PLC 内部的数字量转换成电压、电流等模拟信号以控制外部设备，如变频器和温度控制器等。

（2）电源模块：为 PLC 的各个模块提供工作电源。电源模块的一般输入为 AC 220V（有的 AC 220V 与 AC 110V 均可以），部分电源模块输入为宽电压范围（AC 86～240V），输出电源电压可以是交流的，也可以是直流的。

（3）通信模块：主要通过通信网络实现 PLC 之间、PLC 与个人计算机间及与其他设备间的信息交换。通信模块实现 PLC 与各种控制总线或工业以太网的通信，如西门子 S7-200CN PLC 的 CP243-1、CP243-1IT CP241 等。通信模块使得 PLC 与其他计算机系统和被控对象之间形成一个统一的整体，使分散集中的远程控制和信息交换成为可能。

5）PLC 的外部设备

（1）编程器，是用户进行 PLC 程序设计和系统监控的必备设备，可以对 PLC 在线编程和修改程序。

（2）存储设备，用于永久性地存储用户资料，PLC 应用中一般为专用的存储卡。

（3）I/O 设备，用于接收输入信号和发送输出信号，如打印机和键盘等。

4. PLC 程序的存储和执行过程

作为一种用于工业控制的计算机，PLC 与通用的个人计算机有所不同，这主要表现在程

序存储方式和程序执行过程两方面。

1）程序存储方式　通用个人计算机的内部存储器里只存放少量系统程序，用于系统自检和从外部存储器（如硬盘等）将操作系统（如 DOS、Windows 和 Linux 等）程序加载到内部存储器，然后由操作系统进行用户应用程序的管理。而 PLC 的用户应用程序可以预先存放在内部存储器上，CPU 上电复位后，先由操作系统启动 PLC，然后 PLC 进入运行模式并运行用户应用程序。这种程序存储方式的特点是，断电后 PLC 的操作系统程序、用户应用程序和一些数据还保存在内部存储器（是非易失存储器）中，一旦恢复供电 PLC 就可以重新运行程序。

2）程序执行过程　一般的微型计算机程序在执行时，CPU 根据当前程序指针的内容取出指令并执行指令，然后再取出下一条指令并执行，如此循环下去，直到遇到程序结束指令时才停止执行。而 PLC 采用循环扫描的方式工作，遇到程序结束指令后程序会自动重复执行，其典型的循环扫描周期如图 1-2 所示。可见 PLC 在一次上电初始化后，就会重复进行顺序扫描循环，这种循环由操作系统控制完成，是 PLC 自动化控制系统的基础。该循环扫描过程包含以下主要步骤。

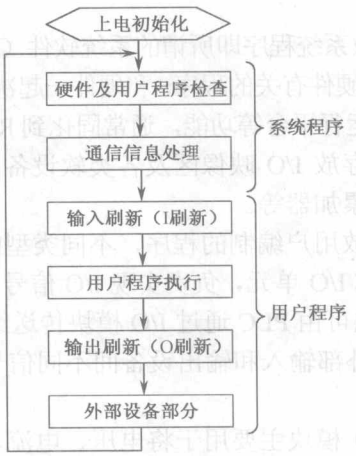

图 1-2　典型的 PLC 循环扫描周期

（1）上电初始化：对堆栈指针、工作单元和编程接口进行初始化，并进行 PLC 工作状态的选择（主要是设置编程状态和运行状态），这部分工作由操作系统完成，并且只进行一次。

（2）循环扫描：这部分由系统程序扫描和用户程序扫描两部分构成，并在 PLC 运行状态下不断重复执行。

系统程序扫描阶段（CPU 自诊断阶段）主要完成以下工作。

- 检查 PLC 硬件状态是否正常。
- 检查用户程序是否存在语法错误。
- 对监控定时器进行定期复位，监控定时器又称“看门狗”（Watch Dog Timer，WDT），是用于检测程序是否跑飞和是否进入死循环的一种方法。
- 与其他 PLC 和计算机等网络上的其他设备进行通信。

用户程序扫描阶段由输入扫描、用户程序执行、输出扫描及外部设备服务 4 部分组成，它们的功能分别如下。

- 输入扫描。在输入扫描阶段（又称输入信号采样阶段），PLC 以扫描方式顺序读入所有输入模块的数据，即从连接到输入模块的传感器获取数据（该数据表示开关的接通或断开状态等），并将其保存到输入映像存储器中。输入映像存储器中的状态被刷

新后，将一直保存到下一个扫描周期才会被重新刷新。在此阶段，用户程序执行、输出扫描及外部设备服务 3 部分处于禁止状态。

- 用户程序执行。在本阶段用户程序将被顺序执行一遍，在此过程中，CPU 首先读取并解释每条指令，然后从输入映像存储器和输出映像存储器中读取输入和输出的状态，并在此基础上完成相应的算术、逻辑等运算，最后把处理结果存入相应的寄存器或输出到数据映像存储器中。

需要注意的是：用户程序检测到的输入状态只是输入状态最近的映像；用户程序运行结果只改变输出映像存储器中的内容，而且只有输出映像存储器中的内容才会真正传送到输出模块（有的系列 PLC 具有立即输出指令，实现立即更新输出或输入功能）。

- 输出扫描。将输出映像存储器中的数据输出到输出锁存寄存器中，输出锁存寄存器对应着物理输出口，这才是 PLC 的实际输出。
- 外部设备服务。在本阶段，PLC 与外部设备（如打印机和编程器等）交换信息，还可以进行人机界面的实时信息交换。

5. PLC 的分类

鉴于 PLC 在工业控制领域中的重要作用，有很多公司（如欧姆龙、西门子、三菱、施耐德、松下和 LG 等）从事 PLC 的设计生产，因此目前 PLC 产品种类繁多，且规格和性能也不尽相同。为便于系统的配置及使用，PLC 可按 3 种方式分类，即按结构形式分类，按功能强弱分类和按控制规模分类。

1）按结构形式分类　可分为整体式、模块式（组合式）和叠装式 3 种。

（1）整体式：PLC 的 CPU 板、I/O 板、显示面板、内存块、电源等部件组合成一个整体，不可拆卸。这种 PLC 结构紧凑，体积小，价格低，一般小型 PLC 采用这种结构。

（2）模块式：PLC 由 CPU 模块、I/O 模块、内存、电源模块、底板或机架等多个模块按照一定规则组合配置，各模块相对独立，可以拆卸，便于安装、扩展和维护。大、中型 PLC 一般采用模块式结构，如西门子公司的 S7-300 系列、S7-400 系列 PLC 都采用这种结构形式。

（3）叠装式：将整体式和模块式的特点结合起来，将相互独立的 CPU 模块、电源模块、通信模块和一定数量的 I/O 单元集合在一个机壳内，各模块间通过电缆进行连接，并且各模块可以一层层地叠装。这种结构方式的 PLC 系统配置灵活，体积较小，安装方便，本书介绍的西门子公司 S7-200CN 系列 PLC 就采用这种结构形式。

2）按功能强弱分类　根据 PLC 功能的不同，可将 PLC 分为低档、中档和高档 3 类。低档 PLC 功能和结构都相对简单，仅具备基本的逻辑运算、定时、计数、自诊断和监控等功能，主要用于单机控制系统，可实现逻辑控制、顺序控制和少量的模拟量控制。中档 PLC 在低档 PLC 的基础上增强了模拟量 I/O 功能，同时具有通信网络、算术运算、数据传送等功能，甚至还具有中断控制和 PID 控制等复杂控制功能。高档 PLC 在中档 PLC 的基础上增强了算术运算功能（如可进行矩阵运算和有符号数运算），另外还支持显示、打印等人机交互功能，适合大规模过程控制。

3）按控制规模分类（按 I/O 点数分类）　控制规模主要指 PLC 输入（用 I 表示）和输出（用 O 表示）的开关量的点数（或个数）和模拟量的路数，但主要按开关量个数计算，因此，通常将模拟量的路数按一路相当于 8～16 点折算成开关量的点数。

PLC 按 I/O 点数可分为 5 类：

（1）微型机，I/O 点数小于 64 点；

（2）小型机，I/O 点数在 256 点以下；
（3）中型机，I/O 点数在 512～2 048 点之间；
（4）大型机，I/O 点数在 2 048 点以上；
（5）巨型机，I/O 点数可达万点，甚至几万点。

1.2　PLC 的特点及其在工业现场的应用

PLC 之所以在工业控制中受到广泛青睐，与其鲜明的技术特点有关，本节将主要介绍 PLC 的特点及其在工业现场的应用情况。

1．PLC 的特点

1）可靠性高，抗干扰性强　PLC 用程序代替继电器和计时器，最大限度地减少了机械触点和硬件连线的数量，降低了硬件故障发生率。目前，PLC 都以大规模集成电路技术为基础，采用先进的生产工艺进行制造，内部结构设计和电路设计充分考虑了抗干扰性能。另外，PLC 自身带有硬件故障自我检测功能，也允许用户加入自己的故障诊断程序。而且在外围电路设计方面，PLC 所有的 I/O 接口电路均进行了光电隔离，并采用各种滤波和屏蔽措施，有效克服了电气和辐射等干扰对系统性能的影响。上述因素使 PLC 的可靠性和抗干扰性得到了保障。

2）模块化设计，灵活性强，功能丰富　目前，大多数 PLC 均采用模块化结构设计，各模块（如 I/O 模块和电源模块等）由机架和电缆连接起来构成系统，不但大量节约了 PLC 系统安装、调试和维护的时间和成本，而且用户可以根据需求对系统功能和规模进行组合、调配，增强了系统设计的灵活性。另外，PLC 厂商生产了大量先进的 PLC 模块，如电源模块、存储扩展模块、开关量模块、模拟量模块、温度模块、位置控制模块和通信模块等，使得 PLC 系统功能更加丰富。

3）编程简单、方便　梯形图是 PLC 程序设计中使用最多的一种编程语言，它的电路符号和表达方式类似于继电器控制线路图，很容易被熟悉继电气控制的工程技术人员掌握。

梯形图编程技术诞生于 20 世纪 70 年代，这项技术对 PLC 在工业界的推广和快速发展起到了至关重要的推动作用，可以说没有梯形图就没有 PLC 的今天。

4）体积小，功耗低，性价比高　PLC 用程序代替继电器和计时器的功能，大量降低了继电器和定时器的使用量，不但大大减小了 PLC 控制系统的体积，而且大大降低了能耗和设备成本，使整个系统的性价比得到大幅提高。

2．PLC 在工业现场的应用

PLC 广泛应用于工业控制的各个领域，如电动机控制、车床控制、电梯控制、交通信号灯控制、供电系统控制等。按 PLC 具体功能，其应用可分为以下几种。

1）逻辑控制　PLC 利用其“与”、“或”、“非”等逻辑运算功能，取代传统的继电器，实现顺序逻辑控制、组合逻辑控制和定时控制。这种逻辑控制可以实现生产过程控制、电梯控制和交通信号灯控制等。

2）运动控制　PLC 可以控制步进电动机、伺服电动机或车床等机械进行圆周运动或直线运动。当这种控制为闭环时，可以实现对机械运动速度、位置或加速度等的精密控制。PLC 的

运动控制功能常用于步进电动机和伺服电动机的速度控制、电梯位置控制及精密车床控制中。

3）通信联网　PLC 的通信模块支持其与其他 PLC、个人计算机及设备间的远程通信和信息交换，从而形成 PLC、其他计算机系统和被控对象之间的通信网络，进而实现分散集中的远程 PLC 控制系统。

1.3　S7-200CN 系列可编程控制器及其 I/O 模块

PLC 在工业控制领域中具有重要的作用，欧姆龙、西门子、三菱、施耐德、松下和 LG 等众多国际知名公司都在进行 PLC 的研发和生产。在中国 PLC 产品中，西门子（SIEMENS）公司生产的 PLC 在我国工业控制领域中占有重要份额，受到了广泛好评。本节将介绍西门子公司生产的 S7-200CN 系列 PLC 的结构及其 I/O 模块。

1. S7-200CN 系列 PLC

西门子公司的第一代 PLC 产品 SIMATIC S3 于 1975 年投入市场，其后经过几次升级换代，产品性能得到极大提高和完善。目前，该公司的 PLC 产品包括 S5 系列、LOGO、S7-200、S7-300、S7-400。

诞生于 1994 年的 SP7 系列是西门子 PLC 的典型代表，该系列 PLC 性能高，体积小，并且具有基于 Windows 的用户开发界面，在我国应用非常广泛。SP7 系列 PLC 共有 3 个机型，即 S7-200、S7-300 和 S7-400。其中，S7-200 属于微型机，适合低性能要求的模块化小型控制系统；S7-300 是中型机，模块多于 S7-200，适合中型控制系统；而 S7-400 属于中/大型机，规模更大，性能也更强。

只在中国销售的 S7-200CN 系列是 S7-200 PLC 中的经典产品，针对小型模块化控制系统设计，继承了 S7-200 的优良性能，适用于各种检测、监测及自动化系统，应用领域包括机床、机械和电力设施等。S7-200CN 系列 PLC 有 4 个不同的基本型号的 8 种规格的 CPU，其主要优点是可靠性高，指令集丰富，实时性好，扩展模块丰富，通信能力强和内置集成功能丰富等。

S7-200CN PLC 系统由 S7-200CN CPU 模块、个人计算机主机、编程器和通信电缆等组成。CPU 模块又称为主机，是 S7-200CN PLC 系统的基本组成单元，包括中央处理器（CPU）、存储器卡（存放程序和数据）、通信口（RS-485 串行通信接口）、电源和数字量输入/输出端子（I/O 端子）等。

S7-200CN CPU 模块外观如图 1-3 所示，其中关键部件包括：

（1）状态 LED，指示 CPU 运行状态，如系统错误/诊断（SF/DLAG）、RUN（运行）、STOP（停止）。

（2）可选卡插槽，可插存储卡、时钟卡和电池卡。

（3）前盖，内置 CPU 工作模式选择开关（RUN/STOP）、模拟电位器和扩展 I/O 接口（连接主机和扩展 I/O 模块）。

（4）顶部端子盖，内置 CPU 电源和输出端子。

（5）底部端子盖，内置传感器接口电源和输入端子。

（6）DIN 导轨是可编程控制器的机械安装导轨，可利用 PLC 或扩展模块上的标准（DIN）导轨夹片将 PLC 或扩展模块固定在 DIN 导轨上，实现 PLC 系统的快速安装。

（7）串行通信口，为 RS-485 通信接口，通过该接口可实现与其他 PLC、编程器、打印机、显示器等外部设备的通信。

（8）I/O LED，指示 I/O 端口的工作状态。

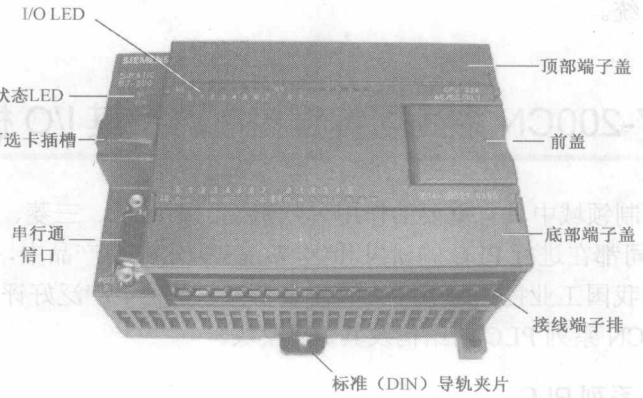

图 1-3　SP-200CN CPU 模块外观

2. S7-200CN 系列 PLC 的 I/O 模块

PLC 内部是低电压、低电流和低功率的，而大多数传感器和执行机构却是大电压、大电流和高功率的，二者不能直接相连。输入/输出（I/O）模块的作用是进行 PLC 与传感器和执行器间不同电气标准的转换，以实现 PLC 与传感器和执行机构的连接。

S7-200CN 主机自身带有一定数量的 I/O 端口，当该端口数量不够时，可以通过前盖内的扩展 I/O 接口进行 I/O 模块扩展。S7-200CN 的 I/O 模块可分 3 种，即数字量 I/O 模块、模拟量 I/O 模块和智能 I/O 模块。

1）数字量 I/O 模块　用于连接 PLC 和开关控制的传感器或执行机构，可分为数字量输入模块、数字量输出模块和数字量输入/输出模块 3 种。

（1）数字量输入模块：允许 CPU 读取输入映像存储器的数据，该数据的每个位反映了一个独立开关或开关传感器（如按钮、限位开关或继电器触点等）的开关状态，其原理如图 1-4 所示。

（2）数字量输出模块：从输出映像存储器接收输出数据，该数据的每个位将控制一个独立的开关或开关传感器（如继电器线圈、接触线圈或指示灯等）的开和关，其原理如图 1-5 所示。

图 1-4 和图 1-5 中电源可以是直流的，也可以是交流的，据此数字量输入（或输出）模块可以分成直流输入（或输出）模块和交流输入（或输出）模块两种。

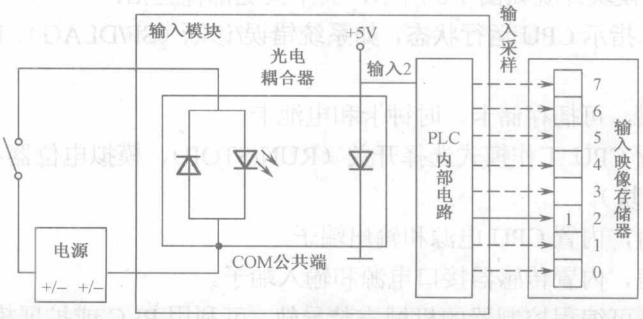

图 1-4　数字量输入模块原理图

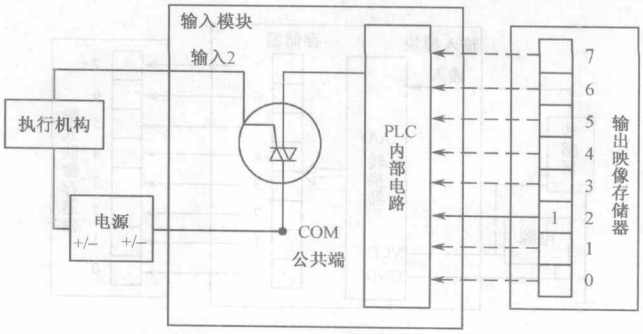

图 1-5　数字量输出模块原理图

（3）数字量输入/输出模块：在一个模块上既能输入又能输出数字量的模块称为组合模块或输入/输出模块，组合模块使 PLC 系统配置更灵活、方便。

S7-200CN 常用的数字量输入模块、数字量输出模块和数字量输入/输出模块分别为 EM221、EM222 和 EM223。

2）模拟量 I/O 模块　在工业控制中，除了利用数字量模块控制继电器、接触开关等类开关器件外，还需要进行模拟量（如温度、湿度和压力等）的控制，而 PLC 的 CPU 只能处理数字信号，因此需要把 PLC 输出的数字量转换成模拟量（D/A 转换）或把 PLC 输入的模拟量转换成相应的数字量（A/D 转换）。模拟量 I/O 模块可以完成这种转换。

（1）模拟量输出模块（D/A）：需要接收 CPU 写入的二进制数值，然后利用 D/A 转换芯片产生与该二进制数值成比例变化的模拟量输出信号（如电压或电流），该模拟信号可以用来控制电动阀门和变频器等需模拟量驱动的执行机构。模拟量输出模块原理如图 1-6 所示，数字量转换为模拟量的基本步骤如图 1-7 所示。

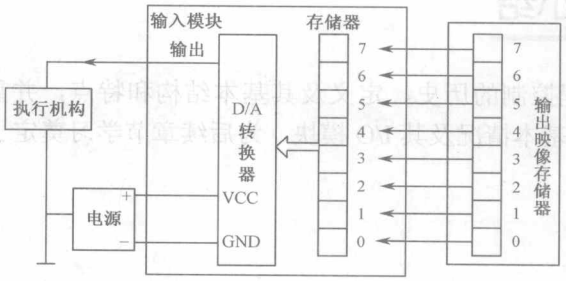

图 1-6　模拟量输出模块原理图

图 1-7　数字量转换为模拟量的基本步骤

（2）模拟量输入模块（A/D）：其作用与模拟量输出模块相反，它要将电压或电流信号转换成 PLC 的 CPU 可以读的数字量。模拟量输入模块原理如图 1-8 所示，模拟量转换为数字量的基本步骤如图 1-9 所示。

（3）模拟量输入/输出模块：同时具有模拟量输入通道和模拟量输出通道，使用灵活方便。S7-200CN 常用的模拟量输入模块、模拟量输出模块和模拟量输入/输出模块分别为 EM231、EM232 和 EM235。