双色版

西门子 S7-300/400PLC 从入门到精通

陈忠平　邬书跃　梁　华　侯玉宝　编著

XIMENZI S7-300/400PLC
CONGRUMEN DAO JINGTONG

中国电力出版社
CHINA ELECTRIC POWER PRESS

西门子 S7-300/400PLC 从入门到精通

XIMENZI S7-300/400PLC
CONGRUMEN DAO JINGTONG

陈忠平　邬书跃　梁　华　侯玉宝　编著

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

西门子 S7-300/400 PLC（可编程逻辑控制器）是国内应用较广、市场占有率较高的大中型产品。本书从实际工程应用出发，以 S7-300/400 PLC 为对象，讲解模块式 PLC 的基础与实际应用等方面的内容。本书共分 10 章，主要介绍了 PLC 的基本概况、S7-300/400 PLC 的硬件系统、S7-300/400 PLC 编程软件的使用方法、S7-300/400 PLC 的基本指令、S7-300/400 PLC 的功能指令、S7-300/400 PLC 的程序结构、梯形图的顺序控制设计方法、S7-300/400 PLC 模拟量功能与 PID 闭环控制、PLC 的通信与网络、PLC 的安装与维护等内容。

本书语言通俗易懂，实例的实用性和针对性较强，特别适合初学者使用，对有一定 PLC 基础知识的读者也会有很大帮助。本书既可作为电气控制领域技术人员的自学教材，也可作为高职高专院校、成人高校的电气工程、自动化、机电一体化、计算机控制等专业的参考书。

图书在版编目（CIP）数据

西门子 S7-300/400 PLC 从入门到精通/陈忠平等编著．—北京：中国电力出版社，2019.1

ISBN 978-7-5198-2455-6

Ⅰ．①西… Ⅱ．①陈… Ⅲ．①PLC 技术 Ⅳ．①TM571.61

中国版本图书馆 CIP 数据核字（2018）第 224210 号

出版发行：中国电力出版社

地　　址：北京市东城区北京站西街 19 号（邮政编码 100005）

网　　址：http://www.cepp.sgcc.com.cn

责任编辑：刘　炽（liuchi1030@163.com）

责任校对：黄　蓓　常燕昆　太兴华

装帧设计：左　铭

责任印制：杨晓东

印　　刷：三河市航远印刷有限公司

版　　次：2019 年 1 月第一版

印　　次：2019 年 1 月北京第一次印刷

开　　本：787 毫米×1092 毫米　16 开本

印　　张：35.5

字　　数：836 千字

印　　数：0001—2000 册

定　　价：128.00 元

版 权 专 有　侵 权 必 究

本书如有印装质量问题，我社发行部负责退换

此为试读，需要完整PDF请访问：www.ertongbook.com

前言

PLC（可编程控制器）是以微处理器为基础，综合了计算机技术、自动控制技术和通信技术而发展起来的一种新型、通用工业自动控制装置。PLC以其可靠性高、灵活性强、易于扩展、通用性强、使用方便等优点，已成为工业自动化领域中最重要、应用最广的控制设备之一。

德国西门子SIMATIC[1]S7-300/400 PLC属于模块式、大中型可编程序控制器，它是西门子PLC的主流产品，在国内应用范围较广，具有较高的市场占有率。为便于学习和理解S7-300/400 PLC控制系统的相关技术，特编写此书。本书特点如下：

（1）由浅入深，循序渐进。本书在内容编排上采用由浅入深、由易到难的原则，在介绍PLC的组成及工作原理、硬件系统构成、软件的使用等基础上，在后续章节中结合具体的实例，逐步讲解相应指令的应用等相关知识。

（2）技术全面，内容充实。全书重点突出，层次分明，注重知识的系统性、针对性和先进性。对于指令的讲解，不是泛泛而谈，而是辅以简单的实例，使读者更易于掌握。注重理论与实践相结合，培养工程应用能力。本书的大部分实例取材于实际工程项目或其中的某个环节，对读者从事PLC应用和工程设计具有较大的实践指导意义。

（3）分析原理，步骤清晰。对于每个实例，都分析其设计原理，总结实现的思路和步骤。读者可以根据具体步骤实现书中的例子，将理论与实践相结合。

（4）软硬结合，实例仿真。由于昂贵的培训费用和硬件价格，一般人很难通过大量的PLC硬件进行S7-300/400 PLC的实际操作学习。S7-PLCSIM是S7-300/400 PLC的仿真软件，具有功能强大、使用方便等特点，是学习S7-300/400 PLC的较好工具。所以书中大部分实例都是基于STEP 7编程软件和S7-PLCSIM仿真软件相结合的方式进行讲解，使读者能够按实例中的叙述生成项目、硬件组态、编写程序和做仿真实验，能够在尽量少花钱的情况下快速学好这门技术。

本书主要内容如下：

第1章为PLC的基本概况，主要介绍了对PLC的定义、基本功能与特点、应用和分类，以及PLC的组成及工作原理。

第2章为S7-300/400 PLC的硬件系统，主要介绍了S7-300/400 PLC的系统构成与连接、CPU模块、数字量I/O模块、数制与数据类型、存储区与寻址方式。

第3章为S7-300/400 PLC编程软件的使用，主要介绍了PLC编程语言的种类，并重点讲述STEP 7 V5.5编程软件及S7-PLCSIM仿真软件的使用。

第4章为S7-300/400 PLC的基本指令，主要介绍了位逻辑指令、定时器指令、计数器指令，并通过实例讲解这些基本指令的使用方法。

第5章为S7-300/400 PLC的功能指令，主要介绍了数据装入与传送指令、

[1] 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）。

数据转换与比较指令、数学运算指令、逻辑运算指令、程序控制指令等内容。

第6章为S7-300/400 PLC的程序结构，主要介绍了S7-300/400 PLC中程序的分类、用户程序中的块及用户程序的编程方法，其次通过实例具体讲解了常用组织块、功能和功能块、系统功能和系统功能块、数据块的使用方法。

第7章为梯形图的顺序控制设计方法，主要介绍了梯形图的设计方法、顺序控制设计法与顺序功能图、常见的顺序控制编写梯形图的方法、S7 Graph的基本知识及参数设置方法，然后通过多个实例重点讲解了S7 Graph在单序列顺序控制、选择序列顺序控制、并行序列顺序控制中的应用。

第8章为S7-300/400 PLC的模拟量功能与PID闭环控制，主要介绍了模拟量的基本概念、S7-300/400 PLC的模拟量功能、PID闭环控制等内容。

第9章为PLC的通信与网络，主要介绍了数据通信的基础知识、工业局域网的基础知识、西门子PLC的MPI通信、西门子PLC的PROFIBUS通信、工业以太网通信等内容。

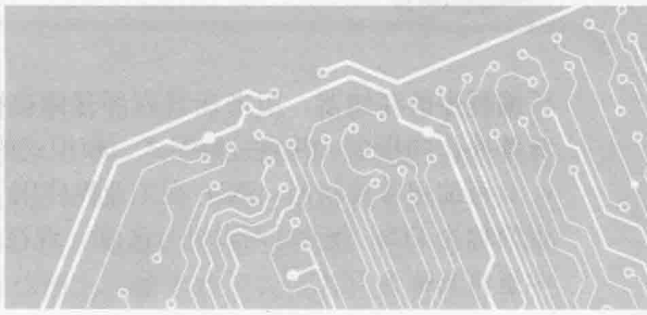
第10章为PLC的安装与维护，主要介绍了PLC的安装注意事项与步骤、S7-300/400 PLC的硬件安装、S7-300/400 PLC的维护和检修等内容。

参加本书编写工作的有湖南工程职业技术学院陈忠平，湖南涉外经济学院侯玉宝、高金定、梁华，衡阳技师学院胡彦伦，湖南航天诚远精密机械有限公司刘琼，湖南科技职业技术学院高见芳，湖南工程职业技术学院尹梅、邓霆、龙晓庆和龚亮，湖南三一重工集团王汉其等。全书由湖南工程职业技术学院陈建忠教授主审。此外，在编写过程中，还得到了武娟梅、陶有香、段秀莉、黄树辉、葛建、廖亦凡等同志的帮助和支持，在此一并表示感谢。

限于编者水平和编写经验，书中难免有错漏之处，敬请广大读者批评指正。

作者

目录



第1章

PLC的基本概况

自20世纪60年代末期世界第一台PLC问世以来，PLC发展十分迅速，特别是近些年来，随着微电子技术和计算机技术的不断发展，PLC在处理速度、控制功能、通信能力及控制领域等方面都有新的突破。PLC将传统的继电-接触器的控制技术和现代计算机信息处理技术的优点有机结合起来，成为工业自动化领域中最重要、应用最广的控制设备之一，并已成为现代工业生产自动化的重要支柱。

1.1 PLC 简 介

1.1.1 PLC的定义

可编程控制器是在继电器控制和计算机控制的基础上开发出来的，并逐渐发展以微处理器为基础，综合计算机技术、自动控制技术和通信技术等现代科技为一体的新型工业自动控制装置。目前广泛应用于各种生产机械和生产过程的自动控制系统中。

因早期的可编程控制器主要用于代替继电器实现逻辑控制，因此将其称为可编程逻辑控制器（Programmable Logic Controller，PLC）。随着技术的发展，许多厂家采用微处理器（Micro Processor Unit，MPU）作为可编程控制的中央处理单元（Central Processing Unit，CPU），大大加强了PLC的功能，使它不仅具有逻辑控制功能，还具有算术运算功能和对模拟量的控制功能。据此美国电气制造协会（National Electrical Manufacturers Association，NEMA）于1980年将它正式命名为可编程序控制器（Programmable Controller，PC），且对PC作如下定义："PC是一种数字式的电子装置，它使用了可编程序的存储器以存储指令，能完成逻辑、顺序、计时、计数和算术运算等功能，用以控制各种机械或生产过程"。

国际电工委员会（IEC）在1985年颁布的标准中，对可编程序控制器作如下定义："可编程序控制器是一种专为工业环境下应用而设计的数字运算操作的电子系统。它采用

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、模拟式的输入和输出，控制各种机械或生产过程。”

可编程序控制器（PC）在工业界使用了多年，但因个人计算机（personal computer）也简称为 PC，为了对两者进行区别，现在通常把可编程序控制器简称为 PLC，所以本书中也将其称为 PLC。

1.1.2 PLC 的基本功能与特点

1.1.2.1 PLC 的基本功能

PLC 基本功能包括逻辑控制功能、定时控制功能、计数控制功能、步进控制功能、数据处理功能、A/D 与 D/A 转换功能、通信联网功能和监控功能。

（1）逻辑控制功能。逻辑控制又称为顺序控制或条件控制，它是 PLC 应用最广泛的领域。逻辑控制功能实际上就是位处理功能，使用 PLC 的“与”（AND）、“或”（OR）、“非”（NOT）等逻辑指令，取代继电器触点的串联、并联及其他各种逻辑连接，进行开关控制。

（2）定时控制功能。PLC 的定时控制，类似于继电-接触器控制领域中的时间继电器控制。在 PLC 中有许多可供用户使用的定时器，这些定时器的定时时间可由用户根据需要进行设定。PLC 执行时根据用户定义时间长短进行相应限时或延时控制。

（3）计数控制功能。PLC 为用户提供了多个计数器，PLC 的计数器类似于单片机中的计数器，其计数初值可由用户根据需求进行设定。执行程序时，PLC 对某个控制信号状态的改变次数（如某个开关的动合次数）进行计数，当计数到设定值时，发出相应指令以完成某项任务。

（4）步进控制功能。步进控制（又称为顺序控制）功能是指在多道加工工序中，使用步进指令控制在完成一道工序后，PLC 自动进行下一道工序。

（5）数据处理功能。PLC 一般具有数据处理功能，可进行算术运算、数据比较、数据传送、数据移位、数据转换、编码、译码等操作。中、大型 PLC 还可完成开方、PID（即比例、积分、微分）运算、浮点运算等操作。

（6）A/D 与 D/A 转换功能。有些 PLC 通过 A/D、D/A 模块完成模拟量和数字量之间的转换、模拟量的控制和调节等操作。

（7）通信联网功能。PLC 通信联网功能是利用通信技术，进行多台 PLC 间的同位链接、PLC 与计算机链接，以实现远程 I/O 控制或数据交换。可构成集中管理、分散控制的分布式控制系统，以完成较大规模的复杂控制。

（8）监控功能。监控功能是指利用编程器或监视器对 PLC 系统各部分的运行状态、进程、系统中出现的异常情况进行报警和记录，甚至自动终止运行。通常小型低档 PLC 利用编程器监视运行状态；中档以上的 PLC 使用 CRT 接口，从屏幕上了解系统的工作状况。

1.1.2.2 PLC 的特点

PLC 的特点如下：

（1）可靠性高、抗干扰能力强。继电-接触器控制系统使用大量的机械触点，连接线路比较繁杂，且触点通断时有可能产生电弧和机械磨损，影响其寿命，降低了可靠性。

PLC中采用现代大规模集成电路，比机械触点继电器的可靠性要高。在硬件和软件设计中都采用了先进技术以提高可靠性和抗干扰能力。比如，用软件代替传统继电-接触器控制系统中的中间继电器和时间继电器，只剩下少量的输入/输出硬件，将触点因接触不良造成的故障大大减小，提高了可靠性；所有I/O接口电路采用光电隔离，使工业现场的外电路与PLC内部电路进行电气隔离；增加自诊断、纠错等功能，使其在恶劣工业生产现场的可靠性、抗干扰能力提高了。

(2) 灵活性好、扩展性强。继电-接触器控制系统由继电器等低压电器采用硬件接线实现的，连接线路比较繁杂，而且每个继电器的触点有数目有限。当控制系统功能改变时，需改变线路的连接。所以继电-接触器控制系统的灵活性、扩展性差。而由PLC构成的控制系统中，只需在PLC的端子上接入相应的控制线即可，减少接线。当控制系统功能改变时，有时只需编程器在线或离线修改程序，就能实现其控制要求。PLC内部有成大量的编程元件，能进行逻辑判断、数据处理、PID调节和数据通信功能，可以实现非常复杂的控制功能，若元件不够时，只需加上相应的扩展单元即可，因此PLC控制系统的灵活性好、扩展性强。

(3) 控制速度快、稳定性强。继电-接触器控制系统是依靠触点的机械动作来实现控制的，其触点的动断速度一般在几十毫秒，影响控制速度，有时还会出现抖动现象。PLC控制系统由程序指令控制半导体电路来实现的，响应速度快，一般执行一条用户指令在微秒内即可，PLC内部有严格的同步，不会出现抖动现象。

(4) 延时调整方便，精度较高。继电-接触器控制系统的延时控制是通过时间继电器来完成的，而时间继电器的延时调整不方便，且易受环境温度和湿度的影响，延时精度不高。PLC控制系统的延时是通过内部时间元件来完成的，不受环境温度和湿度的影响，定时元件的延时时间只需改变定时参数即可，因此其定时精度较高。

(5) 系统设计安装快、维修方便。继电-接触器实现一项控制工程，其设计、施工、调试必须依次进行，周期长、维修较麻烦。PLC使用软件编程取代继电-接触器中的硬件接线而实现相应功能，使安装接线工作量减小，现场施工与控制程序的设计还可同时进行，周期短、调试快。PLC具有完善的自诊断、履历情报存储及监视功能，对于其内部工作状态、通信状态、异常状态和I/O点的状态均有显示，若控制系统有故障时，工作人员通过它即可迅速查出故障原因，及时排除故障。

1.1.3 PLC的应用和分类

1.1.3.1 PLC的应用

以前由于PLC的制造成本较高，其应用受到一定的影响。随着微电子技术的发展，PLC的制造成本不断下降，同时PLC的功能大大增强，因此PLC目前已广泛应用于冶金、石油、化工、建材、机械制造、电力、汽车、造纸、纺织、环保等行业。从应用类型看，其应用范围大致归纳以下几种：

(1) 逻辑控制。PLC可进行“与”“或”“非”等逻辑运算，使用触点和电路的串联、并联代替继电-接触器系统进行组合逻辑控制、定时控制、计数控制与顺序逻辑控制。这是PLC应用最基本、最广泛的领域。

(2) 运动控制。大多数PLC具有拖动步进电动机或伺服电动机的单轴或多轴位置的

此为试读，需要完整PDF请访问：www.ertongbook.com

专用运动控制模块，灵活运用指令，使运动控制与顺序逻辑控制有机结合在一起，广泛用于各种机械设备。如对各种机床、装配机械、机械手等进行运动控制。

(3) 过程控制。现代中、大型 PLC 都具有多路模拟量 I/O 模块和 PID 控制功能，有的小型 PLC 也具有模拟量输入/输出模块。PLC 可将接收到的温度、压力、流量等连续变化的模拟量，通过这些模块实现模拟量和数字量的 A/D 或 D/A 转换，并对被控模拟量进行闭环 PID 控制。这一控制功能广泛应用于锅炉、反应堆、水处理、酿酒等方面。

(4) 数据处理。现代 PLC 具有数学运算（如矩阵运算、函数运算、逻辑运算等）、数据传送、转换、排序、查表、位操作等功能，可进行数据采集、分析、处理，同时可通过通信功能将数据传送给别的智能装置，如 PLC 对计算机数值控制 CNC 设备进行数据处理。

(5) 通信联网控制。PLC 通信包括 PLC 与 PLC、PLC 与上位机（如计算机）、PLC 与其他智能设备之间的通信。PLC 通过同轴电缆、双绞线等设备与计算机进行信息交换，可构成“集中管理、分散控制”的分布式控制系统，以满足工厂自动化（factory automation，FA）系统、柔性制造系统（flexible manufacturing system，FMS）、集散控制系统（distributed control system，DCS）等发展的需要。

1.1.3.2 PLC 的分类

PLC 种类繁多，性能规格不一，通常根据其流派、结构形式、性能高低、控制规模等方面进行分类。

1. 按流派分类

世界上有 200 多个 PLC 厂商，400 多种 PLC 产品。根据地域的不同，主要分成 3 个流派：美国流派产品、欧洲流派产品和日本流派产品。美国和欧洲的 PLC 技术是在相互隔离情况下独立研究开发的，因此美国和欧洲的 PLC 产品有明显的差异性，且以大中型 PLC 而闻名。而日本的 PLC 技术是由美国引进的，对美国的 PLC 产品有一定的继承性，但日本的主推产品定位在小型 PLC 上。

(1) 美国 PLC 产品。美国是 PLC 生产大国，有 100 多家 PLC 厂商，著名的有 A-B、通用电气（GE）公司、莫迪康（MODICON）公司、德州仪器（TI）公司、西屋公司等。

A-B（Allen-Bradley，艾伦-布拉德利）是罗克韦尔自动化有限公司（Rockwell Automation）的知名品牌，其 PLC 产品规格齐全、种类丰富。A-B 小型 PLC 为 MicroLogix PLC，主要型号有 MicroLogix1000、MicroLogix1100、MicroLogix1200、MicroLogix1400、MicroLogix1500，其中 MicroLogix1000 体积小巧、功能全面、是小型控制系统的理想选择；MicroLogix1200 能够在空间有限的环境中，为用户提供强大的控制功能，满足不同应用项目的需要；MicroLogix1500 不仅功能完善，而且还能根据应用项目的需要进行灵活扩展，适用于要求较高的控制系统。A-B 中型 PLC 为 CompactLogix PLC，该系列 PLC 可以通过 EtherNet/IP、控制网、设备网来远程控制输入/输出和现场设备，实现不同地点的分布式控制。A-B 大型 PLC 为 ControlLogix PLC，该系列 PLC 提供可选的用户内存模块（750kB～8MB），能解决有大量输入/输出点数系统的应用问题（支持多达 4000 点模拟量和 128 000 点数字量）；可以控制本地输入/输出和远程输入/输出；可以通过以太网 EtherNet/IP、控制网 ControlNet、设备网 DeviceNet 和远程输入/输出 Universal Remote I/O 来监控系统中的输入和输出。

GE公司的PLC代表产品是：小型机GE－1、GE－1/J、GE－1/P等，除GE－1/J外，均采用模块结构。GE－1用于开关量控制系统，最多可配置到112个I/O点。GE－1/J是更小型化的产品，其I/O点最多可配置到96点。GE－1/P是GE－1的增强型产品，增加了部分功能指令（数据操作指令）、功能模块（A/D、D/A等）、远程I/O功能等，其I/O点最多可配置到168点。中型机GE－Ⅲ，它比GE－1/P增加了中断、故障诊断等功能，最多可配置到400个I/O点。大型机GE－Ⅴ，它比GE－Ⅲ增加了部分数据处理、表格处理、子程序控制等功能，并具有较强的通信功能，最多可配置到2048个I/O点。GE－Ⅵ/P最多可配置到4000个I/O点。

德州仪器（TI）公司的小型PLC产品有510、520和TI100等，中型PLC产品有TI300、5TI等，大型PLC产品有PM550、530、560、565等系列。除TI100和TI300无联网功能外，其他PLC都可实现通信，构成分布式控制系统。

莫迪康（MODICON）公司有M84系列PLC。其中M84是小型机，具有模拟量控制、与上位机通信功能，最多I/O点为112点。M484是中型机，其运算功能较强，可与上位机通信，也可与多台联网，最多可扩展I/O点为512点。M584是大型机，其容量大、数据处理和网络能力强，最多可扩展I/O点为8192。M884增强型中型机，它具有小型机的结构、大型机的控制功能，主机模块配置2个RS－232C接口，可方便地进行组网通信。

（2）欧洲PLC产品。德国的西门子（SIEMENS）公司、AEG公司、法国的TE公司是欧洲著名的PLC制造商。德国西门子的电子产品以性能精良而久负盛名。在中、大型PLC产品领域与美国的A－B公司齐名。

（3）日本PLC产品。日本的小型PLC最具特色，在小型机领域中颇具盛名，某些用欧美的中型机或大型机才能实现的控制，日本的小型机就可以解决。在开发较复杂的控制系统方面明显优于欧美的小型机，所以格外受用户欢迎。日本有许多PLC制造商，如三菱、欧姆龙、松下、富士、日立、东芝等，在世界小型PLC市场上，日本产品约占有70%的份额。

三菱公司的PLC是较早进入中国市场的产品。其小型机F1/F2系列是F系列的升级产品，早期在我国的销量也不小。F1/F2系列加强了指令系统，增加了特殊功能单元和通信功能，比F系列有了更强的控制能力。继F1/F2系列之后，20世纪80年代末三菱公司又推出FX系列，在容量、速度、特殊功能、网络功能等方面都有了全面的加强。FX2系列是在20世纪90年代开发的整体式高功能小型机，它配有各种通信适配器和特殊功能单元。FX2N为高功能整体式小型机，它是FX2的换代产品，各种功能都有了全面的提升。近年来还不断推出满足不同要求的微型PLC，如FXOS、FX1S、FX0N、FX1N及α系列等产品。

三菱公司的大中型机有A系列、QnA系列、Q系列，具有丰富的网络功能，I/O点数可达8192点。其中Q系列具有超小的体积、丰富的机型、灵活的安装方式、双CPU协同处理、多存储器、远程口令等特点，是三菱公司现有PLC中最高性能的PLC。

欧姆龙（OMRON）公司的PLC产品，大、中、小、微型规格齐全。微型机以SP系列为代表，其体积极小，速度极快。小型机有P型、H型、CPM1A系列、CPM2A系列、CPM2C、CQM1等。P型机现已被性价比更高的CPM1A系列所取代，CPM2A/2C、

CQM1 系列内置 RS-232C 接口和实时时钟，并具有软 PID 功能，CQM1H 是 CQM1 的升级产品。中型机有 C200H、C200HS、C200HX、C200HG、C200HE、CS1 系列。C200H 是前些年畅销的高性能中型机，配置齐全的 I/O 模块和高功能模块，具有较强的通信功能和网络功能。C200HS 是 C200H 的升级产品，指令系统更丰富、网络功能更强。C200HX/HG/HE 是 C200HS 的升级产品，有 1148 个 I/O 点，其容量是 C200HS 的 2 倍，速度是 C200HS 的 3.75 倍，有品种齐全的通信模块，是适应信息化的 PLC 产品。CS1 系列具有中型机的规模、大型机的功能，是一种极具推广价值的新机型。大型机有 C1000H、C2000H、CV（CV500/CV1000/CV2000/CVM1）等。C1000H、C2000H 可单机或双机热备运行，安装带电插拔模块，C2000H 可在线更换 I/O 模块；CV 系列中除 CVM1 外，均可采用结构化编程，易读、易调试，并具有更强大的通信功能。

进入 21 世纪后，OMRON PLC 技术的发展日新月异，升级换代呈明显加速趋势，在小型机方面已推出了 CP1H/CP1L/CP1E 等系列机型。其中，CP1H 系列 PLC 是 2005 年推出的，与以往产品 CPM2A 40 点 PLC 输入输出型尺寸相同，但处理速度可达其实 10 倍。该机型外形小巧，速度极快，执行基本命令需 0.1μs，且内置功能强大。

松下公司的 PLC 产品中，FP0 为微型机，FP1 为整体式小型机，FP3 为中型机，FP5/FP10、FP10S（FP10 的改进型）、FP20 为大型机，其中 FP20 是最新产品。松下公司近几年 PLC 产品的主要特点是：指令系统功能强；有的机型还提供可以用 FP-BASIC 语言编程的 CPU 及多种智能模块，为复杂系统的开发提供了软件手段；FP 系列各种 PLC 都配置通信机制，由于它们使用的应用层通信协议具有一致性，这给构成多级 PLC 网络和开发 PLC 网络应用程序带来方便。

2. 按结构形式分类

根据 PLC 的硬件结构形式，将 PLC 分为整体式、模块式和混合式三类。

（1）整体式 PLC。整体式 PLC 是将电源、CPU、I/O 接口等部件集中配置装在一个箱体内，形成一个整体，通常将其称为主机或基本单元。采用这种结构的 PLC 具有结构紧凑、体积小、重量轻、价格较低、安装方便等特点，但主机的 I/O 点数固定，使用不太灵活。一般小型或超小型的 PLC 通常采用整体式结构。

（2）模块式 PLC。模块式 PLC 又称为积木式 PLC，它是将 PLC 各组成部分（如 CPU 模块、输入模块、输出模块、电源模块等）以独立模块的形式分开。模块式 PLC 由框架或基板和各种模块组成，将模块插在带有插槽的基板上，组装在一个机架内。采用这种结构的 PLC 具有配置灵活、装配方便、便于扩展和维修。大、中型 PLC 一般采用模块式结构。

（3）混合式 PLC。混合式 PLC 是将整体式的结构紧凑、体积小、安装方便和模块式的配置灵活、装配方便等优点结合起来的一种新型 PLC。如西门子公司生产的 S7-200（小型）、S7-300（中型）PLC。

3. 按性能高低分类

根据性能的高低，将 PLC 分为低档 PLC、中档 PLC 和高档 PLC 三类。

（1）低档 PLC。低档 PLC 具有基本控制和一般逻辑运算、计时、计数等基本功能，有的还具有少量模拟量输入/输出、算术运算、数据传送和比较、通信等功能。这类 PLC 只适合于小规模的简单控制，在联网中一般作为从机使用。如西门子公司生产的 S7-200

就属于低档 PLC。

(2) 中档 PLC。中档 PLC 有较强的控制功能和运算能力，它不仅能完成一般的逻辑运算，也能完成比较复杂的三角函数、指数和 PID 运算，工作速度比较快，能控制多个输入/输出模块。中档 PLC 可完成小型和较大规模的控制任务，在联网中不仅可作从机，也可作主机，如 S7 - 300 就属于中档 PLC。

(3) 高档 PLC。高档 PLC 有强大的控制和运算能力，不仅能完成逻辑运算、三角函数、指数、PID 运算、还能进行复杂的矩阵运算、制表和表格传送操作。可完成中型和大规模的控制任务，在联网中一般作主机，如西门子公司生产的 S7 - 400 就属于高档 PLC。

4. 按控制规模分类

根据 PLC 控制器的 I/O 总点数的多少可分为小型机、中型机和大型机。

(1) 小型机。I/O 总点数在 256 点以下的 PLC 称为小型机，如西门子公司生产的 S7 - 200 PLC、三菱公司生产的 FX2N 系列 PLC、欧姆龙公司生产的 CP1H 系列 PLC 均属于小型机。小型 PLC 通常用来代替传统继电-接触器控制，在单机或小规模生产过程中使用，它能执行逻辑运算、定时、计数、算术运算、数据处理和传送、高速处理、中断、联网通信及各种应用指令。I/O 总点数等于或小于 64 点的称为超小型或微型 PLC。

(2) 中型机。I/O 总点数在 256～2048 点之间的 PLC 称为中型机，如西门子公司生产的 S7 - 300 PLC、欧姆龙公司生产的 CQM1H 系列 PLC 属于中型机。中型 PLC 采用模块化结构，根据实际需求，用户将相应的特殊功能模块组合在一起，使其具有数字计算、PID 调节、查表等功能，同时相应的辅助继电器增多，定时、计数范围扩大，功能更强，扫描速度更快，适用于较复杂系统的逻辑控制和闭环过程控制。

(3) 大型机。I/O 总点数在 2048 以上的 PLC 称为大型机，如西门子公司生产的 S7 - 400 PLC、欧姆龙公司生产的 CS1 系列 PLC 属于大型机。I/O 总点数超过 8192 的称为超大型 PLC 机。大型 PLC 具有逻辑和算术运算、模拟调节、联网通信、监视、记录、打印、中断控制、远程控制及智能控制等功能。目前有些大型 PLC 的使用 32 位处理器，多 CPU 并行工作，具有大容量的存储器，使其扫描速度高速化，存储容量大大加强。

1.1.4 西门子 PLC 简介

德国西门子公司是欧洲最大的电子和电气设备制造商之一，生产的 SIMATIC 可编程序控制器在欧洲处于领先地位。其著名的“SIMATIC”商标，就是德国西门子在自动化领域的注册商标。其第一代可编程序控制器是 1975 年投放市场的 SIMATIC S3 系列的控制系统。

在 1979 年，微处理器技术被广泛应用于可编程序控制器中，产生了 SIMATIC S5 系列，取代了 S3 系列，之后在 20 世纪末又推出了 S7 系列产品。

经过多年的发展演绎，西门子公司最新的 SIMATIC 产品可以归结为 SIMATIC S7、M7 和 C7 等几大系列。

M7 - 300/400 采用与 S7 - 300/400 相同的结构，它可以作为 CPU 或功能模块使用。具有 AT 兼容计算机的功能，其显著特点是具有 AT 兼容计算机功能，使用 S7 - 300/400 的编程软件 STEP7 和可选的 M7 软件包，可以用 C、C++或 CFC（连续功能图）等语言来编程。M7 适用于需要处理数据量大，对数据管理、显示和实时性有较高要求和系统

使用。

C7 由 S7-300PLC、HMI（人机接口）操作面板、I/O、通信和过程监控系统组成。整个控制系统结构紧凑，面向用户配置/编程、数据管理与通信集成于一体，具有很高的性价比。

现今应用最为广泛的 S7 系列 PLC 是德国西门子公司在 S5 系列 PLC 基础上，于 1995 年陆续推出的性能价格比较高的 PLC 系统。

西门子 S7 系列 PLC 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。S7 系列 PLC 产品可分为微型 PLC（如 S7-200），小规模性能要求的 PLC（如 S7-300）和中、高性能要求的 PLC（如 S7-400）等。

S7-200 PLC 是超小型化的 PLC，由于其具有紧凑的设计、良好的扩展性、低廉的价格和强大的指令系统，它能适用于各行各业，各种场合中的自动检测、监测及控制等。S7-200 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。

S7-300 是模块化小型 PLC，能满足中等性能要求的应用。各种单独的模块之间可进行广泛组合构成不同要求的系统。与 S7-200 PLC 比较，S7-300 PLC 采用模块化结构，具备高速（0.6～0.1μs）的指令运算速度；用浮点数运算比较有效地实现了更为复杂的算术运算；一个带标准用户接口的软件工具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 S7-300 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 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；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）；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 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。具备强大的通信功能，S7-300 PLC 可通过编程软件 Step 7 的用户界面提供通信组态功能，这使得组态非常容易、简单。S7-300 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触点到点的通信系统；多点接口（MPI）集成在 CPU 中，用于同时连接编程器、PC 机、人机界面系统及其他 SIMATIC S7、M7、C7 等自动化控制系统。

S7-400 PLC 是用于中、高档性能范围的可编程序控制器。该系列 PLC 采用模块化无风扇的设计、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专用系统。当控制系统规模扩大或升级时，只要适当地增加一些模板，便能使系统升级和充分满足需要。

随着技术和工业控制的发展，西门子在技术层面上对 S7 系列 PLC 进一步升级。近几年推出了 S7-200 SMART、S7-1200、S7-1500 系列 PLC 产品。

S7-200 SMART 是西门子公司于 2012 年推出的专门针对中国市场的高性价比微型 PLC，可作为中国国内广泛使用的 S7-200 PLC 的替代产品。S7-200 SMART 的 CPU 内可安装一块多种型号的信号板，配置较灵活，保留了 S7-200 的 RS-485 接口，增加了一个以太网接口，还可以用信号板扩展一个 RS-485/RS-232 接口。S7-200 SMART 的编程语言、指令系统和监控方法与 S7-200 兼容。除了少数几条与硬件有关的指令，其

他指令与 S7 - 200 相同。S7 - 200 SMART 软件自带 Modbus RTU 指令库和 USS 协议指令库，而 S7 - 200 需要用户安装这些库。

S7 - 200 SMART 主要应用于小型单机项目，而 S7 - 1200 定位于中低端小型 PLC 产品线，可应用于中型单机项目或一般性的联网项目。S7 - 1200 是西门子公司于 2009 年推出的一款紧凑型、模块化的 PLC。S7 - 1200 的硬件由紧凑模块化结构组成，其系统 I/O 点数、内存容量均比 S7 - 200 多出 30%，充分满足市场的针对小型 PLC 的需求，可作为 S7 - 200 和 S7 - 300 之间的替代产品。

S7 - 1500 是西门子公司于 2012 年推出的大中型模块式 PLC，其模块比 S7 - 300 稍大，机架类似于 S7 - 300 的机架。相对于 S7 - 300/400 而言，S7 - 1500 采用新型的背板总线技术，采用高波特率和高传输协议，使其信号处理速率更快；S7 - 1500 支持的数据类型更为广泛，基本数据长度达到 64 位，而 S7 - 300/400 支持的基本数据长度为 32 位。

由于 S7 - 1200、S7 - 1500 是近几年才推出的产品，目前在许多控制领域还是以 S7 - 300/400 为主，要完全取代 S7 - 300/400 仍要经历一定的时间，因此本书以 S7 - 300/400 为例，讲述西门子大、中型 PLC 的相关知识。

1.2 PLC的组成及工作原理

1.2.1 PLC的组成

PLC 的种类很多，但结构大同小异，PLC 的硬件系统主要由中央处理器（CPU）、存储器、I/O 接口，电源、通信接口、扩展接口等单元部件组成，这些单元部件都是通过内部总线进行连接，如图 1 - 1 所示。

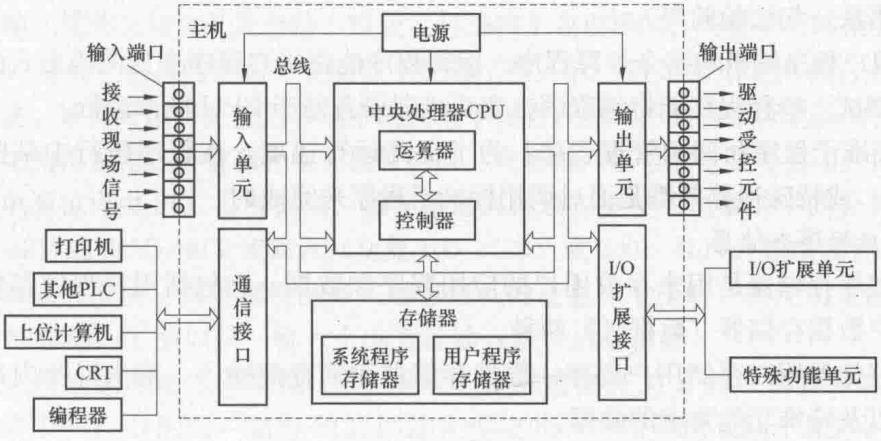


图 1 - 1 PLC 内部硬件结构框图

1.2.1.1 中央处理器

PLC 的中央处理器与一般的计算机控制系统一样，由运算器和控制器构成，是整个

系统的核心，类似于人类的大脑和神经中枢。它是 PLC 的运算、控制中心，用来实现逻辑和算术运算，并对全机进行控制，按 PLC 中系统程序赋予的功能，有条不紊地指挥 PLC 进行工作，主要完成以下任务：

(1) 控制从编程器、上位计算机和其他外部设备键入的用户程序数据的接收和存储。

(2) 用扫描方式通过输入单元接收现场输入信号，并存入指定的映像寄存器或数据寄存器。

(3) 诊断电源和 PLC 内部电路的工作故障和编程中的语法错误等。

(4) PLC 进入运行状态后，执行相应工作：①从存储器逐条读取用户指令，经过命令解释后，按指令规定的任务产生相应的控制信号去启闭相关控制电路，通俗讲就是执行用户程序，产生相应的控制信号；②进行数据处理，分时、分渠道执行数据存取、传送、组合、比较、变换等动作，完成用户程序中规定的逻辑运算或算术运算等任务；③根据运算结果，更新有关标志位的状态和输出寄存器的内容，再由输入映像寄存器或数据寄存器的内容，实现输出控制、制表、打印、数据通信等。

1.2.1.2 存储器

PLC 中存储器的功能与普通微机系统存储器的结构类似，它由系统程序存储器和用户程序存储器等部分构成。

1. 系统程序存储器

系统程序存储器是用可擦写可编程只读存储器（erasable programmable read-only memory，EPROM）或电可擦除可编程只读存储器（electrically erasable programmable read-only memory，EEPROM）来存储厂家编写的系统程序，系统程序是指控制和完成 PLC 各种功能的程序，相当于单片机的监控程序或微机的操作系统，在很大程度上它决定该系列 PLC 的性能与质量，用户无法更改或调用。系统程序有系统管理程序、用户程序编辑和指令解释程序、标准子程序和调用管理程序这 3 种类型。

(1) 系统管理程序：由它决定系统的工作节拍，包括 PLC 运行管理（各种操作的时间分配安排）、存储空间管理（生成用户数据区）和系统自诊断管理（如电源、系统出错，程序语法、句法检验等）。

(2) 用户程序编辑和指令解释程序：编辑程序能将用户程序变为内码形式以便于程序的修改、调试。解释程序能将编程语言变为机器语言便于 CPU 操作运行。

(3) 标准子程序和调用管理程序：为了提高运行速度，在程序执行中某些信息处理（I/O 处理）或特殊运算等都是通过调用标准子程序来完成的。

2. 用户程序存储器

用户程序存储器是用来存放用户的应用程序和数据，它包括用户程序存储器（程序区）和用户数据存储器（数据区）两种。

程序存储器用以存储用户程序。数据存储器用来存储输入、输出以及内部触点和线圈的状态以及特殊功能要求的数据。

用户存储器的内容由用户根据控制需要可读、可与、可任意修改、增删。常用的用户存储器形式有高密度、低功耗的 CMOS RAM（由锂电池实现断电保护，一般能保持 5～10 年，经常带负载运行也可保持 2～5 年）、EPROM 和 EEPROM 三种。

此为试读，需要完整PDF请访问：www.ertongbook.com