CMP科技经典
PLC

XITONG SHEJI JICHU YU KAIFA JIQIAO

实例解析 S7-300/400 PLC 系统设计基础与开发技巧

◎ 边春元　程立英　任双艳　渠丰沛　等编著

机械工业出版社
CHINA MACHINE PRESS

实例解析 S7-300/400 PLC 系统设计基础与开发技巧

边春元　程立英　任双艳　渠丰沛　等编著

机械工业出版社

西门子公司主流的 S7-300/400 系列 PLC 以其优越的性能和较高的性价比而得到广泛的应用。本书通过大量 S7-300/400 的应用实例，采用系统逐步深入的讲解方法，更直观有效地向读者阐述 PLC 系统的开发技巧。首先介绍了 S7-300/400 的硬件系统、指令系统、STEP7、通信与网络功能，其中内容是经总结并与实际开发最直接、最密切的基础知识。后半部分包括了十余个开发实例，最后三个实例的实用价值尤为突出。

本书既适用于初学者，也可作为工程技术人员的技术参考书或高校相关专业的参考书。

图书在版编目（CIP）数据

实例解析 S7-300/400PLC 系统设计基础与开发技巧/边春元等编著. —北京：机械工业出版社，2008.4

ISBN 978-7-111-23150-9

Ⅰ.实… Ⅱ.边… Ⅲ.可编程序控制器 Ⅳ.TP332.3

中国版本图书馆 CIP 数据核字（2007）第 199789 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：张俊红 责任编辑：王 欢 版式设计：冉晓华

责任校对：陈立辉 封面设计：陈 沛 责任印制：邓 博

北京市朝阳展望印刷厂印刷

2008 年 3 月第 1 版第 1 次印刷

184mm×260mm · 19.75 印张 · 488 千字

0001—4000 册

标准书号：ISBN 978-7-111-23150-9

定价：40.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

销售服务热线电话：（010）68326294

购书热线电话：（010）88379639 88379641 88379643

编辑热线电话：（010）88379768

封面无防伪标均为盗版

前　言

可编程序控制器（PLC）是以微处理器技术、电子技术、网络通信技术和先进可靠的工业手段为基础，综合了计算机技术、网络通信和自动控制技术的一种新型的通用自动控制装置。它具有功能强、可靠性高、使用灵活方便、易于编程以及适于在工业环境下应用等一系列优点，在工业自动化、机电一体化、传统产业技术改造等方面的应用越来越广泛，已成为现代工业控制的四大支柱（可编程序控制器技术、机器人技术、CAD/CAM 和数控技术）之一。

西门子公司的 S7-300/400 在大中型 PLC 中应用最广，市场占有率最高。S7-300/400 及其编程软件 STEP-7 和通信网络的功能强大，程序结构复杂。因此，一本系统讲解 S7-300/400 软硬件知识及其应用实例的书籍成为广大工程技术人员和高等院校师生的迫切需求。

本书在介绍 S7-300/400 PLC 的硬件、指令系统、编程环境、编程方法、程序结构、通信网络等方面内容的基础上，通过大量典型的应用实例，向读者深入浅出地介绍了 S7-300/400 PLC 应用开发的方法和手段。本书既适用于初学者，又可作为工程技术人员的技术参考书和高校相关专业研究生的教材。

本书共 11 章。第 1 章概括地介绍了 PLC 基础知识；第 2 章分析了 S7-300/400 系列 PLC 的硬件系统及内部资源；第 3 章介绍了 S7-300/400 系列 PLC 的指令系统及应用系统的设计；第 4 章介绍了 STEP7 软件的编程环境；第 5 章介绍了 PLC 的通信与网络功能；第 6 章介绍了应用 PLC 实现基本逻辑控制的典型实例；第 7 章讲述了 PLC 实现 PID 控制的方法和实例；第 8 章介绍了 PLC 电动机控制实例；第 9 章介绍了几种常用机床设备的 PLC 控制实例；第 10 章和 11 章分别介绍了热轧层流冷却控制系统实例和可逆冷轧机控制系统实例。

本书主要由边春元、程立英、任双艳和渠丰沛共同编写，参与部分章节编写、资料收集整理及程序调试的还有李爱平、王志强、张春有、梁洪力、王宇龙、何大勇、闫向峰、彭泽波、姜雪辉、田雪、徐福斌、黄慈君、马良玉、金东光和姜雪松。特别感谢沈阳理工大学机械工程学院液压教研室和东北大学信息学院电气自动化研究所的全体老师对本书编写过程中的指导和技术支持。

由于写作时间仓促，加上作者精力有限，书中难免有错漏之处，恳请广大读者批评指正，联系 E-mail 为 buptzjh@163.com。

作　者

2008 年 1 月

目　录

前言

第 1 章　绪论 …… 1

1.1　PLC 概述 …… 1

1.1.1　PLC 的发展 …… 1

1.1.2　PLC 的基本组成和工作原理 …… 3

1.1.3　PLC 的功能特点和分类 …… 7

1.2　西门子 S7 系列 PLC …… 11

1.3　系统的设计方法 …… 12

1.4　PLC 的应用 …… 15

第 2 章　硬件系统及内部资源 …… 16

2.1　硬件系统的基本结构 …… 16

2.1.1　基本组成 …… 17

2.1.2　基本结构 …… 19

2.2　PLC 的 CPU 模块和 I/O 模块 …… 21

2.2.1　S7-300 系列 PLC …… 21

2.2.2　S7-400 系列 PLC …… 29

2.2.3　I/O 模块的地址确定 …… 33

2.3　PLC 的分布式 I/O 模块 …… 34

2.4　PLC 的内部资源模块 …… 36

2.4.1　内部存储区 …… 36

2.4.2　外设 I/O 存储区 …… 39

2.4.3　累加器 …… 39

2.4.4　状态字寄存器 …… 40

第 3 章　指令系统及应用系统的设计 …… 42

3.1　指令系统预备知识 …… 42

3.1.1　数制 …… 42

3.1.2　数据类型 …… 42

3.2　S7-300/400 PLC 的指令系统 …… 44

3.2.1　指令的构成 …… 44

3.2.2　指令的操作数 …… 44

3.2.3　寻址方式 …… 45

3.3　S7-300/400 PLC 的常用指令 …… 46

3.3.1　位逻辑指令 …… 46

3.3.2　数据处理指令 …… 50

3.3.3　计数器与定时器指令 …… 54

3.3.4　数据运算指令 …… 57

3.3.5　程序控制指令 …… 63

3.3.6　数据块指令 …… 64

3.3.7　逻辑控制指令 …… 65

3.3.8　累加器操作指令 …… 66

3.4　PLC 应用系统的设计 …… 67

3.4.1　PLC 应用系统的硬件设计 …… 67

3.4.2　PLC 应用系统的软件设计 …… 71

第 4 章　STEP7 编程环境的使用 …… 74

4.1　STEP7 编程的流程 …… 76

4.1.1　创建与编辑项目 …… 78

4.1.2　硬件组态 …… 82

4.1.3　定义符号 …… 93

4.1.4　生成逻辑块 …… 99

4.1.5　参考数据的显示 …… 103

4.1.6　程序的上传和下载 …… 113

4.1.7　程序的调试和故障诊断 …… 119

4.2　PLC 程序结构 …… 134

4.2.1　CPU 程序 …… 135

4.2.2　用户程序 …… 135

4.2.3　功能块 …… 140

4.2.4　数据块 …… 142

4.2.5　组织块 …… 152

第 5 章　PLC 的通信与网络 …… 164

5.1　PLC 控制网络和通信功能 …… 164

5.2　S7-300/400 PLC 的通信网络 …… 165

5.3　工业以太网 …… 167

5.3.1　概述 …… 167

5.3.2　工业以太网的构成 …… 167

5.3.3　工业以太网的网络方案 …… 168

5.3.4　工业以太网的交换技术 …… 169

5.3.5　自适应与冗余网络 …… 170

5.4　MPI 网络 …… 170

5.4.1　概述 …… 170

5.4.2　全局数据通信 …… 171

5.4.3 MPI 网络的组态 …… 172
5.4.4 事件驱动的 GD 通信 …… 175
5.4.5 不用 GD 通信组态的 MPI 通信 … 175
5.5 AS-I 网络 …… 177
5.5.1 概述 …… 177
5.5.2 AS-I 网络部件 …… 178
5.5.3 AS-I 的寻址模式 …… 178
5.5.4 AS-I 的通信方式 …… 179
5.5.5 AS-I 的工作模式 …… 179
5.6 PROFIBUS 通信网络 …… 179
5.6.1 概述 …… 179
5.6.2 PROFIBUS 的通信协议 …… 180
5.6.3 PROFIBUS 的网络部件 …… 181
5.6.4 利用 STEP7 组态 PROFIBUS-DP 通信网络 …… 182
5.7 点对点通信 …… 187
5.7.1 点对点通信的硬件 …… 187
5.7.2 点对点通信协议 …… 188
5.7.3 用于点对点通信的功能块 …… 189

第 6 章 基本逻辑控制 …… 192
6.1 交通信号灯控制硬件配置及梯形图程序 …… 192
6.2 电梯控制硬件配置及梯形图程序 …… 194
6.3 开发技巧与经验总结 …… 198

第 7 章 PID 控制 …… 200
7.1 模拟量的 PID 控制 …… 200
7.2 PID 算法模拟量的闭环控制 …… 203
7.3 开发技巧与经验总结 …… 210

第 8 章 S7-300/400 PLC 电动机控制 …… 211
8.1 Y-△起动电动机控制 …… 211
8.2 双速电动机控制 …… 212
8.3 开发技巧与经验总结 …… 229

第 9 章 机床控制 …… 231
9.1 剪板机的 PLC 控制 …… 231
9.2 模压机的 PLC 控制 …… 233
9.3 自动选刀的 PLC 控制 …… 237
9.4 机械手的 PLC 自动控制 …… 240
9.5 开发技巧与经验总结 …… 243

第 10 章 热轧层流冷却控制系统 …… 244
10.1 层流冷却控制系统的功能 …… 244
10.1.1 控冷区控制功能概述 …… 244
10.1.2 控冷区域的设备概况及功能 …… 245
10.2 层流冷却控制系统硬件设计 …… 249
10.2.1 层流冷却系统的硬件配置 …… 249
10.2.2 层流冷却系统的网络组成 …… 249
10.2.3 定义 I/O 表及硬件控制原理 …… 250
10.3 层流冷却控制系统软件设计 …… 259
10.3.1 项目的创建 …… 260
10.3.2 硬件组态 …… 260
10.3.3 程序块的编写 …… 260
10.3.4 PLC 调试 …… 273
10.4 开发技巧与经验总结 …… 277

第 11 章 可逆冷轧机控制系统 …… 278
11.1 可逆冷轧机控制系统的功能 …… 278
11.2 可逆冷轧机控制系统的硬件设计 …… 285
11.2.1 系统的硬件配置 …… 285
11.2.2 系统的通信设置 …… 289
11.3 可逆冷轧机控制系统的软件设计 …… 290
11.3.1 系统的设计原理 …… 290
11.3.2 系统的软件实现 …… 290
11.4 开发技巧与经验总结 …… 297

附录 …… 299
附录 A 所有语句表指令 …… 299
附录 B 组织块、系统功能与系统功能块 …… 301
附录 C 常用英文缩写 …… 306

参考文献 …… 309

第1章 绪 论

可编程序控制器在其早期主要应用于开关量的逻辑控制，因此也被称为可编程序逻辑控制器，即 PLC（Programmable Logic Controller）。可编程序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通用的工业自动控制装置。它具有体积小、编程简单、功能强、抗干扰能力强、可靠性高、灵活通用与维护方便等优点，目前在冶金、化工、交通、电力等工业控制领域获得了广泛的应用。

1.1 PLC 概述

为了使 PLC 设计开发人员更好地了解 PLC 系统，本节将首先简要介绍 PLC 的发展，接下来将重点介绍 PLC 系统的基本组成和工作原理，最后讨论 PLC 的功能特点和分类。

1.1.1 PLC 的发展

本小节在回顾 PLC 的由来和发展历史的基础上，对 PLC 的发展趋势进行展望。

1. PLC 的由来

在可编程序控制器问世以前，工业控制领域中是以继电器控制占主导地位。这种由继电器构成的控制系统存在明显的缺点：体积大、耗电多、可靠性差、寿命短、运行速度不高，尤其是对生产工艺多变的系统适应性更差。如果生产任务和工艺发生变化，就必须重新设计，并且要改变硬件结构，这不仅影响了产品更新换代的周期，而且对于比较复杂的控制系统来说，不但设计制造困难，而且其可靠性不高，查找和排除故障也往往是费时和困难的。

1968 年，美国通用汽车公司（GM，General Motors）根据市场形势与生产发展的需要，提出了“多品种、小批量、不断翻新汽车品牌型号”的战略。为了尽可能地减少重新设计和重新接线的工作，从而降低成本、缩短周期，提出了研制新型逻辑顺序控制装置来取代继电器控制装置。第二年，美国数字设备公司（DEC，Digital Equipment Corporation）就研制出了基于集成电路和电子技术的控制装置，并将其应用于美国通用汽车自动装配生产线上，这是首次采用程序化的手段应用于电气控制，这台控制装置就是第一台 PLC。

2. PLC 的发展历程

虽然 PLC 问世时间不长，但随着计算机技术、半导体集成技术、控制技术和通信网络技术等高新技术的迅速发展，PLC 也迅速发展。PLC 的发展过程大致经历了以下四个阶段：

第一阶段，从第一台 PLC 问世到 20 世纪 70 年代中期，是 PLC 的初创阶段。

该时期 PLC 产品的主要功能只是执行原先由继电器完成的顺序控制、逻辑运算、定时和计数等。它的 CPU 由中小规模的数字集成电路组成，在 I/O 接口电路上做了改进以适应工业控制现场的要求，它的控制功能比较简单。在软件编程上，采用广大电气工程技术人员所熟悉的继电器控制线路的方式——梯形图。该阶段的代表产品有 MODICON 公司的 084、AB 公司的 PDQII、DEC 的 PDP-14 和日立公司的 SCY-022 等。

第二阶段，从 20 世纪 70 年代中期到末期，是 PLC 的实用化发展阶段。

20 世纪 70 年代，微处理器的出现使 PLC 发生了巨大的变化。随着多种 8 位微处理器的相继问世，PLC 技术产生了飞跃。该时期的 PLC 产品的主要控制功能得到了较大的发展，在逻辑运算功能的基础上，增加了数值运算、闭环调节功能，提高了运算速度，扩大了输入/输出规模，使得 PLC 的应用范围得以扩大。该阶段的代表产品有 MODICON 公司的 184、284、384，西门子公司的 SIMATIC S3 系列，富士电机公司的 SC 系列等。

第三阶段，从 20 世纪 70 年代末期到 80 年代中期，是 PLC 通信功能的实现阶段。

与计算机通信的发展相联系，PLC 在通信方面也有了很大的发展，初步形成了分布式的通信网络体系。但是，由于生产厂家各自为政，通信系统自成系统，因此，各产品互相通信是较困难的。在该阶段，由于生产过程控制的需要，对 PLC 的需求大大增加，产品的功能也得到了发展，数学运算的功能得到了较大的扩充，产品的可靠性进一步提高。该阶段的代表产品有富士电机公司的 MI-CREX 和德州仪器公司的 TI530 等。

第四阶段，从 20 世纪 80 年代中期开始，是 PLC 的开放阶段。

由于开放系统的提出，使 PLC 也得到了较大的发展。主要表现为通信系统的开放，使各生产厂家的产品可以互相通信，通信协议的标准化使用户得到了好处。在这一阶段，产品的规模增大，功能不断完善，大中型产品多数有 CRT 屏幕的显示功能，产品的扩展也因通信功能的改善而变得方便，此外，还采用了标准的软件系统，增加了高级编程语言等。该阶段的代表产品有西门子公司的 SIMATIC S7 系列和 AB 公司的 PLC-5 等。

3. PLC 的发展趋势

PLC 从诞生至今，虽然只有近 40 年的历史，但其发展势头十分迅猛。如今在工业自动化领域中，PLC 已经无处不在。随着技术的发展和市场需求的增加，PLC 的结构和功能得到不断改进，生产厂家不断推出功能更强的 PLC 产品，平均 3 ~ 5 年更新换代一次。今后，PLC 的发展可归纳于以下几个方面：

（1）人机界面更加友好

PLC 制造商纷纷通过收购或联合软件企业，发展软件产业，大大提高了其软件水平，多数 PLC 品牌拥有与之相应的开发平台和组态软件。软件和硬件的结合，提高了系统的性能，同时，为用户的开发和维护降低了成本，更易形成人机友好的控制系统。

（2）网络通信能力不断增强

PLC 厂家在原来 CPU 模板上提供物理层 RS-232/422/485 接口的基础上，逐渐增加了各种通信接口，提供完整的通信网络。由于近来数据通信技术发展很快，用户对开放性要求很高，现场总线技术及以太网技术也同步发展。

计算机与 PLC 之间，以及各个 PLC 之间的联网和通信能力的不断增强，使工业网络可以有效地节省资源、降低成本、提高系统可靠性和灵活性，使网络的应用有普遍化的趋势。工业中普遍采用金字塔结构的多级工业网络，与可编程序控制器硬件技术的发展相适应，工业软件的发展非常迅速，它使系统应用更加简单易行，大大方便了 PLC 系统的开发人员和操作使用人员。

（3）开放性和互操作性逐渐发展

PLC 在发展过程中，各 PLC 制造商为了垄断和扩大各自市场，处于群雄割据的局面，各自发展自己的标准，兼容性很差，这给用户使用带来不便，并增加了维护成本。开放是发

展的趋势，这已被各厂商所认识，逐渐形成了长期妥协与竞争的过程，并且这一过程还在继续。为了推动技术标准化的进程，一些国际性组织，如国际电工委会（IEC，International Electro Technical Commission），不断为 PLC 的发展制定一些新的标准，对各种类型的产品作一定的归纳或定义，对 PLC 未来的发展制定一种方向（或框架）。模块式结构使系统的构成更加灵活、方便；功能明确化、专用化的复杂功能由专门模块来完成。一般的 PLC 可分为主模块、扩展模块、I/O 模块以及各种高性能模块等，每种模块的体积都较小，相互连接方便、使用更简单、通用性更强。主机仅仅通过通信设备向模块发布命令和测试状态，这使得 PLC 的系统功能增强，控制系统设计更加简化，这进一步增强了软硬件的互操作性。

（4）PLC 的应用范围越来越广泛

大型 PLC 采用多微处理器系统，如有的采用了 32 位微处理器，可同时进行多任务操作，处理速度提高，存储容量大大增加，PLC 的网络能力、模拟量处理能力、复杂运算能力均大大增强，这使得 PLC 的功能进一步加强，不再局限于逻辑控制的应用，而越来越多地应用于过程控制和数据处理方面。另外，PLC 可以代替计算机进行管理、监控。智能 I/O 组件也将进一步发展，用来完成各种专门的任务（如位置控制、PID 调节、远程通信等）。

（5）以太网的发展对 PLC 有重要影响

以太网应用非常广泛，与工业网络相比，其成本非常低。为此，人们致力于将以太网引进控制领域。但是目前的挑战在于：①硬件上如何适应恶劣的工业环境；②通信机制如何提高其可靠性。以太网能否顺利进入工控领域，还存在争议，但以太网在工控系统的应用却日益增多。为适应这一过程，各 PLC 厂商纷纷推出适应以太网的产品或中间产品。

1.1.2 PLC 的基本组成和工作原理

在介绍 PLC 的基本组成和工作原理之前，首先了解一下传统继电器控制系统和 PLC 控制系统的组成。

传统的继电器控制系统通常由输入设备、继电器控制盘和输出设备三大部分组成，如图 1-1 所示。输入设备通常由被控对象的各种开关、按钮、传感器等构成。继电器控制盘通常由中间继电器、时间继电器和将这些器件连接起来的导线等组成。复杂的继电器控制系统，一般由一个或几个控制柜构成，系统构成比较庞大。输出设备由被控对象执行元件组成，如电磁阀、接触器等。

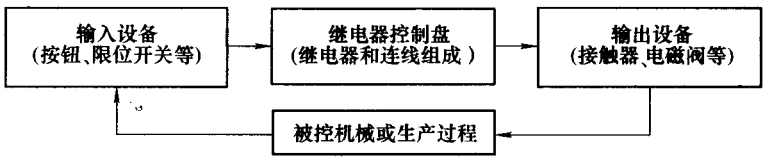

图 1-1 继电器控制系统

PLC 控制系统是从继电器控制系统发展而来的，其构成如图 1-2 所示。可以看出，这两种控制系统有很多相同之处，其中输入设备和输出设备基本相同，只是用 PLC 控制器取代了继电器控

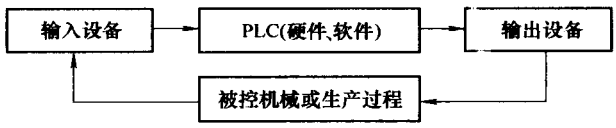

图 1-2 PLC 控制系统

制盘。传统的继电器控制线路的控制作用是通过许多导线与继电器硬件连接实现的，而 PLC 控制系统的控制作用是通过软件编程实现的。后者可以通过修改程序来改变其控制作用，而前者则需要改变控制线路的硬件连接才能做到。

1. PLC 的基本组成

PLC 控制系统的硬件简化框图如图 1-3 所示。其中点划线框部分为 PLC 的基本组成，可以将其分为四部分：中央处理器（CPU）、存储器、输入/输出（I/O）模块和电源。

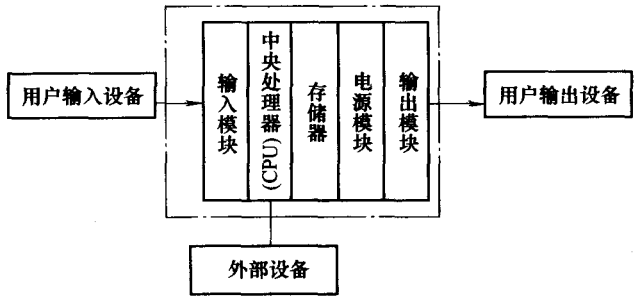

图 1-3 PLC 控制系统结构简化框图

（1）中央处理器（CPU）

CPU 是 PLC 的核心，起神经中枢的作用，每套 PLC 至少有一个 CPU，它按 PLC 的系统程序赋予的功能接收并存储用户程序和数据，用扫描的方式采集由现场输入装置送来的状态或数据，并存入规定的寄存器中，同时诊断电源和 PLC 内部电路的工作状态和编程过程中的语法错误等。进入运行后，从用户程序存储器中逐条读取指令，经分析后再按指令规定的任务产生相应的控制信号，去指挥有关的控制电路。

CPU 由控制器、运算器和寄存器组成，这些电路集成在一个芯片上。内存主要用于存储程序及数据，是 PLC 不可缺少的组成单元。CPU 的控制器控制 CPU 工作，由它读取指令、解释指令及执行指令。运算器用于进行数字或逻辑运算，在控制器指挥下工作。寄存器参与运算，并存储运算的中间结果，它也是在控制器指挥下工作。CPU 通过地址总线、数据总线与 I/O 接口电路相连接。CPU 速度和内存容量是 PLC 的重要参数，它们决定着 PLC 的工作速度，I/O 数量及软件容量等，因此限制着控制规模。

（2）存储器

存储器是具有记忆功能的半导体电路，是 PLC 存放系统程序、用户程序和运行数据的单元。它包括随机存取存储器（RAM）和只读存储器（ROM）。随机存取存储器（RAM）在使用过程中随时可以读取和存储；而只读存储器（ROM）在使用过程中只能读取，不能存储。RAM 有静态 RAM（SRAM）和动态 RAM（DRAM）两种；ROM 按其编程方式不同，可分为掩膜 ROM、可编程 ROM（PROM）、可擦除可编程 ROM（EPROM）和电擦除可编程 ROM（E^2PROM）等。

由于 PLC 的软件由系统软件和用户软件构成，因此 PLC 的存储器可分为系统程序存储器和用户程序存储器。通常将存放应用软件的存储器称为用户程序存储器。不同类型的 PLC 其存储容量各不相同。

（3）输入/输出（I/O）模块

I/O 模块是 CPU 与现场 I/O 设备或其他外部设备通信的桥梁。I/O 模块集成了 PLC 的 I/O电路，其输入暂存器反映输入信号状态，输出点反映输出锁存器状态。输入模块将电信号变换成数字信号进入 PLC 系统，输出模块相反。PLC 提供了具有各种操作电平与输出驱动能力的 I/O 模块和各种用途的功能模块供用户选用。

I/O模块分为开关量输入（DI）、开关量输出（DO）、模拟量输入（AI）、模拟量输出（AO）等模块。常用的I/O分类如下：

对于开关量I/O来说，按电压水平分，有AC 220V、AC 110V、DC 24V等；按隔离方式分，有继电器隔离和晶体管隔离。对于模拟量I/O来说，按信号类型分，有电流型（4～20mA，0～20mA）、电压型（0～10V，0～5V，－10～10V）等；按精度分，有12bit，14bit，16bit等。除了上述通用I/O外，还有特殊I/O模块，如热电阻、热电偶、脉冲等模块。

一般PLC均配置I/O电平转换及电气隔离。输入电平转换是用来将输入端的不同电压或电流信号源转换成微处理器所能接收的低电平信号；输出电平转换是用来将微处理器的低电平控制信号转换为控制设备所需的电压或电流信号；电气隔离是在微处理器与I/O回路之间采用的防干扰措施，常用的电气隔离是由两个发光二极管和光敏晶体管组成的光耦合器。I/O模块既可以与CPU放置在一起，也可远程放置。一般I/O模块具有I/O状态显示和接线端子排。另外，有些PLC还具有一些其他功能的I/O模块，如串/并行变换、数据传送、A/D或D/A转换及其他功能控制等。

（4）电源

PLC配有开关式稳压电源模块，用来给PLC各模块的集成电路提供工作电源。同时，有的还为输入电路提供24V的工作电源。电源输入类型有：交流电源（AC 220V或AC 110V），直流电源（常用的为DC 24V）。

2. PLC的工作原理

PLC虽然同微机有许多相同的地方，但它的工作方式却与微机有很大不同。微机一般采用等待命令的工作方式，如常见的键盘扫描方式或I/O扫描方式。当按下键盘键或I/O动作后，计算机则转入相应的子程序和运行程序，无键按下或无I/O动作则继续扫描。PLC则采用循环扫描的工作方式，整个扫描过程可分为输入采样、内部处理、用户程序执行、输出刷新4个阶段。PLC周而复始地循环执行这4个阶段，这种工作方式称为扫描工作方式。PLC每重复一次这4个阶段所用的时间称为一个扫描周期（或称循环周期、工作周期）。而内部处理阶段实际上就是运行PLC内部系统的管理程序，它由下面4个过程组成：

（1）系统自监测

PLC检查CPU模块内部硬件是否正常，如果超时复位监视计时器（看门狗，watchdog）则停止中央处理器工作，以及完成一些其他检测。

（2）与编程器交换信息

这在使用编程器输入和调试程序时才执行。

（3）与数据处理器交换信息

这只有在PLC中配置有专用数字处理器时才执行。

（4）外部通信

当PLC配置有通信接口或模块时，与外部通信对象（如磁带机、其他PLC或计算机等）进行数据交换。

内部处理阶段是运行PLC内部系统的管理程序，该程序是厂家在PLC出厂时就已经固化好了的，与用户的控制程序无关，一般比较固定，其运行时间与用户程序运行时间相比，要短得多。通常忽略内部处理阶段，而认为PLC的工作过程为3个阶段：输入采样阶段、用户程序执行阶段、输出刷新阶段，并近似地认为每重复一次这3个阶段所用的时间为一个扫描

周期。其工作过程如图 1-4 所示。

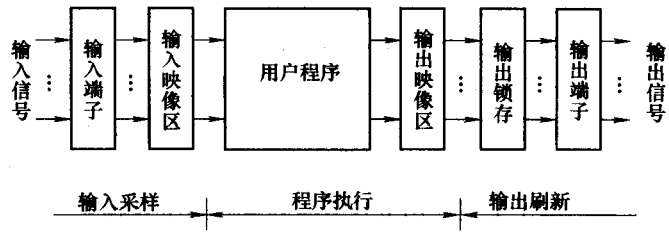

图 1-4　PLC 的工作过程图

（1）输入采样阶段

在输入采样阶段，PLC 以扫描方式依次地读入所有输入状态和数据，并将它们存入 I/O 映像区中的相应单元内，这一过程称为采样。输入采样结束后，转入用户程序执行和输出刷新阶段。在这两个阶段中，即使输入状态和数据发生变化，I/O 映像区中的相应单元的状态和数据也不会改变，而且这个采样结果将在 PLC 执行程序时被使用。如果输入是脉冲信号，则该脉冲信号的宽度必须大于一个扫描周期，才能保证在任何情况下，该输入均能被读入。

（2）程序执行阶段

在用户程序执行阶段，PLC 总是按顺序对程序进行扫描，即从上到下、从左到右地顺序依次地扫描用户程序（梯形图），并分别从输入映像寄存器、内部元件寄存器（内部继电器、定时器、计数器等）和输出映像寄存器中获得所需的数据进行运算、处理，再将程序执行的结果写入寄存执行结果的输出映像寄存器中保存，但这个结果在整个程序未执行完毕之前不会送到输出端口上。这就是说，反映各输出元件状态的输出元件映像存储器中所储存的内容，会随着程序执行的进程而变化，当所有程序全都执行完毕后，输出元件映像存储器的内容就固定下来。

这里要特别注意，当执行控制程序时，如果程序要求某个输出继电器动作，此时这个动作要求并没有直接实时地传送到该继电器，而只是将输出映像存储器中代表该继电器的对应位置置“1”，等待所有程序段都执行完毕后，才将全部程序执行后产生的输出结果（输出映像存储器的内容）一次送到输出锁存器。

（3）输出刷新阶段

在执行完所有用户程序后，PLC 就进入输出刷新阶段。在此期间，CPU 按照 I/O 映像区内对应的状态和数据刷新所有的输出锁存电路，再经输出电路驱动相应的用户设备。这时，才是 PLC 的真正输出。

PLC 重复执行上述三个阶段，每重复一次的时间即为一个扫描周期，用符号 T 表示。PLC 在一个扫描周期中，输入扫描和输出刷新的时间一般为 4 ms 左右，而程序执行时间可因程序的长度不同而不同。PLC 的一个扫描周期一般在 40 ~ 100 ms 之间。

PLC 的扫描工作是重复进行的，因此，其输入和输出存储器不断被刷新（I/O 刷新）。一个扫描周期内输入刷新之前，若外部输入信号状态没有变化，则此次的输入刷新就没有变化，经运算处理后，相应的输出刷新也无变化，输出的控制信号也没有变化，只是重新被刷新一次。若在一个扫描周期内，输入刷新之前，输入的外部输入信号状态发生了变化，则此次输入刷新就有了变化，经运算处理后，其输出刷新也可能有变化，输出的控制信号亦可能有变化。不管输出控制信号有无变化，一个扫描周期内对所有输出只刷新一次，即前一次和后一次输出状态的变化，至少要经历一个扫描周期的时间。

PLC 工作的主要特点是输入信号集中批处理、执行过程集中批处理和输出控制也集中批处理。PLC 的这种“串行”工作方式，可以避免继电器-接触器控制系统中触点竞争和时序失配

的问题，并增强系统的抗干扰能力。由于干扰常常是脉冲式的、短时的，只要 PLC 不是正好工作在输入刷新阶段，就不会受到干扰的影响。因此，瞬间干扰所引起的误动作将会大大减少，从而增加了系统的抗干扰能力。这是 PLC 可靠性高的原因之一。但是这种工作方式又导致输出对输入在时间上的滞后，对于要求快速响应的控制系统，这也是 PLC 的缺点之一。

还需要指出一点，在 PLC 中常采用一种称之为“看门狗”的监视定时器来监视 PLC 的实际工作周期是否超出预定的时间，以避免 PLC 在执行程序过程中进入死循环，或“跑飞”（PLC 执行非预定的程序）而造成系统瘫痪。

1.1.3　PLC 的功能特点和分类

1. PLC 的功能

随着计算机技术、工业控制技术、电子技术和通信技术的发展，PLC 已从小规模的单机顺序控制，发展到包括过程控制、位置控制等场合的所有控制领域，能组成工厂自动化的 PLC 综合控制系统。如今的 PLC 一般都有如下丰富的功能：

（1）信号采集功能

PLC 可采集开关信号、模拟信号及脉冲信号。

（2）开关量逻辑控制功能

这是 PLC 的最基本功能之一。逻辑控制功能实际上就是位处理功能，它用 PLC 的与、或、非指令取代继电器触点串联、并联和其他逻辑连接，实现开关控制、逻辑控制和顺序控制。它既可用于单机控制或多机控制，又可用于自动化生产线的控制。PLC 可根据操作按钮、限位开关及其他现场给出的指令信号或检测信号，控制机械运动部件进行相应的动作。

（3）定时/计数控制功能

定时/计数（TIM/CNT）控制功能是指利用 PLC 提供的定时器、计数器指令实现对某种操作的定时或计数控制，以取代时间继电器和计数继电器。定时器和计数器的设定值可以在编程时设定，也可以在运行过程中根据需要进行修改，使用方便灵活。

（4）数据处理功能

数据处理功能是指 PLC 能进行数据传送、数据比较、数据移位、数制转换、算术运算与逻辑运算以及编码和译码等操作。中、大型 PLC 数据处理功能更加齐全，可完成开方、PID 运算、浮点运算等操作，还可以和 CRT、打印机相连，实现程序、数据的显示和打印。

（5）监控、故障诊断功能

PLC 设置了较强的监控、故障诊断功能。利用编程器或监视器，操作人员可监视 PLC 各部分的运行状态和进程；也可以在线调整和修改控制程序中定时器、计数器的设定值或强制 I/O 的状态。PLC 可以对系统构成、某些硬件状态、指令的合法性等进行自诊断，发现异常情况，发出报警并显示错误类型，如遇严重错误则自动中止运行。PLC 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。

（6）步进控制功能

步进控制功能是用步进指令来实现有多道加工工序的控制，只有前一道工序完成后，才能进行下一道工序操作的控制，以取代由硬件构成的步进控制器。PLC 为用户提供了多个移位寄存器，可以实现由时间、计数或其他指定逻辑信号为转步条件的步进控制。PLC 能通过移位寄存器方便地完成步进控制功能。有些 PLC 专门设有步进控制指令，使得编程更为方

便。此功能在进行顺序控制时非常有效。

（7）A/D、D/A 转换功能

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。一般情况下，模拟量为 4～20mA 的电流，或 1～5V、0～10V 的电压；数字量为 8 位或 12 位的二进制数。通过 A/D、D/A 转换功能可对温度、压力、速度、流量等连续变化的模拟量进行控制，而且编程和使用都很方便。大、中型的 PLC 还具有 PID 闭环控制功能，运用 PID 子程序或使用专用的智能 PID 模块，可以实现对模拟量的闭环过程控制。

（8）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能够长期保存。利用某些记忆指令可以对工作状态进行记忆，以保持 PLC 断电后的数据内容不变。PLC 电源恢复后，可以在原工作状态基础上继续工作。

（9）远程 I/O 功能

远程 I/O 功能是指通过远程 I/O 单元将分散在远距离的各种输入、输出设备与 PLC 主机相连接，进行远程控制，接收输入信号，传出输出信号。

（10）通信联网功能

新一代的 PLC 具有通信功能。PLC 的通信包括 PLC 相互之间、PLC 与上位计算机间的通信及 PLC 与其他智能设备间的通信。PLC 系统与计算机可以直接或通过通信处理单元、通信转接器相连构成网络，从而实现信息的交换，也可构成“集中管理，分散控制”的分布式控制系统，满足工厂自动化系统的发展要求。

（11）扩展功能

扩展功能是指通过连接 I/O 扩展单元模块来增加 I/O 点数，也可通过附加各种智能单元及特殊功能单元来提高 PLC 的控制能力。

PLC 的丰富功能为其广泛应用提供了可能，同时，也为工业系统的自动化、远程化、信息化及智能化创造了条件。

2. PLC 的特点

PLC 能如此迅速发展的原因，除了工业自动化的客观需要外，还有许多独特的优点。它较好地解决了工业控制领域中普遍关心的可靠、安全、灵活、方便、经济等问题。它具有以下主要特点：

（1）可靠性高，抗干扰能力强

高可靠性是 PLC 最突出的特点之一。由于工业生产过程是昼夜连续的，一般的生产装置要几个月、甚至几年才大修一次，这就对用于工业生产过程的控制器提出了高可靠性的要求。PLC 采用微电子技术，大量的开关动作由无触点的半导体电路来完成，用软件代替大量的中间继电器和时间继电器，仅剩下与输入和输出有关的少量硬件，接线可减少到继电器控制系统的 1/10～1/100，因触点接触不良造成的故障大为减少。此外，PLC 还采取了屏蔽、滤波、隔离、故障检测与诊断等抗干扰措施，具有很强的抗干扰能力，平均无故障时间达到数万小时以上，可以直接用于有强烈干扰的工业生产现场。大型的 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，使可靠性更进一步提高。PLC 已被广大用户公认为是最可靠的工业控制设备之一。

（2）编程、操作简易方便、程序修改灵活

PLC 采用面向控制过程、面向问题的“自然语言”编程，容易掌握。目前，PLC 的编程大多采用类似于继电器控制线路的梯形图形式，既继承了传统控制线路的清晰直观感，又易于编程，程序改变时也易于修改。

（3）硬件配套齐全，用户使用方便，适应性强

PLC 产品已经标准化、系列化、模块化，配备有品种齐全的各种硬件装置供用户选用。用户能灵活方便地进行系统配置，组成不同功能、不同规模的系统。PLC 具有丰富的 I/O 接口，针对不同的工业现场信号（交流或直流；电压或电流；开关量或模拟量；脉冲或电位等），有相应的 I/O 模块与工业现场的器件或设备（按钮、行程开关、接近开关、传感器及变送器、电磁线圈、电动机起动器、控制阀等）直接连接。另外，为了提高操作性能，PLC 还有多种人—机对话的接口模块；为了组成工业局部网络，它还有多种通信联网的接口模块。PLC 有较强的带负载能力，可以直接驱动一般的电磁阀和交流接触器。硬件配置确定后，可以通过修改用户程序，方便快速地适应工艺条件的变化。

（4）安装简单，调试和维修方便

PLC 用软件功能取代了继电器控制系统中大量的中间继电器、时间继电器、计数器等器件，使控制柜的设计、安装、接线工作量大大减少。

PLC 可以在实验室模拟调试，输入信号用小开关来模拟，通过 PLC 上的发光二极管可观察输出信号的状态。用户程序不需要专门的机房，可以在各种工业环境下直接运行。使用时只需将现场的各种设备与 PLC 相应的 I/O 端相连接，即可投入运行。完成了系统的安装和接线后，在现场的统调过程中发现的问题一般通过修改程序就可以解决，系统的调试时间比继电器系统要少得多。

PLC 的故障率很低，且由于采用模块化结构，PLC 有完善的自诊断和显示功能，可编程序控制器或外部的输入装置和执行机构发生故障时，可以根据 PLC 上的发光二极管或编程器提供的信息迅速地查明产生故障的原因。因此，一旦某模块发生故障，用户可以通过更换模块的方法，使系统迅速恢复运行。

（5）体积小、质量轻、功耗低、响应快

由于 PLC 是将微电子技术应用于工业控制设备的新型产品，其体积小、质量轻、功耗低、响应快。对于复杂的控制系统，使用 PLC 后，可以减少大量的中间继电器和时间继电器，小型 PLC 的体积仅相当于几个继电器的大小，因此可将开关柜的体积缩小到原来的1/2 ~ 1/10。PLC 的配线比继电器控制系统的配线少得多，故可以省下大量的配线和附件，减少大量的安装接线工时，加上开关柜体积的缩小，可以节省大量的费用。传统继电器节点的响应时间一般需要几百毫秒，而 PLC 的节点反应很快，内部是微秒级的，外部是毫秒级的。

3. PLC 的分类

PLC 种类很多，其功能、内存容量、控制规模、外形等方面均存在较大差异，且还没有一个权威的统一分类标准。通常根据其结构形式的不同、功能的差异和 I/O 点数的多少等进行大致分类如下：

（1）按结构形式分类

根据 PLC 的结构形式，可将 PLC 分为整体式和模块式两类。

整体式 PLC 是将电源、CPU、I/O 接口等部件都集中装在一个机箱内，具有结构紧凑、体积小、价格低的特点。小型 PLC 一般采用这种整体式结构。整体式 PLC 由不同 I/O 点数

的基本单元（又称主机）和扩展单元组成。基本单元内有 CPU、I/O 接口、与 I/O 扩展单元相连的扩展口，以及与编程器或 EPROM 写入器相连的接口等。扩展单元内只有 I/O 和电源等，没有 CPU。基本单元和扩展单元之间一般用扁平电缆连接。整体式 PLC 一般还可配备特殊功能单元，如模拟量单元、位置控制单元等，使其功能得以扩展。

模块式 PLC 是将 PLC 各组成部分，分别做成若干个单独的模块，如 CPU 模块、I/O 模块、电源模块（有的含在 CPU 模块中）以及各种功能模块。模块式 PLC 由框架或基板和各种模块组成。模块装在框架或基板的插座上。这种模块式 PLC 的特点是配置灵活，可根据需要选配不同规模的系统，而且装配方便，便于扩展和维修。大、中型 PLC 一般采用模块式结构。

还有一些 PLC 将整体式和模块式的特点结合起来，构成所谓叠装式 PLC。叠装式 PLC 其 CPU、电源、I/O 接口等也是各自独立的模块，但它们之间是靠电缆进行连接，并且各模块可以一层层地叠装。这样，不但系统可以灵活配置，还可做得体积小巧。

（2）按功能分类

按 PLC 功能强弱来分，可分为低档机、中档机和高档机三类。

低档 PLC 具有逻辑运算、定时、计数、移位以及自诊断、监控等基本功能，还可有少量模拟量 I/O、算术运算、数据传送和比较、通信等功能。主要用于逻辑控制、顺序控制或少量模拟量控制的单机控制系统。

中档 PLC 除具有低档 PLC 的功能外，还具有较强的模拟量 I/O、算术运算、数据传送和比较、数制转换、远程 I/O、子程序、通信联网等功能。有些还可增设中断控制、PID 控制等功能，适用于复杂控制系统。

高档机 PLC 除具有中档机的功能外，可进行函数运算、矩阵运算，完成数据管理工作，有更强的通信能力，还具有模拟调节、联网通信、监视、记录和打印等功能，使 PLC 的功能更多更强，能进行智能控制、远程控制、大规模控制，构成分布式生产过程综合控制管理系统，成为整个工厂的自动化网络。

（3）按 I/O 点数分类

为了适应不同工业生产过程的应用要求，PLC 能够处理的输入/输出信号数是不一样的。一般将一路信号称为一个点。PLC 按控制规模分类主要以开关量计数，模拟量的路数可折算成开关量的点数，一般一路相当于 8 点或 16 点。根据 I/O 点数的多少，可将 PLC 分为微型机、小型机、中型机、大型机、超大型机。

1）微型机

I/O 点数小于 100 点，内存容量为 256B ~ 1KB。微型机特点是体积小，功能简单，是实现小型机械自动化的理想控制器。

2）小型机

I/O 点数在 100 ~ 500 点左右，内存容量为 1 ~ 3.6KB。小型机主要用于中等容量的开关量控制，具有逻辑运算、定时、计数、顺序控制、通信等功能，是代替继电器接触器控制的理想控制器，应用非常广泛。

3）中型机

I/O 点数在 500 ~ 1000 点左右，内存容量为 3.6 ~ 13KB。中型机除具有小型、超小型 PLC 的功能外，还增加了数据处理能力，适用于小规模的综合控制系统。

4）大型机

I/O 点数在 1000 点以上，内存容量在 13KB 以上。大型 PLC 用于大规模过程控制或分布式控制系统。

5）超大型机

I/O 点数可达几千点，甚至几万点，内存容量在 13KB 以上。大型 PLC 的应用已从逻辑控制发展到过程控制、数字控制、集散控制等广阔领域。大型 PLC 使用 32 位微处理器，多 CPU 并行工作，并具有大容量存储器。

PLC 按功能划分及按点数规模划分是有一定联系的。一般来说，大型机、超大型机都是高档机。机型和机器的结构形式及内部存储器的容量一般也有一定的联系，大型机一般都是模块式机，都有很大的内存容量。

1.2　西门子 S7 系列 PLC

德国西门子公司是世界上较早研制和生产 PLC 产品的主要厂家之一，其产品具有各种尺寸以适应各种不同的应用场合，有适合于起重机械或各种气候条件的坚固型；有适用于狭小空间具有高处理性能的密集型；有的运行速度极快且具有优异的扩展能力。它包括从简单的小型控制器到具有过程计算机功能的大型控制器，可以配置各种输入/输出模块、编程器、过程通信和显示部件等。西门子公司的 PLC 发展到现在已有很多系列产品，如 S5、S7、C7、M7 系列等，本书主要以 S7 系列为例讲解 PLC 的理论和应用。

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。

1. S7-200

S7-200 PLC 是超小型化的 PLC，可提供 4 个不同的基本型号与 8 种 CPU 可供选择使用。

S7-200 PLC 结构紧凑、价格低廉，适用于小型的自动化控制系统。其指令处理时间短，减少了循环时间，高速计数器使其可应用于更广泛的领域，高速中断处理能分别响应各种过程事件；对性能的扩展提供了模块化的扩展能力，用于控制步进电动机的脉冲输出同样可用于脉冲宽度的调制，为快速方便地解决最复杂问题提供高效的指令集。此外，附加性能有点对点接口（PPI）支持编程、操作员接口与串行设备接口；用户界面友好的 STEP7 Micro/DOS 软件和高效的编程器简化了编程；三级口令用于保护用户程序；TD200 和 COROS 操作员面板提供简单的人机接口功能。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。

2. S7-300

S7-300 是模块化小型 PLC 系统，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（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