



工业自动化实用技术丛书

GONGYE ZIDONGHUA SHIYONG JISHU CONGSHU

西门子S7-300/400系列

PLC

快速入门与实践

■ 王占富 谢丽萍 岂兴明 主编



人民邮电出版社
POSTS & TELECOM PRESS

工业自动化实用技术

GONGYE ZIDONGHUA SHIYONG JISHU CONGSHU

西门子S7-300/400系列

PLC

-13

快速入门与实践

■ 王占富 谢丽萍 岂兴明 主编

TM571.6

w451

人民邮电出版社

北京

图书在版编目 (CIP) 数据

西门子S7-300/400系列PLC快速入门与实践 / 王占富, 谢丽萍, 岂兴明主编. — 北京: 人民邮电出版社, 2010. 5

(工业自动化实用技术丛书)

ISBN 978-7-115-22208-4

I. ①西… II. ①王… ②谢… ③岂… III. ①可编程
序控制器 IV. ①TM571.6

中国版本图书馆CIP数据核字(2010)第009279号

内 容 提 要

本书主要介绍西门子公司 S7-300/400 系列 PLC 的硬件资源、指令系统等基础知识, 并详细讲解了编程软件的安装和使用方法、PLC 控制系统的设计方法与步骤, 并通过两个综合实例介绍了 S7-300/400 系列 PLC 在控制领域的应用与开发方法。本书采用图、表、文相结合的方法, 使书中的内容通俗易懂又不失专业性。

本书可供工程技术人员自学使用, 还可作为相关专业培训的参考教材。

工业自动化实用技术丛书

西门子 S7-300/400 系列 PLC 快速入门与实践

- ◆ 主 编 王占富 谢丽萍 岂兴明
责任编辑 张 鹏
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
中国铁道出版社印刷厂印刷
- ◆ 开本: 787×1092 1/16
印张: 23.75
字数: 579 千字
印数: 1—4 000 册
- 2010 年 5 月第 1 版
2010 年 5 月北京第 1 次印刷

ISBN 978-7-115-22208-4

定价: 45.00 元

读者服务热线: (010)67129264 印装质量热线: (010)67129223
反盗版热线: (010)67171154

前言

可编程控制器 (PLC) 以微处理器为核心, 将微型计算机技术、自动控制技术及网络通信技术有机地融为一体, 是应用十分广泛的工业自动化控制装置。PLC 应用技术具有控制能力强、可靠性高、配置灵活、编程简单、使用方便、易于扩展等优点, 不仅可以取代继电器控制系统, 还可以进行复杂的生产过程控制以及应用于工厂自动化网络, 它已成为现代工业控制的四大支柱技术 (可编程控制器技术、机器人技术、CAD/CAM 技术和数控技术) 之一。因此, 学习、掌握和应用 PLC 技术已成为工程技术人员的迫切需求。

西门子公司生产的 PLC 可靠性高, 在我国的应用很广泛。西门子的 S7 系列 PLC 是 S5 系列 PLC 的更新换代产品, 包括 S7-200、S7-300 和 S7-400 三大系列, 其中 S7-300 和 S7-400 属于大中型 PLC (如无特殊说明, 书中提到的 S7-300/400 PLC 均指 S7-300/400 系列 PLC)。西门子公司虽然对其产品编写了相应的硬件安装手册、程序编写手册和网络通信手册, 但在介绍的时候对所有类型的 PLC 一视同仁, 没有突出介绍现阶段重点使用的几种类型。并且有的参考手册是英文版的, 这就要求用户具有较高的英语水平, 给 PLC 的普及和学习带来了一定的困难。

本书从 PLC 技术初学者自学的角度出发, 由浅入深地从入门、提高、实践三个方面介绍 S7-300/400 系列 PLC 的基础知识和应用开发方法。书中内容包括 S7-300/400 系列 PLC 硬件及其内部资源、基本指令系统、编程系统使用方法、PLC 的用户程序结构、应用系统设计方法、PLC 的网络与通信技术, 并通过两个大型综合实例详细介绍了 S7-300/400 系列 PLC 在现代工业控制系统中的应用开发方法。本书在编写时力图文字精练, 分析步骤详细、清晰, 且图、文、表相结合, 内容充实、通俗易懂。读者通过本书的学习, 可以全面快速地掌握 S7-300/400 系列 PLC 的应用方法。本书适合广大初中级工控技术人员自学之用, 也可供技术培训及在职人员进修学习使用。书中部分实例程序可从人民邮电出版社网站 (<http://www.ptpress.com.cn>) 查询下载。

本书由王占富、谢丽萍、岂兴明主编, 付亚超、郭正彪、王真真、矫津毅、钟丰灿、朱冬、陈柯、邢朝阳、章巧娟、汪国民、龚明杨、张君、刘增莲、矫志斌、刘佳、张成兰等人参与了资料整理和部分编写工作。

由于我们水平有限且编写时间仓促, 书中如有疏漏之处欢迎广大读者提出宝贵的意见和建议。

编者

目 录

入 门 篇

第 1 章 S7-300/400 系列 PLC 的硬件系统及内部资源	3
1.1 硬件系统基本构成	3
1.1.1 概述	3
1.1.2 S7-300/400 系列 PLC 的组成	4
1.1.3 S7-300/400 系列 PLC 的结构	9
1.2 CPU 模块及性能特点	12
1.2.1 S7-300 系列 PLC 的 CPU 模块	13
1.2.2 S7-400 系列 PLC 的 CPU 模块	17
1.3 输入/输出模块及模块地址的确定	21
1.3.1 S7-300 系列 PLC 的信号模块	21
1.3.2 S7-400 系列 PLC 的信号模块	39
1.3.3 模块诊断与过程中断	42
1.3.4 信号模块地址的确定	43
1.4 S7-300/400 系列 PLC 的内部资源	45
1.4.1 装载存储区	46
1.4.2 工作存储区	46
1.4.3 系统存储区	46
1.4.4 外设 I/O 存储区与累加器	47
1.4.5 状态寄存器	48
1.4.6 系统存储器区域的划分及功能	49
1.5 分布式 I/O	51
本章小结	52
第 2 章 S7-300/400 系列 PLC 的指令系统	53
2.1 编程语言及 PLC 程序结构	53
2.1.1 STEP 7 的编程语言概述	53
2.1.2 PLC 的程序结构概述	56
2.2 指令系统的基本知识	56



2.2.1	数制	56
2.2.2	数据类型	57
2.3	S7-300/400 系列 PLC 的指令系统	66
2.3.1	位逻辑指令	66
2.3.2	比较指令	74
2.3.3	转换指令	76
2.3.4	计数器指令	79
2.3.5	数据块操作指令	81
2.3.6	逻辑控制指令	82
2.3.7	整数运算指令	88
2.3.8	浮点运算指令	89
2.3.9	赋值指令	91
2.3.10	程序控制指令	95
2.3.11	移位和循环指令	101
2.3.12	状态位指令	104
2.3.13	定时器指令	109
2.3.14	字逻辑指令	117
2.3.15	累加器指令	118
	本章小结	122

提 高 篇

第 3 章	STEP 7 编程软件的使用方法及应用系统设计	125
3.1	S7-300/400 系列 PLC 应用系统设计概述	125
3.1.1	PLC 选型	125
3.1.2	PLC 容量估算	126
3.1.3	I/O 模块的选择	127
3.2	STEP 7 编程软件概述	128
3.2.1	STEP 7 编程软件的标准软件包	128
3.2.2	人机接口	132
3.3	STEP 7 编程软件的启动	133
3.4	创建和编辑项目	135
3.4.1	利用 STEP 7 编程软件创建项目的步骤	135
3.4.2	项目结构	136
3.4.3	创建项目	137
3.4.4	编辑项目	139
3.5	硬件组态	141
3.5.1	硬件组态的任务与步骤	141
3.5.2	CPU 的参数设置	144

3.5.3 I/O 模块的参数设置	153
3.6 定义符号	158
3.6.1 共享符号与局域符号	158
3.6.2 符号表	161
3.7 逻辑块的生成	163
3.7.1 建立逻辑软件块	163
3.7.2 编辑变量声明表	165
3.7.3 编辑语句和文字注释时的注意事项	166
3.8 刷新块调用与逻辑块存盘	167
3.9 程序的下载和调试	168
3.9.1 下载程序及模块信息	168
3.9.2 用 S7-PLCSIM 调试程序	170
本章小结	172
第 4 章 S7-300/400 系列 PLC 的用户程序结构	174
4.1 用户程序的基本结构	174
4.1.1 用户程序中的块	174
4.1.2 用户程序使用的堆栈	175
4.1.3 STEP 7 的编程方法	177
4.2 功能块与功能的生成与调用	177
4.2.1 局域变量的类型	178
4.2.2 功能块与功能的调用	179
4.3 数据块	187
4.3.1 数据块中的数据类型	187
4.3.2 数据块的生成与使用	190
4.4 多重背景	192
4.4.1 多重背景功能块	193
4.4.2 多重背景数据块	195
4.5 组织块与中断处理	195
4.5.1 中断的基本概念	195
4.5.2 组织块的变量声明表	197
4.5.3 日期时间中断组织块	197
4.5.4 延时中断组织块	201
4.5.5 循环中断组织块	203
4.5.6 硬件中断组织块	206
4.5.7 背景数据块	209
4.5.8 启动时使用的组织块	210
4.5.9 错误处理组织块	212



本章小结	213
第 5 章 S7-300/400 系列 PLC 的通信与网络	214
5.1 计算机通信方式与串行通信接口	214
5.1.1 计算机的通信方式	214
5.1.2 串行通信接口类型	216
5.2 计算机通信的国际标准	217
5.2.1 开放系统互连模型 (OSI)	217
5.2.2 现场总线及其国际标准	218
5.3 S7-300/400 的通信网络	219
5.3.1 工业自动化网络	219
5.3.2 S7-300/400 的通信网络	220
5.3.3 S7 通信的分类	221
5.4 MPI 网络与全局数据通信	222
5.4.1 MPI 网络	222
5.4.2 MPI 网络的组态	223
5.4.3 全局数据表	225
5.4.4 事件驱动的全局数据通信	228
5.4.5 不用连接组态的 MPI 通信	228
5.5 执行器传感器接口 AS-i 网络	230
5.5.1 AS-i 的网络结构	230
5.5.2 AS-i 的寻址模式	231
5.5.3 AS-i 的主从通信方式	231
5.5.4 AS-i 从站的通信接口	232
5.5.5 AS-i 的工作阶段	232
5.6 工业以太网	234
5.7 PROFIBUS 介绍	235
5.7.1 PROFIBUS 的组成	236
5.7.2 PROFIBUS 介质存取协议	237
5.7.3 PROFIBUS-DP 设备的分类	238
5.7.4 PROFIBUS 的通信协议	239
5.7.5 基于组态的 PROFIBUS 通信	240
5.8 点对点通信	246
5.8.1 点对点通信的硬件与通信协议	246
5.8.2 ASCII Driver 通信协议	246
5.8.3 3964 (R) 通信协议	250
5.8.4 RK512 通信协议	251
本章小结	257

实 践 篇

第 6 章 S7-300/400 系列 PLC 在小功率金卤石英吹泡机控制系统中的应用	261
6.1 系统总统设计	261
6.1.1 系统功能分析	261
6.1.2 系统原理分析	262
6.2 系统的工艺流程图和气路图	263
6.2.1 工艺流程	263
6.2.2 系统控制气路图	264
6.3 系统 PLC 选型和资源配置	264
6.3.1 模块构成图	264
6.3.2 特殊模块功能概述	265
6.3.3 各个模块的具体功能及特性分析	265
6.4 系统程序设计与调试	267
6.4.1 编程语言 STEP 7 的语言特点	267
6.4.2 系统工艺表图	267
6.4.3 系统主程序流程图、规格选择及相关设置	270
6.5 系统 PLC 程序	274
6.5.1 程序的构成	275
6.5.2 系统所用到的符号	275
6.5.3 主程序	281
6.5.4 子程序	301
本章小结	313
第 7 章 S7-300/400 系列 PLC 在啤酒发酵自动控制系统中的应用	314
7.1 系统总体设计	314
7.1.1 系统功能分析	314
7.1.2 控制原理分析	315
7.2 系统工艺流程	315
7.3 系统 PLC 选型和资源配置	316
7.3.1 PLC 选型	316
7.3.2 PLC 的 I/O 资源配置	316
7.3.3 PLC 其他资源配置	317
7.3.4 PLC 硬件资源设计	317
7.4 系统 PLC 程序设计	318
7.4.1 程序流程图设计	318
7.4.2 PLC 功能模块程序设计	318

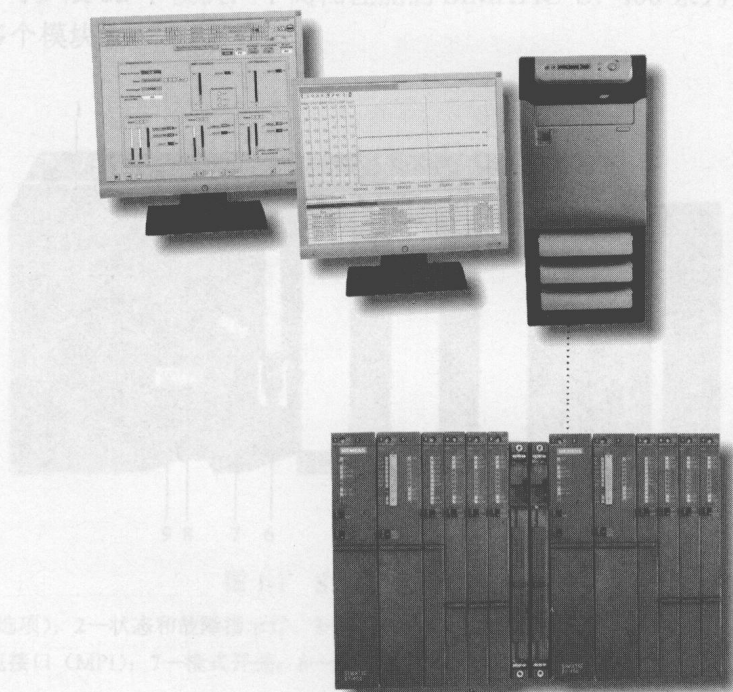


7.5 系统程序模块	319
7.5.1 I/O 采样及输出程序	322
7.5.2 发酵罐的温度信号转换程序	329
7.5.3 发酵温度控制程序	330
7.5.4 发酵罐单罐计时程序	341
7.5.5 分计时控制程序	344
7.5.6 流量累积子程序	347
7.5.7 单罐储酒控制程序	349
7.5.8 出酒控制程序	350
本章小结	353
附录	354
附录 A S7-300/400 系列 PLC 的指令一览表	354
附录 B 组织块、系统功能与系统功能块一览表	359
附录 C 常用缩写词	366
参考文献	370

第1章 S7-300/400 系列 PLC 的硬件系统及内部资源

第2章 S7-300/400 系列 PLC 的指令系统

SIMATIC S7 系列 PLC 是德国西门子公司于 1995 年陆续推出的性能价格比较高的 PLC 系列产品。SIMATIC S7 系列包括：微型 SIMATIC S7-200 系列，最小配置为 8DI/6DO，可扩展 2~7 个模块，最大 I/O 点数为 64DI/64DO、12AI/4AO；中小型 SIMATIC S7-300 系列，如图 1-1 所示，最多可扩展 32 个模块；中高档性能的 SIMATIC S7-400 系列，如图 1-2 所示，最多可扩展 300 多个模块。



S7-300/400 系列 PLC 均采用模块式结构，由机架和模块组成。品种繁多的 I/O 模块、计数模块和功能模块能满足各种领域的自动控制任务。用户可以根据需要的具体情况选择合适的模块，维修时更换模块也很方便。当系统规模扩大和更为复杂时，可以更换机架，对 PLC

第 1 章 S7-300/400 系列 PLC 的 硬件系统及内部资源

本章主要介绍西门子公司的 S7-300/400 系列 PLC 的特性、硬件系统及内部资源。

1.1 硬件系统基本构成

1.1.1 概述

SIMATIC S7 系列 PLC 是德国西门子公司于 1995 年陆续推出的性能价格比较高的 PLC 系列产品。SIMATIC S7 系列包括：微型 SIMATIC S7-200 系列，最小配置为 8DI/6DO，可扩展 2~7 个模块，最大 I/O 点数为 64DI/64DO、12AI/4AO；中小型 SIMATIC S7-300 系列，如图 1-1 所示，最多可扩展 32 个模块；中高档性能的 SIMATIC S7-400 系列，如图 1-2 所示，最多可扩展 300 多个模块。

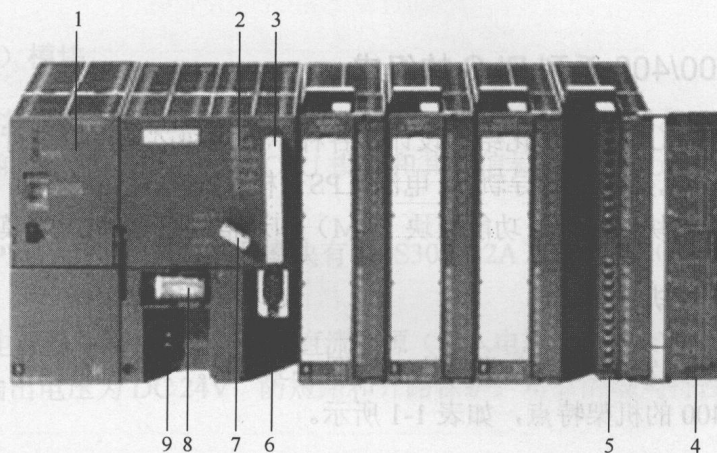


图 1-1 S7-300 系列 PLC

1—电源模块（选项）；2—状态和故障指示灯；3—存储器卡（CPU313 以上）；4—前门；5—前连接器；
6—多点接口（MPI）；7—模式开关；8—后备电池（CPU313 以上）；9—DC 24V 连接器

S7-300/400 系列 PLC 均采用模块式结构，由机架和模块组成。品种繁多的 CPU 模块、信号模块和功能模块能满足各种领域的自动控制任务，用户可以根据系统的具体情况选择合适的模块，维修时更换模块也很方便。当系统规模扩大和更为复杂时，可以增加模块，对 PLC

进行扩展。简单实用的分布式结构和强大的通信连网能力，使其应用十分灵活。近年来，它被广泛应用于机床、纺织机械、包装机械、通用机械、控制系统、普通机床、楼宇自动化、电器制造工业及相关产业等诸多领域。

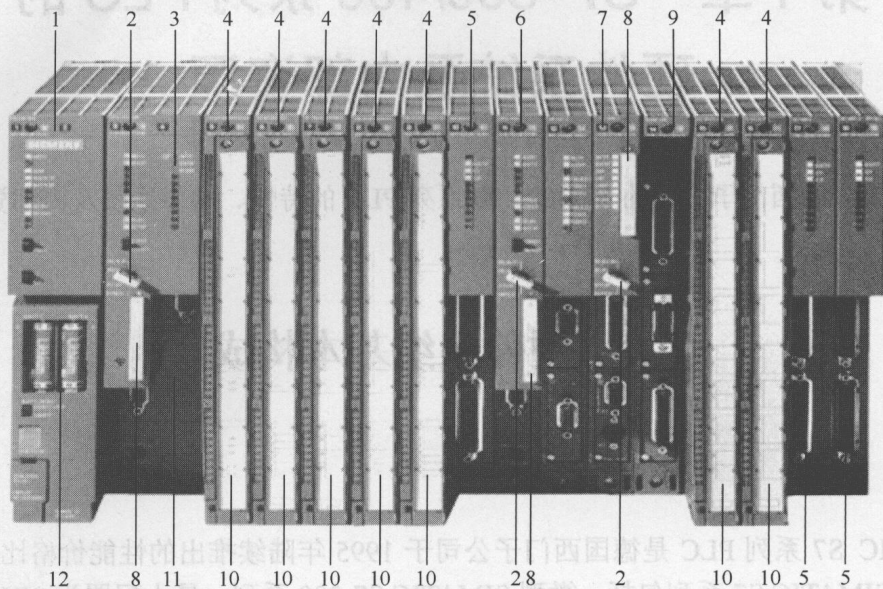


图 1-2 S7-400 系列 PLC (CR2 机架)

- 1—电源模块；2—状态开关（钥匙操作）；3—状态和故障 LED；4—I/O 模块；5—接口模块（IM）；
6—CPU2；7—FM 456-4（M7）应用模块；8—存储卡；9—M7 扩展模块；
10—带标签的前连接器；11—CPU1；12—后备电池

1.1.2 S7-300/400 系列 PLC 的组成

S7-300/400 系列 PLC 是模块化结构设计，各种单独模块之间可以进行广泛组合和扩展。它的主要组成部分有机架（或者导轨）、电源（PS）模块、中央处理单元（CPU）模块、接口模块（IM）、信号模块（SM）、功能模块（FM）和通信处理器（CP）模块。

1. 机架（或者导轨）

机架用来安装和固定 PLC 的各类模块，如图 1-3 所示。

S7-300 和 S7-400 的机架特点，如表 1-1 所示。

表 1-1

S7-300 和 S7-400 的机架

PLC 名称	导轨介绍
S7-300	S7-300 的机架是特质不锈钢或者铝制型板（称为导轨），它的长度有 160mm、482mm、530mm、830mm、2000mm 共 5 种，可根据实际需要选择。电源模块、CPU 及其信号模块都可方便地安装在机架上。除 CPU 模块外，每块信号都带有总线连接器，安装时先将总线连接器装在 CPU 模块上，并固定在机架上，然后依次将各模块装入，通过背板总线将各模块从物理上和电气上连接起来即可

续表

PLC 名称	导轨介绍
S7-400	S7-400 的机架为各类模块提供支架和电源, 并通过背板总线连接各模块。采用分布式总线 (P 总线和 C 总线), 使 CPU 与中央 I/O 间的通信速度非常快, P 总线 (I/O 总线) 用于 I/O 信号的高速交换和对信号模块数据的高速访问; C 总线 (通信总线, 也称为 K 总线) 用于在 C 总线各站之间的高速数据交换, C 和 K 分别是英语单词 Communication 和德语单词 Konununikation (通信) 的缩写。两种总线分开后, 控制和通信分别有各自的数据通道

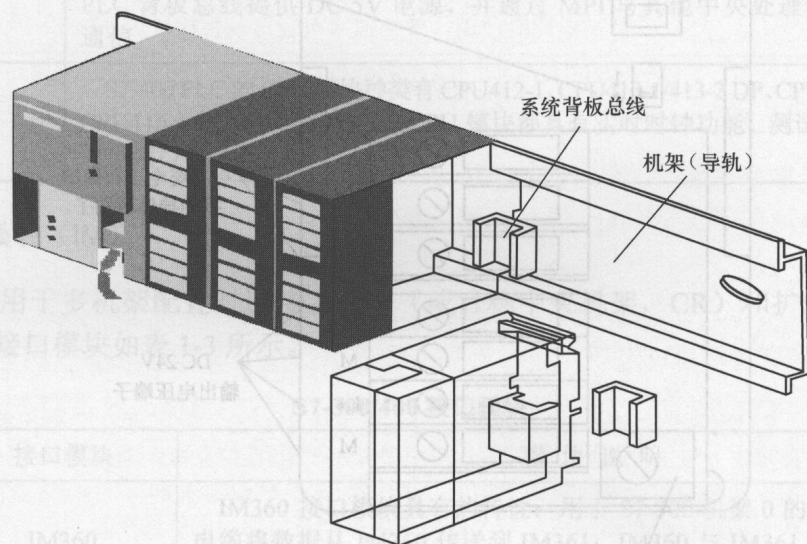


图 1-3 PLC 机架示意图

2. 电源 (PS) 模块

电源模块用于将 AC 120/230V 电源或者 DC 24V 转换为 DC 24V 和 5V 电源, 供 CPU、I/O 模块、传感器和执行器使用。它与 CPU 模块和其他信号模块之间通过电缆连接, 而不是通过背板总线连接。

S7-300 系列 PLC 可供选择的电源模块有: PS305 (2A)、PS307 (2A)、PS307 (5A) 和 PS307 (10A) 等。

PS305 (2A) 电源模块的特点为: 连接直流电源 (输入电压为 DC 24V/48V/72V/96V/110V); 输出电流为 2A, 输出电压为 DC 24V; 防短路和开路保护; 可靠的隔离特性, 符合 EN 60950; 可用作负载电源。

PS307 系列电源模块是西门子公司为 S7-300 PLC 专配的 DC 24V 电源, 可安装在 S7-300 PLC 的专用导轨上, 其额定输出电流有 2A、5A 和 10A 等多种。PS307 系列电源模块除输出额定电流不同, 它们的工作原理和各种参数都基本相同。

图 1-4 所示为 PS307 电源模块的布置图, 图 1-5 所示为 PS307 电源模块的基本电路原理图。

PS307 系列电源模块的特点为: 连接单相交流系统 (输入电压为 AC 120V/230V, 50/60Hz); 输出电流为 2A/5A/10A, 输出电压为 DC 24V; 防短路和开路保护; 可靠的隔离特性, 符合



EN 60950；可用作负载电源。

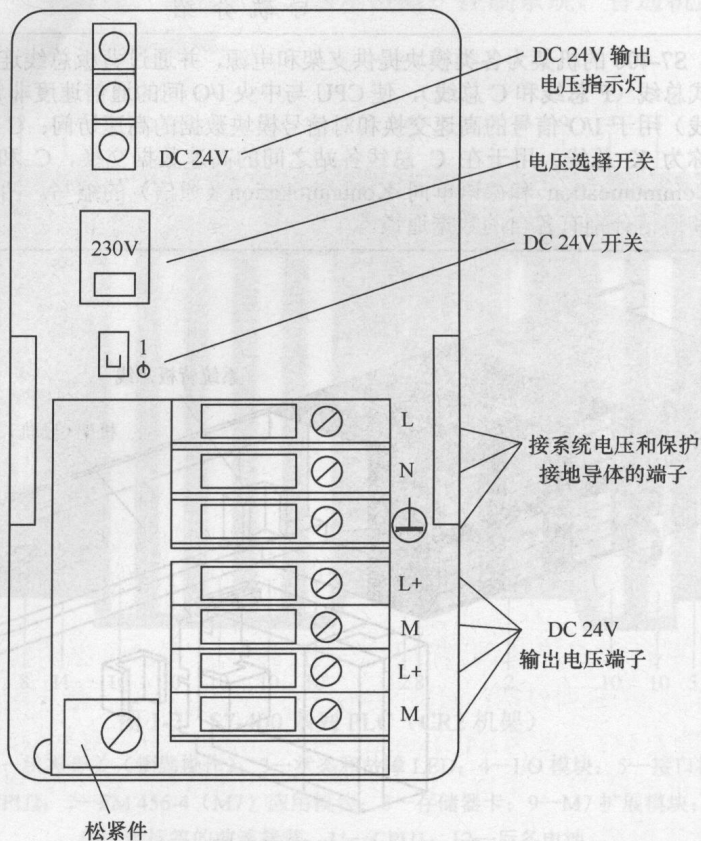


图 1-4 PS307 电源模块的布置示意图

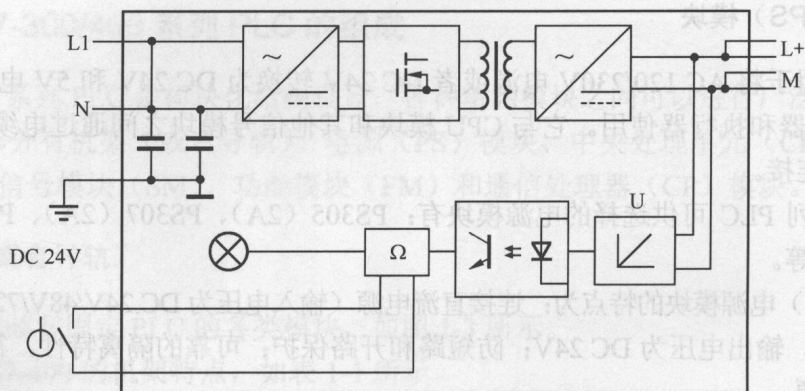


图 1-5 PS307 电源模块的基本电路

PS307 系列电源模块的输入和输出有可靠的隔离，输出正常电压为 24V 时，绿色 LED 亮；输出过载时，LED 闪烁；输出过电流时，以 PS307 (10A) 为例，输出电流大于 13A 时，电压跌落，跌落后自动恢复；输出短路时，输出电压消失，短路故障排除后，电压自动恢复。

3. 中央处理单元 (CPU) 模块

SIMATIC S7-300/400 系列 PLC 提供了多种不同性能的 CPU 模块，以满足用户不同的要

求,如表 1-2 所示。各种 CPU 有不同的性能,例如有的 CPU 模块集成有数字量和模拟量输入/输出点,有的 CPU 集成有 PROFIBUS-DP 等通信接口。CPU 模块前面板上有状态故障指示灯、模式开关、24V 电源端子、电池盒与存储器模块盒(有的 CPU 没有)等。

表 1-2 S7-300/400 中央处理单元

PLC 类别	中央处理单元介绍
S7-300	S7-300 PLC 的 CPU 模块种类有 CPU312 IFM、CPU313、CPU314、CPU315、CPU315-2DP 等。CPU 模块除完成执行用户程序的主要任务外,还为 S7-300 PLC 背板总线提供 DC 5V 电源,并通过 MPI 与其他中央处理器或者编程装置通信
S7-400	S7-400 PLC 的 CPU 模块种类有 CPU412-1、CPU413-1/413-2 DP、CPU414-1/414-2 DP、CPU416-1 等。S7-400 PLC 的 CPU 模块都具有实时时钟功能、测试功能、内置两个通信接口等特点

4. 接口模块 (IM)

接口模块用于多机架配置时连接主机架(或者称中央机架,CR)和扩展机架(ER),S7-300/400 的接口模块如表 1-3 所示。

表 1-3 S7-300/400 接口模块

PLC 类别	接口模块	模块说明
S7-300	IM360	IM360 接口模块具有的特性:用于 S7-300 机架 0 的接口;通过连接电缆将数据从 IM360 传送到 IM361;IM360 与 IM361 之间的最大距离为 10m
	IM361	IM361 接口模块具有的特性:DC 24V 电源;用作 S7-300 机架 1 到机架 3 的接口;通过 S7-300 背板总线的最大电流输出为 0.8A;通过连接电缆将数据从 IM360 传送到 IM361 或者从 IM361 传送到 IM361;IM360 和 IM361 之间的最大距离为 10m;IM361 和 IM361 之间的最大距离为 10m
	IM365	IM365 接口模块具有的特性:为机架 0 和机架 1 预先组合好的配对模块;总电流为 1.2A,其中每个机架最大能使用 0.8A;已固定连接好一个长 1m 的连接电缆;机架 1 中只能安装信号模块
S7-400	IM460/461-0	用于不带 PS 发送器的局域连接,带通信总线,其中 IM460-0 为发送 IM,IM461-0 为接收 IM
	IM460/461-1	用于带 PS 发送器的局域连接,不带通信总线,其中 IM460-1 为发送 IM,IM461-1 为接收 IM
	IM460/461-3	IM460/461-3 接口模块,用于最大 102m 的远程连接,带通信总线,其中 IM460-3 为发送 IM,IM461-3 为接收 IM
	IM460/461-4	用于最长 605m 的远程连接,不带通信总线,其中 IM460-4 为发送 IM,IM461-4 为接收 IM
	IM463-2	用于 S5 扩展单元与 S7-400 的分布式连接。在 S7-400 系列 PLC 的中央机架(CR)中使用 IM463-2,在 S5 扩展单元中使用 IM314。可以连接到 S7-400 的 S5 扩展单元为 EU183U、EU185U、EU186U、ER701-2、ER701-3,并可以使用适合于这些 EU 与 ER 的各种数字量和模拟量 I/O 模块