

SIEMENS



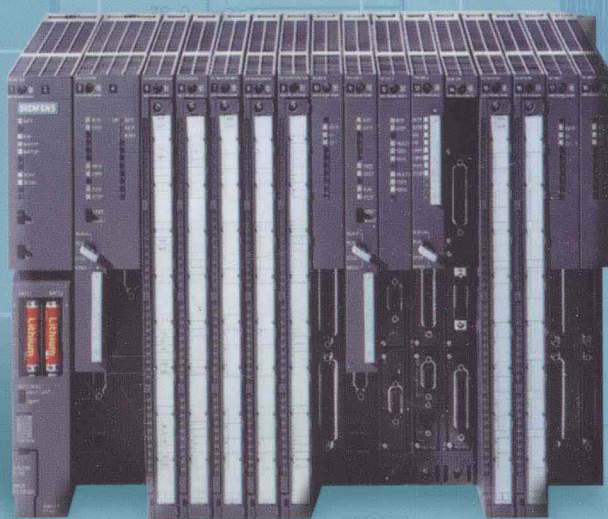
西门子工业自动化系列教材

S7-300/400 PLC

应用教程

廖常初 主编

第2版



内含：
可用于 Windows 7 的 STEP 7 V5.5 中文版 + PLCSIM
V5.4 SP5 中文版 + Graph V5.3 SP6
视频教程 + 用户手册 + 配套例程



机械工业出版社
CHINA MACHINE PRESS



西门子工业自动化系列教材

S7 – 300/400 PLC 应用教程

第2版

廖常初 主编

机械工业出版社

本书介绍了西门子 S7-300/400 的硬件结构和硬件组态、指令系统、程序结构、编程软件和仿真软件的使用方法；一整套易学、易用的开关量控制系统的编程方法；西门子的各种通信网络、通信服务的组态和编程的方法，以及网络控制系统的故障诊断方法，并针对学习中的难点提供了大量的例程。读者还可以用本书中的例程和仿真软件来学习 PID 参数的整定方法。

随书光盘提供了可用于 Windows 7 的 STEP 7 中文版、中文仿真软件 PLCSIM 和编程语言 S7-Graph 的试用版、大量的最新中文用户手册、与正文配套的 30 多个例程和多媒体视频教程。读者可以用仿真软件在计算机上模拟运行和监控 PLC 的用户程序。

本书可作为大专院校电类和机电一体化等专业的教材，也可作为工程技术人员参考用书。

图书在版编目 (CIP) 数据

S7-300/400 PLC 应用教程/廖常初主编. —2 版. —北京:
机械工业出版社, 2011.12
西门子工业自动化系列教材
ISBN 978-7-111-36917-2

I. ①S… II. ①廖… III. ①plc 技术-教材 IV. ①TM571.6

中国版本图书馆 CIP 数据核字 (2011) 第 273708 号

机械工业出版社 (北京市百万庄大街 22 号 邮政编码 100037)

责任编辑: 时 静

责任印制: 杨 曦

保定市中华美凯印刷有限公司印刷

2012 年 2 月第 2 版·第 1 次印刷

184mm×260mm·20 印张·490 千字

0001—4000 册

标准书号: ISBN 978-7-111-36917-2

ISBN 978-7-89433-272-1 (光盘)

定价: 49.80 元 (含 1DVD)

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

电话服务

网络服务

社服务中心: (010) 88361066

门户网: <http://www.cmpbook.com>

销 售 一 部: (010) 68326294

教材网: <http://www.cmpedu.com>

销 售 二 部: (010) 88379649

读者购书热线: (010) 88379203

封面无防伪标均为盗版

前 言

本书对 S7-300/400 PLC 的硬件结构与硬件组态、编程语言、指令、程序结构、通信网络、PID 闭环控制、编程软件与仿真软件的使用等做了全面深入的介绍。本书还介绍了设计数字量控制梯形图的一整套先进完整的编程方法, 以及使用顺序功能图语言 S7-Graph 的程序设计方法。这些方法易学易用, 可以节约大量的设计时间。

本书吸收了作者主编的《西门子工业通信网络组态编程与故障诊断》的部分内容, 全面改写了通信部分, 增加了网络故障和模块故障的简单实用的诊断方法。本书还全面改写了中断组织块应用程序, 对全书的内容作了优化处理, 对学习中的难点增加了例程。读者可以通过随书光盘中的例程和仿真来学习 PID 参数的整定方法, 实验结果用曲线显示, 形象直观。

为了方便教学, 各章配有习题, 有 20 多个实验的指导书。使用 PLCSIM 仿真软件, 只用计算机就可以做实验指导书中的绝大多数实验。

经西门子公司授权, 随书光盘提供了 STEP 7 V5.5 中文版、仿真软件 PLCSIM V5.4 + SP5 的中文版和编程语言 S7-Graph V5.3 + SP6 (均为试用版)、大量的最新中文用户手册、与正文配套的 30 多个例程和多媒体视频教程。上述软件可以用于 Windows 7。

本书可作为大专院校电类和机电一体化等专业的教材, 本书对应的工程应用科技书为《S7-300/400 PLC 应用技术》, 其内容更为丰富, 建议工程技术人员选用。该书在科技金书网的年销售排行榜中居前 20 名和 PLC 类图书排行居第一名, 在华储网上电脑书店自动化类图书销售排行榜中居第一名。

作者主编的《跟我动手学 S7-300/400 PLC》适合于初学者, 该书有 40 多个实训, 读者一边看书, 一边根据实训的要求在计算机上做仿真实验, 就能较快地掌握 S7-300/400 PLC 的使用方法。

本书由廖常初主编, 陈晓东、王云杰、李远树、陈曾汉、范占华、关朝旺、余秋霞、廖亮、文家学、孙明渝、郑群英、万莉、唐世友、左源洁、孙剑等参加了编写工作。

因作者水平有限, 书中难免有错漏之处, 恳请读者批评指正。

作者 E-mail 地址为 liaosun@cqu.edu.cn。从中华工控网的博客首页可以进入作者的博客, 欢迎读者访问。

重庆大学 廖常初

目 录

前言

第1章 概述 1

1.1 PLC 的基本概念 1

1.1.1 模块式 PLC 的基本结构 1

1.1.2 PLC 的特点 3

1.1.3 PLC 的应用领域 4

1.1.4 怎样下载西门子 PLC 的 资料 and 软件 4

1.2 PLC 的工作原理 5

1.2.1 逻辑运算 5

1.2.2 PLC 的循环处理过程 6

1.2.3 PLC 的工作原理 7

第2章 S7-300/400 的 硬件与组态 10

2.1 SIMATIC 自动控制系统简介 10

2.1.1 SIMATIC 自动化控制 系统的组成 10

2.1.2 全集成自动化 11

2.2 S7-300 系列 PLC 简介 12

2.2.1 S7-300 的物理结构 12

2.2.2 CPU 模块的元件 14

2.2.3 CPU 的存储器 16

2.2.4 CPU 模块的分类 18

2.3 S7-400 系列 PLC 简介 18

2.3.1 S7-400 的基本结构与特点 18

2.3.2 CPU 模块与电源模块 20

2.3.3 S7-400 的特殊应用 22

2.4 编程软件 STEP 7 的安装 与使用入门 23

2.4.1 STEP 7 的版本与许可证密钥 23

2.4.2 安装 STEP 7 与 PLCSIM 24

2.4.3 项目的创建 26

2.4.4 STEP 7 与 PLC 通信 连接的组态 29

2.5 硬件组态 31

2.5.1 硬件组态概述 31

2.5.2 S7-300 的组态 32

2.5.3 I/O 模块的地址分配 33

2.5.4 CPU 模块的参数设置 35

2.6 信号模块与功能模块 36

2.6.1 数字量输入模块 37

2.6.2 数字量输出模块 38

2.6.3 模拟量输入模块 40

2.6.4 根据模拟量输入模块的输出值 计算对应的物理量 43

2.6.5 其他信号模块 44

2.6.6 功能模块 46

2.7 习题 47

第3章 S7-300/400 编程基础与 STEP 7 的使用方法 48

3.1 程序的生成与仿真实验 48

3.1.1 STEP 7 的编程语言 48

3.1.2 生成用户程序 50

3.1.3 用仿真软件调试程序 54

3.2 S7-300/400 CPU 的存储区 57

3.2.1 数制 57

3.2.2 基本数据类型 59

3.2.3 系统存储器 62

3.2.4 CPU 中的寄存器 64

3.3 STEP 7 在编程与调试中的应用 67

3.3.1 符号表 67

3.3.2 程序编辑器 68

3.3.3 用变量表监控程序 状态监控 69

3.3.4 数据传送指令与程序 在线操作 71

3.3.5 73

3.4 位逻辑指令 75

3.5 定时器与计数器指令 81

3.5.1 定时器指令	81	4.5 多重背景	134
3.5.2 计数器指令	88	4.6 组织块与中断处理	136
3.6 逻辑控制指令与间接寻址	91	4.6.1 中断的基本概念	136
3.6.1 逻辑控制指令	91	4.6.2 启动组织块与循环 中断组织块	138
3.6.2 寻址方式与间接寻址	93	4.6.3 时间中断组织块	140
3.6.3 循环指令	96	4.6.4 硬件中断组织块	142
3.7 数据处理指令	97	4.6.5 延时中断组织块	145
3.7.1 比较指令	97	4.6.6 异步错误组织块	147
3.7.2 数据转换指令	98	4.6.7 其他组织块	148
3.7.3 移位与循环移位指令	101	4.7 显示参考数据	148
3.8 数学运算指令	103	4.8 习题	150
3.8.1 整数数学运算指令	103		
3.8.2 浮点数数学运算指令	104	第5章 数字量控制系统梯形图	
3.8.3 字逻辑运算指令	106	设计方法	152
3.9 其他指令	107	5.1 梯形图的经验设计法与继电器 电路转换法	152
3.9.1 主控继电器指令与 数据块指令	107	5.1.1 梯形图的经验设计法	152
3.9.2 累加器指令	108	5.1.2 根据继电器电路图 设计梯形图	154
3.10 习题	109	5.2 顺序控制设计法与顺序功能图	158
第4章 S7-300/400 的用户		5.2.1 顺序控制设计法	158
程序结构	111	5.2.2 步与动作	158
4.1 用户程序的基本结构	111	5.2.3 有向连线与转换	160
4.1.1 用户程序中的块	111	5.2.4 顺序功能图的基本结构	161
4.1.2 用户程序使用的堆栈	113	5.2.5 顺序功能图中转换实现的 基本规则	163
4.2 共享数据块与复杂数据类型	114	5.3 使用置位复位指令的顺序控制梯形图 编程方法	165
4.2.1 共享数据块与数据类型	114	5.3.1 设计顺序控制梯形图的一些 基本问题	165
4.2.2 复杂数据类型的生成与应用	116	5.3.2 单序列的编程方法	166
4.3 功能块和功能的生成与调用	118	5.3.3 选择序列与并行序列的 编程方法	168
4.3.1 功能块	119	5.3.4 应用举例	169
4.3.2 功能	121	5.4 具有多种工作方式的系统的顺序控制 编程方法	172
4.3.3 块调用指令与块结束指令	122	5.4.1 系统的硬件结构与工作方式	172
4.3.4 功能与功能块的调用	124	5.4.2 公用程序与手动程序	174
4.3.5 复杂数据类型作块的 输入参数	125	5.4.3 自动程序	175
4.4 寄存器间接寻址与参数类型	126	5.5 顺序功能图语言 S7-Graph	
4.4.1 寄存器间接寻址	126		
4.4.2 参数类型 Pointer 的应用	129		
4.4.3 参数类型 ANY 的应用	130		
4.4.4 时间标记冲突与一致性检查	133		

的应用	179	6.7.2 变频器 DP 通信的数据 区结构	224
5.5.1 S7 - Graph 语言概述	179	6.7.3 S7 - 300 与变频器的 DP 通信实验	225
5.5.2 使用 S7 - Graph 编程的例子 ...	181	6.8 DP 网络其他通信方式的 组态与编程	226
5.5.3 顺序器的运行模式与 监控操作	186	6.8.1 S7 通信的组态与编程	226
5.5.4 顺序器中的动作与转换	188	6.8.2 PROFIBUS - DP 通信的 其他应用	231
5.5.5 用 S7 - Graph 编写具有多种工作方式的 控制程序	190	6.9 使用 STEP 7 和中断组织块 诊断故障	232
5.6 习题	193	6.9.1 与 DP 通信有关的中断 组织块	232
第 6 章 PROFIBUS 网络的组态编程与 故障诊断	196	6.9.2 DP 从站的故障诊断	233
6.1 串行通信接口	196	6.9.3 DP 从站中信号模块的 故障诊断	238
6.1.1 串行通信基础知识	196	6.10 故障诊断的其他问题	243
6.1.2 串行通信接口标准	197	6.10.1 用模块上的 LED 诊断故障 ...	243
6.2 计算机通信的国际标准	198	6.10.2 故障诊断自动化简介	244
6.2.1 开放系统互连模型	198	6.10.3 编程错误的诊断	244
6.2.2 IEEE 802 通信标准	199	6.10.4 项目的上载	246
6.2.3 现场总线及其国际标准	200	6.11 习题	247
6.3 SIMATIC 通信网络与通信服务	202	第 7 章 其他网络通信	249
6.4 PROFIBUS 网络与通信服务	204	7.1 工业以太网与 PROFINET	249
6.4.1 PROFIBUS 的物理层	204	7.1.1 工业以太网概述	249
6.4.2 PROFIBUS 的通信服务与 协议结构	206	7.1.2 以太网的地址	250
6.4.3 PROFIBUS - DP 的功能	208	7.1.3 工业以太网的通信服务	250
6.4.4 PROFIBUS - DP 设备	209	7.1.4 用普通网卡实现计算机与 S7 - 300 的通信	252
6.5 主站与标准 DP 从站通信的组态	212	7.1.5 TCP 连接通信的组态与编程 ...	254
6.5.1 组态 PROFIBUS - DP 网络	212	7.1.6 基于工业以太网的 PROFINET	257
6.5.2 主站与 ET 200 通信的组态	214	7.2 MPI 网络通信	259
6.5.3 安装 GSD 文件	215	7.2.1 全局数据通信的组态	259
6.6 DP 主站与智能从站通信的 组态与编程	216	7.2.2 S7 基本通信与 S7 通信	263
6.6.1 DP 主站与智能从站主从 通信的组态	216	7.3 其他网络与通信服务	267
6.6.2 设计验证通信的程序	219	7.3.1 AS - i 网络	267
6.6.3 用 SFC 14 和 SFC 15 传输 一致性数据	221	7.3.2 点对点通信	269
6.7 PLC 与变频器 DP 通信的 组态与编程	222	7.3.3 工业无线局域网	269
6.7.1 S7 - 300 与变频器 DP 通信 的组态	222	7.3.4 KNX/EIB	270

7.3.5 广域网	271	A.6 功能与功能块的应用实验	295
7.4 习题	271	A.7 寄存器间接寻址的应用实验	296
第8章 S7-300/400 在模拟量闭环		A.8 循环中断实验	296
控制中的应用	273	A.9 时间中断实验	296
8.1 模拟量闭环控制与 PID 控制器	273	A.10 硬件中断实验	297
8.1.1 模拟量闭环控制系统	273	A.11 延时中断实验	297
8.1.2 PID 控制器	275	A.12 顺序控制程序的编程实验	297
8.2 连续 PID 控制器 FB 41	280	A.13 具有多种工作方式的顺序控制程序	
8.2.1 设定值与过程变量的处理	280	编程实验	298
8.2.2 PID 控制算法	281	A.14 顺序功能图语言 S7-Graph 的	
8.2.3 控制器输出值的处理	282	编程实验	299
8.3 PID 控制器的示例程序	282	A.15 具有多种工作方式的 S7-Graph 的	
8.3.1 系统简介	282	编程实验	299
8.3.2 程序设计	283	A.16 DP 网络主从通信的组态与	
8.4 PID 控制器的参数整定方法	288	编程实验	299
8.4.1 PID 控制器的参数整定方法 ...	288	A.17 S7 单向通信的组态编程与	
8.4.2 PID 控制器参数整定的		仿真实验	300
仿真实验	289	A.18 DP 从站故障诊断实验	300
8.5 习题	292	A.19 DP 从站中模块的故障	
附录	293	诊断试验	300
附录 A 实验指导书	293	A.20 编程错误的中断实验	301
A.1 STEP 7 编程软件与仿真软件		A.21 MPI 全局数据通信的	
应用实验	293	组态实验	301
A.2 硬件组态实验	293	A.22 PID 控制器参数整定的	
A.3 定时器计数器应用实验	294	仿真实验	302
A.4 指令应用实验	294	附录 B S7-300/400 的指令一览表	302
A.5 存储器间接寻址的应用实验	295	附录 C 随书光盘简要说明	306
		参考文献	309

第1章 概 述

1.1 PLC 的基本概念

随着微处理器、计算机和数字通信技术的飞速发展，计算机控制已经广泛地应用在几乎所有的工业领域。现代社会要求制造业对市场需求做出迅速的反应，生产出小批量、多品种、多规格、低成本和高质量的产品。为了满足这一要求，生产设备和自动生产线的控制系统必须具有极高的可靠性和灵活性。可编程序控制器正是顺应这一要求出现的，它是以微处理器为基础的通用工业控制装置。

可编程序控制器（Programmable Logic Controller, PLC）的应用面广、功能强大、使用方便，已经成为当代工业自动化的主要支柱之一。国际电工委员会（IEC）对 PLC 作了如下定义：“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，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，控制各种类型的机械或生产过程。可编程序控制器及其有关设备，都应按易于使工业控制系统形成一个整体，易于扩充其功能的原则设计。”

PLC 已经广泛地应用在各种机械设备和生产过程的自动控制系统中，并在其他领域，例如在民用和家庭自动化中的应用也得到了迅速的发展。

1.1.1 模块式 PLC 的基本结构

本书以西门子公司的 S7 - 300/400 系列大中型 PLC 为主要讲授对象。西门子的 PLC 以其极高的性能价格比，在国际国内市场占有很大的份额，在我国的各行各业得到了广泛的应用。S7 - 300/400 属于模块式 PLC，主要由机架、CPU 模块、信号模块、功能模块、接口模块、通信处理器、电源模块和编程计算机组成（见图 1-1），各种模块安装在机架上。通过 CPU 模块或通信模块上的通信接口，PLC 被连接到通信网络，可以与计算机、其他 PLC 或其他设备通信。

1. CPU 模块

CPU 模块主要由微处理器（CPU 芯片）和存储器组成。在 PLC 控制系统中，CPU 模块相当于人的大脑和心脏，它不断地采集输入信号，执行用户程序，刷新系统的输出；存储器用来储存程序和数据。S7 - 300/400 将 CPU 模块简称为 CPU。

2. 信号模块

输入（Input）模块和输出（Output）模块简称为 I/O 模块，开关量输入、开关量输出模块简称为 DI 模块和 DO 模块，模拟量输入、模拟量输出模块简称为 AI 模块和 AO 模块，它们统称为信号模块。信号模块是系统的眼、耳、手、脚，是联系外部现场设备和 CPU 模块的桥梁。

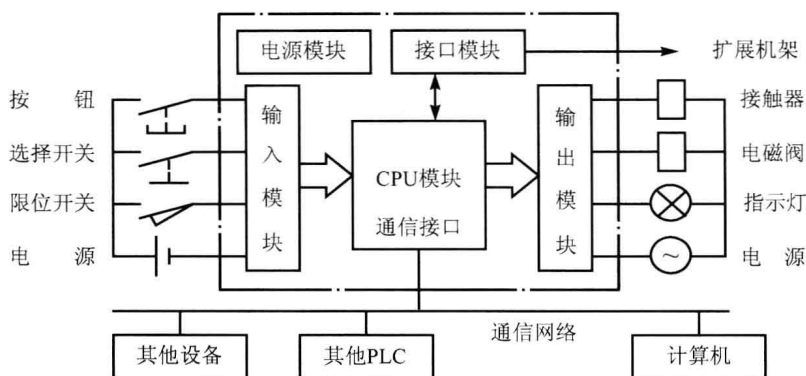


图 1-1 PLC 控制系统示意图

输入模块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、测速发电机和各种变送器提供的连续变化的模拟量电流、电压信号，或者直接接收热电阻、热电偶提供的温度信号。

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电动调节阀、变频器等执行器。

CPU 模块内部的工作电压一般是 DC 5 V，而 PLC 的外部输入/输出信号电压一般较高，例如 DC 24 V 或 AC 220 V。从外部引入的尖峰电压和干扰噪声可能损坏 CPU 模块中的元器件，或使 PLC 不能正常工作。在信号模块中，用光耦合器和小继电器等器件来隔离 PLC 的内部电路和外部的输入、输出电路。信号模块除了传递信号外，还有电平转换与隔离的作用。

3. 功能模块

为了增强 PLC 的功能，扩大其应用领域，减轻 CPU 的负担，PLC 厂家开发了各种各样的功能模块。它们主要用于完成某些对实时性和存储容量要求很高的控制任务，例如高速计数、位置控制和闭环控制等。

4. 接口模块

CPU 模块所在的机架称为中央机架，如果一个机架不能容纳全部模块，可以增设一个或多个扩展机架。接口模块（简称为 IM）用来实现中央机架与扩展机架之间的通信。

5. 通信处理器

通信处理器（简称为 CP）用于 PLC 之间、PLC 与远程 I/O 之间、PLC 与计算机和其他智能设备之间的通信，可以将 S7-300/400 接入各种通信网络，CP 也用于实现点对点通信。CPU 模块集成有 MPI 通信接口，有的 CPU 模块还集成了其他通信接口。

6. 电源模块

电源模块（简称为 PS）用于将输入的 AC 220 V 电源或 DC 24 V 电压转换为稳定的 DC 24 V 和 DC 5 V 电压，供其他模块和输出模块的负载使用。

7. 编程设备

S7-300/400 一般使用安装了编程软件 STEP 7 的个人计算机作为编程设备，可以

生成和编辑各种文本程序或图形程序。程序被编译后下载到 PLC，也可以将 PLC 中的程序上传到计算机。编程软件还有对网络和硬件组态、参数设置、监控和故障诊断等功能。

1.1.2 PLC 的特点

1. 编程方法简单易学

梯形图是使用得最多的 PLC 的编程语言，其电路符号和表达方式与继电器电路原理图相似。梯形图语言形象直观、易学易懂，熟悉继电器电路图的电气技术人员只需花几天时间就可以熟悉梯形图语言，并用来编制数字量控制系统的用户程序。

2. 功能强，性能价格比高

一台小型 PLC 内有成百上千个可供用户使用的编程元件，可以实现非常复杂的控制功能。与相同功能的继电器系统相比，具有很高的性能价格比。PLC 可以通过通信联网，实现分散控制、集中管理。

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 的安装接线也很方便，一般用接线端子连接外部接线。PLC 有较强的带负载能力，可以直接驱动大多数电磁阀和中小型交流接触器。

硬件配置确定后，通过修改用户程序，就可以方便快速地适应工艺条件的变化。

4. 可靠性高，抗干扰能力强

传统的继电器控制系统使用了大量的中间继电器和时间继电器。由于触点接触不良，容易出现故障。PLC 用软件代替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外部硬件元件，接线可减少到继电器控制系统的 1/10 以下，大大减少了因触点接触不良造成的故障。PLC 使用了一系列硬件和软件抗干扰措施，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，现已被广大用户公认为最可靠的工业控制设备之一。

5. 系统的设计、安装、调试工作量少

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 的梯形图程序可以用顺序控制设计法来设计。这种设计方法很有规律，很容易掌握。对于复杂的控制系统，用这种方法设计程序的时间比设计继电器系统电路图的时间要少得多。

在现场调试过程中，一般通过修改程序就可以解决发现的问题，系统的调试时间比继电器系统少得多。

6. 维修工作量小，维修方便

PLC 的故障率很低，并且有完善的故障诊断功能。S7-300/400 提供了多种多样的故障诊断和显示的方法，使用户能方便快速地查明故障的原因，迅速地排除故障。

7. 体积小，能耗低

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。PLC 控制系统与继电器控制系统相比，配线用量和安装接线所需工时减少，加上开关柜体积的缩小，可以节省大量的费用。

1.1.3 PLC 的应用领域

在发达的工业国家，PLC 已经广泛地应用在不同的工业部门。随着其性能价格比的不断提高，应用范围不断扩大，主要有以下几个方面。

1. 开关量逻辑控制

PLC 具有“与”、“或”、“非”等逻辑指令，可以实现梯形图中触点和电路的串、并联，代替继电器进行组合逻辑控制、定时控制与顺序逻辑控制。开关量逻辑控制可以用于单台设备，也可以用于自动生产线，其应用领域已遍及各行各业，甚至深入到民用和家庭。

2. 运动控制

PLC 使用专用的指令或运动控制模块，对直线运动或圆周运动的位置、速度和加速度进行控制，可以实现单轴或多轴联动的位置控制，使运动控制与顺序控制功能有机地结合在一起。PLC 的运动控制功能广泛地用于各种机械，例如金属切削机床、金属成形机械、装配机械、机器人、电梯等场合。

3. 闭环过程控制

闭环过程控制是指对温度、压力、流量等连续变化的模拟量的闭环控制。PLC 通过模拟量 I/O 模块，实现模拟量（Analog）和数字量（Digital）之间的 A/D 转换与 D/A 转换，并对模拟量实行闭环 PID（比例 - 积分 - 微分）控制。S7 - 300/400 有闭环控制模块、用于闭环控制的功能块和闭环控制软件包供用户选用。其闭环控制功能广泛地应用于塑料挤压成形机、加热炉、热处理炉、锅炉等设备，以及轻工、化工、机械、冶金、电力、建材等行业。

4. 数据处理

现代的 PLC 具有整数四则运算、浮点数运算、函数运算、字逻辑运算、求反码和补码、循环、移位等运算功能，以及数据传送、转换、排序、查表、位操作等功能，可以完成数据的采集、分析和处理。这些数据可以与存储器中的参考值比较，也可以用通信功能传送到其他的智能装置，或者将它们打印制表。

5. 通信联网

PLC 的通信包括 PLC 与远程 I/O 之间的通信、多台 PLC 之间的通信、PLC 与其他智能控制设备（例如计算机、变频器、数控设备）之间的通信。PLC 与其他智能控制设备一起，可以组成“集中管理、分散控制”的分布式控制系统。

1.1.4 怎样下载西门子 PLC 的资料和软件

我国有不少厂家研制和生产 PLC，但是还没有出现具有较大影响力和有较大市场占有率的产品，目前我国使用的 PLC 主要是国外品牌的产品。

在全世界上百个 PLC 制造厂中，有几家举足轻重的公司。它们是德国的西门子（Siemens）公司、美国 Rockwell 自动化公司所属的 A - B（Allen & Bradley）公司、GE-Fanuc 公司、法国的施耐德（Schneider）公司、日本的三菱公司和欧姆龙（OMRON）公司。

与个人计算机相比，PLC 的标准化较差，其软件、硬件的体系结构基本上是封闭的而不是开放的，各厂家的 PLC 的编程语言、寻址方式、程序结构和通信网络的差异很大，各种

PLC 互不兼容。国际电工委员会（IEC）的 IEC 61131-3（PLC 的编程语言标准）为 PLC 编程的标准化打下了基础。

用户可以在西门子自动化与驱动集团的中文网站（www.ad.siemens.com.cn）下载西门子的 PLC 资料。单击该网站主页的“支持中心”中的“下载中心”，可以下载各种工控产品的中英文说明书、用户手册、产品介绍和一些软件。单击“下载中心”中的“英文资料下载”，将会打开西门子自动化的支持中心网站。在该中心的主页可以将语言设置为中文，在左边的导航窗口中选择感兴趣的产品，在右边的窗口中可以下载软件和手册，查看常见问题的解答和技术参数等。

为了阅读 PDF 格式的手册，需要在计算机上安装 Adobe 阅读器或其他兼容的阅读器。

1.2 PLC 的工作原理

1.2.1 逻辑运算

在数字量（或称为开关量）控制系统中，变量仅有两种相反的工作状态，例如高电平和低电平、继电器线圈的通电和断电，可以分别用逻辑代数中的 1 和 0 来表示这些状态。在波形图中，用高电平表示 1 状态，用低电平表示 0 状态。

使用继电器电路、数字电路或 PLC 的梯形图都可以实现数字量的逻辑运算。图 1-2 的上面是 PLC 的梯形图，下面是对应的数字门电路。

图 1-2 中的 I0.0 ~ I0.4 为数字输入变量，Q4.0 ~ Q4.2 为数字输出变量，它们之间的“与”、“或”、“非”逻辑运算关系如表 1-1 所示。“与”运算仅在输入均为 1 时，输出才为 1；“或”运算仅在输入均为 0 时，输出才为 0；“非”运算的输出与输入的状态总是相反，非运算又称为“取反”。

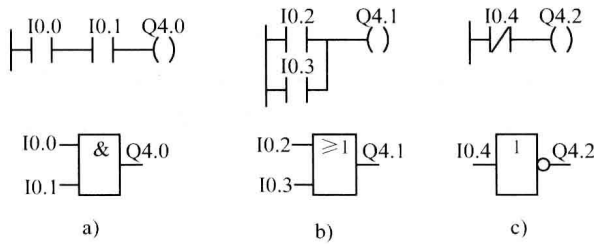


图 1-2 基本逻辑运算

a) 与 b) 或 c) 非

表 1-1 逻辑运算关系表

与			或			非	
$Q4.0 = I0.0 \cdot I0.1$			$Q4.1 = I0.2 + I0.3$			$Q4.2 = \overline{I0.4}$	
I0.0	I0.1	Q4.0	I0.2	I0.3	Q4.1	I0.4	Q4.2
0	0	0	0	0	0	0	1
0	1	0	0	1	1	1	0
1	0	0	1	0	1		
1	1	1	1	1	1		

用继电器电路或梯形图可以实现基本的逻辑运算，触点的串联可以实现“与”运算，触点的并联可以实现“或”运算，用常闭触点控制线圈可以实现“非”运算。

多个触点的串、并联电路可以实现复杂的逻辑运算，例如图 1-3 中的继电器电路实现的逻辑运算可以用逻辑代数表达式表示为

$$KM = (SB1 + KM) \cdot \overline{SB2} \cdot \overline{FR}$$

式中的加号（+）表示逻辑或，乘号（·）或星号（*）表示逻辑与，变量上面的水平线表示“非”运算。与普通算术运算“先乘除后加减”类似，逻辑运算的规则为先“与”后“或”。为了先作“或”运算（触点的并联），用括号将“或”运算式括起来，括号中的运算优先执行。

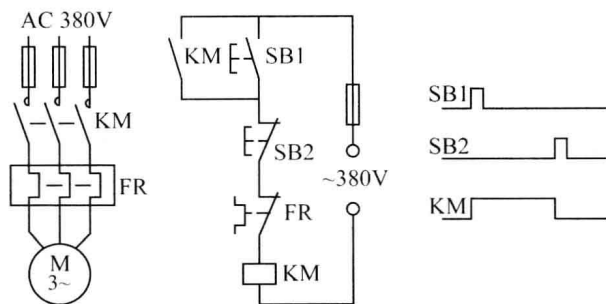


图 1-3 异步电动机控制电路

1.2.2 PLC 的循环处理过程

1. PLC 的循环处理过程

CPU 的程序分为操作系统和用户程序。操作系统用来处理 PLC 的启动、刷新过程映像输入/输出区、调用用户程序、处理中断和错误、管理存储区和通信等任务。

用户程序由用户生成，用来实现用户要求的自动化任务。STEP 7 将用户编写的程序和程序所需的数据放置在块中，功能块 FB 和功能 FC 是用户编写的子程序，系统功能块 SFB 和系统功能 SFC 是操作系统提供给用户使用的标准子程序，它们和组织块 OB 统称为逻辑块。

PLC 得电或由 STOP 模式切换到 RUN 模式时，CPU 执行启动操作，将没有断电保持功能的位存储器、定时器和计数器清零，清除中断堆栈和块堆栈的内容，复位保存的硬件中断等。此外还要执行一次用户生成的“系统启动”组织块 OB100，完成用户指定的初始化操作。以后 PLC 采用循环执行用户程序的方式，这种运行方式也称为扫描工作方式。

在 PLC 的存储器中，设置了一片区域用来存放输入信号和输出信号的状态，它们分别称为过程映像输入区和过程映像输出区。PLC 梯形图中的其他编程元件也有对应的存储区。

下面是循环处理的各个阶段的任务（见图 1-4）：

- 1) 操作系统启动循环时间监控。
- 2) CPU 将过程映像输出区的数据写到输出模块。
- 3) CPU 读取输入模块的输入状态，并存入过程映像输入区。
- 4) CPU 处理用户程序，执行用户程序中的指令。
- 5) 在循环结束时，操作系统执行其他任务，例如下载和删除块，接收和发送全局数据等。
- 6) CPU 返回第一阶段，重新启动循环时间监控。

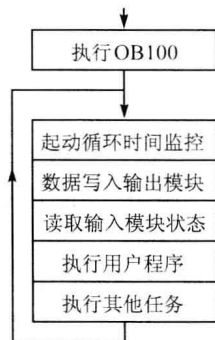


图 1-4 扫描过程

在启动完成后，每次循环都要调用一次组织块 OB1。OB1 是用户程序中的主程序，它可以调用别的逻辑块（FB、FC、SFB 或 SFC）。循环程序处理过程可以被某些事件中断。如果有中断事件出现，当前正在执行的块被暂停执行，并自动调用分配给该事件的组织块。该组织块被执行完后，被暂停执行的块将从被中断的地方开始继续执行。

在循环程序处理过程中，CPU 并不直接访问 I/O 模块中的输入地址区和输出地址区，而是访问 CPU 内部的过程映像区。

在写输出模块阶段，CPU 将过程映像输出区的状态传送到输出模块。梯形图中某一数字量输出位（例如 Q4.0）的线圈“通电”时，对应的过程映像输出位为 1 状态。信号经输出模块隔离和功率放大后，继电器型输出模块中对应的硬件继电器的线圈通电，其常开触点闭合，使外部负载通电工作。若梯形图中输出位的线圈“断电”，对应的过程映像输出位为 0 状态，在写输出模块阶段之后，继电器型输出模块中对应的硬件继电器的线圈断电，其常开触点断开，外部负载断电，停止工作。

在读输入模块阶段，PLC 把所有外部输入电路的接通/断开状态读入过程映像输入区。

外部输入电路接通时，对应的过程映像输入位（例如 I0.0）为 1 状态，梯形图中该输入位的常开触点接通，常闭触点断开。外部输入电路断开时，对应的过程映像输入位为 0 状态，梯形图中该输入位的常开触点断开，常闭触点接通。

某一编程元件对应的位为 1 状态时，称该编程元件的状态为 ON；该位为 0 状态时，称该编程元件的状态为 OFF。在程序执行阶段，即使外部输入电路的状态发生了变化，过程映像输入位的状态也不会随之而变，输入信号变化了的状态只能在下一个扫描周期的读取输入模块阶段被读入过程映像输入区。

PLC 的用户程序由若干条指令组成，指令在存储器中顺序排列。在没有跳转指令和块调用指令时，CPU 从第一条指令开始，逐条顺序地执行用户程序，直到用户程序结束之处。在执行指令时，从过程映像输入区或其他存储区中将有关编程元件的 0、1 状态读出来，并根据指令的要求执行相应的逻辑运算，运算的结果写入到对应的存储区中，因此，各编程元件的存储区的内容随着程序的执行而变化。

2. 扫描周期

扫描周期（Scan Cycle）是指操作系统执行一次如图 1-4 所示的循环操作所需的时间，扫描周期又称为扫描扫描周期（Scan Cycle Time）。扫描周期与用户程序的长短、指令的种类和 CPU 执行指令的速度有很大的关系。当用户程序较长时，指令执行时间在扫描循环时间中占相当大的比例。在 PLC 处于运行模式时，可以从 CPU 的模块信息对话框或 OB1 的局部变量获得最大循环时间、最小循环时间和上一次的循环时间。

扫描周期会因为下列事件而延长：中断处理、诊断和故障处理、测试和调试功能、通信、传送和删除块、压缩用户程序存储器、读/写微存储卡（MMC）等。

1.2.3 PLC 的工作原理

1. PLC 的工作原理

下面用一个简单的例子来进一步说明 PLC 的循环工作过程。图 1-5 所示的开关 S1 和 S2 的常开触点分别接在输入模块上 I0.1 和 I0.2 对应的输入端，接触器 KM 的线圈接在输出模块上 Q4.0 对应的输出端。

图 1-5 所示的梯形图中的 I0.1 是过程映像输入位，与接在对应的输入端的 S1 的常开触点相对应，梯形图中的 Q4.0 是过程映像输出位，与接在对应的输出端子的输出模块内的输出电路相对应。梯形图以指令的形式储存在 PLC 的用户程序存储器中，图 1-5 中的梯形图与下面的 3 条指令相对应，“//”之后是该指令的注释。

A	I 0.1	//接在左侧“电源线”上的 I0.1 的常开触点
AN	I 0.2	//串联的 I0.2 的常闭触点
=	Q 4.0	//Q4.0 的线圈

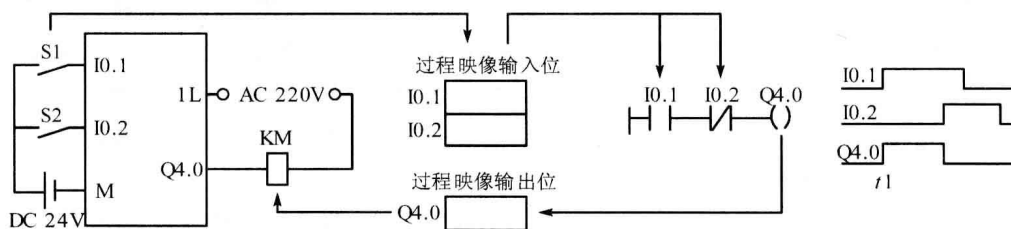


图 1-5 PLC 外部接线图与梯形图

A (And, 与) 指令表示常开触点串联, AN (And Not) 指令表示常闭触点串联, 赋值指令 “=” 表示将逻辑运算的结果传送给指定的地址。图 1-5 中的梯形图完成的逻辑运算为

$$Q4.0 = I0.1 \cdot \overline{I0.2}$$

在读取输入模块阶段, CPU 将 S1 和 S2 的常开触点的 ON/OFF 状态读入对应的过程映像输入位, 外部触点接通时将二进制数 1 存入过程映像输入位, 反之存入 0。

执行第 1 条指令时, 从过程映像输入位 I0.1 中取出二进制数并暂时保存起来。

执行第 2 条指令时, 取出过程映像输入位 I0.2 中的二进制数, 因为是常闭触点, 首先对取出的二进制数作“非”运算, 然后与 I0.1 对应的二进制数作“与”运算, 触点的串联对应“与”运算。

执行第 3 条指令时, 将前面的二进制数运算的结果传送给过程映像输出位 Q4.0。

在下一扫描周期的数据写入输出模块阶段, CPU 将各过程映像输出位中的二进制数传送给输出模块, 并由后者将数据锁存起来。如果过程映像输出位 Q4.0 中存放的是二进制数 1, 外接的 KM 的线圈将通电, 反之将断电。

图 1-5 的波形图中的高电平表示外部开关接通或 KM 的线圈通电, 当 $t < t_1$ 时, 读入的过程映像输入位 I0.1 和 I0.2 的值均为二进制数 0, 此时过程映像输出位 Q4.0 中存放的亦为 0。在程序执行阶段, 经过上述逻辑运算过程之后, 运算结果仍为 $Q4.0 = 0$ 。所以 KM 的线圈处于断电状态。 $t = t_1$ 时开关 S1 的外接触点接通, I0.1 变为 1 状态, 经逻辑运算后 Q4.0 也变为 1 状态。在输出处理阶段, 将 Q4.0 对应的过程映像输出位中的 1 送到输出模块, 输出模块中与 Q4.0 对应的物理继电器的常开触点接通, 接触器 KM 的线圈通电。

2. 输入/输出滞后时间

输入/输出滞后时间又称为系统响应时间, 是指 PLC 的外部输入信号发生变化的时刻至它控制的外部输出信号发生变化的时刻的时间间隔。它由输入电路的滤波时间、输出电路的滞后时间和因扫描工作方式产生的滞后时间这三部分组成。

数字量输入模块的 RC 滤波电路用来滤除由输入端引入的干扰噪声, 消除因外接输入触点动作时产生的抖动引起的不良影响, 滤波电路的时间常数决定了输入滤波时间的长短, 有的输入模块的输入延迟时间可以用 STEP 7 设置。

输出模块的滞后时间与模块的类型有关, 继电器型输出电路的滞后时间一般在 10 ms 左

右；双向晶闸管型输出电路在负载通电时的滞后时间约为 1 ms，负载由通电到断电的最大滞后时间为 10 ms；晶体管型输出电路的滞后时间一般在 1 ms 以下。

由扫描工作方式引起的滞后时间最长可达两三个扫描周期。

PLC 总的响应延迟时间一般只有几毫秒到几十毫秒，对于一般的系统无关紧要。要求输入、输出信号之间的滞后时间尽量短的系统，可以选用扫描速度快的 PLC 或采取中断等措施。