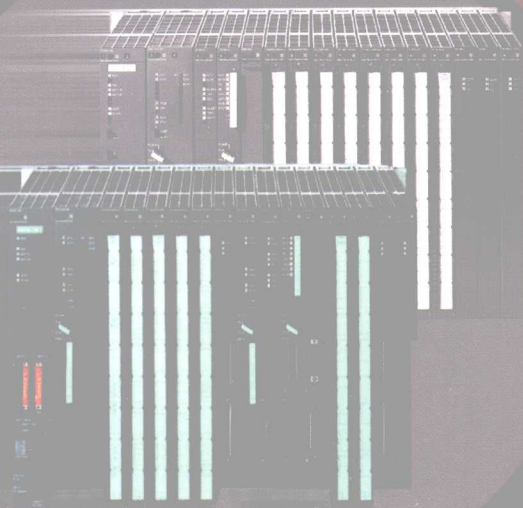


普通高等学校教材
西门子自动化产品培训用书
SIEMENS

STEP7

开发基础及应用指南



SIEMENS

任双艳 边春元 满永春 于艳秋 等编著



普通高等学校教材

西门子自动化产品培训用书

STEP7 开发基础及应用指南

任双艳 边春元 满永奎 于艳秋 等编著



机械工业出版社

SIMATIC STEP7 作为一个平台可以集成各种控制设备的软件,使不同设备以及西门子 PLC 站点具有相同的数据库,所有设备的编程、配置、调试、数据路由以及通信工作只需在 STEP7 中就可以完成,从而实现一个项目中所有控制任务的集成。掌握 STEP7 是学习西门子公司自动化产品的基础。

本书在介绍 PLC 的基本原理的基础上,重点对 SIMATIC STEP7 的编程软件、编程指令、编程方法、系统设计方法等方面做了较为系统深入的讲解。本书共 9 章。第 1 章介绍了 PLC 的发展、特点、组成及简单的工作原理;第 2 章分析了 S7-300/400 系列 PLC 的硬件系统;第 3 章对 S7 系列 PLC 编程软件——STEP7 做了简要介绍;第 4 章介绍了 S7-300/400 系列 PLC 的数据类型与地址区;第 5 章介绍了 S7-300/400 系列 PLC 的编程指令,并结合实例重点讲解了语句表 (STL) 及梯形图 (LAD) 指令的使用方法;第 6 章介绍了数据结构及用户程序结构;第 7 章介绍使用 STEP7 软件进行 PLC 应用系统设计的内容和方法;第 8 章结合具体实例介绍了如何利用 STEP7 编辑逻辑块;第 9 章给出了 PLC 应用系统设计的具体实例。

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专业的教学参考书。

图书在版编目 (CIP) 数据

STEP7 开发基础及应用指南/任双艳等编著. —北京:机械工业出版社, 2008. 11

普通高等学校教材
(西门子自动化产品培训用书)
ISBN 978-7-111-25158-3

I. S… II. 任… III. 软件开发—程序设计—指南
IV. TP311.52-62

中国版本图书馆 CIP 数据核字 (2008) 第 145331 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:林 楨

版式设计:霍永明 责任校对:姜 婷

封面设计:鞠 杨 责任印制:邓 博

北京诚信伟业印刷有限公司印刷

2009 年 1 月第 1 版第 1 次印刷

184mm×260mm·16.75 印张·399 千字

0001—4000 册

标准书号:ISBN 978-7-111-25158-3

定价:38.00 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) 88379764

封面无防伪标均为盗版

西门子自动化产品培训用书

编 委 会

主 编	边春元	满永奎					
副主编	任双艳	王志强					
编 委	姜雪松	李艳杰	李爱平	邓 伟	王 璐		
	崔广臣	刘长勇	孙亦红	李 策	孟晓芳		
	王 珏	于艳秋	王卫红	胡 博	田有文		
	王 俊	解东光	王宇龙	杨 晨	杨 萍		

丛书序

当今科技的飞速发展，对于改变人类社会的生产和生活面貌、推动人类社会的精神文明和物质文明向前发展，无疑具有极其重要的作用和意义。作为一门现代科学技术，自动化技术反映了人们改造大自然的能力，它是多种学科和技术的交叉与综合，尤其是在信息技术飞速发展和日益普及的今天，自动化新技术和新产品更是日新月异、层出不穷。毋庸置疑，自动化技术在推动社会进步、促进经济发展、改善生活质量和建设可持续发展的和谐社会等方面将发挥越来越重要的作用。

西门子（Siemens）公司是当今世界上最大的电气自动化公司之一，其自动化产品遍布于生产和生活的各个方面，电气自动化解决方案是其核心业务领域之一。以应用场合的可编程序控制器和各种控制系统配套解决方案为代表的西门子自动化产品，广泛应用于冶金、造纸、采矿、水处理、造船、石油和天然气、智能交通管理、工业服务和 IT 工厂解决方案等领域。

随着西门子自动化产品在我国各个应用领域的逐步普及和大量应用，需要掌握西门子自动化产品基础和实用开发技术的工程人员和技术人员等群体也在不断扩大，国内多所高等院校和高职高专院校也已先后开设了与西门子自动化产品相关的专业课程，要求某些专业的本科生和研究生必须学习这些课程。可见，西门子公司自动化产品开发技术已经成为广大院校师生、工程人员和技术人员等竞相掌握的一门重要技能。

随着西门子自动化产品的广泛应用，如何更好地使用西门子自动化产品？如何更好地在实践中进行西门子自动化产品的应用开发？如何更好地利用特定西门子自动化产品的内部资源来完成复杂项目的开发？……这些问题不断地在困扰着采用西门子自动化产品进行项目开发的相关人员。因此，如何帮助广大工程人员和技术人员迅速解决上述难题成为一个困扰已久的问题。目前，解决这个问题的重要手段就是在学习源头上多下功夫，即编写和出版一些高质量的科技书。通过学习这些科技图书，读者能够解决在实际开发工作中遇到的各种困扰，真正地掌握西门子自动化产品的基础知识和各种实用开发技术，从而能够更快、更好地完成实际项目的开发。

通过多年的教学实践和培训经验以及广泛的技术交流，广大院校师生、工程人员和技术人员等需要全面系统地阐述西门子自动化产品的书籍，这些书籍不应以介绍产品手册内容为主，而是应该在介绍基础知识的基础上能够介绍具有实际工程背景的实例，同时能够对实际应用中的使用方法、开发技巧和涉及到的重要知识点进行重点阐述。

基于目前西门子自动化产品图书的现状，决定立项出版这套“西门子自动化产品培训用书”，以满足广大读者希望快速、全面地学习和掌握西门子自动化产品系列应用技术的迫切愿望。

这套丛书在总体上遵循循序渐进、理论与实践相结合的原则，内容涵盖了西门子 S7 系

列 PLC、变频器、现场总线、工业网络、触摸屏、STEP7、WinCC、PLC 的梯形图与语句表编程方法等内容。另外,编写本丛书的目的不仅是对所积累知识的一个总结,更希望能将它与广大读者分享,共同探讨与进步。概括起来,这套丛书的主要特点体现在以下方面:

内容全面、体系完备:从不同层面和深度介绍利用西门子自动化产品开发工具进行应用开发的全过程,内容详实,覆盖面广。

实践性强、实例典型:最大程度地强调了实践性,书中所有的实例都经过验证可实现,并具有代表性,读者可通过实例对相应技术点有清晰直观的了解。

把握新知、结合实际:对西门子自动化系列产品的新知识、新特性做了详细的介绍。书中很多技术点都是作者已经在实际工作中大量运用的,它们是开发经验的提炼和总结,相信会给读者带来很大的帮助。

相信这套丛书对于读者掌握西门子自动化产品将发挥重要的作用,使读者能够对西门子自动化产品和技术有一个系统的、全面的、深入的理解,同时能够利用它们开发出满足需要的工业自动化控制系统。

最后对参与这套丛书编写工作的各位作者表示衷心的感谢,感谢大家为我国工业自动化技术的发展和人才培养所作的巨大努力!

同时,也恳切希望读者能够对这套丛书的不足之处提出宝贵意见和建议,以便再版时更正,从而更好地服务广大读者。

是为序。

本丛书编委会

前言

自从西门子公司 1996 年提出崭新的自动化理念——全集成自动化 (Totally Integrated Automation, TIA) 以来, 如何帮助广大的自动化工程师广泛深入地理解和掌握全集成自动化 (TIA) 的三个要素共同的通信、共同的组态与编程、共同的数据库便成为重要问题。STEP7 作为一个平台可以集成各种控制设备的软件, 使不同设备以及 PLC 站点具有相同的数据库, 所有设备的编程、配置、调试、数据路由以及通信工作只需在 STEP7 中就可以完成, 从而实现了一个项目中所有控制任务的集成。掌握 STEP7 是学习西门子公司自动化产品的基础。

西门子公司 PLC 系统功能强大, 配置、编程方法灵活, 但提供的手册过于繁琐, 不少初学者感到入门困难, 希望能有一本适合初学者学习西门子公司 S7-300/400 系列 PLC 编程软件 SIMATIC STEP7 的教材, 本书就是为了适应这部分读者的需要而编写的。除此之外, 本书总结了一些常见问题的解决方法和编程示例, 可以使初学者的技术水平快速提高。

本书在介绍 PLC 的基本原理的基础上, 重点对 SIMATIC STEP7 的编程软件、编程指令、编程方法、系统设计方法等方面做了较为系统深入的讲解。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本科生的教材。

本书共 9 章。第 1 章介绍了 PLC 的发展、特点、组成及简单工作原理; 第 2 章分析了 S7-300/400 系列 PLC 的硬件系统; 第 3 章对 S7 系列 PLC 编程软件——STEP7 做了简要介绍; 第 4 章介绍了 S7-300/400 系列 PLC 的数据类型与地址区; 第 5 章介绍了 S7-300/400 系列 PLC 的编程指令, 并结合实例重点讲解了语句表 (STL) 及梯形图 (LAD) 指令的使用方法; 第 6 章介绍了数据结构及用户程序结构; 第 7 章介绍了使用 STEP7 进行 PLC 应用系统设计的内容和方法; 第 8 章结合具体实例介绍了如何利用 STEP7 编辑逻辑块; 第 9 章给出了 PLC 应用系统设计的具体实例。

本书第 1 章由边春元编写, 第 2 章由满永奎编写, 第 3、4、5、6、7、8 章由任双艳主要编写, 第 9 章由于艳秋编写, 参与部分章节编写、资料收集整理及程序调试的还有孙亦红、姜春和、李爱平、崔广臣、刘长勇、王志强、廖三三、何大勇、蒋越、范家蓬、吕兴君、姜兴旭、闫向峰。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力系统与电力传动研究所的全体老师对本书编写过程中的指导和技术支持。

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

2008 年 10 月

目 录

丛书序

前言

第1章 绪论..... 1

- 1.1 PLC的发展概况..... 1
- 1.2 PLC的功能..... 2
- 1.3 PLC的基本组成..... 2
- 1.4 PLC的简单工作原理..... 3
- 1.5 S7系列PLC介绍..... 5
- 1.6 PLC的应用及其发展趋势..... 6
 - 1.6.1 PLC的应用..... 6
 - 1.6.2 PLC的发展趋势..... 7
- 1.7 STEP7编程软件..... 8
 - 1.7.1 编程功能..... 8
 - 1.7.2 TIA软件平台..... 10

第2章 S7-300/400 PLC的硬件系统..... 12

- 2.1 硬件系统基本构成..... 12
 - 2.1.1 概述..... 12
 - 2.1.2 S7-300/400 PLC的组成..... 14
 - 2.1.3 S7-300/400 PLC的结构..... 17
 - 2.1.3.1 S7-300 PLC的结构..... 17
 - 2.1.3.2 S7-400 PLC的结构..... 18
- 2.2 CPU模块及性能特点..... 19
 - 2.2.1 S7-300 PLC的CPU模块..... 19
 - 2.2.1.1 CPU模块的性能概述..... 19
 - 2.2.1.2 CPU模块的面板..... 20
 - 2.2.1.3 CPU模块的测试和诊断故障功能..... 23
 - 2.2.2 S7-400 PLC的CPU模块..... 23
 - 2.2.2.1 CPU模块的性能概述..... 23

- 2.2.2.2 CPU模块的面板..... 24
- 2.3 输入/输出模块及模块地址的确定..... 25
 - 2.3.1 S7-300 PLC的SM..... 25
 - 2.3.1.1 数字量模块..... 25
 - 2.3.1.2 模拟量模块..... 28
 - 2.3.2 S7-400 PLC的SM..... 32
 - 2.3.2.1 数字量模块..... 32
 - 2.3.2.2 模拟量模块..... 32
 - 2.3.3 模块诊断与过程中断..... 33
 - 2.3.4 信号模块地址的确定..... 33
 - 2.3.4.1 S7-300 PLC信号模块的地址..... 33
 - 2.3.4.2 S7-400 PLC信号模块的地址..... 34

第3章 S7系列PLC编程软件——

STEP7简介..... 35

- 3.1 STEP7编程软件的订货版本..... 36
- 3.2 STEP7编程软件的安装..... 36
 - 3.2.1 硬件要求..... 36
 - 3.2.2 软件要求..... 36
 - 3.2.3 语言设置..... 37
 - 3.2.4 安装步骤..... 37
- 3.3 STEP7编程软件的卸载..... 40
- 3.4 STEP7的标准软件包..... 40
 - 3.4.1 STEP7标准软件包的应用程序..... 40
 - 3.4.2 人机接口..... 42
- 3.5 STEP7的启动..... 42
- 3.6 STEP7的编程语言概述..... 44

第4章 S7-300/400系列PLC数据

类型与地址区..... 47

- 4.1 数制..... 47



4.2 数据类型	47
4.2.1 基本数据类型	48
4.2.2 复合数据类型	52
4.3 参数类型	52
4.4 数据的格式标记	53
4.5 地址区与寻址方式	55
4.5.1 CPU 地址区的划分	55
4.5.2 全局变量与区域变量	57

第5章 编程指令

5.1 S7-300/400 PLC 指令系统的基本知识	58
5.1.1 指令的基本组成	58
5.1.2 操作数	59
5.1.3 寻址方式	60
5.2 位逻辑指令	63
5.2.1 基本逻辑指令	63
5.2.2 置位/复位指令	69
5.2.3 边沿信号识别指令	71
5.2.4 定时器指令	78
5.2.5 计数器指令	84
5.3 数据传送与转换指令	86
5.3.1 传送指令	86
5.3.2 转换指令	89
5.4 运算指令	94
5.4.1 整数算术运算指令	94
5.4.2 扩展的浮点数算术运算指令	96
5.4.3 加、减、乘、除运算	97
5.4.4 算术运算指令实例	103
5.5 移位指令	107
5.6 累加器操作和地址寄存器操作指令	117
5.7 控制指令	121

第6章 S7-300/400 PLC 的用户程序结构

6.1 用户程序	124
6.1.1 程序块	124
6.1.2 堆栈	126

6.2 功能块与功能	128
6.2.1 局域数据类型	128
6.2.2 功能块与功能的调用	129
6.2.3 功能块调用编程举例	130
6.3 数据块与数据结构	133
6.3.1 数据块的生成	133
6.3.2 数据块中的数据结构	135
6.4 组织块与中断处理	139
6.4.1 中断的基本概念	139
6.4.2 组织块的变量声明表	140
6.4.3 用于中断程序处理的组织块	141
6.4.4 日期时钟中断组织块 (OB10 ~ OB17)	141
6.4.5 时间延迟中断组织块 (OB20 ~ OB23)	143
6.4.6 循环中断组织块 (OB30 ~ OB38)	144
6.4.7 硬件中断组织块 (OB40 ~ OB47)	146
6.4.8 背景组织块 (OB90)	147
6.4.9 启动组织块 (OB100 ~ OB102)	147
6.4.10 故障处理组织块 (OB70 ~ OB87/OB121、OB122)	149

第7章 使用 STEP7 进行 PLC 应用系统设计

7.1 创建与编辑项目	151
7.1.1 利用 STEP7 创建项目的步骤	151
7.1.2 项目结构	153
7.1.3 创建项目	154
7.1.4 编辑项目	155
7.2 硬件组态	157
7.2.1 硬件组态的任务与步骤	157
7.2.2 CPU 的参数设置	159
7.2.3 I/O 模块的参数设置	163
7.3 定义符号	167
7.3.1 共享符号与局域符号	168



7.3.2 符号表	168	7.8.3.2 程序状态的显示	193
7.3.2.1 输入共享符号	169	7.8.3.3 单步与断点功能的使用	195
7.3.2.2 导入/导出符号表	170	7.9 故障诊断	197
7.4 逻辑块的生成	170	7.9.1 诊断硬件和故障诊断	197
7.4.1 建立逻辑软件块	170	7.9.1.1 故障诊断的基本步骤	197
7.4.2 编辑变量声明表	171	7.9.1.2 在线视窗中的诊断符号	197
7.4.3 编制并输入程序	171	7.9.2 用诊断视窗诊断硬件	198
7.5 刷新块调用与逻辑块存盘	172	7.9.3 模块信息功能	199
7.6 显示参考数据	172	7.9.4 在停机模式下诊断	200
7.6.1 参考数据类型	172	7.10 PLC 应用系统设计实例	201
7.6.1.1 交叉参考列表	173		
7.6.1.2 程序结构	175	第 8 章 利用 STEP7 编辑逻辑块	205
7.6.1.3 输入、输出和位存储赋值表	177	8.1 程序布局及编程规则	205
7.6.1.4 显示 LAD、FBD 和 STL 的块信息	178	8.1.1 梯形图	205
7.6.2 参考数据的使用	178	8.1.2 语句表	206
7.6.2.1 参考数据显示方式	178	8.1.3 功能块图	207
7.6.2.2 生成并显示参考数据	179	8.2 在 OB1 中创建程序	208
7.6.2.3 在程序中快速查找地址的位置	179	8.2.1 编程的准备工作	208
7.7 下载与上传	182	8.2.2 用梯形图编写 OB1	211
7.7.1 在线连接的建立与在线操作	182	8.2.3 用语句表编写 OB1	213
7.7.2 下载	183	8.2.4 用功能块图编写 OB1	214
7.7.2.1 下载方式	183	8.3 创建一个有功能块和数据块的程序	215
7.7.2.2 下载的方法	184	8.3.1 创建并打开功能块	215
7.7.2.3 下载组态	184	8.3.1.1 用梯形图编写 FB1	216
7.7.3 上传	185	8.3.1.2 用语句表编写 FB1	218
7.7.3.1 上传站参数	185	8.3.1.3 用功能块图编写 FB1	218
7.7.3.2 上传硬件组态和连接组态	185	8.3.2 生成背景数据块并修改实际值	219
7.8 程序的调试	186	8.3.3 编程块调用	220
7.8.1 PLC 应用系统的调试	186	8.3.3.1 用梯形图编写块调用	220
7.8.2 用变量表调试程序	187	8.3.3.2 用语句表编写块调用	221
7.8.2.1 变量表的基本功能	187	8.3.3.3 用功能块图编写块调用	222
7.8.2.2 创建变量表	188	8.4 编写一个功能	223
7.8.2.3 使用变量表	190	8.4.1 创建并打开功能	223
7.8.3 用程序状态功能调试程序	193	8.4.2 在 OB1 中调用功能	225
7.8.3.1 程序状态功能的启动	193		
		第 9 章 PLC 应用系统设计实例	227
		9.1 长钢轨群吊多吊集控的功能	227
		9.1.1 长轨吊的主要组成部分	227



9.1.2 长轨吊的主要工作	228
9.1.3 各部分控制功能	228
9.2 长钢轨群吊多吊集控的硬件设计	230
9.2.1 定义 I/O 表	230
9.2.2 PLC 的硬件配置	240
9.2.3 设置通信参数	243
9.2.4 PLC 硬件的连接	244
9.2.5 PLC 输入输出外围接口电路设计	244
9.2.6 PLC 硬件组装调试	245

9.3 长钢轨群吊多吊集控的软件设计	245
9.3.1 创建项目	245
9.3.2 硬件组态	245
9.3.3 编写程序块	247
9.3.4 利用模拟软件包进行程序测试	255
9.3.5 软硬件联调	256
9.4 开发技巧和经验总结	257

参考文献	258
------	-----

第 1 章

绪 论

可编程序控制器 (Programmable Controller, PC) 在其早期主要应用于开关量的逻辑控制, 因此也称为 PLC (Programmable Logic Controller), 即可编程序逻辑控制器。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, 成为了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。为了避免与个人计算机 (Personal Computer) 的缩写 PC 混淆, 本书中可编程序控制器均简称为 PLC。

1.1 PLC 的发展概况

在可编程序控制器问世以前, 工业控制领域中是由继电器控制占主导地位的。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的适应性更差。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) 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) 就研制出了第一台 PLC, 将其应用于美国通用汽车自动装配生产线上, 并取得了极大的成功。

PLC 的发展与计算机技术、半导体集成技术、控制技术、数字技术、通信网络技术等高新技术的发展息息相关。这些高新技术的发展推动了 PLC 的发展, 而 PLC 的发展又对这些高新技术提出了更高、更新的要求, 促进了它们的发展。

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 SYMATIC SY5 和 S7 系列以及 AB 公司的 PLC-5 等。

1.2 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。现在的 PLC 一般具有如下主要功能:

- 1) 开关量逻辑控制功能;
- 2) 定时/计数控制功能;
- 3) 数据处理功能;
- 4) 监控、故障诊断功能;
- 5) 步进控制功能;
- 6) A/D、D/A 转换功能;
- 7) 停电记忆功能;
- 8) 远程 I/O 功能;
- 9) 通信连网功能;
- 10) 扩展功能。

1.3 PLC 的基本组成

由 PLC 构成的基本控制系统硬件简化框图如图 1-1 所示。其中 PLC 的基本组成为点划线框内的四部分:中央处理器单元(CPU)、存储器、输入/输出(I/O)模块和电源。



图 1-1 PLC 控制系统结构简图

1. 中央处理器单元 (CPU)

CPU 是 PLC 的神经中枢,是系统的运算、控制中心。它按照系统程序所赋予的功能,完成以下任务

- 1) 接收并存储用户程序和数据;
- 2) 用扫描的方式接收现场输入设备的状态和数据;
- 3) 诊断电源、PLC 内部电路工作状况和编程过程中的语法错误;
- 4) 完成用户程序中规定的逻辑运算和算术运算任务;

(5) 更新有关标志位的状态和输出状态寄存器的内容, 实现输出控制、制表打印或数据通信等功能。

2. 存储器

存储器是 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。随机存取存储器 (RAM) 有静态 RAM (SRAM) 和动态 RAM (DRAM) 两种; 只读存储器 (ROM) 按其编程方式不同, 可分为掩膜只读存储器 (ROM)、可编程只读存储器 (PROM)、可擦除可编程只读存储器 (EPROM) 和电擦除可编程只读存储器 (E²PROM) 等。

由于 PLC 的软件由系统软件 and 用户软件构成, 因此 PLC 的存储器可分为系统程序存储器和应用程序存储器。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, 但根据其工作原理, 其存储空间一般包括以下三个区域:

1) 系统程序存储区。存放着相当于计算机操作系统的系统程序。它包括监视程序、管理程序、命令解释程序、功能子程序、系统诊断程序等。由制造商将其固化在 ROM 中, 用户不能直接存取。

2) 系统 RAM 存储区。包括 I/O 映像区以及各类软设备 (如各种逻辑线圈、数据存储器、定时器、计数器、累加器、变址寄存器等) 存储区。

3) 用户程序存储区。存放用户编制的应用控制程序, 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的桥梁。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。

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。

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 的内部电路供电。

1.4 PLC 的简单工作原理

PLC 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、输出刷新四个阶段。PLC 周而复始地循环执行这四个阶段, 这种工作方式称为扫描工作方式。PLC 每重复一次这四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)。

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。因此，为了理解上的方便，通常忽略内部处理阶段，而认为 PLC 的工作过程为三个阶段：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三个阶段所用的时间为一个扫描周期。

PLC 工作过程的三个阶段：输入采样阶段、用户程序执行阶段和输出刷新阶段，如图 1-2 所示。

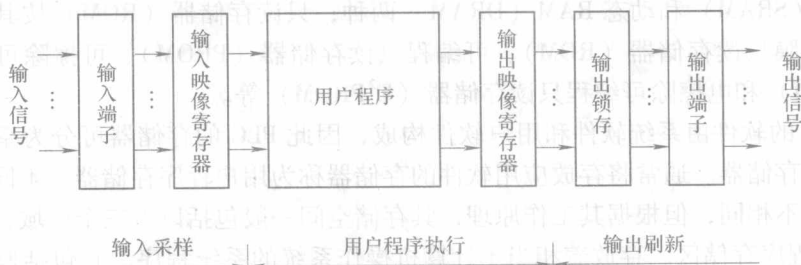


图 1-2 PLC 的工作过程图

1. 输入采样阶段

PLC 以扫描工作方式，按顺序将所有信号读入到寄存输入状态的输入映像寄存器中存储，这一过程称为采样。在本工作周期内，这个采样结果的内容不会改变，而且这个采样结果将在 PLC 执行程序时被使用。

2. 用户程序执行阶段

PLC 按顺序对程序进行扫描，即从上到下、从左到右地扫描每条指令，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存储的内容，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最后固定下来了。

3. 输出刷新阶段

在执行完所有用户所有程序后，PLC 将映像寄存器中的内容送入到寄存输出状态的输出锁存器中，再去驱动用户设备，这就是输出刷新。

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 4ms 左右，而程序执行时间可因程序长度的不同而不同。PLC 的一个扫描周期一般在 $40 \sim 100\text{ms}$ 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）。在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来说, 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”(Watchdog) 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。

1.5 S7 系列 PLC 介绍

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。西门子的 PLC 发展到现在已有很多系列产品, 如 S5、S7、C7、M7 系列 PLC 等, 本书主要以 S7 系列 PLC 为例讲解 PLC 的理论和应用。

S7 系列 PLC 是在 S5 系列基础上研制出来的, 它由微型 S7-200 PLC、中小型 S7-300 PLC 和大型 S7-400 PLC 组成。

1. S7-200 PLC

微型 S7-200 PLC 的结构紧凑、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, 可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)、操作员接口和串行设备接口支持编程; 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。

2. S7-300 PLC

模块化中小型 S7-300 PLC 适用于极其快速的过程处理或对数据处理能力有特别要求的中小型自动化控制系统。其具有高速的计算能力, 完整的指令集, 多点接口 (MPI) 和通过 SINEC LAN 的连网能力; 内置功能, 综合的诊断能力, 将推出的口令保护, 简便的连接系统和无限的插入模块组态, 使系统组态处理更加方便; 极快的指令处理速度, 缩短了循环时间; 高性能模块和多种 CPU 为各种各样的需求提供了合适的解决方案; 模块扩展能力最多可增加到三个扩展基架 (ER), 极高的安装密度, 背板总线安装在每个模块中, 预先接线系统 (TOP 接线), 减少了所需空间和费用; 为连接 SIMATIC 系列各种部件提供了接口, 内置的人机接口 (HMI) 服务, 对用户友好的 Windows STEP7 Mini 编程软件和功能强大的编程器。



3. S7-400 PLC

快速、坚固和极具通信能力的大中型 S7-400 PLC 适用于大、中型自动控制系统。其在程序执行方面，指令执行时间极短；在恶劣、不稳定的工业环境下，坚固、全部密封的模板依然可正常工作；无风扇操作降低了安装的费用；在操作运行过程中模板可插拔；分布式的内部总线允许在 CPU 与中央 I/O 间进行非常快的通信（P 总线与输入/输出模板间进行数据交换，C 总线可将大量数据传送到功能模板和通信模板）；一些 CPU 装备了内置的 SINEC L2 DP 接口，保证了对分布式 I/O 进行快速数据交换；强大的通信模板允许点到点通信，以及用 SINEC L2 和 SINEC H1 总线系统进行通信。

1.6 PLC 的应用及其发展趋势

1.6.1 PLC 的应用

PLC 的产生初期，由于其价格高于继电器控制装置，使得其应用受到限制。但最近几年来，随着 PLC 性能价格比的不断提高，PLC 的应用面越来越广，其主要原因是：一方面由于微处理器芯片及有关元件的价格大大下降，使得 PLC 的成本下降；另一方面 PLC 的功能大大增强，使它也能解决复杂的计算和通信问题。目前，PLC 已广泛用于工业控制的各个领域，包括从单机自动化到工厂自动化；从机器人、柔性制造系统到工业局部网络。

从 PLC 的功能来分，PLC 的应用领域主要有以下几方面：

1. 开关量逻辑控制

这是 PLC 最基本、最广泛的应用领域，它完全取代了传统的继电器等顺序控制装置。开关量逻辑控制可以代替继电器完成组合逻辑控制、定时与顺序逻辑控制，它既可用于单机控制，又可用于多机群控，以及生产线的自动控制。并广泛应用于电力、机械制造、钢铁、石油、化工、采矿、汽车、造纸、纺织等行业，如机床电气控制、包装机械的控制、运输带与电梯的控制、汽车装配生产线及自动生产线中各种泵和电磁阀的控制等。

2. 运动控制

利用配合 PLC 使用的专用智能模块，可以对步进电动机或伺服电动机的单轴或多轴系统实现位置控制。在多数情况下，PLC 把描述目标位置的数据传送给模块，模块驱动轴系到目标位置。当每个轴转动时，位置控制模块使其保持适当的速度和加速度，确保运动平滑。例如对具有多轴的机器人进行控制，自动地处理它的机械运动。

3. 过程控制

过程控制是指对温度、压力、流量等连续变化的模拟量实现的闭环控制。现代的 PLC 一般都有 PID 闭环控制功能。当控制过程中某一个输出变量出现偏差时，PLC 按照 PID 控制算法计算出正确的输出，使输出变量保持在设定值上。PLC 的过程控制功能已经广泛地应用在化工、机械、轻工、冶金、电力、建材等行业。

4. 机械加工机床的数字控制

PLC 和计算机数控（CNC）装置组合成一体，可以实现数值控制，组成数控机床。现代的 PLC 具有数字运算、数据传送、转换、排序、查表和位操作等功能。可以完成数据的采集、分析和处理。预计今后几年 CNC 系统将变成以 PLC 为主体的控制和管理系统。