



普通高等教育“十二五”规划教材

可编程控制器原理及应用 (西门子机型)

杨晋萍 主 编
孙竹梅 副主编



中国电力出版社
CHINA ELECTRIC POWER PRESS

013067545

TP332.3-43
59



普通高等教育“十二五”规划教材

主要内容

可编程控制器原理及应用 (西门子机型)

主 编 杨晋萍
副主编 孙竹梅
编 写 高 佳
主 审 周美兰



TP332.3-X3

59



北航

C1675378



中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书为普通高等教育“十二五”规划教材。

本书全面深入地介绍了西门子 S7-300/400 的硬件结构与硬件组态、编程语言、指令、通信网络、闭环控制、编程软件的使用。主要内容包括可编程控制器工作原理、S7-300/400 的体系结构和硬件组态、STEP 7 的使用、编程语言与指令系统、组织块及系统功能块的使用、PLC 控制系统的软件设计方法、SIMATIC S7 PLC 的通信技术、西门子 S7-300/400 在模拟量控制系统中的应用等,在第 9 章中设置了基础实验和综合型实验实训,帮助读者理解和掌握编程语言及编程方法。

本书内容紧扣实践教学的要求,理论联系实际,既可作为本科电气信息类、自动化类专业和高职高专相关专业的教学和实验用书,也可作为相关技术类培训教材,还可供编程人员参考使用。

图书在版编目(CIP)数据

可编程控制器原理及应用: 西门子机型 / 杨晋萍主编.
北京: 中国电力出版社, 2013.8
普通高等教育“十二五”规划教材
ISBN 978-7-5123-4663-5

I. ①可… II. ①杨… III. ①可编程序控制器—高等学校—教材 IV. ①TM571.6

中国版本图书馆 CIP 数据核字 (2013) 第 154257 号

中国电力出版社出版、发行

(北京市东城区北京站西街 19 号 100005 <http://www.cepp.sgcc.com.cn>)

北京市同江印刷厂印刷

各地新华书店经售

*

2013 年 8 月第一版 2013 年 8 月北京第一次印刷

787 毫米×1092 毫米 16 开本 18.25 印张 444 千字

定价 33.00 元

敬告读者

本书封底贴有防伪标签,刮开涂层可查询真伪
本书如有印装质量问题,我社发行部负责退换

版权专有 翻印必究

前 言

可编程控制器（PLC）是计算机家族中的一员，为工业控制应用而设计制造，是综合了计算机技术、自动化控制技术和通信技术的一种新型的、通用的自动控制装置。PLC 以其功能强、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，成为控制领域中增长速度迅猛的工业控制设备。

据统计，德国西门子公司的 PLC 在我国的 PLC 市场上的占有量已超过 30%，特别是西门子公司推出的 S7-300/400 系列的 PLC 以其功能强大、性价比高等特点而深受国内用户的欢迎，因此本书以 S7-300/400 机型为例介绍可编程控制器的原理及应用。

本书对 S7-300/400 的硬件结构与硬件组态、编程语言、指令、通信网络、闭环控制、编程软件的使用都进行了全面深入的介绍。本书以“突出实践，够用为度”为原则，以 S7-300 为样机，在第 4~6 章中给出了大量的例题，帮助读者快速理解编程语言、掌握编程方法。

PLC 课程是一门以实践为主的课程，本书在内容上由浅入深，紧扣实践教学的要求，以强化工程训练及培养创新能力为目的。本书除了在编程语言中辅以实例之外，在第 9 章中还给出了基础实验和综合型实验实训，以提高读者的实践能力，了解 PLC 对模拟量的控制功能，达到快速入手的效果。在学习过程中，若没有西门子 S7-300 实验设备，本书第 3 章介绍了 STEP 中 PLCSIM 仿真软件的使用方法，读者可以在 PLCSIM 仿真软件上进行调试，也可根据第 7 章的内容与 WinCC 连接，进行仿真实验。本书内容不涉及高深的理论，既可作为大专院校相关专业教材，也可为工程技术人员提供参考。

本书第 1、2、4 章由山西大学杨晋萍编写，第 3、5、9 章由山西大学孙竹梅编写，第 6~8 章由山西大学高佳编写。在本书的编写过程中，得到了许多同事以及西门子公司的支持和帮助，并参考了一些科教人员已出版的书籍和资料，在此一并表示衷心的感谢。

本书承蒙哈尔滨理工大学周美兰教授仔细审阅，提出不少宝贵意见，在此表示深深感谢。由于编者水平有限，疏漏和不足之处在所难免，恳请读者不吝指正。

编 者

2013 年 5 月

目 录

前言

绪论	1
0.1 可编程控制器的产生与定义	1
0.2 PLC 的主要特点及应用领域	2
第 1 章 可编程控制器工作原理	5
1.1 可编程控制器的组成及各部分功能	5
1.2 PLC 的工作原理	6
1.3 PLC 的编程语言	9
第 2 章 S7-300/400 的体系结构和硬件组态	11
2.1 S7 系列的体系结构	11
2.2 S7-300 的模块简介	12
2.3 S7-400 系列 PLC 简介	27
2.4 S7-300 硬件模块的安装	30
2.5 S7-300 I/O 模块的地址分配	31
2.6 模拟量输入/输出模块与 PLC 的连接	33
第 3 章 STEP 7 的使用	41
3.1 概述	41
3.2 安装与卸载 STEP 7	42
3.3 SIMATIC 管理器	45
3.4 设置 PG/PC	46
3.5 硬件组态	47
3.6 硬件组态的调试	53
3.7 离线/在线程序块的比较	56
3.8 利用变量表调试	56
3.9 PLCSIM 简介	59
第 4 章 编程语言与指令系统	61
4.1 STEP 7 的编程语言	61
4.2 S7-300 指令基础	62
4.3 位逻辑指令	69
4.4 定时器与计数器指令	76
4.5 字逻辑指令	84
4.6 控制指令	88

4.7 PLC 控制系统的设计与应用	91
第 5 章 组织块及系统功能块的使用	106
5.1 组织块	106
5.2 循环处理的主程序 OB1	107
5.3 日期时间中断组织块 (OB10~OB17)	108
5.4 延时中断组织块 (OB20~OB24)	111
5.5 循环中断组织块 (OB30~OB38)	112
5.6 硬件中断组织块 (OB40~OB47)	115
5.7 启动组织块 (OB100~OB102)	116
5.8 结构化编程	117
5.9 数据块中的数据存储	119
5.10 功能和功能块编程及调用举例	120
第 6 章 PLC 控制系统的软件设计方法	130
6.1 梯形图的经验设计法与继电器电路转换法	130
6.2 顺序功能图	135
6.3 顺控器设计举例	137
6.4 S7 GRAPH 语言及其应用	145
第 7 章 SIMATIC S7 PLC 的通信技术	155
7.1 计算机通信原理	155
7.2 SIMATIC 通信网络	159
7.3 MPI 通信技术	160
7.4 PROFIBUS 通信技术	168
7.5 工业以太网	183
7.6 S7 与 WinCC 的通信	185
第 8 章 西门子 S7-300/400 在模拟量控制系统中的应用	195
8.1 数字 PID 控制器	195
8.2 PID 控制器的数字化	196
8.3 连续 PID 控制器 SFB41	198
8.4 脉冲发生器 SFB43	202
8.5 PID 控制器参数的整定方法	205
第 9 章 实验实训	209
9.1 基本指令练习	209
9.2 综合实训	219
9.3 组织块及系统功能实训	233
附录 S7-300/400 指令一览表	279
参考文献	284

绪 论

0.1 可编程控制器的产生与定义

世界上第一台可编程序控制器产生于 1969 年,是由当时美国数字设备公司(DEC)为美国通用汽车公司(GM)研制开发的,成功应用于汽车生产线上,被人们称为可编程序逻辑控制器(Programmable Logic Controller, PLC)。

当时,GM 公司为适应世界上汽车型号不断更新的形势,以求在激烈的竞争中取得优势,设想试制一种尽可能减少因汽车型号改变而需要重新设计汽车装配线上各种控制继电器线路的方法,以降低生产成本,缩短新产品的开发时间,提出了 10 项指标:

- (1) 编程简单,现场可修改程序;
- (2) 维护方便,采用插件式结构;
- (3) 可靠性高于继电器控制系统;
- (4) 体积小于继电器控制系统;
- (5) 数据可以直接送入计算机;
- (6) 成本可与继电器系统竞争;
- (7) 输入可为市电;
- (8) 输出可为市电,能直接驱动电磁阀、交流接触器等;
- (9) 通用性强、易于扩展;
- (10) 用户存储器大于 4KB。

美国数字设备公司(DEC)根据这 10 项指标,于 1969 年研制出第一台可编程控制器,型号为 PDP-14,并安装在 GM 公司的汽车装配线上,替代了传统的继电器控制盘,取得了明显的效果。它的开创性意义在于引入了程序控制功能,为计算机技术在工业控制领域的应用开辟了空间。

在 20 世纪 70 年代,随着电子及计算机技术的发展,出现了微处理器和微计算机,并被应用于 PLC 中,使其具备了逻辑控制、运算、数据分析、处理以及传输等功能。电气制造商协会(National Electrical Manufacturers Association, NEMA)于 1980 年正式命名其为可编程序控制器(Programmable Controller, PC)。为与个人计算机(Personal Computer, PC)相区别,同时也使用其早期名称 PLC,国际电工技术委员会(International Electrotechnical Commission, IEC)分别于 1982 年 11 月和 1985 年 1 月颁布了 PLC 的第一稿和第二稿标准。以后 PLC 开始向小型化、高速度、高性能、高可靠性方面发展,并形成多种系列产品,编程语言也不断丰富,使其在 20 世纪 80 年代工业控制领域中占据着主导地位。

国际电工委员会(IEC)于 1985 年对可编程控制器作了如下定义:可编程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指令,并通过数字式和模拟式的输入和输出,控制各种类型的机械或生产过程。可编程控制器及其有关设备,都

应按易于与工业控制系统形成一个整体,并易于扩充其功能的原则设计。

事实上,近年来,PLC 技术发展很快,每年都推出很多新产品,其功能已超出上述定义的范围。

可编程控制器是以微处理器为基础,综合计算机技术与自动控制技术为一体的工业控制产品,是在硬接线逻辑控制技术和计算机技术的基础上发展起来的。通常把 PLC 认为是由等效的继电器、定时器、计数器等元件组成的装置。

PLC 是计算机家族中的一员,是为工业控制应用而设计制造的。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。PLC 已经广泛应用在各种机械设备和生产过程的自动化控制系统中,PLC 在其他领域,例如在民用和家庭自动化设备中,应用也得到了迅速的发展。

0.2 PLC 的主要特点及应用领域

0.2.1 PLC 的主要特点

1. 可靠性高,抗干扰能力强

在传统的继电器控制系统中,使用了大量的中间继电器、时间继电器等,由于器件的老化、脱焊、触点的抖动、接触不良等现象,大大降低了系统的可靠性。而在 PLC 控制系统中,大量的开关动作是由无触点的半导体电路完成的,即 PLC 用软件代替继电器控制系统中大量的中间继电器和时间继电器,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等原因造成的故障。S7-300/400 具有极强的故障诊断能力。

其中,高可靠性表现在:

(1) 所有的 I/O 接口电路均采用光电隔离,使工业现场的外电路与 PLC 内部电路之间电气上隔离。

(2) 各输入端均采用阻—容滤波器,其滤波时间常数一般为 10~20ms。

(3) 各模块均采用屏蔽措施,以防止辐射干扰。

(4) 采用性能优良的开关电源。

(5) 对采用的器件进行严格的筛选。

(6) 具有良好的自诊断功能,一旦电源或其他软、硬件发生异常情况,CPU 立即采用有效措施,以防止故障扩大。

(7) 大型 PLC 还可以采用由双 CPU 构成冗余系统或有三 CPU 构成表决系统,使可靠性更进一步提高。

2. 丰富的 I/O 接口模块

PLC 针对不同的工业现场信号,如交流或直流、开关量或模拟量、电压或电流、脉冲或电位、强电或弱电等,有相应的 I/O 模块与工业现场的器件或设备(如按钮、行程开关、接近开关、传感器及变送器、电磁线圈、控制阀等)直接连接。另外,为了提高操作性能,它还有多种人一机对话的接口模块;并且为了组成工业局部网络,它还有多种通信联网的接口模块等。

3. 采用模块化结构

为了适应各种工业控制需要,除了整体式的小型 PLC 以外,绝大多数 PLC 均采用模块

化结构。PLC 的各个部件,包括 CPU、电源、I/O 等,均采用模块化设计,由机架及电缆将各模块连接起来,系统的规模和功能可根据用户的需要自行组合。

4. 编程方法简单易学

梯形图是使用得最多的 PLC 的编程语言,其指令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,易学易用,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,并用来编制用户程序。

5. 拆装简单,维修方便

PLC 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。有些模块上均有运行和故障指示装置,便于用户了解运行情况和查找故障。由于采用模块化结构,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。

0.2.2 PLC 的应用领域

目前,PLC 在国内外已广泛应用于钢铁、石油、化工、电力、建材、机械制造、汽车、轻纺、交通运输、环保及文化娱乐等各个行业,其应用范围不断扩大,主要有以下几个方面:

1. 开关量的逻辑控制

这是 PLC 最基本、最广泛的应用领域,它取代传统的继电器控制,实现逻辑控制、顺序控制,既可用于单台设备的控制,也可用于多机群控及自动化流水线,如注塑机、印刷机、订书机械、组合机床、磨床、包装生产线、电镀流水线等。

2. 模拟量控制

在工业生产过程当中,有许多连续变化的量(如温度、压力、流量、液位和速度等)是模拟量,为了使可编程控制器处理模拟量,必须实现模拟量(Analog)和数字量(Digital)之间的 A/D 转换及 D/A 转换。PLC 厂家都生产配套的 A/D 和 D/A 转换模块,使可编程控制器用于模拟量控制。

3. 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、双轴、三轴和多轴的位置控制,使运动控制与顺序控制功能有机结合在一起。PLC 的运动控制功能广泛用于各种机械,例如金属切削机床、金属成形机械、装载机械、机器人、电梯等场合。

4. 过程控制

闭环过程控制是指对温度、压力、流量等模拟量的闭环控制。作为工业控制计算机,PLC 能编制各种各样的控制算法程序,完成闭环控制。PID 调节是一般闭环控制系统中用得较多的调节方法。大中型 PLC 都有 PID 模块,目前许多小型 PLC 也具有此功能模块。PID 处理一般是运行专用的 PID 子程序,过程控制在冶金、化工、热处理、锅炉控制等场合有非常广泛的应用。

5. 数据处理

现代 PLC 具有数学运算(含矩阵运算、函数运算、逻辑运算)、数据传送、数据转换、排序、查表、位操作等功能,可以完成数据的采集、分析及处理。这些数据可以与存储在存储器中的参考值比较,完成一定的控制操作,也可以利用通信功能传送到别的智能装置,或将它们打印制表。数据处理一般用于大型控制系统(如无人控制的柔性制造系统),也可用于

过程控制系统(如造纸、冶金、食品工业中的一些大型控制系统)。

6. 通信及联网

PLC 通信含 PLC 间的通信及 PLC 与其他智能设备间的通信。随着计算机控制的发展,工厂自动化网络发展得很快,各 PLC 厂商都十分重视 PLC 的通信功能,纷纷推出各自的网络系统。新近生产的 PLC 都具有通信接口,通信非常方便,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。

2. 特殊功能

PLC 不需要专门的 I/O 接口,可以在各种工业环境中直接运行。有些特殊 I/O 接口,如与 PLC 相应的 I/O 接口,即可接入运行。有些特殊 I/O 接口,如与 PLC 相应的 I/O 接口,即可接入运行。有些特殊 I/O 接口,如与 PLC 相应的 I/O 接口,即可接入运行。有些特殊 I/O 接口,如与 PLC 相应的 I/O 接口,即可接入运行。

0.2.2 PLC 的应用领域

目前,PLC 在国内外已广泛应用于冶金、机械、轻工、纺织、化工、交通、环保及文化娱乐等各个行业,其应用范围不断扩大,主要有以下几个方面:

1. 开关量的逻辑控制

这是 PLC 最基本、最广泛的应用领域。它取代传统的继电器控制,实现逻辑控制、顺序控制、联锁控制等。也可用于单机控制及自动控制系统,如注塑机、印刷机、自动机床、组合机床、磨床、包装机等。

2. 模拟量控制

在工业生产过程中,有许多连续变化的物理量(如温度、压力、流量、液位和速度等)是模拟量。为了使 PLC 能对这些模拟量进行控制,必须安装模拟量(A/D 和 D/A 转换)接口。PLC 厂家通常都提供 A/D 和 D/A 转换接口,使 PLC 能对这些模拟量进行控制。

3. 运动控制

PLC 使用专用的运动控制模块,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、双轴、三轴和全轴的位置控制、速度控制和加速度控制。PLC 的运动控制功能广泛应用于各种机械,例如金属切削机床、金属成型机械、包装机械、机器人、电梯等。

4. 过程控制

过程控制是指对温度、压力、流量等连续变化的物理量进行控制。作为工业控制计算机,PLC 能编制各种控制算法程序,实现闭环控制。PID 控制是一种闭环控制系统中用得最多的调节方法。大中型 PLC 都有 PID 模块,目前许多小型 PLC 也具有此功能模块。PID 控制一般运行专用的 PID 子程序,过程控制在冶金、化工、热处理、锅炉控制等场合有非常广泛的应用。

5. 数据处理

现代 PLC 具有算术运算(含矩阵运算)、逻辑运算、移位运算、数据传送、数据比较、排序、查表、线性插补等功能,可以完成数据的采集、分析及处理。这些数据可以由传感器采集,也可以通过通信功能从其他智能设备中采集。完成一定的逻辑操作,也可以利用通信功能将数据传送到其他智能设备中。将它们的打印出来,数据报表一般用于大型控制系统(如无人控制的柔性制造系统),也可用于

第 1 章 可编程控制器工作原理

1.1 可编程控制器的组成及各部分功能

PLC 的硬件结构图如图 1-1 所示。

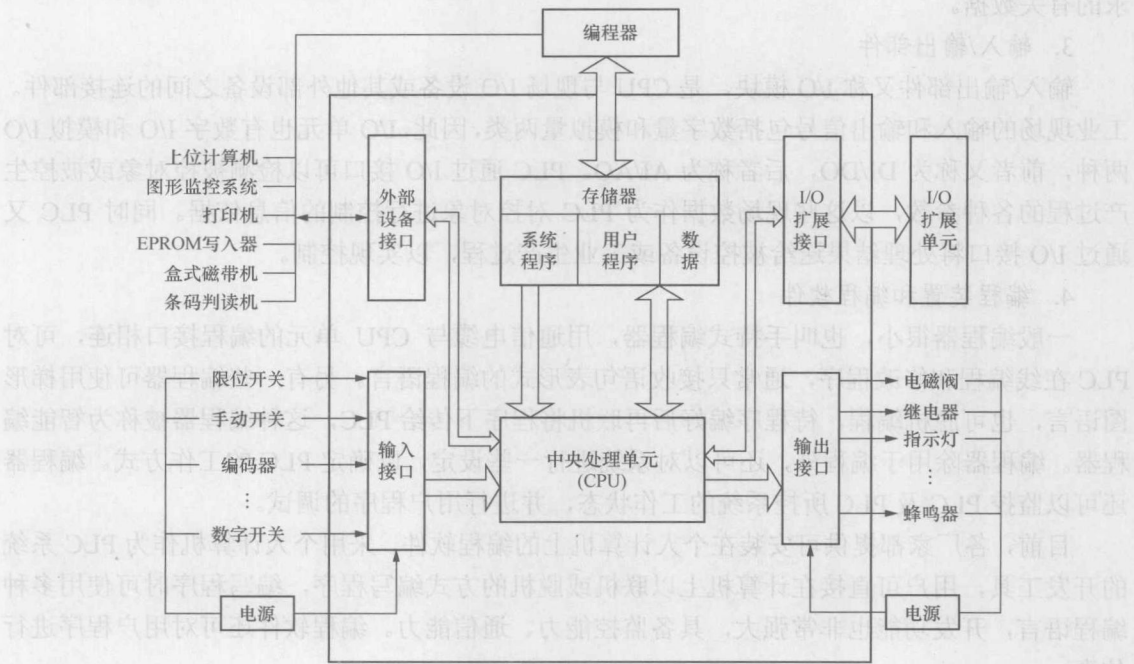


图 1-1 PLC 硬件结构图

PLC 主要由中央处理单元、输入接口、输出接口、通信接口等部分组成，其中 CPU 是 PLC 的核心，I/O 部件是连接现场设备与 CPU 之间的接口电路，通信接口用于与编程器和上位机连接。对于整体式 PLC，所有部件都装在同一机壳内；对于模块式 PLC，各功能部件独立封装，称为模块或模板，各模块通过总线连接，安装在机架或导轨上。不同厂商生产的不同系列产品，在每个机架上可插放的模块数是不同的，一般为 3~10 块。可扩展的机架数也不同，一般为 2~8 个机架。基本机架与扩展机架之间的距离不宜太长，一般不超过 10m。

1. 中央处理单元 CPU

CPU 通过输入装置读入外设的状态，由用户程序去处理，并根据处理结果通过输出装置去控制外设。一般的中型可编程控制器多为双微处理器系统：一个是字处理器，它是主处理器，由它处理字节操作指令，控制系统总线、内部计数器、内部定时器，监视扫描时间，统一管理编程接口，同时协调位处理器及输入/输出；另一个为位处理器，也称布尔处理器，它是从处理器，它的主要作用是处理位操作指令和在机器操作系统的管理下实现 PLC 编程语言向机器语言转换。CPU 处理速度是指 PLC 执行 1000 条基本指令所花费的时间。

2. 存储器

存储器主要存放系统程序、用户程序及工作数据。PLC 所用的存储器基本上由 PROM、EPROM、EEPROM 及 RAM 等组成。

PLC 配有系统程序存储器和用户程序存储器。系统程序存储器用来存储厂家编写的系统程序,系统程序在出厂时已经被固化在 PROM 或 EPROM 中,不需要用户干预,用户不能访问或修改,PLC 的所有功能都是在系统程序的管理下实现的。用户程序存储器用来存储用户通过编程设备输入的用户程序,用户程序存储器一般分为程序存储区和数据存储器区,程序存储区用于存储用户程序;数据存储器区用于存储输入、输出与触点线圈的状态以及特殊功能要求的有关数据。

3. 输入/输出部件

输入/输出部件又称 I/O 模块,是 CPU 与现场 I/O 设备或其他外部设备之间的连接部件。工业现场的输入和输出信号包括数字量和模拟量两类,因此,I/O 单元也有数字 I/O 和模拟 I/O 两种,前者又称为 DI/DO,后者称为 AI/AO。PLC 通过 I/O 接口可以检测被控对象或被控生产过程的各种参数,以这些现场数据作为 PLC 对控对象进行控制的信息依据。同时 PLC 又通过 I/O 接口将处理结果送给被控设备或工业生产过程,以实现控制。

4. 编程装置和编程软件

一般编程器很小,也叫手持式编程器,用通信电缆与 CPU 单元的编程接口相连,可对 PLC 在线编程和修改程序,通常只接收语句表形式的编程语言。另有一些编程器可使用梯形图语言,也可脱机编程,待程序编好后再联机将程序下传给 PLC,这种编程器被称为智能编程器。编程器除用于编程外,还可以对系统进行一些设定,以确定 PLC 的工作方式。编程器还可以监控 PLC 及 PLC 所控系统的工作状态,并进行用户程序的调试。

目前,各厂家都提供可安装在个人计算机上的编程软件,采用个人计算机作为 PLC 系统的开发工具,用户可直接在计算机上以联机或脱机的方式编写程序,编写程序时可使用多种编程语言,开发功能也非常强大,具备监控能力、通信能力。编程软件还可对用户程序进行仿真。

5. 电源部件

电源部件将外界提供的电源转换成 PLC 的工业电源后,提供给 PLC。有些电源部件也可以作为负载电源,通过 PLC 的 I/O 接口向负载提供 24V DC 电源。PLC 的电源一般采用开关电源,输入电压范围宽,抗干扰能力强。电源部件的输入与输出之间有可靠的隔离,以确保外界的扰动不会影响到 PLC 的正常工作。

6. 通信接口

在 PLC 的 CPU 或专用的通信模块上,集成有 RS-232C 口或 RS-422 口,可与 PLC、上位机、远程 I/O、监视器、编程器等外部设备相连,实现 PLC 与上述设备之间的数据及信息交换,组成局域网络或集中管理、分散控制的多级分布式控制系统。

1.2 PLC 的工作原理

1. PLC 的循环处理过程

CPU 中的程序分为系统程序和用户程序。操作系统用来完成 PLC 的启动、刷新过程映像

寄存器、调用用户程序、处理中断和错误、管理存储区和通信等任务。

PLC 的循环处理过程如图 1-2 所示。

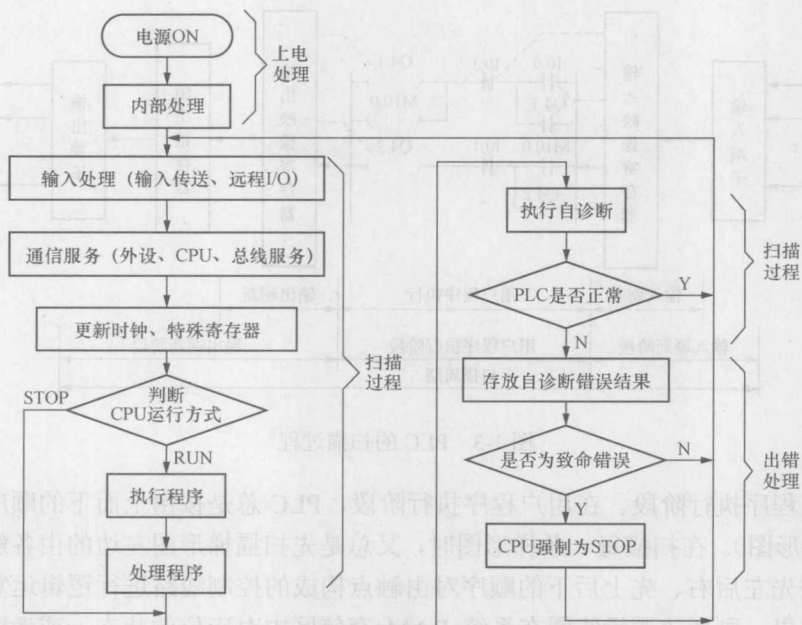


图 1-2 PLC 的循环处理过程

PLC 得电或由 STOP 切换到 RUN 模式时，CPU 执行启动操作，清除没有保持功能的位存储器、定时器和计数器，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。之后，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。循环扫描的各个阶段的任务如下：

(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，操作系统执行所有挂起的任务，例如下载或删除块、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。

2. PLC 的扫描过程

当 PLC 投入运行后，其工作过程一般分为三个阶段，即输入采样、用户程序执行和输出刷新三个阶段。这三个阶段构成为一个扫描周期。在整个运行期间，PLC 的 CPU 以一定的扫描速度重复执行上述三个阶段，如图 1-3 所示。

(1) 输入刷新阶段。在输入刷新阶段，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 映像区中的相应的单元内。输入刷新结束后，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。因此，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。

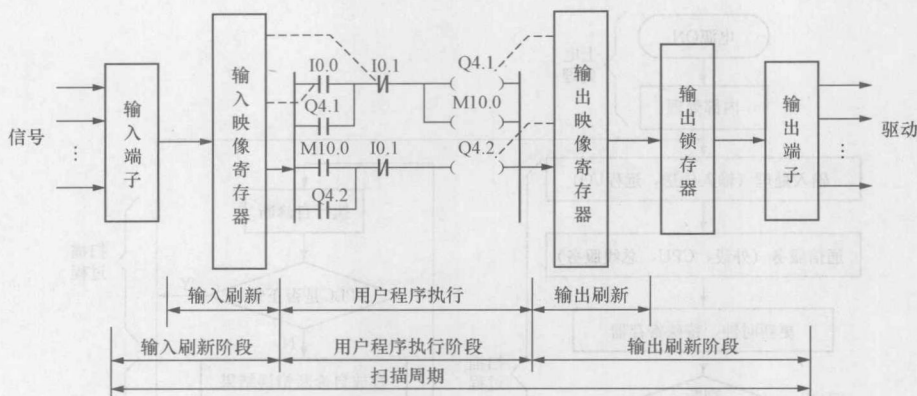


图 1-3 PLC 的扫描过程

(2) 用户程序执行阶段。在用户程序执行阶段，PLC 总是按由上而下的顺序依次地扫描用户程序（梯形图）。在扫描每一条梯形图时，又总是先扫描梯形图左边的由各触点构成的控制线路，并按先左后右、先上后下的顺序对由触点构成的控制线路进行逻辑运算，然后根据逻辑运算的结果，刷新该逻辑线圈在系统 RAM 存储区中对应位的状态；或者刷新该输出线圈在 I/O 映像区中对应位的状态；或者确定是否要执行该梯形图所规定的特殊功能指令。

在用户程序执行过程中，只有输入点在 I/O 映像区内的状态和数据不会发生变化，而其他输出点和软设备在 I/O 映像区或系统 RAM 存储区内的状态和数据都有可能发生变化，而且排在上面的梯形图，其程序执行结果会对排在下面的凡是用到这些线圈或数据的梯形图起作用；相反，排在下面的梯形图，其被刷新的逻辑线圈的状态或数据只能到下一个扫描周期才能对排在其上面的程序起作用。

(3) 输出刷新阶段。当扫描用户程序结束后，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外设。这时，才是 PLC 的真正输出。同样的若干条梯形图，其排列次序不同，执行的结果也不同。另外，采用扫描用户程序的运行结果与继电器控制装置的硬逻辑并行运行的结果有所区别。当然，如果扫描周期所占用的时间对整个运行来说可以忽略，那么二者之间就没有什么区别了。

3. 循环扫描时间

一般来说，PLC 的扫描周期是指操作系统执行一次图 1-2 所示的循环处理操作所需用的时间，包括自诊断、通信等，即一个扫描周期等于自诊断、通信、输入采样、用户程序执行、输出刷新等所有时间的总和。循环扫描时间与用户指令的长短、指令的种类和 CPU 执行指令的速度有关，当用户指令较长时，指令执行时间在扫描周期中占相当大的比例。

在 PLC 处于运行模式时，利用编程软件的监控功能，在 OB1 的局部数据表中，可以获得最大的循环时间、最小循环时间和上一次的循环时间。

循环时间往往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、传输和传输块、压缩用户程序存储器、读/写微存储卡（MMC）等。

4. PLC 的响应滞后现象

PLC 有很多优点,但也有不足之处,最明显的是输入/输出有响应滞后现象。PLC 总的响应延迟时间一般只有几毫秒到几十毫秒,对于一般的工业设备来说,这些滞后现象是完全允许的,而对某些设备,需用输出对输入作出快速反应,此时可采用快速响应模块、高速计数模块以及中断处理等措施来尽量减少滞后时间。

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所控制的外部输出信号发生变化的时刻之间的时间间隔,它由输入电路滤波时间、输出电路的滞后时间和因扫描工作方式产生的滞后时间三部分组成。

造成输入/输出响应滞后的原因主要有两个:

(1) 执行程序按工作周期进行,每一次扫描的工作周期都按输入刷新、程序执行、输出刷新三个阶段进行,其最大和最小 I/O 响应时间如图 1-4 所示。

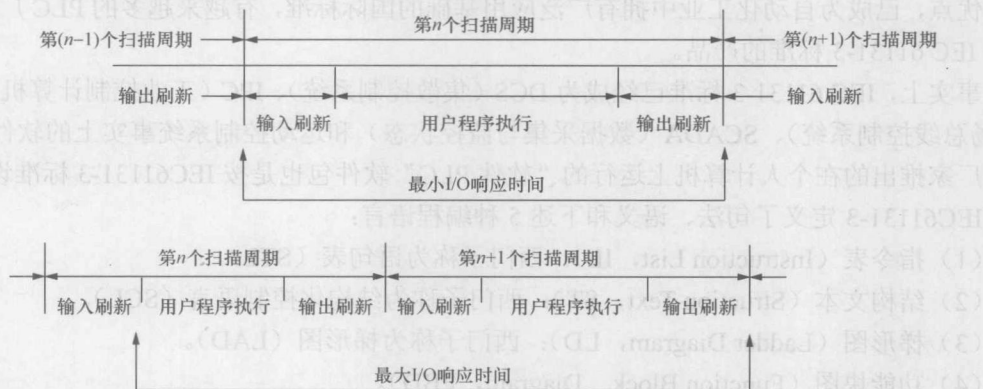


图 1-4 PLC 的 I/O 响应滞后

(2) 输入滤波器电路的滞后和输出继电器的机械滞后作用等。

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,其典型值为 10ms 左右。

输出模块的滞后时间与模块类型有关:继电器型输出电路的滞后时间一般在 10ms 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 1ms,负载由通电到断电时的最大滞后时间为 10ms;晶体管型输出电路的滞后时间一般在 1ms 以下。

1.3 PLC 的编程语言

PLC 中有多种程序设计语言,它们是梯形图语言、布尔助记符语言、功能表图语言、功能模块图语言及结构化语句描述语言等。梯形图语言和布尔助记符语言是基本程序设计语言,它通常由一系列指令组成,用这些指令可以完成大多数简单的控制功能(例如代替继电器、计数器、计时器完成顺序控制和逻辑控制等),通过扩展或增强指令集,它们也能执行其他的基本操作。

功能表图语言和结构化语句描述语言是高级的程序设计语言,它可根据需要去执行更有

效的操作,例如模拟量的控制、数据的操纵、报表的打印和其他基本程序设计语言无法完成的功能。功能模块图语言采用功能模块图的形式,通过软连接的方式完成所要求的控制功能,它不仅在 PLC 中得到了广泛的应用,在集散控制系统的编程和组态时也常常被采用,由于它具有连接方便、操作简单、易于掌握等特点,为广大工程设计和应用人员所喜爱。

根据 PLC 应用范围,程序设计语言可以组合使用,常用的程序设计语言是:梯形图程序设计语言;布尔助记符程序设计语言(语句表);功能表图程序设计语言;功能模块图程序设计语言;结构化语句描述程序设计语言;梯形图与结构化语句描述程序设计语言;布尔助记符与功能表图程序设计语言;布尔助记符与结构化语句描述程序设计语言。

1.3.1 PLC 编程语言的国际标准

IEC(国际电工委员会)是为电子技术的所有领域制定全球标准的国际组织。IEC 61131 是 PLC 的国际标准,其中的 IEC 61131-3 部分是 PLC 的编程语言标准。由于 IEC 61131-3 的诸多优点,已成为自动化工业中拥有广泛应用基础的国际标准,有越来越多的 PLC 厂家提供符合 IEC 61131-3 标准的产品。

事实上,IEC 61131-3 标准已经成为 DCS(集散控制系统)、IPC(工业控制计算机)、FCS(现场总线控制系统)、SCADA(数据采集与监控状态)和运动控制系统事实上的软件标准。有的厂家推出的在个人计算机上运行的“软件 PLC”软件包也是按 IEC 61131-3 标准设计的。

IEC 61131-3 定义了句法、语义和下述 5 种编程语言:

- (1) 指令表(Instruction List, IL): 西门子称为语句表(STL)。
- (2) 结构文本(Structural Text, ST): 西门子称为结构化控制语言(SCL)。
- (3) 梯形图(Ladder Diagram, LD): 西门子称为梯形图(LAD)。
- (4) 功能块图(Function Block Diagram, FBD)。
- (5) 顺序功能图(Sequential Function Chart, SFC): 对应于西门子的 S7-GRAPH 编程语言。

1.3.2 STEP 的编程语言

STEP 7 是 S7-300/400 系列 PLC 应用设计软件包,所支持的 PLC 编程语言非常丰富,该软件的标准版支持 STL(语句表)、LAD(梯形图)及 FBD(功能块图)3 种基本编程语言,并且在 STEP 7 中可以相互转换;专业版附加对 GRAPH(顺序功能图)、SCL(结构化控制语言)、HiGraph(图形编程语言)、CFC(连续功能图)等编程语言的支持。

在 STEP 7 的编程软件中,如果程序块没有错误,并且被正确地划分为程序段,梯形图、语句表和功能块图可以相互转换。用语句表编写的程序不一定能转换为梯形图,不能转换的程序仍然保留语句表的形式。

第2章 S7-300/400 的体系结构和硬件组态

2.1 S7 系列的体系结构

西门子公司的 PLC 产品有 SIMATIC S7、M7 和 C7 等几大系列。S7 系列是传统意义的 PLC 产品，是 SIMATIC（西门子自动化）自动控制系统的关键部件。

S7-200 是针对低性能要求的小型 PLC，是在美国德州仪器公司的小型 PLC 的基础上发展起来的，其编程软件为 STEP7-Micro/WIN 32。S7-300/400 的前身是西门子公司的 S5 系列 PLC，S7-300 是针对中等性能要求的模块式中小型 PLC，最多可以扩展 32 个模块；S7-400 是用于高性能要求的大型 PLC，可以扩展 300 多个模块，S7-300/400 的编程软件为 STEP 7。S7-200 和 S7-300/400 虽然有许多共同之处，但是在指令系统、程序结构和编程软件等方面均有相当大的差异。S7-200 和 S7-300/400 可以接入 MPI（多点接口）、工业以太网、现场总线 AS-i 和 PROFIBUS 等通信网络。

1. S7-300 的系统结构

S7-300 是模块化的中小型 PLC，如图 2-1 所示，适用于中等性能的控制要求。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。

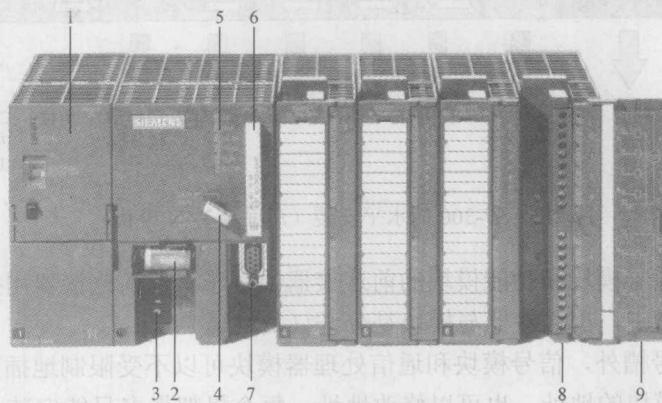


图 2-1 S7-300 PLC

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

S7-300 的每个 CPU 都有一个编程用的 RS-485 接口，使用西门子的 MPI（多点接口）通信协议。有的 CPU 还带有集成的现场总线 PROFIBUS-DP 接口或 PtP（点对点）串行通信接口。S7-300 不需要附加任何硬件、软件和编程，就可以建立一个 MPI 网络，通过 PROFIBUS-DP 接口可以建立一个 DP 网络。

S7-300 是一种通用型的 PLC，能适合自动化工程中的各种应用场合，尤其是在生产制造工