

西门子PLC

通信与控制应用编程实例

李江全 严海娟 刘姣娣 邓红涛 编著



- 实例源程序
- 程序运行录屏
- 系统测试录像
- 软硬件资源



中国电力出版社
CHINA ELECTRIC POWER PRESS

西门子

通信与控制应用编程实例

李江全 严海娟 刘姣娣 邓红涛 编著



YZLI0890108352



中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书从应用的角度全面系统地介绍了西门子 S7-200 系列 PLC 通信技术。全书共分 10 章, 分别为: PLC 概述、西门子 S7-200 系列 PLC 简介、计算机串行通信概述、西门子 S7-200 系列 PLC 数据通信基础、PLC 与 PLC 通信编程实例、S7-200 PLC 与 PC 通信之模拟量输入、S7-200 PLC 与 PC 通信之模拟量输出、S7-200 PLC 与 PC 通信之开关量输入、S7-200 PLC 与 PC 通信之开关量输出、S7-200 PLC 与其他智能装置的通信实例。

本书内容丰富, 可供各类自动化、计算机应用、机电一体化等专业的大学生、研究生学习西门子 S7-200 系列 PLC 通信技术, 也可供计算机控制系统研发的工程技术人员参考。

为方便读者学习, 本书提供超值配套光盘, 内容包括实例源程序、程序运行录屏、系统测试录像、软硬件资源等。

图书在版编目 (CIP) 数据

西门子 PLC 通信与控制应用编程实例/李江全等编著. —北京: 中国电力出版社, 2011. 7

ISBN 978-7-5123-1990-5

I. ①西… II. ①李… III. ①可编程序控制器—程序设计
IV. ①TM571.6

中国版本图书馆 CIP 数据核字 (2011) 第 157009 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>)

航远印刷有限公司印刷

各地新华书店经售

*

2012 年 1 月第一版 2012 年 1 月北京第一次印刷
787 毫米×1092 毫米 16 开本 17.25 印张 420 千字
印数 0001—3000 册 定价 38.00 元 (含 1DVD)

敬告读者

本书封面贴有防伪标签, 加热后中心图案消失
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

可编程序逻辑控制器（简称 PLC）主要是为现场控制而设计的，其人机界面主要是开关、按钮、指示灯等。因其良好的适应性和可扩展能力而得到越来越广泛的应用。采用 PLC 的控制系统或装置具有可靠性高、易于控制、系统设计灵活、能模拟现场调试、编程使用简单、性价比高、有良好的抗干扰能力等特点。但是，PLC 也有不易显示各种实时图表、曲线和汉字、无良好的用户界面、不便于监控等缺陷。

现代 PLC 的通信功能很强，可以实现 PLC 与计算机、PLC 与 PLC、PLC 与其他智能控制装置之间的通信联网。PLC 与计算机联网，可以发挥各自所长。PLC 用于现场设备的直接控制，作为下位机，执行可靠有效的分散控制。计算机作为上位机可以提供良好的人机界面，进行系统的监控和管理，进行程序编制、参数设定和修改、数据采集等，既能保证系统性能，又能使系统操作简便，便于生产过程的有效监督。PLC 与 PLC 联网能够扩大控制地域，提高控制规模，还可以实现 PLC 之间的综合协调控制；PLC 与智能控制装置（如智能仪表）联网，可以有效地对智能装置实施管理，充分发挥这些装置的效益。除此之外，联网可极大节省配线，方便安装，提高可靠性，简化系统维护等。因此，要求 PLC 与计算机、PLC、其他智能控制装置之间具有稳定、可靠的数据通信。

本书从应用的角度全面系统地介绍了西门子 S7-200 系列 PLC 通信技术。内容包括 PLC 数据通信目的、类型和连接方式，个人计算机与 PLC 的通信方法、通信内容和通信方式，PC 编程软件的串行通信开发工具；S7-200 系列 PLC 的数据通信协议及应用，S7-200 系列 PLC 的特殊功能模块，PLC 与 PLC、PLC 与其他智能装置的通信编程实例；应用 S7-200 系列 PLC 的 PPI 协议与自由端口模式，采用 Visual Basic、LabWindows/CVI 和 KingView（组态王）软件编写 PC 与 S7-200 系列 PLC 通信程序，实现 PLC 模拟量输入与输出、开关量输入与输出。

本书内容丰富，可供各类自动化、计算机应用、机电一体化等专业的大学生、研究生学习西门子 S7-200 系列 PLC 通信技术，也可供计算机控制系统研发的工程技术人员参考。

为方便读者学习，本书提供超值配套光盘，内容包括分实例源程序、程序运行录屏、系统测试录像、软硬件资源等。

本书由石河子大学刘姣娣编写第 1~3 章，严海娟编写第 4、5 章，邓红涛编写第 6、7 章，李江全编写第 8~10 章，全书由李江全教授担任主编并统稿，刘姣娣、严海娟、邓红涛担任副主编。参与编写、程序设计、插图绘制和文字校核工作的人员还有刘恩博、田敏、郑瑶、朱东芹、李宏伟、郑重、任玲、王洪坤、汤智辉、胡蓉、张茜等老师，编者借此机会对他们致以深深的谢意。

由于编者水平有限，书中难免存在不妥或错误之处，恳请广大读者批评指正。

编 者

目 录

前言

第1章 PLC 概述	1
1.1 PLC 的硬件组成与工作原理	1
1.1.1 PLC 的定义	1
1.1.2 PLC 的硬件组成	2
1.1.3 PLC 的工作原理	3
1.1.4 PLC 的操作模式	6
1.2 PLC 的软件组成与编程语言	6
1.2.1 PLC 的软件组成	6
1.2.2 PLC 的编程语言	7
1.2.3 PLC 的程序结构	9
1.3 PLC 的技术指标与功能特点	10
1.3.1 PLC 的分类	10
1.3.2 PLC 的技术指标	11
1.3.3 PLC 的功能与特点	12
1.3.4 PLC 与工业 PC 及 DCS 的比较	14
第2章 西门子 S7-200 系列 PLC 简介	16
2.1 S7-200 系列 PLC 的基本组成	16
2.1.1 存储器	16
2.1.2 I/O 模块	17
2.1.3 工作过程	18
2.1.4 编程软件和显示面板	20
2.1.5 S7-200 PLC 的特点	21
2.2 S7-200 系列 PLC 的功能模块	22
2.2.1 S7-200 系列 PLC 的 CPU 模块	22
2.2.2 S7-200 系列 PLC 的数字量扩展模块	26
2.2.3 S7-200 系列 PLC 的模拟量扩展模块	28
2.2.4 S7-200 系列 PLC 的温度扩展模块	33
第3章 计算机串行通信概述	35
3.1 串行通信的基本概念	35
3.1.1 并行通信与串行通信	35

3.1.2 串行通信工作模式	36
3.1.3 异步传输与同步传输	37
3.1.4 串行通信的基本参数	38
3.2 串行通信的接口标准	39
3.2.1 RS-232C 接口标准	39
3.2.2 RS-422/485 接口标准	41
3.3 个人计算机中的串行端口	43
3.3.1 查看串行端口信息	43
3.3.2 串口通信线路连接	44
3.3.3 串口通信调试	45
3.3.4 虚拟串口的使用	47
3.4 PC 编程软件的串行通信开发工具	48
3.4.1 西门子 S7-200 PLC 组态王设置	48
3.4.2 VB 串行通信控件 MSComm	49
3.4.3 LabWindows/CVI 串口通信函数	56

第4章 西门子 S7-200 系列 PLC 数据通信基础 **60**

4.1 PLC 数据通信概述	60
4.1.1 PLC 数据通信的目的	60
4.1.2 PLC 数据通信的类型	62
4.1.3 S7-200 PLC 数据通信的连接方式	66
4.1.4 数据在 PLC 存储器中存取的方式	67
4.1.5 PLC 数据通信介质	70
4.2 个人计算机与 PLC 的通信	72
4.2.1 计算机与 PLC 通信的方法与条件	72
4.2.2 计算机与 PLC 的通信内容	73
4.2.3 PLC 控制系统的信号类型	74
4.2.4 计算机与 PLC 通信程序的设计要点与方法	76
4.2.5 PLC 串口通信调试软件及其应用	81
4.3 西门子 S7-200 系列 PLC 的通信协议及应用	83
4.3.1 S7-200 PLC 的通信功能	84
4.3.2 S7-200 PLC 的通信指令	88
4.3.3 PPI 网络及其通信协议	91
4.3.4 自由端口模式	99
4.3.5 Modbus 通信协议	105
4.3.6 USS 通信协议及应用	111
4.3.7 S7-200 PLC 通信部件简介	117

第5章 PLC 与 PLC 通信编程实例 **119**

5.1 S7-200 PLC 与 S7-200 PLC 的通信实例	119
--	------------

5.1.1	S7-200 PLC 之间的 PPI 通信	119
5.1.2	S7-200 PLC 之间的 Modbus 通信	127
5.1.3	S7-200 PLC 之间的以太网通信	129
5.2	S7-200 PLC 与 S7-300 PLC 的通信实例	137
5.2.1	S7-200 与 S7-300 PLC 之间的 MPI 通信	137
5.2.2	S7-200 与 S7-300 PLC 之间的以太网通信	138
5.3	S7-200 PLC 与 FX _{2N} -32MR PLC 的通信实例	143
第6章	S7-200 PLC 与 PC 通信之模拟量输入	147
6.1	系统设计说明	147
6.1.1	设计任务	147
6.1.2	线路连接	147
6.2	采用 PPI 协议编写模拟电压输入程序	148
6.2.1	PLC 端电压输入程序	148
6.2.2	PC 端采用 Visual Basic 实现电压输入	151
6.2.3	PC 端采用 LabWindows/CVI 实现电压输入	154
6.2.4	PC 端采用 KingView 实现电压输入	157
6.3	采用自由端口模式编写模拟电压输入程序	164
6.3.1	PLC 端电压输入程序	164
6.3.2	PC 端采用 Visual Basic 实现电压输入	167
6.3.3	PC 端采用 LabWindows/CVI 实现电压输入	170
第7章	S7-200 PLC 与 PC 通信之模拟量输出	174
7.1	系统设计说明	174
7.1.1	设计任务	174
7.1.2	线路连接	174
7.2	采用 PPI 协议编写模拟电压输出程序	175
7.2.1	PLC 端电压输出程序	175
7.2.2	PC 端采用 Visual Basic 实现电压输出	177
7.2.3	PC 端采用 LabWindows/CVI 实现电压输出	180
7.2.4	PC 端采用 KingView 实现电压输出	183
第8章	S7-200 PLC 与 PC 通信之开关量输入	189
8.1	系统设计说明	189
8.1.1	设计任务	189
8.1.2	线路连接	189
8.2	采用 PPI 协议编写开关量输入程序	190
8.2.1	PC 与西门子 S7-200 PLC 串口通信调试	190
8.2.2	PC 端采用 Visual Basic 实现开关量输入	191

8.2.3	PC 端采用 LabWindows/CVI 实现开关量输入	195
8.2.4	PC 端采用 KingView 实现开关量输入	198
8.3	采用自由端口模式编写开关量输入程序	204
8.3.1	PLC 端开关量输入程序	204
8.3.2	PC 端采用 Visual Basic 实现开关量输入	207
8.3.3	PC 端采用 LabWindows/CVI 实现开关量输入	211
第9章	S7-200 PLC 与 PC 通信之开关量输出	216
9.1	系统设计说明	216
9.1.1	设计任务	216
9.1.2	线路连接	216
9.2	采用 PPI 协议编写开关量输出程序	217
9.2.1	PC 与西门子 S7-200 PLC 串口通信调试	217
9.2.2	PC 端采用 Visual Basic 实现开关量输出	218
9.2.3	PC 端采用 LabWindows/CVI 实现开关量输出	221
9.2.4	PC 端采用 KingView 实现开关量输出	224
9.3	采用自由端口模式编写开关量输出程序	230
9.3.1	PLC 端开关量输出程序	230
9.3.2	PC 端采用 Visual Basic 实现开关量输出	233
9.3.3	PC 端采用 LabWindows/CVI 实现开关量输出	236
第10章	S7-200 PLC 与其他智能装置的通信实例	241
10.1	PLC 与 MODEM 通信	241
10.1.1	实例 1	241
10.1.2	实例 2	249
10.2	PLC 与 GPRS 模块通信	252
10.2.1	任务描述	252
10.2.2	任务实施	253
10.3	PLC 与变频器通信	260
10.3.1	任务描述	260
10.3.2	任务实施	263
10.4	PLC 与条形码阅读器通信	264
10.4.1	任务描述	264
10.4.2	任务实施	265
10.5	PLC 与打印机通信	266
10.5.1	任务描述	266
10.5.2	任务实施	266
参考文献		268

PLC 概 述

可编程序逻辑控制器 (Programmable Logic Controller, 简称 PLC, 有时也简称为可编程控制器, 如图 1-1 所示) 最初用于机械制造行业的顺序控制器, 与集散控制系统是完全不同的两种技术, 其高可靠性是公认的。经过几十年的发展, PLC 增加了许多功能。例如, 通信功能、模拟控制功能、远程数据采集功能。人们很快发现, 用 PLC 构成一个网络是一个不错的选择。现在, 在许多场合利用 PLC 网络构成一个计算机监控系统, 或是将其作为集散控制系统的一个下位机子系统, 此种方案基本上成为首选。

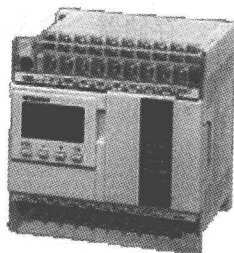


图 1-1 PLC 产品

1.1 PLC 的硬件组成与工作原理

1.1.1 PLC 的定义

现代社会要求制造业对市场需求作出迅速的反应, 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, PLC 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。

PLC 的应用面广、功能强大、使用方便, 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, PLC 在其他领域, 例如在民用和家庭自动化的应用中也得到了迅速的发展。目前 PLC 仍然处于不断的发展之中, 其功能在不断增强, 而且更为开放, 它不但是单机自动化中应用最广的控制设备, 在大型工业网络控制系统中也占有不可动摇的地位。PLC 应用面之广、普及程度之高, 是其他计算机控制设备所无法比拟的。

国际电工委员会 (IEC) 在 1985 年对 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。”从上述定义可以看出, PLC 是一种用程序来改变控制功能的工业控制计算机, 除了能完成各种各样的控制功能外, 还有与其他计算机通信联网的功能。

本书以西门子公司的 S7-200 系列小型 PLC 为讲授对象。S7-200 具有极高的可靠性、丰富的指令集和内置的集成功能、强大的通信能力和品种丰富的扩展模块。S7-200 可以单机运行，用于代替继电器控制系统，也可以用于复杂的自动化控制系统。由于它有极强的通信功能，在网络控制系统中也能充分发挥其作用。

1.1.2 PLC 的硬件组成

可编程序控制器是基于微处理器技术的通用工业自动化控制设备。它采用了计算机的设计思想，实际上就是一种特殊的工业控制专用计算机，只不过它的最主要的功能是数字逻辑控制。因此，PLC 具有与通用的微型个人计算机相类似的硬件结构。PLC 由中央处理器（CPU）、存储器、输入输出接口、智能接口模块和编程器构成，其组成结构如图 1-2 所示。

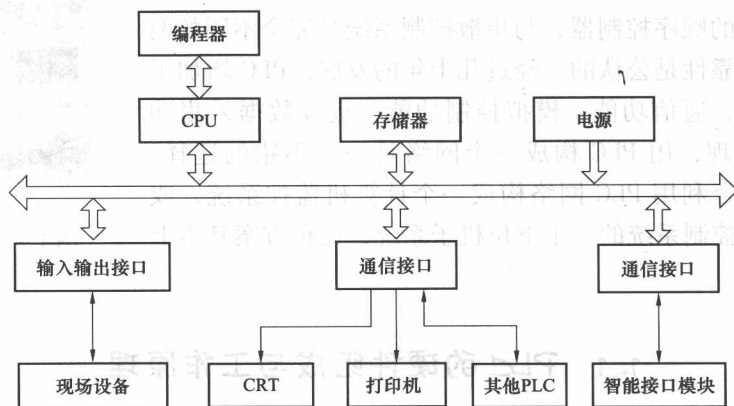


图 1-2 PLC 组成结构

1. 中央处理器（CPU）

中央处理器是整个 PLC 的核心组成部分，是系统的控制中枢。它的主要功能是实现逻辑运算、数学运算，协调控制可编程控制器内部的各部分工作。PLC 的 CPU 内部结构与微型计算机的 CPU 结构基本相同，PLC 的整体性能取决于 CPU 的性能，因此，常用的 CPU 主要是通用的微处理器、单片机或工作速度较快的双极型位片式微处理器。

2. 存储器

存储器主要用于存放系统程序、用户程序以及工作时产生的数据。系统程序是指控制 PLC 完成各种功能的系统管理程序、监控程序、用户逻辑解释程序、标准子程序模块和各种系统参数，由 PLC 生产厂家编写并固化在只读存储器（ROM）中。用户程序指由用户根据工业现场的要求所编写的控制程序，允许用户修改，最终固化并存储于 PLC 中。

PLC 的存储空间根据存储的内容可分为系统程序存储区、系统 RAM 存储区和用户程序存储区。

3. 输入输出接口

输入输出接口是可编程序控制器与现场各种信号相连接的部件，要求它能够处理这些信号并具有抗干扰能力。因此，输入输出接口通常配有电子变换、光电隔离和滤波电路。输入输出接口可分为数字量输入、数字量输出、模拟量输入和模拟量输出。

数字量（开关量）输入信号类型有直流和交流两种，均采用光电隔离器件将现场电信



号与 PLC 内部实现电气上的隔离,同时转换成系统内统一的信号范围。输出接口除了也具有光电隔离外,还具有各种输出方式:有的采用直流输出方式,有的采用交流输出方式,有的采用继电器输出方式等。

模拟量有各种类型,包括 $0 \sim 10V$, $-10 \sim 10V$, $4 \sim 20mA$ 。它们首先要进行信号处理。将输入模拟量转换成统一的电压信号,然后再进行模拟量到数字量的转换,即 A/D 变换。通过采样、保持和多路开关的切换,多个模拟量的 A/D 变换就可以共用一个 A/D 转换器来完成。转换为数字量的模拟量就可以通过光电隔离、数据驱动输入到 PLC 内部。

模拟量的输出是把可编程控制器内的数字量转换成相应的模拟量输出,因此,它是与输入相反的过程。整个过程可分为光电隔离、数/模转换和模拟信号驱动输出等环节。PLC 内的数字量经过光电隔离实现两部分电路上电气隔离,数字量到模拟量的转换由数/模转换器(即 D/A 转换器)完成。转换后的模拟量再经过运算放大器等模拟器件进行相应的驱动,形成现场所需的控制信号。

4. 智能接口模块

为了进一步提高 PLC 的性能,各大 PLC 厂商除了提供以上输入输出接口外,还提供各种专用的智能接口模块,用以满足各种控制场合的要求。智能接口模块是 PLC 系统中的一个较为独立的模块,它们具有自己的处理器和存储器,通过 PLC 内部总线在 CPU 的协调管理下独立地进行工作。智能接口模块既扩展了 PLC 可处理的信号范围,又可使 CPU 能处理更多的控制任务。

智能接口模块包括高速脉冲计数器、定位控制智能单元、PID 调节智能单元、PLC 网络接口、PLC 与计算机通信接口、传感器输入智能单元等。

5. 编程器

编程器用来生成用户程序,并用它来编辑、检查、修改用户程序,监视用户程序的执行情况。手持式编程器不能直接输入和编辑梯形图,只能输入和编辑指令表程序,因此又叫做指令编程器。它的体积小,价格便宜,一般用来给小型 PLC 编程,或者用于现场调试和维护。

使用编程软件可以在计算机屏幕上直接生成和编辑梯形图或指令表程序,并且可以实现不同编程语言之间的相互转换。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。程序可以存盘或打印,还可以通过网络或电话线实现远程编程和传送。

现在的发展趋势是用编程软件取代手持式编程器,西门子 PLC 只用编程软件编程。给 S7-200 编程时,应配备一台安装有 STEP7-Micro/WIN 编程软件的计算机,以及一根连接计算机和 PLC 的 RS-232C/PPI 通信电缆或 USB/PPI 多主站电缆。现在的笔记本电脑一般都没有 RS-232C 通信接口,可以选用 USB/PPI 电缆,用 USB 接口与 PLC 通信。

6. 电源

PLC 使用 AC 220V 电源或 DC 24V 电源。内部的开关电源为各模块提供不同电压等级的直流电源。小型 PLC 可以为输入电路和外部的电子传感器(例如接近开关)提供 DC 24V 电源,驱动 PLC 负载的直流电源一般由用户提供。

1.1.3 PLC 的工作原理

1. PLC 的扫描工作方式

当 PLC 运行时,是通过执行反映控制要求的用户程序来完成控制任务的,需要执行众

多的操作，但 CPU 不可能同时去执行多个操作，它只能按分时操作（串行工作）方式，每一次执行一个操作，按顺序逐个执行。由于 CPU 的运算处理速度很快，所以从宏观上来看，PLC 外部出现的结果似乎是同时（并行）完成的。这种串行工作过程称为 PLC 的扫描工作方式。

扫描工作方式在执行用户程序时，是从第一条程序开始，在无中断或跳转控制的情况下，按程序存储顺序的先后，逐条执行用户程序，直到程序结束。然后再从头开始扫描执行，周而复始重复运行。

PLC 控制系统的工作与继电器控制系统的工作原理明显不同。继电器控制装置采用硬逻辑的并行工作方式，如果某个继电器的线圈通电或断电，那么该继电器的所有动合和动断触点不论处在控制线路的哪个位置上，都会立即同时动作；而 PLC 采用扫描工作方式（串行工作方式），如果某个软继电器的线圈被接通或断开，其所有的触点不会立即动作，必须等扫描到该指令时才会动作。但由于 PLC 的扫描速度快，通常 PLC 与继电器控制装置在 I/O 的处理效果上并没有多大差别。

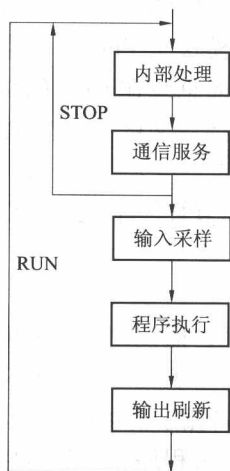


图 1-3 循环扫描工作过程

2. PLC 的扫描工作过程

PLC 的扫描工作过程中除了执行用户程序外，在每次扫描工作过程中还要完成内部处理、通信服务等工作。循环扫描工作过程如图 1-3 所示，整个扫描工作过程包括内部处理、通信服务、输入采样、程序执行、输出刷新五个阶段。整个过程扫描执行一遍所需的时间称为扫描周期，扫描周期与 CPU 运行速度、PLC 硬件配置及用户程序长短有关，典型值为 1 ~ 100ms。

在内部处理阶段，PLC 进行自检，检查内部硬件是否正常，对监视定时器（WDT）复位并完成其他一些内部处理工作。

在通信服务阶段，PLC 与其他智能装置实现通信，响应编程器键入的命令，更新编程器的显示内容等。

当 PLC 处于停止（STOP）状态时，只完成内部处理和通信服务工作。当 PLC 处于运行（RUN）状态时，除完成内部处理和通信服务工作外，还要完成输入采样、程序执行、输出刷新工作。

PLC 的扫描工作方式简单直观，便于程序的设计，并为可靠运行提供了保障。当 PLC 扫描到的指令被执行后，其结果马上就被后面将要扫描到的指令所利用，而且还可通过 CPU 内部设置的监视定时器来监视每次扫描是否超过规定时间，避免由于 CPU 内部故障使程序执行进入死循环。

3. PLC 执行程序的过程

PLC 执行程序的过程分为三个阶段，即输入采样阶段、程序执行阶段和输出刷新阶段。PLC 执行程序过程如图 1-4 所示。

（1）输入采样阶段。在输入采样阶段，PLC 以扫描工作方式按顺序对所有输入端的输入状态进行采样，并存入输入映像寄存器中，此时输入映像寄存器被刷新。接着进入程序处理阶段，在程序执行阶段或其他阶段，即使输入状态发生变化，输入映像寄存器的内容也不

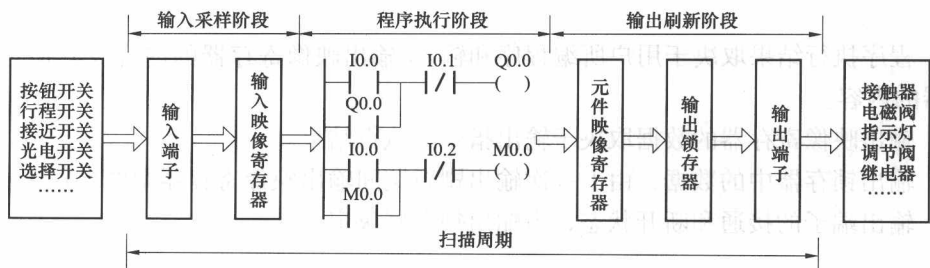


图 1-4 PLC 执行程序过程

会改变，输入状态的变化只有在下一个扫描周期的输入处理阶段才能被采样到。

(2) 程序执行阶段。在程序执行阶段，PLC 对程序按顺序进行扫描执行。若程序用梯形图来表示，则总是按先上后下，先左后右的顺序进行。当遇到程序跳转指令时，则根据跳转条件是否满足来决定程序是否跳转。当指令中涉及输入、输出状态时，PLC 从输入映像寄存器和元件映像寄存器中读出，根据用户程序进行运算，运算的结果再存入元件映像寄存器中。对于元件映像寄存器来说，其内容会随程序执行的过程而变化。

(3) 输出刷新阶段。当所有程序执行完毕后，进入输出处理阶段。在这一阶段里，PLC 将输出映像寄存器中与输出有关的状态（输出继电器状态）转存到输出锁存器中，并通过一定方式输出，驱动外部负载。

因此，PLC 在一个扫描周期内，对输入状态的采样只在输入采样阶段进行。当 PLC 进入程序执行阶段后输入端将被封锁，直到下一个扫描周期的输入采样阶段才对输入状态进行重新采样。这种方式称为集中采样，即在一个扫描周期内，集中一段时间对输入状态进行采样。

在用户程序中如果对输出结果多次赋值，则最后一次有效。在一个扫描周期内，只在输出刷新阶段才将输出状态从输出映像寄存器中输出，对输出接口进行刷新。在其他阶段里输出状态一直保存在输出映像寄存器中。这种方式称为集中输出。

对于小型 PLC，其 I/O 点数较少，用户程序较短，一般采用集中采样、集中输出、循环扫描的工作方式，虽然在一定程度上降低了系统的响应速度，但使 PLC 工作时大多数时间与外部输入/输出设备隔离，从根本上提高了系统的抗干扰能力，增强了系统的可靠性。而对于大中型 PLC，其 I/O 点数较多，控制功能强，用户程序较长，为提高系统响应速度，可以采用定期采样、定期输出方式，或中断输入、输出方式以及采用智能 I/O 接口等多种方式。

从上述分析可知，从 PLC 的输入端输入信号发生变化到 PLC 输出端对该输入变化作出反应，需要一段时间，这种现象称为 PLC 输入/输出响应滞后。对一般的工业控制，这种滞后是完全允许的。应该注意的是，这种响应滞后不仅是由于 PLC 的扫描工作方式造成的，更主要是因为 PLC 输入接口的滤波环节带来的输入延迟，以及输出接口中驱动器件的动作时间带来的输出延迟，同时还与程序设计有关。滞后时间是设计 PLC 应用系统时应注意把握的一个参数。

4. PLC 对输入/输出的处理原则

(1) 输入映像寄存器的数据取决于输入端子板上各输入点在上一刷新期间的接通和断

开状态。

(2) 程序执行结果取决于用户所编程序和输入/输出映像寄存器的内容及其他各元件映像寄存器的内容。

(3) 输出映像寄存器的数据取决于输出指令的执行结果。

(4) 输出锁存器中的数据, 由上一次输出刷新期间输出映像寄存器中的数据决定。

(5) 输出端子的接通和断开状态, 由输出锁存器决定。

1.1.4 PLC 的操作模式

1. 操作模式

PLC 有两种操作模式, 即 RUN (运行) 模式与 STOP (停止) 模式。在 CPU 模块的面板上用“RUN”和“STOP”LED 显示当前的操作模式。

在 RUN 模式, 通过执行反映控制要求的用户程序来实现控制功能。

在 STOP 模式, CPU 不执行用户程序, 可以用编程软件创建和编辑用户程序, 设置 PLC 的硬件功能, 并将用户程序和硬件设置信息下载到 PLC。

如果有致命错误, 在消除它之前不允许从 STOP 模式进入 RUN 模式。PLC 操作系统可储存非致命错误供用户检查, 但是不会从 RUN 模式自动进入 STOP 模式。

2. 用模式开关改变操作模式

CPU 模块上的模式开关在 STOP 位置时, 将停止用户程序的运行; 在 RUN 位置时, 将启动用户程序的运行。模式开关在 STOP 或 TERM (Terminal, 终端) 位置时, 电源通电后 CPU 自动进入 STOP 模式; 在 RUN 位置时, 电源通电后自动进入 RUN 模式。

3. 用 STEP7 - Micro/WIN 编程软件改变操作模式

用编程软件控制 CPU 的操作模式必须满足下面的两个条件: ① 在编程软件与 PLC 之间建立起通信连接; ② 将 PLC 的模式开关放置在 RUN 模式或 TERM 模式。

在编程软件中单击工具条上的运行按钮或执行菜单命令“PLC/RUN”, 将进入 RUN 模式。单击停止按钮或执行菜单命令“PLC/STOP”, 将进入 STOP 模式。

4. 在程序中改变操作模式

在程序中插入 STOP 指令, 可以使 CPU 由 RUN 模式进入 STOP 模式。

1.2 PLC 的软件组成与编程语言

1.2.1 PLC 的软件组成

可编程序控制器 (PLC) 作为一种具有通信功能与可扩展输入/输出接口的工业计算机, 它必须具备相应的控制软件。PLC 控制软件 (系统程序) 根据生产厂家、型号的不同有所区别, 但总体上说, 可以分为系统程序 and 应用程序两大部分, 两者相对独立。系统程序和应用程序又包括若干不同用途的组成程序, 具体见下述。

1. 系统程序

PLC 的系统程序一般由管理程序、指令译码程序、标准功能块三部分组成, 其用途各不相同。

(1) 管理程序。

管理程序是系统程序的主体，主要作用是控制 PLC 进行正常工作，包括如下三个方面。

1) 系统运行管理。如控制 PLC 输入采样、输出刷新、逻辑运算、自诊断、数据通信等的时间次序。

2) 系统内存管理。如规定各种数据、程序的存储区域与地址，将用户程序中使用的数据、存储地址转化为系统内部数据格式及实际的物理存储单元地址等。通过系统内存管理，PLC 可以将有限的资源转变为可供用户程序使用的大量编程元件，如将实际 PLC 中存在的有限的 CTC 扩展为多个用户定时器、计数器等；并可建立起用户程序所使用的编程元件空间、程序存储空间与实际物理存储器、PIO、CTC 之间对应关系。

3) 系统自诊断。PLC 自诊断包括系统错误检测、用户程序的语法检查、指令格式检查、通信超时检查等。当系统发生上述错误时，可进行相应的报警与提示。

(2) 指令译码程序。

由于计算机最终可以执行的语言只能是机器码，为此，在 PLC 内部必须将编程语言编制的用户程序转化为机器码。指令译码程序的作用，就是在执行指令过程前将用户程序逐条“翻译”成为计算机能够识别的机器码。

指令译码需要一定的时间，它将降低 PLC 的处理速度，因此，在编制 PLC 用户程序时应尽可能简洁、明了，避免重复动作，这样不仅使程序便于检查，而且还可以提高程序的执行速度。

(3) 标准功能块。

在部分 PLC 中，为方便用户编程，PLC 生产厂家常将一些实现“标准动作”或特殊功能的 PLC 程序段，以类似“子程序”的形式存储于系统程序中，这样的“子程序”称为“标准功能块”。用户程序中如需完成“标准功能块”动作或功能，只须通过调用相应的“标准功能块”，并对其执行条件进行赋值即可。

标准功能块的多少代表了 PLC 的可编程性能，可以使用（调用）的“标准功能块”越多，用户程序编制就越容易、方便。

注意

以上所述的 PLC 系统程序，是指控制 PLC 系统自身运行的控制程序，它不向用户开放。因此，PLC 系统程序不包括用来支持 PLC 编程与调试的编程软件与仿真软件，后两种属于 PLC 编程、调试用工具软件的范畴。

2. 应用程序

PLC 应用程序是指 PLC 的使用者（用户）根据各种控制要求与控制条件编制的 PLC 用户控制程序，因此常称为“用户程序”。

应用程序的编制方法决定于所使用的编程工具（编程器与编程软件），目前最为常用的编程语言是梯形图，其程序通俗易懂，编程直观方便。此外，指令表、逻辑功能图、顺序功能图、流程图以及其他高级语言也可以在不同的场合使用。

1.2.2 PLC 的编程语言

IEC（国际电工委员会）的 PLC 编程语言标准（IEC 61131-3）中有顺序功能

(Sequential Function Chart, SFC)、梯形图 (Ladder Diagram, LD)、功能块图 (Function Block Diagram, FBD)、指令表 (Instruction List, IL) 和结构文本 (Structured Text, ST) 五种编程语言。

这五种编程语言中的顺序功能图 (SFC)、梯形图 (LD) 和功能块图 (FBD) 是图形编程语言, 指令表 (IL) 和结构文本 (ST) 是文字语言。

目前已有越来越多的 PLC 生产厂家提供符合 IEC 61131-3 标准的产品, 有的厂家推出的在个人计算机上运行的“软 PLC”软件包也是按 IEC 61131-3 标准设计的。

1. 顺序功能图

顺序功能图 (SFC) 是一种位于其他编程语言之上的图形语言, 用来编制顺序控制程序, 如图 1-5 所示。顺序功能图提供了一种组织程序的图形方法, 在其中可以用其他语言嵌套编程。步、转换和动作是顺序功能图中三种主要的元件。顺序功能图用来描述开关量控制系统的功能, 根据它可以很容易地画出顺序控制梯形图程序。

2. 梯形图

梯形图 (LD) 是使用最广泛的 PLC 图形编程语言, 如图 1-6 所示。梯形图与继电器控制系统的电路图很相似, 直观易懂, 很容易被工厂熟悉继电器控制的电气人员掌握, 特别适用于开关量逻辑控制。

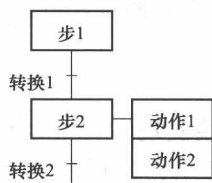


图 1-5 顺序功能图

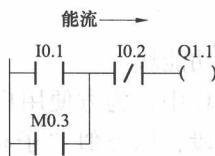


图 1-6 梯形图

梯形图由触点、线圈和应用指令等组成。触点代表逻辑输入条件, 例如外部的开关、按钮和内部条件等。线圈通常代表逻辑输出结果, 用来控制外部的指示灯、交流接触器和内部的输出标志位等。

在分析梯形图中的逻辑关系时, 为了借用继电器电路图的分析方法, 可以想象左右两侧垂直母线之间有一个左正右负的直流电源电压 (有时省略了右侧的垂直母线), 当图 1-6 中 I0.1 或 M0.3 触点接通时, 有一个假想的“能流” (Power Flow) 流过 Q1.1 的线圈。利用能流这一概念, 可以帮助我们更好地理解和分析梯形图, 能流只能从左向右流动。

3. 功能块图

功能块图 (FBD) 是一种类似于数字逻辑门电路的编程语言, 有数字电路基础的人很容易掌握。该编程语言用类似与门、或门的方框来表示逻辑运算关系, 方框的左侧为逻辑运算的输入变量, 右侧为输出变量, 输入、输出端的小圆圈表示“非”运算, 方框被“导线”连接在一起, 信号自左向右流动。功能块图如图 1-7 所示, 图 1-7 所表示的控制逻辑与图 1-6 所表示的相同。国内很少有人使用功能块图语言。

4. 指令表

PLC 的指令是一种与微机的汇编语言中的指令相似的助记符表达式, 由指令组成的程序叫做指令表程序。指令表程序较难阅读, 其中的逻辑关系很难一眼看出, 所以在设计时一般

使用梯形图语言。图 1-8 所示的指令表即是由图 1-6 所示的梯形图转换而来。如果使用手持式编程器, 必须将梯形图转换成指令表后再写入 PLC。在用户程序存储器中, 指令按步序号顺序排列。西门子的说明书中将指令表称为语句表。

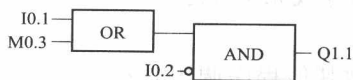


图 1-7 功能块图

LD	I0.1
O	M0.3
AN	I0.2
=	Q1.1

图 1-8 指令表

5. 结构文本

结构文本 (ST) 是为 IEC 61131-3 标准创建的一种专用的高级编程语言。与梯形图相比, 它能实现复杂的数学运算, 编写的程序非常简洁和紧凑。

6. 编程语言的相互转换与选用

在 S7-200 的编程软件中, 用户可以选择梯形图、功能块图和语句表来编程, 软件编程可以自动切换用户程序使用的编程语言。

梯形图与继电器电路图的表达方式极为相似, 梯形图中输入信号与输出信号之间的逻辑关系一目了然, 易于理解。语句表程序较难阅读, 其中的逻辑关系很难一眼看出。在设计复杂的数字量控制程序时建议使用梯形图语言。但是语句表输入方便快捷, 还可以为每一条语句加上注释, 便于复杂程序的阅读。在设计通信、数学运算等高级应用程序时, 建议使用语句表。

梯形图在一个网络中只能有一块独立电路。在语句表中, 几块独立电路对应的语句可以放在一个网络中, 但是这样的网络不能转换为梯形图。梯形图程序一定能转换为语句表。

7. SIMATIC 指令集与 IEC 61131-3 指令集

STEP7-Micro/WIN 编程软件提供了: SIMATIC 指令集与 IEC 61131-3 指令集两种指令集, 前者由西门子公司提供, 它的某些指令不是 IEC 61131-3 中的标准指令。通常 SIMATIC 指令的执行时间短, 可以使用梯形图、功能块图和语句表语言, 而 IEC 61131-3 指令集只提供前两种语言。

IEC 61131-3 指令集的指令较少, 其中的某些指令可以接受多种数据格式。例如 SIMATIC 指令集的加法指令分为 ADD_I (整数相加)、ADD_DI (双字整数相加) 与 ADD_R (实数相加) 等, IEC 61131-3 的加法指令 ADD 则未作区分, 而是通过检验数据格式, 由 CPU 自动选择正确的指令。因为 IEC 指令要检查参数中的数据格式, 可以减少程序设计中的错误。

在 IEC 61131-3 指令编辑器中, 有些指令是 SIMATIC 指令集中的指令, 它们作为 IEC 61131-3 指令集的非标准扩展, 在编程软件的指令树内用红色的“+”号标记。

1.2.3 PLC 的程序结构

S7-200 CPU 的控制程序由主程序、子程序和中断程序组成, 如图 1-9 所示。

1. 主程序

主程序是程序的主体, 每一个项目都必须并且只能有一个主程序。在主程序中可以调用子程序和中断程序。主程序通过指令控制整个应用程序的执行, 每个扫描周期都要执行一次。