

KEBIANCHENG KONGZHIQI YINGYONGJIEXI

隋振有 隋凤香 编著 ■

可编程控制器应用解析



中国电力出版社
www.cepp.com.cn

隋振有 隋凤香 编著 ■

可编程控制器应用解析



中国电力出版社

www.cepp.com.cn

内 容 提 要

本书以 S7—200 为样机,系统地介绍了 PLC 的应用技术,其内容包括 PLC 的数学基础、S7—200 的硬件、软件等方面的技术知识。

从 S7—200 系列入手,对 PLC 硬件、软件的配置,系统的安装调试和运行操作都做了较全面的介绍。尤其,以 S7—200 的编程软件 STEP7—Micro/WIN32 为范例,对编程技术做了详细的介绍和探讨,为解决 PLC 编写程序这一最大的难题,提供了一些帮助。

本书可供广大工程技术人员和在校的大学、高职学生选用。

图书在版编目 (CIP) 数据

可编程控制器应用解析/隋振有,隋凤香编著. —北京:
中国电力出版社, 2006

ISBN 7—5083—3731—X

I. 可… II. ①隋… ②隋… III. 可编程序控
制器 IV. TP332.3

中国版本图书馆 CIP 数据核字 (2005) 第 139856 号

中国电力出版社出版、发行

(北京三里河路 6 号 100044 <http://www.cepp.com.cn>)

北京丰源印刷厂印刷

各地新华书店经售

*

2006 年 1 月第一版 2006 年 1 月北京第一次印刷

850 毫米×1168 毫米 32 开本 15.875 印张 419 千字

印数 0001—4000 册 定价 29.00 元

版 权 专 有 翻 印 必 究

(本书如有印装质量问题,我社发行部负责退换)

前 言



英国数学家布尔总结论述了逻辑代数理论，为研制二值逻辑元器件提供理论基础和数学模型，也为研制数字电子计算机(PC)、可程序控制器奠定了理论和物质基础。

可程序控制器(PLC)是专门用于工业控制的计算机，它功能强大，性能高。它的问世，使自动化技术进入数字信息化的智能控制时代。因此，认识它、掌握它、应用它是更新技术的需要，是适应科学技术发展的需要。在自动控制技术领域中，PLC必定得到普及性的应用。

本书以 S7—200 为样机，从 PLC 的数学基础入手，较系统地介绍了 S7—200 的软硬件资源及选型、安装、调试和运行技术。尤其，结合 S7—200 编程软件 STEP7 - Micro/WIN32 对 PLC 的编程技术做了较全面的探讨，编者深信，对 PLC 技术的应用，必将起到触类旁通、举一反三的作用。

本书文字简洁，层次清晰，通俗易懂。面向广大技术工人、工程技术人员、工控专业的大学生和高等职业学校的学生。期望本书成为深受广大读者喜爱的读物，并使每一位读者得到应有的帮助，这是编者编写此书的目的。

本书编写过程中，得到北京四通工控技术有限公司李晓通、郭劲松等大力的支持，北京交通大学耿文学教授对本书进行了全面的审阅，在此表示深深的谢意。

由于编者知识水平所限，书中会存在不妥，甚至会有谬误，望广大读者能坦诚地提出批评，以便修正，编者则表示衷心的感谢。

编 者

目 录



前言

第1章 可程序控制器概论	1
1.1 PLC 主机模块和扩展功能模块	2
1.1.1 中央微处理器 (CPU)	2
1.1.2 存储器	5
1.1.3 PLC 的 I/O 通道	9
1.1.4 电源模块	13
1.1.5 主机输入输出元器件	15
1.1.6 扩展功能模块	23
1.2 PLC 的工作原理和控制过程	24
1.2.1 PLC 的工作原理	24
1.2.2 PLC 的控制过程	25
1.3 PLC 的技术特性及其应用	29
1.3.1 PLC 与继电器控制电路相比较	29
1.3.2 PLC 与个人计算机 (PC) 相比较	30
1.3.3 PLC 的技术指标	31
1.3.4 PLC 系统主要的控制功能	33
1.3.5 PLC 的分类	36
1.3.6 PLC 的应用简述	37
1.4 PLC 的配置	39
1.4.1 系统基本配置	39
1.4.2 扩展功能模块的配置	41
1.4.3 系统冗余配置	44

1.4.4 系统附加配置	45
第2章 PLC 的数学基础	46
2.1 数制和数制间的转换	46
2.1.1 数制	46
2.1.2 数制间的相互转换	47
2.1.3 二进制数的四则运算	52
2.1.4 二进制编码简介	55
2.2 二进制编码	58
2.2.1 常用的二—十进制编码	59
2.2.2 标准代码	62
2.3 逻辑代数	69
2.3.1 二值逻辑	69
2.3.2 基本逻辑代数及其运算方法	70
2.3.3 复合逻辑及其运算方法	72
2.3.4 逻辑代数的运算法则	76
2.3.5 逻辑代数的运算定律	77
2.3.6 逻辑代数的运算定理	83
2.4 逻辑函数及其表示方法	84
2.4.1 表示逻辑函数的方法	85
2.4.2 逻辑函数表示方法间的相互转换	86
2.4.3 逻辑函数式的化简	87
第3章 S7—200 系列 PLC 的硬件	93
3.1 S7—200 系列 PLC 的硬件概述	93
3.1.1 S7—200 主机 CPU 模块	93
3.1.2 数字量输入/输出模块	113
3.1.3 模拟量输入输出模块	123
3.1.4 EM253 位控模块	127

3.1.5	S7—200 的编程器和电源	131
3.1.6	S7—200 的附加硬件	132
3.1.7	S7—200 主机输入输出的配置	137
3.2	S7—200 的通信网络	139
3.2.1	通信网络元器件	139
3.2.2	网络传输介质	145
3.2.3	S7—200 通信智能模块	147
第4章	PLC 的软件	157
4.1	指令	157
4.1.1	指令的分类	157
4.1.2	指令的组成	158
4.1.3	寻址方式	159
4.1.4	数据	160
4.2	程序	164
4.2.1	程序的特性	165
4.2.2	程序的分类	165
4.2.3	程序语言	166
4.2.4	程序的执行时间	166
4.3	S7—200 的软件资源	167
4.3.1	S7—200 数据存储器	167
4.3.2	S7—200 特殊标志存储器 (SM)	176
4.3.3	变量存储器 (V) 存放的信息	192
4.4	S7—200 的特殊功能软件	200
4.4.1	高速计数器 (HSC)	200
4.4.2	高速脉冲输出	201
4.4.3	比例、积分、微分控制软件	202
4.5	S7—200 运行信息	207

4.5.1	S7—200 程序的执行时间	207
4.5.2	S7—200 系列的中断控制	218
4.5.3	错误信息	221
4.5.4	其他软件	227
4.6	通信软件	230
4.6.1	通信方式	230
4.6.2	通信网络	231
4.6.3	通信协议	233
4.6.4	通信网站	235
4.6.5	通信参数	236
4.6.6	变频器控制软件	237
第5章	S7—200 指令系统	241
5.1	S7—200 指令系统	241
5.1.1	位逻辑指令	241
5.1.2	逻辑堆栈指令	249
5.1.3	中断和中断指令	252
5.1.4	通信控制和通信指令	261
5.1.5	比较指令	272
5.1.6	转换指令	276
5.1.7	计数器指令	286
5.1.8	高速计数器 (HSC) 及其指令	288
5.1.9	高速脉冲输出指令	298
5.1.10	定时器及其指令	308
5.1.11	时钟指令	311
5.1.12	逻辑运算指令	313
5.1.13	数学运算指令	317
5.1.14	数学功能指令	326
5.1.15	PID 控制及指令	330

5.1.16	传送指令	332
5.1.17	移位和循环指令	337
5.1.18	程序控制指令	343
5.1.19	表功能指令	349
5.1.20	字符串 (STR) 指令	353
第6章	编程软件及其应用	357
6.1	S7—200 系列的编程软件	357
6.1.1	STEP7 – Micro/DOS	357
6.1.2	STEP7 – Micro/WIN32 (V3.1)	367
6.2	通信网络	376
6.2.1	设置网络参数时调用软件的过程	376
6.2.2	通信网络的最小配置	385
6.2.3	设置通信网络参数	386
6.3	离线编程和在线编程	387
6.3.1	离线编程	387
6.3.2	在线编程	390
第7章	编程技术	404
7.1	编程语言	404
7.1.1	梯形图 (LAD)	404
7.1.2	功能块图 (FBD)	407
7.1.3	语句表 (STL)	407
7.1.4	顺序功能图 (SFC)	408
7.1.5	高级语言	412
7.2	编程	412
7.2.1	编程规则	412
7.2.2	编制梯形图的规律及其技巧	414
7.2.3	编程方法	417

7.2.4 将继电器控制电路转换为梯形图	424
7.2.5 编程须知	428
7.3 S7—200 的应用程序	435
7.3.1 定时器程序	435
7.3.2 计数器应用程序	437
7.3.3 中断程序	439
7.3.4 子程序	441
7.3.5 顺序控制程序	443
7.3.6 高速计数器 (HSC) 程序	447
7.3.7 高速脉冲输出程序	447
7.3.8 PID (比例、积分、微分) 控制程序	452
7.3.9 S7—200 通信程序	464
第8章 PLC 的安装调试运行和维护	469
8.1 PLC 的安装	469
8.1.1 安装应遵守的技术规范	469
8.1.2 PLC 安装的一般要求	471
8.1.3 S7—200 的安装工艺	474
8.1.4 通信网络元器件的安装	478
8.2 PLC 系统的调试	479
8.3 S7—200PLC 的运行	481
8.3.1 S7—200 的运行操作	481
8.3.2 S7—200PLC 的运行监视及其测控	485
8.3.3 PLC 运行故障处理及其维护	486
附录 S7—200 语句表指令表	491
参考文献	497

第 1 章 可编程序控制器概论

可编程序控制器是以计算机为基础的专用控制装置，自 1966 年，美国通用汽车（GM）公司委托美国数据设备公司（DEC）研制成功第一台可编程序控制器以来，近 50 年，可编程序控制器得到迅速发展。至今，生产厂商已有 200 多家，400 余种规格的产品。在美国、日本、德国等发达国家所生产的可编程序控制器，质量优良，功能强大，专用性突出，各有特长，被应用在电力生产、电力拖动、机床控制、石油化工、交通运输、汽车制造工业等领域的控制技术中。

1987 年，国际电工委员会（IEC）颁布的《可编程序控制器标准草案》第三版中，对可编程序控制器给出如下定义：

可编程序控制器是一种数字运算操作的电子系统，专为工业环境下应用设计。它采用可编程的存储器，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、模拟式输入输出，控制各类机械和生产过程。可编程序控制器和它的有关设备，应按易于和工业控制系统联成一体，并易于扩充功能的设计原则。

1980 年美国电气制造商协会（NEMA）给它起了个名字：“Programmable Controller”，简称 PC。由于我国已经把个人计算机称为 PC，为了避免学术名词的混淆，则把可编程序控制器称为：Prgramble Logic Controller，简称“PLC”。

可编程序控制器（PLC）的产品达几百种。在机型上，有微型 PLC、小型 PLC、中型 PLC 和大型 PLC。机型不同，功能不同。随着机型的增大，功能也不断增强。对于同一种机型，比如都为小型机，却因生产厂家不同，设计理念不同，在功能上存在一定的差异。但是，它们的基本结构、工作原理和基本功能是相同

的。只要能熟练地应用一种型号的 PLC, 对其他型号的 PLC 也就能基本理解, 做到触类旁通, 举一反三。

除微型 PLC 是一块高度集成的电路板, 小型乃至中型以上的 PLC 都已模块化, 则以主机模块为基本的控制系统, 然后, 再根据功能的需要, 配置扩展功能模块。

1.1 PLC 主机模块和扩展功能模块

PLC 主机模块由中央处理器 (CPU)、存储器、标准电源、I/O 通道和 I/O 元器件等组成。

1.1.1 中央微处理器 (CPU)

中央处理器 (CPU) 是 PLC 主机模块的心脏和大脑。它具有理想的控制功能。PLC 的 CPU 由各生产厂家商研制设计。各种型号的 PLC 都有对应的 CPU 系列相匹配, 由于研制设计者的独具匠心, 不同型号的 PLC, CPU 的结构和性能都有些变化。尤其, 存储区的设置和容量分配是不一样的。因此, 应该熟悉和充分地掌握所选用的 PLC 的 CPU 的工作性能及基本结构。

1. CPU 的基本结构

CPU 由运算器和控制器组成。其中运算器由算术逻辑单元及一些寄存器组成。运算器是 PLC 执行算术运算和逻辑运算的逻辑元器件, 负责对输入的数据信息进行加工处理。控制器是由指令译码器、时序发生器和操作控制器等元器件组成。控制器负责经指令译码器译制好的二进制代码的调用, 发出控制信号, 协调各部分的正常工作。

PLC 对系统程序、用户程序和控制操作所用的数据分区存储。尤其, 对输入输出信号数据映像存储; 对定时器、计数器及其他数据信号存入对应的存储区, 供 CPU 随时调用。

CPU 内部能够有条不紊地工作, 是在运算器和控制器协调工作的条件下实现的。但是, 它们离不开总线。总线是它们相互间传输控制命令和信息数据的通道。组成 CPU 的所有元器件都挂在总线上, 组成内部通信网络。

总线分内部总线和外部总线, 组织连接 CPU 内部元器件的

总线，称内部总线。CPU 与整机系统相连接的总线称外部总线，亦称系统总线。

总线又分为控制总线、地址总线和数据总线。其中，控制总线是传输 CPU 的控制命令的，地址总线是传输存储单元地址的，数据总线是传输数据信息的。

2. CPU 的功能

CPU 具有接收程序、运行程序和监控系统运行的功能。

接收程序 CPU 对系统程序和用户程序都能接收。比如，厂家编制的编译程序、系统管理程序、上电初始化程序、驱动程序、输入输出刷新程序以及一些常用的子程序、中断程序、监控程序等，经测试合格后，固化在只读存储器（ROM）中，终生不能变动。用户根据生产工艺及其控制要求编制的程序，称为用户程序。用户程序可因工艺流程和控制要求的变动，予以变动或改写。因此，存储在随机存储器（RAM）中，既可以读，又可以写。

CPU 要义不容辞地接收系统程序和执行系统程序。而对用户程序，CPU 要调用系统程序进行编译和编辑，然后，经测试存放在 RAM 中。当输入控制信号，执行用户程序时，则把用户程序转存到内存中，再进行处理运算，用于控制之中。

当扩展系统功能时，如配置位控模块、通信功能模块及其他扩展功能模块等功能时，要将配置模块的规格型号、结构参数及其存储地址存放在 EEPROM 存储卡中，然后，输入到内存，才能执行扩展功能。

运行程序 无论是系统程序，还是用户程序，或者是扩展功能的控制程序，在执行时，都必须把它们调入内存（或在内存中直接调用）。其过程是：

CPU 通过控制总线发出操作命令，通过地址总线读取数据存放的地址，通过数据总线读取指令和操作数据，将它们存入指令寄存器。然后，通过译码器对程序中的指令代码逐条翻译，变成控制信号，同时信号合成，经放大形成可驱动指令代码信号的脉

冲，去驱动负载元器件。

监控系统运行 PLC 可工作在运行状态，也可以工作在监控状态对系统实施监控。并可以工作在编程状态，修改程序，改变相关数据和监控系统运行状态。

3. CPU 模块性能参数

CPU 模块是数字系统的核心元器件，它必须具备一定的性能和在相关的性能参数允许的范围内工作，才能达到理想的最佳效果。

(1) 主频 就是 CPU 的工作频率，是系统时钟在单位时间内振荡的次数，主频越高，CPU 运行的速度越快。但是，并不是主频越快越好。由于主频必须与外频相匹配，因此，只能说适宜的主频是最理想的。

(2) 外频 就是整机系统总线的工作频率。CPU 要通过系统总线从外部存储器取得数据，又要通过系统总线把内存中的数据传送出去。这样，系统总线的工作频率（外频）必须与主频相匹配。外频过高或过低都会产生传输瓶颈。一般情况下，外频低于主频。但主频与外频之间必须以一定的倍数关系相匹配。

(3) 差频（或称倍频） 就是主频和外频之间相差的倍数，即主频 = 外频 × 倍频。为了提高 CPU 的工作效率，采取提高外频的措施比较好。

(4) 运算速度 CPU 在每秒钟能执行的指令数，称为 CPU 的运算速度，单位是每秒百万条指令。

(5) 字长 是 CPU 一次传送数据的二进制数的位数，一般的字长为 8 位、16 位、32 位及 64 位。

(6) 工作电压 CPU 的额定工作电压，一般为 5V。由于 CPU 模块集成度高，工作速度高，功耗大，发热严重，而降低使用寿命。因此，只有降低工作电压是降低功耗的较好的办法。Intel 公司生产的 CPU 的工作电压已降至 1.45V。

(7) 周期 PLC 的 CPU 的周期分为三种：一是时钟周期；二是机器周期；三是扫描周期。时钟周期是 CPU 内核时钟振荡一

次所占的时间。机器作一个基本操作所占有的时间，称为一个机器周期。CPU 执行一次扫描所占用的时间称为扫描周期。三者的关系：若干个时钟周期构成一个机器周期。若干个机器周期构成一个扫描周期。周期的单位：s（秒）、ms（毫秒）、 μs （微秒）、ns（纳秒），它们之间的换算关系为 $1\text{s} = 1000\text{ms}$ 、 $1\text{ms} = 1000\mu\text{s}$ 、 $1\mu\text{s} = 1000\text{ns}$ 。

(8) 总线宽度 CPU 中配置了地址总线、数据总线和控制总线。其中，地址总线宽度就是地址码长的位数所对应的地址线的条数。有八条、十六条、三十二条等。数据总线宽度就是 CPU 一次传输数据的位数所对应的数据线的条数。数据的位数越多，传输的信息量越大。控制线是 CPU 下达控制操作命令的信号线，一般为多个元器件共用 1 根控制线。

1.1.2 存储器

计算机或者可编程序控制器等数字系统在实施自动控制过程中，最突出的一个特点是存储记忆。对采集的信号要在输入后马上映像存储，CPU 调度过程中首先缓存，之后，才参与译码、运算处理。对运算处理后的数据中间结果或最终结果，还必须存储后，才能调用处理或输入锁存器（对输出加以缓存）。从上述可看出，数字系统对处理的数据是步步存储，然后才能调用。从而，加强了控制的逻辑性，提高了可靠性。尤其，系统程序或者用户程序经测试合格，将其指令和数据分区存储，并根据程序和数据的重要性用不同的存储器存放。比如：系统程序固化在 ROM 中，用户程序则存放在随机存储器 RAM 中。

存储器是存放信息数据的载体，故也称存储体。长期以来，人们多以磁性材料做信息数据的载体，如磁盘、磁带等。过去的留声机就是典型的磁性存储器。而现在使用的硬盘、软盘，则是磁存储器延用的新型产品。尤其光盘是光电技术与磁性存储技术有机结合的产物，它们都可以做成存储容量相当大的虚拟存储器。

1. 存储器的分类

按功能特性可把存储器分为只读存储器、读写存储器、闪存存储器和虚拟存储器等。

只读存储器，英文名称缩写 ROM，故简称 ROM。它所存储的数据只能读，不能随意改写，多数用于存放系统程序和一些重要的系统默认的数据。这些程序是厂家编制或出厂时赋予的数据，终生不变。如控制输入/输出的驱动程序，监测系统运行状态的监控程序、翻译（解释）程序、操作系统的程序以及主机配置方面主要的数据等。出厂时，输入 ROM，固化掩膜，加以保护。

ROM 因其性能又分为固定的只读存储器（ROM）、可编程只读存储器（EPROM）和多次涂擦编程的只读存储器（EEPROM）。

可编程只读存储器（EPROM） EPROM 中文意思是可编程只读存储器，随着用户对控制技术应用能力的提高和对编程技术的掌握，而且机械设备不断地更新，工艺流程不断地改变，固化在只读存储器中的程序也需要做相应地变动。因此，只能读的 ROM 已不能满足实际需要，则需要既能读出，又能写入的只读存储器。目前，广泛使用雪崩注入的金属—氧化物—半导体三极管（FAMOS）或叠栅注入式的金属—氧化物—半导体三极管（SIROM）构成可编程只读存储器（EPROM）。

EPROM 采用紫外线涂擦其中的信息。波长 $400 \times 10^{-10} \text{m}$ 以下的紫外线光对 EPROM 均有擦除其中信息的作用。波长 $3000 \sim 4000 \times 10^{-10} \text{m}$ 之间的阳光或荧光灯的光对 EPROM 也有消除其中信息的破坏作用。把 EPROM 置于阳光下曝晒，一个星期可把 EPROM 中的信息清除。因此，EPROM 采用不透明的薄膜进行掩膜，防止存储的信息丢失。

当前，使用比较多的 EPROM 的型号有 27011、27512、270512、27513、2764 等产品。

多次涂擦可编程的只读存储器（EEPROM） EEPROM 中文意思是多次涂擦可编程的只读存储器。这种存储器最适合于用户

选用。用户可把应该改动、更新的数据或程序，经过涂擦编程，以 EEPROM 存储卡的形式存放，随着实际需要而进行多次涂擦编程。

读写存储器 读写存储器是既能读出又能写入。可随着需要变动所存储的数据或程序。因此，又称随机存储器。其英文名称缩写为 RAM。

RAM 是靠电路状态的自保功能存储数据信息的。如果失去自保电荷就失去存储数据的能力。如果为其提供电荷又恢复存储数据的功能。因此，用户用其存储编制的程序，对修改、调试十分方便灵活。可随着工艺的更新，流程的变动，运行参数的整定及保护功能的设置，随机变动，易于修改。

RAM 由内部电源提供 3~5V 微小的电荷就能保持其中的数据。断电状态又很容易失去存储的数据。在运行中，对 RAM 采用周期性定时刷新，反复充入电荷，来保持原来存放的数据。但是，由于电路寄生电容等因素的影响，RAM 中所存放的数据状态可能变形走样，对 RAM 中存放的数据和程序应做好备份。

虚拟存储器 虚拟存储器就是把磁盘存储器当 RAM 来使用，从而扩大内存空间。磁盘的容量可随意扩大。可做成页式虚拟存储器、段式虚拟存储器或页段式虚拟存储器。这样，解决了 ROM、RAM 的存储容量受一定限制，其容量不可能做得特别大的弊病。

闪速存储器 闪速存储器是一种非挥发性的存储技术。只有对其存储元施加一个高电压才能擦除所存储的数据。不然，可以一直保存其中的内容，且不需要保持电源，在不加电的情况下，数据可存放十年之久。

对闪速存储器经高压擦除可再写，其存储容量较大，现已达到 40MB。对其访问时间低于 30ns，比硬盘快 100~1000 倍。抗振能力比硬盘高 10 倍。

2. 存储器的特性参数

(1) 时钟频率 时钟频率是存储器能够稳定运行的最大频