中国书刊发行协会年度全行业优秀畅销品种

SIEMENS 西门子公司重点推荐图书

中国工控网 www.gongkong.com 中华工控网 gkong.com 联袂推介

S7-300/400 PLC 应用技术

第4版

廖常初 主编

赠送超值DVD 光盘：

- STEP 7 V5.5 SP4 中文版 +S7-PLCSIM V5.4 SP5 +S7-Graph V5.3 SP7+WinCC flexible 2008 SP4
- 32 个多媒体视频教程
- 40 多本中文用户手册
- 60 多个与正文配套的例程

机械工业出版社
CHINA MACHINE PRESS

中国书刊发行协会年度全行业优秀畅销品种
西门子公司重点推荐图书
中国工控网、中华工控网联袂推介

S7-300/400 PLC 应用技术

第 4 版

廖常初　主编

机 械 工 业 出 版 社

本书曾荣获中国书刊发行业协会 2012-2013 年度全行业优秀畅销书奖，全面介绍了西门子 S7-300/400 PLC 的硬件结构和硬件组态、指令、程序结构、PID 闭环控制、编程软件和仿真软件的使用方法，以及一整套易学易用的开关量控制系统的编程方法。介绍了西门子的各种通信网络和通信服务的组态和编程的方法、网络控制系统的故障诊断方法、用仿真软件在计算机上模拟运行和监控 PLC 用户程序的方法，以及通过仿真来学习 PID 参数整定的方法。

随书光盘提供了多个中文版软件、大量的中文用户手册、60 多个例程和 30 多个多媒体视频教程。

本书注重实际，强调应用，可供工程技术人员自学和作为培训教材，对 S7-300/400 的用户也有很大的参考价值。《S7-300/400 PLC 应用教程》是本书的教材版。

图书在版编目（CIP）数据

S7-300/400 PLC 应用技术 / 廖常初主编．—4 版．—北京：机械工业出版社，2016.4

ISBN 978-7-111-53570-6

Ⅰ．①S…　Ⅱ．①廖…　Ⅲ．①plc 技术　Ⅳ．①TM571.6

中国版本图书馆 CIP 数据核字（2016）第 080308 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：时　静　　责任编辑：时　静

责任校对：张艳霞　　责任印制：常天培

北京圣夫亚美印刷有限公司印刷

2017 年 1 月第 4 版 • 第 2 次印刷

184mm×260mm • 25.75 印张 • 638 千字

5001－10000 册

标准书号：ISBN 978-7-111-53570-6

ISBN 978-7-89386-050-8（光盘）

定价：75.00 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

服务咨询热线：（010）88379833　　机 工 官 网：www.cmpbook.com

读者购书热线：（010）88379649　　机 工 官 博：weibo.com/cmp1952

教育服务网：www.cmpedu.com

封面无防伪标均为盗版　　金　书　网：www.golden-book.com

前　言

本书是一本全面深入地介绍 S7-300/400 的书籍，曾获中国书刊发行业协会 2012-2013 年度全行业优秀畅销书奖。

第 4 版根据 S7-300/400 最新版的硬件和软件，对全书内容作了优化处理和修订。参考西门子新软件平台博途中的 STEP 7 的处理方法，介绍了一些库里的较常用的指令。删除或精简了一些较少使用的内容，与 PLC 通信的变频器改为当前主流的 G120。以太网已经广泛地应用于西门子的工控产品，为此增加了 S7-300/400 与其他 S7 PLC 通过以太网的 S7 通信和开放式用户通信，以及以太网的多种故障诊断和故障自动显示的方法。

本书对 S7-300/400 的硬件结构与硬件组态、编程软件与仿真软件的使用、编程语言、指令、程序结构、各种通信网络和通信服务、PID 闭环控制等都作了全面深入的介绍。同时介绍了作者总结的设计数字量控制梯形图的一整套易学易用的编程方法，还介绍了用仿真软件在计算机上模拟运行和监控 PLC 用户程序的方法。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。网络故障诊断是现场维护的难点，本书详细介绍了多种简单实用的网络故障的诊断方法和仿真方法。

随书光盘提供了中文版 STEP 7 V5.5 SP4、仿真软件 PLCSIM V5.4 SP5、编程语言 S7-Graph V5.3 SP7、大量的中文用户手册、与正文配套的 60 多个例程和 30 多个多媒体视频教程。

作者主编的《跟我动手学 S7-300/400 PLC》是本书的入门版，适合于初学者，该书有五十个实训，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 的使用方法。《S7-300/400 PLC 应用教程》是本书的教材版，附有习题和实验指导书。

本书注重实际，强调应用，可供工程技术人员自学和作为培训教材，对 S7-300/400 的用户也有很大的参考价值。

本书由廖常初主编，陈晓东、王云杰、李远树、周林、陈曾汉、侯世英、郑连清、范占华、关朝旺、郑群英、余秋霞、张学锋、申敏、罗盛波、廖亮、孙明渝、唐世友、文家学参加了编写工作。

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。欢迎读者访问作者在中华工控网的博客。

重庆大学　廖常初

目　　录

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，可编程序控制器（Programmable Logic Controller）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，已经广泛地应用于各种机械设备和生产过程的自动控制系统。PLC 仍然处于不断的发展之中，其功能不断增强，更为开放，它不但是单机自动化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不可比拟的。

1．S7-300/400 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, 在国际国内均占有很大的市场份额，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、电源模块等组成（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。

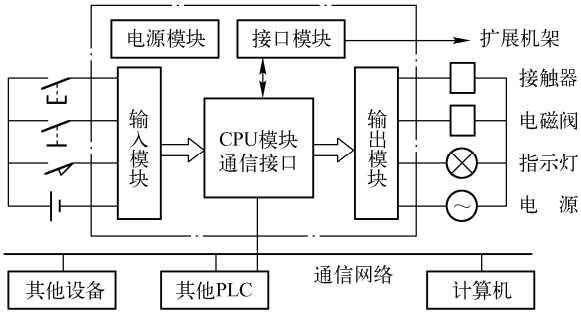

图 1-1　PLC 控制系统示意图

（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；存储器用来储存操作系统、用户程序和数据。S7-300/400 将 CPU 模块简称为 CPU。

CPU 集成了一个或多个通信接口，CPU 31xC 系列还集成有数字量、模拟量输入/输出点。

（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（SM）。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。

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、压力继电器等提供的开关量输入信号。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 5V，而 PLC 的外部输入/输出信号电压一般较高，例如 DC 24V 或 AC 220V。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，用光耦合器和小型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

功能模块简称为 FM，它是智能的信号处理模块，不占用 CPU 的资源，直接对来自现场设备的信号进行控制和处理，并将信息传送给 CPU。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。功能模块包括闭环控制模块、流量测量模块、称重模块、计数器模块和定位模块等。

（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 PROFIBUS-DP、AS-i 和工业以太网，或用于点对点通信。

（6）电源模块

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

（7）导轨和机架

S7-300 的铝质导轨用来固定和安装上述的各种模块。S7-400 的模块安装在机架上。

（8）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。

2．怎样下载西门子 PLC 的资料和软件

西门子工业支持网站的网址为 https://support.industry.siemens.com/cs/start?lc=zh-CN，该网站下载中心可以下载西门子各种工控产品的中英文用户手册、产品样本和软件等。单击

“找答案”“技术论坛”和“在线学习园地”，可以进入相应的版区。单击“全球技术资源库”，将会打开西门子的全球支持网站。

为了阅读 PDF 格式的文件，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 逻辑运算与 PLC 的循环处理过程

1．逻辑运算

在数字量（或称开关量）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”逻辑运算关系见表 1-1。“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”。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。

表 1-1 逻辑运算关系表

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

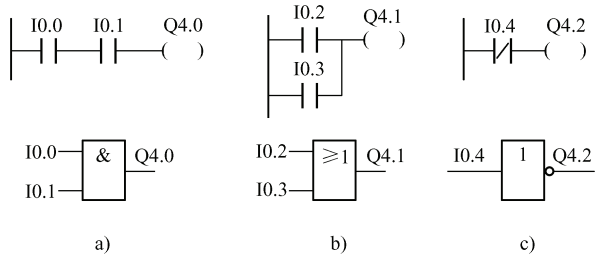

图 1-2 基本逻辑运算

a) 与 b) 或 c) 非

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。因为同一个 BOOL 变量的常开触点和常闭触点的状态相反，有上划线的地址对应于常闭触点。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。

2．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。

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。

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 将过程映像输出表（Q 区）的数据写到输出模块。

3）CPU 读取输入模块的输入状态，并存放到过程映像输入表（I 区）。

4）CPU 处理用户程序，执行用户程序中的指令。

5）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。

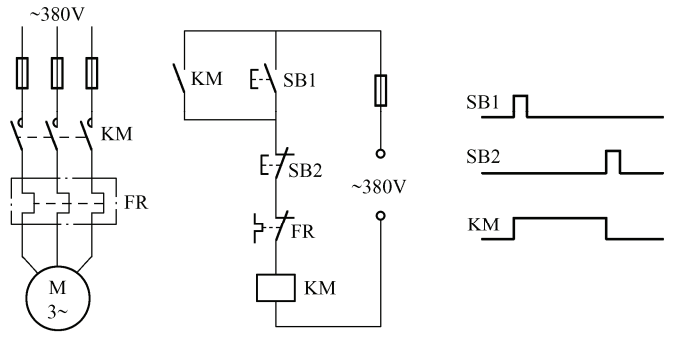

图 1-3　异步电动机控制电路

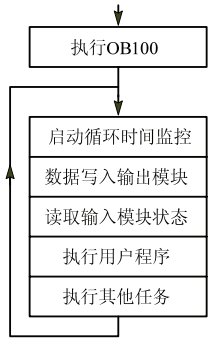

图 1-4　扫描过程

6）CPU 返回第一阶段，重新启动循环时间监控。

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。在启动完成后，每次循环都要调用一次主程序 OB1，OB1 可以调用 OB 之外的逻辑块。被调用的逻辑块又可以调用 OB 之外的下一级的逻辑块。

如果有中断事件出现，循环的程序处理过程被暂停执行，并自动调用分配给该事件的中断组织块。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 并不是直接访问 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（I/Q 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。

某个位地址为 1 状态时，称该位地址的状态为 ON；该位地址为 0 状态时，称该位地址的状态为 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。在执行位逻辑指令时，从过程映像输入区或别的存储区中将有关位地址的 0、1 状态读出来，并根据指令的要求执行相应的逻辑运算，运算结果写入指定的位地址。因此，各位地址的存储区的内容随着程序的执行而变化。

3．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循环时间（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周期中占相当大的比例。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扫描周期、最小扫描周期和上一次的扫描周期。

扫描周期将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。

1.2.2 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 中开关 K1 和 K2 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。

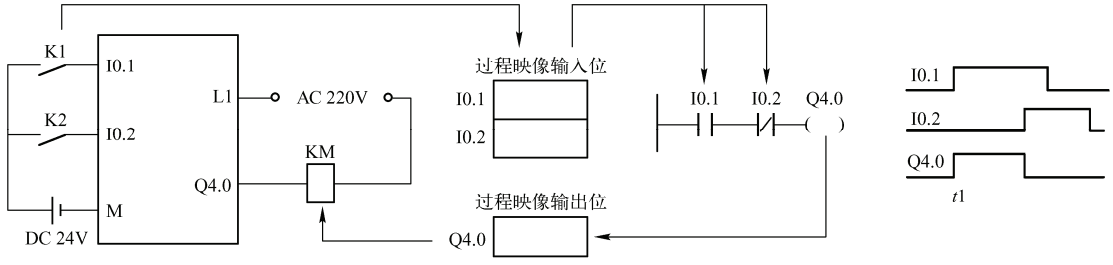

图 1-5　PLC 外部接线图与梯形图

梯形图中的 I0.1 是过程映像输入位，与接在对应的输入端子的 K1 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
```

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 K1 和 K2 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结果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 $t < t1$ 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。在程序执行阶段，经过上述逻辑运算过程之后，运算结果为 Q4.0 = 0，所以 KM 的线圈处于断电状态。$t = t1$ 时开关 K1 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的抖动产生的不良影响，滤波电路的时间常数决定了输入滤波时间的长短。有的输入模块采用数字滤波，滤波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 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。

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。