



高新技术技能系列丛书

GAOXINJISHU JINENG XILIE CONGSHU

从入门到

CONG RUMEN
DAO
JINGTONG

精通

—— 西门子工业网络通信
实战

广东省职业技能鉴定指导中心

华南理工大学工业培训中心PLC培训部 组编

张运刚 宋小春 编著



人民邮电出版社
POSTS & TELECOM PRESS



高新技术技能系列丛书

GAOXINJISHU JINENG XILIE CONGSHU

从入门到

CONG RUMEN
DAO
JINGTONG

精通

—— 西门子工业网络通信
实战

广东省职业技能鉴定指导中心

华南理工大学工业培训中心PLC培训部 组编

张运刚 宋小春 编著

人民邮电出版社
北京

图书在版编目 (CIP) 数据

从入门到精通——西门子工业网络通信实战 / 张运刚, 宋小春编著.

—北京: 人民邮电出版社, 2007.1

高新技术技能系列丛书

ISBN 978-7-115-15460-6

I. 西... II. ①张... ②宋... III. ①通信网—基本知识 ②通信协议—基本知识

IV. ①TN915 ②TN915.04

中国版本图书馆 CIP 数据核字 (2006) 第 135563 号

内 容 提 要

本书主要介绍了西门子 S7-200/300/400 PLC 的自由口通信、PPI 通信、MPI 通信、PROFIBUS-DP 通信及工业以太网通信的基本概念与应用实例。附录部分还给出了三菱 PLC 与三垦变频器通信的实例, 以扩展读者的知识面。书中各部分内容均采用工程实例进行讲解, 并辅以大量图形, 通俗易懂, 初学者可快速入门。

本书可作为工业自动化领域技术人员的入门读物, 也可供大中专院校自动化、机电一体化专业学生参考, 同时还可作为职业培训学校 PLC 的培训教材。

高新技术技能系列丛书

从入门到精通——西门子工业网络通信实战

-
- ◆ 组 编 广东省职业技能鉴定指导中心
华南理工大学工业培训中心 PLC 培训部
 - 编 著 张运刚 宋小春
 - 责任编辑 张 伟
 - ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销
 - ◆ 开本: 787×1092 1/16
印张: 15
字数: 368 千字 2007 年 1 月第 1 版
印数: 1—5 000 册 2007 年 1 月北京第 1 次印刷

ISBN 978-7-115-15460-6/TN · 2896

定价: 30.00 元

读者服务热线: (010)67129264 印装质量热线: (010)67129223

从入门到

CONG RUMEN DAO
JINGTONG



华

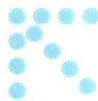
南理工大学工业培训中心PLC培训部是国内专业的自动化技术培训机构，多年来始终致力于为广大从事工业设备制造及工业控制领域的专业技术人员提供广泛的培训服务。培训中心拥有一流的教学设备与教学环境，资深的实践型师资，开设的培训项目包括PLC、人机界面、变频器、工业网络通信与系统监控、交流伺服系统及单片机等。培训中心多年来积累了丰富的培训经验与学习资料，致力成为工业控制领域技术的普及与传播者。

图书服务网站

www.hnlgplc.com

图书服务信箱

hgplc@163.com



从入门到

CONG RUMEN DAO
JINGTONG



丛书特色

全程服务·品质保证

为帮助广大技术人员深入理解本书，工业培训中心PLC培训部开通网站为读者提供网上服务和支
持。读者使用本丛书时遇到的问题，欢迎与我们交流探讨。

突出实践·注重实效

丛书最大的一个特点就是“动了再说”，也就是先编写程序上机实操，然后从实操中理解指令及为什么这样编写，再作小改动上机实操，分析可行或不行的原因，最后作大改动再上机实操，让读者从动手操作中理解编程指令，掌握编程技巧。

实例丰富·轻松上手

丛书内容全部以实例引导，从简单到复杂，让读者一读就会，达到举一反三的作用。同时实例大多是来源于工程实践的典型案例，具有极大的参考价值。

定位准确·面向就业

随着近几年工业制造业的迅猛发展，以自动化控制核心——PLC为中心相关的软件和硬件也蓬勃发展起来，PLC编程和维护人员的社会需求量猛增。本套丛书正是定位于刚刚涉及这一行业或想涉及这一行业而不知如何入门的读者，丛书内容与企业的实际要求密切相关，希望读者能够达到学完即可上岗的效果。

前 言

IT 产业的迅速发展,带领人类进入了信息时代。随着信息技术与计算机技术的飞速发展,工业网络通信将成为工业自动化的又一次革命。

可编程控制器 (PLC) 作为工业自动化的核心控制部分, 单机编程和维护相对简单一点, 而工业网络通信要求同时兼顾稳定性、快速性、灵活性及与第三方设备的兼容性, 所以工业网络通信成为工业自动化系统设置及实施的难点。为了让工业自动化控制的技术人员快速掌握工业网络通信技术, 并能应用于生产实践中, 我们组织编写了本书。

“我梦想一本从简单通信实例到复杂一点的通信实例再到能完成完整系统功能的通信实例——从简单到复杂层层引导, 能做‘老师’的书, 这是我最需要的。”

上面是一些网友在聊天时说出的肺腑之言, 这或许代表了部分在学习工业网络通信知识方面已经花了“九牛二虎之力”, 但还是没有入门而又非常渴望入门的读者们的心声。

很多网友都会问我同样的一个话题“张老师你是怎样入门的?”, 我回答说: “要想入门很容易: 方法是实操、再实操, 最后还是实操。”但很多网友苦于不知道怎样实操, 那么本书一定是你的“指导老师”了。

本书最大的一个特点就是“动了再说”, 也就是先编写程序上机实操, 然后从实操中理解指令及为什么这样编写, 再作小改动上机实操, 分析可行或不行的原因, 最后作大改动再上机实操。这也是我学习工业网络通信从入门到精通的心得。

本书还有一个特点就是以图文形式表达, 力求通俗易懂。书中内容全部以实例引导, 从简单到复杂, 让读者一读就会, 达到举一反三的作用。

全书共分 5 章, 分别介绍了西门子 PLC 的自由口通信、PPI 通信、MPI 通信、PROFIBUS-DP 通信及工业以太网通信的基本概念与应用实例。附录部分给出了三菱 PLC 与三垦变频器通信实例, 目的是扩大读者的知识面和启发读者对系统编程的认识。

华南理工大学工业培训中心的宋小春教授、郭武强、陈耀、何洞宇、周尔根、黄添浓、罗悦文、梁秀洁老师, 华南理工大学工业装备与控制工程学院的宋建老师, 河北华北工程建设公司的黄文涛, 广东省职业技能鉴定指导中心的傅鹤和杨帆对本书的编写和审稿付出了辛勤的汗水, 在此致以诚挚的感谢!

无论你是工业自动化领域的技术人员还是学校里自动化相关专业的师生, 本书一定是你的良师益友, 为你的成功助一臂之力。

由于编者水平所限, 加之时间仓促, 书中难免有不足之处, 恳请广大读者批评指正 (编者 Email:200828029@qq.com), 衷心感谢!

编 者

目 录

第 1 章 西门子 PLC 自由口通信	1
1.1 自由口通信概述	1
1.2 S7-200 CPU 之间的自由口通信实例	3
1.3 S7-200 PLC 与三垦变频器通信实例	16
第 2 章 西门子 PPI 通信	29
2.1 西门子 PPI 通信概述	29
2.2 两台 S7-200 PLC 实现 PPI 通信	30
2.3 多台 S7-200 PLC 实现 PPI 通信	37
第 3 章 西门子 MPI 通信	43
3.1 MPI 通信概述	43
3.2 全局数据包通信方式	43
3.3 无组态连接通信方式	64
3.4 组态连接通信方式	88
第 4 章 PROFIBUS-DP 通信	97
4.1 PROFIBUS-DP 通信概述	97
4.2 与支持 PROFIBUS-DP 协议的第三方设备通信实例	97
4.3 CPU 集成 PROFIBUS-DP 接口连接远程站 ET200M 实例	103
4.4 通过 PROFIBUS-DP 连接智能从站的应用实例	106
4.5 打包式接收与发送, SFC15 及 SFC14 的应用	117
4.6 一主站多从站的 PROFIBUS-DP DX 通信	137
4.7 多主站的 PROFIBUS-DP DX 通信	150
第 5 章 工业以太网通信	167
5.1 以太网 (Ethernet) 概述	167
5.2 工业以太网概述	167

5.3 工业以太网常用的电缆及接头	168
5.4 西门子 S7-200 与 S7-300/400 的以太网通信实例	168
附录 三菱 FX 系列 PLC 与三星变频器通信实例	195
附录实例 1 三菱 PLC 与一台三星变频器通信	195
附录实例 2 三菱 PLC 与多台三星变频器通信	203

第 1 章 西门子 PLC 自由口通信

保 护 密 码 的 系 统 有 许 多 种 形 式 密 码 的 存 储 方 式 密 码 的 输 入 方 式 密 码 的 输 入 时 间 密 码 的 输 入 次 数 密 码 的 输 入 时 间 密 码 的 输 入 次 数 密 码 的 输 入 时 间 密 码 的 输 入 次 数

1.1 自由口通信概述

第三方设备大部分支持 RS485 串口通信，西门子 S7-200 PLC 可以通过选择自由口通信模式控制串口通信。最简单的情况是只用发送指令（XMT）向打印机或者变频器等第三方设备发送信息。不管任何情况，都必须通过 S7-200 PLC 编写程序实现。

当选择了自由口模式，用户可以通过发送指令（XMT）、接收指令（RCV）、发送中断、接收中断来控制通信口的操作。

SMB30（对于 PORT-0 口）或 SMB130（对于 PORT-1 口）用于自由口通信选择、定义波特率和校验类型等。

在 S7-200 处于 STOP 模式时，自由口模式是被禁止的，只有在 RUN 模式，自由口模式才被允许。

SMB30 和 SMB130 分别是 S7-200PLC PORT-0 及 PORT-1 通信口的控制字节，各位表达的意义如表 1-1 所示。

表 1-1 SMB30 和 SMB130 各位的意义

bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
p	p	d	b	b	b	m	m
pp: 校验选择		d: 每个字符的数据位			mm: 协议选择		
00=不校验		0=8 位			00=PPI/从站模式		
01=偶校验		1=7 位			01=自由口模式		
10=不校验					10=PPI/主站模式		
11=奇校验					11=保留（未用）		
bbb: 自由口波特率			（单位：波特）				
000=38400		011=4800			110=115.2k		
001=19200		100=2400			111=57.6k		
010=9600		101=1200			注：查看 CPU 版本		

1. 发送数据

发送指令（XMT）可以发送 1~255 个字节，发送缓冲区的格式如表

1-2 所示。

表 1-2 发送缓冲区的格式

计 数	M	E	S	S	A	G	E
-----	---	---	---	---	---	---	---

MESSAGE——信息字符；

计数——发送信息字符个数（发送前要预先定义）。

检测发送完成有两种方法：①通过发送中断程序；②通过发送完成标志位。

如果有一个中断服务程序连接发送结束事件，在发送信息字符最后一个字符时，则会产生一个中断（对 PORT-0 为中断事件 9，对 PORT-1 为中断事件 26）。

当然也可以不通过中断，而是通过监控 SM4.5（对于 PORT-0）或 SM4.6（对于 PORT-1）的状态来判断发送是否完成，如果状态为 1，说明发送完成。

2. 接收数据

接收指令（RCV）可以接收 1~255 个字节，接收缓冲区的格式如表 1-3 所示。

表 1-3 接收缓冲区的格式

计 数	起始字符	M	E	S	S	A	G	E	结束字符
-----	------	---	---	---	---	---	---	---	------

MESSAGE——信息字符；

计数——接收信息字符计数器（接收到结束字符时自动清零）。

检测接收完成有两种方法：①通过接收中断程序；②通过接收完成标志位。

如果有一个中断服务程序连接接收结束事件，在接收到信息字符最后一个字符时，则会产生一个中断（对 PORT-0 为中断事件 23，对 PORT-1 为中断事件 24）。

当然也可以不通过中断，而是通过监控 SMB86（对于 PORT-0）或 SMB186（对于 PORT-1）的状态来判断发送是否完成，如果状态为非零，说明接收完成。

接收缓冲区的相关字节：

对于 PORT-0 口有 SMB86、SMB87、SMB88、SMB89、SMW90、SMW92、SMB94。

对于 PORT-1 口有 SMB186、SMB187、SMB188、SMB189、SMW190、SMW192、SMB194。

SMB86 和 SMB186 各位表达的意义如表 1-4 所示。

表 1-4 SMB86 和 SMB186 各位表达的意义

bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
n	r	e	0	0	t	c	p

n=1 说明用户通过禁止命令结束接收；

r=1 说明是输入参数错误或者缺少起始和终止条件而接收结束；

e=1 说明是正常接收到结束字符而终止接收；

t=1 说明是接收超时而终止接收；

c=1 说明是接收字符超长而终止接收；

p=1 说明是奇偶校验错误而终止接收。

SMB87 和 SMB187，各位表达的意义如表 1-5 所示。

表 1-5 SMB87 和 SMB187 各位表达的意义

bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
en	sc	ec	il	c/m	tmr	bk	0

- en=0 禁止接收；
 en=1 允许接收；
 sc=0 不使用 SMB88 或 SMB188 起始符检测起始信息；
 sc=1 使用 SMB88 或 SMB188 起始符检测起始信息；
 ec=0 不使用 SMB89 或 SMB189 终止符检测终止信息；
 ec=1 使用 SMB89 或 SMB189 终止符检测终止信息；
 il=0 不使用 SMW90 或 SMW190 的值来检测空闲状态；
 il=1 使用 SMW90 或 SMW190 的值来检测空闲状态；
 c/m=0 定时器是内部字符定时器；
 c/m=1 定时器是信息定时器；
 tmr=0 不用 SMW92 或 SMW192 时间段结束接收；
 tmr=1 使用 SMW92 或 SMW192 时间段结束接收；
 bk=0 不使用中断条件；
 bk=1 使用中断。

1.2 S7-200 CPU 之间的自由口通信实例

1. 所需软硬件及网络配置

本例中用到的软硬件：

- ① S7-200 CPU 两台；
- ② 装有 STEP7 V4.0 软件的个人电脑一台；
- ③ PPI/RS485 编程电缆一条；
- ④ 网络插头及网络电缆。

网络配置如图 1-1 所示。

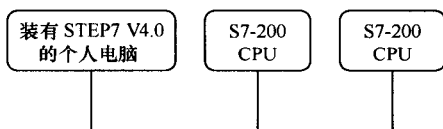


图 1-1 S7-200 CPU 之间的自由口通信网络

2. I/O 分配

两台 S7-200 PLC 通过自由口互相通信，实现甲机 I0.0 启动乙机的电动机星/三角启动控制，甲机 I0.1 终止乙机电机转动；反过来乙机 I0.2 启动甲机的电动机星/三角启动控制，乙

机 I0.3 终止甲机电动机转动。

I/O 分配如表 1-6 所示。

表 1-6

I/O 分配表

甲机 (S7-200 站号 2)	乙机 (S7-200 站号 3)
I0.0 启动乙机的电动机	Q0.0 星形
I0.1 停止乙机的电动机	Q0.1 三角形
Q0.2 星形	I0.2 启动甲机的电动机
Q0.3 三角形	I0.3 停止甲机的电动机

3. 指令表和梯形图程序

S7-200 CPU 之间的自由口通信通过接收中断和发送中断程序实现。

(1) 甲机指令表程序

甲机主程序 (MAIN)

Network 1 // 先让乙机 RUN, 再让甲机 RUN

LD SM0.1

CALL SBR0

Network 2 // 网络标题

// 网络注解

LD SM0.0

CALL SBR1

Network 3

LD SM0.0

MOVB SMB86, VB600

Network 4 // 接收状态计时

LDB= SMB86, 0

TON T40, 10

Network 5 // 接收超时 (超 1s), 自动 STOP

LD T40

STOP

SBR0 程序

Network 1 // 初始化通信参数

// 网络注解

LD SM0.0

MOVB 16#09, SMB30 //PORT-0 口通信参数

MOVB 2#10110000, SMB87 //接收控制信息

MOVB 16#0D, SMB89 //定义结束字符

```

MOVW 5, SMW90      //定义空闲线时间
MOVB 14, SMB94     //定义最大接收字节
                   //中断程序 0 与发送
                   //完成事件联系
                   //允许开中断

```

Network 2 // 声明 50ms 定时中断

// 网络注解

LD SM0.0

MOVB 50, SMB34

ATCH INT0, 10

Network 3 // 声明发送与接收中断

LD SM0.0

ATCH INT1, 9

ATCH INT2, 23

ENI

SBR1 程序

Network 1 //启动乙机星形 M10.0 乙机星形镜像

LD I0.0 //启动乙机星形

EU

AN M10.1 //如果还没启动

S M10.0, 1

Network 2 //星形计时

LD M10.0 //当星形启动后

TON T38, 50 //延时 5s

Network 3 //时间到转三角形 M10.1 乙机三角形镜像

LD T38 //5s 到后

S M10.1, 1 //转换三角形运行

R M10.0, 1 //复位星形

Network 4 //停止乙机

LD I0.1 //停止命令

EU

R M10.0, 2

Network 5 //乙机控制信号星形

LD V201.0 //接收到的状态输出

= Q0.2

Network 6 //乙机控制信号三角形

```
LD V201.1      //接收到的状态输出  
= Q0.3
```

INT0 程序

```
Network 1      //发送  
LD SM0.0  
MOVB 2, VB100  
MOVB MB10, VB101  
MOVB 16#0D, VB102  
XMT VB100, 0
```

INT1 程序

```
Network 1      //接收过程中，禁止时间中断  
//网络注解  
LD SM0.0  
DTCH 10  
Network 2      //发送完就转到接收状态  
//网络注解  
LD SM0.0  
RCV VB200, 0
```

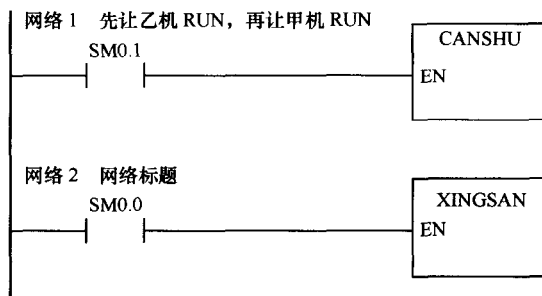
INT2 程序

```
Network 1      //接收完就允许定时中断  
//网络注解  
LD SM0.0  
ATCH INT0, 10
```

(2) 甲机梯形图程序

主程序如图 1-2 所示。

主程序



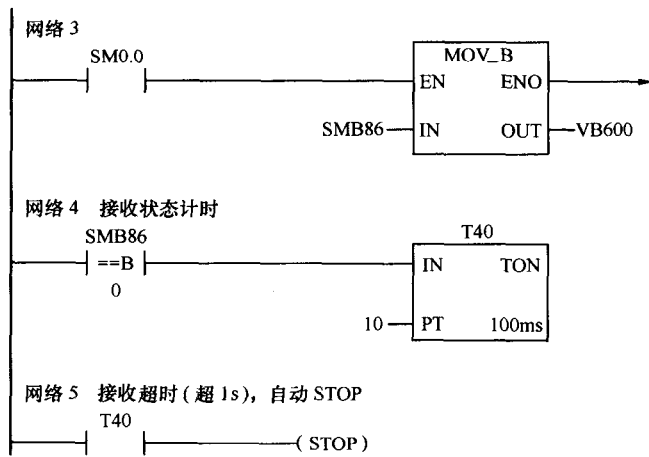
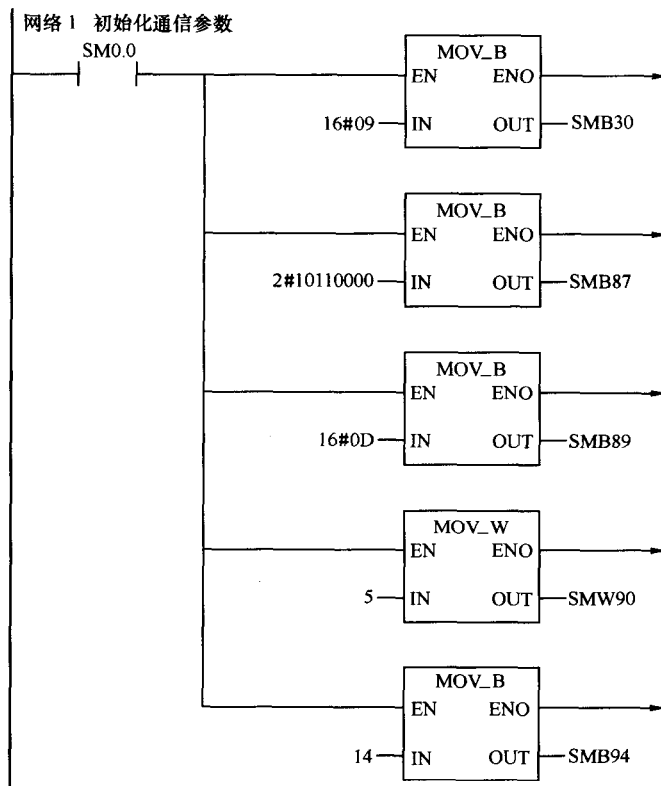


图 1-2 甲机主程序

子程序 0 如图 1-3 所示。

子程序 0



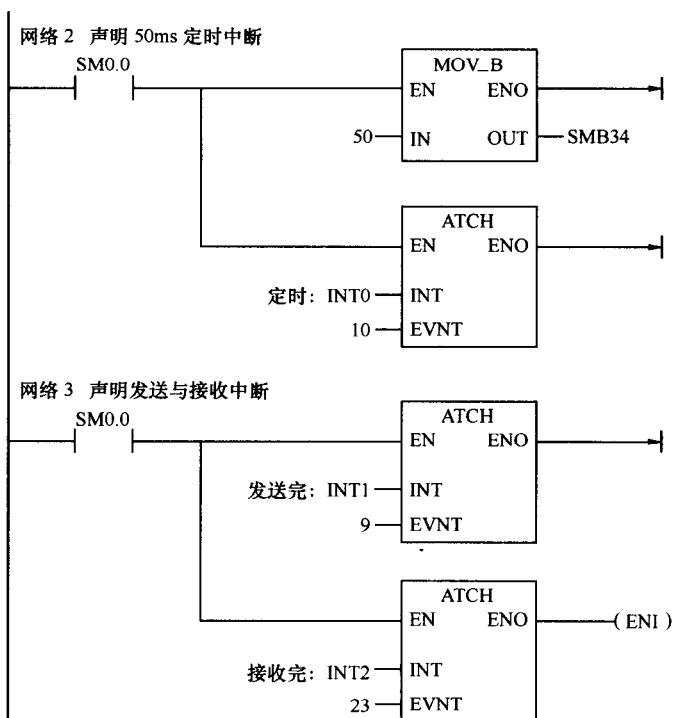
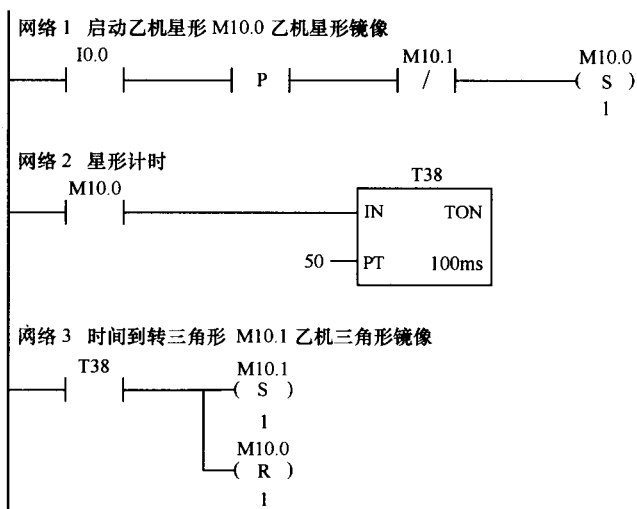


图 1-3 甲机子程序 0

子程序 1 如图 1-4 所示。

子程序 1



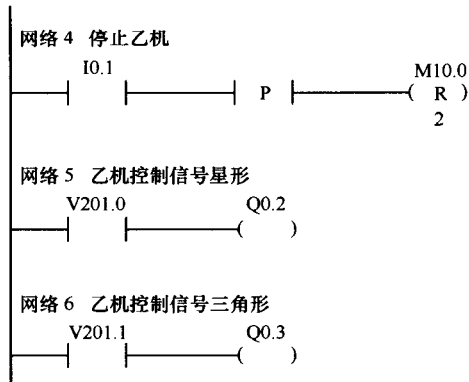


图 1-4 甲机子程序 1

中断程序 0 如图 1-5 所示。

中断程序 0

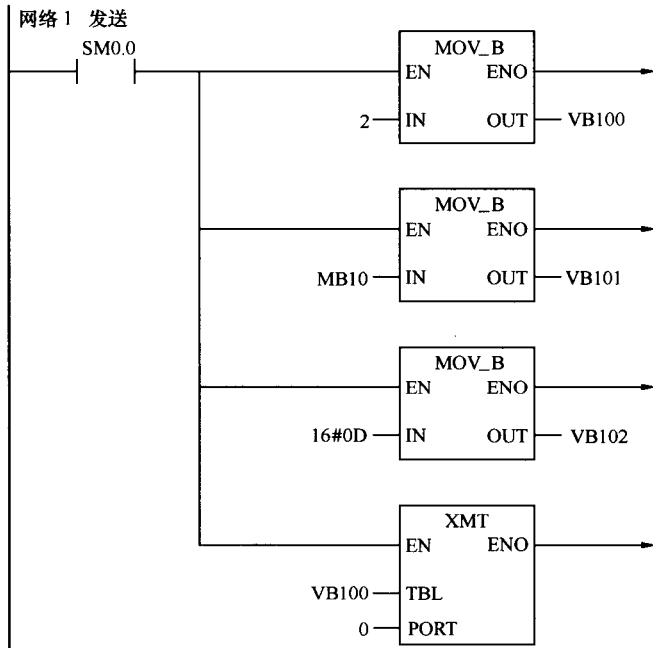


图 1-5 甲机中断程序 0

中断程序 1 如图 1-6 所示。