基于自由口模式的 S7-200 PLC 与上位机的通信*

余中正[1],武 玉[1],夏永胜[2],贡马林[1]
(1.中国科学院等离子体物理研究所,安徽 合肥 230001;
2.合肥工业大学 机械与汽车工程学院,安徽 合肥 230009)

摘 要:详细说明了西门子 S7-200 PLC 在自由口模式下与上位机通信的实现,主要包括该系统的硬件构成,自由口通信协议的标准,以及上位机软件流程和主控 PLC 软件设计。通过自由口通信可实现对 ITER 导体穿缆测力测长系统的监控,将 PLC 数据传送至上位机,实现对数据的处理以及现场数据的实时显示和远程控制等功能。

关键词:PLC;通信协议;自由口模式;ITER 导体穿缆测力测长系统;上位机
中图分类号:TP273.01 **文献标识码**:A **文章编号**:1674-7720(2011)13-0042-03

Communication between S7-200 PLC and host computer based on free-port mode

Yu Zhongzheng[1], Wu Yu[1], Xia Yongsheng[2], Gong Malin[1]
(1.Institute of Plasma Physics, CAS, Hefei 230001, China;
2.School of Mechanical and Automotive Engineering, Hefei University of Technology, Hefei 230009, China)

Abstract: The communication between the Siemens S7-200 PLC and the host computer under the free-port mode is illuminated in detail. The system hardware configuration and the standard free port communication protocols are included and the software program designing method for host PC and main PLC are also given. This communication is applied to monitor the force and length measurement system for ITER conductor insertion and transport data from PLC to the host computer and also realize the function of data processing, real-time display of on-site data, long distance control and so on.

Key words: PLC; communication protocol; free-port mode; force and length measurement system for ITER conductor insertion; host computer

西门子公司的 SIMATIC S7-200 系列 PLC 是广泛适用于中小型设备控制的工业可编程控制器,以其可靠性高、丰富的指令和内置功能、通信能力强、性价比较高等特点,在工业控制领域中得到越来越广泛的应用[1]。在本文的控制系统中,PLC 作为下位机完成现场各种信号和数据的采集、运算和控制[2-4]。工控 PC 机作为上位机可提供人机交互界面,实现数据的处理以及现场数据的实时显示等监视和远程控制等功能。S7-200 系列的 PLC 可以在四种通信模式下工作:PPI 模式、MPI 模式、PROFIBUS-DP 模式和自由口通信模式。其中,PPI 和 MPI 是西门子专门开发的通信协议。PPI 协议用于点对点接口,是一个主/从协议。MPI 协议适用于多点接口,可以是主/主协议或主/从协议。PROFIBUS-DP 是西门子支持的现场总线网络[5]。而大多数用户则是选用对用户完全开放的自由口通信模式。在自由口通信模式下,通信协议是由用户定义的。用户可以用梯形图程序调用接收中断、发送中断、发送指令(XMT)、接收指令(RCV)来控制通信操作。本设计采用自由口方式,重点介绍工控 PC 机与主控 PLC 的通信原理与实现。

*基金项目:国家 ITER 计划 (2008GB101000)

1 硬件组成

ITER 导体穿缆测力测长控制系统的框图如图 1 所示。将测力传感器和测长编码器通过信号线与 PLC 相连,这样穿缆过程中的拉力数据和行程数据就能够实时写入 PLC 的寄存器中。PLC 通过通信电缆与 PC 机的串行通信口相连,在 PC 机中设置 VB 的 MSCOMM 控件来实现

串口通信，这样 PC 机就能读取 PLC 寄存器中的拉力和行程数据，对穿缆过程进行实时监控。

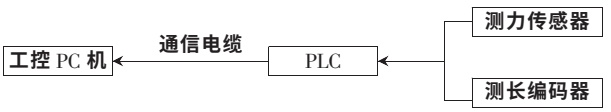

图 1 ITER 导体穿缆测力测长控制系统硬件框图

2 工控 PC 机与主控 PLC 的自由口通信协议

工控 PC 机标准的串口为 RS232C，S7-200 系列提供的串口为 RS485，利用西门子公司提供的 PC/PPI 电缆，可以方便地实现 S7-200 系列 PLC 与 PC 之间硬件连接[1]。

上位机向 PLC 发送指令(即指令帧)，指令帧格式如图 2 所示，由起始字符、指令类型、目标 PLC 站地址、目标寄存器地址、读/写字节数、待写入的数据(当从 PLC 读数据时，具体数据部分为空)、校验码和结束字符组成。

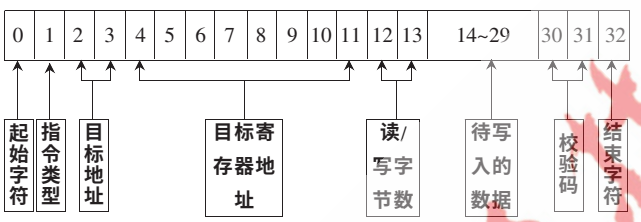

图 2 上位机指令格式

例如写 VB100 开始的两个字节的指令帧如下：83H，06H，08H，00H，00H，64H，30H，32H，31H，32H，33H，34H，35H，36H，115H。下面按顺序说明每段字节的含义：

83H 为字符"S"的 ASCII 码，表示指令的开始，在本设计中是固定的。

06H 表示指令的类型，为写操作。在本文中定义 05H 代表读操作，06H 代表写操作。

08H，00H 表示要写 PLC 中 V 存储区的内容。

00H，64H 表示要从 VB100 开始写。

30H，32H 表示要写两个字节。

31H，32H，33H，34H 表示 VB100 写入 12H，VB101 写入 34H。

35H，36H 是校验和。

115H 为字符"s"的 ASCII 码，是结束字符，表示指令的结束，在本设计中是固定的。

一条指令除包含数据外，还包含必要的控制字（如起始字符、结束字符、指令类型等）。如果指令中的数据直接以其原本的形式传输，则不可避免地会与指令中的控制字发生混淆。为了避免这种情况的发生，可以用文本来传送二进制数据。通过 16 进制 ASCII 码的格式来描述数据，每个二进制的字节都可以表示成一对 ASCII 编码，这对编码表示这个字节的两个 16 进制字符。这种格式可以表示任何的数值，仅仅使用 ASCII 代码的 30H~39H(表示 0~9)和 41H~46H(表示 A~F)。ASCII 码的其余部分可以用作控制字。这样就避免 PLC 因接收到数据中错误的标志位而停止接收的错误。

在 PLC 接到上位机指令后，会向上位机发送一个反馈消息，即反馈帧，反馈帧格式如图 3 所示。其组成与指令帧基本相同，但它是由 PLC 发出的，所以具体数据段不同，在向 PLC 写数据时，反馈帧的具体数据部分为空，而在从 PLC 读数据时，具体数据部分不能为空。

图 3 反馈帧格式

例如，PLC 接收到写 VB100 开始两个字节后的发送反馈帧如下：83H，02H，08H，00H，00H，64H，30H，32H，35H，36H，115H。下面按顺序说明每段字节的含义：

83H 为字符"S"的 ASCII 码，与指令帧相同。

02H 为状态信息，表示接收到上位机指令后 PLC 的执行状态。在本文中 02H 表示写入正确，相应地规定 01H 表示读取正确，03H 表示 BCC 校验码错误，04H 表示指令不合法。

08H，00H 表示要写入 PLC 中 V 存储区的内容，与指令帧相同。

00H，64H 表示要从 VB100 开始写，与指令帧相同。

30H，32H 表示要写两个字节，与指令帧相同。需注意的是，此时具体数据段为空。

35H，36H 是校验和，因无数据段，与指令帧可能不同。

115H 为字符"s"的 ASCII 码，表示此帧结束，与指令帧相同。

3 工控 PC 机软件设计

工控 PC 机端通信程序流程图如图 4 所示。发送指令帧后，注意查询反馈帧，如一定时间内没有接收到，应再次发送，两次无响应，则要提示通信故障或 PLC 不存在。

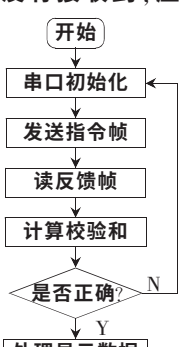

图 4 工控 PC 机通信程序框图

在工控 PC 机中可采用 VB 来实现上位机监控程序，通过 MSCOMM 控件就可控制串口通信[6]，主要参数设置代码如下：

```
MSComm1.Settings="9600,N,8,1"
                    //串口通信参数设置
MSComm1.CommPort=1
MSComm1.PortOpen=True
MSComm1.InputLen=0
```

4 主控 PLC 软件设计

CPU224XP 自由口通信模式的初始化是通过对特殊存储字节 SMB30(PORT0)写入通信控制字来设置通信的波特率、奇偶校验、停止位和数据位数[7]。SMB30 中的内容如下：

PP：奇偶选择。00 为无奇偶校验；01 为偶校验；10 为奇校验；11 为保留。

D：每个字符的数据位。0 为每个字符 8 位；1 为每个字符 7 位。

BBB：自由端口波特率。本设计为 010，表示波特率为 9 600 b/s。

MM：协议选择。00 为点到点接口协议的 PPI 从站模式；01 为自由端口协议；10 为 PPI 主站模式；11 为保留。缺省设置为 00，即 PPI 从站模式。

本文中传输速率固定为 9 600 b/s，数据格式由 1 位起始位、8 位数据位、无校验位、1 位停止位组成。

配置自由口通信模式后，就可以进行数据的收发了。PLC 通信程序框图如图 5 所示。接收数据指令 RCV 的命令格式为 RCV TABLE，Port0，RCV 指令可以接收一个或多个字符，一次最多接收 255 个字符。发送数据指令 XMT 的命令格式为 XMT TABLE，Port0，激活发送缓冲区 TABLE 中的数据。数据缓冲区的第一个数据指明了要发送的字节数，最多有 255 个字符的缓冲区。

图 5 PLC 通信程序框图

通信程序的设计需遵循一定的规则，例如，中断通信处理程序要短小精悍，要避免 XMT 与 RCV 指令在一个端口同时执行[8]。本设计采用主从方式通信，PC 设为主机，PLC 设置为从机。只有 PLC 接收到指令帧后，才可能根据接收数据情况发送反馈帧。为简化程序设计，PC 机只发出读指令和写指令两种指令帧。若为读指令，PLC 准备好发送数据后执行 XMT 指令；若为写指令，PLC 先把数据写入指定存储区，准备好应答数据后同样执行 XMT 命令；若接收到错误帧(如校验错误及不能识别的命令)，PLC 准备相应标志数据执行 XMT 指令。

主要代码如下：

```
LD    SM0.0
MOVB  9，SMB30          //设置端口 0 为：9 600，N，8，1
LD    SM0.0             //RCV 指令初始化
MOVB  16#EC，SMB87
                        //允许接收信息，使用 SMB88，SMB89。
MOVB  83，SMB88         //设置起始字符为"S"
MOVB  115，SMB89        //设置结束字符为"s"
MOVB  +1000，SMW92/     /接收信息时间不能超过 1 ms
MOVB  30，SMB94 //接收的最大字符数，这里设置为 30
R     SMB87.2，1 //复位 SMB87.2，使其为 0，忽略 SMW92
LD    SM0.0
ATCH  RCVOVER，23
        //将 0 口接收完成中断事件连接到 RCVOVER 上
LD    SM0.0
ATCH  XMTOVER，9 、
        //将 0 口发送完成中断事件连接到 XMTOVER 上
LD    SM0.0
ENI                     //允许中断
```

S7-200 自由口通信方式使用户可以自己定义 PLC 指令通信协议，与任何公开通信协议(如 RS-422 或 RS-232C)接口设备进行通信，使通信范围大大增加，控制系统配制更加灵活。本通信程序用于 ITER 导体穿缆测力测长监控系统，PLC 完成数据采集及现场控制，工控 PC 机实时显示导体穿缆的速度及行程，同时以梯形图和通信控件显示动作过程，便于监控及故障诊断，得到用户好评。本文设计的通信协议也可用于其他控制系统的监控。

参考文献

[1] SIEMENS 公司.SIMATIC S7-200 可编程控制器系统手册[M]. http://www2.ad.siemens.com.cn/download/Upload/AS/manual/1109582.pdf, 2008-08-01.

[2] 吉顺平.西门子 PLC 与工业网络技术[M].北京：机械工业出版社，2008.

[3] 刘杰，阳林，陈超丽.三菱 FX2N 系列 PLC 与 PC 通讯的简易实现[J].制造业自动化，2006(1)：65-67.

[4] 陈明意. 基于 VC6.0 的 PC 与 FX2NPLC 通信的实现[J].武汉工业学院学报，2005，24(4)：14-16.

[5] 丁莉君，李宏燕.自由口模下 S7-200 PLC 与上位机的通信[J].机床电器，2009(1)：26-28.

[6] 汤光华，吴青.自由口模式下 S7-200 PLC 与上位机的通信[J].微计算机信息，2008(24)：62-64.

[7] 刘红兵.S7-200 自由口通讯的实现及应用[J].PLC&FA，2009(2)：58-62.

[8] 李绍民，潘登.S7-200 PLC 与上位机的通信[J].大连民族学院学报，2009，11(3)：209-211.

(收稿日期：2011-03-05)

作者简介：

余中正，男，1986 年生，硕士研究生，主要研究方向：运动控制。

武玉，男，1964 年生，研究员，博士生导师，主要研究方向：超导磁体与核能科学。