中国农业大学学报 2005,10(2):65-69
Journal of China Agricultural University

基于 VC 的上位机与 PLC 可靠通信的实现方法

侯军卫 刘玉锋 王荣杰
(中国农业大学 工学院,北京 100083)

摘 要 针对目前市场上上位机通信软件专用、封闭、不兼容等问题,提出了用 VC 实现上位机与 PLC 通信的方法。采用西门子公司的 S7-200 系列 PLC 为下位机,按照 RS-485 标准与上位机通信;通信协议为以自由口模式创建用户自定义的协议,数据传输格式为 16 进制 ASCII 编码,求和校验;上位机采用 VC 编程的可视化界面,在编程过程中采用不可中断方式和多缓冲区结构,并建立相应的控制指针。试验结果表明,当数据传输速率为 9.6 kbit/s 时误码率 $< 10^{-5}$,能够实现现场网络的在线监控、调试及数据修改。

关键词 串行通信;可编程控制器;VC 编程;PLC
中图分类号 TP 271.4 **文章编号** 1007-4333(2005)02-0065-05 **文献标识码** A

A VC-based approach to realize a reliable communication between PLC and IPC

Hou Junwei, Liu Yufeng, Wang Rongjie
(College of Engineering, China Agricultural University, Beijing 100083, China)

Abstract The interfaces of most PC(IPC) communication software in the market has the problems of individual, enclosed, and less compatibility. The paper developed a VC-based communication approach for the communications between PLC and IPC and adopted PLC-S7-200 of SIEMENS as slave device, which communicate with IPC by RS-485 standard, in the realized system. A user-defined protocol created by freeport mode was taken as the communication protocol, and hexadecimal ASCII code as the form of data transform to verify the sum of ASCII. A non-maskable-interrupt and a multi-buffer structure were adopted and a corresponding controlling pointer was set up during the course of date receiving and sending. The test results indicated that the functions of online surveillance and remote debugging and amending could be realized with code-error less than 10^{-5} when transferring data at a speed of 9.6 kbit/s.

Key words serial communication; programmable controller; VC programming; PLC

可编程控制器由于可靠性高、抗干扰能力强等优点广泛应用于工业、农业、国防等自动控制领域[1-2]。实际工程中为了便于现场设备的监控,需要与 PLC 具有通信功能的上位机来获取现场数据[3]。随着个人计算机的普及和开放系统概念的推广,基于个人计算机的监控系统开始进入市场。目前国外开发的上位机监控应用软件很多,如工控组态软件 WINCC、InTouch 和 FIX 等,但都是专用(即与硬件相关)和封闭的,各自为一套体系,互不兼容;同时国内应用的可编程控制器大部分是国外产品,所提供的与其配套的上位机产品功能复杂、价格高,用户量少,不适合广泛推广使用。国内有多家独立的软件商专门从事工业控制组态软件的开发;但大多是基于 MS-DOS 用汇编语言实现的,随着 Windows 操作系统的普及产品竞争力逐渐降低[4]。针对上述问题笔者以西门子公司的 S7-200 系列的 PLC①为研究对象,提出了一种用 VC 实现上位机与 PLC 通信的方法。

收稿日期:2004-11-04
作者简介:侯军卫,硕士研究生;刘玉锋,副教授,主要从事新型机电一体化设备研究,E-mail:L168yf@tom.com
① SIMATIC S7-200 可编程序控制系统手册. SIEMENS 公司,2002

1 通信协议原理

根据双方的通信要求,自定义了通讯协议[5]:上位机向目标从站PLC发出接收数据的指令,每个从站PLC都接收来自上位机的指令后,各自进行目标站地址的确认;如果目标站地址和本从站事先设置好的地址不同则不做出响应,反之开始判断接收的数据是否完整正确;如果数据完整正确,目标从站PLC开始读取接收缓冲区内的数据,完成一系列的内部逻辑判断、数据移动后,再按要求向上位机发送返回数据;如果不正确则拒绝接执行上位机传送的数据,并向上位机发送错误信息。上位机接收各从站传送上来的数据完成数据信息的交换,达到通信的目的。

本研究采用了自定义的通信协议,格式如下:

上位机发送指令

SA	DT	DA	LE	DU	FC	EA

上位机接收指令

SA	DU	FC	EA

PLC发送指令

SL	SA	DU	FC	EA

PLC接收指令

RL	SA	DT	DA	LE	DU	FC	EA

其中各指令代码的意义为:

SA,起始字符;

DT,指令类型;

DA,目标PLC站地址;

LE,读写字节长度;

DU,数据区;

FC,校验码;

EA,结束字符;

SL,发送的字节数;

RL,接收的字节数。

在自定义的通信协议中起始字符定义为ASCII码的"q",结束字符为"Q",指令类型定义为:57H代表"读"ASCII码为"W",52H代表"写"ASCII码为"R"。目标从站PLC地址占2B以16进制ASCII码表示,读写字节数占2B以16进制的ASCII码表示,数据区固定为8B也以16进制的ASCII码表示,这样1次可传输4B的信息。校验码采用指令类型+目标PLC站地址+读写字节数+数据区以字节为单位作异或和。1条指令除包含数据外,还包含必要的控制指令(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,则不可避免的会与指令中的控制指令发生混淆,有可能使PLC接收到的指令不完整,产生误动作。为了避免这种情况的发生,采用文本传输二进制数格式。例如上位机向目标站地址为5(00000101B)的PLC写入4B的数据E6H、27H、A1H、C3H,则整个上位机数据发送字符格式为:

q	W	0	5	0	4	E	6	2	7	A	1	C	3	2	D	Q

2 硬件连接

计算机的串行接口适用于数据传输速率0～20 kbit/s的通信。西门子公司的S7-200系列PLC内部有集成的通信接口,其中有自由端口模式,符合IEEE-RS-485标准协议[6]。该端口模式可以由用户程序控制,因此在程序中可以利用接收完成中断、字符接收中断、发送完成中断、发送指令和接受指令等功能来控制通信过程。在自由端口模式下,通信协议完全由用户自己决定,这样就可以把不同的通讯口连接起来。计算机串口采用EIA-RS-232标准[6],其数据信息逻辑"1"的电平<-3 V,逻辑"0"的电平>3 V;对于控制信号,接通状态即3 V<信号有效电平<15 V,断开状态即-15 V<信号无效电平<-3 V。RS-485协议利用差分方式传输信号,系统只需检测两线之间的电位差而无需有电压参考点,因此为了实现计算机和PLC的通信就必须进行物理层电气协议转换[5]。本研究采用了电平转换驱动芯片MAX232和SN75176。开始工作时,上位机发送数据给各个从站,数据格式以零电平为起始位,起始位后跟随地址和数据字节等,从站中的地址与目标站地址一致时从站被激活。因为只有上位机对驱动芯片作初始化操作,从站只在被激活后应答,所以在1次通讯中不会出现数据冲突。为了保证数据可靠传输,上位机与各个从站采用同一地为参考;为保证静态条件下$U_a - U_b > 200$ mV,没有在RS-485芯片上附加额外的上拉电阻和下拉电阻[6]。这样就完成物理层协议的转换任务。硬件连接见图1。

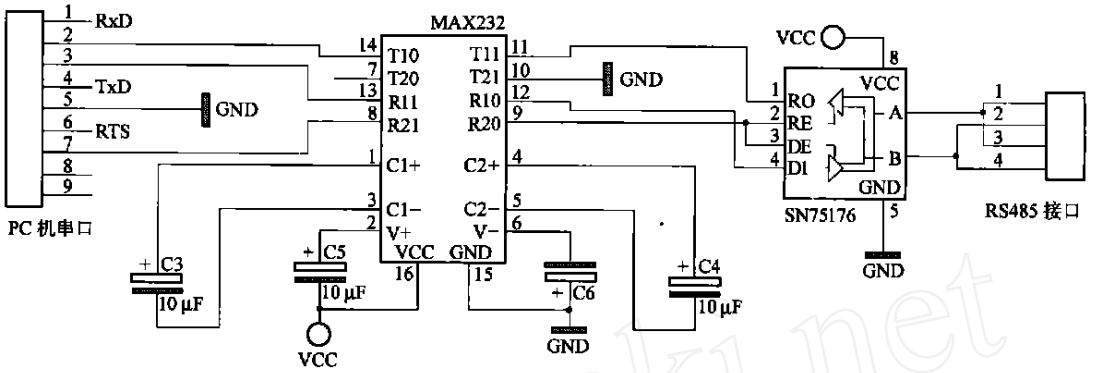

图 1　计算机和 PLC 硬件连接图

Fig. 1　Connection between IPC and PLC

3　软件设计

3.1　上位机部分程序

VC 提供了 MSComm(microsoft communications control)控件,通过串行口进行数据传输和接收,为应用程序提供串行通信功能。可以通过选择“Project →Add To Project →Components and Controls”菜单命令把 MSComm 控件加入到工程中。MSComm 控件通信功能的实现实际上是调用了 API 函数,而 API 函数是由 Comm.drv 解释并传递给设备驱动程序进行的,即 MSComm 控件的属性提供了通信接口的参数设置,能实现串行通信[7]。MSComm 控件有关属性如下。

CommPort:设置并返回通信端口号,Windows 系统将会利用该端口与外界通信;

Setings:设置并返回初始化参数,其组成格式为“BBBB,P,D,S”,BBBB 为数据速率,P 为奇偶校验,D 为数据比特,S 为停止位;

PortOpen:设置并返回通信端口的状态,也可以打开和关闭端口;

Ouptut:向传输缓冲区写 1 B 的数据;

Input:将传送到输入缓冲区的字符读到程序里;

RThreshold:设置在产生 OnComm 之前要接受的字符数;

InputLen:设置并返回 Input 属性从接收缓冲区读取的字符数;

InBbuffersize:设置或返回输入缓冲区的大小;

InBufferCount:返回输入缓冲区内等待读区的字节个数,可通过设置该属性值为 0 来清除接收缓冲区;

InputMode:设置或返回传输数据的类型;

CommEvent:传回 OnComm 事件发生时的数值码;

装载窗体时初始化并打开串口:

```
m_Com.SetCommPort(1);
m_Com.SetInBufferSize(1024);
m_Com.SetOutBufferSize(512);
if(!m_Com.GetPortOpen())
m_Com.SetPortOpen(TRUE);
m_Com.Settings("9600,n,8,1");
m_Com.SetRThreshold();
m_Com.SetInputLen(1);
m_Com.SetInputMode(0);
```

接收主程序:

```
void CmainFrame::OnCommMscomm()
{VARIANT vResponse;
int n;
if(m_Com.GetCommEvent() == 2);
{n = m_Com.GetInBufferCount();
if(n > 0){
vResponse = m_Com.GetInput();
…//以下是对数组的处理,包括数据校验,数据转换等。
}
}
}
```

发送主程序:

```
void CmainFrame::OnCommSend()
{…//准备要发送的数据存放在数组 SxData[]中
```

```
CbyteArray Send;
Send. RemoveAll() ;
Send. SetSize(m) ;
For(i = 0;i < m;i + +)
Array. SetAt(i,SxData[i]) ;
m.Com. SetOutput(ColeVariant(Send)) ;
}
```

在实际应用中,从站被动的接收上位机发出的指令后做出响应,然后将信息传回上位机,由于上位机在整个通信的过程中不能被中断,因此上位机在接收与发送数据过程中采用了不可中断的方法。本研究把通信软总线设计在单独的线程中,专门用于监视串行口的输入,从计算机串口设备接收数据,并将接收到的数据送到数据处理线程中显示和处理。为保证数据传输的实时性和完整性,采用多缓冲区结构,并建立相应的控制指针[4-6]。

3.2 从站 PLC 程序

S7-200 系列 PLC 选择了自由口通信方式后,在程序中就可以使用接收中断、发送中断、接收指令(RCV)、发送指令(XMT)来控制通信操作,当处于自由口模式时通信协议完全由用户程序指令控制。SMB30 被用于选择比特率和校验类型,各个位的配置为:

	7							0
SMB30	p	p	d	b	b	b	m	m

pp,校验选择:00 为不校验,01 为偶校验,10 为不校验,11 为奇校验;

d,每个字符的数据位数:0,每个数字符 8 位;1,每个数字符 7 位。

bbb,自由口比特率,kbit/s:000 为 38.4,001 为 19.2,010 为 9.6,011 为 4.8,100 为 2.4,101 为 1.2,110 为 115.2,111 为 57.6。

mm,协议选择:00,PPI/从站模式;01,自由口模式;10,PPI/从站模式;11,保留。

接收指令(RCV)启动或终止接收信息功能,必须为接收操作指定开始和结束条件。发送指令(XMT)在自由口模式下依靠通讯口发送数据。

PLC 程序分为主程序和中断程序。主程序完成初始化通信口、开中断、判断、发送数据等功能,中断程序完成接收和发送数据的功能。主程序为:

```
NETWORK 1
LD SM0.1
CALL Initialize
NETWORK 2
LDB = VB118, VB131
AB = VB102, 52H
A M0.0
CALL Write
NETWORK 3
LD M0.1
CALL Switch
NETWORK 4
LD SM4.5
RCV VB100,0
```

初始化:

```
Initialize
NETWORK 1
LD SM0.0
MOVB 9, SMB30
NETWORK 2
LD SM0.0
MOVB 16# EC, SMB87
MOVB 113, SMB88
MOVB 81, SMB89
MOVB +1000, SMW92
MOVB 36, SMB94
R SM87.2, 1
NETWORK 3
LD SM0.0
ATCH Receive, 23
NETWORK 5
LD SM0.0
ENI
NETWORK 6
LD SM0.0
MOVB 5, VB199
NETWORK 7
LD SM0.0
MOVB &VB102, VD123
```

中断程序为:

```
Receive
NETWORK 1
LD SM0.0
ATH VB103, VB118,2
ATH VB115, VB119,2
S M0.1, 1
```

```
MOVB 0, VB120
MOVB &VB102, VD123
Switch
NETWORK 1
LD SM0.0
R M0.1, 1
NETWORK 2
LD SM0.0
FOR VW121, +1, +13
NETWORK 3
LD SM0.0
XORB *VD123, VB120
NETWORK 4
LD SM0.0
INCD VD123
NETWORK 5
NEXT
NETWORK 6
LDB = VB120, VB119
AB = VB117, 81
S M0.0, 1
Write
NETWORK 1
LD SM0.0
R SM87.7, 1
R M0.0, 1
RCV VB100, 0
NETWORK 2
LD SM0.0
MOVD &VB107, VD127
NETWORK 3
LD SM0.0
ATH VD127, *VD135, 8
```

4　结束语

以中国农业大学工学院 Me093399 型机电一体化系统为平台,对通信协议采用的数据传输格式和处理方法进行了实验验证,结果表明:该方法以 9.6 kbit/s 的数据传输速率传输数据时误码率 $< 10^{-5}$,能够实现现场网络的在线监控、调试及数据修改;由于程序中采用了以 16 进制 ASCII 码描述数据传输格式,因此 1 条指令中的数据字节和控制字节不可能发生混淆,通信更加可靠。

本方法可应用于其他机电一体化通信工程中。

参　考　文　献

[1] 郑晟,巩建平,张学. 现代可编程序控制其原理与应用[M]. 北京:科学出版社,2003. 3 - 9

[2] 廖常初. PLC 编程及应用[M]. 北京:机械工业出版社,2002. 6 - 12,133 - 162

[3] 阳宪惠. 现场总线技术及其应用[M]. 北京:清华大学出版社,1999. 4 - 16

[4] 王亚民,陈青,刘畅生,等. 组态软件设计与开发[M]. 西安:安电子科技大学出版社,2003. 4 - 11,89 - 132

[5] 李增智. 计算级网络原理[M]. 西安:西安交通大学出版社,1998. 37 - 108

[6] GB/T 6107—2000 串行二进制数据交换的数据终端设备和数据电路终接设备之间的接口[S].

[7] 李现勇. Visual C++ 传口通信技术与工程实践[M]. 北京:人民邮电出版社, 2002. 56 - 144