

S7-200 系列 PLC 自由口模式下实时通信技术研究

刘瑞婷, 张南平, 陈 勇

(武汉理工大学 计算机与技术学院, 湖北 武汉 430070)

摘 要:在实际工业控制系统应用环境中,研究 PLC 自由口模式的通信有助于实现 PLC 与 Windows 程序开发环境间的实时通信。通过研究 PLC 自由口模式的通信,系统实现了 C++ Builder 6.0 与 PLC 的实时通信,从而实现工业控制系统中上下位机的通信,将由 PLC 采集的数据进行实时显示和控制,并将数据以数据库的形式存储起来以便研究和分析。

关键词:PLC; 实时通信; 数据采集; 自由口模式

中图分类号: TP335

文献标识码: A

文章编号: 1673-629X(2006)12-0156-03

Research of Real-Time Communication Between PC and Series S7-200 PLC in Free-Mode

LIU Rui-ting, ZHANG Nan-ping, CHEN Yong

(School of Computer Techn., Wuhan Univ. of Techn., Wuhan 430070, China)

Abstract: In real industry control system application environment, it's helpful to realize the real-time communication between PLC and Windows. According to research on free-mode communication of PLC, this system has achieved real-time communication between C++ Builder 6.0 and PLC. So as to achieve up and down machine communication in industry control system, display and control the data collected by PLC software in real-time and save the data to database for research and analysis.

Key words: PLC; real-time communication; data-collection; free-mode

0 引言

在实际工业控制中,西门子 S7-200 系列 PLC 可以实现对传感器数据的采集,但 PLC 对数据的显示和控制没有 Windows 图形控制界面方便。PLC 编程软件只能对所采集的数据瞬时存放,并不能对数据进行批量数据库形式的存储,且 PLC 编程软件对采集参数的显示并不直观和友好,所以需要 Step7-Micro/WIN 所采集的参数进行集中管理和实时显示。尽管 SIEMENS 提供了大量的通信方式和组态软件,但费用偏高,不适用于中小规模控制系统的应用^[1]。故而在实际工业控制系统应用环境中,有必要研究 PLC 自由口模式的通信,实现 PLC 与 Windows 程序开发环境间的实时通讯。此研究将可以很大程度上提高工业控制系统效率及缩小开发成本。C++ Builder 6.0 是 Borland 公司推出的集成度较高、较复杂的可视化开发环境,是很理想的实现界面控制的工具,其对串口编程的支持为其实现与 PLC 的实时通讯提供了良好的研究条件。由 C++ Builder 开发的上位机通信程序可以提供良好的人机界面,具有强大的数据处理能力和图像

显示能力,能够进行全系统的监控和管理,而 PLC 作为下位机能适应恶劣的工业环境,可靠性高,适合现场控制。因此,把 PLC 和 PC 机通过通信线连接起来,达到优势互补,就能形成一个功能良好的数据采集显示以及控制系统。

1 使用自由端口通信功能和 PC/PPI 电缆的通信

因为上位机采用的是 RS232 接口,而 PLC 只配有一个 RS485 接口,所以利用西门子公司 PC/PPI 电缆,可将 PC 机与西门子的 S7-200 PLC 连接起来组成 PC/PPI 网络,实现点对点的控制。RS485 只需 2 根数据线 TXD 和 RXD 来发送数据和接收数据,但通信双方不能同时收发(即只能采用半双工制)。由于只有 2 根数据线而无硬件握手信号线,所以只能采用软件握手的通信方式来保持数据传输的同步。使用 PC/PPI 电缆和自由端口通信功能可实现 S7-200 CPU 与 RS-232 标准兼容的设备的通信。使用带 RS-232 口的隔离型 PC/PPI 电缆,用 5 个 DIP 开关设置波特率和其他配置项。当数据从 RS-232 传送到 RS-485 口时,PC/PPI 电缆是发送模式。当数据从 RS-485 传送到 RS-232 口时,PC/PPI 电缆是接收模式。检测到 RS-232 的发送线有字符时,电缆立即从接收模式切换到发送模式。RS-232 发送线处于闲置的时间超过电缆切换时间时,电缆又切换到接收模式。这个时

收稿日期:2006-03-29

作者简介:刘瑞婷(1982-),女,河南郑州人,硕士研究生,研究方向为计算机网络技术、计算机应用技术;张南平,教授,硕士研究生导师,研究方向为计算机网络技术、ERP、办公自动化。

间与电缆上的 DIP 开关设置的波特率有关,见表 1。

表 1 PC/PPI 电缆切换时间

波特率/bps	切换时间/ms
38 400	0.5
19 200	1
9 600	2
4 800	4
2 400	7
1 200	14
600	28

5 开关 PC/PPI 电缆的 5 号开关设为 0 时,RS-232 口为数据通信设备(DCE)模式;设为 1 时,为数据终端设备(DTE)模式。这个接口上提供的信号有发送数据、申请发送、接收数据和地。5 开关 PC/PPI 电缆不使用或不提供清除发送信号(CTS)。表 2 是 PC/PPI 电缆各引脚的定义。

表 2 RS-485 到 RS-232 DTE 连接器引脚

RS-485 连接器引脚		RS-232 DTE 连接器引脚	
引脚号	信号说明	引脚号	信号说明
1	地(RS-485 逻辑地)	1	数据载波检测(DCD 不用)
2	24V(RS-485 逻辑地)	2	接收数据(RD,输入到 PC/PPI 电缆)
3	信号 B(RxD/TxD+)	3	发送数据(TD,从 PC/PPI 电缆输出)
4	RTS(TTL 电平)	4	数据终端就绪(DTR 不用)
5	地(RS-485 逻辑地)	5	地(RS-232 逻辑地)
6	+5V	6	数据设置就绪(DSR 不用)
7	24V 电源	7	申请发送(RTS,PC/PPI 电缆输出)
8	信号 A(RxD/TxD-)	8	清除发送(CTS 不用)
9	协议选择	9	振铃指示器(RI 不用)

为保证通信的安全性,必须对传送的数据进行校验,主要措施是:把所发送的字节进行异或运算后连同要发送的有效数据一起发送。接收方收到后,同样对所接收的有效数据进行异或处理,并把处理结果与接收到的在发送方已进行异或处理的字符相比较,如果两者不相等就认为传输数据出错。对于检验到出错的数据采取放弃的措施,并立即发送反馈信号给上位机要求重新发送数据^[2]。

2 系统通信原理

自由通信模式下 PLC 的控制程序可以使用接收中断、发送中断、发送指令(XMT)和接收指令(RCV)来控制通信操作。S7-200 的 CPU 处于 RUN 模式时,能够进行自由端口通讯。在这一模式下,用户可以通过 PLC 程序来选择协议,可以使用接收中断、发送中断、发送指令(XMT)和接收指令(RCV)来进行通信操作^[3]。在 RUN 模式下,对于 PORT0(PORT1),当 SMB30 协议选择域(nm)置 1(SMB130 协议选择域(nm)置 1)时,便选择了自由端口模式。在 STOP 状态下,自由端口模式被禁止,CPU 能够与可编程设备(如编程器)之间通讯。

SMB30 用于设置端口 0 通信的波特率和奇偶校验等参数。CPU 模块如果有两个端口,SMB130 用于端口 1 的设置。自由端口控制字节描述如表 3 所示。

表 3 自由端口控制字节

端口 0	端口 1	描述								
SMB30 的格式	SMB130 的格式	<table><tr><td>P</td><td>P</td><td>D</td><td>B</td><td>B</td><td>B</td><td>M</td><td>M</td></tr></table>	P	P	D	B	B	B	M	M
P	P	D	B	B	B	M	M			
SM30.6 和 SM30.7	SM130.6 和 SM130.7	PP: 奇偶校验选择, 00 = 不校验, 01 = 偶校验, 10 = 不校验, 11 = 奇校验								
SM30.5	SM130.5	D: 每个字符的数据位, 0 = 8 位 / 字符, 1 = 7 位 / 字符								
SM30.2 ~ SM30.4	SM130.2 ~ SM130.4	BBB: 自由端口的波特率 / bps 000 = 38400, 001 = 19200, 010 = 9600, 011 = 4800, 100 = 2400, 101 = 1200, 110 = 600, 111 = 300								
SM30.0 和 SM30.1	SM130.0 和 SM130.1	MM: 协议选择, 00 = PPI / 从站模式, 01 = 自由口协议, 10 = PPI / 主站模式, 11 = 保留								

本上下位机通信系统通信原理如图 1 所示。

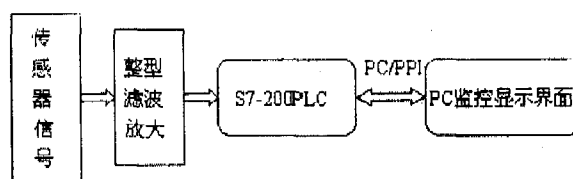


图 1 上下位机及系统通信原理

3 上下位机通信软件实现

3.1 S7-200 PLC 自由通讯口编程

自由口通讯是通过用户程序控制 S7-200CPU 通讯口的操作模式。通过自由口模式可以连接多种职能设备:比如打印机、条形码读写设备、PC 机等,而且用户利用自由口通讯可以浏览 Web 站点。在自由口模式下,通过使用接收中断、发送中断、发送指令(XMT)和接收指令(RCV)来和上位机通信。此时,通讯协议完全由用户程序控制^[4]。

3.1.1 PC 机定时接收 PLC 发送的数据

PLC 通信程序设计部分代码如下:

```

LD SM0.1 //MAIN
MOVB 9, SMB30 MOVB 250, SMB34
MOVB 2, VB100 MOVB 16#45, VB101
MOVB 16#46, VB102 ATCH INT-0, 10
ENI
LD SM0.0 //INT0
XMT VB100, 0 ATCH INT-1, 9
CRETI
  
```

实际工业测控数据采集测控系统中,只需要将存储所采集数据的存储区中的内容传送给相应的 PLC 发送单元即可完成实时采集数据的实时显示。

3.1.2 PLC 接收自 PC 机发送的数据

在以下通信程序中,PLC 接收自 PC 机发送的数据,当接收到字符结束标志符时,信息又发回到发送方。其 PLC 程序部分代码如下:

```

LD SM0.1 MOVB 16#9,SMB30 //MAIN
MOVB 16#B0,SMB87 MOVB 16#23,SMB89
MOVB +5,SMW90 MOVB 100,SMB94
ATCH 0,23 ATCH 2,9
  
```

```

ENI RCV VB100,0
//INT0
LDB= SMB86,16#20 MOVB 10,SMB34
ATCH 1,10 CRETI
NOT RCV VB100,0
RETI
//INT1
LD SM0.0 DTCH 10
XMT VB100,0 RETI
//INT2LD SM0.0 RCV VB100,0
RETI

```

3.2 C++ Builder 6.0 通信程序设计

上位机软件通信部分使用了 MSComm 控件,通过设置其属性参数就可以实现串行通信,所以大大简化了程序设计。通信程序的部分代码如下^[5]:

串口及通信参数初始化

```

MSComm1 -> CommPort = 1;
If (MSComm1 -> PortOpen == false)
MSComm1 -> PortOpen = true;
MSComm1 -> Settings = "9600,N,8,1";
... //通信参数初始化

```

PC 与 PLC 通信程序部分关键代码如下:

```

Void_fastcall TMainForm::SendToPLCClick (TObject *
Sender)
{ MSComm1 -> Output = InputData -> Text; }
Void_fastcall TMainForm::ReceiveFromPLCClick (TObject *

```

(上接第 155 页)

由于安装在十字路口的摄像头和固定线圈采集点对实时视频信息质量要求特别高,为了分辨出违章的车牌号码和采集到实时、可靠的路况交通情况等信息,基于 P800 的信息采集系统对视频信息的采集、压缩、转送的编码应用程序基于以上流程很好地实现了需求的功能。大致实现过程为:把采集到的原始 YUV 数据从内存映像表中以合适的 API 函数取出,再通过编码插件(H.264 编码方式)程序对 YUV 原始数据进行高质量压缩,然后按照系统给的相关文件接口把压缩好的数据转化成 AVI 文件格式,最后通过 FTP 协议进行封装把数据包传送给服务器。如果为了快速传送的需求,可以把 AVI 文件转化成 3GP 文件,不过这样传送的视频图像效果会不理想。

3 基于 P800 智能终端信息采集平台在移动奥运智能交通中的应用

P800 智能终端的开发主要服务于北京 2008 移动奥运智能交通项目,为了体现出 2008 奥运会“科技奥运”的理念,P800 智能终端的开发紧密结合了科技最新进展,集成科技创新成果,可以体现北京奥运会成为展示高新技术成果和创新实力的窗口。通过系统测试和局部地区的投

Sender)

```

{ MSComm1 -> InputLen = 0; DisplayData -> Text =
MSComm1 -> Input;
MSComm1 -> PortOpen = false; }

```

4 结 论

通过对 S7-200PLC 自由端口模式通信的软硬件研究,本通信系统成功地实现了 PLC 与 PC 机之间的实时串行通信,为工业控制系统数据监控及存储提供了良好的解决方案,大大缩减了工业数据采集控制系统的开发费用。并在汽车车载数据采集系统中投入实际应用且运行稳定,完全能满足实时数据采集监控系统的要求。

参考文献:

- [1] 李腊元,李春林.计算机网络技术[M].北京:国防工业出版社,2001:60-80.
- [2] Filicori P F, Hill L H. Error estimation in sampling digital wattmeters[J]. IEEE Proceedings, 1985, 132: 166-173.
- [3] 许毅,熊文龙,雷静.基于 PC 与 S7200 实现自由通信协议的研究[J].武汉理工大学学报:交通科学与工程版, 2002, 26(4): 513-515.
- [4] 西门子公司. STEP7 用户手册[M].北京:西门子(中国)有限公司自动化部,1996.
- [5] 范逸之,江贤文,陈立元. C++ Builder 与 RS-232 串行通信控制[M].北京:清华大学出版社,2002.

入使用后,经实践证明 P800 工作状态良好,满足了需求。

4 结束语

P800 智能终端使用 A-GPS 模块能使移动车辆的地理位置定位信息更精确、更可靠;且能够采集到清晰的视频图像供实时监控使用;另外,通过实践测试证明,预计在 2008 奥运会 P800 的投入使用除了会体现“科技奥运”的理念外,另一方面也会发掘和体现 IPv6 的特点,并验证 IPv4 业务的平滑过渡和兼容性。

参考文献:

- [1] Kaplan E D. GPS 原理与应用[M].北京:电子工业出版社, 2002.
- [2] Lagrange X. GSM 网络与 GPRS[M].北京:电子工业出版社, 2002.
- [3] Sony Ericsson Mobile Communications International. GR47 Design Guidelines[R]. [s.l.]: Sony Ericsson Inc, 2003.
- [4] 李云,杨玉峰,梅顺良. ITS 系统中 GPRS 智能移动终端的设计[J]. 电讯技术, 2004, 16(3): 25-28.
- [5] 杨东凯,张其善. 集群通信技术在 GPS 车辆监控系统中的应用[J]. 电子产品世界, 2000, 11(6): 15-18.