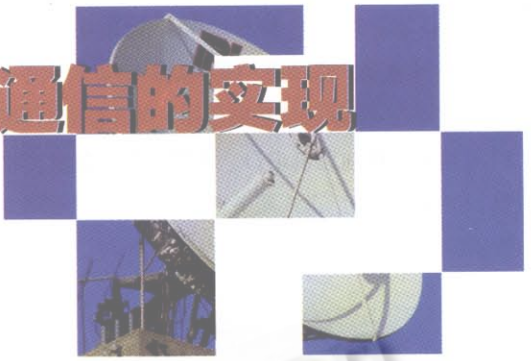
变电站SCADA系统上位前置机与PLC通信的实现

湖南大学电气与信息工程学院　魏育成　王耀南　何庆宁



本文介绍了一种以PLC为IED设备的新型SCADA系统的结构，并说明了SIEMENS公司的S7-200系列的PLC的功能和特点。分析和讨论了上、下位机之间的通信方式和工作原理，以及前置机与PLC通信的具体实现。

引言

随着大量的智能设备(IED-intelligent electronic device)在变电站系统的装备，变电站综合自动化的研究也逐渐成为一个新的热点。SCADA(Supervisory Control and Data Acquisition)系统是变电站综合自动化的最基本的功能，它的主要任务是采集和管理各IED的实时生产数据，对生产过程进行监视和控制，并保存历史数据和故障事件，提供报表输出和计算、分析。所以，SCADA系统的首要任务是按一定格式的规约完成与底层IED设备的通信功能，以实现实时现场数据的采集和控制数据的发送。

当今，由于PLC(Programmable Logic Computer)具有结构小巧，运行速度高，可靠性强，价格低廉及多功能、多用途的一系列特点，较原有的基于单片机的二次设备有明显的性能/价格比优势，因此，在变电站IED设备中占有一定的比例，被广泛使用在变电站综合自动化系统中。这同时也提出了一个新问题，即在SCADA系统中如何实现上位机与底层PLC之间的通信。

在我们最近开发的一套SCADA系统中，底层一些IED设备选择了PLC，因此，就这个问题进行了一些研究，现阐述如下:

监控系统的结构

此套SCADA系统按IEC的标准结构分析，站级层(Station Level)为一个以太网，连接了主、备服务器，SCADA工作站，主、备前置机。主、备前置机同时挂接在底层现场总线上，互为热备份，负责搜集底层IED设备的数据，完成一个实时网关的功能。二次设备层(Bay Level)部分IED设备选用了PLC来完成对变电站的一次设备的测、保、控功能(如线路保护、母线保护等)。SCADA上位机的管理和通信模块采用VC++5.0编制。其系统结构图如图1所示:

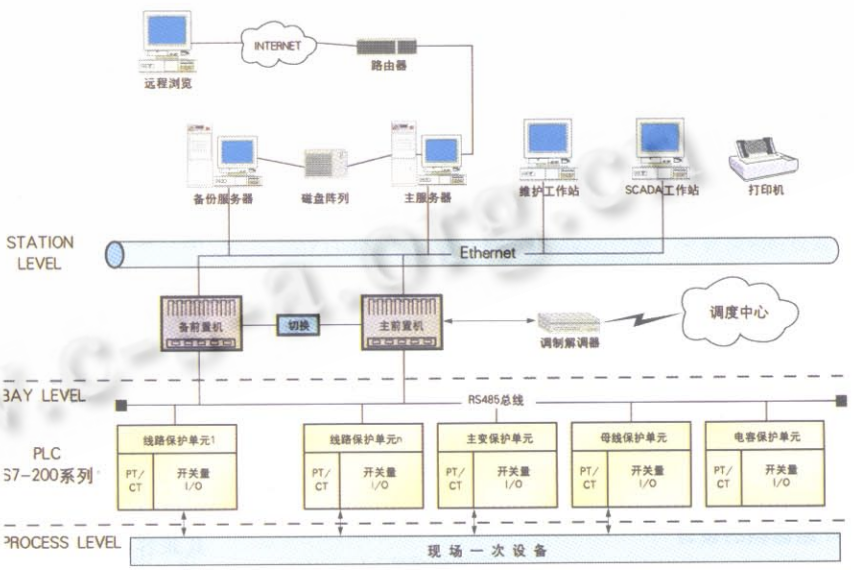


图 1　基PLC的变电站SCADA系统结构示意图

本系统所采用的PLC为SIEMENS公司的S7200系列，集成度高，体积小，易于安装和配置，比较适合恶劣工况，以实现变电站的全分散系统结构。其主要特点为:①良好的开发界面STEP-7，提供梯形图和语句表两种编程方式。②I/O功能强，可带扩展模块(EM)进行I/O扩展。③灵活的中断输入，便于采集遥测越限、变位遥信等

© 中国科学院软件研究所 http://www.c-s-a.org.cn

重要信息。④配有高速计数器，可采集脉冲量。⑤具有强大的通信功能。因此，极其适合SCADA数据库中三大类型数据(状态量、模拟量、脉冲量)的采集，本文重点讨论PLC的通信问题，如结构图所示，直接选用485通信线将PLC接入上位前置机串口。前置机的任务是接收现场数据，进行处理之后送入服务器的SCADA数据库中，并接收系统控制指令转发给底层的PLC单元。

通信规约的设计

1. 通信方式的选择

底层485总线的通信规约设计大致有两种方式：一是循环式(Cyclic Type)，即现场发送端循环不断的将数据发送到主站前置机的接收端，这需要独占信道，较适合IED设备较少的情况。二是应答式(Polling Type)，由主站前置机依次查询各IED设备，相应的设备收到查询后给予响应，送出相应的数据。基于485通信总线的特点，我们选用Polling方式作为本系统的通信方式。其应答流程见图2：

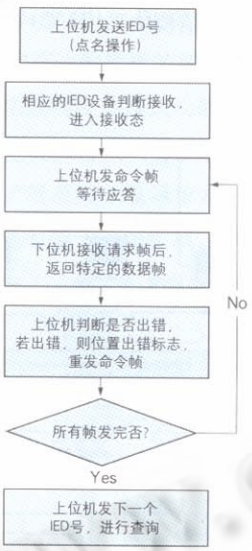


图2 上下位机的通信流程

2. 通信帧的设计

通信帧大致分为上行帧和下行帧两大类。上行帧也称应答帧，是根据不同查询返回不同的数据，包括线路的断路器状态、隔离开关的状态等遥信量，线路Ia、Ic、Uab、Q、P等遥测量，电度量等脉冲量，此处还有SOE，SSW等事件量。下行帧也称请求帧，是前置机向底层IED设计索要数据的命令，不同的命令对应不同的数据帧。此外，下行帧中也包括一些控制命令，如对时命令、调继电器参数命令、继电器分合命令等。按功能分，通信帧可分为测量帧、状态帧、SOE帧、读取参数帧、对时帧、控制帧的几种类型。表1、表2说明了某条线路的测量帧结构：

表1 下行请求帧结构(测量帧)

站址	功能码	特征码		出错校验
	0x11	0	0	

表2 上行数据帧结构(测量帧)

站址	特征码		Ia		Ic		Uab		...
	高	低	高	低	高	低	高	低	

...	Uac		P		Uac		出错校验
	高	低	高	低	高	低	

通信的具体实现

1. 前置机通信功能的实现

前置机为主备机结构，同时连接底层485通信网和上层LAN监控网，具备通信网关的功能。其程序在VC++5.0下开发实现，充分利用了WINDOWS系统的多线程、多任务的特点。利用一个线程循环不断的从串口采集各PLC模块的数据并进行处理，送入缓存。另一个线程通过WINSOCK套接口将处理之后的数据进行网络发送，送入各节点的内存实时库和主、备服务器的历史数据库。再利用一个线程向网络发平安报文。若主前置机出现故障，备份前置机没有收到正常报文，则备份服务器自动代替主服务器的位置进行采集工作，并发出报警信号。这样做，整个系统的冗余度大，可靠性高。

而在VC++5.0中，具体如何实现向串口读、写数据帧呢?一般文献中介绍较少，下面结合实际开发经验作一些小总结：

2. VC++中对串口操作的两种方式

(1)利用_inp(),_outp()直接对串口操作。这种方式是直接对串口通信控制芯片8250编程，8250是IBM/PC及其兼容机异步通信的核心芯片，它有10个可供CPU存取的寄存器，可对串口的通信状态进行设置。串口基址加1为中断允许寄存器位置，串口基址加2为中断识别寄存器位置，串口基址加3为通信线路控制寄存器位置，串口基址加5为通信线路状态寄存器位置，当通信线路控制寄存器的MSB为1时，串口基址和基址加1为波特率除数寄存器位置，可设置波特率数目。

若进行通信，首先进行通信初始化，得到串口基址后设置相应串口的波特率、数据位、奇偶校验位、停止位等。

© 中国科学院软件研究所 http://www.c-s-a.org.cn

假设设置COM1为9600bps，8位数据位，1位停止位，无奇偶校验位。其实现如下：

```
WORD DataPort;
DataPort=1060;//得到串口地址 0x3F8--com1的基地址(com2 为0x2F8，com3为0x3E8，com4为0x2E8)
-outp(DataPort+3,0x80);//通信线路控制寄存器设置：0x80可访问“波特率除数寄存器”
-outp(DataPort,0x0c);//设备不同的除数寄存器的值以标识波特率
-outp(DataPort+1,0x00);//0x0180--300bps;0x0060--1200bps;0x0030--2400bps,0x0018--4800bps,0x000c--9600bps,0x0004--28800bps等
-outp(DataPort+2,0xcf);//enable fifo 16 byte.
-outp(DataPort+1,0);//disable interupt
-outp(DataPort+3,0x3b);//8bits,stop=1;no parity
```

接着，对串口进行读操作：

```
byte COMDATA;
if((_inp(DataPort+5) & 0x1)==0x1) { //
通信线路状态寄存器第0位=1表示数据就绪。
COMDATA=_inp(DataPort);
}
```

写操作：

```
Byte OUTDATA;
if((_inp(DataPort+5)& 0x40){//通信线路状态寄存器第6位=1表示发送保持寄存器已空。
-outp(DataPort,OUTDATA);
```

此处，仅以读、写一个字节为例。若收发一帧，则用一个循环并加上超时设置即可。

这种方式只能在WIN95，WIN98下使用，比较依赖硬件的具体结构，在单机的SCADA监控系统中有一定的应用。

(2)利用读、写文件的方式操作串口。在MFC中，可以将串口资源创建成一个文件对象，并且利用返回的句柄对这个对象进行访问。其核心操作函数为CREATEFILE、READFILE、WRITEFILE等。由于此方式不能对硬件直接操作，所以对串口的设置要通过对设备控制块DCB(Device Control Block)和COMMTIMEOUTS结构的参数进行赋值来完成，再利用SetCommState、SetCommtimeouts函数将参数写入串口，完成设置。具体步骤如下：

①串口初始化。主要完成生成串口文件，并设置DCB和COMMTIMEOUTS完成波特率、数据位、停止位、奇偶校验位等的设置。假设设置COM1为9600bps，8位数据位，1位停止位，无奇偶校验位。其实现如下：

```
……
char buf [100];
COMMTIMEOUTS My Timeouts;//超时设置
DCB dcb;//设备控制块
  hComFile=CreateFile ("Com1", GENERIC - READ|GENERIC - WRITE, 0, NULL, OPEN - EXISTING, FILE - FLAG - WRITE - THROUGH, NULL); //将COM1作为一个文件对象，返回句柄hComFile。
if((hComFile==INVALID_HANDLE_VALUE)) {//打开串口错误
wsprintf(buf,"Open Com1 error");
MessageBox(buf,"注意!", MB_OK);
return;
}
else {
GetCommState(hComFile, &dcb); //读当前端口的DCB设置
wsprintf (buf, "Com1:baud=9600 data-%d", 8);
Istrcat(buf, "stop=1");
Istrcat(buf, "parity=N");
BuildCommDCB(buf, &dcb);//改变串口设置
SetCommState (hComFile, &dcb);;; DCB结构的内容写入端口设置
MyTimeouts.ReadIntervalTimeout=90; //区间超时设置
MyTimeouts.ReadTotalTimeMultiplier=10;
//超时系统设置
MyTimeouts.ReadTotalTimeoutConstant=3;
//超时常量设置
if(!SetCommTimeouts(hComFile,&MyTimeouts)) //改变超时设置
{ CloseHandle(hComFile);
return;//参数设置错}
}……
```

②串口操作。进行完串口设置之后，即可以读、写串口、读串口：

```
char buf [256];//读入缓存区
byte COMDATA [256];
DWORD num;
if(ReadFile(hComFile,buf,128,&num,NULL)) {
for(int n=0;n<(int)num;n++){
COMDATA [n] =buf [n];}
```


© 中国科学院软件研究所 http://www.c-s-a.org.cn

写串口:

```
char CommCon [10];//欲送出的字符串
DWORD num;
If(WriteFile(hComFile, CommCon, 5, (unsigned long*)
&num, NULL)){
wsprintf(msg, "Send OPeration! ");
MessageBox(msg, "注意! ", MB_OK);
}
```

关闭串口:

```
CloseHandle(hComFile);
```

这种方式可以在WIN95、WIN98、WINNT下使用，由于不直接操作硬件，因而兼容性较强，安全性也较好，尤其适合大型变电站的全NT网络监控系统。

3. 底层PLC通信功能的实现

(1)PLC通信方式的设置。S7-200系列PLC提供特殊存储位SMB30以设置自由通信口0(Freeport0)的通信方式。其结构如表3所示:

表 3 通信控制字SMB30

MSB							LSB
p	p	d	b	b	b	m	m
校验方式		长度	波特率			通信协议	

其中PP=00--无校验; PP=01--偶校验;

PP=10--无校验; PP=11--奇校验;

d=0--8位字符; d=1-7位字符;

bbb=000—38400bps; bbb=001—1920bps;

bbb=010—9600bps; bbb=011—4800bps;

bbb=100—2400bps; bbb=101—1200bps等;

mm=00—PPI协议(从机); mm=01—自由口协议;

mm=10—PPI协议(主机) ;mm=11—保留;

因此，如设置FREEPORT0为波特率9600，无奇偶校验位，8位数据位，1位停止位，则用一条MOVB 9，SMB30即可完成。

(2)PLC的通信流程。PLC首先上电完成通信方式的设置，处于接收等待态，若收到上位机的"点名"命令后，则进入接收态，准备接收命令帧，收到一个整帧后存入命令缓存区，开始命令处理。如果是请求帧，就从不同的数据区中取出实时数据组帧发送，如果是控制帧，则进行相应的调整、控制。大致流程如图3所示:

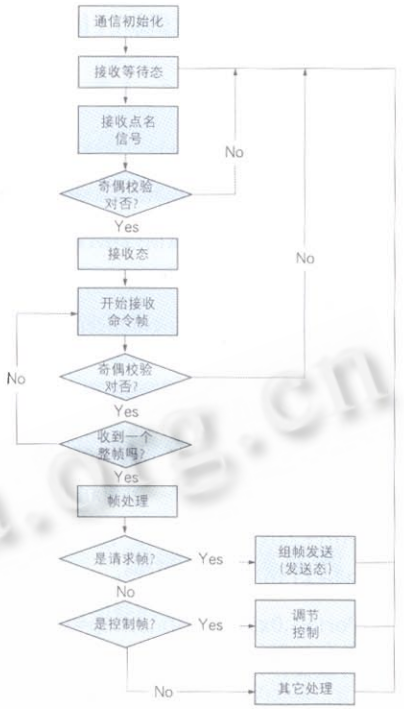


图 3 PLC通信流程图

这里，我们利用了PLC提供的三种中断事件源: 接收中断(Event8)、发送完中断(Event9)、定时器中断(Event10),通过将不同的中断响应程序(INT0-INT6)连接不同的中断源，来设置三种通信状态: 接收等待态、接收态、发送态、以完成通信要求。见表4所示:

表 4 PLC通信状态的设置

接收等待态	INT0-) EVENT 10; INT6->EVENT 8
接收态	INT2-) EVENT 10; INT4, 5-) EVENT 8
发送态	INT1-) EVENT 10; INT3-) EVENT 9

结束语

上述这个SCADA系统已基本完成，现场调试证明，前置机使用上面所介绍的通信策略与底层PLC进行485通信，运行可靠，实时性好，速度响应快。由于PLC产品是特别为恶劣的现场环境、复杂的工业过程设计的，所以抗干扰性强，工作可靠，更适合担任现场控制单元的角色，以构成全分散的变电站综合自动化系统，因而在电力系统中将得到广泛的应用。■

参考文献

1 周京阳等. 能量管理系统之第三讲—数据收集与监视(SCADA)。电力系统自动化, 1997, 21(3)。

2 蔡运清, 北美变电站综合自动化现状, 电力系统自动化, 1997, 21(7)。

3 S7-200 PLC 用户指南, SIEMENS公司。1998, 6

© 中国科学院软件研究所 http://www.c-s-a.org.cn