智能设备的通用测试

王建明 包头职业技术学院电子工程系(014030)
马玉春 宋瀚涛 北京理工大学计算机系 (100081)

Abstract

According to the characteristics of computer measurement and control system,develop this software by VB 6.0.It can be used as a Supervisor Computer or a Slave one,and can be used to solve communication protocol between computers connected through serial ports,having high performance both in liability and utility.Meanwhile,the bug in MSComm is mended.

Keywords:general software,measurement and control,supervisor/slave computer,communication,bug

摘 要

根据计算机监控系统的特点,用 VB 6.0 开发通用的计算机监控系统测试软件。该软件既能充当主控机,又能充当受控机,还可用来破译通讯协议,可靠性高,实用性强,可广泛应用于智能设备的测试及计算机监控系统。同时,对 Microsoft 的 MSComm 通讯控件中的 bug 作了修正。

关键词:通用软件,监控,主/受控机,通讯,bug

1 MSComm 控件中存在的问题及解决方法

VB5.0/6.0 的 MSComm 通信控件提供了一系列标准通信命令的接口,它允许建立串口连接,可连接到其它通信设备(如 Modem),还可发送命令,进行数据交换以及监视和响应在通信过程中可能发生的各种错误和事件,从而建立全双工的、事件驱动的、高效实用的通信程序。但在实际通信软件设计过程中,MSComm 控件并非想象中的那么完美和容易控制,特别是在中文 Win9X 环境下通信时更会出现问题。

由于在中文 Win9X 环境下使用的是双字节字符集(DBCS)系统,MSComm.Output=Chr(I),当 0≤I<129 或 I=255 时,能正确发送数据,128<I<255 时,发送出去的全是 0。解决这个问题的方法是将需要发送的数据放入一个 Byte 型数组中。类似的,在接收数据时,也不能简单地将 MSComm.Input 中的内容放入一个字符串变量中,否则,同样会丢失数据,这可通过采用 Variant 变量来解决。

RThreshold 属性为设置并返回需要接收多少数据才能激发 ONComm 事件 comEvReceive。如果取 1,则一接收到数据便产生 comEvReceive 事件,当数据量较大时,一个数据包将被分成多个小的数据包;如果为 N(N>1),则接收到 N-1 个数据时,却不会产生 comEvReceive 事件,这样就不能及时响应并处理受控机主动发送过来的较短的报警信息。显然,该属性应取 1,对于大批量数据,估算其时间,进行累加即可。因为在计算机监控系统中,通讯协议是明确的,最大的数据包的长度以及主控机发送查询命令时,受控机的响应数据长度也是已知的。其它有关属性可以参考 Visual Basic 的例子程序 VBTerm。

MSComm 控件是用 32 位 Windows API 函数来实现的,其中,COMMTIMEOUTS 结构用来限时。其结构成员 ReadIntervalTimeout 表示相邻两个字节之间的最大延时(单位为毫秒,下同),如果超过这段时间,则立即返回,其后的数据被当做下一个数据包。经过调试跟踪发现,在运行过程中,ReadIntervalTimeout 被设置为-1, WriteTotalTimeoutConstant=5000 (即 5 秒),其余成员的值均为 0。即对于读操作,一接收到数据则立即返回,即使没有收到数据也可导致返回,这就可能导致接收时数据丢失;对于写操作,不能超过 5 秒,5 秒后的数据被中断,这对于低传输率的计算机监控造成了困难。解决方法见以下程序,这是对 MSComm 控件的修正。

```
Public Type COMMTIMEOUTS
    ReadIntervalTimeout As Long
    ReadTotalTimeoutMultiplier As Long
    ReadTotalTimeoutConstant As Long
    WriteTotalTimeoutMultiplier As Long
    WriteTotalTimeoutConstant As Long
End Type
Public timeouts As COMMTIMEOUTS
Declare Function GetCommTimeouts Lib "Kernel32" _
    (ByVal hFile As Long, lpCommTimeouts As COMMTIMEOUTS) As Long
```

```
Declare Function SetCommTimeouts Lib "Kernel32" _
    (ByVal hFile As Long, lpCommTimeouts As COMM-
TIMEOUTS) As Long
Public Sub OpenAndAdjustPort()
    Dim Ret As Long
    If Main.MSComm1.PortOpen=False Then
        Main.MSComm1.PortOpen=True
        Ret=GetCommTimeouts(Main.MSComm1.CommID,
timeouts)
        timeouts.ReadIntervalTimeout=1000 * 10\Val(Main.
MSComm1.Settings) +100
        timeouts.ReadTotalTimeoutMultiplier =1000*10\Val
(Main.MSComm1.Settings) +100
        timeouts.ReadTotalTimeoutConstant=1000
        timeouts.WriteTotalTimeoutMultiplier=1000 * 10\Val
(Main.MSComm1.Settings)+100
        timeouts.WriteTotalTimeoutConstant=1000
        Ret = SetCommTimeouts (Main.MSComm1.Com-
mID, timeouts)
    End If
End Sub
```

2 软件的设计与开发

主界面见图 1 所示。其中,Hex 与 Char 文本框以两种方式显示需要发送或接收到的数据。下面的客户区用来监视通讯状态,包括当前端口的开关、参数等,以及信号线的变化、接收到的数据。所有事件均在客户区显示其发生的时间(TickCount)。Open 按钮打开串口,Close 关闭串口,Setup 设置串口参数 (见图 2),Send 则用来发送数据(当 Hex 与 Char 文本框中都有数据时,Hex 中的数据优先),Parity(见图 6)用来计算 Xor、Add、Crc 校验码,还可计算数据长度,Char/Hex 实现字符与 ASCII 码的相互转换,Find 用来查找客户区中的信息,Clear 则清除所有文本框中的内容。主界面如此小巧, 是为了实现在同一屏幕对多个串口同时进行监控或测试。

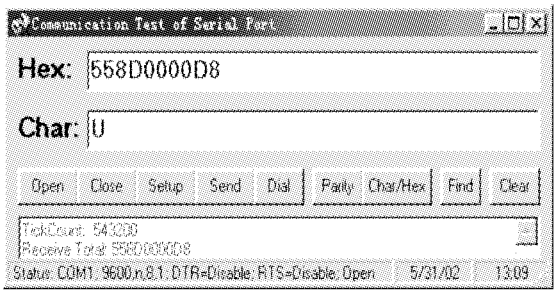

图 1 主界面

在图 1 中按下 Setup 按钮时,显示图 2 所示的对话框。Port 可从 1 至 16,因而,理论上,本软件可以同时调试 16 个串行口;波特率从 110 至 256000,选择范围较大。某些带隔离的 RS232/485 转换器在 RS232 端需要通过设置 DTR 有效来提供电源(RS485 端另配电源),这可通过核选 DTR 来实现。RecErr 核选框用来记录错误数据包,图 2 表示,如果接收到的数据不是 Crc 校验,则认为数据有误,并记录之。图 3 为错误记录,包括发生时间及数据,图 4 为测试报告,其中包括详细的测试时间,发送的数据报文总数,响应和未响应的数目、错误的数目,最后是用百分数表示的正确率。同时,图 2 的校验也是数据报文的校验,根据图 2 的选择,可以在图 1 发送的数据中自动添加相应的数据报文校验码。Length 文本框中为一次接收的最大数据长度, 因为有些智能设备或数采器的数据发送并不太连续,需要作一定的等待,本程序根据数据长度及波特率决定等待的时间长度。其下的组合框主要用来破译通讯协议,如图 2 选择 Receive 时,主控机发送图 5 所示的第 1 栏中的数据时,自动记录受控机响应的数据(放入对应的第 2 栏中)。Auto 核选框用来选择是否工作在自动状态, 当选择自动时, 如果 Time (ms)中的数据为零,则该计算机可作为受控机使用,当收到图 5 所示的 “ff03fc010016” 时, 则自动应答 “ff0312345600000078”;如果 Time(ms)中的数据不为零,则该计算机作主控机使用,每隔一段时间(Time (ms)中所示的毫秒数),轮流发送图 5 第 1 栏中的通讯协议,并接收受控机的响应。核选 Sound 核选框时,当有数据到达,则声音提示,否则关闭此功能。

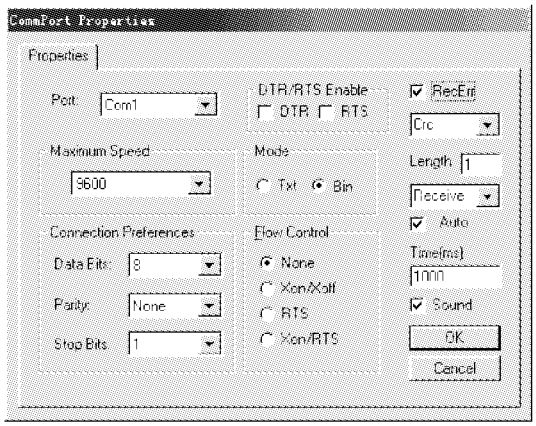

图 2 串口参数的综合设置

在图 1 中按下 Parity 按钮时,显示图 6 所示的对话框。此对话框可计算四种校验码及字节长度。BCS 也是一种累加和校验,但是,它是以字节累加成 16 位和,除以 65536 取余,再求其补码。这种校验方法广泛应用于计算机网络及手机的短消息中。

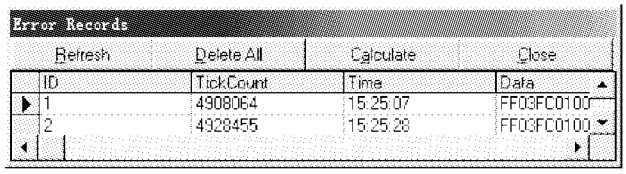

图 3 错误数据报文的自动记录

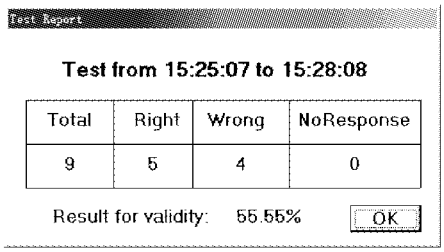

图 4 通讯测试报告

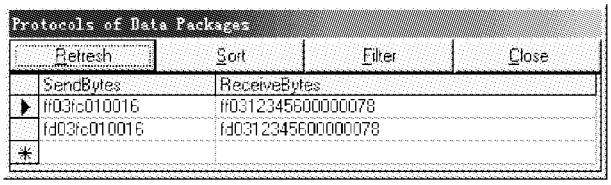

图 5 自动应答数据库的输入

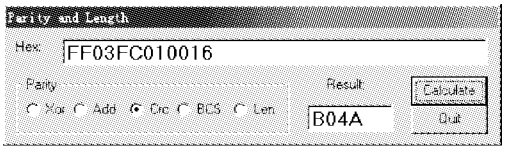

图 6 校验码的计算

3 软件的应用

3.1 一般应用

在图 2 中设置好串口参数,校验码,如 Add,所接收的最大的数据字节数即可。然后,在图 1 中打开串口,在 Hex 文本框中输入需要发送的数据,如 320F,再点击 Send 按钮,则发送 320F41(41 为自动计算的 Add 校验码)。

如果需要发送的数据在校验码后还有其它数据时,就得另行计算了。如对于松下 PLC,报文“%01#WDD 10000 10001 0100 5000 BCC CR”的含义为:往 PLC 的 10000 数据寄存器中写入 0001(低字节在前),10001 中写入 0050,BCC 为异或校验码,CR 为回车符 0X0D。将 BCC 以前的字符输入图 1 中的 Char 文本框中,点击 Char/Hex 按钮,即可在 Hex 文本框中得到对应的 16 进制值,再点击 Parity 按钮,将原先的 16 进制值输入图 6 中的 Hex 文本框中(可利用剪贴板进行),点击 Calculate 按钮,即可在 Result 文本框中得到异或结果,将此结果追加至图 1 中的 Hex 文本框中,再添上 0D(即 CR,松下 PLC 的报文结束标志),点击 Send 按钮,任务完成。

3.2 作为受控机

如果核选图 2 中的 Auto 核选框,并且,Time(ms)中的数据为零,则该计算机可充当受控机角色,自动应答主控机的查询命令,如图 5 所示,当收到第 1 栏中的数据时,自动发送对应的第 2 栏中的内容。这种功能可用来调试或开发主控机程序,特别地,当受控机为昂贵的智能设备时,可用下文 3.4 和 3.5 介绍的方法截取通讯协议,然后,用多台计算机模拟该昂贵的智能设备,使多位科研人员并行开发,从而大大节省了投资,也极大地提高了工作进度。

3.3 作为主控机

如果核选图 2 中的 Auto 核选框,并且,Time(ms)中的数据不为零,则该计算机可充当主控机角色,根据 Time(ms)文本框中确定的毫秒数,自动发送图 5 第 1 栏中的通讯协议,同时接收受控机响应的数据,并在图 1 以两种格式(16 进制及字符)进行显示。这种功能可以用来调试受控机程序。

如果同时核选 RecErr 核选框,并选择其下的校验标志,则在作为主控机使用的同时,可以测试受控机的性能(测试报告格式见图 4 所示),在计算机监控系统中,需要选择一些数采器,可用此方法测试该数采器的性能,从而决定取舍。

3.4 截取测试机发送的通讯协议

现假设某公司生产一智能设备,与该设备配套的厂家的测试软件运行于测试机上。作者的通用多功能计算机监控系统测试软件运行于侦听机上,现欲截取测试机与智能设备之间的通讯协议,并破译之。见图 7 所示。

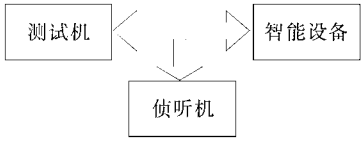

图 7 通讯协议的截取

将侦听机中的软件设置为受控机状态(见 3.2 节),并在图 2 中选择 Send(与 Receive 相对),则测试机发往智能设备的所有通讯协议全部被收录进图 5 所示的第 1 栏中,而对于重复的数据,只记录第一批。

3.5 截取智能设备响应的通讯协议

将侦听机中的软件设置为主控机状态(见 3.3 节),并在图 2 中选择 Receive(与 Send 相对),改为由侦听机向智能设备发送通讯协议,则智能设备所响应的通讯协议自动收录进图 5 所示的第 2 栏中,并且,新数据将覆盖旧数据。

3.6 破译通讯协议

由于图 1 下面的客户区充分地显示了串口的历史状态,又能采用 3.4 与 3.5 两节的方法完全截取通讯协议,破译通讯协议就不难了,只要根据数据库中的内容和相应的历史状态进行编程即可,实现用自己的软件来监控智能设备。例如,当手机发生死锁时,也可截取其通讯协议,以后发生类似的情况后,可以自己进行解锁了。

(下转第 48 页)

```
STB  AL,[BX]+;
LDB  COUT,#08H;8 个字节数据;
TDATA:LDB  AL,[DATA]+;CPU 内的发送数据缓存区首址
STB  AL,[BX]+;
DJNZ  COUT,TDATA;8 个字节发完否?
LDB  AL,#01H;
STB  AL,CMR;发送
RET
RECEIVE:          ;(接收中断程序)
PUSHF;保护现场
LDB  AL, IR;
JBC  AL,0,OTHER;接收中断否?
LD  BX,#RXB;接收缓存器首址
LDB  AL,[BX]+;
JBC  AL,6, RCDATA;标识符的 RTR=1?
LDB  AL,#04H;是远程帧,释放接收缓
STB  AL,CMR;存区
LCALL  TRANSMIT;响应远程帧,发送相应数据
SJMP  BACK;
RCDATA:
ANDB  AL,#0FH;取低四位数据长度
ADDB  AL,#03H;
STB  AL,R1;该报文含有的字节数
LD  BX,#RXB;接收缓存器的首地址
LD  CX,#CRBF;CPU 内的接收数据缓存区首址
RECE:
LDB  AL,[BX]+;
STB  AL,[CX]+;
INCB  R1
DJNZ  R1,RECE;接收完否?
LDB  AL,#04H;
STB  AL,CMR;释放接收缓存区
BACK:
POPF
RET
```

3 结束语

文中的智能节点来源于一电源组集散控制系统，其硬、软件电路的设计方法同样适合于其他基于 CAN 总线的分布式控制系统的节点设计。文中软件设计所涉及到的 CAN 控制器 SJA1000 内部各寄存器的详细功能因篇幅原因没作介绍，请参考文献[3]。

参考文献

1 邬宽明.CAN 总线原理和应用系统设计.北京:北京航空航天大学出版社,1996

2 孙涵芳.Intel 16 位单片机. 北京: 北京航空航天大学出版社,1999

3 PHILIPS SJA1000 Stand-alone CAN controller DATA SHEET .2000

4 PHILIPS PCA82C250 CAN controller interface DATA SHEET,2000

[收稿日期:2002.5.13]

(上接第 12 页)

本软件的主界面较小,对话框为非模型的,因而,可以在一个屏幕上同时监控多个智能串口设备,而且,可以共享一个校验码对话框。

3.7 通过 Modem 进行远程测试

在图 8 中选择电话号码，如果不需要电话卡,直接输入电话号码即可,然后,点击“Exit”按钮退出,程序自动生成 Modem 的 AT 命令 “ATDT025-1234567;”,并显示在图 1 的 Char 文本框中。在图 2 右侧的第一个下拉框中选择“+0D”,点击 Send 按钮,即可与区号为“025”,电话号码为“1234567”的智能设备建立连接 (“;” 表示拨通对方后保持连接状态),从而,使远端设备可以当作本地设备进行测试。

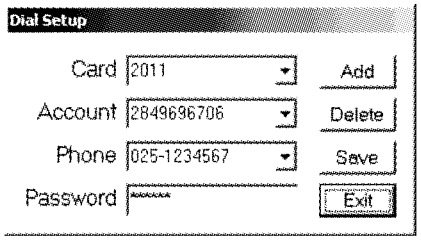

图 8 远程测试电话参数设置

3.8 发送手机的短消息

手机短消息协议如图 9 所示。欲发送短消息“OK！”，只需通过图 1 将字符转换为对应的 ASCII 码，输入图 6 的 Hex 文本框，选择 BCS 校验，点击 Calculate 按钮,即可得到 BCS 校验码“45FF”,将图 9 的协议写入图 1 的 Hex 文本框,由于在该处的校验码是高字节在前,因而,应将“45FF”变为“FF 45”,点击 Send 按钮即可发送此短消息。

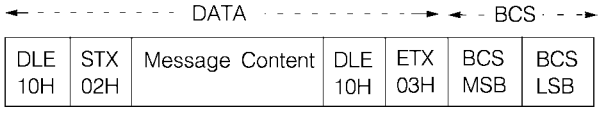

图 9 手机短消息协议

4 结束语

该软件经过反复调试，在实际工作及工程中得到了验证,并多次进行了改进和加强,可靠性高,方便实用,可广泛应用于智能设备的测试及计算机监控系统。

参考文献

1 Microsoft 著,Microsoft Visual Basic 6.0 Component Tools Guide,America,Microsoft Press,1999

2 Microsoft 著.欣力,李莉等,译.Microsoft Win32 程序员大全(1~5).北京:清华大学出版社,1995

[收稿日期:2002.6.4]