VB与西门子S7-300的通讯方式

西门子S7-300通讯协议不公开，我们无法按相应的协议写程序，但是西门子提供给我们更为简单的方式来与之通讯。

大家可以在某些组态软件中找到这样一个DLL：w95_s7.dll,就是这个DLL，使的我们与PLC进行数据交互极为简单

在DLL时定义了如下一些接口函数：

Public Declare Function load_tool Lib "w95_s7.dll" (ByVal nrAs Byte, ByVal dev As String, adr As Type_PlcAddressType) As Long

这个函数是初始化连接用的，这个过程比较慢，大约要20S左右，这大概也是西门子为什么启动那么慢的原因吧；包括了如下几个参数：nr是指激活的连接数，范围是1-4

dev是设备名,SetPG/PC里面有这个指定，一般用S7ONLINE就可以了，adr是指参数表，它是这样的一个type:

Type Type_PlcAddressType

bytAddress As Byte’这是站号，默认是2

bytPlcSegmentID As Byte’SegmentID，默认是0

bytPlcSlotNo As Byte’槽号，默认是2

bytPlcRackNo As Byte’Rack号，默认是0

End Type

Public Declare Function new_ss Lib "w95_s7.dll" (ByVal nr As Byte) As Long

这个函数没用到，可以去找一些资料来看

Public Declare Function unload_tool Lib "w95_s7.dll" () As Long’这个函数是程序退出时用的，用来断开连接

’ no, amount, value

Public Declare Function d_field_read Lib "w95_s7.dll" (ByVal dbAs Long, ByVal nr As Long, ByVal anz As Long, value As Byte) As Long’这是读取DB块中数据的函数

db 是指DB块号，比如DB10，则这个参数指定为10就可以了

nr 是指起始地址，比如读DB10的第4个字节中数据，则指定为4

anz是指读取的长度

value是返回的值，表面上看这是一个字节，但实际上它是一个字节数组，比如你要读取二十个字节的数据，那么应定义dim ReturnValue(20) as byte,然后用ReturnValue来做为传递的参数

Public Declare Function d_field_write Lib "w95_s7.dll" (ByVal db AsLong, ByVal nr As Long, ByVal anz As Long, value As Byte) As Long

这是写DB块数据的函数，参数跟读数据函数一样，不多说了

’ no, amount, value

Public Declare Function e_field_read Lib "w95_s7.dll" (ByVal nr AsLong, ByVal anz As Long, value As Byte) As Long

‘这个是用来读取外部输入的值，包括开关量输入，模拟量输入

nr 是指起始地址

anz是指读取的长度

value是返回的值，表面上看这是一个字节，但实际上它是一个字节数组，比如你要读取二十个字节的数据，那么应定义dim ReturnValue(20) as byte,然后用ReturnValue来做为传递的参数

从分析也可以看出，只有外部输入的值不可以写，因而它单独存在

Public Declare Function a_field_read Lib "w95_s7.dll" (ByValnr As Long, ByVal anz As Long, value As Byte) As Long

‘这是用来读取外部输出的值，包括开关量输出，模拟量输出，参数可以参照上面的函数，

Public Declare Function a_field_write Lib "w95_s7.dll" (ByValnr As Long, ByVal anz As Long, value As Byte) As Long

‘这是用来写外部输出的值，包括开关量输出，模拟量输出
nr 是指起始地址，
anz是指读取的长度
value是返回的值
Public Declare Function m_field_read Lib "w95_s7.dll" (ByValnr As Long, ByVal anz As Long, value As Byte) As Long
读取内存变量的函数（M的值）
nr 是指起始地址
anz是指读取的长度
value是返回的值
Public Declare Function m_field_write Lib "w95_s7.dll" (ByValnr As Long, ByVal anz As Long, value As Byte) As Long
写内存变量的函数
nr 是指起始地址
anz是指读取的长度
value是返回的值
Public Declare Function t_field_read Lib "w95_s7.dll" (ByValnr As Long, ByVal anz As Long, value As Integer) As Long
’读定时器的值
nr 是指起始地址
anz是指读取的长度
value是返回的值，这个返回的是整型量的值
Public Declare Function z_field_read Lib "w95_s7.dll" (ByValnr As Long, ByVal anz As Long, value As Integer) As Long
‘读计数器的值
nr 是指起始地址
anz是指读取的长度
value是返回的值，这个返回的是整型量的值
Public Declare Function z_field_write Lib "w95_s7.dll" (ByValnr As Long, ByVal anz As Long, value As Integer) As Long
‘写计数器的值
nr 是指起始地址
anz是指读取的长度
value是返回的值，这个返回的是整型量的值
有了以上这样函数，相信会VB的人都可以写跟西门子通讯的程序了。
但是如何知道读或写是否成功呢，这就是每个函数的返回值来决定，返回为0时，说明操作成功，否则为通讯出错。