浙江工商职业技术学院　王子娜　李方园

摘要：在现场总线应用中，最常用的就是Modbus总线。本文主要介绍一种基于Modbus的远程温度采样控制，给出了PLC硬件接线原理，阐述了软件设置与编程，在实际应用中获得了很好的效果。

文章编号：150606

基于Modbus的远程温度采样控制系统

Remote temperature sampling control system based on Modbus

1 前言

Modbus是由Modicon公司(现为施耐德电气的一个品牌)在1978年发明的，这是一个划时代、里程碑式的网络协议，是全球第一个真正用于工业现场的总线协议。

Modbus的巨大成功，可以归结到以下3个方面：

a．标准、开放：用户可以免费、放心地使用Modbus协议，不用交纳许可证费，也不会侵犯知识产权。目前，支持Modbus的厂家超过400家，支持Modbus的产品超过600种，而且在国内也有很多的用户支持和使用Modbus的产品。

b．Modbus是面向消息的协议。可以支持多种电气接口，如：RS232、RS422、RS485等，还可以在多种介质上传送，如：双绞线、光缆、无线射频等。要说明的是：和很多的现场总线不同，它不用专用的芯片与硬件，完全采用市售的标准部件。这就保证了采用Modbus的产品造价最为低廉。

c．Modbus协议的帧格式是最简单、最紧凑的协议。可以说：简单高效，通俗易懂。所以用户使用容易，厂商开发简单。用户和厂商可以通过ww.Modbus-IDA.org网站和其他网站，下载各种语言的样例程序、控件、以及各种Modbus工具软件，更好地使用Modbus。

本文将主要阐述一种基于Modbus的远程温度采样控制系统，使用2台西门子S7-200 PLC，将连接在从站PLC上的PT100温度，显示在具有Modbus总线接口的温度表上。

2 Modbus在远程温度采样控制系统中的总体设计

系统总框图如图1所示。S7-200 PLC从站获取温度信号（即PT100），将信息通过Modbus反馈到S7-200 PLC主站上，再通过Modbus总线反馈到温度表上，将温度的上限和下限可以设置，并在信号灯进行输出，这样就能够更容易得观察到温度变化现象，时时记录数据，更具人性化。

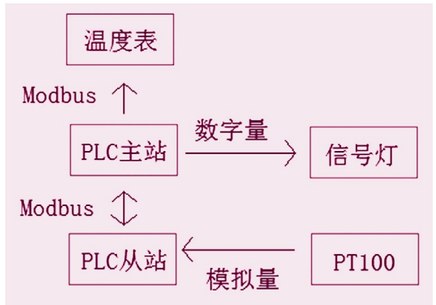

图1 系统总体框图

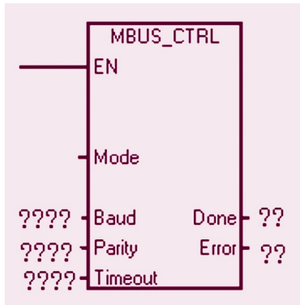

图2 MBUS_CTRL指令

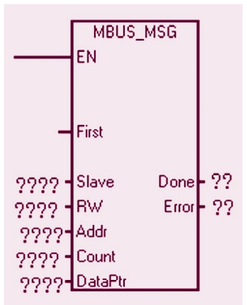

图3 MBUS_MSG指令

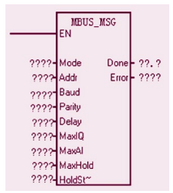

图4 MBUS_INIT指令

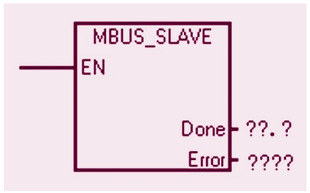

图5 MBUS_SLAVE指令

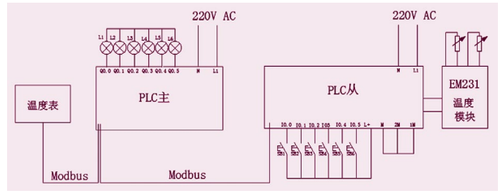

图6 PLC硬件接线图

2.1 Modbus报文传输协议

Modbus地址通常是包含数据类型和偏移量的5个或6个字符值。第一个或前面两个字符决定数据类型，最后的4个字符是符合数据类型的一个适当的值。Modbus主站指令可以将地址映射至相应的功能，以发送到从站。Modbus地址与S7-200地址对应关系如表1所示。

Modbus通信协议有ASCII和RTU（远程传输单元）两种报文传输模式。Modbus网络中所有的站必须采用相同的传输模式和串口参数。本系统采用RTU模式，其报文格式如表2所示。

地址：Modbus地址，1个字节。

功能码：Modbus功能代码，1个字节；Modbus协议支持的功能码共16条（1-16）。

2.2 Modbus通信指令

西门子专门为Modbus RTU通信开发了指令库，及大地简化了Modbus RTU通信的开发，以便于快速实现相关应用。通过Modbus RTU从站指令库，使得S7-200可作为ModbusRTU中的从站设备集成到Modbus网络中，以实现与Modbus主站设备的通信。

西门子Modbus主站协议库包括两条主站协议指令：MBUS_CTRL指令和MBUS_MSG指令。MBUS_CTRL指令用于初始化主站通信，MBUS_MSG指令（或用于端口1的MBUS_MSG_P1）用于启动对Modbus从站的请求并处理应答。

2.2.1 MBUS_CTRL指令

如图2所示，主要参数含义如下：

Mode：“模式”参数，输入数值来选择通信协议。1将CPU端口分配给Modbus协议并启用该协议；0将CPU端口分配给PPI系统协议，并禁用Modbus协议。

Baud：“波特率”参数。MBUS_CTRL指令支持的波特率为19200、38400、57600或115200bit/s。

Parity：“奇偶校验”参数。“奇偶校验”参数被设为与Modbus从站奇偶校验相匹配。所有设置使用一个起始位和一个停止位。可接受的数值为：0-无奇偶校验，1-奇校验，2-偶校验。

2.2.2 MBUS_MSG指令

如图3所示，主要参数含义如下：

First：“首次”参数。“首次”参数应该在有新情求要发送时才打开以进行一次扫描。“首次”输入应当通过一个边沿检测元素（例如上升沿）打开，这将导致请求被传送一次。

Slave：“从站”参数。“从站”参数是Modbus从站的地址，允许的范围是0-247，地址0是广播地址，只能用于写请求，不存在对地址0的广播请求的应答。并非所有的从站会支持广播地址，S7-200Modbus从站协议库不支持广播地址。

RW：“读写”参数。“读写”参数指定是否要读取或写入该消息。“读写”参数允许使用下

图7 温度表

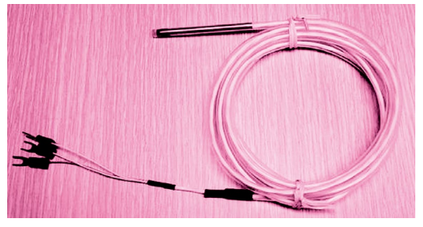

图8 PT100外表

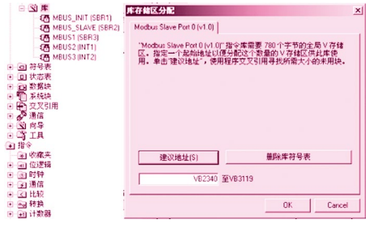

图9 调用的库要分配系统内存地址区

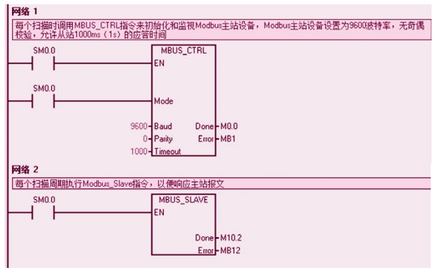

图10 调用ModbusPTU通信指令库

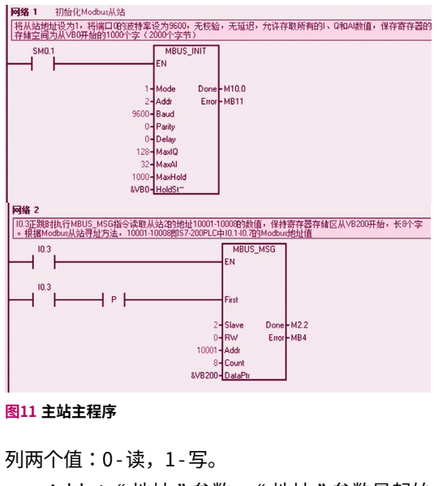

图11 主站主程序

列两个值：0-读，1-写。

Addr：“ 地址 ”参数。“ 地址 ”参数是起始的Modbus地址。

Count：“ 计数 ”参数。“ 计数 ”参数指定在该请求中读取或写入的数据元素的数目。“ 计数 ”数值是位数（对于位数据类型）和字数（对于字数据类型）。

西门子Modbus从站协议库包括两条从站指令：MBUS-INIT指令和MBUS-SLAVE指令（图4和图5）。

3 系统硬件电路的设计

PLC硬件接线图如图6所示。PLC部分略去不讲，主要介绍外部元器件。

3.1 温度表

由于是总线控制的温度表，一般都选用支持Modbus的RS485型数显仪（如图7所示）。

3.2 PT100

西门子S7-200支持两种类型的温度传感器，即热电阻和热电偶，其温度模块也有不同，必须合理配置。图8为常用的PT100热电阻。

000001	Q0.0
000002	Q0.1
000003	Q0.2
…	…
000127	Q15.6
000128	Q15.7
010001	I0.0
010002	I0.1
010003	I0.2
…	…
010127	I15.6
010128	I15.7
030001	AIW0
030002	AIW2
030003	AIW4
…	…
030032	AIW62
040001	HoldStart
040002	HoldStart+2
040003	HoldStart+4
…	…
04xxxx	HoldStart+2x（xxxx-1）

表1 映射Modbus地址到S7-200

地址	功能码	数据1	…	数据n	CRC高字节	CRC低字节

表2 RTU模式的报文格式

4 系统软件程序的设计

利用指令库编程前首先应为Modbus从站分配存储区，否则Micro/Win软件编译时会报错。通过Micro/Win软件菜单命令“ 文件 ”→“ 库存储区 ”，打开“ 库存储区分配 ”对话框。在“ 库存储区分配 ”对话框中输入库存储区的起始地址，注意避免该地址和程序中已经采用或准备采用的其他地址重合。单击“ 建议地址 ”按钮，系统将自动计算存储区的截止地址。

而对于从站来说，S7-200作Modbus通信要用到自由口通信下的Modbus Slave库，对于此库的应用要注意的是： Modbus Slave库仅支持Modbus PTU通信模式，不支持ASCII通信模式；目前的Modbus Slave库仅支持通信口Port0。使用Modbus Slave库时也要注意对库分配内存区空间，否则编译后会出现很多的错误。如图9所示。

编程时使用SM0.1调用子程序MBUS_INIT进行初始化，使用SM0.0调用MBUS_SLAVE，并指导相应参数。关于参数的详细说明，可在子程序的局部变量表中找到。

初始化Modbus从站如图10所示。

图中参数意义如下：

a．模式选择：启动/停止Modbus，1=启动；0=停止；

b．从站地址：Modbus从站地址，取值1-247；

c．波特率：可选1200，2400，4800，9600，19200，38400，57600，115200；

d．奇偶校验：0=无校验；1=奇校验；2=偶校验；

e．延时：附加字符间延时，缺省值为0；

f．最大I/O位：参与通信的最大I/O点数，S7-200的I/O映像区为128/128，缺省值为128；

g．最大AI字数：参与通信的最大AI通道数，可为16或32；

h．最大保持寄存器区：参与通信的最大V存储区字（VW）；

i．保持寄存器区起始地址：以&VBx指定（间接寻址方式）；

j．初始化完成标志：成功初始化后置1；

k．初始化错误代码；

l．Modbus执行：通信中时置1，无Modbus通信活动时为0；

m．错误代码：0=无错误；

从程序截图中可见，S7-200作为Modbus从站，从站地址为10，接收存储区为VB0开始。

调用Modbus主站指令编程前也应分配库存储区，与从站编程类似。主站主程序如图11所示。

5 结束语

Modbus是公开通信协议，其具有两种串行传输模式，ASCII和RTU。它们定义了数据如何打包、解码的不同方式。通信双方必须同时支持上述模式中的一种，通常支持Modbus通信的设备大都支持RTU格式。本文主要介绍了其中的一种RTU协议，应用在远程温度采样控制中。该系统可以在需要实时了解和掌握恶劣现场工矿的温度采样控制中进行实施。CD