**基于Modbus RTU的S7-1500与2台FP23通讯**

赵勇

（西安高压电器研究院有限责任公司，西安710077）

**摘要：**通过对Modbus RTU工业网络协议的研究，并基于西门子S7-1500系统通过CM1541进行Modbus RTU通讯，PLC作为主站轮询多个从站，实现了对2台FP23仪表的监测和控制。同时还介绍FP23智能仪表作为从站的系统设置和仪表命令。

关键词：Modbus；FP23；S7-1500；轮询

作者简介：赵勇（1974-），汉，甘肃天水，工程师，主要从事自动控制系统设计及应用工作

中文分类好：TP216 文献标识码：A

**0 引言**

随着智能仪表的快速发展，建立在液晶显示及微处理器在基础上的智能仪表以较高的控制精度能力，被广泛应用于各种控制过程。本文选用的FP23智能温度控制仪表具有高速采样周期、自整定PID/专家PID控制、可编程和运算控制等功能，并且提供了工业标准的RS485通信接口及Modbus协议。

工业电炉温度控制系统逻辑控制功能由PLC完成，温度模拟量的闭环测量和控制选用2台FP23完成。温度仪作为控制核心，大大减轻了PLC（可编程逻辑控制器）的CPU负荷，所以PLC选用S7-1511-1 。S7-1511-1 PN作为主站与温控仪之间作Modbus-RTU通讯，并通过以太网和上位机通讯。即使在上位机SCADA系统宕机的情况下，PLC和温控仪依然可以按照设定的曲线完成控制。这种方案在提高系统稳定性的同时有效的降低了项目投资。

**1 Modbus-RTU简介**

Modbus是一种串行通信协议，是莫迪康公司于1979年为使用PLC通信而发表，是工业设备之间常用的连接方式。Modbus协议是定义在OSI网络模型第7层（应用层）的报文发送协议，是一种单主站的主/从通信模式。Modbus网络上只能有一个主站存在，主站在 Modbus网络上没有地址，从站的地址范围为 0 - 247，其中 0 为广播地址，从站的实际地址范围为 1 - 247。Modbus协议包括RTU、ASCII、TCP。其中MODBUS-RTU在仪表上最为常用模式。在RTU（Remote Terminal Unit）模式下，每个字节可以传输两个十六进制字符，比如十六进制数0xAE，直接以十六进制0xAE（二进制：10101110）进行发送，因此它的发送密度比ASCII模式高一倍，RTU模式采用循环冗余校验（CRC）。Modbus-RTU模式数据以数值型式传输，通讯帧格式见表1

表1

|  |  |  |  |
| --- | --- | --- | --- |
| 地址码 | 功能码 | 数据 | 校验 |
| 1字节 | 1字节 | 0-252字节 | 2字节 |

**2 FP23智能仪表设置**

FP23智能仪表Modbus RTU数据帧通过RS485总线进行串行通信，数据以字节型式传输，传输时低位在前，高位在后，串行通信采用固定的波特率进行数据传输。FP23智能仪表通讯参数:通信模式设置为COM，通信协议选择MOD\_RTU，通信地址二块表分别选择2和3，通信速度选择9600bps，8个数据位，无校验，1个停止位。FP23支持仪表的读和写模式，命令为03H和06H，数据格式如下：

读命令主站发送：从站地址+命令（03H）+数据地址+数据数量+校验；

读命令从站返回：从站地址+命令（03H）+返回字节数+数据值+校验；

写命令主站发送：从站地址+命令（06H）+数据地址+数据值+校验；

写命令从站返回：从站地址+命令（06H）+数据地址+数据值+校验；

当从站返回的读命令为83H，写命令为86H时则读写有错误。

**3 S7-1500组态和编程**

3.1设备组态

根据系统需求CPU选择S7-1511-1 PN，这个CPU最多可以配置4个通信模块，在CPU右侧第2个槽位插入CM1541（RS422/485）模块，模块的硬件标识符为257。CPU设置（见图1）：常规选项的系统和时钟存储器中选择启用系统存储器字节MB1，则系统上电首次标识位为M1.0。485通信模块CM1541的属性下端口组态中设置（见图2）：协议为自由口，操作模式为半双工（RS-485）2线制模式，传输率=9.6Kbps，奇偶校验=无奇偶校验，数据位=8位字符，停止位=1。

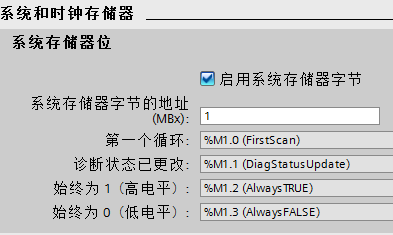


图1

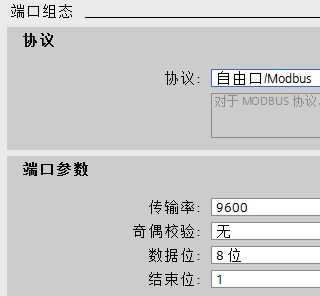


图2

3.2软件编程

创建Modbus RTU主站编程需要调用Modbus\_Comm\_Load 指令和Modbus\_Master 指令，其中Modbus\_Comm\_Load 指令通过 Modbus RTU 协议对用于通信的通信模块进行组态，组态数据将保存在CM模块中。Modbus\_Master 指令可通过由 Modbus\_Comm\_Load 指令组态的端口作为 Modbus 主站进行通信。程序流程图见图3。

（1）创建轮询函数块FC100：在轮询函数块中添加Modbus\_Comm\_Load 指令和Modbus\_Master 指令。自动产生背景数据块“Modbus\_Comm\_Load\_DB”（%DB4）和“Modbus\_Master\_DB” （%DB5）。



图3

（2）设置Modbus\_Comm\_Load指令（见图4）：Modbus\_Comm\_Load指令输入位“REQ”需使用上升沿触发，本例中该输入位采用 “FirstScan” 系统存储器位；输入为“PORT”与硬件硬件标识符一致为257；“BAUD”通讯速率为9600；“PARITY”奇偶校验为0；“RESP\_TO”为默认值1000即响应超时时间为1S；“MB\_DB”必须连接到 Modbus\_Master 指令的背景数据块的（静态）MB\_DB 参数"Modbus\_Master\_DB".MB\_DB；静态参数“MODE”更改为4半双工 (RS485) 二线制模式。

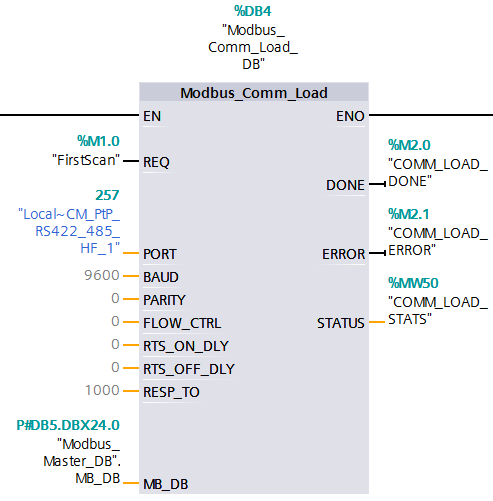


图4

（3）设置Modbus\_Master 指令（见图5）：Modbus\_Master 指令“REQ”需使用上升沿触发；“MB\_ADDR”为从站地址；“MODE”0为读，1为写，“DATA\_ADDR”起始地址；“DATA\_LEN”数据长度；“DATA\_PTR”参数用于指向要进行数据写入或数据读取的数据区域地址。

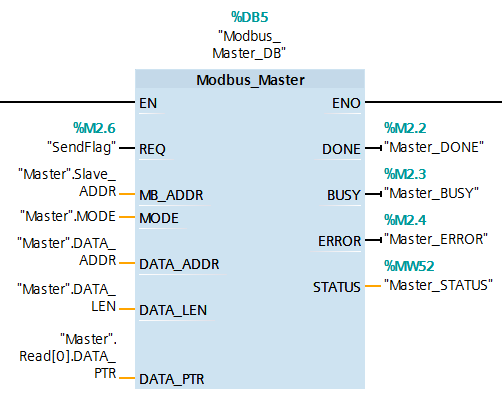


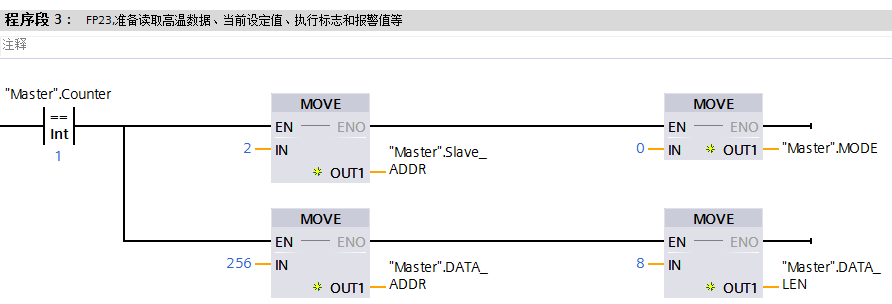
图5

（4）设置从站访问参数：添加DB数据块DB3（见表2）,里面的参数分别对应Modbus\_Master 指令输入参数，设置指令计数器（Counter）在1-2之间循环。本例为2个从站，在指令计数器为1和2时分别初始化从站地址、数据地址和长度（见图六）。“MODE”本例0。

表2从站方位参数数据块：Master%DB3

|  |  |  |
| --- | --- | --- |
| 名称 | 数据类型 | 注释 |
| Counter | Int | 指令计数器 |
| Read | Array[0..2]ofstruct | 从站数据存储地址 |
| Slave\_ADDR | UInt | 从站地址 |
| MODE | USInt | 读写模式 |
| DATA\_ADDR | UDInt | 数据起始地址 |
| DATA\_LEN | UInt | 数据长度 |

（5）访问从站：当调用Modbus\_Comm\_Load指令调用成功则其作业完成位“DONE”置位为1，这时设置指令计数器为1。调用Modbus\_Master 指令，读取从站地址1的值，并将“DATA\_PTR”读取的值赋值给从站1对应的数组。



图六

（6）指令计数器更新：Modbus\_Master指令的“REQ”检测到一个上升沿时，启动发送作业，从站收到主站请求后发送响应数据，从站的响应数据送回给CPU处理。

发送作业完成位“DONE”置位，同时指令计数器加1，构造下条指令，更新Modbus\_Master指令输入区地址，同时触发Modbus\_Master指令的“REQ”上升沿，启动下一个新的发送作业。

发送作业出错“ERROR”置位，那么判断该次发送作业失败，指令计数器加1，更新发送区地址和接收区地址启动下一个发送作业；

如果DONE和ERROR由于某些故障未能置位，为防止程序进入锁定状态，程序启动超时定时器本例设定为2S，超时时间到那么判断该次发送作业失败，指令计数器加1，更新发送区地址和接收区地址启动下一个发送作业。

当指令计数器超过最小和最大限值时，将最小值赋给指令计数器。

**4 结语**

ModbusRTU协议传输字节数少，效率高. 得到了众多仪表厂商的支持.在工业控制领域可以方便的与PLC组成工业网络，进行通信。本文提供了S7-1500作为主站轮询2个从站FP23的程序思路及部分程序，程序不用多次调用Modbus\_Maser指令，根据指令计数器的当前值，只需要更改背景数据块从站地址、读或写模式、数据地址、长度等就可以方便的读写不同的从站的不同地址空间；在实际应用中可根据实际情况更改背景数据块的参数还可方便的扩展从站的数量和读写模式。在程序中对于指令计数器的控制除了Modbus\_Maser指令的DONE和ERROR外增加超时计时器，防止程序意外进入锁定状态。

**参考文献**

[1]GB/T19582.2-2008基于Modbus协议的工业自动化网络规范第2部分：Modbus协议在串行链路上的实现指南[s]北京：中国标准出版社，2008.5

[2] 向晓汉 西门子S7-1500 PLC完全精通教程 化学工业出版社，2018.4