

基于 PLC 的 MODBUS 通信协议的实现

摘要：文章首先简要介绍了基于 PLC 的 MODBUS 通讯协议发展现状, 其次对 MODBUS 协议作了详细的阐述, 其中 S7-200 系列的 PLC 根据自身组网特点占有了相当大的比例，在处理流程中对其进行了详细的分析，对 PLC 中 MODBUS 协议的程序实现作了详细的介绍，充分展示了 MODBUS 通讯协议有着较为安全可靠特点。

关键词：MODBUS 通信协议，PLC，现场总线，串行通讯，

一、MODBUS 协议简介

MODBUS 协议是一种能够为工业控制体系进行正常通信的协议，其由 MODICON 公司为解决自身控制器问题而设计的。主要是根据 Master/Slave 的数据通讯方式进行数据通讯，前者（Master 端）发出信息的查询请求，再由后者（Slave 端）接收信息并满足前者发出的消息请求。也可以由 Master 端直接向 Slave 端发送消息以修改相关数据信息，以达到相互读写功能。

MODBUS 协议有两种传输模式:ASCII 模式和 RTU 模式，其通信格式如表 1。

在 ASCII 模式下的通讯方式是由两个 ASCII 字符作为一个 8Bit 字节应用并传送；在 RTU 模式下的通讯方式是由两个 4Bit 的 16 进制字符表示一个 8Bit 字节。显然，RTU 模式在相同波特率的情况下传输速率是大于 ASCII 模式的。

表 1 MODBUS 通信格式表

模式	起始位	数据位	校验位	停止位
ASCII	1Bit	7Bit	1Bit	1Bit
RTU	1Bit	8Bit	1Bit	1Bit

二、处理流程

编程时，一般利用通讯口的控制进行中断接收、发送、定时以及相关指令的发送和接收。其中断时间在 S7-200 中的具体情况如下：

表 2 S7-200 通讯编程中的中断事件

事件号	中断描述	优先组
9	端口 0：信息发送完成	通讯（最高）

23	端口 0: 信息接收完成	通讯 (最高)
10	定时中断 0	定时 (最低)

三、PLC 中 MODBUS 协议的程序实现

MODBUS 协议如果想要在 S7-200 中实现,就必须要在 S7-200 和 Modicon 公司的 PLC 性能能够支持的 S7-200 的前提下进行,但 S7-200 并不能够被 MODBUS 协议里的 24 种编码全应用,包括现场实际应用的情况和因素。且 Intellution 所支持的 MODBUS 驱动功能类型只包括以下几种:

01 读线圈状态; 02 读输入状态; 03 读保持寄存器。在 S7-200 中, V 存储区即 MODICONPLC 的保持寄存器; 04 读输入寄存器。在 S7-200 中, 模拟 t 输入寄存器即 MODICONPLC 的输入寄存器,通常将模拟 t 先存入指定的 V 存储区,这样读输入寄存器也就是读该指定的 V 存储区; 05 写单个输出线圈状态; 06 写单个保持寄存器值; 07 强制多轴输出线圈状态; 08 强制多保持寄存器。以上的全部功能均可以由 S7-200 的开发者实现,不过需要对几个问题进行注意: (1)首先要对帧的开始与结束进行正确的鉴别,不能有差错,3.5 字符的间隔是必须要有非常正确的识别,在 9600 的波特率下是大约有 4Ins 的时间。(2)查表法是校验 CRC 值计算的常用方法,且在计算一个 CRC 的校验值的过程是非常耗时的,在初始系统主程序时务必要有 CRC 表格的生成,以减少计算 CRC 的时间。(3)尽管能够实现 MODBUS 驱动 (IFix) 所提供的六项功能,但是偶尔会有失误的出现,甚至会造成从机能够达到的范围之外有了被寻址的变量,这样一来使得从机例外发送了相关相应。(4)访问寄存器的进行时依据字的在 MODBUS 内,不过 S7-216 能够实现从 V 存储区向字节、字、位以及双字的存取功能,因此可以变换主机所请求的寄存器的具体地址。

五、小结

S7-200 可编程控制器,在 MODBUS 通讯协议的协助下可以让大多数的现场扩展系统以及操作实现了 PC 机的信息联系。且 MODBUS 通讯协议有着较为安全可靠、透明的特点,无需过多流程就可将多家厂家结成网络,使得系统集成得以建立,从而减少了工厂开发产品和采购设备等的花销。

参考文献

- [1] SIEMENS 公司, SIMATIC S7-200 可编程序控制器系统手册[Z], 2000, 23-24.
- [2] 沈被娜等, 计算机软件技术基础[M]. 清华大学出版社, 2000, 34-36.