通过串行口访问 Modbus 现场控制网络

陈柏金

摘要：简要介绍了 Modbus 控制网络的特点、Modbus 协议、错误校验方法及与串行口的连接方式，对主要功能及其实现方法和技术进行了具体阐述，并简要分析了 Modbus 命令的响应时间。

关键词：Modbus Plus 网络　Modbus 协议　控制网络　串行口　通讯

Access Modbus field control network via serial port

Chen Baijin

Abstract: The Modbus control network, Modbus protocol, error checkout method and connection pattern are introduced in this paper, the main function of Modbus, implement means and technique are also described, the command respond time for Modbus is analyzed too.

Keywords: Modbus Plus network　Modbus protocol　Control network　Serial port　Communication

1 引言

Modbus 是一种工业通信和分布式控制系统协议，由美国可编程控制器制造商莫迪康（Modicon Inc.）公司出品，现已被众多的硬件厂商所支持并广泛应用。通过 Modbus 协议可以组成 Modbus Plus（MB+）现场控制网络，实现 PC 机与 PLC 及其它现场设备的互连。MB+是一种高速、对等工业控制网络，这一网络允许多台计算机、PLC 及其它数据源通过低成本的双绞线对等通信。MB+采用令牌总线结构，网络可靠性高、实时性好。图 1 是 MB+控制网络的示意图。

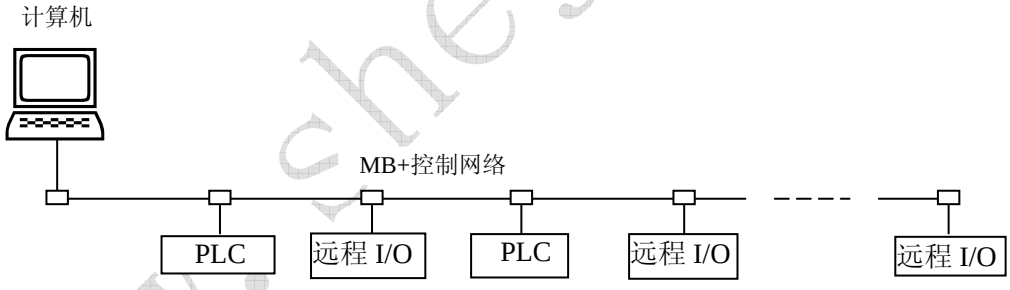

图 1　控制网络结构图

计算机访问 MB+网络有两种接入方式：

方式一：增加物理设备如 Modicon 公司的 SA85 系列网卡，将计算机与 Modbus 网络连成一体，直接应用网卡的驱动程序，采用 NetBIOS 调用编程，这种方式适用于数据交换比较大的应用，但成本较高。

方式二：不增加任何硬件，直接利用计算机的串行口访问 Modbus 网络，这种方式比较简单，能满足相当多的应用要求，但当数据量大时延迟时间较长。

2 Modbus 协议

2.1 协议简介

Modbus 协议通过主从设备间的询问应答环路交换信息。图 2 是 Modbus 协议的询问应答环路

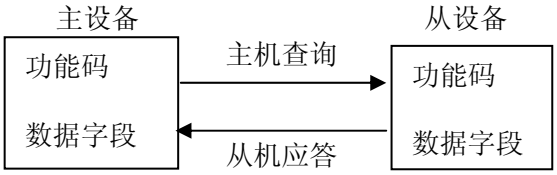

图 2　Modbus 协议的询问应答环路

主设备发送的报文通过接口到通讯线路，然后被传送到某台被编址设备。报文到达 Modbus 从机接口后，通过相同的端口进入被编址从机，从机读出报文，若无错误发生，便按要求执行任务，然后再将报文返回发送者。

Modbus 协议上允许 1 台主机和至多 247 台从属 PLC。只有主机才能启动事务处理程序。事务处理可以是应答式（只对一台 PLC 单机寻址），亦可是广播式（无应答，对所有 PLC 寻址）。事务处理程序由询问和应答帧组成，或由一个广播帧组成。

Modbus 的帧格式、帧顺序、通讯错误和异常处理，以及所执行的功能都不能随便更改，但传输介质的选择、波特率、字符奇偶校验、停止位的个数及传输模式等都能选择。用户选择的参数置入每一个站（用硬件或编程方式置入），这些参数在系统运行时不能改变。

Modbus 协议有两种传输模式可选择，这两种模式与从机 PLC 通讯的能力是同等的，每个 Modbus 系统只能使用其中一种模式。一种模式是 ASCII，另一种模式是 RTU（远程终端设备）。在控制系统中应用较多的是 RTU 模式。

RTU 报文的帧格式如图 3 所示。

地址码 (8 位)	功能码 (8 位)	数据 (N*8 位)	校验码 (16 位)

图 3　Modbus RTU 报文格式

地址码字段表示接收主机报文的从机地址。用户必须设置每台从机的地址。

功能码字段通知从站应执行何种功能。

数据字段含有从机执行某项具体功能的信息，或含有从机应答询问的信息，这些信息可以是数值、地址参数或范围。

校验码字段是用来检查通讯报文有无错误，RTU 模式采用 CRC-16（循环冗余错误检验）校验。

2.2 错误校验

Modbus系统采用CRC-16 校验来保证数据传输质量。Modbus报文被看作是一个连续的二进制数，报文先左移 16 位，然后被$X^{16}+X^{15}+X^2+1$（即二进制数 11000000000000101）除。整数商位忽略不计。16 位余数加入该报文，成为 2 个CRC校验字节。经上述处理而含有CRC字节的报文，若无错误，到接收设备后再被同一多项式（$X^{16}+X^{15}+X^2+1$）除，会得到一个零余数。

下面是用 8086 汇编写成的 CRC-16 过程。报文的起始地址送 SI 寄存器，报文长度送 CX 寄存器，最后运算的 CRC 结果存 BX 寄存器。

```
crc_parity:   cld
              mov     bx,0ffffh
crc@1:        lodsb
              xor     ah,ah
              xor     bx,ax
              push    cx
```

```
            mov     cx,8
crc@2:      shr     bx,1
            jnc     crc@3
            xor     bx,0a001h
crc@3:      loop    crc@2
            pop     cx
            loop    crc@1
            ret
```

2.3 与串行口的连接

图 4 是 9 芯标准串行口与 Modbus 口的接线图

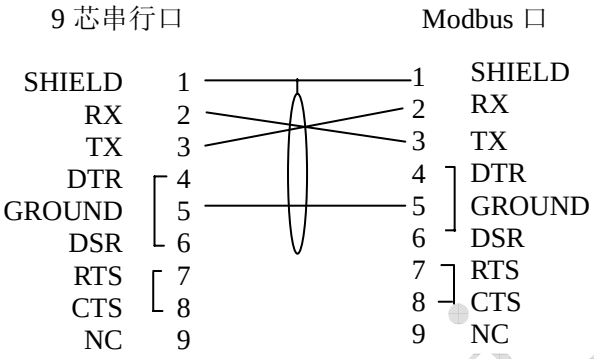

图 4　串行口与 Modbus 口连接示意图

3 功能描述

3.1 读取输出状态（功能码 01）

本功能可使用户取得被编址从机逻辑线圈的通断状态（ON/OFF）。

询问报文除从机地址和功能字段外，报文还含有要使用的初始线圈的起始地址和被询问数量及错误检验字段，线圈编号从 0 开始。

应答报文含从机地址，功能码，数据字符量，数据字符及错误校验。每个线圈只占一位（1=ON，0=OFF），第一个字符的最低位是被读取起始线圈地址，余者依次排列。若线圈数量不是偶数 8，最后一个字符的高位端将置 0。

如图 5 为读取 9 号从机的线圈 0020~0056 状态的示例报文：

读取输出状态询问报文（均为 16 进制数）：

地址	功能	数据起始地址高位	数据起始地址低位	数据线圈数高位	数据线圈数低位	错误检验字段
9	1	00	13	00	25	5C0D

读取输出状态应答报文：

地址	功能	字节计数	数据线圈状态 20~27	数据线圈状态 28~35	数据线圈状态 36~43	数据线圈状态 44~51	数据线圈状态 52~56	错误检验字段
09	01	5	12	34	56	78	AB	68A5

图 5　读取输出状态报文格式

该报文用 8086 汇编语言定义如下：

```
；询问报文
PLC_Require          db      09,01       ;读 9 号从机输出线圈状态
PLC_StartAddress     db      0,13        ;从线圈 0020 开始，所有编号均从 0 开始
PLC_ReadLength       db      0,25        ;总共 37 个线圈
PLC_CommandCRC       dw      ?           ;上述命令进行 CRC-16 运算生成的结果
；应答报文
PLC_Answer           db      ?,?         ;从机返回状态，如正确则返回值同 PLC_Require
PLC_AnswerLength     db      ?           ;返回值为 PLC_ReadLength/8 取整的结果
PLC_AnswerData       db      5 dub(?)    ;返回的线圈状态，个数为 PLC_ReadLength/8
PLC_AnswerCRC        dw      ?           ;从机返回的应答报文 CRC-16 结果
```

询问报文的校验结果由用户根据报文命令生成，用户收到应答报文后应用 CRC-16 算法验证报文的正确性，然后根据报文返回的状态进行相应处理。

3.2 读取输入状态（功能码 02）

本功能使用户取得被编址从机 PLC 的离散输入通断状态（ON/OFF）。如要读取 9 号从机的输入 10197~10218 状态的询问与应答报文如图 6 所示，输入编号从 0 开始，每一个输入状态仅占 1 位，第一个字符的低位是编址的第一个输入，余者依次排列。

读取输入状态询问报文：

地址	功能	数据起始地址高位	数据起始地址低位	数据输入点数高位	数据输入点数低位	错误检验字段
09	02	00	C4	00	20	6739

读取输入状态应答报文：

地址	功能	字节计数	数据开关输入 10197~10204	数据开关输入 10205~10212	数据开关输入 10213~10218	错误检验字段
09	02	3	AB	CD	10	BA5D

图 6　读取输入状态报文格式

3.3 读取保持寄存器（功能码 03）

本功能允许读取从机 PLC 中寄存器状态，每个寄存器为 2 字节，先高位后低位，从 9 号从机读取寄存器 40150、40151 内容的报文如图 7 所示。

读取保持寄存器询问报文：

地址	功能	数据起始寄存器高位	数据起始寄存器低位	数据寄存器数高位	数据寄存器数低位	错误检验字段
09	03	00	95	00	02	6FD5

读取保持寄存器应答报文：

地址	功能	字节计数	数据输出寄存器高位 40150	数据输出寄存器低位 40150	数据输出寄存器高位 40151	数据输出寄存器地位 40151	错误检验字段
09	03	04	12	34	56	78	C708

图 7　读取输出寄存器报文格式

3.4 读取输入寄存器（功能码 04）

本功能报文格式同功能码 04，如读 9 号从机 30120 号寄存器的报文格式如图 8 所示：

读取输入寄存器询问报文：

地址	功能	数据起始寄存器高位	数据起始寄存器低位	数据寄存器数高位	数据寄存器数低位	错误检验字段
09	04	00	77	00	01	9880

读取输入寄存器应答报文：

地址	功能	字节计数	数据输入寄存器高位 30120	数据输入寄存器低位 30120	错误检验字段
09	04	02	12	34	C1DE

图 8　读取输入寄存器报文格式

3.5 强置单线圈（功能码 05）

本功能可将 PLC 中单个线圈强置为 ON 或 OFF 状态，数据 0FF00 置线圈为 ON 状态，数据 0 置线圈为 OFF 状态，如强制 5 号从机的 0300 线圈为 ON 状态的报文如图 9 所示。

强置单线圈询问报文：

地址	功能	数据线圈号高位	数据线圈号低位	数据通断指示	数据通断指示	错误检验字段
09	05	01	2B	FF	00	86FC

强置单线圈应答报文：在线圈状态已改变后将收到的报文原文发回。

图 9　读取输入寄存器报文格式

3.6 强置多线圈（功能码 15）

本功能可把一组连续线圈中的每一个线圈强置为所要求的通/断状态，控制器内任何线圈均可被强置为 ON 或 OFF 状态。如将 9 号从机 20 开始的 10 个线圈中线圈 27、26、23、22 及 20 强置为 ON 状态的报文如图 10 所示。

强置多线圈询问报文：

地址	功能	线圈起始地址高位	线圈起始地址低位	线圈数高位	线圈数低位	字节计数	线圈状态 20-27	线圈状态 28-29	错误检验字段
09	0F	00	13	00	0A	02	CD	00	CBD4

强置多线圈应答报文：

地址	功能	线圈起始地址高位	线圈起始地址低位	线圈数高位	线圈数低位	错误检验字段
09	0F	00	13	00	0A	4125

图 10　强置多线圈报文格式

3.7 预置多寄存器（功能码 16）

本功能可以修改控制器内保持寄存器的内容，不用的高位必须置 0。从机地址为 0 时，即广播模式（只有 5、15、16 功能码在广播模式有效），所有从机均把指定值装入指定的寄存器。如将 09 号从机的 40200、40201 寄存器置成 0A00h 和 0201h 的报文如图 11 所示。

预置多寄存器询问报文：

地址	功能	起始地址高位	起始地址低位	寄存器数高位	寄存器数低位	字节计数	数据高位	数据低位	数据高位	数据低位	错误检验字段
09	10	00	C7	00	02	04	00	0A	01	02	2A34

预置多寄存器应答报文：

地址	功能	起始地址高位	起始地址低位	寄存器数高位	寄存器数低位	错误检验字段
09	10	00	C7	00	02	7DF1

图 11　预置多寄存器报文格式

4 Modbus 命令响应时间

Modbus 命令的响应时间主要由下述因素决定：

⑴ 主机编排报文时间；

⑵ 向从机 PLC 传送数据时间(ms) = (1000*字符数*每字符所含位数)/波特率；

⑶ 从机处理报文

由于 Modbus 命令是在控制器扫描终了时得到处理，因此，接收报文和开始处理该报文之间最长延时是一个扫描周期（这种情况发生在报文恰好在 Modbus 窗口闭合时到达从机 PLC），平均延时为 1/2 扫描周期。若报文处理的数据量较大，可能需多个 Modbus 窗口，每个窗口时间约为 1ms 左右。

⑷ 从机 PLC 执行错误校验的时间，CRC-16 运算时间对应答的每一个 8 位数据都是 0.3ms。

⑸ 向主机发回应答报文时间(ms) =(1000*字符数*每字符所含位数)/波特率

⑹ 主机接收应答、核查错误校验、数据输出，并把数据送至应用程序。

5 结论

上述方法已成功地在多个工程项目中得到应用。实际证明：这种方式组成的系统结构简单，组态灵活，应用方便，能满足多数工程的实际需要。

参考文献：

[1]　陈柏金，黄树槐，靳龙等，Modbus Plus 网络在快锻液压机组控制系统中的应用，微计算机信息，1999.1

作者简介：陈柏金　男，37 岁，工学博士，副教授

作者单位：华中科技大学材料学院(430074)

通信地址：武汉市珞喻路 1037 号华中科技大学主校区材料学院　430074

陈柏金　email: chenbaijin@sina.com　Tel:027-87541145-809