ModBus通讯协议

目录

一、接线说明

1. RS485 抄表－利用RS485 通讯硬件进行的4 线制较远距离的串行通讯；
2. 总线为4芯线，信号线－A、B、地、电源12V-24V；
3. 表上有4芯线、 B(蓝)、A（黄）、地（黑）、电源（12V），对应接好（分极性，接错可能烧毁）；如为红黑黄棕时， B(黄)、A（棕）、地（黑）、红、电源（12V），对应接好（分极性，接错可能烧毁）
4. 在800 米以内通讯，最多244个终端；
5. 波特率(默认)为9600bps（可选）,无校验（可选），一起始位，一停止位，8位数据位；
6. 水表响应数据时，字节与字节之间的停顿时间大约为4ms；
7. 全部明文传输，无加密；
8. 校验方式CRC-16/ModBus,x16+x15+x2+1；

二、协议说明

1：支持功能码

03 读取寄存器

06 写入单个寄存器

2：1、通讯说明

上位机发送：01 03 00 01 00 02 95 CB

解析说明：

1：地址

03：功能码

00 01：起始寄存器地址

00 02：数据长度

95 CB:CRC16 校验低字节在前

表回复：01 03 04 86 9F 00 01 22 95

01：地址

03：功能码

04：数据长度

86 9F 00 01：表具数据（十六进制）表示表数据为 0*1869F 对应十进制数据为 99999

22 95：CRC16 校验低字节在前

2、广播读取表仪表 MODBUS 地址

上位机下发：00 03 00 01 00 02 94 1A

解析说明：

00：广播地址 03：功能码

00 01：起始寄存器地址

00 02：数据长度

94 1A :CRC16 校验低字节在前

表回复：01 03 04 86 9F 00 01 22 95

01：为仪表地址

03：功能码

04：数据长度

86 9F 00 01：表具数据（十六进制）表示表数据为 0*1869F 对应十进制数据为 99999

22 95：CRC16 校验低字节在前

3、修改表具通讯地址

举例：1 改为 2

上位机发送：01 06 00 00 00 02 08 0B

01:表具旧地址

06：写入功能码

00 00：写入寄存器地址

00 02：写入寄存器地址（02 位**新地址**）

08 0B：CRC16 校验低字节在前

4、改波特率指令

2400 改 9600：FE FE FE 42 42 42 42 53 FF FF FF FF 58 23 C1 EC 45

9600 改 2400：FE FE FE 42 42 42 42 53 FF FF FF FF 58 21 C1 EE 45

5、**Modbus 地址**：仪表出厂地址不固定，用户可用广播读地址指令读取。

三、测试实例：

1、如用 ModScan32 软件测试时：

启动 ModScan32.exe 测试软件，Device Id(仪表地址 LocalAdress)设为 1，MODBUS Point Type(命令字)设为 03，Adress(数据地址)设为 0002（本来应该是地址 1，但是这个软件会自动将地址减一，所以该为 2），Length(数据长度)设为 2。如图

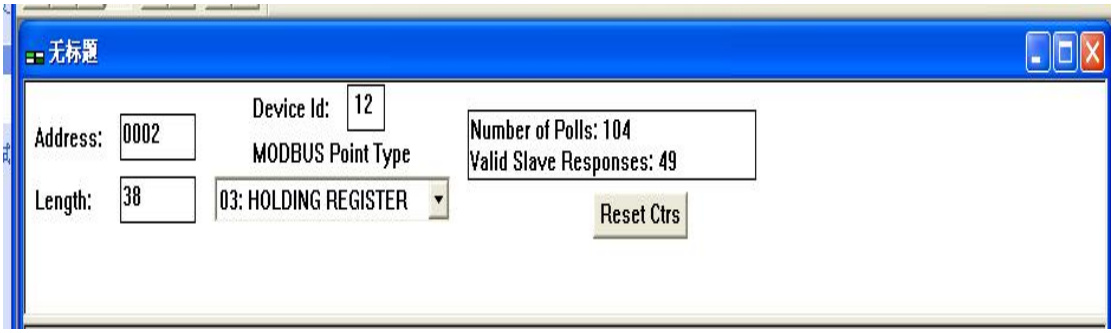

图 1

使用菜单“Connection/Connect”，选择 Connect 为相应端口号，baud 波特率(根据实际表里的波特率进行填写），word(数据位)为 8，Parit 校验位(根据实际表里

的波特率进行填写），Stop(停止位)为 1，”Rotocal Selection\Transmission Mode”选择”STANDARD RTU”。然后点击“OK”键确定。如图 2