1 MODBUS RTU 通讯协议  
**1.1** 通讯数据的类型及格式：  
信息传输为异步方式，并以字节为单位。在主站和从站之间传递的通讯信息是11位的字格式：  
表1：

|  |  |
| --- | --- |
| 字格式（串行数据） | 11位二进制 |
| 起始位 | 1位 |
| 数据位 | 8位 |
| 奇偶校验位 | 无 |
| 停止位 | 2位 |

**1.2** 通讯数据（信息帧）格式  
表2：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据格式 | 地址码 | 功能码 | 数据区 | CRC校验 |
| 数据长度 | 1字节 | 1字节 | N字节 | 16位CRC码（冗余循环码） |

2 通讯信息传输过程：  
当通讯命令由发送设备（主机）发送至接收设备（从机）时，符合相应地址码的从机接收通讯命令，并根  
据功能码及相关要求读取信息，如果CRC校验无误，则执行相应的任务，然后把执行结果（数据）返送给主机。  
返回的信息中包括地址码、功能码、执行后的数据以及CRC校验码。如果CRC校验出错就不返回任何信息。  
**2.1** 地址码：  
地址码是每次通讯信息帧的第一字节（8位），从0到254。这个字节表明由用户设置地址的从机将接收由主  
机发送来的信息。每个从机都必须有唯一的地址码，并且只有符合地址码的从机才能响应回送信息。当从机回  
送信息时，回送数据均以各自的地址码开始。主机发送的地址码表明将发送到的从机地址，而从机返回的地址  
码表明回送的从机地址。相应的地址码表明该信息来自于何处。  
**2.2** 功能码：  
功能码是每次通讯信息帧传送的第二个字节。 ModBus通讯规约可定义的功能码为1到127。作为主机请求  
发送，通过功能码告诉从机应执行什么动作。作为从机响应，从机返回的功能码与从主机发送来的功能码一样，  
并表明从机已响应主机并且已进行相关的操作。  
表3 MODBUS部分功能码

|  |  |  |
| --- | --- | --- |
| 功能码 | 定 义 | 操 作（二进制） |

2

|  |  |  |
| --- | --- | --- |
| 0x03 | 读保持寄存器数据 | 读取一个或多个寄存器的数据（最大128个寄存器） |
| 0x04 | 读输入寄存器 | 读取一个或多个输入寄存器的数据（最大128个寄存器） |
| 0x10 | 写多路保持寄存器 | 把多组二进制数据写入多个寄存器（最大128个寄存器） |
| 0x43 | 修改波特率 |  |

**2.3** 数据区：  
数据区包括需要由从机返送何种信息或执行什么动作。这些信息可以是数据（如：开关量输入/输出、  
模拟量输入/输出、寄存器等等）、参考地址等。例如，主机通过功能码03告诉从机返回寄存器的值（包含要读  
取寄存器的起始地址及读取寄存器的长度），则返回的数据包括寄存器的数据长度及数据内容。对于不同的从  
机，地址和数据信息都不相同（应给出通讯信息表）。  
  
**2.4** 静止时间要求  
发送数据前要求数据总线静止时间即无数据发送时间大于（5ms 波特率为115200时） .  
**2.5** 寄存器定义  
输入寄存器： 1F40– 1FBF  
保持寄存器： 2000 – 2040  
3 **MODBUS**功能码简介  
**3.1** 功能码“**03**”：读多路保持寄存器输入  
例如：主机要读取地址为01，起始地址为2000的2个从机寄存器数据。  
从机数据寄存器的地址和数据为：  
主机发送的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机发送 | 字节数 | 发送的信息 | 备 注 |
| 从机地址 | 1 | 01 | 发送至地址为01的从机 |
| 功能码 | 1 | 03 | 读寄存器 |
| 起始地址 | 2 | 2000 | 起始地址为2000 |
| 读数据长度 | 2 | 0002 | 读取2个寄存器（共4个字节） |

|  |  |  |
| --- | --- | --- |
| 寄存器地址 | 寄存器数据（16进制） | 对应参数 |
| 2000 | 0E10 |  |
| 2001 | C0CB |  |

3

|  |  |  |  |
| --- | --- | --- | --- |
| CRC码 | 2 | CFCB | 由主机计算得到CRC码 |

从机响应返回的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 从机响应 | 字节数 | 返回的信息 | 备 注 |
| 从机地址 | 1 | 01 | 来自从机01 |
| 功能码 | 1 | 03 | 读寄存器 |
| 数据长度（字节数） | 1 | 08 | 共8个字节 |
| 寄存器1的数据 | 2 | 0E10 | 地址为2000寄存器的内容 |
| 寄存器2的数据 | 2 | C0CB | 地址为2001寄存器的内容 |
| CRC码 | 2 | 6089 | 由从机计算得到CRC码 |

**3.2** 功能码“**04**”：读多路输入寄存器  
例如：主机要读取地址为01，起始地址为1F40的2个从机寄存器数据。  
从机数据寄存器的地址和数据为：  
主机发送的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机发送 | 字节数 | 发送的信息 | 备 注 |
| 从机地址 | 1 | 01 | 发送至地址为01的从机 |
| 功能码 | 1 | 04 | 读寄存器 |
| 起始地址 | 2 | 1F40 | 起始地址为1F40 |
| 读数据长度 | 2 | 0002 | 读取2个寄存器（共4个字节） |
| CRC码 | 2 | 77CB | 由主机计算得到CRC码 |

从机响应返回的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 从机响应 | 字节数 | 返回的信息 | 备 注 |
| 从机地址 | 1 | 01 | 来自从机01 |
| 功能码 | 1 | 04 | 读寄存器 |
| 数据长度（字节数） | 1 | 04 | 共4个字节 |
| 寄存器1的数据 | 2 | 0E10 | 地址为1F40寄存器的内容 |
| 寄存器2的数据 | 2 | C0CB | 地址为1F41寄存器的内容 |
| CRC码 | 2 | E93E | 由从机计算得到CRC码 |

**3.3** 功能码“**10**”：写多路保持寄存器  
主机利用这个功能码把多个数据保存到仪器的数据存储器中去。 Modbus通讯规约中的寄存器指的是16  
位（即2字节），并且高位在前。  
例如：主机要把0E10保存到地址为2000的从机寄存器中去（从机地址码为01）。  
主机发送的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机发送 | 字节数 | 发送的信息 | 备 注 |
| 从机地址 | 1 | 01 | 发送至地址为01的从机 |
| 功能码 | 1 | 10 | 写多路寄存器 |
| 起始地址 | 2 | 2000 | 要写入的寄存器的起始地址 |

|  |  |  |
| --- | --- | --- |
| 寄存器地址 | 寄存器数据（16进制） | 对应参数 |
| 1F40 | 0E10 |  |
| 1F41 | C0CB |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 保存数据长度 | 2 | 0001 | 保存数据的字长度 |
| 保存数据字节长 | 1 | 02 | 保存数据的字节长度（4字节） |
| 保存数据1 | 2 | 0E10 | 待写入2000地址的数据 |
| CRC码 | 2 | 823E | 由主机计算得到CRC码 |

从机响应返回的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 从机响应 | 字节数 | 发送的信息 | 备 注 |
| 从机地址 | 1 | 01 | 发送至地址为01的从机 |
| 功能码 | 1 | 10 | 写多路寄存器 |
| 起始地址 | 2 | 2000 | 要写入的寄存器的起始地址 |
| 保存数据长度 | 2 | 0001 | 保存数据的字长度 |
| CRC码 | 2 | 0A09 | 由从机计算得到CRC码 |

**3.4** 功能码“**43**”： 修改波特率  
主机利用这个功能码从机修改波特率。  
例：修改波特率为115200（0x0001C200） 指令如下（从机地址码为01）：  
主机发送的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机发送 | 字节数 | 发送的信息 | 备 注 |
| 从机地址 | 1 | 01 | 发送至地址为01的从机 |
| 功能码 | 1 | 43 | 修改波特率 |
| 数据长度 | 1 | 04 | 数据长度 |
| 数据 | 4 | 0001C200 | 波特率 |
| CRC码 | 2 | 2063 | 由主机计算得到CRC码 |

从机响应返回的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 从机响应 | 字节数 | 发送的信息 | 备 注 |
| 从机地址 | 1 | 01 | 发送至地址为01的从机 |
| 功能码 | 1 | 43 | 远程升级 |
| 数据长度 | 1 | 04 | 数据长度 |
| 数据 | 4 | 0001C200 | 波特率 |
| CRC码 | 2 | 0263 | 由从机计算得到CRC码 |

4 错误校验码（**CRC**校验）：  
主机或从机可用校验码进行判别接收信息是否正确。由于电子噪声或一些其它干扰，信息在传输过程中有  
时会发生错误，错误校验码（CRC）可以检验主机或从机在通讯数据传送过程中的信息是否有误，错误的数据  
可以放弃（无论是发送还是接收），这样增加了系统的安全和效率。  
MODBUS通讯协议的CRC（冗余循环码）包含2个字节，即16位二进制数。 CRC码由发送设备（主机）计  
算，放置于发送信息帧的尾部。接收信息的设备（从机）再重新计算接收到信息的CRC，比较计算得到的CRC  
是否与接收到的相符，如果两者不相符，则表明出错。  
  
**4.1 CRC**码的计算方法  
1、预置 1 个 16 位的寄存器为十六进制 FFFF（即全为 1）；称此寄存器为 CRC 寄存器；  
2、把第一个 8 位二进制数据（既通讯信息帧的第一个字节）与 16 位的 CRC 寄存器的低 8 位相异或，把结果  
放于 CRC 寄存器；  
3、把 CRC 寄存器的内容右移一位（朝低位）用 0 填补最高位，并检查右移后的移出位；  
4、如果移出位为 0：重复第 3 步（再次右移一位）； 如果移出位为 1： CRC 寄存器与多项式 A001（1010 0000  
0000 0001）进行异或；  
5、重复步骤 3 和 4，直到右移 8 次，这样整个 8 位数据全部进行了处理；  
6、重复步骤 2 到步骤 5， 进行通讯信息帧下一个字节的处理；  
7、将该通讯信息帧所有字节按上述步骤计算完成后，得到的 16 位 CRC 寄存器的高、低字节进行交换；  
8、最后得到的 CRC 寄存器内容即为： CRC 码。  
C 语言例程如下：  
unsigned short crc\_calc(unsigned char \*p,unsigned char len)  
{  
//1、准备 CRC 校验初始值  
unsigned short crc\_data = 0xffff;  
unsigned char i ;  
unsigned char j ;  
//6、重复步骤 2 到步骤 5，进行通讯信息帧下一个字节的处理；  
while( len-- )  
{  
i = \*p++;  
//2、 CRC 寄存器的低 8 位相异或  
crc\_data ^= i;  
//5、重复步骤 3 和 4，直到右移 8 次，这样整个 8 位数据全部进行了处理；  
for(j=0;j<8;j++)  
{  
//4.1、如果移出位为 1： CRC 寄存器与多项式 A001（1010 0000 0000 0001）进行异或；  
if( crc\_data & 0x01 )  
{  
//3、把 CRC 寄存器的内容右移一位（朝低位）用 0 填补最高位，并检查右移后的移出位；  
crc\_data >>= 1;  
crc\_data ^= 0xA001;  
}  
//4.2、如果移出位为 0：重复第 3 步（再次右移一位）；  
else  
{  
crc\_data >>= 1;  
}  
}  
}  
//7、将该通讯信息帧所有字节按上述步骤计算完成后，得到的 16 位 CRC 寄存器的高、低字节进行交换；  
  
i = crc\_data >> 8;  
crc\_data <<= 8;  
crc\_data |= i;  
//8、最后得到的 CRC 寄存器内容即为： CRC 码。  
return crc\_data;  
} 5  
参数说明  
**5.1** 输入寄存器**(**功能码**04)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 功能 | 类型 | 单位 | 取值范围 | 占用字节数 | 输入寄存器地址 | 备注 |
| 软件版本 | 字符串 | -- | 4 | 1F40 | 例如： V00.90 记为 0x30303930 |  |
| MSN 地址 | 整形 | -- | 4 | 1F46 |  |  |
| 动压 | 浮点 | Pa | 0～2000 | 4 | 1F48 |  |
| 流速 | 浮点 | m/s | 0～40 | 4 | 1F4A |  |
| 温度 | 浮点 | ℃ | 0～500 | 4 | 1F4C |  |
| 流量 | 浮点 | m³/s | 0～3200 | 4 | 1F4E |  |
| 压力 | 浮点 | kPa | ﹣ 10～﹢ 10 | 4 | 1F50 |  |
| 大气压 | 浮点 | kPa | 70～130 | 4 | 1F52 |  |
| 电压值 | 浮点 |  | 4 | 1F70 |  |  |
| 反吹气压力 | 浮点 | MPa | 4 | 1F72 |  |  |
| 波特率 | 整形 | -- | 4 | 1F76 |  |  |
| 湿度 | 浮点 | % | 4 | 1F82 |  |  |

**5.2** 保持寄存器**(**功能码**03)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 功能 | 读写属性 | 类型 | 单位 | 取值范围 | 占用字节数 | 保持寄存器地址 | 备注 |
| 设备地址 | 读/写 | 整形 | -- | 0～255 | 2 | 2000 |  |
| 预留 | 禁止写入 | -- | -- | -- | 2 | 2001 | 写入时， 请恢复 出厂设置 |
| 反吹时间间隔 | 读/写 | 整形 | 分 | 1～960 | 4 | 2002 |  |
| 预留 | 禁止写入 | -- | -- | -- | 2 | 2004 | 写入时， 请恢复 出厂设置 |
| 动压量程 | 读/写 | 整形 | Pa | 300,1000 ,2000， | 2 | 2005 | 300： 0-300， 1000:0-1000， 2000： 0-2000 其中一个选择 |
| 流速量程 | 读/写 | 整形 | m/s | 15， 30， 40 | 2 | 2006 | 15： 0-15， 30： 0-30， 40： 0-40 其中一个选择 |
| 预留 | 禁止写入 | 整形 | -- | -- | 2 | 2007 | 写入时， 请恢复 出厂设置 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 2008 | 写入时， 请恢复 出厂设置 |
| 预留 | 禁止写入 | 浮点 | -- | 4 | 200A | 写入时， 请恢复 出厂设置 |  |
| 预留 | 禁止写入 | -- | -- | -- | 4 | 200C | 写入时， 请恢复 出厂设置 |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 200E | 大气压控制使 用输入值时有 效 |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 2010 | 写入时， 请恢复 出厂设置 |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 2012 | 写入时， 请恢复 出厂设置 |
| 压力量程上限 | 读/写 | 整形 | KPa | 2,5,10,1 30 | 2 | 2013 | 2：±2、 5：±5， 10：±10、 130： 70-130 其中一个选择 |
| 压力量程下限 | 读 | 整形 | KPa | 2 | 2014 | 不需要写入 |  |
| 温度量程 | 读/写 | 整形 | ℃ | 300,500 | 2 | 2015 | 300： 0-300， 500： 0-500 其中一个选择 |
| 预留 | 禁止写入 | 整形 | -- | -- | 2 | 2016 | 1 使用采集值， 0 使用输入值 |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 2018 | 写入时， 请恢复 出厂设置 |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 201A | 写入时， 请恢复 出厂设置 |
| 预留 | 禁止写入 | -- | -- | -- | 2 | 201C | 写入时， 请恢复 出厂设置 |
| 流量量程 | 读/写 | 整形 | m³/s | 0～3200 | 2 | 201D |  |
| 烟道截面积 | 读/写 | 浮点 | m² | 0.0～ 80.0 | 4 | 201E |  |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 2020 | 写入时， 请恢复 出厂设置 |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 2022 | 写入时， 请恢复 出厂设置 |
| 反吹控制标志 位 | 读/写 | 整形 | -- | 1 | 2 | 2024 | 设置为 备进行反吹 1 时，设 |
| 校零控制标志 位 | 读/写 | 整形 | -- | 1 | 2 | 2025 | 设置为 备进行校零 1 时，设 |
| 预留 | 禁止写入 | -- | -- | -- | 4 | 2026 | 写入时， 请恢复 出厂设置 |
| 预留 | 禁止写入 | -- | -- | -- | 4 | 2028 | 写入时， 请恢复 出厂设置 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 预留 | 禁止写入 | -- | -- | -- | 2 | 202A | 写入时， 请恢复 出厂设置 |
| 预留 | 禁止写入 | -- | -- | -- | 2 | 202B | 写入时， 请恢复 出厂设置 |
| 预留 | 禁止写入 | 整形 | -- | -- | 2 | 202C | 1 时允许自动 校零/0 时关闭 校零 |
| 预留 | 禁止写入 | -- | -- | -- | 2 | 202D | 写入时， 请恢复 出厂设置 |
| 恢复出厂设置 标志 | 读/写 | 整形 | -- | 0,1 | 2 | 202E | 1 时恢复出厂 设置 |
| 预留 | 禁止写入 | 整形 | -- | -- | 2 | 202F | 写入时，请恢复 出厂设置 |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 2030 | 写入时，请恢复 出厂设置 |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 2032 | 写入时，请恢复 出厂设置 |
| 预留 | 禁止写入 | 浮点 | -- | -- | 4 | 2034 | 写入时，请恢复 出厂设置 |

6 （ModBus-RTU） 协议实例V1.1  
**6.1** 读取参数一个  
FF 03 20 05 00 01 8A 15  
//( 03)读取 FF 设备的地址 20 05 寄存器开始 00 01 个的值， CRC 校验为 8A 15  
下位机返回： FF 03 02 05 00 92 C0  
**6.2** 读取参数多个  
FF 03 20 05 00 03 0B D4  
//( 03)读取 FF 设备的地址 20 05 寄存器开始 00 03 个的值， CRC 校验为 0B D4  
下位机返回： FF 03 06 05 00 CD CC CC 3D 03 06  
**6.3** 写入参数一个  
FF 10 20 05 00 01 02 01 00 CE 33  
//（10） 写入 FF 设备的地址 20 05 寄存器开始的 0001 个的值，数据长共 02 字节，数据为 01 00， CRC 校验  
为 CE 33  
下位机返回： FF 10 20 05 00 01 0F D6  
**6.4** 写入参数多个  
FF 10 1F C0 00 02 04 01 00 00 00 45 D8  
//（10） 写入 FF 设备的地址 1F C0 寄存器开始的 0002 个的值，数据长共 04 字节，数据为 01 00 00 00， CRC  
校验为 45 D8  
下位机返回： FF 10 1F C0 00 02 53 FE  
**6.5** 修改波特率  
01 43 04 00 01 C2 00 F4 53  
//（43） 写入 01 设备的地址， 波特率数据为 00 01 C2 00， CRC 校验为 F4 53  
下位机返回： 01 43 04 00 01 C2 00 F4 53