ES系列三相电力仪表通信协议说明

一、 MODBUS-RTU协议简介

1、 仪表符合MODBUS-RTU通信协议，采用RS485半双工通信，对数据进行16位CRC校验，仪表对校验错误不返回。

1.1 所有RS485回路通信应遵照主、从方式。在这种方式下，信息和数据在单个主站和最多32个从站（监控设备）之间传递；
1.2 主站将初始化和控制所有在RS485通信回路上传递的信息；
1.3 无论如何都不能从一个从站开始通信；
1.4 所有RS485环路上的通信都以“打包”方式发生。一个数据包就是一个通信帧，一个包中最多可含128个字节；
1.5 主站发送称为请求，从站发送称为响应；
1.6 任何情况从站只能响应主站一个请求；

2、数据格式

起始位	数据位	校验位	停止位
1	8	无、偶、奇校验（可编程）	1

3、通信帧格式

帧内容	字节数	说明	
从站地址	1	有效的从站地址范围为1-247	
功能码	1	0X03	读取一个或多个当前寄存器值
		0X06	将指定数值写入内部一个寄存器内
		0X10	将指定数值写入内部多个寄存器内
数据地址	2	从站执行有效命令时数据区域存储的位置。不同变量占用不同寄存器个数，有些地址变量占用两个寄存器，4字节数据，有些变量占用一个寄存器，2字节数据，请根据实际情况使用	
数据长度	2	需要读取或写入的数据长度	
数据	可变	从站返回应答数据或主站待写数据	
CRC校验码	2	MODBUS-RTU模式采用16位CRC校验。发送设备应当对包裹中的每一个数据都进行CRC16计算，最后结果存放入检验域中。接收设备也应当对包裹中的每一个数据（除校验域以外）进行CRC16计算，将结果域校验域进行比较。只有相同的包裹才可以被接受。	

4、通信异常处理

如果主站发送了一个非法的数据包或者是主站请求一个无效的数据寄存器时，异常的数据响应就会产生。这个异常数据响应由从站地址、功能码、故障码和校验域组成。当功能码域的高比特位置为1 时，说明此时的数据帧为异常响应。

根据MODBUS通讯要求，异常响应功能码=请求功能码+0x80；异常应答时，将功能号的最高位置1。例如：主机请求功能号为0x04，则从机返回的功能号对应为0x84。

下表说明异常错误码的含义：

错误码	名称	说明
0X01	功能码错误	仪表接收到不支持的功能号
0X02	变量地址错误	主机指定的数据位置超出仪表的范围或接收到非法的寄存器操作
0X03	数据值越限	主机发送的数据值超出仪表对应的数据范围或数据结构不完整
0X04	帧长度错误	功能码和通信帧长度不一致

5、通信帧延时

主站两帧请求之间应该有适当的延时供从站进行应答处理，当通信波特率为9600时，为保证收到正确的应答，建议两帧请求之间保留300mS延时。波特率降低时，通信延时应该适当的增加。

二、通信帧格式说明

1、功能码“03”：读多路寄存器输入

例：主机读取UA（A相电压），设现测量到A相电压为220.0V。UA的地址编码是0x4000,因为UA是定点数(4字节)，占用2个数据寄存器，220.0V对应的十六进制数据是：0x0000898（2200）。

主机发送的报文格式：（默认高字在前）

主机发送	字节数	发送的信息	发送的信息
从机地址	1	01	发送至地址为01的从机
功能码	1	03	发送至地址为01的从机
起始地址	2	0x4000	起始地址
数据长度	2	0x0002	读取2个寄存器（共4个字节）
CRC码	2	0XD1CB	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	读取寄存器
读取字	1	04	2个寄存器共4个字节
寄存器数据	1	0x00	地址为0x4000内存的内容高高字节
	1	0x00	地址为0x4000内存的内容高字节
	1	0x08	地址为0x4000内存的内容低字节
	1	0x98	地址为0x4000内存的内容低低字节
CRC码	2	0xFC59	由从机计算得到CRC码

2、功能码“06”：写单路寄存器

例：主机写定点数第1路报警方式AD1。假设AD1的地址编码是0x4900，因为AD1是定点数，占用1个数据寄存器，十进制11对应为0X000B。

主机发送的报文格式：

主机发送	字节数	发送信息	举例
从机地址	1	01	发送至从机01
功能码	1	06	写单路寄存器
起始地址	1	0x49	要写入的寄存器地址高字节
	1	0x00	要写入的寄存器地址低字节
待写入数据	1	0x00	数据高字节
	1	0x0B	数据低字节
CRC码	2	0xDE51	由主机计算得到的CRC码

从机响应正确返回的报文格式：

主机发送	字节数	发送信息	举例
从机地址	1	01	发送至从机01
功能码	1	06	写单路寄存器
起始地址	1	0x49	要写入的寄存器地址高字节
	1	0x00	要写入的寄存器地址低字节
待写入数据	1	0x00	数据高字节
	1	0x0B	数据低字节
CRC码	2	0xDE51	由主机计算得到的CRC码

3、功能码“10”：写多路寄存器

例：主机写定点数第1路报警方式AD1。假设AD1的地址编码是0x4900，因为AD1是定点数，占用1个数据寄存器，十进制11对应为0X000B。

主机发送的报文格式：

主机发送	字节数	发送信息	举例
从机地址	1	01	发送至从机01
功能码	1	10	写多路寄存器
起始地址	1	0x49	要写入的寄存器的起始地址高字节
	1	0x00	要写入的寄存器的起始地址低字节
待写数据字长度	1	0x00	写入数据的字长度高字节
	1	0x01	写入数据的字长度低字节
待写数据字节长	1	0x02	数据的字节长度（共1字节）
待写入数据	1	0x00	数据高字节
	1	0x0B	数据低字节
CRC码	2	0x3F53	由主机计算得到的CRC码

从机响应正确返回的报文格式：

从机响应	字节数	发送的信息	发送的信息
从机地址	1	01	来自从机01
功能码	1	10	写多路寄存器
起始地址	2	0x4900	起始地址为0000
保存数据字长度	2	0x0002	保存2个字长度的数据
CRC码	2	0X1795	由从机计算得到CRC码

4、CRC码的计算方法是：

4.1 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；

4.2 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；

4.3 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；

4.4 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；

4.5 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；

4.6 重复步骤2到步骤5，进行通讯信息帧下一个字节的处理；

4.7 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；

4.8 最后得到的CRC寄存器内容即为：CRC码。

附：CRC计算C语言源码

```
unsigned int GET_CRC(unsigned char * buf,unsigned charnum)
{
        unsigned  chari,j;
        unsigned int      WCRC    =       0xffff;
        for(i=0;i<num;i++)
        {
                WCRC              ^=      (unsigned int)(buf[i]);       //      循环冗余校验
                for(j=0;j<8;j++)
                {
                        if(WCRC&1)
                        {
                                WCRC            >>=     1;
                                WCRC            ^=      0XA001;
                        }
                        else
                        WCRC            >>=     1;
                }
        }
        return(WCRC);                                                                   //      获得CRC校验码
}
```

三、电力仪表通信地址映射

三相智能电力仪表地址定义							
只读电力参数通信列表							
序号	通讯地址	参数名称	寄存器数	数据类型	读写类型	单位	备注
1	0x4000	相电压A	2	long	R	0.1V	
2	0x4002	相电压B	2	long	R	0.1V	
3	0x4004	相电压C	2	long	R	0.1V	
4	0x4006	线电压AB	2	long	R	0.1V	
5	0x4008	线电压BC	2	long	R	0.1V	
6	0x400a	线电压CA	2	long	R	0.1V	
7	0x400c	相电流A	2	long	R	0.001A	
8	0x400e	相电流B	2	long	R	0.001A	
9	0x4010	相电流C	2	long	R	0.001A	
10	0x4012	有功功率A	2	long	R	0.1W	
11	0x4014	有功功率B	2	long	R	0.1W	
12	0x4016	有功功率C	2	long	R	0.1W	
13	0x4018	总有功功率	2	long	R	0.1W	
14	0x401a	无功功率A	2	long	R	0.1var	
15	0x401c	无功功率B	2	long	R	0.1var	
16	0x401e	无功功率C	2	long	R	0.1var	
17	0x4020	总无功功率	2	long	R	0.1var	
18	0x4022	视在功率A	2	long	R	0.1VA	
19	0x4024	视在功率B	2	long	R	0.1VA	
20	0x4026	视在功率C	2	long	R	0.1VA	
21	0x4028	总视在功率	2	long	R	0.1VA	
22	0x402a	功率因数A	2	long	R	0.001	
23	0x402c	功率因数B	2	long	R	0.001	
24	0x402e	功率因数C	2	long	R	0.001	
25	0x4030	总功率因数	2	long	R	0.001	
26	0x4032	频率	2	long	R	0.01HZ	
27	0x4034	有功电度	2	long	R	0.001kWh	数码管类仪表无电能计量功能，读数据无效
28	0x4036	无功电度	2	long	R	0.001kvarh	
29	0x4038	正向有功电度	2	long	R	0.001kWh	
30	0x403a	负向有功电度	2	long	R	0.001kWh	
31	0x403c	正向无功电度	2	long	R	0.001kvarh	
32	0x403e	负向无功电度	2	long	R	0.001kvarh	

保留扩展							
系统设置参数列表							
1	0x4800	接线方式	1	short	R	无小数点	附1
2	0x4801	电压变比PT1	1	short	R/W	0.1kV	固定小数点
3	0x4802	电压变比PT2	1	short	R/W	0.1V	
4	0x4803	电流变比CT1	1	short	R/W	1A	
5	0x4804	电流变比CT2	1	short	R/W	0.1A	固定小数点
6	0x4805	通信地址1	1	short	R/W	无小数点	
7	0x4806	波特率1	1	short	R/W		附2
8	0x4807	数据格式1	1	short	R/W		
9	0x4808	通信地址2	1	short	R/W		备用
10	0x4809	波特率2	1	short	R/W		
11	0x480a	数据格式2	1	short	R/W		
12	0x480b	开关量输出	1	short	R		附4
13	0x480c	开关量输入	1	short	R		附5
14	0x480d	遥控输入	1	short	R/W		附6
保留扩展							
报警通信参数列表							
1	0x4900	第1路报警方式	1	short	R/W	无小数点	
2	0x4901	第1路报警单位	1	short	R/W		附3
3	0x4902	第1路报警值	1	short	R/W	0.1	固定小数点
4	0x4903	第1路回差值	1	short	R/W	0.1	
5	0x4904	第1路报警输出方式	1	short	R	无小数点	
6	0x4905	第1路动作延时	1	short	R/W	0.1s	固定小数点
7	0x4906	第1路切除延时	1	short	R/W	0.1s	
第二路或更多路报警通信地址请从第一路地址结束处顺延读取							
保留扩展							

附1：接线方式说明：

通信地址	数值	显示字符	说明
0X4800	0	3-4	三相四线连接
	1	3-3	三相三线连接

附2：通信波特率

通信地址	数值	显示字符	说明
0X4805	0	1.2K	波特率1200bps
	1	2.4K	波特率2400bps
	2	4.8K	波特率4800bps
	3	9.6K	波特率9600bps
	4	19.2K	波特率19200bps

附3：报警及变送单位

通信地址	数值	显示字符	说明
0X4901、0X4908 0X4A01、0X4A05	0	1	单位为1
	1	K	单位为K
	2	M	单位为M

附4：报警输出状态指示

通信地址	通信地址	报警回路	说明
0X480B	BIT2-BIT15	未用	未用
	BIT1	报警2	0：报警未动作；
			1：报警动作；
	BIT0	报警1	0：报警未动作；
			1：报警动作；

附5：开关量输入状态指示

通信地址	通信地址	报警回路	说明
0X480C	BIT4-BIT15	未用	未用
	BIT3	开关量输入4	0：断开；
			1：接通；
	BIT2	开关量输入3	0：断开；
			1：接通；
	BIT1	开关量输入2	0：断开；
			1：接通；
	BIT0	开关量输入1	0：断开；
			1：接通；

附6：遥控输出命令说明

通信地址	位序号	报警回路	说明
0X480D	BIT2-BIT15	未用	未用
	BIT1	遥控2	0：断开继电器；
			1：接通继电器；
	BIT0	遥控1	0：断开继电器；
			1：接通继电器；