MODBUS 通讯协议

1、完成功能：共使用 4 种功能码，完成 8 种功能，**高字节在前，低字节在后**，具体描述如下；

（一） 功能码 2：上传开关量

主机向从机发送的数据为：

序号	1	2	3	4	5	6	7	8
	设备地址	0x 02	0x00	0x00	0x00	N	CRC 高位	CRC 低位

Eg.01 02 00 00 0020 79 D2

从机向主机发送的数据为：（数据为 BIT 类型）

序号	1	2	3	4~14	15	16
	设备地址	0x 02	0x 0B	遥信信息	CRC 高位	CRC 低位

（二） 功能码 3：上传遥测量、脉冲值、及整定值

1.上传遥测量

主机向从机发送的数据为：

序号	1	2	3	4	5	6	7	8
	设备地址	0x03	0x01	0x00	**0x00**	N	CRC 高位	CRC 低位

eg：01 03 01 00 00 0E C5 F2

3－4 表起始地址，遥测量从 0x0100 开始,每个遥测量占一个地址；

5－6 表读取遥测量个数；

从机向主机发送的数据为：　　数据为 INT 类型

序号	1	2	3	4~N*2+3	N*2+4	N*2+5
	设备地址	0x03	N*2	数据	CRC 高位	CRC 低位

3：主机向从机发送的数据说明，N 表示需要上传的遥测个数，

4－N*2+3：遥测量，高字节在前，低字节在后

2.上传整定值

主机向从机发送的数据为：

序号	1	2	3	4	5	6	7	8
	设备地址	0x03	0x02	0x00	**0x00**	N	CRC 高位	CRC 低位

eg：01 03 02 00 00 20 45 AA

3－4 表起始地址，整定值从 0x0200 开始，每个定值占一个地址；

5－6 表读取定值个数，点号详见说明书的定值表；

从机向主机发送的数据为：　　数据为 INT 类型

序号	1	2	3	4~N*2+3	N*2+4	N*2+5
	设备地址	0x03	N*2	数据	CRC 高位	CRC 低位

3：主机向从机发送的数据说明，N 表示需要上传的定值个数，

4－N*2+3：定值，高字节在前，低字节在后，为定值实际值乘以 100

3.上传脉冲量（仅支持具有电度功能的产品）

主机向从机发送的数据为：

序号	1	2	3	4	5	6	7	8
	设备地址	0x03	0x03	0x00	**0x00**	N	CRC 高位	CRC 低位

eg：01 03 03 00 00 04 44 4D

3－4 表起始地址，遥脉量从 0x0300 开始，每个遥脉量占 2 个地址；

5－6 表读取脉冲量 word 个数

从机向主机发送的数据为：　　数据为 INT 类型

序号	1	2	3	4~N*4+3	N*4+4	N*4+5
	设备地址	0x03	N*4	数据	CRC 高位	CRC 低位

3：主机向从机发送的数据说明，N 表示需要上传的脉冲量个数，

4－N*4+3：遥脉量，高字节在前，低字节在后

（三） 功能码 5： 下传开关量、遥控复归

1. 下传开关量

主机向从机发送的数据为：　　数据为 INT 类型

序号	1	2	3	4	5	6	7	8
	设备地址	0x05	0x00	N	0xff	0x00	CRC 高位	CRC 低位

Eg :01 05 00 00 ff 00 8C 3A

N 表示要遥控的位号，0x00~0x7 表示 1K~8K，

特殊的，遥控复归命令位号为 0xff：

序号	1	2	3	4	5	6	7	8
	设备地址	0x05	0x00	0xff	0xff	0x00	CRC 高位	CRC 低位

从机向主机返回完全一样的数据作为应答。

（四） 功能码 06：下传对时信息和整定值

1. 下传对时信息

主机向从机发送的数据为：　　数据为 char 类型

序号	1	2	3	4	5	6	7	8
	0xcc	0x06	0x04	N	0x00	0x01	CRC 高位	CRC 低位

Eg :CC 06 04 00 00 08 99 21,表将年设为 08 年，注：下传时间用压缩 BCD 码表示。

3－4 表对时地址，时钟地址从 0x0400 开始

5－6 表对时下传的时间值

N=0---6　分别为年、月、日、时、分、秒、毫秒的高位和低位，十六进制数。每次上位机仅下传一种对时信息，分 7 次传完。

从机向主机返回完全一样的数据作为应答。

2. 下传整定值

主机向从机发送的数据为：　　数据为 char 类型

序号	1	2	3	4	5	6	7	8
	设备地址	0x06	0x02	N	0x00	0x01	CRC 高位	CRC 低位

Eg :01 06 02 00 00 64 89 99，表示将第 1 号定值设为 1（实际下传值为 100）；

3－4 表设定值地址，定值地址从 0x0200 开始

5－6 表下传的定值，注意：下传的设定值为实际值的 100 倍，如定值为 10.5A，下传值应为 1050；

从机向主机返回完全一样的数据作为应答。

附录通讯点表

一、遥信点表

遥信点表：本区域为当前数字量输入 DI 状态、投退和事件遥信，用户可采用 Modbus 协议 02 号功能码读取				
地址	参数	数值范围	数据类型	读写属性
0000H~000FH	DI1~DI16	1=ON，0=OFF	Bit	R
0010H~002FH	事件1~事件32	1=ON，0=OFF	Bit	R
0030H~004FH	投退 1~投退 32	1=ON，0=OFF	Bit	R
0050H~0057H	备用	1=ON，0=OFF	Bit	R

注意：DI 具体每一位所对应的开入量信息，请参考现场图纸；

投退和事件具体每一位所对应的事件信息，请参考各型号说明书的事件表。

二、遥测点表

遥测点表：本区域的各参数均为遥测输出，采用 Modbus 协议 03 功能码读取				
地址	参数	数值范围	数据类型	读写属性
0100H~0111H	遥测1~遥测18	-32767~32767	Word	R

说明：各型装置点表详见附录

三、定值点表

定值点表：本区域的各参数均为定值参数，采用 Modbus 协议 03 功能码读取，06 功能码写				
地址	参数	数值范围	数据类型	读写属性
0200H~021FH	定值1~定值32	0~32767	Word	R/W

说明：定值具体每一位所对应的定值信息，请参考各型号说明书对应的定值表。

四、遥脉点表

遥脉点表：本区域的各参数均为遥脉输出，采用 Modbus 协议 03 功能码读取				
地址	参数	数值范围	数据类型	读写属性
0300H	遥脉1低16位	0~32767	Word	R
0301H	遥脉1高16位	0~32767	Word	R
0302H	遥脉2低16位	0~32767	Word	R
0303H	遥脉2高16位	0~32767	Word	R
0304H	遥脉3低16位	0~32767	Word	R
0305H	遥脉3高16位	0~32767	Word	R
0306H	遥脉4低16位	0~32767	Word	R
0307H	遥脉4高16位	0~32767	Word	R

说明：该功能仅支持具有电度功能的装置（查看装置是否具有“电能脉冲”菜单）

四、遥控点表

遥控点表：本区域的各参数均为遥控参数，采用Modbus协议05功能码写					
地址1	地址2	参数	命令码	数据类型	读写属性
0000H	0001H	出口1	0x00FF	Word	W
0001H	0002H	出口 2	0x00FF	Word	W
0002H	0004H	出口 3	0x00FF	Word	W
0003H	0008H	出口 4	0x00FF	Word	W
0004H	0010H	出口 5	0x00FF	Word	W
0005H	0020H	出口 6	0x00FF	Word	W

0006H	0040H	出口 7	0x00FF	Word	W
0007H	0080H	出口 8	0x00FF	Word	W
00ffH	00ffH	复归	0x00FF	Word	W

说明：SPMC3000 系列装置遥控点表使用地址 2；特殊型号使用地址 1

附录：遥测点表

1、 SPMC3000

2、 SPMC3000 遥测点表：f,Uab,Ubc,Uca,Ua,Ub,Uc, IA,IB,IC,P,Q,cos,I0,U0