通讯规约

1. 引言

通讯规约详细描述了本机串行口通讯的读、写命令格式及内部信息数据的定义，以便第三方开发使用。

1.1. PLC ModBus 兼容性

ModBus 通讯规约允许与施耐德、西门子、AB、GE、Modicon 等多个国际著名品牌的可编程顺序控制器(PLC)、RTU、SCADA 系统、DCS 或第三方具有 ModBus 兼容的监控系统之间进行信息和数据的有效传递。有了智能表，就只要简单的增加一套基于 PC(或工控机)的中央通讯主控显示软件(如：组态王、Intouch、FIX、synall 等)就可建立一套监控系统。

1.2. 广泛的通讯集成

智能表提供与 Modicon 系统相兼容的 ModBus 通讯规约，这个通讯规约被广泛作为系统集成的标准。兼容 RS-485/232C 接口的可编程逻辑控制器 ModBus 通讯规约允许信息和数据在智能表与 Modicon 可编程逻辑控制器(PLC)，RTU、SCADA 系统、DCS 系统和另外兼容 ModBus 通讯规约的系统之间进行有效传递。

2. ModBus 基本规则

2.1. 所有 RS485 通讯回路都应遵照主/从方式。依照这种方式，数据可以在一个主站(如：PC)和 32 个子站(如：)之间传递。

2.2. 主站将初始化和控制在 RS485 通讯回路上传递的所有信息。

2.3. 任何一次通讯都不能从子站开始。

2.4. 在 RS485 回路上的所有通讯都以“信息帧”方式传递。

2.5. 如果主站或子站接收到含有未知命令的信息帧，则不予以响应。

“信息帧”就是一个由数据帧(每一个字节为一个数据帧)构成的字符串(最多 255 个字节)，是由信息头和发送的编码数据构成标准的异步串行数据，该通讯方式也与 RTU 通讯规约相兼容。

3. 数据帧格式：

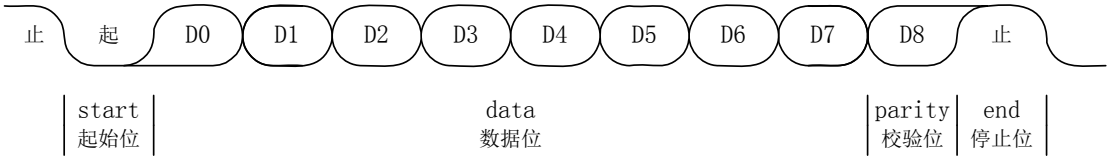
通讯传输为异步方式，并以字节(数据帧)为单位。在主站和子站之间传递的每一个数据帧都是11位的串行数据流。

数据帧格式：

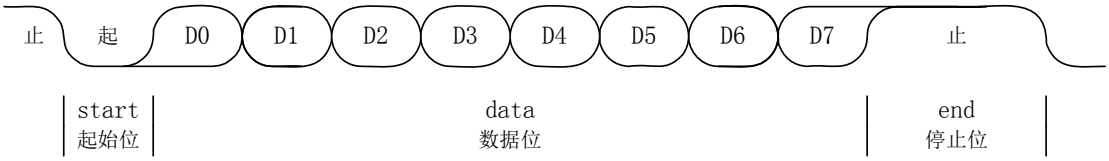
起始位	1 位

数据位	8 位(低位在前、高位在后)
奇偶校验位	1 位：有奇偶校验位；无：无奇偶校验位
停止位	1 位：有奇偶校验位；2 位：无奇偶校验位

有校验位的时序图：



无校验位的时序图：



4. 通讯规约

当通讯命令发送至仪器时，符合相应的地址码的设备接收通讯命令，并除去地址码，读取信息，如果没有出错，则执行相应的任务；然后把执行结果返送给发送者。返送的信息中包括地址码、执行动作的功能码、执行动作后的数据以及错误校验码(CRC)。如果出错就不发送任何信息。

4.1. 信息帧格式

START	ADD	CS	DATA	CRC	END
初始结构	地址码	功能码	数据区	错误校验	结束结构
延时(相当于4 个字节的时间)	1 字节 8 位	1 字节 8 位	N 字节 N×8 位	2 字节 16 位	延时(相当于4 个字节的时间)

4.1.1. 地址码(ADD)

地址码为每次通讯传送的信息帧中的第一个数据帧(8 位)，从 0 到 255。这个字节表明由用户设定地址码的子机将接收由主机发送来的信息。并且每个子机都有唯一的地址码，并且响应回送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子机地址，而子机发送的地址码表明回送的子机地址。

4.1.2.　功能码(CS)

功能码是每次通讯传送的信息帧中的第二个数据帧。ModBus 通讯规约定义功能码为 1～127(01H～7FH)。利用其中的一部分功能码。作为主机请求发送，通过功能码告诉子机执行什么动作。作为子机响应，子机发送的功能码与主机发送来的功能码一样，并表明子机已响应主机进行操作。如果子机发送的功能码的最高位是 1(功能码＞127)，则表明子机没有响应或出错。

下表列出的功能码都具体的含义及操作。

MODBUS 部分功能码

功能码	定义	操作
03H	读寄存器	读取一个或多个寄存器的数据
06H	写单个寄存器	把一个 16 位二进制数写入单个寄存器

1、 03，读寄存器

智能表采用 ModBus 通讯规约，利用通讯命令，可以进行读取点(保持寄存器或返回值输入寄存器)。功能码 03H 映射的数据区的保持和输入寄存器值都是 16 位(2 字节)。这样从读取的寄存器值都是 2 字节。一次最多可读取寄存器数是 125。由于一些可编程控制器不用功能码 03，所以功能码 03 被用作读取点和返回值。

子机响应的命令格式是子机地址、功能码、数据区及 CRC 码。数据区的数据都是每 2 个字节为一组的双字节数，且高字节在前。

2、 06，写单个寄存器：

主机利用这条命令把单点数据保存到智能电力监测仪的存储器。子机也用这个功能码向主机返送信息。

3、 10，写多个点连续寄存器：

主机利用这条命令把多点数据保存到系列数字式多功能电力监测仪的存储器。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。这样智能电力监测仪的点都是二字节。用一条命令保存的最大点数取决于子机。因为 Modbus 通讯规约允许最多保存 60 个寄存器，这样系列智能电力监测仪允许一次最多可保存 60 个寄存器。智能电力监测仪的命令格式是子机地址、功能码、数据区及 CRC 码。

4.1.3.　数据区(DATA)：

数据区随功能码不同而不同。由主机发送的读命令(03H)信息帧的数据区与子机应答信

息帧的数据区是不同的，由主机发送的写命令(06H、10H)信息帧的数据区与子机应答信息帧的数据区是完全相同。数据区包含需要子机执行什么动作或由子机采集的需要回送的信息。这些信息可以是数值、参考地址等等。例如，功能码告诉子机读取寄存器的数值，则数据区必须包含要读取寄存器的起始地址及读取长度(寄存器个数)。

a) 与功能码 03 对应的数据区格式：

◆ 主机发送

数据顺序	1	2
数据含义	起始地址	读寄存器个数
字节数	2	2

◆ 子机应答

数据顺序	1	2
数据含义	回送字节数	N 个寄存器的数据
字节数	1	2×N

b) 与功能码 06 对应的数据区格式：

数据顺序	1	2
数据含义	起始地址	写入寄存器的数据
字节数	2	2

c) 与功能码 10 对应的数据区格式：

数据顺序	1	2	…	N
数据含义	起始地址	写入数据 1	…	写入数据 N
字节数	2	2	…	2

4.1.4. 错误校验码(CRC)：

主机或子机可用校验码进行判别接收信息是否出错。有时，由于电子噪声或其他一些干扰，信息在传输过程中会发生细微的变化，错误校验码保证了主机或子机对在传送过程中出错的信息不起作用。这样增加了系统的安全和效率。错误校验码采用 CRC-16 校验方法。

二字节的错误校验码，低字节在前，高字节在后。

注意：	信息帧的格式都是相同的：地址码、功能码、数据区和错误校验码。

4.2. 错误校验

冗余循环码(CRC)包含 2 个字节，即 16 位二进制。CRC 码由发送端计算，放置于发送信息的尾部。接收端的设备再重新计算接收到信息的 CRC 码，比较计算得到的 CRC 码是否与接收到的相符，如果二者不相符，则表明出错。

CRC 码的计算方法是，先预置 16 位寄存器全为。再逐渐把每 8 位数据信息进行处理。在进行 CRC 码计算时只用 8 位数据位，起始位及停止位，如有奇偶校验位的话也包括奇偶校验位，都不参与 CRC 码计算。

在计算 CRC 码时，8 位数据与寄存器的数据相异或，得到的结果向低位移一位，用 0 填补最高位。再检查最低位，如果最低位为 1，把寄存器的内容与预置数相异或，如果最低位为 0，不进行异或运算。

这个过程一直重复 8 次。第 8 次移位后，下一个 8 位再与现在寄存器的内容相异或，这个过程与上以上一样重复 8 次。当所有的数据信息处理完后，最后寄存器的内容即为 CRC 码值。

4.3. CRC-16 码的计算步骤

1、 置 16 位寄存器为十六进制 FFFF(即全为 1)。称此寄存器为 CRC 寄存器。

2、 把一个 8 位数据与 16 位 CRC 寄存器的低位相异或，把结果放于 CRC 寄存器。

3、 把寄存器的内容右移一位(朝低位)，用 0 填补最高位，检查最低位(移出位)。

4、 如果最低位为 0：复第 3 步(再次移位)。

如果最低位为 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，进行下一个 8 位的处理。

7、 最后得到的 CRC 寄存器即为 CRC 码，低字节在前，高字节在后。

4.4. 信息帧格式举例

4.4.1. 功能码 03

子机地址为 01，起始地址 0032 的 3 个寄存器。

此例中寄存器数据地址为：

地 址	数据(16 进制)
0032	EA60
0034	C350
0036	DB6C

主机发送	字节数	举　例(16 进制)	
子机地址	1	01	送至子机 01
功能码	1	03	读取寄存器
起始地址	2	00	起始地址为 0032
		32	
读取个数	2	00	读取 3 个寄存器(共 6 字节)
		03	
CRC 码	2	A4	由主机计算得到的 CRC 码
		04	

子机响应	字节数	举　例(16 进制)	
子机地址	1	01	送至子机 01
功能码	1	03	读取寄存器
读取字节数	1	06	3 个寄存器(共 6 字节)
寄存器数据 1	2	EA	地址为 0032 内的内容
		60	
寄存器数据 2	2	C3	地址为 0034 内的内容
		50	
寄存器数据 3	2	DB	地址为 0036 内的内容
		6C	
CRC 码	2	D1	由子机计算得到的 CRC 码
		3F	

4.4.2.　功能码 06

子机地址为 01,保存起始地址 0002 的 2 个值。在此例中，数据保存结束后，子机中地址为 0002 内的内容为 0002。

主机发送	字节数	举　例(16 进制)	
子机地址	1	01	发送至子机 01
功能码	1	06	单个数据(2 字节)保存
起始地址	2	00	起始地址为 0002
		02	
保存数据	2	00	保存的数据为 0002
		02	
CRC 码	2	A9	由主机计算得到的 CRC 码
		CB	

子机响应	字节数	举　例(16 进制)	
子机地址	1	01	来自子机 01
功能码	1	06	单点保存
起始地址	2	00	起始地址为 0002
		02	

保存数据	2	00	保存的数据为 0002
		02	
CRC 码	2	A9	由子机计算得到的 CRC 码
		CB	

4.4.3. 功能码 10

子机地址为 01，把 0064 保存到地址 0000。在此例中，数据保存结束后，地址为 01 的系列智能电力监测仪内保存的信息为：

地址	数据(16 进制)
0000	0064

主机发送	字节数	举 例(16 进制)	
子机地址	1	01	发送至子机 01
功能码	1	10	多点保存
起始地址	2	00	起始地址为 0000
		00	
保存数据数	2	00	保存 2 点(共 4 字节)
		02	
字节数	1	04	
保存数据 1	2	00	数据地址为 0002
		64	
保存数据 2	2	00	数据地址为 0000
		00	
CRC 码	2	B2	由主机计算得到的 CRC 码
		70	

子机响应	字节数	举 例(16 进制)	
子机地址	1	01	来自子机 01
功能码	1	10	多点保存
起始地址	2	00	起始地址为 0000
		00	
保存数据数	2	00	保存 2 点(共 4 字节)
		02	
CRC 码	2	41	由子机计算得到的 CRC 码
		C8	

4.5. 出错处理

当系列智能电力监测仪检测到了 CRC 码出错以外的错误时，必须向主机回送信息，

功能码的最高位置为 1，即子机返送给主机的功能码是在主机以送的功能码的基础上加 128。以下的这些代码表明有意外的错误发生。

从主机接收到的信息如有 CRC 错误，则将被系列智能电力监测仪忽略。

子机返送的错误码的格式如下(CRC 码除外)

地址码：	1 字节
功能码：	1 字节(最高位为 1)
错误码：	1 字节
CRC 码：	2 字节

系列数字式多功能电力监测仪响应回送如下出错命令

01	非法的功能码。 接收到的功能码系列智能电力监测仪不支持。
02	非法的数据位置。 指定的数据位置超出系列智能电力监测仪范围
03	非法的数据值 接收到主机发送的数据值超出相应地址的数据范围。

附录一：数据和地址

表 1：功能码 03H 所映射的数据区-基本数据：

基本数据(Basic)

序号	地址(Address)	项目(Item)	说明	数据格式
1	0000H	Ua	相电压 Ua	0.01V
2	0001H	Uca	线电压 Uca	0.01V
3	0002H	Ia	A 相电流	0.0001A
4	0003H			
5	0004H	Pa	A 相有功功率	0.4W
6	0005H	PFa	A 相功率因数	0.0001
7	0006H	Qa	A 相无功功率	0.4Var
8	0007H	Sa	A 相视在功率	0.2VA
9	0008H	Ub	相电压 Ub	0.01V
10	0009H	Uab	线电压 Uab	0.01V
11	000AH	Ib	B 相电流	0.0001A
12	000BH			
13	000CH	Pb	B 相有功功率	0.4W
14	000DH	PFb	B 相功率因数	0.0001
15	000EH	Qb	B 相无功功率	0.4Var
16	000FH	Sb	B 相视在功率	0.2VA
17	0010H	Uc	相电压 Uc	0.01V
18	0011H	Ubc	线电压 Ubc	0.01V
19	0012H	Ic	C 相电流	0.0001A
20	0013H			
21	0014H	Pc	C 相有功功率	0.4W
22	0015H	PFc	C 相功率因数	0.0001
23	0016H	Qc	C 相无功功率	0.4Var
24	0017H	Sc	C 相视在功率	0.2VA
25	0018H	Uav	三相平均相电压	0.01V
26	0019H	Ulv	三相平均线电压	0.01V
27	001AH	Iav	三相平均相电流	0.0001A
28	001BH	F	频率	0.00106813
29	001CH	Psum	三相有功功率	0.4W
30	001DH	PFav	三相总功率因数	0.0001
31	001EH	Qsum	三相无功功率	0.4Var
32	001FH	Ssum	三相视在功率	0.2VA
33	0020H	Phase Rotation		

表 2：功能码 03H 所映射的数据区-电能质量数据：

序号	地址(Address)	项目(Item)	说明	数据格式
1	0100H	U1	正序电压	0.01V
2	0101H	U2	负序电压	0.01V
3	0102H	Uo	零序电压	0.01V
4	0103H	ε U2	电压不平衡度（负序）	0.1%
5	0104H	I1	正序电流	0.0001A
6	0105H	I2	负序电流	0.0001A
7	0106H	Io	零序电流	0.0001A
8	0107H	ε I2	电流不平衡度（负序）	0.1%

表 3：功能码 03H 所映射的数据区-电能：

电能

序号	地址	项目	说明	数据格式
1	0021H	+Wh(L)	正向有功电能累加值低位字	Wh
2	0022H	+Wh(H)	正向有功电能累加值高位字	
3	0023H	-Wh(L)	负向有功电能累加值低位字	Wh
4	0024H	-Wh(H)	负向有功电能累加值高位字	
5	0025H	+Varh(L)	正向无功电能累加值低位字	Vrah
6	0026H	+Varh(H)	正向无功电能累加值高位字	
7	0027H	- Varh(L)	负向无功电能累加值低位字	Varh
8	0028H	- Varh(H)	负向无功电能累加值低高字	

电能数据为 2 个字长，解析方法：

如 正向有功电能数据= Wh(H)*65536+Wh(L)

其他电能数据解析方法也一样。

表 4：功能码 03H/06H 所映射的系统参数：

参数地址	项目	字节数	说明	初始状态
0300H	本机地址	2	1～247	0
0301H	被测系统负载接线方式	2	0 三相四线 1 一相二线 2 三相三线 3 三相三线平衡 4 一相三线 5 三相四线平衡	0
0303H	校验位	2	0 无校验 1 奇校验 2 偶检验	0

0304H	波特率	2	0 1200 1 2400 2 4800 3 9600 4 19200	3
0307H	PT	2	1～60000	1
0309H	CT	2	1～60000	1
0313H	功率反向	2		0
031FH	光亮强度		1	0-7
0340H～035FH	厂家保留			

附录二：数据变换

所有从响应输出的数据都被按一定公式规范成 2 个字节 Rx，电能除外，为 4 个字节。

NO	项目	公式	取值范围	符号	说明			
1	电压 V	U = Rx×PT×0.01	0～65535	无	Ua	Ub	Uc	Ue0
					Uca	Uab	Ubc	Ue
2	电流 A	I =Rx×CT×0.0001	0～65535	无	Ia	Ib	Ic	Ie
3	频率 Hz	F =Rx×0.00106813	0～65535	无	F			
4	功率因数 PF	PF =Rx×0.0001	-10000～10000	有	PFa	PFb	PFc	PFs
					+:滞后负载 /-:超前负载			
5	有功功率 W	P = Rx×PT×CT×0.4	-32768～32768	有	Pa	Pb	Pc	P
6	无功功率 Q	Q =Rx×PT×CT×0.4	-32768～32768	有	Qa	Qb	Qc	Q
7	视在功率 S	S = Rx×PT×CT×0.2	0～65535	无	Sa	Sb	Sc	S
8	电能 Wh	Wh = Rx×PT×CT	0～10^9	无	+Wh	-Wh	+Varh	-Varh