

Modbus 通讯协议

1.1 通信地址表

MODBUS-RTU 通讯地址信息表 (03 04 读 10 为写 万能地址为 00)						
地址 (Hex)	数据内容	数据格式	数据长度 (word)	单位	读/写 R/ W	说明
0x100	A 相电压	Int32	2	0.1V	R	Ua (举例说明: Addr 04 01 00 00 02 CRC0 CRC1)
0x102	B 相电压	Int32	2	0.1V	R	Ub
0x104	C 相电压	Int32	2	0.1V	R	Uc
0x106	A 相电流	Int32	2	0.001A	R	Ia
0x108	B 相电流	Int32	2	0.001A	R	Ib
0x10A	C 相电流	Int32	2	0.001A	R	Ic
0x10C	空					
0x10E	总有功功率	Int32	2	0.1W	R	ΣP
0x110	A 相有功功率	Int32	2	0.1W	R	Pa
0x112	B 相有功功率	Int32	2	0.1W	R	Pb
0x114	C 相有功功率	Int32	2	0.1W	R	Pc
0x116	总无功功率	Int32	2	0.1Var	R	ΣQ
0x118	A 相无功功率	Int32	2	0.1Var	R	Qa
0x11A	B 相无功功率	Int32	2	0.1Var	R	Qb
0x11C	C 相无功功率	Int32	2	0.1Var	R	Qc
0x11E	总视在功率	Int32	2	VA	R	ΣS
0x120	A 相视在功率	Int32	2	VA	R	Sa
0x122	B 相视在功率	Int32	2	VA	R	Sb
0x124	C 相视在功率	Int32	2	VA	R	Sc
0x126	总功率因数	Int32	2	0~1.000	R	cosQ S
0x128	A 相功率因数	Int32	2	0~1.000	R	cosQ A
0x12A	B 相功率因数	Int32	2	0~1.000	R	cosQ B
0x12C	C 相功率因数	Int32	2	0~1.000	R	cosQ C
0x12E	A 相线电压	Int32	2	0.1V	R	Uab
0x130	B 相线电压	Int32	2	0.1V	R	Ubc
0x132	C 相线电压	Int32	2	0.1V	R	Uca
0x134	A 相电压频率	Int32	2	0.01Hz	R	FRa
0x136	B 相电压频率	Int32	2	0.01Hz	R	FRb

0x138	C相电压频率	Int32	2	0.01Hz	R	FRb
电表设置参数(读)						
0x61	仪表通讯地址	UInt16	1		R	1-247
0x62	通信波特率	UInt16	1		R	0-600; 1-1200; 2-2400; 3-4800; 4-9600
0x63	通信数据格式	UInt16	1		R	数据格式 0-N. 8.1 1-0. 8. 1 2-E. 8. 1
0x64	拉合闸命令状态	UInt16	1		R	0x55 代表命令合闸, 0xAA 代表命令拉闸
0x65	电表类型	UInt16	1		R	0x00 代表单相表, 0x01 代表三相表
电表设置参数(写)						
0x61	仪表通讯地址	UInt16	1		W	1-247
0x62	通信波特率	UInt16	1		W	0-600; 1-1200; 2-2400; 3-4800; 4-9600
0x63	通信数据格式	UInt16	1		W	数据格式 0-N. 8.1 1-0. 8. 1 2-E. 8. 1
0x0010	拉合闸操作	XXXX	1		W	(数据域位: 0x5555 为合闸, 0xAAAA 为拉闸)
0x0020	电表清0	XXXX	1		W	(数据域位: 0x5555 代表清0)
时间和费率设置						
0x210	当前时间(秒、分、时、日、月、年)	ss. mm. hh. DD. . MM. YY	3		R/W	00 10 02 10 00 03 06 ss mm hh DD MM YY crc0 crc1(举例说明)
0x213	时区(时段表号、日、月)	NN. DD. MM	3		R/W	00 10 02 13 00 03 06 NN DD MM NN DD MM crc0 crc1(举例说明)
0x216	时段表1(费率号、分、时)	NN. mm. hh	12		R/W	00 10 02 16 00 0C 18 NN mm hh NN mm hh NN mm hh NN mm hh NN mm hh NN mm hh NN mm hh CRC0 CRC1(时段表1举例说明)
0x222	时段表2(费率号、分、时)	NN. mm. hh	12		R/W	00 10 02 22 00 0C 18 NN mm hh NN mm hh NN mm hh NN mm hh NN mm hh NN mm hh NN mm hh CRC0 CRC1(时段表2举例说明)
当前电能						
0x001D	当前总有功电能	UInt32	2	0.01Kwh	R	
0x001F	当前总尖有功电能	UInt32	2	0.01Kwh	R	
0x0021	当前总峰有功电能	UInt32	2	0.01Kwh	R	
0x0023	当前总平有功电能	UInt32	2	0.01Kwh	R	

0x0025	当前总谷有功电能	UInt32	2	0.01Kwh	R	
0x0027	当前正向总有功电能	UInt32	2	0.01Kwh	R	
0x0029	当前正向尖有功电能	UInt32	2	0.01Kwh	R	
0x002B	当前正向峰有功电能	UInt32	2	0.01Kwh	R	
0x002D	当前正向平有功电能	UInt32	2	0.01Kwh	R	
0x002F	当前正向谷有功电能	UInt32	2	0.01Kwh	R	
0x0031	当前反向总有功电能	UInt32	2	0.01Kwh	R	
0x0033	当前反向尖有功电能	UInt32	2	0.01Kwh	R	
0x0035	当前反向峰有功电能	UInt32	2	0.01Kwh	R	
0x0037	当前反向平有功电能	UInt32	2	0.01Kwh	R	
0x0039	当前反向谷有功电能	UInt32	2	0.01Kwh	R	
0x003B	当前总无功电能	UInt32	2	0.01Kvarh	R	
0x003D	当前尖无功电能	UInt32	2	0.01Kvarh	R	
0x003F	当前峰无功电能	UInt32	2	0.01Kvarh	R	
0x0041	当前平无功电能	UInt32	2	0.01Kvarh	R	
0x0043	当前谷无功电能	UInt32	2	0.01Kvarh	R	
0x0045	当前正向总无功电能	UInt32	2	0.01Kvarh	R	
0x0047	当前正向尖无功电能	UInt32	2	0.01Kvarh	R	
0x0049	当前正向峰无功电能	UInt32	2	0.01Kvarh	R	
0x004B	当前正向平无功电能	UInt32	2	0.01Kvarh	R	
0x004D	当前正向谷无功电能	UInt32	2	0.01Kvarh	R	
0x004F	当前反向总无功电能	UInt32	2	0.01Kvarh	R	
0x0051	当前反向尖无功电能	UInt32	2	0.01Kvarh	R	
0x0053	当前反向峰无功电能	UInt32	2	0.01Kvarh	R	
0x0057	当前反向平无功电能	UInt32	2	0.01Kvarh	R	
0x0059	当前反向谷无功电能	UInt32	2	0.01Kvarh	R	

1. 数据格式：单个寄存器占2个字节，高位在前，低位在后。

2. UInt8: 1个字节，无符号整数；UInt32: 4个字节，无符号整数；

UInt16: 2个字节，无符号整数；Int32: 4个字节，带符号整数；

3. SDT670 通讯中读出的数值均为二次值，取出后需乘以 CT 或 PT 互感器变比。

1.2 端口

1. 导轨表配置 2 线制半双工 RS485 通信接口，内嵌标准的 Modbus-RTU 通信协议；为保证通信质量请选用直径大于 0.5 mm² 的双芯屏蔽线；
2. 在同一条 RS485 总线上，最多可接 32 个设备；每只导轨表的通信地址必须设置为不同；
3. RS485 连接线应该远离高压线或高压环境，以防止辐射干扰，建议用手拉手的 T 型接法，避免用星型接法；
4. 导轨表的通信波特率可设置为 9600, 4800, 2400, 1200bps, 19200bps, 38400bps
默认为 9600bps
5. 上位机读取 RS485 端口间隔时间最好大于 500 毫秒，不能小于 300 毫秒。

1.3 协议

Modbus-RTU 协议在一根通讯线上采用主从应答方式的通讯连接方式。首先，主计算机的信号寻址到一台唯一地址的终端设备(从机)，然后，终端设备发出的应答信号以相反的方向传输给主机，即：在一根单独的通讯线上信号沿着相反的两个方向传输所有的通讯数据流(半双工的工作模式)。MODBUS 协议只允许在主机(PC, PLC 等)和终端设备之间通讯，而不允许独立的终端设备之间的数据交换，这样各终端设备不会在它们初始化时占据通讯线路，而仅限于响应到达本机的查询信号。

主机查询：查询消息帧包括设备地址、功能代码、数据信息码、校验码。地址码表明要选中的从机设备；功能代码告之被选中的从设备要执行何种功能，例如功能代码 03 或 04 是要求从设备读寄存器并返回它们的内容；数据段 包含了从设备要执行功能的任何附加信息，校验码用来检验一帧信息的正确性，从设备提供了一种验证消息内容 是否正确的方法，它采用 CRC16 的校准规则。

数据帧的结构,即报文格式：

通信地址	功能码	通信数据	CRC 校验
1 个字节	1 个字节	N 个字节	2 个字节

从机响应：如果从设备产生正常的回应，在回应消息中有从机地址码、功能代码、数据信息码和 CRC16 校验码。数据信息码则包括了从设备收集的数据：像寄存器值或状态。如果有错误发生，我们约定是从机不进行响应。功能代码：告诉了被寻址到的终端执行何种功能。下表列出仪表所支持的功能代码，以及它们的功能。

16 进制命令	功 能
03H/04H	读 1 个或多个寄存器
10H	写 1 个或多个寄存器

数据段：包含了终端执行特定功能所需要的数据或者终端响应查询时采集到的数据。这些数据的内容可能是数值、参考地址或者设置值。校验码：CRC16 占用两个字节，包含了一个 16 位的二进制值。CRC 值由传输设备计算出来，然后附加到数据帧 上，接收设备在接收数据时重新计算 CRC 值，然后与接收到的 CRC 域中的值进行比较，如果这两个值不相等，就 发生了错误。

生成一个 CRC16 的流程为：

- (1) 预置一个 16 位寄存器为 0FFFFH (全 1)，称之为 CRC 寄存器。
- (2) 把数据帧中的第一个字节的 8 位与 CRC 寄存器中的低字节进行异或运算，结果存回 CRC 寄存器。
- (3) 将 CRC 寄存器向右移一位，最高位填以 0，最低位移出并检测。
- (4) 如果最低位为 0：重复第三步（下一次移位）；如果最低位为 1：将 CRC 寄存器与一个预设的固定值 (0A001H) 进行异或运算。
- (5) 重复第三步和第四步直到 8 次移位。这样处理完了一个完整的八位。
- (6) 重复第 2 步到第 5 步来处理下一个八位，直到所有的字节处理结束。
- (7) 最终 CRC 寄存器的值就是 CRC16 的值。

通信举例

1. 读寄存器：读通信地址为 01 的导轨表的三相的电流：

上位机命令：

设备通信地址	功能码	起始寄存器偏置位	需读寄存器个数	CRC16
01H	03H	01H,06H	00H,06H	24H,35H

导轨表回复：

设备通信地址	功能码	返回字节数	数据	CRC16
01H	03H	0CH	00H 00H 27H,27H,00H 00H 27H,11H,00H 00H 27H,0AH	FDH,12H

$$IA=(27H \times 100H + 27H) / 100 = 100.23A$$

$$IB=(27H \times 100H + 11H) / 100 = 100.01A$$

$$IC=(27H \times 100H + 0AH) / 100 = 99.94A$$

2. 读寄存器：读通信地址为 11 的导轨表的 A 相的电压：

上位机命令：

设备通信地址	功能码	起始寄存器偏置位	需读寄存器个数	CRC16
0BH	03H	01H,00H	00H,02H	C5H,5DH

导轨表回复：

设备通信地址	功能码	返回字节数	数据	CRC16
0BH	03H	04H	00H 00H 55H,E6H	EEH,E9H

$$UA=(55H \times 100H + E6H) / 100 = 219.9V$$

2. 读寄存器：读通信地址为 01 的导轨表相的有功电能：

上位机命令：

设备通信地址	功能码	起始寄存器偏置位	需读寄存器个数	CRC16
01H	03H	00H,1DH	00H,02H	54H,0DH

导轨表 回复：

设备通信地址	功能码	返回字节数	数据	CRC16
01H	03H	04H	01H,02H,03H,04H	5BH,3CH

$$\text{有功电能} = (10000H \times (100H \times 01H + 02H) + (100H \times 03H + 04H)) / 100 = 169090.00 \text{ kWh}$$

常见问题

通讯问题

- 导轨表不回送数据

- (1) 检查导轨表的通讯设置，如通讯地址、波特率、数据格式等与上位机软件是否一致；
- (2) 当上位机发读命令时，观察 LCD 显示上有没有闪烁：如有闪烁，则电表接收到数据，同时回送了数据；如无闪烁，则电表没有接收上位机数据，或接收到错误数据；
- (3) 如果现场多台导轨表通讯都没有数据回送，请检测现场 RS485 通讯总线的连接是否正确、RS485 转换器或串口服务器是否正常工作；
- (4) 如果只有一台导轨表或者少数导轨表通讯异常，请断开这台导轨表的 RS485 的接线，用万用表测量其 RS485 的 A、B 直接的电压，是否有 DC4V~5V 的直流电压：如果有电压，基本排除电表硬件故障，请检查 RS485 总线；如果没有电压或电压低于 3V，则电表 RS485 接口已经损坏，请联系本公司售后服务部门；
- (5) 如果导轨表是单相供电，必须在 A 或 B 相，导轨表才能通讯。

- 导轨表回送数据不准确

请仔细阅读通讯地址表中关于数据存放地址和存放格式的说明，并确保按照相应的数据格式转换。

电参数测量不准确

- (1) 请确保正确的电压和电流信号连接到导轨表上，可使用万用表来测量输入电压，钳形表来测量输入电流；
- (2) 当外接电流互感器时，确保电流、电压接线相位一致；如不一致，将计量不准确；
- (3) 需要注意的是仪表显示的电量为一次值，如果表内设置的电压电流互感器的变比与实际使用互感器倍率不一致，将导致仪表电量显示不准确；
- (4) 接线网络可以按照现场实际接法修改，但设置菜单中接线方式的设置应与实际接线方式一致，否则也将导致错误的显示信息；
- (5) 导轨表测量的是真有效值，电压信号和电流信号会与万用表的测试值有偏差，这是正常现象，因为两种的测量方式不一样。

电能数值不准确

- (1) 电能累加是基于对功率的测量，先观测仪表的功率值与实际负荷是否相符；
- (2) 导轨表支持双向电能计量，在接线错误的情况下，当总有功功率为负，电能会累加到反向有功电能，正向有功电能不累加。
- (3) 在现场使用最多出现的问题是电流互感器进线和出线接反。
- (4) 相序接错也会引起仪表电能走字异常。

导轨表不亮

- (1) 导轨表电压范围必须在额定电压上下 1.2 倍以内：
* 超过规定范围的电压可能会损坏仪表，并且不能恢复。
* 低于规定范围的电压，电表将不亮，请在侧面铭牌上查看导轨表的电压等级；
- (2) 外接互感器时，必须接电压信号线，导轨表才能工作。