

Modbus-RTU 通信协议说明

一. Modbus 协议简介

Modbus 协议定义了一个控制器能认识使用的消息结构,而不管它们是通过何种网络进行通信的,它制定了消息域的格局和内容的公共格式,描述了一个控制器请求访问其它设备的过程,回应来自其它设备的请求,以及如何侦测并记录错误信息。

通过此协议,控制器相互之间、控制器经由网络(例如以太网)和其它设备之间可以完成信息和数据的交换与传送,使各种不同的公司和厂家的可编程顺序控制器(PLC)、RTU、SCADA 系统、DCS 或与兼容 Modbus 协议的第三方设备之间可以连成工业网络,构建各种复杂的监控系统,并利于系统的维护和扩展,这个通讯协议已广泛被国内外电力行业及工控行业作为系统集成的一种通用工业标准协议。

ModScan32 是美国 Win-Tech 公司开发的 Modbus 协议通信 Master 端的检测软件。

WB 系列智能传感器采用 Modbus-RTU 通讯规约,支持组态王、Intouch、FIX、synall 等流行软件,能与 AB、西门子、施耐德、GE 等多个国际著名品牌的设备及系统之间实现数据通信,特别适用于电力系统综合自动化,智能电力电子设备,智能楼宇,工业自动化等领域,是构建、扩建 DCS 系统或制造智能电力电子设备的理想功能部件。

WB 系列智能传感器采用电磁隔离原理、专业 MCU 控制器,自动完成电压、电流、频率、有功功率、无功功率、功率因数、有功电能、无功电能,谐波等综合电参数检测和计算功能,并以 RS-485 接口总线输出数据,可直接与符合 Modbus(RTU)协议的 RS-485 接口总线连接,成为系统的一个功能部件。

二. Modbus-RTU 协议说明

WB 系列智能传感器实现 Modbus 通信协议时,遵循 Modbus 通信过程,采用了 Modbus-RTU 协议的命令子集,使用了[读保持寄存器\(功能码 0x03\)](#)、[预置单个或多个寄存器\(功能码 0x10\)](#)、[强制单个线圈\(功能码 0x05\)](#)等功能代码。具体情况详见产品说明书。

1. 数据传输方式

WB 智能传感器型号中的通讯校验方式代码说明如表 2.1。

表 2.1: WB 智能传感器通讯校验方式代码说明

通讯校验方式	通讯校验方式	起始位	数据位	校验位	停止位	总位数
无校验, 2 个停止位	B0	1 位	8 位	无校验	2 位	11 位
奇校验, 1 个停止位	B1	1 位	8 位	奇校验	1 位	11 位
偶校验, 1 个停止位	B2	1 位	8 位	偶校验	1 位	11 位
无校验, 1 个停止位	B3	1 位	8 位	无校验	1 位	10 位

如表 2.1 所示, 通讯时 1 个字节 B0、B1、B2 都是 11 位, 只有 B3 为 10 位。如果通讯的波特率是 9600,

则 1 个字节通讯需要的时间： $11 \times 1000 / 9600 \approx 1.15 \text{ ms}$ ($10 \times 1000 / 9600 \approx 1.04 \text{ ms}$)。如果要求采集系统时间响应快的话，建议用户一次读的数据不易过多。

公司传感器出厂默认：通讯产品地址为 1，波特率 9600bps，无校验，1 个停止位。

2. 数据传输速率

通过传感器上的拨码开关或者没有拨码开关的可以通过通讯设置，可设置为 19200BPS、9600BPS、4800BPS、2400BPS，缺省波特率为 9600BPS，设置后将传感器重新加电复位后方可生效。

3. 地址

3.1 传感器有拨码开关的产品地址设置（例如：WB6830R2-P）

1~64，用户可通过传感器上的拨码开关随时进行设置。具体详见说明书。

3.2 传感器没有拨码开关产品地址设置

1~247 用户可通过上位机发通讯命令进行设置。

4. 功能码说明

功能码告诉了被寻址到的终端执行何种功能。下表列出智能传感器所支持的功能码，以及它们的意义和功能。

代码	意义	行为
0x03	读取数据寄存器	获得当前传感器内部一个或者多个寄存器值
0x05	强制单个线圈	强制单个线圈为ON或OFF状态
0x10	预置单个或多个寄存器	将指定数值写入传感器内部一个或多个寄存器内

数据码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。例如：功能域码告诉终端读取一个寄存器，数据域则需要指明从哪个寄存器开始及读取多少个数据，而从机数据码回送内容则包含了数据长度和相应的数据。

校验码错误校验（CRC）域占用两个字节，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CRC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。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。

4、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。

5、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。

6、最终CRC 寄存器的值就是CRC的值。

5. 异常响应

当模块检测到了除 CRC 校验码出错以外的其它错误时，将向主机回送信息，功能码的最高位置为 1，即从机返送给主机的功能码是在主机发送的功能码的基础上加 128。从机返回的错误信息帧格式如下：

地址码	功能码(最高位为 1)	错误码	CRC 校验码低字节	CRC 校验码高字节
1 字节	1 字节	1 字节	1 字节	1 字节

错误码如下：

01H	非法的功能码	接收到的功能码传感器不支持
02H	非法的寄存器地址	接收到的寄存器地址超出传感器的寄存器地址范围
03H	非法的数据值	接收到的数据值超出相应地址的数据范围

6. 通讯报文举例说明

6.1 读保持寄存器（功能码 0x03）

由主站机发送读寄存器的包裹请求，装置响应所有有效的寄存器（在起始寄存器和终止寄存器之间）。报文格式如下：

读寄存器包裹格式（主机→装置）		响应格式（装置→主机）	
从站地址	1 字节	从站地址	1 字节
功能码 03H	1 字节	功能码 03H	1 字节
开始地址	2 字节	字节数(2*寄存器数目)	1 字节
寄存器个数	2 字节	第一个寄存器数据	2 字节
CRC 校验码	2 字节	第二个寄存器数据	2 字节
	
		CRC 校验码	2 字节

6.2 强制单个线圈（功能码 0x05）（继电器控制）

控制继电器格式（主机→装置）		响应格式（装置→主机）	
从站地址	1 字节	从站地址	1 字节
功能码 05H	1 字节	功能码 05H	1 字节
通道地址	2 字节	通道地址	2 字节
控制指令	2 字节	控制指令	2 字节
CRC 校验码	2 字节	CRC 校验码	2 字节

6.3 预置单个或多个寄存器（功能码0x10）

该命令允许主站配置装置工作参数，以下为数据格式：

写寄存器包裹格式（主机→装置）			响应格式（装置→主机）	
从站地址	1 字节		从站地址	1 字节
功能码 10H	1 字节		功能码 10H	1 字节
开始地址	2 字节		开始地址	2 字节
寄存器个数	2 字节		寄存器个数	2 字节
字节个数（2*寄存器个数）	1 字节		CRC 校验码	2 字节
第一个寄存器数据	2 字节			
.....			
CRC 校验码	2 字节			

7. 产品通讯举例说明：

7.1 功能码 0x03 举例

表 7.1 WB6830R2-P 实时测量数据寄存器表

序号	寄存器	名字	数据类型	计算因子	说明
...
34	0x0022	有功总功率	INT16	10	单位：瓦特
35	0x0023	A 相有功功率	INT16	10	单位：瓦特
36	0x0024	B 相有功功率	INT16	10	单位：瓦特
37	0x0025	C 相有功功率	INT16	10	单位：瓦特
38	0x0026	无功总功率	INT16	10	单位：乏
39	0x0027	A 相无功功率	INT16	10	单位：乏
40	0x0028	B 相无功功率	INT16	10	单位：乏
41	0x0029	C 相无功功率	INT16	10	单位：乏
42	0x002A	视在总功率	UINT16	10	单位：伏安
43	0x002B	A 相视在功率	UINT16	10	单位：伏安
44	0x002C	B 相视在功率	UINT16	10	单位：伏安
45	0x002D	C 相视在功率	UINT16	10	单位：伏安
46	0x002E	总功率因数	INT16	0.001	
47	0x002F	A 相功率因数	INT16	0.001	
48	0x0030	B 相功率因数	INT16	0.001	

49	0x0031	C 相功率因数	INT16	0.001	
50	0x0032	频率	UINT16	0.01	单位：赫兹
51	0x0033	A 相电压	UINT16	0.1	单位：伏特
52	0x0034	B 相电压	UINT16	0.1	单位：伏特
53	0x0035	C 相电压	UINT16	0.1	单位：伏特
54	0x0036	A 相电流	UINT16	0.01	单位：安培
55	0x0037	B 相电流	UINT16	0.01	单位：安培
56	0x0038	C 相电流	UINT16	0.01	单位：安培

读取表 7.1 中 序号 34~56 的参数命令如下，

发送通讯数据如下：01 03 00 22 00 17 A5 CE。

发送数据解析如下：01（产品地址）03（功能码）00 22（寄存器起始地址）00 17（寄存器个数）A5 CE（CRC16 校验）。

由于数值范围的限制，产品的很多数据寄存器都采用了计算因子，这就意味着用户如果要得到真实值，还必须乘上对应的计算因子方可。

例如：频率寄存器的计算因子为 0.01, 此时用户读取的数值为 5000, 则说明当前频率为：5000×0.01 = 50Hz.

7.2 功能码 0x10 举例

表 7.2 WB6830R2-P 配置数据寄存器表

序号	寄存器	名字	数据类型	说明	默认设置
...
18	0x0111	接线模式	UINT16	0: 三相四线, 1: 三相三线, 2: 单相	0
19	0x0112	电压变比 PT	UINT16	范围: 1-5000	1
20	0x0113	电流变比 CT	UINT16	范围: 1-9999	1
...

例如：设置接线模式为三相三线，PT 为 1，CT 为 20，产品地址为 1.

发送通讯数据如下：01 10 01 11 00 03 06 00 01 00 01 00 14 DE 23。

发送数据解析如下：01（产品地址）10（命令码）01 11（寄存器起始地址）00 03（寄存器个数）06（数据字节数）00 01（接线模式）00 01（PT）00 14(CT) DE 23(CRC16 校验)

7.3 功能码 0x05 举例

功能码 0x05 控制指令：0xFF00 控制继电器闭合，0x0000 控制继电器释放。

控制 WB5110-D 多功能谐波仪表 继电器通道 1 输出高电平。发送通讯数据如下：01 05 00 00 FF 00 8C 3A.

发送数据解析如下：01（产品地址）05（功能码）00 00（通道地址）FF 00（控制码）8C 3A(CRC16 校验)。

控制 WB5110-D 多功能谐波仪表 继电器通道 2 输出低电平。发送通讯数据如下：01 05 00 01 00 00 9C 0A。

发送数据解析如下：01（产品地址）05（功能码）00 01（通道地址）00 00（控制码）9C 0A(CRC16 校验)。