C20 三相电力监控智能仪表

Modbus 通讯规约
V1.2

深圳市康必达控制技术有限公司

目　录

1.引言

1.1 范围

本规约适用于我公司生产的 C20 三相电力监控仪表。

本规约是表述串行链路上的 Modbus-RTU 协议。

1.2 协议概述

Modbus 串行链路协议是一个主/从协议。

本规约旨在规定终端设备（C20 三相电表）与总线接口（通讯管理机）之间的数据交换以 Modbus 的 RTU（Remote Terminal Unit）模式进行。

采用异步主从半双工方式通讯。总线接口单元（通讯管理机）始终作为主站，终端设备（C20）作为从站进行工作。

2 物理层

2.1 传输接口

RS-485。

2.2 通讯地址

1~254(从站)。

2.3 通讯波特率

2400bps，4800bps，9600bps，19200bps。

2.4 通讯介质

屏蔽双绞线。

3 数据链路层

3.1 Modbus 主站/从站协议原理

Modbus 串行链路协议是一个主-从协议。 在同一时刻，只有一个主节点连接于总线，一个或多个子节点 (最大编号为 254) 连接于同一个串行总线。Modbus 通信总是由主节点发起。子节点在没有收到来自主节点的请求时，从不会发送数据。子节点之间从不会互相通信。主节点在同一时刻只会发起一个 Modbus 事务处理。

主节点以两种模式对子节点发出 Modbus 请求:

(1)在单播模式，主节点以特定地址访问某个子节点，子节点接到并处理完请求后，子节点向主节点返回一个报文(一个‘应答’)。在这种模式，一个 Modbus 事务处理包含 2 个报文： 一个来自主节点的请求， 一个来自子节点的应答。

每个子节点必须有唯一的地址 (1 到 254)，这样才能区别于其它节点被独立的寻址。

（2）在广播模式，主节点向所有的子节点发送请求。对于主节点广播的请求没有应答返回。 广播只用来校时。所有设备必须接受广播模式的写功能。地址 FF 是专门用于表示广播校时的。

3.2 字节(11 位)的格式

MODBUS 协议可以采用ASCII 或者RTU 模式传送数据,C20 仅支持RTU模式,8 位数据位,无校验位,1 位停止位。信息传输为异步方式，并以字节为单位。在主站和从站之间传递的通讯信息是10位的字格式:

表3 字格式

字格式（串行数据）	10位二进制
起始位	1位
数据位	8位
奇偶校验位	无
停止位	1

3.3 Modbus 帧描述

通讯数据（信息帧）格式

数据格式:	地址码	功能码	数据区	错误校检
对应数据长度:	1字节	1字节	N字节	16位CRC码（冗余循环码）

主站请求帧结束到从站响应帧开始之间的时间,最小为20 毫秒,最大为250 毫秒,典型值为60 毫秒

从站响应帧结束到主站下一请求帧开始之间的时间,在16 位模式下典型值为 100 毫秒,在 32 位模式下典型值为 500 毫秒

数据长度不定，但最长为 255 个字节。数据域是主站和子站以读写寄存器的方式来进行数据交换的

3.3.1 地址（Address）域

Modbus 寻址空间有 255 个不同地址。

FF	1 ~ 254
广播地址	子节点单独地址

所有的子节点必须识别广播地址。Modbus 总线接口单元没有地址，只有子节点必须有一个地址。该地址必须在 Modbus 串行总线上唯一。

地址域在数据包的开头部分，有一个 8bits 的数据组成。当主站发送数据包后，只有与主站查询地址相同的终端设备（从站）才会有响应。

3.3.2 功能(Function)码

功能码是每次通讯信息帧传送的第二个字节。作为主机请求发送，通过功能码告诉从机应执行什么动作。作为从机响应，从机返回的功能码与从主机发送来的功能码一样，并表明从机已响应主机并且已进行相关的操作。

功能码	定　义	操　作（二进制）
01H	读开关量输出	读取一路或多路开关量输出状态数据
02H	读开关量输入	读取一路或多路开关量状态输入数据
03H	读寄存器数据	读取一个或多个寄存器的数据（读 SOE、定值）
04H	读寄存器数据	读取一个或多个寄存器的数据（读 SOE、定值）
05H	写开关量输出	控制一路继电器“合/分”输出
06H	写单个寄存器	把一组二进制数据写入单个寄存器
10H	写多个寄存器	校时、修改定值

3.3.3 数据(Data) 域

数据域包括需要由从机返送何种信息或执行什么动作。这些信息可以是数据（如：开关量输入/输出、模拟量输入/输出、寄存器等等）、参考地址等。数据区的数据一般是两个字节，并且高字节在前，低字节在后；对于多字节数据，高位字在前，低位字在后。

3.3.4 校验（CRC）域

主机或从机可用校验码进行判别接收信息是否正确。由于电子噪声或一些其它干扰，信息在传输过程中有时会发生错误，错误校验码（CRC）可以检验主机或从机在通讯数据传送过程中的信息是否有误，错误的数据可以放弃（无论是发送还是接收），这样增加了系统的安全和效率。

通讯协议的 CRC（冗余循环码）包含 2 个字节，低位字节在前，高位字节在后。CRC 码由发送设备（主机）计算，放置于发送信息帧的尾部。接收信息的设备（从机）再重新计算接收到信息的 CRC，比较计算得到的 CRC 是否与接收到的相符，如果两者不相符，则表明出错。

在进行 CRC 计算时只用 8 个数据位，起始位及停止位，偶校验位，都不参与 CRC 计算。

3.3.5 CRC 校验方法

（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；

（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；

（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）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；

（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，进行通讯信息帧下一个字节的处理；

（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；

（8）最后得到的 CRC 寄存器内容即为：CRC 码。

4 C20 MODBUS-RTU 功能码及地址表

4.1 功能码“01H”、“02H”：读开入和开出状态

遥信下传：

定义	地址（1 字节）	功能码(1 字节)	寄存器起始地址（2 字节）	寄存器个数（2 字节）	CRC 校验（2 字节）
报文举例	01	01\02	00 01	00 02	CRCL CRCH

遥信正常返回：

定义	地址（1 字节）	功能码（1 字节）	数据长度（1 字节）	返回数据（数据长度）	CRC 校验（2 字节）
报文举例	01	01\02	01	00	CRCL CRCH

（ 注：“数据长度”指实际返回的字节个数，正常返回时，“数据长度”= 01）

4.2 功能码“03H”、“04H”、：读寄存器

4.2.1 定值

下传：

定义	地址（1 字节）	功能码(1 字节)	寄存器起始地址（2 字节）	寄存器个数（2 字节）	CRC 校验（2 字节）
报文举例	01	03\04	0B B9	00 02	CRCL CRCH

正常返回：

定义	地址（1 字节）	功能码（1 字节）	数据长度（1 字节）	返回数据（数据长度）	CRC 校验（2 字节）
报文举例	01	03\04	04	00 00 00 00	CRCL CRCH

（ 注：“数据长度”指实际返回的字节个数，正常时返回时，“数据长度”=寄存器个数*2）

4.2.2 事件的读取

先用“03\04”功能码读取新事件起始地址（8001）和个数（8002），通过返回值判断是否有新事件发生，有就读取事件寄存器，没有就轮询下个命令。

报文举例：

下发：01 03 1F 41 00 02 CRCL CRCH

无事件时返回：01 03 04 00 00 00 00 CRCL CRCH

有事件时返回：01 03 04 1F 4B(新事件起始地址) 00 01 (新事件个数)CRCL CRCH（有 1 个

新事件，新事件起始地址是 0x1F4B）

有事件接着下发：01 03 1F 4B 00 05 CRCL CRCH（1 个事件占 5 个寄存器 10 字节）

返回：01 03 0A 11(事件代号) 01 (事件值)0B 0C 0E 0E 10 23 01 25 CRCL CRCH（DI1 合 2011.12.14 14:16:35.293）

事件结构参见 5.寄存器表下面的事件结构说明。

4.3 功能码“05H”、“06H”：遥控

遥控下传：

定义	地址（1 字节）	功能码(1 字节）	寄存器起始地址（2 字节）	写入的值（2 字节）	CRC 校验（2 字节）
报文举例	01	05\06	03 E9	FF 00	CRCL CRCH

遥控正常返回：

定义	地址（1 字节）	功能码（1 字节）	寄存器起始地址（2 字节）	写入的值（2 字节）	CRC 校验（2 字节）
报文举例	01	05\06	03 E9	FF 00	CRCL CRCH

(注：遥控命令：0xFF00 为合，0x0000 为分)

在一个远程设备上，使用该功能码写单个输出为 ON 或 OFF。请求数据域中的常量说明请求的 ON/OFF 状态。十六进制值 FF 00 请求输出为 ON。十六进制值 00 00 请求输出为 OFF。其它所有值均是非法的，并且对输出不起作用,注：DO 在报警模式操作无效。。

4.4 功能码“10H”：校时、修改定值

4.4.1 校时

下发：

01(设备地址) 10 1D 4D 00 06 0C 00 0C(年) 00 04(月) 00 19(日) 00 0E(时) 00 0B(分) 00 20(秒) CRCL CRCH

上送：

01 10 1D 4D 00 06 CRCL CRCH

广播校时：

下发：

FF(广播地址) 10 1D 4D 00 06 0C 00 0C(年) 00 04(月) 00 19(日) 00 0E(时) 00 0B(分) 00 20(秒) CRCL CRCH

注：校时的起始地址必须为 7501(0x1D4D)，长度必须为 6。地址和长度不对时，校时是不会成功的。

4.4.2 修改定值

功能码 10 也能修改定值，但只能连续修改定值。

修改定值：

修改定值下发报文格式：

装置地址	
功能码 10H	
寄存器起始地址 H	
寄存器起始地址 L	
寄存器个数(n+1)H	
寄存器个数(n+1)L	
字节个数（修改定值个数 n*2+2）	
修改定值密码 ABH	
修改定值密码 BAH	
参数 1(H)	定值 1
参数 1(L)	
……	
参数 n(H)	定值 n
参数 n(L)	
CRC 校验码（L）	
CRC 校验码（H）	

寄存器个数=需要修改定值的寄存器个数+1，有 1 个寄存器（2 个字节）是密码。

修改定值装置上送报文格式：

设备地址
功能码 10H
寄存器起始地址 H
寄存器起始地址 L
寄存器个数(n+1)H
寄存器个数(n+1)L
CRC 校验码（L）
CRC 校验码（H）

报文举例：

下发：01 10 1B 5B 00 03 06 AB BA(密码) 00 05 00 0A CRCL CRCH（修改装置的 PT、CT 变比）

上送：01 10 1B 5B 00 03 CRCL CRCH

5 寄存器表

寄存器表（1 个寄存器占 2 个字节，高字节在前。32 位数据（2 寄存器）高字在前）：

以下地址全为 10 进制，发报文时请转换为 16 进制发送

地址	定义	数据类型	属性	寄存器个数	说明
开入量(01\02 读)					
0001	开入 1	bit	RO	1	0:分　　1:合
0002	开入 2	bit	RO	1	0:分　　1:合
开出（01 读 05\06 写）					
1001	开出 1	bit	RW	1	0:分　　1:合 注:作报警模式时写无效
1002	开出 2	bit	RW	1	0:分　　1:合 注:作报警模式时写无效
模拟量(03\04 读)　高字节在前					
3001	第一路电压 Ua	INT16U	RO	1	0-9999 单位 0.1V
3002	第二路电压 Ub	INT16U	RO	1	0-9999 单位 0.1V
3003	第三路电压 Uc	INT16U	RO	1	0-9999 单位 0.1V
3004	第一路电流 Ia	INT16U	RO	1	0-9999 单位 0.001A
3005	第二路电流 Ia	INT16U	RO	1	0-9999 单位 0.001A
3006	第三路电流 Ia	INT16U	RO	1	0-9999 单位 0.001A
3007	软件版本号	INT16U	RO	1	100 ~ 999　　缩小 100 倍
3008					
注：C20S 读取第三路电流寄存器值					
定值（03\04 读 10H 写）				**定值范围**	
7001	RS485 地址	INT16U	RW	1~254	
7002	RS485 波特率	INT16U	RW	0~3	0 = 2400, 1 = 4800, 2 = 9600, 3 = 19200。
7003	PT 变比	INT16U	RW	1~9999	
7004	CT 变比	INT16U	RW	1~9999	
7005	DI 滤波时间	INT16U	RW	1~9999	单位 1ms
7006	DO1 控制模式	INT16U	RW	0~1	0:表示作开关量 1:作报警输出
7007	DO1 脉冲宽度	INT16U	RW	0~9999	单位 1MS　　0:表示继电器工作在保持方式
7008	DO2 控制模式	INT16U	RW	0~1	0:作开关量　1: 作报警输出
7009	DO2 脉冲宽度	INT16U	RW	0~9999	单位 1MS　0:表示继电器工作在保持方式
7010	报警使能设置	INT16U	RW	BIT0 – BIT2	BIT0　= 0 禁止　= 1 高报警使能 BIT1　= 0 禁止　= 1 低报警使能

7011	高报警值设置	INT16U	RW	0000 ~ 9999	电压保留 1 位小数 电流保留 3 位小数
7012	低报警值设置	INT16U	RW	0000 ~ 9999	电压保留 1 位小数 电流保留 3 位小数
7013	RES	INT16U	RW		
7014	报警延时时间	INT16U	RW	0000 ~ 9999	分辨率：1s
7015	高报警输出	INT16U	RW	0 - 2	0 ：只报警不输出 1：继电器 1 2 :继电器 2
7016	低报警输出	INT16U	RW	0 – 2	0 ：只报警不输出 1:继电器 1 2: 继电器 2
7017	RES	INT16U	RW		
7018	设置 LCD 背光等级	INT16U	RW	1 - 8	
7019	用户密码	INT16U	RW	0 ~ 9999	默认： 8000
7020	清除 SOE 记录	INT16U	RW	0 ~ 1	1：清除 SOE 记录
7021					
7022	恢复出厂设置	INT16U	RW	0 - 1	1:恢复出厂设置
7023	电压或电流校表	INT16U	RO	0 - 1	1:电压或电流校表
7024	误差校正密码	INT16U	RO	密码 = 1234 才校正	
7025	第一路电压或电流校表高 2 个字节	INT16U	RO	4 个字节表示一个 float 型变量（浮点数）	
7026	第一路电压或电流校表低 2 个字节	INT16U	RO		
7027	第二路电压或电流校表高 2 个字节	INT16U	RO	4 个字节表示一个 float 型变量（浮点数）	
7028	第二路电压或电流校表低 2 个字节	INT16U	RO		
7029	第三路电压或电流校表高 2 个字节	INT16U	RO	4 个字节表示一个 float 型变量（浮点数）	
7030	第三路电压或电流校表	INTU	RO		

	低 2 个字节				
7031					
装置校时					
7501	装置时间年	INT16U	WO	0~99	校时参见 4.41
7502	装置时间月	INT16U	WO	1~12	
7503	装置时间日	INT16U	WO	1~31	
7504	装置时间时	INT16U	WO	0~23	
7505	装置时间分	INT16U	WO	0~59	
7506	装置时间秒	INT16U	WO	0~59	
事件(03\04 读)					
8001	新事件起始地址	INT16U	RO		读取事件参见 4.2.3
8002	新事件个数	INT16U	RO		
8011	事件 1	事件结构 F1	RO	事件区，必须先读新事件地址和个数，才能读到新事件	
…			RO		
…			RO		
…			RO		
…			RO		
8389	事件 64		RO		

注：RO 为只读，WO 为只写，RW 为读写均可。

注 1：以上数据（Ai）与实际值之间的对应关系为:

电压: U = （Ai / 10） * PT,Ai = 无符号整数，单位 V。

电流： I = （Ai / 1000） * CT,Ai = 无符号整数，单位 A。

报警参数设置	电压	电流	
高报警	AH = (Ai / 10)	AH = (Ai / 1000)	
低报警	AH = (Ai / 10)	AH = (Ai / 1000)	

一个事件记录 12 个字节，以事件记录结构的顺序上送。时间用 16 进制数表示。SOE 的结构如下：

事件结构 F1

字节顺序	字节长度	说明
0～1	2 字节	事件代号
2～3	2 字节	事件值
4	1 字节	年（0————99，实时值要加上 2000）
5	1 字节	月（1————12）
6	1 字节	日（1————31）
7	1 字节	时（0————23）
8	1 字节	分（0————59）
9	1 字节	秒（0————59）
10~11	2 字节	毫秒（0————999）（高位在前，低位在后）

事件表

事件代号	事件描述	事件值
17	DI1	0x00 分 0x01 合
18	DI2	0x00 分 0x01 合
09	DO1	0x10: 就地分
		0x11: 就地合
		0x00: 远方分
		0x01: 远方合
10	DO2	0x10: 就地分
		0x11: 就地合
		0x00: 远方分
		0x01: 远方合
32 (0x20)	第一路 A 电压高报警	单位 0.1V
33 (0x21)	第二路 B 电压高报警	
34 (0x22)	第三路 C 电压高报警	
35 (0x23)	第一路 A 电流高报警	单位 0.001A
36 (0x24)	第二路 B 电流高报警	
37 (0x25)	第三路 C 电流高报警	
41 (0x29)	第一路 A 电压低报警	单位 0.1V
42 (0x2A)	第二路 B 电压低报警	
43 (0x2B)	第三路 C 电压低报警	
44 (0x2C)	第一路 A 电流低报警	单位 0.001A
45 (0x2D)	第二路 B 电流低报警	
46 (0x2E)	第三路 C 电流低报警	

160	第一路 A 电压高报警返回	单位 0.1V
161	第二路 B 电压高报警返回	
162	第三路 C 电压高报警返回	
163	第一路 A 电流高报警返回	单位 0.001A
164	第二路 B 电流高报警返回	
165	第三路 C 电流高报警返回	
169	第一路 A 电压低报警返回	单位 0.1V
170	第二路 B 电压低报警返回	
171	第三路 C 电压低报警返回	
172	第一路 A 电流低报警返回	单位 0.001A
173	第二路 B 电流低报警返回	
174	第三路 C 电流低报警返回	

6 异常代码

在出问题的时候，有一系列定义过的异常代码被从站送回。
所有的异常通过添加0x80 到请求的功能代码来标记，跟随此字节的是一个单一的原因字节
如下例所示：
发送： 01 03 12 34 00 01 crcl crch
响应： 01 83 01 crcl crch
当索引0x1234 响应异常类型2-“非法的数据地址”时请求读1 寄存器
异常情况列举如下：

01 非法的功能码
对从站来说，在询问过程中收到的功能代码是不允许的行为。

02 非法的数据地址
对从站来说，在询问过程中收到的数据地址不是允许的地址。

03 非法的数据值或查询长度
对从站来说，在询问数据区段所包含的值是不允许的。查询的长度是不正确的。