RD 系列保护装置 MODBUS-RTU 通讯规约

1 引言

1.1 范围

本规约适用于我公司生产的 RD 系列微机保护装置。

1.2 协议概述

本规约是表述串行链路上的 Modbus 协议。

本规约规定保护装置与上位机之间的传输模式为 Modbus RTU 模式。

采用异步主从半双工方式通讯。上位机始终作为主站，保护装置始终作为从站。

2 物理层

2.1 传输接口：RS-485

2.2 接线方式：A 线、B 线、屏蔽地(屏蔽双绞线)

2.3 工作方式：异步半双工

2.3 从站地址：1～99

2.3 通讯波特率：1200bps，2400bps，4800bps，9600bps

2.4 通讯格式：1 位起始位、8 位数据位、无校验、1 位停止位

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 99) 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 99)，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。 广播请求一般用于写命令。所有设备必须接受广播模式的写功能。地址 0 是专门用于表示广播数据的。

3.2 Modbus 帧描述

地址域	功能码	数据域	校验域

两个报文之间的线路空闲间隔最少需 33 位。总线接口单元（上位机）等待单元报文的超时时间为 50ms，即总线接口单元在发送完需要单元应答的报文后，50ms 内还未接收到应答报文的第一个字节就认为是超时。有错误码，当从站检查出命令有误时作回答。

可以发送的最大报文长度为 178 字节。所以主站发送的命令，其对应的响应报文长度不要超过 178 字节。

3.2.1 地址（Address）域

Modbus 寻址空间有 256 个不同地址。

0	1 ～ 99	100～255
广播地址	子节点单独地址	保留

地址 0 保留为广播地址。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

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
03H	读寄存器数据	读取一个或多个寄存器的数据
04H	读保持寄存器	读取一个或多个寄存器的数据
05H	写开关量输出	控制一路继电器“合/分”输出
06H	写单路寄存器	把一组二进制数据写入单个寄存器
10H	写多路寄存器	把多组二进制数据写入多个寄存器

注：（1）功能码 10H 只用于广播校时。

（2）功能码 01H 报文中的起始地址必须为 8 的整倍数。

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，并且高位字节在前，低位字节在后；对于多字节数据，高位字在前，低位字在后。

3.3.4 校验（CRC）域

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。

4　Modbus 功能码及地址表

4.1 功能码“01H”和“05H”：“读 1 路或多路”和“写 1 路”开关量输出状态

（1）功能码01H。在一个远程设备中，使用该功能码读取开关量的1至128连续状态。地址,即指定的第一个开关量地址和编号。从零开始寻址开关量。因此寻址开关量1-16 为0-15。根据数据域的每个比特将响应报文中的开关量分成为一个开关量。指示状态为 1 = ON 和 0 = OFF。第一个数据字节的LSB（最低有效位）包括在询问中寻址的输出。其它开关量依次类推，一直到这个字节的高位端为止，并在后续字节中从低位到高位的顺序。

请求			响应		
地址	1个字节	1～99	地址	1个字节	1～99
功能码	1个字节	01H	功能码	1个字节	01H
起始地址	2个字节	0000～0126	字节数	1个字节	N/8
开关量数量	2个字节	N	开关量状态	n个字节	n=N/8

校验	2个字节	CRC	校验	2个字节	CRC

（2）功能码05H。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。从零开始寻址开关量。因此，寻址开关量1为0。

请求			响应		
地址	1个字节	1～99	地址	1个字节	1～99
功能码	1个字节	05H	功能码	1个字节	05H
输出地址	2个字节	0000～0007	输出地址	2个字节	0000～0007
输出值	2个字节	0x0000或0xff00	输出值	2个字节	0x0000或0xff00
校验	2个字节	CRC	校验	2个字节	CRC

4.2 功能码“03H”、“04H”、“06H”、“10H”：读/写寄存器

（1）功能码03H。在一个远程设备中，使用该功能码读取保持寄存器连续块的内容。请求说明了起始寄存器地址和寄存器数量。从零开始寻址寄存器。因此，寻址寄存器1-16 为0-15。将响应报文中的寄存器数据分成每个寄存器有两字节，在每个字节中直接地调整二进制内容。对于每个寄存器，第一个字节包括高位比特，并且第二个字节包括低位比特。

请求			响应		
地址	1个字节	1～99	地址	1个字节	1～99
功能码	1个字节	03H	功能码	1个字节	03H
起始地址	2个字节	0000～0100	字节数	1个字节	寄存器数量×2
寄存器数量	2个字节	0000～0100	寄存器值	N个字节	寄存器值
校验	2个字节	CRC	校验	2个字节	CRC

（2）功能码04H。在一个远程设备中，使用该功能码读取输入寄存器连续块的内容。请求说明了起始寄存器地址和寄存器数量。从零开始寻址寄存器。因此，寻址寄存器1-16 为0-15。将响应报文中的寄存器数据分成每个寄存器有两字节，在每个字节中直接地调整二进制内容。对于每个寄存器，第一个字节包括高位比特，并且第二个字节包括低位比特。

请求			响应		
地址	1个字节	1～99	地址	1个字节	1～99
功能码	1个字节	03H	功能码	1个字节	03H
起始地址	2个字节	0000～0100	字节数	1个字节	寄存器数量×2
寄存器数量	2个字节	0000～0100	寄存器值	N个字节	寄存器值
校验	2个字节	CRC	校验	2个字节	CRC

（3）功能码06H。在一个远程设备中，使用该功能码写单个保持寄存器。请求说明了被写入寄存器的地址。信号复归从第99寄存器。

请求			响应		
地址	1个字节	1～99	地址	1个字节	1～99
功能码	1个字节	06H	功能码	1个字节	06H
寄存器地址	2个字节	0063	寄存器地址	2个字节	0063
寄存器值	2个字节	0x8000	寄存器值	2个字节	0x8000
校验	2个字节	CRC	校验	2个字节	CRC

（4）功能码10H。在一个远程设备中，使用该功能码写连续5个寄存器块在请求数据域

中说明了请求写入的值。每个寄存器将数据分成两字节。

请求			响应		
地址	1个字节	0	地址	1个字节	0
功能码	1个字节	10H	功能码	1个字节	10H
起始地址	2个字节	0064	起始地址	2个字节	0064
寄存器数量	2个字节	0005	寄存器数量	2个字节	0005
寄存器字节数	1个字节	10	检验	2个字节	CRC
寄存器内容	10个字节	寄存器值			
校验	2个字节	CRC			

4.3MODBUS 异常码：

MODBUS异常码		
代码	名称	含义
0X01	非法功能码	接收到的功能码从机不支持
0X02	非法数据地址	指定的数据地址超出从机范围
0X03	非法数量值	接收到主机发送的数据超出从机相应地址范围