

REJ-600、GC-820通用型 微机保护装置

Modbus串行通信协议

(V1.01)-2019

惠州高驰科技有限公司

电 话：13809668007

邮 箱：302179774@qq.com

地 址：惠州市惠城区水口镇龙湖九路 28 号

网 址：<http://www.hzgcth.com>

目 录

1	简介	3
1.1	1.1 通讯协议的目的	3
2	MODBUS 串行通信协议详细说明	3
2.1	2.1 MODBUS 协议基本规则	3
2.2	2.2 传送模式	3
2.3	2.3 MODBUS 数据包结构描述	3
2.3.1	2.3.1 地址域	3
2.3.2	2.3.2 功能码域	3
2.3.3	2.3.3 数据域	4
2.3.4	2.3.4 校验域	4
2.5	2.5 广播命令	4
3	通信数据包	4
3.1	3.1 读取寄存器（功能码 0x03）	4
3.1.1	3.1.1 下行报文，如表 3-1	4
3.1.2	3.1.2 上行报文，如表 3-2	4
3.2	3.2 读取事件（功能码 0x03）	5
3.2.1	3.2.1 查询 SOE 事件	5
1	1 下行报文	5
2	2 上行报文	5
3.3	3.3 写单个线圈（功能码 0x05）	6
3.3.1	3.3.1 下行报文，如表 3-7	6
3.3.2	3.3.2 上行报文，如表 3-8	6
3.4	3.4 数据类型	6
4	寄存器列表	6
4.1	4.1 实时数据寄存器	6
4.2	4.2 事件查询寄存器表	7
4.3	4.3 时间寄存器	9
4.4	4.4 事件查询寄存器表	9
4.5	4.5 遥控寄存器表	9

1 简介

通信协议详细地描述了REJ-600、GC-820在MODBUS通讯模式下如何进行信息交换和数据传送，以便第三方使用和开发。

1.1 通讯协议的目的

通信协议的作用使信息和数据在上位机主站和子站之间有效地传递，它包括：

- (1) 允许主站访问和设定所有子站的全部设置参数；
- (2) 允许主站访问子站的所有测量数据。

2 MODBUS串行通信协议详细说明

2.1 MODBUS协议基本规则

MODBUS协议广泛用于RS-485通信网中，一个RS-485通信网可支持多个子站：

- 1) 所有通信应遵照主/从方式。在这种方式下，信息和数据在单个MODBUS主站和最多32个子站监控设备之间传递；
- 2) 主站将初始化和控制所有在RS485通信回路上传递的信息；
- 3) 子站不能发起通信；
- 4) 所有信息以“数据包”形式进行传递，数据包由一串字节组成（每个字节8位）。一个数据包中最多可含255个字节。
- 5) 主站发送数据包称为请求，子站发送数据包称为响应；
- 6) 任何时候只能有一个子站响应主站一个请求。

2.2 传送模式

MODBUS协议包括ASCII和RTU两种模式。本协议采用MODBUS-RTU模式，数据位：8位；校验方式：偶校验，无校验，奇校验，默认设置无校验；在奇、偶校验情况下，数据按照1位启动位、8位数据位、1位校验位、1位停止位传送，无校验时按照1位启动位、8位数据位、2位停止位进行传送。

2.3 MODBUS 数据包结构描述

每个MODBUS 数据包都由以下几个部分组成：

- 1) 地址域
- 2) 功能码域
- 3) 数据域
- 4) 校验域

2.3.1 地址域

MODBUS的子站地址域长度为一个字节，有效的子站地址范围从1~247。子站如果接收到数据包中的地址域与自身地址相符合，应当执行数据包中所包含的命令。子站所响应的数据包中包含同样的地址域。

2.3.2 功能码域

MODBUS包裹中功能码域长度为一个字节，用以通知子站应当执行何操作。子站响应数据包裹中应当包含相同的功能码字节。有关装置的功能码参照下表：

表2-1 功能码

功能码	含义	功能描述
0x03	读取多个寄存器	获得子站内部一个或多个寄存器值
0x10	设置多个寄存器	将指定值写入子站内一个或多个寄存器内
0x06	写单个寄存器	专用于遥控继电器、信号复归、事件确认

2.3.3 数据域

MODBUS 数据域长度不定，依据其具体功能而定。MODBUS 数据域采用“BIG INDIAN”模式，即是高位字节在前，低位字节在后。举例如下：

例如：某 16 位寄存器的数值为 0x12AB，则数值发送顺序为

高位字节= 0x12

低位字节= 0xAB

2.3.4 校验域

MODBUS-RTU模式采用16位CRC校验，发生器多项式为 $(X_{16}+X_{15}+X_2+1)$ 。发送设备应当对数据包中的每一个数据都进行CRC16计算，最后结果存放入检验域中。接收设备也应当对数据包中的每一个数据（除校验域以外）进行CRC16计算，将结果与校验域进行比较。只有相同的数据包才可以被接受。具体的CRC校验算法可参照附录。

2.5 广播命令

地址域为 00H 时认为是广播命令，只在10H功能码时有效。广播命令时，子站只接收数据包，不响应，这是为了防止网络内的子站同时响应时堵塞网络。广播命令只用于广播对时。

3 通信数据包

3.1 读取寄存器（功能码 0x03）

3.1.1 下行报文，如表3-1

表 3-1

子站地址	1 个字节
功能码	1 个字节
起始寄存器地址	2 个字节
寄存器个数 n	2 个字节
CRC 校验码	2 个字节

3.1.2 上行报文，如表3-2

表 3-2

子站地址	1 个字节
功能码	1 个字节
字节个数 (寄存器个数 n×2)	1 个字节
第一个寄存器数据	2 个字节
第二个寄存器数据	2 个字节
.....
第 n 个寄存器数据	2 个字节
CRC 校验码	2 个字节

注：1) 读取保留寄存器时，返回值为 0；
2) 最多读取 125 个寄存器。

3.2 读取事件 (功能码 0x03)

功能码：03 起始地址：0x0500 长度：0x32 事件码高位 事件码低位 事件记录位号 事件值
事件确认码 年高 年低 月 日 时 分 ms高 ms低

从机装置中有一个能存放255 条事件信息的保护事件缓冲区。

主机收到该标志后就可进行事件查询来获取这些事件信息，1 次查询只能获取到1 条事件信息。

主机可根据功能需要决定是否要读取事件信息。若主机不读取事件信息，从机的255 条事件信息缓冲区存满后，若再有新事件产生，自动清除旧的事件信息以存放新事件。

每查询一次，可查询一个新事件，直到所有新事件都被查询完毕。

3.2.1 查询SOE事件

1 下行报文

子站地址	1 个字节
功能码 03h	1 个字节
起始寄存器地址 (0x500)	2 个字节
寄存器个数 (07h)	2 个字节
CRC 校验码	2 个字节

2 上行报文

子站地址	1 个字节
功能码 03h	1 个字节
字节个数 (10h)	1 个字节
第一个寄存器数据	2 个字节
第二个寄存器数据	2 个字节
.....
第 6 个寄存器数据	2 个字节
CRC 校验码	2 个字节

3.3 写单个线圈（功能码 0x05）

3.3.1 下行报文，如表3-7

表 3-7

子站地址	1 个字节
功能码 0x05	1 个字节
输出地址	2 个字节
输出值 0x0001/0x0002	2 个字节
CRC 校验码	2 个字节

3.3.2 上行报文，如表3-8

表 3-8

响应格式（子站→主站）	
子站地址	1 个字节
功能码 0x05	1 个字节
输出地址	2 个字节
输出值 0x0001/0x0002	2 个字节
CRC 校验码	2 个字节

注：1) 输出值只能是 0x0001 或 0x0002，其他所有值均是非法的。返回错误码 04 无效操作

3.4 数据类型

寄存器的数据有以下几种类型：

UINT16 数值范围：0~65535；

INT16 数值范围：-32768~32767；

UINT32 数值范围：0~4294967295；

INT32 数值范围：-2147483648~2147483647；

16 位数据占用 1 个寄存器，通信时先传送高位字节，再传送低位字节。32 位数据需要占用 2 个寄存器，通信时先传高位字，再传低位字。

4 寄存器列表

4.1 实时数据寄存器

寄存器地址	类型	描述	数据格式	单位/范围	备注
0x100	RO	合位开入	UINT16		
0X101	RO	跳位开入	UINT16		
0X102	RO	闭锁重合闸	UINT16		
0X103	RO	手动信号	UINT16		

0X104	RO	弹簧未储能	UINT16		
0X105	RO	远方	UINT16		
0X110	RO	UAB	UINT16	V	
0X111	RO	UBC	UINT16	V	
0X112	RO	UCA	UINT16	V	
0X113	RO	U0	UINT16	V	
0X114	RO	Ia	UINT16	V	
0X115	RO	Ib	UINT16	V	
0X116	RO	Ic	UINT16	V	
0X117	RO	3IO	UINT16	A	
0X118	RO	IA	UINT16	A	
0X119	RO	IB	UINT16	A	
0X11A	RO	IC	UINT16	A	
0X11B	RO	P	UINT16	A	
0X11C	RO	Q	UINT16	A	
0X11D	RO	COS	UINT16	A	
0X11E	RO	F	UINT16	W	

4.2 事件查询寄存器表

寄存器地址	类型	描述	数据格式	备注
0X160		合位开入	UINT16	
0X161		跳位开入	UINT16	
0X162		闭锁重合闸	UINT16	
0X163		手动信号	UINT16	
0X164		弹簧未储能	UINT16	
0X165		远方	UINT16	
0X166		事故总	UINT16	
0X167		告警总	UINT16	
0X168		RAM 错误	UINT16	
0X169		ROM 错误	UINT16	
0X16A		闪存错误	UINT16	
0X16B		EEPROM 错误	UINT16	
0X16C		实时时钟错误	UINT16	
0X16D		开出异常	UINT16	

0X16E		零漂越限	UINT16	
0X16F		无效定值区	UINT16	
0X170		定值校验错误	UINT16	
0X171		TV 断线	UINT16	
0X172		弹簧未储能告警	UINT16	
0X173		控制回路断线	UINT16	
0X174		控制回路异常	UINT16	
0X175		开关位置异常	UINT16	
0X176		跳位有流	UINT16	
0X177		单相接地告警	UINT16	
0X178		零序 II 段告警	UINT16	
0X179		过负荷告警	UINT16	
0X17A		跳闸失败	UINT16	
0X17B		启动	UINT16	
0X17C		过流 I 段动作	UINT16	
0X17D		过流 II 段动作	UINT16	
0X17E		过流 III 段动作	UINT16	
0X17F		过流加速段动作	UINT16	
0X180		过流反时限动作	UINT16	
0X181		零序 I 段动作	UINT16	
0X182		零序 II 段动作	UINT16	
0X183		零序加速段动作	UINT16	
0X184		过负荷动作	UINT16	
0X185		重合闸启动	UINT16	
0X186		重合闸一次动作	UINT16	
0X187		重合闸二次动作	UINT16	
0X188		重合闸三次动作	UINT16	
0X189		重瓦斯跳闸	UINT16	
0X18A		轻瓦斯告警	UINT16	
0X18B		超温跳闸	UINT16	
0X18C		过流告警	UINT16	
0X18D		网门打开跳闸	UINT16	
0X18E		低压动作	UINT16	
0X18F		低压告警	UINT16	

0X190		过压动作	UINT16	
-------	--	------	--------	--

4.3 时间寄存器

寄存器地址	类型	描述	数据格式	范围/备注
0X00	WO	当前时间	H: 年 (2 字节) H: 月 (1 字节) L: 日 (1 字节) H: 时 (1 字节) L: 分 (1 字节) H: 毫秒 (2 字节)	年: 2000~2099 月: 1~12 日: 1~28/29/30/31 时: 0~23 分: 0~59 毫秒: 0~60000

4.4 事件带时标查询寄存器表

寄存器地址	类型	描述	数据格式	单位	范围/备注
0X0500	RO	记录标识			0X81: 后续未读完 0X01: 已读完
0X0501	RO	事件编码高位	UINT8		
0x0502	RO	事件编码	UINT8		
0x0503	RO	事件值	UINT8		
0x0504	RO	事件确认码	UINT8		
0x0505	RO	年高	UINT8		
0x0506	RO	年低	UINT8		
0x0507	RO	月	UINT8		
0x0508	RO	日	UINT8		
0x0509	RO	时	UINT8		
0x050A	RO	分	UINT8		
0x050B	RO	毫秒高	UINT8		
0x050C	RO	毫秒低	UINT8		

4.5 遥控寄存器表

寄存器地址	类型	描述	数据格式	范围/备注
0X300	WO	遥控选择	UINT16	
0X301	WO	遥控执行	UINT16	
0X302	WO	遥控撤销	UINT16	
0X303	WO	远方复归	UINT16	

遥控命令: 0x0001 分闸, 0x0002 合闸