

易事特集团股份有限公司	文件编号		文件版本	V1.0
	文件密级	秘密	生效日期	2019.4
	制定部门	软件部		

EA900 6-20k G4 项目 用户 Modbus 通讯协议

易事特集团股份有限公司	文件编号		文件版本	V1.0
	文件密级	秘密	生效日期	2019.4
	制定部门	软件部		

序号	版本	修改内容	修改时间	备注
1	Ver 1.0	新拟制	2019-4-25	Zhongth

目 录

一、协议相关说明	1
1、协议简介	1
2、接口方式	1
3、协议格式	1
3.1 RTU 模式的帧格式	1
4、响应信息分类	3
5、功能代码	5
二、通信内容	6
1、遥信量（功能码 0x02）	6
3、遥测量（功能码 0x04）	10
4、读取设备参数（功能码 0x03）	错误!未定义书签。
5、设置设备参数（功能码 0x06/0x10）	12
附录 A CRC 校验	15
CRC 循环冗余校验	15

一、协议相关说明

1、协议简介

通信采用 Modbus 协议，通过该协议使控制器经由 RS485 网络与监控器进行通信。

本通信采用应答方式，由主机发起请求（发送遥测信息），从机执行请求并且应答。从机需通过地址加以区分，从机可设置的地址范围为 1~247。

2、接口方式

RS232 接口：异步，半双工；

波特率：9600 bps，可设

数据长度：8 位，固定

奇偶校验位：无，固定

停止位：1 位，固定

3、协议格式

本协议支持 Modbus RTU 模式。

3.1 RTU 模式的帧格式

控制器以 RTU 模式在 Modbus 总线上进行通讯时，信息中的每 8 bit 字节包含 2 个 4 bit 十六进制的字符。RTU 模式中每个字节的格式为：

编码系统 : 8 位二进制；
 起始位 : 1 位
 数据位 : 8 位数据位，低位先送；
 奇/偶校验 : 奇校验或者偶校验时为 1 位；无奇偶校验时该位为 1 位停止位；
 停止位 : 1 位
 错误校验区 : 循环冗余校验(CRC)

RTU 模式的请求帧格式为：

起始	设备地址	功能代码	寄存器起始地址	寄存器个数	CRC 低字节	CRC 高字节	结束
至少 3.5 个字符空闲时间	8 bit	8 bit	16 bit	16 bit	8 bit	8 bit	至少 3.5 个字符空闲时间

其中 RTU 模式字符传输格式采用 10 位传输，其中数据位为 8 位；位序列为：（无奇偶校验位，所以为 10 位）

起始位	1	2	3	4	5	6	7	8	停止位 (奇/偶校验位)	停止位
-----	---	---	---	---	---	---	---	---	--------------	-----

RTU 模式的响应帧格式为:

起始	设备地址	功能代码	数据	CRC 低字节	CRC 高字节	结束
至少 3.5 个字符空闲时间	8 bit	8 bit	8n 个 bit	8 bit	8 bit	至少 3.5 个字符空闲时间

消息发送至少需要 3.5 个字符时间的停顿间隔开始。在最后一个传输字符之后, 需要至少 3.5 个字符时间的停顿来标定消息的结束。一个新的消息可在此停顿后开始。

整个消息帧必须作为一连续的流转输。如果在帧完成之前两个字符间有超过 1.5 个字符空闲的停顿时间, 认为帧错误, 停止接收, 并重新启动接收。也就是要保证两个帧间的间隔至少大于 3.5 个字符的时间, 1.5 个字符时间和 3.5 个字符时间与具体的通信波特率有关, 计算方法如下: 如通信波特率为 9600, 那么

$$1.5 \text{ 个字符间隔时间} = (1/9600) \times 11 \times 1.5 \times 1000 = 1.72 \text{ ms}$$

$$3.5 \text{ 个字符间隔时间} = (1/9600) \times 11 \times 3.5 \times 1000 = 4.01 \text{ ms}$$

【例如】***

请求帧信息: 请求 1 号机的数据, 位置为: 寄存器起始地址 0002, 寄存器个数为 1 个

	地址	功能码	寄存器起始地址		寄存器个数		CRC 校验	
数据	0x01	0x03	0x00	0x02	0x00	0x01	0x25	0xCA
字节数	1	1	2		2		2	

响应帧信息: 1 号机的响应帧

	地址	功能码	返回数据字节数	数据内容		CRC 校验	
数据	0x01	0x03	0x02	0x12	0x22	0xE9	0x5C
字节数	1	1	1	2		2	

4、响应信息分类

主机向从机设备发送查询并希望有一个正常响应，主机查询中有可能产生 4 种事件：

(1) 从机接收查询，无通讯错误，正常处理信息，则返回一个正常响应事件。

(2) 由于通讯出错，从机不能接收查询数据，因而不返回响应。此时，主机依靠处理程序判定为查询超时。

(3) 若从机接收查询，发现有 (CRC) 通讯错误，不返回响应，此时依靠主机处理程序判定为查询超时。

(4) 从机接收查询，无通讯错误，但无法处理 (如读不存在的寄存器地址或错误的寄存器个数) 时，向主机报告错误的性质。

向主机报告错误的响应信息有 2 个与正常响应不相同的区域：

功能代码区：正常响应时，从机的响应功能代码区，带原查询的功能代码。所有功能代码的 MSB 为 0 (其值低于 80H)。不正常响应时，从机把功能代码的 MSB 置为 1，使功能代码值大于 80H，高于正常响应的值。这样，主机应用程序能识别不正常响应事件，能检查不正常代码的数据区。

数据区：正常响应中，数据区含有 (按查询要求给出的) 数据或统计值，在不正常响应中，数据区为一个不正常代码，它说明从机产生不正常响应的条件和原因。

不正常代码及含义如下表所示：

代码	名称	含义
0x01	非法的功能代码	从机接收的是一种不能执行的功能代码。发出查询命令后，该代码指示无程序功能。
0x02	非法的数据地址	接收的数据地址，是从机不允许的地址；如：寄存器起始地址错误，查询的寄存器个数错误。
0x03	非法的寄存器个数	寄存器个数超范围；
0x04	非法设备地址	设别地址错误，不需要回复
0x05	非法 CRC	CRC 校验错误
0x06	非法数据长度	数据长度超范围

【例如】***

RTU 模式:

命令信息: 请求 1 号机的数据, 位置为: 寄存器起始地址 0066, 寄存器个数为 2 个

	地址	功能码	寄存器起始地址		寄存器个数		CRC 校验	
数据	0x01	0x03	0x00	0x66	0x00	0x02	0x24	0x14

响应信息: 1 号机的响应帧, 因为寄存器起始地址错误, 因此返回信息为不合法的数据地址

	地址	功能码	数据内容	CRC 校验	
数据	0x01	0x83	0x02	0xC0	0xF1

5、功能代码

功能码	名称	作用
0x02	读离散量输入	读取状态信息和告警信息
0x03	读取保持寄存器	读取当前参数设置信息
0x04	读取输入寄存器	读取当前模拟量
0x06	写单个保持寄存器	写单个设置参数
0x10	写多个保持寄存器	写多个设置参数

二、通信内容

1、遥信量（功能码 0x02）

1) MCU 请求命令格式:

定义	地址	功能码	起始离散量地址		离散量个数		CRC 校验	
数据	ADDR	02H	高位	低位	高位	低位	低位	高位
字节数	1	1	2		2		2	

2) DSP 正常响应格式:

定义	地址	功能码	应答数据字节数	返回的离散量状态	CRC 校验	
数据	ADDR	02H	DATA_BYTES		低位	高位
字节数	1	1	1		2	

3) DSP 异常响应格式:

定义	地址	差错码	异常码	CRC 校验	
数据	ADDR	82H	ERR_CODE	低位	高位
字节数	1	1	1	2	

遥信量寄存器表:

地址	名称	数据类型	数据长度	状态含义	级别
0	BUS 高压	bit	1	1: 发生; 0: 消失	研发/用户
1	BUS 低压	bit	1	1: 发生; 0: 消失	研发/用户
2	BUS 不平衡	bit	1	1: 发生; 0: 消失	研发/用户
3	BUS 软启动失败	bit	1	1: 发生; 0: 消失	研发/用户
4	逆变软启动失败	bit	1	1: 发生; 0: 消失	研发/用户
5	逆变高压	bit	1	1: 发生; 0: 消失	研发/用户
6	逆变低压	bit	1	1: 发生; 0: 消失	研发/用户
7	逆变禁止	bit	1	1: 发生; 0: 消失	研发/用户
8	过温	bit	1	1: 发生; 0: 消失	研发/用户
9	输出短路	bit	1	1: 发生; 0: 消失	研发/用户
10	过载故障	bit	1	1: 发生; 0: 消失	研发/用户
11	负功异常	bit	1	1: 发生; 0: 消失	研发/用户
12	关机故障	bit	1	1: 发生; 0: 消失	研发/用户
13	并机软件版本不一致(未使用)	bit	1	1: 发生; 0: 消失	研发/用户
14	同步信号异常(未使用)	bit	1	1: 发生; 0: 消失	研发/用户
15	同步脉冲异常	bit	1	1: 发生; 0: 消失	研发/用户
16	逆变继电器粘死	bit	1	1: 发生; 0: 消失	研发/用户
17	BUS 短路	bit	1	1: 发生; 0: 消失	研发/用户
18	CAN 通讯异常	bit	1	1: 发生; 0: 消失	研发/用户

19	物理地址冲突	bit	1	1: 发生; 0: 消失	研发/用户
20	并机机型不兼容	bit	1	1: 发生; 0: 消失	研发/用户
21	电池节数设置错误	bit	1	1: 发生; 0: 消失	研发/用户
22	输入 SCR 软启动失败	bit	1	1: 发生; 0: 消失	研发/用户
23	整流 SCR 故障(未使用)	bit	1	1: 发生; 0: 消失	研发/用户
24	逆变器异常	bit	1	1: 发生; 0: 消失	研发/用户
25	并机旁路接线错误	bit	1	1: 发生; 0: 消失	研发/用户
26	逆变开路	bit	1	1: 发生; 0: 消失	研发/用户
27	PFC 异常	bit	1	1: 发生; 0: 消失	研发/用户
28	逆变电容异常	bit	1	1: 发生; 0: 消失	研发/用户
29	风扇故障	bit	1	1: 发生; 0: 消失	研发/用户
30	EPO	bit	1	1: 发生; 0: 消失	研发/用户
31	辅助电源丢失	bit	1	1: 发生; 0: 消失	研发/用户
32	预留 1	bit	1	1: 发生; 0: 消失	研发/用户
33	预留 2	bit	1	1: 发生; 0: 消失	研发/用户
34	预留 3	bit	1	1: 发生; 0: 消失	研发/用户
35	预留 4	bit	1	1: 发生; 0: 消失	研发/用户
36	预留 5	bit	1	1: 发生; 0: 消失	研发/用户
37	预留 6	bit	1	1: 发生; 0: 消失	研发/用户
38	预留 7	bit	1	1: 发生; 0: 消失	研发/用户
39	预留 8	bit	1	1: 发生; 0: 消失	研发/用户
40	预留 9	bit	1	1: 发生; 0: 消失	研发/用户
41	预留 10	bit	1	1: 发生; 0: 消失	研发/用户
42	预留 11	bit	1	1: 发生; 0: 消失	研发/用户
43	预留 12	bit	1	1: 发生; 0: 消失	研发/用户
44	预留 13	bit	1	1: 发生; 0: 消失	研发/用户
45	预留 14	bit	1	1: 发生; 0: 消失	研发/用户
46	预留 15	bit	1	1: 发生; 0: 消失	研发/用户
47	预留 16	bit	1	1: 发生; 0: 消失	研发/用户
48	并机线连接异常	bit	1	1: 发生; 0: 消失	研发/用户
49	并机设置错误	bit	1	1: 发生; 0: 消失	研发/用户
50	电池反接	bit	1	1: 发生; 0: 消失	研发/用户
51	过载告警	bit	1	1: 发生; 0: 消失	研发/用户
52	电池未接	bit	1	1: 发生; 0: 消失	研发/用户
53	输入过流	bit	1	1: 发生; 0: 消失	研发/用户
54	电池电压高	bit	1	1: 发生; 0: 消失	研发/用户
55	开机异常	bit	1	1: 发生; 0: 消失	研发/用户
56	充电器故障	bit	1	1: 发生; 0: 消失	研发/用户
57	EEPROM 异常	bit	1	1: 发生; 0: 消失	研发/用户
58	输入过流超时	bit	1	1: 发生; 0: 消失	研发/用户

59	电池低压	bit	1	1: 发生; 0: 消失	研发/用户
60	AD 采样异常	bit	1	1: 发生; 0: 消失	研发/用户
61	同步脉冲异常	bit	1	1: 发生; 0: 消失	研发/用户
62	同步信号异常	bit	1	1: 发生; 0: 消失	研发/用户
63	CAN 通讯异常	bit	1	1: 发生; 0: 消失	研发/用户
64	旁路高压	bit	1	1: 发生; 0: 消失	研发/用户
65	旁路故障	bit	1	1: 发生; 0: 消失	研发/用户
66	市电高压	bit	1	1: 发生; 0: 消失	研发/用户
67	市电频率异常	bit	1	1: 发生; 0: 消失	研发/用户
68	旁路频率超跟踪	bit	1	1: 发生; 0: 消失	研发/用户
69	旁路逆变切换次数超 限	bit	1	1: 发生; 0: 消失	研发/用户
70	电池放电终止	bit	1	1: 发生; 0: 消失	研发/用户
71	电池测试成功	bit	1	1: 发生; 0: 消失	研发/用户
72	禁止开机	bit	1	1: 发生; 0: 消失	研发/用户
73	电池测试未通过	bit	1	1: 发生; 0: 消失	研发/用户
74	并机均流异常	bit	1	1: 发生; 0: 消失	研发/用户
75	逆变锁相异常	bit	1	1: 发生; 0: 消失	研发/用户
76	电池维护成功	bit	1	1: 发生; 0: 消失	研发/用户
77	电池维护异常	bit	1	1: 发生; 0: 消失	研发/用户
78	输入电流不平衡	bit	1	1: 发生; 0: 消失	研发/用户
79	预留 16	bit	1	1: 发生; 0: 消失	研发/用户
80	PFC 异常	bit	1	1: 发生; 0: 消失	研发/用户
81	母线低压切电池次 数超限	bit	1	1: 发生; 0: 消失	研发/用户
82	市电异常	bit	1	1: 发生; 0: 消失	研发/用户
83	旁路异常	bit	1	1: 发生; 0: 消失	研发/用户
84	旁路频率异常	bit	1	1: 发生; 0: 消失	研发/用户
85	逆变输出电压检测 不一致	bit	1	1: 发生; 0: 消失	研发/用户
86	电池电压异常	bit	1	1: 发生; 0: 消失	研发/用户
87	旁路输出电压检测 不一致	bit	1	1: 发生; 0: 消失	研发/用户
88	负载不稳定 (未使 用)	bit	1	1: 发生; 0: 消失	研发/用户
89	维修旁路使能	bit	1	1: 发生; 0: 消失	研发/用户
90	过温频繁	bit	1	1: 发生; 0: 消失	研发/用户
91	并机电池节数设置 不一致	bit	1	1: 发生; 0: 消失	研发/用户
92	电池温度补偿异常 (未使用)	bit	1	1: 发生; 0: 消失	研发/用户

93	旁路电压不稳定(未使用)	bit	1	1: 发生; 0: 消失	研发/用户
94	测试模式	bit	1	1: 发生; 0: 消失	研发/用户
95	过载频繁	bit	1	1: 发生; 0: 消失	研发/用户

3、遥测量（功能码 0x04）

1) 上位机请求命令格式:

定义	地址	功能码	起始寄存器地址		寄存器个数		CRC 校验	
数据	ADDR	04H	高位	低位	高位	低位	低位	高位
字节数	1	1	2		2		2	

2) 正常响应格式:

定义	地址	功能码	应答数据字节数	返回的数据		CRC 校验	
数据	ADDR	04H	DATA_BYTES	高位	低位	低位	高位
字节数	1	1	1	2*寄存器个数		2	

3) 异常响应格式:

定义	地址	差错码	异常码	CRC 校验	
数据	ADDR	84H	ERR_CODE	低位	高位
字节数	1	1	1	2	

遥测量寄存器表:

地址	寄存器名称	数据长度	数据类型	单位	系数	级别
0	旁路 A 相电压 bypass phase A votage	2Bytes	INT16	V	0.1	研发/用户
1	预留 2	2Bytes	INT16	/	0.1	研发/用户
2	预留 3	2Bytes	INT16	/	0.1	研发/用户
3	旁路 A 相电流 bypass phase A current	2Bytes	INT16	A	0.1	研发/用户
4	预留 5	2Bytes	INT16	/	0.1	研发/用户
5	预留 6	2Bytes	INT16	/	0.1	研发/用户
6	旁路频率 bypass frequency	2Bytes	INT16	Hz	0.1	研发/用户
7	预留 8	2Bytes	INT16	/	0.1	研发/用户
8	预留 9	2Bytes	INT16	/	0.1	研发/用户
9	旁路 PF bypass pf	2Bytes	INT16	/	0.01	研发/用户
10	预留 11	2Bytes	INT16	/	1	研发/用户
11	预留 12	2Bytes	INT16	/	1	研发/用户
12	输入 A 相电压 input phase A votage	2Bytes	INT16	V	0.1	研发/用户
13	输入 B 相电压 input phase B votage	2Bytes	INT16	/	0.1	研发/用户
14	输入 C 相电压 input phase C votage	2Bytes	INT16	/	0.1	研发/用户

15	输入 A 相电流 input phase A current	2Bytes	INT16	A	0.1	研发/用户
16	输入 B 相电流 input phase B current	2Bytes	INT16	/	0.1	研发/用户
17	输入 C 相电流 input phase C current	2Bytes	INT16	/	0.1	研发/用户
18	输入频率 input frequency	2Bytes	INT16	Hz	0.1	研发/用户
19	预留 20	2Bytes	INT16	/	0.1	研发/用户
20	预留 21	2Bytes	INT16	/	0.1	研发/用户
21	输入 PF input pf	2Bytes	INT16	/	0.01	研发/用户
22	预留 23	2Bytes	INT16	/	1	研发/用户
23	预留 24	2Bytes	INT16	/	1	研发/用户
24	输出 A 相电压 output phase A vottage	2Bytes	INT16	V	0.1	研发/用户
25	预留 26	2Bytes	INT16	/	0.1	研发/用户
26	预留 27	2Bytes	INT16	/	0.1	研发/用户
27	输出 A 相电流 output phase A current	2Bytes	INT16	A	0.1	研发/用户
28	预留 29	2Bytes	INT16	/	0.1	研发/用户
29	预留 30	2Bytes	INT16	/	0.1	研发/用户
30	输出频率 output frequency	2Bytes	INT16	Hz	0.1	研发/用户
31	预留 32	2Bytes	INT16	/	0.1	研发/用户
32	预留 33	2Bytes	INT16	/	0.1	研发/用户
33	输出 PF output pf	2Bytes	INT16	/	0.01	研发/用户
34	预留 35	2Bytes	INT16	/	1	研发/用户
35	预留 21	2Bytes	INT16	/	1	研发/用户
36	输出视在功率 outpur apparent power	2Bytes	INT16	KVA	0.1	研发/用户
37	预留 38	2Bytes	INT16	/	0.1	研发/用户
38	预留 39	2Bytes	INT16	/	0.1	研发/用户
39	输出有功功率 active power	2Bytes	INT16	KW	0.1	研发/用户
40	预留 41	2Bytes	INT16	/	0.1	研发/用户
41	预留 42	2Bytes	INT16	/	0.1	研发/用户
42	输出无功功率 reactive power	2Bytes	INT16	KVAR	0.1	研发/用户
43	预留 44	2Bytes	INT16	/	0.1	研发/用户
44	预留 45	2Bytes	INT16	/	0.1	研发/用户

45	输出负载百分比 output load percentage	2Bytes	INT16	%	0.1	研发/用户
46	预留 47	2Bytes	INT16	/	1	研发/用户
47	预留 48	2Bytes	INT16	/	1	研发/用户
48	预留 49	2Bytes	INT16	/	1	研发/用户
49	电池电压 battery voltage	2Bytes	INT16	V	0.1	研发/用户
50	预留 51	2Bytes	INT16	/	1	研发/用户
51	电池电流 battery current	2Bytes	INT16	A	0.1	研发/用户
52	预留 53	2Bytes	INT16	/	1	研发/用户
53	电池温度 battery temperature	2Bytes	INT16	C	0.1	研发/用户
54	电池剩余放电时间 remain discharge time	2Bytes	INT16	Min	1	研发/用户
55	电池容量 battery capcaty	2Bytes	INT16	%	0.1	研发/用户
56	逆变电流 inverter current	2Bytes	INT16	A	0.1	研发/用户
57	整流温度 Rectifier temperature	2Bytes	INT16	C	0.1	研发/用户
58	逆变温度 inverter temperature	2Bytes	INT16	C	0.1	研发/用户
59	预留 60	2Bytes	INT16	/	1	研发/用户
60	预留 61	2Bytes	INT16	/	1	研发/用户
61	预留 62	2Bytes	INT16	/	1	研发/用户
62	预留 63	2Bytes	INT16	/	1	研发/用户
63	预留 64	2Bytes	INT16	/	1	研发/用户
64	预留 65	2Bytes	INT16	/	1	研发/用户
65	预留 66	2Bytes	INT16	/	1	研发/用户
66	预留 67	2Bytes	INT16	/	1	研发/用户
67	软件版本号 1-2 software version	2Bytes	Char	/	1	研发/用户
68	软件版本号 3-4 software version	2Bytes	Char	/	1	研发/用户
69	软件版本号 5-6 software version	2Bytes	Char	/	1	研发/用户
70	状态字	2Bytes	Uint16	/	1	研发/用户
71	系统工作模式 system work mode	2Bytes	Uint16	/	1	研发/用户

5、设置设备参数（功能码 0x06/0x10）

5.1 0x06 命令帧格式

1) 上位机请求命令格式:

定义	地址	功能码	寄存器地址		寄存器值		CRC 校验	
数据	ADDR	06H	高位	低位	高位	低位	低位	高位
字节数	1	1	2		2		2	

2) 正常响应格式:

定义	地址	功能码	寄存器地址		寄存器值		CRC 校验	
数据	ADDR	06H	高位	低位	高位	低位	低位	高位
字节数	1	1	2		2		2	

3) 异常响应格式:

定义	地址	差错码	异常码	CRC 校验	
数据	ADDR	86H	ERR_CODE	低位	高位
字节数	1	1	1	2	

命令寄存器表:

地址	寄存器名称	数据长度	数据类型	含义
0x8000	清除故障 clear fault	2Bytes	INT16	1: 清除故障, 0: 忽略
0x8001	清除历史记录 clear history log	2Bytes	INT16	1: 清除历史记录, 0: 忽略
0x8002	蜂鸣器消音 buzzer off	2Bytes	INT16	1: 蜂鸣器消音, 0: 蜂鸣器正常工作
0x8003	手动切旁路 manual switch to bypass	2Bytes	INT16	1: 切旁路 (逆变供电状态下且旁路正常时有效), 0: 忽略
0x8004	手动切逆变 manual switch to inverter	2Bytes	INT16	1: 切逆变 (手动切至旁路供电后, 逆变正常时有效), 0: 忽略
0x8005	清除电池数据 clear battery data	2Bytes	INT16	1: 清除电池数据, 0: 忽略
0x8006	电池测试 battery test	2Bytes	INT16	测试类型: 1: 电池检测 (放电 20s) 2: 电池维护 (放电至电池低压)
0x8007	终止电池测试 stop battery test	2Bytes	INT16	1: 终止电池自检, 0: 忽略

附录 A CRC 校验

□ CRC 校验

CRC 循环冗余校验

循环冗余校验 CRC 区为 2 字节，含一个 16 位二进制数据。由发送设备计算 CRC 值，并把计算值附在信息中，接收设备在接收信息时，重新计算 CRC 值，并把计算值与接收的在 CRC 区中实际值进行比较，若两者不相同，则产生一个错误。

CRC 开始时先把寄存器的 16 位全部置成“1”，然后把相邻 2 个 8 位字节的数据放入当前寄存器中，只有每个字符的 8 位数据用作产生 CRC，起始位、停止位和奇偶校验位不加入到 CRC 中。

产生 CRC 期间，每 8 位数据与寄存器中值进行异或运算，其结果向右移一位(向 LSB 方向)，并用“0”填入 MSB，检测 LSB，若 LSB 为“1”则与预置的固定值异或，若 LSB 为“0”则不作异或运算。

重复上述过程，直至移位 8 次，完成第 8 次移位后，下一个 8 位数据，与该寄存器的当值异或，在所有信息处理完后，寄存器中的最终值为 CRC 值。