



EBYTE

成都亿佰特电子科技有限公司

Chengdu Ebyte Electronic Technology Co.,Ltd.

4G/RS485 NET IO

用户使用手册



E850-DTU (4440-4G)

本说明书可能会随着产品的改进而更新，请以最新版的说明书为准
成都亿佰特电子科技有限公司保留对本说明中所有内容的最终解释权及修改权

功能特点

- 支持 4 路模拟量输入，默认电流检测；
- 支持 4 路数字量输入，默认干接点；
- 支持 4 路继电器输出；
- 支持 socket 连接远程服务器，支持 TCP/UDP；
- 采用 Modbus TCP/RTU 协议数据处理；
- 支持 2 种工作模式，主机模式，从机模式，从机可通过 RS485 级联多个设备；
- 支持 Re load 轻触按键，长按 5s，Modbus 设备地址、RS485 串口波特率和校验位恢复出厂设置；
- 硬件看门狗，具有高度的可靠性；
- 多个指示灯显示工作状态；
- 电源具有良好的过流、过压、防反接等功能。

注意：客户可定制功能，如条件控制（根据输入状态判定如何输出）

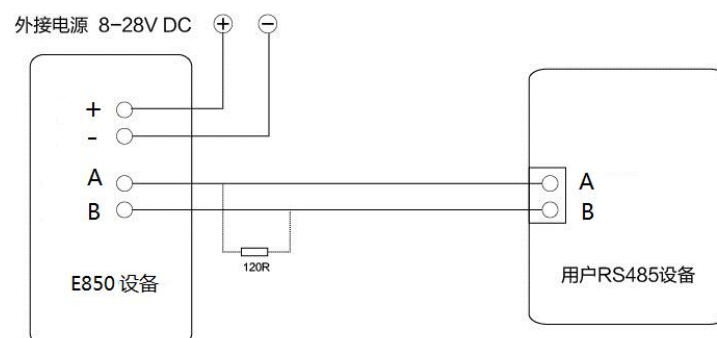
1、 快速入门

本章是针对E850-DTU(4440-4G)系列产品的快速入门介绍，建议用户系统的阅读本章并按照指示操作一遍，将会对模块产品有一个系统的认识，用户也可以根据根据需要选择你感兴趣的章节阅读。针对特定的细节和说明，请参考后续章节。

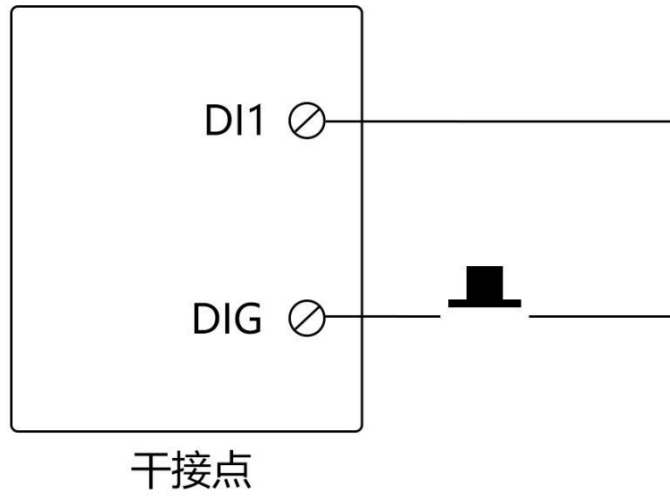
1.1. 端口连接

1.1.1. RS485 连接

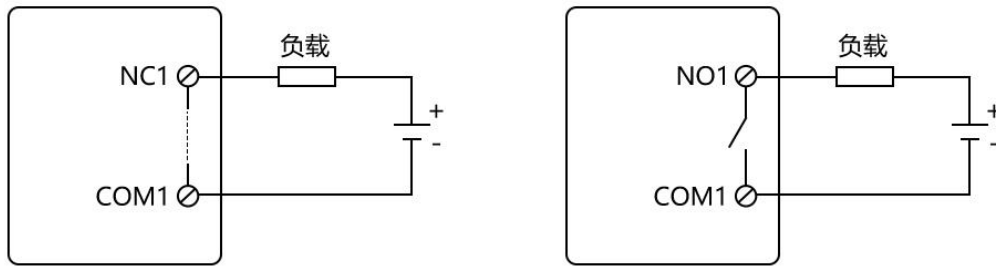
RS485接线图



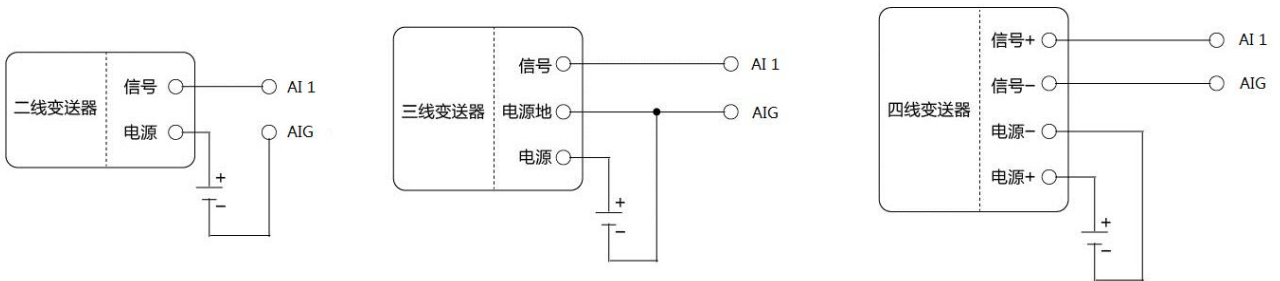
1.1.2. 开关量输入连接



1.1.3. 继电器输出连接



1.1.4. 模拟量输入连接



模拟量输入连接

1.2. 简单使用

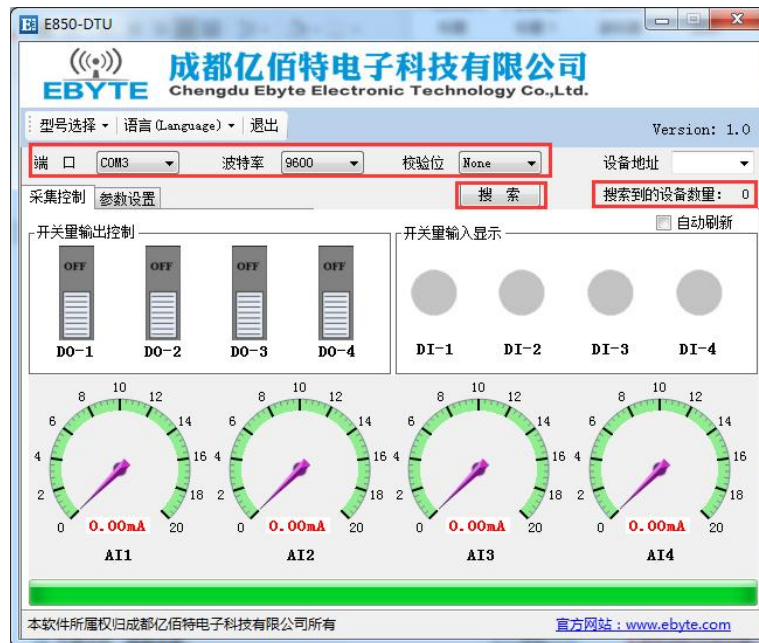
接线：电脑通过 USB 转 RS485 连接 E850-DTU(4440-4G)。

联网：在断电状态下插入 SIM 卡。

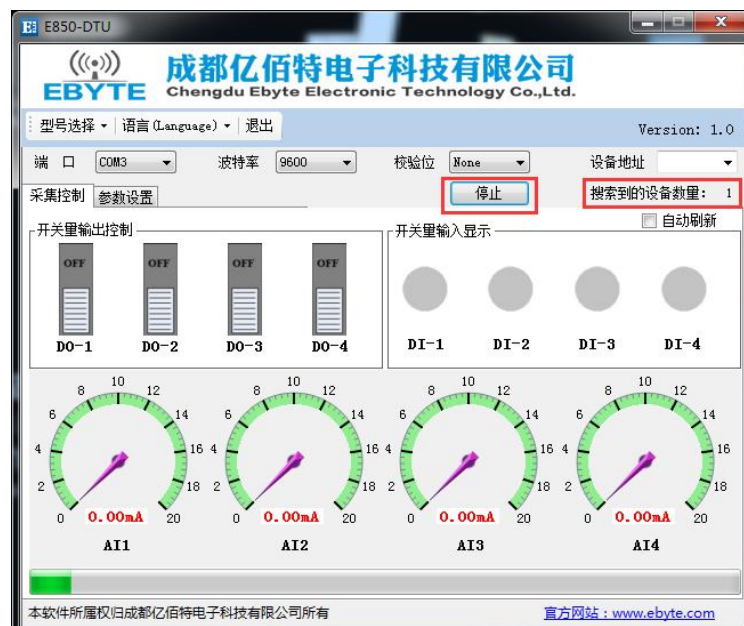
供电：E850-DTU(4440-4G) 工作电压为 DC 8~28V。

1.2.1. RS485 总线控制

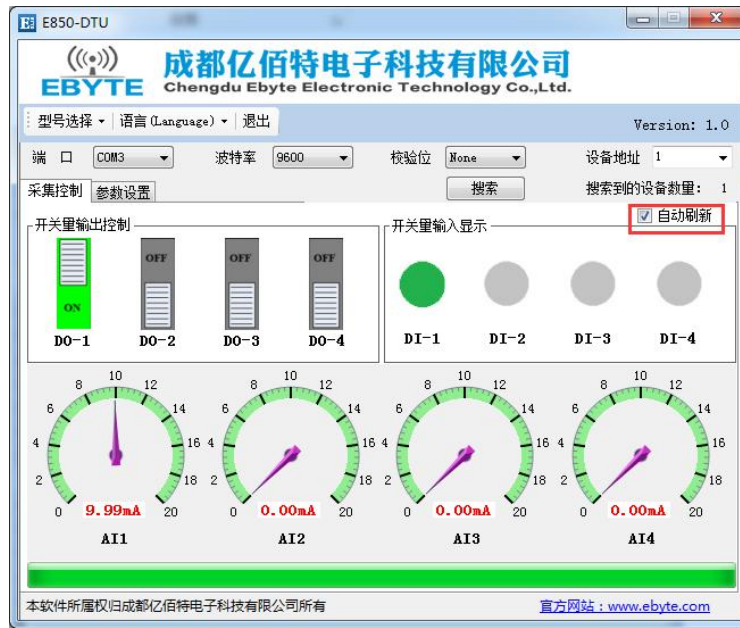
选择相应端口，单击“搜索”，搜索设备。



搜索到设备后，单击“停止”

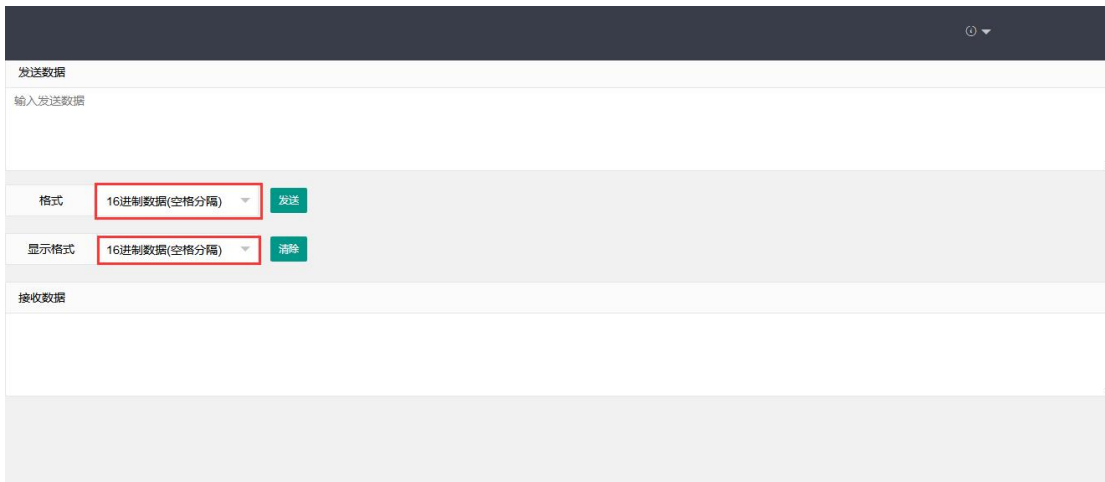


这时，可看到当前设备的设备地址，对“自动刷新”√处理，可进行开关量输出控制、开关量输入读取、模拟量输入读取



1.2.2. 网络控制

输入 http://yun.cdebyte.com/www/data_direct 网址，可通过命令来控制采集，命令采用 Modbus TCP/RTU 协议。



2、 产品介绍

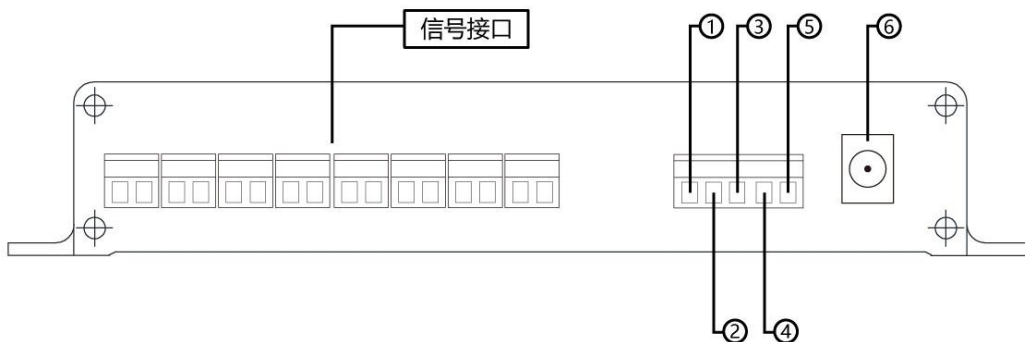
E850-DTU (4440-4G) 是款支持 4 路数字量输入（默认干接点），4 路模拟量输入，4 路继电器输出的网络 IO 产品。支持 Modbus TCP/RTU

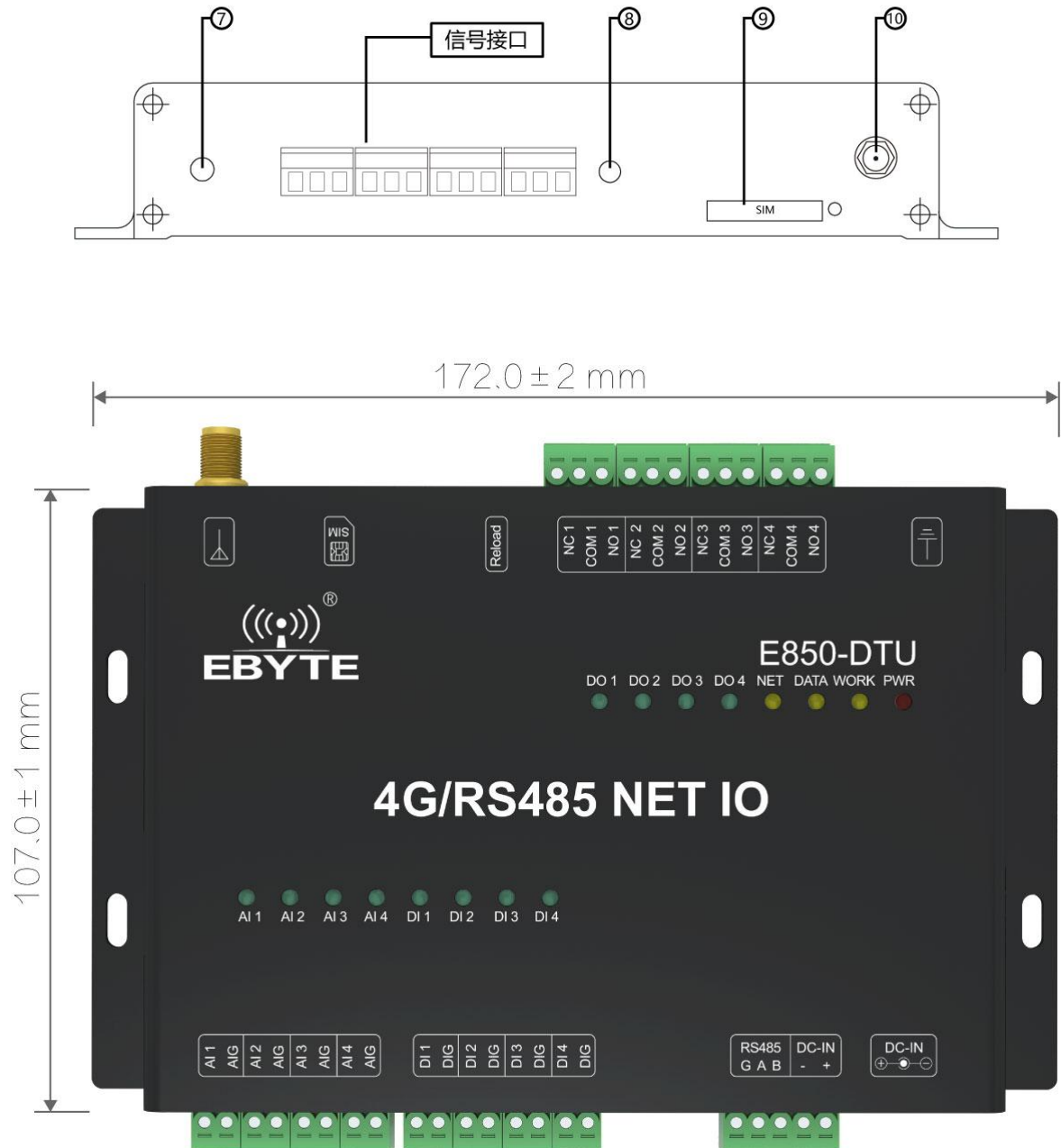
协议。该产品具有高度易用性，用户可方便快速地集成于自己的系统中，以实现基于 4G 的远程控制。

2.1. 基本参数

	项目	指标
无线参数	标准频段	LTE-FDD: B1/B3/B5/B8
		LTE-TDD: B38/B39/B40/B41
		WCDMA: B1/B8
		TD-SCDMA: B34/B39
		CDMA: BC0
		GSM: 900/1800MHz
硬件参数	产品尺寸 (H*W*D)	172*107*29mm
	产品重量	460g ± 9g
	工作温度	-20°C ~ +70°C
	存储温度	-40°C ~ +85°C
	工作湿度	5%~95%
	存储湿度	1%~95%
	工作电压	8V~28V
	电流采集范围	0mA~20mA/4mA-20mA 可配置
	精度	0.2%
	数据接口	RS485: 1200~115200bps
软件参数	网络类型	4G
	配置命令	Modbus TCP/RTU
	网络协议	Modbus TCP/RTU
	工作模式	主机模式、从机模式
	数据传输方式	TCP/UDP

2.2. 尺寸、接口描述





序号	端口及其他定义	功能	说明
1	RS485 G	信号参考地	信号参考地，可不连
2	RS485 A	RS485 接口 A	RS485 接口 A 与设备 A 接口相连
3	RS485 B	RS485 接口 B	RS485 接口 B 与设备 B 接口相连
4	DC-IN -	压线式电源输入负极	电源参考地
5	DC-IN +	压线式电源输入正极	电源输入，DC 8V~28V，建议 12V/24V
6	DC-IN 座子	DC 插座 5.5*2.1mm	电源输入端，DC 8V~28V，建议 12V/24V
7	接地螺丝	与大地连接	与大地连接
8	Reload	复位按键	长按 5s 起作用，
9	SIM 卡槽	SIM 卡槽	插入 SIM 卡，连网
10	ANT	天线接口	4G 天线

信号接口			
1	AI 1	模拟量输入通道 1	模拟量输入引脚, 与 AIG 形成输入
2	AIG	模拟量输入地	可与 AI 1 成对使用
3	AI 2	模拟量输入通道 2	模拟量输入引脚, 与 AIG 形成输入
4	AIG	模拟量输入地	可与 AI 2 成对使用
5	AI 3	模拟量输入通道 3	模拟量输入引脚, 与 AIG 形成输入
6	AIG	模拟量输入地	可与 AI 3 成对使用
7	AI 4	模拟量输入通道 4	模拟量输入引脚, 与 AIG 形成输入
8	AIG	模拟量输入地	可与 AI 4 成对使用
9	DI 1	开关量输入通道 1	与 DIG 形成干接点
10	DIG	开关量输入地	可与 DI 1 成对使用
11	DI 2	开关量输入通道 2	与 DIG 形成干接点
12	DIG	开关量输入地	可与 DI 2 成对使用
13	DI 3	开关量输入通道 3	与 DIG 形成干接点
14	DIG	开关量输入地	与 DI 3 成对使用
15	DI 4	开关量输入通道 4	与 DIG 形成干接点
16	DIG	开关量输入地	可与 DI 4 成对使用
17	NC 1	继电器 1 常闭引脚	与继电器 1 公共端配合使用
18	COM 1	继电器 1 公共端	与继电器 1 常开引脚/常闭引脚配合使用
19	NO 1	继电器 1 常开引脚	与继电器 1 公共端配合使用
20	NC 2	继电器 2 常闭引脚	与继电器 2 公共端配合使用
21	COM 2	继电器 2 公共端	与继电器 2 常开引脚/常闭引脚配合使用
22	NO 2	继电器 2 常开引脚	与继电器 2 公共端配合使用
23	NC 3	继电器 3 常闭引脚	与继电器 3 公共端配合使用
24	COM 3	继电器 3 公共端	与继电器 3 常开引脚/常闭引脚配合使用
25	NO 3	继电器 3 常开引脚	与继电器 3 公共端配合使用
26	NC 4	继电器 4 常闭引脚	与继电器 4 公共端配合使用
27	COM 4	继电器 4 公共端	与继电器 4 常开引脚/常闭引脚配合使用
28	NO 4	继电器 4 常开引脚	与继电器 4 公共端配合使用
LED 灯			
1	AI 1	模拟量输入通道 1 指示	绿色 LED, 足够大的输入量 ($\geq 0.5\text{mA}$) 亮起
2	AI 2	模拟量输入通道 2 指示	绿色 LED, 足够大的输入量 ($\geq 0.5\text{mA}$) 亮起
3	AI 3	模拟量输入通道 3 指示	绿色 LED, 足够大的输入量 ($\geq 0.5\text{mA}$) 亮起
4	AI 4	模拟量输入通道 4 指示	绿色 LED, 足够大的输入量 ($\geq 0.5\text{mA}$) 亮起
5	DI 1	开关量输入通道 1 指示	绿色 LED, DI 1、DIG 短接亮起
6	DI 2	开关量输入通道 2 指示	绿色 LED, DI 2、DIG 短接亮起
7	DI 3	开关量输入通道 3 指示	绿色 LED, DI 3、DIG 短接亮起
8	DI 4	开关量输入通道 4 指示	绿色 LED, DI 4、DIG 短接亮起
9	DO 1	继电器 1 输出指示	绿色 LED, NO 1、COM 1 闭合亮起
10	DO 2	继电器 2 输出指示	绿色 LED, NO 2、COM 2 闭合亮起
11	DO 3	继电器 3 输出指示	绿色 LED, NO 3、COM 3 闭合亮起
12	DO 4	继电器 4 输出指示	绿色 LED, NO 4、COM 4 闭合亮起
13	NET	网络指示	黄色 LED, 入网后长亮

14	DATA	串口数据指示	黄色 LED, RS485 接口有数据传输时亮起 (表现为闪烁)
15	WORK	工作/复位指示	黄色 LED, 规律闪烁/复位成功后快闪
16	PWR	电源指示	红色 LED, 长亮

注意:

接地: 建议将壳体与大地相连

2.3. Reload 轻触按键描述

长按 5S 有效, 复位成功后, WORK 灯快闪, Modbus 设备地址、RS485 串口波特率和校验位恢复出厂设置。

3、Modbus

3.1 寄存器地址表

寄存器地址表 (功能码: 0x01H、0x05H、0x0FH、0x03H、0x06H、0x10H)					
寄存器地址	寄存器数量	寄存器属性	寄存器类型	寄存器值范围	支持功能码
00017 (0x0010)	1	D01 开关量输出	读/写	0x0000 或 0xFF00 (0x05 功能码) 0-1 (0x01、0x0F 功能码)	0x01 0x05 0x0F
00018 (0x0011)	1	D02 开关量输出	读/写		
00019 (0x0012)	1	D03 开关量输出	读/写		
00020 (0x0013)	1	D04 开关量输出	读/写		
保留					
10017 (0x0010)	1	D11 开关量输入	只读	0-1	0x02
10018 (0x0011)	1	D12 开关量输入	只读		
10019 (0x0012)	1	D13 开关量输入	只读		
10020 (0x0013)	1	D14 开关量输入	只读		
保留					
30017 (0x0010)	1	A11 输入值, 单位 (uA)	只读	0-20000	0x03 0x04
30018 (0x0011)	1	A12 输入值, 单位 (uA)	只读		
30019 (0x0012)	1	A13 输入值, 单位 (uA)	只读		
30020 (0x0013)	1	A14 输入值, 单位 (uA)	只读		
保留					
40049 (0x0030)	1	D11 脉冲计数值	只读	0-65535	0x03
40050 (0x0031)	1	D12 脉冲计数值	只读	0-65535	
40051 (0x0032)	1	D13 脉冲计数值	只读	0-65535	
40052 (0x0033)	1	D14 脉冲计数值	只读	0-65535	
保留					
40065 (0x0040)	1	D11-D14 脉冲计数清零	只写	0x00 - 0x0F	0x06
保留					
40078 (0x004D)	1	设备地址	读/写	1 - 247	0x03 0x06 0x10
40079 (0x004E)	1	波特率	读/写	0 - 7	
40080 (0x004F)	1	校验位	读/写	0 - 2	
40081 (0x0050)	1	主机模式或从机模式	读/写	0 - 1	
40082 (0x0051)	1	开关量自动上报	读/写	0 - 2	

40083 (0x0052)	1	开关量输出时间设置(毫秒)	读/写	300-65535	
40084 (0x0053)	1	模拟量量程设置	读/写	0 - 1	
40085 (0x0054)	1	开关量重启输出状态设置	读/写	0x00 - 0x10	
保留					
40100 (0x0063)	22	服务器 IP 或域名(域名以 ASCII)	读/写	--	
40122 (0x0079)	1	服务器端口	读/写	1 - 65535	
40123 (0x007A)	1	协议类型(UDP、TCP)	读/写	0 - 1	0x03
40124 (0x007B)	22	自定义注册包	读/写	--	0x06
40146 (0x0091)	1	注册包机制	读/写	0 - 4	0x10
40147 (0x0092)	22	心跳包	读/写	--	
40169 (0x00A8)	1	心跳包时间	读/写	0 - 65535	
40170 (0x00A9)	1	云透传功能	读/写	0 - 1	
40171 (0x00AA)	11	IMEI 值	只读	--	
40182 (0x00B5)	11	SN 码值	只读	--	0x03
40193 (0x00C0)	20	LBS	只读	--	
保留					
40300 (0x012B)	1	版本号	只读	--	0x03

3.2 Modbus 地址表

Modbus 地址表	
1 (默认)	1
2	2
3	3
...	...
245	245
246	246
247	247

3.3 RS485 串口波特率码值表

波特率码值表	
0	1200
1	2400
2	4800
3 (默认)	9600
4	19200
5	38400
6	57600
7	115200

3.4 RS485 串口校验位码值表

校验位码值表	
0 (默认)	无校验
1	偶校验
2	奇校验

通过上位机配置参数

选择“参数设置”栏，可进行读取参数，写入参数，具体实现功能，见下文产品功能介绍。



4、 产品功能

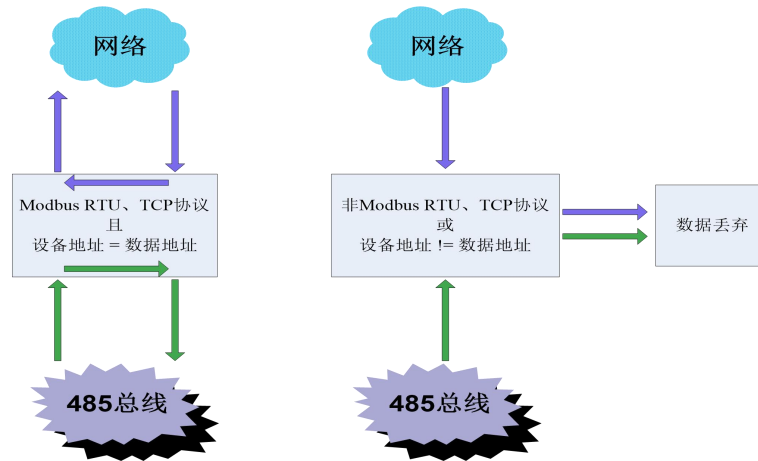
4.1. 工作模式

工作模式分为主机模式和从机模式，通过 Modbus 寄存器 40081 (0x0050) 配置。当寄存器值为 0 的时候为主机模式；当寄存器值为 1 的时候为从机模式，默认从机模式。

4.1.1. 从机模式

从机模式下(寄存器值为 0x01)，网络端或者 485 总线端(发送端)向设备发送的数据满足 Modbus RTU、Modbus TCP 协议，并且数据中的地址为设备地址，设备会以相同协议应答发送端；若网络端或者 485 总线端向设备发送的数据不满足 Modbus RTU、Modbus TCP 协议，或者满足 Modbus RTU、Modbus TCP 协议但是数据地址不是设备地址的情况下，发送端的数据将被丢弃。

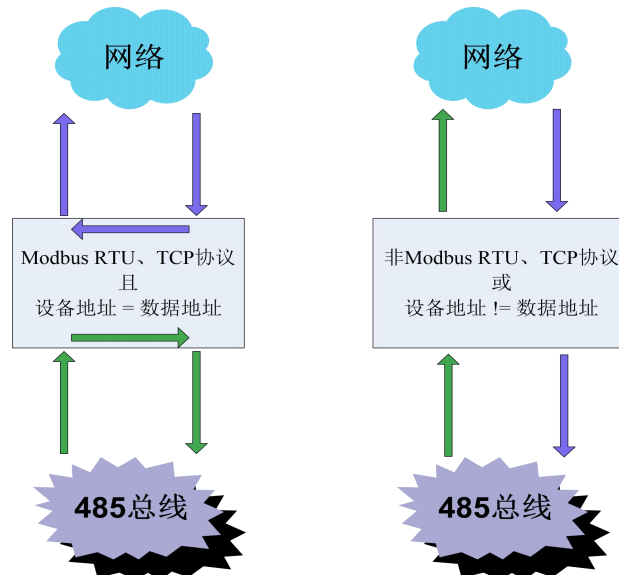
从机模式下，设备可以直接通过 485 总线连接主机模式下的设备，实现从机不联网的情况下，网络端也可以通过主机访问从机的数据。



4.1.2. 主机模式

主机模式下（寄存器值为 0x00），网络端或者 485 总线端（发送端）向设备发送的数据满足 Modbus RTU、Modbus TCP 协议，并且数据中的地址为设备地址，设备会以相同协议应答发送端；若网络端或者 485 总线端向设备发送的数据不满足 Modbus RTU、Modbus TCP 协议，或者满足 Modbus RTU、Modbus TCP 协议但是数据地址不是设备地址的情况下，485 总线来的数据将被传输到网络上，网络上来的数据将被传输到 485 总线上。

主机模式的这个功能可以实现设备级联功能和 485 总线与网络的数据传输。



4.2. IO 基本功能

4.2.1. 开关量 D0 输出

- **读开关量 D0 输出**

功能码：01，读线圈状态

地址范围：00017 (0x0010) ~ 00020 (0x0013)

说明：设备继电器无源输出，线圈不通电情况下，继电器 NC 口与 COM 口常闭，NO 口与 COM 口常开，取值为 0；线圈通电，则现象相反，继电器 NC 口与 COM 口断开，NO 口与 COM 口闭合，取值为 1。通过指令查询继电器状态。

例子：

读取 4 路开关量输出状态，假设返回值为 03，对应二进制位 0000 0011，低四位四个 bit 代表开关量输出状态，依次为 D04、D03、D02、D01。

Modbus RTU 协议读取开关量输出：

发送	01	01	00 10	00 04	3C 0C
	设备 ModBus 地址	功能码	开关量起始地址	读开关量数量	CRC 校验码

接收	01	01	01	03	11 89
	设备 ModBus 地址	功能码	返回字节数	开关量输出值	CRC 校验码

Modbus TCP 协议读取开关量输出：

发送	00 01	00 00	00 06	01	01	00 10	00 04
	传输标识	协议标识	长度	单元标识	功能码	开关量起始地址	读开关量数量

接收	00 01	00 00	00 04	01	01	01	03
	传输标识	协议标识	长度	单元标识	功能码	返回字节数	开关量输出值

- **控制开关量 D0 输出**

功能码：05，写单个线圈状态；0F，写多个线圈状态

地址范围：00017 (0x0010) ~ 00020 (0x0013)

说明：设备继电器无源输出，线圈不通电，继电器 NC 口与 COM 口闭合，NO 口与 COM 口断开；线圈通电，继电器 NC 口与 COM 口断开，NO 口与 COM 口闭合。通过指令控制继电器状态。

例子：

功能码 0x05 写 D02 开关量输出，使 NC2、COM2 断开，NO2、COM2 闭合，写入值为 FF 00；使 NC2、COM2 闭合，NO2、COM2 断开，写入值 00 00。

Modbus RTU 协议写开关量输出：

发送	01	05	00 11	FF 00	DC 3F
	设备 ModBus 地址	功能码	开关量地址	写入值	CRC 校验码

接收	01	05	00 11	FF 00	DC 3F
	设备 ModBus 地址	功能码	开关量地址	写入值	CRC 校验码

Modbus TCP 协议写开关量输出：

发送	00 01	00 00	00 06	01	05	00 11	FF 00
	传输标识	协议标识	长度	单元标识	功能码	开关量地址	写入值

接收	00 01	00 00	00 06	01	05	00 11	FF 00
	传输标识	协议标识	长度	单元标识	功能码	开关量地址	写入值

功能码 0x0F 写 D02、D03 开关量输出，使 NC2、COM2 断开，NO2、COM2 闭合；使 NC3、COM3 断开，NO3、COM3 闭合。写入值应为 0x03，对应二进制位 0000 0011

Modbus RTU 协议写开关量输出：

发送	01	0F	00 11	00 02	01	03	62 95
	设备 ModBus 地址	功能码	开关量地址	写开关量数量	字节数	写入值	CRC 校验码

接收	01	0F	00 11	00 02	84 0F
	设备 ModBus 地址	功能码	开关量地址	写入值	CRC 校验码

Modbus TCP 协议写开关量输出：

发送	00 01	00 00	00 08	01	0F	00 11	00 02	01	03
	传输标识	协议标识	长度	单元标识	功能码	开关量地址	写开关量数量	字节数	写入值

接收	00 01	00 00	00 06	01	0F	00 11	00 02
	传输标识	协议标识	长度	单元标识	功能码	开关量地址	写开关量数量

4.2.2. 读开关量 DI 输入

功能码：02，读（开关量）输入状态

地址范围：10017(0x0010)~10020(0x0013)

说明：设备默认干接点输入，DI 和 COM 短接时，读取值应为 1；DI 和 COM 不短接时，读取值应为 0。

例子：

读取 4 路开关量输入值，DI 输入端 DI1、COM1 短接，DI2、COM2 不短接，DI3、COM3 短接，DI4、COM4 不短接。读取到的开关量输入值为 0x05，对应二进制位 0000 0101，低四位四个 bit 代表开关量输入值，依次为 DI4、DI3、DI2、DI1。

Modbus RTU 协议读取开关量输入：

发送	01	02	00 10	00 04	78 0C
	设备 ModBus 地址	功能码	开关量起始地址	读开关量数量	CRC 校验码
接收	01	02	01	05	61 8B
	设备 ModBus 地址	功能码	返回字节数	开关量输入值	CRC 校验码

Modbus TCP 协议读取开关量输入：

发送	00 01	00 00	00 06	01	02	00 10	00 04
	传输标识	协议标识	长度	单元标识	功能码	开关量起始地址	读开关量数量
接收	00 01	00 00	00 04	01	02	01	05
	传输标识	协议标识	长度	单元标识	功能码	返回字节数	开关量输入值

4.2.3. 读模拟量 AI 输入

功能码：03，读保持型寄存器；04，读输入寄存器

地址范围：30017 (0x0010) ~ 30020 (0x0013)

说明：模拟量输入值单位为 uA

例子：

功能码 0x03，读取 AI1 输入，假设 AI1 输入为 9946uA，对应值应为 0x0x26DA

Modbus RTU 协议读取模拟量输入：

发送	01	03	00 10	00 01	85 CF
	设备 ModBus 地址	功能码	模拟量起始地址	读取数量	CRC 校验码
接收	01	03	02	26 DA	23 BF
	设备 ModBus 地址	功能码	返回字节数	模拟量输入值	CRC 校验码

Modbus TCP 协议读取模拟量输入：

发送	00 01	00 00	00 06	01	03	00 10	00 01
	传输标识	协议标识	长度	单元标识	功能码	模拟量起始地址	读取数量
接收	00 01	00 00	00 05	01	03	02	26 DA
	传输标识	协议标识	长度	单元标识	功能码	返回字节数	模拟量输入值

功能码 0x04，读取 AI1 输入，假设 AI1 输入为 9946uA，对应值应为 0x0x26DA

Modbus RTU 协议读取模拟量输入：

发送	01	04	00 10	00 01	30 0F
	设备 ModBus 地址	功能码	模拟量起始地址	读取数量	CRC 校验码

接收	01	04	02	26 DA	22 CB
	设备 ModBus 地址	功能码	返回字节数	模拟量输入值	CRC 校验码

Modbus TCP 协议读取模拟量输入：

发送	00 01	00 00	00 06	01	04	00 10	00 01
	传输标识	协议标识	长度	单元标识	功能码	模拟量起始地址	读取数量

接收	00 01	00 00	00 05	01	04	02	26 DA
	传输标识	协议标识	长度	单元标识	功能码	返回字节数	模拟量输入值

4.2.4. 模拟量 AI 量程设置

当寄存器 0x40084 (0x0053) 值为 0 的时候，模拟量输入量程为 0 -- 20mA；

当寄存器 0x40084 (0x0053) 值为 1 的时候，模拟量输入量程为 4 -- 20mA；

4.3. IO 特色功能

4.3.1. 脉冲计数及计数清零

脉冲计数断电后不会保存，脉冲电平维持时间必须大于 10ms 才有效。开关量输入由断开状态变为闭合状态并且维持 10ms 以上的闭合时间，再变为断开状态，完成一次脉冲计数。

- 读取脉冲计数值

功能码：03，读保持型寄存器

地址范围：40049 (0x0030) ~ 40052 (0x0033)

说明：脉冲计数的最大值为 65535

例子：

D11 当前已检测到 16 次脉冲，D12 当前已检测到 3 次脉冲，读取 D11、D12 开关量输入计数值，

Modbus RTU 协议读脉冲计数值：

发送	01	03	00 30	00 02	C4 04
	设备 ModBus 地址	功能码	起始地址	读取数量	CRC 校验码

接收	01	03	04	00 10	00 03	BB F7
	设备 ModBus 地址	功能码	返回字节数	D11 计数值	D12 计数值	CRC 校验码

Modbus TCP 协议读脉冲计数值：

发送	00 01	00 00	00 06	01	03	00 30	00 02
	传输标识	协议标识	长度	单元标识	功能码	起始地址	读取数量

接收	00 01	00 00	00 07	01	03	04	00 10	00 03
	传输标识	协议标识	长度	单元标识	功能码	返回字节数	D11 计数值	D12 计数值

● **清零脉冲计数值**

功能码：06，写保持型寄存器

地址范围：40065 (0x0040)

说明：寄存器值低四位分别代表 DI4、DI3、DI2、DI1 计数，写入“1”代表计数清零，重新开始脉冲计数。

例子：

清除 DI2、DI4 脉冲计数值，保留 DI1、DI3 脉冲计数值。写入值应为 0x0a，对应二进制值为 0000 1010，

Modbus RTU 协议清零脉冲计数值

发送	01	06	00 40	00 0a	08 19
	设备 ModBus 地址	功能码	地址	写入值	CRC 校验码

接收	01	06	00 40	00 0a	08 19
	设备 ModBus 地址	功能码	地址	写入值	CRC 校验码

Modbus TCP 协议清零脉冲计数值

发送	00 01	00 00	00 06	01	06	00 40	00 0a
	传输标识	协议标识	长度	单元标识	功能码	地址	写入值

接收	00 01	00 00	00 06	01	06	00 40	00 0a
	传输标识	协议标识	长度	单元标识	功能码	地址	写入值

4.3.2. 开关量输入 DI 自动上报

开关量输入自动上报功能是在当开关量发生变化的时候，将变化值传输出去。可以选择通过 RS485 传输或者 4G 传输，也可以关闭自动上报功能。

开关量自动上报设置对应的 Modbus 寄存器为 40082 (0x0051)，值对应功能：

关闭开关量自动上报功能

开关量自动上报通过 RS485 传输

开关量自动上报通过 4G 网络传输

开关量变化上传协议如下表，其中帧头 0xAA、0xBB 固定不变，DI1、DI2、DI3、DI4 的值范围为 0x00、0x01、0xFF，其中

0x00 代表开关量输入断开,

0x01 代表开关量输入闭合,

0xff 代表开关量输入未发生改变,

表格中 D11、D12、D13、D14 的值代表 D11、D12 状态更新为断开, D13 状态更新为闭合, D14 状态未发生改变。最后两个字节为 modbus CRC16 计算值。

帧头	D11	D12	D13	D14	Modbus CRC
0xAA 0xBB	0x00	0x00	0x01	0xff	0xBD 0xDA

4.3.3. 开关量输出 D0 时间设置

开关量脉冲输出时间设置也就是设置开关量输出时间(继电器 NO、COM 闭合时间), 对应的 Modbus 寄存器为 40083 (0x0052), 其值范围为 300-65535ms, 如果值低于 300ms, 默认开关量输出闭合为保持状态, 即开关量输出闭合后一直保持。若设置为 300ms 及以上, 如 500ms, 发送开关量输出闭合命令后, 开关量闭合将维持 500ms, 500ms 后再自动断开。

4.3.4. 重启开关量输出状态设置

设备断电重启是否保持断电前的状态或者重启保持特定的输出状态的设置, 该功能仅当设备开关量输出时间设置寄存器值小于 300ms 有效。

开关量重启输出状态设置对应的 Modbus 寄存器为 40085 (0x0054), 其值范围为 0x00-0x10。当此寄存器值为 0x10 的时候, 断电重启后保持上一次的开关量输出状态; 当此寄存器值为 0x00-0x0F 时, 由低四位决定设备重启开关量输出状态, bit4 对应 D04, bit3 对应 D03, bit2 对应 D02, bit1 对应 D01, 如当上电时, D04、D02 处于闭合状态(继电器 NO、COM 闭合) D03、D01 处于断开状态(继电器 NO、COM 断开), 对应寄存器值为 0000 1010, 即 0xa0, “1”为闭合状态, “0”为断开状态。

4. 4. 网络相关功能

4. 4. 1. 服务器 IP 或域名、端口、TCP 或 UDP 设置 (Socket)

服务器 IP 或域名由 22 个 modbus 寄存器保存, 第一个寄存器用于存放 IP 或域名对应的 ASCII 码长度, 剩下的寄存器用于存放 IP 或域名对应的 ASCII 码值。如 IP 为 116.62.42.192, 端口为 31687, 共 13 个字符, 即长度为 0x000D, IP 对应的 ASCII 码值为 31 31 36 2E 36 32 2E 34 32 2E 31 39 32, 这对应的 modbus 寄存器存储值如下表。如果是域名, 也是将对应的域名转化为 ASCII 对应的十六进制进行存放。(注: 域名最大长度不超过 40 个 ASCII 码)

40101 (0x0063)	40101 (0x0064) -- 40121 (0x0078)
长度	IP 或者域名值
00 0D	31 31 36 2E 36 32 2E 34 32 2E 31 39 32

端口 31687, 对应十六进制 7BC7; 协议类型 (TCP、UDP) 使用协议寄存器保存, 值 0x0001 对应 TCP 协议, 值 0x0000 对应 UDP 协议。即当 IP 为 116. 62. 42. 192, 端口为 31687, TCP 协议, 未使用到的 IP 或域名寄存器可以以“0”填充或者不填, 如果需要使用功能码“0x10”一次性写完 IP、域名、端口、协议类型, 那么未使用到的寄存器必须填充值, 才能连续写 modbus 寄存器, 对应的寄存器值如下表:

40100 (0x0063)	40101 (0x0064) -- 40121 (0x0078)	40122 (0x0079)	40123 (0x007A)
IP 或域名长度	IP 或者域名值	服务器端口	TCP 协议
00 0D	31 31 36 2E 36 32 2E 34 32 2E 31 39 32 00	7B C7	00 01

由于 IP 或者域名寄存器长度是大于 IP 或域名值的长度的, 因此在写 IP 寄存器时需要考虑 IP 或域名的长度, 即需要占用多少个寄存器。如将上述 IP 写入 modbus 寄存器:

Modbus RTU 协议写 Socket 寄存器:

发送	01	10	00 63	00 18	30	00 0D 31 31 36 2E 36 32 2E 34 32 2E 31 39 32 00 7B C7 00 01	7B F0
	设备 ModBus 地址	功能 码	地址	寄存器 长度	字节 数	写入值	CRC 校验码

接收	01	10	00 63	00 18	30 1D
	设备 ModBus 地址	功能码	地址	寄存器长度	CRC 校验码

Modbus TCP 协议写 Socket 寄存器:

发送	00 01	00 00	00 37	01	10	00 63	00 18	30	00 0D 31 31 36 2E 36 32 2E 34 32 2E 31 39 32 00 7B C7 00 01
	传输 标识	协议 标识	长度	单元 标识	功 能 码	地址	寄存器 长度	字 节 数	写入值

接收	00 01	00 00	00 06	01	10	00 63	00 18
	传输标识	协议标识	长度	单元 标识	功能码	地址	寄存器长度

4.4.2. 自定义注册包

自定义注册包可以为 ASCII 码或者 hex, hex 的长度不能大于 20 字节, ASCII 码长度不能大于 40 字节。自定义注册包第一个寄存

器用于存放注册包类型,值 0x0000 表示注册包为 hex 格式,值 0x0001 表示注册包为 ASCII 码格式,当值为 0x0001,注册包值为 ABCDEFGHIJ,对应的 ASCII 码值如下表注册包值。自定义注册包第二个寄存器用于存放注册包值的长度,注册包值长度为 10,对应十六进制为 0x0A。和 IP 寄存器一样,未使用的注册包值寄存器可以以“0”填充或者不填。

40124 (0x007B)	40125 (0x007C)	40126 (0x007D) -- 40145 (0x0090)	40146 (0x0091)
类型	长度	注册包值	注册包机制
00 01	00 0A	41 42 43 44 45 46 47 48 49 4A 00	00 01

注册包机制有 5 种模式:

注册包机制寄存器值 (0x0091)	对应功能说明
00 00	关闭注册包机制
00 01	在每一包发送到服务器的数据前加上 MAC/IMEI 作为注册包数据
00 02	在每一包发送到服务器的数据前加上自定义注册包数据
00 03	只有第一次连接到服务器时发送一个 MAC/IMEI 的注册包
00 04	只有第一次连接到服务器时发送一个用户自定义注册包

Modbus RTU 协议写注册包寄存器:

发送	01	10	00 7B	00 17	2E	00 01 00 0A 41 42 43 44 45 46 47 48 49 4A 00 01	00 F4
	设备 ModBus 地址	功能 码	地址	寄存器 长度	字节 数	写入值	CRC 校验码

接收	01	10	00 7B	00 17	F0 1E
	设备 ModBus 地址	功能码	地址	寄存器长度	CRC 校验码

Modbus TCP 协议写注册包寄存器:

发送	00 01	00 00	00 33	01	10	00 7B	00 17	2E	00 01 00 0A 41 42 43 44 45 46 47 48 49 4A 00 01
	传输 标识	协议 标识	长度	单元 标识	功 能 码	地址	寄存器 长度	字节 数	写入值
接收	00 01	00 00	00 06	01	10	00 7B	00 17		

	传输标识	协议标识	长度	单元标识	功能码	地址	寄存器长度
--	------	------	----	------	-----	----	-------

4.4.3. 心跳包

心跳包可以为 ASCII 码或者 hex, hex 的长度不能大于 20 字节, ASCII 码长度不能大于 40 字节。心跳包第一个寄存器用于存放心跳包数据类型, 值 0x0000 表示心跳包为 hex 格式, 值 0x0001 表示心跳包为 ASCII 码格式, 当值为 0x0000, 心跳包值为 0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09。心跳包第二个寄存器用于存放心跳包值的长度, 心跳包值长度为 10, 对应十进制 0x0A。和自定义注册包寄存器一样, 未使用的心跳包值寄存器可以以“0”填充或者不填。

40147 (0x0092)	40148 (0x0093)	40149 (0x0094) -- 40168 (0x00A7)
类型	长度	注册包值
00 00	00 0A	00 01 02 03 04 05 06 07 08 09 00

Modbus RTU 协议写注册包寄存器:

发送	01	10	00 92	00 16	2C	00 00 00 0A 00 01 02 03 04 05 06 07 08 09 00	52 9E
	设备 ModBus 地址	功能 码	地址	寄存器 长度	字节 数	写入值	CRC 校验码

接收	01	10	00 92	00 16	E0 2A
	设备 ModBus 地址	功能码	地址	寄存器长度	CRC 校验码

Modbus TCP 协议写注册包寄存器:

发送	00 01	00 00	00 33	01	10	00 92	00 16	2C	00 00 00 0A 00 01 02 03 04 05 06 07 08 09 00
	传输标识	协议标识	长度	单元标识	功能码	地址	寄存器长度	字节数	写入值

接收	00 01	00 00	00 06	01	10	00 92	00 16
	传输标识	协议标识	长度	单元标识	功能码	地址	寄存器长度

4.4.4. 心跳包时间

心跳包时间设置范围为 0-65535 秒，当心跳包时间设置为 0 时，即关闭心跳包。如下设置心跳包时长为 5s。

Modbus RTU 协议写心跳包时间寄存器：

发送	01	06	00 A8	00 05	C8 29
	设备 ModBus 地址	功能码	地址	写入值	CRC 校验码

接收	01	06	00 A8	00 05	C8 29
	设备 ModBus 地址	功能码	地址	写入值	CRC 校验码

Modbus TCP 协议 Modbus RTU 协议写心跳包时间寄存器：

发送	00 01	00 00	00 06	01	06	00 A8	00 05
	传输标识	协议标识	长度	单元标识	功能码	地址	写入值

接收	00 01	00 00	00 06	01	06	00 A8	00 05
	传输标识	协议标识	长度	单元标识	功能码	地址	写入值

4.4.5. IMEI 读取

IMEI 寄存器读取起始地址为 40171 (0x00AA)，寄存器总长度为 11，其中，第一个寄存器为 IMEI 长度，第二个寄存器到第十一个寄存器存储 IMEI 值。如 IMEI:867732035802677，对应的寄存器值如下表，在寄存器中，IMEI 值以十六进制的 ASCII 值存在。

40171 (0x00AA)	40172 (0x00AB) --40181 (0x00B4)
IMEI 长度	IMEI 值
00 0F	38 36 37 37 33 32 30 33 35 38 30 32 36 37 37 00 00 00 00 00

4.4.6. SN 读取

SN 寄存器读取起始地址为 40182 (0x00B5)，寄存器总长度为 11，其中，第一个寄存器为 SN 长度，第二个寄存器到第十一个寄存器存储 SN 值。如 SN:181101194228B027，对应的寄存器值如下表，在寄存器中，SN 值以十六进制的 ASCII 值存在。

40182 (0x00B5)	40183 (0x00B6) --40192 (0x00BF)
SN 长度	SN 值
00 10	31 38 31 31 30 31 31 39 34 32 32 38 42 30 32 37

4.4.7. 基站定位值 LBS 读取

基站定位寄存器读取起始地址为 40193 (0x00C0)，寄存器总长度为 20，其中，第一个寄存器为基站定位信息长度，第二个寄存器到第二十一个寄存器存储基站定位值。如基站定位值 LAC:812F, CID:8056B08，对应的寄存器值如下表，在寄存器中，基站定位值以十六进

制的 ASCII 值存在。

40193 (0x00C0)	40194 (0x00C1) --40213 (0x00D4)
基站定位值长度	基站定位值
00 14	4C 41 43 3A 38 31 32 46 2C 43 49 44 3A 38 30 35 36 42 30 38

5、 重要声明

- 亿佰特保留对本说明书中所有内容的最终解释权及修改权。
- 由于随着产品的硬件及软件的不断改进，本说明书可能会有所更改，恕不另行告知，最终应以最新版的说明书为准。
- 保护环境，人人有责：为减少纸张使用，本说明书只印刷中文部分，英文说明书只提供电子文档，若有需要，请到我司官网下载；另外，若非用户特别要求，用户批量订货时，我们只按订货数量的一定比例提供产品说明书，并非每个数传电台都一一配上，敬请谅解。

6、 修订历史

版本	修订日期	修订说明	维护人
1.2	2025-05-06	版本修改	Blue



销售热线：4000-330-990（24 小时可拨打）

官方网址：www.ebyte.com

公司地址：四川省成都市高新西区西区大道 199 号 B5 栋

ISO9001:2008

ISO14001:2004

成都亿佰特电子科技有限公司保留对本说明中所有内容的最终解释

