

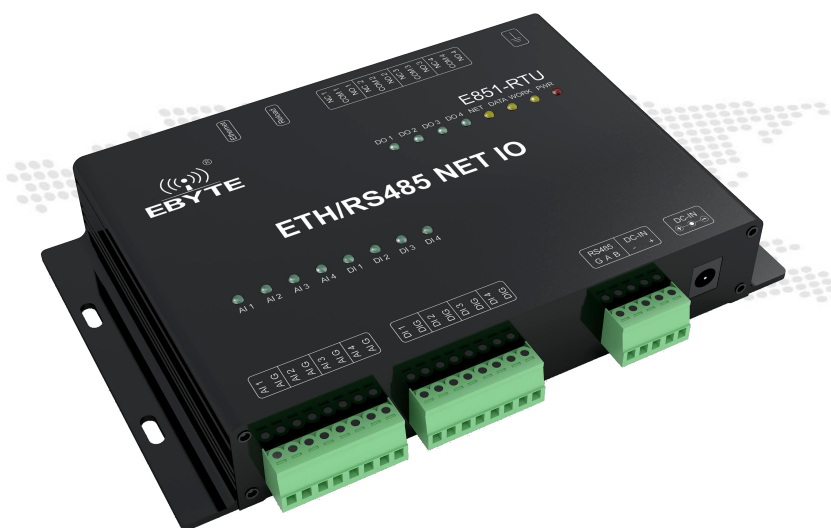


Chengdu Ebyte Electronic Technology Co.,Ltd

Wireless Modem

User Manual

E851-RTU(4440-ETH) User Manual



All rights to interpret and modify this manual belong to
Chengdu Ebyte Electronic Technology Co., Ltd.

Contents

1. Quick Start.....	3
1.1. Port connection.....	3
1.1.1. RS485 connection.....	3
1.1.2. Switch Input Connection.....	4
1.1.3. Relay output connection.....	4
1.1.4. Differential analog input connection.....	4
1.2. Quick Use.....	5
2. Product Introduction.....	7
2.1. Basic parameters.....	7
2.2. Size, interface description.....	8
2.3. Reload touch button description.....	11
3. Modbus.....	11
3.1. Modbus address table.....	11
3.2. Modbus Address Table.....	12
3.3. RS485 Serial Port Baud Rate Code Table.....	13
4. Product Function.....	14
4.1. Working mode.....	14
4.1.1. Slave mode.....	14
4.1.2. Host mode.....	15
4.2. Basic functions of IO.....	16
4.2.1. Switch DO Output.....	16
4.2.2. Read switch DI input.....	18
4.2.3. Read analog AI input.....	19
4.2.4. Analog AI range setting.....	21
4.3. IO Feature Function.....	21
4.3.1. Pulse count and count clear.....	21
4.3.2. Switching input DI is automatically reported.....	22
4.3.3. DO Time Settings for Switch Output.....	23
4.4 Network related functions.....	24
4.4.2. Custom registration package.....	25
4.4.3. Heartbeat package.....	27
4.4.4. Heartbeat packet time.....	28
4.4.5. Heartbeat packet mode.....	29
4.4.6. IP parameter setting of local WAN port.....	30
4.4.7. DNS settings.....	31
4.4.8. Ebyte Cloud Transparent Transmission.....	32
4.4.9. Clear cache.....	32
4.4.10. Keep alive connection.....	32
4.4.11. Timeout restart.....	33
4.4.12. SOCKET Local Port Settings.....	33
Important statement.....	34
Revision History.....	34

Features

- Support 4 differential analog inputs, default current detection;
- Supports 4-way digital input, dry contact as default ;
- Support 4-way relay output;
- Support socket connection to remote server, support TCP Client;
- Data processing using Modbus TCP/RTU protocol;
- Support connection to Ebyte cloud, command control;
- Support two working modes, host mode, slave mode, slave can connect to multiple devices through RS485;
- Support reload touch button, long press 5s, Modbus device address, RS485 serial baud rate and check digit to restore factory settings;
- Hardware watchdog with high reliability;
- Multiple indicator lights show working status.
- The power supply has good functions of over-current, over-voltage and anti-backconnection.

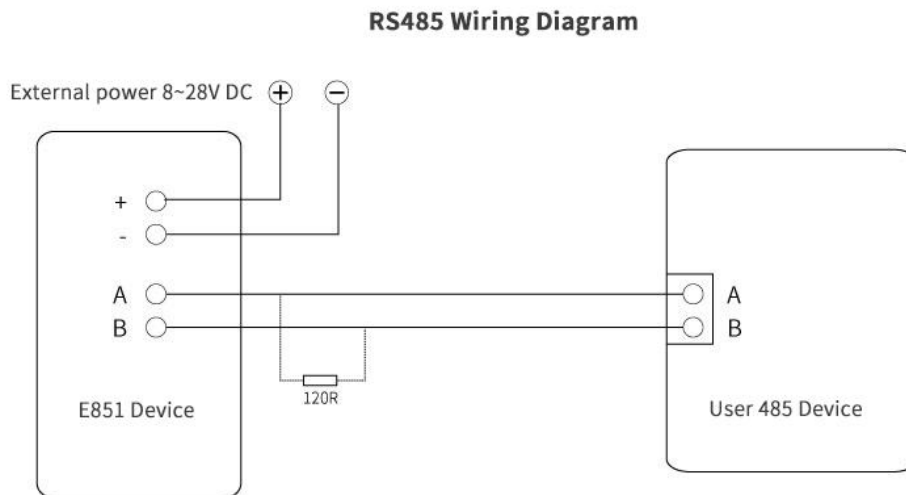
Note: Customization functions are available, such as conditional control (how to output based on input state)

1. Quick Start

This chapter is a quick introduction to E851-RTU (4440-ETH) series products. It is recommended that users read this chapter systematically and operate it according to the instructions. It will have a systematic understanding of the module products. Users can also choose the chapters you are interested in to read according to their needs. For specific details and instructions, please refer to the following chapters.

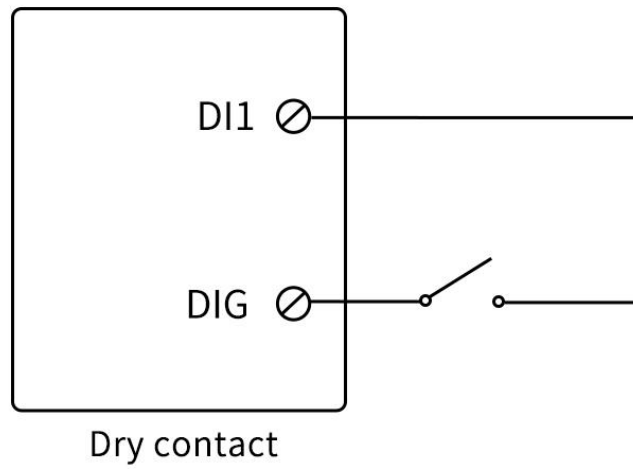
1.1. Port connection

1.1.1. RS485 connection

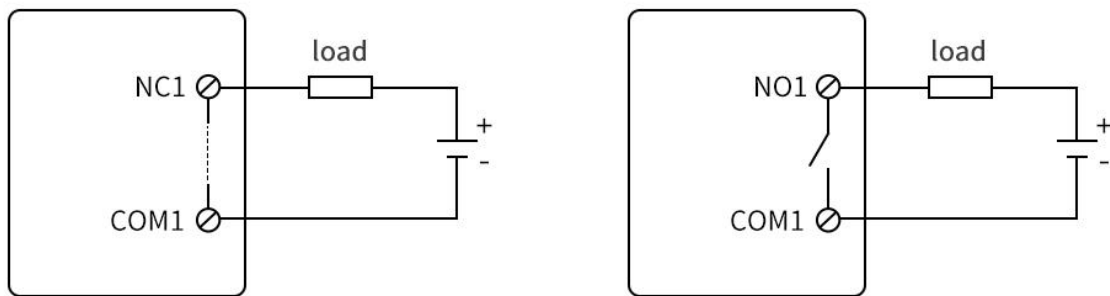


Note: When the 485 bus high frequency signal is transmitted, the signal wavelength is shorter than the transmission line. The reflected wave will form at the terminal of the transmission line and interfere with the original signal. Therefore, terminal resistance should be added at the end of the transmission line so that the signal will not reflect when it reaches the end of the transmission line. The terminal resistance should be the same as the impedance of the communication cable with a typical value of 120 ohms. Its function is to match the bus impedance and improve the anti-interference and reliability of data communication.

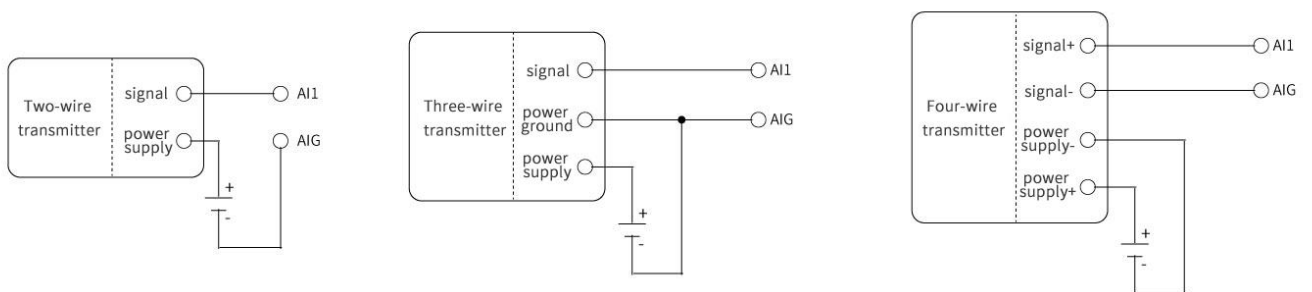
1.1.2. Switch Input Connection



1.1.3. Relay output connection



1.1.4. Differential analog input connection



1.2. Quick Use

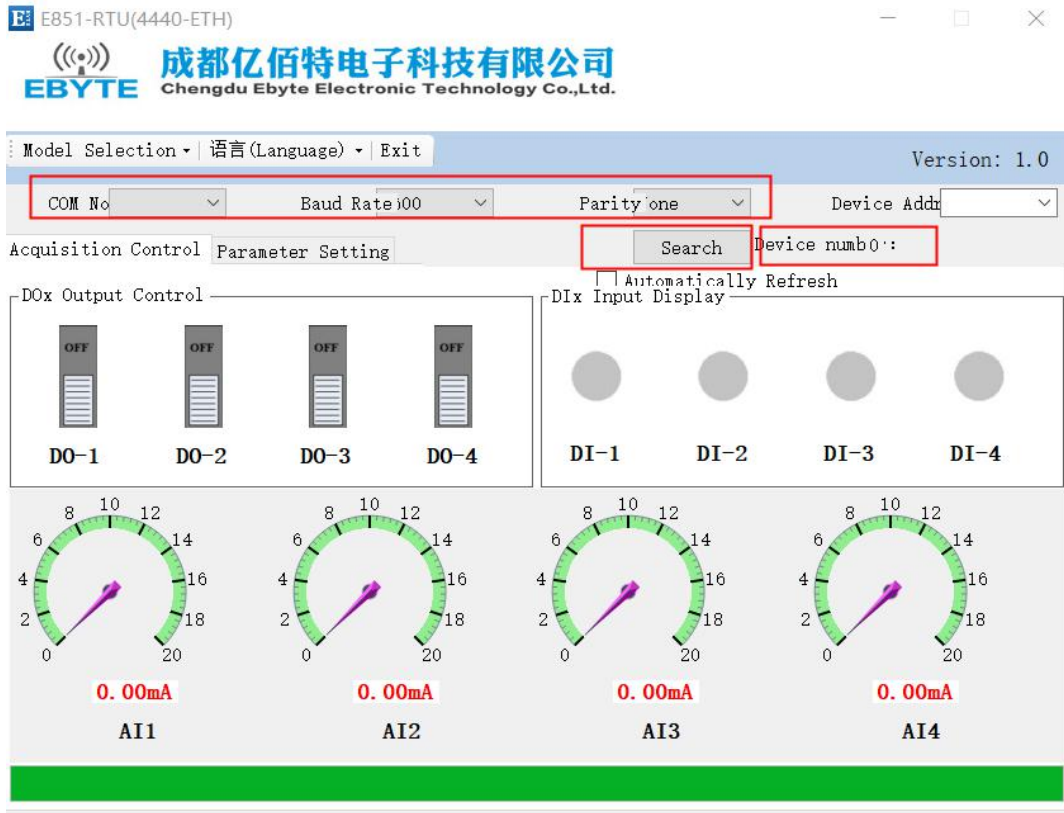
Wiring: Computer connects to E851-RTU (4440-ETH) via USB to RS485

Networking: Plug the network cable into the RJ45 port

Power supply: E851-RTU (4440-ETH) working voltage is DC 8~28V

1.2.1. RS485 Bus Control

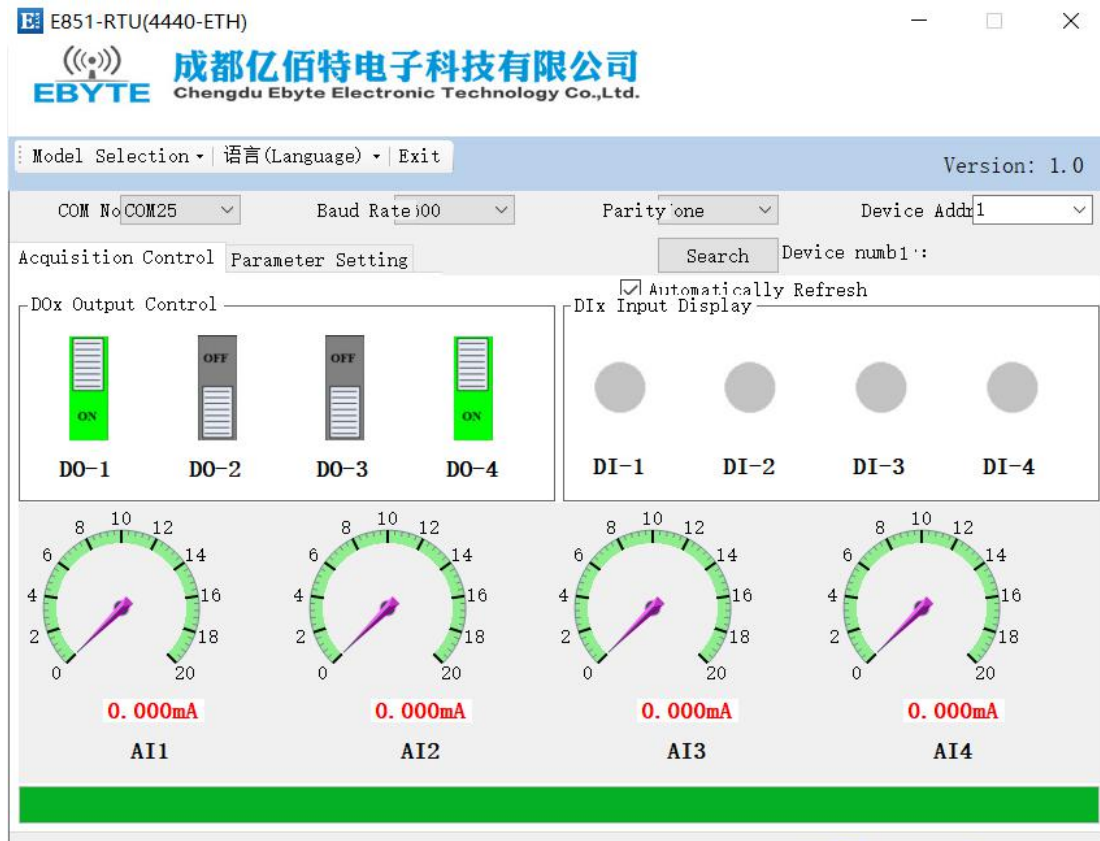
Select the appropriate port and click “Search” to search for the device.



After searching for the device, click “Stop”.



At this time, the device address of the current device can be seen, and the "auto refresh" processing can be performed, and the switch output control, the digital input read, and the differential analog input can be read.



1.2.2. Network control

Input http://yun.cdebyte.com/www/data_direct, The acquisition can be controlled by command, which adopts Modbus TCP/RTU protocol.

The screenshot shows a web interface for network control. It has a dark header bar with a refresh icon. Below the header, there are two main sections: '发送数据' (Send Data) and '接收数据' (Receive Data). The '发送数据' section contains a text input field labeled '输入发送数据'. Below this, there are two dropdown menus for '格式' (Format) and '显示格式' (Display Format), both set to '16进制数据(空格分隔)'. To the right of each dropdown is a button: '发送' (Send) for the format dropdown and '清除' (Clear) for the display format dropdown. The '接收数据' section is currently empty.

2. Product Introduction

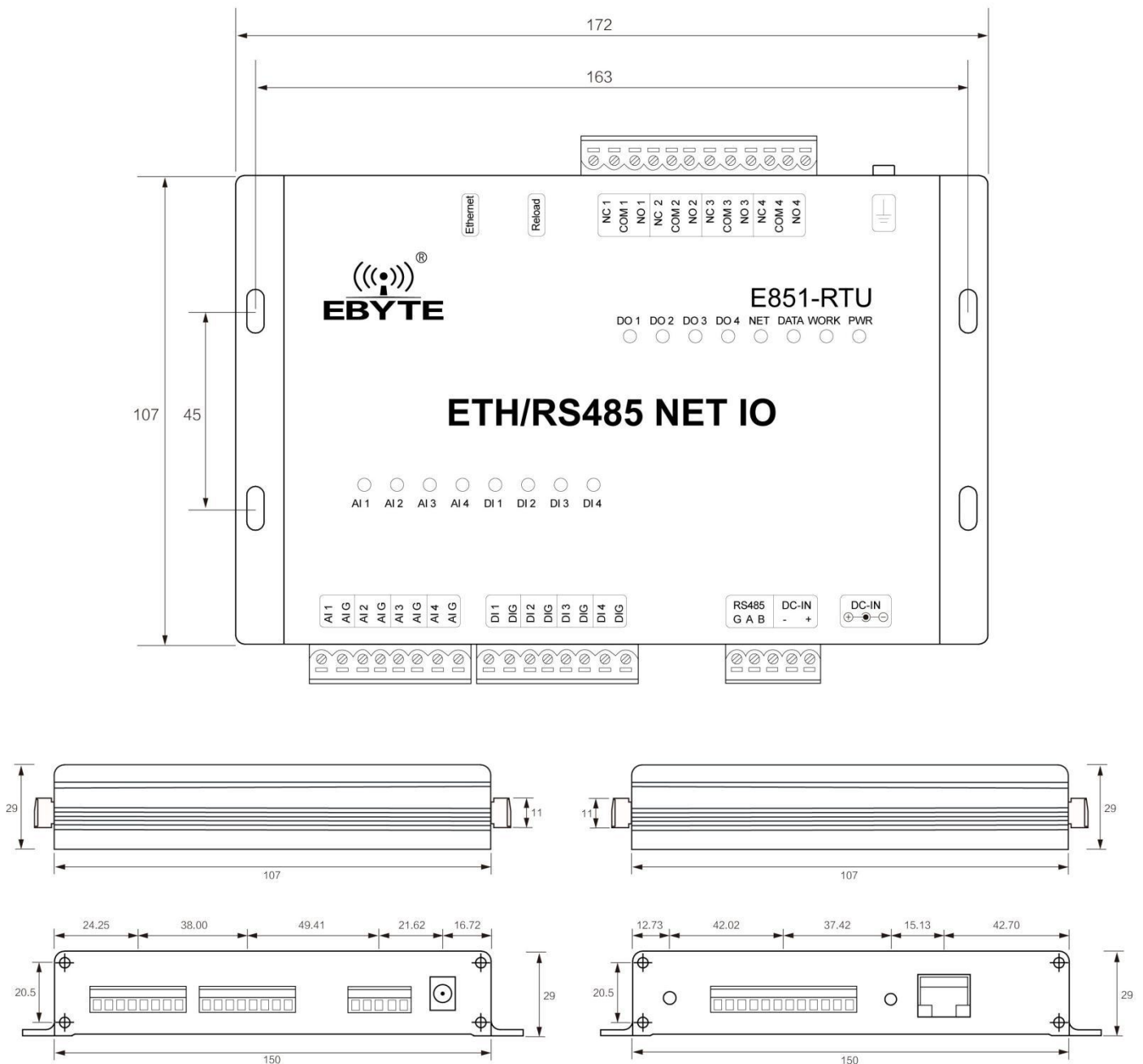
E851-RTU (4440-ETH) is a network IO product that supports 4-way digital input (default trunk connection), 4-way differential analog input and 4-way relay output. Support Modbus TCP/RTU protocol. The product is highly user-friendly, and users can easily and quickly integrate into their own systems to achieve remote control based on Ethernet.

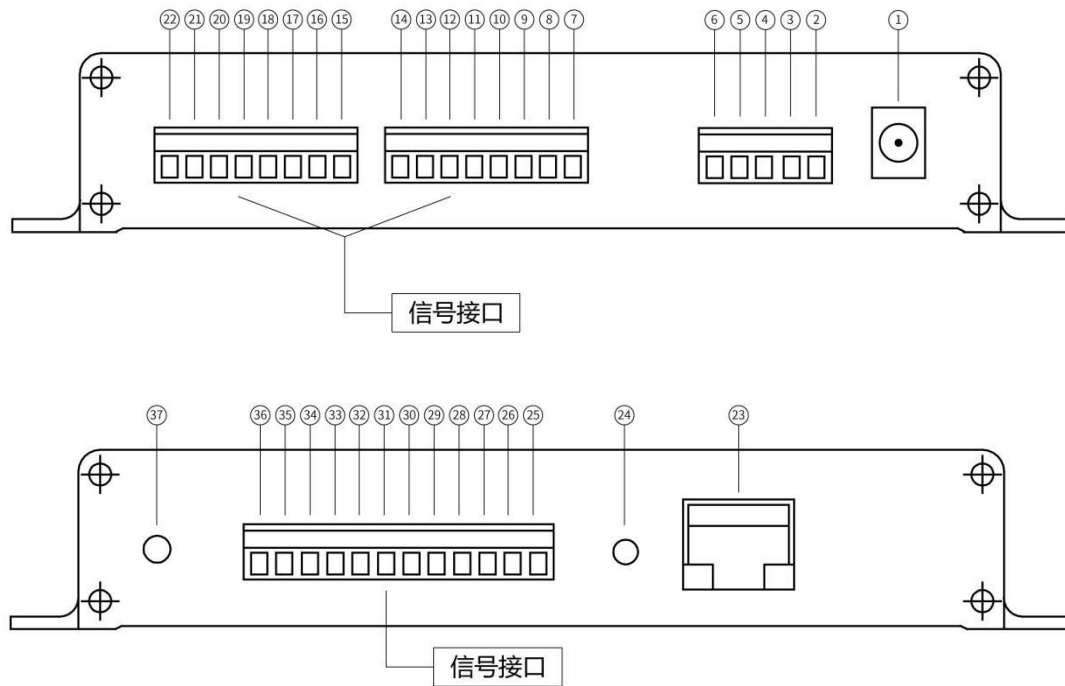
2.1. Basic parameters

	Name	Value
Hardware parameters	Product size(H*W*D)	172*107*29mm
	Product weight	457.5±5g
	Working temperature	-20°C~+70°C
	Storage temperature	-40°C~+85°C
	Working humidity	5%~95%
	Storage humidity	1%~95%
	Working voltage	8V~28V
	Current acquisition range	0mA~20mA
	Precision	0.2%
	Data interface	RS485: 1200~115200bps

Software parameters	Network Type	Ethernet
	Configuration command	Modbus TCP/RTU
	Network protocol	Modbus TCP/RTU
	Working mode	Host mode、Slave mode
	Data transmission mode	TCP Client

2.2. Size, interface description





SN	Ports	Function	Illustration
1	DC-IN transposon	DC socket 5.5*2.1mm	Power input, DC 8V~28V, 12V/24V is recommended, cannot be powered with the crimp terminal at the same time
2	DC-IN +	Crimped power input positive	power input, DC 8V~28V, 12V/24V is recommended, cannot be powered with the DC socket at the same time
3	DC-IN -	Crimped power input negative	Power reference ground
4	RS485 B	RS485 interface B	RS485 interface B is connected with device B interface
5	RS485 A	RS485 interface A	RS485 interface A is connected with device A interface
6	RS485 G	Signal reference	can be unconnected
7	DIG	Switching input	Can be used in pairs with DI 4
8	DI 4	Switch input channel 4	Form dry contact with DIG
9	DIG	Switching input	Can be used in pairs with DI 3
10	DI 3	Switch Input Channel 3	Form dry contact with DIG
11	DIG	Switching input	Can be used in pairs with DI 2
12	DI 2	Switch Input Channel 2	Form dry contact with DIG
13	DIG	Switching input	Can be used in pairs with DI 1
14	DI 1	Switch Input Channel 1	Form dry contact with DIG
15	AIG	Differential analogue input	Can be used in pairs with AI 4
16	AI 4	Differential analog input channel 4	Differential analog input pin, forming input with AIG

17	AIG	Differential analogue input	Can be used in pairs with AI 3
18	AI 3	Differential analog input channel 3	Differential analog input pin, forming input with AIG
19	AIG	Differential analogue input	Can be used in pairs with AI 2
20	AI 2	Differential analog input channel 2	Differential analog input pin, forming input with AIG
21	AIG	Differential analogue input	Can be used in pairs with AI 1
22	AI 1	Differential analog input channel 1	Differential analog input pin, forming input with AIG
23	Ethernet	Mesh port	Ethernet Connection Port
24	Reload	Reset button	Long press 5s to work
25	NC 1	Normally closed pin of Relay 1	Cooperate with common end of relay 1
26	COM 1	Relay 1 Common End	Cooperate with the normally open/closed pin of relay 1
27	NO 1	Normally open pin of Relay 1	Cooperate with common end of relay 1
28	NC 2	Normally closed pin of Relay 2	Cooperate with common end of relay 2
29	COM 2	Relay 2 Common End	Cooperate with the normally open/closed pin of relay 2
30	NO 2	Normally open pin of Relay 2	Cooperate with common end of relay 2
31	NC 3	Normally closed pin of Relay 3	Cooperate with common end of relay 3
32	COM 3	Relay 3 Common End	Cooperate with the normally open/closed pin of relay 3
33	NO 3	Normally open pin of Relay 3	Cooperate with common end of relay 3
34	NC 4	Normally closed pin of Relay 4	Cooperate with common end of relay 4
35	COM 4	Relay 4 Common End	Cooperate with the normally open/closed pin of relay 4
36	NO 4	Normally open pin of Relay 4	Cooperate with common end of relay 4
37	Ground screw	Connected to the earth	Connected to the earth
LED light			
AI 1	Differential analog input channel 1 indication	Green LED, lights up when input $\geq 0.5\text{mA}$	
AI 2	Differential analog input channel 2 indication	Green LED, lights up when input $\geq 0.5\text{mA}$	
AI 3	Differential analog input channel 3 indication	Green LED, lights up when input $\geq 0.5\text{mA}$	
AI 4	Differential analog input channel 4 indication	Green LED, lights up when input $\geq 0.5\text{mA}$	
DI 1	Switch Input Channel 1 indication	Green LED,lights up when DI 1、DIG short connect	
DI 2	Switch Input Channel 2 indication	Green LED,lights up when DI 2、DIG short connect	
DI 3	Switch Input Channel 3 indication	Green LED,lights up when DI 3、DIG short connect	
DI 4	Switch Input Channel 4 indication	Green LED,lights up when DI 4、DIG short connect	
DO 1	Relay 1 output indication	Green LED,lights up when NO 1, COM 1 closed	
DO 2	Relay 2 output indication	Green LED,lights up when NO 2, COM 2 closed	
DO 3	Relay 3 output indication	Green LED,lights up when NO 3, COM 3 closed	

DO 4	Relay 4 output indication	Green LED,lights up when NO 4, COM 4 closed
NET	Network indication	Yellow LED, long bright after entering the network
DATA	Serial data indication	Yellow LED, lights up when there's data transmitted in RS485 interface (expressively flashes)
WORK	Work/reset indication	Yellow LED, flashing regularly / flashing after successful reset
PWR	Power indicator	Red LED, long bright

Note:

Grounding: It is recommended to connect the housing to the ground.

2.3. Reload touch button description

Long press 5S is valid, after the reset is successful, the WORK lamp flashes quickly, and the Modbus device address, RS485 serial port baud rate and check digit are restored to the factory settings.

3. Modbus

3.1. Modbus address table

Register address table (function code: 0x01H、0x05H、0x0FH、0x03H、0x06H、0x10H)					
Register address	Register quantity	Register attribute	Register type	Register value range	Support function code
00017 (0x0010)	1	DO1 Switch Output	Read / write	0x0000 or 0xFF00 (0x05function code) 0-1 (0x01、0x0Ffunction code)	0x01 0x05 0x0F
00018 (0x0011)	1	DO2 Switch Output	Read / write		
00019 (0x0012)	1	DO3 Switch Output	Read / write		
00020 (0x0013)	1	DO4 Switch Output	Read / write		
Reserve					
10017 (0x0010)	1	DI1 Switch input	Read only	0-1	0x02
10018 (0x0011)	1	DI2 Switch input	Read only		
10019 (0x0012)	1	DI3 Switch input	Read only		
10020 (0x0013)	1	DI4 Switch input	Read only		
Reserve					
30017 (0x0010)	1	AI1 input value, Unit(uA)	Read only	0-20000	0x03 0x04
30018 (0x0011)	1	AI2 input value, Unit(uA)	Read only		
30019 (0x0012)	1	AI3 input value, Unit(uA)	Read only		
30020 (0x0013)	1	AI4 input value, Unit(uA)	Read only		
Reserve					
40049 (0x0030)	1	DI1 pulse counting value	Read only	0-65535	0x03
40050 (0x0031)	1	DI2 pulse counting value	Read only	0-65535	
40051 (0x0032)	1	DI3 pulse counting value	Read only	0-65535	
40052 (0x0033)	1	DI4 pulse counting value	Read only	0-65535	
Reserve					

40065 (0x0040)	1	DI1-DI4 Pulse count clear	Write only	0x00 - 0x0F	0x06
Reserve					
40078 (0x004D)	1	Device address	Read/write	1 - 247	0x03 0x06 0x10
40079 (0x004E)	1	Baud rate	Read/write	0 - 7	
40080 (0x004F)	1	Parity bit	Read/write	0 - 2	
40081(0x0050)	1	Host mode or slave mode	Read/write	0 - 1	
40082 (0x0051)	1	Automatic report of switch qty	Read/write	0 - 2	
40083 (0x0052)	1	Switch output time setting (ms)	Read/write	300-65535	
40084(0x0053)	1	Analog range setting	Read/write	0 - 1	
40085 (0x0054)	1	Switch restart output status setting	Read/write	0x00 - 0x10	
Reserve					
40100 (0x0063)	22	Server IP or domain name (domain name ASCII)	Read/write	--	0x03 0x06 0x10
40122 (0x0079)	1	Server Port	Read/write	1 - 65535	
40123 (0x007A)	1	Protocol type (UDP、TCP)	Read/write	0 - 1	
40124(0x007B)	22	Custom registration package	Read/write	--	
40146(0x0091)	1	Registration package mechanism	Read/write	0 - 4	
40147(0x0092)	22	Heartbeat package	Read/write	--	
40169 (0x00A8)	1	Heartbeat packet time	Read/write	0 - 65535	
40170 (0x00A9)	1	Heartbeat packet mode	Read/write	0 - 1	
40171 (0x00AA)	1	Cloud transparent transmission	Read/write	0 -1	
40172 (0x00AB)	3	Active connection	Read/write	0, 2-7200	
40173 (0x00AE)	1	Ethernet timeout restart	Read/write	0, 60-65535	
40174 (0x00AF)	1	Clear cache	Read/write	0 - 1	
40175 (0x00B0)	1	Local port number	Read/write	0-65535	
40176 (0x00B1)	1	IP acquisition method	Read/write	0 -1	
40177 (0x00B2)	11	Local IP address	Read/write	--	
40188 (0x00BD)	11	Subnet mask	Read/write	--	
40199 (0x00C8)	11	Gateway	Read/write	--	
40210 (0x00D3)	11	Preferred DNS	Read/write	--	
40221(0x00DE)	11	Standby DNS	Read/write	--	
40232 (0x00E9)	11	MAC value	Read only	--	0x03
40243 (0x00F4)	11	SN code value	Read only	--	
Reserve					
40300(0x012B)	1	version number	Read only	--	0x03

3.2. Modbus Address Table

Modbus address table	
1 (default)	1

2	2
3	3
...	...
245	245
246	246
247	247

3.3. RS485 Serial Port Baud Rate Code Table

Baud Rate Code Table	
0	1200
1	2400
2	4800
3 (default)	9600
4	19200
5	38400
6	57600
7	115200

3.4. RS485 serial port check bit value table

check bit value table	
0 (default)	No check
1	even parity check
2	Odd parity check

3.5. Host computer configuration parameters

Select the "Parameter Settings" column, you can read parameters, write parameters. For the specific realization of functions, see the product functions described below.

E851-RTU(4440-ETH)

成都亿佰特电子科技有限公司
Chengdu Ebyte Electronic Technology Co.,Ltd.

Model Selection | 语言(Language) | Exit Version: 1.0

COM No: COM25 Baud Rate: 9600 Parity: none Device Addr: 1

Acquisition Control Parameter Setting Search Device num1:

Modbus Address: 1 RS485 Baud Rate: 9600 IP Address Access: STATIC IP

Mode Choose: Slaver Mode RS485 Parity: None Local port: 0

DI Auto Upload: Auto Upload By AI Input Range: 4-20mA Local IP: 192.168.1.192

DO Restart: Hold The Last DO Hold Time: 10 SubNetMask: 255.255.255.0

Protocol Type: TCP Cloud: Close Default Gateway: 192.168.1.1

Server Port: 31687 Heartbeat: 0 Prefer DNS: 168.32.43.195

Keep alive: Close Setting Timeout restart: 0 Alternative DNS: 168.33.55.168

Heartbeat mode: Serial heartbeat

Server IP Or Domain: 116.62.42.192 Clear cache: No

Connreg Mode: 0x0000, Close the Connreg

SN: 1905211400491D68

MAC: B2FAEAF1FF30 Hex

Heartbeat: 00 01 02 03 04 05 06 07 08 09

Connreg: ABCDEFGHIJ

Read Parameter Write Parameter

4. Product Function

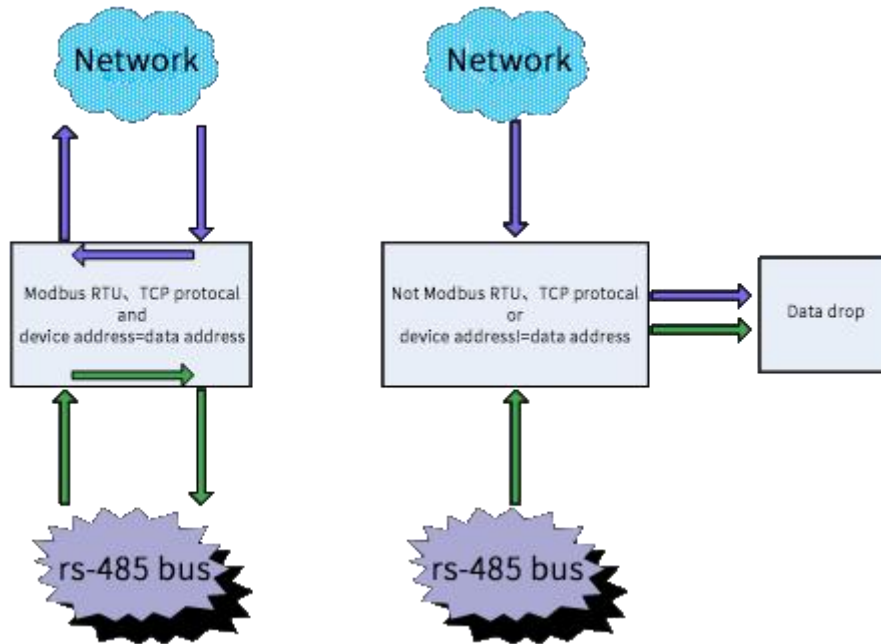
4.1. Working mode

The working mode has host mode and slave mode, which is configured by Modbus register 40081 (0x0050). It will be Host mode when the register value is 0; slave mode when the register value is 1, default slave mode.

4.1.1. Slave mode

In slave mode (register value 0x01), the data sent to the device by the network or 485 terminal (sender) satisfies the Modbus RTU, Modbus TCP protocol, and the address in the data is the device address, and the device will reply with the same protocol. If the data sent by the network or 485 bus to the device does not satisfy the Modbus RTU, Modbus TCP protocol, or the Modbus RTU or Modbus TCP protocol is met but the data address is not the device address, the data of the sender will be discarded.

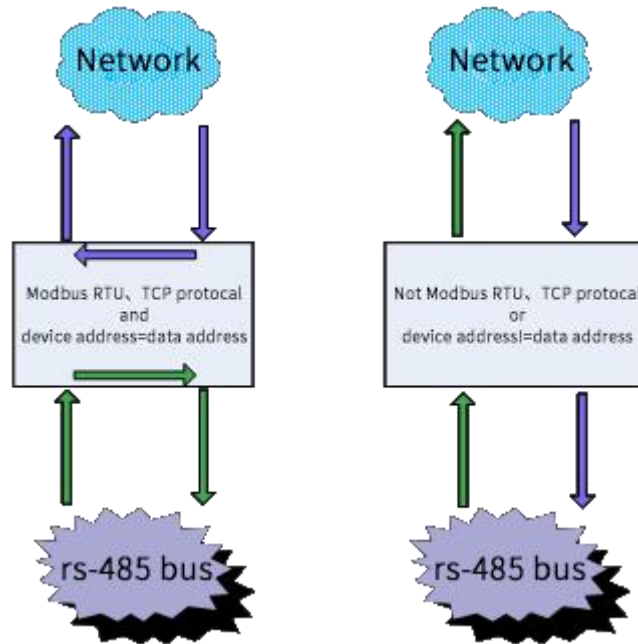
In slave mode, the device can connect to the device in host mode directly through 485 bus, so that the data of slave can also be accessed by the network terminal when the slave is not connected to the network.



4.1.2. Host mode

In host mode (register value is 0x00), the data sent by the network or 485 bus (transmitter) to the device satisfies the Modbus RTU, Modbus TCP protocol, and the address in the data is the device address, and the device responds to the sender with the same protocol. If the data sent by the network or 485 bus to the device does not satisfy the Modbus RTU, Modbus TCP protocol, or satisfy the Modbus RTU, Modbus TCP protocol but the data address is not the device address, the data from the 485 bus will be transmitted to the network, and the data from the network will be transmitted to the 485 bus.

This function of host mode can realize the cascade function of devices and the data transmission between 485 bus and network.



4.2. Basic functions of IO

4.2.1. Switch DO Output

4.2.1.1 Read Switch DO Output

Function code: 01, read coil status

Address range: 00017 (0x0010) ~ 00020 (0x0013)

Explanation: When equipment relay passive output and coil is not powered on, relay NC port and COM port are usually closed, NO port and COM port are often open, with a value of 0; when coil is energized, the phenomenon is opposite, relay NC port and COM port are disconnected, NO port and COM port are closed, with a value of 1. Query relay status by instruction.

Example:

Read the 4-way switch output state, assuming a return value of 03, corresponding to the binary bit 0000 0011, the lower four bits and four bits represent the switch output state, which in turn is DO4, DO3, DO2, DO1.

Modbus RTU protocol reads switching output:

Transmit	01	01	00 10	00 04	3C 0C
	Device ModBus address	Function code	Switch start address	Read switch quantity	CRC check code

Receive	01	01	01	03	11 89
	Device ModBus address	Function code	Return bytes	Switch output value	CRC check code

Modbus TCP protocol reads switching output:

Transmit	00 01	00 00	00 06	01	01	00 10	00 04
	Transmission identifier	Protocol identifier	length	Unit identification	Function code	Switch start address	Read switch quantity

Receive	00 01	00 00	00 04	01	01	01	03
	Transmission identifier	Protocol identifier	length	Unit identification	Function code	Return bytes	Switch Output Value

4.2.1.2. Control switch quantity DO output

Function code: 05, write single coil state; 0F, write multiple coil state

Address range: 00017 (0x0010) ~00020 (0x0013)

Description: Equipment relay passive output, coil is not energized, relay NC port and COM port are closed, NO port and COM port are disconnected; coil is energized, relay NC port and COM port are disconnected, NO port and COM port are closed. The state of relay is controlled by command.

Example:

Function code 0x05 write DO2 switch output, make NC2, COM2 open, NO2, COM2 close, write value is FF 00; make NC2, COM2 close, NO2, COM2 open, write value 00 00.

Modbus RTU protocol write switch output:

Transmit	01	05	00 11	FF 00	DC 3F
	Device ModBus address	Function code	Switching address	Write value	CRC check code

Receive	01	05	00 11	FF 00	DC 3F
	Device ModBus address	Function code	Switching address	Write value	CRC check code

Modbus TCP protocol write switch output:

Transmit	00 01	00 00	00 06	01	05	00 11	FF 00
	Transmission identifier	Protocol identifier	length	element ID	Function code	Switching address	Write value

Receive	00 01	00 00	00 06	01	05	00 11	FF 00
	Transmission identifier	Protocol identifier	length	element ID	Function code	Switching address	Write value

Function code 0x0F writes DO2, DO3 switch output, making NC2, COM2 disconnected, NO2, COM2 closed; NC3, COM3 disconnected, NO3, COM3 closed. Write value should be 0x03, corresponding to binary bit 0000 0011

Modbus RTU protocol write switch output:

	01	0F	00 11	00 02	01	03	62 95
Transmit	Device ModBus address	Function code	Switching address	Write switch quantity	Bytes	Write value	CRC check code

Receive	01	0F	00 11	00 02	84 0F
	Device ModBus address	Function code	Switching address	Write value	CRC check code

Modbus TCP Write Switch Output:

	00 01	00 00	00 08	01	0F	00 11	00 02	01	03
Transmit	Transmission identifier	Protocol identifier	length	element ID	Function code	Switching address	Write Switch Quantity	Bytes	Write value

Receive	00 01	00 00	00 06	01	0F	00 11	00 02
	Transmission identifier	Protocol identifier	length	element ID	Function code	Switching address	Write Switch Quantity

4.2.2. Read switch DI input

Function Code: 02, Read (Switch) Input Status

Address range: 10017 (0x0010) ~10020 (0x0013)

Description: Default Dry Contact Input for Device, when DI and COM are short connected, the read value should be 1; when DI and COM are not short connected, the read value should be 0.

Example:

Read 4 way switch input value, In DI input terminal, DI1, COM1 short connection, DI2, COM2 are not short connection, DI3, COM3 short connection, DI4, COM4 are not short connection. The input digital input value is 0x05, corresponding to the binary bit 0000 0101, and the four bits of the lower four bits represent the digital input value, which are in turn DI4, DI3, DI2, DI1.

Modbus RTU protocol reads switching input:

	01	02	00 10	00 04	78 0C
Transmit	Device ModBus address	Function code	Switch start address	Read the quantity of switches	CRC check code

	01	02	01	05	61 8B
Receive	Device ModBus address	Function code	Return bytes	Switch Input Value	CRC check code

Modbus TCP protocol reads switch input:

	00 01	00 00	00 06	01	02	00 10	00 04
Transmit	Transmission identifier	Protocol identifier	length	element ID	Function code	Switch start address	Read the quantity of switches

	00 01	00 00	00 04	01	02	01	05
Receive	Transmission identifier	Protocol identifier	length	element ID	Function code	Return bytes	Switch Input Value

4.2.3. Read analog AI input

Function code: 03, read holding register; 04, read input register

Address range: 30017 (0x0010) ~30020 (0x0013)

Note: The input unit of differential analogue is uA.

Example:

Function code 0x03, read AI1 input, assuming AI1 input is 9946uA, the corresponding value should be 0x0x26DA

The Modbus RTU protocol reads the differential analog input:

	01	03	00 10	00 01	85 CF
Transmit	Device ModBus address	Function code	Analog start address	Read quantity	CRC check code

	01	03	02	26 DA	23 BF
Receive	Device ModBus address	Function code	Return bytes	Input value of differential analogue	CRC check code

Modbus TCP protocol reads differential analog input:

Transmit	00 01	00 00	00 06	01	03	00 10	00 01
	Transmission identifier	Protocol identifier	length	element ID	Function code	Analog start address	Read quantity

Receive	00 01	00 00	00 05	01	03	02	26 DA
	Transmission identifier	Protocol identifier	length	element ID	Function code	Return bytes	Input value of differential analogue

Function code 0x04, read AI1 input, assuming AI1 input is 9946uA, the corresponding value should be 0x0x26DA

Modbus RTU protocol reads differential analog input:

Transmit	01	04	00 10	00 01	30 0F
	Device ModBus address	Function code	Analog Start Address	Read quantity	CRC check code

Receive	01	04	02	26 DA	22 CB
	Device ModBus address	Function code	Return bytes	Differential analog input value	CRC check code

Modbus TCP protocol reads differential analog input:

Transmit	00 01	00 00	00 06	01	04	00 10	00 01
	Transmission identifier	Protocol identifier	length	element ID	Function code	Analog Start Address	Read quantity

Receive	00 01	00 00	00 05	01	04	02	26 DA
	Transmission identifier	Protocol identifier	length	element ID	Function code	Return bytes	Differential analog input value

4.2.4. Analog AI range setting

When the value of register 0x40084 (0x0053) is 0, the differential analog input range is 0 -- 20mA;

When the value of register 0x40084 (0x0053) is 1, the differential analog input range is 4 - 20mA;

4.3. IO Feature Function

4.3.1.Pulse count and count clear

The pulse counting will not be saved after power off. The maintenance time of the pulse level must be longer than 10ms before it is valid. Switch input changes from open state to closed state and maintains a close time of more than 10 ms, then to open state, completing a pulse count.

4.3.1.1 Read pulse count value

Function code: 03, read hold register

Address range: 40049 (0x0030)~40052 (0x0033)

Description: The maximum pulse count is 65535

Example:

DI1 has detected 16 pulses at present, DI2 has detected 3 pulses at present, and reads the DI1 and DI2 switch input count values.

Modbus RTU protocol read pulse count value:

	01	03	00 30	00 02	C4 04
Transmit	Device ModBus address	Function code	Initial address	Read quantity	CRC check code

	01	03	04	00 10	00 03	BB F7
Receive	Device ModBus address	Function code	Return bytes	DI1 count value	DI2 count value	CRC check code

Modbus TCP protocol read pulse count value:

	00 01	00 00	00 06	01	03	00 30	00 02
Transmit	Transmission identifier	Protocol identifier	length	element ID	Function code	Initial address	Read quantity

	00 01	00 00	00 07	01	03	04	00 10	00 03
Receive	Transmission identifier	Protocol identifier	length	element ID	Function code	Return bytes	DI1 count value	DI2 count value

4.3.2.1. Clear pulse count value

Function code: 06, write hold register

Address range: 40065 (0x0040)

Note: The lower four bits of the register value represent the DI4, DI3, DI2, and DI1 counts respectively. Writing "1" indicates that the count is cleared and the pulse count is restarted.

Example:

Clear the pulse count values of DI2 and DI4, and retain the pulse count values of DI1 and DI3. Write value should be 0x0a, corresponding to the binary value of 0000 1010.

Modbus RTU protocol clear pulse count value:

	01	06	00 40	00 0a	08 19
Transmit	Device ModBus address	Function code	Address	Write value	CRC check code

	01	06	00 40	00 0a	08 19
Receive	Device ModBus address	Function code	Address	Write value	CRC check code

Modbus TCP protocol clear pulse count value:

	00 01	00 00	00 06	01	06	00 40	00 0a
Transmit	Transmission identifier	Protocol identifier	length	element ID	Function code	Address	Write value

	00 01	00 00	00 06	01	06	00 40	00 0a
Receive	Transmission identifier	Protocol identifier	length	element ID	Function code	Address	Write value

4.3.2. Switching input DI is automatically reported

The automatic input function of the digital input is to transmit the change value when the switching quantity changes. You can choose to transmit via RS485 or GPRS, or you can turn off the automatic reporting function.

The corresponding Modbus register of the switch automatic reporting setting is 40082 (0x0051), and the value corresponds to the function:

Switch off automatic reporting function

Switching quantity is automatically reported and transmitted via RS485

Switching quantity is automatically reported and transmitted via GPRS Network

The switch change upload protocol is as follows. The frame headers is 0xAA and 0xBB are fixed, and the values range of DI1, DI2, DI3, and DI4 are 0x00, 0x01, and 0xFF, while

0x00 represents the switch input disconnection.

0x01 represents the switch input closed.

0xff represents that the switch input has not changed.

The values of DI1, DI2, DI3, and DI4 in the table indicate that the DI1, DI2 status is updated to open, the DI3 status is updated to closed, and the DI4 status is unchanged. The last two bytes are modbus CRC16 calculated values.

Frame header	DI1	DI2	DI3	DI4	Modbus CRC
0xAA 0xBB	0x00	0x00	0x01	0xff	0xBD 0xDA

4.3.3. DO Time Settings for Switch Output

The setting of switching pulse output time is to set the switching output time (relay NO, COM closing time). The corresponding Modbus register is 40083 (0x0052). Its value range is 300-65535 Ms. If the value is less than 300 ms, the default switching output is closed to hold state, that is, the switching output is kept after closing.

If it is set to 300ms or more, such as 500 ms, after sending the closing command, the closing of the switch will be maintained 500 ms, and then it will be automatically disconnected after 500 ms.

4.3.4. Switch DO Restart Output State Settings

Whether the device restarts to maintain the state before the power is turned off or to maintain the setting of the specific output state, This function is only valid if the output time of the device switch is set to register value less than 300 ms.

The corresponding Modbus register is 40085 (0x0054) when the switch restart output state is set, Its value range is 0x00-0x10. When this register value is 0x10, the last switch output state is maintained after the power is turned off and restarted; When the register value is 0x00-0x0F, the output state of the device restart switch is determined by the low four bits. Bit 4 corresponds to DO4, Bit 3 corresponds to DO3, Bit 2 corresponds to DO2, Bit 1 corresponds to DO1, When power on, DO4, DO2 are in closed state (relay NO, COM closed) DO3, DO1 is in open state (relay NO, COM disconnected), corresponding register value is 0000 1010, that is, 0xa0, "1" is closed state, "0" is disconnected state.

4.4 Network related functions

4.4.1. Server IP or domain name, port, TCP or UDP settings (Socket)

The server IP or domain name is stored by 22 modbus registers. The first register is used to store IP or the length of the ASCII code corresponding to the domain name, the remaining registers are used to store IP or the ASCII code value corresponding to the domain name. For example, the IP is 116.62.42.192, the port is 31687, a total of 13 characters, that is, the length is 0x000D, and the IP corresponding ASCII code value is 31 31 36 2E 36 32 2E 34 32 2E 31 39 32. The corresponding modbus register storage value is as follows table. If it is a domain name, the corresponding domain name is also converted into ASCII corresponding hexadecimal storage. (Note: The maximum length of the domain name does not exceed 40 ASCII codes)

40101(0x0063)	40101(0x0064) -- 40121(0x0078)
length	IP or domain name value
00 0D	31 31 36 2E 36 32 2E 34 32 2E 31 39 32

Port 31687, corresponding to hexadecimal 7BC7; The protocol type (TCP, UDP) is saved using the protocol register, the value 0x0001 corresponds to the TCP protocol, and the value 0x0000 corresponds to the UDP protocol. That is, when the IP is 116.62.42.192 and the port is 31687, the TCP protocol, the unused IP or domain name register can be filled as "0" or not filled. If you need to use the function code "0x10" to write the IP, domain name, port, and protocol type at one time, the unused registers must be filled with values to continuously write the modbus register. The corresponding register values are as follows:

40100(0x0063)	40101(0x0064) -- 40121(0x0078)	40122(0x0079)	40123(0x007A)
IP or domain name length	IP or domain name value	Server port	TC Pprotocol
00 0D	31 31 36 2E 36 32 2E 34 32 2E 31 39 32 00	7B C7	00 01

Because the length of IP or domain name register is longer than that of IP or domain name value, it is necessary to consider the length of IP or domain name when writing IP register, that is, how many registers need to be occupied. If the above IP is written to the Modbus register:

Modbus RTU protocol writes Socket registers:

Transmit	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
	Device ModBus address	Function code	address	Register Length	Bytes	Write value	CRC check code

Receive	01	10	00 63	00 18	30 1D
	Device ModBus address	Function code	address	Register Length	CRC check code

Modbus TCP protocol writes Socket registers:

Transmit	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
	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Register Length	Bytes	Write value

Receive	00 01	00 00	00 06	01	10	00 63	00 18
	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Register Length

4.4.2. Custom registration package

The custom registration package can be ASCII code or hex, the length of hex cannot be greater than 20 bytes, and the length of ASCII code cannot be greater than 40 bytes.

The first register of the custom registration package is used to store the registration packet type. The value 0x0000 indicates that the registration packet is in hex format, and the value 0x0001 indicates that the registration packet is in ASCII format. When the value is 0x0001, the registration packet value is ABCDEFGHIJ, the corresponding ASCII code value is as follows. The second register of the custom registry package is used to store the length of the registered package value. The length of the registered package value is 10, corresponding to the hexadecimal system is 0x0A. Like IP registers, unused registered packet value registers can be "0" filled or not filled.

40124(0x007B)	40125(0x007C)	40126(0x007D) -- 40145(0x0090)	40146(0x0091)
type	length	Register package value	Registered Packet Mechanism
00 01	00 0A	41 42 43 44 45 46 47 48 49 4A 00	00 01

The registration package mechanism has 5 modes:

Registration packet mechanism register value (0x0091)	Corresponding function description
00 00	Close the registration package mechanism
00 01	Add MAC/IMEI as registration packet data before each packet is sent to the server.
00 02	Add custom registration package data before each packet is sent to the server.
00 03	Send a MAC/IMEI registration package only when connecting to the server for the first time
00 04	Send a user-defined registration package only when connecting to the server for the first time you

Modbus RTU Write Register:

Transmit	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
	Device ModBus address	function code	address	Register length	Bytes	Write value	CRC check code

Receive	01	10	00 7B	00 17	F0 1E
	Device ModBus address	function code	address	Register length	CRC check code

Modbus TCP Write Register:

Transmit	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
	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Register Length	Bytes	Write value

Receiver	00 01	00 00	00 06	01	10	00 7B	00 17
	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Register Length

4.4.3. Heartbeat package

The heartbeat packet can be ASCII code or hex, the length of hex cannot be greater than 20 bytes, and the length of ASCII code cannot be greater than 40 bytes. The first register of the heartbeat packet is used to store the heartbeat packet data type. The value 0x0000 indicates that the heartbeat packet is in hex format, and the value 0x0001 indicates that the heartbeat packet is in ASCII format. When the value is 0x0000, the heartbeat packet value is 0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09. The second register of heartbeat packet is used to store the length of heartbeat packet value. The length of heartbeat packet value is 10, corresponding to decimal 0x0A. Like custom registry packages, unused heartbeat pack value registers can be filled with "0" or not.

40147(0x0092)	40148(0x0093)	40149(0x0094) -- 40168(0x00A7)
type	length	Register package value
00 00	00 0A	00 01 02 03 04 05 06 07 08 09 00

Modbus RTU Write Register:

Transmit	01	10	00 92	00 16	2C	00 00 00 0A 00 01 02 03 04 05 06 07 08 09 00	52 9E
	Device ModBus address	function code	address	Register length	Bytes	Write value	CRC check code

Receive	01	10	00 92	00 16	E0 2A
	Device ModBus address	function code	address	Register length	CRC check code

Modbus TCP Write Register:

Transmit	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
	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Register Length	Bytes	Write value

Receive	00 01	00 00	00 06	01	10	00 92	00 16
	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Register length

4.4.4. Heartbeat packet time

The heartbeat packet time setting range is 0-65535 seconds. When the heartbeat packet time is set to 0, the heartbeat packet is closed. Set the heartbeat packet length to 5s as follows.

Modbus RTU protocol write heartbeat packet time register:

Transmit	01	06	00 A8	00 05	C8 29
	Device ModBus address	function code	address	Write value	CRC check code

Receive	01	06	00 A8	00 05	C8 29
	Device ModBus address	function code	address	Write value	CRC check code

Modbus TCP protocol Modbus RTU protocol write heartbeat packet time register:

Transmit	00 01	00 00	00 06	01	06	00 A8	00 05
	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Write value

Receive	00 01	00 00	00 06	01	06	00 A8	00 05
	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Write value

4.4.5. Heartbeat packet mode

The heartbeat packet mode is divided into a serial heartbeat packet and a network heartbeat packet (the default is a network heartbeat packet). When writing 0 to this register, it is a network heartbeat packet. When writing 1, it is a serial heartbeat packet.

Modbus RTU protocol write heartbeat packet mode register:

Transmit	01	06	00 A9	00 01	98 2A
	Device ModBus address	function code	address	Write value	CRC check code

Receive	01	06	00 A9	00 01	98 2A
	Device ModBus address	function code	address	Write value	CRC check code

Modbus TCP protocol write heartbeat packet mode register:

Transmit	00 01	00 00	00 06	01	06	00 A9	00 00
	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Write value

Receive	00 01	00 00	00 06	01	06	00 A9	00 00
---------	-------	-------	-------	----	----	-------	-------

	Transmission identifier	Protocol identifier	length	element ID	Function code	address	Write value
--	-------------------------	---------------------	--------	------------	---------------	---------	-------------

4.4.6. IP parameter setting of local WAN port

Local IP acquisition includes static IP acquisition and dynamic IP acquisition (DHCP). There are 34 registers from 0xb1 to 0xd2. When the value in the first register (0XB1) is 1, it is static IP mode and dynamic acquisition mode when it is 0. From 0XB2 to 0XBC, a total of 11 registers are stored in the local ip address, where 0XB2 stores the length of the ip address, and 0XB3 to 0XBC stores the ASCII value of the IP address. From 0XBD to 0XC7, a total of 11 registers are stored in the subnet mask information, where 0XBD stores the length of the subnet mask address, and 0XBE to 0XC7 stores the ASCII code value of the subnet mask address. From 0XC8 to 0XD2, a total of 11 registers are stored in the gateway address, where 0XC8 stores the length of the gateway address, and 0XC9 to 0XD2 stores the ASCII code value of the gateway address.

You can use 10 function codes to write in one time. As with the server IP settings, note that the unfilled registers are filled with 0. The following command indicates that it is set to static IP, the local IP address is 192.168.4.101, the subnet mask is 255.255.255.0, and the gateway is 192.168.4.1. Note that the corresponding ASCII code value should be written when writing, and Convert to hexadecimal.

Modbus RTU protocol configures WAN port parameters:

Transmit	01	10	00 B1	00 22	44	00 01 00 0D 31 39 32 2E 31 36 38 2E 34 2E 31 30 31 00 00 00 00 00 00 00 00 0D 32 35 35 2E 32 35 35 2E 32 35 35 2E 30 00 00 00 00 00 00 00 00 0B 31 39 32 2E 31 36 38 2E 34 2E 31 00 00 00 00 00 00 00 00 00	31 16
	Device ModBus address	function code	address	Register Length	Bytes	Write value	CRC check code

Receive	01	10	00 B1	00 22	10 37
	Device ModBus address	function code	address	Register Length	CRC check code

Modbus TCP protocol writes WAN port parameters:

Transmit	00 01	00 00	00 4B	01	10	00 B1	00 22	44	00 01 00 0D 31 39 32 2E 31 36 38 2E 34 2E 31 30 31 00 00 00 00 00 00 00 00 0D 32 35 35 2E 32 35 35 2E 32 35 35 2E 30 00 00 00 00 00 00 00 00 0B 31 39 32 2E 31 36 38 2E 34 2E 31 00 00 00 00 00 00 00 00 00 00
	Transmission identifier	Protocol identifier	length	element ID	function code	address	Register Length	Bytes	Write value

Receive	00 01	00 00	00 06	01	10	00 B1	00 22
	Transmission identifier	Protocol identifier	length	element ID	function code	address	Register Length

4.4.7. DNS settings

There are 22 registers from 0XD3 to 0XDE, which store DNS information. DNS addresses are divided into preferred DNS and standby DNS. Register 0xD3 stores the address length of preferred DNS, and 0xD4 to 0xDD stores the address ASCII code value of preferred DNS. Register 0XDE stores the length of the standby DNS address, and from 0XDE to 0XE8 stores the ASCII code value of the address of the standby DNS.

The preferred DNS and standby DNS can be configured with 10 function codes at one time. The table below shows the configuration preferred and alternate DNS are 61.139.2.69 and 192.168.4.1 respectively.

Modbus RTU protocol configuration preferred and standby DNS:

Transmit	01	10	00 D3	00 16	2C	00 0B 36 31 2E 31 33 39 2E 32 2E 36 39 00 00 00 00 00 00 00 00 00 00 0B 31 39 32 2E 31 36 38 2E 34 2E 31 00 00 00 00 00 00 00 00 00	D9 F2
	Device ModBus address	function code	address	Register Length	Bytes	Write value	CRC check code

Receive	01	10	00 D3	00 16	B0 3E
	Device ModBus address	function code	address	Register Length	CRC check code

Modbus TCP protocol configuration preferred and standby DNS:

Transmit	00 01	00 00	00 33	01	10	00 D3	00 16	2C	00 0B 36 31 2E 31 33 39 2E 32 2E 36 39 00 00 00 00 00 00 00 00 00 0B 31 39 32 2E 31 36 38 2E 34 2E 31 00 00 00 00 00 00 00 00 00
	Transmission identifier	Protocol identifier	Length	element ID	function code	address	Register Length	Bytes	Write value

Receive	00 01	00 00	00 06	01	10	00 D3	00 16
	Transmission identifier	Protocol identifier	Length	element ID	function code	address	Register Length

4.4.8. Ebyte Cloud Transparent Transmission

The function of Ebyte cloud transparent transmission can be turned on or off. The register for this function is 40169 (0x00AA), which supports 0x0003, 0x0006 and 0x0010 function codes:

When the register value is 0x0000, the cloud transmission function is turned off.

When the register value is 0x0001, the cloud transmission function is turned on.

The default is Cloud Transfer Closed.

4.4.9. Clear cache

Register 0xAF can set whether to clear the cache in the network SOCKET, support 0x0003, 0x0006, 0x0010 function code:

When the value of this register is 0x0000, the empty cache function is turned on.

When the value of this register is 0x0001, the empty cache function is turned off.

4.4.10. Keep alive connection

Register 40170 (0x00AB) is a keep-alive connection register, which needs to be used with 40171 (0x00AC), 40172 (0x00AD).

The 40170 (0x00AB) register indicates how many seconds after the TCP connection has no data message transmission to start the probe message. When the value of this register is 0, it means to disable this function. When it is 2-7200, it means to turn on the function and take effect the parameters of the next two registers.

The 40171 (0x00AC) register indicates the time interval between the previous probe packet and the next probe packet.

The value is 2~7200 in seconds.

The 40172 (0x00AD) register indicates the maximum number of probe failures. When sniffing the number of times, the TCP connection will be disconnected. The value is 2~255 in units.

4.4.11. Timeout restart

The register 40173 (0x00AE) is used to set how long to restart the Ethernet physical layer module in RTU after there is no data in the network, the range is 0, 60-65535 seconds. When set to 0, this function is disabled, When set to 60-65535, this parameter will take effect.

4.4.12. SOCKET Local Port Settings

The register 40175 (0x00B0) is used to set the local port number of SOCKET. It supports 0x0003, 0x0006 and 0x0010 function codes. When the value is 0, it means using random port number, and 1-65535 means setting the corresponding port number.

4.4.13. MAC reading

The starting address of MAC register reading is 40232 (0x00E9), and the total length of register is 11, wherein the first register is the MAC length, and the second register to the eleventh register stores the MAC value. For example, MAC: B2FAEAF2C427, the corresponding register values are as follows. In the register, the IMEI value exists in hexadecimal ASCII value.

40171 (0x00AA)	40172 (0x00AB) --40181(0x00B4)
MAC length	MAC value
00 0C	42 32 46 41 45 41 46 32 43 34 32 37 00 00 00 00 00 00 00 00

4.4.14. SN reading

The starting address of SN register reading is 40243 (0x00F4), and the total length of the register is 11, wherein the first register is the SN length, and the second register to the eleventh register stores the SN value. For example, SN: 190521135939C140, the corresponding register value is as follows. In the register, the SN value exists in hexadecimal ASCII value.

40182 (0x00B5)	40183 (0x00B6) --40192(0x00BF)
SN length	SN value
00 10	31 39 30 35 32 31 31 33 35 39 33 39 43 31 34 30 00 00 00 00

Important statement

- Ebyte reserves the right to interpret and modify all contents of this manual.
- Due to the continuous improvement of the hardware and software of the product, this specification may be changed without further notice. Ultimately, the latest version of the specification shall prevail.

Revision History

Version	Date	Description	Issued by
1.0	-	initial version	-
1.1	2019/8/19	Format revision	lyl

About us

Website: www.ebyte.comSales: info@cdebyte.comSupport: support@cdebyte.com

Tel: +86-28-61399028 Ext. 812

Fax: +86-28-64146160

Address: Innovation Center B333~D347, 4# XI-XIN road, High-tech district (west), Chengdu, Sichuan, China

**Chengdu Ebyte Electronic Technology Co.,Ltd.**