Modbus RTU introduction of instruction

Modbus device through receive from external control terminal (like Host computer/MCU) Modbus RTU instruction to perform related operations, one frame instruction generally consists of device address, function code, register address, register data, and check code,frame length is related to function code. Each frame date's first byte is the device address. Can set range on 1-255 default 255(scilicet 0xFF),the last 2byte is CRC check code.

Suppose the device address is 255, the commonly used Modbus RTU instructions are as follows:

1. Open no.1 relay (manual mode)
send: FF 05 00 00 FF 00 99 E4
return: FF 05 00 00 FF 00 99 E4
remarks:
(1)the 3--4th byte of the transmitted frame represents the relay address,the relay 1-relay 8 address are respectively 0x0000, 0x0001, 0x0002, 0x0003, 0x0004, 0x0005, 0x0006, 0x0007
(2)the 5--6th byte of the transmitted frame represents Data, 0xFF00 represent turn on relay, 0x0000 represents turn off relay

2. Turn off the relay No. 1 (manual mode)
send: FF 05 00 00 00 00 D8 14
return: FF 05 00 00 00 00 D8 14

3. Turn on the relay No. 2 (manual mode)
send: FF 05 00 01 FF 00 C8 24
return: FF 05 00 01 FF 00 C8 24

4. Turn off the relay no.2 (manual mode)
send: FF 05 00 01 00 00 89 D4
return: FF 05 00 01 00 00 89 D4

5. Turn on all relay
send: FF 0F 00 00 00 08 01 FF 30 1D
return: FF 0F 00 00 00 08 41 D3

6. Turn off all relay
send: FF 0F 00 00 00 08 01 00 70 5D
return: FF 0F 00 00 00 08 41 D3

7. Set the device address to 1
send: 00 10 00 00 00 01 02 00 01 6A 00
return: 00 10 00 00 00 01 02 00 01 6A 00
remark: The 9th byte of the transmitted frame, 0x01 is the written device address.

8. Set the device address to 255
send: 00 10 00 00 00 01 02 00 FF EB 80
return: 00 10 00 00 00 01 02 00 FF EB 80
remark: The 9th byte of the transmitted frame, 0xFF is the written device address.

9. Read device address
send: 00 03 00 00 00 01 85 DB
return: 00 03 02 00 FF C5 C4
remarks: The 5th byte of the Return frame, 0xFF is the read device address

10. Read relay state
send: FF 01 00 00 00 08 28 12
return: FF 01 01 01 A1 A0
remarks: The 4th byte of the Return frame, Bit0--Bit7 of 0x01 representing relay 1-relay 8, 0 is turn off, 1 is turn on.

11. Read optocoupler input status
send: FF 02 00 00 00 08 6C 12
return: FF 02 01 01 51 A0
remarks: The 4th byte of the Return frame, Bit0--Bit7 of 0x01 represent optocoupler 1 - optocoupler 8 input signal, 0 represent low level, 1 represent high level

12. Set the baud rate to 4800
send: FF 10 03 E9 00 01 02 00 02 4A 0C
return: FF 10 03 E9 00 01 C5 A7
remarks: the 9th byte of the transmitted frame is the baud rate setting value ,0x02, 0x03, x04 represents 4800, 9600, 19200

13. Set the baud rate to 9600
send: FF 10 03 E9 00 01 02 00 03 8B CC
return: FF 10 03 E9 00 01 C5 A7

14. Set the baud rate to 9600
send: FF 10 03 E9 00 01 02 00 04 CA 0E
return: FF 10 03 E9 00 01 C5 A7

15. Read the baud rate
send: FF 03 03 E8 00 01 11 A4
return: FF 03 02 00 04 90 53
remarks: The 5th byte of the Return frame represent baud rate, 0x02, 0x03, x04 represents 4800,9600,19200.

16. Turn on no. 1 relay (flash ON mode)
send: FF 10 00 03 00 02 04 00 04 00 14 C5 9F
return: FF 10 00 03 00 02 A4 16
remarks:

(1)the 3-4th byte of the transmitted frame is represent relay address, relay1-relay8's address separately is 0x0003, 0x0008, 0x000D, 0x0012, 0x0017, 0x001C, 0x0021, 0x0026

(2)The 10th-11th byte of the transmitted frame represents the delay setting value, and the delay base is 0.1S, so the delay time is 0x0014*0.1=20*0.1S=2S, and the relay automatically turns off after turned on 2S

17. Turn off no. 1 relay (flash OFF mode)

send: FF 10 00 03 00 02 04 00 02 00 1E A5 99

return: FF 10 00 03 00 02 A4 16

remarks:

(1)the 3-4th byte of the transmitted frame is represent relay address, relay1-relay8's address separately is 0x0003, 0x0008, 0x000D, 0x0012, 0x0017, 0x001C, 0x0021, 0x0026

(2)The 10th-11th byte of the transmitted frame represents the delay setting value, and the delay base is 0.1S, so the delay time is 0x001E*0.1=30*0.1S=3S,and the relay automatically turns off after turned on 3S

Simple instructions

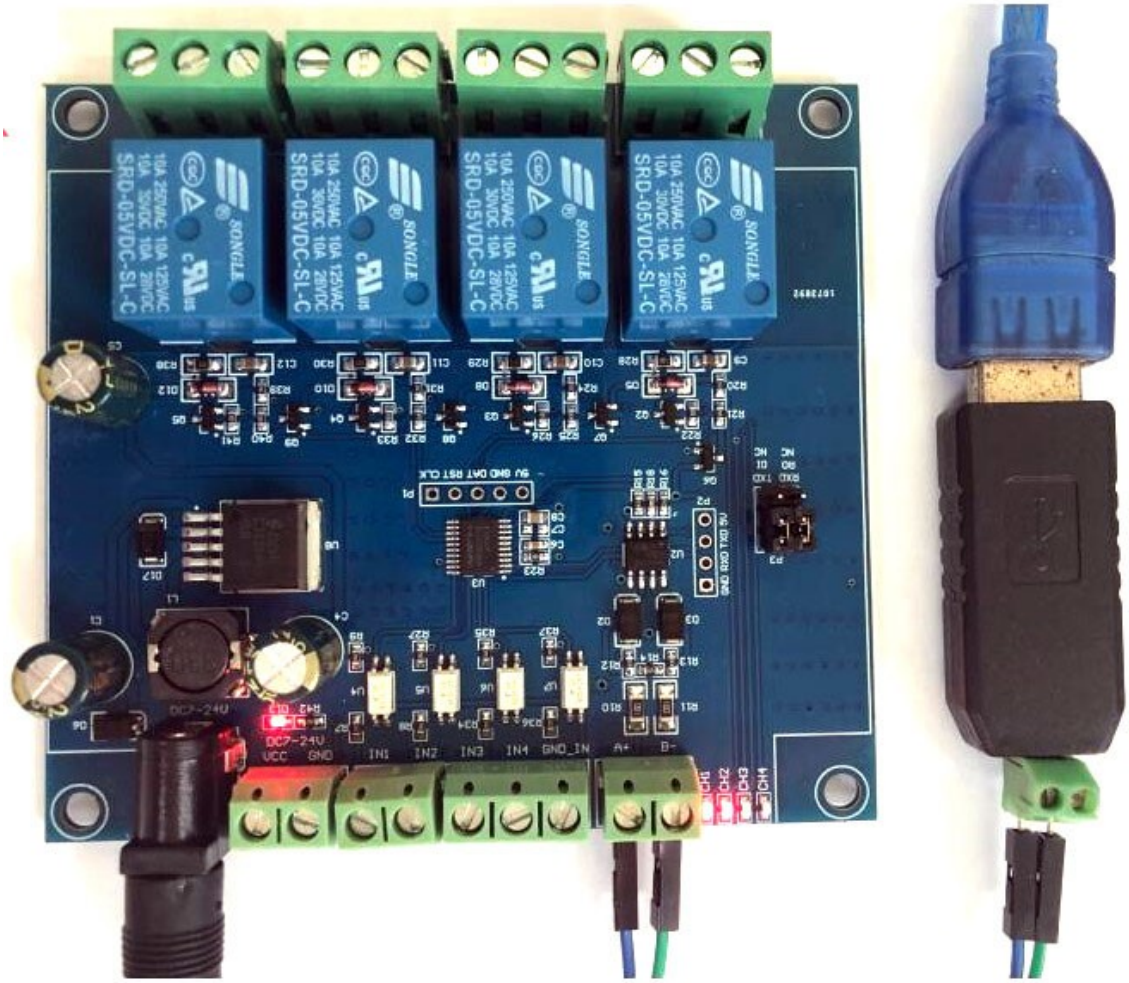
Modbus relay module can via RS485/TTL UART interface received from host computer /MCU's Modbus RTU command to perform related operations.The following is an example of using the host computer software via the RS485 interface to open relay 1 (manual mode),suppose device address for 255.baud rate is 9600. Then steps of usage as follows:

1, VCC, GND: Connect to the power

2, A+, B- : Connect to A+ and B- of external device

3, turn on host computer software ModbusRTU configuration Tool,choose correct port number, baud rate is 9600.default address is 255,click open serial ports4,

then click "JD1 ON" button can turn on relay 1 ,meanwhile indicator of relay 1 lights up as below:



How to generate check code

Modbus RTU command are send through upper PC software (like:ModbusRTU configuration Tool),CRC check code is auto generated, if want use serial debugging software (like SSCOM)to test Modbus relay module then need manually generated
CRC check code put on the end of transmitted frame, such as turn on the first relay (manual mode)

1. Turn on/off of relay (manual mode) transmitted frame composition :
device address （1Byte）+function code（1Byte）+ register address（2Byte） +register data (2Byte）+CRC check code (2Byte）

2. Suppose the device address is 0xFF, Then the first 6 bytes of the transmitted frame are
FF 05 00 00 FF 00

3. Use the CRC check tool to check the 6 bytes
http://www.ip33.com/crc.html

4. Exchange checksum calculation result E499 high and low byte position then get CRC check code 99E4 and complete transmission frame: FF 05 00 00 FF 00 99 E4

5. Through serial port debugging software SSCOM V5.13.1 use the transmission frame send to modbus relay module can open first way relay (manual mode),as bellow: