R4IOH08 MODBUS RTU Commamd

(4DI-4DO)

MODBUS command (function code, write 05/06/15/16, read 01/02/03)

Note :
1 MODBUS command must be HEX
2 Slave address (device address) must be the same as the setting. You can also use this command to query the current device address: FF 03 00 FD 00 01 00 24
3 The Baudrate and parity should be consistent
4 If communication fails, please short the RES jumper on the board for 5 seconds to restore the factory settings

Supported function codes:

Function Code	Modbus Address (PLC)	Register Address	Describe
01:	00001	0x0004-0x0007 (4-7)	Read DO digital output status (relay)
05:	00001	0x0004-0x0007 (4-7)	Write a single DO digital output (relay)
15:	00001	0x0004-0x0007 (4-7)	Write multiple DO digital output (relay)
02:	10001	0x0000-0x0003 (0-3)	Read DI digital input (optical isolation input)
03	40001		
		0x0080-0x00FF (128-255)	Read special function registers (baud rate 485 address, etc.)
06	40001		
		0x0080-0x00FF (128-255)	Write a single special function register (baud rate 485 address, etc.)
16(0x10)	40001		
		0x0080-0x00FF (128-255)	Write multiple special function registers (baud rate 485 address, etc.)

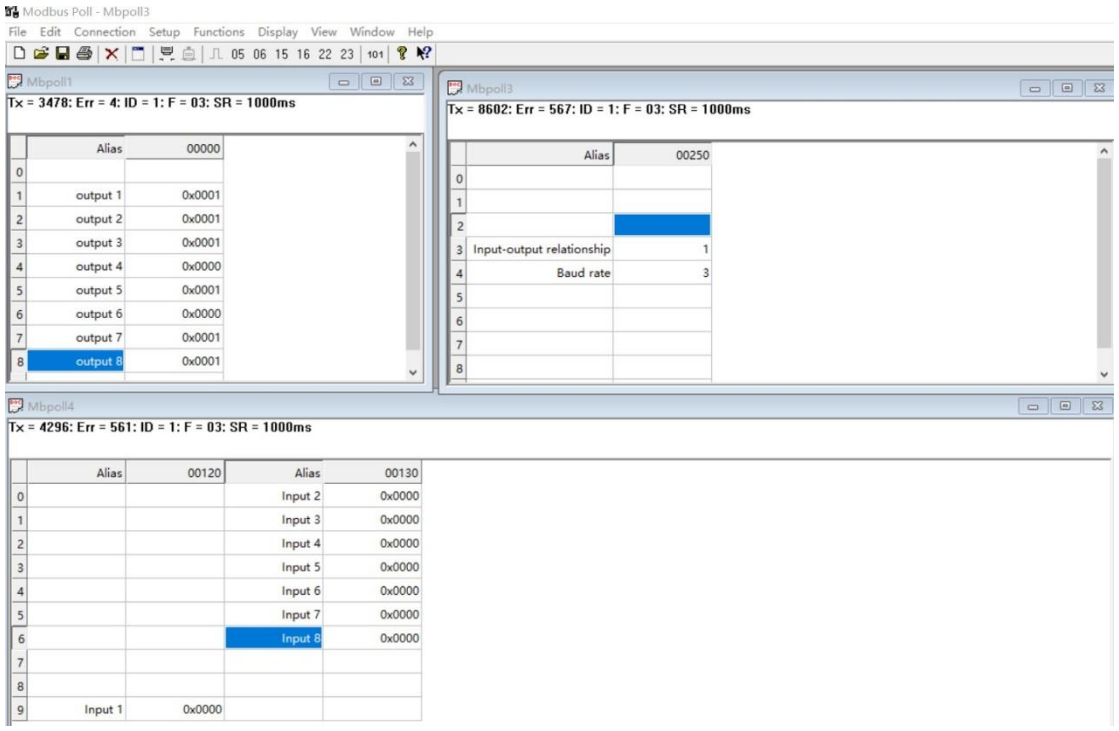
All states are mapped into 4xxxx range registers. The user can monitor the input and output status of the module by reading or modifying the value of the 4xxxx interval register (03 06 16 function code)

Register address	Register contents	Register value	Remarks	R/W
0x0080 (128)	DO digital output	0-65536	Digital output status 4-7 bits	R/W
0x0090 (144)	DI digital input	0	Digital input status 0-3 bits	R
The following are special function registers				
0X00F5 (245)	Input port level	0X0000 NPN Low level input (default) 0X0001 PNP High level input		R/W
0X00F6 (246)	Output port level	0X0000 NPN Low level output (default) 0X0001 PNP High level output		R/W
0X00F8 (248)	Automatic reporting of digital input(DI) status	0: Query function (default) 1-255: Automatically report, the unit is second. 1: Report every 1 second 2: Report every 2 seconds 10: Report every 10 seconds Maximum interval of 255 seconds		R/W
0x00FA (250)	Input and output relationship (DI-DO relationship)	0X0000-0X0005	0x0000 Unrelated(default) 0x0001 Self-locking 0x0002 Interlocking 0x0003 Momentary 0x0004 Interlocking(2 ch) 0x0005 Output=Input Other values are the same as 0	R/W
0x00FB (251)	Factory Reset	Factory Reset: 1 Short the RES jumper for 5 seconds 2 Enter the following command at the current baud rate: FF 06 00 FB 00 00 ED E5		R/W
0x00FC (252)	Command Return Time	0-25	Time interval for command return (unit: 40MS) Setting value: 0-25	R/W
0x00FD (253)	RS485 address (Slave ID)	Read address: FF 03 00 FD 00 01 00 24; Set address to 0x02: FF 06 00 FD 00 02 8C 25		R/W
0x00FE (254)	Baud rate	0-255	0:1200 1:2400 2:4800 3:9600 (default) 4:19200 5:38400 6: 57600 7: 115200 Others: Factory reset	R/W
0x00FF (255)	Parity	0-2	0 None Parity 1 Odd Parity 2 Even Parity	R/W

9600 Band ,8 Data bits,None Parity,1 Stop Bit。

MODBUS commands you can use "Modbus Poll" input, as shown below

（CRC check generated automatically）



You can also use HyperTerminal serial input, as shown below

（Manually add CRC check）

1 Read DI digital input status:

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC)：10001-10004
RS485 address : 0x01~0x3F
Function code: 0x02
Register address:0x0000-0x0003
Read number :0x0001-0x0004

For example, read the status of DI digital input of channel 0-3:
Send data(address 1): 01 02 00 00 00 04 79 C9
Return data : 01 02 01 03 E1 89
01 RS485 address, 02 function code, 01 length, 03 refers to the current DI digital input status, converted to binary 00000011, indicating that 0/1 channels have input, and other channels have no input.

In addition, the DI digital input is also mapped to the 40000 interval register. The user can read the value of the DI digital input through the 03 function code.

Modbus Address(PLC)：40145
RS485 address : 0x01~0x3F
Function code:0x03
Register address:0x0090
Read number: 0x0001

For example, read the status of DI digital input of channel 0-3:
Send data(address 1): 01 03 00 90 00 01 84 27
Return data : 01 03 02 00 05 78 47
01 RS485 address, 03 function code, 02 length, 0005 refers to the current DI digital input status, converted to binary 00000101, indicating that 0/2 channels have input, and other channels have no input.

2.Read DO digital output status:

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC)：00005-00008
RS485 address : 0x01~0x3F
Function code: 0x01
Register address:0x0004-0x0007
Read number :0x0001-0x0004

For example, read the status of DO digital output of channel 4-7:
Send data(address 1): 01 01 00 00 00 08 3D CC
Return data : 01 01 01 B8 51 FA
01 RS485 address, 01 function code, 01 length, B8 refers to the current DO digital output status, converted to binary 10111000, indicating that 7/5/4/3 channels have output, and other channels have no output.

In addition, the DO digital output is also mapped to the 40000 interval register. The user can read the value of the DO digital output through the 03 function code.

Modbus Address(PLC)：40129
RS485 address : 0x01~0x3F
Function code:0x03
Register address:0x0080
Read number: 0x0001

For example, read the status of DO digital output of channel 4-7:
Send data(address 1): 01 03 00 80 00 01 85 E2
Return data : 01 03 02 00 38 B9 96
01 RS485 address, 03 function code, 02 length, 0038 refers to the current DO digital output status, converted to binary 00111000, indicating that 3/4/5 channels have output, and other channels no output.

3. Write single DO digital output status:

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC)：00005-00008
RS485 address : 0x01~0x3F
Function code:0x05
Register address:0x0004-0x0007

For example 2, Write channel 5 to ON, others OFF:

Send data(address 1):01 05 00 05 FF 00 9C 3B
Return data :01 05 00 05 FF 00 9C 3B

For example 3, Write channel 7 to ON, others OFF:
Send data(address 1):01 05 00 07 FF 00 7C 0B
Return data :01 05 00 07 FF 00 7C 0B

In addition, the DO digital output is also mapped to the 40000 interval register. The user can write the DO digital output value through the 06/16 function code.

Modbus Address(PLC)：40129
RS485 address :0x01~0x3F
Function code:0x06/0x10
Register address:0x0080

For example, Write channel 7 to ON:
Send data(address 1):01 06 00 80 00 80 89 82
Return data :01 06 00 80 00 80 89 82

4.Write multiple DO digital output status (relay output):

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC)：00005-00008
RS485 address :0x01~0x3F
Function code:0x0F
Register address:0x0004-0x0007

For example 1, Write channel 4-7 to OFF:
Send data(address 1):01 0F 00 00 00 08 01 00 FE 95
Return data :01 0F 00 00 00 08 54 0D

For example 1, Write channel 4-7 to ON:
Send data(address 1):01 0F 00 00 00 08 01 FF BE D5
Return data :01 0F 00 00 00 08 54 0D

For example 3, Write channel 0/1/3/7 to ON, others OFF:
Send data(address 1):01 0F 00 00 00 08 01 8B BE F2
Return data :01 0F 00 00 00 08 54 0D

In addition, the DO digital output is also mapped to the 40000 interval register. The user can write the DO digital output value through the 06/16 function code.

Modbus Address(PLC)：40129
RS485 address :0x01~0x3F
Function code:0x06/0x10
Register address:0x0080

For example, Write channel 6/7 to ON, others OFF:
Send data(address 1):01 06 00 80 00 C0 88 72
Return data :01 06 00 80 00 C0 88 72

Special function Register

1.Set the 485 address(Slave ID)

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC)：40254
RS485 address :0x01~0Xf8/0XFF
Function code:Write 0x06/0x10,Read 0x03
Register address:0x00FD(253)
Value: 2 bytes (values 1-248)

For example 1: Set the current device address to 0x02
Send data(address is 1): 01 06 00 FD 00 02 99 FB
Return data : 01 06 00 FD 00 02 99 FB
Send data(don't know the address): FF 06 00 FD 00 02 8C 25
Return data : FF 06 00 FD 00 02 8C 25

For example 2: Read device address(0X0001)
Send data : FF 03 00 FD 00 01 00 24
Return data : 01 03 02 00 01 79 84

Note：With this command, there can be only one module on the bus 485, More than one will go wrong!

2.Write baud rate

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC)：40255
RS485 address :0x01~0x3F
Function code:Write 0x06/0x16;Read 0x03
Register address:0x00FE(254)
Value: 2 bytes (values 0-7)

For example 1, Change the baud rate to 4800bps:
Send data(address 1):01 06 00 FE 00 02 69 FB
Return data :01 06 00 FE 00 02 69 FB

Baud rate corresponds to the number: 0:1200 1:2400 2:4800 3:9600
4:19200 5：38400 8: Factory reset
Note: 1 The baud rate will be updated only when the module is powered on again when this command is used!
2 When the number corresponding to the baud rate is 8, the factory settings can be restored
For example:01 06 00 FE 00 08 E9 FC

For example 2 Read the current baud rate:
Send data(address 1):01 03 00 FE 00 01 E5 FA
Return data :01 03 02 00 03 F8 45

01 RS485 address, 03 Function,02 length,F8 45 crc16,03 means the current baud rate is 9600bps

Baud rate corresponds to the number: 0:1200 1:2400 2:4800 3:9600
4:19200 5：38400

3. Set digital input and output relationship (DI-DO relationship):

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC):40251
RS485 address :0x01~0x3F
Function code:Write 0x06/0x16;Read 0x03
Register address:0x00FA(250)
Value: 2 bytes (values 0-5)

For example, set the input and output to be unrelated, and change the register value to 0X0000:
Send data(address 1):01 06 00 FA 00 00 A9 FB
Return data :01 06 00 FA 00 00 A9 FB

Register value:
0x0000 Unrelated(default)
0x0001 Self-locking relationship
0x0002 Interlocking relationship
0x0003 Momentary relationship
0x0004 Interlocking relationship (2 channels)
0x0005 Output=Input
Other values are the same as 0x0000

For example: read the current input-output relationship
Send data(address 1):01 03 00 FA 00 01 A4 3B
Return data :01 03 02 00 01 79 84
01 RS485 address, 03 Function,02 length 0001is Self-locking relationship ,15 FA crc16

4. Set DI digital input status to automatically report (8 channels are set at the same time):(Automatic reporting of digital input(DI) status)

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC)：40249
RS485 address :0x01~0x3F
Function code:Write 0x06/0x16;Read 0x03
Register address:0x00F8(248)
Value: 2 bytes (values 0-255)

For example : For example, the current query function should be changed to automatic reporting:

1 second automatic report : 01 06 00 F8 00 01 C9 FB
2 second automatic report : 01 06 00 F8 00 02 89 FA
3 second automatic report : 01 06 00 F8 00 03 48 3A
4 second automatic report : 01 06 00 F8 00 04 09 F8
5 second automatic report : 01 06 00 F8 00 05 C8 38
10 second automatic report : 01 06 00 F8 00 0A 88 3C

Disable reporting function(Query function): 01 06 00 F8 00 00 08 3B

5.Set Command(Date) Return Time

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC): 40253
RS485 address :0x01~0x3F
Function code:Write 0x06/0x16;Read 0x03
Register address:0x00FC(252)
Value: 2 bytes (values 0-25)

For example, set the data return delay to 200ms
Send data(address 1):01 06 00 FC 00 05 89 F9
Return data :01 06 00 FC 00 05 89 F9
Return the delay time calculation formula:X = 05 * 40 = 200MS

Note: The maximum can be set to 1000MS. If it exceeds 1000MS, that is, the setting value is greater than 25, and the data return delay will be initialized.
That is: 01 06 00 FC 00 20 48 22 can make the data return delay to restore initialization 0

6.Set Parity

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC): 40256
RS485 address :0x01~0x3F
Function code:Write 0x06/0x16;Read 0x03
Register address:0x00FF(255)
Value: 2 bytes (values 0-2)

For example, set the parity to even parity
Send data(address 1):01 06 00 FF 00 01 78 3A
Return data :01 06 00 FF 00 01 78 3A
0 None Parity 1 Odd Parity 2 Even Parity

Note: 1. When using this command, the module is powered on again, and the check digit will be updated!

2. When the setting is greater than 2, the default value will be restored to 0 after powering on again, and there will be no verification.

7. Factory reset:

Send data

RS485 address (Station address) (1)	Function (1)	Register address (2)	Read number (2)	CRC16(2)

Returns data

RS485 address (Station address) (1)	Function (1)	Number of bytes (1)	data (n)	CRC16(2)

Modbus Address(PLC): 40252
RS485 address : 0x01~0x3F
Function code:Write 0x06;
Register address:0x00FB(251)
Send data(address 1):FF 06 00 FB 00 00 ED E5
Return data :FF 06 00 FB 00 00 ED E5

Reset the hardware: Short the RES jumper of the board for 5 seconds, then power on again.