Manual for RS232/RS485/Ethernet Digital Products(Version 1.0)

Scope of Application:

All the relay output modules, all the digital input products and all the digital input output products developed by Foshan Qingjun Electronics Co., Ltd.

Contents

一、Hardware Parameters 3

1.1：Relay Output Parameters 3

1.2：Transistor Output Parameters 3

1.3：Digital Input parameters 3

1.4：Requirements on Power Supply(Reference) 3

1.5：Parameters of Communication Circuit 4

1.6： Nerwork Port Parameters 4

二、Setting of Communication Ways 5

Input 192.168.1.80 Directly at the Address Column of the Browser 5

The User may Directly use the USB adapter for 485， the USB Adapter for 232 or the standard DB9 Serial Port to Connect the Computer Directly and have an all-around checking or allocation of the module with the attached special software for management and checking. 6

2.1：Setting of Even-Odd Verification (Applicable to RS485/RS232) 7

2.2：Setting of Baud Rate (Applicable to RS485/RS232) 8

2.3：Setting of Module Address(Applicable to RS485/RS232/LAN) 8

三、About Registers 9

3.1-3.4: The Related Information About Relay Output Registers 9-11

3.5-3.8：The Related Information About Digital Input Registers 12-15

3.9: About Special Registers 16

四、Function Code Explanantion about RS232 and RS485 17

4.1：Brief Introduction to Modbus-RTU Working Mechansim 17

4.2：Modbus-RTU Function Codes 18

4.3：Illustration of Function Codes 18

五、Setting of RS232 Reading Order 31

六、Setting of RS485 Reading Order 31

七、MODBUS-TCP 32

八、 PC Test 35

一、 Hardware Parameters

1.1： Relay Output Parameters

Parameters of relays of different models and different brands:

Comparison of relay parameters(coil voltage 12V/24V)			
Brand	Model	Touching type	Contact Capacity
Omron	G2R-1（with base）	One Open and one close	10A/250VAC 10A/30VDC
IDEC	RJ1V-C-D24(with base)	One Open and one close	12A/250VAC 12A/30VDC
Hongfa	HF115F(with base)	One Open and one close	12A/250VAC
Tyco	RT114024(with base)	One Open and one close	12A/250VAC

1.2：Transistor Output Parameters

Transistor Types: IRF9540N(field-effect tube)

Controlling Load Voltage: 12~24VDC

Continuous load Current: <=2A(with radiator)

Instant Peak Current: 16A (duration: 300mS)

Output type: output voltage after trigger : 12~24VDC; Floating without trigger

Output insulation: sustainable voltage±1500V

Output indicator: attached

1.3：Digital input parameters

Input way: compatible with NPN/PNP

Triggering voltage: 3.3V / 5V / 12V / 24V （optional）

Input Insulation： sustainable voltage ±1500V

Input indicator: Attached

1.4：Requirements on Power Supply(Reference)

Working Voltage: default value:24 V and 12 V (optional)

Maximum Voltage: 24V(18~30V) / 12V(10~15V)

Requirements on power supply: relay output model : 0.2A(4 channels triggered)

0.95A(32-channel triggered)

Transistor output model: 0.5A (16 channels triggered)

Pure input model: 0.3A(32-channel triggered)

Reversal connection protection: compatible

1.5： Parameters of communication circuits

Insulation or not: all insulated

Insulation Voltage: ±1500V

Communication Protocol：Modbus-RTU、Modbus-TCP

Baud rate: 1200/2400/4800/9600/19200/38400/57600/115200BPS

Data format: 1 starting point 8 data points parity checking, 1 or 2 stopping points

Maximum panel points: the BUS shared by 32 modules

Transmission distance: ≥1000M(Double twisted cable)

Screening terminals: Compatible

1.6： Network Port Parameters

1) Compatible with the PCs of Siemens ,Omron, Panasonic, King View and MCGS and Kunlun Tongtai

2) The following new functions are added to the port----an independent standard RJ45 network port, with the setting of IP address, port and gateway, makes the reading, input and control of load in the distance impossible.

3) It is applicable to 10M/100M ports and can work directly with exchange board.

4) It can be connected to LAN network port, RS485 and RS232 and communicate with them simultaneously without interference. It can work with a single communication according to the customer's requirement.

5) A built-in web management panel makes configurations and checking of module parameters possible with a cable.

6) Compatible with TCP server、TCP client at the same time. It can be used as either a sever in the network and or a customer's terminal.

7) the cable is compatible with hot swap and it can automatically search network when it is plugged in(with the customer's terminal).

二、Setting of Communication Ways

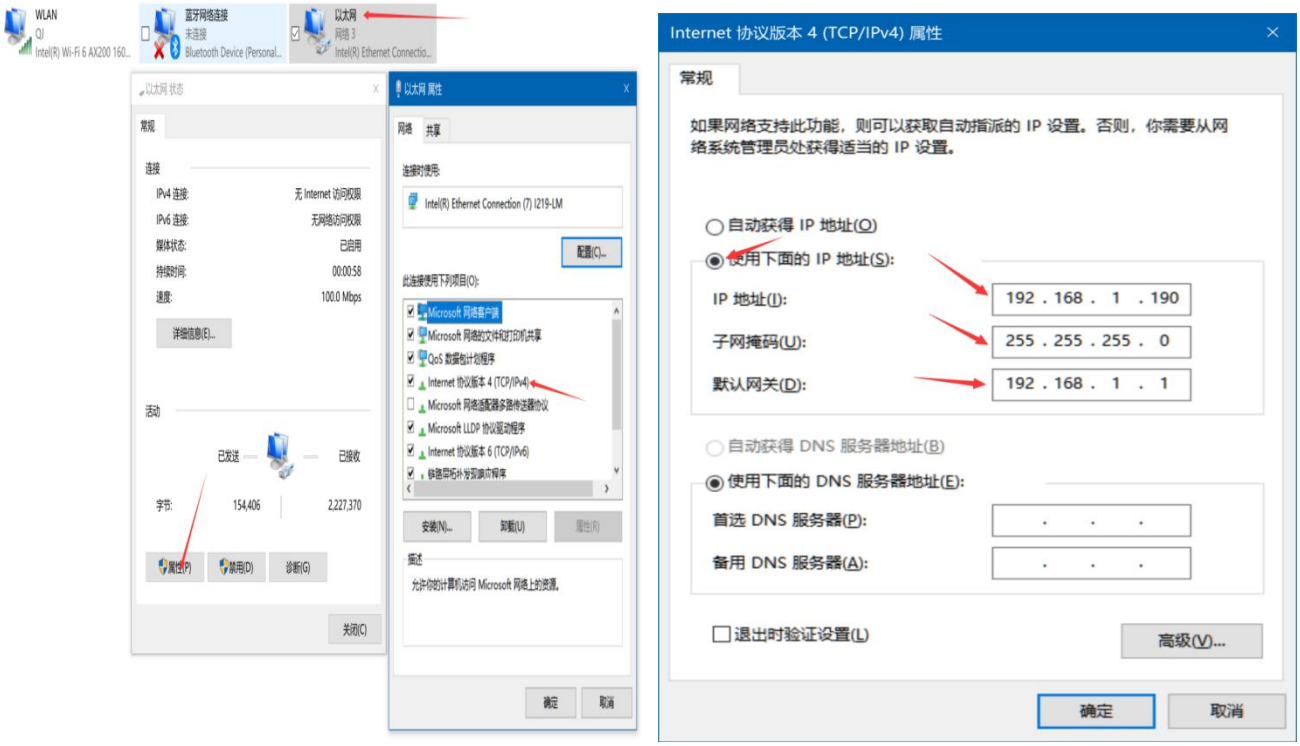
1) 10 read dial code switches set on the board make the operation easier.

With RS232 and RS485 communication, the even-odd verification way and baud rate and module address should be set the same as those of the PC.

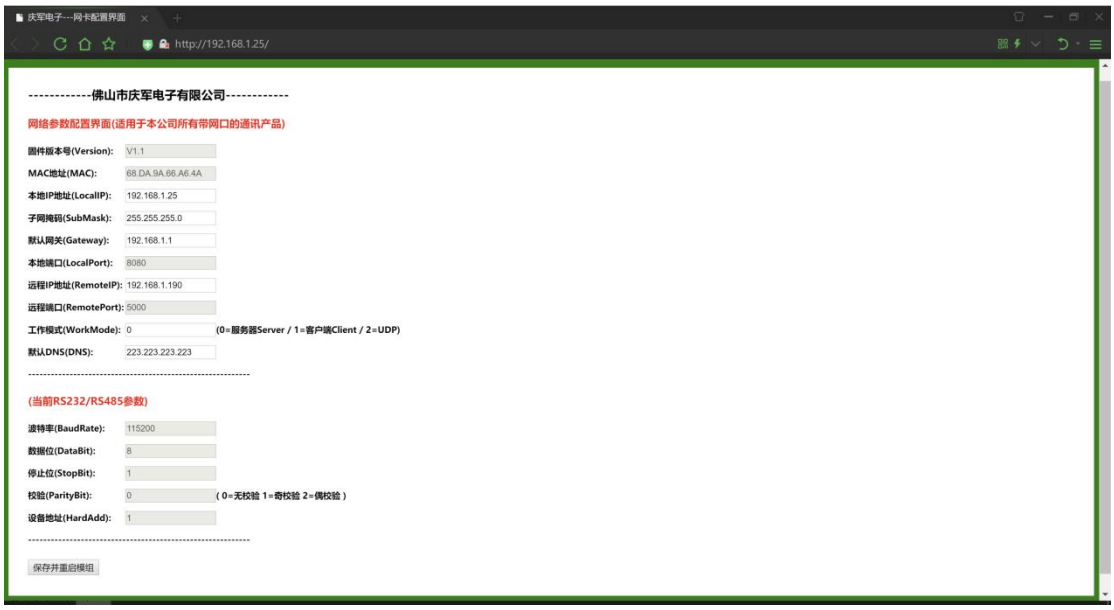
With network LAN communication, it is necessary to set the module IP address, No. of port, default gateway and working mode.

Attention: **The dial switches have to be pre-set to initialize all the communication modules developed by our company. Restarting is necessary once the state of the dial switch is changed.**

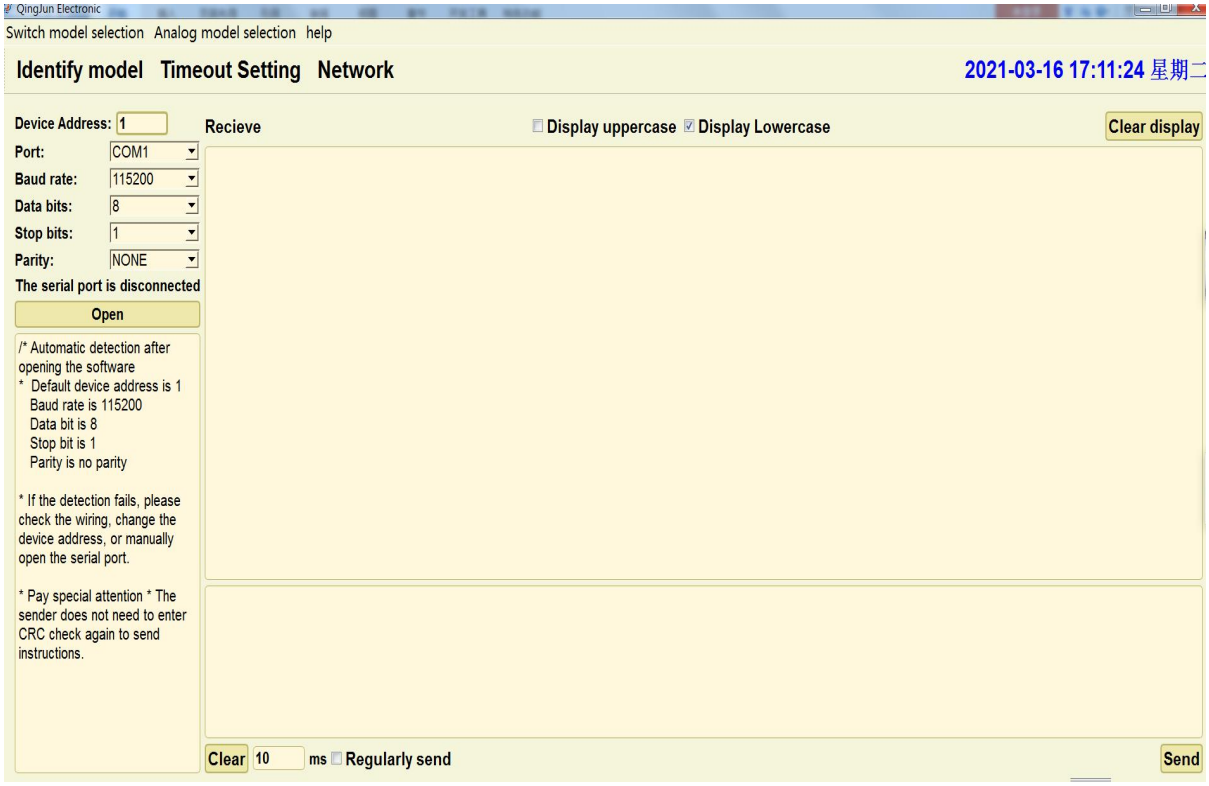
If the products with network port are chosen, the user can connect the module with the computer with cable and set the IP address, mask off code of net and the gateway as below.

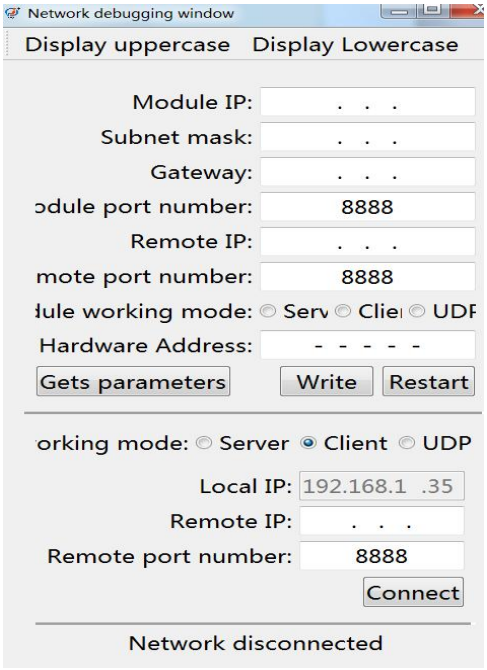


Open a browser and then input 192.168.1.80 directly at the address column and get access to the configuration page to configure the module.



The user can also use a USB adapter for 485, or a USB adapter for 232 or a standard DB9 serial port cable to connect directly with a computer to test and configure the module with the attached special software for management and checking.





2.1 Setting of Odd-even verification (applicable to RS485/RS232)

Verification for communication port data	S1	S2
No verification, 1 stopping point	0FF	OFF
No verification, 2 stopping points	0FF	ON
Odd verification , 1 stopping point	ON	0FF
EVEN verification, 1 stopping point	ON	ON

2.2 Setting of Baud Rate(applicable to RS485/RS232)

Choice of Baud rate	S3	S4	S5
1200	OFF	OFF	OFF
2400	OFF	OFF	ON
4800	OFF	ON	OFF
9600	OFF	ON	ON
19200	ON	OFF	OFF
38400	ON	OFF	ON
57600	ON	ON	OFF
115200	ON	ON	ON

2.3 Setting of module address（applicable to RS485/ RS232/LAN）

Setting of module hardware address	S6	S7	S8	S9	S10
0	OFF	OFF	OFF	OFF	OFF
1	OFF	OFF	OFF	OFF	ON
2	OFF	OFF	OFF	ON	OFF
3	OFF	OFF	OFF	ON	ON
4	OFF	OFF	ON	OFF	OFF
5	OFF	OFF	ON	OFF	ON
6	OFF	OFF	ON	ON	OFF
7	OFF	OFF	ON	ON	ON
8	OFF	ON	OFF	OFF	OFF
9	OFF	ON	OFF	OFF	ON
10	OFF	ON	OFF	ON	OFF
11	OFF	ON	OFF	ON	ON
12	OFF	ON	ON	OFF	OFF
13	OFF	ON	ON	OFF	ON
14	OFF	ON	ON	ON	OFF
15	OFF	ON	ON	ON	ON
16	ON	OFF	OFF	OFF	OFF
17	ON	OFF	OFF	OFF	ON
18	ON	OFF	OFF	ON	OFF
29	ON	OFF	OFF	ON	ON
20	ON	OFF	ON	OFF	OFF

21	**ON**	**OFF**	**ON**	**OFF**	**ON**
22	**ON**	**OFF**	**ON**	**ON**	**OFF**
23	**ON**	**OFF**	**ON**	**ON**	**ON**
24	**ON**	**ON**	**OFF**	**OFF**	**OFF**
25	**ON**	**ON**	**OFF**	**OFF**	**ON**
26	**ON**	**ON**	**OFF**	**ON**	**OFF**
27	**ON**	**ON**	**OFF**	**ON**	**ON**
28	**ON**	**ON**	**ON**	**OFF**	**OFF**
29	**ON**	**ON**	**ON**	**OFF**	**ON**
30	**ON**	**ON**	**ON**	**ON**	**OFF**
31	**ON**	**ON**	**ON**	**ON**	**ON**

三、About Registers

3.1: The related information about relay output modules (less than 16 channels)(applicable to RS485/RS232/LAN)

Modbus Register address	PLC Address	Controlling coil of registers	Compatible function code	Related products	Explanation
0000H	40001	Coil Q0.0 Coil Q0.1 Coil Q0.2 Coil Q0.3 Coil Q0.4 Coil Q0.5 Coil Q0.6 Coil Q0.7 Coil Q0.8 Coil Q0.9 Coil Q1.0 Coil Q1.1 Coil Q1.2 Coil Q1.3 Coil Q1.4 Coil Q1.5	01 , 03 05 , 06 15 , 16	4-channel、 8-channel 12-channel、 16-channel、 20-channel、 24-channel 32-channel、 64-channel (relay output, transistor output)	1=close 0=Open readable Editable No saving

3.2: The related information about relay output registers of 16-31 channels (applicable to RS485/RS232/LAN)

Modbus Register address	PLC Address	Channels of register control coil output	Compatible function codes	The related products	Explanation
0001H	40002	Coil Q1.6 Coil Q1.7 Coil Q1.8 Coil Q1.9 Coil Q2.0 Coil Q2.1 Coil Q2.2 Coil Q2.3 Coil Q2.4 Coil Q2.5 Coil Q2.6 Coil Q2.7 Coil Q2.8 Coil Q2.7 Coil Q3.0 Coil Q3.1	01 , 03 05 , 06 15 , 16	4-channel、 8-channel、 12-channel、 16-channel、 -channel、 24-channel、 32-channel、 64-channel (relay output, transistor output)	1=close 0=open readable editable Break off No saving

3.3: The related information about the relay output registers of 32-47 channels(applicable to RS485/RS232/LAN)

Modbus Register address	PLC Address	Register control coil	Compatible function codes	The related products	Explanation
		Coil Q3.2 Coil Q3.3 Coil Q3.4 Coil Q3.5 Coil Q3.6 Coil Q3.7 Coil Q3.8 Coil Q3.9	01 , 03 05 , 06 15 , 16	4-channel、 8-channel、	1=Close 0=open Readable Editable Break off No saving

0002H	40003	Coil Q4.0 Coil Q4.1 Coil Q4.2 Coil Q4.3 Coil Q4.4 Coil Q4.5 Coil Q4.6 Coil Q4.7		12-channel、 16-channel 20-channel、 24-channel 32-channel、 64-channel (relay output, transistor output)	

3.4: The related information about relay output registers of 48-63 channels(applicable to RS485/RS232/LAN)

Modbus Register address	PLC Address	Register control coil	Compatible function codes	The related products	Explanation
0003H	40004	Coil Q4.8 Coil Q4.9 Coil Q5.0 Coil Q5.1 Coil Q5.2 Coil Q5.3 Coil Q5.4 Coil Q5.5 Coil Q5.6 Coil Q5.7 Coil Q5.8 Coil Q5.9 Coil Q6.0 Coil Q6.1 Coil Q6.2 Coil Q6.3	01 , 03 05 , 06 15 , 16	4-channel、 8-channel 12-channel、 16-channel 20-channel、 24-channel 32-channel、 64-channel (relay out, transistor output)	1=close 0=open Readable editable Break off No saving

3.5: The related information about the registers with less than 16 channels(applicable to RS485/RS232/LAN)

Modbus Register address	PLC address	Input channel	The corresponding position of the input channel	Compatible function codes	The related products	Explanation
0004H	40005	1st channel DI	40005.00	03、 16	4-channel、 8-channel、 12-channel、 16-channel -channel、 24-channel 32-channel、 64-channel compatible with NPN and PNP	1=Valid 0=invalid Read only Break off No saving
		2nd channel DI	40005.01			
		3rd channel DI	40005.02			
		4th channel DI	40005.03			
		5th channel DI	40005.04			
		6th channel DI	40005.05			
		7th channel DI	40005.06			
		8th channel DI	40005.07			
		9th channel DI	40005.08			
		10th channel DI	40005.09			
		11th channel DI	40005.10			
		12th channel DI	40005.11			
		13th channel DI	40005.12			
		14th channel DI	40005.13			
		15th channel DI	40005.14			
		16th channel DI	40005.15			

3.6: The related information about the digital input registers of 17-32 channels(applicable to RS485/RS232/LAN).

Modbus Register address	PLC address	Input channel	The corresponding position of the input channel	The compatible function codes	The related products	Explanation
0005H	40006	17th channel DI	40006.00	03、16	4-channel、8-channel、12-channel、16-channel、20-channel、24-channel、32-channel、64-channel (compatible with NPN and PNP)	1=Valid 0=Invalid Read only Break off No saving
		18th channel DI	40006.01			
		19th channel DI	40006.02			
		20th channel DI	40006.03			
		21st channel DI	40006.04			
		22nd channel DI	40006.05			
		23rd channel DI	40006.06			
		24th channel DI	40006.07			
		25th channel DI	40006.08			
		26th channel DI	40006.09			
		27th channel DI	40006.10			
		28th channel DI	40006.11			
		29th channel DI	40006.12			
		30th channel DI	40006.13			
		31st channel DI	40006.14			
		32nd channel DI	40006.15			

3.7: The related information about the digital input registers of 33-48 channels(applicable to RS485/RS232/LAN).

Modbus Register address	PLC address	Input channel	The corresponding position of the input channel	The compatible function codes	The related products	Explanation
0006H	40007	33rdchannel DI	40007.00	03、16	4-channel、8-channel 12-channel、16-channel 20-channel、24-channel 32-channel、64-channel Compatible with NPN and PNP	1=valid 0=invalid Read only **Break off No saving**
		34th channel DI	40007.01			
		35th channel DI	40007.02			
		36th channel DI	40007.03			
		37th channel DI	40007.04			
		38th channel DI	40007.05			
		39th channel DI	40007.06			
		40th channel DI	40007.07			
		41st channel DI	40007.08			
		42nd channel DI	40007.09			
		43rd channel DI	40007.10			
		44th channel DI	40007.11			
		45th channel DI	40007.12			
		46th channel DI	40007.13			
		47th channel DI	40007.14			
		48th channel DI	40007.15			

3.8: The related information about the digital input registers of 49-64 channels

Modbus Register address	PLC address	Input channel	The corresponding position of the input channel	The compatible function codes	The related products	Explanation
0007H	40008	49th channel DI	40008.00	03、16	4-channel、8-channel、12-channel、16-channel、20-channel、24-channel、32-channel、64-channel Compatible with PNP and NPN	1=valid 0=invalid Read only **Break off** **No saving**
		50th channel DI	40008.01			
		51st channel DI	40008.02			
		52nd channel DI	40008.03			
		53rd channel DI	40008.04			
		54th channel DI	40008.05			
		55th channel DI	40008.06			
		56th channel DI	40008.07			
		57th channel DI	40008.08			
		58th channel DI	40008.09			
		59th channel DI	40008.10			
		60th channel DI	40008.11			
		61st channel DI	40008.12			
		62nd channel DI	40008.13			
		63rd channel DI	40008.14			
		64th channel DI	40008.15			

3.9 Registers of Special Functions

Registers of special functions	The related products	Modbus address 16 bytes	PLC address	Default	Compatible function codes	compatible with step-step operation	Properties
Overtime time registers(high 16 bytes +low 16 bytes)	(relay/transistor module(digital input module	7530H (high 16 bytes)	430001	0x0000	03、06、16	NO	1=Close 0=Open Readable Editable Break off Saving
		7531H (low 16 bytes)	430002	0x2710 (10s)			
Mask off code registers of Frontal 16 channels	4channels，8 channels，16 channels，24 channels，32 channels (relay/transistor modules)	7532H OR mask off code	430003	0x0000			
		7533H AND mask off code	430004				
Mask off registers of rear 16 channels	24 channels，32 channels (relay/transistor modules)	7534H OR mask off code	430005				
		7535H AND mask off code	430006				

Explanation about Overtime time registers:

It is reckoned as communication overtime if the communication is broken for some reasons and the breakdown time is beyond that specified in the register. The indicator is ON until the problem is solved.

At the time of breakdown, the output states of channels are decided by the following formula.

“ Output state=(pre-overtime/OR)&AND”

Overtime output state	**OR** OR mask off code	**AND** AND mask off code
Keeping the same	**0**	**1**
Open(default)	**0**	**0**
Close	**1**	**1**

Just take the relay module of 16 channels as an example to explain.

when the communication breakdown lasts for 3 seconds, 0-7 channels open, 8-11 channels remain unchanged and 12-15 channels close.

1) First, set the overtime time to be 3 seconds, i.e. register 7530H=0x0000 and 7531=0x0bb8
   Analysis: 【0x0000(high 16 bytes) *65536】+ 0x0bb8(low 16 bytes) = 0x0bb8 （i.e. 3000mS）
2) Second, set the corresponding OR mask off register or AND mask off register.
   7532H=0xF000 （1111 0000 0000 0000）
   7533H=0xFF00 （1111 1111 0000 0000）
3) The result comes out 3 seconds after the communication breakdown.

Attention: The user just needs to set the frontal 16 mask off registers in the case of 16 channel relay module and in the case of 4 channel relay module or 32 channel relay module, the rear 16 mask off registers are also required to be set.

Chapter 4 Function Codes Explanation for RS232 and RS485 Modules

4.1 An Brief introduction to Modbus-RTU working principle.

Modbus-RTU protocol works under the mode of response with enquiry. The main station sends an order to the specified address of the sub station and the message includes the main station command on the sub-station and the affiliated inform that is necessary to execute the order. The selected sub-station starts to carry out the order once it receives it from the main station and feedback to the main station according to the execution. If the order is carried out successfully, the feedback is normal and an abnormal feedback will be sent to the main station if the sub-station failed to execute the order. The main station makes a judgment according to the feedback and decides what to do next.

4. 2: Modbus-RTU function codes

Function codes	Objects	Functions	Properties	The related products
01	Coil	Read multiple coils	read	(relay/transistor)module
02	Dispersed registers	Read multiple dispersed registers	read	Digital input module
03	Holding registers	Read multiple holding registers	read	(relay/transistor)module Digital input module
05	Coil	Edit a single coil	edit	(relay/transistor)module
06	Holding registers	Edit a single holding register	edit	(relay/transistor)module
15	Coil	Edit multiple coils	edit	(relay/transistor)module
16	Holding registers	Edit multiple holding registers	edit	(relay/transistor)module Digital input module

4.3：Illustration of Function Codes:

4.3.1: No.01 code The state of reading coil

No.01 code can read 1 or several coils successively from the address 0-31 according to the user's demand.

Attention: It can not read the coil that does not exist within the scope. It will feedback ERROR if it is asked to do so.

1)The main station demand(from the PLC/touching screen/ computer)

For example, the state of reading 16 coils starting from Coil 0.

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function Code	1 byte	0x01	0x01
Initial address	2 bytes	0x0000～0x000F	0x0000
Coil quantity	2 bytes	0x0001～0x0010	0x0010
CRC verification	2 bytes	0x0000～0xFFFF	0x3DC6

Attention： The amount of demanded coils must be controlled within the maximum of module channel. Otherwise, the module will feedback ERROR.

2）Normal response from the sub-station

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x01	0x01
Byte quantity	2 bytes	N	0x02
Input state	N bytes	0x0001～0x0010	0x00FF
CRC Verification	2 bytes	0x0000～0xFFFF	0XF9BC

Remarks: N=coils quantity/8, if the remainder is not 0, N=N+1.
The result is 0 for coil of Q15~Q8 and 1 for Q7~Q0.

3）Abnormal response from the sub-station

Message contents	Length	Scope	Sample
Sub-station	1 byte	0x00∽0x1F	0x01
Function code	1 byte	0x81	0x81
Error code	1 byte	0x01（not a supported function code）	0x01
		0x02（initial address is out range of the scope）	
		0x03（the coil quantity is beyond the scope）	
		0x04（data verification error）	
CRC verification	2 bytes	0x0000∽0xFFFF	0x8190

4.3.2: No. 02 code The state of reading the dispersed digital input register.

It can read 1 or several input states successively from the address 0-31 according to the user's

requirement.

Attention: It can not read the input state that does not exist. It will feedback ERROR if it is asked to do so.

1) The main station demand(from the PLC/touching screen/ computer)

For example, the state of reading 16 coils starting from Coil 0.

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x02	0x02
Initial address	2 bytes	0x0000～0x000F	0x0000
Input quantity	2 bytes	0x0001～0x0010	0x0010
CRE verification	2 bytes	0x0000～0xFFFF	0x79C6

Attention： The amount of demanded coils must be controlled within the maximum of module channel. Otherwise, the module will feedback ERROR.

2）Normal response from the sub-station

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x02	0x02
Initial address	2 bytes	N	0x02
Input quantity	N bytes	0x0001～0x0010	0x00FF
CRE verification	2 bytes	0x0000～0xFFFF	0XF9F8

Remarks: N=coils quantity/8, if the remainder is not 0, N=N+1.

The result is 0 for coil of DI15~DI8 and 1 for DI7~DI0.

3）Abnormal response from the sub-station

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x82	0x82
Error code	1 byte	0x01（not a supported function code）	0x01
		0x02（the initial address is out range of the scope）	
		0x03（the coil quantity is beyond the scope）	
		0x04（data verification error）	
CRC verification	2 bytes	0x0000～0xFFFF	0x8160

4.3.3 No.03 code The state of reading the coil or digital input of holding registers.

Attention: it can not read the dispersed register or the holding register that does not exist. Otherwise, the module will feedback ERROR.

1）Demand from the main station

The main station demanding to read 1 holding register from address 0000H.

Message contents	Length	Scope	Sample
Substation address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x03	0x03
Initial address	2 bytes	0x0000～0x000F	0x0000
Input quantity	2 bytes	0x0001～0x0010	0x0001
CRC Verification	2 bytes	0x0000～0xFFFF	0x840A

2） Normal response from the sub-station

Message contents	Length	Scope	Sample
Substation address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x03	0x03
Byte quantity	1 byte	N	0x02
Input state	N bytes		0x00FF
CRC verification	2 bytes	0x0000～0xFFFF	0xF804

Attention: N=the valid byte number
When the substation works in a normal way, the coil state for Q15-Q8 is 0 and Q7-Q0 1.

3） Abnormal response from the sub-station

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x83	0x83
Error code	1 byte	0x01（not a supported function code）	0x01
		0x02（the initial address is out range of the scope）	
		0x03（the holding register does not exist）	
		0x04（data verification error）	
CRC verification	2 bytes	0x0000～0xFFFF	0x80F0

4.3.4: No. 05 code The state of editing a single coil.

Attention: the specified coil must exist and is editable. Otherwise, the module will feedback ERROR.

1) **The main station demand**

The main station demands to turn the coil state into Close, i.e. Q0=1.

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x05	0x05
Coil address	2 bytes	0x0000～0x000F	0x0000
Coil state	2 bytes	0x0000 or 0Xff00	0xFF00
CRC Verification	2 bytes	0x0000～0xFFFF	0x8C3A

2）Normal response from the sub-station

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00∽0xlF	0x01
Function code	1 byte	0x05	0x05
Coil address	2 bytes	0x0000∽0x000F	0x0000
Coil state	2 bytes	0x0000 or 0xFF00	0XFF00
CRC Verification	2 bytes	0x0000∽0xFFFF	0x8C3A

3）Abnormal response from the sub-station

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00∽0xlF	0x01
Function code	1 byte	0x85	0x85
Error code	1 byte	0x01（not a supported function code）	0x01
		0x02（the coil does not exist）	
		0x03（the coil data is out the range of the scope）	
		0x04（data verification error）	
CRC verification	2 bytes	0x0000∽0xFFFF	0x8350

4.3.5: NO. 06 code The state of editing a single holding register

Attention: The holding register specified in the request message must exist and be writable, otherwise the module will feedback ERROR

1) The main station demand

The main station asks the constant 0x0001 to be edited into the holding register 0000H.

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x06	0x06
Initial address	2 bytes	0x0000～0x000F	0x0000
Register value	2 bytes	0x0000～0xFFFF	0x0001
CRC verification	2 bytes	0x0000～0xFFFF	0x480A

2）Normal response from the sub station

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x06	0x06
Initial address	bytes	0x0000～0x000F	0x0000
Register value	2 bytes	0x0000～0xFFFF	0x0001
CRC verification	2 bytes	0x0000～0xFFFF	0x480A

3）Abnormal response from the sub-station

Message contents	Length	Scope	Sample
Substation address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x86	0x86
Error code	1 byte	0x01（not a supported function code）	0x01
		0x02（the initial address is out the range of the scope.）	
		0x03（the holding register does not exist.）	
		0x04（data verification error）	
CRC verification	2 bytes	0x0000～0xFFFF	0x830A

4.3.6: No. 15 code The state of editing several coils

Attention: the specified coil must exist and is editable. Otherwise, the module will feedback ERROR.

1) The Main station Demand

The main station asks to edit a coil. The state of coil from 0-16 is 1, i.e. Q15=1 and Q14-Q00 is 0.

Message contents	Length	Scope	Sample
Substation address	1 byte	0x00∽0x1F	0x01
Function code	1 byte	0x0F	0x0F
Initial address	2 bytes	0x0000∽0x000F	0x0000
Coil quantity	2 bytes	0x0001∽0x0010	0x0010
Byte quantity	1 byte	N	0x02
Coil state	N bytes		0x8000
CRC verification	2 bytes	0x0000∽0xFFFF	0x83E0

Attention: N=coil quantity/8, if the remainder is not 0, N=N+1

2）**Normal response from the sub-station**

Message contents	Length	Scope	Sample
Substation address	1 byte	0x00∽0xlF	0x01
Function code	1 byte	0x0F	0x0F
Initial address	2 bytes	0x0000∽0x000F	0x0000
Coil quantity	2 Bytes	0x0001∽0x0010	0x0010
CRC verification	bytes	0x0000∽0xFFFF	0x5407

3）**Abnormal response from the sub-station**

Message contents	Length	Scope	Sample
Substation address	1 byte	0x00∽0x1F	0x01
Function code	1 byte	0x8F	0x8F
Error code	1 byte	0x01（not a supported function code）	0x01
		0x02（the initial address does not exist）	
		0x03（the coil quantity is out the range of the scope.）	
		0x04（data verification error）	
CRC verification	2 bytes	0x0000∽0xFFFF	0x85F0

4.3.7: No. 16 code the state of editing several holding registers

Attention: the specified register must exist and is editable. Otherwise, the module will feedback ERROR.

1）Main station demand

The main station asks to edit 4 holding registers from 30000. 30000 and 30001 refer to the overtime time parameters and their values are the same, i.e. 0x00002710(10000mS). 30002 and 30003 refer to the parameters of OR mask off code and AND mask off code and their values are 0xFFFF and 0x0081 respectively. In the case of overtime breakdown, the module output Q7 and Q0 mean Close and the states of other cases remain unchanged.

Message contents	Length	Scope	Sample
Substation address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x10	0x10
Initial address	2 bytes	0x7530	0x7530
Register quantity	2 bytes	N	0x0004
Byte quantity	1 byte	2*N	0x08
Register Value	2*N bytes		0x0000, 0x2710
			0x0081, 0xFFFF
CRC verification	2 bytes	0x0000～0xFFFF	0xD383

Attention: N must be the even numbers that are greater than 0, such 2,4,6,8,etc.

2）Normal response from the sub-station

Message contents	Length	Scope	Sample
Sub-station address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x10	0x10
Initial address	2 bytes	0x7530	0x7530
Register quantity	2 bytes	N	0x0004
CRC verification	2 bytes	0x0000～0xFFFF	0xDBC9

3）Abnormal response from the sub-station

Message contents	Length	Scope	Sample
Substation address	1 byte	0x00～0x1F	0x01
Function code	1 byte	0x90	0x90
Error code	1 byte	0x01（not a supported function code）	0x01
		0x02（the initial address does not exist.）	
		0x03（the register quantity goes beyond the scope）	
		0x04（data verification error）	
CRC verification	2 bytes	0x0000～0xFFFF	0x8DC0

Chapter 5 Setting for RS232 Reading Communication

	Register address	Scope	Compatible Function Codes	Explanation
Baud Rate	10100	0=NONE_232 1=1200bps 2=2400bps 3=4800bps 4=9600bps 5=19200bps 6=38400bps 7=57600bps 8=115200bps	03	RS232 can only read the setting state of communication
ODD-EVEN Verification	10101	0：No verification 1： ODD verification 2： EVEN verification		
Stop bit	10102	0： 1 stop bit 1： 2 stop bits		
Module address	10103	Address scope:0-31		

Chapter 6 Setting of RS485 Reading Communication

	Register address	Scope	Compatible Function Codes	Explanation
Baud Rate	10104	0=NONE_485 1=1200bps 2=2400bps 3=4800bps 4=9600bps 5=19200bps 6=38400bps 7=57600bps 8=115200bps	03	RS485 can only read the setting state of communication
ODD-EVEN Verification	10105	0：No verification 1：ODD verification 2 :EVEN verification		
Stop bit	10106	0：1 stop bit 1: 2 stop bits		
Module address	10107	Address scope: 0-31		

七、MODBUS-TCP

7.1: Setting of Ethernet

	Format	Register address	Default
IP address	xx .xx .xx .xx	10000. 10001. 10002. 10003	192.168.1.80
Mask off code of subnet	xx .xx .xx .xx	10004. 10005. 10006. 10007	255.255.255.0
Gateway	xx .xx .xx .xx	10008. 10009. 10010. 10011	192.168.1.1
Port No.	xxxxx (Scope 0~65535)	10012	8080
Remote IP Address	xx .xx .xx .xx	10013. 10014. 10015. 10016	
Remote Port	xxxxx (Scope 0~65535)	10017	4000
Working mode	0: User 1: Sever 2: UDP mode	10018	0:User
MAC hardware address	xx:xx:xx:xx:xx:xx	10019~10024	12:41:171:124:00:01

7.2: Modification of IP address

The modification of Ethernet communication is realized by the adjustment of IP and gateway of the corresponding registers RS232 or RS485. It is necessary to re-start the device to make the medication valid.

7.2.1 modification of module IP

For example: Use 10 codes to modify the register corresponding to the module's IP address through RS485 or RS232

Send: **01 10 27 10 00 04 08 00 C0 00 A8 00 01 00 C7 B2 24**

01: The module address is the dial code address.

10：Edit several registers

27 10：The module IP address consists of 4 parts, starting from 10000 to 10003.

00 04：The quantity of the registers that can be edited simultaneously.

08：Byte quantity of the editable registers

00 C0 : The first byte in the IP address

00 A8 : The second byte in the IP address

00 01 : The 3rd byte in the IP address

00 C7 : The 4th byte in the IP address

B2 24 : The CRC of the sent Data

7.2.2 Modification of gateway of the module

Use No.10 code of RS485 or RS232 to modify the corresponding register of the default gateway. **01 10 27 13 00 04 08 00 C0 00 A8 00 01 00 01 32 76**

01: The module address, i.e. the dial code address

10：Edit several registers

27 13：The module gateway address consists of 4 parts, starting from10000 to 10003.

00 04：The quantity of the registers that can be edited simultaneously.

08: Byte quantity of the editable registers

00 C0 : The first byte in the IP address

00 A8 : The second byte in the IP address

00 01 : The 3rd byte in the IP address

00 01 : The 4th byte in the IP address

32 76 : CRC The CRC of the sent Data

7.2.3 Modification of module port(customized module could modify module port number)

Use No. 10 code of RS485 or RS232 to modify the corresponding register of the module port.

01 10 27 1C 00 01 02 00 01 32 CE

01 : The module address, i.e. the dial code address.

10 ： Edit several registers

27 1C ： The module port address consists of 4 parts, starting from 10012.

00 01 ： The quantity of register that can be edited alone.

02 ： The byte quantity of the editable registers. N= editable register quantity*2

00 01 : The port value is 1 with the scope of 0-65535.

32 CE ： CRC The CRC of the sent data

MODBUS-TCP Protocol

Its function codes are compatible with MODBUS-RTU and can work with the following function codes.

Function codes	Object	Functions	Properties	The related products
01	Coil	Read several coils	Read	(relay/transistor)module
02	Dispersed registers	Read several dispersed registers	Read	digital input module
03	Holding register	Read several holding registers	Read	(relay/transistor)module Digital input module
05	Coil	Edit a single coil	edit	(relay/transistor)module
06	Holding register	Edit a single holding register	edit	(relay/transistor)module
15	Coil	Edit several coils	edit	(relay/transistor)module
16	Holding registers	Edit several holding registers	edit	(relay/transistor)module digital input module

This explanation aims to show the difference between MODBUS-TCP and MODBUS-RTU.

Just take NO. 06 code for example to explain. If input 0x1234 into register 0x0001(hardware address is 1), MODBUS-RTU will send the data 01 06 00 01 12 34 D5 7D while MODBUD-TCP xx xx 00 00 00 06 01 06 00 01 12 34

Illunstration of MODBUS-TCP: xx xx, checking the information(relay module takes responsibities of this and send the data back to the main station directly)

00 00：referring to the MODBUS-TCP protocol

00 06：referring to the Number of the valid bytes

01：MODBUS hardware address

06： function code

00 01： target register address

12 34：register value

MODBUS-TCP returning code:xx xx 00 00 00 06 01 06 00 01 12 34

In the case of No. 06 code, the sending code is same as the returning code

00 00：representing the MODBUS-TCP protocol

00 06：referring to the Number of the valid bytes

01：MODBUS hardware address

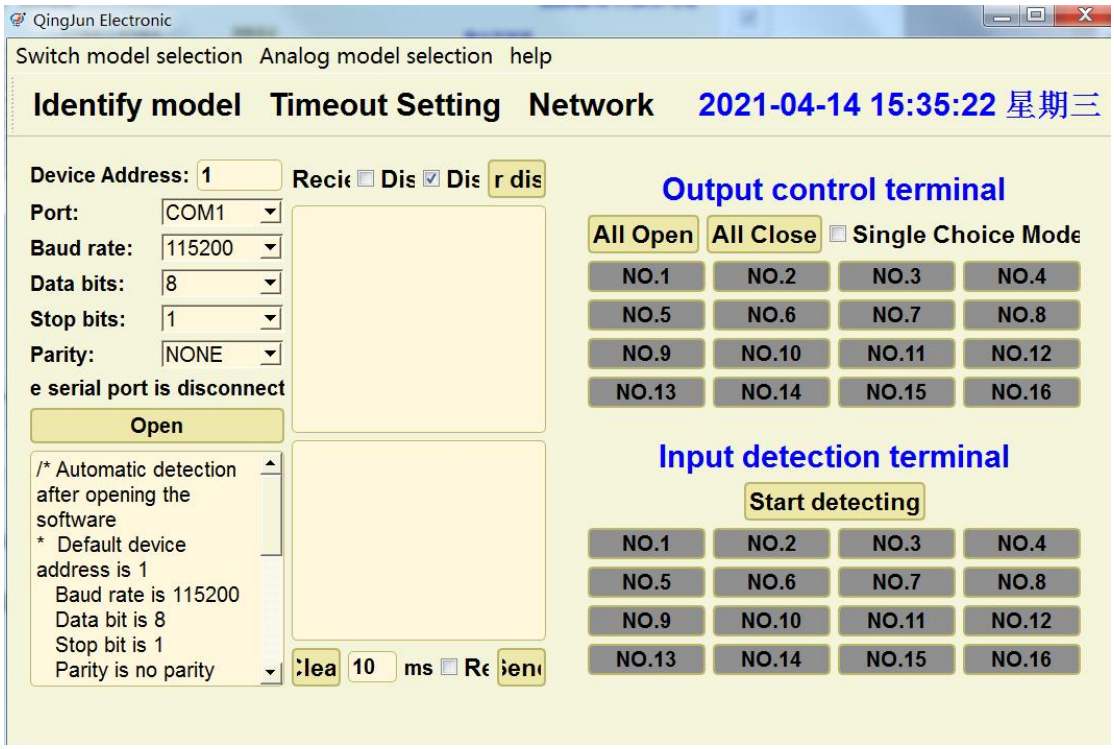
06：function code(single register)

00 01：target register address

12 34：register value

What described above shows the difference between MODBUS-TCP protocol and MODBUS-RTU protocol. It is true of the other function codes.

八、PC Testing



The software of PC testing is provided by our company to test, configure and check the function of the module parameters. Please get the USB adapter for RS485, or USB adapter for RS232 or the serial port for DB9 ready in advance and connect the computer to the module and the software will automatically search for the module when the power supply is switched on. If the module can not recognize the order, that would necessitate a manual operation to control the module in the way as below. Click “serial port” after selecting IP address, port, Baud rate, data bit, stop bit, verification bit and choose the product type in left top corner. Thus you can control the module with the control bottoms on the right side.

The demos of all brands of PLCs and configuration software of touch screens and the solutions are available in our company. Please contact us without hesitation if you want to know moe details about the products.

Foshan Qingjun Electronics Co., Ltd.
Address：Room 307，the 3rd floor， Building B，Chaofa Chuangyi Park，2# Lianhe Road，Nanhai District，Foshan city，Guangdong，China.
TEL：（86）1770 8670 771
FAX：（86）0757 81809249
Company website：fsqjkj.en.alibaba.com