Modbus/ Profibus-DP Gateway

PM-160

User Manual

REV 2.3

Sibotech Automation Co., Ltd

Technical Support: +86-21-5102 8348
E-mail: support@sibotech.net

Table of Contents

1 About This Document....3
1.1 General....3
1.2 Important user information....3
1.3 Terms....3
2 About the Gateway....4
2.1 Product Function....4
2.2 Technical Specifications....4
2.3 Electromagnetic Compatibility....5
2.4 Attention....6
2.5 Related Products....6
3 Quick Start Guide....7
3.1 Wiring power....7
3.2 Wiring with PC....7
3.3 Configuration method....7
3.4 Wiring with serial device....8
3.5 Wiring Profibus-DP interface....8
3.6 Debug....9
4 Hardware Descriptions....10
4.1 Product appearance....10
4.2 Indicators....10
4.3 Configuration switch....11
4.3.1 Status setting switch....11
4.3.2 Setting switch of Profibus-DP address....11
4.4 Interface....12
4.4.1 Power Interface....12
4.4.2 Profibus-DP interface....12
4.4.3 RS-485/RS-422 interface....12
4.4.4 RS232 interface....13
5 Instructions of Configuration Software....14
5.1 Notes before configurating....14
5.2 User Interface....15
5.3 The operation of equipment view....17
5.3.1 Equipment view interface....17
5.3.2 Operation mode of equipment view....17
5.3.3 Operation types of equipment view....18
5.4 The operation of configuration view....19
5.4.1 Interface of fieldbus configuration view....19
5.4.2 Interface of subnet configuration view....20
5.4.3 Interface of node configuration view....24
5.4.4 Interface of command configuration view....24

5.4.5 Notes View 26
5.5 Conflict Detect 26
5.5.1 Operation of command list 27
5.5.2 Operation of memory mapping area 27
5.6 Hardware communication 28
5.6.1 Serial Configuration 28
5.6.2 Upload configuration 29
5.6.3 Download configuration 29
5.7 Load and save configuration 30
5.7.1 Save Configuration project 30
5.7.2 Load configuration project 30
5.8 Output excel document 31
5.9 Debug 32
6Universal mode 35
6.1 Data exchange 35
6.2 Universal Protocol 36
7 How STEP7 Access Data of Gateway and Select Data Module 37
7.1 How STEP7 access data of gateway 37
7.2 How STEP7 select data module 38
8 Installation 40
8.1 Machine Dimension 40
8.2 Installation Method 40
9 Introduction to optional attachment 41
Appendix A: Using STEP 7 Set Profibus- DP 42
Appendix B: Modbus Protocol 48

1 About This Document

1.1 General

This manual describes every parameter of the gateway PM-160 and provides using methods and some announcements that help users use the gateway. Please read this document carefully before using the gateway.

1.2 Important user information

The data and examples in this document can not be copied without authorization. Sibotech maybe upgrades the product without notifying users.

SiboTech is the registered trade mark of SiboTech Automation Co., Ltd.

The product has many applications. The users must make sure that all operations and results are in accordance with the safety of relevant field, and the safety includes laws, rules, codes and standards.

1.3 Terms

Profibus-DP: Profibus-DP protocol

Modbus: Modbus Protocol

RS485/RS422/RS232: There kind of hardware specification of serial interface

PM-160: Modbus (RS485/RS232/RS422) /Profibus-DP gateway

2 About the Gateway

2.1 Product Function

The gateway PM-160 can connect multiple devices with Modbus/RS485/RS232/RS422 interface with Profibus-DP, and establish the communication between them. Modbus/RS485/RS232/RS422 network devices can be converted to Profibus-DP network devices.

2.2 Technical Specifications

1. Act as a Profibus-DP slave at the side of Profibus-DP, while Modbus master, Modbus slave and Universal mode can be selected at serial side and serial interface can be selected RS232, RS485 or RS422. The mapping of Profibus-DP and Modbus communication data area can achieve transparent communication of PROFIBUS and Modbus;
2. Serial: RS485, RS232, RS422, half-duplex. Baud rate: 300, 600, 1200, 2400, 9600, 19.2 K, 38.4K, 57.6K and 115.2Kbps can be selected. Parity check mode: None, Odd Even, Mark and space can be selected;
3. As a Modbus master supports 01H, 02H, 03H, 04H, 05H, 06H, 0FH and 10H function codes. It can be configured up to 48 Modbus commands. 03H and 04H support "**Word / Byte mapping**". Through the high-byte or low-byte mapping of the registers can effectively utilize Profibus-DP input-byte; **Support monitoring status of Modbus slave; Support clearing data or keep the last data when input-data is abnormal; Support re-transmitting data when response is timeout;**
4. As a Modbus slave supports 03H, 04H, 06H and 10H function codes;
5. Support the control mode of character timeout and character number in universal mode, and have the function of sending automatically;
6. DP/V0 Profibus-DP communication capability, in accordance with EN50170;
7. As a Profibus-DP slave, baud rate is self-adaptive, and the maximum baud rate is 12Mbps;
8. Profibus-DP input-byte and output-byte number can be freely set and the maximum input and output bytes are:

   Max Input bytes ≤224 Bytes

   Max Output bytes ≤224 Bytes

   Max Input Bytes + Output Bytes ≤224Bytes
9. Support clearing data or keep the last data when input-data is abnormal;
10. Update firmware function;
11. Power: 24VDC (11V~30V), 80mA;
12. Working circumstance temperature: -20~60℃, Humidity: 95%;
13. External dimensions:（Width）40mm*（Height）125mm*（Depth)110mm;

14. Installation: 35mm DIN RAIL;
15. Protection Level: IP20;
16. Test standard: In accordance with EMC test standard.

2.3 Electromagnetic Compatibility

High-frequency interference test (GB/T15153.1 classⅢ)

Imposed place	Power input circuit–GND Between the power input circuits AC input circuit–GND	
Imposed waveform	The first value of peak Oscillation frequency 1/2 Decay time The frequency of duplicate Impedance outputted by the test equipment	2.5～3kV 1.0～1.5MHz ≥6μs More than 50/s 150～200Ω

Fast Transient Pulse Burst Test (GB/T17626.4 classⅢ)

Voltage peak	Power input and AC input circuit：2kV Weak current circuit：1kV
Repetition rate	5 kHz

Electrostatic discharge interference (GB/T 17626.2 classⅢ)

Imposed place	Usual use ,the parts touched by the operator
Voltage, current	6kV contact discharge, the first peak of discharge current is 22.5A
Times	More than 10 times with the space more than 1 second in every part
Polarity	Positive

Radiate electromagnetic field (GB/T 17626.3 classⅢ)

Radio frequency	150MHz, 400MHz, 900MHz
Test field strength	10 V/m
Radiation method	Make the front of antenna touch devices, or near terminal, intermittently radiate radio wave

2.4 Attention

- To prevent stress, prevent module panel damage;
- To prevent bump, module may damage internal components;
- Power supply voltage control in the prospectus, within the scope of the requirements to burn module;
- To prevent water, water module will affect the normal work;
- Please check the wiring, before any wrong or short circuit.

2.5 Related Products

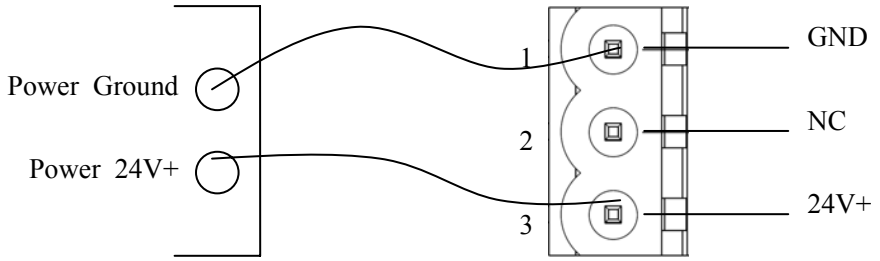
Other related products in SiboTech: PM-127, PM-125 and so on.

If you want to get more information about these products, please visit SiboTech website: http://www.sibotech.net/en , or call the technical support hotline: +86-21-5102 8348.

3 Quick Start Guide

3.1 Wiring power

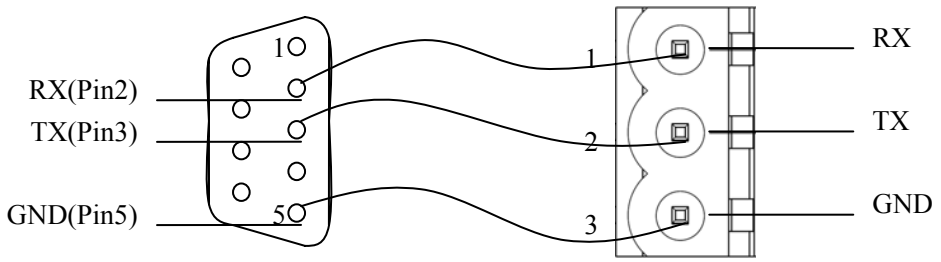
The power is 24V DC, wiring method is shown as follow:



Power: 24V DC The power interface of PM-160

3.2 Wiring with PC

Establish the connection the RS232 interface of gateway with PC, the wiring method is shown as follow:



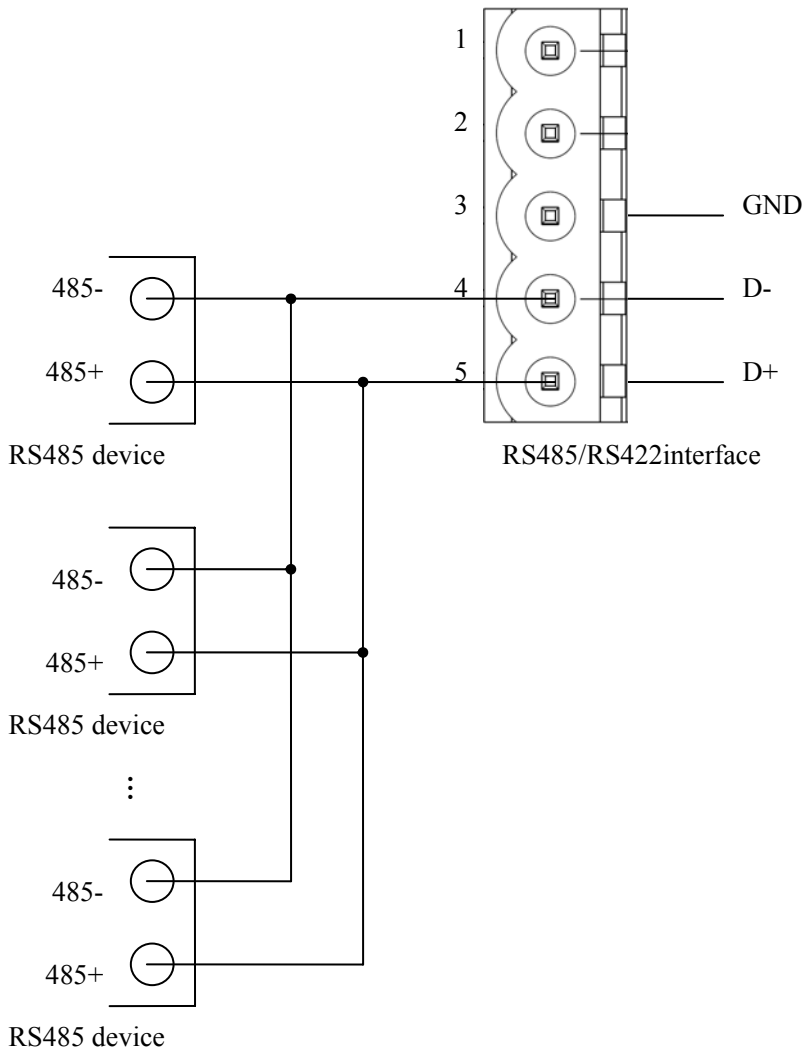
The RS232 interface of PC The RS232 interface of PM-160

3.3 Configuration method

Put the CD-ROM to the CD driver of PC, open the CD and install the configuration software GT-123. Users can finish the installation lightly according to the wizard. Take the “Mode” bit of DIP switch of PM-160 to the “Configure”, power on and the LED show “CF”, that is to say, PM-160 is in the status of configurating. Open the software GT-123 and users can configurate PM-160.

3.4 Wiring with serial device

After finishing configurating, wire communication interface, the wiring method of RS232 is the same with “wiring with PC”, the wiring method of RS485/RS422 is shown as follow:



When RS485 is in the communication of point to multi-point, to prevent the reflection and obstruction of signal, users need to use two terminal resistances in furthest ports of line, and the parameters are 120Ω 1/2W.

Note: There is no terminal resistances inside RS485 interface of PM-160.

3.5 Wiring Profibus-DP interface

Suggest wiring Profibus-DP with standard Profibus-DP connector. The description of Profibus-DP interface has been shown in chapter 4.4.2.

Set the address of Profibus-DP through the rotary switches on the panel.

Take the “Mode” bit of PM-160 to “Run”, and “Debug” bit to “Normal”, power on and LED show the address of Profibus-DP (decimalization).

Register GSD file (in the product CD) to Profibus-DP master configuration software (STEP7), and configurate parameters.

PBF light being off and STA light being blinking show the connection with Profibus-DP master is successful!

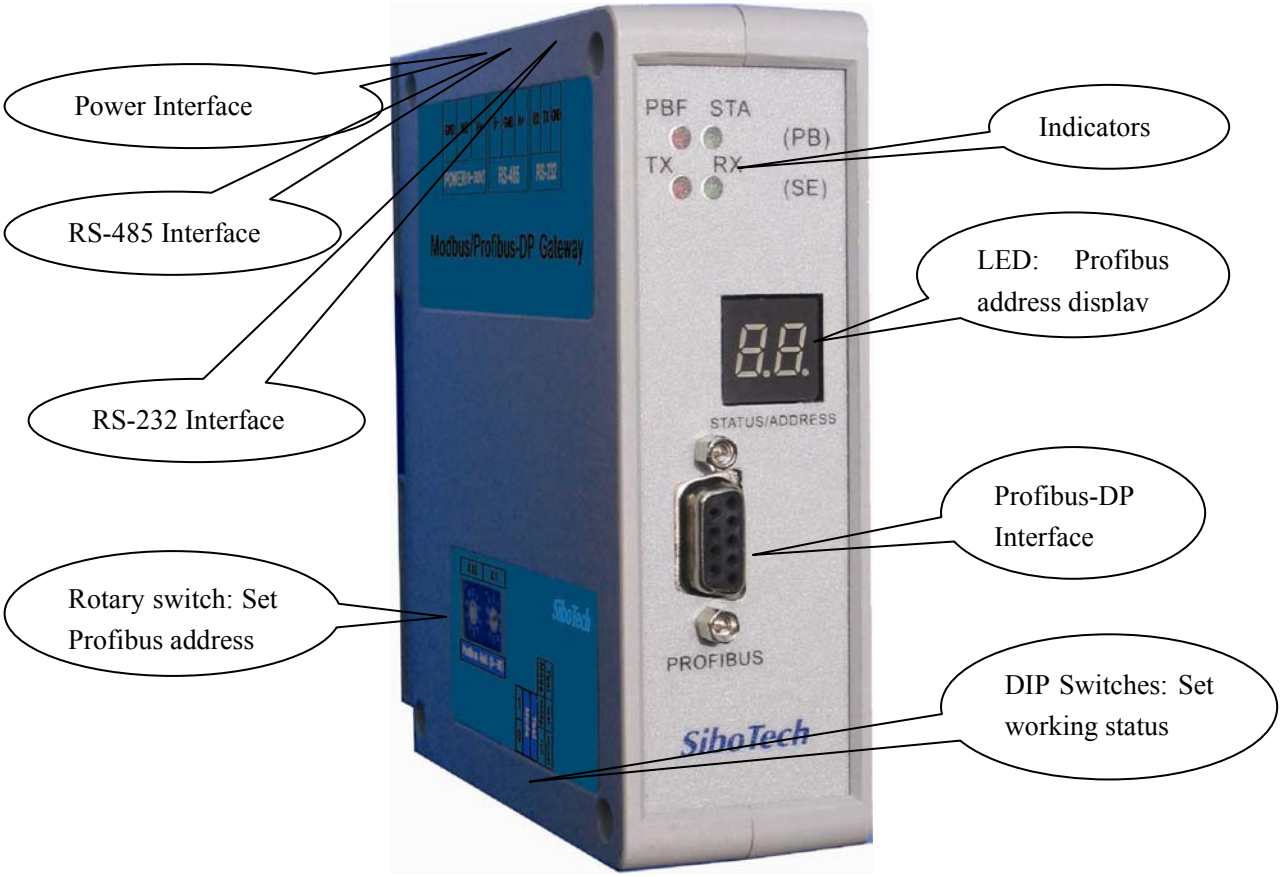
3.6 Debug

PM-160 has the function of debugging, and users can debug the communication of Modbus network when the gateway in the “Modbus master” mode. LED show “db” when the gateway in the status of debugging.

Note: PM-160 support the function of debugging only in the “Modbus master” mode!

4 Hardware Descriptions

4.1 Product appearance



Note: This picture is for reference only. Product appearance should accord to the real object.

4.2 Indicators

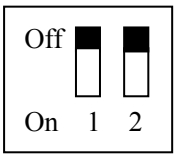
Indicator	Status	Description
PBF	Always Red	Profibus-DP communication fails.
	Close	Communication is ok.
STA	Green Blinking	Profibus-DP is communicating.
	Close	Be not communicating.
TX	Green Blinking	Serial port is sending data.
	Close	Serial has no data sent.
RX	Red Blinking	Serial port is receiving data.

	Red out	Serial has no data receive.

4.3 Configuration switch

4.3.1 Status setting switch

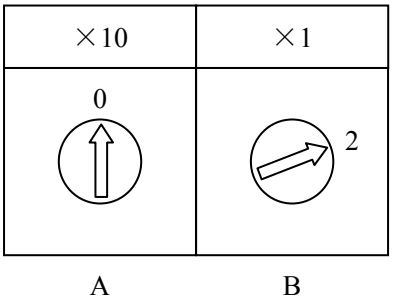
Configuration switch locates at the bottom of product, bit 1 is the debugging bit and bit 2 is the mode bit.



Mode（bit 2）	Debugging（bit 1）	Description
Off	Off	Running mode
Off	On	Debugging mode
On	Off or On	Configuration Mode

Note: After re-configure the switch, you have to restart the PM-160 to make the settings take effect!

4.3.2 Setting switch of Profibus-DP address

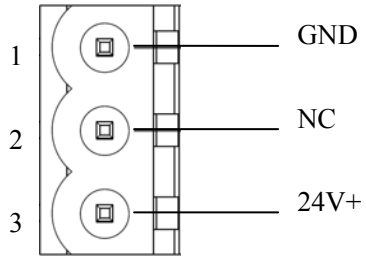


According to the above, the Profibus-DP address is calculated as follow:

Profibus-DP Address = （ A × 10 ） + （ B × 1 ）

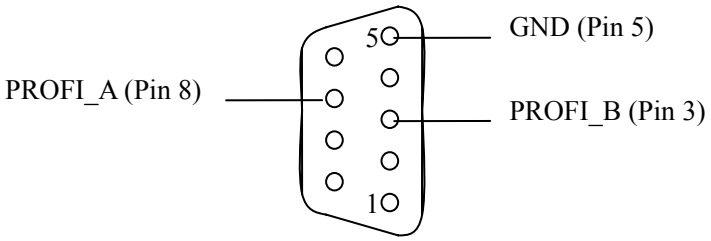
4.4 Interface

4.4.1 Power Interface



Pin	Function
1	GND
2	NC(No Connect)
3	24V+，DC plus 24V

4.4.2 Profibus-DP interface



Profibus-DP interface uses DB9 male-connector, and the pins are defined as follow:

Pin	Signal Description
3	PROFI_B，Data positive
5	GND
8	PROFI_A，Data negative

4.4.3 RS-485/RS-422 interface

The RS-485 interface of PM-160 is standard, and the RS-485 characteristics of the product are shown as follows:

1. The basic characteristics of RS-485 transmission technology

① Network topology: Linear bus, there are active bus termination resistors at both sides.

② Transfer rate: 300 bps~115.2Kbps.

③ Media: Shielded twisted-pair cable and also can cancel the shielding, depending on

environmental conditions (EMC).

④Site number: 32 stations per subsection (without repeater), and can up to 127 stations (with RS485 repeater).

⑤Plug connection: 3-pin pluggable terminal.

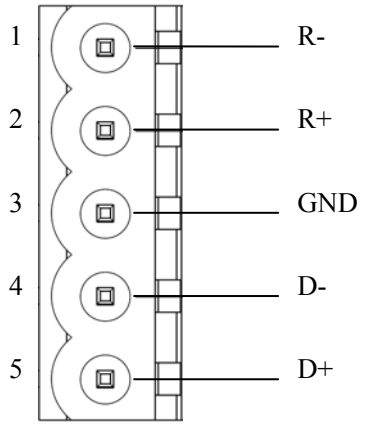
2. The main points on RS-485 transmission equipments installation

①All the equipments be connected with RS-485 bus;

②Subsection can be connected up to 32 sites;

③The farthest end of each bus has a termination resistor—120Ω 1/2W to ensure reliable operation of the network.

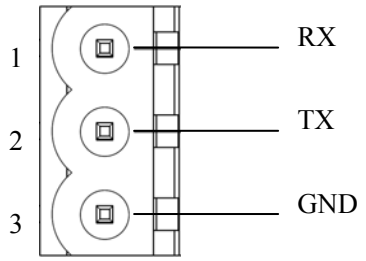
Serial interface uses 5-pin pluggable terminal and users can wire it according to the wiring instructions on the panel.



引脚	功能
1	R-，RS-422 Receive Negative
2	R+，RS-422 Receive Positive
3	GND
4	D-，RS-485/RS-422 Transmit Negative
5	D+，RS-485/RS-422Transmit Positive

4.4.4 RS232 interface

RS232 interface uses a 3-pin pluggable open terminal, and its pin description is shown as follows:



Pin	Function
1	RX，Connect user device RS232's RX
2	TX，Connect user device RS232's TX
3	GND，Connect user device RS232's GND

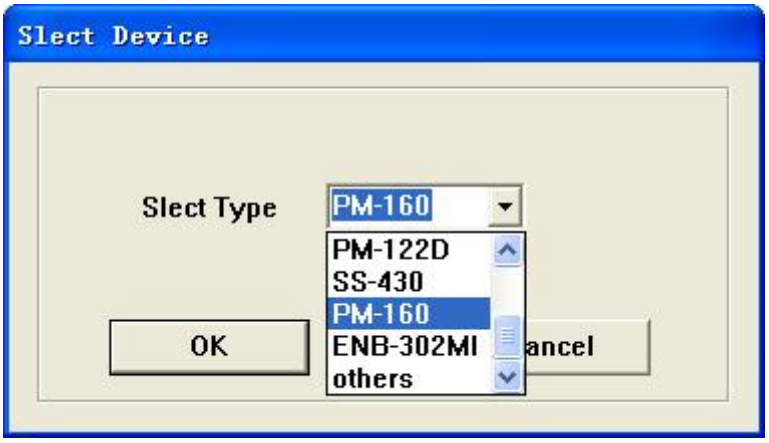
5 Instructions of Configuration Software

5.1 Notes before configurating

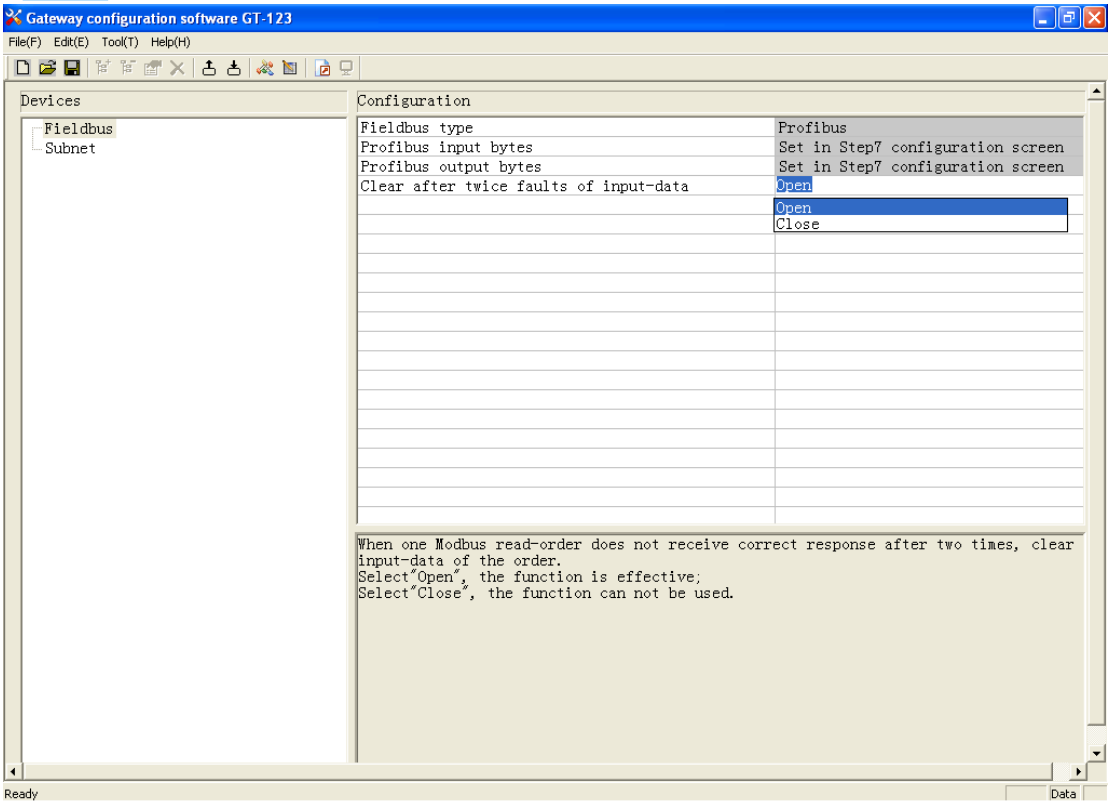
GT-123 is a product based on Windows platform, and used to configurate a variety of fieldbus gateway devices, including PM-120, MD-21, SS-430, PM-160 and other products. It can set related parameters and commands of Modbus and other bus.

The document mainly introduces the use method of PM-160.

Double-click the icon to enter the main interface of the software:



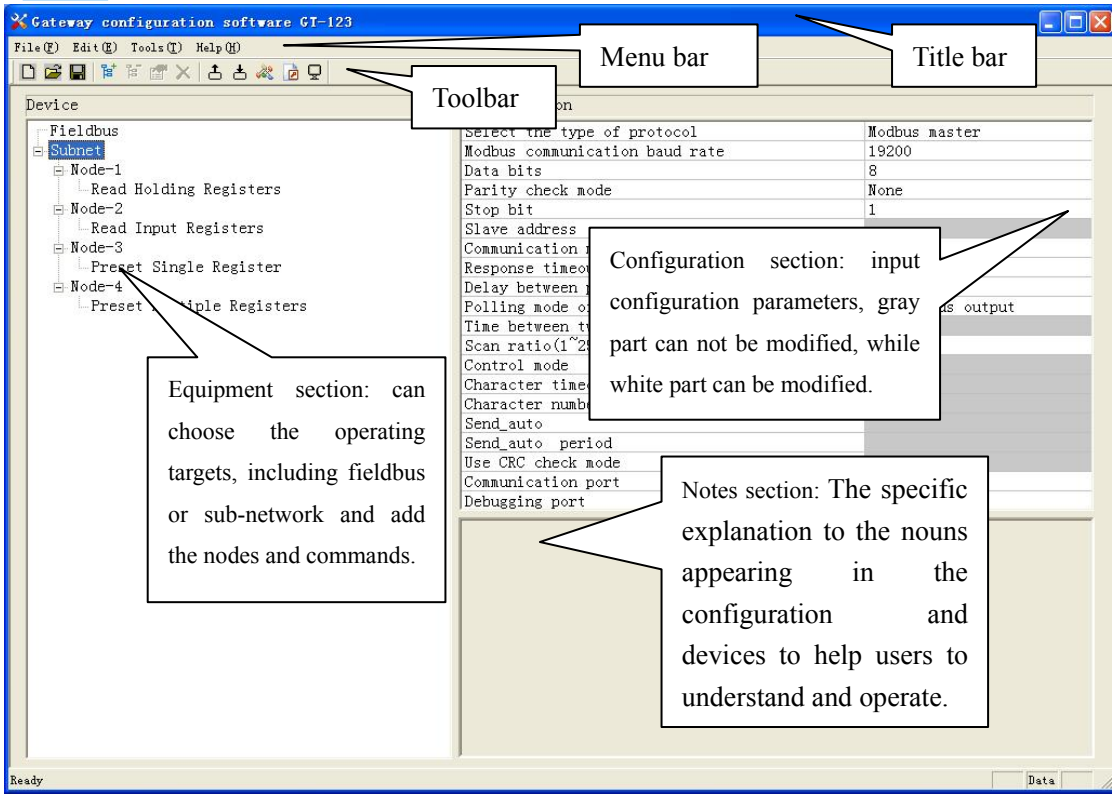
Choose "PM-160" to enter configuration interface:



5.2 User Interface

GT-123 interface include: title bar, menu bar, toolbar, status bar, equipment section, configuration section and notes section.

Note: All the gray part in the software can not be changed.



Toolbar is shown as below:

Functions separately from left to right are: new, open, save, add nodes, delete nodes, add commands, delete commands, upload configuration, download configuration, conflict detect, output Excel configuration document and debug.

New: Create a new configuration project

Open: Open a configuration project

Save: Save the current configuration

Add nodes: Add a Modbus slave node

Delete nodes: Delete a Modbus slave node

Add commands: Add a Modbus command

Delete commands: Delete a Modbus command

Upload configuration: Read the configuration from the module and show it in the software

Download configuration: Download the configuration from the software to the module

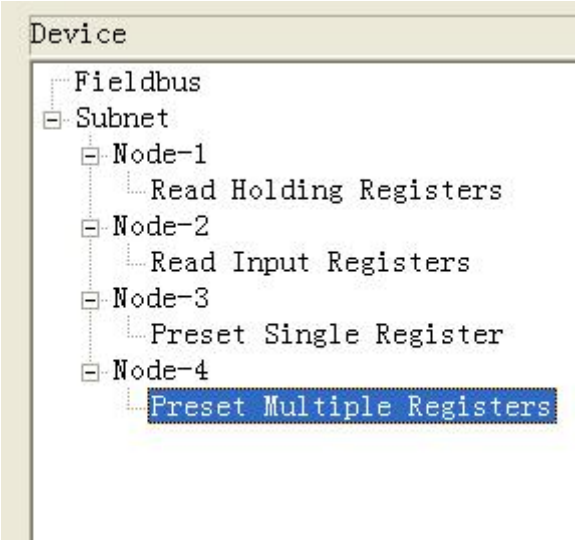
Conflict Detect: Detect whether there is conflict in memory data buffer of the gateway

Output Excel document: Output the current configuration to local hard disk and save it as .xls file

Debug: For debugging Modbus communications, and defining the network fault.

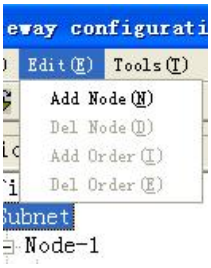
5.3 The operation of equipment view

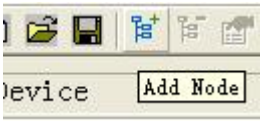
5.3.1 Equipment view interface

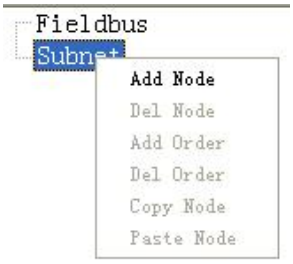


5.3.2 Operation mode of equipment view

The equipment view supports three types of operation: Edit Menu, Edit Toolbar and Right click edit Menu.







5.3.3 Operation types of equipment view

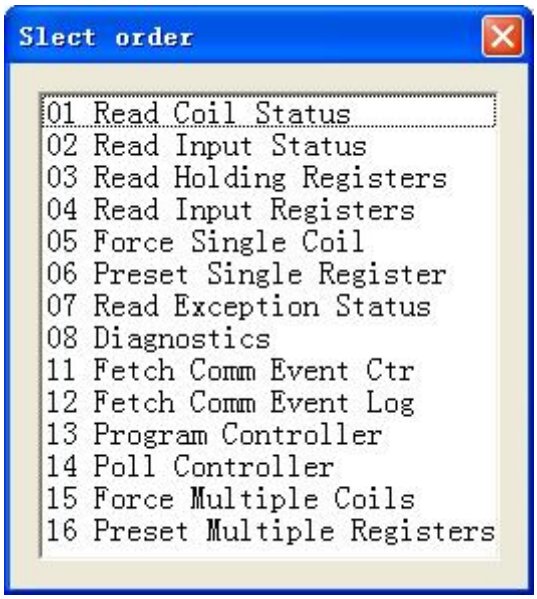
1 Add nodes: Right click on subnet or existing nodes, and then perform the operation of adding a new node. Then there is a new node named "new node" under subnet.

2 Delete nodes: Right click on the node to be deleted, and then perform the operation of deleting the node. The node and its all commands will be deleted.

3 Add commands: Right click on the node, and then perform the operation of adding command to add a command for the node. The dialog box will be shown as follow：

Currently, it supports the commands: 01, 02, 03, 04, 05, 06, 15 and 16.

Select the command: Double click the command



4 Delete commands: Right-click on the command and then perform the operation of deleting the command.

5 Rename nodes: Left click on the node to be renamed, and then the edit status will be shown

and you can rename it.

5.4 The operation of configuration view

5.4.1 Interface of fieldbus configuration view

In the interface of device view, click fieldbus, and then the configuration view is shown as follows:

Configurable items include: input-byte and output-byte number of Profibus-DP. If the "Universal mode" is selected as the protocol type of subnet, Profibus-DP input-data effective length can be selected to be opened or closed.

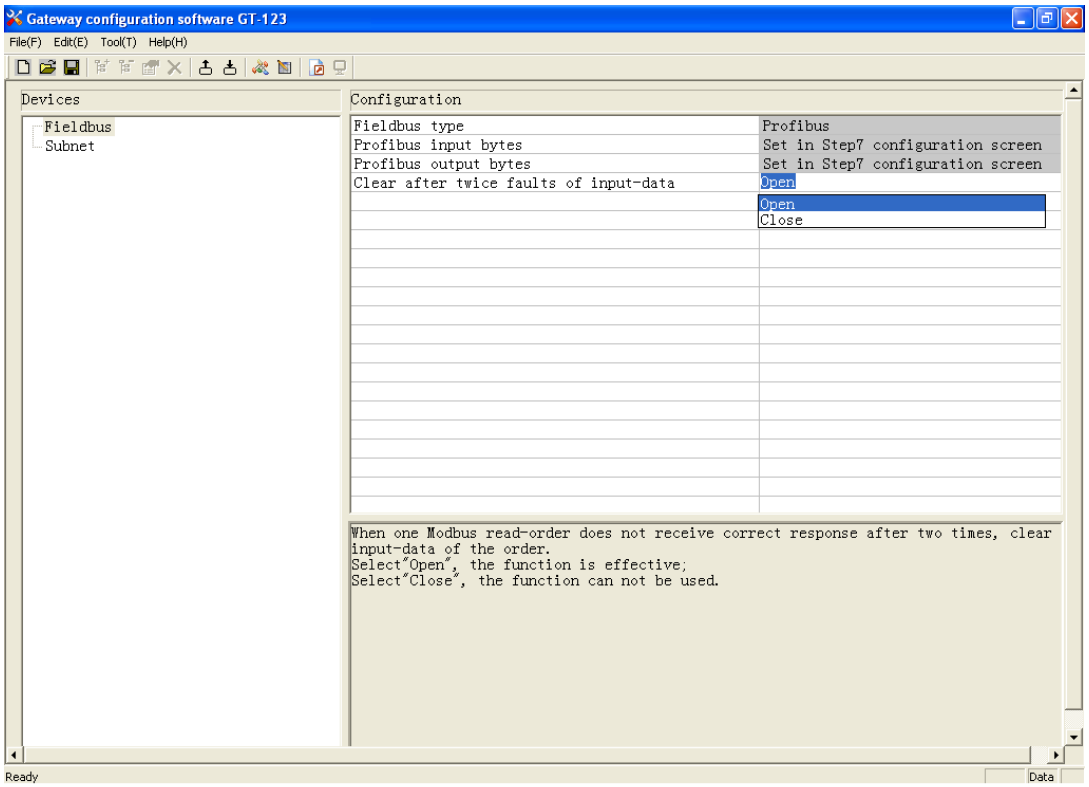
Profibus-DP input-byte number: Set in Step7 (Profibus-DP master configuration software)

Profibus-DP output-byte number: Set in Step7 (Profibus-DP master configuration software)

Profibus-DP input-data timeout: Clear data or keep the last data can be selected.

Timeout times: 2 to 254 can be selected.

Profibus input-data effective length: Open or close can be selected.



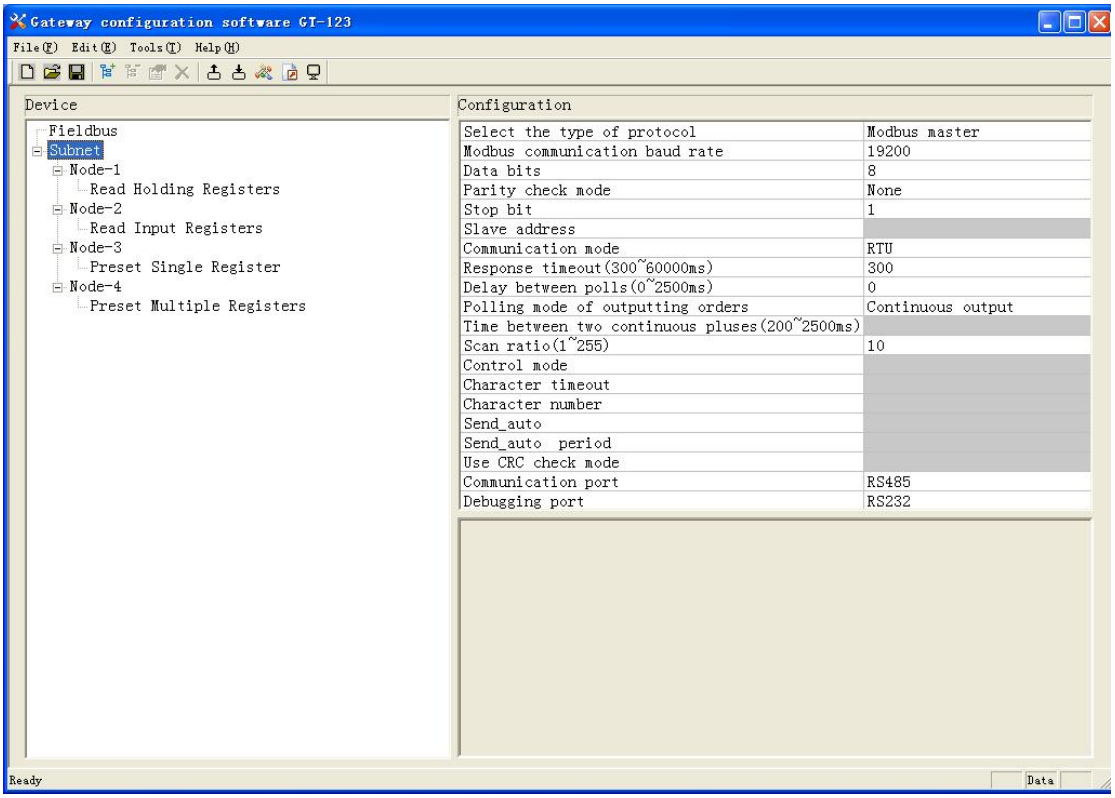
5.4.2 Interface of subnet configuration view

1 Choose Modbus Master in protocol type

Configurable parameters are shown as follows:

Modbus communication baud rate, Data bits, Parity check mode, Stop bit, Transmission mode, Response timeout, Delay between polls, Polling mode of outputting commands, Time between two continuous pluses (the polling mode of outputting commands is pulse output), Scanning ratio, status of Modbus commands, Communication port.

Interface of configuration view is shown as follow:



Modbus communication baud rate: There are 300, 600, 1200, 2400, 9600, 19200, 38400, 57600 and 115200bps to be selected.

Data bits: 8 bits

Parity check mode: There are none, odd, even, mark and space to be selected.

Stop bits: There are 1 and 2 to be selected.

Transmission mode: There are RTU and ASCII to be selected.

Response timeout: When the Modbus master send commands, the time waiting for response

from the slave, the range is 300~60000ms.

Delay between polls: After an command of Modbus having been sent and having received correct response, the time before next command being sent, the range is: 0 ~ 2500ms.

Polling mode of outputting command:

Modbus writing command (output command) has 4 kinds of outputting modes: Continuous output, 0utput disable, Change-of–state output, Pulse output, Communication port

Continuous output: The same with Modbus read command, and output according to the scanning ratio.

0utput disable: Prohibit outputting Modbus write command.

Change of state output: When the output data has changed, it output the write command and stop outputting after receiving correct response.

Pulse output: Output the write command according to the pulse period.

Scan ratio: Ratio of slow-scan and quick-scan. If the quick-scan command sends 10 times, slow-scan command sends 1 time.

Status of Modbus commands: close, one byte, two bytes, three bytes, four bytes, five bytes and six bytes can be selected. They locate in the first bytes of input-data and show the status of Modbus commands. The bit 0 of the first byte show the status of the first Modbus command and six bytes can show all status of 48 commands. The value of status is 0, when the communication is OK and the value change to 1.

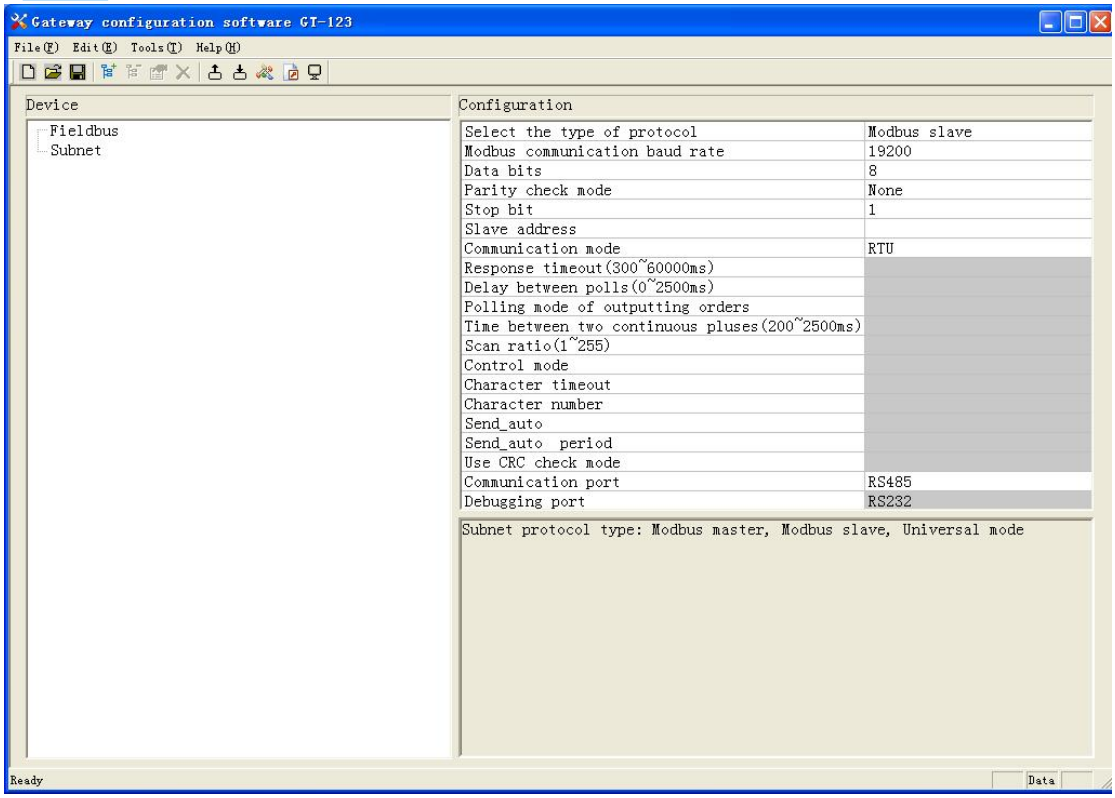
Communication port: There are RS232 and RS485 to be selected.

2 Choose Modbus Slave in protocol type

Configurable parameters are shown as follows:

Modbus communication baud rate, Data bits, Parity mode, Stops bits, Slave address, Transmission mode, Communication port.

Interface of configuration view is shown as follow:



Modbus communication baud rate: There are 300, 600, 1200, 2400, 9600, 19200, 38400, 57600 and 115200bps to be selected.

Data bits: 8 bits.

Parity check mode: There are none, odd, even, mark and space to be selected.

Stop bits: There are 1 and 2 to be selected.

Slave address: The range is 0~247.

Transmission mode: There are RTU and ASCII to be selected.

Communication port: There are RS232 and RS485 to be selected.

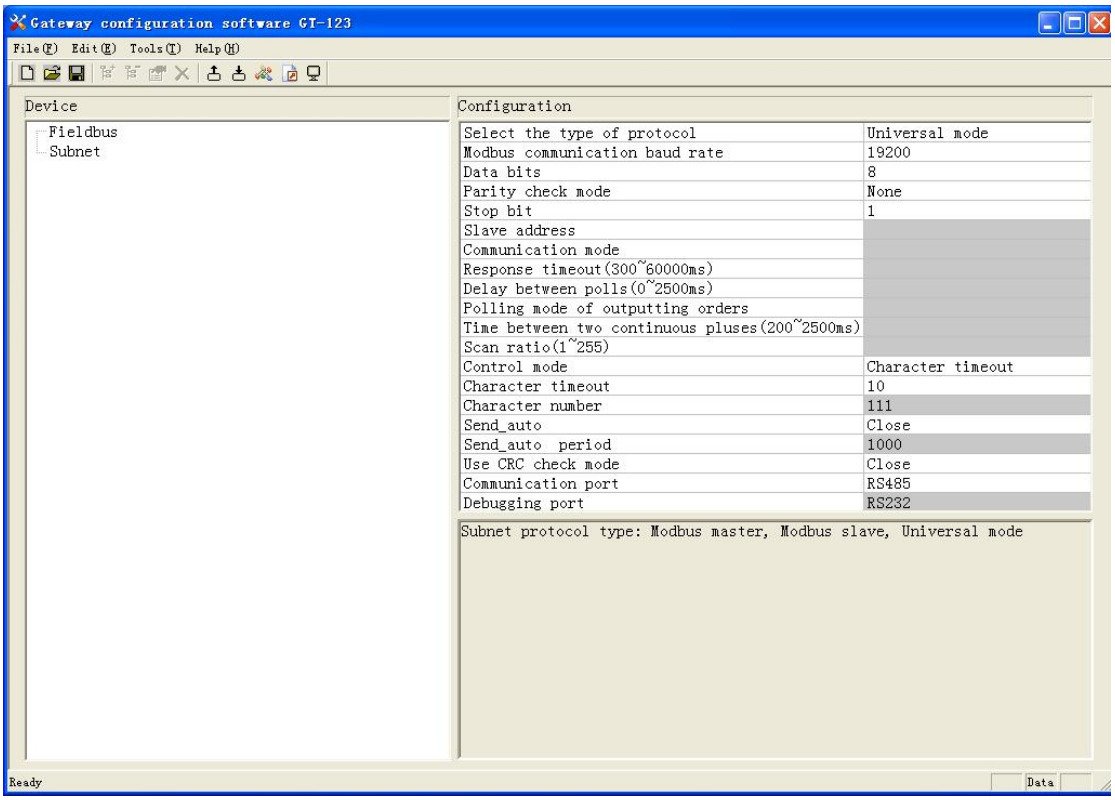
3 Universal mode:

Configurable parameters are shown as follows:

Modbus communication baud rate, Data bits, Parity mode, Stop bits, Control mode, Character timeout, Character number, Send_auto, Send_auto period, Use CRC check mode, Communication port.

Note: "Debug port" of three modes can not be set and the value is opposite to the "Communication port", and it has meaning in the “Modbus Master” only.

Interface of configuration view is shown as follow:



Modbus communication baud rate: There are 300, 600, 1200, 2400, 9600, 19200, 38400, 57600 and 115200bps to be selected.

Data bits: 8 bits.

Parity check mode: There are none, odd, even, mark and space to be selected.

Stop bits: There are 1 and 2 to be selected.

Control mode: There are Character timeout and Character number to be selected.

Character timeout: User input, the default is 10, and the range is 10 ~ 60000ms.

Character number: User input, the default is 111 and the range is 1 ~ 223, only when the control mode is character number, it can be effective.

Send_auto: There are open and close to be selected.

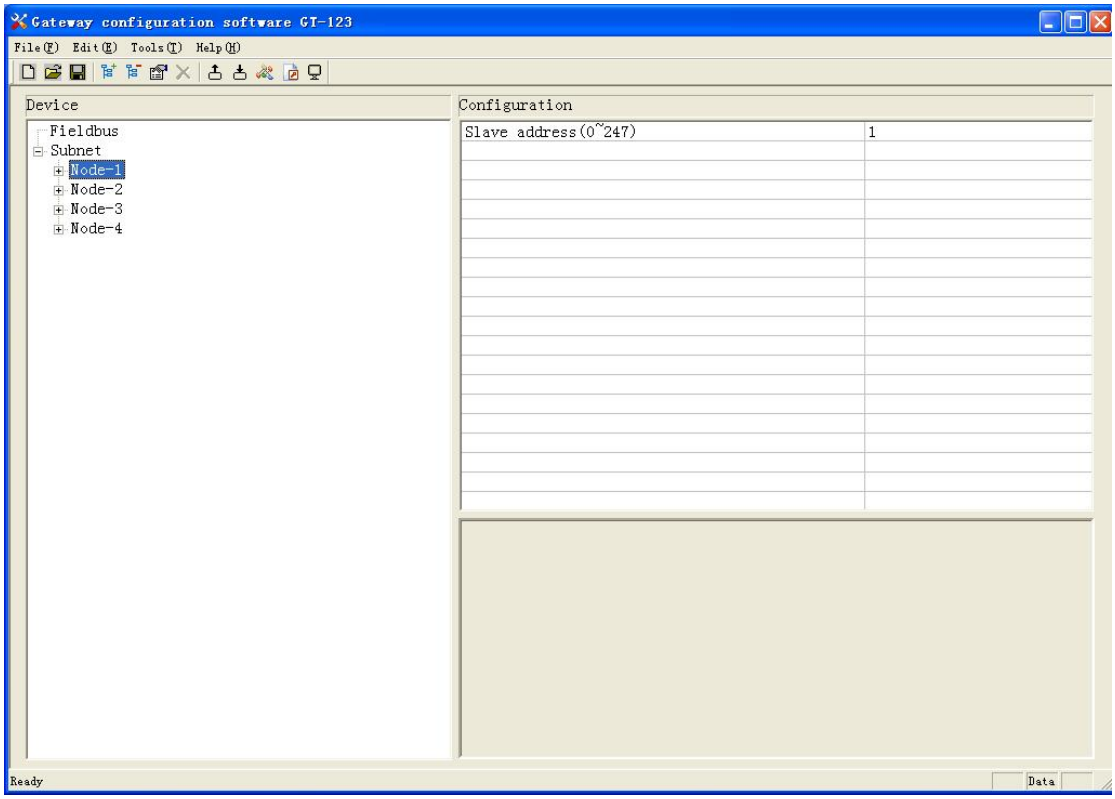
Send_auto period: User input, the default is 1000 and the range is 10 ~ 60000ms, only when the send_auto is opened, it can be effective.

Use CRC check mode: There are open and chose to be selected.

Communication port: There are RS232 and RS485 to be selected.

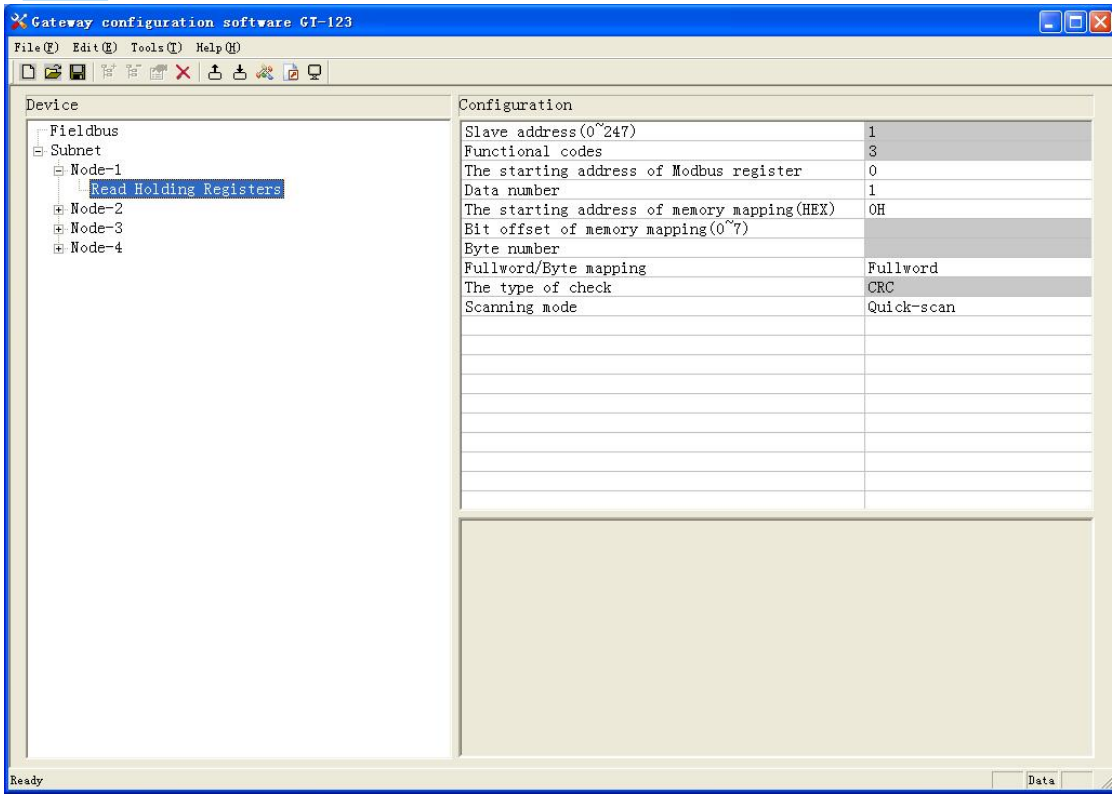
5.4.3 Interface of node configuration view

When the protocol type of subnet is “Modbus master”, in the interface of device view, left click a node, and then configuration interface is shown as follow:



5.4.4 Interface of command configuration view

In the interface of device view, left click a command and then configuration interface is shown as follow:



The starting address of Modbus register: The starting address of register or switching value or loop and so on in Modbus slave and the range is 0~65535.

Data number: The length of data. Two bytes are one data length.

The starting address of memory mapping (hexadecimal): The starting address of data in memory buffer of the module.

The address range of data mapping in the module memory:

Read command: 0x0000~ 0x00DF

Write command: 0x4000 ~ 0x40DF

When write command is used exchanging locally, it also can use: 0x0000 ~ 0x00DF

Bit offset of memory mapping (0 ~ 7): For the bit operation commands, the position range of start-bit byte is 0 ~ 7.

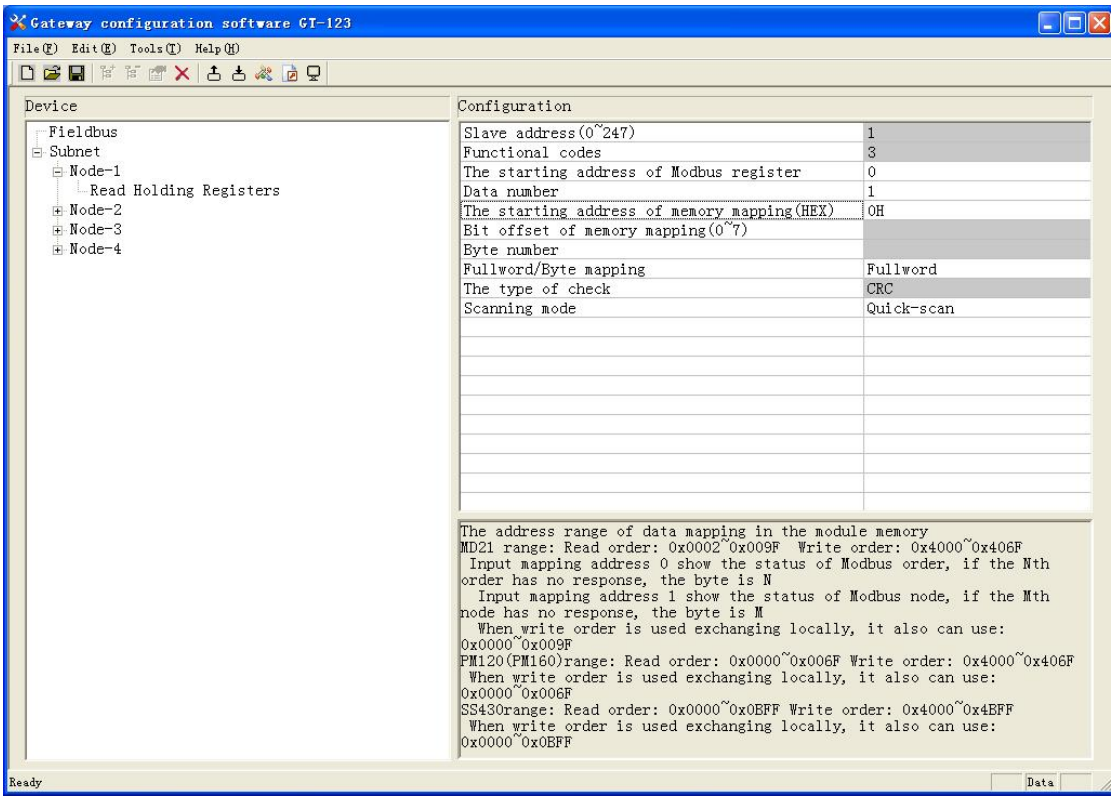
Fullword/Byte mapping: There are three kinds of types: fullword, high byte, low byte. Every register has two bytes. Fullword mapping is taking two bytes of register into gateway memory buffer; High byte mapping is taking the high byte of register into gateway memory buffer; Low byte mapping is taking the low byte of register into gateway memory buffer.

Scanning mode: There are two kinds of scanning mode: quick-scan and slow-scan. It is fit for

requests of user about quick-scan or slow-scan of different commands. Slow-scan is equal to quick-scan being multiplied by scan ratio. (Configure it in the interface of subnet configuration interface)

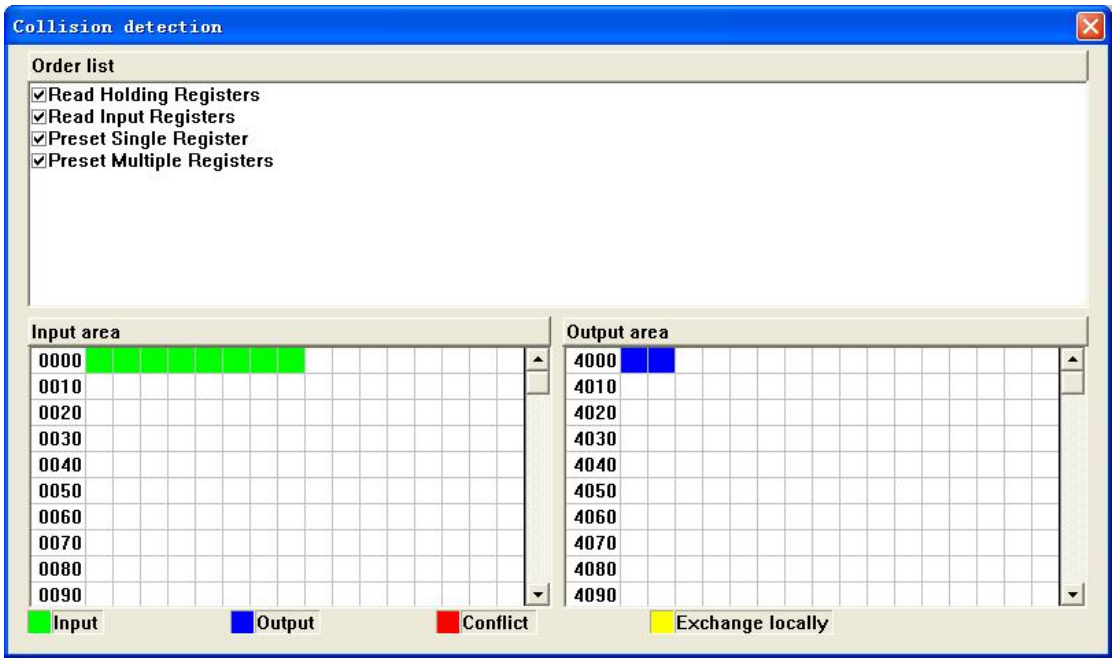
5.4.5 Notes View

Notes view displays the explanation of configuration. The notes that show how to configurate the starting address of memory mapping is shown as follow:



5.5 Conflict Detect

For the detection of whether there is conflict of "the starting address of memory mapping", if conflict it can adjust in time. The interface is shown as follow:



5.5.1 Operation of command list

All the configuration commands can be shown at the command list. Each select box before command is used for checking the memory-mapping location of that command. Click on the command can select the check box, and in the memory-mapping area it can show the corresponding share of spatial location. Click the command again will remove the selected box and it doesn't show the mapping location. The function can be used to conflict detect of memory-mapping area.

5.5.2 Operation of memory mapping area

Memory mapping area is divided two parts: input area and output area.

Input-mapping address: 0x0000 ~ 0x3FFF;

Output-mapping address: 0x4000 ~ 0x7FFF.

Each box represents a byte address.

Green: Read command show in the input-mapping area; no conflict;

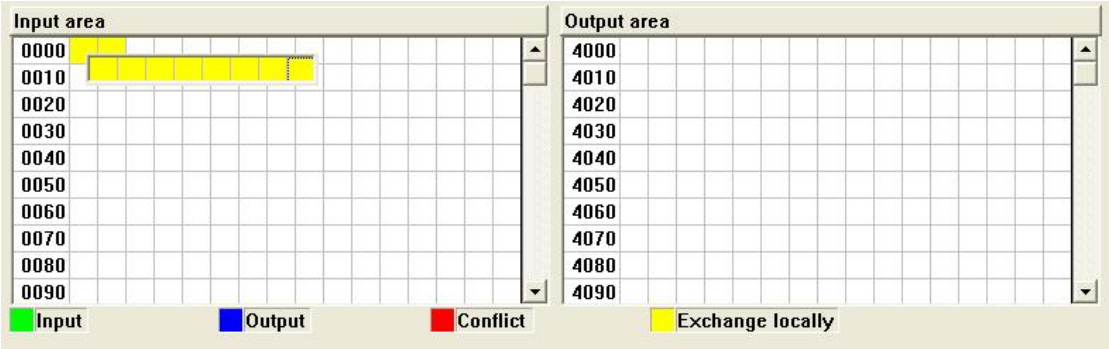
Yellow: Write command show when the mapping address in the input area; no conflict;

Blue: When the address mapping area is located in the output area; no conflict.

Red: Output area or input area, different commands occupy the same byte address, the byte is shown as red.

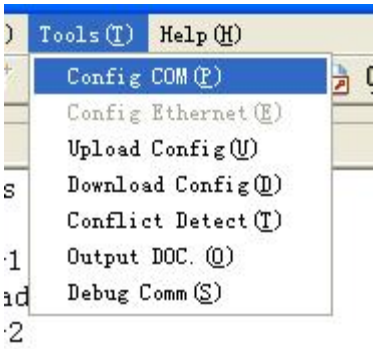
For bit operation commands, the meanings of above shows are also applicable.

Click the input-output regional grid, whether the grid is occupied or not is shown as follows:



5.6 Hardware communication

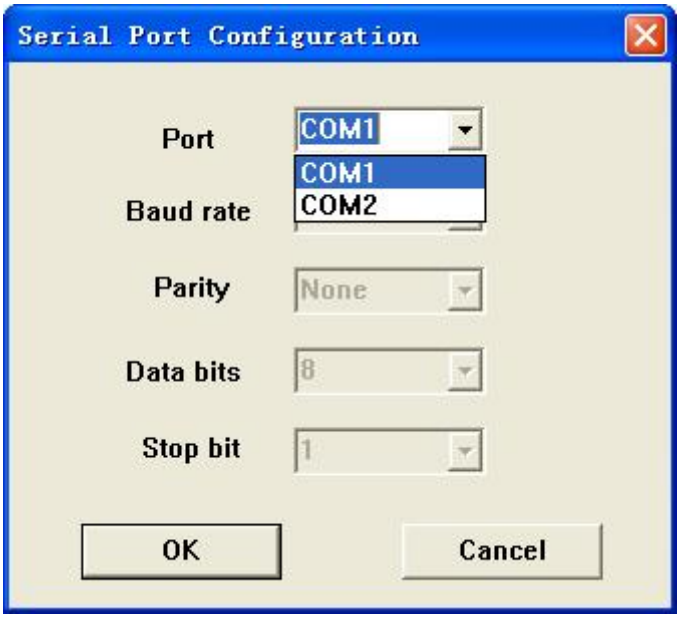
Hardware communications' menu items are shown as follow:



5.6.1 Serial Configuration

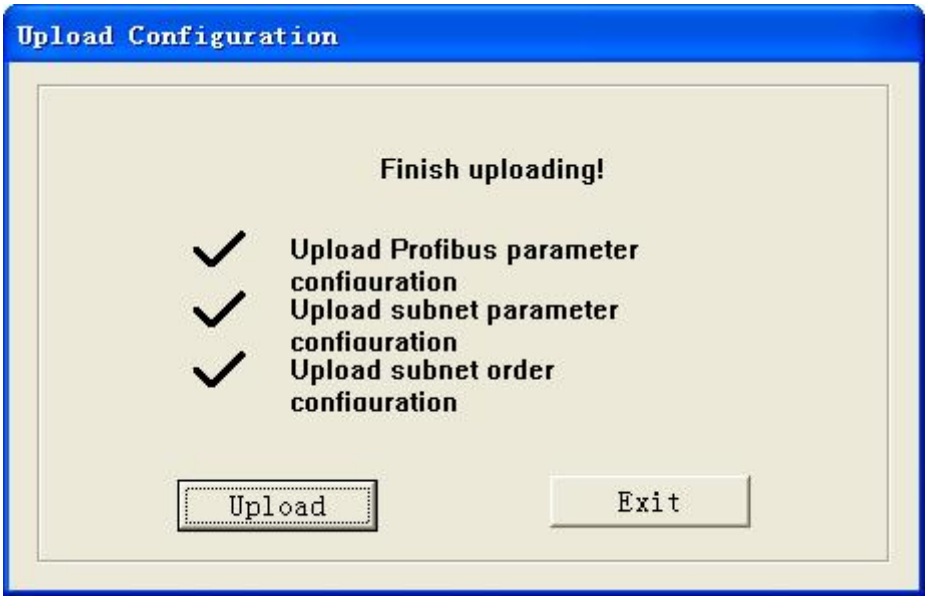
The software automatically scan the available serial port of system, and the available serial can be shown in serial list. After modifying all items, pressing "OK" to save your settings.

Notes: Apart from the serial port number, the other parameters are fixed values: 19200, 8, N, 1.



5.6.2 Upload configuration

Choose upload configuration, upload the configuration from gateway to the software, the display interface is shown as follows:

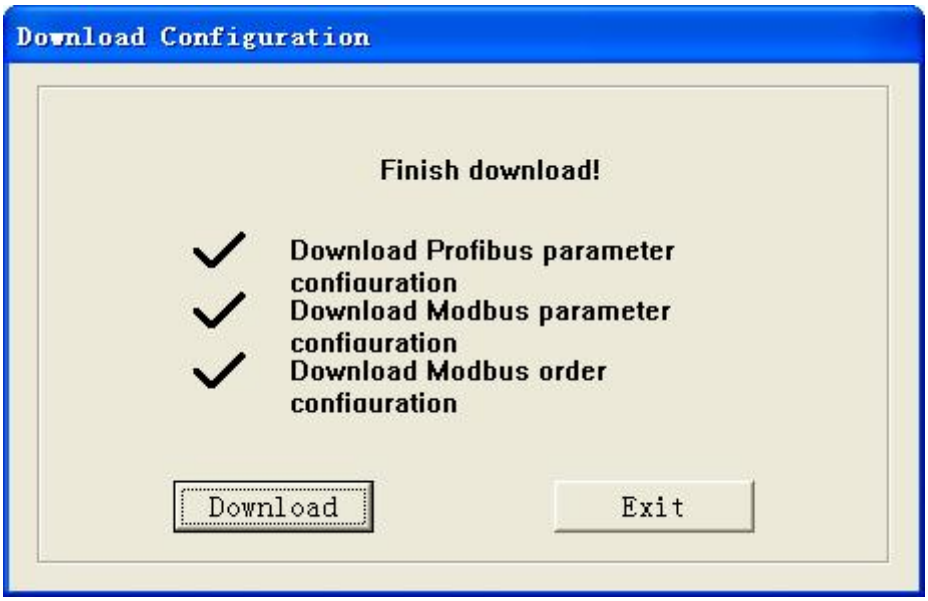


Note: Before uploading the configuration, please check whether the "serial port configuration" is the available port.

5.6.3 Download configuration

Choose download configuration, download the configuration from software to the gateway,

the display interface is shown as follows:



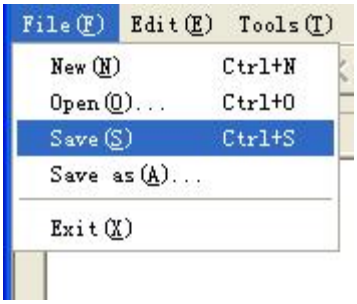
Note 1: Before downloading the configuration, please check whether the "serial port configuration" is the available port.

Note 2: Before downloading the configuration, make sure that all configuration has been completed.

5.7 Load and save configuration

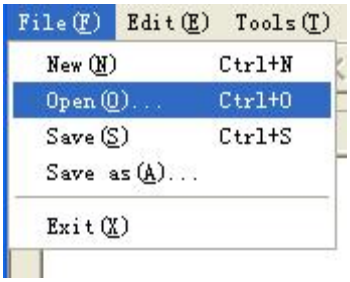
5.7.1 Save Configuration project

Choosing "Save" can save a project.



5.7.2 Load configuration project

Choosing "Open" can open a saved project before.



5.8 Output excel document

Excel document helps users to examine the configuration related.

Choose the icon , save the configuration as excel document and choose the right path.

Double-click to open excel document, three modes as "Modbus master", "Modbus slave", "Universal mode" are different from each other slightly.

Modbus master: The document has there parts: "Command List", "Fieldbus", and "Subnet".

Command list: Modbus command list

Fieldbus: Bus type and relevant parameters

Subnet: Modbus subnet parameters

As follows:

	A	B	C	D	E	F	G
1	Serial number	Slave address	Functional code	Starting address	Data number	Byte number	Starting address of memory
2	1	1	3	0	2		0H
3	2	2	4	0	2		4H
4	3	3	6	0	1		4000H
5	4	4	16				H

Fieldbus / Subnet / Order list

Modbus slave: The document has two parts: "Subnet" and "Fieldbus".

Subnet: Modbus subnet parameters

Fieldbus: Bus type and relevant parameters

As follows:

A	B	C	D	E	F	G	H
Protocol type	Baud rate	Data bits	Parity check	Stop bit	Slave address	Transmission mode	Communication port
Modbus slave	19200	8	None	1	1	RTU	Open

Fieldbus \ Subnet /

Universal mode: The document has two parts: "Subnet" and "Fieldbus".

Subnet: Modbus subnet parameters

Fieldbus: Bus type and relevant parameters

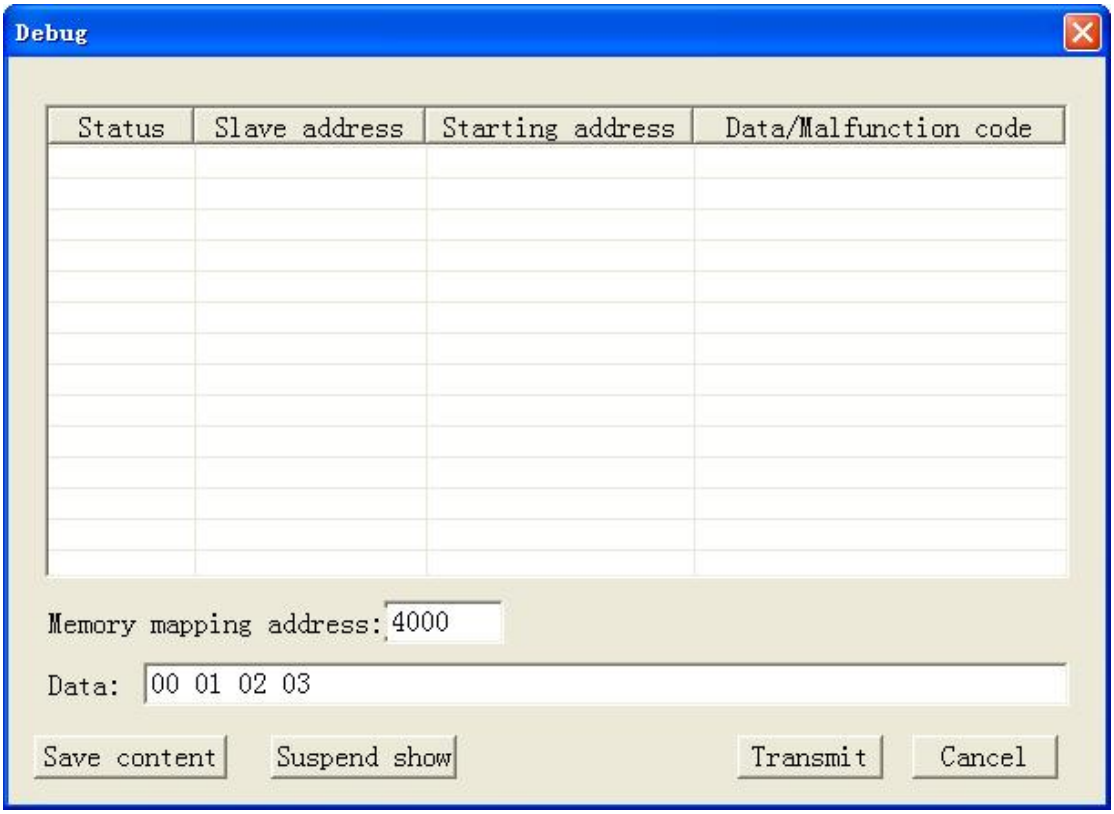
As follows:

A	B	C	D	E	F	G	H
Protocol type	Baud rate	Data bit	Parity check	Stop bit	Control mode	Character timeout (ms)	Character number
Universal mode	19200	8	None	1	Character timeout	10	111

Fieldbus \ Subnet /

5.9 Debug

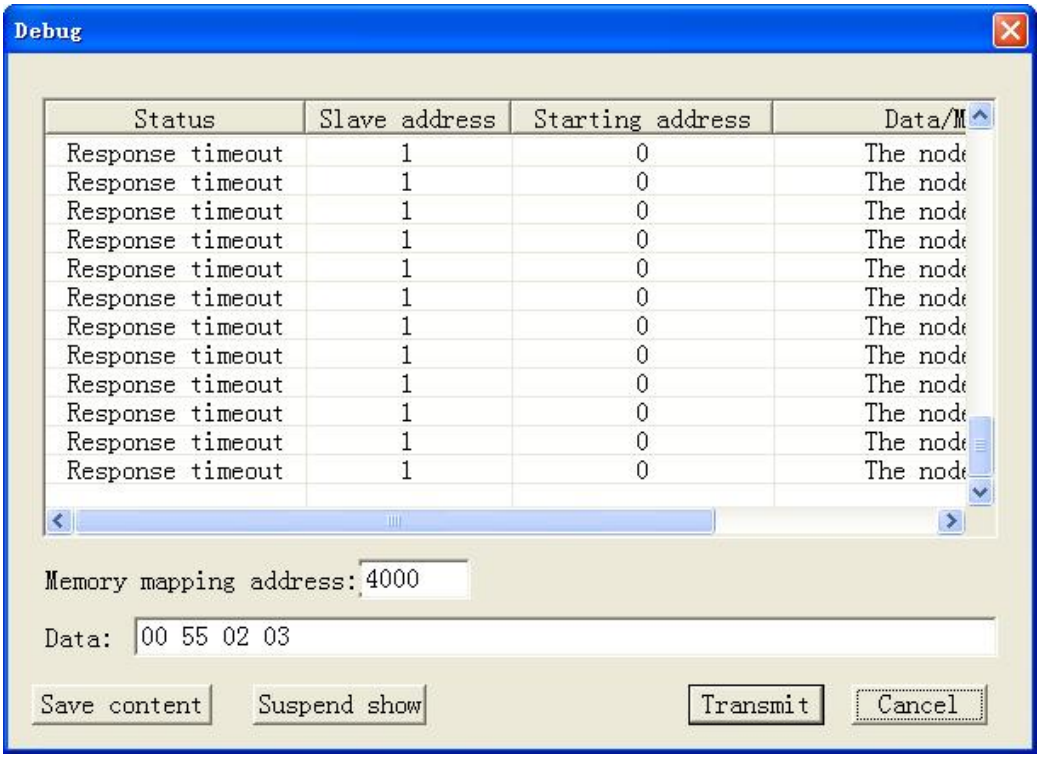
The function is for debugging Modbus network communications, the interface is shown as follows:



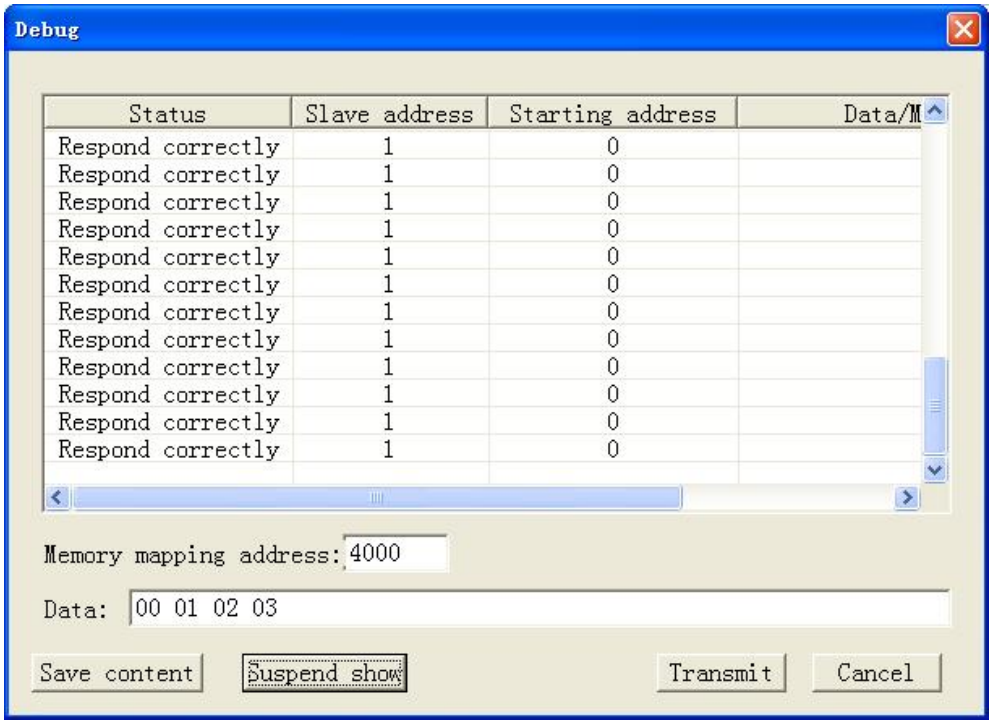
Memory mapping address: Starting address of data writing in the gateway

Data: Data writing into the gateway

When Modbus has no response or response timeout:



When Modbus responses are right:



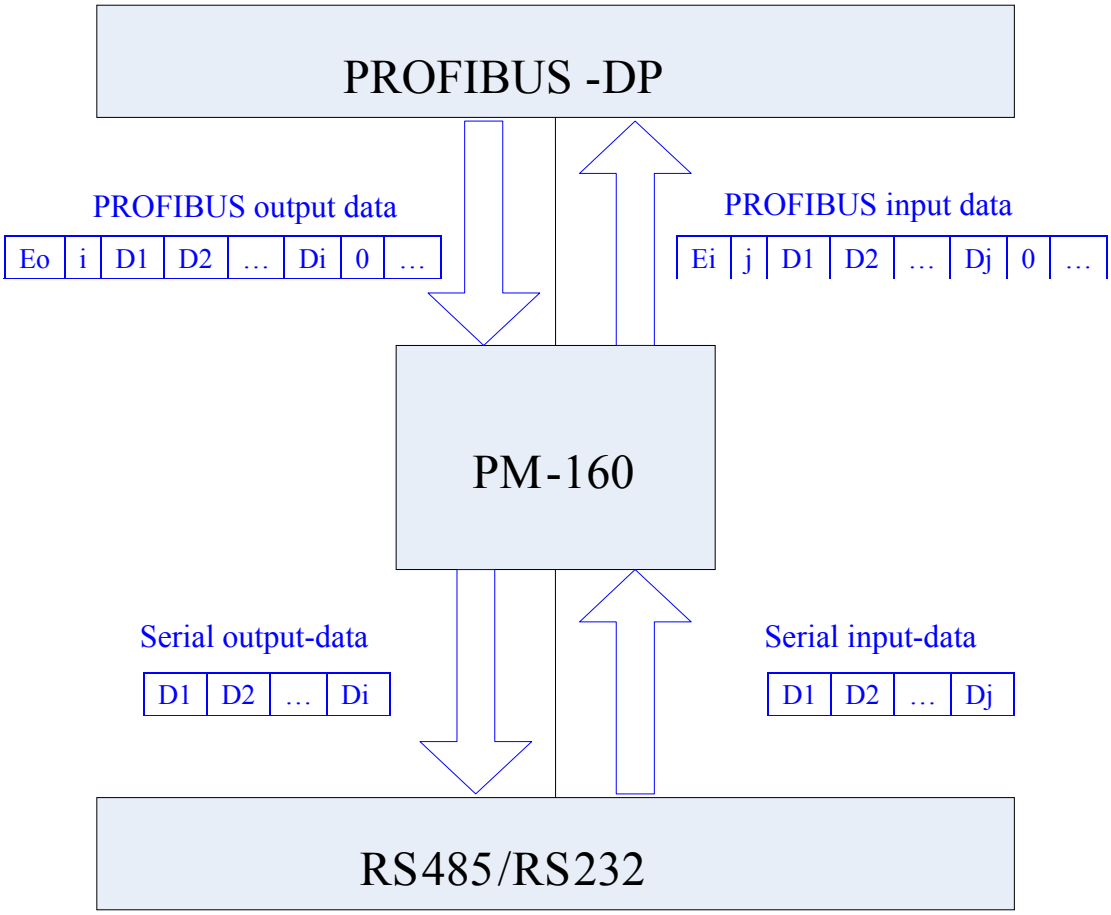
After filling the "Memory mapping address" and "Data" rightly, users can click on "Transmit" button to transmit the packet.

User clicks on the "Save content" button can save the received data to a computer's hard disk.

6Universal mode

6.1 Data exchange

This product provides the communication between Profibus-DP and RS485/RS232. The communication between Profibus-DP and RS485/RS232 is bidirectional. The output-data of Profibus-DP can be sent to RS485/RS232 fieldbus through the interface of RS485/RS232 and the data received from RS485/RS232 is put into input-data of Profibus-DP. Data exchange is shown as follows:



Above, "E_O" is transaction number of Profibus output data; "i" is serial data number included in output data being transmitted; "D1" to "Di" are data being transmitted by serial; "E_i" is transaction number of Profibus input data; "j" is serial data number included in input data receiving form serial; "D1" to "Dj" are data receiving form serial.

6.2 Universal Protocol

Profibus-DP output-data format:

[Transaction number][Length of serial output-data n][Serial output-data 1]…[Serial output-data n] [0x00] … [0x00]

|— n —|

|— m —|

Note:

The number of Profibus-DP output-byte should be greater than or equal to n + 1;

M 0x00 are filling data (also for arbitrary number), n + m +1 should be equal to the number of Profibus-DP output-byte.

Transaction number: When transmit output-data, the transaction number must add 1 to show a new frame data.

Example:

If users select the number of Profibus-DP input-byte and output-byte is 8-byte input and 8-byte output, length of serial output-data is 3, data are 01 02 03. Current transaction number is 0.

The format of output-data is:

[01][03][01][02][03][00][00][00][00]

Profibus-DP input-data format:

[Transaction number][Length of serial input-data n] [Serial input-data 1] … [Serial input-data n] [0x00] … [0x00]

|— n —|

|— m —|

Note:

The number of Profibus-DP input-byte should be greater than or equal to n + 1;

M 0x00 are filling data (also for arbitrary number), n + m +1 should be equal to the number of Profibus-DP input-byte.

Transaction number: The transaction number adds 1 showing a new frame input data.

Example:

If users select the number of Profibus-DP input-byte and output-byte is 8-byte input and 8-byte output, length of serial input-data is 3, data are 04 05 06. Current transaction number is 0.

The format of input-data is:

[01][03][04][05][06][00][00][00][00]

7 How STEP7 Access Data of Gateway and Select Data Module

7.1 How STEP7 access data of gateway

PM-160 provide Modules shown as follow. The max number of modules is 64 when configuring Step7. The max number of input bytes is 224, the max number of output bytes is 224 and the max number of input bytes add output bytes is 224.

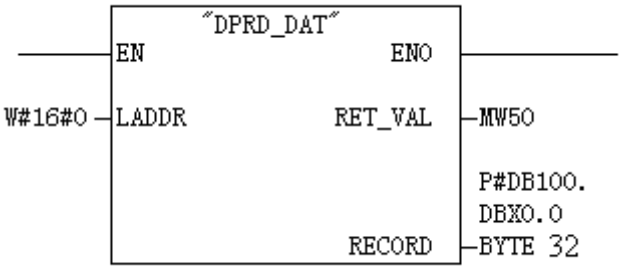
Module	Consistent
4 Words Input, 4 Words Output	Word
8 Words Input, 8 Words Output	Word
24 Words Input, 24 Words Output	Word
56 Words Input, 56 Words Output	Word
1 Byte Input	Byte
1 Word Input	Word
2 Word Input	Word
4 Word Input	Word
8 Word Input	Word
16 Word Input	Word
32 Word Input	Word
64 Word Input	Word
2 Word Input Consistent	Total Length
4 Word Input Consistent	Total Length
8 Word Input Consistent	Total Length
16 Word Input Consistent	Total Length
1 Byte Output	Byte
1 Word Output	Word
2 Word Output	Word
4 Word Output	Word
8 Word Output	Word
16 Word Output	Word
32 Word Output	Word
64 Word Output	Word
2 Word Output Consistent	Total Length
4 Word Output Consistent	Total Length

8 Word Output Consistent	Total Length
16 Word Output Consistent	Total Length

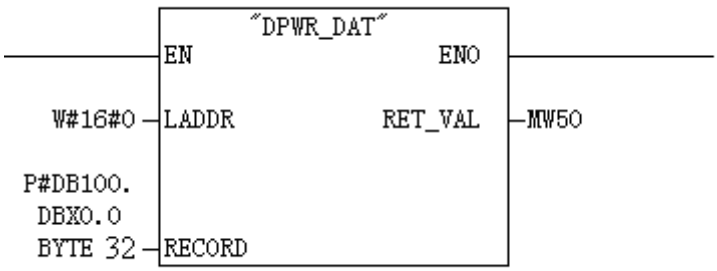
Above, the modules of PM-160 include: word consistent, byte consistent and total length.

For modules which with word and byte as its consistent, users can apply “MOVE” command read and write data in Step7 programming.

For modules which with total length as its consistent, users can apply “SFC 14” read data and “SFC 15” write data in Step 7 programming.



SFC14



SFC15

7.2 How STEP7 select data module

General, when the module include “consistent” show the module with total length as its consistent, such as “2 words Input Consistent”. When you choose the module, you must use “SFC 14” access the data address and read data. When a data of Modbus slave is two-word data, and need high accuracy and real-time, users general select “2 words Input Consistent”, and do not

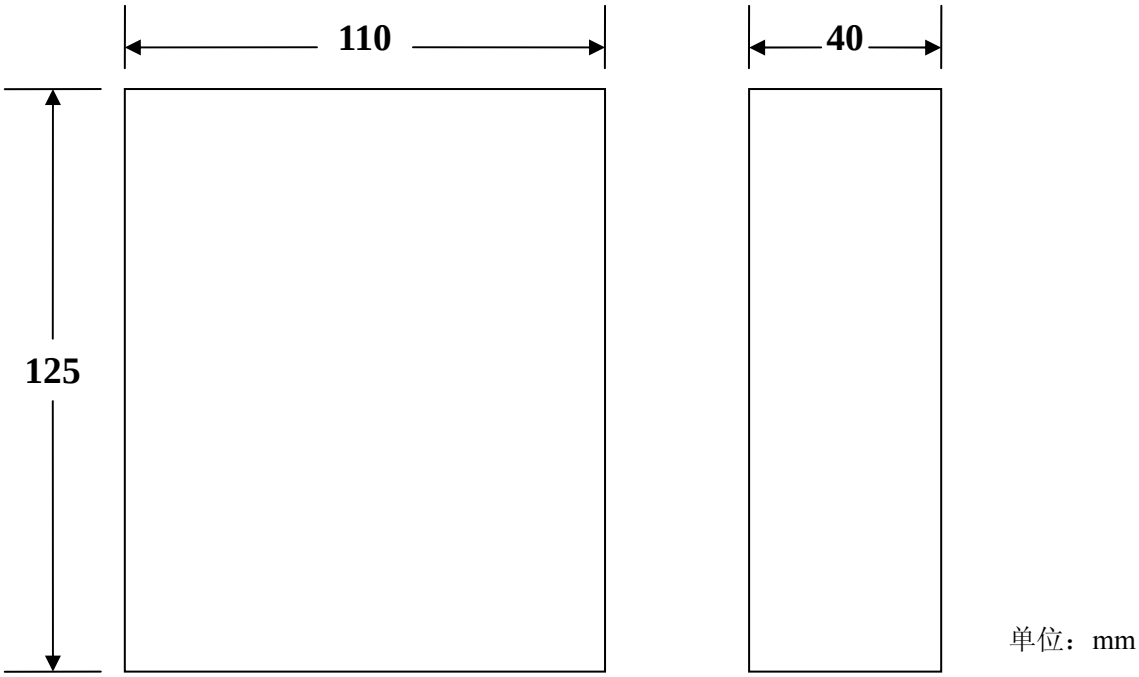
select “2 words Input”. When PLC read data it access the data module through “SFC14”, and it can prevent data jump in process of data transmission.

The selection can be many for user’s need of different bytes. Such as: When users need 20-word input (The data number of PLC reading form Modbus slave is 20), users can select input modules that are grater than or equal to “20 word input” module (32words Input、64words Input…) or input and output modules that are grater than or equal to “20 word input” module (56 words Input，56words Output…).

8 Installation

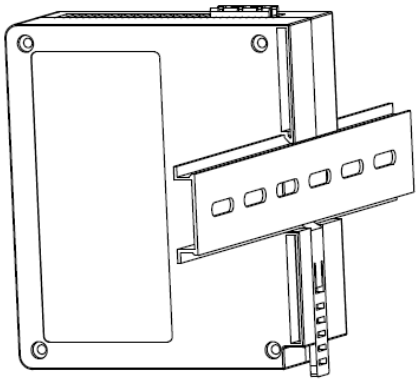
8.1 Machine Dimension

Size: 40mm (weight)*125mm (height)*110mm (depth)



8.2 Installation Method

Using 35mm DIN RAIL



9 Introduction to optional attachment

RS25——RS232/RS485 Isolated converters

RS25 is a product of Sibotech, and it is a RS232/RS485 isolated converter.

Function: Provides communication between RS232 and RS485.

Features: With 3000V photoelectric isolation, be applicable to the industrial scene with multivariate environment.

More information, please visit: www.sibotech.net/en

Appendix A: Using STEP 7 Set Profibus-DP

The following show how to use STEP7 to configure PM-160:

First of all, copy *. gsd file to the following path: ***Step7\S7data\gsd***

1. Open SIMATIC Manager ; Figure 1:

Figure 1

2. Open File, and then New, create a new project; Figure 2:

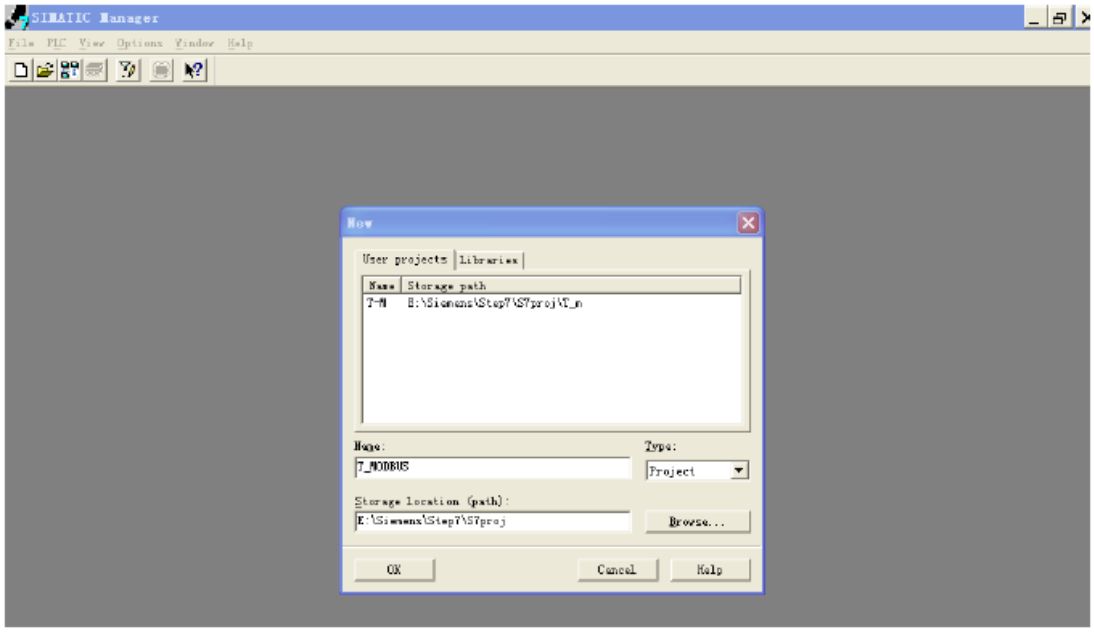


Figure 2

3. Click Insert, Station and then SIMATIC 300 Station; Figure 3

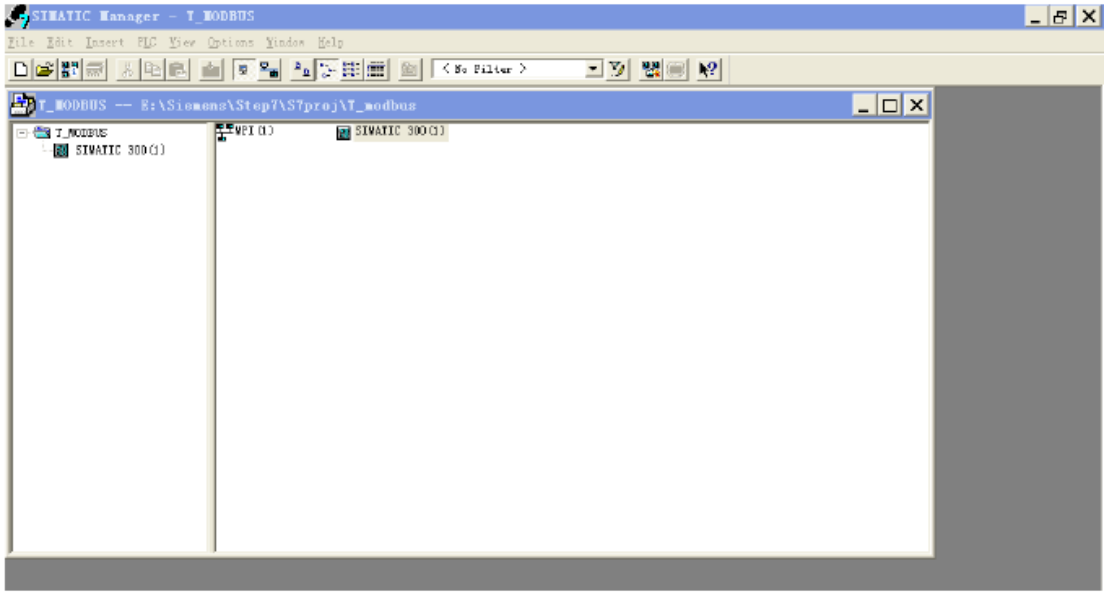


Figure 3

4. Open S7 PLC hardware configuration

   Open SIMATIC 300(1) and then double-click Hardware; Figure 4

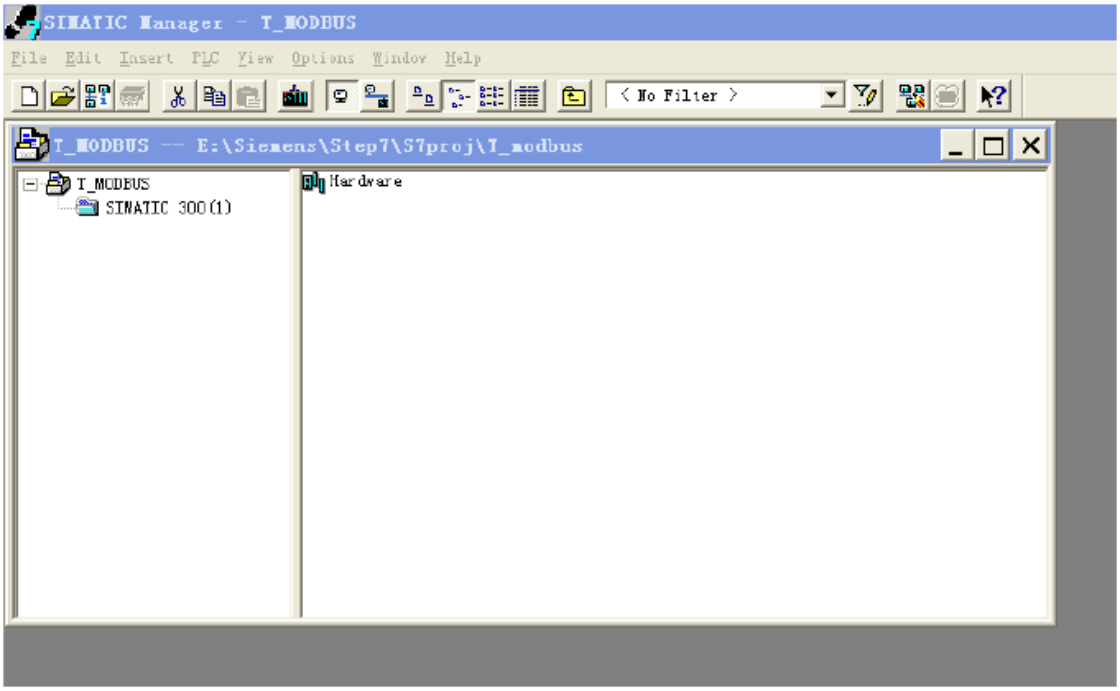


Figure 4

5. In the menu, select Options and Install GSD file, Update GSD in the device catalog

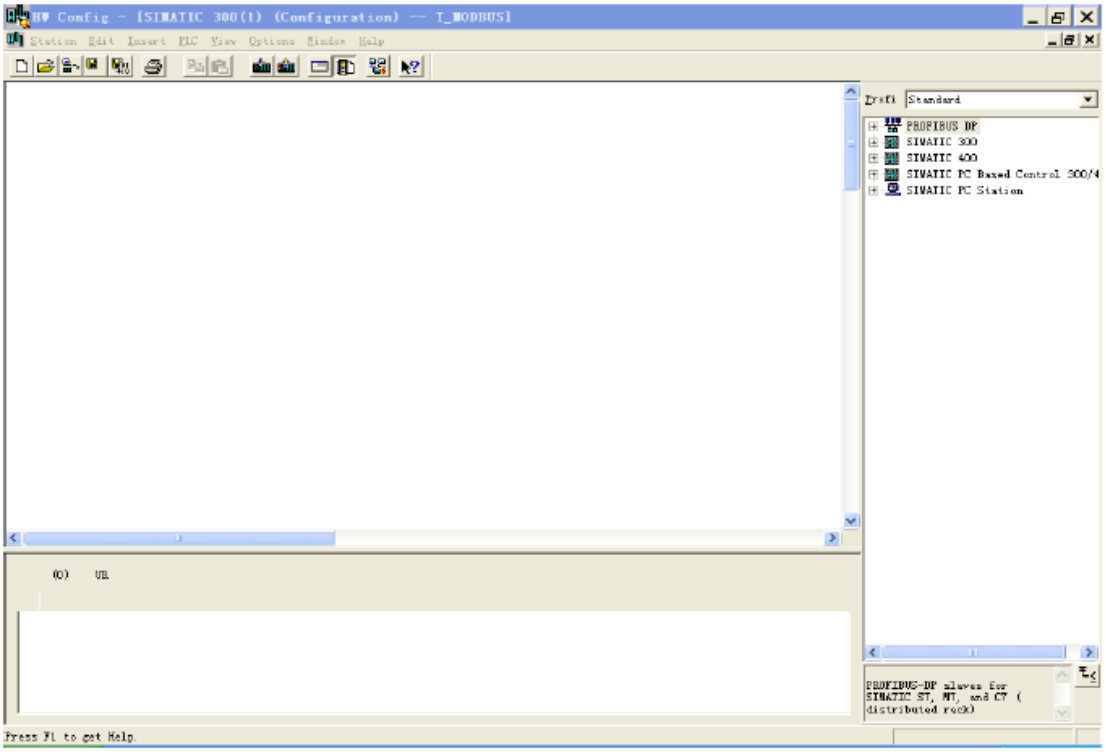


Figure 5

6. Here you can find your equipment in the right side of the window ; Figure 6

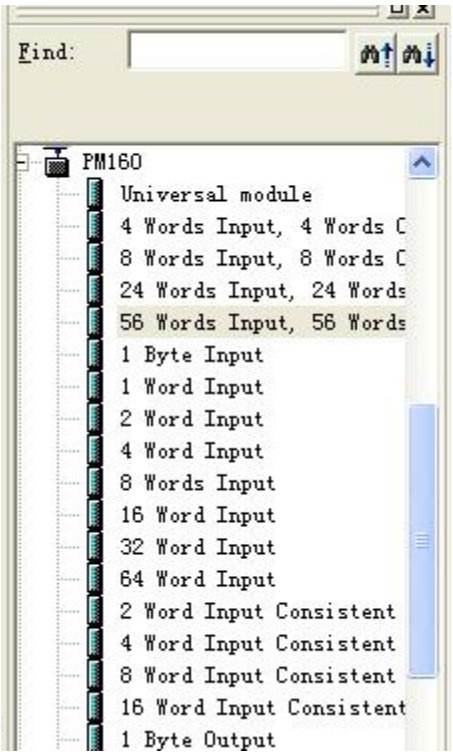


Figure 6

7. Set PLC rack, click the "Hardware Catalog \ SIMATIC 300 \ RACK-300 \ Rail"; Figure 7

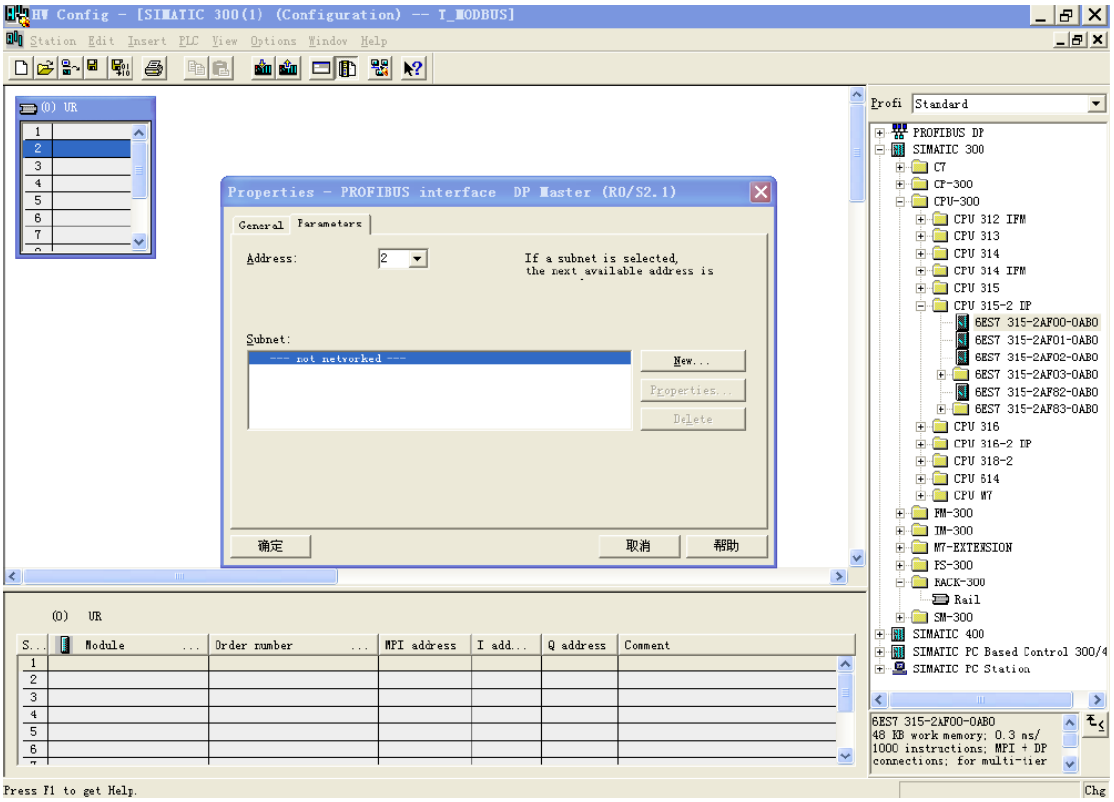
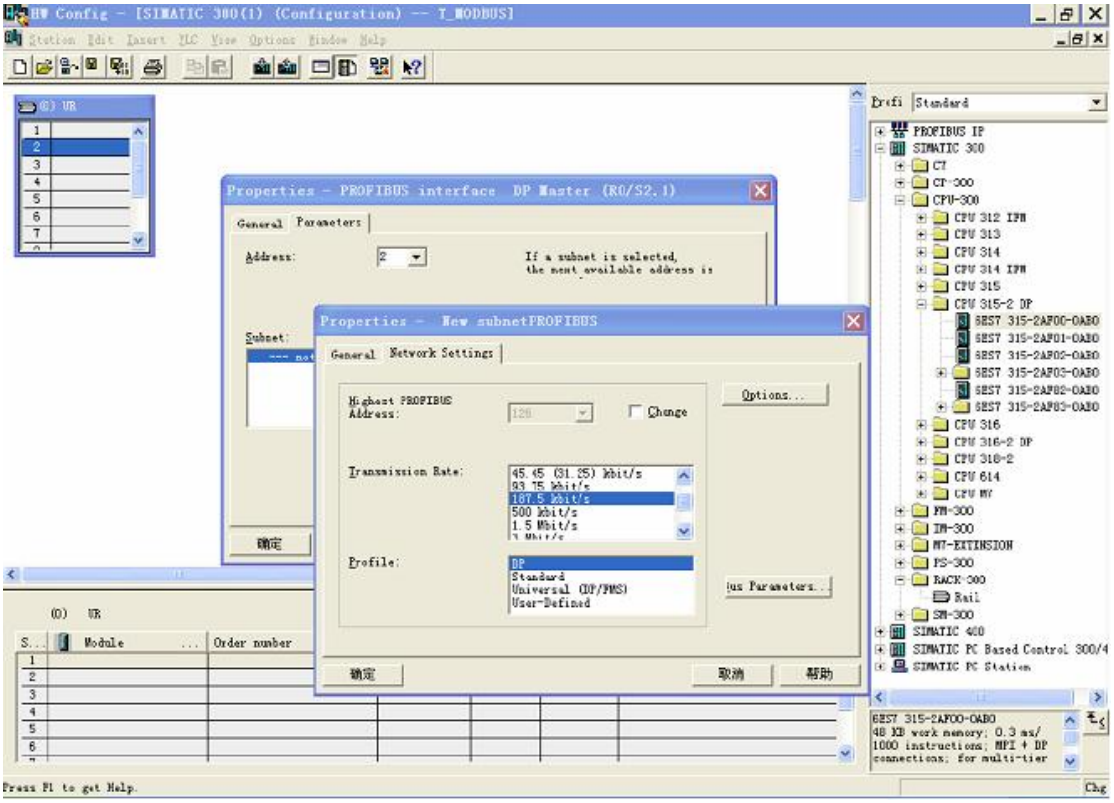


Figure 7

8. Set CPU module and select the corresponding device type and the occupied slots.
9. Create Profibus-DP network and set up Profibus-DP: Click New and then Network settings, select DP; select a baud rate such as 187.5Kbps, then "OK". Double-click it; Figure 8



10. Select Profibus-DP Master address; Figure 9:

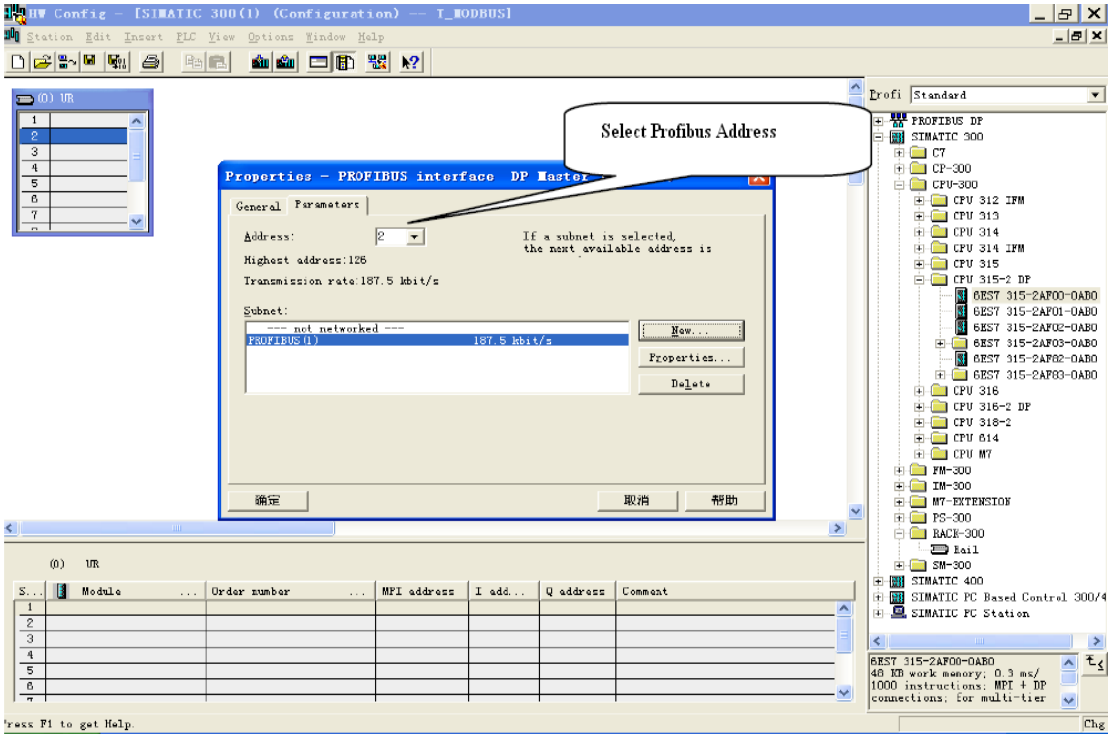


Figure 9

11. Put configuration into Profibus-DP network, and map the input and output data block into other controller's memory; Figure 10:

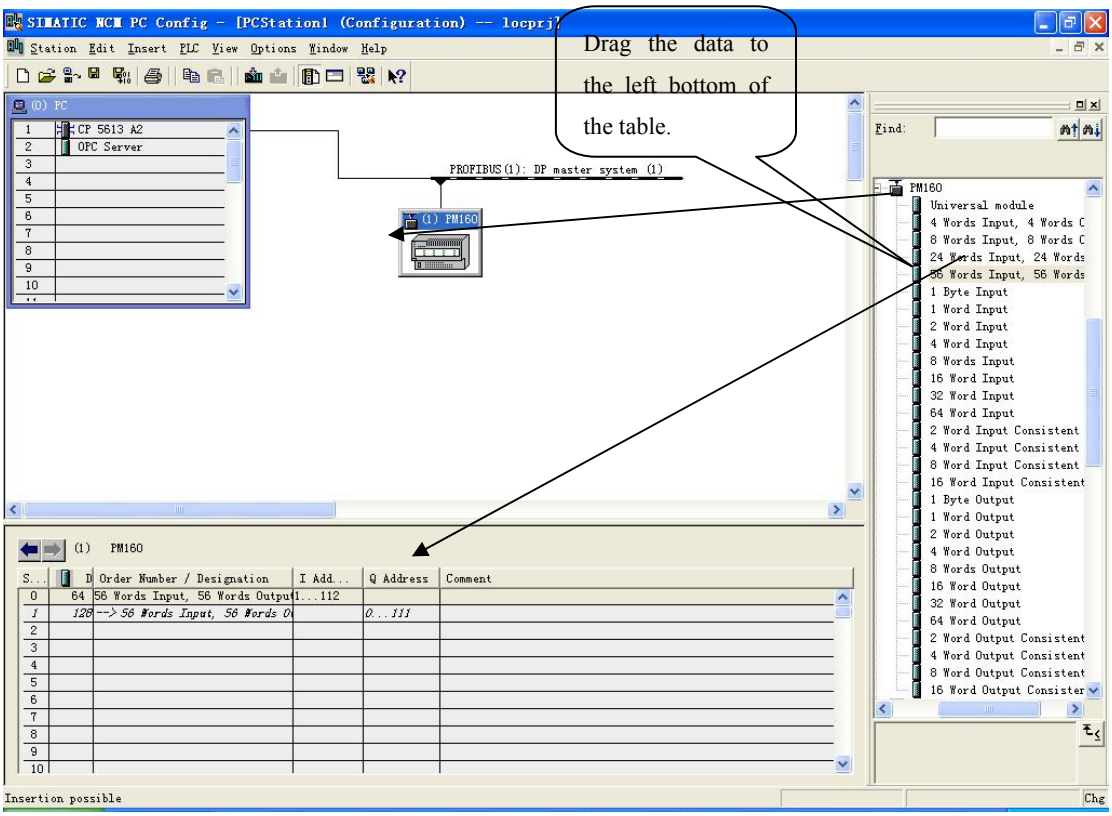


Figure 10

Operation is divided into two steps, the first step is dragging PM-160 into the network configuration on the upper left, the mouse will change shape, and that is to say, it can be placed. The second step is dragging data block into the data mapping table at the bottom left, mapping to the PLC memory.

Note: Profibus input and output bytes of PM-160are set in Profibus master configuration software. **The max number of modules is 64 when configuring Step7. The max number of input bytes is 224, the max number of output bytes is 224 and the max number of input bytes add output bytes is 224.**

Note: The address must be the same with the settings of module switch!

12. Compiler and download into PLC.

Appendix B: Modbus Protocol

Modbus-RTU Protocol:

Note: The equipments being connected with this product must have Modbus interface, and Modbus protocol of the equipments must be in line with the following rules. Our company provides customer-oriented services.

1 Description of protocol

Physical layer: transmission mode: RS485

Address: 0-247

Baud rate: Can configurate

Medium: STP

Transmission mode: Half-duplex mode

The connection is established throng one line with half-duplex mode, and that is to say that signals transmit through the only one line with opposite directions. Firstly, host computer find the only terminal and then the terminal transmits response signals on the opposite direction.

Protocol only allows the communication between host computers and terminals, while the communications between terminals are not allowed. Thus, they will not occupy communication line when they are in the status of being initialized and respond the polling signals which are transmitted to the local terminal only.

Format of a data frame:

1 bit start bit, 8 bits data and 1 bit stop bit.

Format of a data packet

Address	Function Code	Data	check code
8-Bits	8-Bits	N x 8-Bits	16-Bits

The protocol defines check code, data serial and so on in details, which are important contents when communicating specific data.

When data frames reach terminal, they access to the equipment through a simple entrance. The equipment delete the “envelop” of the data frame, and read the data. If there are no faults, the required tasks are executed. Then, it adds the data being generated by itself to the obtained “envelop”, and return the data frame to the sender. The response data include: the address of terminal, the executed function, and the required data and a check code by executing the command. Any faults won’t lead to respond successfully.

Address field

Address field is located at the beginning, composed of 8 bits (0-255). These bits indicate the

address of the terminal being specified by users. The equipment will receive data from the host computer being connected with it. Every address of terminal must be the only one. Only the terminal being addressed will respond the polling with its address. when the terminal transmit a response, the response tell the host computer the terminal which is communicating with it.

Function field

Codes of function field show the function being executed by terminals which are addressed. Diagram 1-1 lists all the function codes, their meanings and their initial functions.

Diagram 1-1 Function codes

code	meaning	action
03	Read data	obtain current binary value of single or multiple registers
06	Preset single register	Place one specific binary value into the single register
16	Preset multiple registers	Place specific binary values to a series of multiple registers

Data field

Data field includes data when specific functions are executed by terminals or data being collected when the terminal responds to query. The content of these data may be value of number, reference address or limit value. For instance, functional code indicates terminals read a register, data field, on the other hand, clearly show the register and the number of data to be read, the inside address, the type of data and different capacity of different computers.

Fault check code

The field allows checking the fault in the transmission between host computer and terminals. Sometimes, due to electrical noise and other interference, a set of data may change when transmitting from one equipment to another. The fault checking code can guarantee that host computer don't respond to the changed data in the transmission, which improves safety and efficiency of the system. The fault code apply 16 bit CRC.

Note: The transmitting serial is always the same- address, functional code, data and the fault checking code relating to direction.

The fault checking

CRC field occupy 2 bytes, including 16 bits binary value. The value of CRC is calculated by transmitting equipment, and then added to the data frame, the receiving equipment calculate the CRC value again while receiving data. Then it is compared with receiving CRC value. If the two values are not the same, the fault occurs.

When calculating CRC, preset a 16-bit register to one firstly, and then calculate 8-bit bytes in the data frame with the current value of the register. Only 8 data bits of each byte participate in the generation of CRC. The initial bit, final bit and occasional odd and even bit don't influence the value of CRC.

The process of generating a CRC:

Preset a 16-bit register to 0FFFFH, and the register is named CRC register.

When generating CRC, exclusive each 8 bit with the content of the register, and then shift result to the low byte, the high bit is filled with zero, the LSB is shifted out and checked. If it is one, the register exclusives with a presetting fixed value. If the lowest bit is zero, there is no settlement.

The above settlement is repeated before executing the shifting 8 times. After finishing shifting the last bit, the next 8-bit byte has the same exclusive calculation with the register, and the another 8-time shifting is carried out. When all the bytes are settled, the final value is CRC value.

The process of generating a CRC:

Preset a 16-bit register 0FFFFH(all one), and name it CRC register.

Exclusive the first 8-bit byte in the data frame with the low byte in the CRC register, and restore CRC register. Shift CRC register to the right bit, fill the highest bit with zero, shift the lowest bit out and check them.

If the lowest bit is zero, repeat the third step (next shift)

If the lowest if one, exclusive CRC register with a presetting fixed value (0A001H).

Repeat the third step and the fourth step until shifting eight times, which settle the entire eight bit down.

Repeat the second step to the fifth step to deal with the next eight-bit until all the bytes are settled down.

In the end, CRC register value is the CRC value.

2. Functions of application layer

The first chapter has described the protocol and data frame. The processors of the software can use the following methods establish their specific application program via protocols without fault.

The protocol in this chapter use the follow format as many as possible, the format is shown as diagram 2-1(digital is set in hexadecimal)

Diagram 2-1

Address	Functional code	The high byte of the starting address of the variable	The low byte of the starting address of the variable	The high byte of the number of the variable	The low byte of the number of the variable	The low byte of checking code	The high byte of checking code
03H	03H	00H	01H	00H	03H	55H	E9H

Read Holding Registers (Function code 03)

Query

The Diagram 2-2 is an example that reading there collected data U1, U2, and U3 to the slave. The address of U1 is 0001H, the address of U2 is 0002H, and the address of U3 is 0003H.

Diagram 2-2

Address	Functional code	The high byte of the starting address of the variable	The low byte of the starting address of the variable	The high byte of the number of the variable	The low byte of the number of the variable	The low byte of checking code	The high byte of checking code
03H	03H	00H	01H	00H	03H	55H	E9H

Response

The response include: the address of slave, functional code, the number of the data and the CRC check.

The example diagram 2-3 is reading the response of U1, U2, and U3.

Diagram 2-3

Address	Functional code	The byte number of the variable	The high byte of the variable	The low byte of the variable	The high byte of the variable	The low byte of the variable	The high byte of the variable	The low byte of the variable	The low byte of checking code	The high byte of checking code
03H	03H	06H	01H	7CH	01H	7DH	01H	7CH	F9H	9BH

Preset Multiple Registers (Functional code 10)

Query

The functional code 10 allows users changing the content of multiple registers. The device can be set 16 values from any starting address. The controller work with the mode of dynamic scanning, and it can change the content of the register anytime.

The Diagram 2-4 is an example changing the action and delay setting values of the monitor 1 and monitor 2 of the slave. The address of the action setting value of the monitor 1 is 2AH, and the delay setting value is 2BH. The address of the action setting value of the monitor 2 is 2CH, and the delay setting value is 2DH

Diagram 2-4

Address	Functional code	The high byte of the starting address of the variable	The low byte of the starting address of the variable 节	The high byte of the number of the variable	The low byte of the number of the variable	The byte number of the variable	The high byte of the variable	The low byte of the variable	The high byte of the variable	The low byte of the variable	The high byte of the variable	The low byte of the variable	The high byte of the variable	The low byte of the variable	The low byte of checking code	The high byte of checking code
03H	10H	00H	2AH	00H	04H	08H	07H	D0H	00H	0AH	07H	0D0H	00H	0AH	25H	7CH

Response

The Diagram 2-5 is the response of changing the action and delay setting values of the monitor 1 and monitor 2.

Diagram 2-5

Address	Functional code	The high byte of the starting address of the variable	The low byte of the starting address of the variable	The high byte of the number of the variable	The low byte of the number of the variable	The low byte of checking code	The high byte of checking code
03	10H	00H	2AH	00H	04H	EBH	8DH

Preset Single Register (Functional code 06)

Query

The functional code 06 allows users changing the content of single register. Any single register of DAE system can use the command change the value. The controller work with the mode of dynamic scanning, and it can change the content of the register anytime.

The following example is changing the overload-action value Ir1. The address of Ir1 is 002EH.

Diagram 2-6

Address	Functional code	The high byte of the starting address of the variable	The low byte of the starting address of the variable	The high byte of the variable	The low byte of the variable	The low byte of checking code	The high byte of checking code
03H	06H	00H	2EH	07H	0D0H	EBH	8DH

Response

The normal response of preset single register is transmitting the receiving data after changing the value of the register.

Diagram 2-7

Address	Functional code	The high byte of the starting address of the variable	The low byte of the starting address of the variable	The high byte of the variable	The low byte of the variable	The low byte of checking code	The high byte of checking code
03H	06H	00H	2EH	07H	0D0H	EBH	8DH