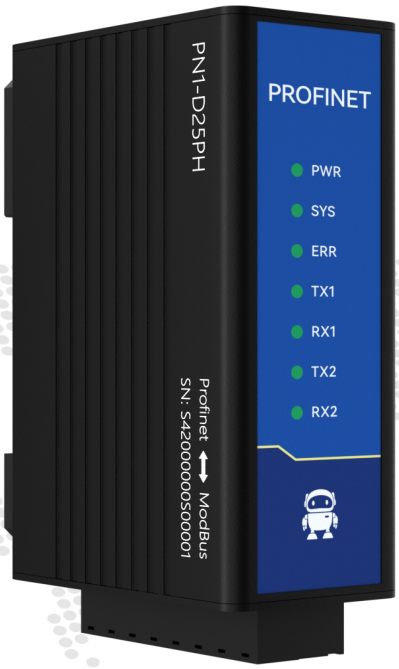
Chengdu Ebyte Electronic Technology Co.,Ltd

Wireless Modem

User Manual



Profinet Gateway

PN1-D25 Series

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

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Table of contents

Chapter 1 Product Overview 1
1.1 Product introduction 1
1.2 Features 1
Chapter 2 Technical Parameters 2
2.1 Product model list 2
2.2 Specifications 2
2.3 Dimensional drawing 3
2.4 Indicator light description 4
2.5 Port and button description 6
Chapter 3 Product Function Introduction 7
3.1 PN1-D25 Series function overview 7
3.2 Modify IP address 7
3.3 Upgrade function 7
Chapter 4 Equipment Alarm Information Description 8
Chapter 5 Tutorial on Device Loading by SIMATIC Step 7 9
5.1 Preparation before connection 9
5.2 Add GSDML file to SIMATIC Step 7 9
5.3 Adding Profinet Devices to the Project 10
5.4 Configure modbus communication parameters 12
5.5Configure Modbus message (function code) 15
5.5.1. Example 16
5.6 Configuring status word and control word 18
5.6.1. Example 19
5.7 Use SIMATIC Step 7 to modify module name and query IP address 20
Chapter 6 Using STEP 7 to load device tutorial 21
6.1 Preparation before connection 21
6.2 Adding GSDML file in STEP 7 21
6.3 Add Profinet device to the project 22
6.4 Configure modbus communication parameters 24
6.5Configure Modbus message (function code) 26
6.5.1. Example 27
6.6 Configuring Status Word and Control Word 31
6.6.1. Example 32
6.7 Using STEP 7 to modify the module name and query the IP address 32
Revision History 34
About us 34

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Chapter 1 Product Overview

1.1 Product Introduction



The PN1-D25 series is a Profinet to Modbus RTU gateway used to map Modbus data to Profinet. Use GSD files for integration, code-free reading and writing of Modbus devices, and quickly set up data and transfer it to the PLC. The gateway provides 1 RS485 and 1 RS422 (compatible with RS485) interfaces, each supporting 32 command nodes, a total of 64 command nodes . The PN1-D25 PH supports two RJ45 Ethernet ports and has switch functions . All Modbus commands are loaded in module form , and the memory mapping relationship between Profinet and Modbus is intuitive and can be used in STEP 7 or query in TIA Portal software. You can load the status byte to query the connection status of the Modbus device and monitor the device status in real time .

1.2 Features

- Adopts standard Profinet protocol communication, and can be networked with PLC, configuration, configuration software tool, etc.
- Support Siemens PLC 200/300/1200/1500 full series
- Support SIMATIC Step 7 configuration software tool
- Adopts standard Modbus RTU protocol and can be used as Modbus RTU slave or Modbus RTU master
- Support RS485+RS422 (compatible with RS485) dual serial ports, each channel can be independently configured with parameters
- Profinet and Modbus RTU protocol conversion
- Dual network ports 10/100M adaptive, support switch function
- Supports 8~28V wide voltage input and has power reverse connection protection
- With multiple protections such as static electricity, surge, and electric fast pulse group
- Easy configuration, no configuration software tool required, directly provide GSD file
- The device has built-in software and hardware watchdogs to ensure stable operation of the device and reliable data transmission
- Industrial-grade hardware design, aluminum alloy metal casing
- Support standard 35mm rail installation
- Widely used for acquisition and control of Modbus RTU devices in industrial sites

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Chapter 2 Technical Parameters

2.1 Product Model List

Product Model	Number of network ports	Serial port type
PN1-D25P	1	RS485+RS422 (compatible with RS485)
PN1-D25PH	2	RS485+RS422 (compatible with RS485)

2.2 Specifications

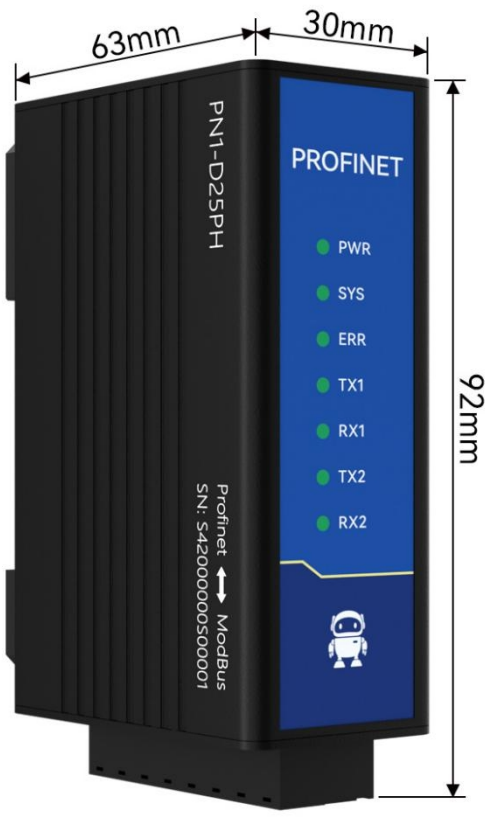
Category	Name	Parameter
power supply	Operating voltage	DC 8 ~ 28 V ; with reverse connection protection
	Power indicator	PWR red LED indicator
Network port parameters	Interface Type	RJ45
	Communication Protocol	Standard Profinet protocol (RT)
	Maximum communication cycle	4ms
	Communication bandwidth	10/100M adaptive
RS485 serial port parameters	Interface Type	RS485 (5.08mm terminal block)
	Communication Protocol	Standard Modbus RTU protocol
	Baud rate	1200 ~ 3.9M bps
	Communication Format	Data bits: 7/8 Bits (default 8) Stop bits: 1/2 Bits (default 1) Check: None/Odd/Even (default None)
RS422 serial port parameters	Interface Type	RS422 (5.08mm terminal block)
	Communication Protocol	Standard Modbus RTU protocol
	Baud rate	1200 ~ 3.9M bps
	Communication Format	Data bits: 7/8 Bits (default 8) Stop bits: 1/2 Bits (default 1)

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

		Check: None/Odd/Even (default None)
Work Environment	Working temperature and humidity	-40 ~ +85℃, 5% ~ 95%RH (no condensation)
	Storage temperature and humidity	-40 ~ +105℃, 5% ~ 95%RH (no condensation)
other	Product size	55 mm * 30 mm * 80 mm (length * width * height)
	Product Weight	1 30 ±5 g
	Installation	Standard industrial grade 35mm rail installation

2.3 Dimensions



92*30*63 (length*width*height)

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

2.4 Indicator Light Description



Label	Name	Description
PWR	Power indicator	Red LED light ; on: system power supply is normal; off: system power supply is abnormal
SYS	System (Profinet connection) indicator	Blue LED light; on: Profinet connection established, off: Profinet connection not established; when software controls the flashing indicator light, it flashes at the same time as ERR
ERR	(Modbus) communication error indicator	Red LED light; On: When an error occurs, it stays on for 3 seconds, and recovers after no error occurs; Off: Moodbus communication is normal ; When the software controls the flashing indicator light, it flashes at the same time as SYS
TX1	Serial port 1 sending data indicator	Yellow LED light; on: flashes quickly when serial port 1 has data to send
RX1	Serial port 1 receiving data indicator	Yellow LED light; on: flashes quickly when serial port 1 receives data
TX2	Serial port 2 sending data indicator	Yellow LED light; on: flashes quickly when serial port 2 has data to send
RX2	Serial port 2 receiving data indicator	Yellow LED light; on: flashes quickly when serial port 2 receives data

Indicator lights during firmware upgrade	
SYS	Enter upgrade mode and keep flashing at 5hz frequency

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

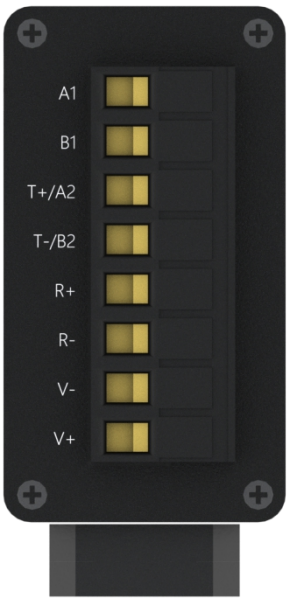
ERR	When the upgrade fails, the 3hz keeps flashing
TX1	During the upgrade process, 1hz flashes
RX1	During the upgrade process, 1hz flashes
TX2	During the upgrade process, 1hz flashes
RX2	During the upgrade process, 1hz flashes

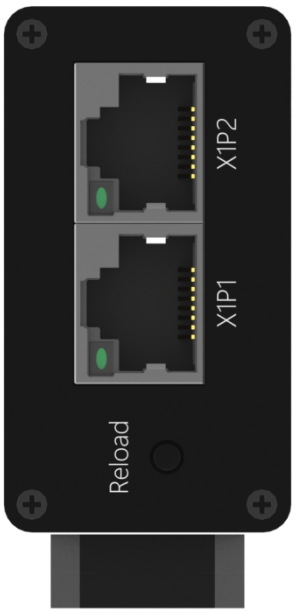
Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

2.5 Port and button description

Note: The following is a display of the dual-port version. The single-port version only has one less port, and there is no other difference





Label	name	Description
A1	RS485 A1 interface	Serial port 1 RS485 A1 interface, 5.08mm terminal
B1	RS485 B1 interface	Serial port 1 RS485 B1 interface, 5.08mm terminal
T+/A2	RS422 T+ interface /RS485 A2 interface	Serial port 2 RS422 T+ interface/RS485 A2 interface, 5.08mm terminal
T-/B2	RS422 T-Interface /RS485 B2 interface	Serial port 2 RS422 T-interface/RS485 B2 interface, 5.08mm terminal
R+	RS422 R+ interface	Serial port 2 RS422 R+ interface, 5.08mm terminal
R-	RS422 R- Interface	Serial port 2 RS422 R- interface, 5.08mm terminal
V-	DC power supply negative pole	DC (8~28V) power negative terminal interface, 5.08mm terminal
V+	DC power supply positive pole	DC (8~28V) power positive terminal, 5.08mm terminal
X1P2	Network port 2	Standard RJ45 network cable interface
X1P1	Network port 1	Standard RJ45 network cable interface
Reload	button	Restore to factory settings: Press and hold for 5 to 10 seconds and then release the power button; Device restart: Release the power button after it is powered on for less than 2 seconds; Firmware upgrade: Press and hold the button in the power-off state, then power on, the device will enter the upgrade mode;

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Chapter 3 Product Features

3.1 PN1-D25 Series Function Overview

This module Modbus RTU supports up to 64 commands, which are divided into master commands and slave commands. The command type, length, and communication interface can be set separately. When using the Modbus RTU master function, the write function call cannot be less than 2 times the polling cycle, otherwise there will be a frame of write function data that is not refreshed. For example, the Modbus RTU master has 5 command nodes, and the polling interval is 10ms. It takes 50ms to complete the polling of all command nodes, so the minimum data change cycle is 50ms *2 = 100ms.

Dual serial ports can be used simultaneously.

3.2 Modify IP address

The IP address of this module can be modified through SIMATIC Step 7/STEP 7 and other software. For detailed settings, please refer to the usage chapter.

3.3 Upgrade Features

Supports firmware upgrade function. For detailed instructions on firmware upgrade, please refer to the firmware upgrade manual.

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Chapter 4 Device alarm information description

When an error occurs in the PN 1 - D25 gateway, the specific error information will be sent to the PLC through the Profinet alarm mechanism. At the same time, the ERR light of the gateway will flash three times continuously, and the indicator light on the PLC will also flash. When the error disappears, the corresponding alarm information will be removed. The specific error information can be viewed through the configuration software tool corresponding to the PLC.

The specific error information is explained below:

Error message	Description
Illegal Fun Code	Slave replies modbus standard error: The requested function is not recognized or supported by the slave device
Illegal Data Address	The slave replies with a modbus standard error: The data address is not within the accessible range of the device
Illegal Data Value	The slave replies with a modbus standard error: The requested operation attempted to set an invalid or illegal value.
Slave Device Failure	Slave replies modbus standard error: Slave device failure, unknown device failure
Frame Length Error	The length of the message received by the master is wrong ; it is too long, too short, or does not match the correct length of the slave reply data.
CRC Check Error	CRC check error of the message received by the master station
Register Number Error	The master station receives the wrong number of message registers
SLave Address Error	The slave address of the message received by the master is wrong
MASTER WATING RSP TIMEOUT	Master receiving timeout
Function Code Different	The function code in the message received by the master station is inconsistent with the request
Register Address Error	The register address of the message received by the master station is wrong
Unknown Error	Unknown error

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

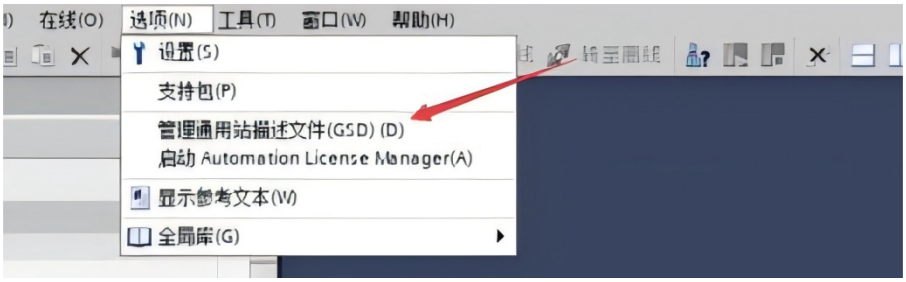
Chapter 5 Tutorial on loading devices using SIMATIC Step 7

5.1 Preparation before connection

1. Prepare the required XML files as follows:
   GSDML-V2.3-EBYTE-PN1-D25-20241025.xml
2. Connect the DC 24V external power supply to the module and power it on. Before powering on, check whether the positive and negative poles of the power supply are connected correctly.
3. Use a network cable to connect the module to the Profinet interface of the PLC controller. (In the same network segment)

5.2 Add GSDML file to SIMATIC Step 7

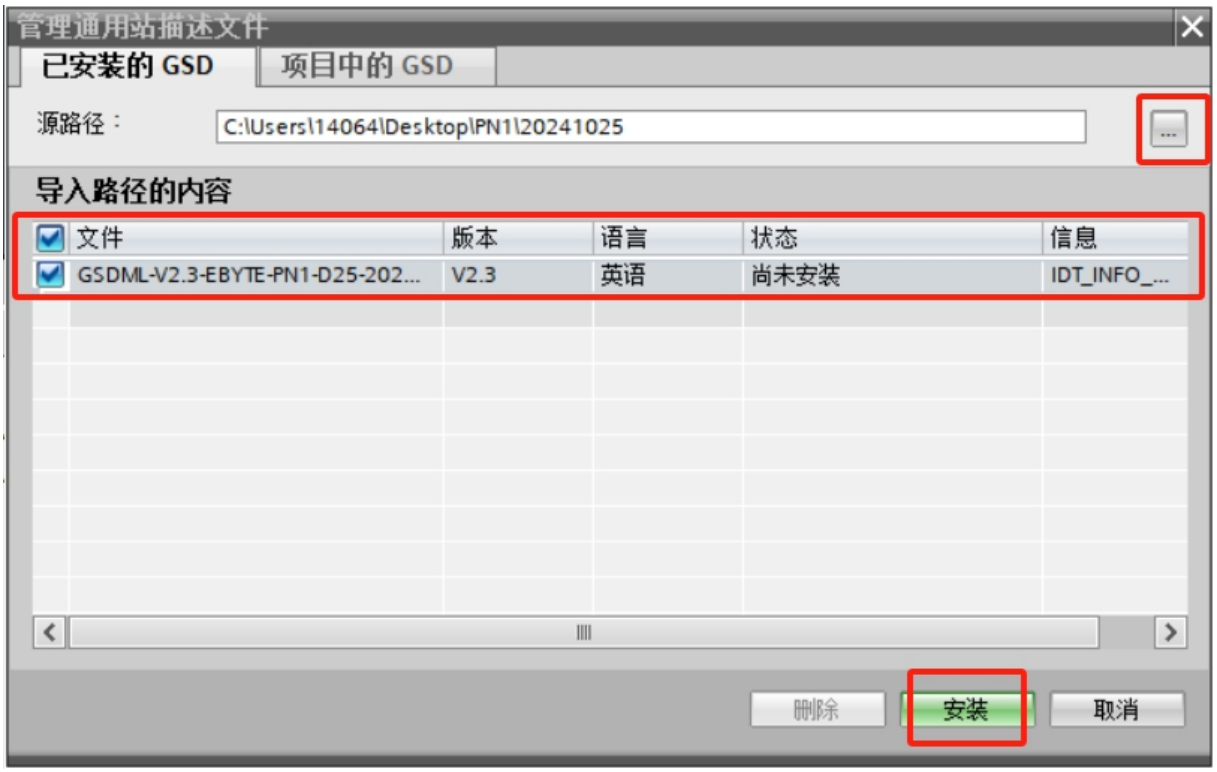
1. Open SIMATIC Step 7, click Options, and manage general site files (gsd)



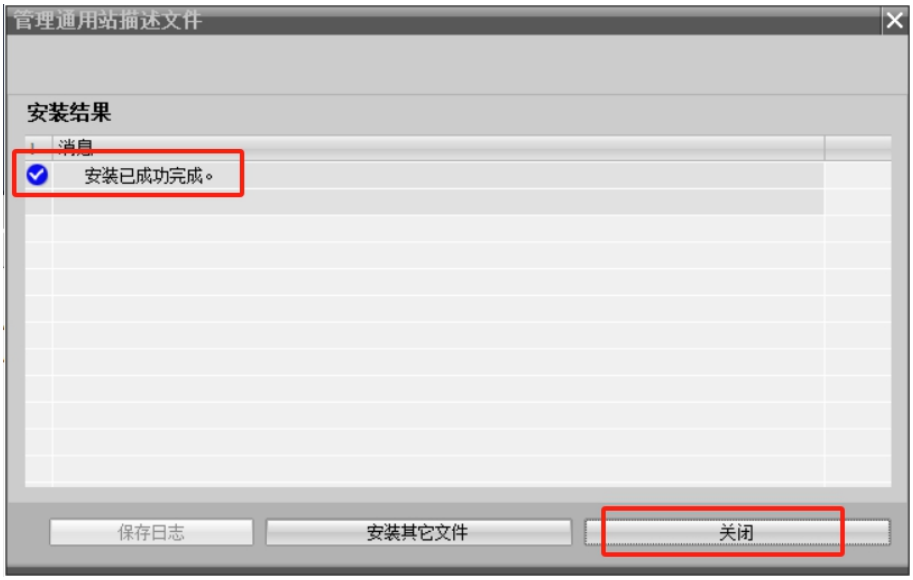
2. Add the GSDML file, find the folder where the GSD is stored, select the folder, and then the software will scan the GSD file by itself, then check the GSD file, and finally click Install.

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



3. After the installation is complete, click Close and then you can configure the device.

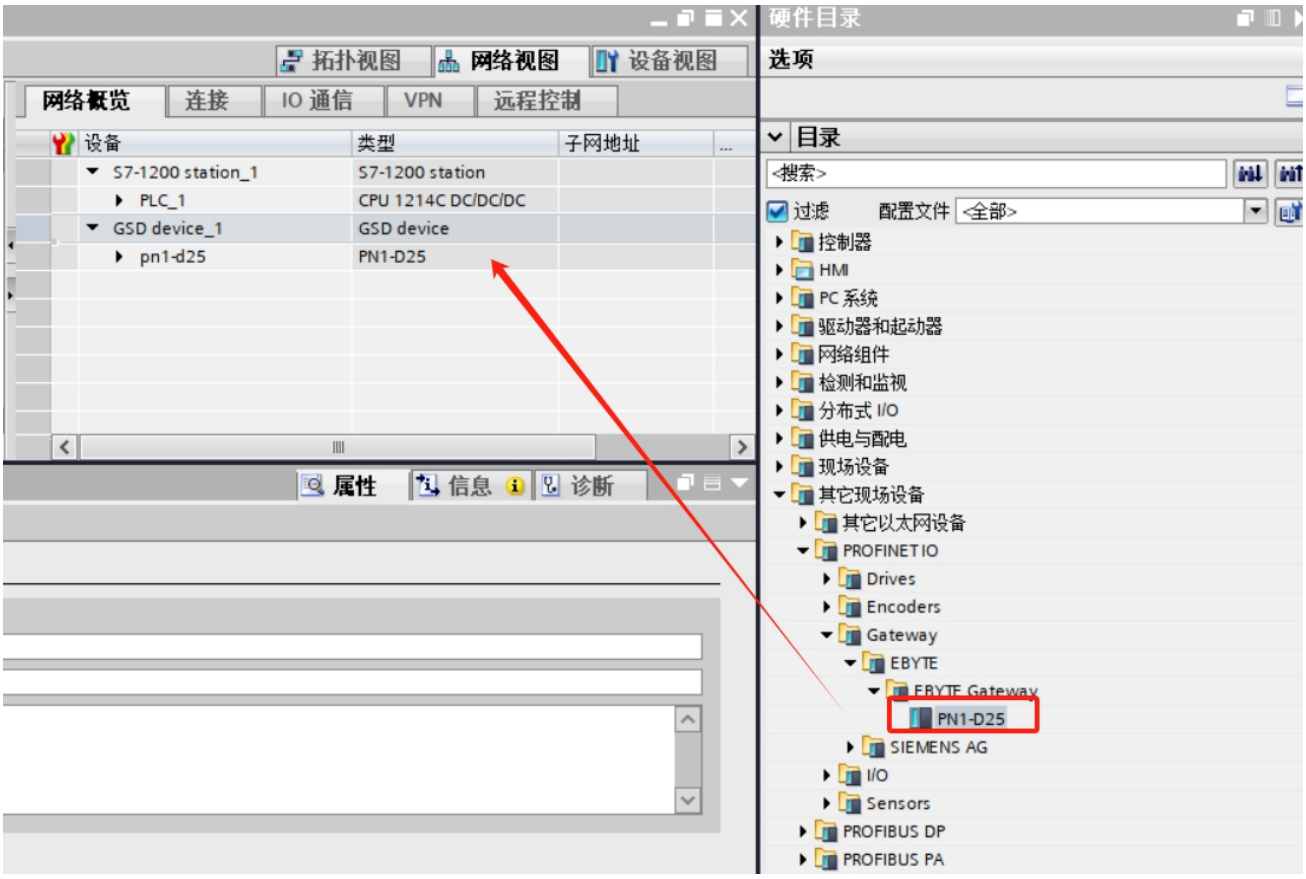


5.3 Add Profinet device to the project

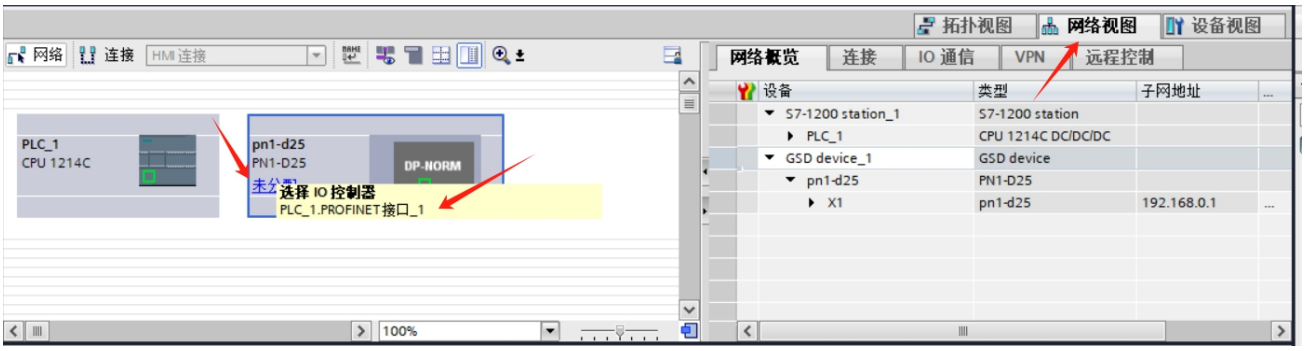
1. Create a new project or open it. If it is a new project, add the controller device first, then go to the device configuration interface, add the corresponding IO module, double-click the module, and it will be added successfully, as shown in the figure:

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

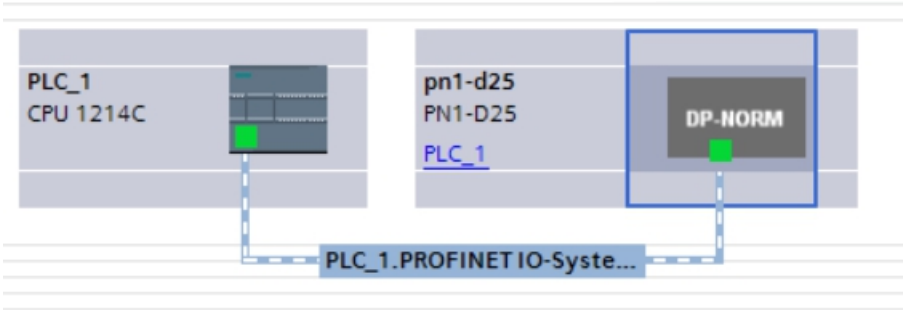
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



2. In the network view, perform device configuration



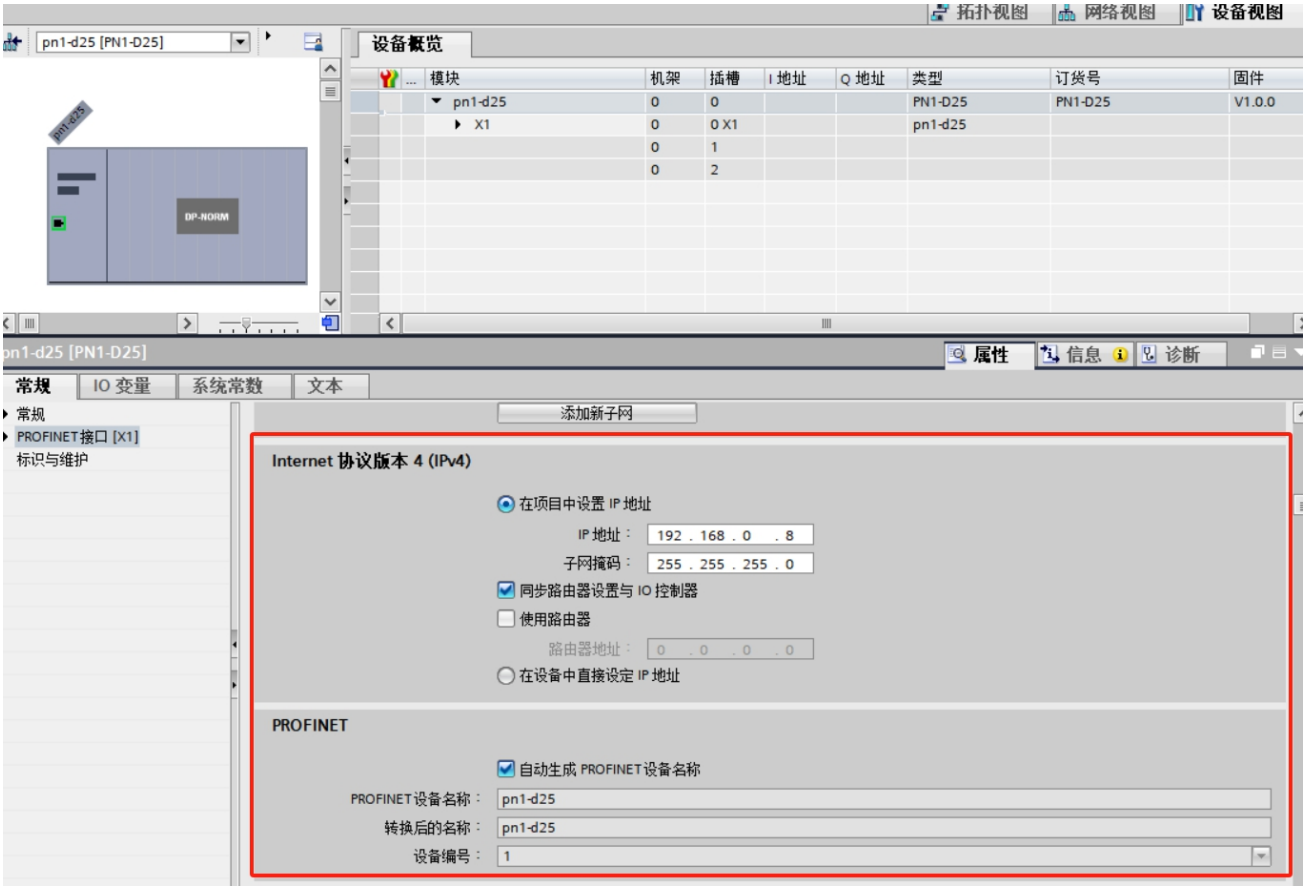
After completion, as shown in the figure:



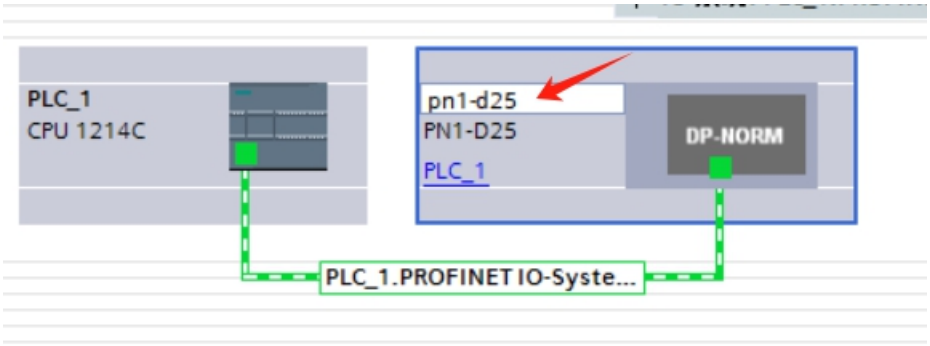
3. In the device view, first locate and select the newly added device, then double-click the module in the picture, and then modify the IP address and device name in the general configuration interface, which must be consistent with the module itself. Alternatively, you can choose to set the IP address directly on the device.

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Click here to modify the device name directly



5.4 Configure modbus communication parameters

After completing the relevant settings, click to enter the device view operation interface. In the device overview area, the system provides two slots for configuring the serial port function module. Each slot can accommodate 32 sub-slots for configuring the Modbus command sub-module. In particular, sub-slot No. 1 corresponds to the serial port status word and serial port control word of the device (applicable to PNMB Master/PNMB Slave configuration). Through the status word, the PLC can obtain the operating status of the PN1-D25 device; and through the control word, the PLC can control the PN1-D25 device.

To adjust the Modbus interface parameters of the PN1-D25 device serial port 1 or serial port 2, first select the target slot (i.e., slot 1 or 2), then select the "Properties" option. During this process, you need to pre-select the serial

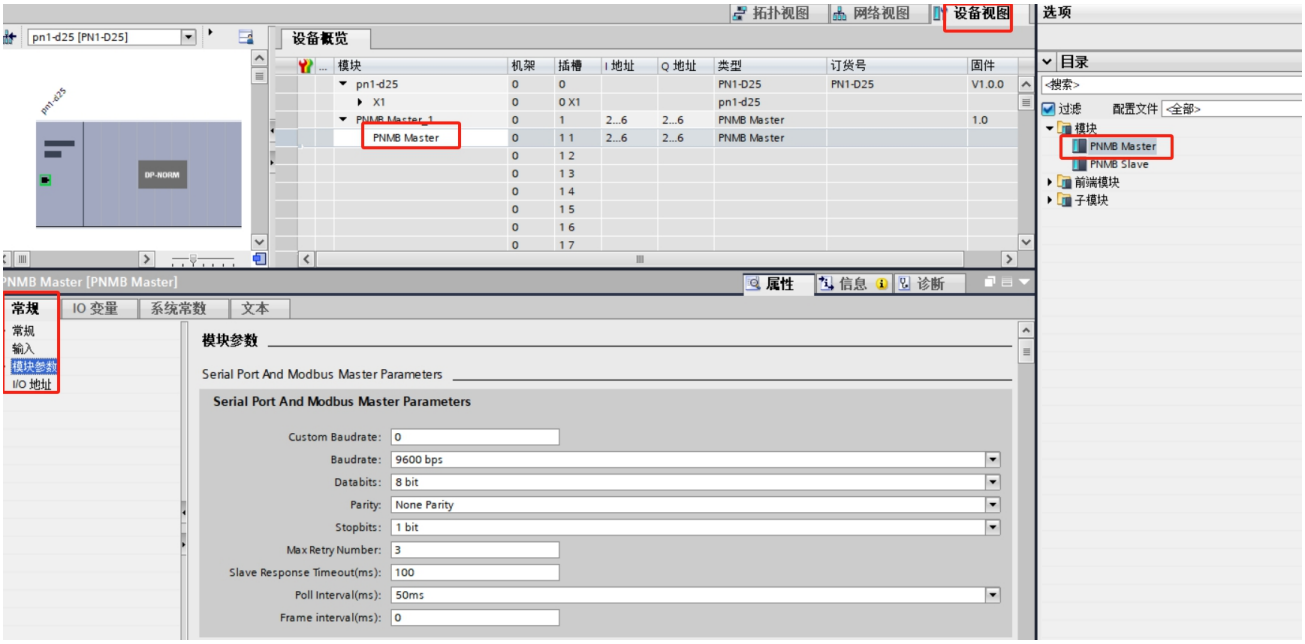
Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

port's operating mode (PNMB Master/PNMB Slave) - Modbus RTU master or slave mode. It is worth noting that the PN1-D25 gateway is compatible with both Modbus RTU master and slave modes.

PN1-D25 device module Modbus communication interface parameters:

PNMB Master



Custom Baud rate:

When the serial port is configured in slave mode and a custom baud rate is required, the default setting is 0. In this case, the custom baud rate is not enabled. To enable the custom baud rate, set a value between 1200 and 3900000. In this case, the "Baud rate" option will not take effect.

Baud rate:

Standard baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800bps, default: 9600.

Databits:

Data bits: 7, 8bit, default: 8.

Parity:

Data verification: None Parity (no verification), Odd Parity (odd verification), Even Parity (even verification), default: None Parity (no verification).

Stopbit:

Data stop bit : 1 , 2 bit , default: 1 .

Max Return Number :

The number of error retries when the serial port is used as a master station, 0-255, 0 means no resend, 255 means unlimited resend, 1-254 means resend according to the number of times , default: 3 .

Slave Response Timeout (ms) :

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

the serial port is used as the master station, the module waits for the Modbus device to respond after sending a Modbus message. If the Modbus device still does not respond within the set waiting time, the module stops waiting and continues to send the next MODBUS message or resends. The selection range is 0 - 65535 ms , default: 100ms .

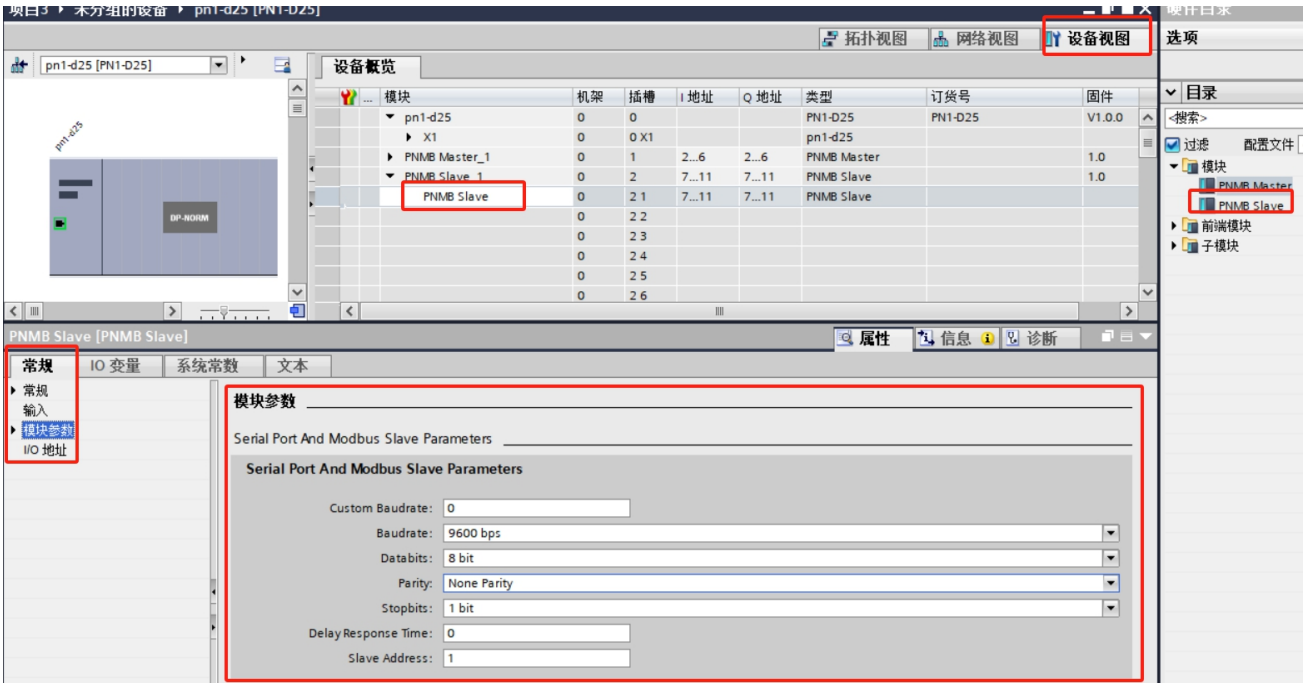
Poll Interval(ms):

the serial port is used as the master station, the bus conversion module delays the time to send the Modbus master station message after receiving the correct message replied by the Modbus slave station. If the Modbus slave station device responds to the master station message slowly, if the bus conversion module sends the Modbus message too quickly, there will be a communication failure. You can increase the message sending interval appropriately. The selection range is 10 , 20, 30, 40, 50, 60, 70, 80, 90, 100, 200 , 500 , 1000ms or no wait (No Delay). The default value is: 50ms .

Frame interval(ms):

Data frame break time: 0-65535ms, 0 means automatic frame break, default: 0.

PNMB Slave



Custom Baud rate:

When the serial port is configured in slave mode and a custom baud rate is required, the default setting is 0. In this case, the custom baud rate is not enabled. To enable the custom baud rate, set a value between 1200 and 3900000. In this case, the "Baud rate" option will not take effect.

Baud rate:

Standard baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800bps, default: 9600.

Databits:

Data bits: 7, 8bit, default: 8.

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Parity:
Data verification: None Parity (no verification), Odd Parity (odd verification), Even Parity (even verification), default: None Parity (no verification).

Stopbit:
Data stop bit : 1 , 2 bit , default: 1 .

Delay Response Time.
When the serial port is a slave, how long does it delay before replying after receiving the polling command sent by the master. Range: 0 ~ 65535 , 0 means immediate reply, unit is ms . Default: 0 .

Slave Address:
The station address when the serial port is used as a slave. Range: 1 ~ 2 47 , default : 1.

Note: The configuration of serial port 2 is the same as that of serial port 1.

5.5 Configure Modbus message (function code)

There are totally 2 slots in the device overview . These 2 slots are used to configure serial port information and master-slave station selection. The status word and control word are already occupied , and the remaining 64 sub -slots (32 sub -slots for each serial port command) are available for configuring MODBUS messages (commands).

Click the module in the hardware directory on the right to provide the master and slave station selection for the serial port, which are PNMB Master (the status word and control word are already occupied and the serial port related parameters need to be configured) and PNMB Slave (the status word and control word are already occupied and the serial port related parameters need to be configured); click the submodule to select the corresponding Modbus RTU command. Simply double-click the message in the hardware directory to configure the message into the MODBUS message queue according to the order of the blank slots.

Modbus RTU Master Commands

Each Modbus RTU master command has five attributes:

Slave Address (1 ~ 247): Indicates the address of the Modbus RTU slave device. The selectable range is 1-247.

Function Code: The function code of the Modbus RTU master. The function code is automatically generated according to the MODBUS command inserted into the slot and cannot be changed.

Start Address: The starting address for Modbus RTU slave data operations. Non-register PLC address , no prefix. Range 0-65535.

XX Quantity : Indicates the number of coils or registers to be read or written. The MODBUS command for inserting data into the slot is automatically generated , and the quantity can be changed within the range .

Transmission Type: Provides the following four transmission types.

Disable: Indicates that the command is not executed.

Poll trigger: After the master station corresponding to Modbus RTU is enabled, the message will be sent in the order of slot number from small to large.

Leve ltrigger (level transmission): After the control transmission flag bit corresponding to the slot number changes from 0 to 1: For a read instruction, the message will be sent. For a write instruction, it will be sent only if

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

the data has changed; after the control transmission flag bit corresponding to the slot number changes from 1 to 0, both the read message and the write message will stop sending. (For example, in the previous section, PLC address QB2-QB 5 is the transmission trigger control bit)

Rising Trigger (send on rising edge): After the trigger control bit corresponding to the slot number changes from 0 to 1, the message will be sent once. (For example, in the previous section, PLC address QB2-QB 5 is the send trigger control bit)

Modbus RTU Slave Commands

Each Modbus RTU slave command is prefixed with Input or Output. Input means data is input into PLC, i.e. the master writes data to the slave, and the slave sends the data to PLC, which corresponds to a write type command. Output means data is output from PLC, i.e. the PLC sends the data to the slave, and the master reads the data from the slave, which corresponds to a read type command. More specifically, each slave command is marked with the supported function code at the end.

Function code	Function	Operation address area (non-register PLC address)	Operation Type
01H	Read multiple coil output states	0XXXX	read
02H	Read multiple input coil states	1xxXX	read
03H	Read multiple holding registers	4xxXX	read
04H	Read Input Register	3XXXX	read
05H	Force a single coil	0XXXX	Write
06H	Presetting a Single Holding Register	4XXXX	Write
OFH	Forced multi-coil	0xXXX	Write
10H	Preset multiple holding registers	4XXXX	Write

5.5.1Routines

Set the device serial port 1 as the master station to write 8-bit coils.

Step 1: Drag PNMB Master into slot 1



Step 2: Select the command in the submodule MBRTU Master Coils 0xxxx

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

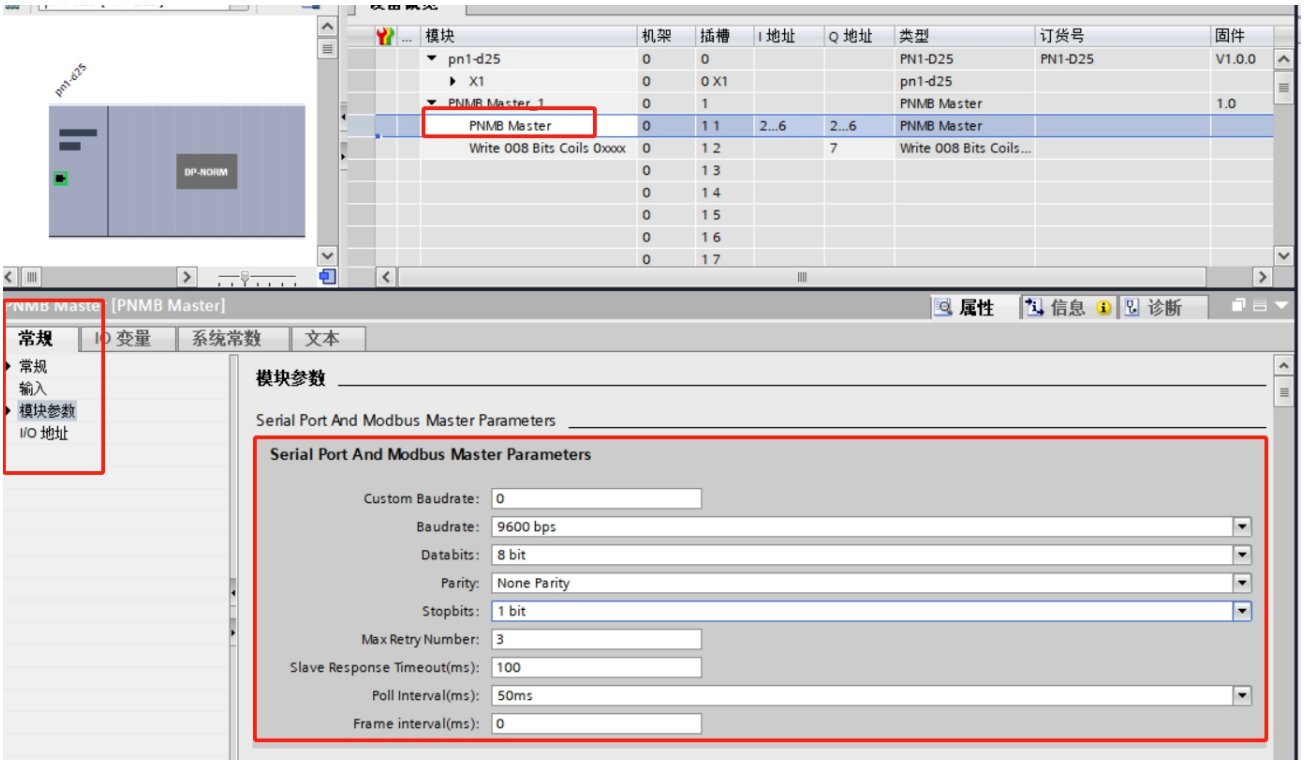
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Step 3: Select MBRTU Write 008 bits 0xxxx



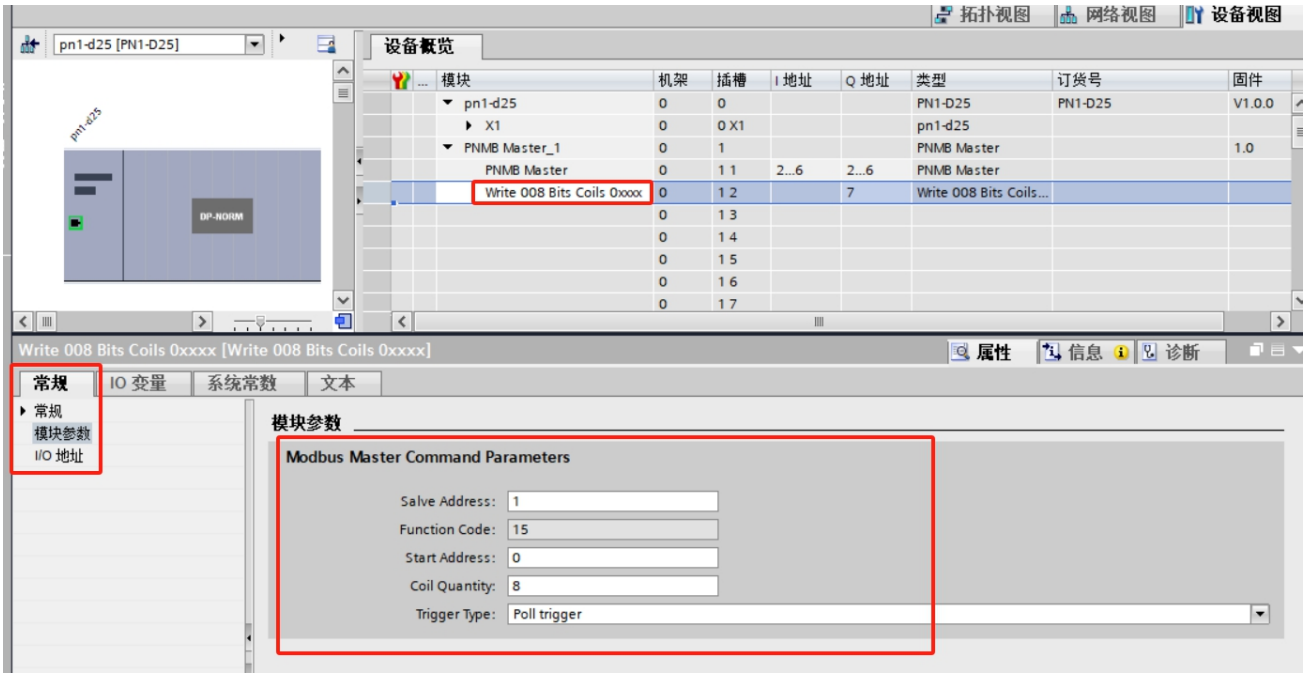
Step 4: Configure the working parameters of the gateway serial port. Select the configuration software tool of the module (PNMB Master) just added. Here you need to configure the serial port parameters of the gateway according to the serial port parameters of the RTU.



Configuration register information for communication between Profinet gateway and RTU;

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



5.6 Configure status word and control word

From the device overview configuration, we can see that slot number 1 can only be used to select PNMB Master/ PNMB Slave. In the I address column, the corresponding Profinet input address IB2-6 is the communication status monitoring bit. In the Q address column, the corresponding Profinet output address QB2-6, QB2 is the communication control word (control) of this bus conversion module, and QB3-6 is the control bit sent for each message.

Communication status monitoring:

1st byte: The slot number of serial port 1 where the error occurred

Byte 2: Serial port 1 error code

The other bytes are reserved.

Error Code	describe
1	The slave replies to the modbus standard error: ILLEGAL FUNCTION
2	The slave replies with modbus standard error: ILLEGAL DATA ADDRESS
3	The slave replies with modbus standard error: ILLEGAL DATA VALUE
4	The slave replies with the modbus standard error: SLAVE DEVICE FAILURE
10	The length of the message received by the master is wrong . It is too long, too short, or inconsistent with the correct length of the slave reply data.
11	CRC check error of the message received by the master station
12	The master station receives the wrong number of message registers
13	The slave address of the message received by the master is wrong
14	Master receiving timeout
15	The function code in the message received by the master station is inconsistent with the request

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

16	The register address of the message received by the master station is wrong
17	Unknown error

Communication control bits:

Bit 0: Whether the Modbus function serial port interface is enabled, 1 = enabled, 0 = not enabled;

Bit 1: Clear fault code. When a rising edge (0→1) is detected, the communication status monitoring is cleared.

The other bits are reserved.

Bytes 2 to 5:

Each slot message corresponds to one bit. The corresponding format is shown in the following table.

When the message is configured as rising edge triggered, when this bit changes from 0 to 1, the message is enabled to be sent once.

When the message is configured as level-triggered, when this position is set to 1, the message enables cyclic transmission, and when it is set to 0, the message stops cyclic transmission.

Byte 2							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Subslot 9	Subslot 8	Subslot 7	Subslot 6	Subslot 5	Subslot 4	Subslot 3	Subslot 2
Byte 3							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Subslot 17	Subslot 16	Subslot 15	Subslot 14	Subslot 13	Subslot 12	Subslot 11	Subslot 10
Byte 4							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Subslot 25	Subslot 24	Subslot 23	Subslot 22	Subslot 21	Subslot 20	Subslot 19	Subslot 18
Byte 5							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Subslot 33	Subslot 32	Subslot 31	Subslot 30	Subslot 29	Subslot 28	Subslot 27	Subslot 26

The configuration status word and control word of slot 2 are consistent with those of slot 1.

5.6.1 Routines

Program segment 1 is used to open the gateway's channel 1 serial port, and program segment 2 uses the PLC's built-in input to control the extended coil

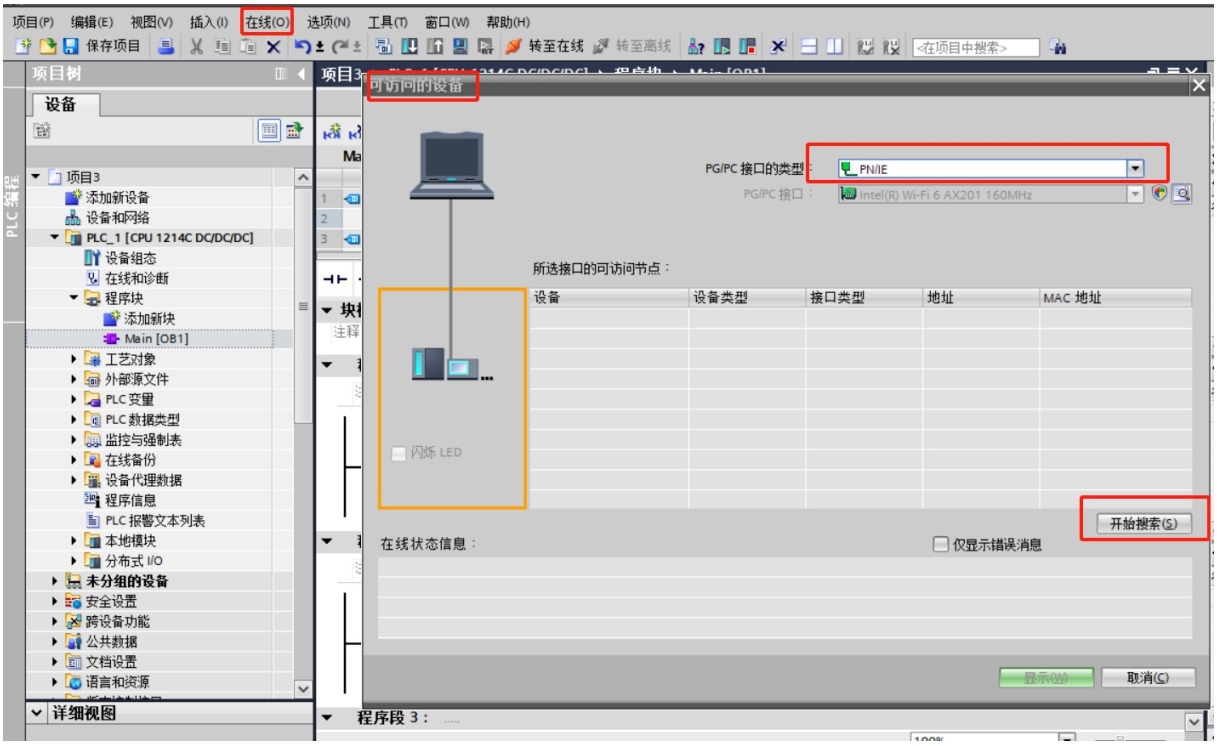
Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



5.7 Use SIMATIC Step 7 to modify module name and query IP address

Open the SIMATIC Step 7 software and click the "Online" option in the menu bar.
In the online access interface that opens, find and select Accessible Devices.
Perform a device search. Once the search is complete, all accessible devices will be listed.
Select the target device whose IP address and name need to be modified from the list.
Modify the IP address and name of the selected device.



Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Chapter 6 Tutorial on devices loading by STEP 7

6.1 Preparation before connection

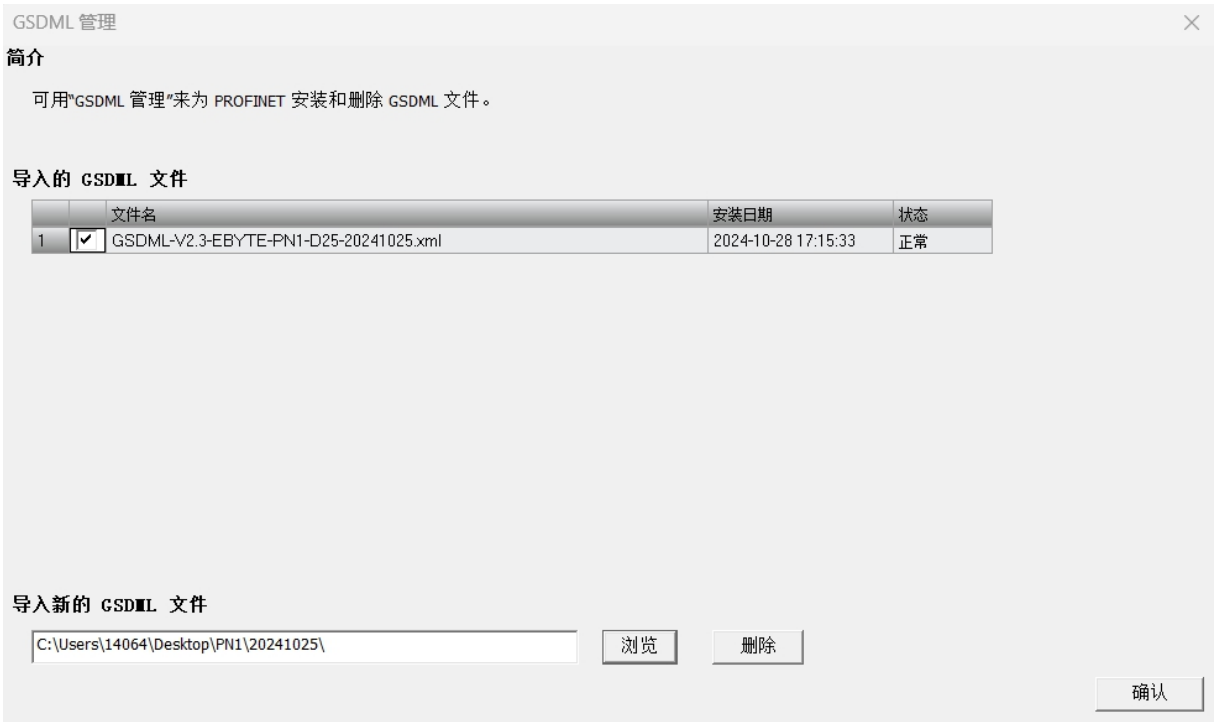
1. Prepare the required XML files as follows:
   GSDML-V2.3-EBYTE-PN1-D25-20241025.xml
2. Connect the DC 24V external power supply to the module and power it on. Before powering on, check whether the positive and negative poles of the power supply are connected correctly.
3. Use a network cable to connect the module to the Profinet interface of the PLC controller. (In the same network segment)

6.2 Add GSDML file by STEP 7

1. Under the File menu, go to GSDML Manager



2. Add GSDML file



Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

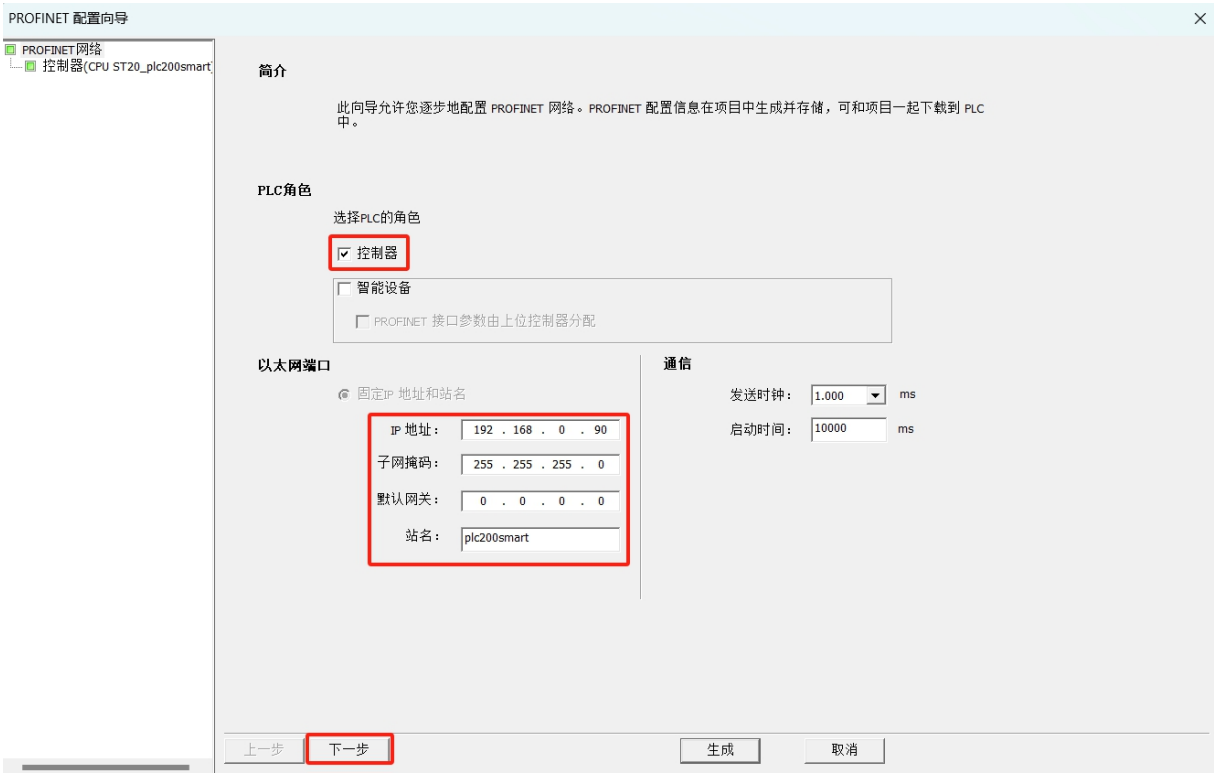
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.3 Add Profinet device to the project

1. Select the PROFINET command under the Tools menu



2. Select the PLC role as PLC controller, set the corresponding PLC controller IP and other related parameters. Click Next after completion.



In the right column , select PROFINET-IO→Gateway→EBYTE→TION→EBYTE Gateway→PN1-D25V1.0.0 by clicking on it, then hold down the left button and drag it into the table on the left.

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

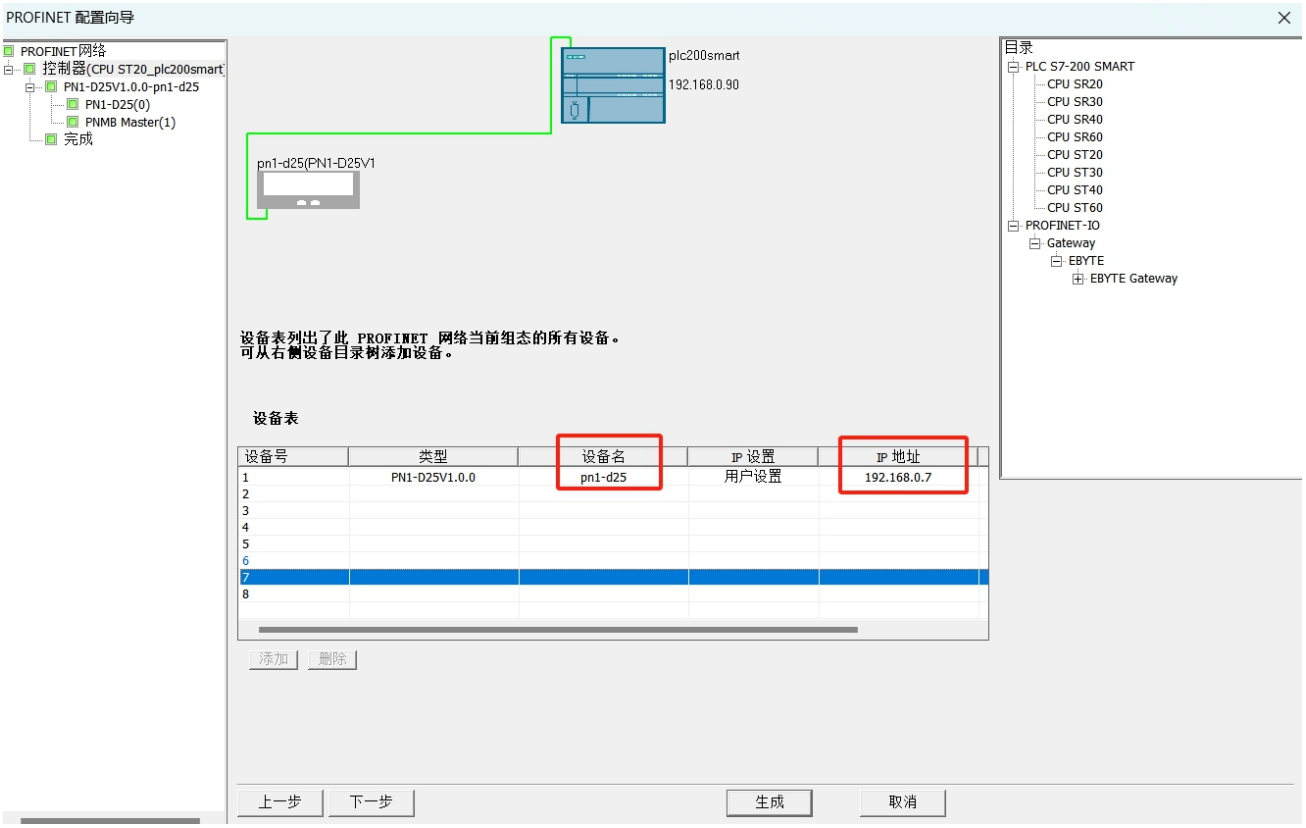


Double-click the device name column and fill in the corresponding device name. There cannot be the same device name in the same project. Similarly, set the IP address and keep it in the same network segment as the PLC controller . Finally, click Generate .

Note: The device name set at this time needs to be consistent with the device. If you are not sure about the device name, you can set it at random first, and then change the device name of the module to be consistent . The IP address set at this time will set the IP of the module with the same device name to the value set here during configuration . For device name modification, please refer to the "STEP 7 Modify Module Name and Query Module IP Address" section .

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



6.4 Configure modbus communication parameters

After completing the relevant settings, click to enter the device view operation interface. In the device overview area, the system provides two slots for configuring the serial port function module. Each slot can accommodate 32 sub-slots for configuring the Modbus command sub-module. In particular, sub-slot No. 1 corresponds to the serial port status word and serial port control word of the device (applicable to PNMB Master/PNMB Slave configuration). Through the status word, the PLC can obtain the operating status of the PN1-D25 device; and through the control word, the PLC can control the PN1-D25 device.

To adjust the Modbus interface parameters of the PN1-D25 device serial port 1 or serial port 2, first select the target slot (i.e., slot 1 or 2), then select the "Properties" option. During this process, you need to pre-select the serial port's operating mode (PNMB Master/PNMB Slave) - Modbus RTU master or slave mode. It is worth noting that the PN1-D25 gateway is compatible with both Modbus RTU master and slave modes.

PN1-D25 device module Modbus communication interface parameters:

PNMB Master

Custom Baudrate:

When the serial port is configured in slave mode and a custom baud rate is required, the default setting is 0. In this case, the custom baud rate is not enabled. To enable the custom baud rate, set a value between 1200 and 3900000. In this case, the "Baudrate" option will not take effect.

Baudrate:

Standard baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800bps, default: 9600.

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Databits:
Data bits: 7, 8bit, default: 8.

Parity:
Data verification: None Parity (no verification), Odd Parity (odd verification), Even Parity (even verification), default: None Parity (no verification).

Stopbit:
Data stop bit : 1 , 2 bit , default: 1 .

Max Return Number :
The number of error retries when the serial port is used as a master station, 0-255, 0 means no resend, 255 means unlimited resend, 1-254 means resend according to the number of times , default: 3 .

Slave Response Timeout (ms) :
the serial port is used as the master station, the module waits for the Modbus device to respond after sending a Modbus message. If the Modbus device still does not respond within the set waiting time, the module stops waiting and continues to send the next MODBUS message or resends. The selection range is 0 - 65535 ms , default: 100ms .

Poll Interval(ms):
the serial port is used as the master station, the bus conversion module delays the time to send the Modbus master station message after receiving the correct message replied by the Modbus slave station. If the Modbus slave station device responds to the master station message slowly, if the bus conversion module sends the Modbus message too quickly, there will be a communication failure. You can increase the message sending interval appropriately. The selection range is 10 , 20, 30, 40, 50, 60, 70, 80, 90, 100, 200 , 500 , 1000ms or no wait (No Delay). The default value is: 50ms .

Frame interval(ms):
Data frame break time: 0-65535ms, 0 means automatic frame break, default: 0.

PNMB Slave
Custom Baudrate:
When the serial port is configured in slave mode and a custom baud rate is required, the default setting is 0. In this case, the custom baud rate is not enabled. To enable the custom baud rate, set a value between 1200 and 3900000. In this case, the "Baudrate" option will not take effect.

Baudrate:
Standard baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800bps, default: 9600.

Databits:
Data bits: 7, 8bit, default: 8.

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Parity:
Data verification: None Parity (no verification), Odd Parity (odd verification), Even Parity (even verification), default: None Parity (no verification).

Stopbit:
Data stop bit : 1 , 2 bit , default: 1 .

Delay Response Time.
When the serial port is a slave, how long does it delay before replying after receiving the polling command sent by the master. Range: 0 ~ 65535 , 0 means immediate reply, unit is ms . Default: 0 .

Slave Address:
The station address when the serial port is used as a slave. Range: 1 ~ 2 47 , default : 1.

Note: The configuration of serial port 2 is the same as that of serial port 1.

6.5 Configure Modbus message (function code)

2 slots in the device overview . These 2 slots are used to configure serial port information and master-slave station selection. The status word and control word are already occupied , and the remaining 64 sub -slots (32 sub -slots for each serial port command) are available for configuring MODBUS messages (commands).

Click the module in the hardware directory on the right to provide the master and slave station selection for the serial port, which are PNMB Master (the status word and control word are already occupied and the serial port related parameters need to be configured) and PNMB Slave (the status word and control word are already occupied and the serial port related parameters need to be configured); click the submodule to select the corresponding Modbus RTU command. Simply double-click the message in the hardware directory to configure the message into the MODBUS message queue according to the order of the blank slots.

Modbus RTU Master Commands

Each Modbus RTU master command has five attributes:

Slave Address (1 ~ 247): Indicates the address of the Modbus RTU slave device. The selectable range is 1-247.

Function Code: The function code of the Modbus RTU master. The function code is automatically generated according to the MODBUS command inserted into the slot and cannot be changed.

Start Address: The starting address for Modbus RTU slave data operations. Non-register PLC address , no prefix. Range 0-65535.

XX Quantity : Indicates the number of coils or registers to be read or written. The MODBUS command for inserting data into the slot is automatically generated , and the quantity can be changed within the range .

Transmission Type: Provides the following four transmission types.

Disable: Indicates that the command is not executed.

Poll trigger: After the master station corresponding to Modbus RTU is enabled, the message will be sent in the order of slot number from small to large.

Leve ltrigger (level transmission): After the control transmission flag bit corresponding to the slot number changes from 0 to 1: For a read instruction, the message will be sent. For a write instruction, it will be sent only if the data has changed; after the control transmission flag bit corresponding to the slot number changes from 1 to 0,

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

both the read message and the write message will stop sending. (For example, in the previous section, PLC address QB2-QB 5 is the transmission trigger control bit)

Rising Trigger (send on rising edge): After the trigger control bit corresponding to the slot number changes from 0 to 1, the message will be sent once. (For example, in the previous section, PLC address QB2-QB 5 is the send trigger control bit)

Modbus RTU Slave Commands

Each Modbus RTU slave command is prefixed with Input or Output. Input means data is input into PLC, i.e. the master writes data to the slave, and the slave sends the data to PLC, which corresponds to a write type command. Output means data is output from PLC, i.e. the PLC sends the data to the slave, and the master reads the data from the slave, which corresponds to a read type command. More specifically, each slave command is marked with the supported function code at the end.

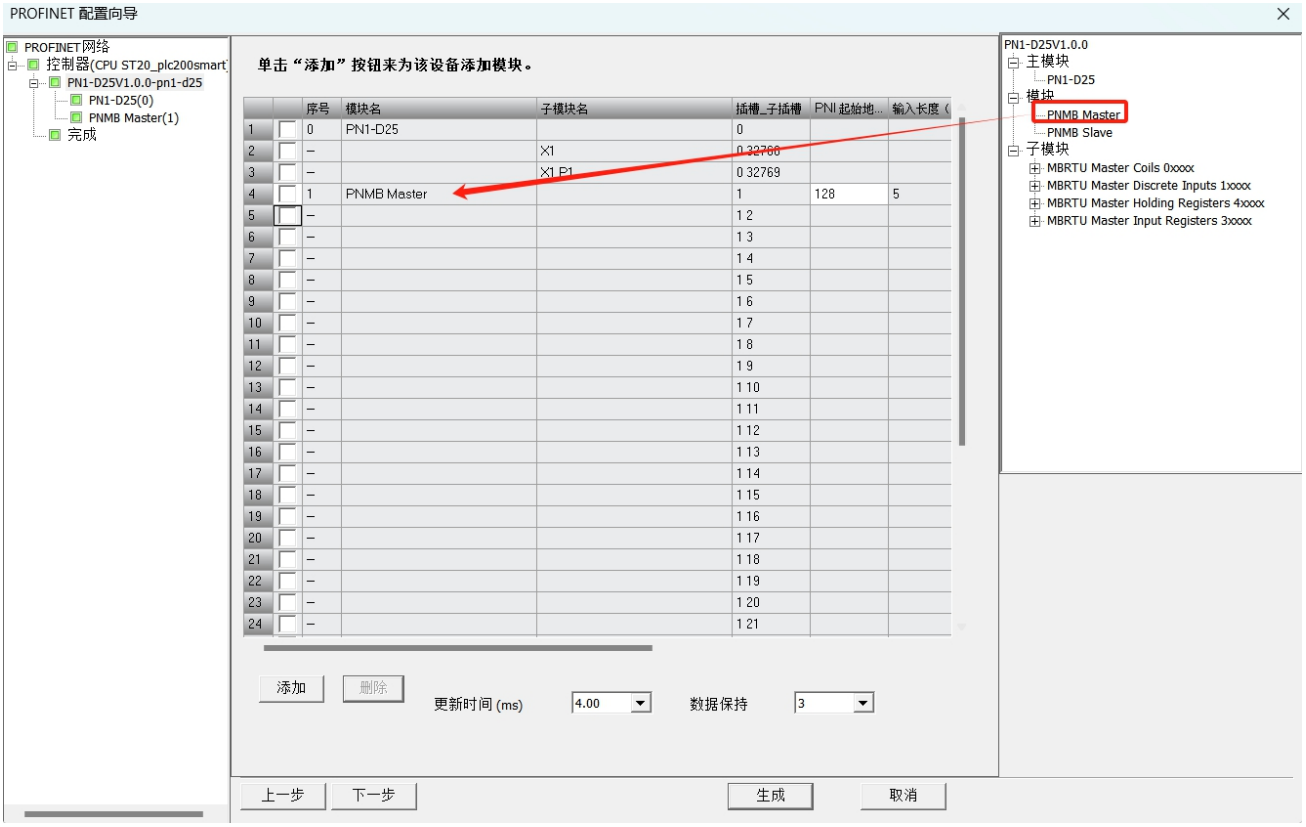
Function code	Function	Operation address area (non-register PLC address)	Operation Type
01H	Read multiple coil output states	0XXXX	read
02H	Read multiple input coil states	1xxXX	read
03H	Read multiple holding registers	4xxXX	read
04H	Read Input Register	3XXXX	read
05H	Force a single coil	0XXXX	Write
06H	Presetting a Single Holding Register	4XXXX	Write
OFH	Forced multi-coil	0xXXX	Write
10H	Preset multiple holding registers	4XXXX	Write

6.5.1 Routines

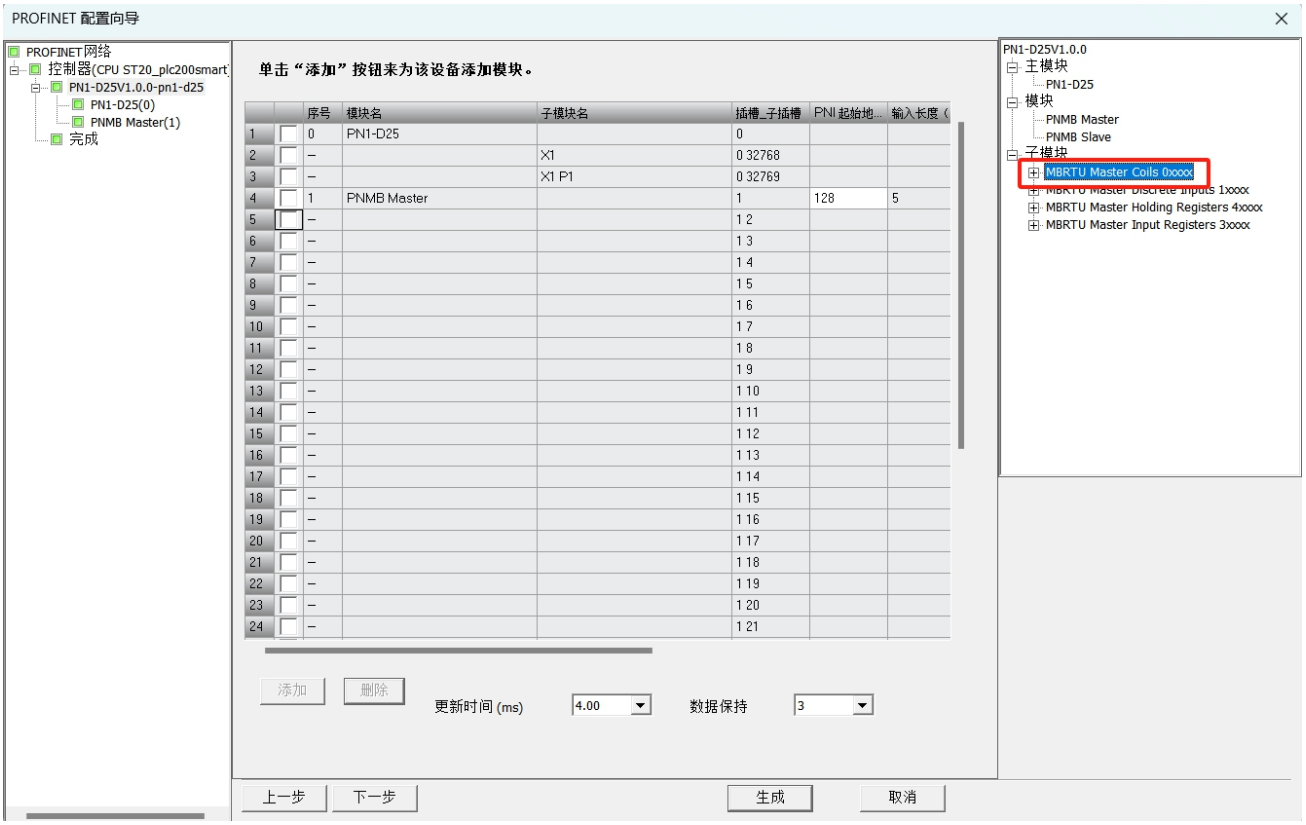
Set the device serial port 1 as the master station to write 8-bit coils.
Step 1: Drag PNMB Master into slot 1,

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



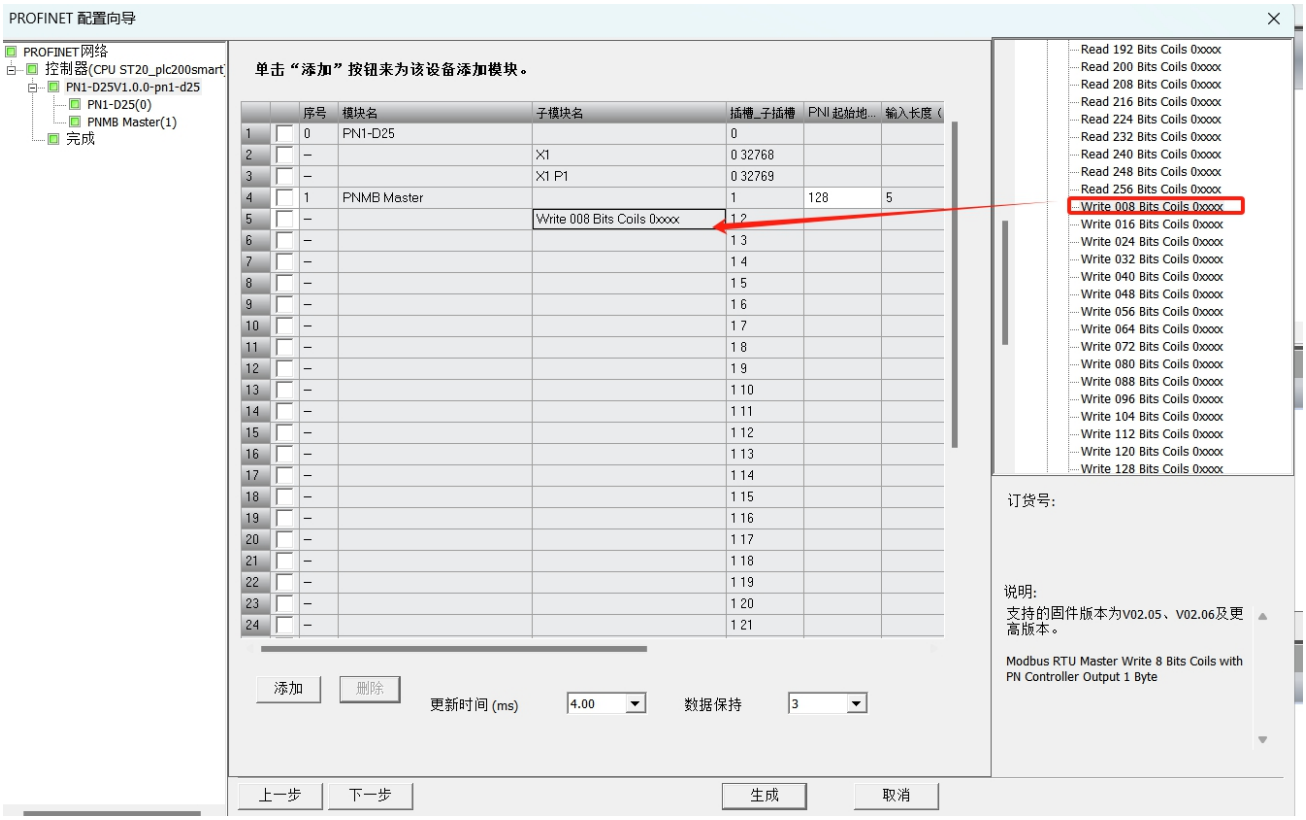
Step 2: Select the command in the submodule MBRTU Master Coils 0xxxx



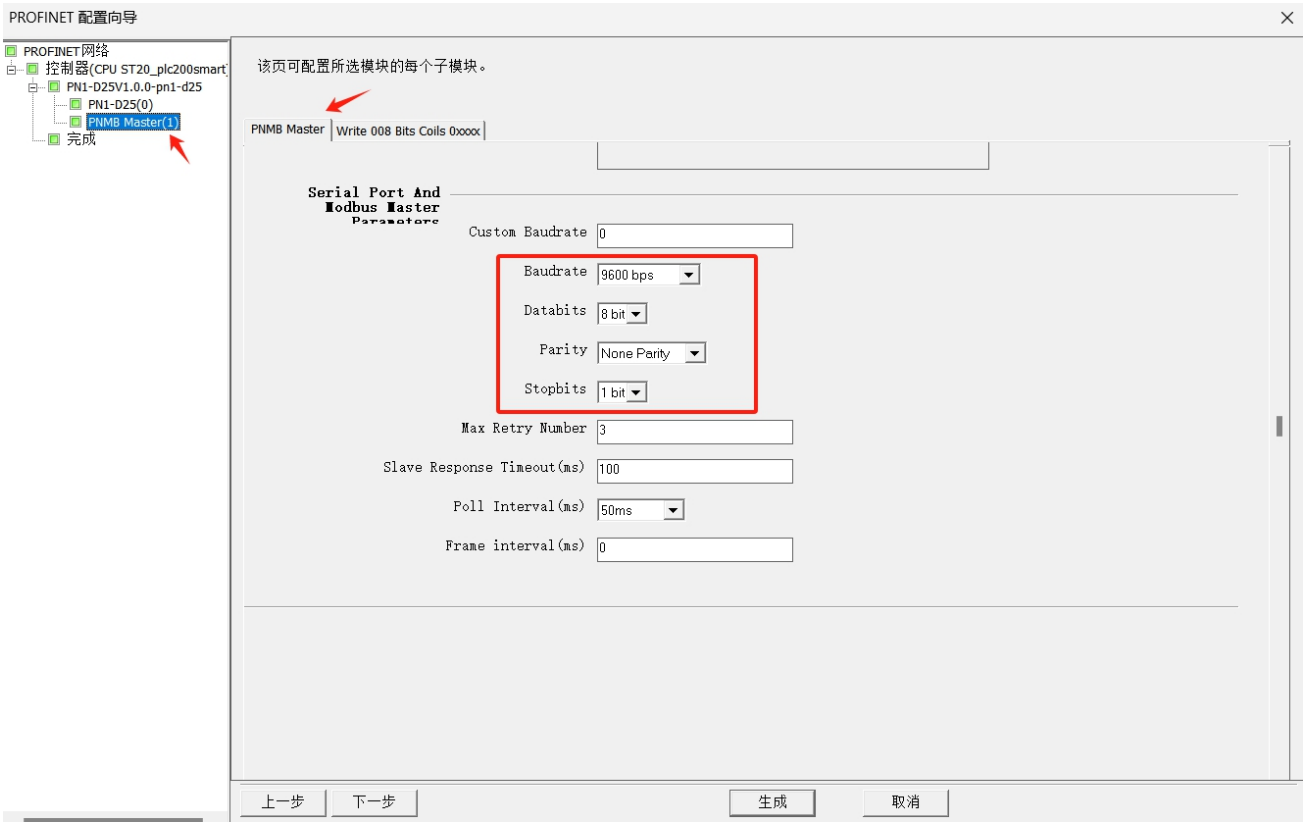
Step 3: Select MBRTU Write 008 bits 0xxxx

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



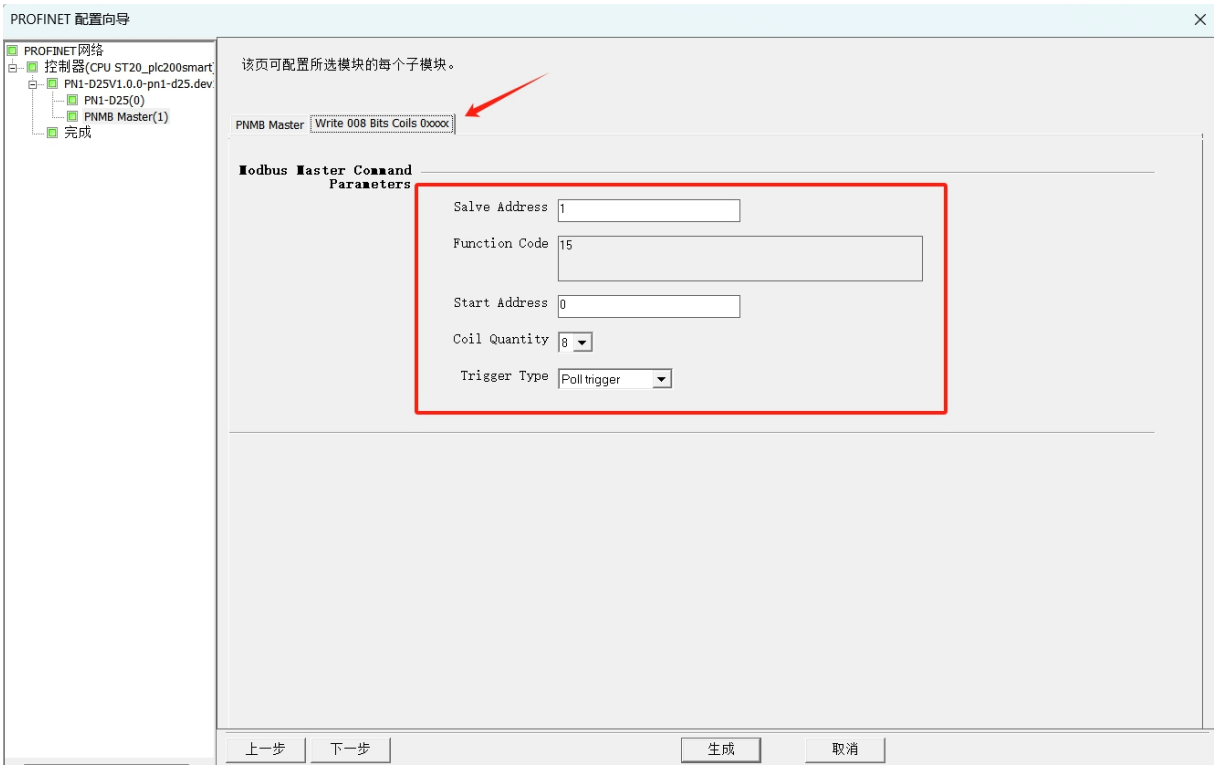
Step 4: Configure the working parameters of the gateway serial port. Select the configuration software tool of the module (PNMB Master) just added. Here you need to configure the serial port parameters of the gateway according to the serial port parameters of the RTU.



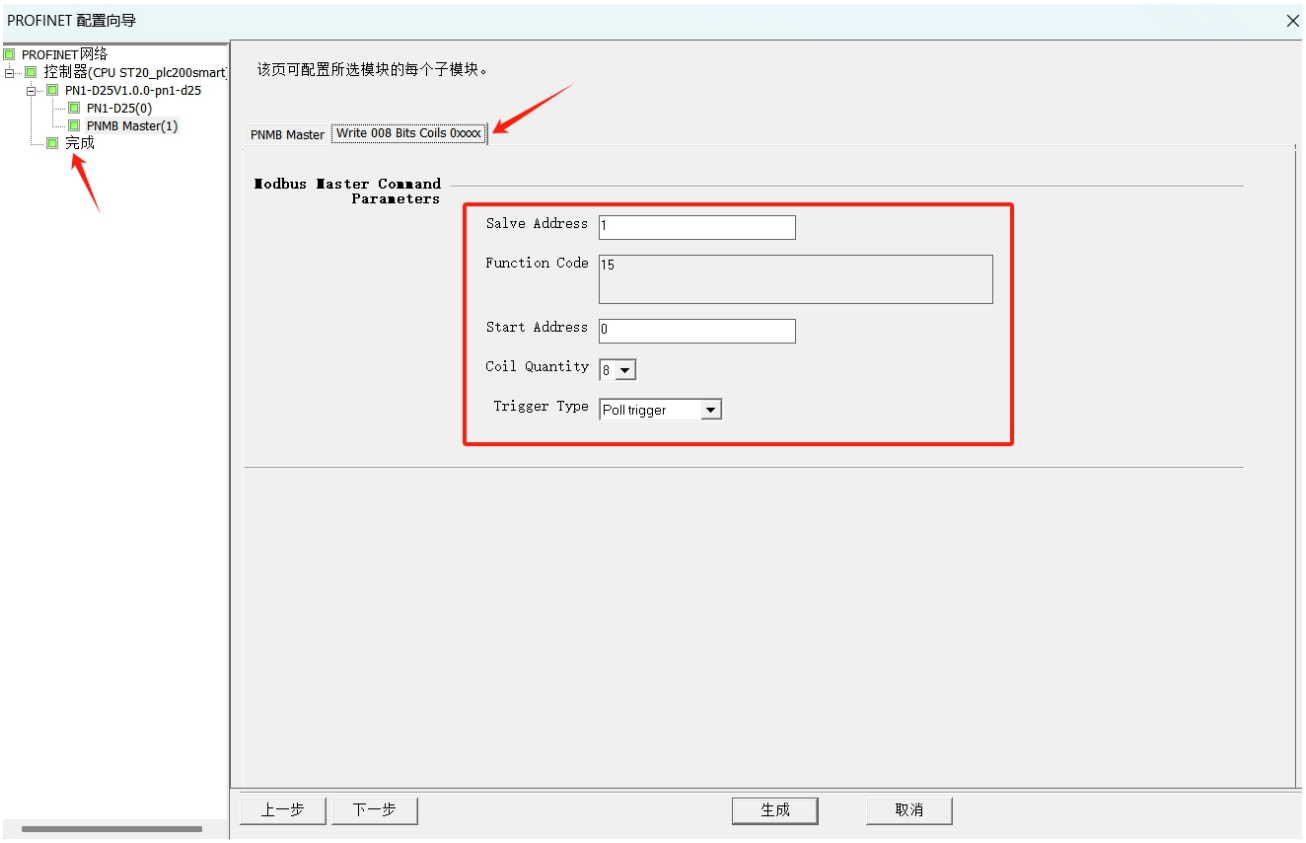
Configuration register information for communication between Profinet gateway and RTU;

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Then click Finish, check the address corresponding to the device, and finally click Generate



Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.6 Configure status word and control word

From the device overview configuration, we can see that slot number 1 can only be used to select PNMB Master/ PNMB Slave. In the I address column, the corresponding Profinet input address IB128-132 is the communication status monitoring bit. In the Q address column, the corresponding Profinet output address QB128-132, QB128 is the communication control word (control) of this bus conversion module, and QB129-132 is the control bit sent for each message.

Communication status monitoring:

1st byte: The slot number of serial port 1 where the error occurred

Byte 2: Serial port 1 error code

The other bytes are reserved.

Error Code	Description
1	The slave replies to the modbus standard error: ILLEGAL FUNCTION
2	The slave replies with modbus standard error: ILLEGAL DATA ADDRESS
3	The slave replies with modbus standard error: ILLEGAL DATA VALUE
4	The slave replies with the modbus standard error: SLAVE DEVICE FAILURE
10	The length of the message received by the master is wrong , too long, too short, or inconsistent with the correct length of the slave reply data.
11	CRC check error of the message received by the master station
12	The master station receives the wrong number of message registers
13	The slave address of the message received by the master is wrong
14	Master receiving timeout
15	The function code in the message received by the master station is inconsistent with the request
16	The register address of the message received by the master station is wrong
17	Unknown error

Communication control bits:

Bit 0: Whether the Modbus function serial port interface is enabled, 1 = enabled, 0 = not enabled;

Bit 1: Clear fault code. When a rising edge (0→1) is detected, the communication status monitoring is cleared.

The other bits are reserved.

Bytes 2 to 5:

Each slot message corresponds to one bit. The corresponding format is shown in the following table.

When the message is configured as rising edge triggered, when this bit changes from 0 to 1, the message is enabled to be sent once.

When the message is configured as level-triggered, when this position is set to 1, the message enables cyclic transmission, and when it is set to 0, the message stops cyclic transmission.

Byte 2							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Subslot 9	Subslot 8	Subslot 7	Subslot 6	Subslot 5	Subslot 4	Subslot 3	Subslot 2

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

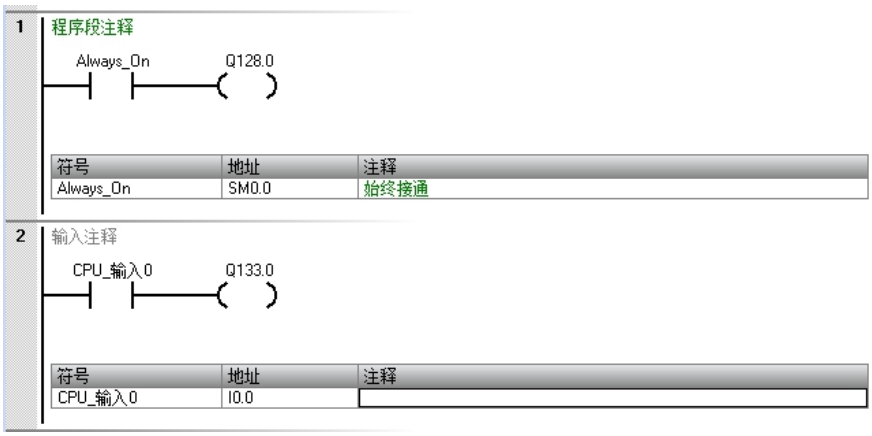
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Byte 3							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Subslot 17	Subslot 16	Subslot 15	Subslot 14	Subslot 13	Subslot 12	Subslot 11	Subslot 10
Byte 4							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Subslot 25	Subslot 24	Subslot 23	Subslot 22	Subslot 21	Subslot 20	Subslot 19	Subslot 18
Byte 5							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Subslot 33	Subslot 32	Subslot 31	Subslot 30	Subslot 29	Subslot 28	Subslot 27	Subslot 26

The configuration status word and control word of slot 2 are consistent with those of slot 1.

6.6.1 Routines

Program segment 1 is used to open the gateway's channel 1 serial port, and program segment 2 uses the PLC's built-in input to control the extended coil



6.7 Use STEP 7 to modify the module name and query the IP address

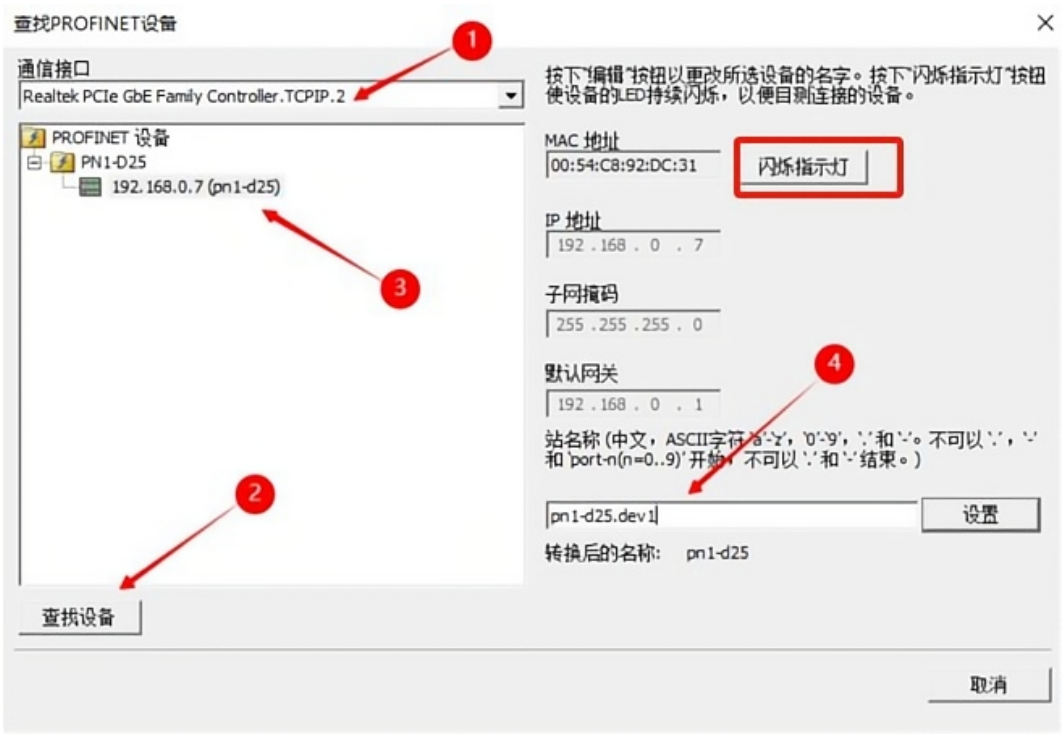
Search for the gateway device through the Profinet tool of STEP 7-MicroWIN SMART, and configure a unique working "station name" for the gateway for communication between the PLC and the corresponding gateway;



Open the tool and select the computer network card connected to the gateway. Select the gateway configuration "station name". If there are multiple modules, you can locate the gateway device that needs to be configured by the flashing indicator light.

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Revision History

Version	Revision Date	Revision Notes	Maintainer
1.0	202 4 - 11 - 14	Initial release	LT

About Us

Sales hotline: 4000-330-990
Technical support: support@cdebyte.com Official website: www.cdebyte.com
Company Address: Building B5, No. 199, Xiqu Avenue, West Hi-Tech Zone, Chengdu, Sichuan

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

Copyright © 2012–2025 , Chengdu Ebyte Electronic Technology Co., Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000