Chengdu Ebyte Electronic Technology Co.,Ltd

Wireless Modem

User Manual



Profinet to Modbus TCP/RTU Gateway PN1-D25PT User Manual

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 Functional 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 descriptions 6
Chapter 3 Product Function Introduction 7
3.1 PN1-D25PT Series Function Overview 7
3.2 Modify IP address 7
3.3 Upgrade function 7
3.4 Reset and factory reset 7
Chapter 4 Explanation of Equipment Alarm Information 8
Chapter 5 Tutorial on Loading Devices Using TIA Portal 9
5.1 Preparation before connection 9
5.2 Add GSDML file to TIBRA 9
5.3 Add Profinet device to project 10
5.4 Configure Modbus communication parameters 13
5.5 Modbus communication interface parameters for PN1-D25PT device module: 14
5.6 Configure Modbus status word and control word 19
5.6.1 Modbus RTU status word and control word 20
5.6.2 Modbus TCP status words and control words 21
5.7 Submodule parameter description 23
5.7.1 Serial Port Enable Routine 24
5.7.2 Network Socket Enabler Routine 25
5.8 Using TIA Portal to modify module names and query IP addresses 25
Chapter 6 Tutorial on Loading Devices Using STEP 7 27
6.1 Preparations before connection 27
6.2 STEP 7 Add GSDML file 27
6.3 Adding Profinet devices to the project 28
6.4 Configure Modbus communication parameters 30
6.5 Configure Modbus status word and control word 34
6.5.1 Serial Port Enable Routine 38
6.5.2 Network Socket Enabler Routine 39
6.6 Using STEP 7 to modify module names and query IP addresses 39
Chapter 7 Precautions 41
Revision History 42
About us 43

Copyright © 2012–2026 , 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-D25PT series gateway primarily features Profinet to Modbus TCP conversion, while also being compatible with Modbus RTU, enabling mapping and transmission of Modbus data to the Profinet protocol.

Device integration is completed simply by importing the GSD file; no programming is required to read and write Modbus device data, quickly configure and upload data to the PLC.

The device is configured with one RS422/RS485 compatible serial port, supporting 48 communication command nodes for both Modbus RTU and Modbus TCP. It is equipped with dual RJ45 network ports with switch functionality, and a dedicated network port for Modbus TCP communication.

Modbus commands are loaded modularly, and the data mapping relationship between the two protocols is clear and can be directly viewed in STEP7 and TIA Portal software. It supports reading status bytes for real-time monitoring of Modbus device connection and operation status.

1.2 Functional Features

- Utilizes standard Profinet protocol for communication, enabling networking with PLCs, configuration files, and host computers.
- Supports the entire Siemens PLC series (200/300/1200/1500).
- Supports TIA Portal/SETP 7 host computer configuration.
- Converts between Profinet and Modbus TCP/RTU protocols, allowing use as a Modbus TCP/RTU slave or master.
- Supports 8 sockets in Modbus TCP mode; as a master, it can connect to 8 slaves simultaneously, and as a slave, it can support 8 master connections simultaneously.
- Supports one RS422 port (compatible with RS485), parameters can be configured as needed.
- Dual network ports with 10/100M auto-sensing, supporting switch functionality.
- Supports 8 ~ 28V wide voltage input, with reverse connection protection.
- Features multiple protections including electrostatic discharge, surge, and electrical fast pulse/burst protection.
- Simple configuration, no host computer required, GSD file provided directly.
- Built-in hardware and software watchdog timers ensure stable operation and reliable data transmission.
- Industrial-grade hardware design with an aluminum alloy metal casing.
- Supports standard 35mm DIN rail mounting.
- Widely used for data acquisition and control of Modbus TCP/RTU devices in industrial settings.

Copyright © 2012–2026 , 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-D25PT	2 (PN) + 1 (Modbus TCP)	1 RS422 port (compatible with RS485)

2.2 Specifications

category	name	parameter
power supply	Working voltage	DC 8 ~ 28 V ; With reverse connection protection
PN Network port parameters	Power indicator	PWR Red LED indicator light
	Interface type	RJ45*2
	Communication protocol	Standard Profinet protocol (RT)
	Maximum communication cycle	4ms
	Communication bandwidth	10/100M Adaptive
Modbus TCP parameters	Interface type	RJ45
	Communication protocol	Modbus TCP
	Minimum communication cycle	10ms
	Communication bandwidth	100Mbps
Modbus RTU parameters	Interface type	RS422 or RS485 (3.81mm 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) Parallelism: None/Odd/Even (default None)
working environment	Working temperature and	-40 ~ +85℃, 5% ~ 95%RH (No condensation)

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

other	humidity	
	Storage temperature and humidity	-40 ~ +105℃, 5% ~ 95%RH (No condensation)
	Product size	55mm*30mm*80mm (Length*Width*Height), excluding terminals, subject to the actual product.
	Product weight	1 30 ±5 g
	Installation method	Standard industrial-grade 35mm guide rail mounting

2.3 Dimensional drawing

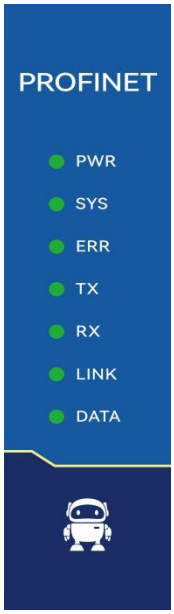


92*30*63 (Length * Width * Height)

Copyright © 2012–2026 , 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	illustrate
PWR	Power indicator light	Red LED light; On: System power supply is normal; Off: System power supply is abnormal.
SYS	System (Profinet connection) indicator lights	Blue LED light; On: Profinet establishes connection; Off: Profinet does not establish connection; When the software controls the flashing indicator light, it flashes simultaneously with ERR.
ERR	(Modbus) Communication Error Indicator	Red LED light; On: Remains on for 3 seconds in case of an error, returns to normal after no error is reported; Off: Moodbus communication is normal; When the indicator light is flashed by software control, it flashes simultaneously with the SYS indicator light.
TX	Serial port data transmission indicator light	Yellow LED light; illuminated: flashes rapidly when data is being transmitted via the serial port.
RX	Serial port data receiving indicator light	Yellow LED light; illuminated: flashes rapidly when data is being received from the serial port.
LINK	TCP link indicator	Yellow LED light; lit: Link connection established/Server connection successful.
DATA	TCP data indicator	Yellow LED light; On: Flashes rapidly when TCP data exchange occurs.

Indicator light description during firmware upgrade	
SYS	Enter upgrade mode and keep flashing at a frequency of 5Hz.
ERR	During the upgrade error, the 3Hz light kept flickering.
TX	During the upgrade process, 1Hz flickering occurred.
RX	During the upgrade process, 1Hz flickering occurred.
LINK	During the upgrade process, 1Hz flickering occurred.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

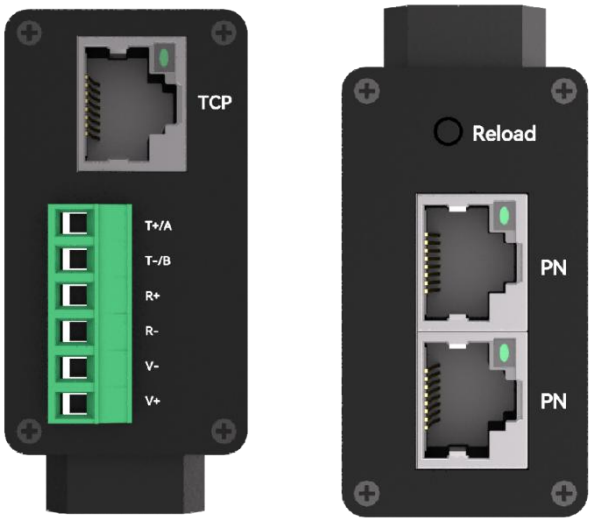
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

DATA	During the upgrade process, 1Hz flickering occurred.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

2.5 Port and button descriptions



Label	name	illustrate
TCP	Modbus TCP Communication network port	Standard RJ45 interface for Modbus TCP protocol data transmission.
T+/A	RS422 T+ interface / RS485 A interface	Serial port RS422 T+ interface/RS485 A interface, 3.81mm terminal block
T-/B	RS422 T-interface / RS485 B-interface	Serial port: RS422 T-interface/RS485 B-interface, 3.81mm terminal block.
R+	RS422 R+ interface	RS422 serial port R+ interface, 3.81mm terminal block
R-	RS422 R-interface	RS422 serial port with R-interface and 3.81mm connector.
V-	DC power supply negative terminal	DC (8-28V) power supply negative terminal, 3.81mm terminal
V+	DC power supply positive terminal	DC (8-28V) power supply positive terminal, 3.81mm terminal
PN	PN communication port	Standard RJ45 interface for Profinet protocol data transmission
PN	PN communication port	Standard RJ45 interface for Profinet protocol data transmission
Reload	button	Factory Reset: Press and hold for 5-10 seconds while powered on, then release; Device Reboot: Press and hold for less than 2 seconds while powered on, then release; Firmware Upgrade: Press and hold the button while powered off, then power on to enter upgrade mode;

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Chapter 3 Product Function Introduction

3.1 PN1-D25PT Series Function Overview

This Modbus module has two master slots, each supporting a maximum of 48 commands. Commands are divided into master commands and slave commands, and their type, length, and communication interface can be configured separately. When using the Modbus master function, the write function call interval cannot be less than twice the polling interval; otherwise, a frame of write function data may not be refreshed. For example, if the Modbus master has 5 command nodes and the polling interval is 10ms, then it will take 50ms to poll all command nodes. Therefore, the minimum data change period is 50ms * 2 = 100ms.

When Modbus TCP slave mode is enabled, the device can be accessed concurrently by up to 8 master devices. Due to the limitations of the main control chip's concurrent processing performance, it is recommended to reasonably control the polling frequency of each master station. Excessive polling rate can easily lead to untimely response, which in turn can cause data packet loss and abnormal communication errors in the master station.

3.2 Modify IP address

The IP address of this module can be modified using tools such as TIA Portal/STEP 7. For detailed configuration instructions, please refer to the usage section.

3.3 Upgrade function

Firmware upgrade is supported. For detailed instructions on firmware upgrade, please refer to the firmware upgrade user manual.

3.4 Reset and factory reset

operate	method	result
Short press Reload	Short press the button while powered on	Device restart
Long press Reload	Press and hold the button while powered on	Clear saved parameters and restore factory settings, then restart.
Enter upgrade mode	Power off, press and hold Reload, then power on.	Enter firmware upgrade process

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Chapter 4 Explanation of Equipment Alarm Information

When an error occurs in the PN1-D25PT gateway, Profinet's alarm mechanism will send specific error information to the PLC. Simultaneously, the gateway's ERR indicator light will illuminate, and the indicator light on the PLC will flash. When the error disappears, the corresponding alarm information will be removed, and the ERR indicator light will turn off. The specific error information can be viewed through the corresponding host computer on the PLC.

The specific error message is explained below:

error message	Description
Illegal Fun Code	The slave device responded with a Modbus standard error: The requested function is not recognized or supported by the slave device.
Illegal Data Address	The slave station responded with a Modbus standard error: Data address is not within the device's accessible range.
Illegal Data Value	The slave station responded with a Modbus standard error: The requested operation attempted to set an invalid or illegal value.
Slave Device Failure	The slave station responded with a Modbus standard error: Slave device failure, unknown device failure.
Frame Length Error	The message length received by the master station is incorrect; it is too long, too short, or does not match the correct length of the slave station's reply data.
CRC Check Error	The CRC checksum of the message received by the master station is incorrect.
Register Number Error	The number of message registers received by the master station is incorrect.
SLave Address Error	The master station received a message with an incorrect slave address.
Master Wating RSP Timeout	Main station received timeout
Function Code Different	The function code in the message received by the master station is inconsistent with the request.
Register Address Error	The master station received a message register address that is incorrect.
Unknown Error	unknown error
TCP CONNECT ERR	TCP connection error on slave.

Copyright © 2012–2026 , 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 TIA Portal

5.1 Preparation before connection

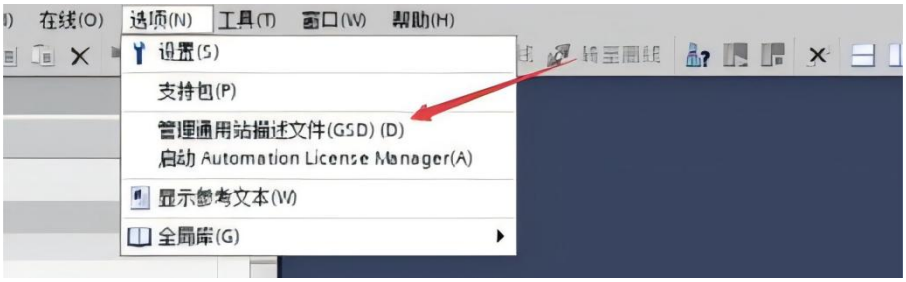
1. Prepare the necessary XML file as shown below.:



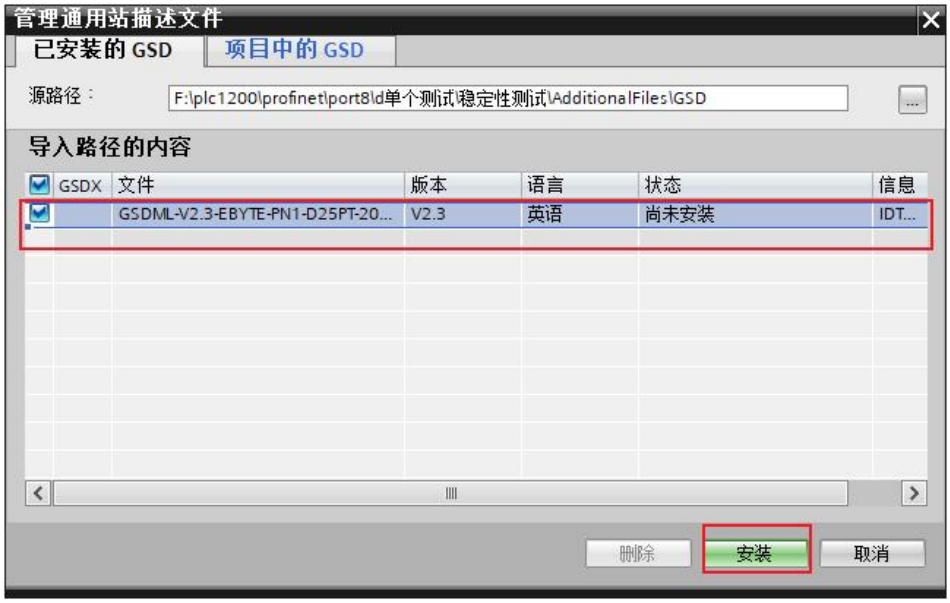
2. Connect the DC 24V external power supply to the module and power it on. Before powering on, please check whether the positive and negative terminals of the power supply are connected correctly.
3. Connect the module to the Profinet interface of the PLC controller using a network cable. (Within the same network segment)

5.2 Add GSDML file to TIBRA

1. Open TIA Portal, click Options, and then manage general site files. (gsd)



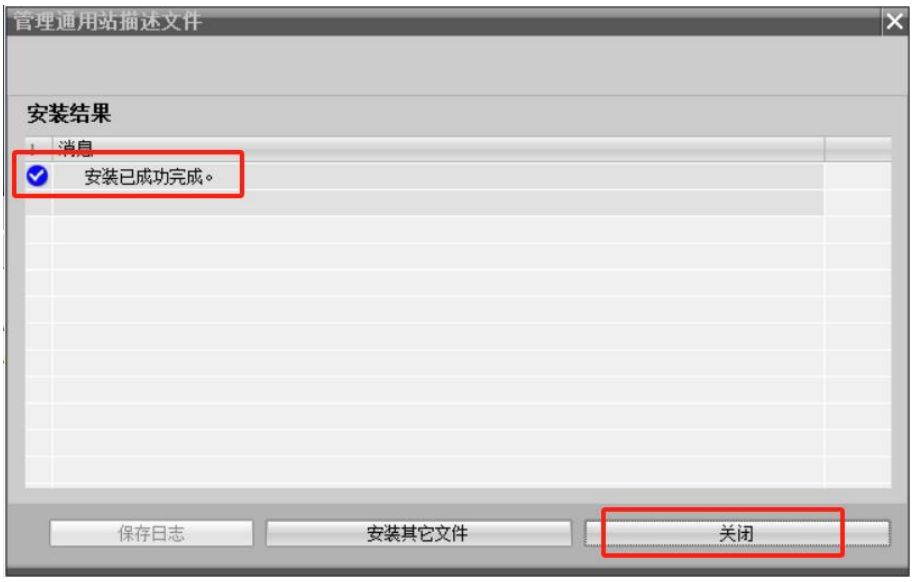
2. GSDMAdd the GSDML file. Locate the folder where the GSD is stored, select the folder, and the software will automatically scan for the GSD file. Then, select the GSD file and click Install.



Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

3. Once the installation is complete, simply click "Close," and then you can configure the device.

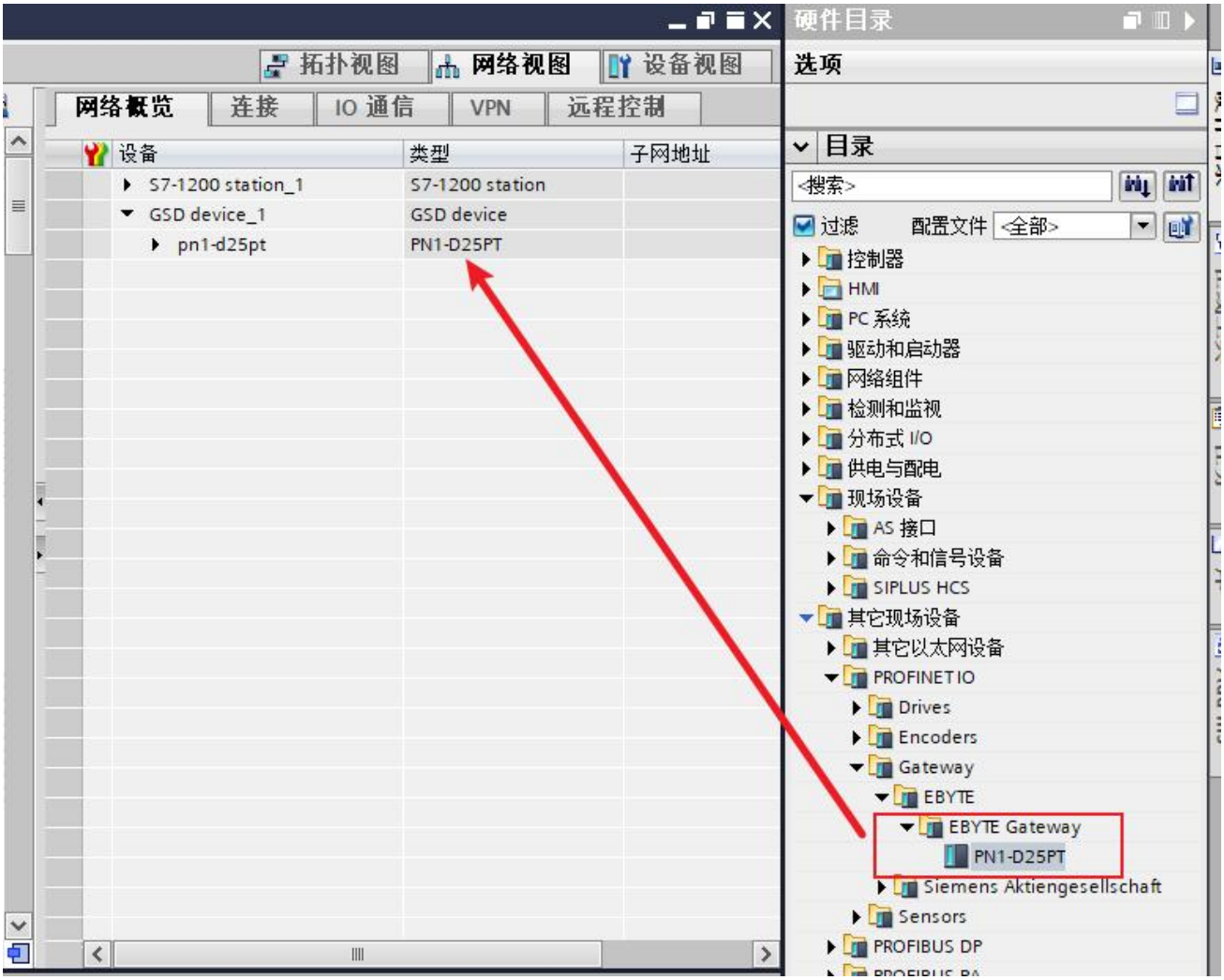


5.3 Add Profinet device to project

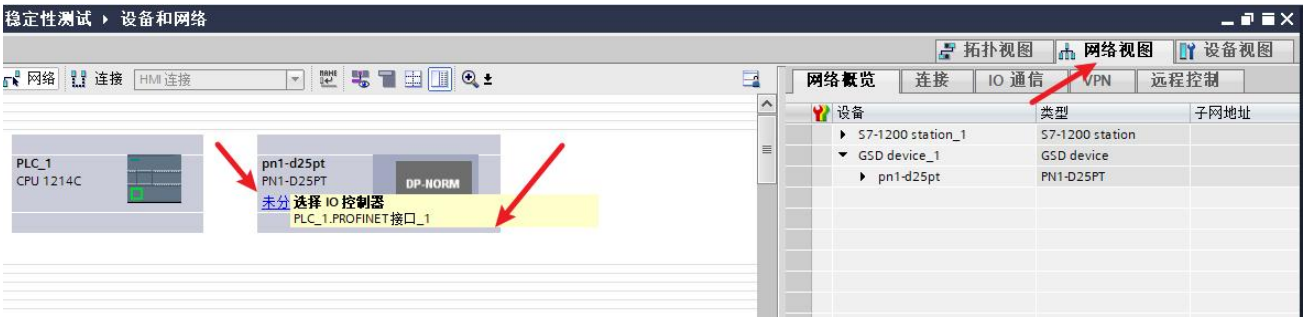
1. To create or open a new project, first add the controller device, then add the corresponding IO module in the device configuration interface. Double-click the module to add it successfully, as shown in the figure:

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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



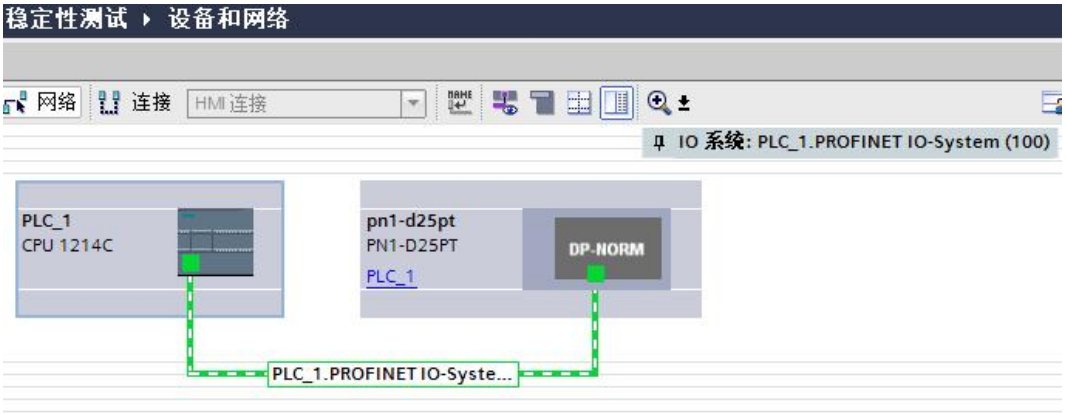
2. Configure devices in the network view.



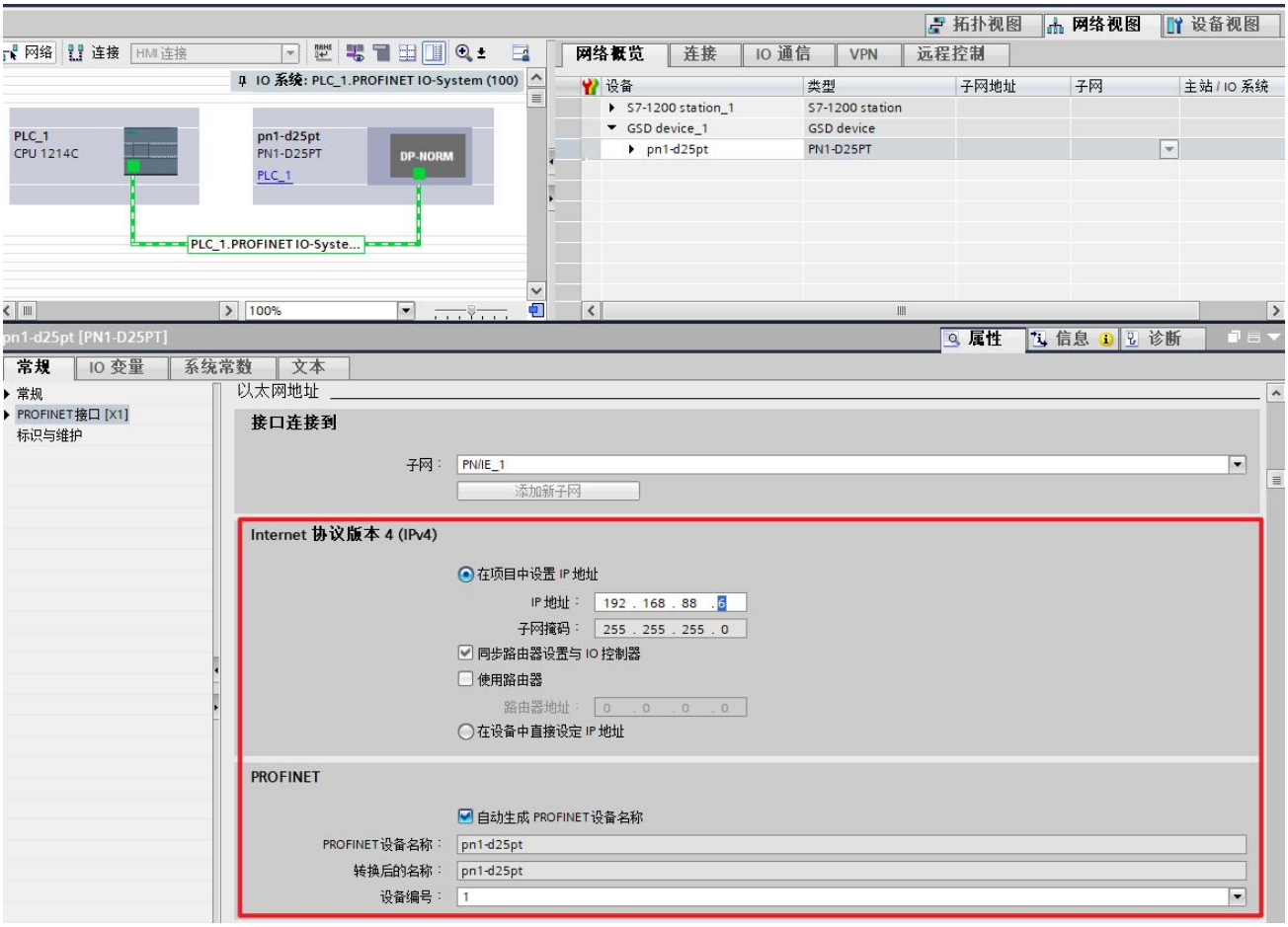
Once completed, it will look like this:

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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



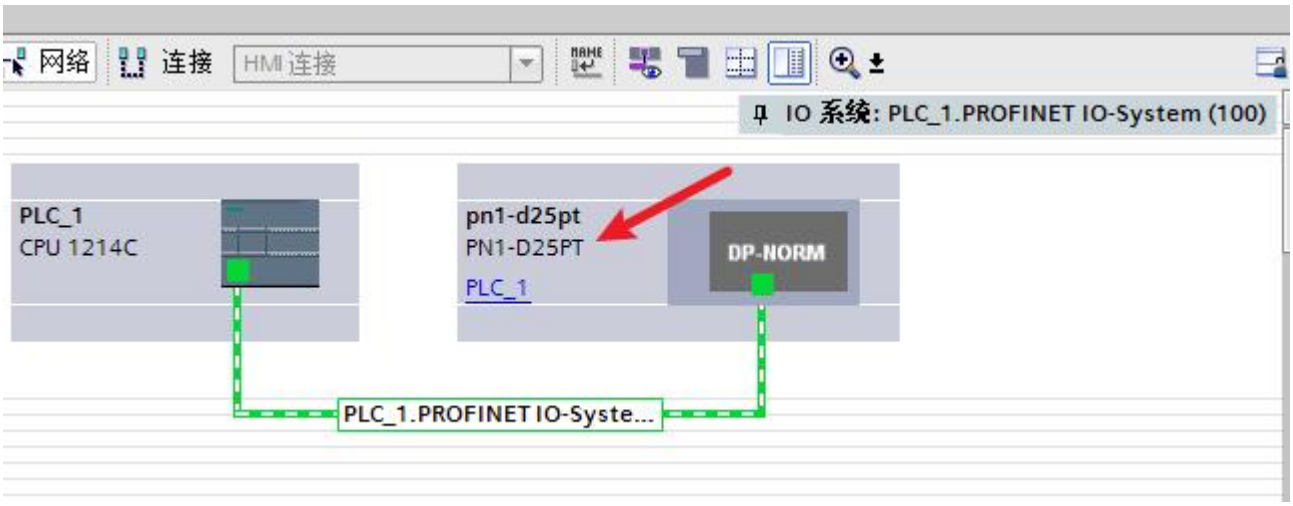
3. In the device view, first locate and select the newly added device, then double-click the module in the image. Next, in the general configuration interface, modify the IP address and device name, ensuring they match the module itself. Alternatively, you can choose to set the IP address directly on the device.



You can also click here to directly change the device name.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

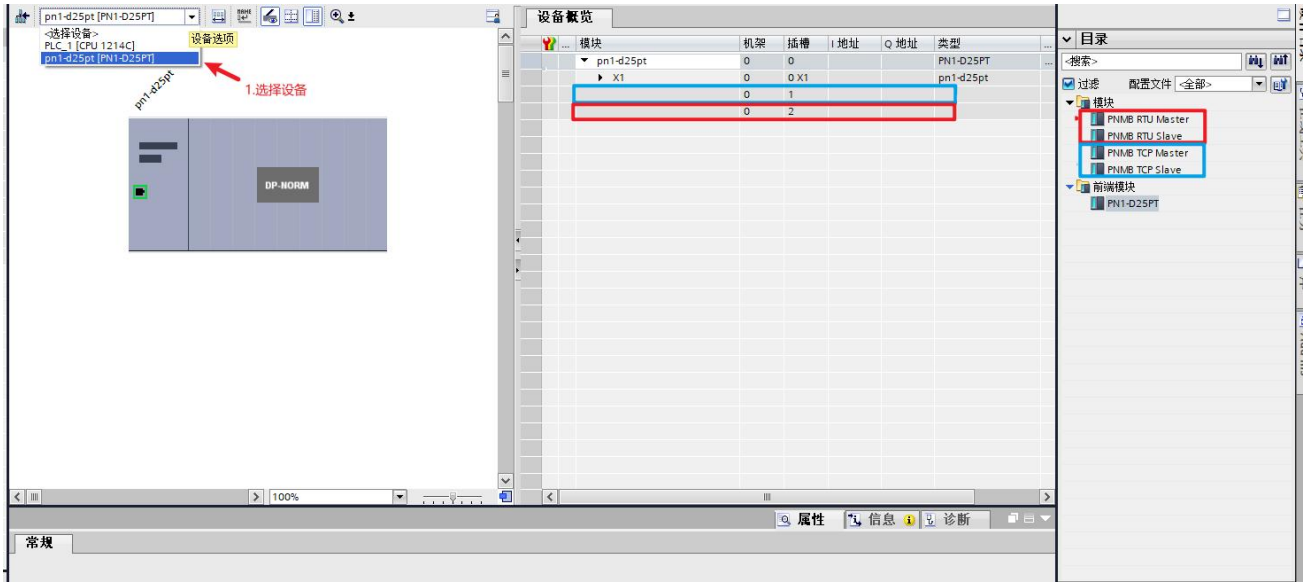


5.4 Configure Modbus communication parameters

The PN1-D25PT gateway supports both Modbus TCP master and slave modes, as well as Modbus RTU master and slave modes, depending on the Profinet configuration.

Select PN1-D25PT in the topology view interface and double-click to enter the device view operation interface.

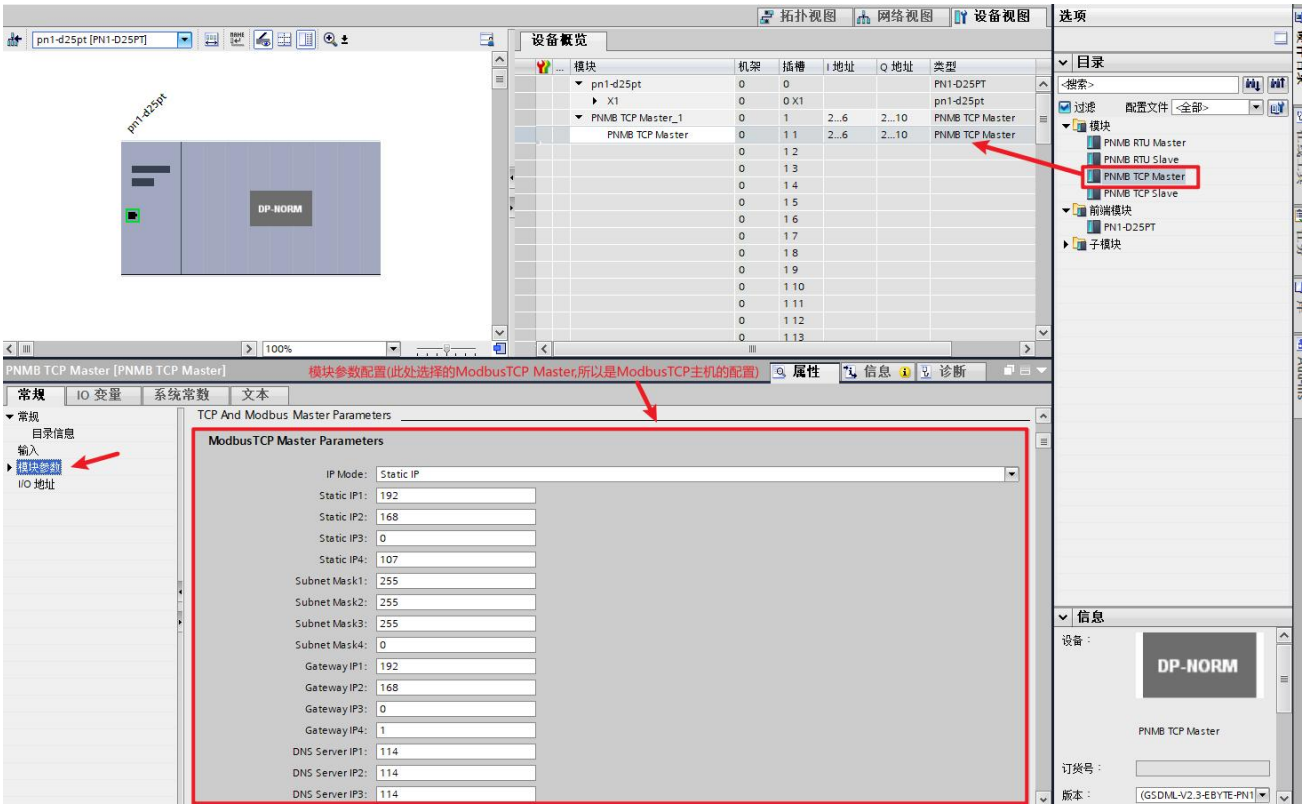
As shown in the figure below, in the device overview area, the system provides two slots for configuring a master slot shared by Modbus TCP master/slave (red in the figure) and a master slot for Modbus RTU master/slave (blue in the figure). Each master slot supports 48 sub-slots for configuring Modbus instruction submodules. Specifically, sub-slot number one corresponds to the device's status word and control word (applicable to PNMB Master/PNMB Slave configurations). The status word allows the PLC to obtain the operating status of the PN1-D25PT device; the control word allows the PLC to control the PN1-D25PT device.



As shown in the figure, add a Modbus TCP Master to the corresponding slot from the right. You can then configure the Modbus TCP Master parameters in "General" -> "Module Parameters" below

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

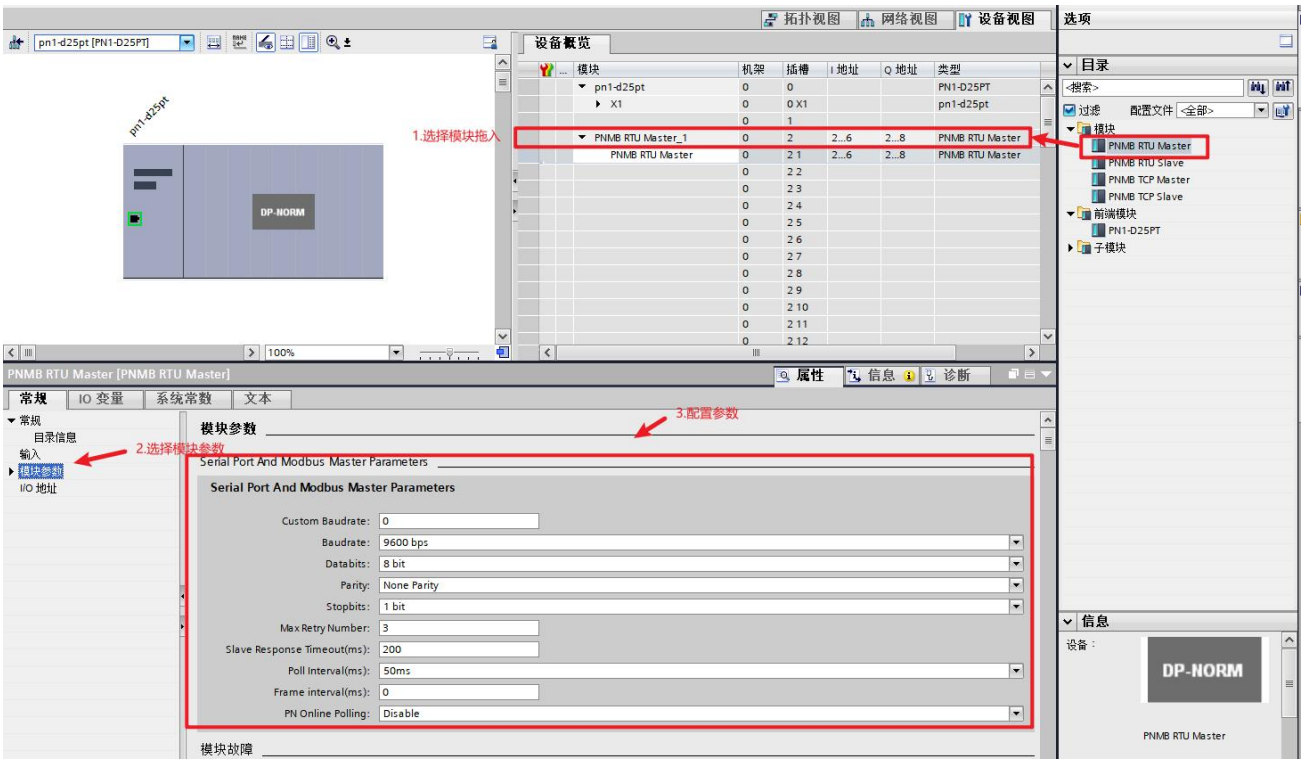


5.5 Modbus communication interface parameters for PN1-D25PT device module:

Modbus RTU Master

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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



Custom Baudrate:

When the serial port is configured as a slave and a custom baud rate is required, the default value is 0. This indicates that the custom baud rate is not enabled. To enable a custom baud rate, set a value between 1200 and 3.9 MHz. 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 or 8 bits, default: 8.

Parity:

Data validation: None Parity, Odd Parity, Even Parity, Default: None Parity.

Stopbit:

Data stop bits : 1 or 2 bits , default: 1 .

Max Retry Number :

The number of error retries when the serial port is used as the master station, 0-255, where 0 means no retransmission, 255 means unlimited retransmission, and 1-254 means retransmission according to the number of attempts . Default: 3 .

Slave Response Timeout (ms) :

the serial port is used as the master station, the module waits for a Modbus device response after sending a

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

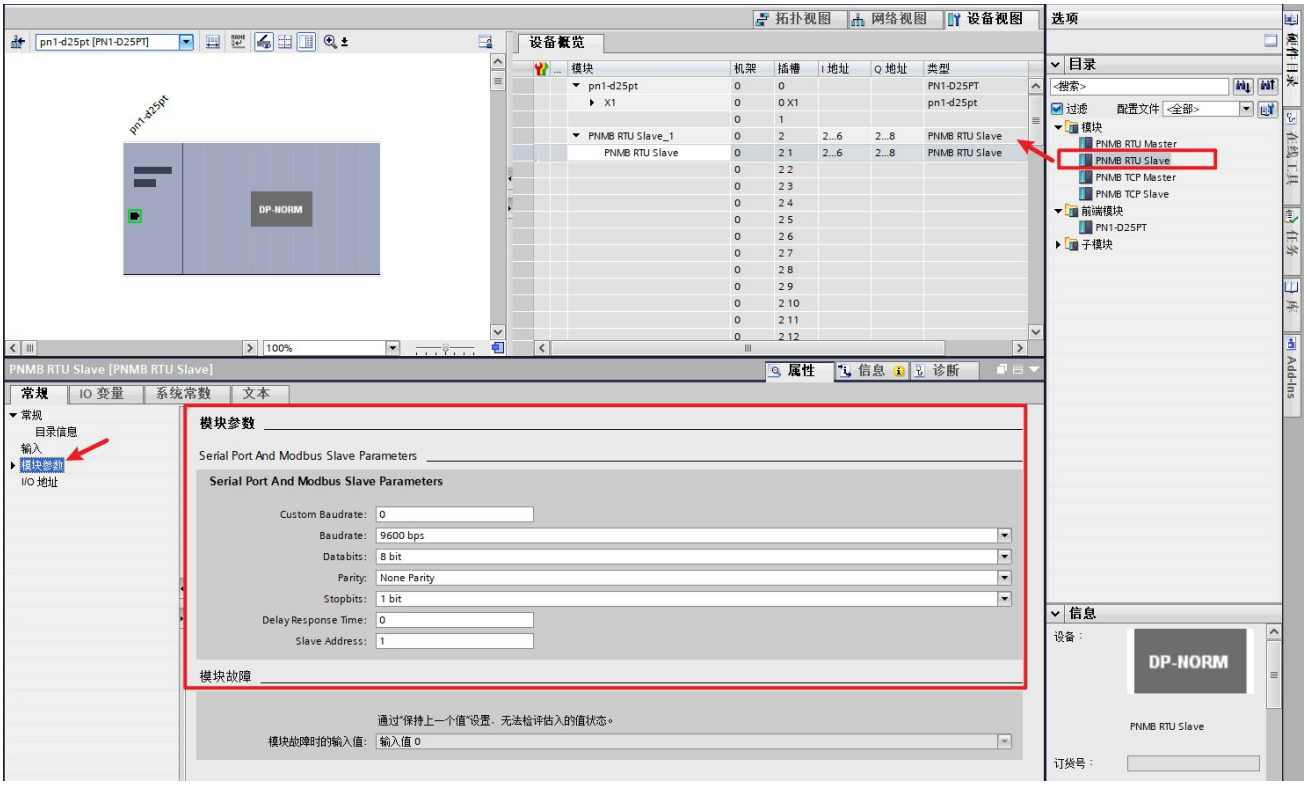
Modbus message . If the Modbus device does not respond within the set waiting time, the module stops waiting and continues to send the next Modbus message or resends it. The selection range is 0 - 65535 ms , with a default of 100ms .

Poll Interval(ms):
the serial port acts as the master station, the bus conversion module delays sending its own Modbus master message after receiving a correct response from the Modbus slave. If the Modbus slave device responds slowly to the master message, and the bus conversion module sends the Modbus message too quickly, a communication failure will occur. The message interval can be appropriately increased. The selection range is 10 , 20, 30 , 40, 50, 60, 70, 80, 90, 100 , 200 , 500, 1000ms, or no delay. The default value is 50ms .

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

PN Online Polling:
Profinet only polls online: Enable/Disable, default: Disable
When enabled, the module only communicates with the slave station when it is communicating normally with the PLC; it is disabled by default .

Modbus RTU Slave



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

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

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

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

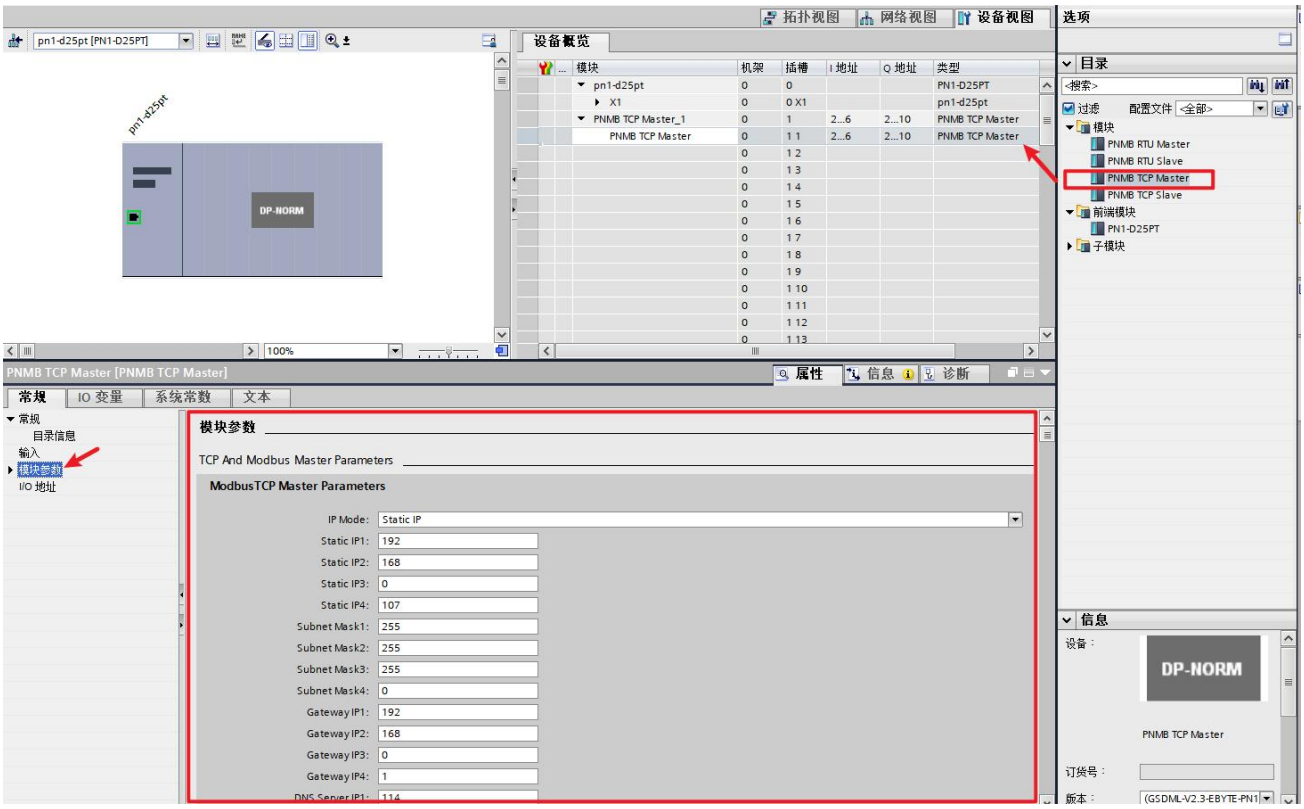
Parity:
Data validation: None Parity, Odd Parity, Even Parity, Default: None Parity.

Stopbit:
Data stop bits : 1 or 2 bits , default: 1 .

Delay Response Time.
the serial port is acting as a slave, how long should it delay before responding to a polling command received from the master? Range: 0 ~ 65535 , where 0 indicates an immediate response, in milliseconds (ms). Default: 0 .

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

Modbus TCP Master



Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

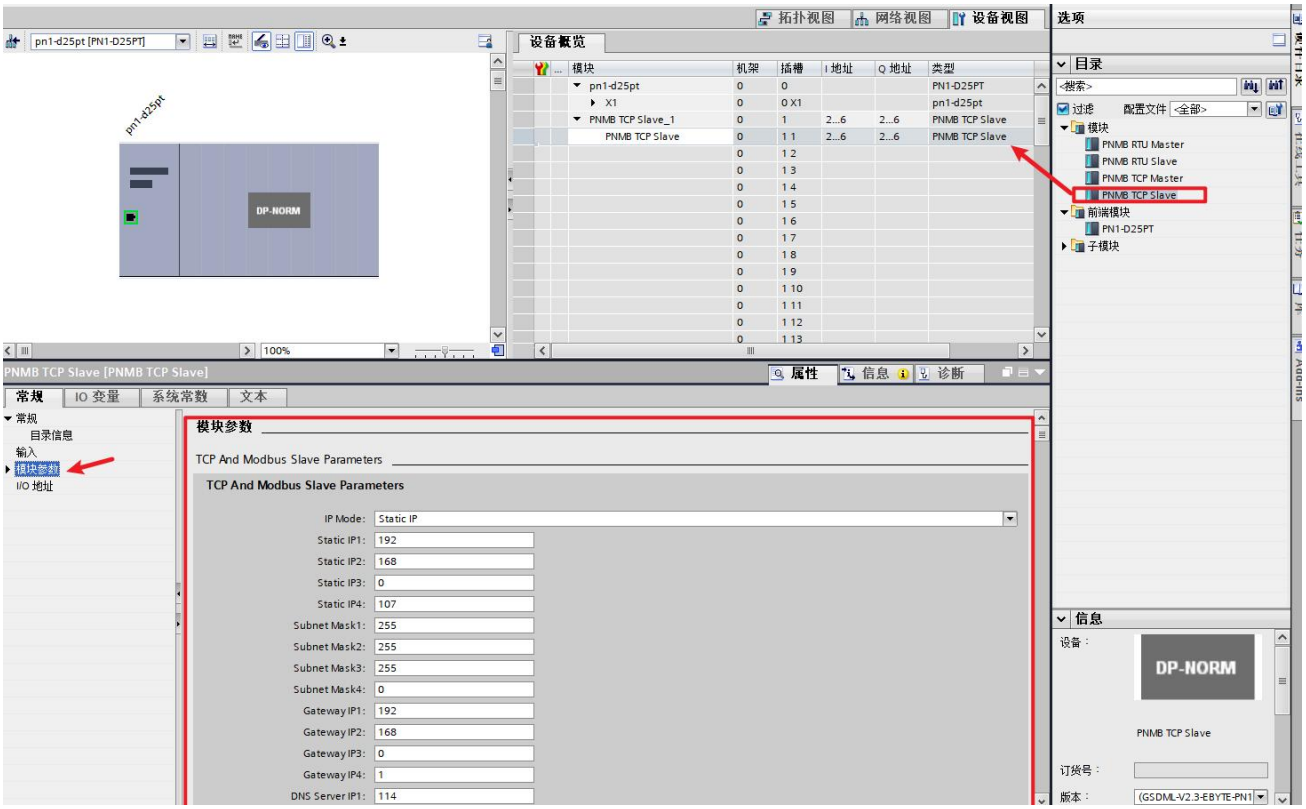
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

parameter	Default value/range	illustrate
Modbus TCP Master Parameters		
IP Mode	The default value is 0; 0 = Static IP, 1 = DHCP	Modbus TCP port IP acquisition method
Static IP (1...4)	192.168.0.107	Static IP address
Subnet Mask (1...4)	255.255.255.0	Subnet mask
Gateway IP (1...4)	192.168.0.1	Default gateway
DNS Server IP (1...4)	114.114.114.114	DNS server address
Connection Parameters		
Reconnection Time (s)	Default time: 3 seconds , range: 0-255 seconds	Reconnection waiting time after disconnection
Max Retry Number	Default value: 3 , range: 0-255	Maximum number of retries when a single command fails
Response Timeout (ms)	Default time: 200 ms , range: 0-65535	Timeout for waiting for Modbus TCP response
Poll interval (ms)	Default time: 50 ms , range: 0-1000	Minimum interval between polling commands
PN Online Polling	Default : Disable, Optional: Enable/Disable	When enabled, the module only communicates with the slave station when it is communicating normally with the PLC; it is disabled by default .
Modbus TCP Master Remote Parameters		
Socket1 ~ Socket8 Slave Address	Default value is 1, range is 0 - 247	Target Modbus slave address
Socket1 to Socket8 Port	Default is 502 , range: 0-65535	Target TCP port
Socket1 to Socket8 Octets	The default IP address is 192.168.0.1.	The target Modbus slave address must be on the same network segment as the Modbus TCP master.

Modbus TCP Slave

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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



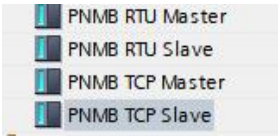
parameter	Default value/range	illustrate
IP Mode	The default value is 0; 0 = Static IP, 1 = DHCP	Modbus TCP port IP acquisition method
Static IP (1...4)	192.168.0.107	The local IP address of the gateway when acting as a TCP slave
Subnet Mask (1...4)	255.255.255.0	Subnet mask
Gateway IP (1...4)	192.168.0.1	Default gateway
DNS Server IP (1...4)	114.114.114.114	DNS server address
Modbus TCP Slave Address (0..255)	Default value is 1, range is 0 - 255	Modbus TCP Unit Identifier/Station Address
Modbus TCP Slave Response Delay Time(ms)	Default 0 ms range: 0-65535	Delayed response time after receiving the request
Modbus TCP Slave Port	Default is 502, range is 1 to 65535	Modbus TCP listening port

5.6 Configure Modbus status word and control word

In the equipment overview, you can see that there are a total of 2 slots. After dragging the module shown in the image below to the corresponding main slot, each main slot will generate 48 sub-slots.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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



Each master slot contains its own "status word" and "control word", for example:

	模块	机架	插槽	I 地址	Q 地址	类型
	pn1-d25pt	0	0			PN1-D25PT
	X1	0	0 X1			pn1-d25pt
	PNMB TCP Slave_1	0	1	2...6	2...6	PNMB TCP Slave
	PNMB TCP Slave	0	1 1	2...6	2...6	PNMB TCP Slave

As shown in the figure, the corresponding PROFINET input addresses IB2-IB6 (can be modified) are the communication status monitoring words. In the Q address field, the corresponding...

PROFINET output addresses QB2-QB6 (can be modified) are communication control words.

5.6.1 Modbus RTU status word and control word

The Modbus RTU communication status monitoring word is 5 bytes, and the meaning of each byte is as follows:

Byte 1: Error slot number

Byte 2: Error Code

Other bytes are reserved.

Error code	describe
1	The slave station responded with a Modbus standard error: ILLEGAL FUNCTION
2	The slave station responded with a Modbus standard error: ILLEGALDAT AADDRESS
3	The slave station responded with a Modbus standard error: ILLEGAL DATA VALUE
4	Slave device responds to Modbus standard error: SLAVE DEVICE FAILURE
10	The message received by the master station is of incorrect length, too long, too short, or does not match the correct length of the slave station's reply data.
11	The CRC checksum of the message received by the master station is incorrect.
12	The number of message registers received by the master station is incorrect.
13	The master station received a message with an incorrect slave address.
14	Main station received timeout
15	The function code in the message received by the master station is inconsistent with the request.
16	The master station received a message register address that is incorrect.
17	Unknown error

Modbus RTU communication control word: 7 bytes, the meaning of each byte is as follows:

Note: Serial port must be enabled before data communication can take place.

Byte 1: Bit 0: Whether Modbus serial port function is enabled. 1 enables, 0 disables. Bit 1: Clear fault codes. When a rising edge (0→1) is detected, the communication status monitoring is cleared. Other bits are reserved.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Byte 2: Slot number: 2-9 trigger bits.
Byte 3: Slot number: 10-17 trigger bits.
Byte 4: Slot number 18-25 trigger bits.
Byte 5: Slot number: 26-33 trigger bits.
Byte 6: Slot number: Trigger bits 34-41.
Byte 7: Slot number: 42-49 trigger bits.

1st byte							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
reserve	reserve	reserve	reserve	reserve	reserve	Clear alarm	Serial port enable
2nd byte							
Sub-slot 9	Sub-slot 8	Sub-slot 7	Sub-slot 6	Sub-slot 5	Sub-slot 4	Sub-slot 3	Sub-slot 2
3rd byte							
Sub-slot 17	Sub-slot 16	Sub-slot 15	Sub-slot 14	Sub-slot 13	Sub-slot 12	Sub-slot 11	Sub-slot 10
4th byte							
Sub-slot 25	Sub-slot 24	Sub-slot 23	Sub-slot 22	Sub-slot 21	Sub-slot 20	Sub-slot 19	Sub-slot 18
5th byte							
Sub-slot 33	Sub-slot 32	Sub-slot 31	Sub-slot 30	Sub-slot 29	Sub-slot 28	Sub-slot 27	Sub-slot 26
6th byte							
Sub-slot 41	Sub-slot 40	Sub-slot 39	Sub-slot 38	Sub-slot 37	Sub-slot 36	Sub-slot 35	Sub-slot 34
7th byte							
Sub-slot 49	Sub-slot 48	Sub-slot 47	Sub-slot 46	Sub-slot 45	Sub-slot 44	Sub-slot 43	Sub-slot 42

5.6.2 Modbus TCP status words and control words

Modbus TCP communication status monitoring word: 5 bytes, the meaning of each byte is as follows:
Byte 1: Error slot number
Byte 2: Error codes are shown in the image below:
Byte 3: Bit 0 is unused; bits 1-7 indicate the connection status of sockets 1-7 respectively. 1 indicates connection, 0 indicates no connection.
Byte 4: Bit 0: Indicates the Socket 8 connection status. Other bits are reserved. 1 indicates connection, 0 indicates no connection.
Byte 5: Reserved and unused

Error code	describe
1	The slave station responded with a Modbus standard error: ILLEGAL FUNCTION

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

2	The slave station responded with a Modbus standard error: ILLEGALDAT AADDRESS
3	The slave station responded with a Modbus standard error: ILLEGAL DATA VALUE
4	Slave device responds to Modbus standard error: SLAVE DEVICE FAILURE
10	The message received by the master station is of incorrect length, too long, too short, or does not match the correct length of the slave station's reply data.
11	The CRC checksum of the message received by the master station is incorrect.
12	The number of message registers received by the master station is incorrect.
13	The master station received a message with an incorrect slave address.
14	Main station received timeout
15	The function code in the message received by the master station is inconsistent with the request.
16	The master station received a message register address that is incorrect.
17	Unknown error
19	TCP connection error: TCP CONNECT ERR

Modbus TCP communication control word: 9 bytes, the meaning of each byte is as follows:

Note: Each socket must be enabled before data communication can take place.

Byte 1: Bit 0 clears the alarm. Triggered on rising edge. Bits 1-7 control socket enable for bits 0-7. 1 enables, 0 disables. When enabled, the client will connect to the corresponding Modbus TCP slave. When disabled, the connection will be closed. (The success of the socket connection can be observed through bytes 3 and 4 of the status word.)

Byte 2: Bit 0 indicates socket8 is enabled. 1 enables, 0 disables. Other bits are reserved and unused.

Byte 3: Reserved and unused

4th byte: Slot number: 2-9 trigger bits.

Byte 5: Slot number: 10-17 trigger bits.

Byte 6: Slot number: 18-25 trigger bits.

Byte 7: Slot number: 26-33 trigger bits.

8th byte: Slot number: Trigger bits 34-41.

9th byte: Slot number: 42-49 trigger bits.

1st byte							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
S7_EN	S6_EN	S5_EN	S4_EN	S3_EN	S2_EN	S1_EN	Clear alarm
2nd byte							
null	null	null	null	null	null	null	S8_EN
3rd byte							
null	null	null	null	null	null	null	null
4th byte							
Sub-slot 9	Sub-slot 8	Sub-slot 7	Sub-slot 6	Sub-slot 5	Sub-slot 4	Sub-slot 3	Sub-slot 2
5th byte							
Sub-slot 17	Sub-slot 16	Sub-slot 15	Sub-slot 14	Sub-slot 13	Sub-slot 12	Sub-slot 11	Sub-slot 10
6th byte							

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Sub-slot 25	Sub-slot 24	Sub-slot 23	Sub-slot 22	Sub-slot 21	Sub-slot 20	Sub-slot 19	Sub-slot 18
7th byte							
Sub-slot 33	Sub-slot 32	Sub-slot 31	Sub-slot 30	Sub-slot 29	Sub-slot 28	Sub-slot 27	Sub-slot 26
8th byte							
Sub-slot 41	Sub-slot 40	Sub-slot 39	Sub-slot 38	Sub-slot 37	Sub-slot 36	Sub-slot 35	Sub-slot 34
9th byte							
Sub-slot 49	Sub-slot 48	Sub-slot 47	Sub-slot 46	Sub-slot 45	Sub-slot 44	Sub-slot 43	Sub-slot 42

5.7 Submodule parameter description

Modbus RTU Master Submodule Parameters

Each Modbus RTU master command has five attributes:

Slave Address (1 ~ 247): Represents the address of the Modbus RTU slave device, with a selectable range of 1-247.

Function Code: The function code of the Modbus RTU master station is automatically generated based on the Modbus command inserted into the slot and cannot be changed.

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

XX Quantity : Indicates the number of coils or registers to be read or written. It is automatically generated based on the Modbus command inserted into the slot and the quantity can be changed within a specified range .

Transmission Type: The following four transmission types are provided.

Disable: indicates that the command will not be executed.

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

Leve `ltrigger` (level transmission): After the control transmission flag corresponding to the slot number changes from 0 to 1: For read commands, this message will be sent. For write commands, it will only be sent if the data has changed; after the control transmission flag corresponding to the slot number changes from 1 to 0, both read and write messages will stop being sent. (Taking the previous section as an example, PLC addresses QB2-QB5 are the transmission trigger control bits.)

Rising Trigger (sent on rising edge): This message will be sent once after the trigger control bit corresponding to the slot number changes from 0 to 1. (In the previous section, PLC addresses QB2-QB5 were the trigger control bits for sending the message.)

Modbus RTU slave module parameters

Each Modbus RTU slave command is prefixed with either Input or Output. Input indicates data input to the PLC, meaning the master station writes data to the slave station, and the slave station then returns the data to the PLC; this corresponds to a write command. Output indicates data output from the PLC, meaning

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

the PLC sends data to the slave station, and the master station then reads the data from the slave station; this corresponds to a read command. More specifically, each slave command ends with a list of supported function codes.

function code	Function	Operating address area (non-register PLC address)	Operation type
01H	Read the output status of multiple coils	0XXXX	read
02H	Read the status of multiple input coils	1xxXX	read
03H	Reading multiple saved registers	4xxXX	read
04H	Read input register	3XXXX	read
05H	Force a single coil	0XXXX	Write
06H	Preset a single holding register	4XXXX	Write
OFH	Forced multi-coil	0xXXX	Write
10H	Multiple pre-set holding registers	4XXXX	Write

Modbus TCP Master Submodule Parameters

Each Modbus TCP master command has five attributes.

Among them, Function Code; Start Address:; XX Quantity; Transmission TypeSame as Modbus RTU master station configuration function.

Socket Config selection (1-8): Select which socket this instruction should use.

Modbus TCP slave submodule parameters

The parameters are similar to those of the Modbus RTU slave submodule.

5.7.1 Serial Port Enable Routine

The following figure shows the Modbus RTU slot information. As can be seen from the figure, I2-I6 are status words, and B2-B8 are control words.

▼ PNMB RTU Master_1	0	2	2...6	2...8	PNMB RTU Master
PNMB RTU Master	0	2 1	2...6	2...8	PNMB RTU Master
	0	2 2			

To enable the serial port, refer to the control word description as shown in the figure:

第 1 字节							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
保留	保留	保留	保留	保留	保留	清除报警	串口使能

B2 is the first byte. Setting Bit0 of B2 to 1 will enable the serial port.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Program example: The following is a code segment for enabling the serial port:



5.7.2 Network Socket Enabler Routine

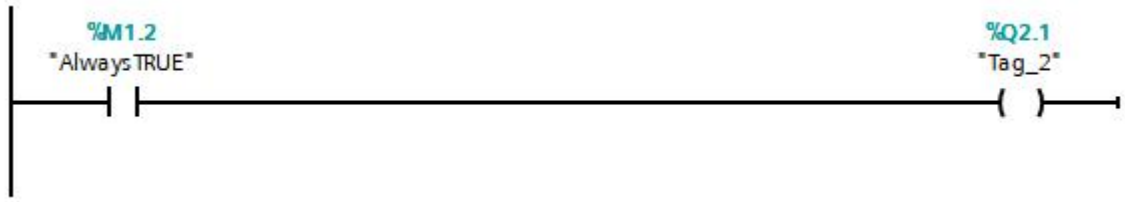
The following figure shows the Modbus TCP slot information. As can be seen from the figure, I2-I6 are status words, and B2-B10 are control words.

PNMB TCP Master_1	0	1	2...6	2...10	PNMB TCP Master
PNMB TCP Master	0	1 1	2...6	2...10	PNMB TCP Master

To enable socket1-socket8, refer to the control word description shown in the figure:

第 1 字节							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
S7_EN	S6_EN	S5_EN	S4_EN	S3_EN	S2_EN	S1_EN	清除报警
第 2 字节							
空	空	空	空	空	空	空	S8_EN

B2 represents the first byte, B3 the second byte, and so on. Setting all bits in B2 to 1 and the first byte of B3 to 1 enables sockets 1-8. Program example: The following is a code segment that enables socket1 alone:

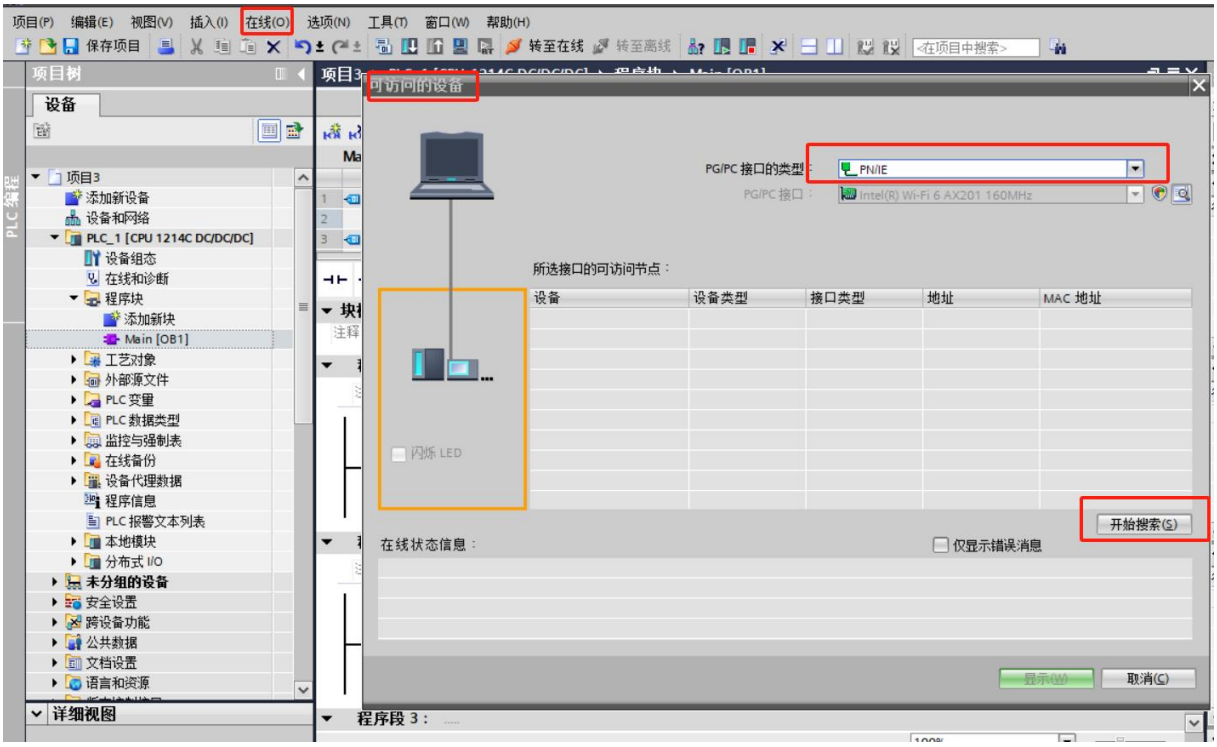


5.8 Using TIA Portal to modify module names and query IP addresses

Open the TIA Portal software and click the "Online" option in the menu bar.
In the opened online access interface, locate and select "Accessible Devices".
Perform a device search. Once the search is complete, all accessible devices will be listed.
Select the target device from the list whose IP address and name you want to modify.
Perform IP address and name modification operations on the selected device.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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



Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Chapter 6 Tutorial on Loading Devices Using STEP 7

6.1 Preparations before connection

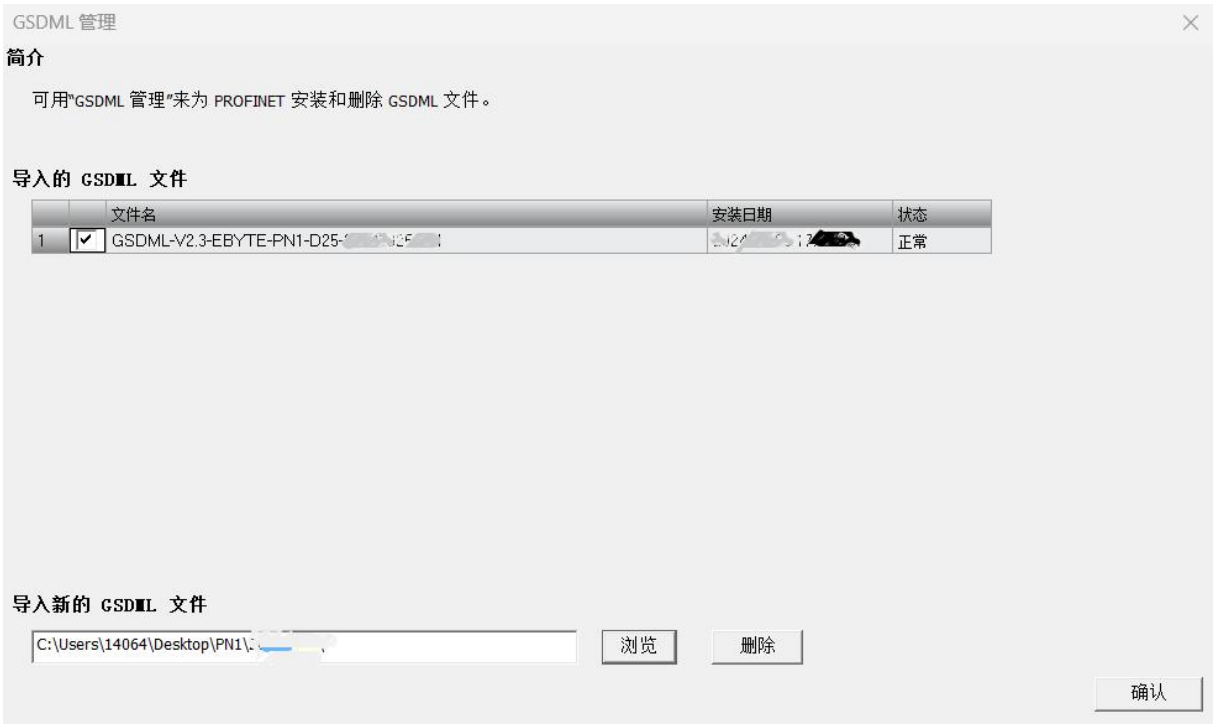
1. Prepare the necessary XML file as follows:
2. In GSDML-V2.3-EBYTE-PN1-D25PT-20260414.xml, connect the DC 24V external power supply to the module and power it on. Before powering on, please check that the positive and negative terminals of the power supply are connected correctly.
3. Connect the module to the Profinet interface of the PLC controller using a network cable. (They should be on the same network segment.)

6.2 STEP 7 Add GSDML file

1. Under the File menu, access GSDML Management.



2. Add GSDML file



Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

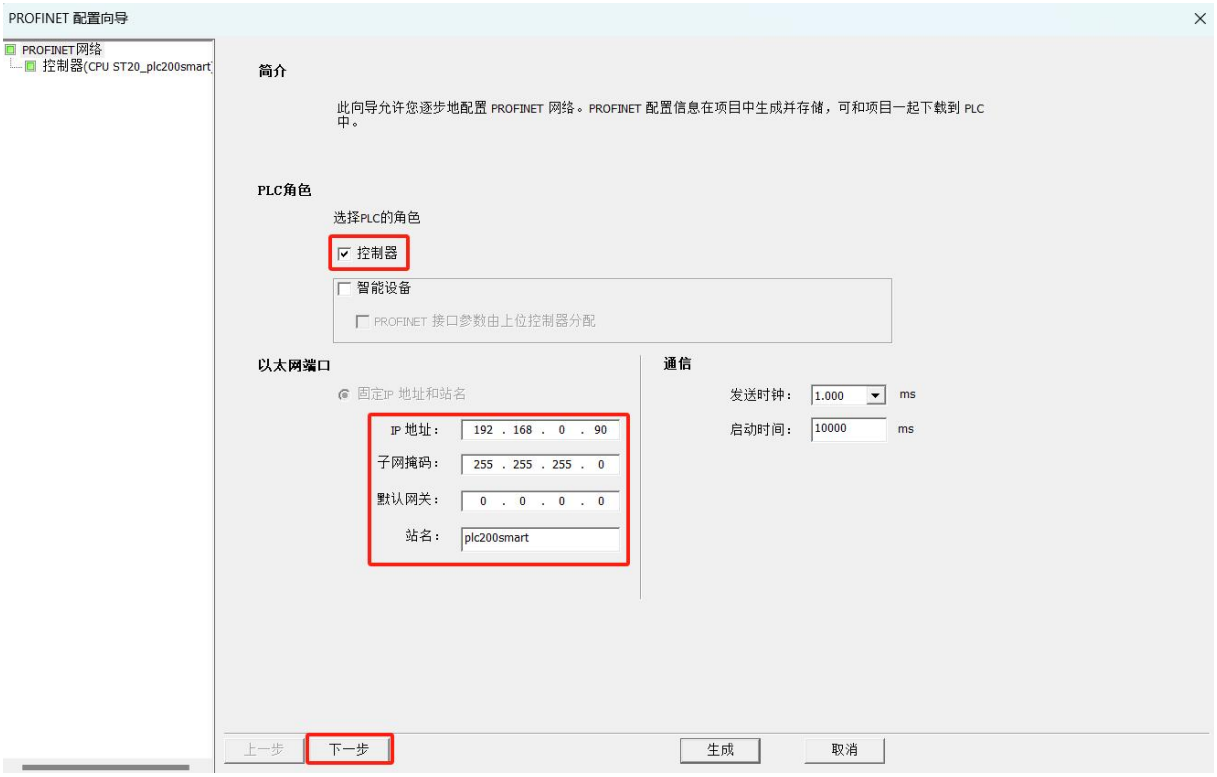
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.3 Adding Profinet devices to the project

1. Select the PROFINET command under the Tools menu.



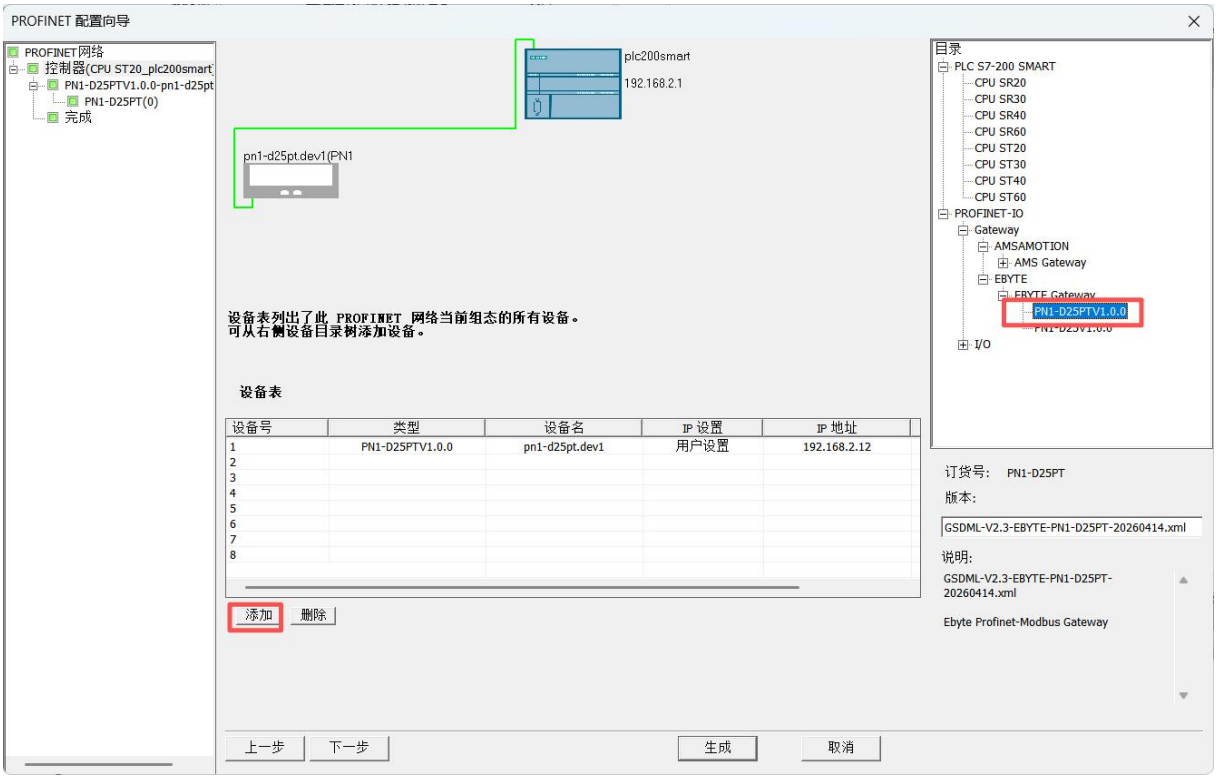
2. Select the PLC role as PLC controller, and set the corresponding PLC controller IP and other relevant parameters. Click Next when finished.



In the right sidebar , select PROFINET-IO→Gateway→EBYTE→TION→EBYTE Gateway→PN1-D25PTV1.0.0, then hold down the left mouse button and drag it into the table on the left.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

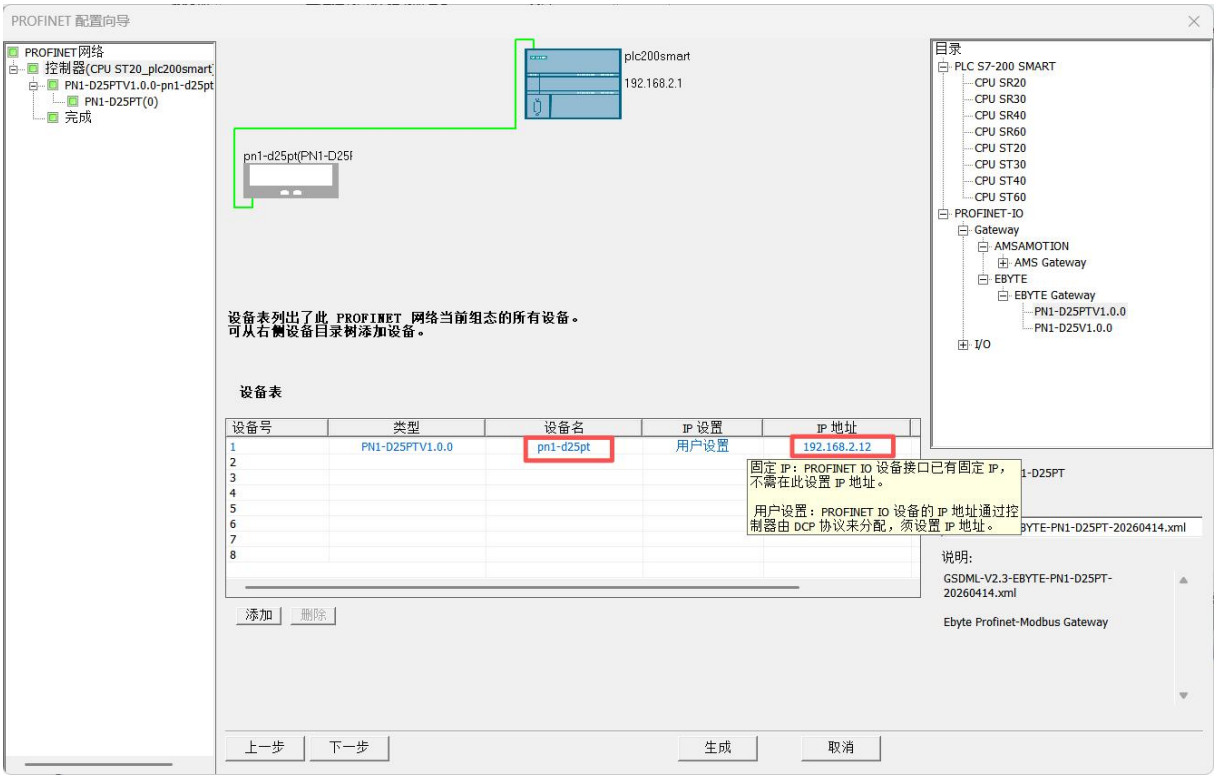


Double-click the device name field, enter the corresponding device name. There cannot be the same device name in the same project. Similarly, set the IP address, keeping it in the same network segment as the PLC controller. Finally, click Generate .

Note: The device name set at this point must match the actual device. If you are unsure of the device name, you can set it arbitrarily first, and then change the module's device name to match it later. The IP address set at this point will be used to set the IP address of modules with the same device name to the value set here during configuration. For instructions on modifying the device name, please refer to the "STEP 7 Modifying Module Name and Querying Module IP Address" section .

Copyright © 2012–2026 , 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 serial port and network port function modules. Each slot can accommodate 48 sub-slots for configuring Modbus instruction sub-modules. The PLC can obtain the operating status of the PN1-D25PT device; and through control words, the PLC can control the PN1-D25PT device.

Modbus serial communication interface parameters for PN1-D25PT device module:

PNMB RTU Master

Custom Baudrate:
When the serial port is configured as a slave and a custom baud rate is required, the default value is 0. This indicates that the custom baud rate is not enabled. To enable a 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 or 8 bits, default: 8 bits.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Parity:
Data validation: None Parity, Odd Parity, Even Parity, Default: None Parity.

Stopbit:
Data stop bits : 1 or 2 bits , default: 1 .

Max Retry Number :
The number of error retries when the serial port is used as the master station, 0-255, where 0 means no retransmission, 255 means unlimited retransmission, and 1-254 means retransmission according to the number of attempts . Default: 3 .

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

Poll Interval(ms):
the serial port acts as the master station, the bus conversion module delays sending its own Modbus master message after receiving a correct response from the Modbus slave. If the Modbus slave device responds slowly to the master message, and the bus conversion module sends the Modbus message too quickly, a communication failure will occur. The message interval can be appropriately increased. The selection range is 10 , 20, 30 , 40, 50, 60, 70, 80, 90, 100 , 200 , 500, 1000ms, or no delay. The default value is 50ms .

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

PNMB RTU Slave

Custom Baudrate:
When the serial port is configured as a slave and a custom baud rate is required, the default value is 0. This indicates that the custom baud rate is not enabled. To enable a 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 or 8 bits, default: 8 bits.

Parity:
Data validation: None Parity, Odd Parity, Even Parity, Default: None Parity.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

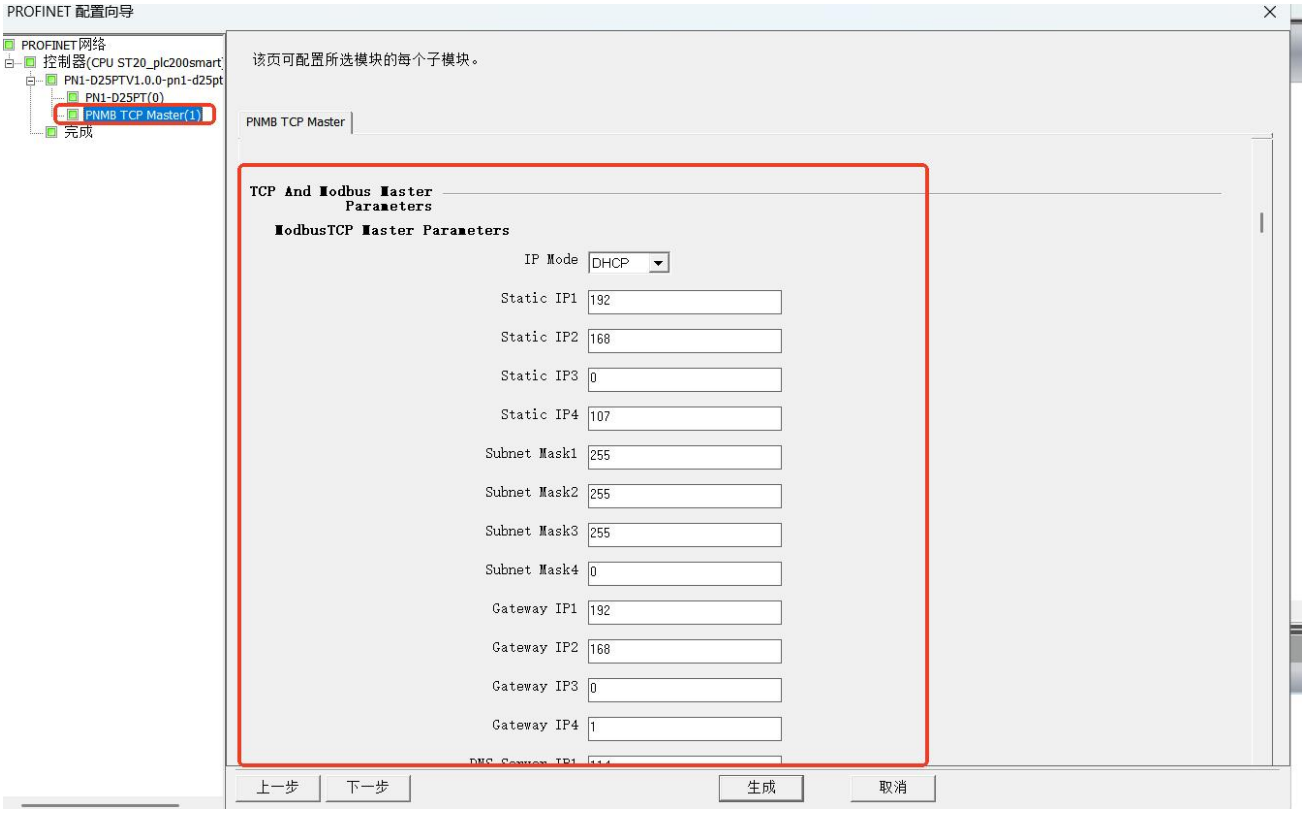
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Stopbit:
Data stop bits : 1 or 2 bits , default: 1 .

Delay Response Time.
the serial port is acting as a slave, how long should it delay before responding to a polling command received from the master? Range: 0 ~ 65535 , where 0 indicates an immediate response, in milliseconds (ms). Default: 0 .

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

Modbus TCP Master



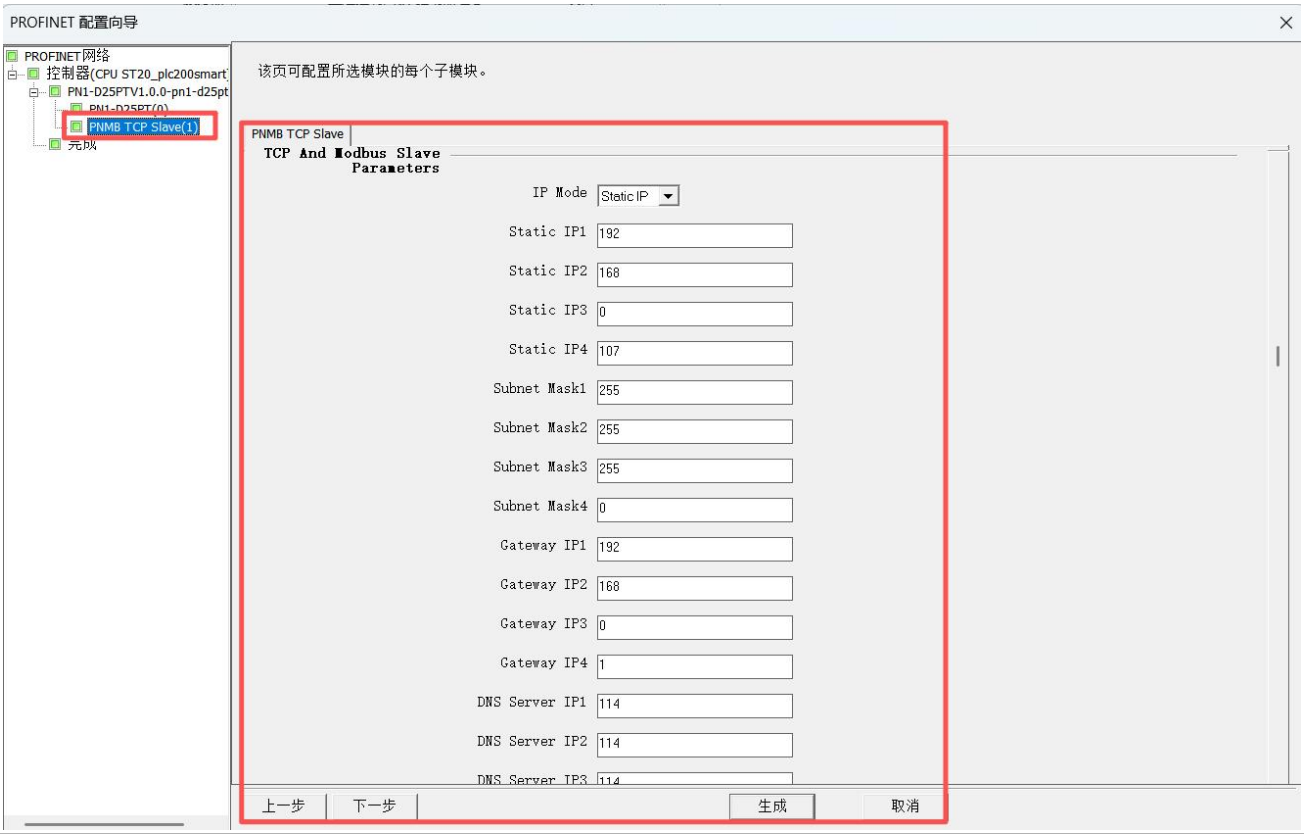
parameter	Default value/range	illustrate
Modbus TCP Master Parameters		
IP Mode	The default value is 0; 0 = Static IP, 1 = DHCP	Modbus TCP port IP acquisition method
Static IP (1...4)	192.168.0.107	Static IP address
Subnet Mask (1...4)	255.255.255.0	Subnet mask
Gateway IP (1...4)	192.168.0.1	Default gateway
DNS Server IP (1...4)	114.114.114.114	DNS server address
Connection Parameters		
Reconnection Time (s)	Default time: 3 seconds , range:	Reconnection waiting time after

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

	0-255 seconds	disconnection
Max Retry Number	Default value: 3 , range: 0-255	Maximum number of retries when a single command fails
Response Timeout (ms)	Default time: 200 ms , range: 0-65535	Timeout for waiting for Modbus TCP response
Poll interval (ms)	Default time: 50 ms , range: 0-1000	Minimum interval between polling commands
PN Online Polling	Default: Disable, Optional: Enable/Disable	When enabled, the module only communicates with the slave station when it is communicating normally with the PLC; it is disabled by default .
Modbus TCP Master Remote Parameters		
Socket1 ~ Socket8 Slave Address	Default value is 1, range is 0 - 247	Target Modbus slave address
Socket1 to Socket8 Port	Default is 502 , range: 0-65535	Target TCP port
Socket1 to Socket8 Octets	The default IP address is 192.168.0.1.	The target Modbus slave address must be on the same network segment as the Modbus TCP master.

Modbus TCP Slave



parameter	Default value/range	illustrate
IP Mode	The default value is 0; 0	Modbus TCP port IP acquisition method

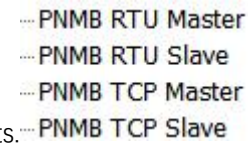
Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

	= Static IP, 1 = DHCP	
Static IP (1...4)	192.168.0.107	The local IP address of the gateway when acting as a TCP slave
Subnet Mask (1...4)	255.255.255.0	Subnet mask
Gateway IP (1...4)	192.168.0.1	Default gateway
DNS Server IP (1...4)	114.114.114.114	DNS server address
Modbus TCP Slave Address (0..255)	Default value is 1, range is 0 - 255	Modbus TCP Unit Identifier/Station Address
Modbus TCP Slave Response Delay Time(ms)	Default 0 ms range: 0-65535	Delayed response time after receiving the request
Modbus TCP Slave Port	Default is 502, range is 1 to 65535	Modbus TCP listening port

6.5 Configure Modbus status word and control word

In the equipment overview, you can see that there are 2 slots in total. After dragging the image below to



the corresponding main slot, each main slot has 48 sub-slots.

Each master slot contains its own "status word" and "control word", for example:



		序号	模块名	子模块名	插槽_子插槽	PNI 起始地...	输入长度 (
1		0	PN1-D25PT		0		
2		–		X1	0 32768		
3		–		X1 P1	0 32769		
4		1	PNMB TCP Slave		1	128	5
5		–			1 2		

The corresponding PROFINET input addresses IB128-IB132 (can be modified) shown in the figure are for communication status monitoring. The corresponding Q address field...

The PROFINET output addresses QB128-QB132 (can be modified) are communication control words.

The Modbus RTU communication status monitoring word is 5 bytes, and the meaning of each byte is as follows:

Byte 1: Error slot number

Byte 2: Error Code

Other bytes are reserved.

Error code	describe
1	The slave station responded with a Modbus standard error: ILLEGAL FUNCTION
2	The slave station responded with a Modbus standard error: ILLEGALDAT AADDRESS
3	The slave station responded with a Modbus standard error: ILLEGAL DATA VALUE
4	Slave device responds to Modbus standard error: SLAVE DEVICE FAILURE

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

10	The message received by the master station is of incorrect length, too long, too short, or does not match the correct length of the slave station's reply data.
11	The CRC checksum of the message received by the master station is incorrect.
12	The number of message registers received by the master station is incorrect.
13	The master station received a message with an incorrect slave address.
14	Main station received timeout
15	The function code in the message received by the master station is inconsistent with the request.
16	The master station received a message register address that is incorrect.
17	Unknown error

Modbus RTU communication control word: 7 bytes, the meaning of each byte is as follows:

Note: Serial port must be enabled before data communication can take place.

Byte 1: Bit 0: Whether Modbus serial port function is enabled. 1 enables, 0 disables. Bit 1: Clear fault codes. When a rising edge (0→1) is detected, the communication status monitoring is cleared. Other bits are reserved.

Byte 2: Slot number: 2-9 trigger bits.

Byte 3: Slot number: 10-17 trigger bits.

Byte 4: Slot number 18-25 trigger bits.

Byte 5: Slot number: 26-33 trigger bits.

Byte 6: Slot number: Trigger bits 34-41.

Byte 7: Slot number: 42-49 trigger bits.

1st byte							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
reserve	reserve	reserve	reserve	reserve	reserve	Clear alarm	Serial port enable
2nd byte							
Sub-slot 9	Sub-slot 8	Sub-slot 7	Sub-slot 6	Sub-slot 5	Sub-slot 4	Sub-slot 3	Sub-slot 2
3rd byte							
Sub-slot 17	Sub-slot 16	Sub-slot 15	Sub-slot 14	Sub-slot 13	Sub-slot 12	Sub-slot 11	Sub-slot 10
4th byte							
Sub-slot 25	Sub-slot 24	Sub-slot 23	Sub-slot 22	Sub-slot 21	Sub-slot 20	Sub-slot 19	Sub-slot 18
5th byte							
Sub-slot 33	Sub-slot 32	Sub-slot 31	Sub-slot 30	Sub-slot 29	Sub-slot 28	Sub-slot 27	Sub-slot 26
6th byte							
Sub-slot 41	Sub-slot 40	Sub-slot 39	Sub-slot 38	Sub-slot 37	Sub-slot 36	Sub-slot 35	Sub-slot 34
7th byte							
Sub-slot 49	Sub-slot 48	Sub-slot 47	Sub-slot 46	Sub-slot 45	Sub-slot 44	Sub-slot 43	Sub-slot 42

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Modbus TCP communication status monitoring word: 5 bytes, the meaning of each byte is as follows:

Byte 1: Error slot number

Byte 2: Error codes are shown in the image below:

Byte 3: Bit 0 is unused; bits 1-7 indicate the connection status of sockets 1-7 respectively. 1 indicates connection, 0 indicates no connection.

Byte 4: Bit 0: Indicates the Socket 8 connection status. Other bits are reserved. 1 indicates connection, 0 indicates no connection.

Byte 5: Reserved and unused

Error code	describe
1	The slave station responded with a Modbus standard error: ILLEGAL FUNCTION
2	The slave station responded with a Modbus standard error: ILLEGALDAT AADDRESS
3	The slave station responded with a Modbus standard error: ILLEGAL DATA VALUE
4	Slave device responds to Modbus standard error: SLAVE DEVICE FAILURE
10	The message received by the master station is of incorrect length, too long, too short, or does not match the correct length of the slave station's reply data.
11	The CRC checksum of the message received by the master station is incorrect.
12	The number of message registers received by the master station is incorrect.
13	The master station received a message with an incorrect slave address.
14	Main station received timeout
15	The function code in the message received by the master station is inconsistent with the request.
16	The master station received a message register address that is incorrect.
17	Unknown error
19	TCP connection error: TCP CONNECT ERR

Modbus TCP communication control word: 9 bytes, the meaning of each byte is as follows:

Note: Each socket must be enabled before data communication can take place.

Byte 1: Bit 0 clears the alarm. Triggered on rising edge. Bits 1-7 control socket enable for bits 0-7. 1 enables, 0 disables. When enabled, the client will connect to the corresponding Modbus TCP slave. When disabled, the connection will be closed. (The success of the socket connection can be observed through bytes 3 and 4 of the status word.)

Byte 2: Bit 0 indicates socket8 is enabled. 1 enables, 0 disables. Other bits are reserved and unused.

Byte 3: Reserved and unused

Byte 4: Slot number: 2-9 trigger bits.

Byte 5: Slot number: 10-17 trigger bits.

Byte 6: Slot number: 18-25 trigger bits.

Byte 7: Slot number: 26-33 trigger bits.

8th byte: Slot number: Trigger bits 34-41.

9th byte: Slot number: 42-49 trigger bits.

1st byte							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
S7_EN	S6_EN	S5_EN	S4_EN	S3_EN	S2_EN	S1_EN	Clear alarm

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

2nd byte							
S15_EN	S14_EN	S13_EN	S12_EN	S11_EN	S10_EN	S9_EN	S8_EN
3rd byte							
null	null	null	null	null	null	null	null
4th byte							
Sub-slot 9	Sub-slot 8	Sub-slot 7	Sub-slot 6	Sub-slot 5	Sub-slot 4	Sub-slot 3	Sub-slot 2
5th byte							
Sub-slot 17	Sub-slot 16	Sub-slot 15	Sub-slot 14	Sub-slot 13	Sub-slot 12	Sub-slot 11	Sub-slot 10
6th byte							
Sub-slot 25	Sub-slot 24	Sub-slot 23	Sub-slot 22	Sub-slot 21	Sub-slot 20	Sub-slot 19	Sub-slot 18
7th byte							
Sub-slot 33	Sub-slot 32	Sub-slot 31	Sub-slot 30	Sub-slot 29	Sub-slot 28	Sub-slot 27	Sub-slot 26
8th byte							
Sub-slot 41	Sub-slot 40	Sub-slot 39	Sub-slot 38	Sub-slot 37	Sub-slot 36	Sub-slot 35	Sub-slot 34
9th byte							
Sub-slot 49	Sub-slot 48	Sub-slot 47	Sub-slot 46	Sub-slot 45	Sub-slot 44	Sub-slot 43	Sub-slot 42

Modbus RTU Master Submodule Parameters

Each Modbus RTU master command has five attributes:

Slave Address (1 ~ 247): Represents the address of the Modbus RTU slave device, with a selectable range of 1-247.

Function Code: The function code of the Modbus RTU master station is automatically generated based on the Modbus command inserted into the slot and cannot be changed.

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

XX Quantity : Indicates the number of coils or registers to be read or written. It is automatically generated based on the Modbus command inserted into the slot and the quantity can be changed within a specified range .

Transmission Type: The following four transmission types are available.

Disable: indicates that the command will not be executed.

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

Leve `ltrigger` (level transmission): After the control transmission flag corresponding to the slot number changes from 0 to 1: For read commands, this message will be sent. For write commands, it will only be sent if the data has changed; after the control transmission flag corresponding to the slot number changes from 1 to 0, both read and write messages will stop being sent. (Taking the previous section as an example, PLC addresses QB2-QB5 are the transmission trigger control bits.)

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Rising Trigger (sent on rising edge): This message will be sent once after the trigger control bit corresponding to the slot number changes from 0 to 1. (In the previous section, PLC addresses QB2-QB5 were the trigger control bits for sending the message.)

Modbus RTU slave module parameters

Each Modbus RTU slave command is prefixed with either Input or Output. Input indicates data input to the PLC, meaning the master station writes data to the slave station, and the slave station then returns the data to the PLC; this corresponds to a write command. Output indicates data output from the PLC, meaning the PLC sends data to the slave station, and the master station then reads the data from the slave station; this corresponds to a read command. More specifically, each slave command ends with a list of supported function codes.

function code	Function	Operating address area (non-register PLC address)	Operation type
01H	Read the output status of multiple coils	0XXXX	read
02H	Read the status of multiple input coils	1xxXX	read
03H	Reading multiple saved registers	4xxXX	read
04H	Read input register	3XXXX	read
05H	Force a single coil	0XXXX	Write
06H	Preset a single holding register	4XXXX	Write
OFH	Forced multi-coil	0xXXX	Write
10H	Multiple pre-set holding registers	4XXXX	Write

Modbus TCP Master Submodule Parameters

Each Modbus TCP master command has five attributes.

The Function Code, Start Address, Coil Quality, and Trigger Type are configured the same as those of the Modbus RTU master station.

Socket Config selection (1-8): Select which socket this instruction should use.

Modbus TCP slave submodule parameters

The parameters are similar to those of the Modbus RTU slave submodule.

6.5.1 Serial Port Enable Routine

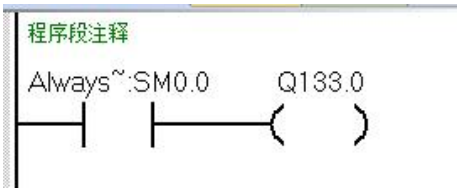
Query control word

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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



Enable the serial port

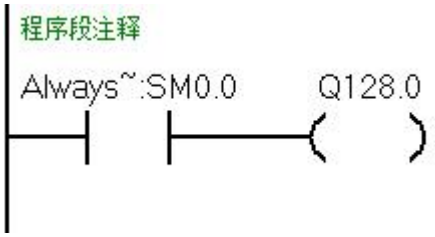


6.5.2 Network Socket Enabler Routine

Query control word



Enable socket1



6.6 Using STEP 7 to modify module names and query IP addresses

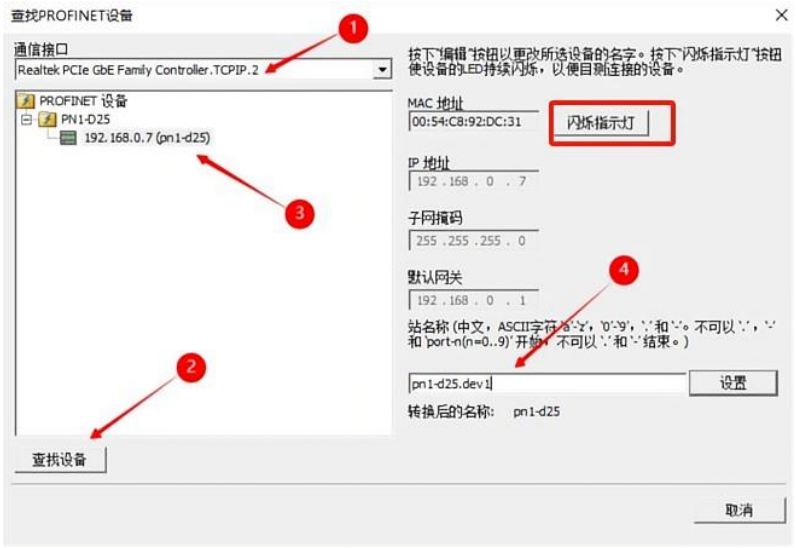
Search for gateway devices using the Profinet tool in STEP 7-MicroWIN SMART, and configure a unique working "station name" for the gateway so that the PLC can communicate with the corresponding gateway;

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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



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



Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

Chapter 7 Precautions

1. If communication fails (data indicator light does not flash), focus on checking if it is enabled (refer to the "Configure Status Word and Control Word" section).
2. The modified Modbus instruction configuration fails to connect after downloading the PLC program; a gateway restart is required.
3. When compiling the PLC, the error " Unsupported startup mode " occurs . The latest GSD file needs to be used. When using it, the old GSD file needs to be removed.
4. When encountering error events such as CRC Check Error, Frame Length Error, or Slave Address Error, please increase the values of Slave Response Timeout (ms) and Frame interval (m; s). Refer to the "Configuring Modbus Communication Parameters" section for instructions on locating these parameters.
5. The device name added in the configuration must be consistent with the device name. If they are inconsistent, please refer to the "Modifying Module Name and Querying IP Address" section.
6. If too many devices are connected to the serial port, or if the wiring is very long, a 120Ω terminating resistor needs to be added.
7. Supports RT real-time communication and is compatible with Profinet IO V2.3 ;
8. Software configuration can be performed using Codesys;

Note: If the above issues still cannot resolve the fault, capture the error message from the configuration software's diagnostic buffer and submit it for after-sales technical assistance.

Copyright © 2012–2026 , 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	2026-6-1	Initial version	LT

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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

About us

Technical support: support@cdebyte.com

Documents and RF Setting download link: www.cdebyte.com

Thank you for using Ebyte products! Please contact us with any questions or suggestions: info@cdebyte.com

---

Phone:4000-330-990

Web: www.cdebyte.com

Address: B5 Mould Park, 199# Xiqu Ave, High-tech District, Sichuan, China

Chengdu Ebyte Electronic Technology Co.,Ltd.

Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co.,Ltd

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