Chengdu Ebyte Electronic Technology Co.,Ltd

Wireless Modem

User Manual

Profinet to Modbus TCP/RTU SMD Gateway Module

PN1-S25T & PN1-S25T-TB



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

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

Table of Contents

1. Product Overview 1
1.1. Product Introduction 1
1.2. Features 1
2. Technical parameters 2
2.1. Product Model List 2
2.2. Specifications 2
2.3. Dimensions 4
2.4. Pin Definitions 5
2.5. Hardware Reference Design 9
2.5.1. Typical application reference links 9
2.5.2. Power circuit reference hardware connection 10
2.5.3. 1.8V serial port circuit reference connection 3.3V 11
2.5.4. 5V serial port circuit reference connection 11
2.5.5. Network port built-in transformer reference connection 12
2.5.6. External transformer reference connection 13
2.5.7. Reset circuit reference connection 14
2.5.8. Watchdog circuit reference connection 15
3. Product Function Introduction 16
3.1. PN1-S25T Series Functional Overview 16
3.2. Change IP address 16
3.3. Profinet to serial port function 16
3.4. Upgrade Feature Tutorial 18
4. Equipment alarm information description 20
5. Tutorial on loading devices using TIA Portal 21
5.1. Preparation before connection 21
5.2. Add GSDML file to TIBRA 21
5.3. Add Profinet device to project 22
5.4. Configure Modbus communication parameters 24
5.5. Modbus communication interface parameters for PN1-S25T device module: 26
5.6. Configure Modbus status word and control word 31
5.6.1. Modbus RTU status word and control word 31
5.6.2. Modbus TCP status word and control word 32
5.7. Submodule parameter description 34
5.7.1. Serial port enable routine 35
5.7.2. Network socket enable routine 36
5.8. Use TOBTA to modify module names and query IP addresses. 36
6. Tutorial on loading devices using STEP 7 37
6.1. Preparation before connection 37
6.2. STEP 7 Add GSDML file 37
6.3. Add Profinet device to project 38
6.4. Configure Modbus communication parameters 40
6.5. Configure Modbus status word and control word 44

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

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

6.5.1. Serial port enable routine 48
6.5.2. Network socket enable routine 48
6.6. Use STEP 7 to modify module names and query IP addresses 49
7. Precautions 50
8. Important Announcement 51
9. Revision History 51

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

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

1. Product Overview

1.1. Product Introduction



The PN1-S25T is a Profinet-to-Modbus TCP/RTU gateway module designed specifically for industrial communication. It maps Modbus data to Profinet. Integration uses GSD files, enabling code-free reading and writing of Modbus devices, allowing for rapid data configuration and transmission to the PLC. All Modbus commands are loaded as modules, and the memory mapping relationship between Profinet and Modbus is intuitive and can be queried in STEP 7 or TIA Portal software. Status bytes can be loaded to query the connection status of Modbus devices, enabling real-time monitoring of device status.

The product uses a 1.27mm stamp-hole packaging, making it compact and easy for users to integrate into their systems.

The PN1-S25T-TB test kit features a built-in Type-C interface for power supply, one independent RS485 serial port, and two Ethernet ports (Professional Ethernet port + Modbus TCP Ethernet port) to meet diverse communication needs. All LEDs, function pins, and reset pins are brought out; the reset pin is connected to an external button for easy operation, and the operating status indicator pin is also connected to an external LED for easy user observation of the status.

1.2. Features

- It uses the standard Profinet protocol for communication and can be networked 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.
- Profinet and Modbus TCP/RTU protocol converter, usable as a Modbus TCP/RTU slave or Modbus TCP/RTU master.
- In Modbus TCP mode, a total of 8 sockets are supported. When the master station is active, 8 slave stations can connect simultaneously, and when the slave station is active, 8 master stations can connect simultaneously.
- Supports 2 Ethernet interfaces, crossover direct connection auto-sensing
- Industrial-grade design with metal shielding
- Supports 3.3V power supply
- 1.27mm stamp-perforated seal, compact size
- Supports Profinet to serial port pass-through
- It provides GSD files directly, offers simple configuration, and requires no host computer.
- Supports firmware upgrade function
- Widely used for data acquisition and control of Modbus RTU devices in industrial fields

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

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

2. Technical parameters

2.1. Product Model List

Product Model	type
PN1-S25T	SMT module
PN1-S25T-TB	Test kit (with built-in PN1-S25T)

2.2. Specifications

PN1-S25T		
category	name	parameter
power supply	Operating voltage	DC 3.3V±0.3V
	Operating current	Peak current: 207mA Operating current: 176mA Standby current: 175mA
	Communication level	3.3V
Packaging	Packaging	1.27mm stamp perforation
Profinet network parameters	Communication Protocol	Standard Profinet protocol (RT)
	Maximum communication cycle	4ms
	Communication bandwidth	10/100M adaptive
Modbus TCP network parameters	Communication Protocol	Modbus TCP
	Minimum communication cycle	10ms
	Communication bandwidth	100Mbps
Serial port parameters	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) Validation: None/Odd/Even (default: None)
Work environment	Operating temperature and humidity	-40 to +85℃, 5% to 95%RH (non-condensing)
	Storage temperature and humidity	-40 to +105℃, 5% to 95%RH (non-condensing)
other	Product Dimensions	27.0 mm * 27.0 mm * 3.0 mm (Length * Width * Height)
	Product weight	4 ± 1 g

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

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

PN1-S25T-TB		
category	name	parameter
power supply	Operating voltage	DC 5V±0.5V
	Communication level	5V
Profinet network parameters	Communication Protocol	Standard Profinet protocol (RT)
	Maximum communication cycle	4ms
	Communication bandwidth	10/100M adaptive
Modbus TCP network parameters	Communication Protocol	Modbus TCP
	Minimum communication cycle	10ms
	Communication bandwidth	100Mbps
Serial port parameters	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) Validation: None/Odd/Even (default: None)
Work environment	Operating temperature and humidity	-40 to +85℃, 5% to 95%RH (non-condensing)
	Storage temperature and humidity	-40 to +105℃, 5% to 95%RH (non-condensing)
other	Product Dimensions	100 mm * 44 mm * 16.5 mm (Length * Width * Height)
	Product weight	40 ± 5 g

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

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

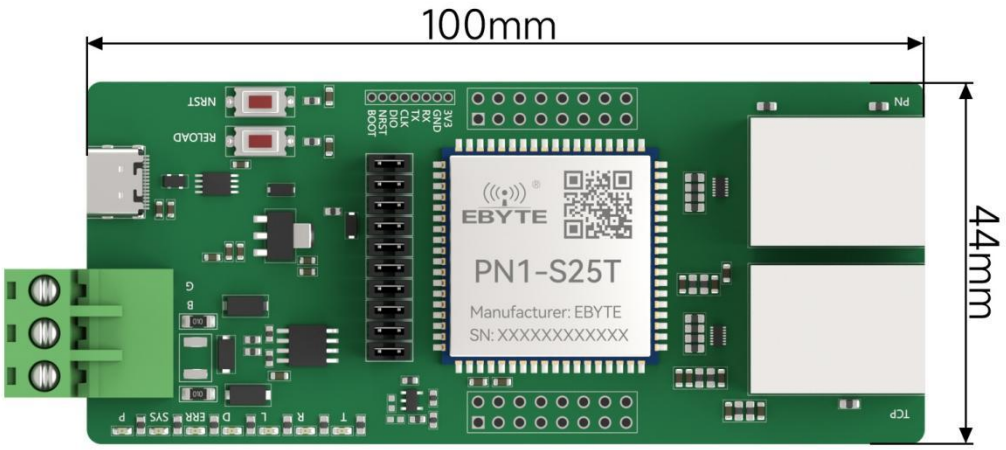
2.3. Dimensions

PN1-S25T:



27.0 mm * 27.0 mm * 3.0 mm (Length * Width * Height)

PN1-S25T-TB:

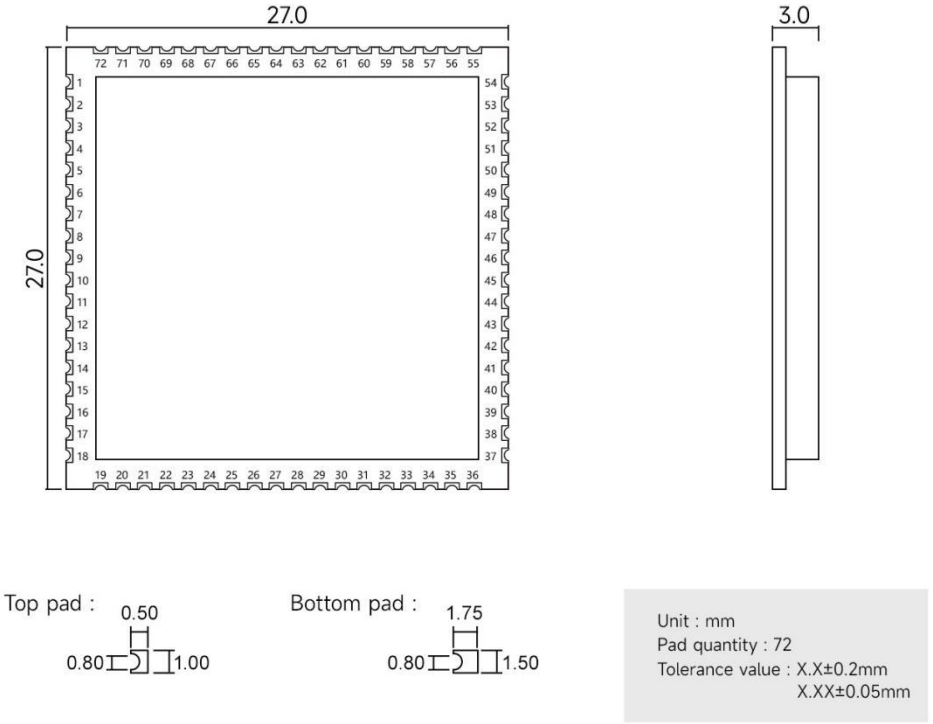


100 mm * 44 mm * 16.5 mm (Length * Width * Height)

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

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

2.4. Pin Definitions



Serial Number	PN1-S25T Pin name	PN1-S25T-TB silkscreen printing (see actual product for details)	describe
1	GND	GND	Common ground terminal, negative power input terminal
2	NC	NC	Suspended
3	NC	NC	Suspended
4	TXD1	485-RXD	For serial data transmission, the TTL level communication voltage is limited to 3.3V.
5	RXD1	485-TXD	For serial port data reception, the TTL level communication voltage is limited to 3.3V.
6	TCP_DATA-LED	TCP_D-LED	The TCP communication data interaction indicator light flashes when there is data interaction.
7	TX1_EN	TX1_EN	Serial Port 1_EN is enabled. The serial port works in full-duplex mode by default. If an external RS485 chip is connected, a 1k pull-down resistor is connected to this pin. The pin function becomes RS485 enable control pin. It is set high when the serial port sends data and low under normal conditions.

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

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

8	NC	NC	Suspended
9	RXD1_LED	RXD1_LED	Serial port 1 flashes rapidly when receiving data, outputs a high level by default, and outputs a 10Hz square wave when receiving data.
10	TXD1_LED	TXD1_LED	Serial port 1 flashes rapidly when data is being sent; the default output is high; and a 10Hz square wave is output when data is being sent.
11	ERR_LED	ERR_LED	(Modbus) Communication Error Indicator Low: Moodbus communication error; High: Moodbus communication is normal; When the software controls the flashing indicator light, it flashes simultaneously with the SYS indicator.
12	SYS_LED	SYS_LED	System (PN connection) lights Pull low: Profinet establishes a connection High: Profinet has not established a connection. When the software controls the flashing indicator light, it flashes simultaneously with ERR.
13	NC	NC	Suspended
14	NC	NC	Suspended
15	NC	NC	Suspended
16	NC	NC	Suspended
17	GND	GND	Common ground terminal, negative power input terminal
18	GND	GND	Common ground terminal, negative power input terminal
19	GND	GND	Common ground terminal, negative power input terminal
20	GND	GND	Common ground terminal, negative power input terminal
twenty one	VCC	VCC	Positive power input, supports 3.3V input.
twenty two	VCC	VCC	Positive power input, supports 3.3V input.
twenty three	NC	NC	Suspended
twenty four	NC	NC	Suspended
25	NRST	NRST	By default, the system internally pulls the price high and pulls it low to initiate a restart.
26	RELOAD	RELOAD	Restore factory settings by connecting the pins with a weak internal pull-up. An external reset button can be connected. A low level for 5-10 seconds will restore factory settings.
27	GND	GND	Common ground terminal, negative power input terminal
28	NC	NC	Suspended
29	NC	NC	Suspended
30	NC	NC	Suspended
31	NC	NC	Suspended

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

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

32	NC	NC	Suspended
33	NC	NC	Suspended
34	NC	NC	Suspended
35	VDD18	VDD18	The output voltage is 1.8V, which is only supplied to the Modbus TCP Ethernet port transformer pull-up.
36	GND	GND	Common ground terminal, negative power input terminal
37	TCP_TX1_P	TCP_TX1_P	Modbus TCP Ethernet port sends TX+ signal
38	TCP_TX1_N	TCP_TX1_N	Modbus TCP Ethernet port sends TX signal
39	TCP_RX1_P	TCP_RX1_P	Modbus TCP Ethernet port receives RX+ signal
40	TCP_RX1_N	TCP_RX1_N	Modbus TCP Ethernet port receives RX signal
41	SPD1-LED	SPD1-LED	Modbus TCP Ethernet port speed indicator. Used to indicate the current network connection speed status.
42	LINK1_LED	LINK1_LED	Modbus TCP Ethernet port link indicator light. Indicates the physical link connection status. A constantly lit indicator light means the network cable is correctly connected. Flashing: This usually indicates that a link has been established and data is being sent or received. Extinguished: Indicates no link.
43	GND	GND	Common ground terminal, negative power input terminal
44	GND	GND	Common ground terminal, negative power input terminal
45	NC	NC	Suspended
46	PN_LINK2_LED	PN_LINK2_LED	The Profinet Ethernet 10M PHY indicator light goes low after successful PHY negotiation and flashes when data is being transmitted or received.
47	PN_SPD2_LED	PN_SPD2_LED	The Profinet Ethernet 100M PHY indicator light goes low after successful PHY negotiation and flashes when data is being transmitted or received.
48	PN_TX_P2	PN_RX_P2	Profinet Ethernet port receives TX+ signal
49	PN_TX_N2	PN_TX_N2	Profinet Ethernet port sends TX- signal
50	PN_RX_P2	PN_RX_P2	Profinet Ethernet port receives RX+ signal
51	PN_RX_N2	PN_RX_N2	Profinet Ethernet port receives RX signal
52	NC	NC	Suspended
53	NC	NC	Suspended
54	NC	NC	Suspended
55	GND	GND	Common ground terminal, negative power input terminal
56	NC	NC	Suspended
57	NC	NC	Suspended
58	NC	NC	Suspended
59	NC	NC	Suspended
60	NC	NC	Suspended
61	NC	NC	Suspended
62	NC	NC	Suspended

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

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

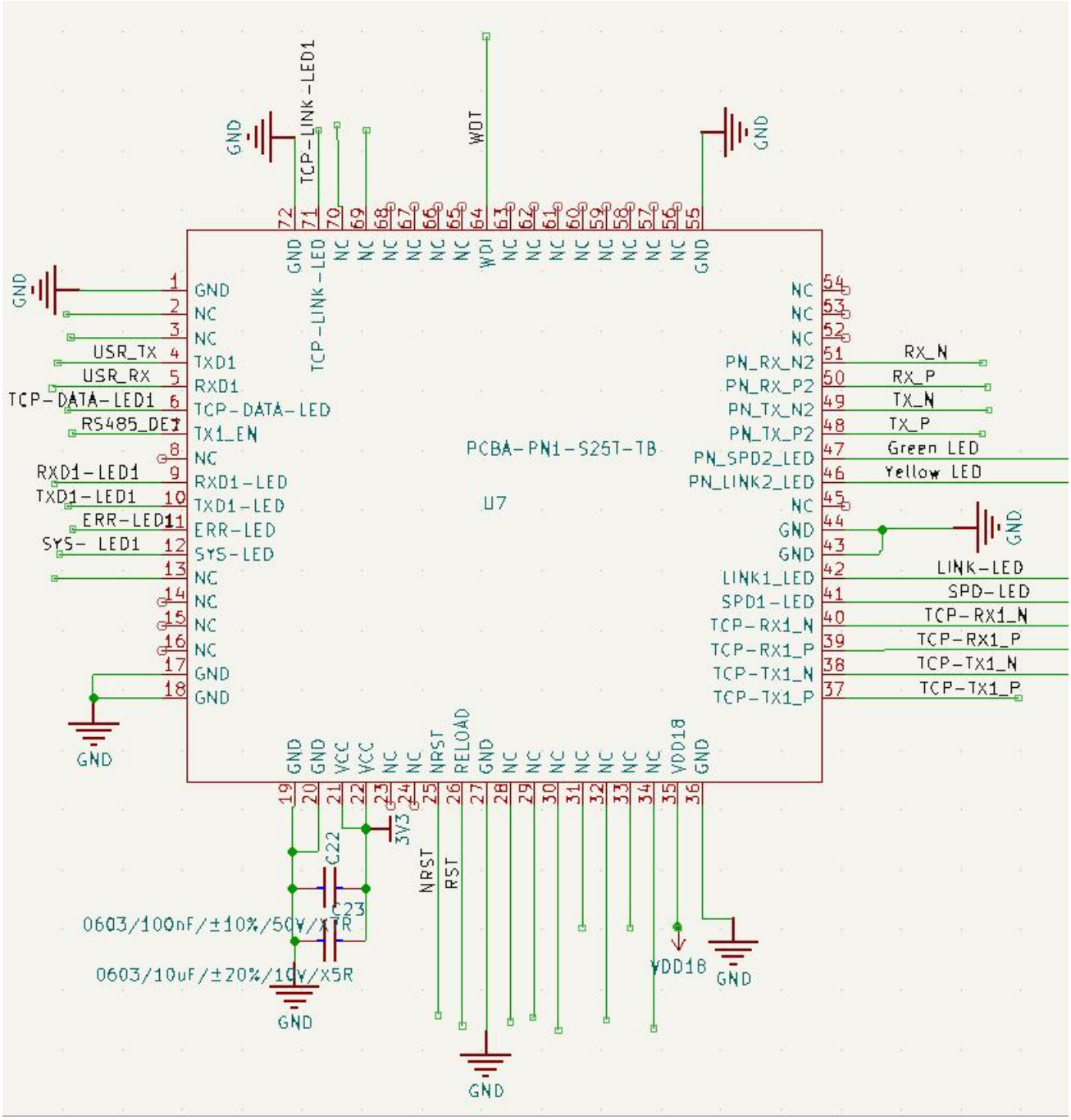
63	NC	NC	Suspended
64	WDI	WDI	External hardware watchdog feed signal, push-pull output. When the program is running normally, the level of this pin will periodically toggle to provide a heartbeat to the external monitoring/watchdog circuit.
65	NC	NC	Suspended
66	NC	NC	Suspended
67	NC	NC	Suspended
68	NC	NC	Suspended
69	NC	NC	Suspended
70	NC	NC	Suspended
71	TCP-LINK-LED	TCP-L-LED	The Modbus TCP light remains on after a connection is established, and remains off when there is no connection.
72	GND	GND	Common ground terminal, negative power input terminal

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

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

2.5. Hardware Reference Design

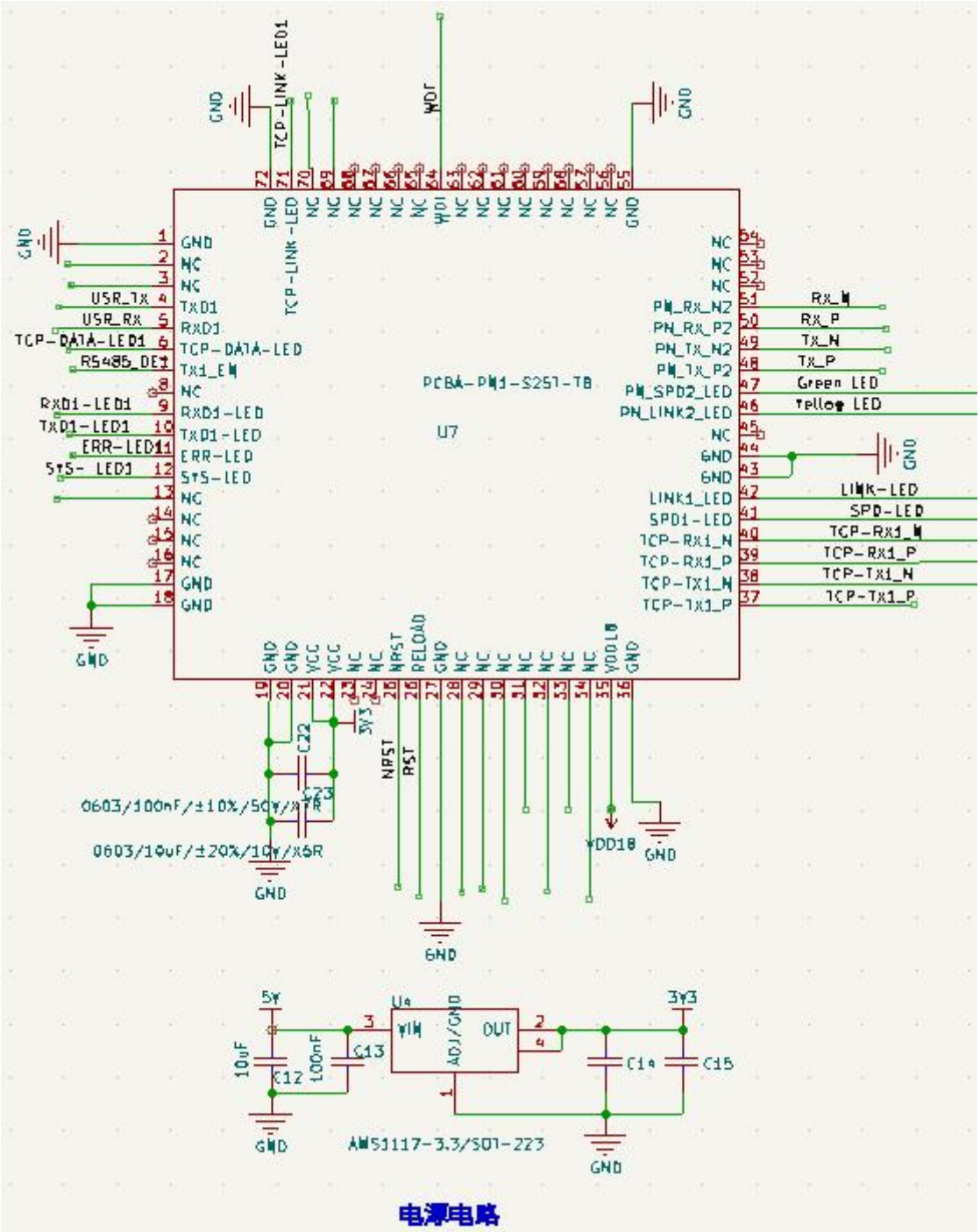
2.5.1. Typical application reference links



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

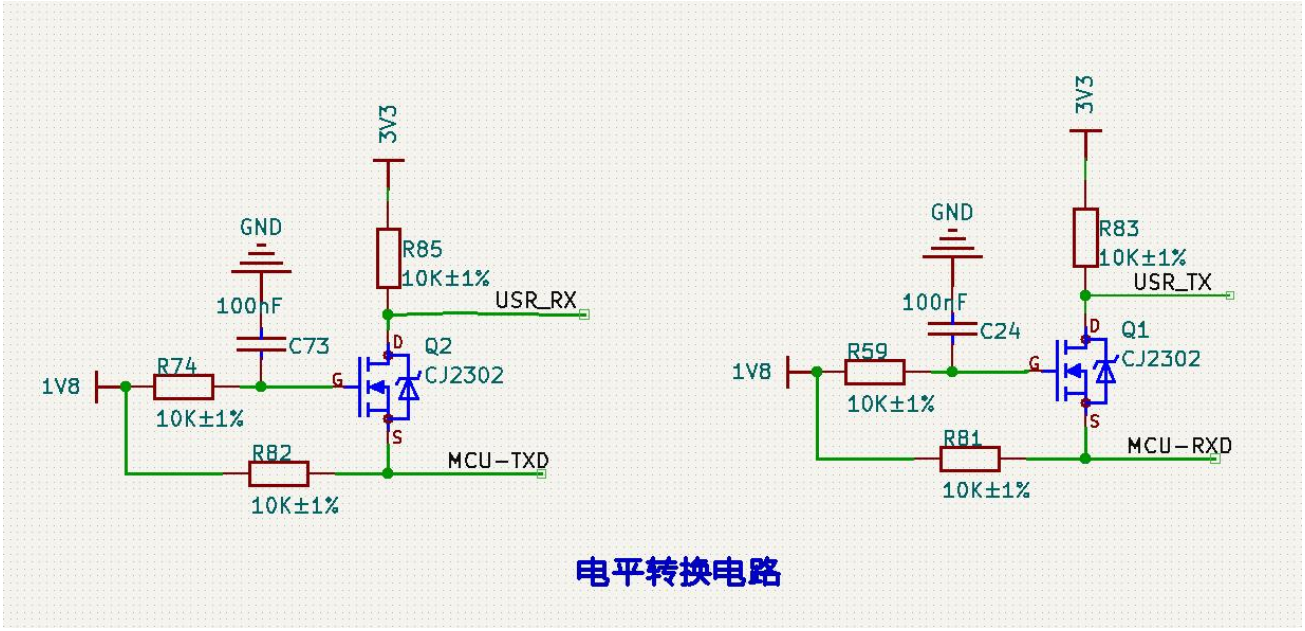
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

2.5.2. Power circuit reference hardware connection

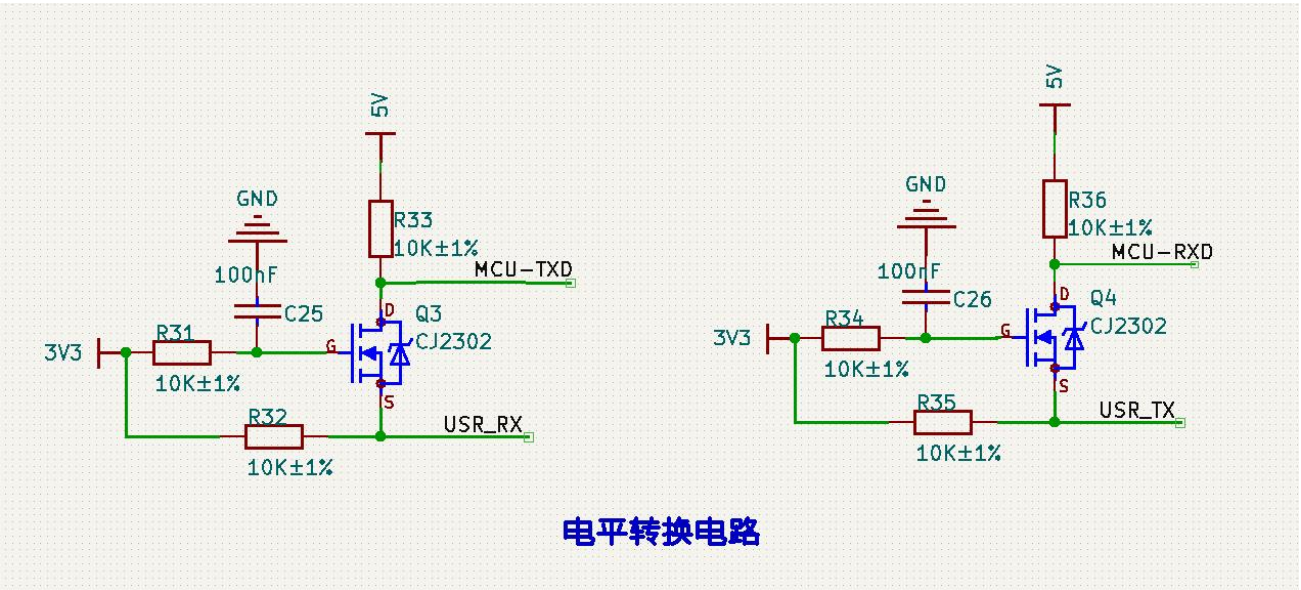


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

2.5.3. 1.8V serial port circuit reference connection 3.3V



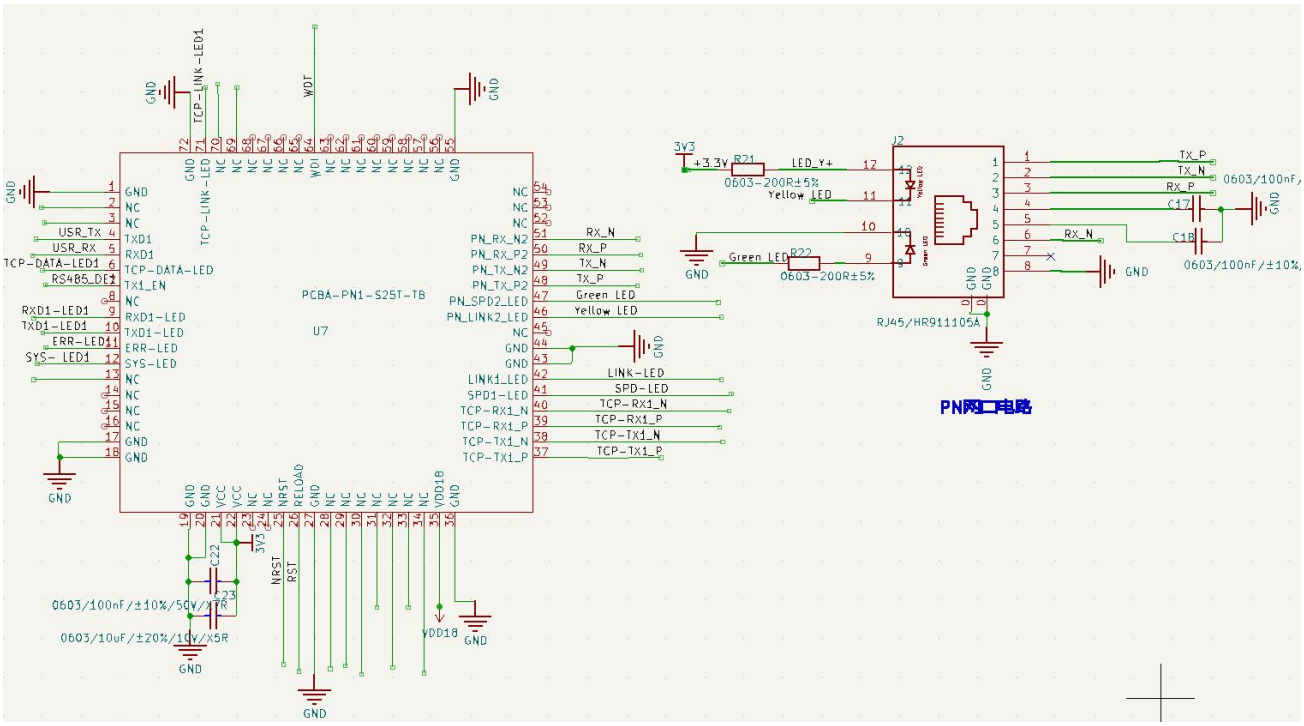
2.5.4. 5V serial port circuit reference connection

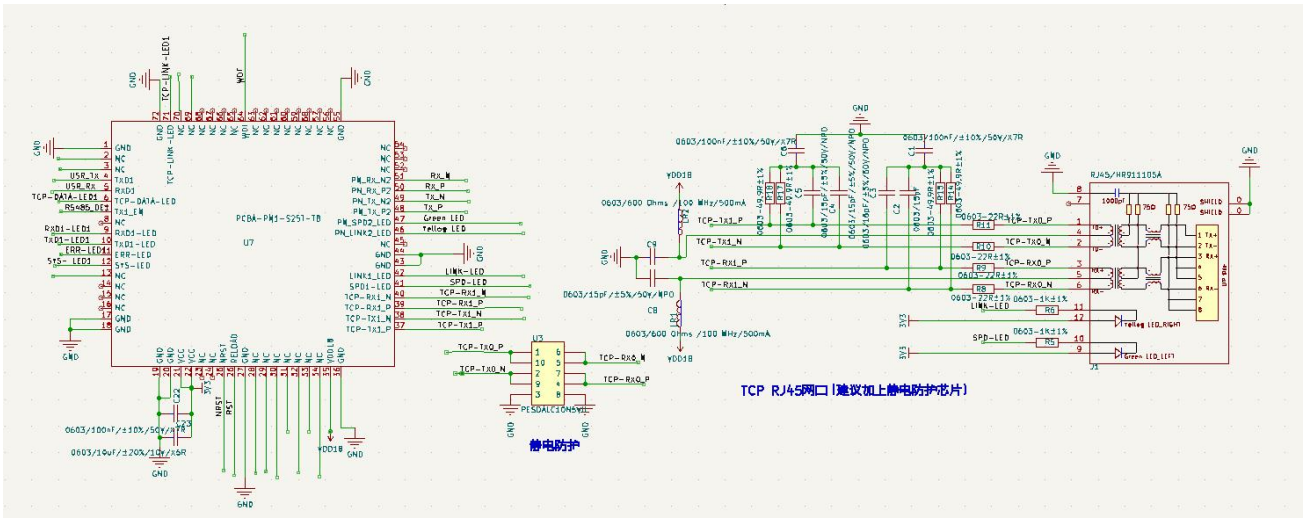


Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co., Ltd.

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

2.5.5. Network port built-in transformer reference connection

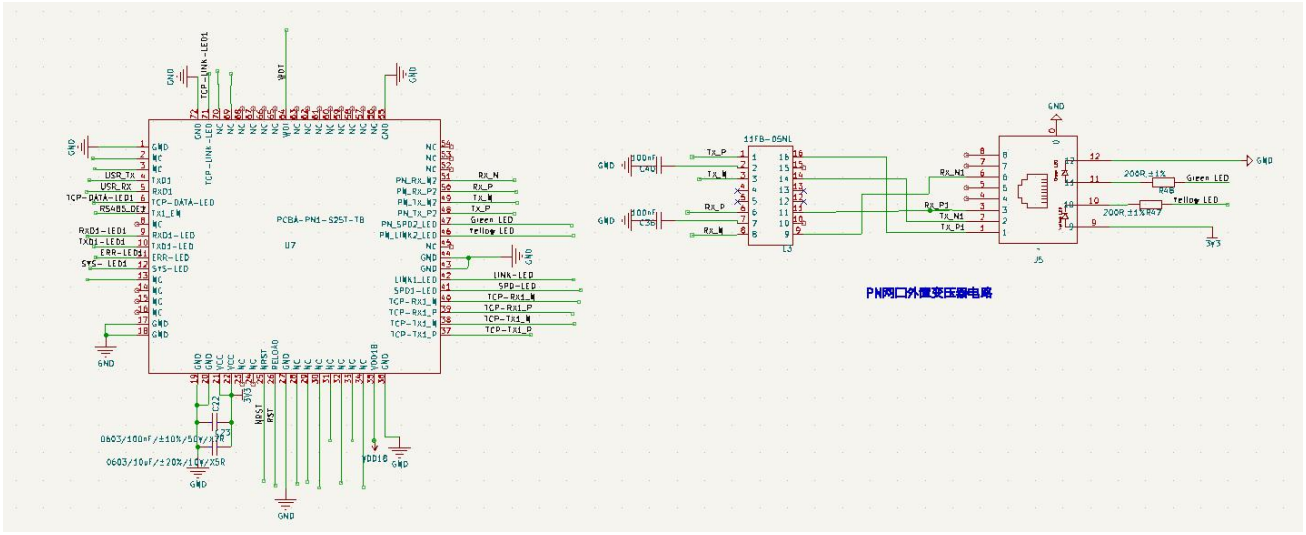


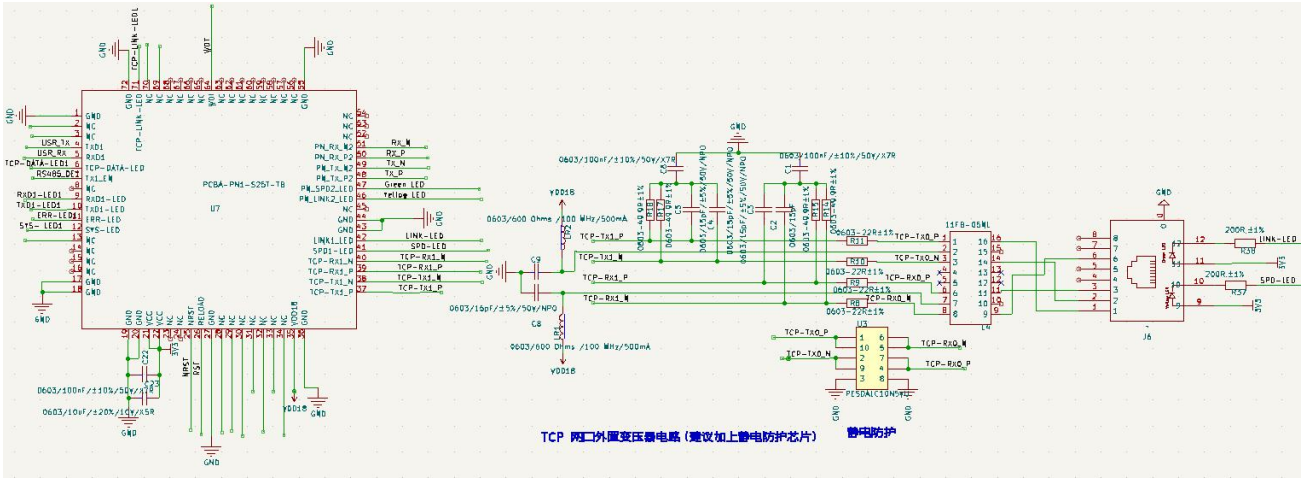


Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co., Ltd.

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

2.5.6. External transformer reference connection

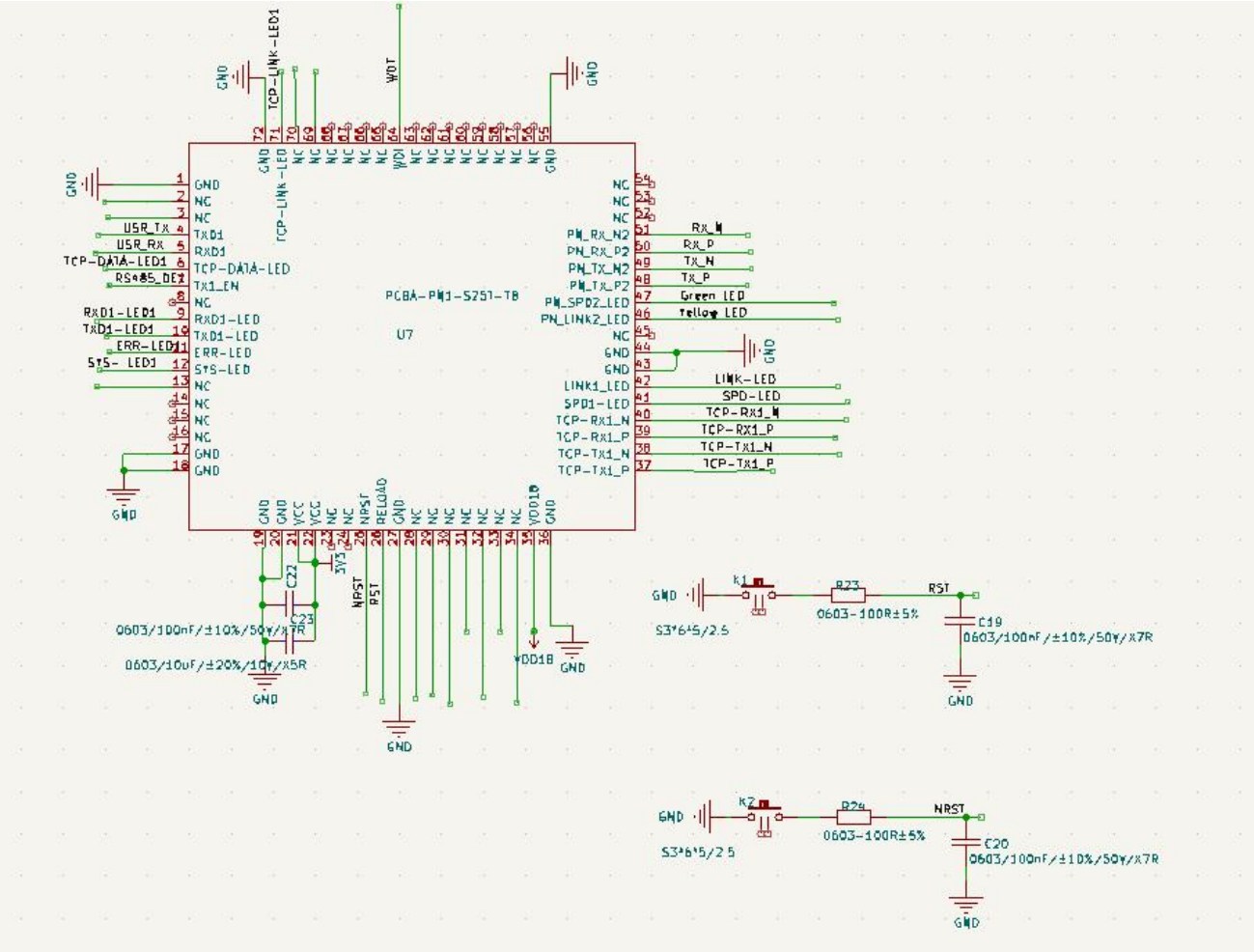




Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co., Ltd.

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

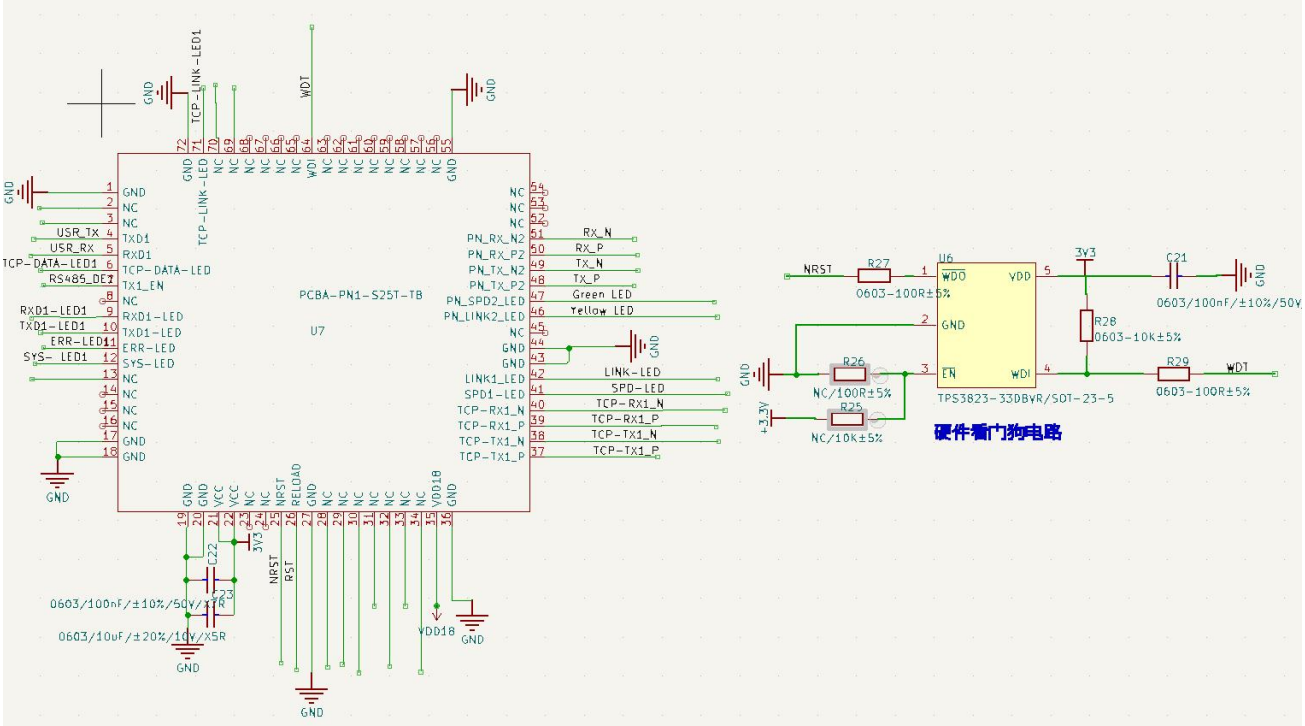
2.5.7. Reset circuit reference connection



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

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

2.5.8. Watchdog circuit reference connection



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

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

3. Product Function Introduction

3.1. PN1-S25T Series Functional 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. Change 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. Profinet to serial port function

The PN to serial port function supports both protocol pass-through and data pass-through modes.
Agreement Transmitted:
Send message: 0xc1 + sub_slot_nbr (sub-slot number, 1 byte) + datalength (data portion length, big-endian, 2 bytes) + data (data portion, length equal to datalength) + mb_CRC_16 (2 bytes, optional)
Received message: 0xd2 + sub_slot_nbr (sub-slot number, 1 byte) + datalength (data length, big-endian, 2 bytes) + data (data portion, length equal to datalength) + mb_CRC_16 (2 bytes, optional)

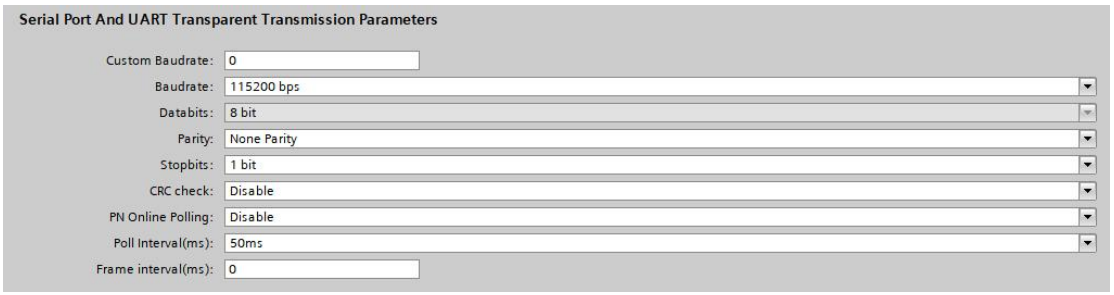
Data pass-through: Only one can be configured, which includes both sending and receiving data.
Send message: data (n bytes) + mb_CRC_16 (two bytes, optional)
Received message: data (n bytes) + mb_CRC_16 (two bytes, optional)

The serial communication status is 8 bytes. The first 4 bytes are used to count the total number of packets received by the serial port. The last 4 bytes, 32 bits, each represent the reception status of a certain sub-slot. A change in bit status (0→1 or 1→0) indicates that data has been received in that sub-slot. Setting the second bit (bit1) of the first byte of the control bit to 1 clears the reception count.

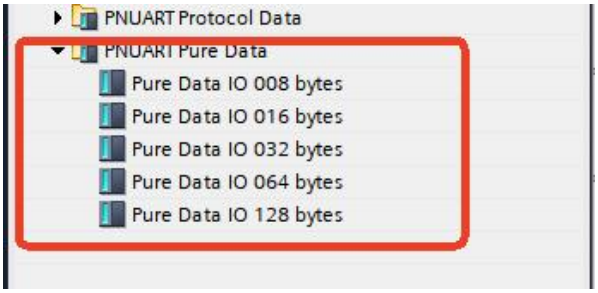
Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co., Ltd.

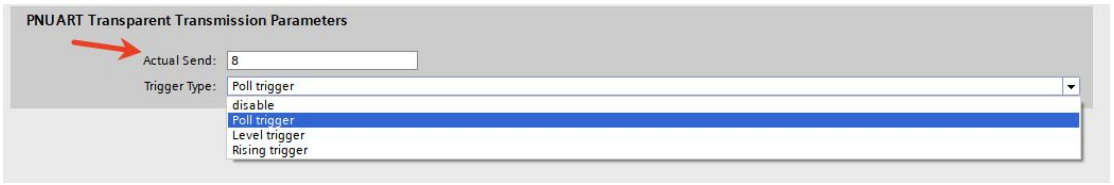
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

1、The serial port and polling parameters are mostly referenced from the Modbus host parameters. It's worth noting that when CRC check is enabled, a 2-byte Modbus CRC16 checksum will be appended to the end of the transmitted message. For received messages, the last two bytes will be checked for compliance. Only if the check is successful will the PLC data be updated; otherwise, the data will be discarded. PC2 (pin 17 VCT6) will be pulled high approximately 2ms after receiving data until a correct message is received (if necessary, it is recommended that users check this pin 3ms after transmission). The EER LED will remain lit for 3 seconds. This is disabled by default.



2. Data pass-through module: Each module supports sending and receiving messages. "Actual send" can be configured to send the actual length of data.



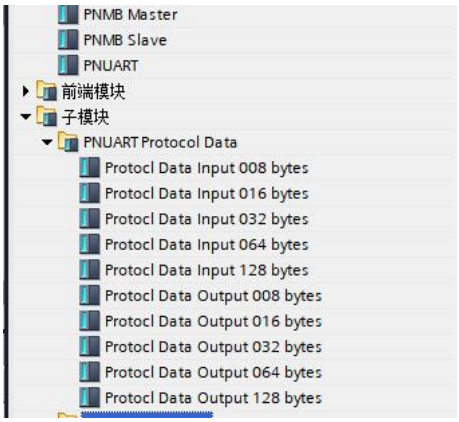


The "Trigger type" trigger mode can be configured to send messages using the trigger mode. Refer to PN to Modbus conversion. The default is polling trigger "pool trigger". Under "Level trigger", output data will only be sent when the control position is 1 and the output data changes.

2、The protocol pass-through mode can be configured as either an input or output mode. The parameter configuration for sending messages is the same as that for the data pass-through mode, and up to 48 messages can be configured in the sub-slot.

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

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





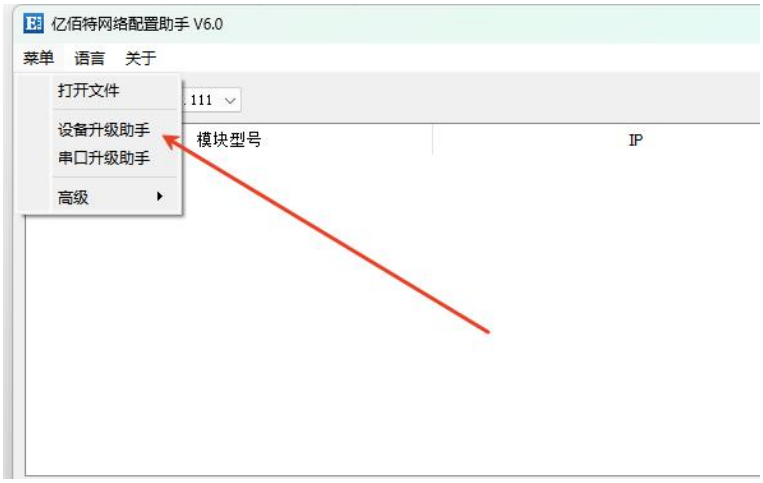
3.4. Upgrade Feature Tutorial

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

1. First, disconnect the power to the equipment.
2. Press the "reload" button to power on the device (PN1-S25T pulls pin25 low).
3. If the device's "sys" light keeps flashing, the device has entered upgrade mode.
4. Open "EBYTE Network Configuration Tool.exe"



5. Open "Device Upgrade Assistant"



6. Complete the upgrade as shown in the image below.

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

4. Equipment alarm information description

When an error occurs on the PN1-S25T 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. Specific error information can be viewed through the PLC's corresponding host computer. 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: the data address is not within the device's accessible range.
Illegal Data Value	The slave 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

5. Tutorial on loading devices using TIA Portal

If you encounter any problems during use, please click the official website link: https://www.cdebyte.com/product_serch/PN1-S25/1/

Note: PN1-S25T is a surface mount version. For first-time use, it is recommended to use a test baseboard (PN1-S25T-TB). This chapter uses PN1-S25T-TB as an example.

5.1. Preparation before connection

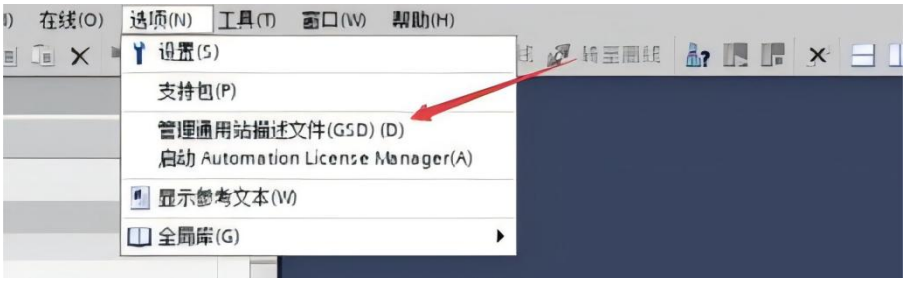
1. Prepare the necessary XML file as follows:



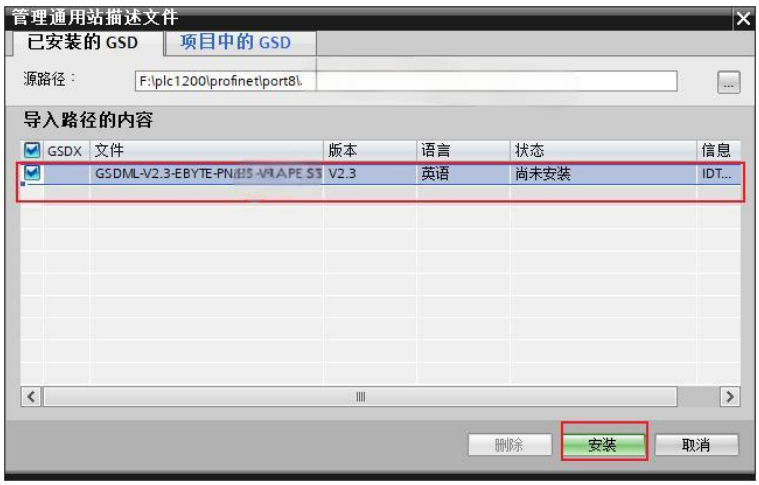
2. Connect the DC 24V external power supply to the module and power it on. Before powering on, please check that the positive and negative terminals of the power supply are connected correctly.
3. Connect the module to the Profinet interface of the PLC controller using a network cable. (Within the same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

5.2. Add GSDML file to TIBRA

1. Open TIA Portal, click Options, and then Manage General Site Files (GSD).



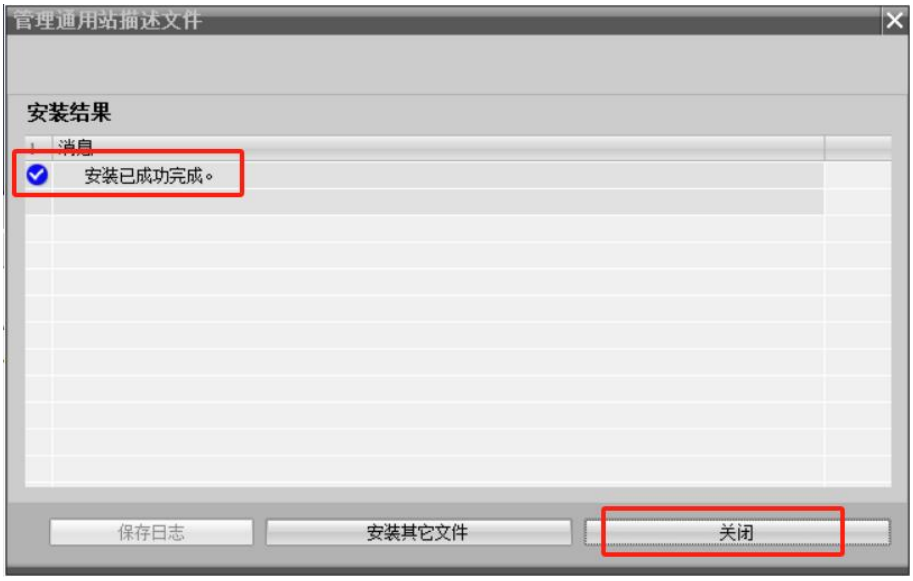
2. Add the GSDML file. Locate the folder where the GSD is stored, select the folder, and the software will automatically scan for the GSD file. Then, select the GSD file and click Install.



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

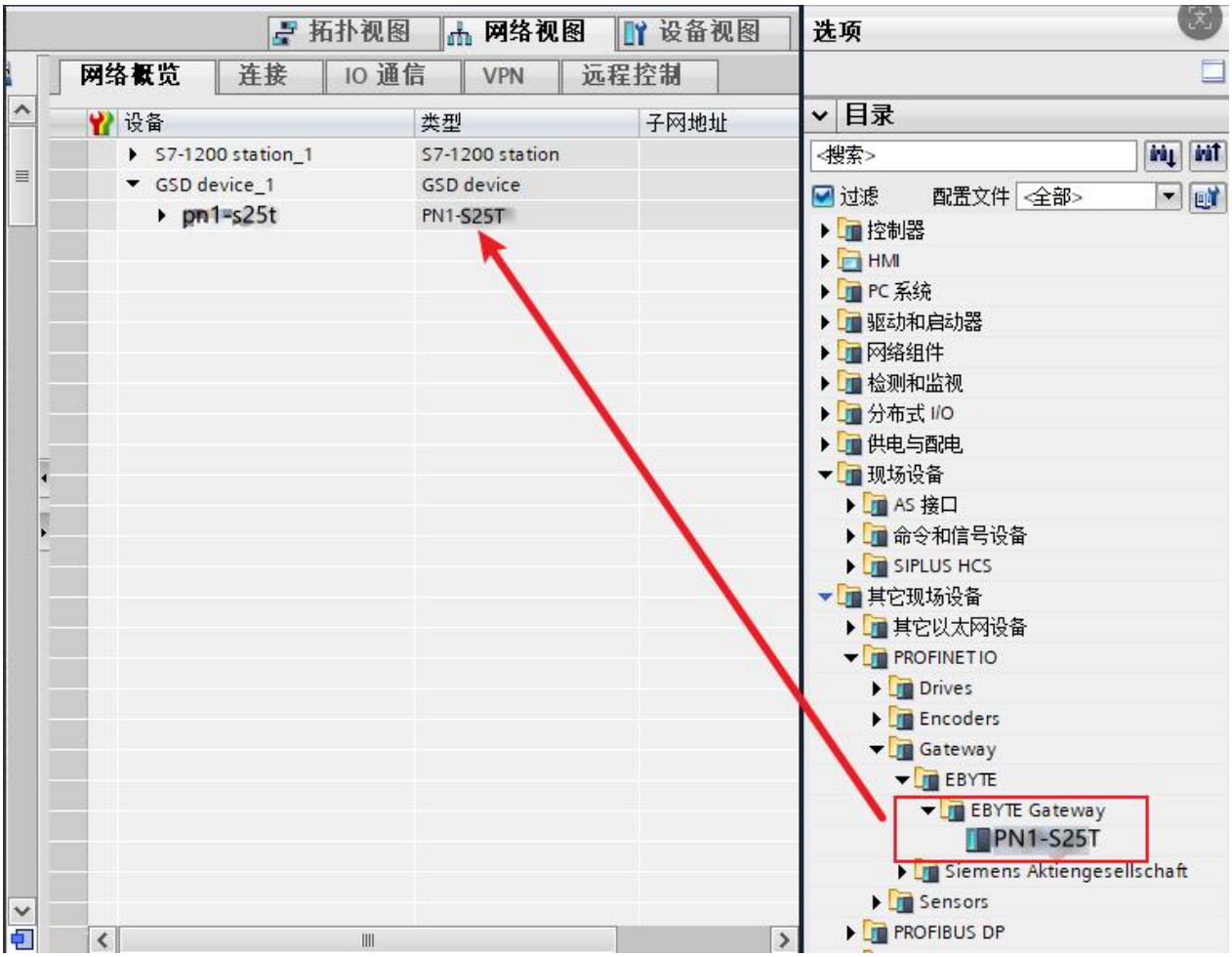
Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co., Ltd.

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



5.3. Add Profinet device to project

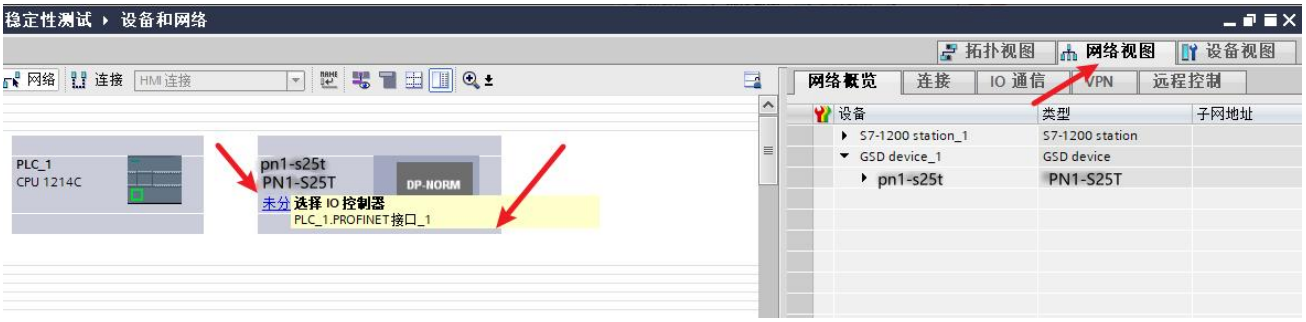
1. To create or open a new project, first add a controller device, then add the corresponding IO module in the device configuration interface. Double-click the module to add it successfully, as shown in the figure:



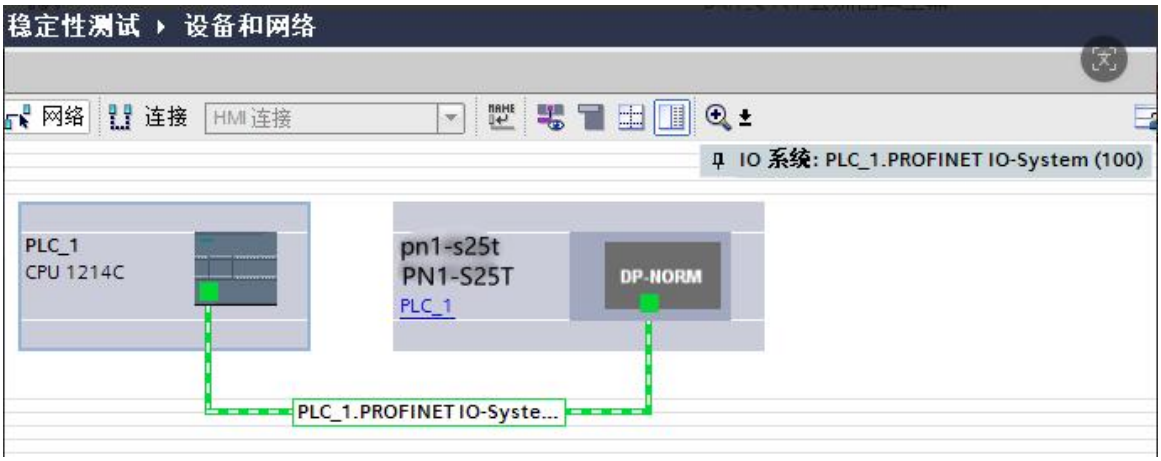
Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co., Ltd.

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

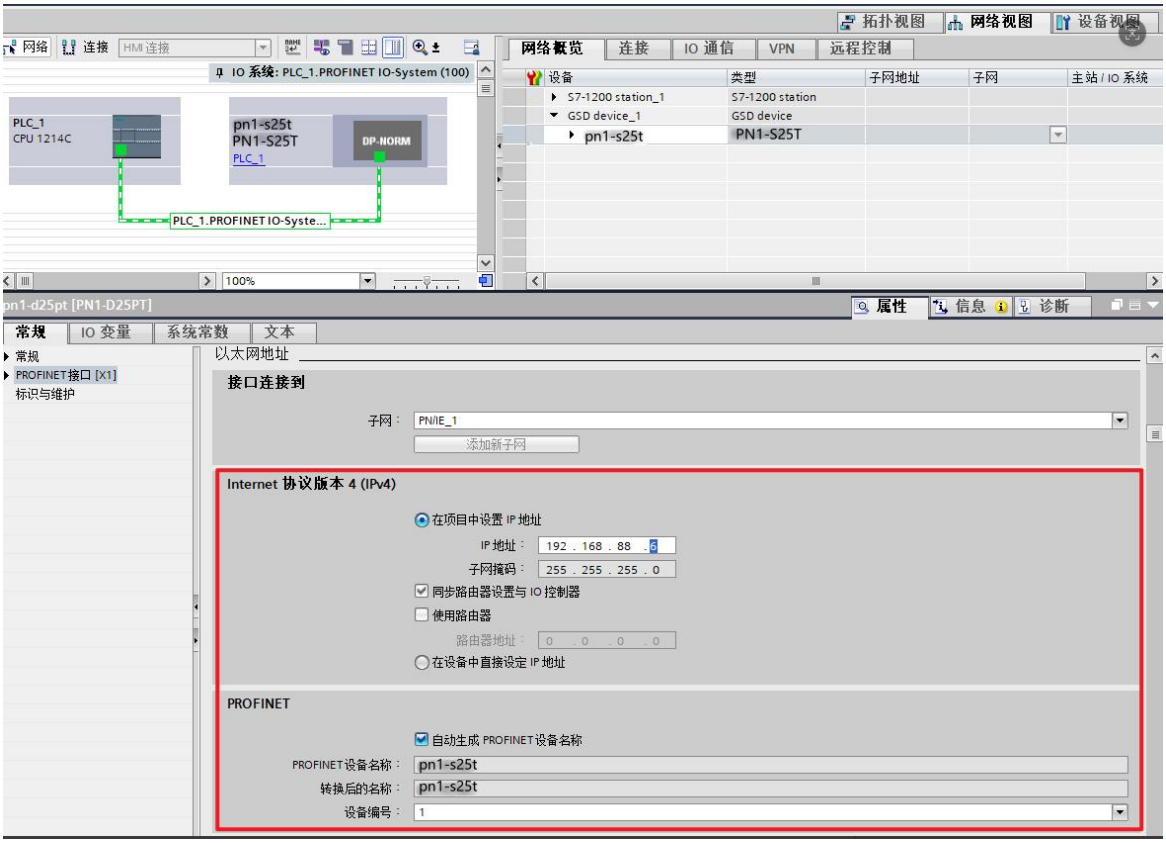
2. Configure devices in the network view.



Once completed, it will look like this:



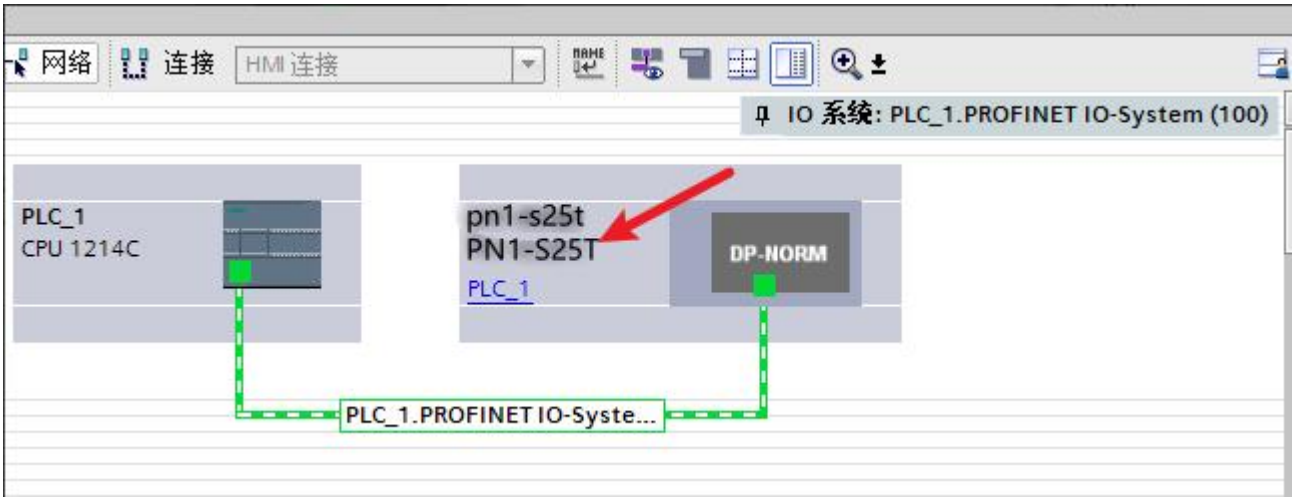
3. In the device view, first locate and select the newly added device, then double-click the module in the image. Next, in the general configuration interface, modify the IP address and device name, ensuring they match the module itself. Alternatively, you can choose to set the IP address directly on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



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

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

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

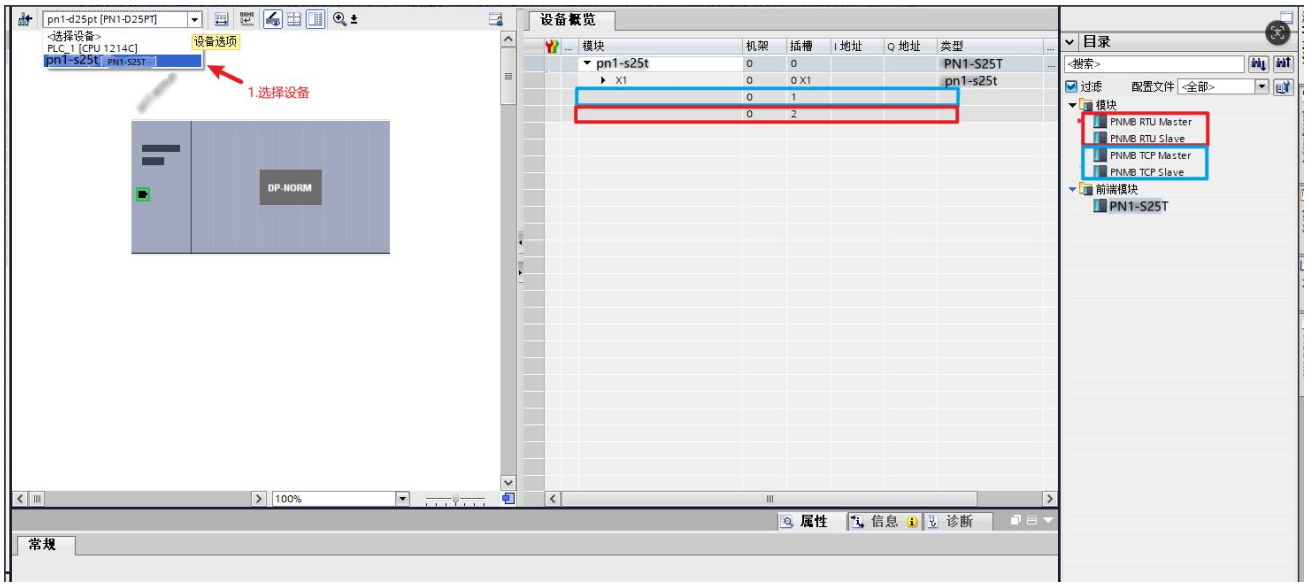


5.4. Configure Modbus communication parameters

The PN1-S25T gateway supports both Modbus TCP master and Modbus TCP slave, as well as Modbus RTU master and Modbus RTU slave, depending on the Profinet configuration.

Select PN1-S25T in the topology view interface and double-click to enter the device view operation interface.

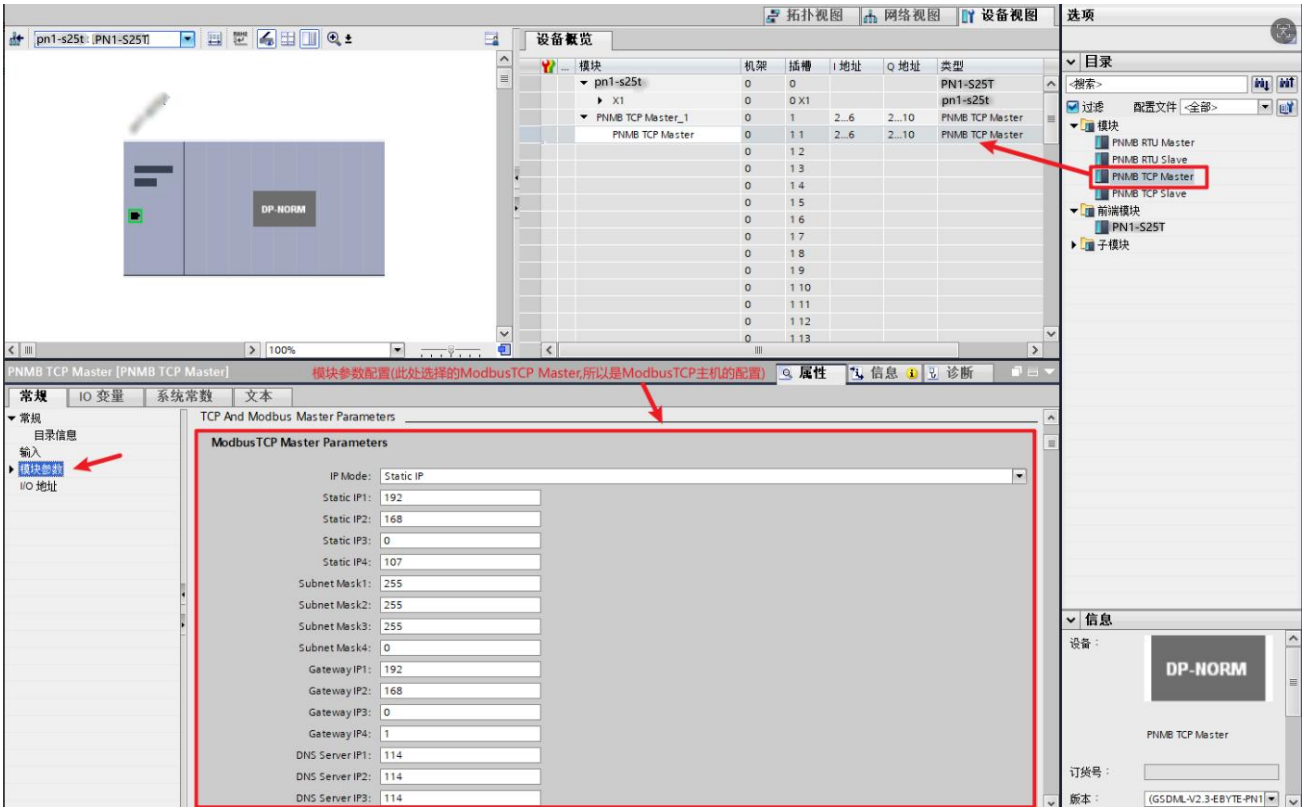
As shown in the diagram below, in the device overview area, the system provides two slots for configuring a master slot shared by Modbus TCP master/slave (corresponding in red in the diagram) and a master slot for Modbus RTU master/slave (corresponding in blue in the diagram). Each master slot supports 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 configuration). Through the status word, the PLC can obtain the operating status of the PN1-S25T device; while through the control word, the PLC can control the PN1-S25T device.



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

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

As shown in the figure, add a Modbus TCP Master to the corresponding slot from the right. You can set the Modbus TCP master parameters in "General" -> "Module Parameters" below. The slave mode parameter settings are similar.

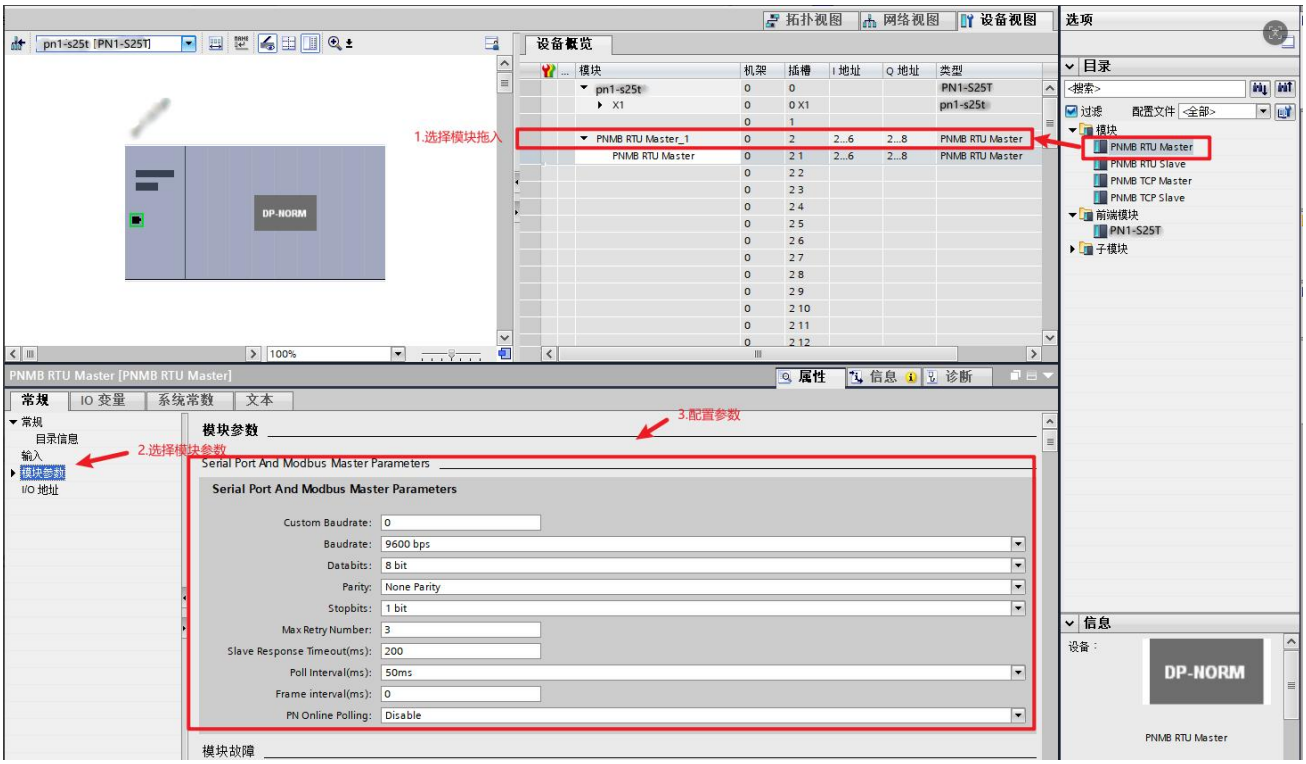


Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co., Ltd.

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

5.5. Modbus communication interface parameters for PN1-S25T device module:

Modbus 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 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 .

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

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

Slave Response Timeout (ms) :

the serial port is used as the master station, the time 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):

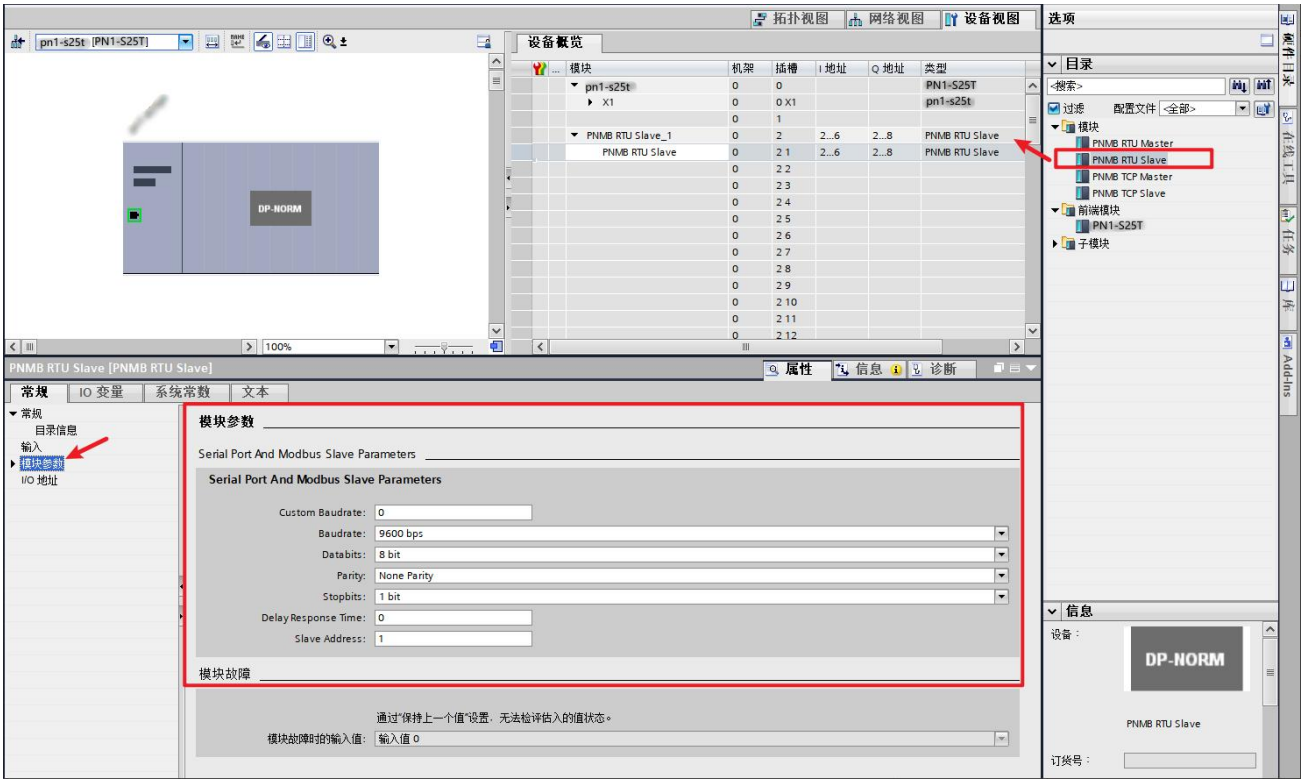
Data frame break time: 0-65535ms, 0 indicates automatic frame break, default: 0.

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

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

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

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.

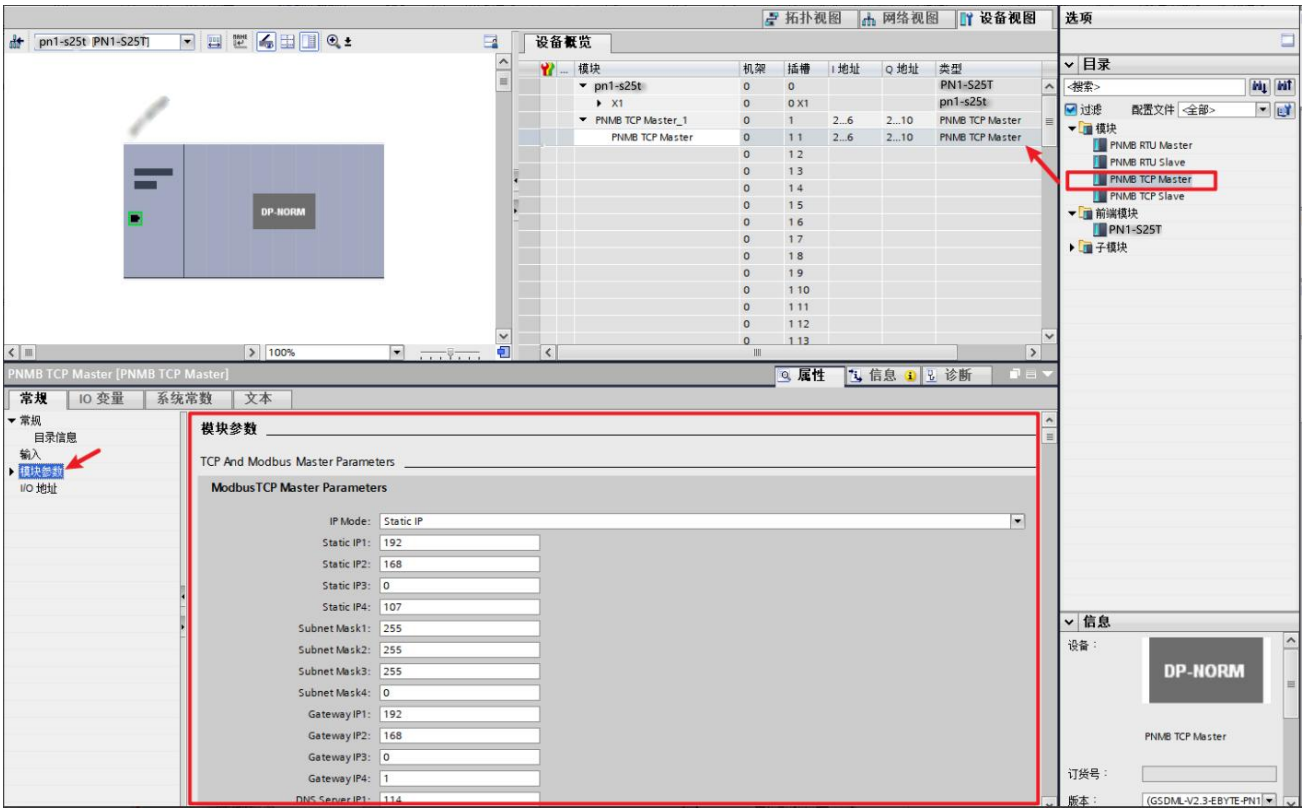
Parity:
Data validation: None Parity, Odd Parity, Even Parity, Default: None Parity.

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

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



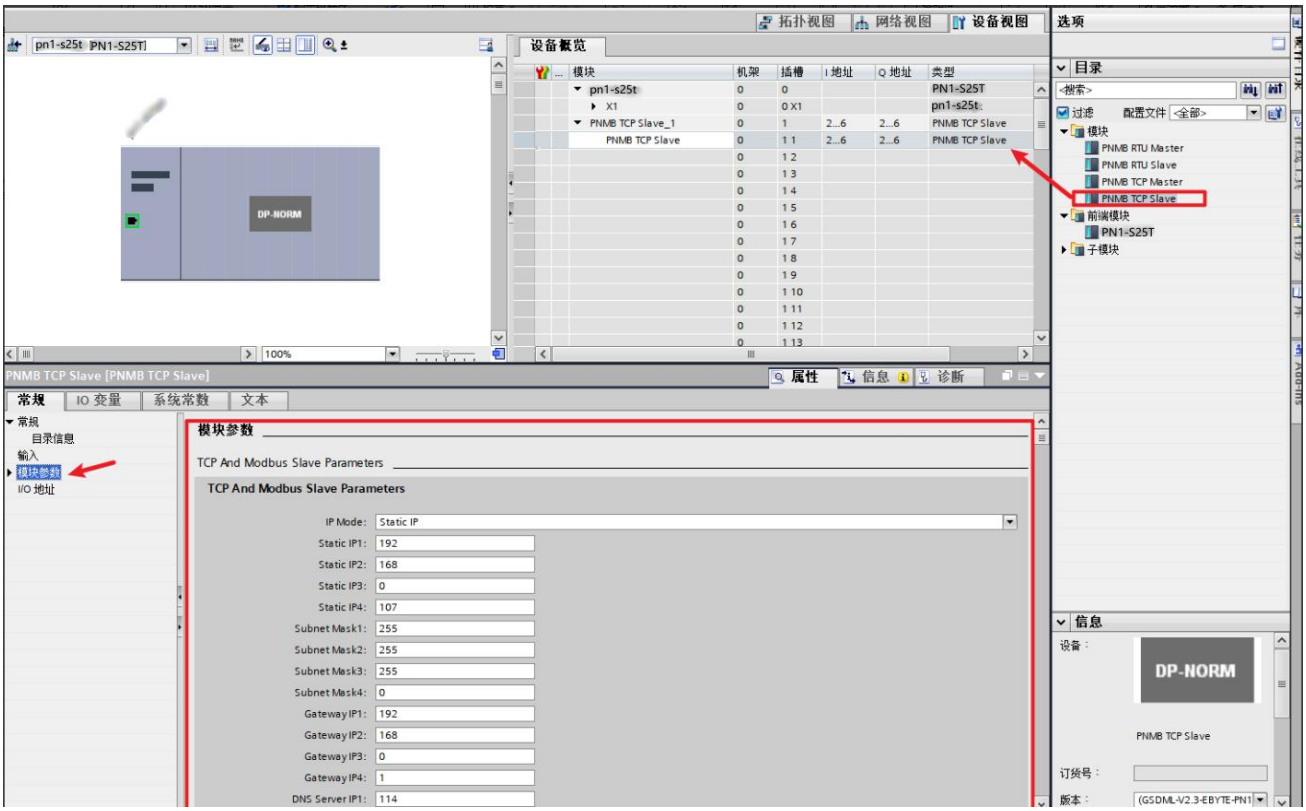
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

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.

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

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

Modbus TCP Slave



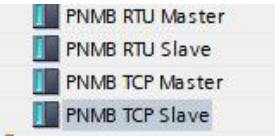
parameter	Default value/range	illustrate
IP Mode	The default value is 0; 0 = Static IP, 1 = DHCP	Modbus TCP port IP acquisition method
Static IP (1...4)	192.168.0.107	The local IP address of the gateway when acting as a TCP slave
Subnet Mask (1...4)	255.255.255.0	Subnet mask
Gateway IP (1...4)	192.168.0.1	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

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

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

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.



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



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 occur.

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

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

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

5.6.2. Modbus TCP status word and control word

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

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

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

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
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	Sub-slot 16	Sub-slot	Sub-slot 14	Sub-slot 13	Sub-slot 12	Sub-slot 11	Sub-slot 10

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

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

17		15					
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

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 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.)

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 are 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

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

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

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 Type are the same as those configured for the Modbus RTU master station.

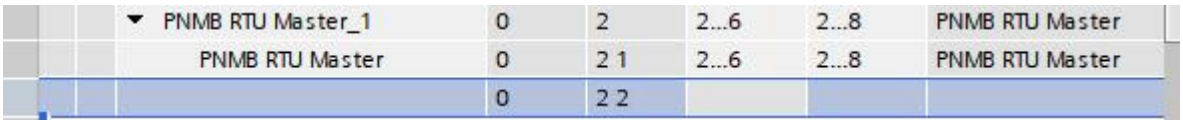
Socket Config selection (1-8): Select which socket this instruction should use.

Modbus TCP slave submodule parameters

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

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.



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.

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



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

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

5.7.2. Network socket enable 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.

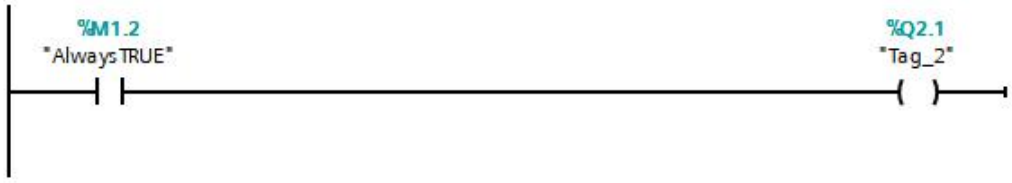
PNMB TCP Master_1	0	1	2...6	2...10	PNMB TCP Master
PNMB TCP Master	0	1 1	2...6	2...10	PNMB TCP Master

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 in B3 to 1 enables socket 1-8.

Program example: The following is a code segment that enables socket1 alone:



5.8. Use TOBTA to modify module names and query IP addresses.

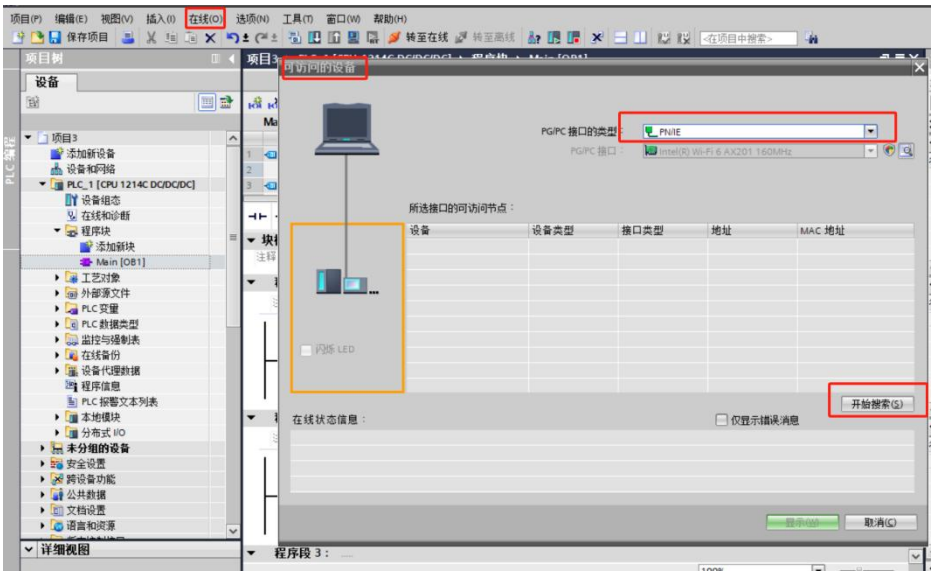
Open the TIA Portal software and click the "Online" option in the menu bar.

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 whose IP address and name you want to modify from the list.

Perform IP address and name modification operations on the selected device.



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

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

6. Tutorial on loading devices using STEP 7

6.1. Preparation before connection

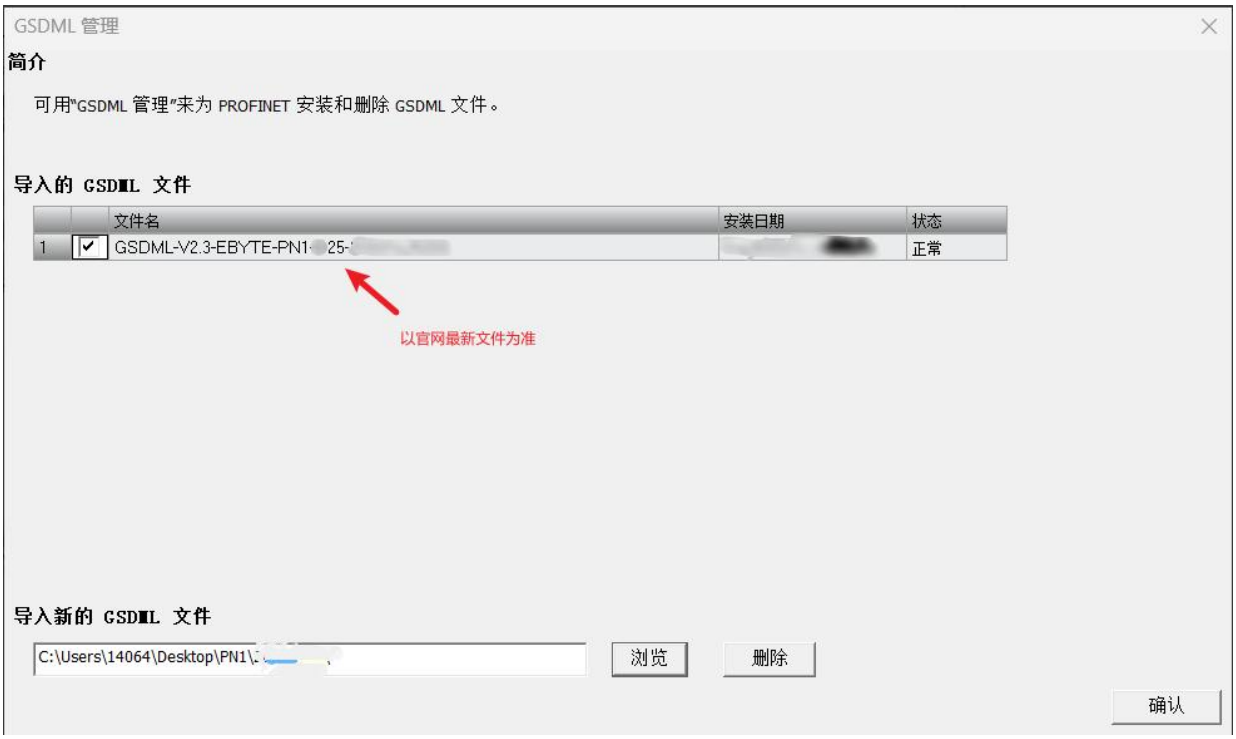
1. Prepare the necessary XML file as follows:
2. In GSDML-V2.3-EBYTE-PN1-S25T-20260414.xml, connect the DC 24V external power supply to the module and power it on. Before powering on, please check that the positive and negative terminals of the power supply are connected correctly.
3. Connect the module to the Profinet interface of the PLC controller using a network cable. (Within 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.

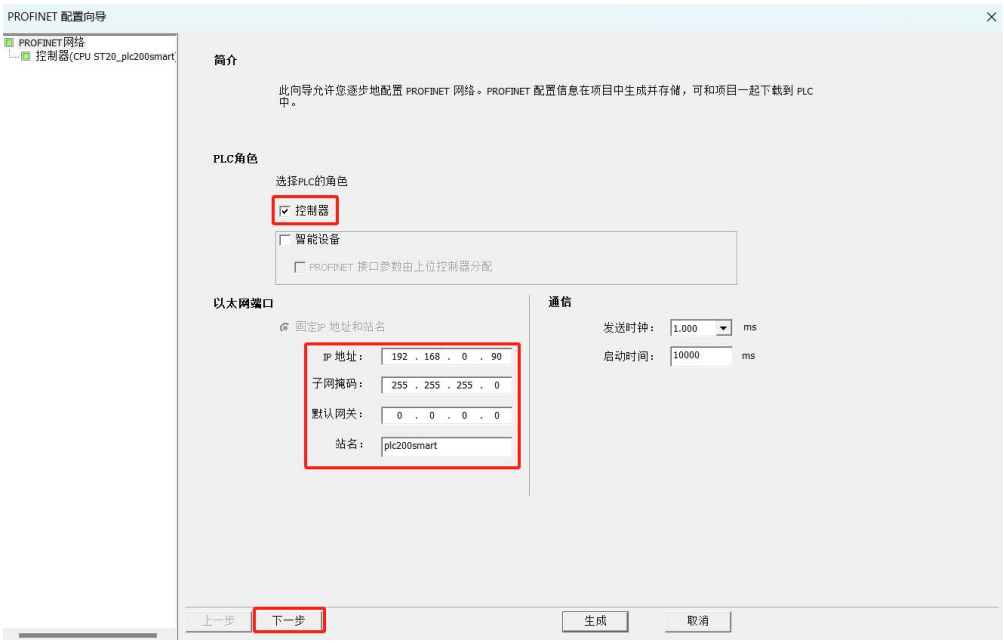
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.3. Add Profinet device to project

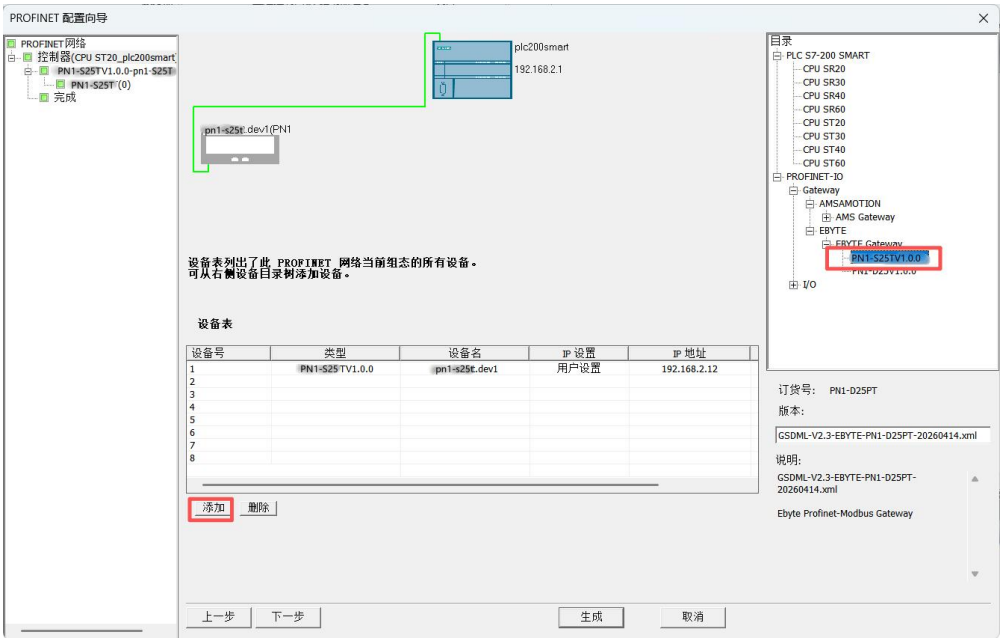
1. Select the PROFINET command under the Tools menu.



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-S25TV1.0.0, then hold down the left mouse button and drag it into the table on the left.

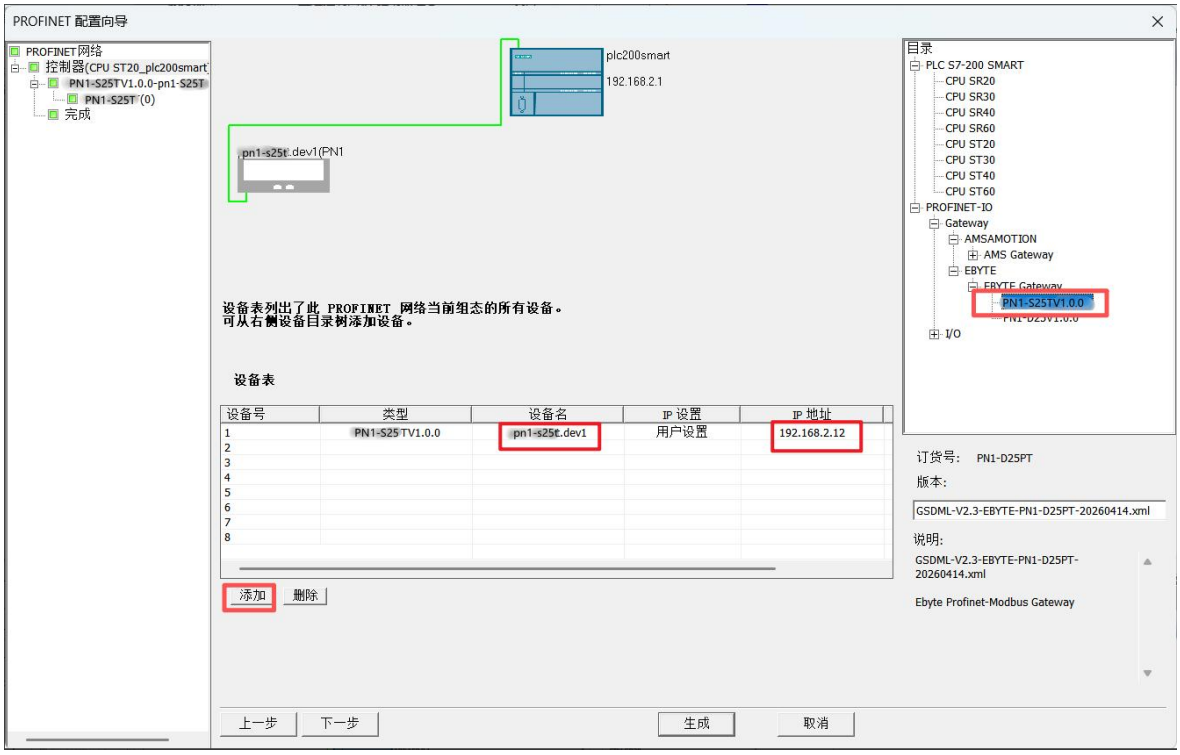


Copyright © 2012–2026 , Chengdu Ebyte Electronic Technology Co., Ltd.

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-S25T device; and through control words, the PLC can control the PN1-S25T device.

Modbus serial communication interface parameters for PN1-S25T 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.

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.

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

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

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.

Parity:

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

Stopbit:

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

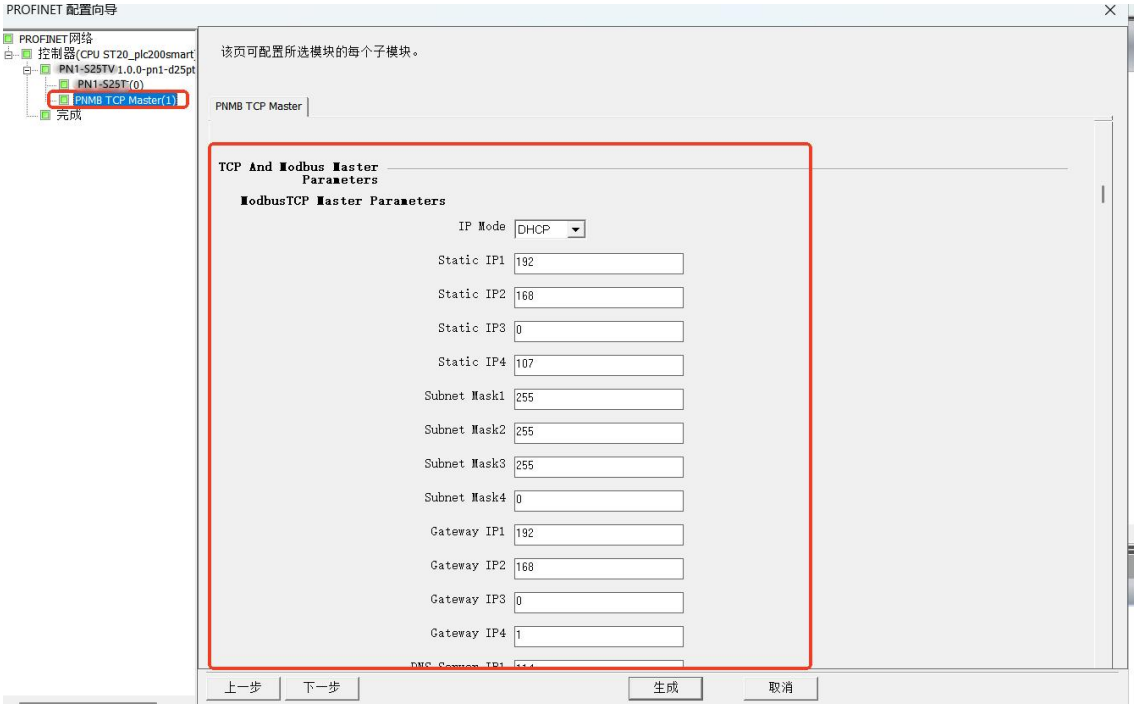
Delay Response Time.

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.

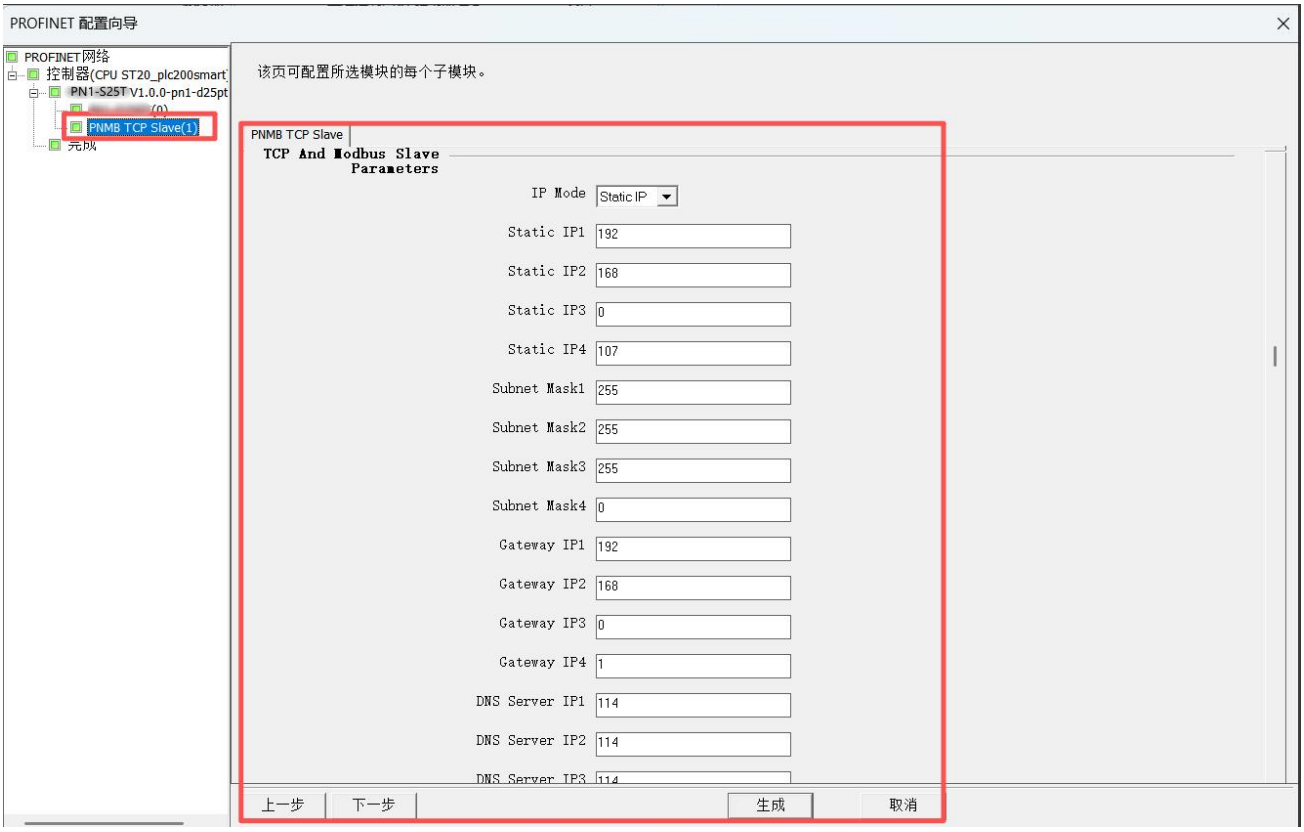
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

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.

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

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

Modbus TCP Slave



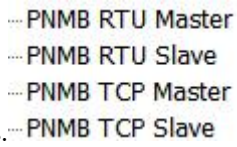
parameter	Default value/range	illustrate
IP Mode	The default value is 0; 0 = Static IP, 1 = DHCP	Modbus TCP port IP acquisition method
Static IP (1...4)	192.168.0.107	The local IP address of the gateway when acting as a TCP slave
Subnet Mask (1...4)	255.255.255.0	Subnet mask
Gateway IP (1...4)	192.168.0.1	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

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

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

6.5. 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 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-S25T		0		
2		–		X1	0 32768		
3		–		X1 P1	0 32769		
4		1	PNMB TCP Slave		1	128	5
5		–			1 2		

As shown in the figure, the corresponding PROFINET input addresses IB128-IB132 (can be modified) are the communication status monitoring words. In the Q address column, the corresponding...

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
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.

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

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

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

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

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
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
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

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

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

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.)

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

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

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

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

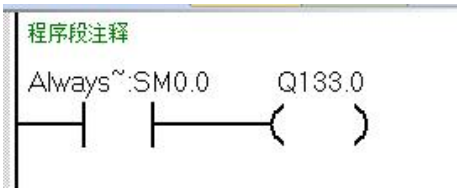
The parameters are similar to those of the Modbus RTU slave submodule.

6.5.1. Serial port enable routine

Query control word



Enable the serial port

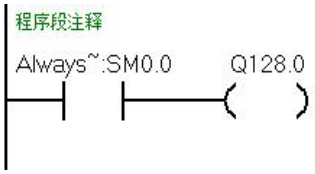


6.5.2. Network socket enable routine

Query control word



Enable socket1



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

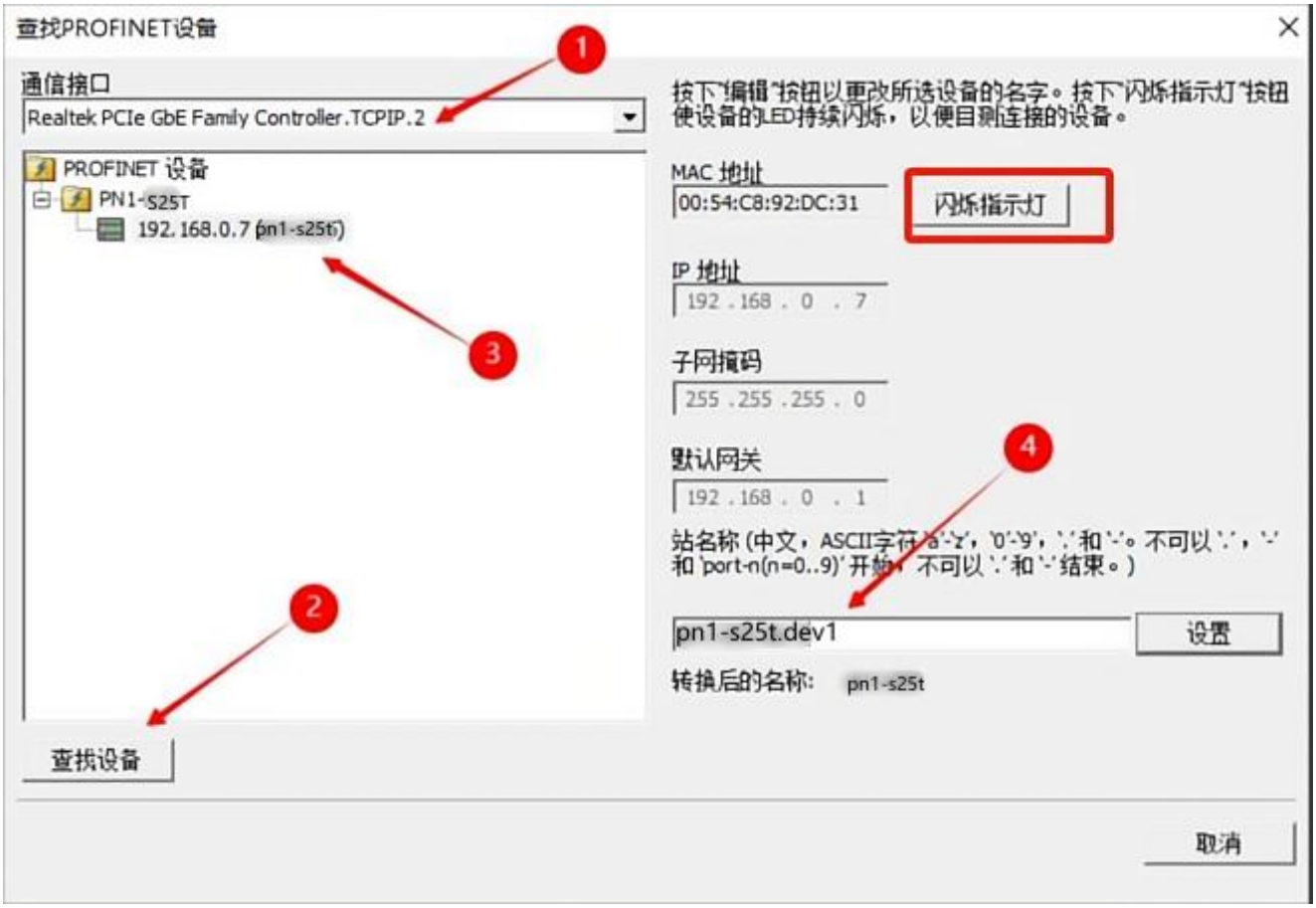
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.6. Use 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;



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

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 "Modify Module Name and Query 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 (absence log) 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

8. Important Announcement

- Ebitech reserves the right to the final interpretation and modification of all contents in this manual.
- As the hardware and software of the product continue to improve, this instruction manual may be subject to change without notice. The latest version of the instruction manual shall prevail.
- Users of this product should visit the official website to follow product updates so that they can get the latest information about the product in a timely manner.
- This product is strictly prohibited from use in military and life-safety related scenarios. The user shall be solely responsible for any consequences arising from unauthorized use.

9. Revision History

Version	Revision Date	Revision Notes	maintainer
1.0	2026-8-14	Initial version	LT

10. Contact 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

---

Official hotline:028-61399028

Web: www.cdebyte.com

Address: B2, Mould Industrial Park, 199# Xiqu Ave, High-tech Zone, Chengdu, 611731, Sichuan, China

成都亿佰特电子科技有限公司
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