

Wireless Modem

用户使用手册



Profinet 转 Modbus TCP/RTU 网关贴片模块 PN1-S25T&PN1-S25T-TB

本说明书可能会随着产品的改进而更新，请以最新版的说明书为准
成都亿佰特电子科技有限公司保留对本说明中所有内容的最终解释权及修改权

目录

第一章 产品概述	1
1.1 产品简介	1
1.2 功能特点	1
第二章 技术参数	2
2.1 产品型号列表	2
2.2 规格参数	2
2.3 尺寸图	4
2.4 引脚定义	5
2.5 硬件参考设计	8
2.5.1. 典型应用参考连接	8
2.5.2. 电源电路参考硬件连接	9
2.5.3. 1.8V 串口电路参考连接 3.3V	10
2.5.4. 5V 串口电路参考连接	10
2.5.5. 网口内置变压器参考连接	10
2.5.6. 网口外置变压器参考连接	12
2.5.7. 复位电路参考连接	13
2.5.8. 看门狗电路参考连接	14
第三章 产品功能介绍	15
3.1 PN1-S25T 系列功能综述	15
3.2 修改 IP 地址	15
3.3 Profinet 转串口功能	15
3.4 升级功能教程	17
第四章 设备报警信息说明	18
第五章 使用博图加载设备教程	19
5.1 连接前准备	19
5.2 博图添加 GSDML 文件	19
5.3 项目添加 Profinet 设备	20
5.4 配置 Modbus 通讯参数	23
5.5 PN1-S25T 设备模块 Modbus 通讯接口参数:	24
5.6 配置 Modbus 状态字和控制字	29
5.6.1. Modbus RTU 状态字和控制字	29
5.6.2. Modbus TCP 状态字和控制字	30
5.7 子模块参数说明	31
5.7.1. 串口使能例程	32
5.7.2. 网口 socket 使能例程	33
5.8 使用博图修改模块名称和查询 IP 地址	33
第六章 使用 STEP 7 加载设备教程	35
6.1 连接前准备	35
6.2 STEP 7 添加 GSDML 文件	35
6.3 项目添加 Profinet 设备	36
6.4 配置 Modbus 通讯参数	38
6.5 配置 Modbus 状态字和控制字	41

6.5.1. 串口使能例程	45
6.5.2. 网口 socket 使能例程	45
6.6 使用 STEP 7 修改模块名称和查询 IP 地址	46
第七章 注意事项	47
第八章 重要声明	48
修订历史	48
关于我们	48

第一章 产品概述

1.1 产品简介

PN1-S25T，一款专为工业通信设计的 Profinet 转 Modbus TCP/RTU 网关模组。用于将 Modbus 数据映射到 Profinet。使用 GSD 文件进行集成，免代码读取、写入 Modbus 设备，可以快速设置数据并将其传输到 PLC 中。所有 Modbus 命令以模块形式加载，Profinet、Modbus 间的内存映射关系直观，可在 STEP 7 或博途软件中查询。可加载状态字节查询 Modbus 设备的连接状态，实时监控设备状态。

产品采用 1.27mm 邮票孔封装，体积小，方便用户集成到系统中。

PN1-S25T-TB 测试套件自带 Type-C 接口支持供电，具备 1 路 RS485 独立串口与 2 个网口（Profinet 网口+Modbus TCP 网口），满足多样通信需求。所有 LED 灯、功能引脚、复位引脚均引出；复位引脚外接按键方便操作，同时也将运作状态指示引脚外接 LED 方便用户观察状态。



1.2 功能特点

- 采用标准 Profinet 协议通讯，可与 PLC、组态、上位机等进行组网
- 支持西门子 PLC 200/300/1200/1500 全系列
- 支持博图/SETP 7 上位机组态
- Profinet 和 Modbus TCP/RTU 协议转换，可作为 Modbus TCP/RTU 从站或 Modbus TCP/RTU 主站使用
- Modbus TCP 模式下共支持 8 个 Socket，主站时可同时连接 8 个从站，从站时支持 8 个主机同时连接
- 支持 2 个以太网接口，交叉直连自适应
- 工业级设计，带金属屏蔽罩
- 支持 3.3V 供电
- 1.27mm 邮票孔封装，体积小
- 支持 Profinet 转串口透传
- 直接提供 GSD 文件，简便的配置，无需上位机
- 支持固件升级功能
- 广泛用于工业现场 Modbus RTU 设备的采集和控制

第二章 技术参数

2.1 产品型号列表

产品型号	类型
PN1-S25T	贴片模组
PN1-S25T-TB	测试套件（内置 PN1-S25T）

2.2 规格参数

PN1-S25T		
类别	名称	参数
电源	工作电压	DC 3.3V±0.3V
	工作电流	峰值电流：207mA 工作电流：176mA 待机电流：175mA
	通讯电平	3.3V
封装	封装	1.27mm 邮票孔
Profinet 网络参数	通讯协议	标准 Profinet 协议（RT）
	最高通讯周期	4ms
	通讯带宽	10/100M 自适应
Modbus TCP 网络参数	通讯协议	Modbus TCP
	最小通信周期	10ms
	通信带宽	100Mbps
串口参数	通讯协议	标准 Modbus RTU 协议
	波特率	1200 ~ 3.9M bps
	通讯格式	数据位：7/8 Bits（默认 8） 停止位：1/2 Bits（默认 1） 校验：None/Odd/Even（默认 None）
工作环境	工作温湿度	-40 ~ +85℃、5% ~ 95%RH（无凝露）
	存储温湿度	-40 ~ +105℃、5% ~ 95%RH（无凝露）
其他	产品尺寸	27.0mm * 27.0mm * 3.0mm (长*宽*高)
	产品重量	4 ± 1 g

PN1-S25T-TB		
类别	名称	参数
电源	工作电压	DC 5V±0.5V
	通讯电平	5V
Profinet 网络参数	通讯协议	标准 Profinet 协议 (RT)
	最高通讯周期	4ms
	通讯带宽	10/100M 自适应
Modbus TCP 网络参数	通讯协议	Modbus TCP
	最小通信周期	10ms
	通信带宽	100Mbps
串口参数	通讯协议	标准 Modbus RTU 协议
	波特率	1200 ~ 3.9M bps
	通讯格式	数据位: 7/8 Bits (默认 8) 停止位: 1/2 Bits (默认 1) 校验: None/Odd/Even (默认 None)
工作环境	工作温湿度	-40 ~ +85℃、5% ~ 95%RH (无凝露)
	存储温湿度	-40 ~ +105℃、5% ~ 95%RH (无凝露)
其他	产品尺寸	100mm * 44mm * 16.5mm (长*宽*高)
	产品重量	40 ± 5 g

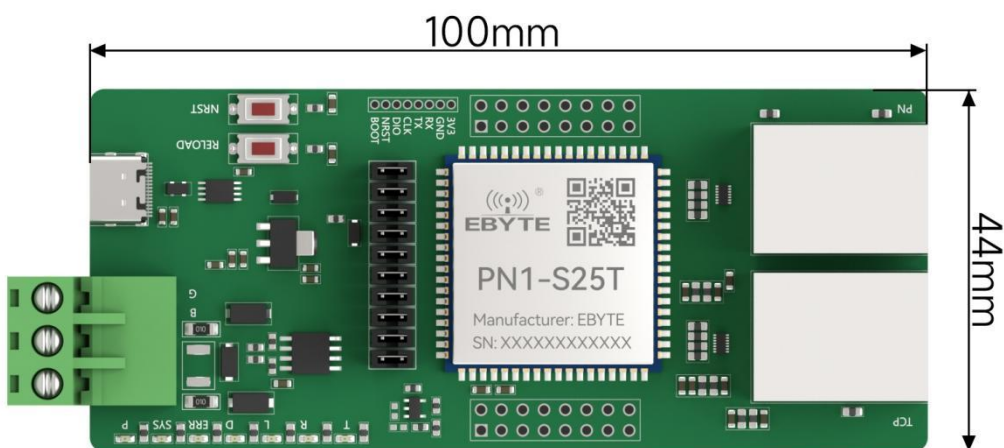
2.3 尺寸图

PN1-S25T:



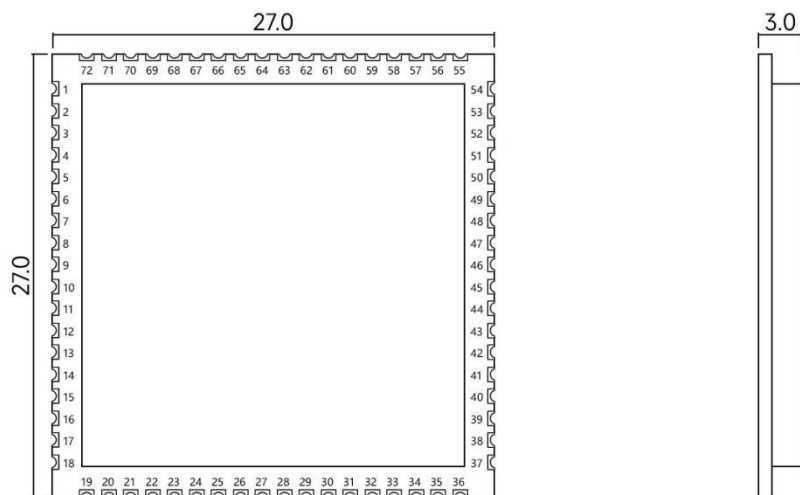
27.0mm * 27.0mm * 3.0mm (长*宽*高)

PN1-S25T-TB:



100mm * 44mm * 16.5mm (长*宽*高)

2.4 引脚定义



Top pad : 0.50
0.80 1.00

Bottom pad : 1.75
0.80 1.50

Unit : mm
Pad quantity : 72
Tolerance value : X.X±0.2mm
X.XX±0.05mm

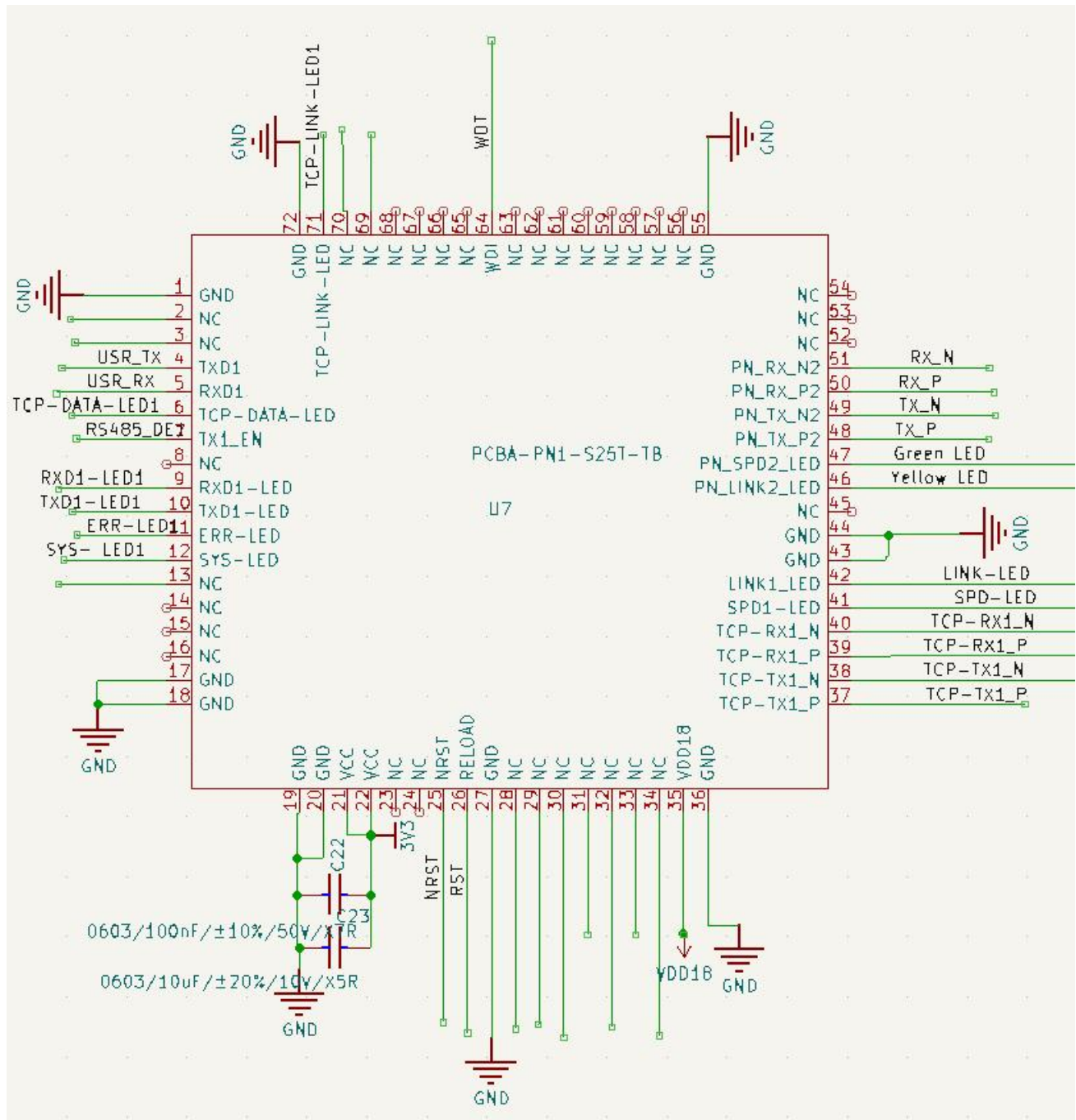
序号	PN1-S25T Pin name	PN1-S25T-TB 丝印(详见实物)	描述
1	GND	GND	公共接地端，电源负端输入
2	NC	NC	悬空
3	NC	NC	悬空
4	TXD1	485-RXD	串口发送数据，TTL 电平通讯电压仅支持 3.3V
5	RXD1	485-TXD	串口接收数据，TTL 电平通讯电压仅支持 3.3V
6	TCP_DATA-LED	TCP_D-LED	TCP 通讯数据交互指示灯，有数据交互时闪烁
7	TX1_EN	TX1_EN	串口 1_EN 使能，串口默认工作在全双工模式，如外接 485 芯片，则该引脚外接 1k 下拉电阻，引脚功能变为 RS485 使能控制引脚，串口发送数据时置高，常态为低；
8	NC	NC	悬空
9	RXD1_LED	RXD1_LED	串口 1 有数据接收时快闪，默认输出高电平，接收数据时输出 10Hz 方波
10	TXD1_LED	TXD1_LED	串口 1 有数据发送时快闪，默认输出高电平，发送数据时输出 10Hz 方波
11	ERR_LED	ERR_LED	(Modbus) 通讯错误指示灯 拉低：Modbus 通讯异常；

			置高：Modbus 通讯正常； 软件控制闪烁指示灯时，与 SYS 同时闪烁
12	SYS_LED	SYS_LED	系统（PN 连接）灯 拉低：Profinet 建立连接 置高：Profinet 未建立连接 软件控制闪烁指示灯时，与 ERR 同时闪烁
13	NC	NC	悬空
14	NC	NC	悬空
15	NC	NC	悬空
16	NC	NC	悬空
17	GND	GND	公共接地端，电源负端输入
18	GND	GND	公共接地端，电源负端输入
19	GND	GND	公共接地端，电源负端输入
20	GND	GND	公共接地端，电源负端输入
21	VCC	VCC	电源正输入，支持 3.3V 输入
22	VCC	VCC	电源正输入，支持 3.3V 输入
23	NC	NC	悬空
24	NC	NC	悬空
25	NRST	NRST	默认内部拉高，拉低进行重启；
26	RELOAD	RELOAD	恢复出厂引脚，内部弱上拉，可外接复位按键，低电平持续 5~10s 左右恢复出厂设置；
27	GND	GND	公共接地端，电源负端输入
28	NC	NC	悬空
29	NC	NC	悬空
30	NC	NC	悬空
31	NC	NC	悬空
32	NC	NC	悬空
33	NC	NC	悬空
34	NC	NC	悬空
35	VDD18	VDD18	输出电压 1.8V，仅供给 Modbus TCP 以太网口变压器上拉
36	GND	GND	公共接地端，电源负端输入
37	TCP_TX1_P	TCP_TX1_P	Modbus TCP 以太网口发送 TX+ 信号
38	TCP_TX1_N	TCP_TX1_N	Modbus TCP 以太网口发送 TX- 信号
39	TCP_RX1_P	TCP_RX1_P	Modbus TCP 以太网口接收 RX+ 信号
40	TCP_RX1_N	TCP_RX1_N	Modbus TCP 以太网口接收 RX- 信号
41	SPD1-LED	SPD1-LED	Modbus TCP 以太网口速度指示灯。用于指示当前网络连接的速率状态
42	LINK1_LED	LINK1_LED	Modbus TCP 以太网口链路指示灯。指示物理链路连接状态。 常亮：表示网线已正确连接 闪烁：通常表示链路已建立，并且有数据正在发送或接收

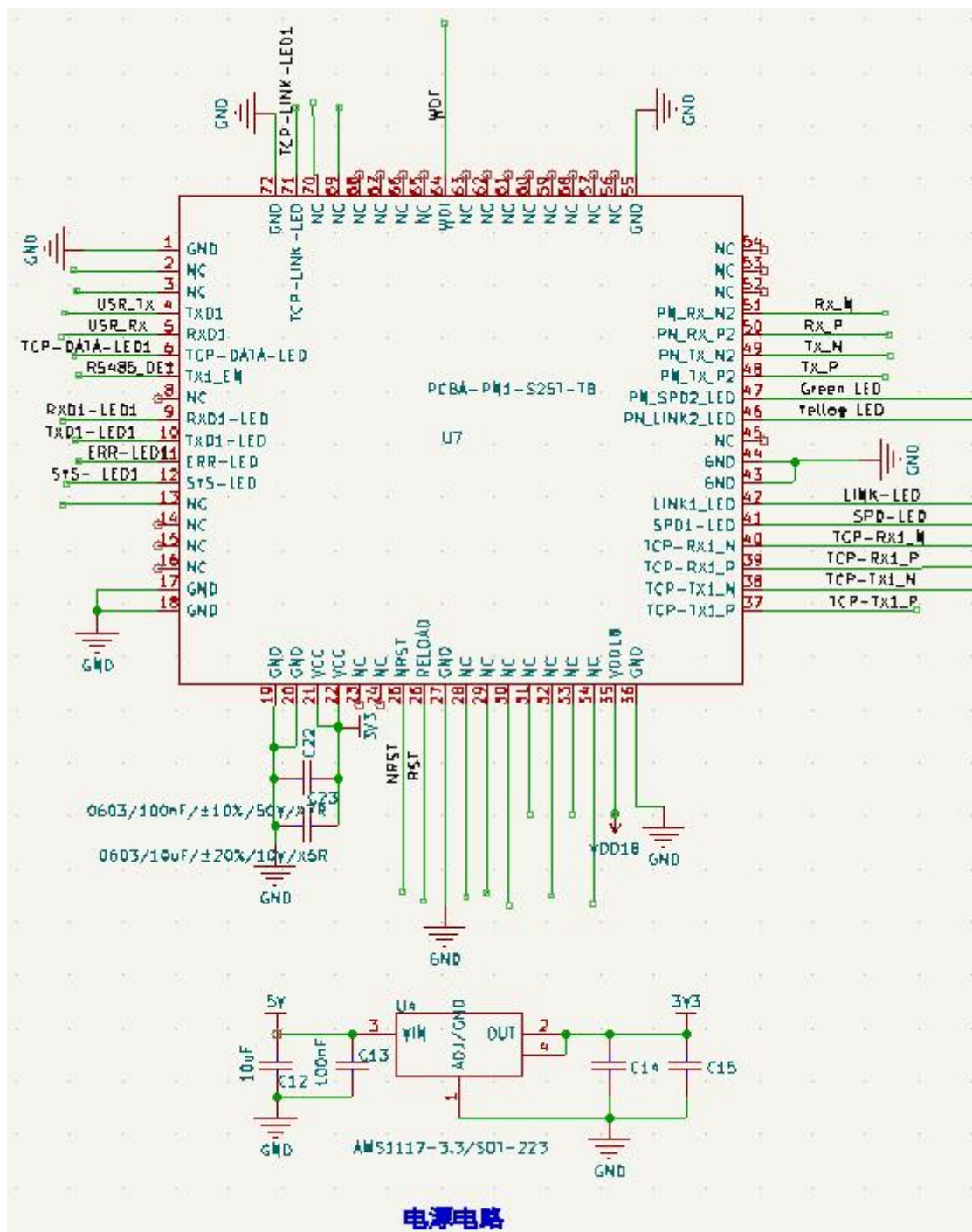
			熄灭：表示无链路。
43	GND	GND	公共接地端，电源负端输入
44	GND	GND	公共接地端，电源负端输入
45	NC	NC	悬空
46	PN_LINK2_LED	PN_LINK2_LED	Profinet 以太网 10M PHY 指示灯，PHY 协商成功后拉低，有数据收发时闪烁；
47	PN_SPD2_LED	PN_SPD2_LED	Profinet 以太网 100M PHY 指示灯，PHY 协商成功后拉低，有数据收发时闪烁；
48	PN_TX_P2	PN_RX_P2	Profinet 以太网口接收 TX+信号
49	PN_TX_N2	PN_TX_N2	Profinet 以太网口发送 TX-信号
50	PN_RX_P2	PN_RX_P2	Profinet 以太网口接收 RX+信号
51	PN_RX_N2	PN_RX_N2	Profinet 以太网口接收 RX-信号
52	NC	NC	悬空
53	NC	NC	悬空
54	NC	NC	悬空
55	GND	GND	公共接地端，电源负端输入
56	NC	NC	悬空
57	NC	NC	悬空
58	NC	NC	悬空
59	NC	NC	悬空
60	NC	NC	悬空
61	NC	NC	悬空
62	NC	NC	悬空
63	NC	NC	悬空
64	WDI	WDI	外部硬件看门狗喂狗信号，推挽输出。程序运行正常时会周期性翻转该引脚电平，用于给外部监控/看门狗电路提供运行心跳。
65	NC	NC	悬空
66	NC	NC	悬空
67	NC	NC	悬空
68	NC	NC	悬空
69	NC	NC	悬空
70	NC	NC	悬空
71	TCP-LINK-LED	TCP-L-LED	Modbus TCP 建立连接后常亮，无连接时常灭
72	GND	GND	公共接地端，电源负端输入

2.5 硬件参考设计

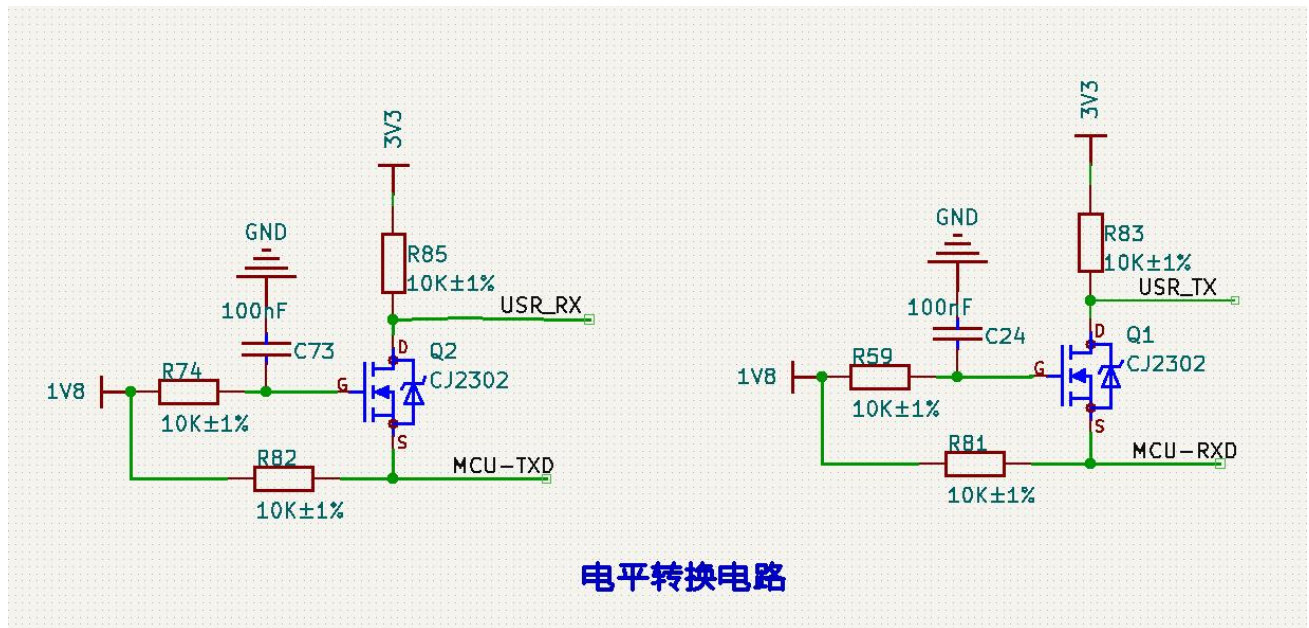
2.5.1. 典型应用参考连接



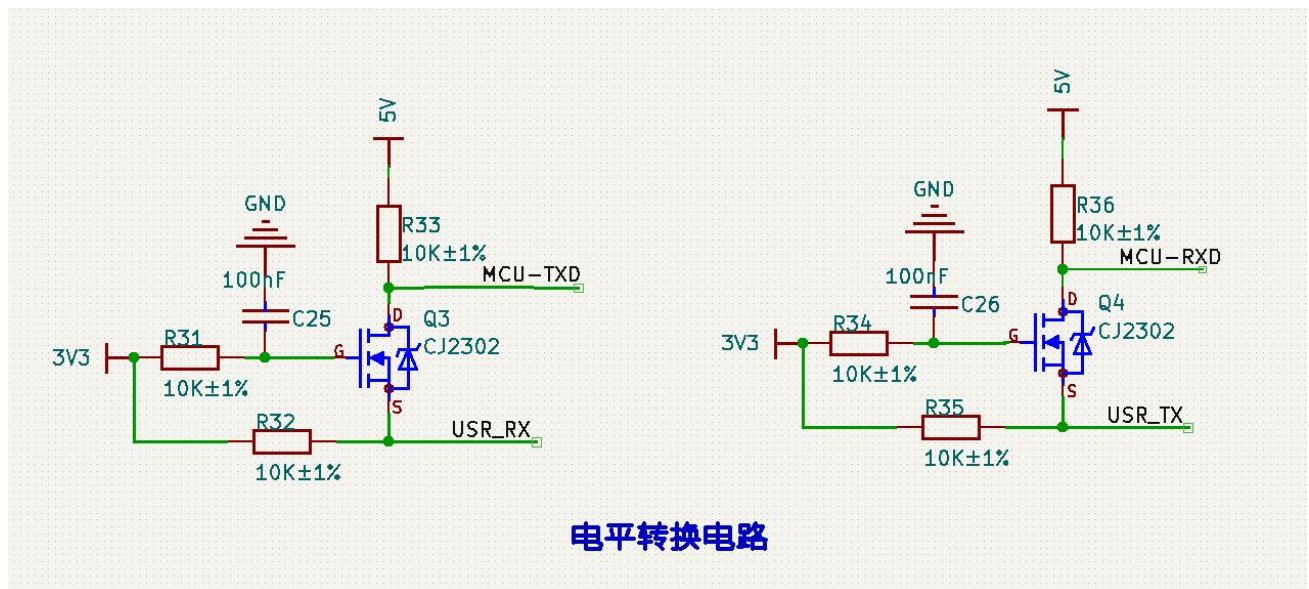
2.5.2. 电源电路参考硬件连接



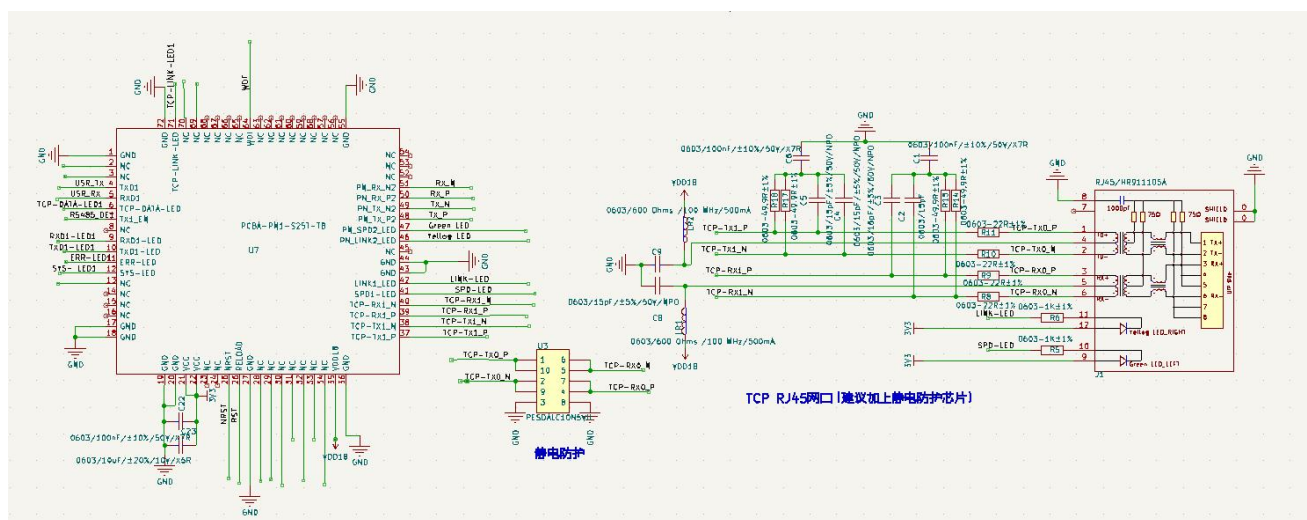
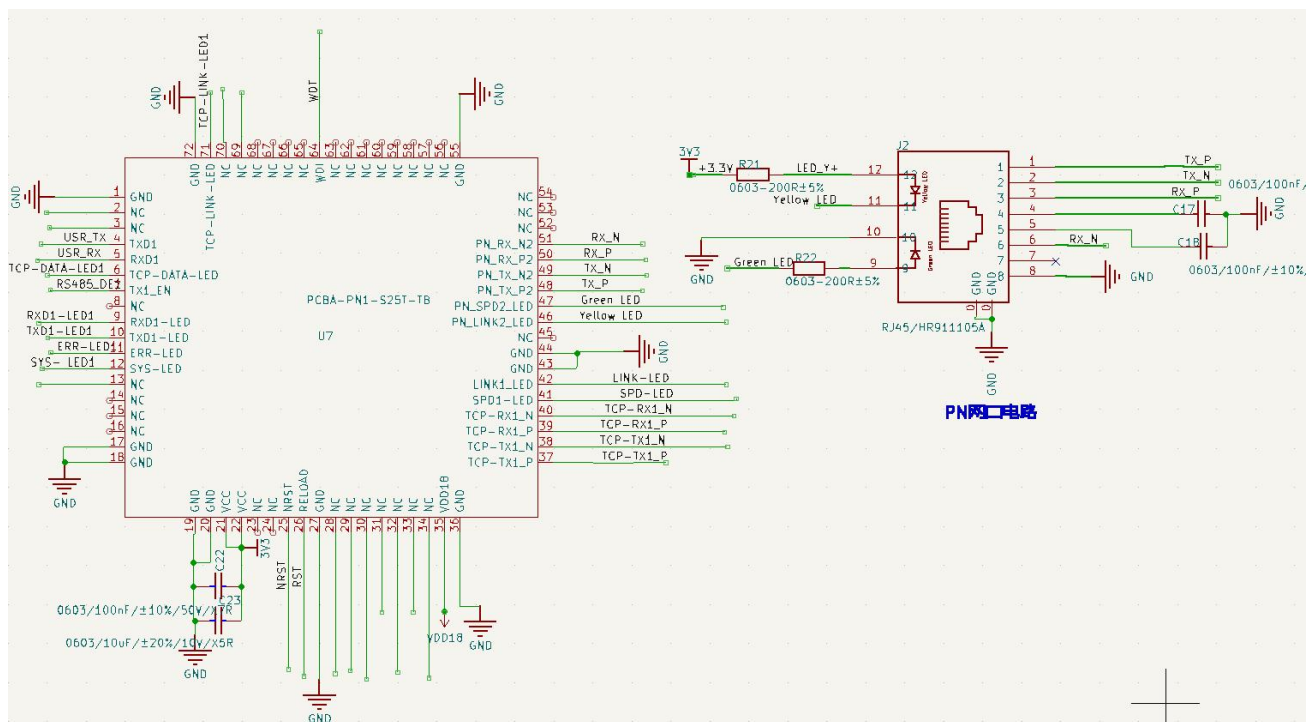
2.5.3. 1.8V 串口电路参考连接 3.3V



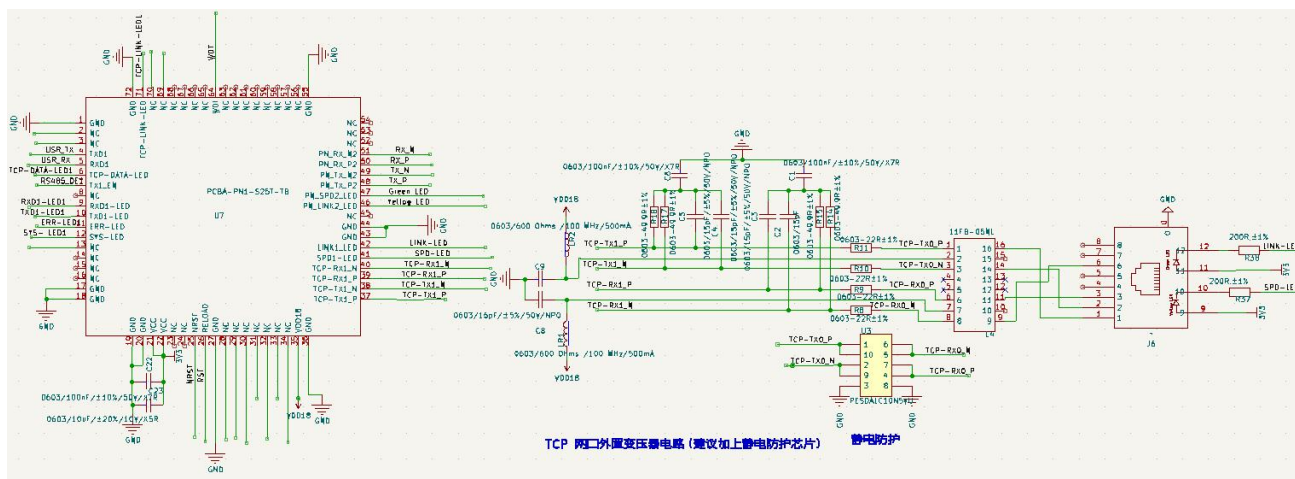
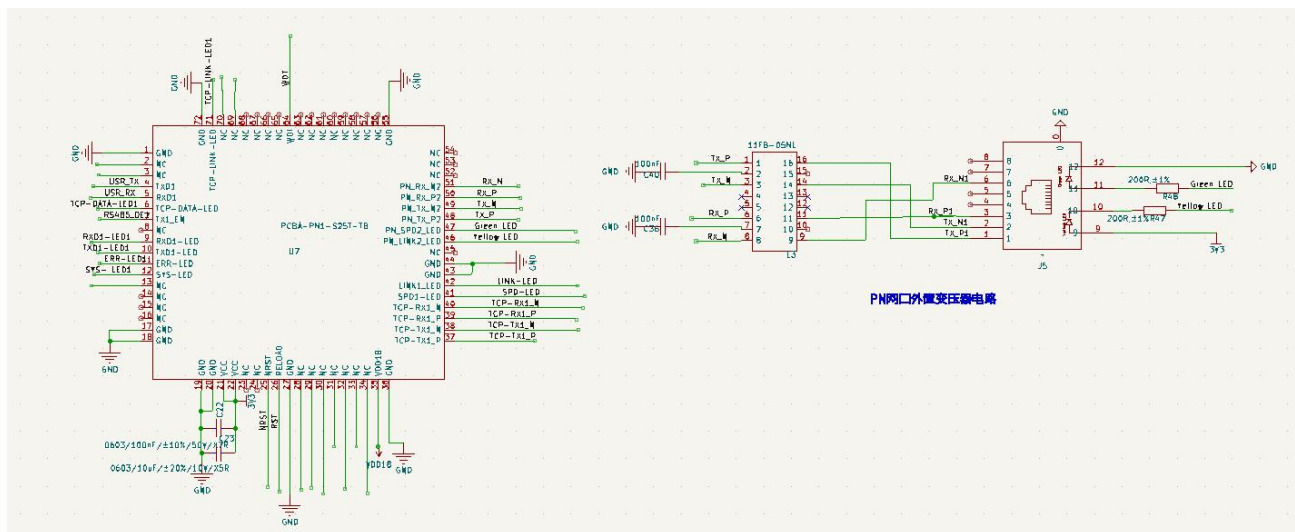
2.5.4. 5V 串口电路参考连接



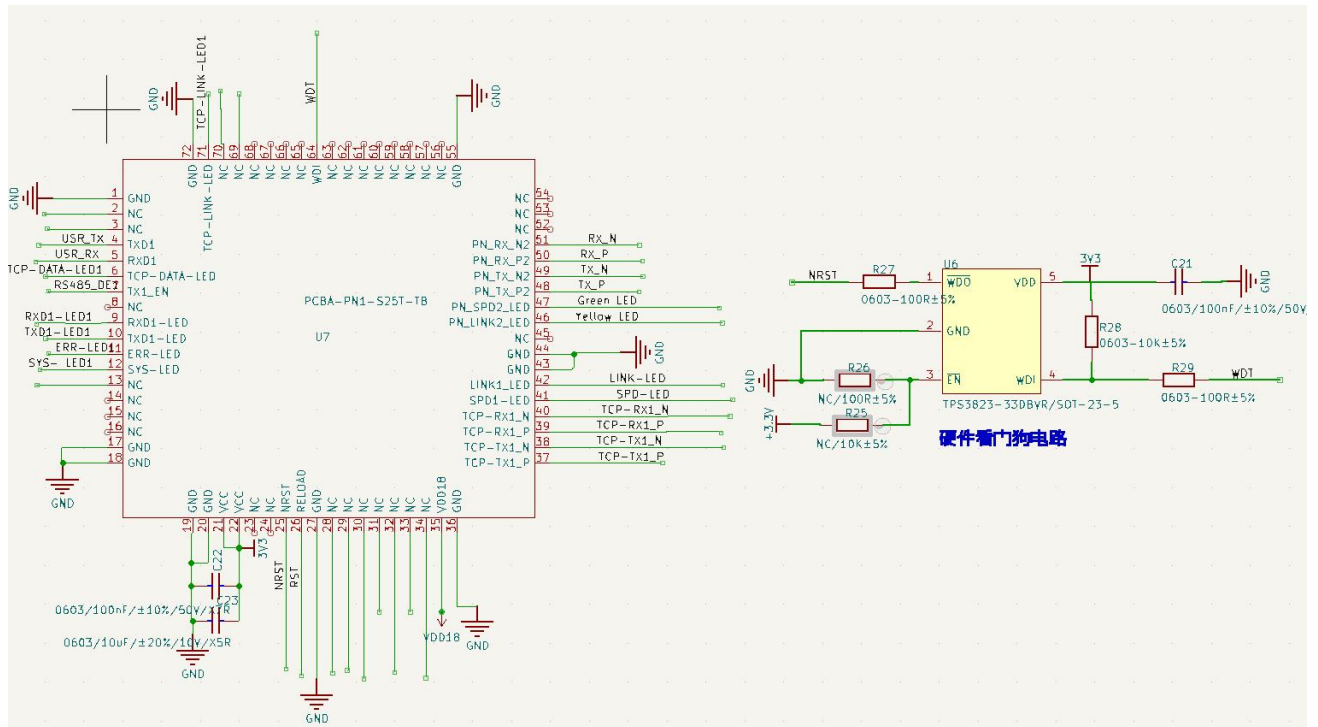
2.5.5. 网口内置变压器参考连接



2.5.6. 网口外置变压器参考连接



2.5.8. 看门狗电路参考连接



第三章 产品功能介绍

3.1 PN1-S25T 系列功能综述

本模块 Modbus 共 2 个主槽每个槽最多支持 48 个命令，命令分为主站命令和从站命令，可分别设置命令类型，长度，通讯接口。使用 Modbus 主站功能时，写功能调用不能小于轮询周期的 2 倍，不然会出现有一帧写功能数据未刷新的情况。例如 Modbus 主站有 5 个命令结点，轮训间隔为 10ms，那么全部命令结轮训完毕就得花费 50ms，则数据变化最小周期为了 $50\text{ms} * 2 = 100\text{ms}$ 。

启用 Modbus TCP 从站模式时，设备可同时接入 8 台主站设备并发访问。受主控芯片并发处理性能限制，建议合理控制各主站轮询频次，轮询速率过高易造成响应不及时，进而引发数据丢包、主站通讯异常报错问题。

3.2 修改 IP 地址

本模块 IP 地址可通过博图/ STEP 7 等件进行修改，详细设置方式见使用章节。

3.3 Profinet 转串口功能

PN 转串口功能支持协议透传与数据透传两种模式

协议透传：

发送报文：0xc1+sub_slot_nbr(子槽号 1 字节)+datalength(数据部分长度，大端 2 字节)+data（数据部分，长度等于 datalength）+mb_CRC_16(两字节，可选)

接收报文：0xd2+sub_slot_nbr(子槽号 1 字节)+datalength(数据部分长度，大端 2 字节)+data（数据部分，长度等于 datalength）+mb_CRC_16(两字节，可选)

数据透传：只能配置一条，同时包含发送与接收数据

发送报文：data（n 字节）+mb_CRC_16(两字节，可选)

接收报文：data（n 字节）+mb_CRC_16(两字节，可选)

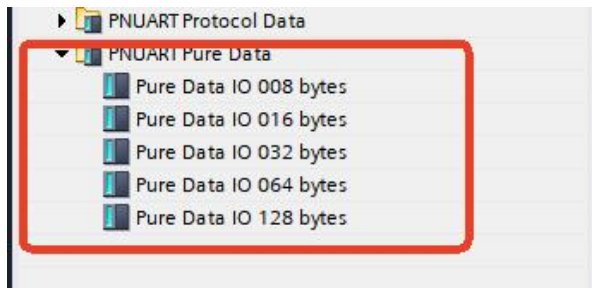
串口通讯状态 8 字节，前 4 字节用于统计串口接收总包数，后 4 字节，32 位，每个位代表某个子槽的接收状态，位状态变化(0→1 或 1→0)代表该子槽接收到数据。控制位第 1 个字节第 2 个位(bit1)置 1 时清零接收计数

1、串口以及轮询参数，大部分参考 modbus 主机参数，其中需要说明一下的是 CRC check 使能后对于发送报文会在最后追加 2 字节 modbus CRC16 校验码，对于接收报文会校验最后两个字节是否符合校验，校验成功才会更新 PLC 数据，校验失败数据丢弃，并且会在接收到数据 2ms 左右拉高 PC2（pin 17 VCT6）直到接收到正确报文才会拉低（如果需要，建议用户在发送完后 3ms 检测该引脚），且 EER 灯常亮 3 秒。默认不使能

Serial Port And UART Transparent Transmission Parameters

Custom Baudrate:	0
Baudrate:	115200 bps
Databits:	8 bit
Parity:	None Parity
Stopbits:	1 bit
CRC check:	Disable
PN Online Polling:	Disable
Poll Interval(ms):	50ms
Frame interval(ms):	0

2、数据透传模块，每个模块都支持发送与接收报文，“Actual send”可配置发送数据实际发送长度



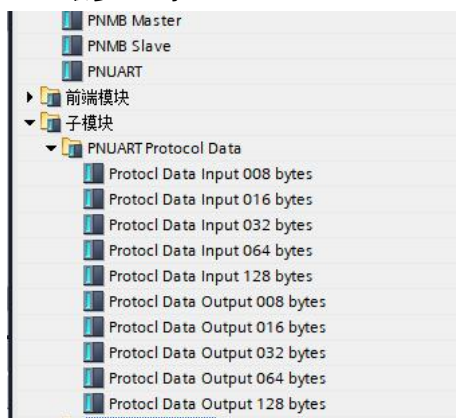
PNUART Transparent Transmission Parameters

Actual Send:	8
Trigger Type:	poll trigger

disable
poll trigger
Level trigger
Rising trigger

“Trigger type”触发模式可配置发送报文的发送触发模式，参考 PN 转 modbus，默认轮询触发“pool trigger”，其中“Level trigger”下输出数据只有在控制位置 1 且输出数据变化时才会发送

2、协议透传模式单独配置成输入或者输出模式，发送报文的参数配置与数据透传模式一致，可在子槽配置最多 48 条



PNUART Transparent Transmission Parameters

Actual Send:	16
Trigger Type:	disable

disable
poll trigger
Level trigger
Rising trigger

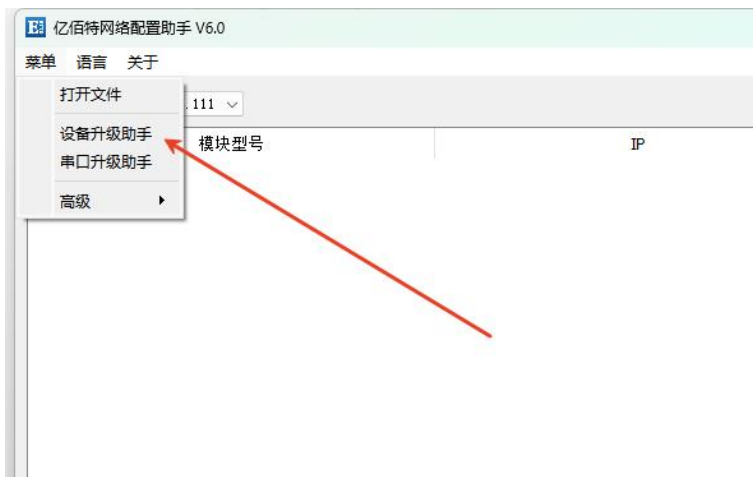
3.4 升级功能教程

支持固件升级功能，固件升级详细说明见固件升级使用说明书。

1. 先给设备断电
2. 按下“reload”按键后给设备上电（PN1-S25T 拉低 pin25）
3. 当设备“sys”灯一直闪烁则设备已进入升级模式
4. 打开“EBYTE 网络配置工具.exe”



5. 打开“设备升级助手”



6. 按照下图完成升级



第四章 设备报警信息说明

当 PN1-S25T 网关出现错误时会通过 Profinet 的报警机制，将具体出错的信息发送给 PLC，同时网关的 ERR 指示灯会亮，PLC 上的指示灯也会闪烁，当错误消失时,对应的报警信息就会被移除,ERR 指示灯熄灭。可以通过 PLC 对应的上位机来查看具体的错误信息。

下面将具体的错误信息解释如下：

错误信息	描述说明
Illegal Fun Code	从站回复 Modbus 标准错误：请求的功能未被从设备识别或不支持
Illegal Data Address	从站回复 Modbus 标准错误：数据地址不在设备的可访问范围内
Illegal Data Value	从站回复 Modbus 标准错误：请求的操作尝试设置一个无效或非法的值
Slave Device Failure	从站回复 Modbus 标准错误：从设备故障，未知的设备故障
Frame Length Error	主站接收的报文长度错误；太长，太短或与正确的从站回复数据长度不符
CRC Check Error	主站接收的报文 CRC 校验错误
Register Number Error	主站接收的报文寄存器数量错误
SLave Address Error	主站接收的报文从站地址错误
MASTER WATING RSP TIMEOUT	主站接收超时
Function Code Different	主站接收的报文中功能码与请求的不一致
Register Address Error	主站接收的报文寄存器地址错误
Unknown Error	未知错误
TCP CONNECT ERR	TCP 连接从站错误

第五章 使用博图加载设备教程

若在使用过程中出现问题，点击官网链接：<https://www.ebyte.com/product-class.aspx>

注：PN1-S25T 为贴片版本，初次使用时，建议使用测试底板（PN1-S25T-TB），本章采用 PN1-S25T-TB 作为讲解。

5.1 连接前准备

1. 准备好需要的 XML 文件，如下所示：

名称	修改日期	类型	大小
GSDML-V2.3-EBYTE-PN1	0	Microsoft Edge ...	1,904 KB

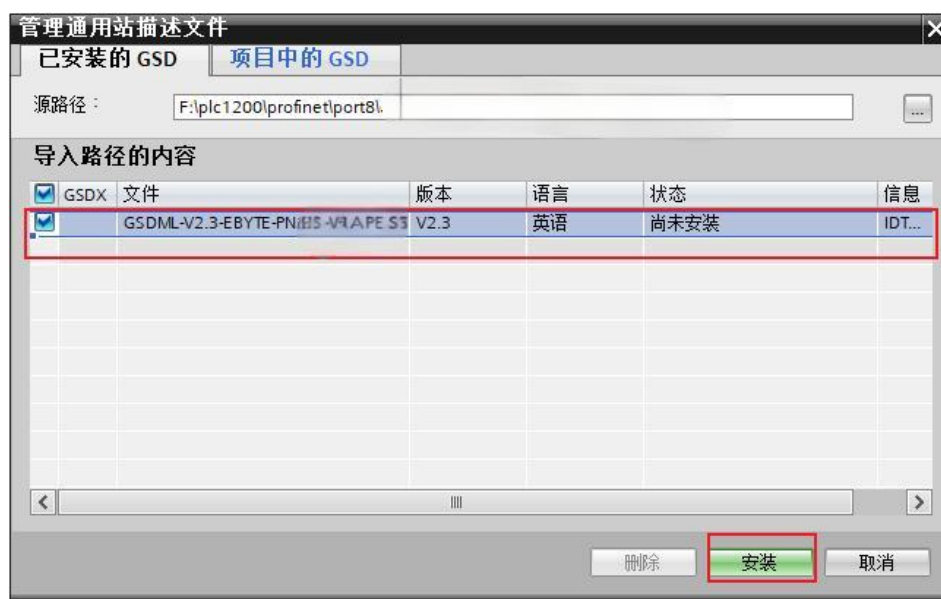
2. 将 DC 24V 外部电源接入模块并通电，通电前请检查电源正、负极是否连接正确。
3. 使用网线将模块连接到 PLC 控制器的 Profinet 接口上。（在同一个网段）

5.2 博图添加 GSDML 文件

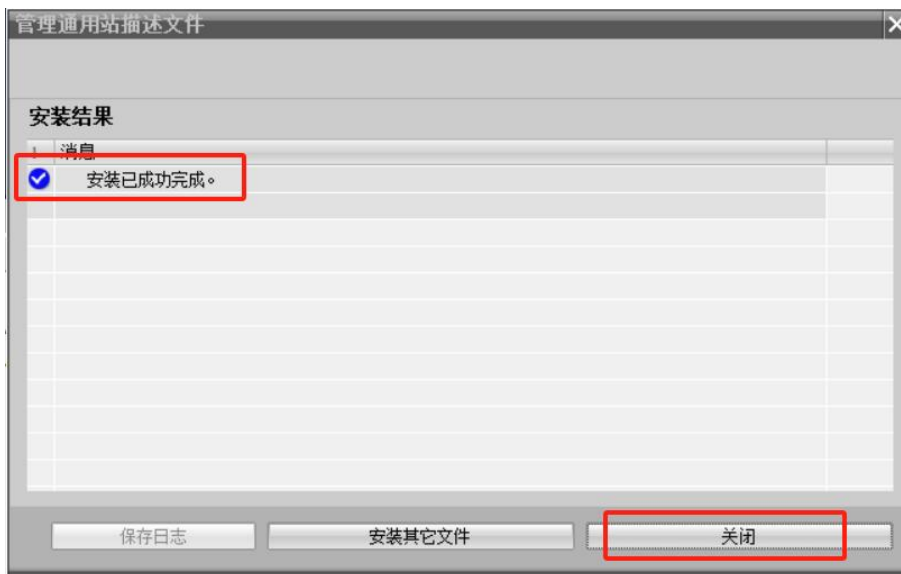
1. 打开博图，点击选项，管理通用站文件（gsd）



2. 添加 GSDML 文件，找到存放 GSD 的文件夹，选择该文件夹，然后软件自己会扫描到 GSD 文件，然后勾选该 GSD 文件，最后点击安装。

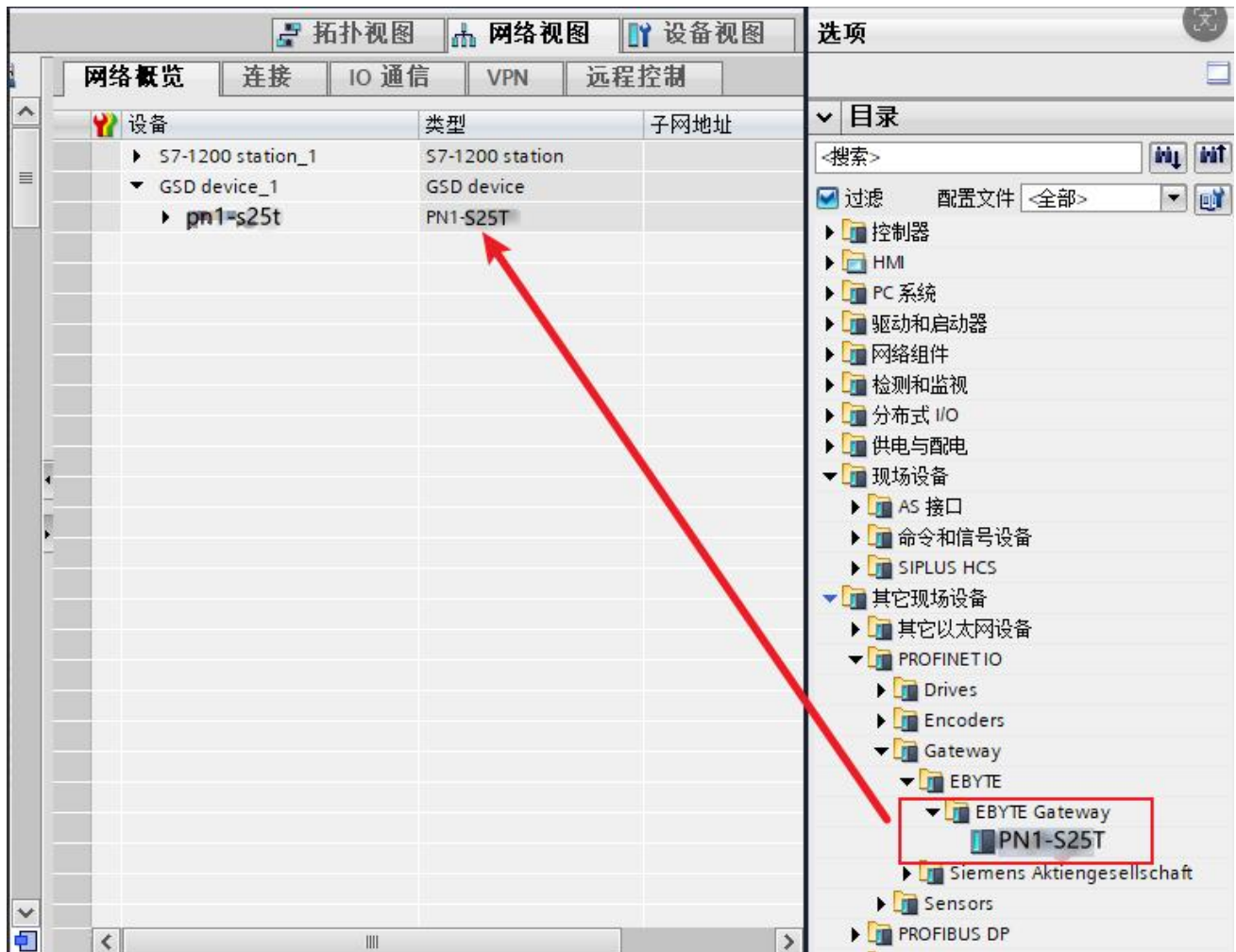


3. 安装完成后点击关闭即可，之后就可以进行设备组态了。

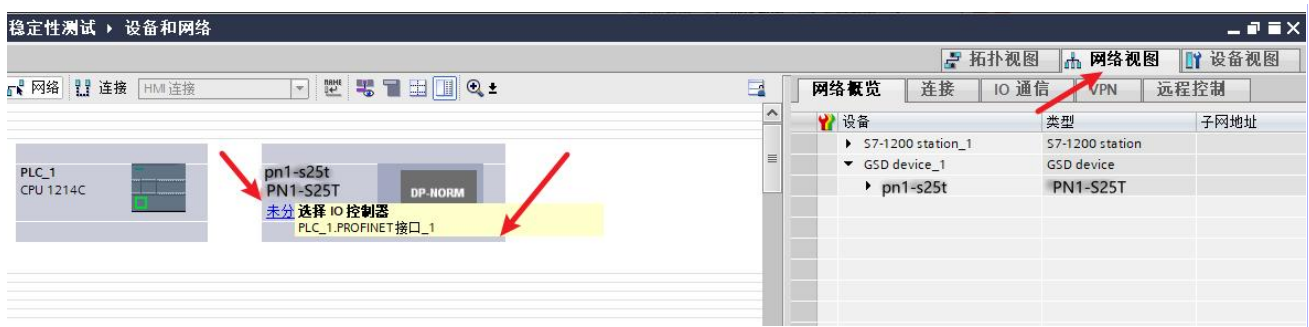


5.3 项目添加 Profinet 设备

1. 进行新建或者打开项目，如果是新建项目，先添加控制器设备，然后再设备组态界面，添加相应 IO 模块，双击该模块，即可添加成功，如图：

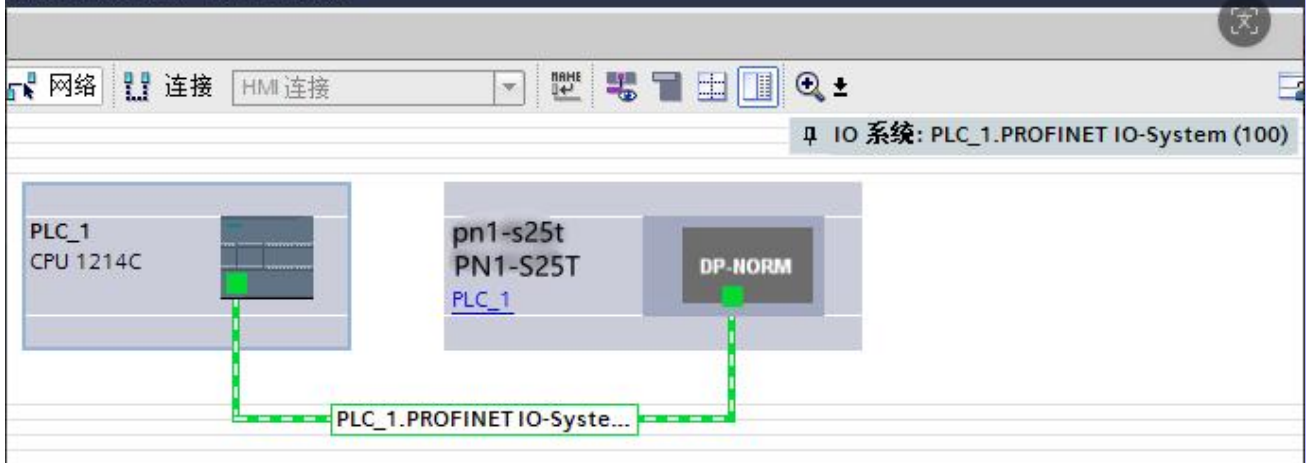


2. 在网络视图中，进行设备组态

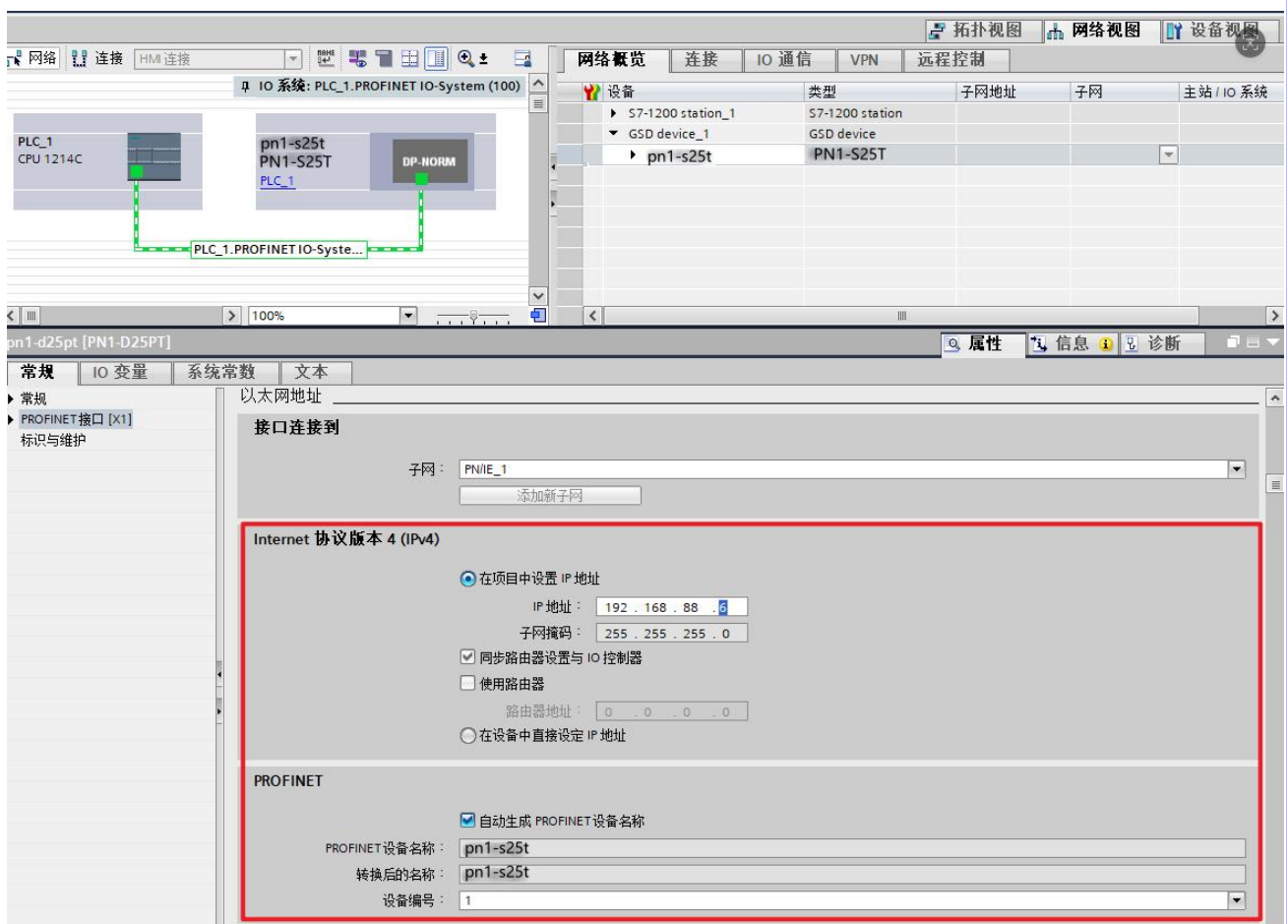


完成后，如图：

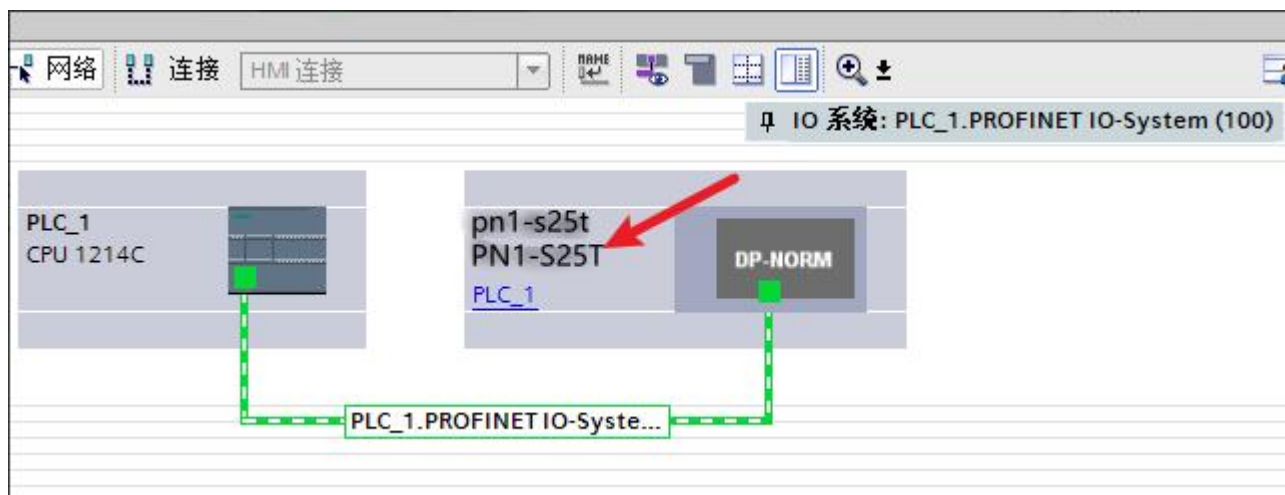
稳定性测试 ▸ 设备和网络



3. 在设备视图中，首先定位并选中新添加的设备，然后双击图中模块，接下来在常规配置界面中，对 IP 地址和设备名称进行修改，需和模块本身保持一致。或者也可以选择直接在设备上进行 IP 地址的设置。



点击此处也可直接进行设备名称修改

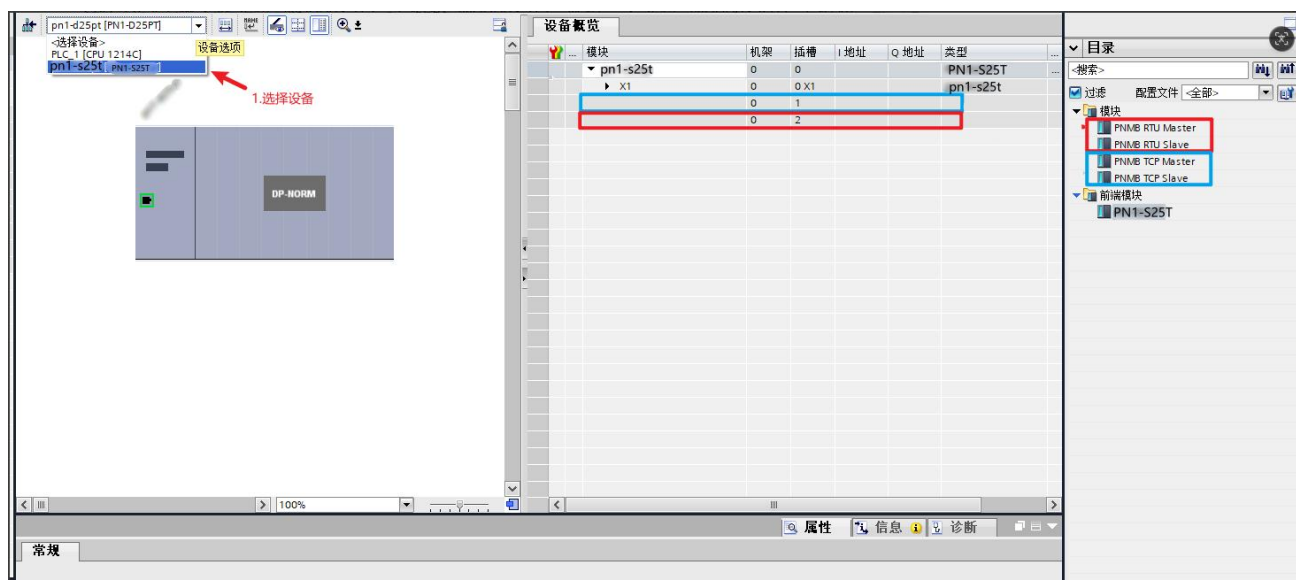


5.4 配置 Modbus 通讯参数

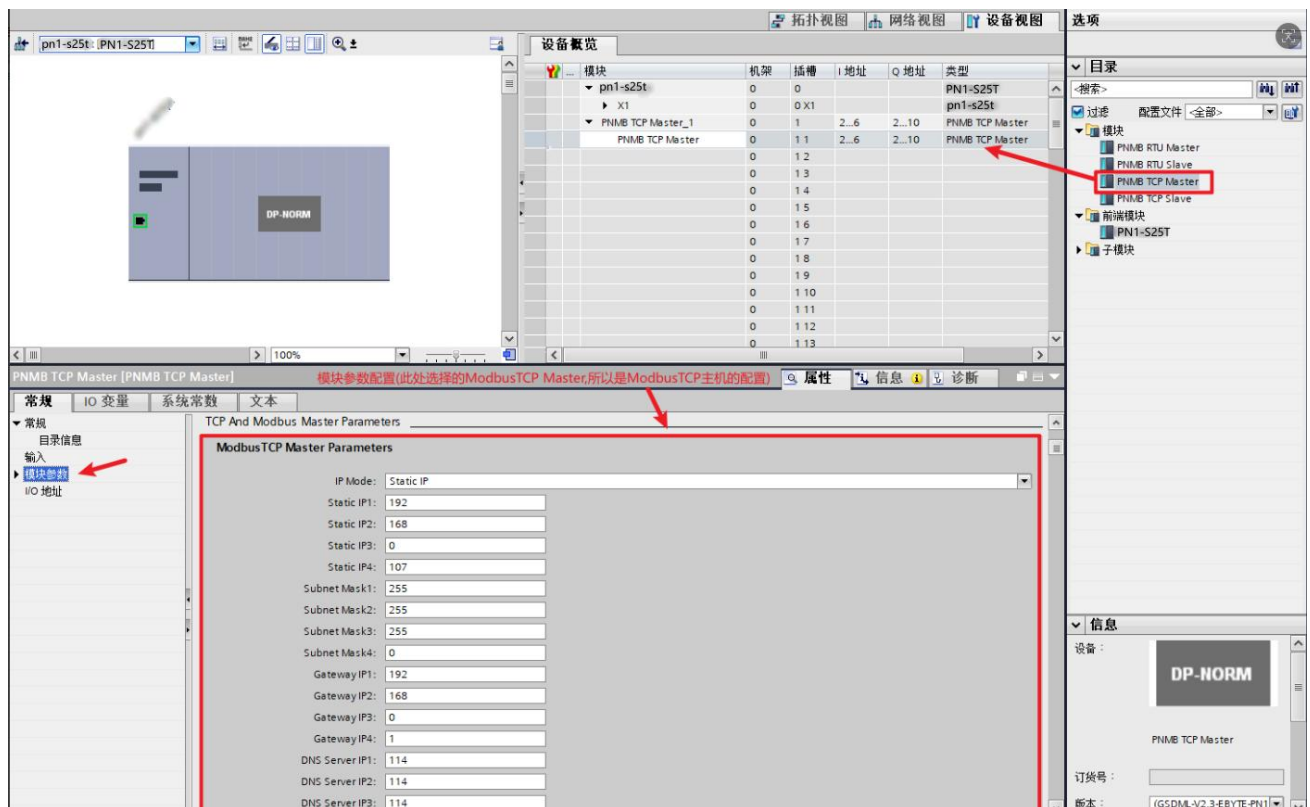
PN1-S25T 网关既支持 Modbus TCP 主站和 Modbus TCP 从站,又支持 Modbus RTU 主站和 Modbus RTU 从站,具体通过 Profinet 的配置来决定。

在拓扑视图界面选中 PN1-S25T 并双击,进入设备视图操作界面。

如下图所示，在设备概览区域，系统提供两个槽位用于配置 Modbus TCP 主机/从机共用(图中红色对应位置)的主槽位和 Modbus RTU 主机/从机(图中蓝色对应位置)的主槽位。每个主槽位支持挂载 48 个子槽位，用于配置 Modbus 指令子模块。特别地，一号子槽分别对应设备的状态字和控制字(适用于 PNMB Master/PNMB Slave 配置)。通过状态字，PLC 能够获取 PN1-S25T 设备的运行状况；而通过控制字，则可以让 PLC 对 PN1-S25T 设备进行操控。

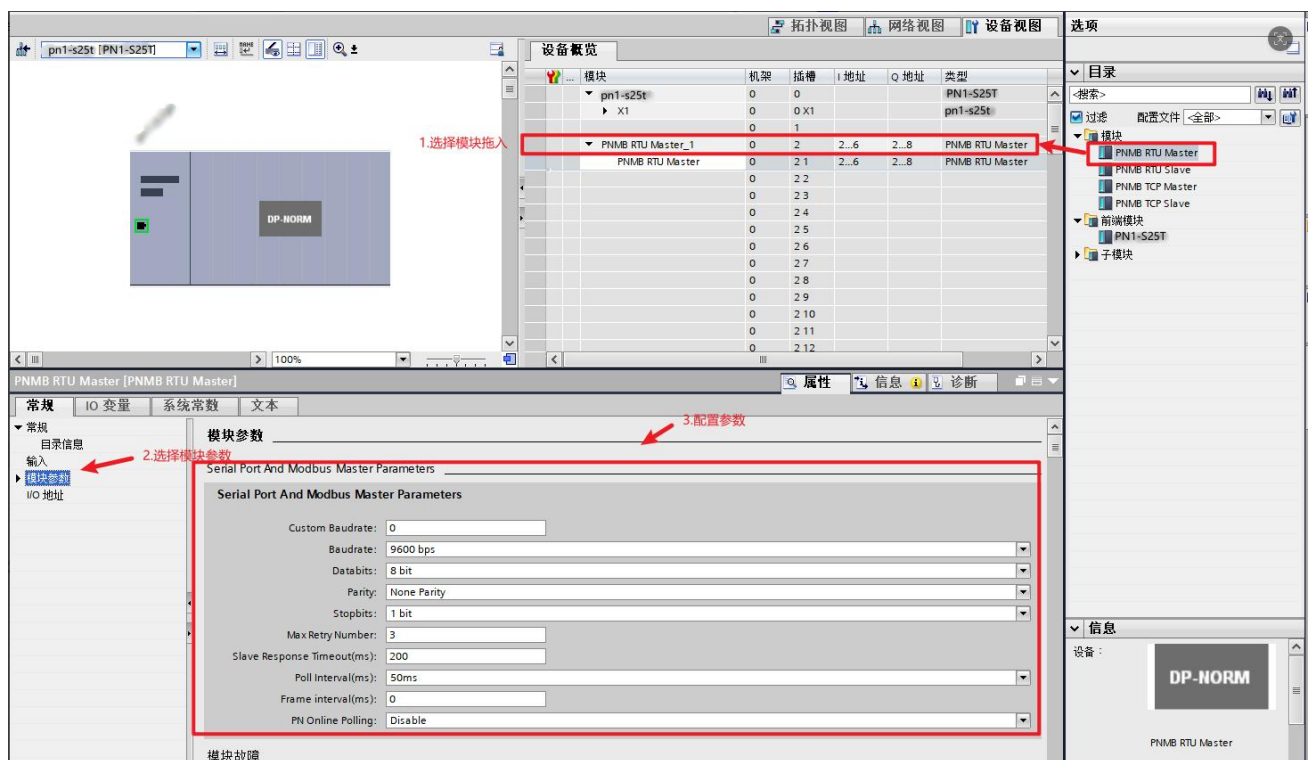


如图从右侧添加一个 Modbus TCP Master 到对应的槽位在下方“常规”->“模块参数”中可针对 Modbus TCP 主机参数进行设置。从机模式参数设置也是类似操作。



5.5 PN1-S25T 设备模块 Modbus 通讯接口参数：

Modbus RTU Master



Custom Baudrate:

当串口配置为从站模式且需要使用自定义波特率时，默认设置为 0。此时，表示自定义波特率未启用。若要启用自定义波特率，请设置一个介于 1200 到 3.9M 之间的数值，在此情况下，“Baudrate”选项将不生效。

Baudrate:

标准波特率：1200、2400、4800、9600、19200、38400、57600、115200、230400、460800bps，默认：9600。

Databits:

数据位：7、8bit，默认：8。

Parity:

数据校验：None Parity（无检验）、Odd Parity（奇检验）、Even Parity（偶检验），默认：None Parity（无检验）。

Stopbit:

数据停止位：1、2bit，默认：1。

Max Retry Number:

串口作为主站时的错误重试次数，0-255，0 不重发，255 无限重发，1-254 按次数重发,默认：3。

Slave Response Timeout(ms):

串口作为主站时模块发出 Modbus 报文后,等待 Modbus 设备响应的的时间，若 Modbus 设备在设定的等待回答时间内仍无响应，模块停止等待，继续发送下一条 Modbus 报文或重发。选择范围 0-65535ms，默认：100ms。

Poll Interval(ms):

串口作为主站时总线转换模块接收到 Modbus 从站回复的正确报文后，延时发送 Modbus 主站报文的时间。若 Modbus 从站设备响应主站报文较慢，如果总线转换模块发送 Modbus 报文过快，那么会出现通信故障，可以适当增加发送报文间隔时间。选择范围 10、20、30、40、50、60、70、80、90、100、200、500、1000ms 或者不等待(No Delay)。默认值为：50ms。

Frame interval(ms):

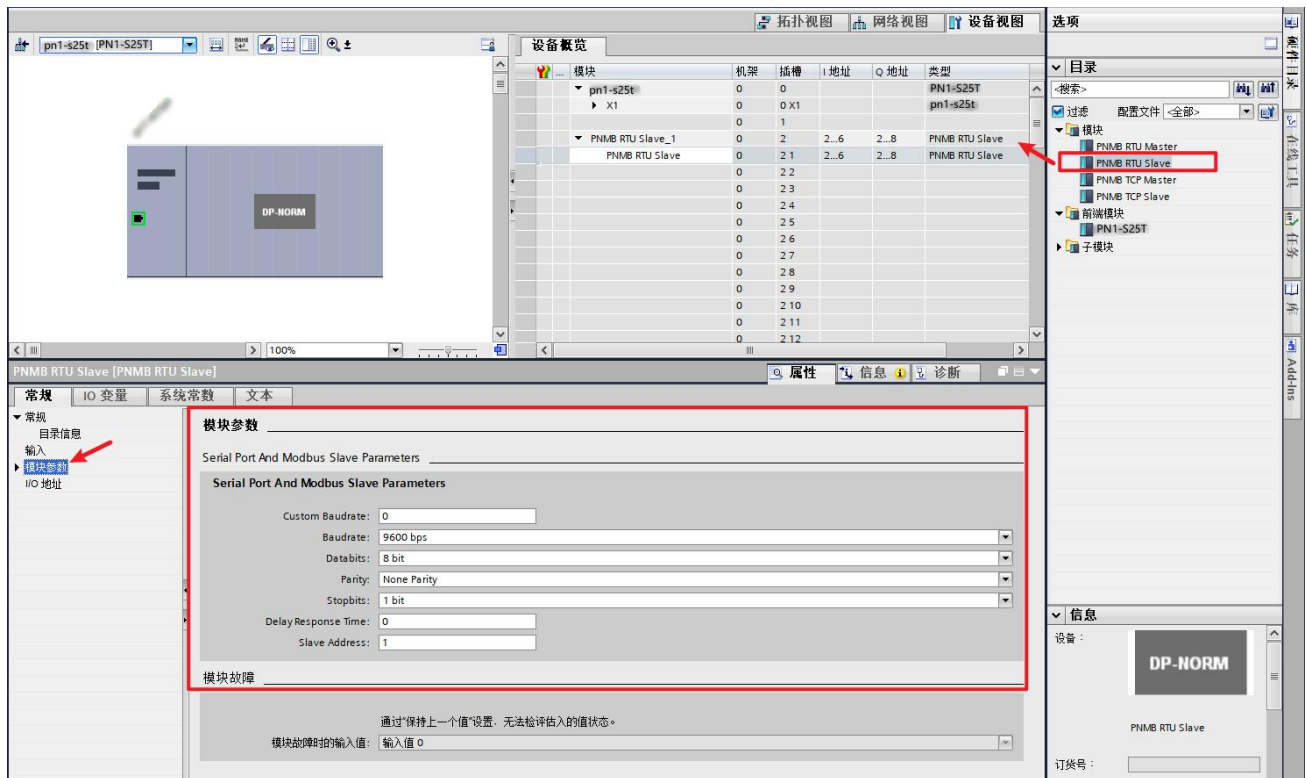
数据断帧时间：0-65535ms，0 表示进行自动断帧，默认：0。

PN Online Polling:

Profinet 仅在线轮询:Enable/Disable,默认:Disable

开启状态下模块只有在和 PLC 正常通信的时候才和从站通信，默认关闭状态

Modbus RTU Slave



Custom Baudrate:

当串口配置为从站模式且需要使用自定义波特率时，默认设置为 0。此时，表示自定义波特率未启用。若要启用自定义波特率，请设置一个介于 1200 到 3900000 之间的数值，在此情况下，“Baudrate”选项将不生效。

Baudrate:

标准波特率：1200、2400、4800、9600、19200、38400、57600、115200、230400、460800bps，默认：9600。

Databits:

数据位：7、8bit，默认：8。

Parity:

数据校验：None Parity（无检验）、Odd Parity（奇检验）、Even Parity（偶检验），默认：None Parity（无检验）。

Stopbit:

数据停止位：1、2bit，默认：1。

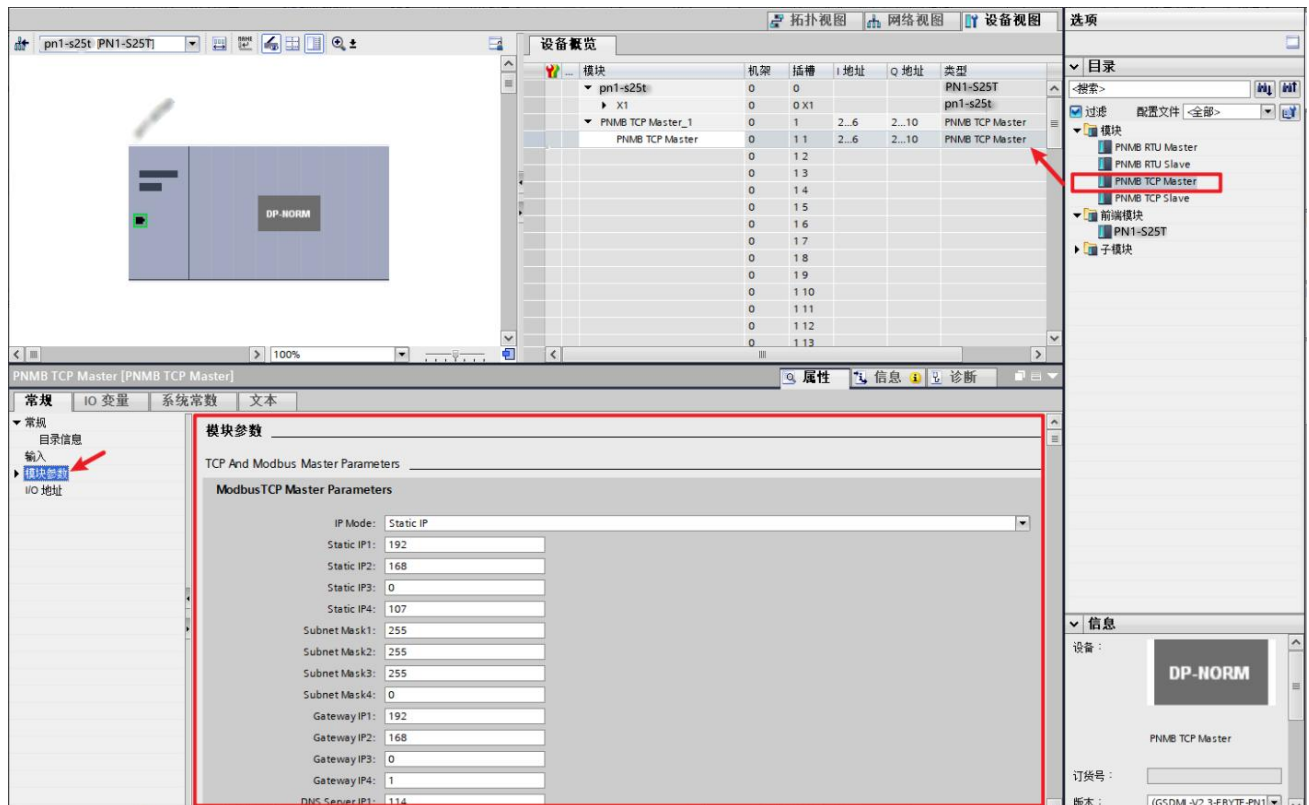
Delay Response Time.

串口作为从站时接收到主站发过来的轮询命令后，延迟多长时间才进行回复。范围：0 ~ 65535，0 表示立即回复，单位是 ms。默认：0。

Slave Address:

串口作为从站时的站地址。范围：1 ~ 247，默认：1。

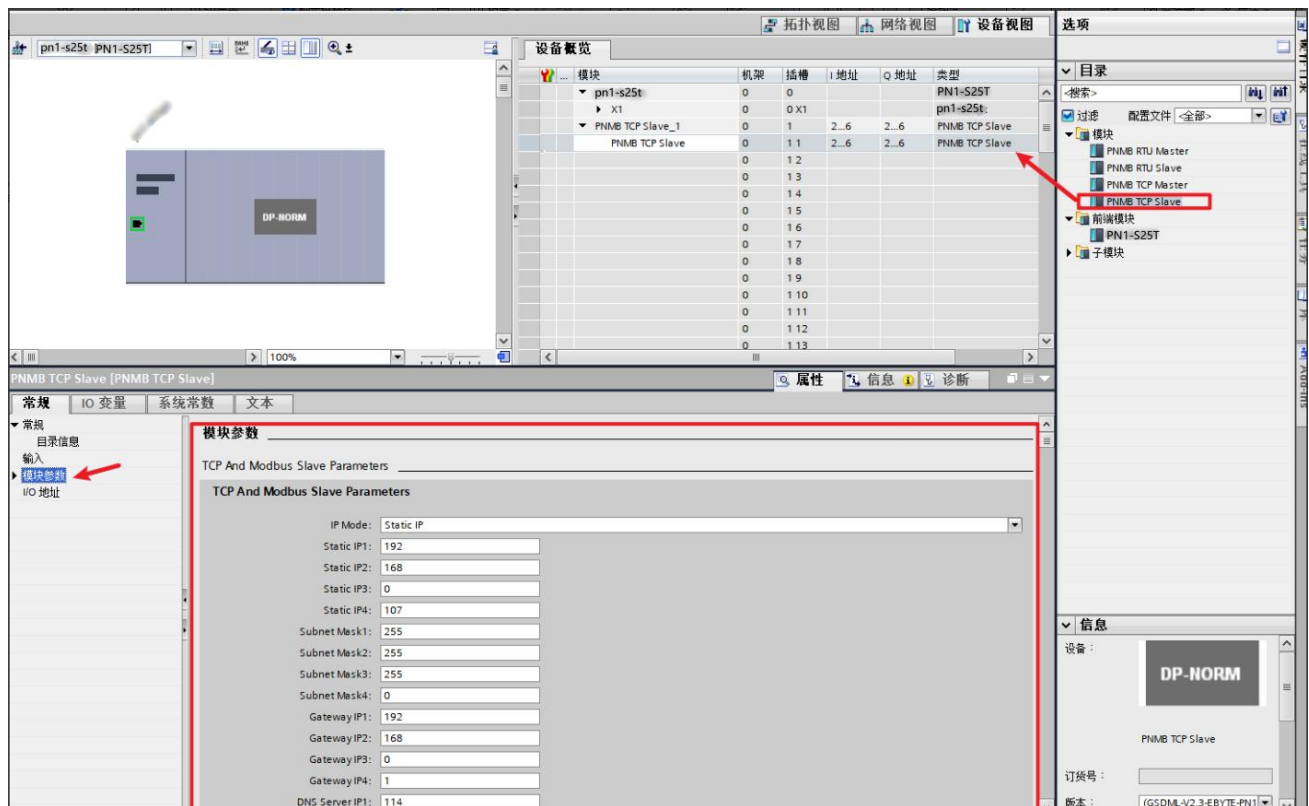
Modbus TCP Master



参数	默认值/范围	说明
Modbus TCP Master Parameters		
IP Mode	默认 0; 0=Static IP, 1=DHCP	Modbus TCP 网口 IP 获取方式
Static IP(1...4)	192.168.0.107	静态 IP 地址
Subnet Mask(1...4)	255.255.255.0	子网掩码
Gateway IP(1...4)	192.168.0.1	默认网关
DNS Server IP(1...4)	114.114.114.114	DNS 服务器地址
Connection Parameters		
Reconnection Time(s)	默认 3 s, 范围:0-255	连接断开后的重连等待时间
Max Retry Number	默认 3, 范围:0-255	单次命令异常时的最大重试次数
Response Timeout(ms)	默认 200 ms, 范围:0-65535	等待 Modbus TCP 响应的超时时间
Poll interval(ms)	默认 50 ms,范围:0-1000	轮询命令之间的最小间隔
PN Online Polling	默认:Disable,可选:Enable/Disable	开启状态下模块只有在和 PLC 正常通信的时候才和从站通信, 默认关闭状态
Modbus TCP Master Remote Parameters		
Socket1 ~ Socket8 Slave Address	默认 1, 范围 0-247	目标 Modbus 从站地址
Socket1 ~ Socket8 Port	默认 502,范围:0-65535	目标 TCP 端口

Socket1 ~ Socket8 Octet	默认 192.168.0.1	目标 Modbus 从站地址，得和 Modbus TCP 主站处于同一网段。
-------------------------	----------------	--

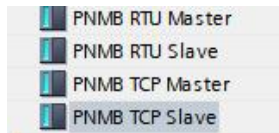
Modbus TCP Slave



参数	默认值/范围	说明
IP Mode	默认 0; 0=Static IP, 1=DHCP	Modbus TCP 网口 IP 获取方式
Static IP(1...4)	192.168.0.107	网关作为 TCP Slave 时的本机 IP
Subnet Mask(1...4)	255.255.255.0	子网掩码
Gateway IP(1...4)	192.168.0.1	默认网关
DNS Server IP(1...4)	114.114.114.114	DNS 服务器地址
Modbus TCP Slave Address(0..255)	默认 1, 范围 0-255	Modbus TCP 单元标识/站地址
Modbus TCP Slave Response Delay Time(ms)	默认 0 ms 范围 :0-65535	收到请求后的延迟响应时间
Modbus TCP Slave Port	默认 502, 范围 1 ~ 65535	Modbus TCP 监听端口

5.6 配置 Modbus 状态字和控制字

在设备概览中可以看到一共有 2 个槽位拖动下图到其中一个模块到对应主槽后，每个主槽又有 48 个子槽产生。



每个主槽包含各自的“状态字”和“控制字”例如：

模块	机架	插槽	I 地址	Q 地址	类型
pn1-s25t	0	0			PN1-S25T
X1	0	0 X1			pn1-s25t
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

如图对应的 PROFINET 输入地址 IB2-IB6(可改)，为通信状态监控字。Q 地址一栏中，对应的 PROFINET 输出地址 QB2-QB6(可改)，为通信控制字。

5.6.1. Modbus RTU 状态字和控制字

Modbus RTU 的通信状态监控字：5 字节,每字节含义如下

第 1 字节:出错槽号

第 2 字节:错误码

其他字节保留

错误码	描述
1	从站回复 Modbus 标准错误：ILLEGAL FUNCTION
2	从站回复 Modbus 标准错误：ILLEGALDATA ADDRESS
3	从站回复 Modbus 标准错误：ILLEGAL DATA VALUE
4	从站回复 Modbus 标准错误：SLAVE DEVICE FAILURE
10	主站接收的报文长度错误，太长，太短或与正确的从站回复数据长度不符
11	主站接收的报文 CRC 校验错误
12	主站接收的报文寄存器数量错误
13	主站接收的报文从站地址错误
14	主站接收超时
15	主站接收的报文中功能码与请求的不一致
16	主站接收的报文寄存器地址错误
17	未知错误

Modbus RTU 的通信控制字：7 字节,每字节含义如下

注：串口必须使能后，才可进行数据通讯

第 1 字节:0 位 Modbus 串口功能是否启用。1 启用，0 不启用。第 1 位 :清除故障码，当检测到上升沿（0→1）时，通讯状态监控清零。 其他位保留。

- 第 2 字节:槽号:2-9 触发位。
- 第 3 字节:槽号:10-17 触发位。
- 第 4 字节:槽号 18-25 触发位。
- 第 5 字节:槽号:26-33 触发位。
- 第 6 字节:槽号:34-41 触发位。
- 第 7 字节:槽号:42-49 触发位。

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
第 2 字节							
子插槽 9	子插槽 8	子插槽 7	子插槽 6	子插槽 5	子插槽 4	子插槽 3	子插槽 2
第 3 字节							
子插槽 17	子插槽 16	子插槽 15	子插槽 14	子插槽 13	子插槽 12	子插槽 11	子插槽 10
第 4 字节							
子插槽 25	子插槽 24	子插槽 23	子插槽 22	子插槽 21	子插槽 20	子插槽 19	子插槽 18
第 5 字节							
子插槽 33	子插槽 32	子插槽 31	子插槽 30	子插槽 29	子插槽 28	子插槽 27	子插槽 26
第 6 字节							
子插槽 41	子插槽 40	子插槽 39	子插槽 38	子插槽 37	子插槽 36	子插槽 35	子插槽 34
第 7 字节							
子插槽 49	子插槽 48	子插槽 47	子插槽 46	子插槽 45	子插槽 44	子插槽 43	子插槽 42

5.6.2. Modbus TCP 状态字和控制字

Modbus TCP 的通信状态监控字：5 字节,每字节含义分别如下

- 第 1 字节:出错槽号
- 第 2 字节:错误码见下图:
- 第 3 字节:0 位没用,1-7 位依次指示 socket1-7 连接状态。1 连接，0 未连接
- 第 4 字节:0 位:指示 Socket8 连接状态。其他位保留。1 连接,0 未连接
- 第 5 字节:保留未使用

错误码	描述
1	从站回复 Modbus 标准错误：ILLEGAL FUNCTION
2	从站回复 Modbus 标准错误：ILLEGALDAT AADDRESS
3	从站回复 Modbus 标准错误：ILLEGAL DATA VALUE
4	从站回复 Modbus 标准错误：SLAVE DEVICE FAILURE
10	主站接收的报文长度错误，太长，太短或与正确的从站回复数据长度不符
11	主站接收的报文 CRC 校验错误
12	主站接收的报文寄存器数量错误
13	主站接收的报文从站地址错误
14	主站接收超时
15	主站接收的报文中功能码与请求的不一致
16	主站接收的报文寄存器地址错误

17	未知错误
19	TCP 连接错误:TCP CONNECT ERR

Modbus TCP 的通信控制字：9 字节,每字节含义分别如下

注：每个 socket 必须使能后，才可进行数据通讯

第 1 字节:0 位清除报警.上升沿触发。1-7 位控制 0-7 的 socket 使能。1 使能，0 不使能。使能后客户端会去连接对应的 Modbus TCP 从站。不使能时将会断开连接。(通过状态字的第 3 字节，第 4 字节可以观察 socket 是否连接成功)

第 2 字节:0 位指示 socket8 使能。1 使能，0 不使能。其他位保留未使用

第 3 字节:保留未使用

第 4 字节:槽号:2-9 触发位。

第 5 字节:槽号:10-17 触发位。

第 6 字节:槽号:18-25 触发位。

第 7 字节:槽号:26-33 触发位。

第 8 字节:槽号:34-41 触发位。

第 9 字节:槽号:42-49 触发位。

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
第 3 字节							
空	空	空	空	空	空	空	空
第 4 字节							
子插槽 9	子插槽 8	子插槽 7	子插槽 6	子插槽 5	子插槽 4	子插槽 3	子插槽 2
第 5 字节							
子插槽 17	子插槽 16	子插槽 15	子插槽 14	子插槽 13	子插槽 12	子插槽 11	子插槽 10
第 6 字节							
子插槽 25	子插槽 24	子插槽 23	子插槽 22	子插槽 21	子插槽 20	子插槽 19	子插槽 18
第 7 字节							
子插槽 33	子插槽 32	子插槽 31	子插槽 30	子插槽 29	子插槽 28	子插槽 27	子插槽 26
第 8 字节							
子插槽 41	子插槽 40	子插槽 39	子插槽 38	子插槽 37	子插槽 36	子插槽 35	子插槽 34
第 9 字节							
子插槽 49	子插槽 48	子插槽 47	子插槽 46	子插槽 45	子插槽 44	子插槽 43	子插槽 42

5.7 子模块参数说明

Modbus RTU 主站子模块参数

每条 Modbus RTU 主站命令有五个属性：

Slave Address(1~247):表示 Modbus RTU 从站设备的地址，可选择范围 1-247。

Function Code:Modbus RTU 主站的功能码,根据插入插槽的 Modbus 命令自动生成功能码,不可更改。

Start Address :对 Modbus RTU 从站数据操作的开始地址。非寄存器 PLC 地址,无前缀。范围 0-65535。

XX Quantity :表示读写的线圈或者寄存器个数。据插入插槽的 Modbus 命令自动生成,可在范围内进行数量更改。

Transmission Type :提供以下四种发送类型。

Disable:表示该命令不执行。

Poll trigger(轮询发送): Modbus RTU 对应的主站使能后,该报文会按照插槽号从小到大的顺序依次发送。

Leve ltrigger(电平发送): 槽号对应的控制发送标志位由 0 变到 1 后:对于读指令,该报文会被发送。对于写指令,如果数据有改变才会被发送;槽号对应的控制发送标志位由 1 变到 0 后,不论是读报文还是写报文都会停止发送。(上节为例,PLC 地址 QB2-QB5 就是发送触发控制位)

Rising trigger(上升沿发送): 槽号对应的触发控制位由 0 变到 1 后,该报文会发送一次。(上节为例,PLC 地址 QB2-QB5 就是发送触发控制位)

Modbus RTU 从站子模块参数

每条 Modbus RTU 从站命令前缀为 Input 或 Output。Input 表示数据输入 PLC,即主站写数据给从站,从站又将数据交给 PLC,对应写类型的命令。Output 表示数据从 PLC 输出,即 PLC 将数据交给从站,主站再来读从站的数据,对应读类型的命令。更具体一点,每条从站命令最后都标明了支持的功能码。

功能码	功能	操作地址区域(非寄存器 PLC 地址)	操作类型
01H	读取多个线圈输出状态	0XXXX	读
02H	读取多个输入线圈状态	1xxXX	读
03H	读取多个保存寄存器	4xxXX	读
04H	读取输入寄存器	3XXXX	读
05H	强置单个线圈	0XXXX	写
06H	预置单个保持寄存器	4XXXX	写
0FH	强置多线圈	0xXXX	写
10H	预置多个保持寄存器	4XXXX	写

Modbus TCP 主站子模块参数

每条 Modbus TCP 主站命令有五个属性

其中,Function Code; Start Address;; XX Quantity; Transmission Type 同 Modbus RTU 主站配置功能一样

Socket Config selection(1-8):选择该条指令使用哪一个 socket 进行工作。

Modbus TCP 从站子模块参数

同 Modbus RTU 从站子模块参数类同。

5.7.1. 串口使能例程

如下图是 Modbus RTU 槽信息由图可知 I2-I6 即状态字, B2-B8 为控制字。

	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			

要使能串口则，在对照控制字说明如图:

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 即为第 1 字节，将 B2 的 Bit0 置位为 1 即使能了串口。

程序示例:如下图是使能串口的程序段:



5.7.2. 网口 socket 使能例程

如下图是 Modbus TCP 槽信息由图可知 I2-I6 即状态字，B2-B10 为控制字。

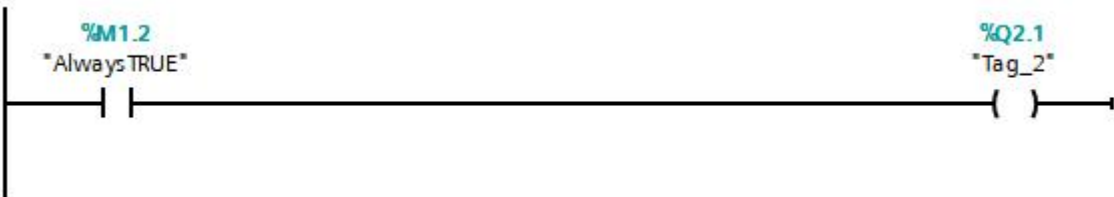
▼ PNMB TCP Master_1	0	1	2...6	2...10	PNMB TCP Master
PNMB TCP Master	0	1 1	2...6	2...10	PNMB TCP Master

要使能 socket1-socket8 则，在对照控制字说明如图:

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

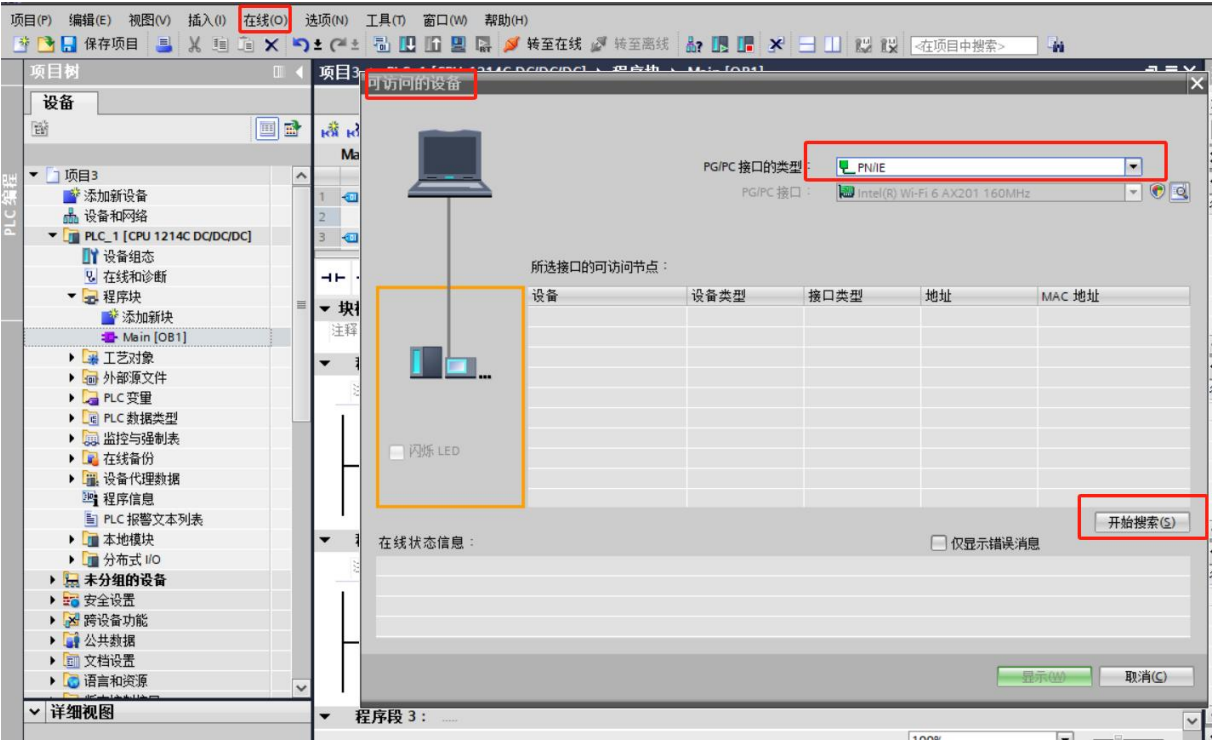
B2 即为第 1 字节，B3 为第 2 字节以此类推。我们将 B2 所有位置 1.B3 第 1 字节置 1 即使能了 socket1-8.

程序示例:如下图是单独使能 socket1 的程序段:



5.8 使用博图修改模块名称和查询 IP 地址

- 打开博图软件，点击菜单栏中的“在线”选项。
- 在打开的在线访问界面中，查找并选择“可访问的设备”。
- 进行设备搜索。搜索完成后，将列出所有可访问的设备。
- 从列表中选择需要修改 IP 地址和名称的目标设备。
- 对选定的设备执行 IP 地址和名称的修改操作。



第六章 使用 STEP 7 加载设备教程

6.1 连接前准备

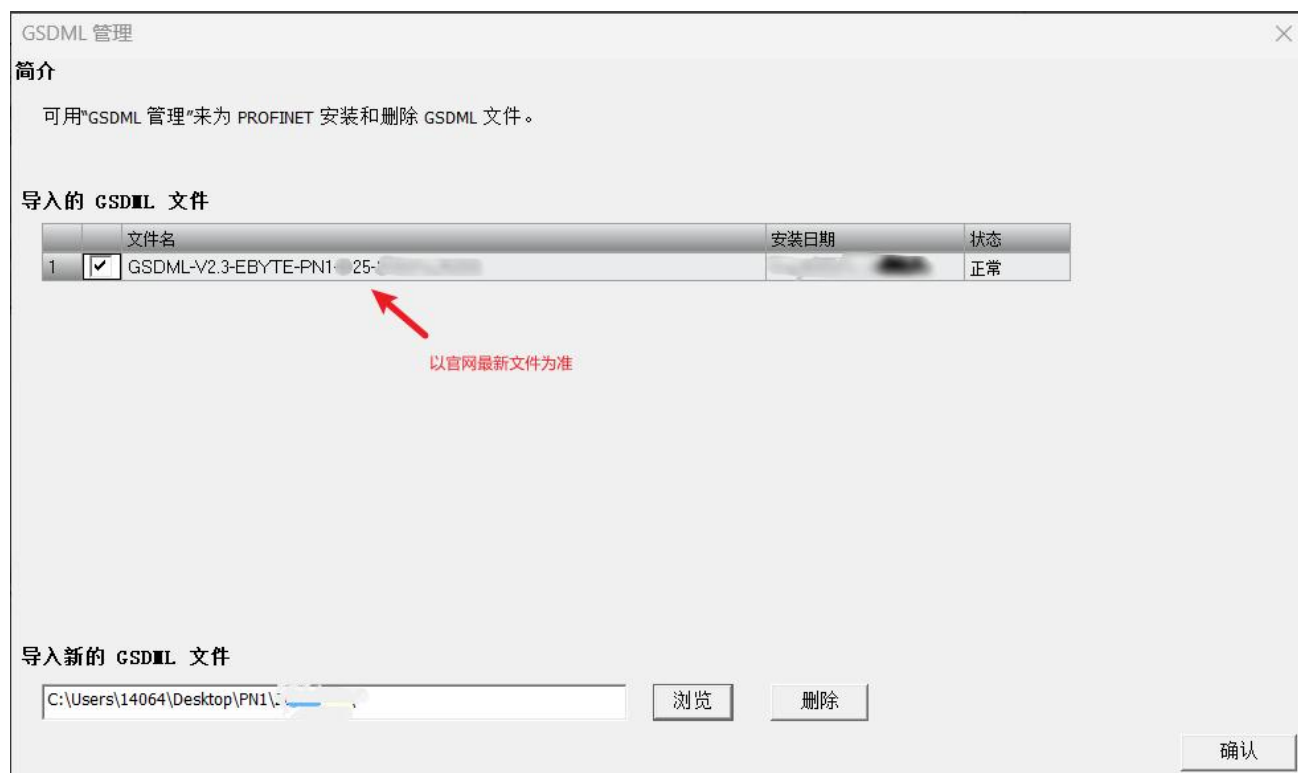
1. 准备好需要的 XML 文件，如下所示：
2. GSDML-V2.3-EBYTE-PN1-S25T-20260414.xml 将 DC 24V 外部电源接入模块并通电，通电前请检查电源正、负极是否连接正确。
3. 使用网线将模块连接到 PLC 控制器的 Profinet 接口上。（在同一个网段）

6.2 STEP 7 添加 GSDML 文件

1. 在文件菜单下，进入 GSDML 管理



2. 添加 GSDML 文件

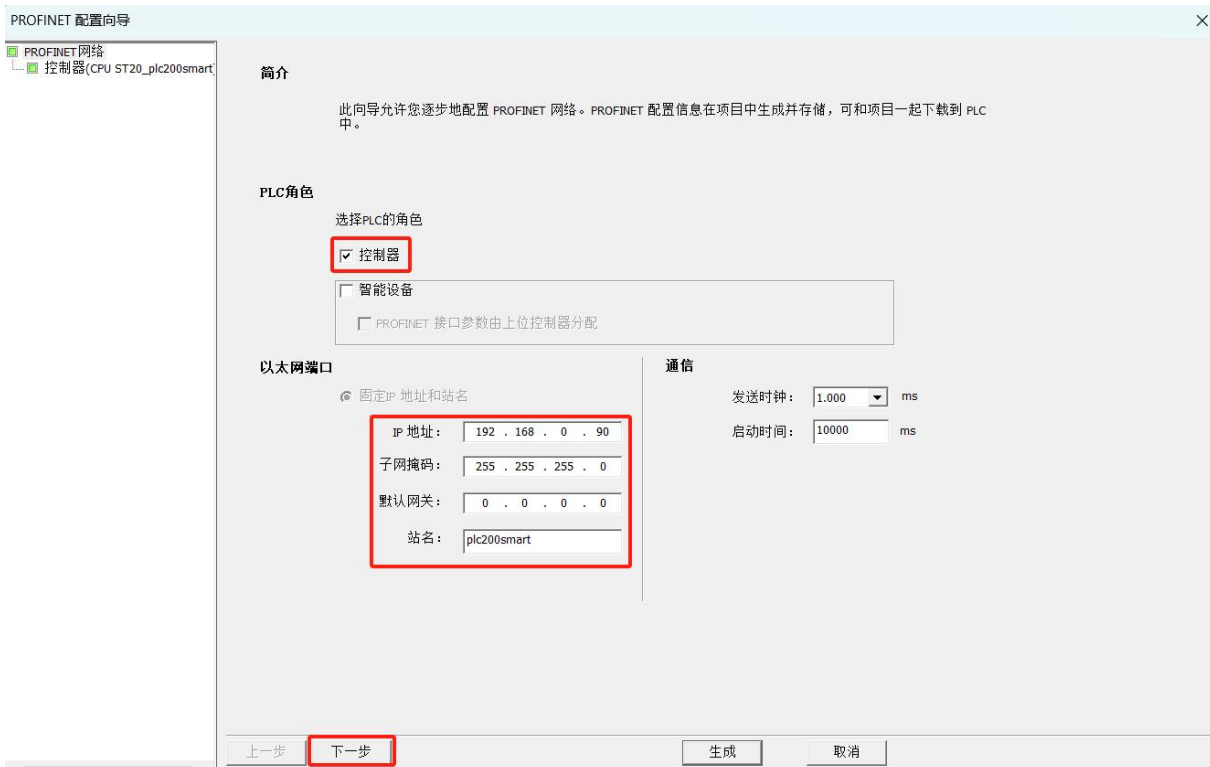


6.3 项目添加 Profinet 设备

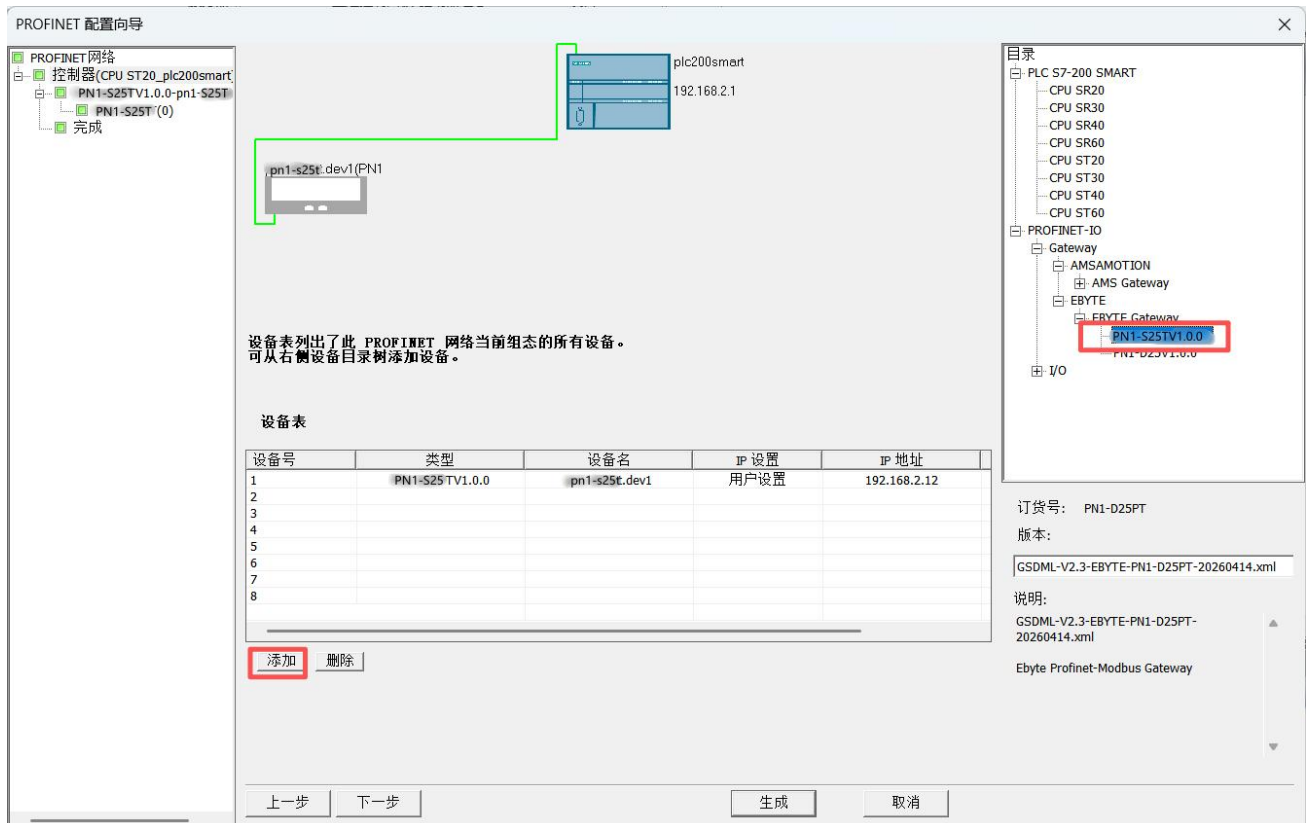
1. 选择工具菜单下面的 PROFINET 命令



2. 选择 PLC 角色为 PLC 控制器，设置对应 PLC 控制器 IP 等相关参数。完成后点击下一步。

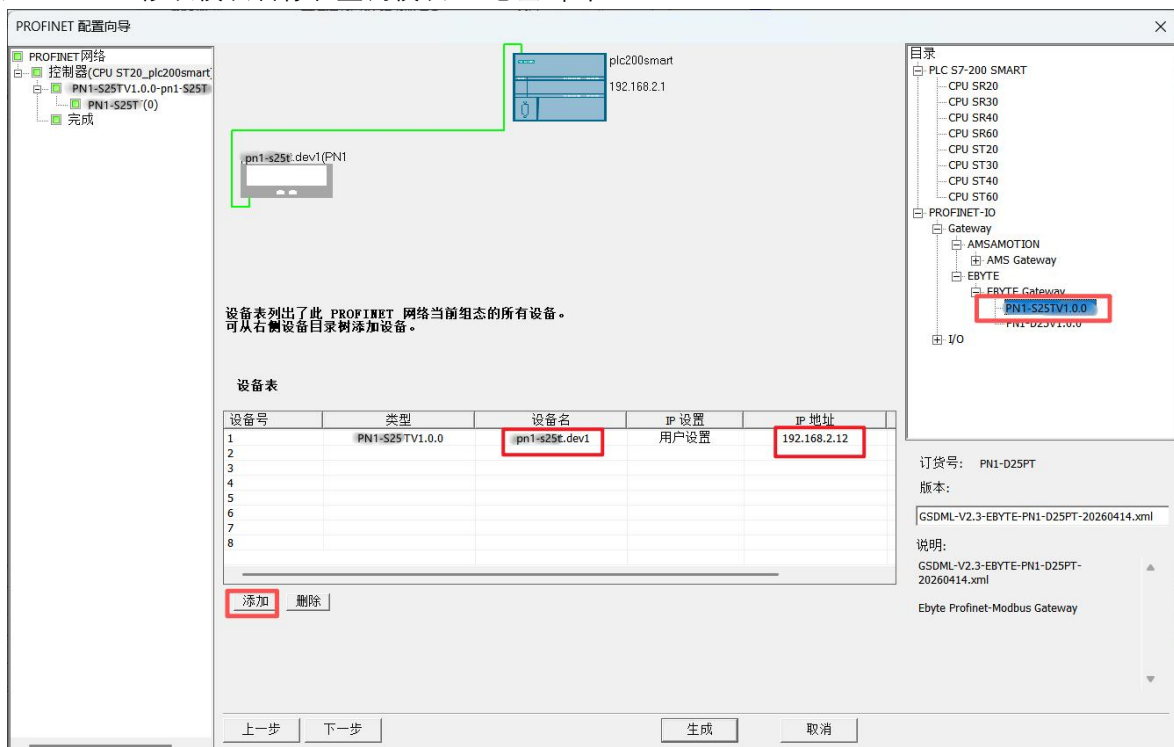


在右边栏中 PROFINET-IO→Gateway→EBYTE→TION→EBYTE Gateway→PN1-S25TV1.0.0 单击选中，然后按住左键，将其拖入左侧表格内。



双击设备名栏，填入相应设备名称，同一项目内不能有相同的设备名，同样设置 IP 地址，保持和 PLC 控制器在同一网段内，最后点击生成。

注意：此时设置的设备名需要和设备保持一致，如果不清楚设备名，可以先随意设置，后将模块的设备名更改一致即可，此时设置的 IP 地址会在组态时，将同设备名的模块的 IP 设置成这里设置的值。设备名称修改请参照“STEP 7 修改模块名称和查询模块 IP 地址”章节。



6.4 配置 Modbus 通讯参数

完成相关设置后，点击进入设备视图操作界面。在设备概览区域，系统提供两个槽位用于配置串口和网口功能模块，每个槽位可容纳 48 个子槽，用于配置 Modbus 指令子模块。PLC 能够获取 PN1-S25T 设备的运行状况；而通过控制字，则可以让 PLC 对 PN1-S25T 设备进行操控。

PN1-S25T 设备模块 Modbus 串口通讯接口参数：

PNMB RTU Master

Custom Baudrate:

当串口配置为从站模式且需要使用自定义波特率时，默认设置为 0。此时，表示自定义波特率未启用。若要启用自定义波特率，请设置一个介于 1200 到 3900000 之间的数值，在此情况下，“Baudrate”选项将不生效。

Baudrate:

标准波特率：1200、2400、4800、9600、19200、38400、57600、115200、230400、460800bps，默认：9600。

Databits:

数据位：7、8bit，默认：8。

Parity:

数据校验：None Parity（无检验）、Odd Parity（奇检验）、Even Parity（偶检验），默认：None Parity（无检验）。

Stopbit:

数据停止位：1、2bit，默认：1。

Max Retry Number:

串口作为主站时的错误重试次数，0-255，0 不重发，255 无限重发，1-254 按次数重发，默认：3。

Slave Response Timeout(ms):

串口作为主站时模块发出 Modbus 报文后，等待 Modbus 设备响应的的时间，若 Modbus 设备在设定的等待回答时间内仍无响应，模块停止等待，继续发送下一条 Modbus 报文或重发。选择范围 0-65535ms，默认：100ms。

Poll Interval(ms):

串口作为主站时总线转换模块接收到 Modbus 从站回复的正确报文后，延时发送 Modbus 主站报文的时间。若 Modbus 从站设备响应主站报文较慢，如果总线转换模块发送 Modbus 报文过快，那么会出现通信故障，可以适当增加发送报文间隔时间。选择范围 10、20、30、40、50、60、70、80、90、100、200、500、1000ms 或者不等待（No Delay）。默认值为：50ms。

Frame interval(ms):

数据断帧时间：0-65535ms，0 表示进行自动断帧，默认：0。

PNMB RTU Slave

Custom Baudrate:

当串口配置为从站模式且需要使用自定义波特率时，默认设置为 0。此时，表示自定义波特率未启用。若要启用自定义波特率，请设置一个介于 1200 到 3900000 之间的数值，在此情况下，“Baudrate”选项将不生效。

Baudrate:

标准波特率：1200、2400、4800、9600、19200、38400、57600、115200、230400、460800bps，默认：9600。

Databits:

数据位：7、8bit，默认：8。

Parity:

数据校验：None Parity（无检验）、Odd Parity（奇检验）、Even Parity（偶检验），默认：None Parity（无检验）。

Stopbit:

数据停止位：1、2bit，默认：1。

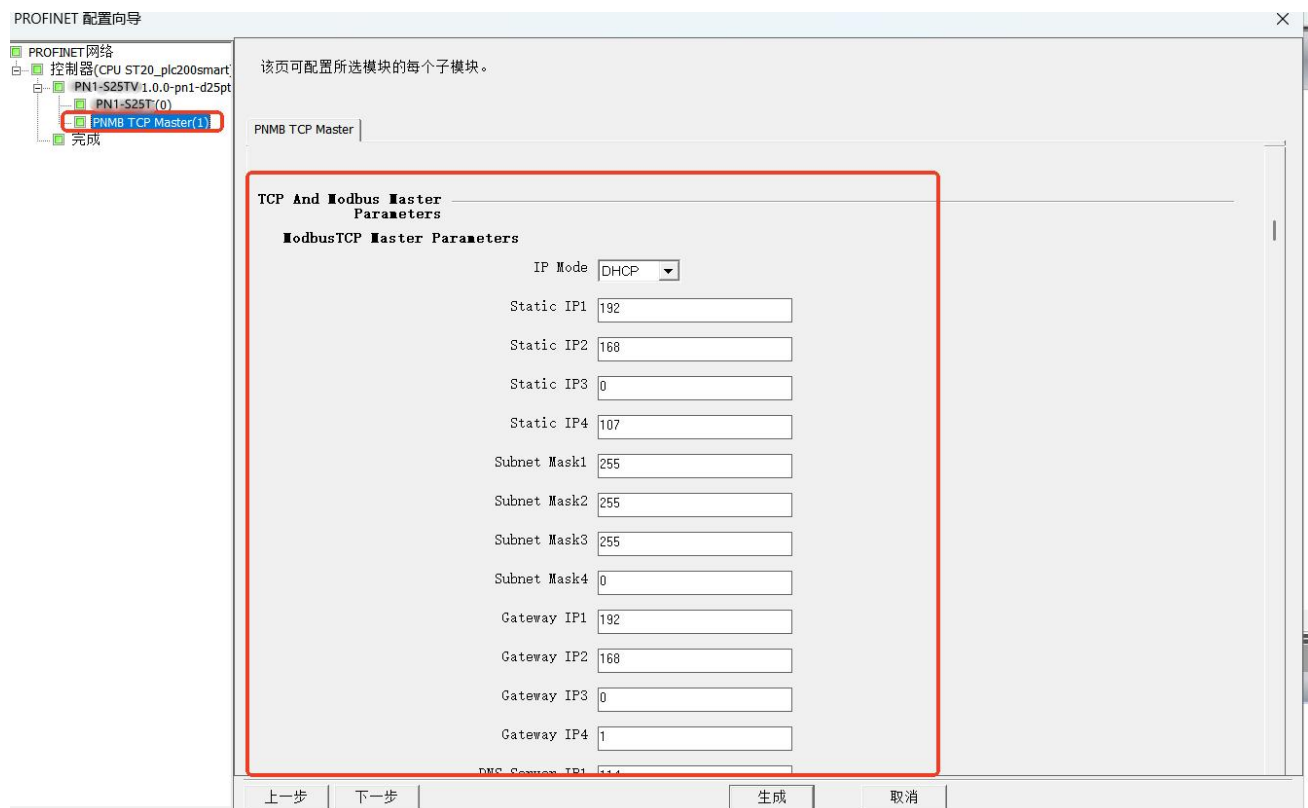
Delay Response Time.

串口作为从站时接收到主站发过来的轮询命令后，延迟多长时间才进行回复。范围：0 ~ 65535，0 表示立即回复，单位是 ms。默认：0。

Slave Address:

串口作为从站时的站地址。范围：1 ~ 247，默认：1。

Modbus TCP Master



参数	默认值/范围	说明
Modbus TCP Master Parameters		
IP Mode	默认 0; 0=Static IP, 1=DHCP	Modbus TCP 网口 IP 获取方式
Static IP(1...4)	192.168.0.107	静态 IP 地址
Subnet Mask(1...4)	255.255.255.0	子网掩码
Gateway IP(1...4)	192.168.0.1	默认网关
DNS Server IP(1...4)	114.114.114.114	DNS 服务器地址
Connection Parameters		
Reconnection Time(s)	默认 3 s, 范围:0-255	连接断开后的重连等待时间
Max Retry Number	默认 3, 范围:0-255	单次命令异常时的最大重试次数
Response Timeout(ms)	默认 200 ms, 范围:0-65535	等待 Modbus TCP 响应的超时时间
Poll interval(ms)	默认 50 ms,范围:0-1000	轮询命令之间的最小间隔
PN Online Polling	默认:Disable,可选:Enable/Disable	开启状态下模块只有在和 PLC 正常通信的时候才和从站通信,默认关闭状态
Modbus TCP Master Remote Parameters		
Socket1 ~ Socket8 Slave Address	默认 1, 范围 0-247	目标 Modbus 从站地址
Socket1 ~ Socket8 Port	默认 502,范围:0-65535	目标 TCP 端口
Socket1 ~ Socket8 Octet	默认 192.168.0.1	目标 Modbus 从站地址, 得和 Modbus TCP 主站处于同一网段。

Modbus TCP Slave

PROFINET 配置向导

PROFINET 网络

控制柜(CPU ST20_plc200smart)

PN1-S25T V1.0.0-pn1-d25pt

PNMB TCP Slave(1)

完成

该页可配置所选模块的每个子模块。

PNMB TCP Slave

TCP And Modbus Slave Parameters

IP Mode Static IP

Static IP1 192

Static IP2 168

Static IP3 0

Static IP4 107

Subnet Mask1 255

Subnet Mask2 255

Subnet Mask3 255

Subnet Mask4 0

Gateway IP1 192

Gateway IP2 168

Gateway IP3 0

Gateway IP4 1

DNS Server IP1 114

DNS Server IP2 114

DNS Server IP3 114

上一步

下一步

生成

取消

参数	默认值/范围	说明
IP Mode	默认 0；0=Static IP，1=DHCP	Modbus TCP 网口 IP 获取方式
Static IP(1...4)	192.168.0.107	网关作为 TCP Slave 时的本机 IP
Subnet Mask(1...4)	255.255.255.0	子网掩码
Gateway IP(1...4)	192.168.0.1	默认网关
DNS Server IP(1...4)	114.114.114.114	DNS 服务器地址
Modbus TCP Slave Address(0..255)	默认 1，范围 0-255	Modbus TCP 单元标识/站地址
Modbus TCP Slave Response Delay Time(ms)	默认 0 ms 范围 :0-65535	收到请求后的延迟响应时间
Modbus TCP Slave Port	默认 502，范围 1 ~ 65535	Modbus TCP 监听端口

6.5 配置 Modbus 状态字和控制字

在设备概览中可以看到一共有 2 个槽位拖动下图到对应主槽后，每个主槽又有 48 个子槽

- PNMB RTU Master
- PNMB RTU Slave
- PNMB TCP Master
- PNMB TCP Slave

每个主槽包含各自的“状态字”和“控制字”例如:

	序号	模块名	子模块名	插槽_子插槽	PN1 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		

如图对应的 PROFINET 输入地址 IB128-IB132(可改), 为通信状态监控字。Q 地址一栏中, 对应的 PROFINET 输出地址 QB128-QB132(可改), 为通信控制字。

Modbus RTU 的通信状态监控字：5 字节,每字节含义如下

- 第 1 字节:出错槽号
- 第 2 字节:错误码
- 其他字节保留

错误码	描述
1	从站回复 Modbus 标准错误：ILLEGAL FUNCTION
2	从站回复 Modbus 标准错误：ILLEGALDATAADDRESS
3	从站回复 Modbus 标准错误：ILLEGAL DATA VALUE
4	从站回复 Modbus 标准错误：SLAVE DEVICE FAILURE
10	主站接收的报文长度错误，太长，太短或与正确的从站回复数据长度不符
11	主站接收的报文 CRC 校验错误
12	主站接收的报文寄存器数量错误
13	主站接收的报文从站地址错误
14	主站接收超时
15	主站接收的报文中功能码与请求的不一致
16	主站接收的报文寄存器地址错误
17	未知错误

Modbus RTU 的通信控制字：7 字节,每字节含义如下

注：串口必须使能后，才可进行数据通讯

- 第 1 字节:0 位 Modbus 串口功能是否启用。1 启用，0 不启用。第 1 位 :清除故障码，当检测到上升沿 (0→1) 时，通讯状态监控清零。 其他位保留。
- 第 2 字节:槽号:2-9 触发位。
- 第 3 字节:槽号:10-17 触发位。
- 第 4 字节:槽号 18-25 触发位。
- 第 5 字节:槽号:26-33 触发位。
- 第 6 字节:槽号:34-41 触发位。
- 第 7 字节:槽号:42-49 触发位。

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
第 2 字节							
子插槽 9	子插槽 8	子插槽 7	子插槽 6	子插槽 5	子插槽 4	子插槽 3	子插槽 2
第 3 字节							
子插槽 17	子插槽 16	子插槽 15	子插槽 14	子插槽 13	子插槽 12	子插槽 11	子插槽 10
第 4 字节							
子插槽 25	子插槽 24	子插槽 23	子插槽 22	子插槽 21	子插槽 20	子插槽 19	子插槽 18
第 5 字节							
子插槽 33	子插槽 32	子插槽 31	子插槽 30	子插槽 29	子插槽 28	子插槽 27	子插槽 26
第 6 字节							
子插槽 41	子插槽 40	子插槽 39	子插槽 38	子插槽 37	子插槽 36	子插槽 35	子插槽 34
第 7 字节							
子插槽 49	子插槽 48	子插槽 47	子插槽 46	子插槽 45	子插槽 44	子插槽 43	子插槽 42

Modbus TCP 的通信状态监控字：5 字节,每字节含义分别如下

第 1 字节:出错槽号

第 2 字节:错误码见下图:

第 3 字节:0 位没用,1-7 位依次指示 socket1-7 连接状态。1 连接, 0 未连接

第 4 字节:0 位:指示 Socket8 连接状态。其他位保留。1 连接,0 未连接

第 5 字节:保留未使用

错误码	描述
1	从站回复 Modbus 标准错误: ILLEGAL FUNCTION
2	从站回复 Modbus 标准错误: ILLEGAL DATA ADDRESS
3	从站回复 Modbus 标准错误: ILLEGAL DATA VALUE
4	从站回复 Modbus 标准错误: SLAVE DEVICE FAILURE
10	主站接收的报文长度错误, 太长, 太短或与正确的从站回复数据长度不符
11	主站接收的报文 CRC 校验错误
12	主站接收的报文寄存器数量错误
13	主站接收的报文从站地址错误
14	主站接收超时
15	主站接收的报文中功能码与请求的不一致
16	主站接收的报文寄存器地址错误
17	未知错误
19	TCP 连接错误:TCP CONNECT ERR

Modbus TCP 的通信控制字：9 字节,每字节含义分别如下

注：每个 socket 必须使能后，才可进行数据通讯

第 1 字节:0 位清除报警.上升沿触发。1-7 位控制 0-7 的 socket 使能。1 使能, 0 不使能。使能后客户端会去连接对应的 Modbus TCP 从站。不使能时将会断开连接。(通过状态字的第 3 字节, 第 4 字节可以观察 socket 是否连接成功)

第 2 字节:0 位指示 socket8 使能。1 使能, 0 不使能。其他位保留未使用

第 3 字节:保留未使用

第 4 字节:槽号:2-9 触发位。

第 5 字节:槽号:10-17 触发位。

第 6 字节:槽号:18-25 触发位。

第 7 字节:槽号:26-33 触发位。

第 8 字节:槽号:34-41 触发位。

第 9 字节:槽号:42-49 触发位。

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

Modbus RTU 主站子模块参数

每条 Modbus RTU 主站命令有五个属性：

Slave Address(1~247):表示 Modbus RTU 从站设备的地址，可选择范围 1-247。

Function Code:Modbus RTU 主站的功能码,根据插入插槽的 Modbus 命令自动生成功能码，不可更改。

Start Address :对 Modbus RTU 从站数据操作的开始地址。非寄存器 PLC 地址,无前缀。范围 0-65535。

XX Quantity :表示读写的线圈或者寄存器个数。据插入插槽的 Modbus 命令自动生成，可在范围内进行数量更改。

Transmission Type :提供以下四种发送类型。

Disable:表示该命令不执行。

Poll trigger(轮询发送): Modbus RTU 对应的主站使能后,该报文会按照插槽号从小到大的顺序依次发送。

Leve ltrigger(电平发送): 槽号对应的控制发送标志位由 0 变到 1 后:对于读指令，该报文会被发送。对于写指令，如果数据有改变才会被发送;槽号对应的控制发送标志位由 1 变到 0 后，不论是读报文还是写报文都会停止发送。(上节为例，PLC 地址 QB2-QB5 就是发送触发控制位)

Rising trigger(上升沿发送): 槽号对应的触发控制位由 0 变到 1 后，该报文会发送一次。(上节为例，PLC 地址 QB2-QB5 就是发送触发控制位)

Modbus RTU 从站子模块参数

每条 Modbus RTU 从站命令前缀为 Input 或 Output。Input 表示数据输入 PLC,即主站写数据给从站,

从站又将数据交给 PLC，对应写类型的命令。Output 表示数据从 PLC 输出，即 PLC 将数据交给从站，主站再来读从站的数据，对应读类型的命令。更具体一点，每条从站命令最后都标明了支持的功能码。

功能码	功能	操作地址区域(非寄存器 PLC 地址)	操作类型
01H	读取多个线圈输出状态	0XXXX	读
02H	读取多个输入线圈状态	1xXX	读
03H	读取多个保持寄存器	4xXX	读
04H	读取输入寄存器	3XXXX	读
05H	强置单个线圈	0XXXX	写
06H	预置单个保持寄存器	4XXXX	写
0FH	强置多线圈	0xXXX	写
10H	预置多个保持寄存器	4XXXX	写

Modbus TCP 主站子模块参数

每条 Modbus TCP 主站命令有五个属性

其中,Function Code; Start Address;; Coil Quantity; Trigger Type 同 Modbus RTU 主站配置功能一样
Socket Config selection(1-8):选择该条指令使用哪一个 socket 进行工作。

Modbus TCP 从站子模块参数

同 Modbus RTU 从站子模块参数类同。

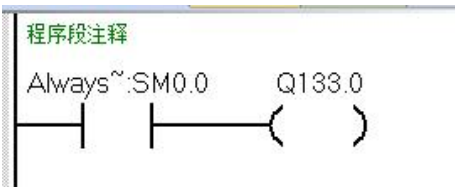
6.5.1. 串口使能例程

查询控制字

单击“添加”按钮来为该设备添加模块。

	子模块名	插槽_子插槽	PN1 起始地...	输入长度 (...	PNQ 起始...	输出长度 (...	固件版本
52		1 49					
53		2	133	5	133	7	1.0
54		2 2					
55		2 3					
56		2 4					
57		2 5					

对串口进行使能

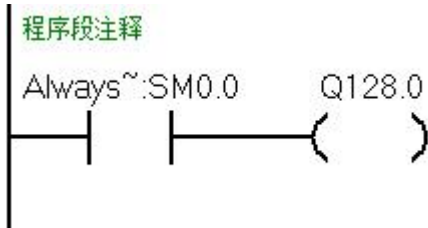


6.5.2. 网口 socket 使能例程

查询控制字

	子模块名	插槽_子插槽	PN1 起始地...	输入长度 (...)	PNQ 起始...	输出长度 (...)	固件版本
1		0					V1.0.0
2	X1	0 32768					
3	X1 P1	0 32769					
4		1	128	5	128		1.0
5		1 2					
6		1 3					

对 socket1 进行使能



6.6 使用 STEP 7 修改模块名称和查询 IP 地址

在通过 STEP 7-MicroWIN SMART 的 Profinet 工具搜索网关设备，为网关配置唯一的工作“站名”，用于 PLC 与对应网关进行通信；



打开工具选择与网关连接的电脑网卡，选择网关配置“站名称”，如有多个模块，可通过闪烁指示灯定位需要配置的网关设备；



第七章 注意事项

1. 通讯连接不上时（数据指示灯不闪烁），重点检查是否使能（参考“配置状态字和控制字章节”）
2. 修改的 Modbus 指令组态组态配置，下载 PLC 程序后连接不上，需要重启网关；
3. PLC 编译时报错“不支持的启动模式”，需要使用最新 GSD 文件，使用时，需要将旧 GSD 文件移除；
4. 错误事件：CRC Check Error/Frame Length Error/SLave Address Error 时，请将 Slave Response Timeout(ms) 和 Frame interval(m; s)这两个参数设置长一点，如何找到此参数，参考“配置 Modbus 通讯参数”章节
5. 组态添加的设备名需要和设备保持一致，如不一致请参考“修改模块名称和查询 IP 地址”章节；
6. 串口上接入设备过多，或者接线很长，需加 120 Ω 终端电阻；
7. 支持 RT 实时通讯，兼容 Profinet IO V2.3；
8. 可以使用 Codesys 进行软件组态；

注：排除上述问题仍无法解决故障，截取组态软件诊断缓冲区（事假日志）报错信息，提交售后技术协助处理。

第八章 重要声明

- 亿佰特保留对本说明书中所有内容的最终解释权及修改权。
- 由于随着产品的硬件及软件不断改进，本说明书可能会有所更改，恕不另行告知，最终应以最新版的说明书为准。
- 使用本产品的用户需到官方网站关注产品动态，以便用户及时获取到本产品的最新息。
- 本产品严禁用于军事及生命安全相关场景，违规使用责任由使用人自负

修订历史

版本	修订日期	修订说明	维护人
1.0	2026-8-14	初始版本	LT

关于我们



销售热线：4000-330-990

技术支持：support@cdebyte.com

官方网站：www.ebyte.com

公司地址：四川省成都市高新西区西区大道 199 号 B5 栋

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