

使用 STEP 7 加载设备教程

1、 连接前准备

1.1. 备好需要的 XML 文件，如下所示：

GSDML-V2.3-EBYTE-PN1-S25-20241025.xml（以官网提供的最新文件为准）

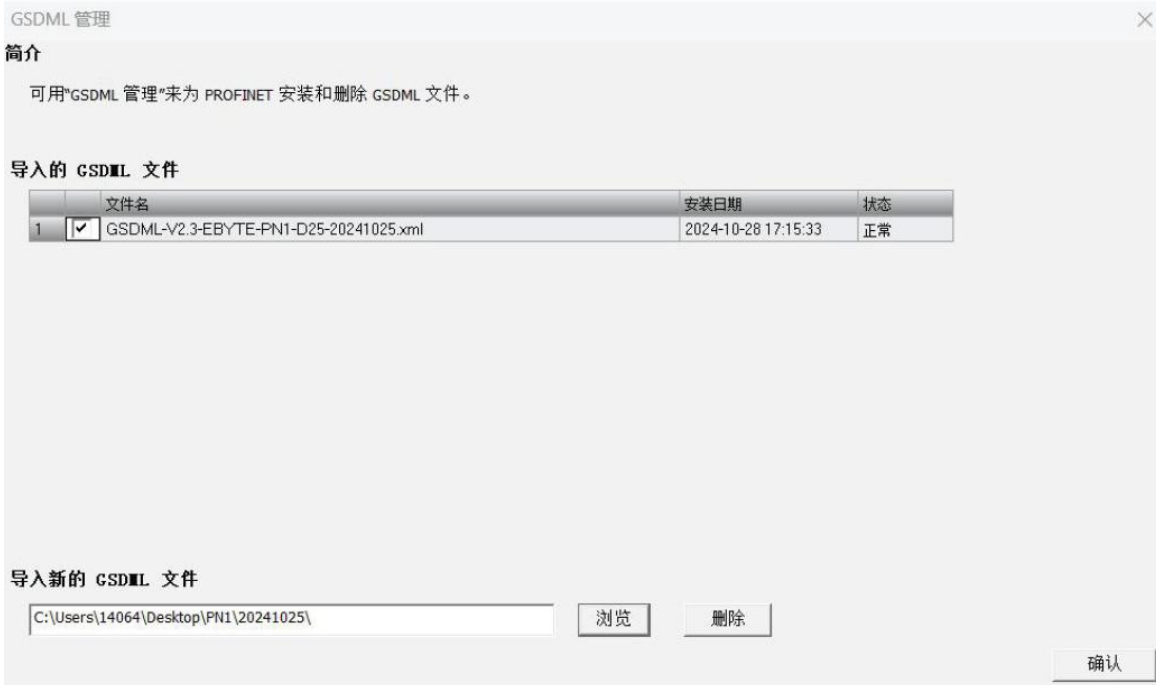
1.2. 使用网线将模块连接到 PLC 控制器的 Profinet 接口上。（在同一个网段）

2、 STEP 7 添加 GSDML 文件

2.1. 在文件菜单下，进入 GSDML 管理



2.2 添加 GSDML 文件

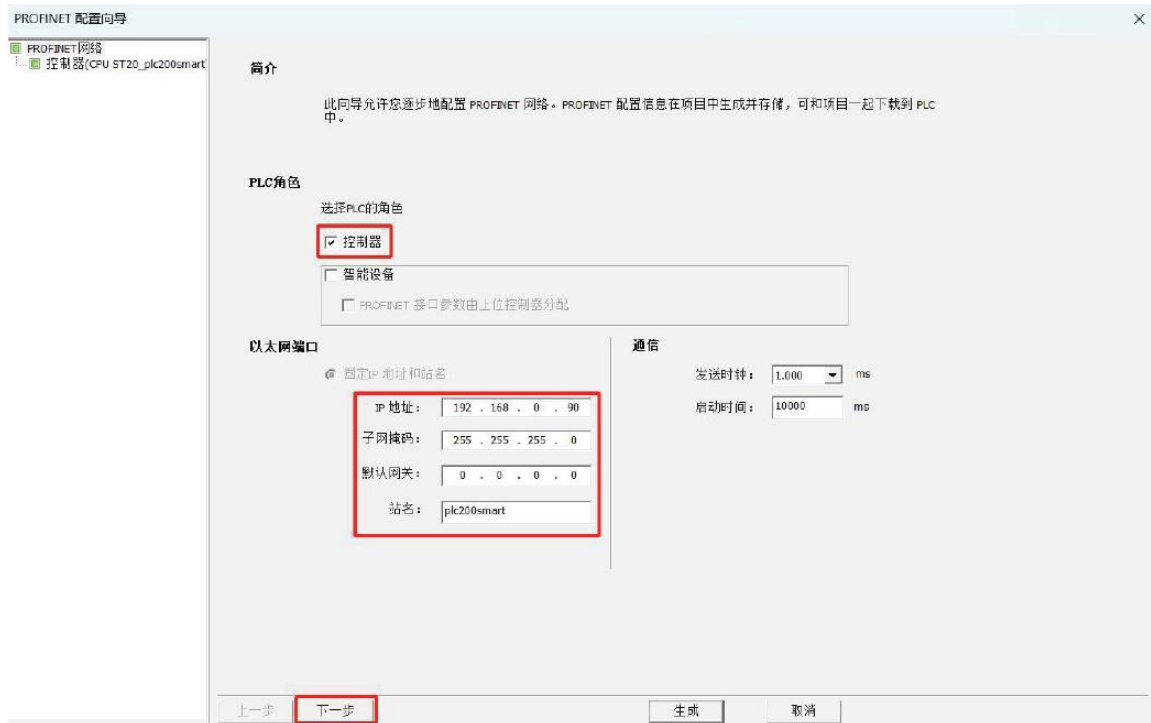


3、 项目添加 Profinet 设备

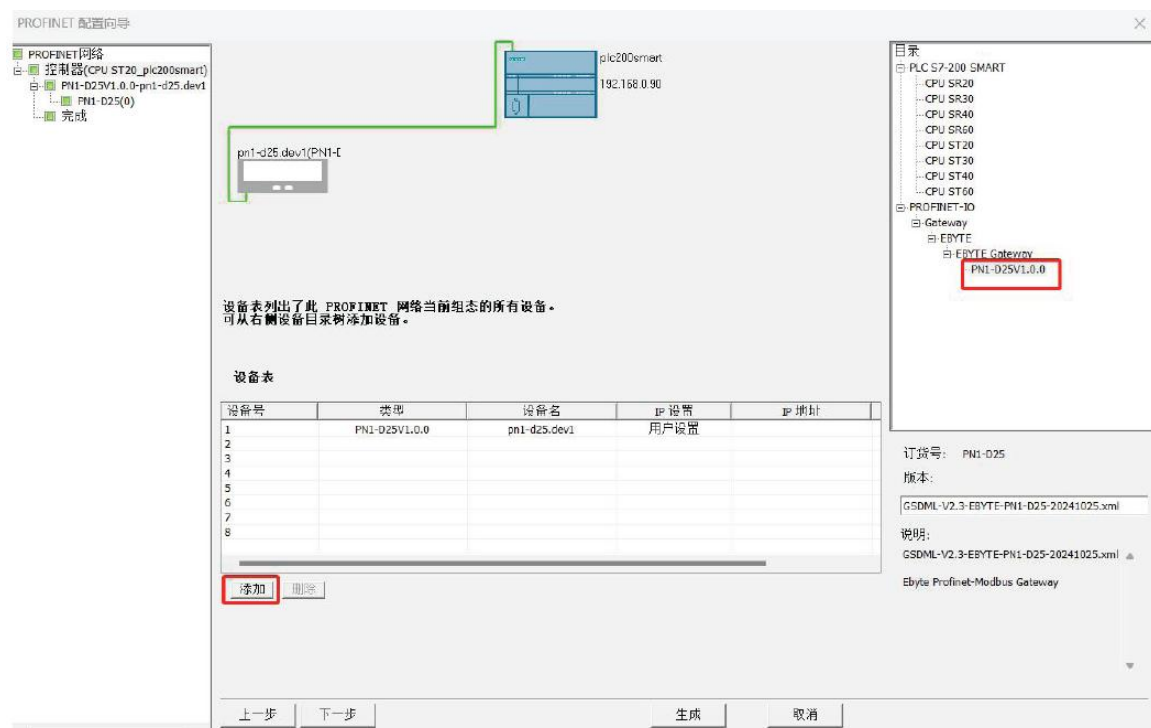
3.1. 选择工具菜单下面的 PROFINET 命令



3.2 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。

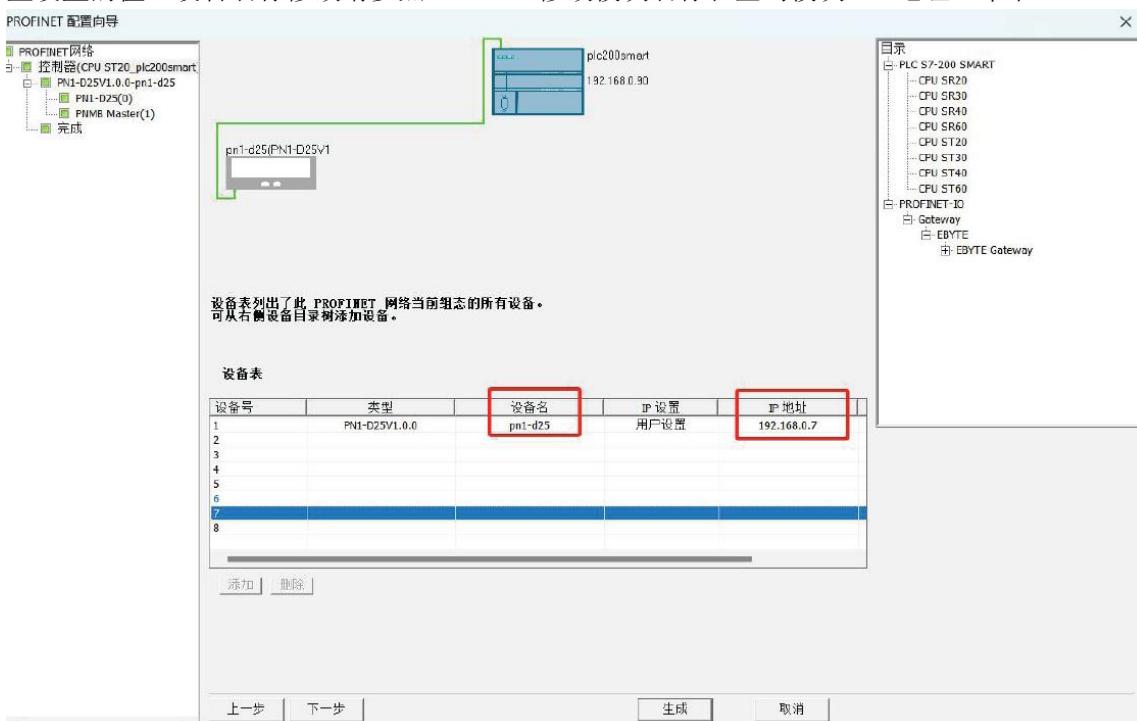


在右边栏中 PROFINET-IO→Gateway→EByte→TION→EByte Gateway→PN1-S25V1.0.0 单击选中，然后按住左键，将其拖入左侧表格内。



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。



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功能模块，每个槽位可容纳 32 个子槽，用于配置 Modbus 指令子模块。特别地，一号子槽分别对应设备的串口状态字和串口控制字（适用于 PNMB Master/PNMB Slave 配置）。通过状态字，PLC 能够获取 PN1-S25 设备的运行状况；而通过控制字，则可以让 PLC 对 PN1-S25 设备进行操控。若要调整 PN1-S25 设备串口 1 或串口 2 的 Modbus 接口参数，请先选定目标槽位（即一号或二号），接着选择“属性”选项。在此过程中，需预先选择串口的工作模式（PNMB aster/PNMB Slave）——Modbus

RTU 主站或从站模式。值得注意的是，PN1-S25 模块兼容 Modbus RTU 主站及从站两种工作方式。

PN1-S25 模块 Modbus 通讯接口参数：

PNMB 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 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。

注: 串口 2 与串口 1 配置一样

5、配置 Modbus 报文（功能码）

在设备概览中一共有 2 个槽位，这 2 个槽位是用来配置串口信息及主从站选择的，为状态字和控制字已被占用，剩下 64 子槽位（每个串口指令各 32 子槽位）可供配置 Modbus 报文（命令）。单击右侧硬件目录中的模块，给串口提供主从站选择，分别是 PNMB Master（为状态字和控制字已被占用需配置串口相关参数）和 PNMB Slave（为状态字和控制字已被占用需配置串口相关参数）；单击子模块，可以选择里面的相应 Modbus RTU 命令。直接左键双击硬件目录中的报文，就可以按照空白的槽位顺序将报文配置到 Modbus 报文队列中。

Modbus RTU 主站命令

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 从站命令

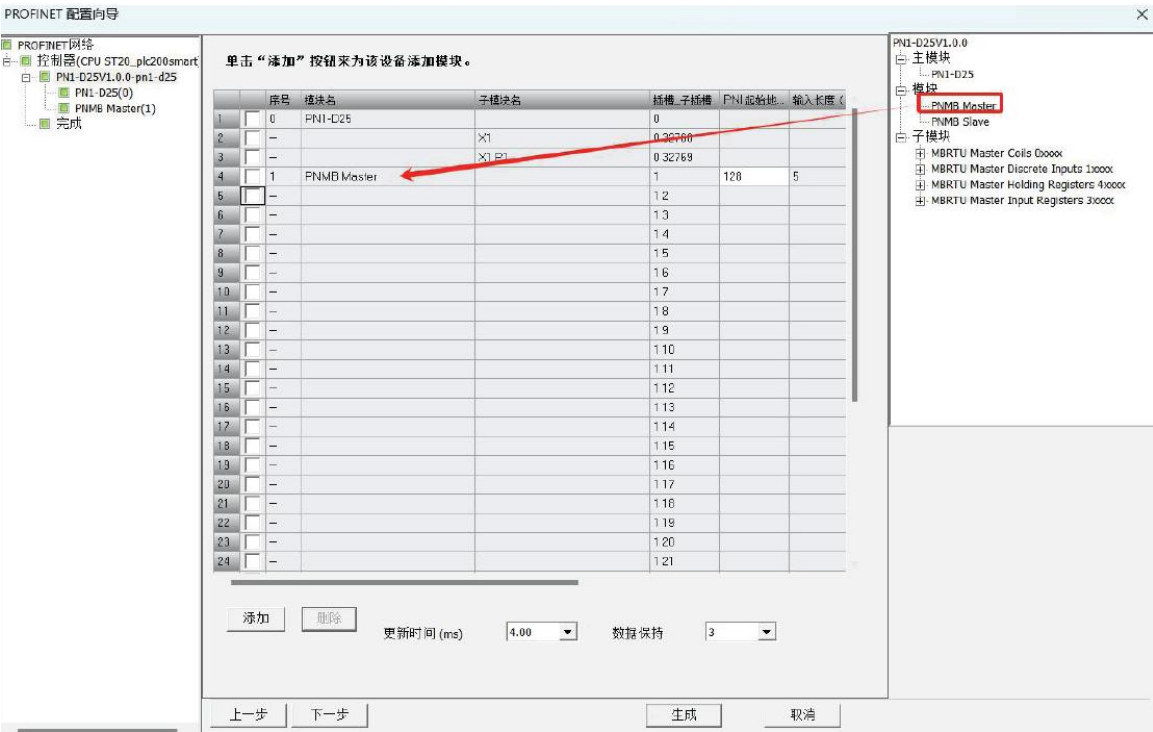
每条 Modbus RTU 从站命令前缀为 Input 或 Output。Input 表示数据输入 PLC, 即主站写数据给从站, 从站又将数据交给 PLC, 对应写类型的命令。Output 表示数据从 PLC 输出, 即 PLC 将数据交给从站, 主站再来读从站的数据, 对应读类型的命令。更具体一点, 每条从站命令最后都标明了支持的功能码。

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	读取多个保持寄存器	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

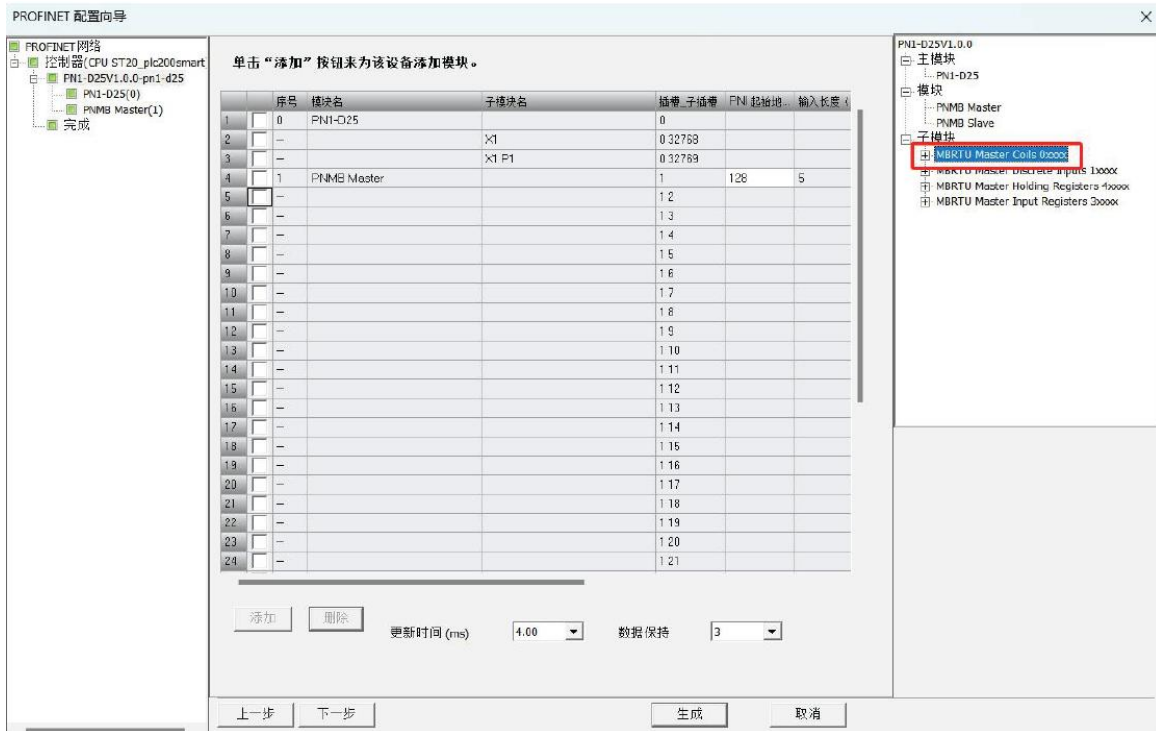
5.1 例程

将设备串口 1 设置为主站写入 8 位的线圈。

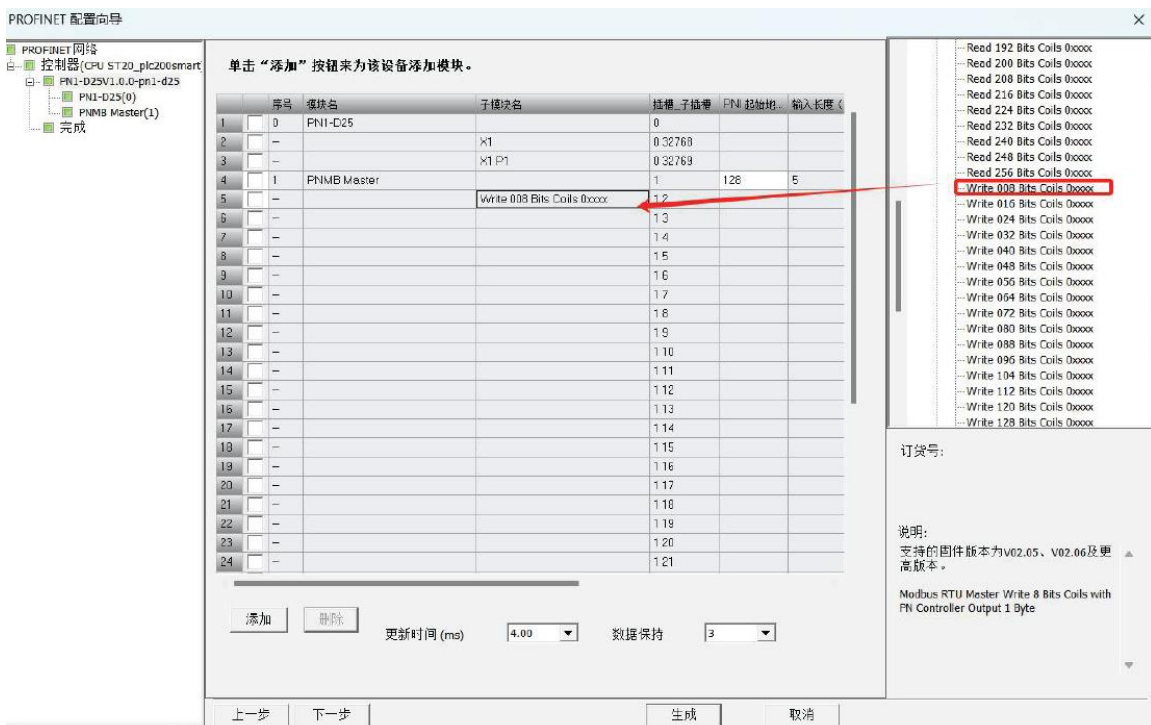
第一步：将 PNMB Master 拖入槽 1，



第二步：选择子模块 MBRTU Master Coils 0xxxx 内的指令



第三步：选择 MBRTU Write 008 bits 0xxxx



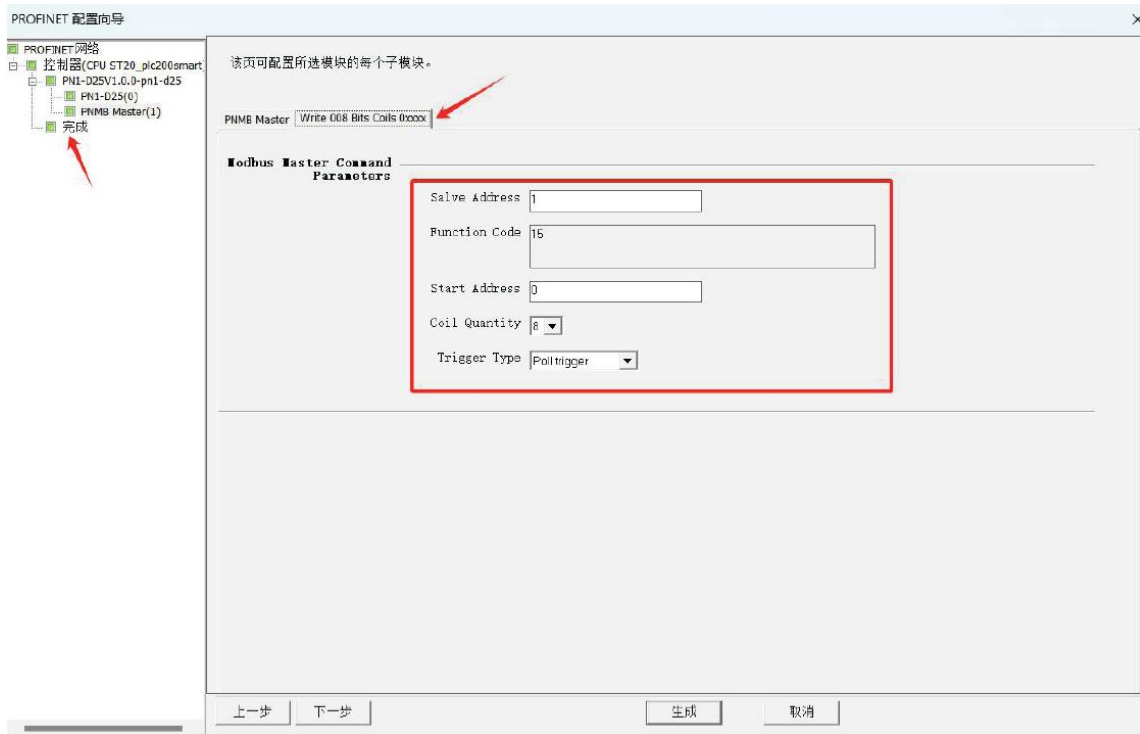
第四步：配置网关串口的工作参数，选择刚才添加的主机模块（PNMB Master），这里需要根据 RTU 工作的串口参数配置网关的串口参数



配置寄存器信息，用于 Profinet 网关与 RTU 通信；



然后点击完成，查看设备对应的地址，最后点击生成



6、配置状态字和控制字

从设备概览配置中可以看到槽号 1，只能用于选择 PNMB Master/PNMB Slave，其中 I 地量一栏中，对应的 Profinet 输入地址 IB128-132，为通讯状态监控位。Q 地址一栏中，对应的 Profinet 输出地址 QB128-132，QB128 为本总线转换模块的通信控制字(control)，QB129-132 为每条报文发送的控制位。

通讯状态监控：

第 1 字节:串口 1 出错的槽号

第 2 字节:串口 1 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: 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

通讯控制位：

Bit 0: Modbus 功能串口接口是否启用，1=启用，0=不启用；
Bit 1: 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 字节到第 5 字节：

每一个槽的报文对应一位。对应形式如下表。

当报文配置为上升沿触发时，将该位由 0→1 时，报文启用一次发送。

当报文配置为电平触发时，将该位置 1 时，报文启用循环发送，置 0 时，报文停止循环发送。

第 2 字节							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
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							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
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							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
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							
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
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

槽 2 同槽 1 配置状态字和控制字一致。

7、 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；

