ODOT-PNM02 V2.0

协议转换器

用户手册

V1.7

2022.02.08

Modbus-RTU/ASCII 或非标协议转 ProfiNet 协议转换器

四川零点自动化系统有限公司

2018-03

版权©2019 四川零点自动化系统有限公司保留所有权利

版本信息

对该文档有如下的修改：

日期	版本号	修改内容	作者
20180301	V1.0	发布版本	CCL
20180801	V1.1	更新内容	CCL
20190520	V1.2	增加在 Step7 中使用的相关描述	LJP
20190924	V1.3	新增自由口模式	CCL
20191118	V1.4	新增自由口模式在 TIA/STEP7 V5.5/STEP 7-MicroWIN SMART 的应用	CCL
20200722	V1.5	硬件改版成小蛮腰外形，产品硬件说明更新。	CCL
20200824	V1.6	主站从站自由透传模式改成两串口独立设置	CCL
20220208	V1.7	硬件改版	CCL

所有权信息

未经版权所有者同意，不得将本文档的全部或者部分以纸质或者电子文档的形式重新发布。

免责声明

本文档只用于辅助读者使用产品，本公司不对使用该文档中的信息而引起的损失或者错误负责。本文档描述的产品和文本正在不断地开发和完善中。公司有权利在未通知用户的情况下修改本文档。

修订说明：

1、GSD 文件 20190312 及以上版本，网关从站模式时：避免客户使用 0 区和 4 区输出数据时发现地址重叠的问题，PN 输出数据使用 1 区和 3 区，输入数据使用 0 区和 4 区。

2、GSD 文件 20190803 及以上版本以适用 ABB　Profinet 主站系统。

3、固件 V1.6 版本及其以上版本增加功能:网关工作在透传模式时，串口选择主从应答模式的时候，同时支持数据主动上报功能。

4、ODOT-PNM02 V2.0 硬件改版，2 路串口独立设置工作模式，功能上不支持 IRT、MRP。

软件下载

请登录零点自动化官网 www.odot.cn，在对应的产品页面点击下载。

免责条款

产品使用

注意
• **在安装、操作和维护设备时，请勿超过电气特性中指定的任何额定值；** • **在安装、操作和维护设备时，请勿超过环境特性中指定的任何额定值。请勿在下列场所使用产品：有灰尘、油烟、导电性尘埃、腐蚀性气体、可燃性气体的场所；请勿暴露于高温、结露、风雨的场合；有振动、冲击的场合也会导致产品损坏；** **未按说明操作则设备提供的保护可能会失效，可能导致轻微身体伤亡或设备损坏。**

免责范围

本公司不对以下情况导致的设备损坏或故障承担任何责任：

1、运输损坏：由于不当运输或包装造成的设备损坏；

2、自然因素：雷击、电压波动、进水或自然灾害（如火灾、洪水等）造成的损坏；

3、不当使用：超负荷、不规范操作、私自改装或使用不合格配件导致的损坏；

4、未授权维修：未经授权的维修或改动所导致的设备故障；

5、其他非产品原因：与设备本身无关的其他原因引起的损坏。

维修服务

1、对于上述原因导致的损坏，本公司将根据实际情况收取维修费用。

2、保修期外，本公司提供有偿维修服务，费用依据维修情况收取。

风险承担

本公司不承担因设备使用过程中产生的人员伤亡、财产损失或其他相关损失。所有风险由使用者自行承担。

目录

一、产品概述.....8
1.1 产品功能.....8
1.2 功能特点.....9
1.3 技术参数.....10
二、硬件说明.....12
2.1 产品外观.....12
2.2 指示灯说明.....13
2.3 端子定义.....14
2.4 外接终端电阻.....15
2.5 安装尺寸.....16
三、产品应用.....17
3.1 网关工作模式.....17
3.2 网关默认参数.....17
3.3 网关读写指令模块.....19
3.3.1 主站模式下模块.....19
3.3.2 从站模式下模块.....20
3.3.3 自由口透传模式下模块.....21
3.4 网关设备名称修改.....23
3.4.1 使用 TIA 修改设备名称.....23
3.4.2 使用 Step7 修改设备名称.....25
3.4.3 使用 STEP 7-MicroWIN SMART 修改设备名称.....27
3.5 网关应用拓扑图.....28
四、在西门子 TIA V14 中使用本模块.....30
4.1 MODBUS 主站模式的配置.....30
4.2 MODBUS 从站模式的配置.....46
4.3 自由口透传模式的配置.....51
五、在西门子 STEP7 V5.5 中使用本模块.....57
5.1 MODBUS 主站模式的配置.....57

5.2 MODBUS 从站模式的配置.....73
5.3 自由口透传模式的配置.....79
六、在西门子 STEP 7-MicroWIN SMART 中使用本模块.....85
6.1 MODBUS 主站模式的配置.....85
6.2 MODBUS 从站模式的配置.....93
6.3 MODBUS 自由口透传模式的配置.....101
6.3.1 自由口透传模式简介.....101
6.3.2 自由口透传模式测试应用.....103
七、固件升级.....109
7.1 串口升级.....109
7.2 网口升级.....110
八、附录.....112
8.1 Modbus-RTU 协议简介.....112
8.1.1 Modbus 存储区.....112
8.1.2 Modbus 功能码.....112
8.2 串口网络拓扑结构简介.....117
8.2.1 RS232.....117
8.2.2 RS422.....119
8.2.2 RS485.....120

一、产品概述

1.1 产品功能

ODOT-PNM02 V2.0 网关是一种 Modbus-RTU/ASCII 或非标协议 转 ProfiNet 协议转换器。它能够实现 Modbus-RTU/ASCII 或非标协议到 ProfiNet 协议的转换。凡具有 RS485/RS232/RS422 接口支持 Modbus-RTU/ASCII 或非标协议的设备都可以使用本产品实现与工业总线 ProfiNet 的互连。如：PLC、DCS、分布式 IO、变频器、扫描枪、电机启动保护装置、智能高低压电器、电量测量装置、智能现场测量设备及仪表等。

注意：

模块右侧打标型号为：ODOT-PNM02，GSD 文件采用 GSDML-V2.33-ODOT-PNM02-20191008.xml 的 PNM02 V1.5 的 GSD 组态。

模块右侧右侧打标型号为：ODOT-PNM02 V2.0，GSD 文件采用 GSDML-V2.33-ODOT-PNM02-V2.0 的 PNM02L V2.0 的 GSD 组态。

模块右侧右侧打标型号为：ODOT-PNM02 V2.1，GSD 文件采用 GSDML-V2.33-ODOT-PNM02-V2.0 的 PNM02L V2.1 的 GSD 组态。

1.2 功能特点

- 安装方式：35mm 标准导轨安装
- 尺寸：30*80*110mm
- 支持标准的 ProfiNet I/O Device V2.3
- ProfiNet 数据区：输入最大 1440 字节，输出最大 1440 字节。
- 支持 RT（同步）,不支持 IRT（等时同步）、MRP（介质冗余协议）、MRPD（介质路径规划冗余）功能。
- 最大槽位：50 个
- 串口隔离：光耦隔离、电源隔离
- 串口数量：支持双串口 RS485/RS232/RS422，2 串口独立工作
- 串口终端电阻：需外置 120Ω 电阻。
- 串口协议：支持 Modbus-RTU/ASCII 主站、Modbus-RTU/ASCII 从站、自由口透传协议。
- 串口参数：支持 1200-115200 波特率，支持无、奇、偶校验
- 串口支持的 Modbus 站点数：50 个（受槽位限制）
- 支持的 Modbus 功能码：01/02/03/04/05/06/15/16
- 工作电源：19.2~28.8VDC 输入，标称 24VDC
- 工作温度：-40~85℃
- 环境湿度：5%-95%(无冷凝)
- 防护等级：IP20

1.3 技术参数

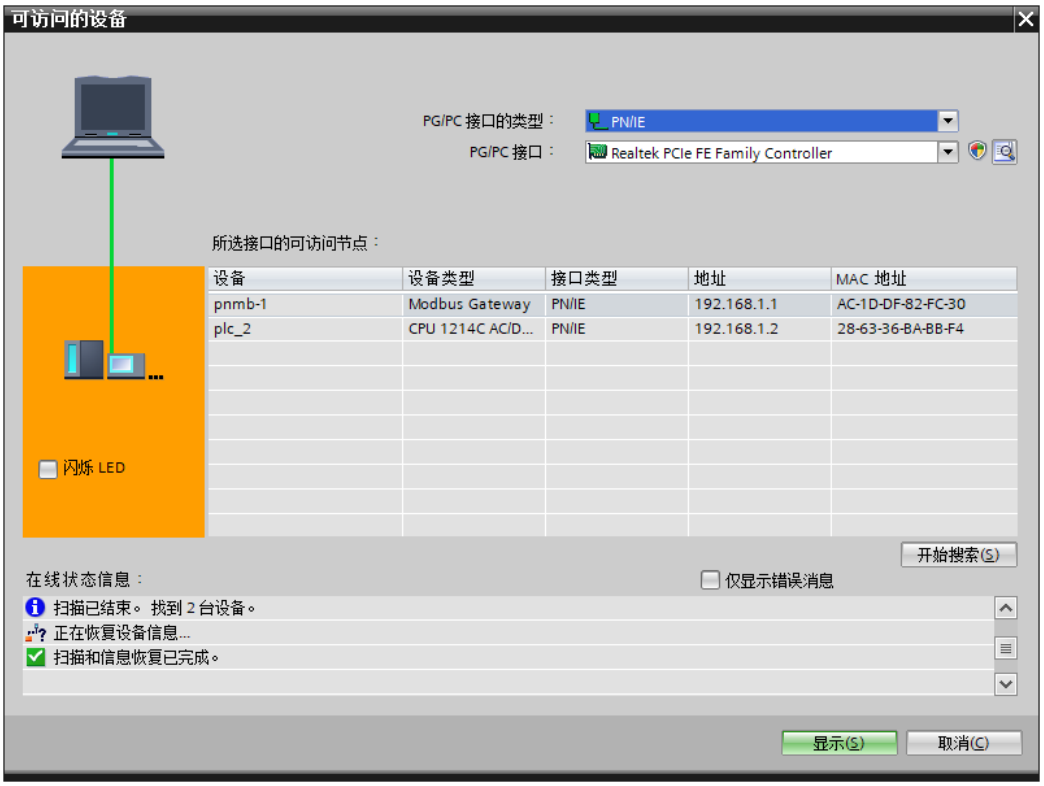
通用参数	
模块描述	Modbus 或私有协议转 Profinet 协议转换器
电源	19.2-28.8VDC（标称 24VDC）
电源保护	电源防反接保护
功耗	Max.86mA@24VDC
隔离	系统电源与 PE 隔离电压 AC 500V I/O 通道与 PE 隔离电压 AC 500V 系统电源与 I/O 通道间隔离电压 AC 500V
电源接线端子	2*3P 弹簧端子
接线线径	Max.1.0mm²(AWG 17) Min.0.2mm²(AWG 24)
尺寸	110*30*80mm
安装方式	35mm 导轨安装
重量	130g
壳体	铝合金
垂直安装工作温度	-40~85℃
水平安装工作温度	-40~75℃
相对湿度	5%~95%RH，无冷凝
存储温度	-55℃~125℃
存储湿度	5%~95%RH，无冷凝
制造测试温度	-40℃~75℃
防护等级	IP20
抗振性能	符合 IEC 61131-2、IEC 60068-2-6 标准
抗冲击性能	符合 IEC 61131-2、 IEC 60068-2-27 标准
EMC 性能	符合 IEC 61131-2、IEC 61000-4 标准
以太网通讯参数	
网口数量	2*RJ45（Port1、Port2）
通讯协议	PROFINET
标准协议	ProfiNet I/O Device
网口参数	10/100Mbps，自适应，全双工
数据区	输入最大 1440 字节，输出最大 1440 字节
默认设备 IP 地址	192.168.0.254
默认设备名称	pnmb-address
RT	支持
IRT	不支持
MRP	不支持

MRPD	不支持
向下兼容	不支持
串口通讯参数	
串口数量	2 *RS485/RS232/RS422
接线端子	16P 螺钉接线端子
通讯协议	Modbus RTU/ASCII、私有协议
工作模式	Modbus 主站 Modbus 从站 自由透传（主动上报、应答模式）
串口独立	两串口工作模式独立
串口参数	300~500000bps 无校验、奇校验、偶校验
终端电阻	需外置 120Ω终端电阻
Modbus 从站数量	50 个（受 TIA 槽位限制）
读写指令数	50 个（受 TIA 槽位限制）
Modbus 功能码	01 / 02 / 03 / 04 / 05 / 06 / 15 / 16
升级软件	Firmware Update Tool（网口、串口）

二、硬件说明

2.1 产品外观

上面板有两个 ProfiNet 接口和电源接线端子。PORT1 与 PORT2，两个接口功能相同，此两接口具有交换机功能，即上位机电脑可以通过 PORT1 接口访问连接于 PORT2 上的设备，如下图（电脑 IP 为 192.168.1.92，电脑接 PORT2 口，西门子 S7-1200 接 PORT1 口）,上位机软件可搜索到同一个 ProfiNet 网络中的设备。



2.2 指示灯说明

设备共有六个 LED 状态指示灯，其符号定义及状态说明如下表所示。

符号	定义	状态	说明
PWR	电源指示	红灯常亮	电源接通
		红灯灭	电源未接通
DF	设备状态指示	红灯常亮	设备故障
		绿灯常亮	设备正常
		红绿交替闪烁	组态错误
SF	系统状态指示	红灯常亮	系统故障
		红灯闪烁	点灯测试
		红灯灭	系统正常
BF	总线状态指示	红灯常亮	网线没接通
		红灯闪烁	总线组态没配置好
		红灯灭	总线正常
CO1	串口 1 状态指示	绿灯闪烁	串口 1 有数据收发
		绿灯灭	串口 1 无数据收发
CO2	串口 2 状态指示	绿灯闪烁	串口 2 有数据收发
		绿灯灭	串口 2 无数据收发

2.3 端子定义

设备接线采用 16Pin 3.81mm 间距拔插式接线端子，RS485 接口的端子定义如下表所示。

序号	标识	接线定义		
		RS485	RS232	RS422
1	1TA+	串口 1 (A+)		串口 1 (TX+)
2	1TB-	串口 1 (B-)		串口 1 (TX-)
3	1R+			串口 1 (RX+)
4	1R-			串口 1 (RX-)
5	GND	公共地(信号地)		
6	1TX		串口 1 (TX)	
7	1RX		串口 1 (RX)	
8	PE	屏蔽地		
9	2TA+	串口 2 (A+)		串口 2 (TX+)
10	2TB-	串口 2 (B-)		串口 2 (TX-)
11	2R+			串口 2 (RX+)
12	2R-			串口 2 (RX-)
13	GND	公共地(信号地)		
14	2TX		串口 2 (TX)	
15	2RX		串口 2 (RX)	
16	PE	屏蔽地		

电源接口的端子定义如下表所示。

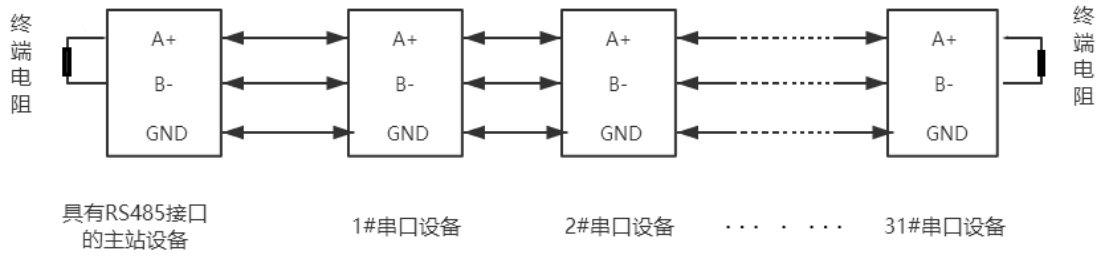
序号	端子	定义
1	PE	接地
2	V-	24Vdc-
3	V+	24Vdc+

2.4 外接终端电阻

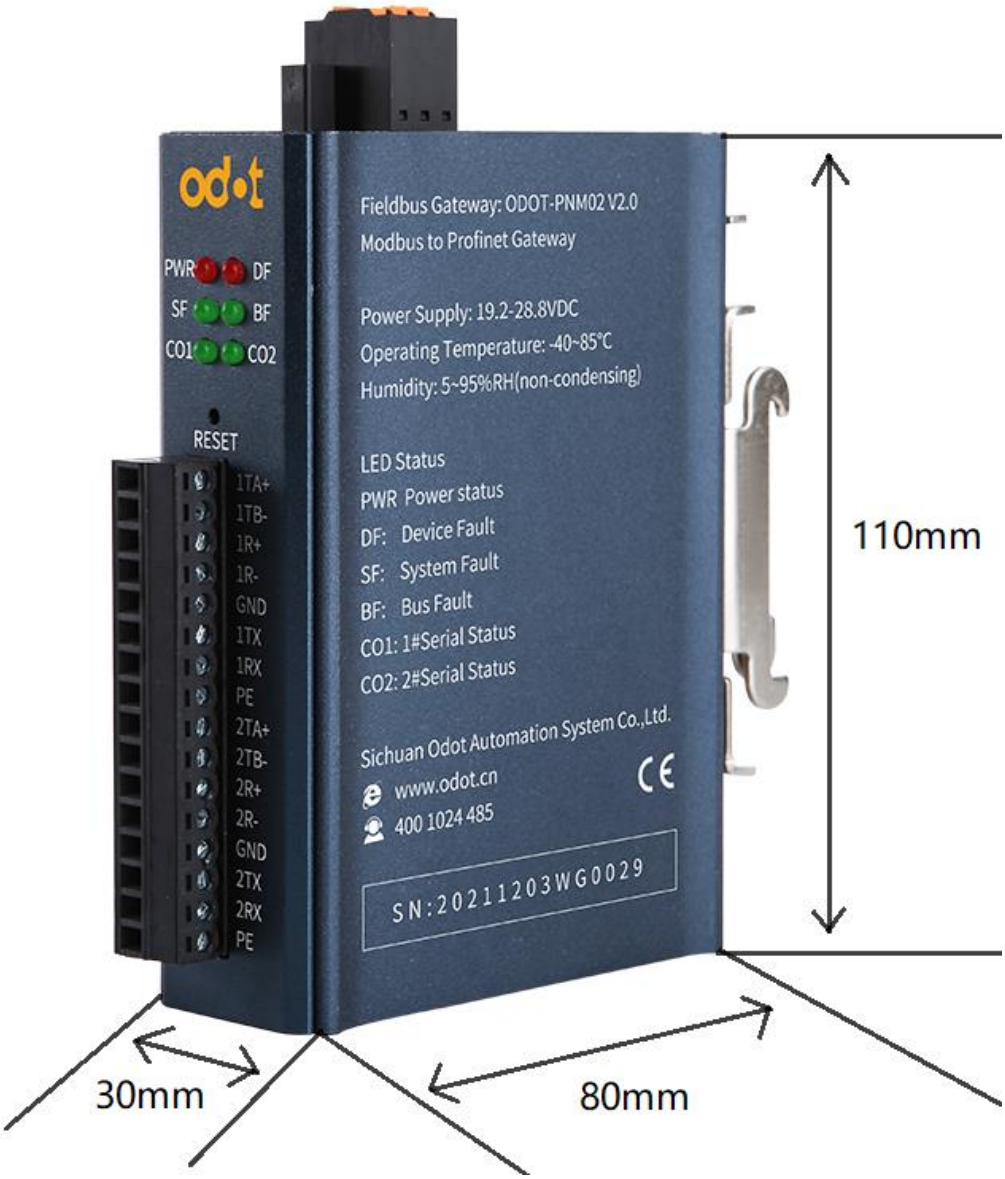
根据现场实际情况，网关串口侧需外接 120Ω 终端电阻。RS485 总线在不加中继的情况下最大支持**32 个**节点，节点与节点之间采用“**菊花链**”的连接方式，在通讯电缆两端需加终端电阻，要求其阻值约等于传输电缆的特性阻抗。在短距离传输时可不需终接电阻，即一般在 300 米以下不需终接电阻。终接电阻接在传输电缆的最两端。

网关在现场应用时，若现场 RS485 总线距离远，现场干扰大就需要在 RS485 总线两端添加 120Ω 终端电阻，以防止串行信号的反射。

注：120Ω 电阻附在包装盒内，注意查收。



2.5 安装尺寸


Fieldbus Gateway: ODOT-PNM02 V2.0
Modbus to Profinet Gateway
Power Supply: 19.2-28.8VDC
Operating Temperature: -40~85℃
Humidity: 5~95%RH(non-condensing)
LED Status
PWR Power status
DF: Device Fault
SF: System Fault
BF: Bus Fault
CO1: 1#Serial Status
CO2: 2#Serial Status
Sichuan Odot Automation System Co.,Ltd.
www.odot.cn
400 1024 485
SN:20211203WG0029
PWR
DF
SF
BF
CO1
CO2
RESET
1TA+
1TB-
1R+
1R-
GND
1TX
1RX
PE
2TA+
2TB-
2R+
2R-
GND
2TX
2RX
PE
110mm
30mm
80mm

三、产品应用

3.1 网关工作模式

该网关的每路串口都具有三种工作模式：**Modbus 主站、Modbus 从站，自由口透传模式。**

串口工作于主站模式时，该串口最多可以连接 31 台 Modbus RTU/ASCII 从站设备；该模式主要用于 ProfiNet 主站与 Modbus RTU/ASCII 从站之间的数据通讯。

串口工作于从站模式时，该串口可以连接至 1 台 Modbus RTU/ASCII 主站设备；实现 ProfiNet 主站与 Modbus RTU/ASCII 主站之间的数据通讯。

串口工作于**自由口透传**模式时，该串口可以连接至 1 台串口设备；实现 ProfiNet 主站与串口设备之间的数据通讯。

3.2 网关默认参数

ProfiNet 配置参数：

网关默认 IP 地址：192.168.0.254，设备名称：默认：pnmb-address。实际在应用的时候需要修改设备名称。组态时，注意配置设备名称和实物名称保持一致。

串口配置参数：

注：M 表示该参数主站模式有效，S 表示该参数从站模式有效，F 表示该参数自由口透传模式有效。

M/S/F :网关工作模式：Modbus 主站、Modbus 从站、自由口透传可选，**默认** Modbus 主站。

M/S/F:波特率选择：标准波特率、自定义波特率可选，默认值：标准波特率。

M/S/F :标准波特率：串口波特率，300-500000bps 可选，**默认 9600bps。**

M/S/F :自定义波特率：0,300-500000bps 可设，**默认 9600bps。**注：少数客户的设备是非标波特率，就可以自定义。

M/S/F :数据位：7 位、8 位可选，**默认 8 位。**

M/S/F :校验位：无、奇、偶、字符、空格校验可选，**默认无校验。**

M/S/F :停止位：1 位、2 位，**默认 1 位。**

M/S :串行模式：RTU/ASCII 模式可选，**默认 RTU 模式。**

M/S/F :字符间隔：接收报文时的帧间隔检测时间，1.5t~2000t 可选，**默认 5t**。（t 为单个字符传送的时间，和波特率有关）。

M/F : 响应超时时间(ms)：主站发送命令后，等待从站响应的时间。1~65535 可选，**默认 500。**

M :轮询延时时间(ms)：Modbus 命令发送的间隔时间(收到从站响应报文到发送下一条命令的延时)，0~65535 可选，**默认 10。**

M :读指令错误处理方式：从站读数据超时后，数据处理方式，保持最后一次输入值、清零输入值可选，**默认保持最后一次输入值。**

M :输出模式：轮询、事件触发（数据发生改变）可选，**默认轮询。**“轮询模式”下 Modbus 周期性地发送写报文。“事件触发”模式时只有 Modbus 输出数据发生变化时才发送写命令。

M :模块控制：禁止、使能可选，默认禁止。当需要对 Modbus 的读写命令进行控制时，选择使能模式，通过控制“模块控制输出”的值控制 Modbus 的读写命令。

M :控制模式：电平触发（持续有效）、上升沿触发（单次触发）可选，**默认电平触发（持续有效）。该值只在**模块控制**使能模式有效**

M :上电首次输出数据（指令）：使能、禁止可选，**默认使能。**

S :从站 ID 号：1-247 可设。该参数只在**从站模式**下有效。

S :响应延时(ms) ：0~65535 可选，**默认 50.**

3.3 网关读写指令模块

3.3.1 主站模式下模块

M:诊断模块

M:读线圈（0xxxx）支持8~200bits可选

M:读离散量输入（1xxxx）支持8~200可选

M:读输入寄存器（3xxxx）支持 1~125words 可选

M:读保持寄存器（4xxxx）支持1~125words可选

M:写线圈（0xxxx）支持single coil、8~200bits可选

M:写保持寄存器（4xxxx）支持 single register、1~125words 可选

M：诊断模块：包括模块状态输入、模块错误代码输入、模块控制输出、轮询时间输入；下拉菜单的命令需添加到插槽前 8 行。

1、模块状态输入：有 8~48 通道可选，模块状态可监测每一个数据插槽的工作状态，当某一个数据插槽出现故障时，对应的状态位被置 1，故障恢复后自动清零。

2、模块错误代码输入：有 1-48 个通道可选，当数据插槽出现故障时，错误代码模块可显示出现错误通道的功能码和具体的错误代码，用户可根据错误代码，判断是何种原因产生故障，进而采取对应的调整方法。详细的描述请参见**“Modbus 错误代码表”**。

3、模块控制输出：有 8~48 通道可选。当串口下参数（**M　:模块控制**）为**使能**模式时，该命令的输出控制读写通道有效。

4、轮询时间输入：用于监视串口的轮询时间。

模块从站输入状态可监控通讯故障，详细的描述请参见“Modbus 错误代码表”。

Modbus 错误代码表

错误代码	故障说明	故障排除方法

0x00	工作正常	无
0x01	非法功能码	设备不支持当前功能码，请参考从站手册选择对应的功能码模块
0x02	非法数据地址	设备数据超出其地址范围，参考从站手册修改数据起始地址或数据长度
0x03	非法数据值	数据长度错误，数据长度超出最大允许值125(Word)或2000(Bit)，修改长度
0x04	数据处理错误	检查数据值范围是否符合从站要求
0x05	应用层长度不匹配	增大接收字符间隔，检查通信参数设置
0x06	协议 ID 错误	检查发送端报文
0x07	缓存地址错误	设备内部错误
0x08	位偏移错误	设备内部错误
0x09	从站 ID 号不匹配	增大超时时间，检查硬件连接状态，检查通信参数设置
0x0A	CRC 错误	CRC 错误，检查通讯线路
0x0B	LRC 错误	LRC 错误，检查通讯线路
0x0C	应答功能码不匹配	检查硬件连接状态
0x0D	应答地址不匹配	检查硬件连接状态
0x0E	应答数据长度不匹配	检查硬件连接状态
0x0F	通信超时	增大超时时间，检查硬件连接状态，检查通信参数设置
0x10	ASCII 模式起始符错误	‘:’冒号起始符错误
0x11	ASCII 模式结束符错误	CR/LF 回车换行结束符错误
0x12	ASCII 模式非字符数据	数据中包含非16进制 ASCII 码
0x13	ASCII 模式字符数错误	从站应答长度错误

3.3.2 从站模式下模块

S :诊断模块

S :读线圈（0xxxx）支持 1~1024Bytes 可选

S :读保持寄存器（4xxxx）支持 1~512words 可选

S:写线圈（0xxxx）支持1~1024Bytes可选

S:写离散量输入（1xxxx）支持8~1024Bytes可选

S:写输入寄存器（3xxxx）支持 1~512words 可选

S:写保持寄存器（4xxxx）支持1~512words可选

S :诊断模块

3.3.3 自由口透传模式下模块

F :控制和状态模块

F :输入输出数据模块均支持 1~512words 可选

控制和状态模块的过程数据定义：

IO 模块数据方向	数据名称	变量名称	数据类型	字节偏移
输入数据	输出控制字-反馈	Control_Word_Feedback	uint16_t	0
	发送帧字节长度-反馈	Send_Data_Len_Feedback	uint16_t	2
	串口状态	COM_Status	uint16_t	4
	接收错误帧计数	Error_Counter	uint16_t	6
	接收总数据帧计数	Received_Counter	uint16_t	8
	当前接收帧字节长度	Received_Data_Len	uint16_t	10
输出数据	输出控制字	Control_Word	uint16_t	0
	发送帧字节长度	Send_Data_Len	uint16_t	2

变量定义：

变量名称	Bit15-6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Control_Word	Reserved	Received Counter Reset	Error Counter Reset	Timeout Error Reset	Parity Error Reset	Done Reset	Trigger
Send_Data_Len	Send_Data_Len						
COM_Status	Reserved			Timeout Error	Parity Error	Done	Busy
Error_Counter	Error_Counter						
Received_Counter	Received_Counter						

Received_Data_Len	Received_Data_Len

输入数据说明：

1. Control_Word_Feedback 为输出控制字 Control_Word 的反馈值，输出控制字刷新到模块后，将更新到控制字反馈中。

2. Send_Data_Len_Feedback 为发送帧字节长度 Send_Data_Len 的反馈值，发送帧字节长度刷新到模块后，将更新到发送帧字节长度反馈中。

3. 应答模式下，串口发送数据时，Busy 位被置 1。

3.1 当在超时时间内串口接收到应答后，Busy 位清零，Done 完成位置 1，Received_Counter 计数值加 1，若接收帧有奇偶校验错误，则 Parity_Error 位被置 1，同时 Error_Counter 计数加 1。Received_Data_Len 中保存当前接收帧的字节数。

3.2 当在超时时间内串口未接收到应答，Busy 位清零，Done 完成位置 1，同时设置 Timeout_Error 为 1，Error_Counter 错误计数值加 1，Received_Data_Len 值清零。

4.在主动上报模式下，从站收到数据包时，Received_Counter 计数值加 1，若接收帧有奇偶校验错误，则 Parity_Error 位被置 1，同时 Error_Counter 计数加 1。

输出数据说明：

1. Received_Counter_Reset 上升沿时，接收计数值 Received_Counter 被清零，
Error_Counter_Reset 上升延时，错误计数值 Error_Counter 被清零，
Timeout_Error_Reset 上升延时，Timeout_Error 被清零，
Parity_Error_Reset 上升延时，Parity_Error 被清零,
Done_Reset 上升延时，Done 被清零。

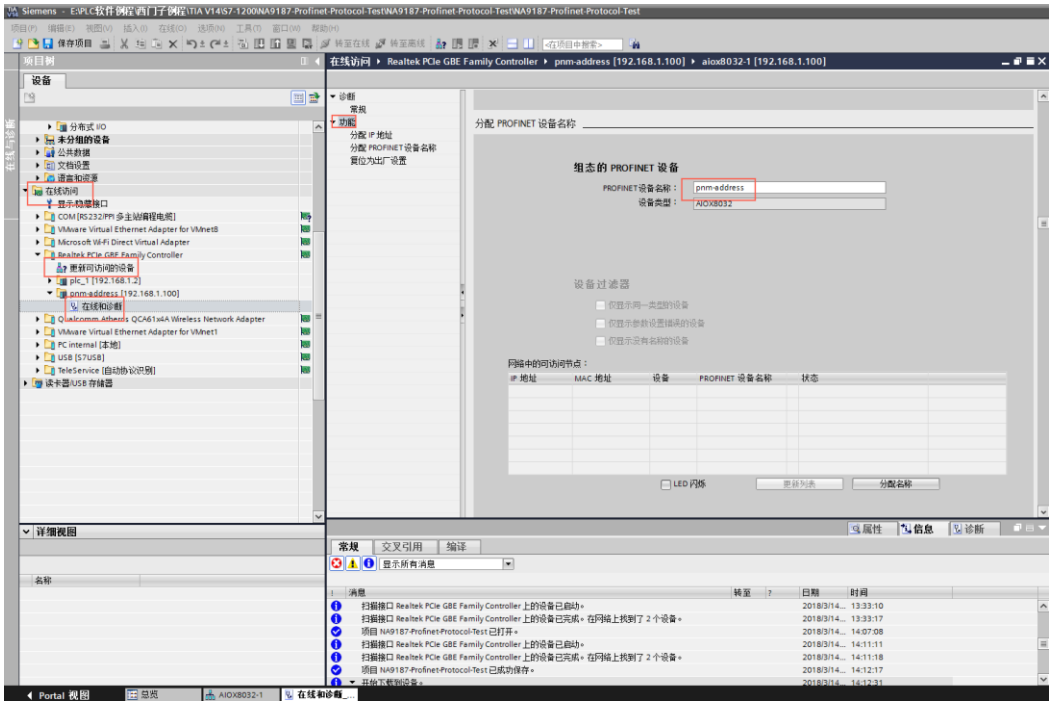
2.主动上报模式下，Trigger 位无效，Send_Data_Len 无效。

3.主从应答模式下，Trigger 上升延时触发一次串口数据发送，串口将按 Send_Data_Len 的数据长度发送数据包并等待应答处理。

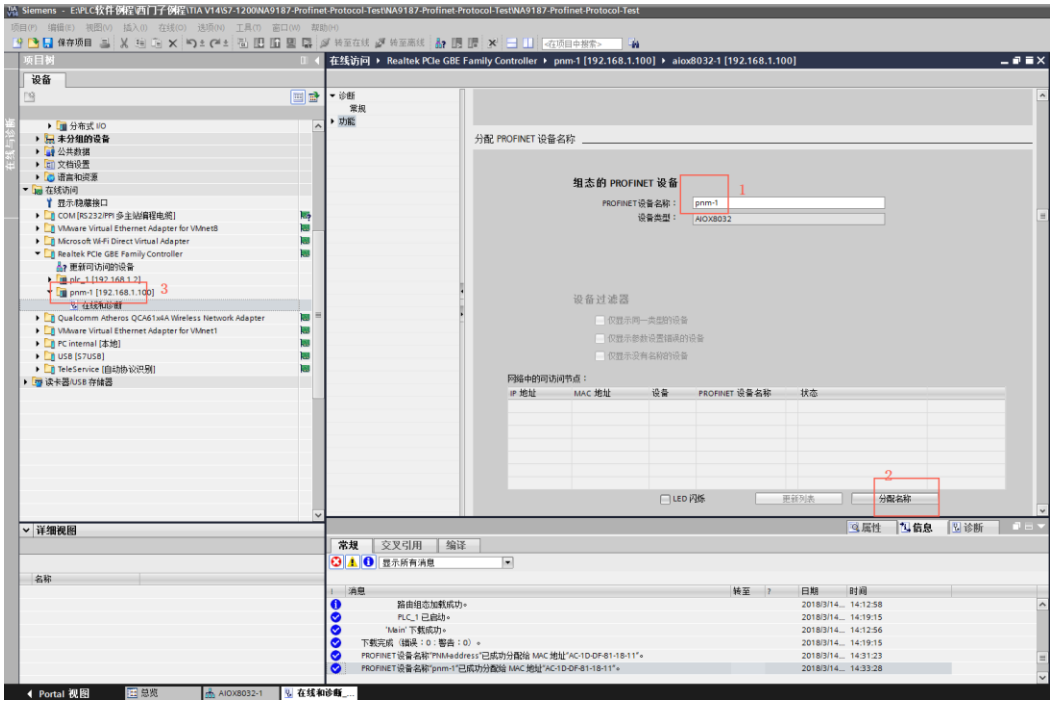
3.4 网关设备名称修改

3.4.1 使用TIA修改设备名称

1、将西门子 PLC 和 ODOT-PNM02 网关上电，同时用网线组网连接到 PC。打开博图软件，点击在线访问，找到本机网卡，双击更新可访问的设备。会搜索到西门子 PLC 和 ODOT-PNM02 网关。

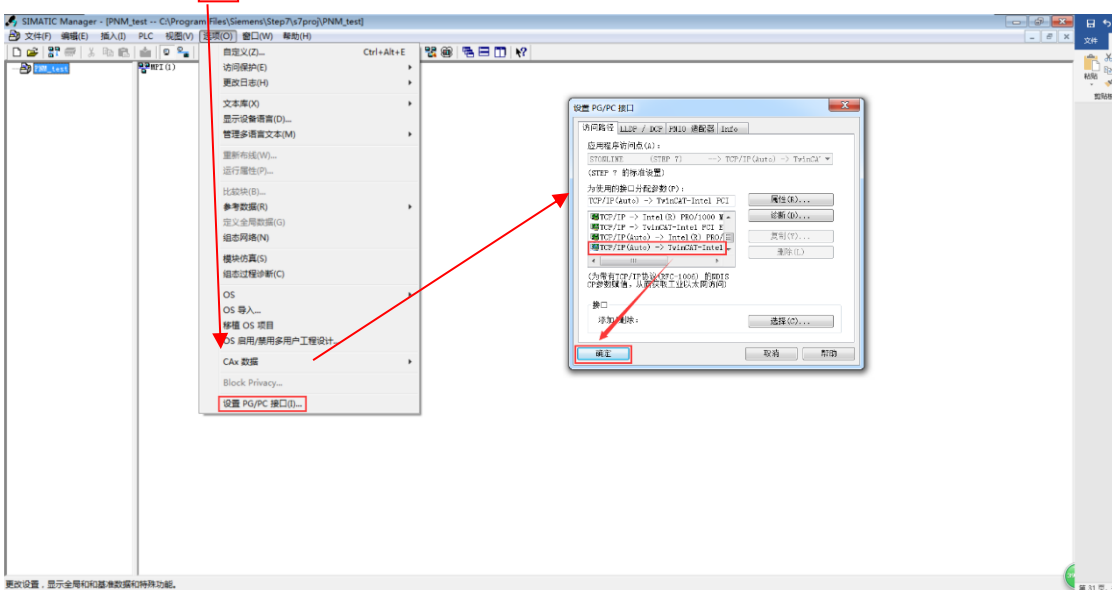


2、点击 PNMB-Address,双击在线和诊断，在右侧的功能下，找到 ProfiNet 设备名称：将默认的 PNMB-Address 改成 PNMB-1，点击右下角分配名称。当左侧本机网卡下拉菜单出现 PNMB-1 表明修改设备名称成功。PNMB-1 该名称用于设备组态时通过该名称来访问模块及分配给模块 IP 地址。

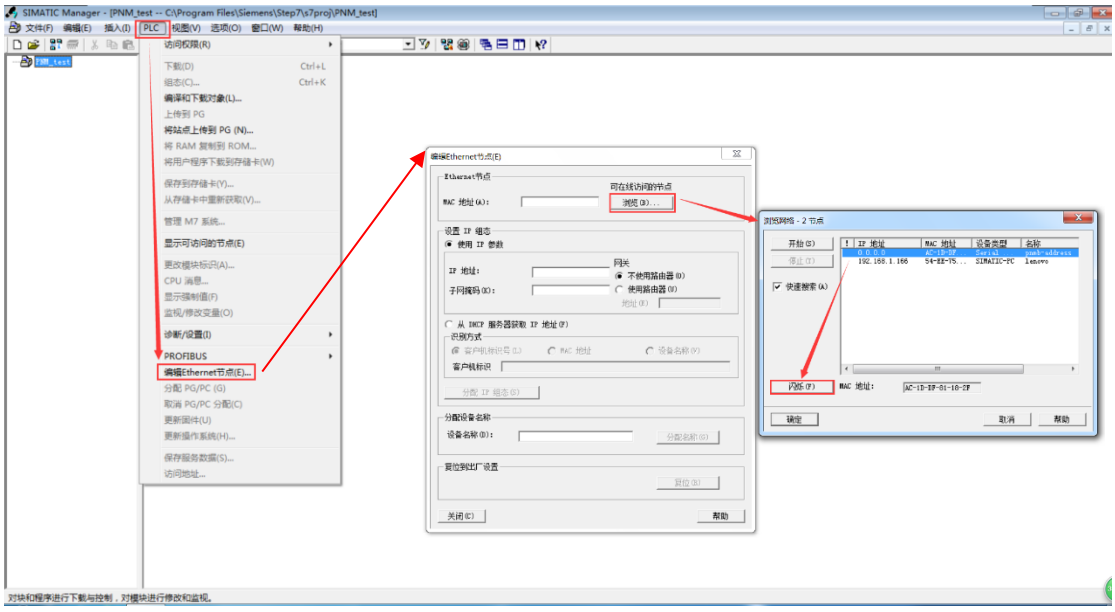

在线访问 ▸ Realtek PCIe GBE Family Controller ▸ pnm-1 [192.168.1.100] ▸ aiox8032-1 [192.168.1.100]
分配 PROFINET 设备名称
组态的 PROFINET 设备
PROFINET 设备名称：
pnm-1
设备类型：
AIOX8032
1
设备过滤器
网络中的可访问节点：
IP 地址
MAC 地址
设备
PROFINET 设备名称
状态
LED 闪烁
更新列表
分配名称
2
3
常规
交叉引用
编译
显示所有消息
消息
日期
时间
Portal 视图
总览
AIOX8032-1
在线和诊断

3.4.2 使用Step7修改设备名称

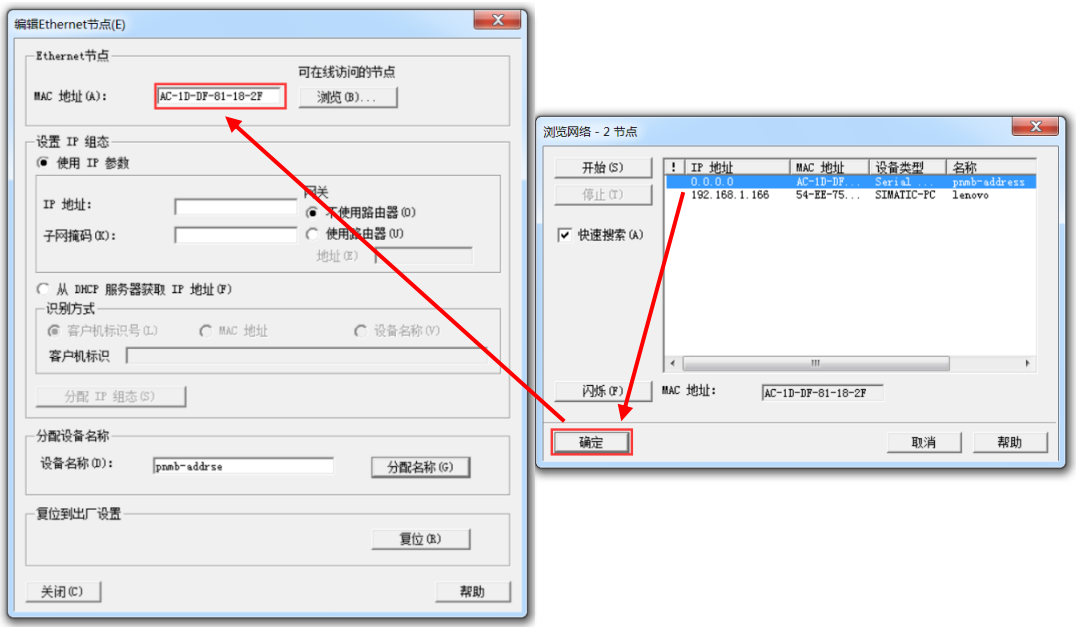
1、点击“选项”→“设置 PG/PC 接口”，在设置 PG/PC 接口页面将通讯接口选择为与网关连接的网卡。



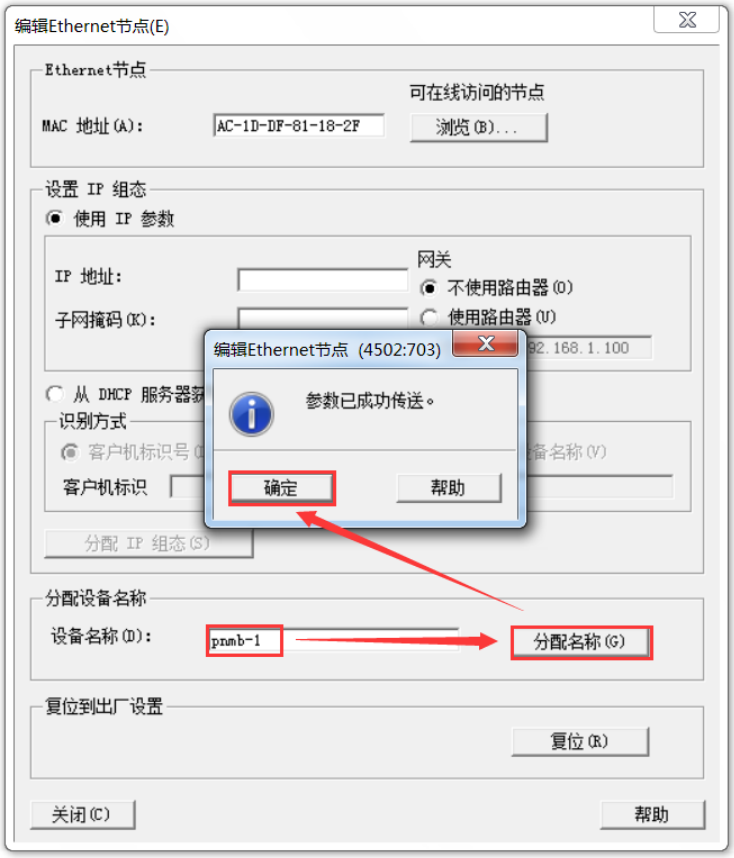
2、点击“PLC” →“编辑 Ethernet 节点”，在“编辑 Ethernet 节点”页面，点击浏览，在“浏览网络”页面，可以看到扫描上来的 ODOT-PNM02 模块，模块的默认名称为“pnmb-address”，选中模块，点击“闪烁”，模块上的 “SF”灯会闪烁，当网络中同时存在多个 PNM 模块时，可以通过该功能对模块进行区分。



3、选中模块点击“确定”，软件会自动将选中的模块的 MAC 地址写入“编辑 Ethernet 节点”页面的相应位置。

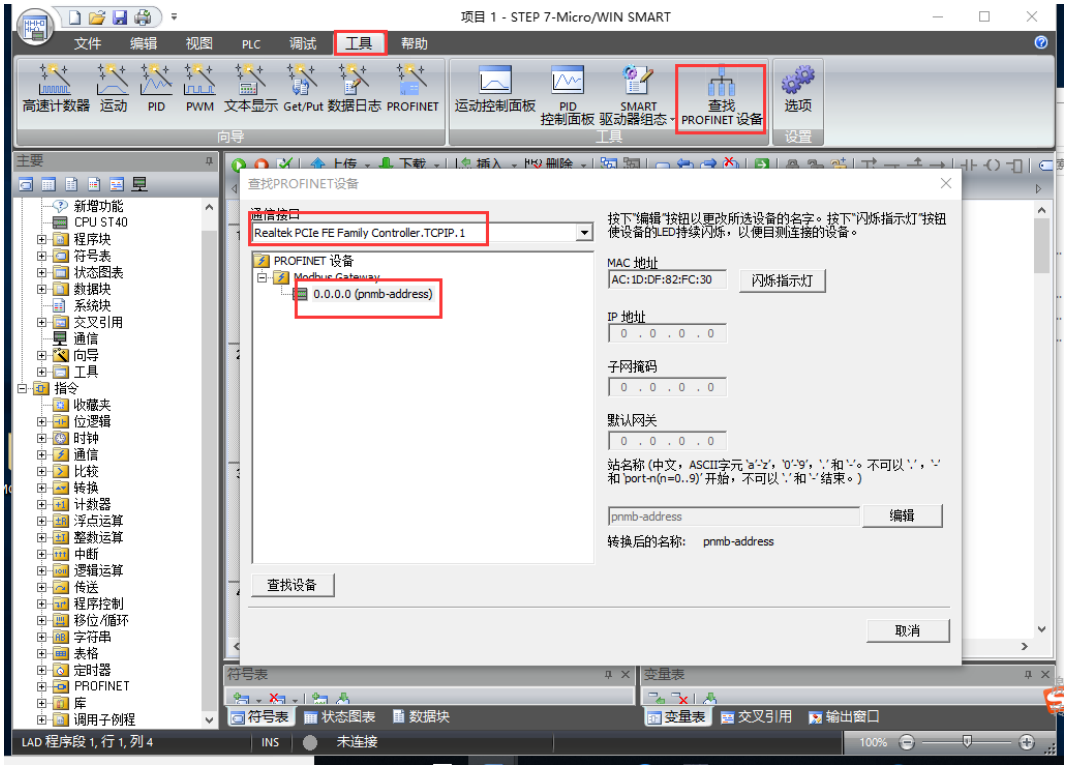


4、修改设备名称，点击“分配名称”，为网关设置新的设备名称，该名称将用于编程组态。注：修改设备名称主要用在网络中同时存在多个 ODOT-PNM02 模块的情况下，如果网络中只有一个 ODOT-PNM02，可以不修改其设备名称，在后面的组态中直接使用其出厂默认名称“pnmb-address”即可。



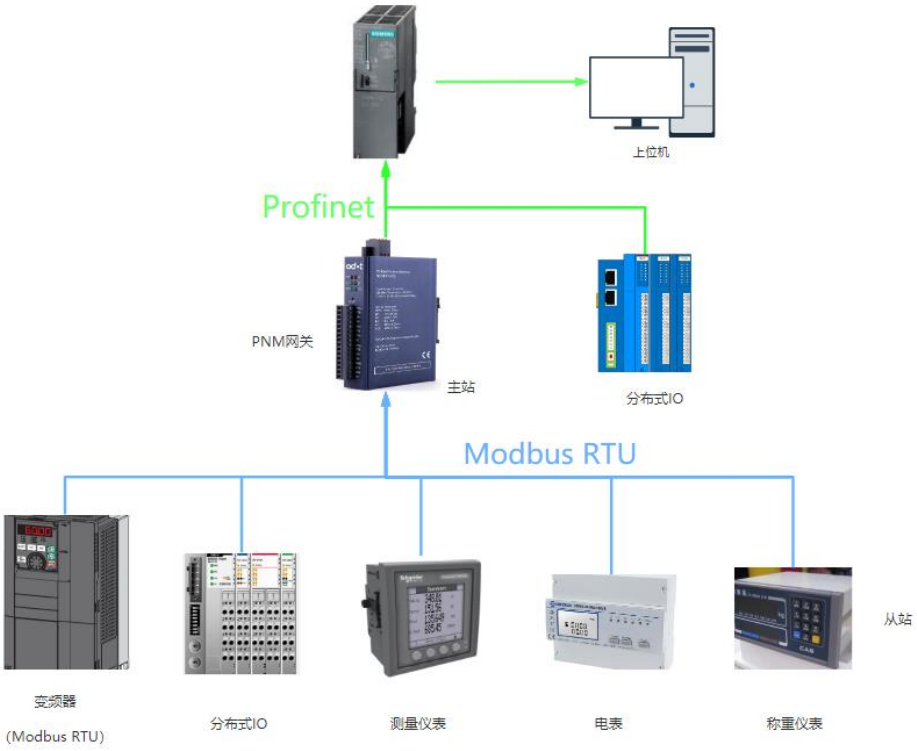
3.4.3 使用STEP 7-MicroWIN SMART修改设备名称

打开 STEP 7-MicroWIN SMART 软件，点击工具，点击查找 PROFINET 设备，选择本机网卡，会自动扫描到所有的 PROFINET 设备，可查看网关的 IP 地址和设备名称。点击编辑，设置网关设备名称。

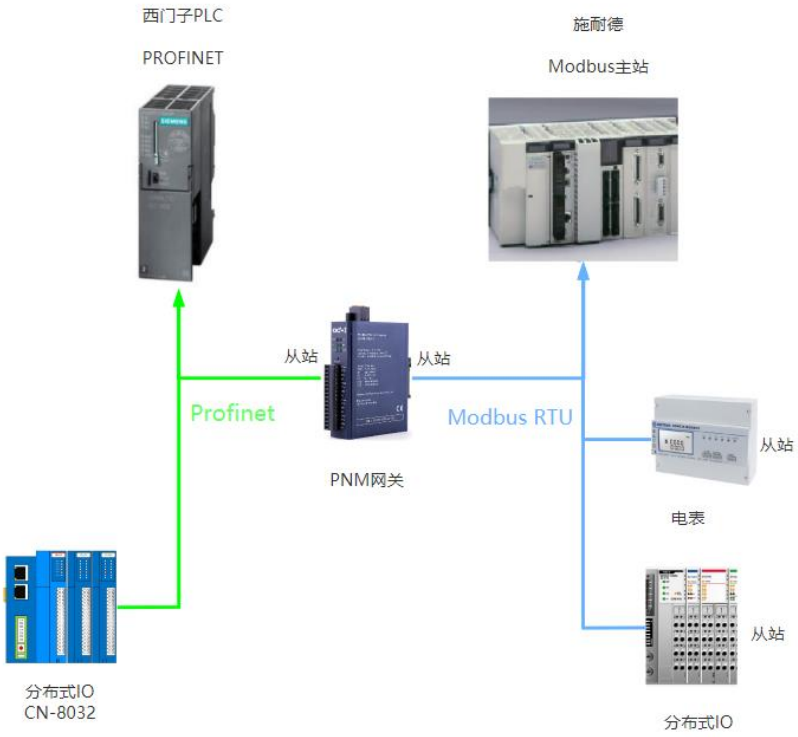


3.5 网关应用拓扑图

主站模式拓扑图



从站模式拓扑图



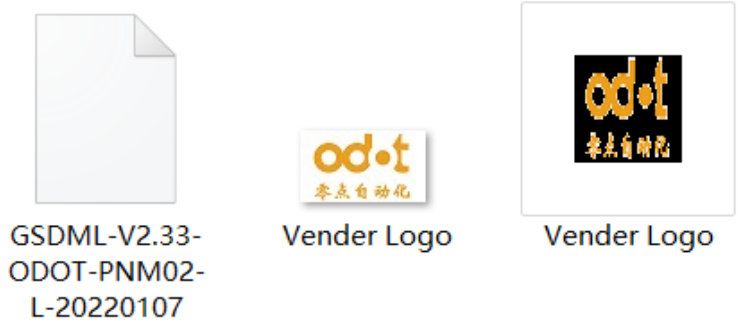
自由口透传模式拓扑图

四、在西门子 TIA V14 中使用本模块

本章将以 SIEMENS 的 315-2 PN/DP 作为 PROFINET 的 Controller，使用 TIA 作为组态软件，举例说明 ODOT-PNM02 的配置方法。

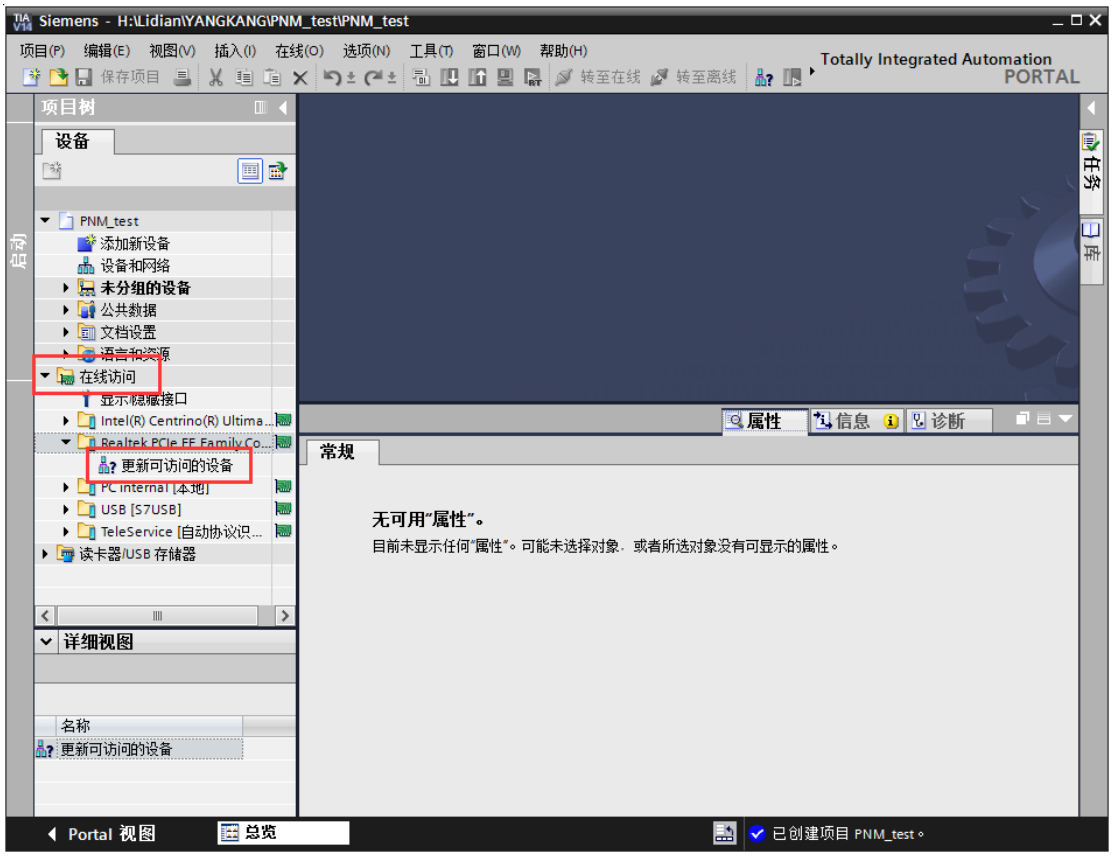
4.1 MODBUS 主站模式的配置

1．找到产品光盘中的 XML 文件夹，并确认文件夹中有以下文件，若没有请联系供应商索取。

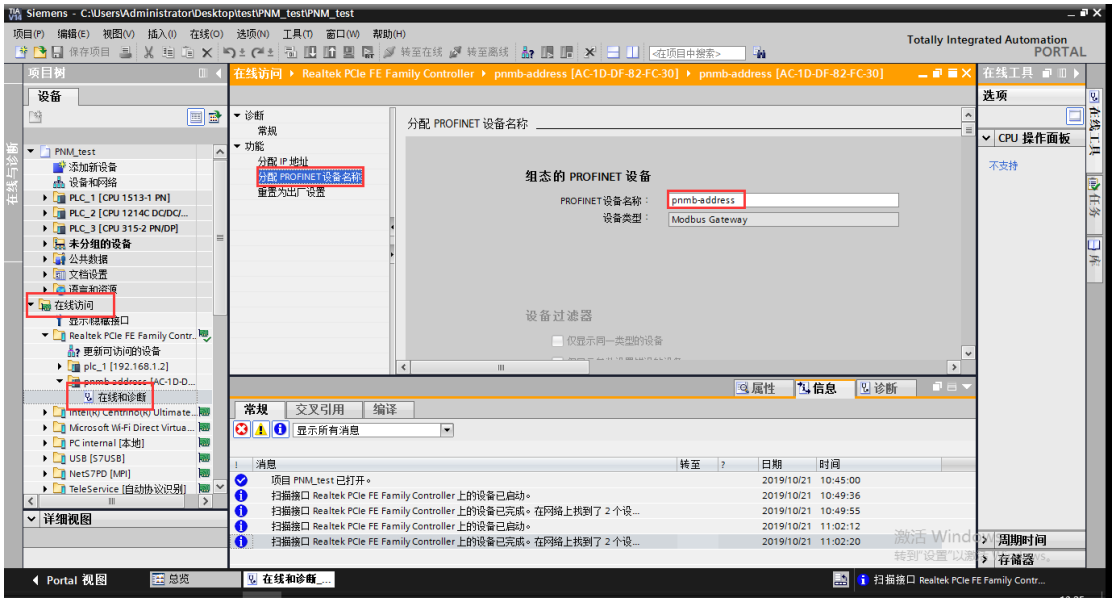


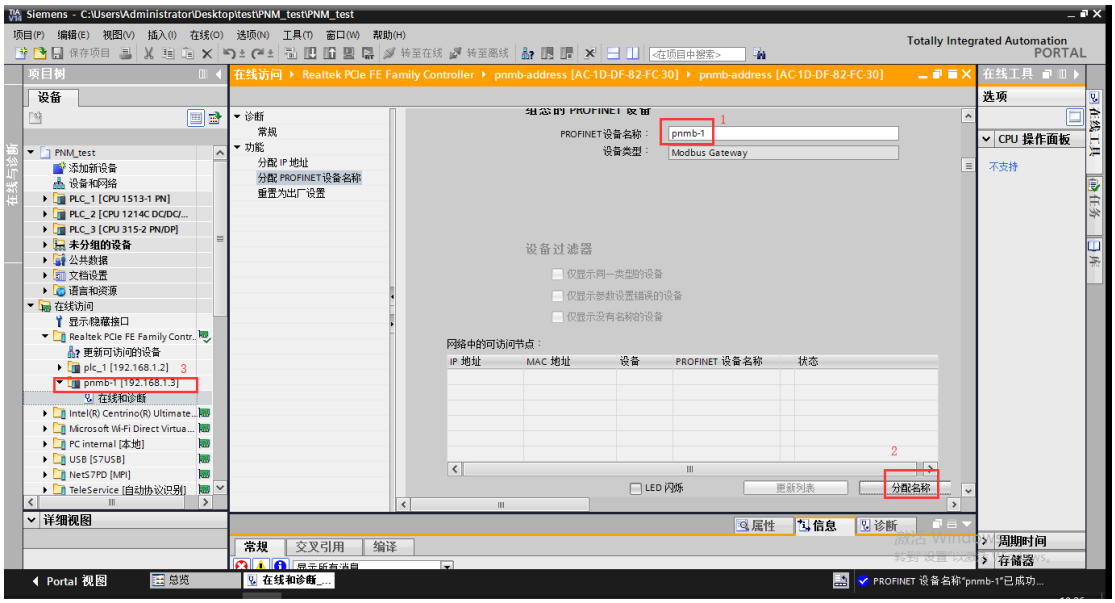
2、打开 TIA V14 软件，点击创建新项目，新建一个工程，命名为“PNM_test”.

3、点击项目视图--“在线访问”找到本机网卡，点击更新可访问的设备。

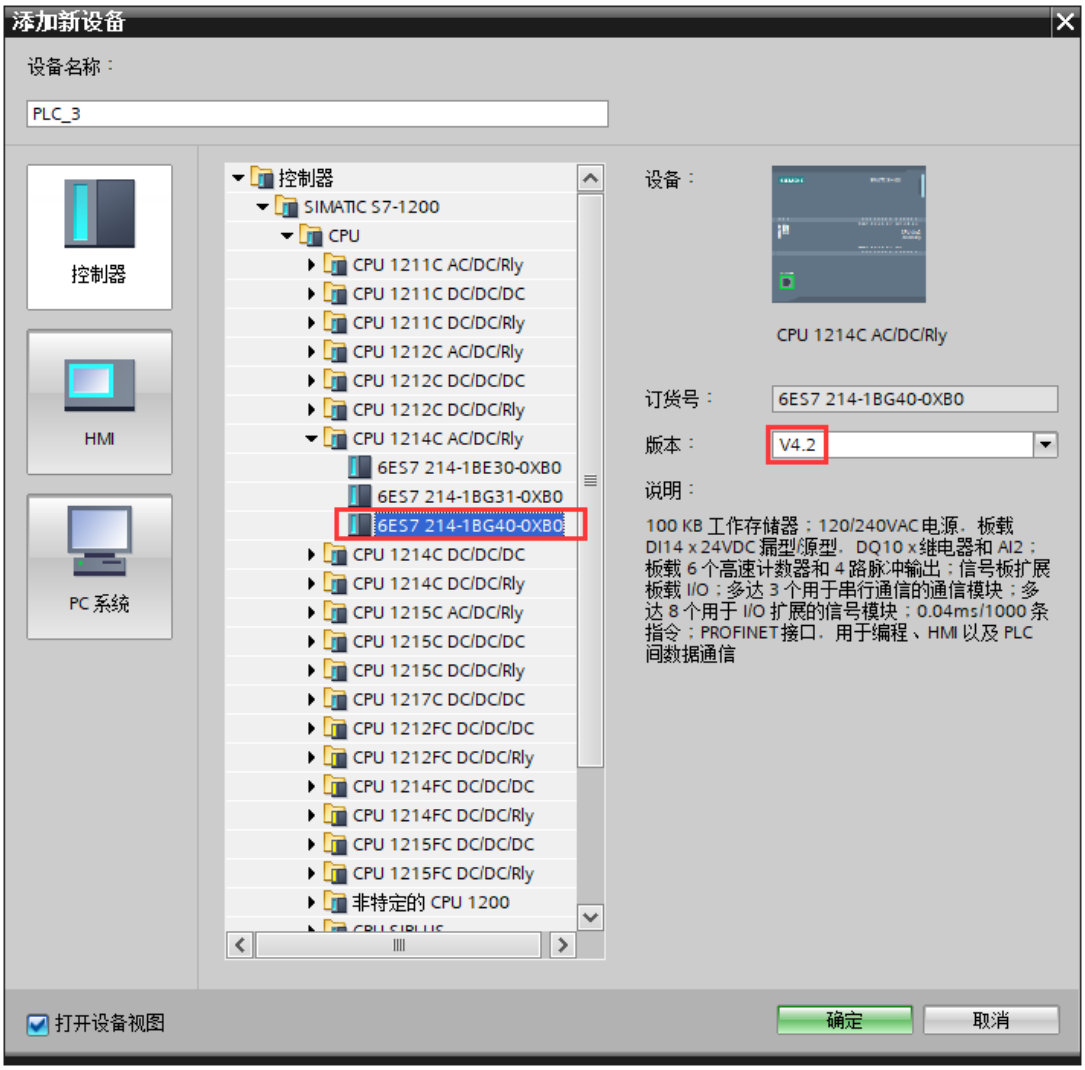


出现“PLC 设备 IP 地址”和“PNMB-Address 设备的 IP 地址”，点击 PNMB-Address 下的“在线和诊断”，可在“功能”下拉菜单设置“ProfiNet 设备名称”，用于后面组态时访问该网关模块。

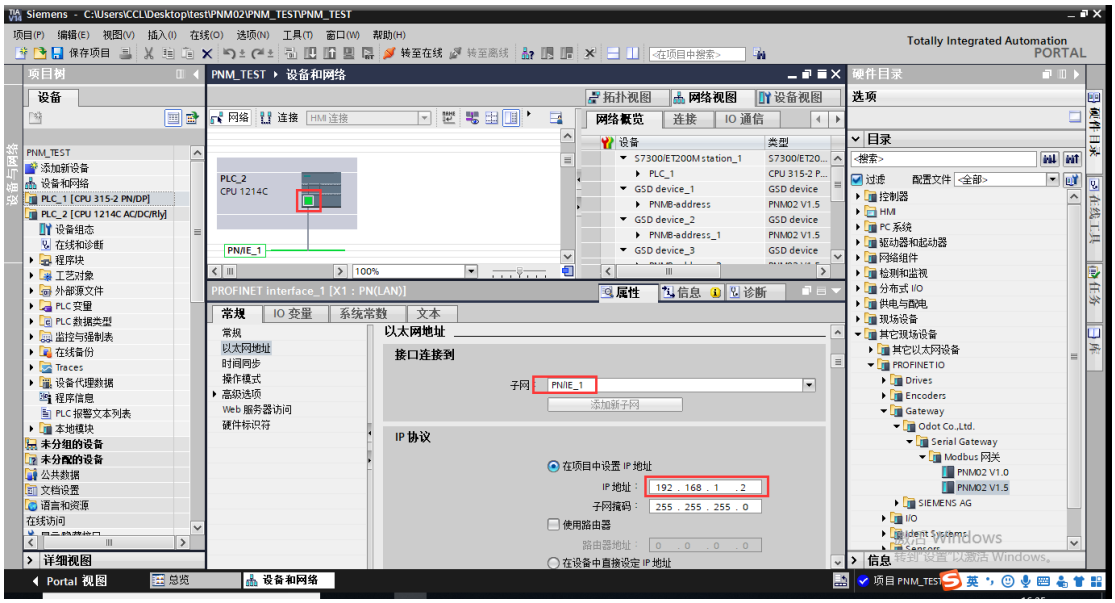




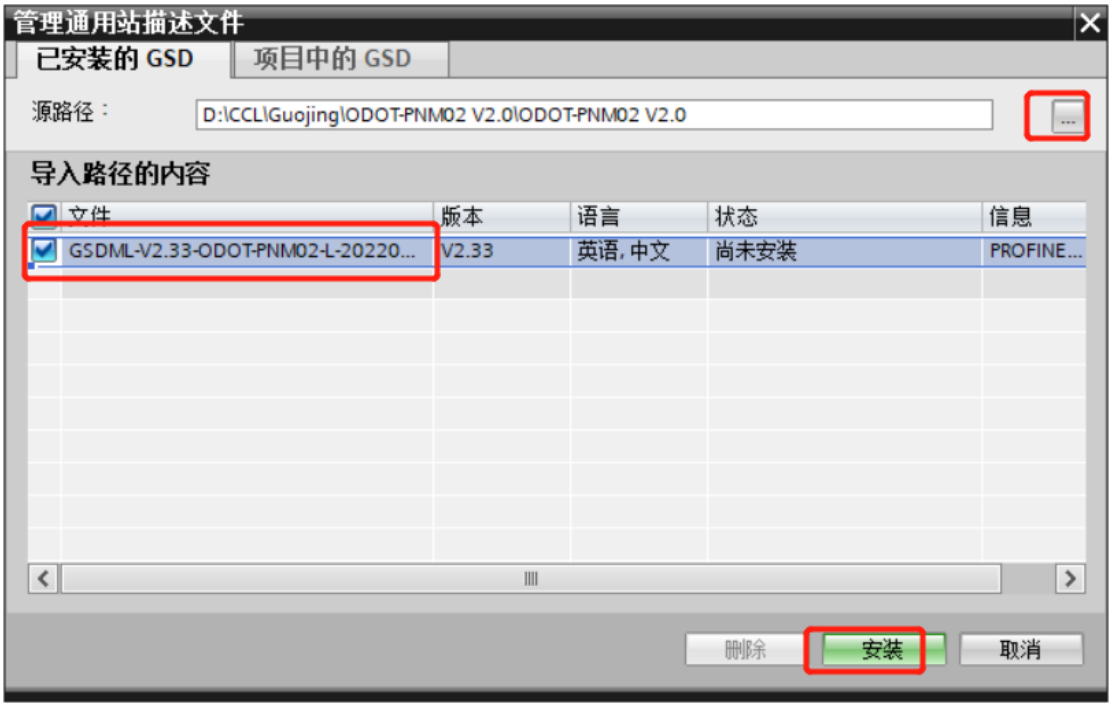
4、点击添加新设备，选择控制器 CPU 1214C AC/DC/Rly(6ES7 214-1BG40-0XB0　V4.2),点击确定。



5、点击 PLC 下设备组态—“网络视图”，点击 PLC 网口，对 PLC 的 PN 口 ProfiNet 网络和 IP 地址进行设置。

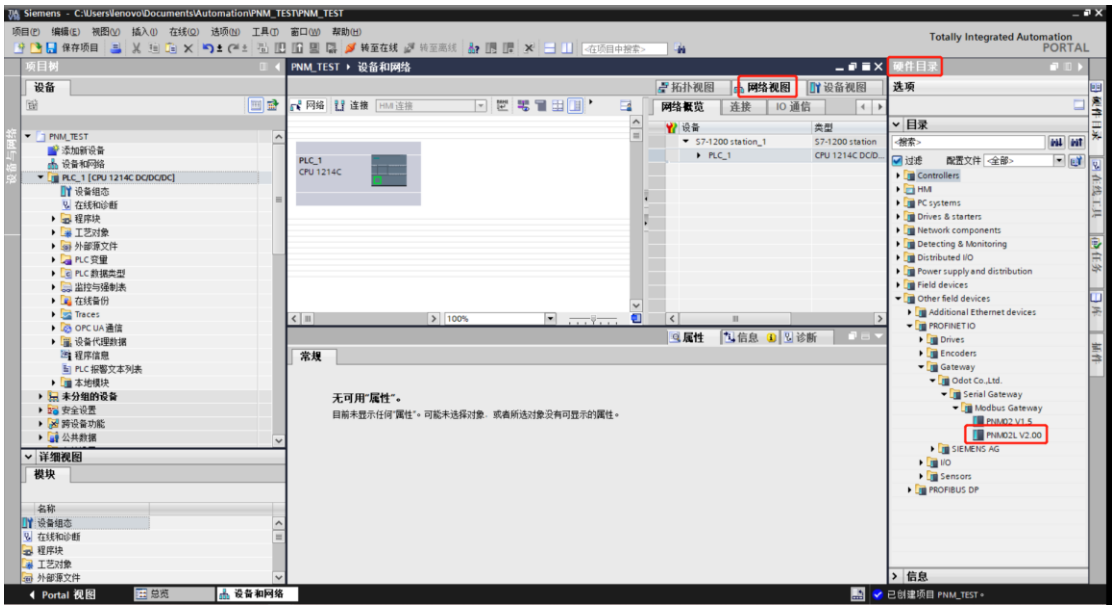


6、在设备组态界面，点击 “选项”→“管理通用站描述文件”，选择路径，找到“GSDML-V2.33-ODOT-PNM02-L-20220107”，添加 GSD 文件。添加 GSD 文件

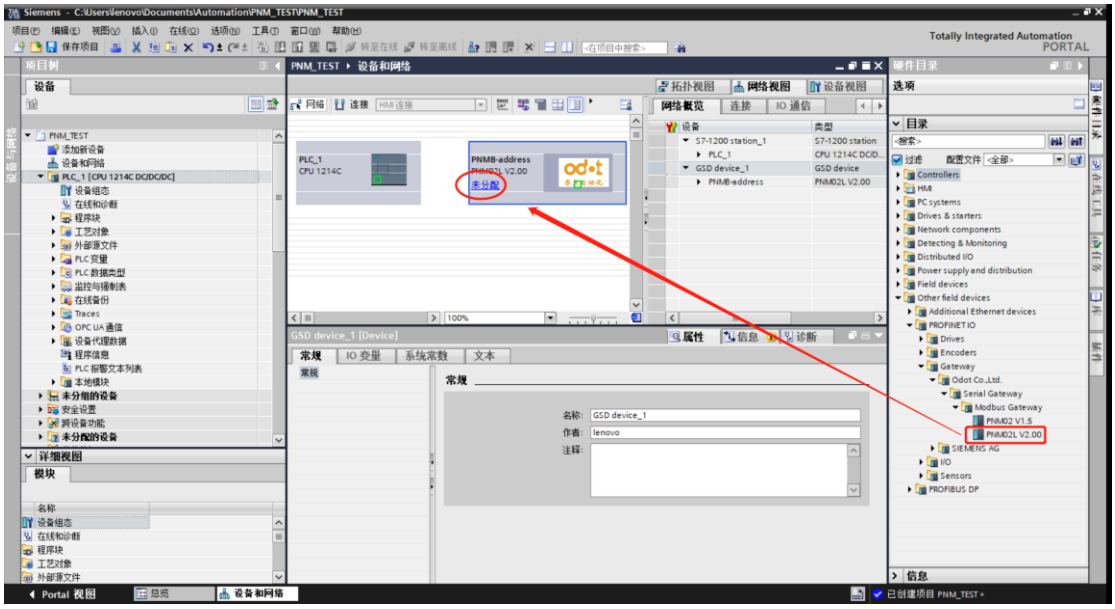


成功后，点击“关闭 ”，退出添加 GSD 对话框。

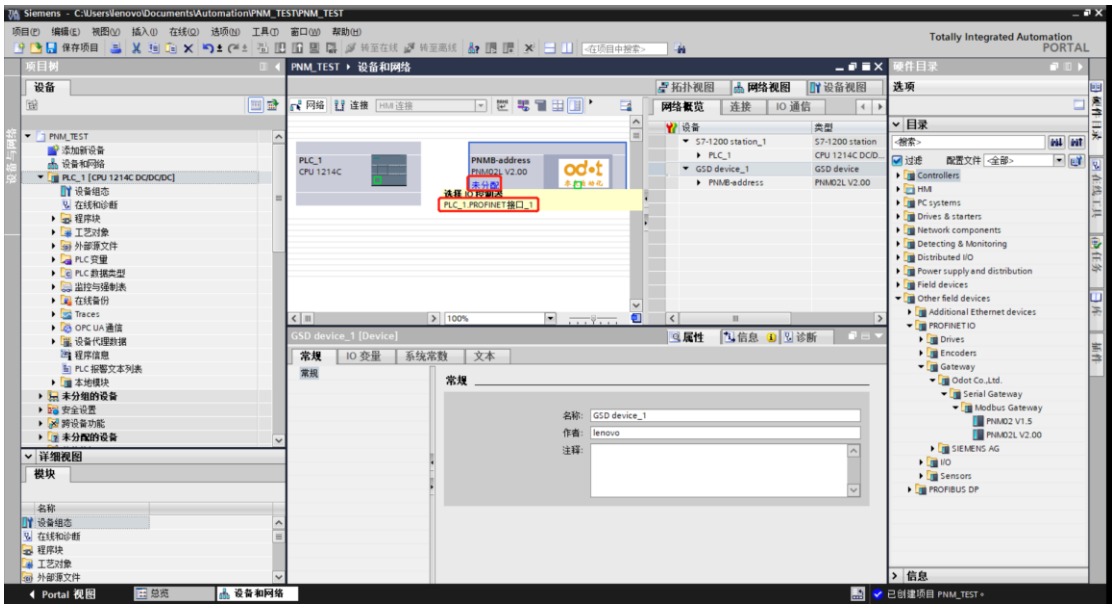
7、点击 PLC 下设备组态—“网络视图”。在硬件目录里点开其他现场设备→“PROFINET IO→Gateway→Odot Co., Ltd→Serial Gateway → ModbusGateway ”，找到“PNM02L V2.00”，说明 GSD 文件添加成功。



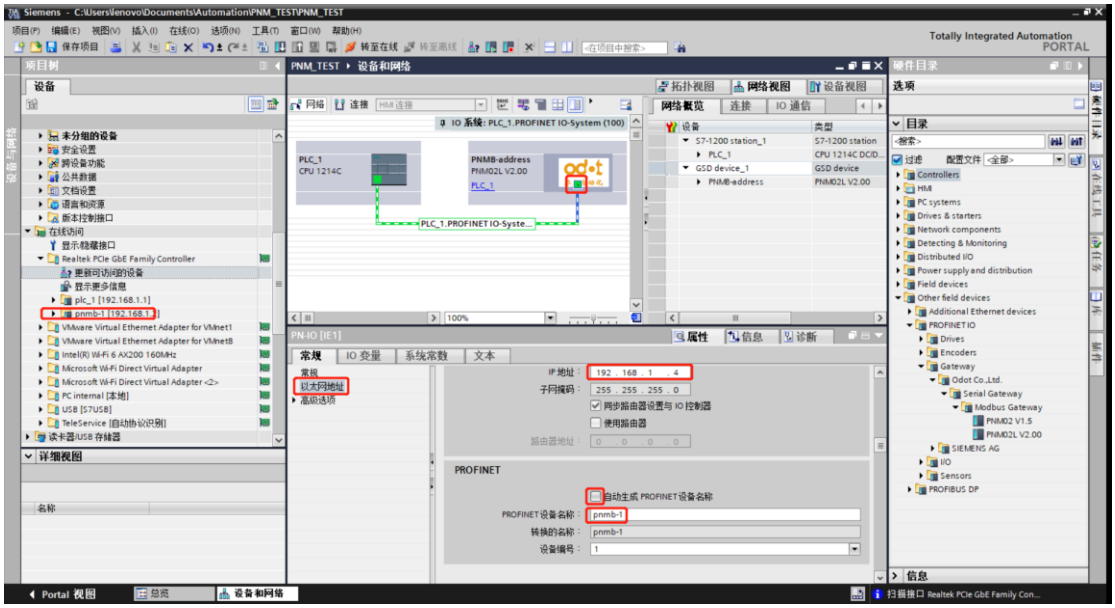
8、将硬件目录里的模块 PNM02 V2.1 拖拽到网络视图里。



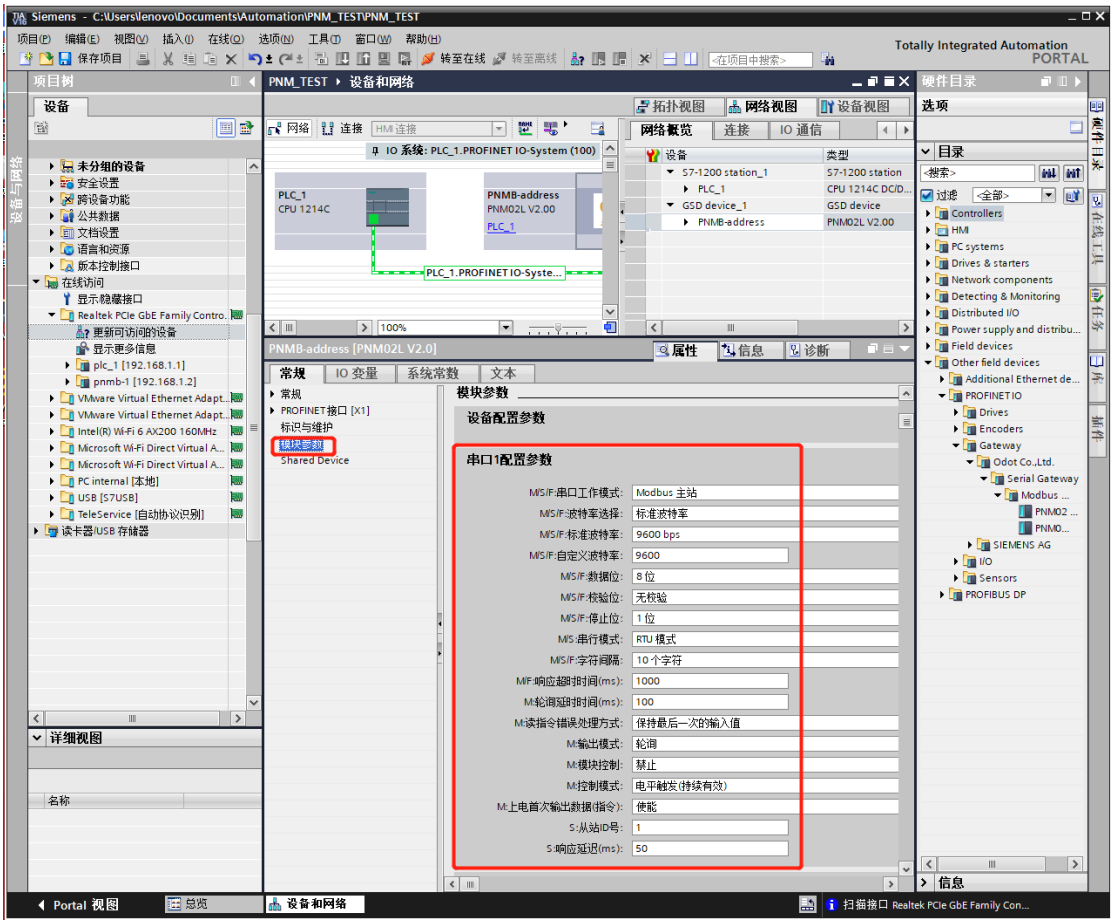
9、连接 PNM02 网关的网络到 S7-1200 PLC 的 PN 接口。



选中 PNM02 网关的 PN 口，点击“以太网地址”设置参数。设置网关通讯 IP 地址，填写之前在线访问设置的“ProfiNet 设备名称”。注：此处设备名称必须和前面设备的保持一致。



10、双击网关进入“设备视图”，选中网关，在“常规”参数下设置模块参数。（设置带 M 前缀的模块参数）



模块串口配置参数：串口 1 和串口 2 配置参数是相同的。

注：M 表示该参数主站模式有效，S 表示该参数从站模式有效，F 表示该参数自由口透传模式有效。

M/S/F :网关工作模式：Modbus 主站、Modbus 从站可选，**默认** Modbus 主站。

M/S/F:波特率选择：标准波特率、自定义波特率可选，默认值：标准波特率。

M/S/F :标准波特率：串口波特率，300-500000bps 可选，**默认 9600bps。**

M/S/F :自定义波特率：0,300-500000bps 可设，**默认 9600bps。**注：少数客户的设备是非标波特率，就可以自定义。

M/S/F :数据位：7 位、8 位可选，**默认 8 位。**

M/S/F :校验位：无、奇、偶、字符、空格校验可选，**默认无校验。**

M/S/F :停止位：1 位、2 位，**默认 1 位。**

M/S :串行模式：RTU/ASCII 模式可选，**默认 RTU 模式。**

M/S/F :字符间隔：接收报文时的帧间隔检测时间，1.5t~2000t 可选，**默认 5t**。（t 为单个字符传送的时间，和波特率有关）。

M/F : 响应超时时间(ms)：主站发送命令后，等待从站响应的时间。1~65535 可选，**默认 500。**

M :轮询延时时间(ms)：Modbus 命令发送的间隔时间(收到从站响应报文到发送下一条命令的延时)，0~65535 可选，**默认 10。**

M :读指令错误处理方式：从站读数据超时后，数据处理方式，保持最后一次输入值、清零输入值可选，**默认保持最后一次输入值。**

M :输出模式：轮询、事件触发（数据发生改变）可选，**默认轮询。**“轮询模式”下 Modbus 周期性地发送写报文。“事件触发”模式时只有 Modbus 输出数据发生变化时才发送写命令。

M :模块控制：禁止、使能可选，默认禁止。当需要对 Modbus 的读写命令进行控制时，选择使能模式，通过控制“模块控制输出”的值控制 Modbus 的读写命令。

M :控制模式：电平触发（持续有效）、上升沿触发（单次触发）可选，**默认电平触发（持续有效）。该值只在**模块控制**使能模式有效**

M :上电首次输出数据（指令）：使能、禁止可选，**默认使能。**

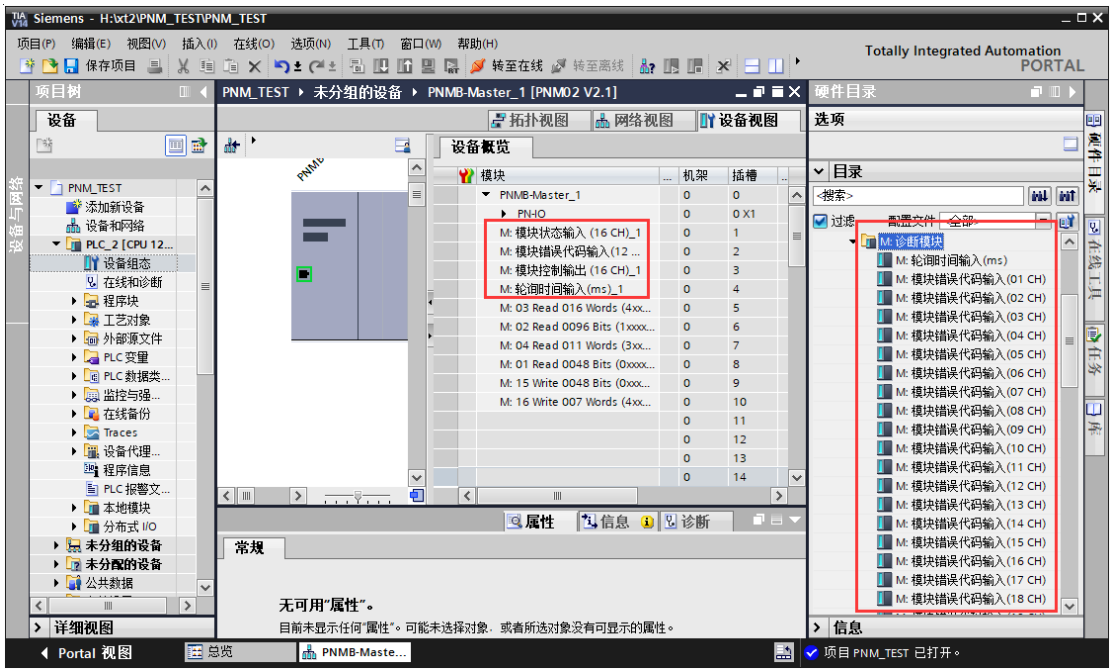
S :响应延时(ms) ：0~65535 可选，**默认 0.**

C、串口 2 参数：

M/S/F :物理层：RS485/RS232 可选

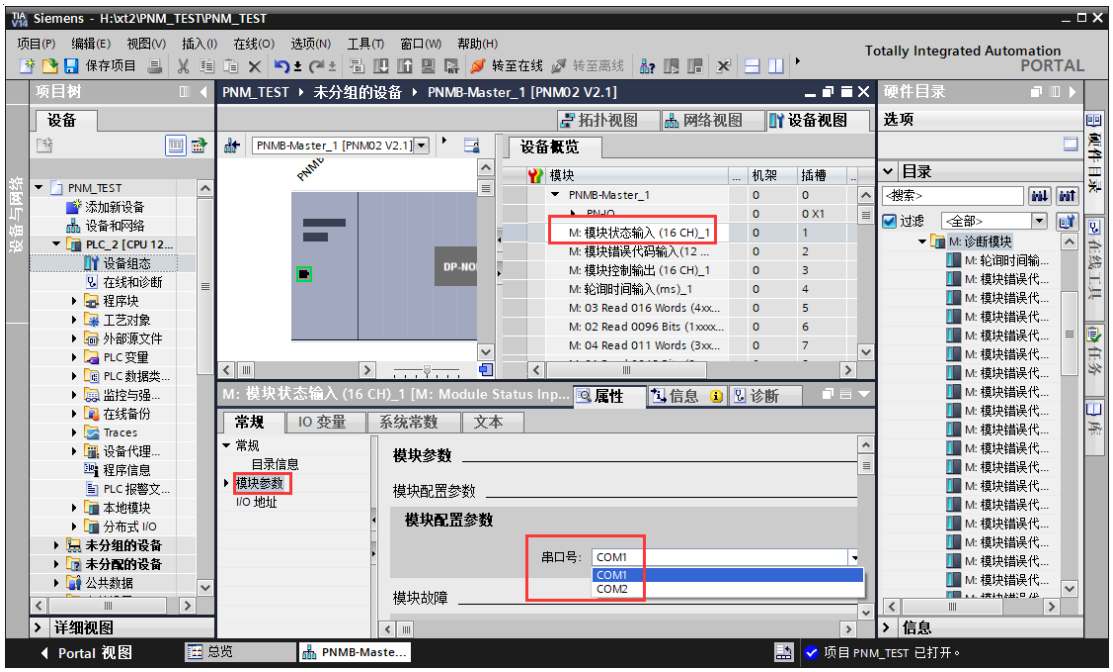
其他参数和串口 1 参数功能相同。

11、在设备视图选中网关，在右侧硬件目录里选择“M 开头的读写命令”。当需要对模块状态进行监视时可先添加“诊断模块”。注：不是必加项。



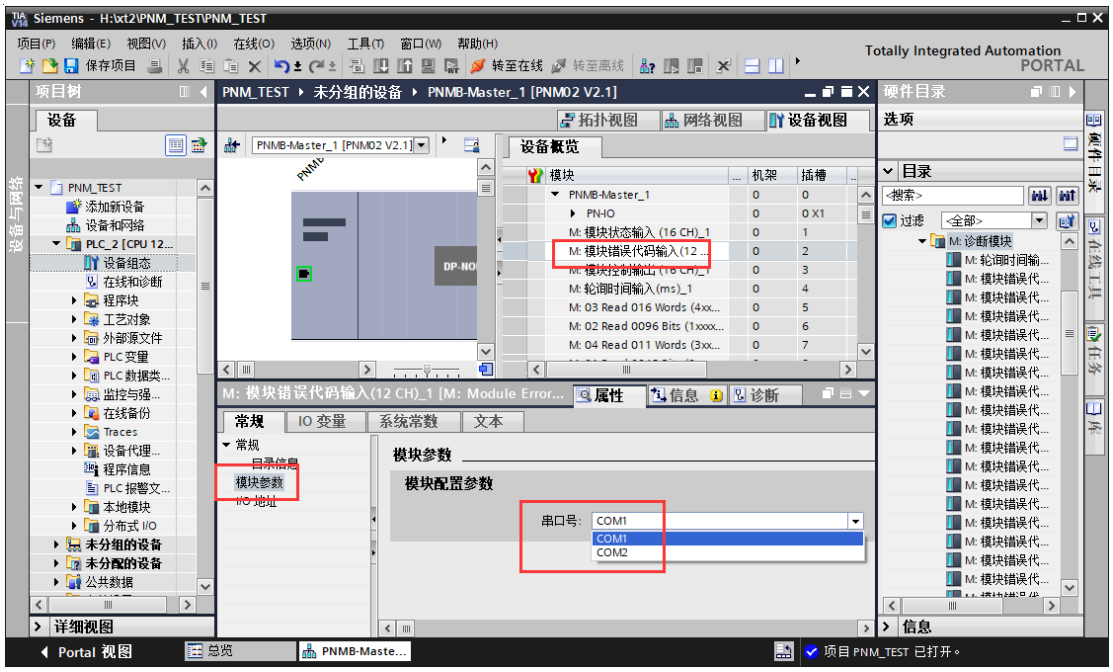
M：诊断模块：包括模块状态输入、模块错误代码输入、模块控制输出、轮询时间输入；下拉菜单的命令需添加到插槽前 8 行。

模块状态输入：有 8~48 通道可选，模块状态可监测每一个数据插槽的工作状态，当某一个数据插槽出现故障时，对应的状态位被置 1，故障恢复后自动清零。



模块错误代码输入：有 1-48 个通道可选，当数据插槽出现故障时，错误代码模块可显示出现错误通道的功能码和具体的错误代码，用户可根据错误代码，判断是何种原因产生故障，进而采取对应的调整方法。详细的描述请参见

“Modbus 主站状态代码表”。



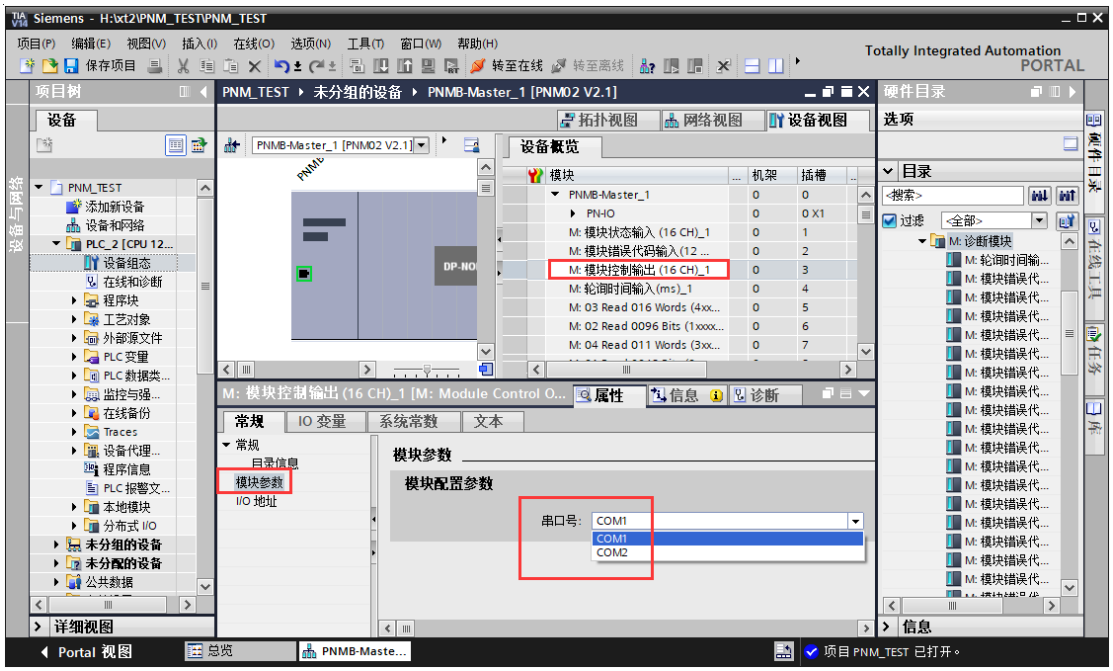
Modbus 错误代码表

错误代码	故障说明	故障排除方法
0x00	工作正常	无
0x01	非法功能码	设备不支持当前功能码，请参考从站手册选择对应的功能码模块
0x02	非法数据地址	设备数据超出其地址范围，参考从站手册修改数据起始地址或数据长度
0x03	非法数据值	数据长度错误，数据长度超出最大允许值125(Word)或2000(Bit)，修改长度
0x04	数据处理错误	检查数据值范围是否符合从站要求
0x05	应用层长度不匹配	增大接收字符间隔，检查通信参数设置
0x06	协议 ID 错误	检查发送端报文
0x07	缓存地址错误	设备内部错误
0x08	位偏移错误	设备内部错误
0x09	从站 ID 号不匹配	增大超时时间，检查硬件连接状态，检查通信参数设置

0x0A	CRC 错误	CRC 错误，检查通讯线路
0x0B	LRC 错误	LRC 错误，检查通讯线路
0x0C	应答功能码不匹配	检查硬件连接状态
0x0D	应答地址不匹配	检查硬件连接状态
0x0E	应答数据长度不匹配	检查硬件连接状态
0x0F	通信超时	增大超时时间，检查硬件连接状态，检查通信参数设置
0x10	ASCII 模式起始符错误	‘:’冒号起始符错误
0x11	ASCII 模式结束符错误	CR/LF 回车换行结束符错误
0x12	ASCII 模式非字符数据	数据中包含非16进制 ASCII 码
0x13	ASCII 模式字符数错误	从站应答长度错误

模块控制输出：有 8~48 通道可选。当串口下参数（**M :模块控制**）为**使能**模式时，该命令的输出控制读写通道有效。

例：Q2.0=1 时，5 号槽的 03 读 16 个字这条命令执行。Q2.0=0 时，5 号槽的 03 读 16 个字这条命令不执行。Q2.1=1 时，6 号槽的 02 读 96 个位这条命令执行。Q2.1=0 时，6 号槽的 02 读 96 个位字这条命令不执行。以此类推。

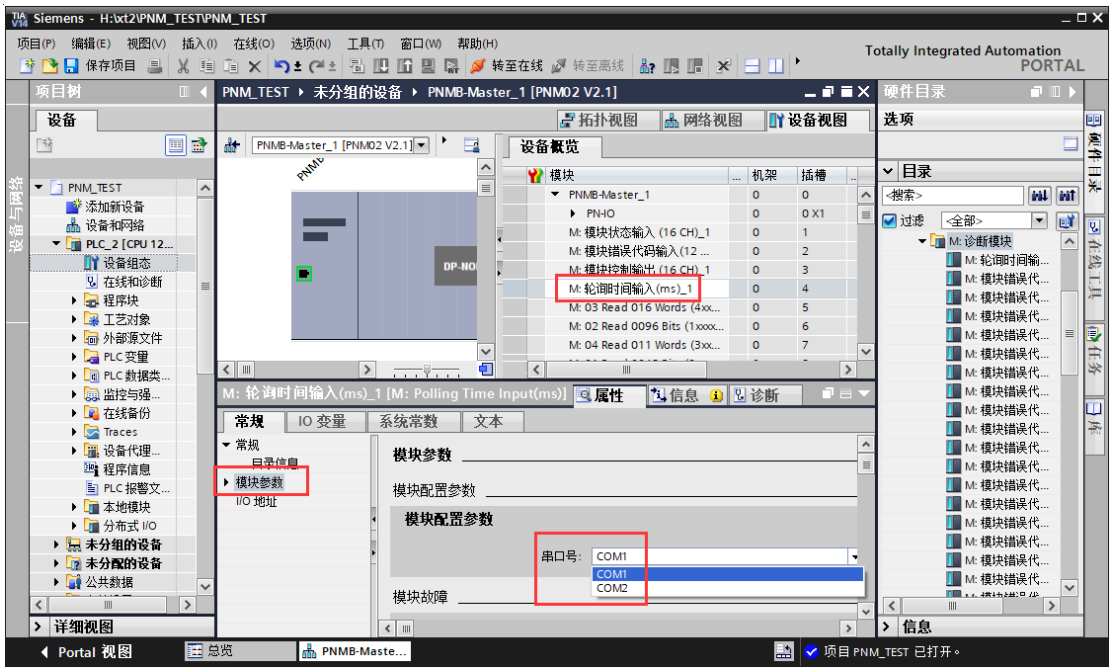


例：手动更改模块控制输出后的 Q 地址是 100...101, Q100.0=1 时，5 号槽的 03 读 16 个字这条命令执行。Q100.0=0 时，5 号槽的 03 读 16 个字这条命令不执行。Q100.1=1 时，6 号槽的 02 读 96 个位这条命令执行。Q100.1=0 时，6 号槽的 02 读 96 个位字这条命令不执行。以此类推。

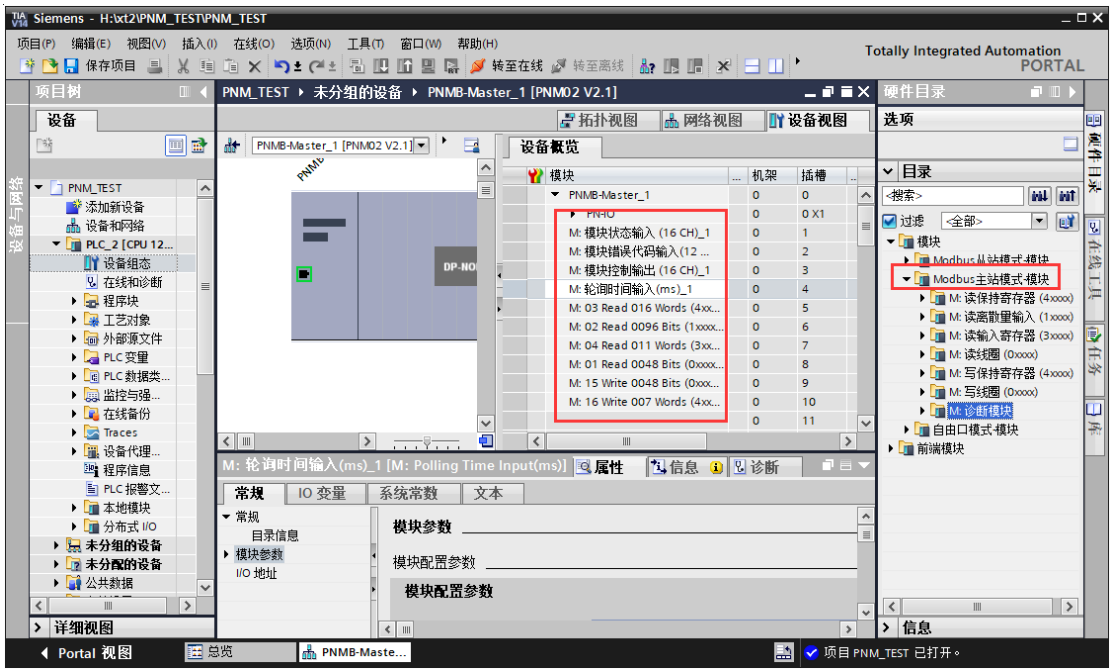
注：模块控制输出功能激活后。在控制范围内的读写命令都需要使能控制。

例：采用**模块控制输出（8 CH）**命令，在后面的槽位添加有 8 个以上的读写命令（10 条命令），前面 8 条读写命令需要使能控制，后面 2 条不需要控制自动执行。

轮询时间输入：用于监视串口的轮询时间，注：串口 1、串口 2 是独立的，所以要使用 2 路串口采集数据时要添加**两条**命令分别监视轮询时间。



12、网关作为主站，支持 Modbus 功能码 01/02/03/04/15/16.将硬件目录的读写命令添加到设备概览的插槽内。



M :读保持寄存器（4xxxx）支持 1~125words 可选

M :读离散量输入（1xxxx）支持 8~200bits 可选

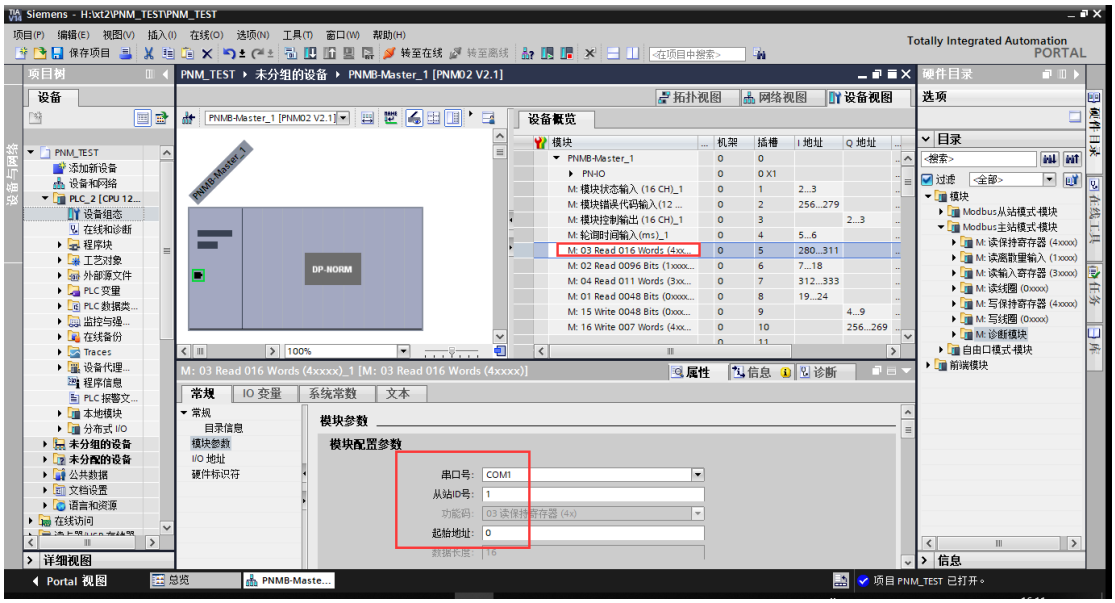
M :读输入寄存器（3xxxx）支持 1~125words 可选

M :读线圈（0xxxx）支持 8~200bits 可选

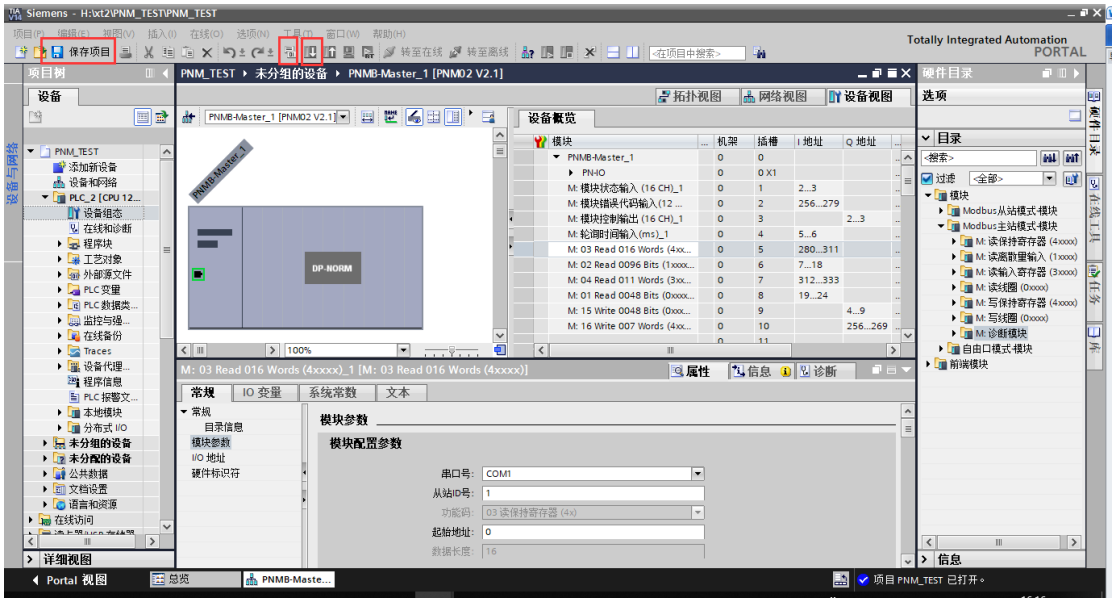
M :写保持寄存器（4xxxx）支持 1~125words 可选

M :写线圈（0xxxx）支持 8~200bits 可选

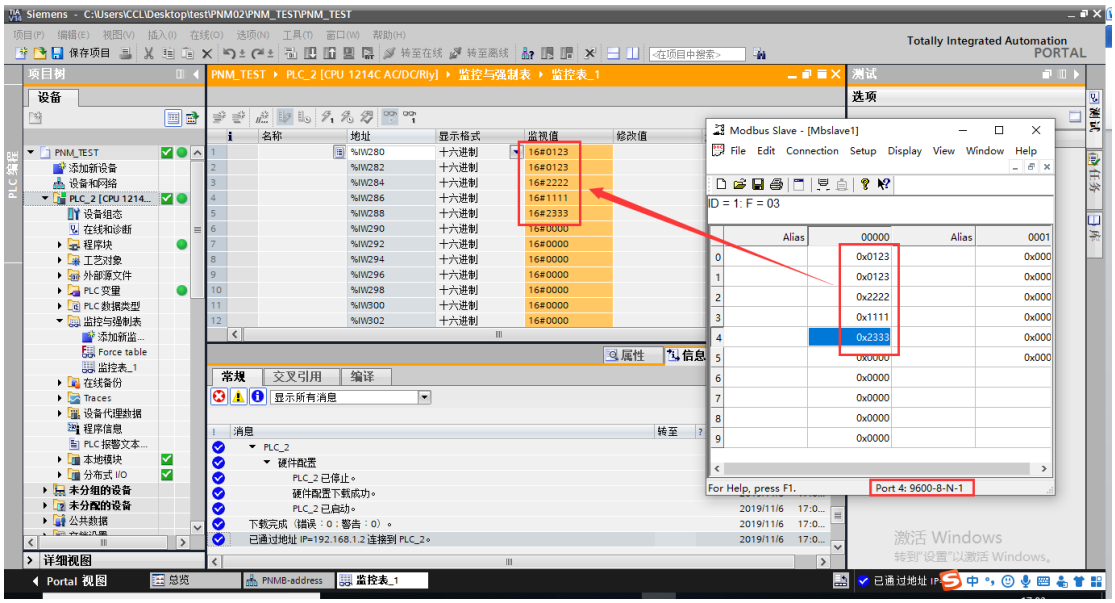
13、添加完读写命令，需要对读写命令进行模块参数设置。该命令属于串口号 COM1 或 COM2,从站 ID 号，数据起始地址。例，从站模块的数据在 40001-40016，起始地址填 0 即可，若从站模块数据在 400200-40215，起始地址填 199 即可。



14、此时硬件组态已基本完成，保存项目，编译。



查看项目是否报错，没有错误时点击下载。下载成功后，打开监控表监控网关采集的数据。采用 Modbus Slave 模拟串口 RS485 侧设备。


Totally Integrated Automation
PORTAL
Modbus Slave - [Mbslave1]
File Edit Connection Setup Display View Window Help
ID = 1: F = 03
Alias 00000 Alias 0001
For Help, press F1.
Port 4: 9600-8-N-1
激活 Windows

4.2 MODBUS 从站模式的配置

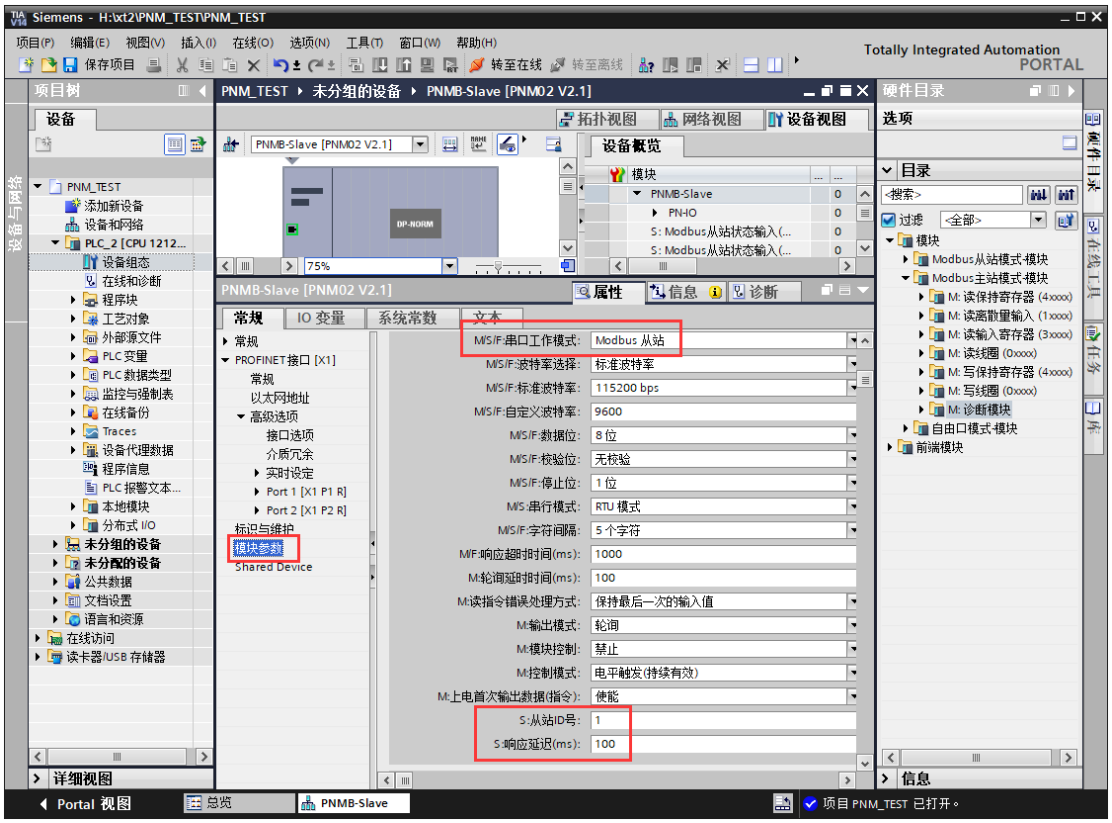
1→9 参照 4.1(主站模式)的 1→9。

10、双击网关进入设备视图，选中网关，在常规参数下设置模块参数。（设置带 S 前缀的模块参数）

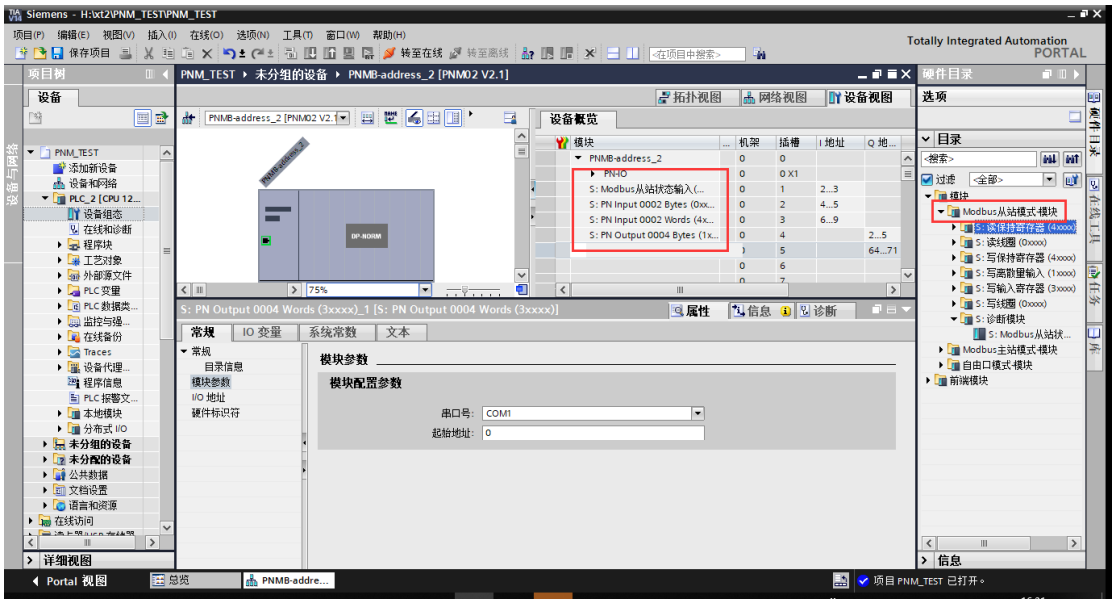
将通用参数的 M/S/F :网关工作模式选择 **Modbus 从站模式。**

S:从站 ID 号：设为 1

串口 1 和串口 2 参数参考主站模式注释。



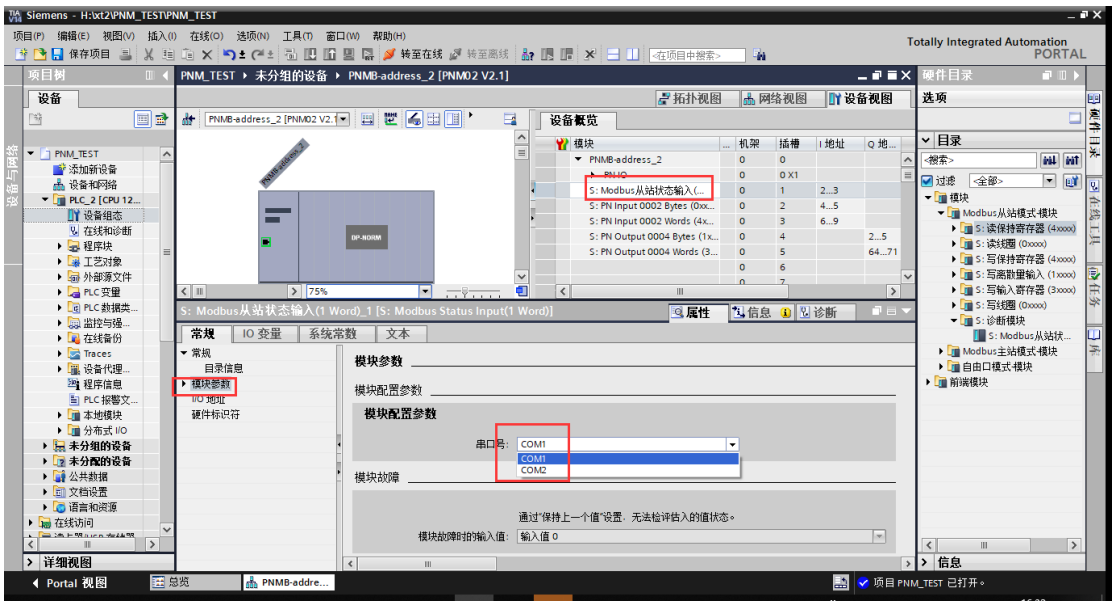
11、在设备视图选中网关，在右侧硬件目录里选择 S 开头的读写命令。当需要对模块状态进行监视时可先添加诊断模块。注：不是必加项。



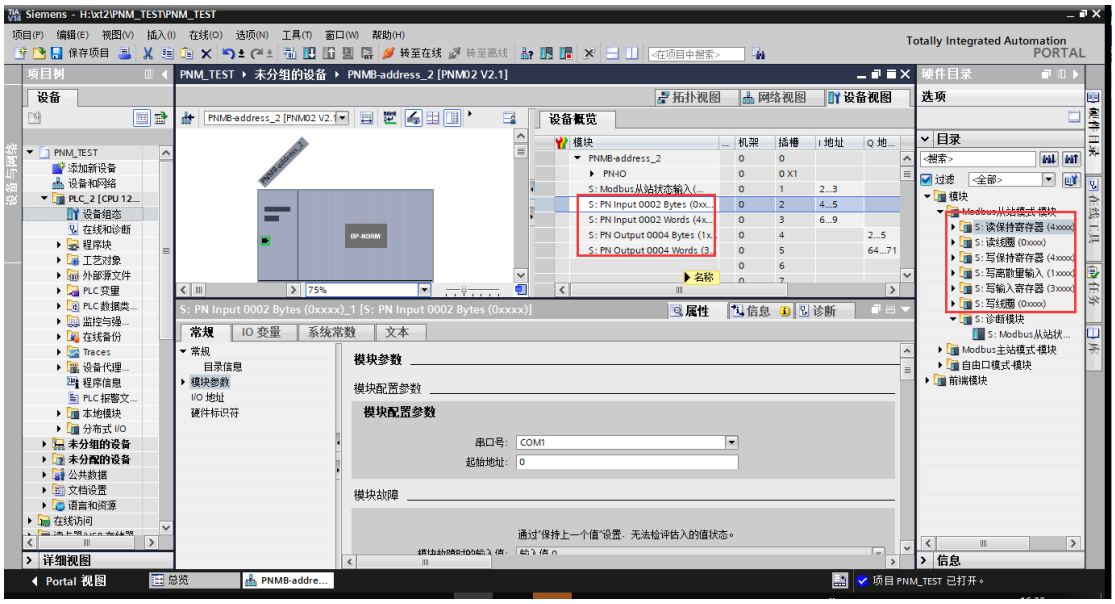
S :诊断模块：

S :**Modbus 从站输入状态**：表示当前串口的主站下发的数据包处理情况。

从站输入状态：仅可在最前插槽内插入 2 条命令。



12、网关作为从站，避免客户使用 0 区和 4 区输出数据时发现地址重叠的问题，PN 输出数据使用 1 区和 3 区，输入数据使用 0 区和 4 区。



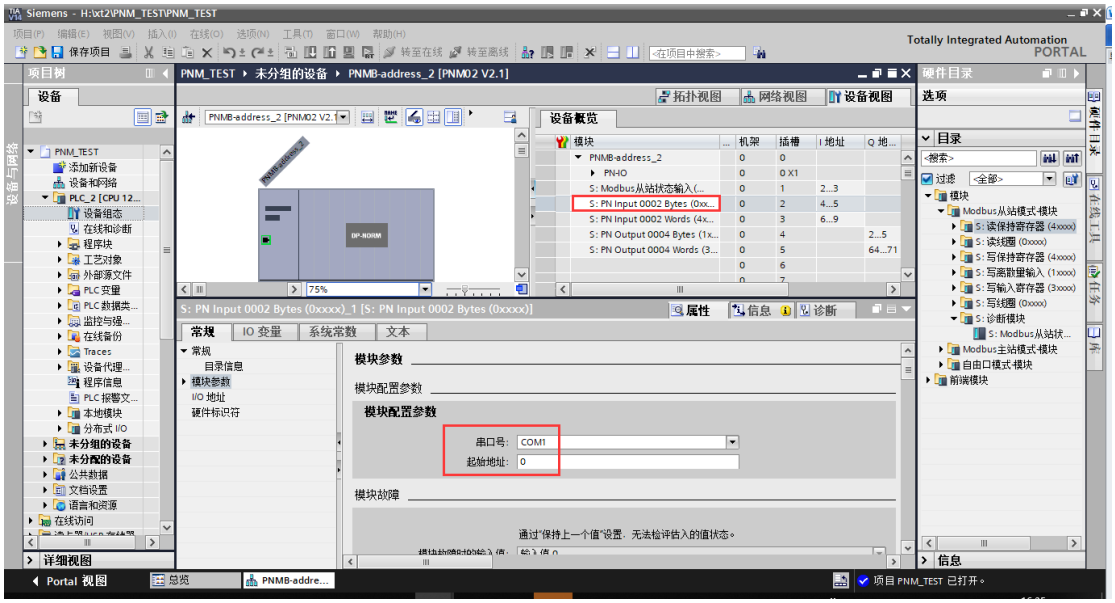
S :读保持寄存器（4xxxx）支持 1~512words 可选

S :读线圈（0xxxx）支持 1~1024Bytes 可选

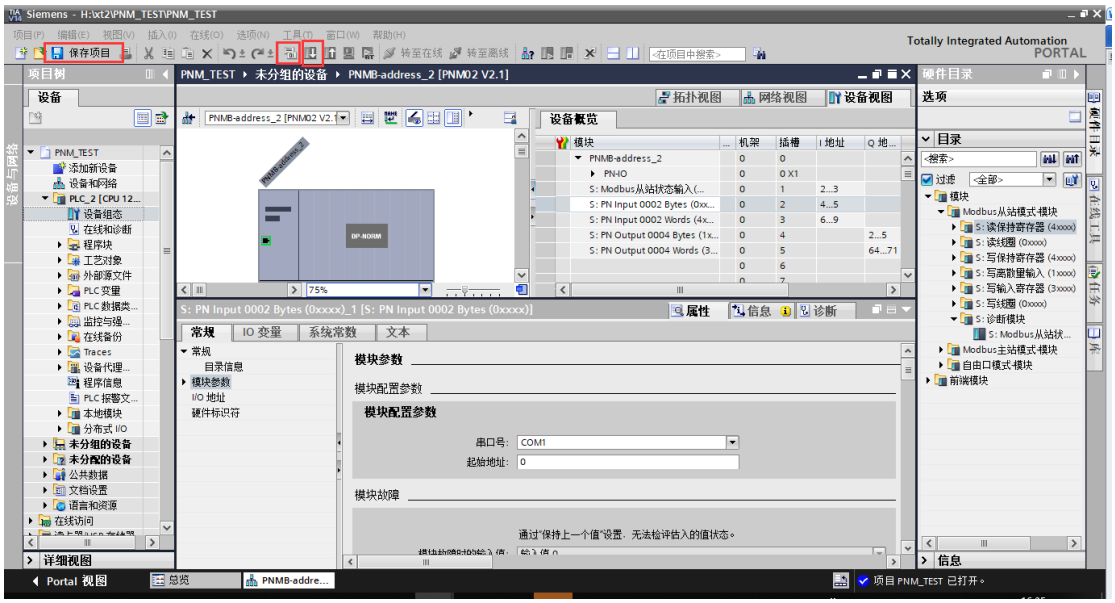
S :写离散量输入（1xxxx）支持 1~1024Bytes 可选

S :写输入寄存器（3xxxx）支持 1~125words 可选

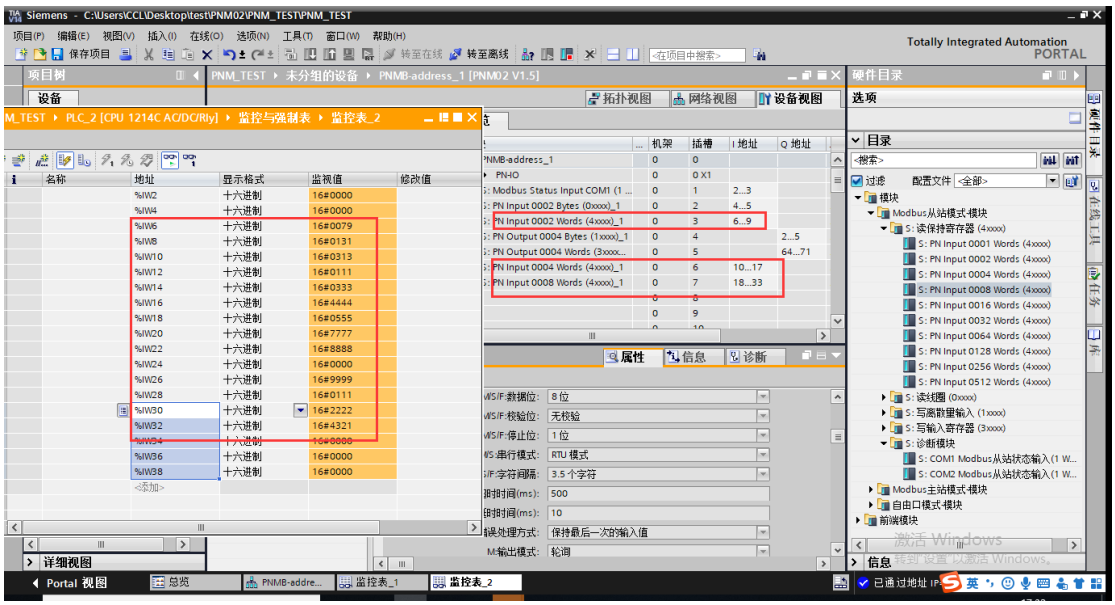
13、添加完读写命令，不需要对读写命令进行模块参数设置。地址访问方式参照如下：红色地址表一一对应插槽内的读写命令。当同一地址区采用多条命令时，地址自动往后加。

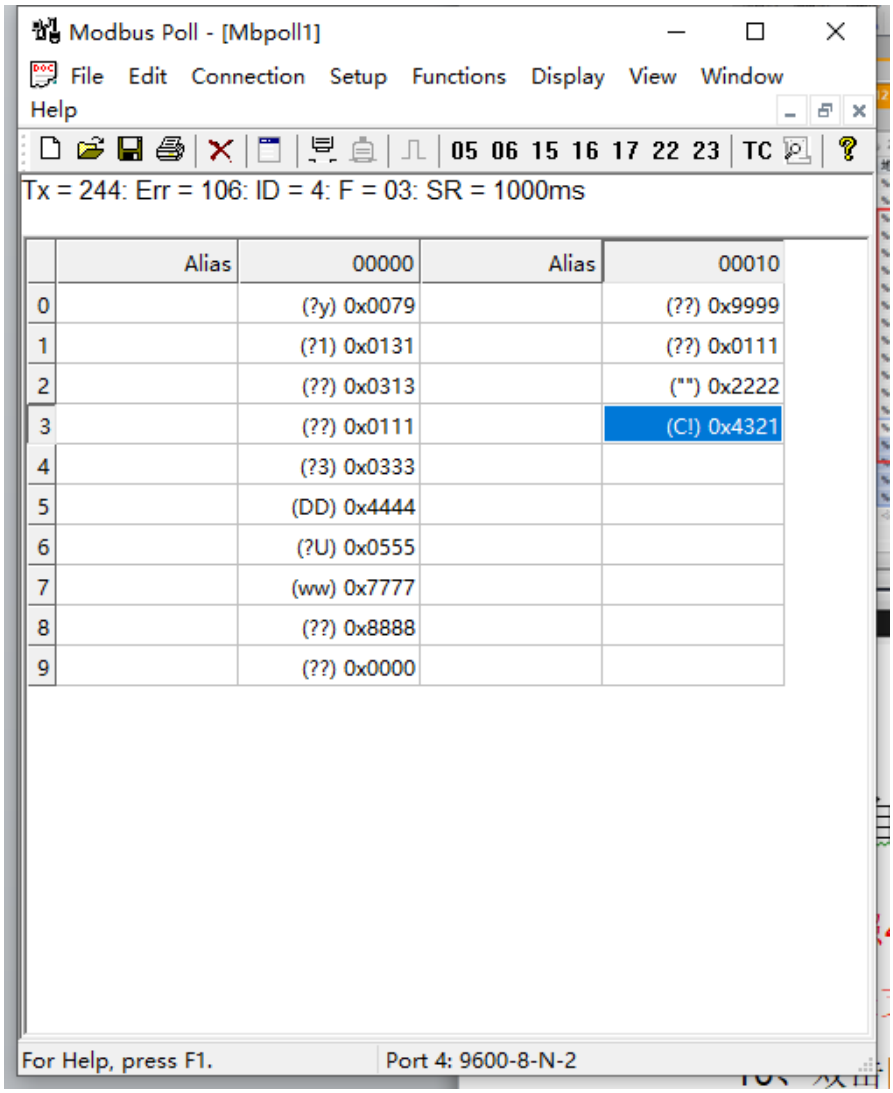


14、此时硬件组态已基本完成，保存项目，编译，下载。



15、下载成功后，打开监控表。串口 485 侧采用 Modbus Poll 模拟 RS485 主站设备。



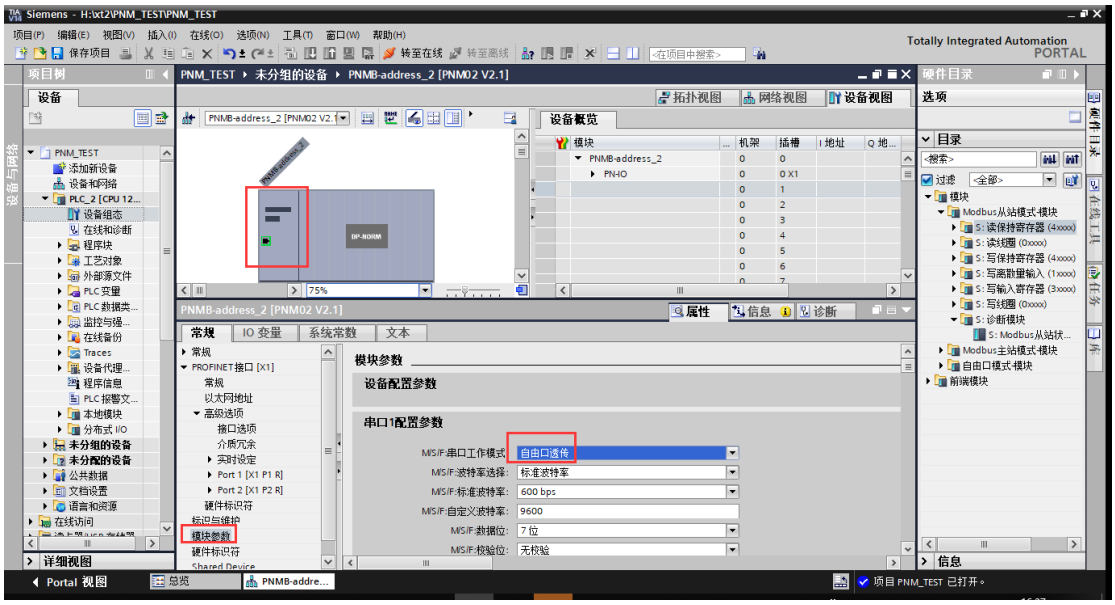

Modbus Poll - [Mbpoll1]
File Edit Connection Setup Functions Display View Window
Help
05 06 15 16 17 22 23 TC
Tx = 244: Err = 106: ID = 4: F = 03: SR = 1000ms
Alias 00000 Alias 00010
0 (?y) 0x0079 (??) 0x9999
1 (?1) 0x0131 (??) 0x0111
2 (??) 0x0313 ("") 0x2222
3 (??) 0x0111 (C!) 0x4321
4 (?3) 0x0333
5 (DD) 0x4444
6 (?U) 0x0555
7 (ww) 0x7777
8 (??) 0x8888
9 (??) 0x0000
For Help, press F1.
Port 4: 9600-8-N-2

4.3 自由口透传模式的配置

1→9 参照 4.1(主站模式)的 1→9。自由口测试使用 S7-1200 组态测试。

注：网关支持该功能的 GSD 文件是 20191008 及其以上版本

10、双击网关进入设备视图，选中网关，在常规参数下设置模块参数。（设置带 F 前缀的模块参数）



通用配置参数：M/S/F:网关工作模式选择**自由口透传**模式。

串口 1 和串口 2 参数注释：

M/S/F :物理层：RS485/RS232/RS422 可选，**默认 RS485。**

M/S/F :自定义波特率：0,300-500000bps 可设，填 0，表示串口使用标准波特率，非 0，及数值在 300-500000 之间时，串口使用自定义波特率，下面的标准波特率选项无效。**默认 0。**注：少数客户的设备是非标波特率，就可以自定义。

M/S/F :波特率：串口波特率，300-500000bps 可选，**默认 9600bps。**

M/S/F :数据位：7 位、8 位可选，**默认 8 位。**

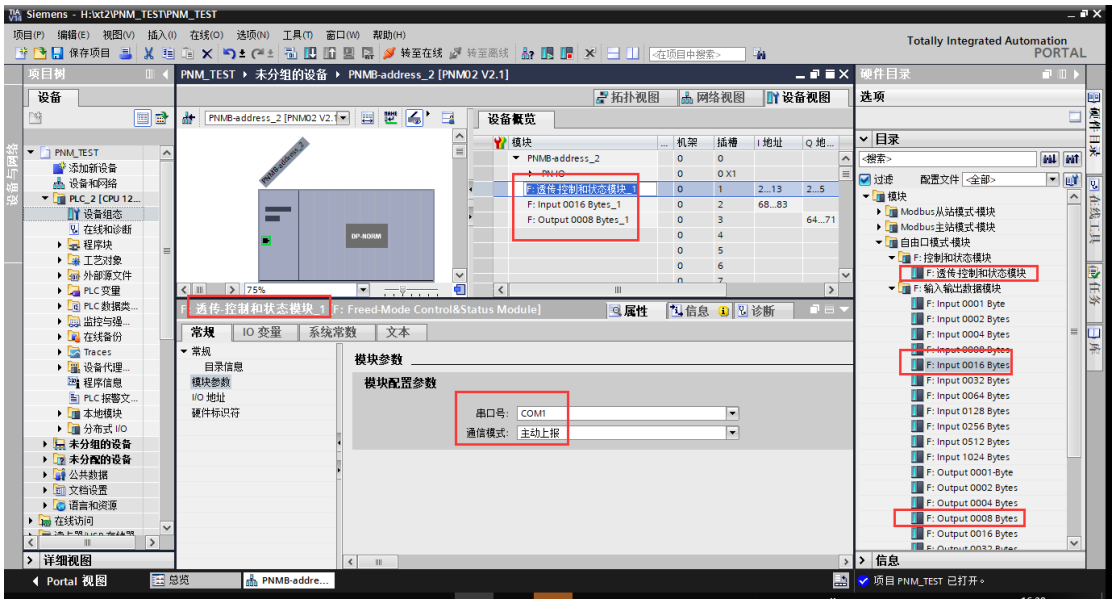
M/S/F :校验位：无、奇、偶、字符、空格校验可选，**默认无校验。**

M/S/F :停止位：1 位、2 位，**默认 1 位。**

M/S/F :字符间隔：接收报文时的帧间隔检测时间，1.5t~2000t 可选，**默认 5t。**（t 为单个字符传送的时间，和波特率有关）。

M/F : 响应超时时间(ms)：主站发送命令后，等待从站响应的时间。1~65535 可选，**默认 500。**

11、在设备视图选中网关，在右侧硬件目录里选择 F 开头的命令。



自由口透传模式下，分控制和状态模块、输入输出数据模块。

（1）控制和状态模块，需要设置串口号，透传通讯方式。透传通讯方式有主动上报模式和主从应答模式。

（2）输入输出数据模块，只需要设置串口号。

控制和状态模块的过程数据定义：

IO 模块数据方向	数据名称	变量名称	数据类型	字节偏移
输入数据	输出控制字-反馈	Control_Word_Feedback	uint16_t	0
	发送帧字节长度-反馈	Send_Data_Len_Feedback	uint16_t	2
	串口状态	COM_Status	uint16_t	4
	接收错误帧计数	Error_Counter	uint16_t	6
	接收总数据帧计数	Received_Counter	uint16_t	8
	当前接收帧字节长度	Received_Data_Len	uint16_t	10
输出数据	输出控制字	Control_Word	uint16_t	0
	发送帧字节长度	Send_Data_Len	uint16_t	2

变量定义：

变量名称	Bit15-6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0

Control_Word	Reserved	Received Counter Reset	Error Counter Reset	Timeout Error Reset	Parity Error Reset	Done Reset	Trigger
Send_Data_Len	Send_Data_Len						
COM_Status	Reserved			Timeout Error	Parity Error	Done	Busy
Error_Counter	Error_Counter						
Received_Counter	Received_Counter						
Received_Data_Len	Received_Data_Len						

输入数据说明：

4. Control_Word_Feedback 为输出控制字 Control_Word 的反馈值，输出控制字刷新到模块后，将更新到控制字反馈中。

5. Send_Data_Len_Feedback 为发送帧字节长度 Send_Data_Len 的反馈值，发送帧字节长度刷新到模块后，将更新到发送帧字节长度反馈中。

6. 应答模式下，串口发送数据时，Busy 位被置 1。

3.1 当在超时时间内串口接收到应答后，Busy 位清零，Done 完成位置 1，Received_Counter 计数值加 1，若接收帧有奇偶校验错误，则 Parity_Error 位被置 1，同时 Error_Counter 计数加 1。Received_Data_Len 中保存当前接收帧的字节数。

3.2 当在超时时间内串口未接收到应答，Busy 位清零，Done 完成位置 1，同时设置 Timeout_Error 为 1，Error_Counter 错误计数值加 1，Received_Data_Len 值清零。

4.在主动上报模式下，从站收到数据包时，Received_Counter 计数值加 1，若接收帧有奇偶校验错误，则 Parity_Error 位被置 1，同时 Error_Counter 计数加 1。

输出数据说明：

2. Received_Counter_Reset 上升沿时，接收计数值 Received_Counter 被清零，

Error_Counter_Reset 上升延时，错误计数值 Error_Counter 被清零，

Timeout_Error_Reset 上升延时，Timeout_Error 被清零，

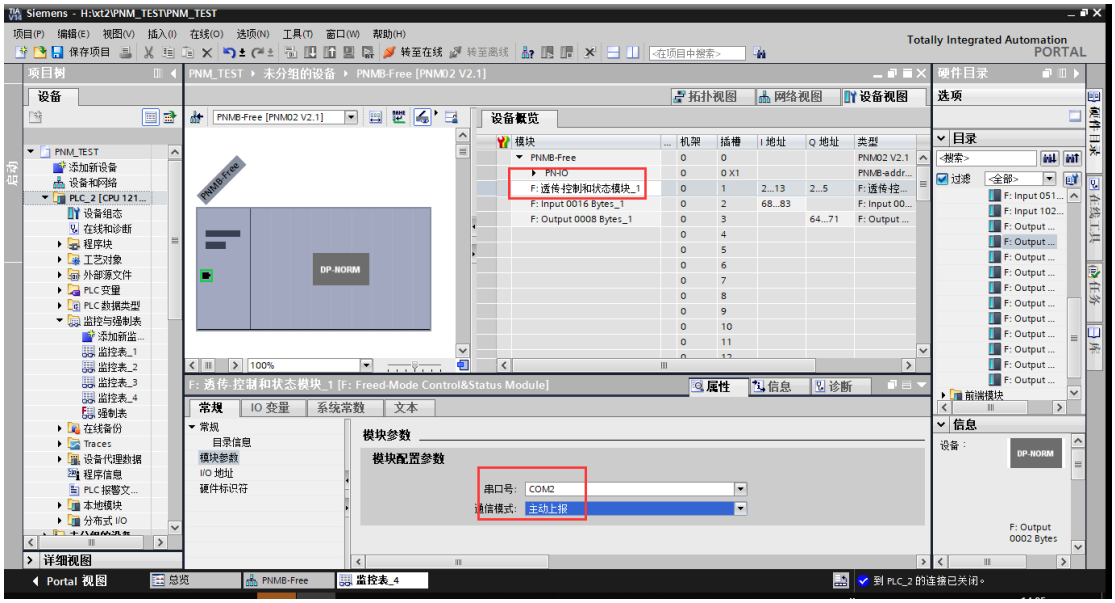
Parity_Error_Reset 上升延时，Parity_Error 被清零,

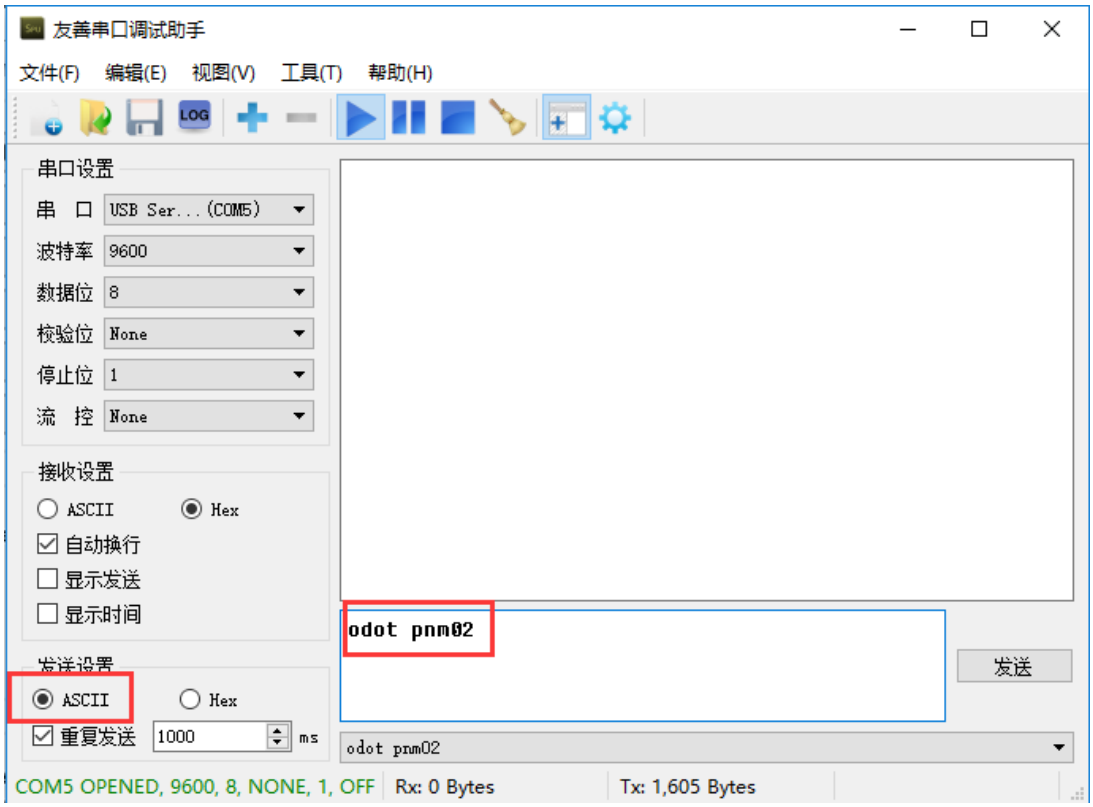
Done_Reset 上升延时，Done 被清零。

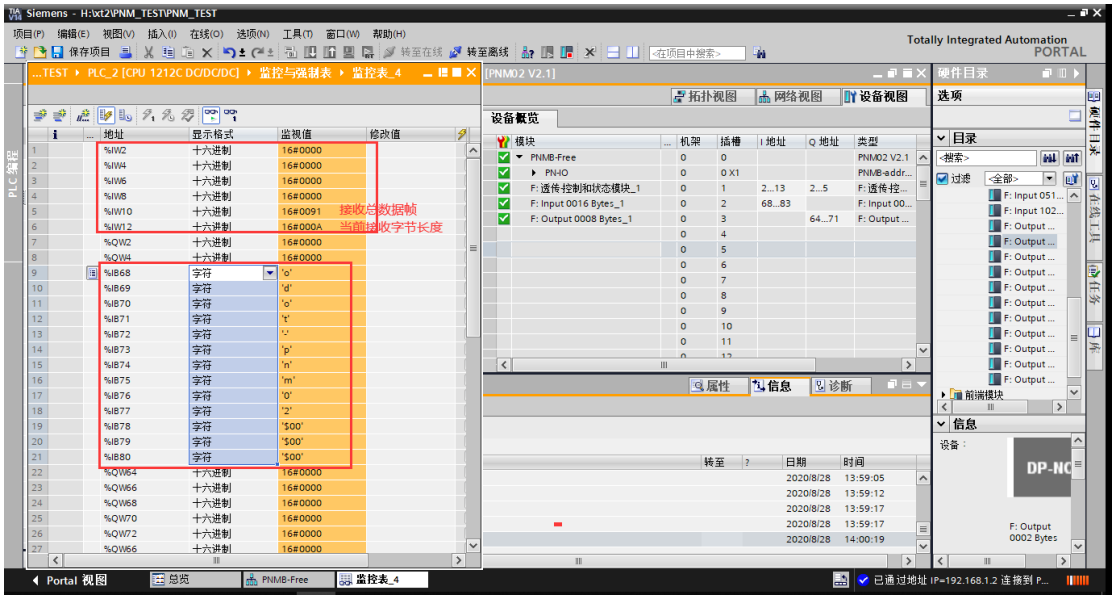
2.主动上报模式下，Trigger 位无效，Send_Data_Len 无效。

3.主从应答模式下，Trigger 上升延时触发一次串口数据发送，串口将按 Send_Data_Len 的数据长度发送数据包并等待应答处理。

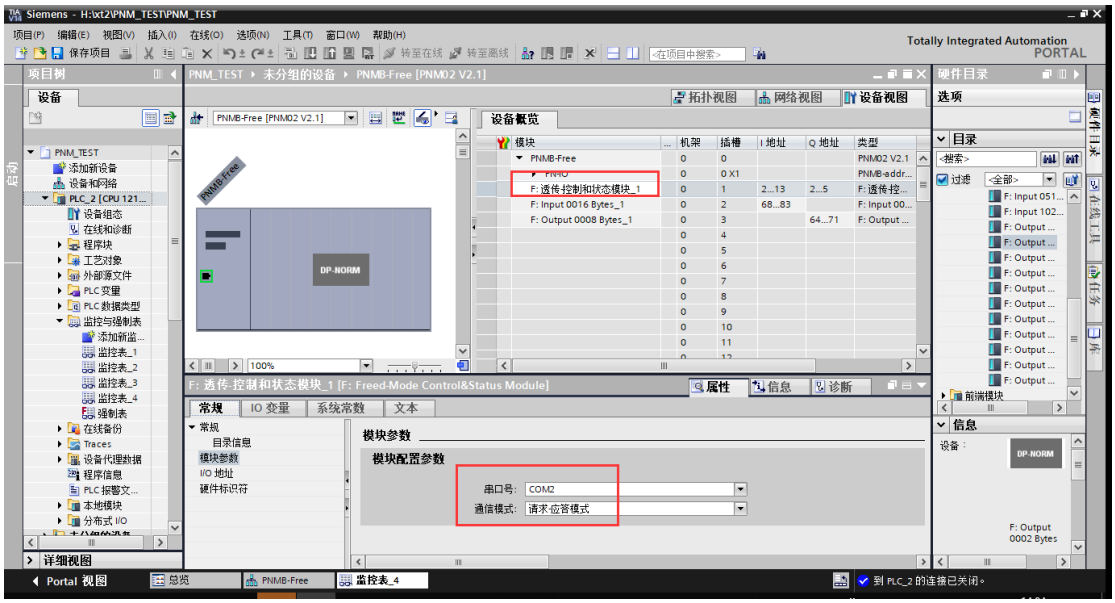
（1）将网关设置为**主动上报**模式，网关串口 1 接调试串口工具模拟现场设备（比如扫码枪、称重仪表等）。可在控制和状态模块、输入输出数据模块监控到相应的值的变化。



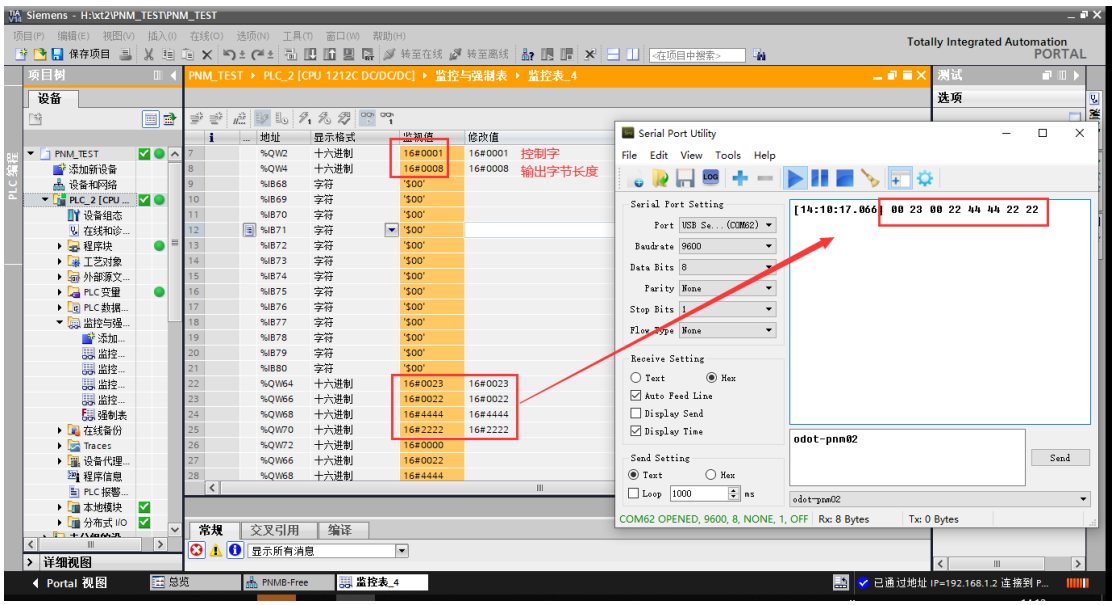




（2）将网关设置为**主从应答**模式。当控制字 Trigger 为 0 无效时，网关保持主动上报形式，接收串口侧的数据。



当控制字 Trigger 为 0-1 脉冲激活时，网关发送数据到串口。注：Trigger 位激活一次，网关发送一次数据。



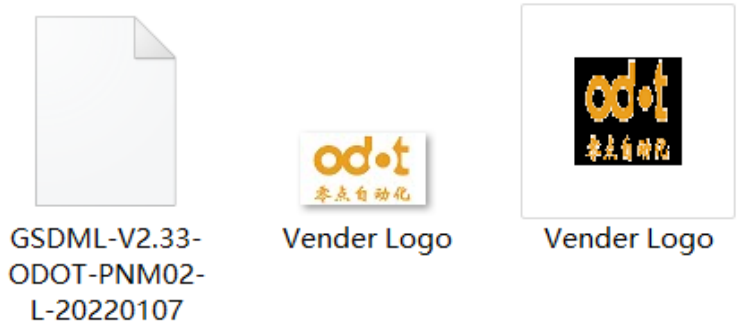
通过一系列的设置调试，PLC 通过网关将串口侧数据采集上来后存储在 PLC 地址区，工程人员自己解析上传报文数据格式，提取有效的数据进行编程处理。项目完成后，保存、编译，下载程序。

五、在西门子 STEP7 V5.5 中使用本模块

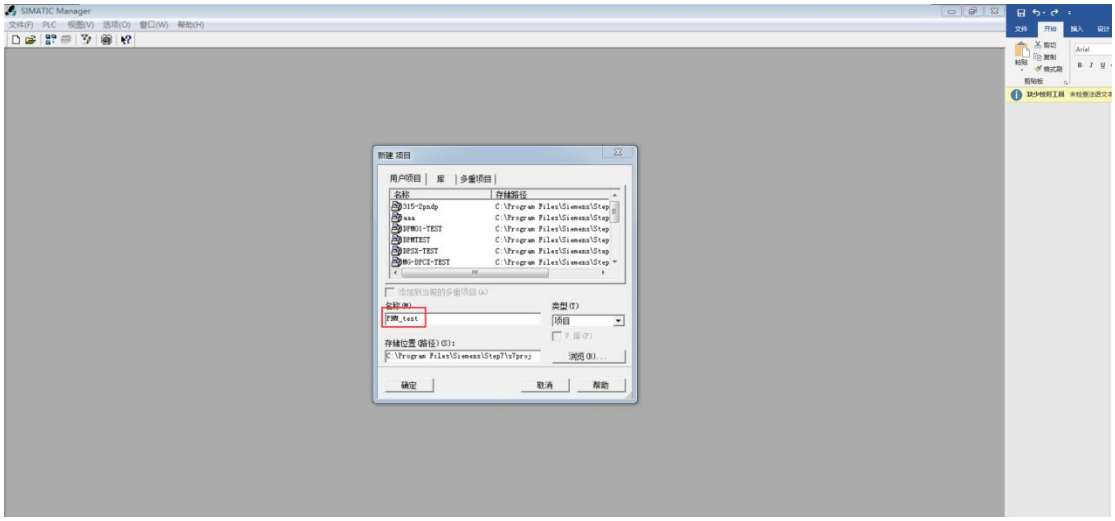
本章将以 SIEMENS 的 315-2 PN/DP 作为 PROFINET 的 Controller，使用 Step7 作为编程软件，举例说明 PNM 的使用方法。先将 PLC、调试电脑、PNM 接入到同一个以太网网络中。

5.1 MODBUS 主站模式的配置

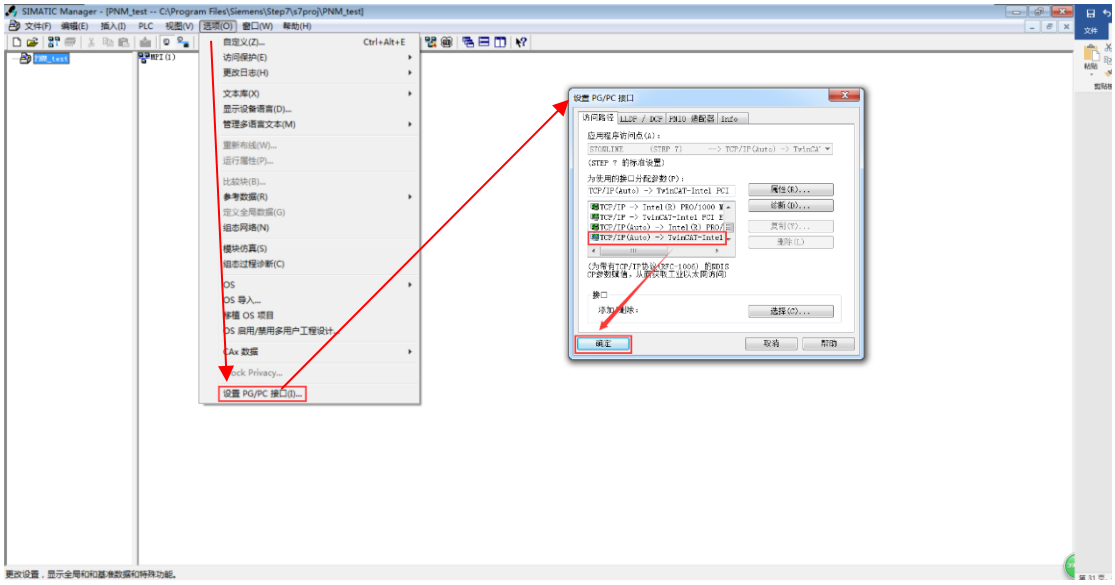
1. 找到产品光盘中的 XML 文件夹，并确认文件夹中是否有网关的 XML 文件，若没有请联系供应商索取。



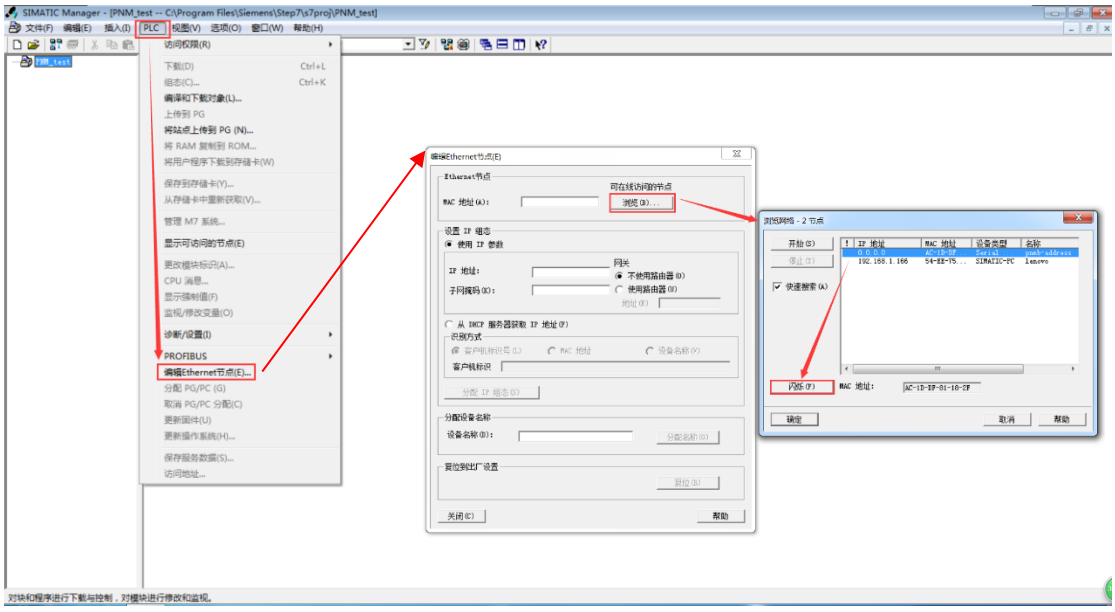
2、打开 STEP7 软件，点击创建新项目，新建一个工程，命名为“PNM_test”.



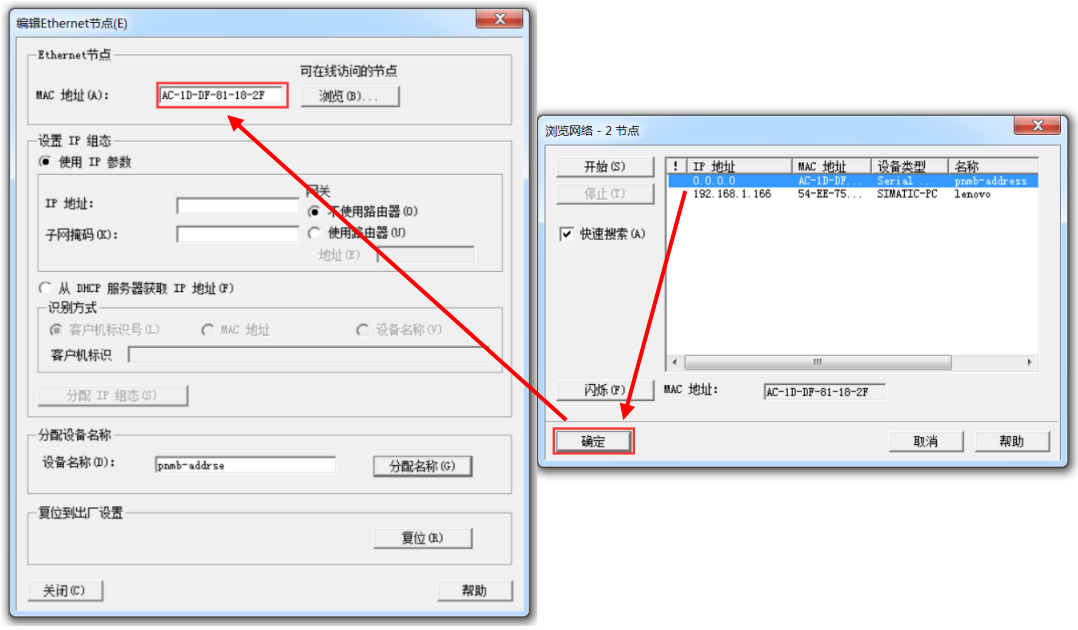
3、点击“选项”→“设置 PG/PC 接口”，在设置 PG/PC 接口页面将通讯接口选择为与 PLC 连接的网卡。



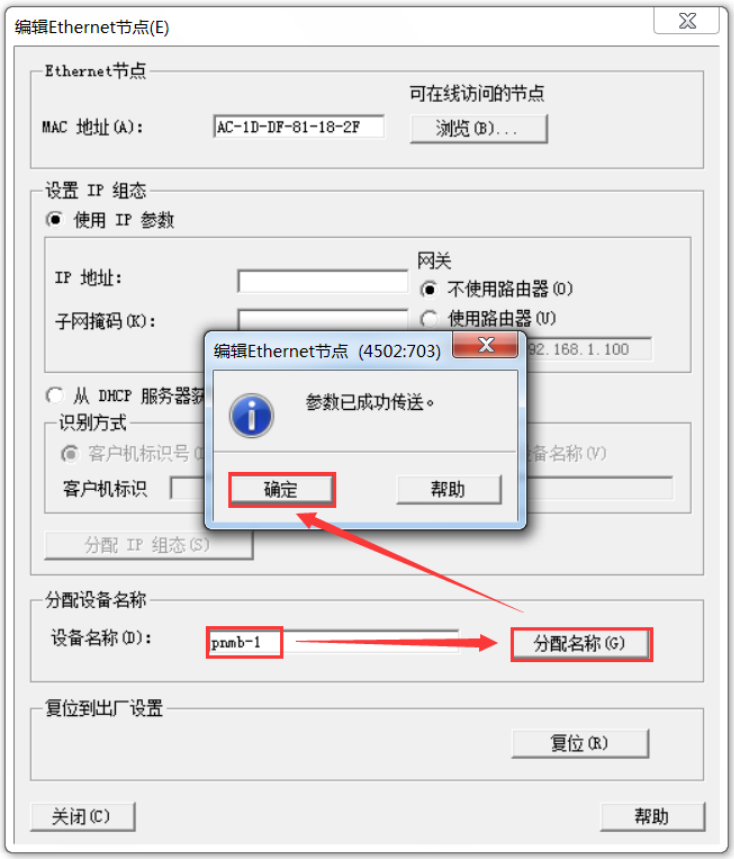
点击“PLC”→“编辑 Ethernet 节点”，在“编辑 Ethernet 节点”页面，点击浏览，在“浏览网络”页面，可以看到扫描上来的 ODOT-PNM02 模块，模块的默认名称为“pnmb-address”，选中模块，点击“闪烁”，模块上的 “SF”灯会闪烁，当网络中同时存在多个 ODOT-PNM02 模块时，可以通过该功能对模块进行区分。



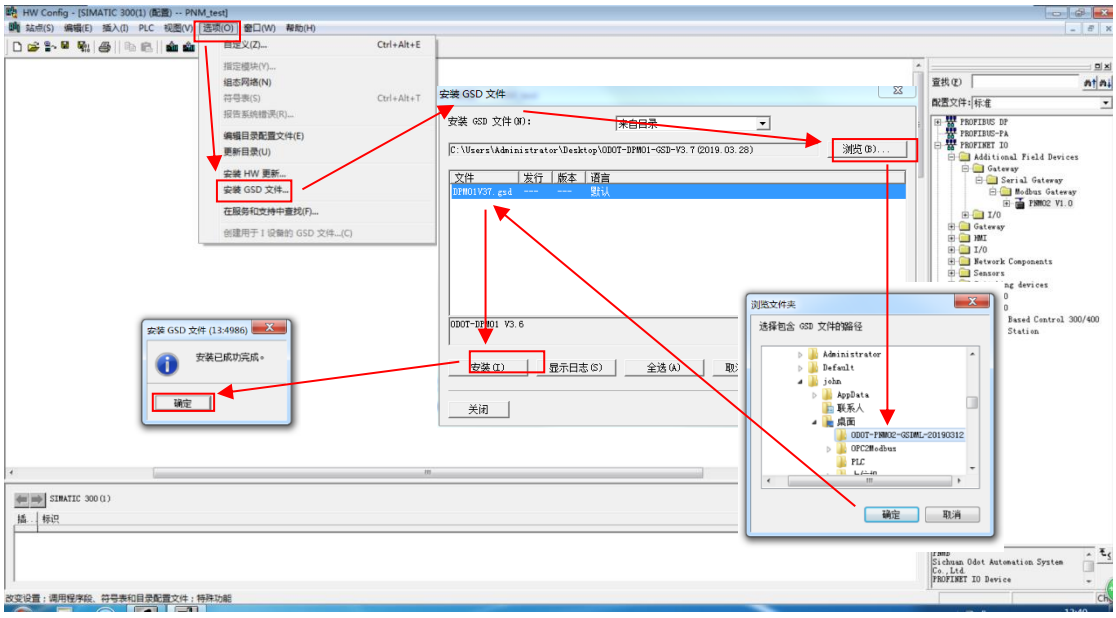
选中模块点击“确定”，软件会自动将选中的模块的 MAC 地址写入“编辑 Ethernet 节点”页面的相应位置。



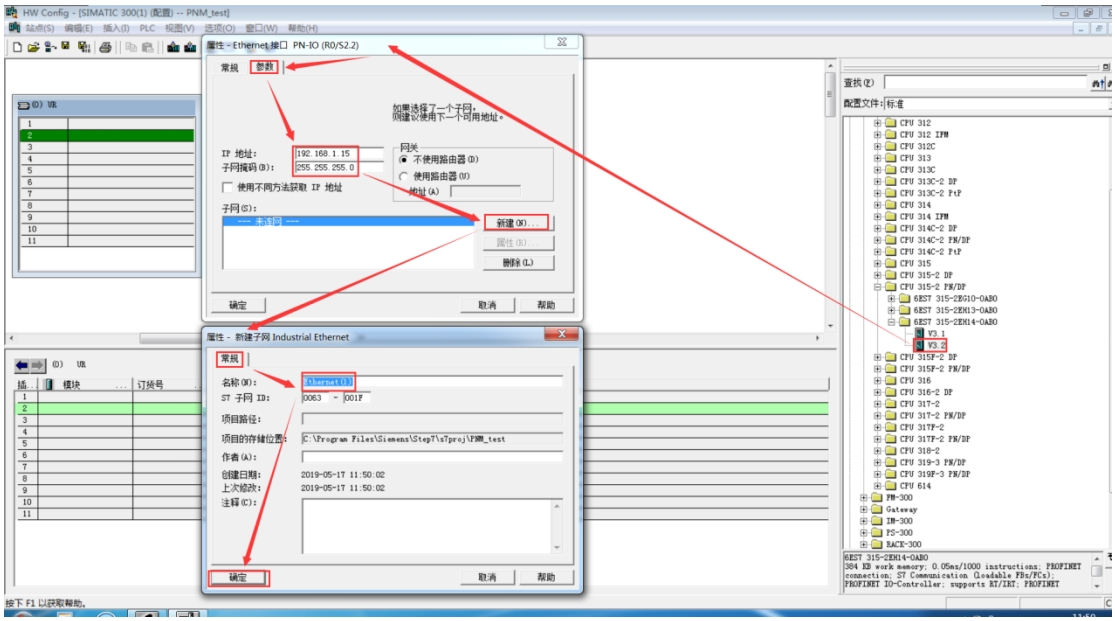
修改设备名称，点击“分配名称”，为 ODOT-PNM02 设置新的设备名称，该名称将用于后面的组态。注：修改设备名称主要用在网络中同时存在多个 ODOT-PNM02 模块的情况下，如果网络中只有一个 ODOT-PNM02，可以不修改其设备名称，在后面的组态中直接使用其出厂默认名称“pnmb-address”即可。



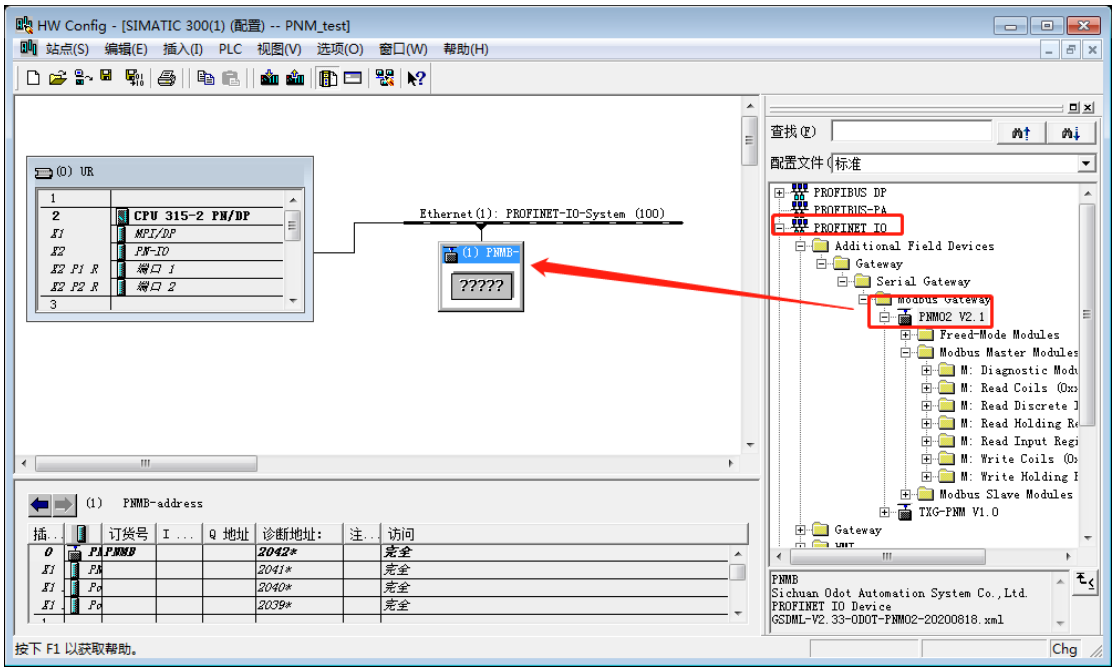
4、在 STEP7 硬件组态页面，点击 “选项”→“安装 GSD 文件”，在“安装 GSD 文件”点击 “浏览”选择路径，找到 ODOT-PNM02 对应的 XML 文件所在文件夹，点击“确定”，选中 XML 文件，点击“安装”，将 ODOT-PNM02 的 XML 文件安装到 STEP7 中。



5、在 STEP7 硬件组态页面，双击组态控制器，设置控制器 IP 并添加子网，点击确定。

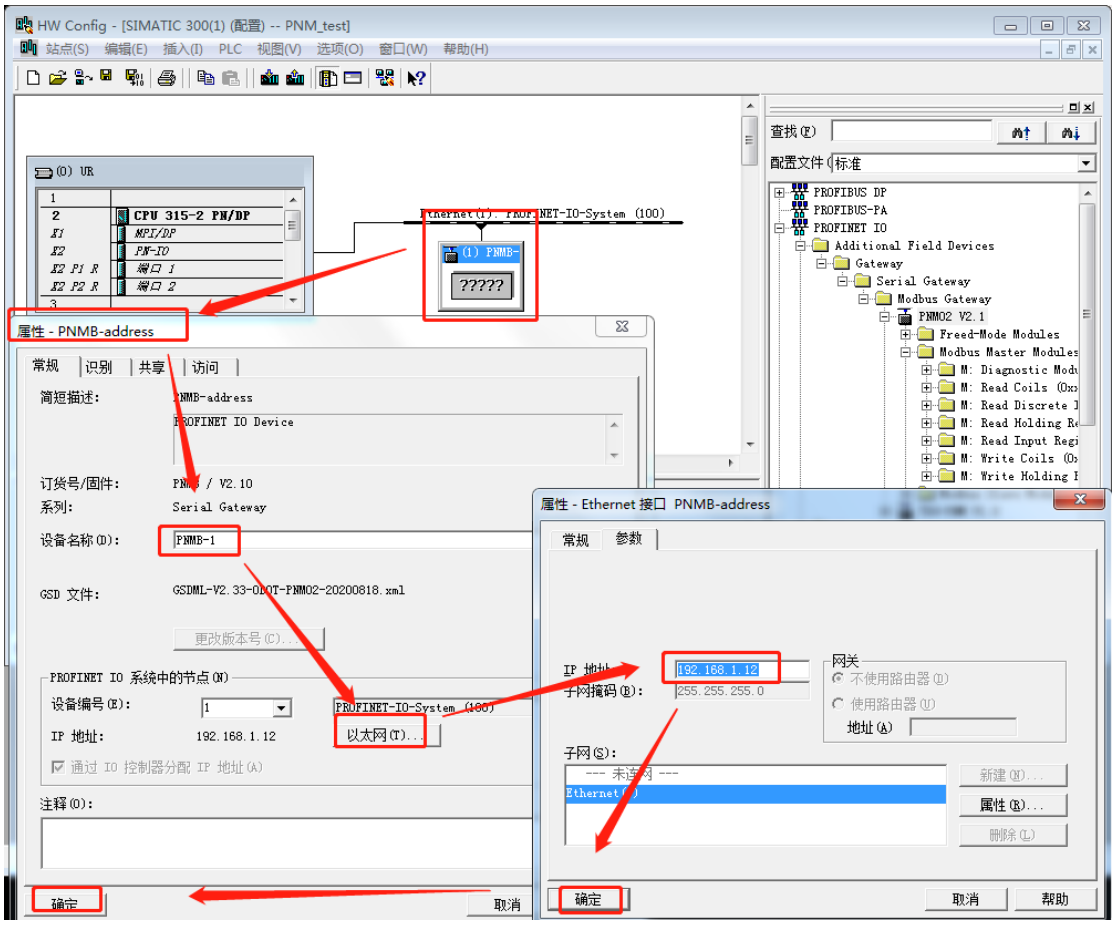


6、选中子网，在硬件目录页面的 PROFINET IO→Additional Field →Devices→Gateway→Serial Getway→Modbus Gateway 下双击 PNM02 将 PNM02 网关组态至 PROFINET 网络 。

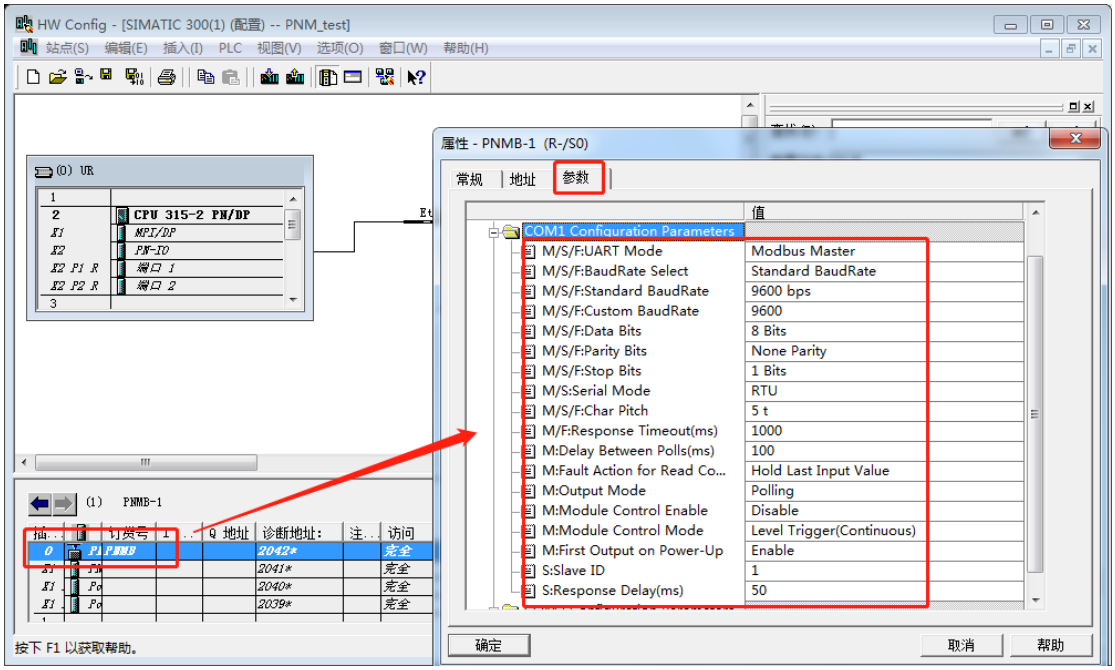


7、选中 ODOT-PNM02 设备图标，在“属性”页面的“常规”选项卡中，填入设

备名称，**该名称一定要与步骤 3 中设置的模块名称一致**，点击“以太网”，设置模块的 IP 地址，点击“确认”。



8、选中 ODOT-PNM02 设备图标，在软件下方的模块插槽信息显示部分，双击第一个插槽，在弹出的属性窗口中，选中参数选项卡，修改 ODOT-PNM02 模块参数。



模块串口配置参数：串口 1 和串口 2 配置参数是相同的。

注：M 表示该参数主站模式有效，S 表示该参数从站模式有效，F 表示该参数自由口透传模式有效。

M/S/F :网关工作模式：Modbus 主站、Modbus 从站可选，**默认** Modbus 主站。

M/S/F:波特率选择：标准波特率、自定义波特率可选，默认值：标准波特率。

M/S/F :标准波特率：串口波特率，300-500000bps 可选，**默认 9600bps。**

M/S/F :自定义波特率：0,300-500000bps 可设，**默认 9600bps。**注：少数客户的设备是非标波特率，就可以自定义。

M/S/F :数据位：7 位、8 位可选，**默认 8 位。**

M/S/F :校验位（Parity Bits）：无、奇、偶、字符、空格校验可选，**默认无校验。**

M/S/F :停止位（Stop Bits）：1 位、2 位，**默认 1 位。**

M/S/F :串行模式（Serial Mode）：RTU/ASCII 模式可选，**默认 RTU 模式。**

M/S/F :字符间隔（Char Pitch）：接收报文时的帧间隔检测时间，1.5t~2000t 可选，**默认 3.5t**。（t 为单个字符传送的时间，和波特率有关）。

M/F : 响应超时时间(Response Timeout)：主站发送命令后，等待从站响应的时间。1~65535 可选，**默认 500。**

M :轮询延时时间(Delay Between Polls)：Modbus 命令发送的间隔时间(收

到从站响应报文到发送下一条命令的延时)，0~65535 可选，**默认 10。**

M :读指令错误处理方式（Fault Action for Read Command）：从站读数据超时后，数据处理方式，保持最后一次输入值、清零输入值可选，**默认保持最后一次输入值。**

M :输出模式（Output Mode）：轮询、事件触发（数据发生改变）可选，**默认轮询。**“轮询模式”下 Modbus 周期性地发送写报文。“事件触发”模式时只有 Modbus 输出数据发生变化时才发送写命令。

M :模块控制（Module Control）：禁止、使能可选，默认禁止。当需要对 Modbus 的读写命令进行控制时，选择使能模式，通过控制“模块控制输出”的值控制 Modbus 的读写命令。

M :控制模式（Control Mode）：电平触发（持续有效）、上升沿触发（单次触发）可选，**默认电平触发（持续有效）。该值只在**模块控制**使能模式有效**

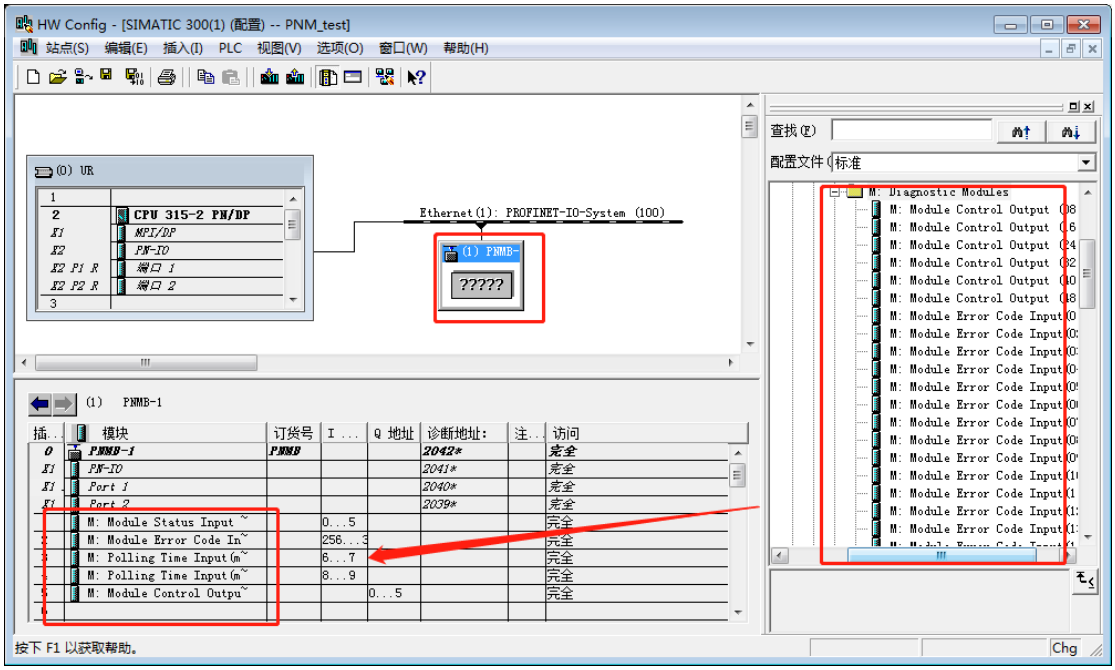
M :上电首次输出数据（First Output on Power-Up）：使能、禁止可选，**默认使能。**

S :响应延时(Response Delay)：0~65535 可选，**默认 0.**

C、串口 2 配置参数（Com2 Configuration Parameters）：

与串口 1 参数功能相同。

9、选中 ODOT-PNM02 设备图标，在软件下方的模块插槽信息显示部分，选中插槽，双击目录视图中 PNM02 下方模块文件夹下的模块，在插槽中插入模块，



当需要对模块状态进行监视时可先添加“诊断模块”。注：不是必加项。主站模式下诊断模块有以下几种类型：

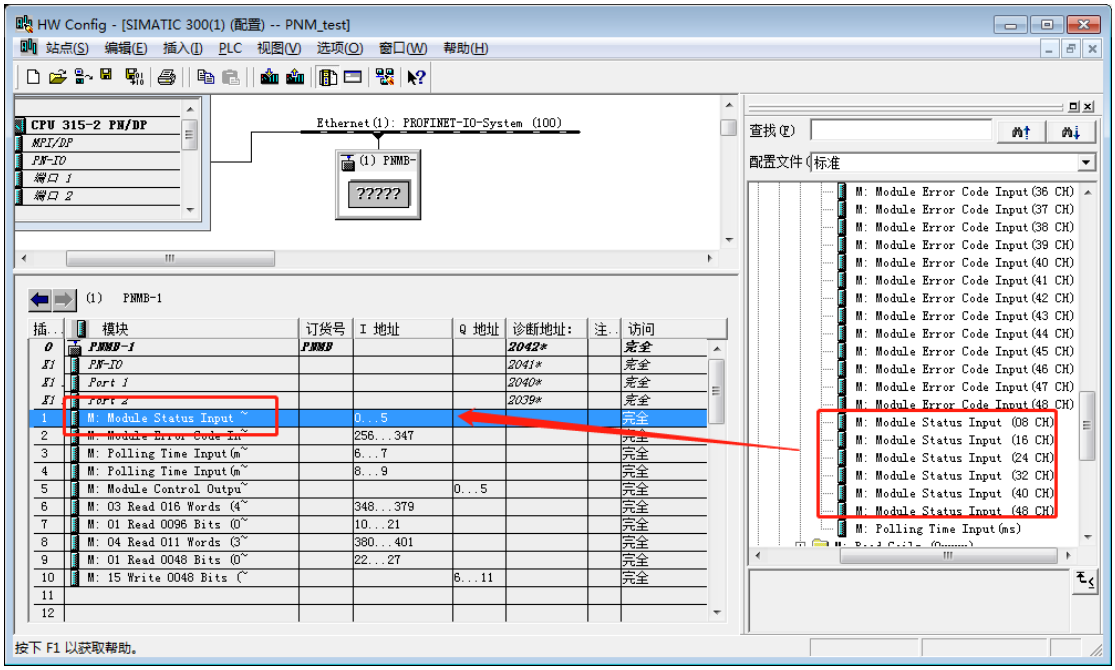
（1）模块状态输入（Module Status Input），只能插入第 1 个插槽；

（2）模块错误代码输入（Module Error Code Input），可以插入前 2 个插槽；

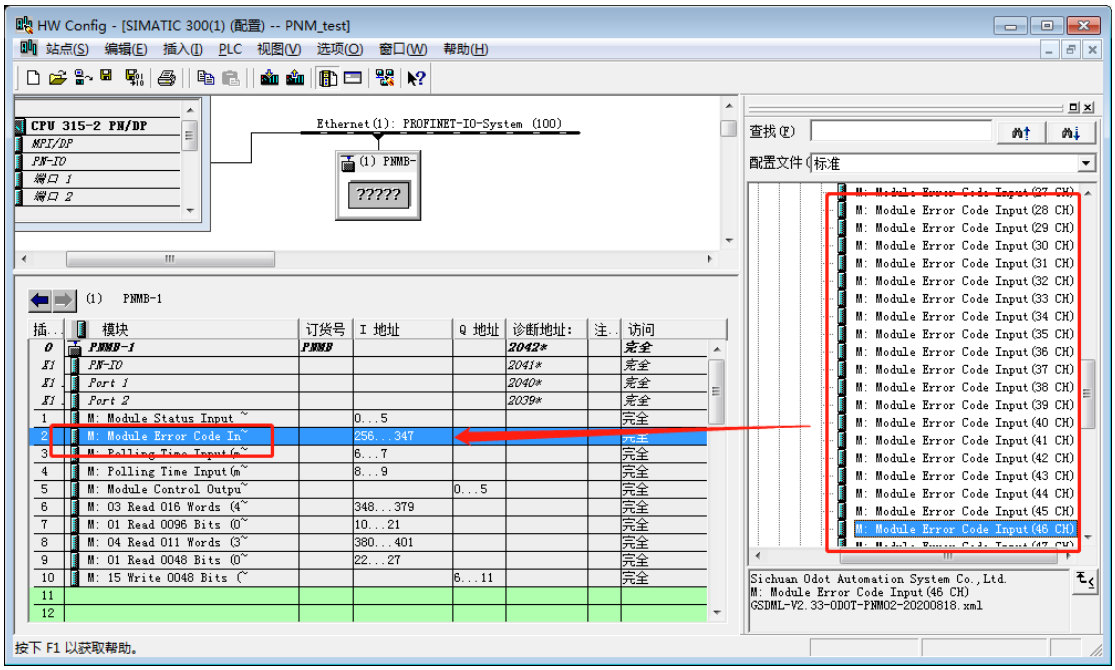
（3）轮询时间输入（Polling Time（ms）Input），可以插入前 4 个插槽；

（4）模块控制输出（Module Control Output），可以插入前 5 个插槽；

模块状态输入：有 8~48 通道可选，“模块状态输入”可监测每一个数据插槽的工作状态，一个“位”对应一条数据通讯命令，当某一个数据通讯插槽的通讯命令出现故障时，对应的状态位被置 1，故障恢复后自动清零。在下图的配置中，如果 6 号插槽的读取数据命令出现故障，I0.0 将被置 1；



模块错误代码输入：有 1-48 个通道可选，一个 “字”对应一条通讯命令，当一个数据插槽的通讯命令出现故障时，错误代码模块可显示出现错误的命令的功能码和具体的错误代码，用户可根据错误代码，判断是何种原因产生故障，进而采取对应的调整方法。详细的描述请参见“错误代码表”。 在下图的配置中，如果 6 号插槽的读取数据命令出现响应超时，PIW256 值将变成 0x0F；

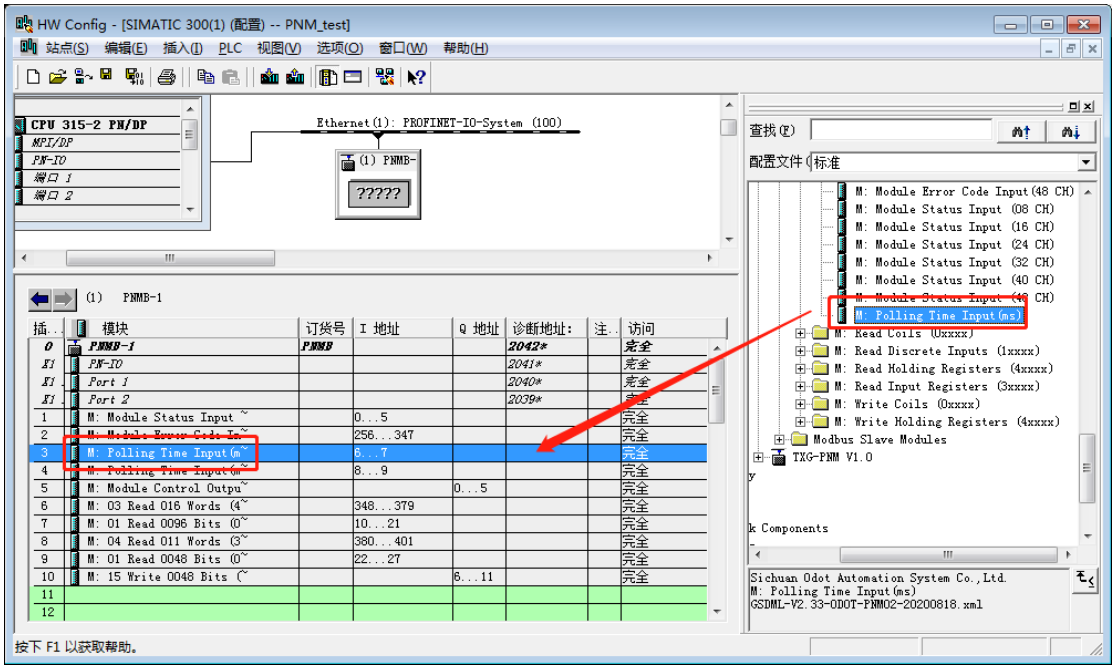


Modbus 错误代码表

错误代码	故障说明	故障排除方法
0x00	工作正常	无
0x01	非法功能码	设备不支持当前功能码，请参考从站手册选择对应的功能码模块
0x02	非法数据地址	设备数据超出其地址范围，参考从站手册修改数据起始地址或数据长度
0x03	非法数据值	数据长度错误，数据长度超出最大允许值125(Word)或2000(Bit)，修改长度
0x04	数据处理错误	检查数据值范围是否符合从站要求
0x05	应用层长度不匹配	增大接收字符间隔，检查通信参数设置
0x06	协议 ID 错误	检查发送端报文
0x07	缓存地址错误	设备内部错误
0x08	位偏移错误	设备内部错误
0x09	从站 ID 号不匹配	增大超时时间，检查硬件连接状态，检查通信参数设置
0x0A	CRC 错误	CRC 错误，检查通讯线路
0x0B	LRC 错误	LRC 错误，检查通讯线路
0x0C	应答功能码不匹配	检查硬件连接状态
0x0D	应答地址不匹配	检查硬件连接状态
0x0E	应答数据长度不匹配	检查硬件连接状态
0x0F	通信超时	增大超时时间，检查硬件连接状态，检查通信参数设置
0x10	ASCII 模式起始符错误	‘:’冒号起始符错误
0x11	ASCII 模式结束符错误	CR/LF 回车换行结束符错误
0x12	ASCII 模式非字符数据	数据中包含非16进制 ASCII 码
0x13	ASCII 模式字符数错误	从站应答长度错误

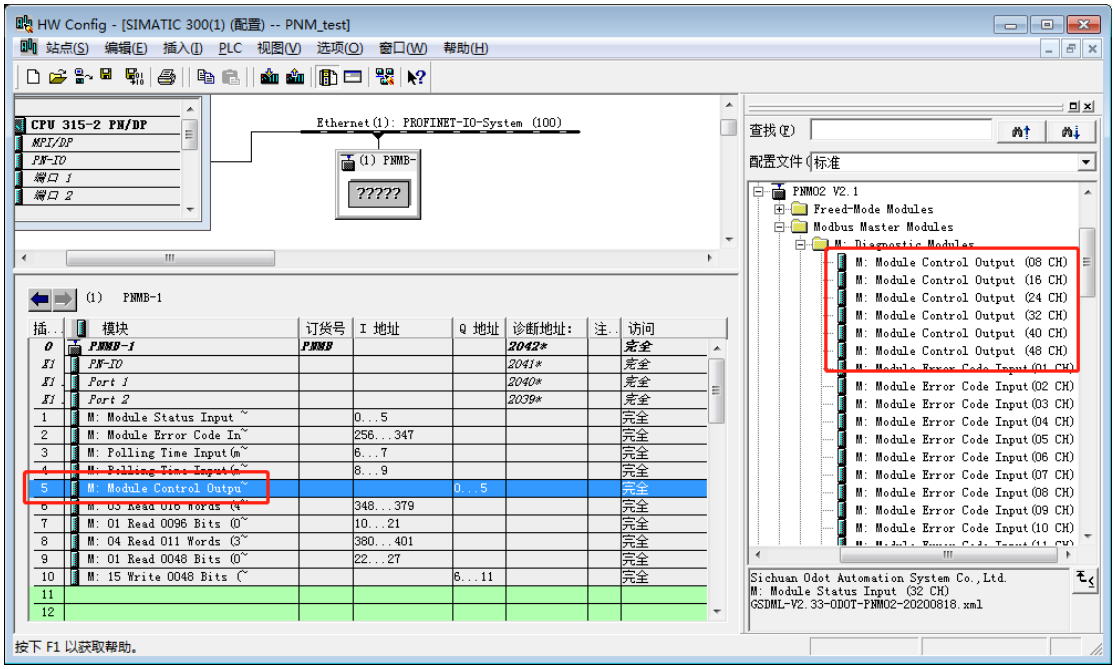
轮询时间输入：用于监视对应串口上所有通讯指令的轮询时间，注：串口 1、

串口 2 是独立的，所以要添加**两条**命令分别监视轮询时间。

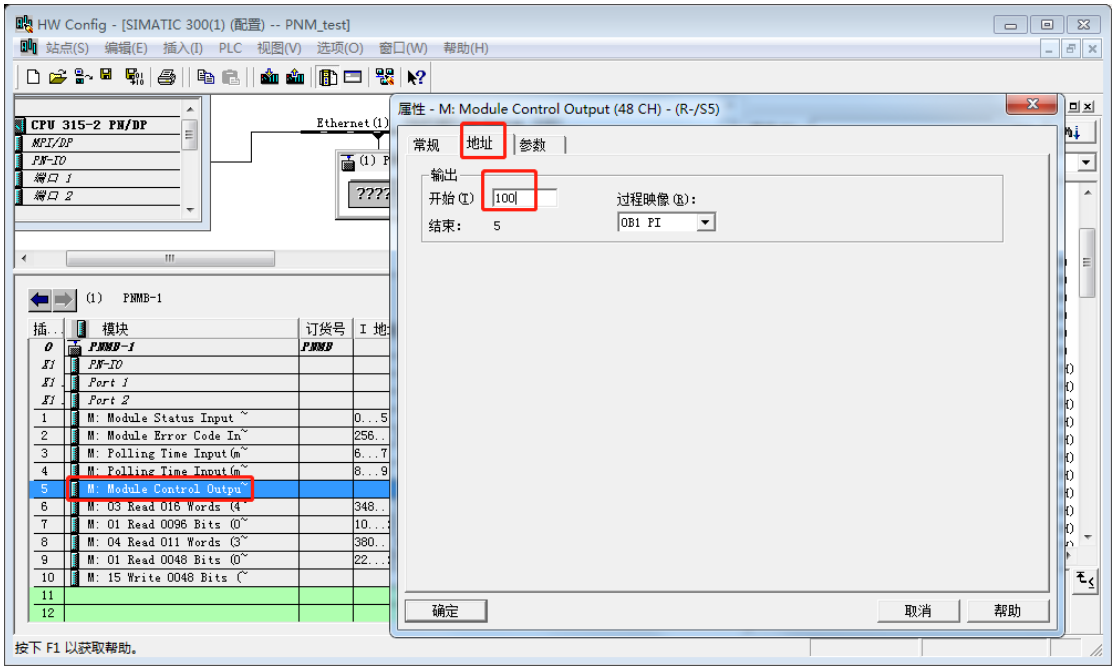


模块控制输出：有 8~48 通道可选。当串口下参数“模块控制（Module Control）”为使能时，该命令模块有效，一个“位”对应一条数据通讯命令。

在下图的例程中，使能串口下参数“模块控制（Module Control）”后，Q0.0=1 时，6 号槽的 03 读 16 个字这条命令执行。Q0.0=0 时，6 号槽的 03 读 16 个字这条命令不执行。Q0.1=1 时，7 号槽的 02 读 96 个位这条命令执行。Q0.1=0 时，7 号槽的 02 读 96 个位字这条命令不执行。以此类推。



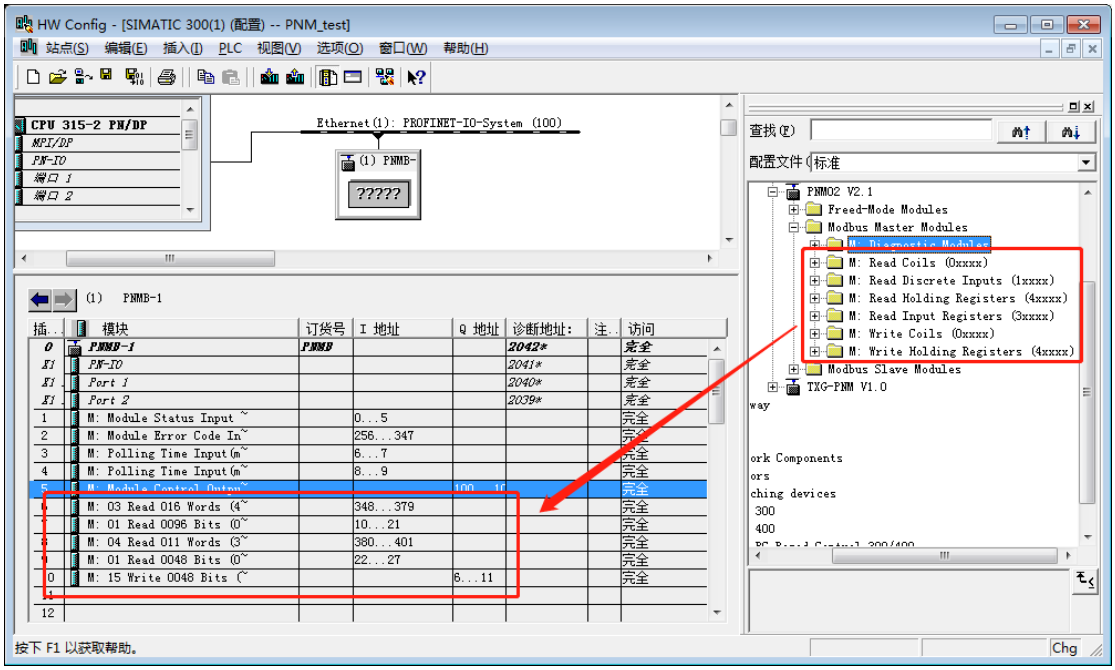
双击该模块控制模块，在“属性”页面的“地址”选项卡下，手动更改模块的输出开始地址为 100 时，当 Q100.0=1 时，6 号槽的 03 读 16 个字这条命令执行。Q100.0=0 时，6 号槽的 03 读 16 个字这条命令不执行。Q100.1=1 时，7 号槽的 02 读 96 个位这条命令执行。Q100.1=0 时，7 号槽的 02 读 96 个位字这条命令不执行。以此类推。



注：模块控制输出功能激活后。在控制范围内的读写命令都需要使能控制。

例：采用**模块控制输出（8 CH）**命令，在后面的槽位添加有 8 个以上的读写命令（10 条命令），前面 8 条读写命令需要使能控制，在程序中使能后才执行，否者不执行，后面 2 条不需要控制自动执行。

9、网关作为主站，支持 Modbus 功能码 01/02/03/04/15/16.将硬件目录的读写命令添加到插槽内。



M :读保持寄存器（Read Holding Registers）支持 1~125words 可选

M :读离散量输入（Read Discrete Inputs）支持 8~200bits 可选

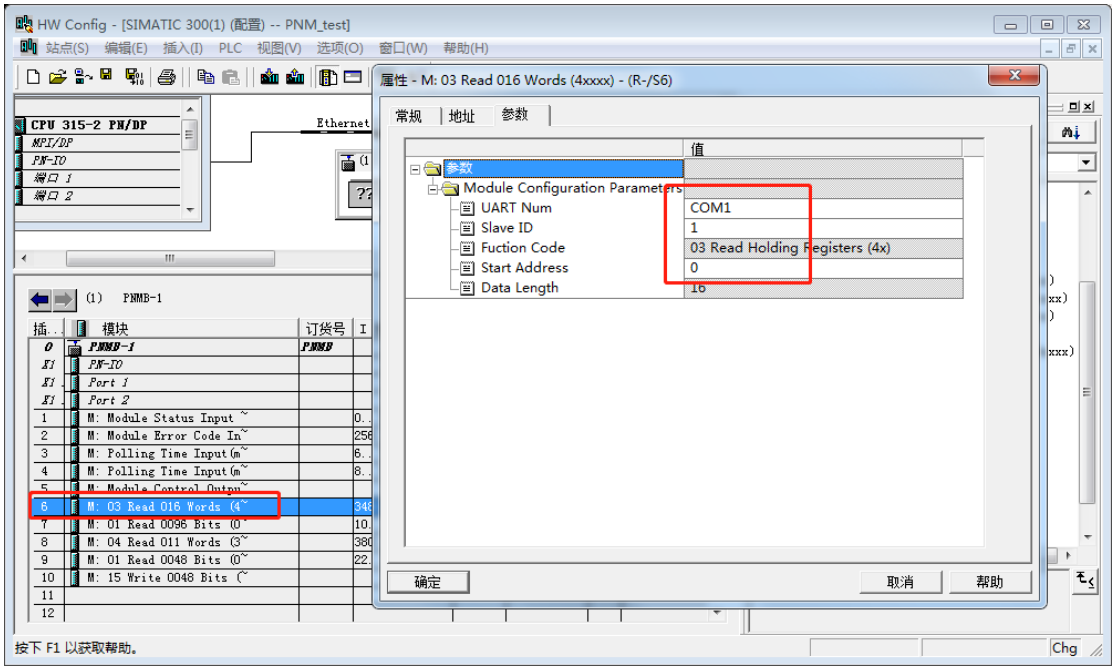
M :读输入寄存器（Read Input Registers）支持 1~125words 可选

M :读线圈（Read Coils）支持 8~200bits 可选

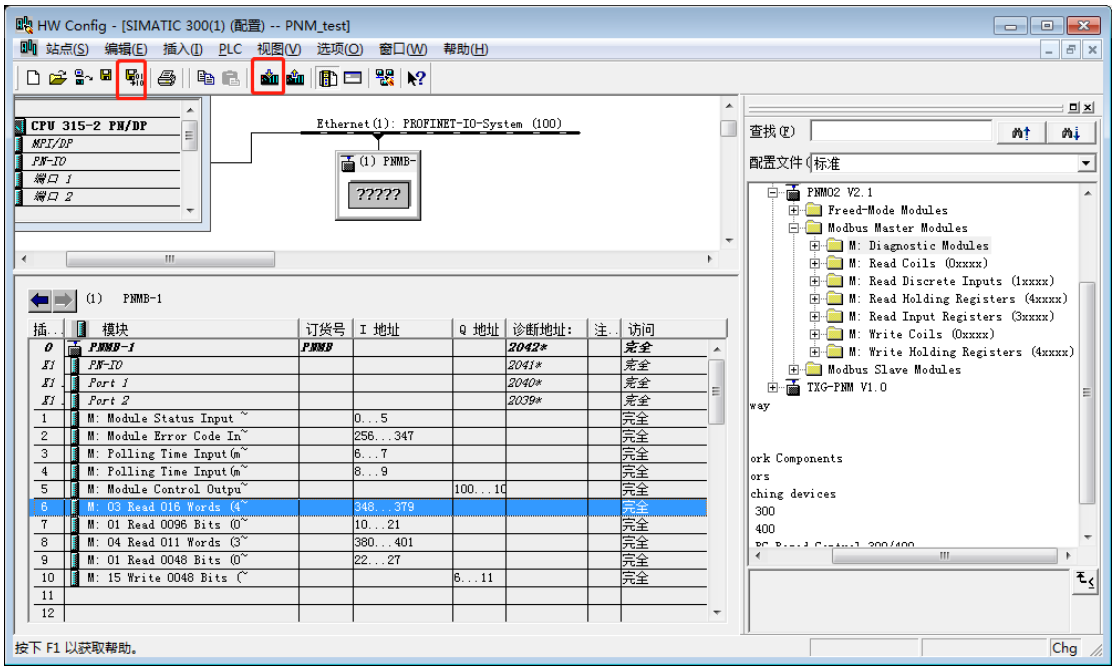
M :写保持寄存器（Write Holding Registers）支持 1~125words 可选

M :写线圈（Write Coils）支持 8~200bits 可选

10、添加完读写命令，双击该命令模块，在“属性”页面的“参数”选项卡下，可对该命令模块进行参数设置。包括该命令对应的 Modbus 从站设备连接的模块串口号（UART Num）COM1 或 COM2, Modbus 从站站号（Slave ID），数据起始地址（Start Address）。例，从站模块的数据在 40001-40016，起始地址填 0 即可，若从站模块数据在 40200-40215，起始地址填 199 即可。

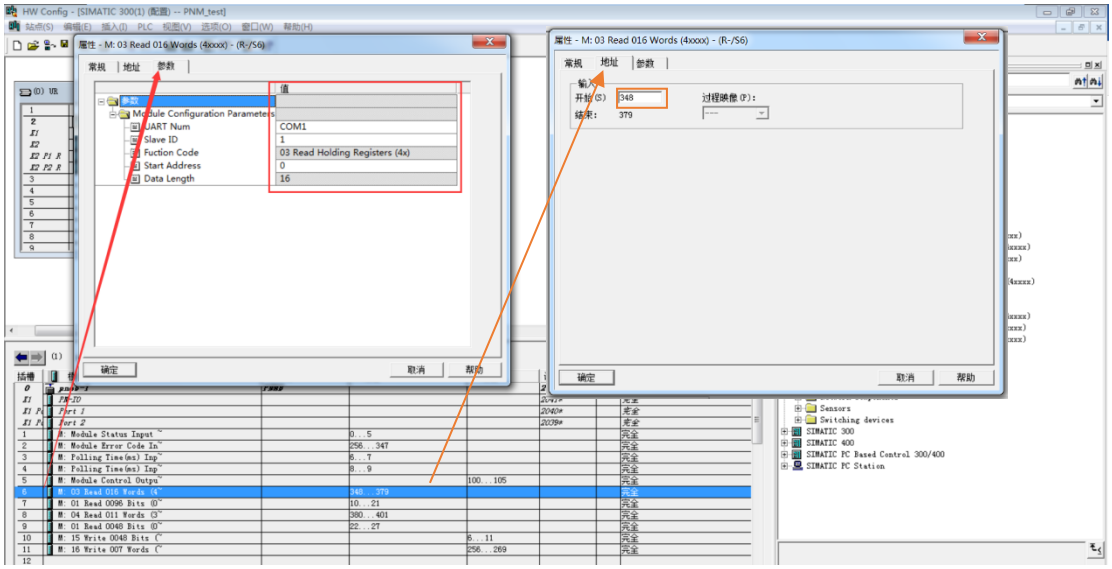


11、此时硬件组态已基本完成，保存、编译硬件组态并下载工程。

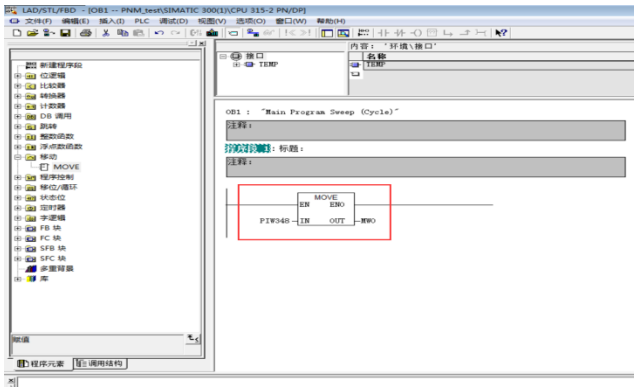


12、数据的监视与使用。

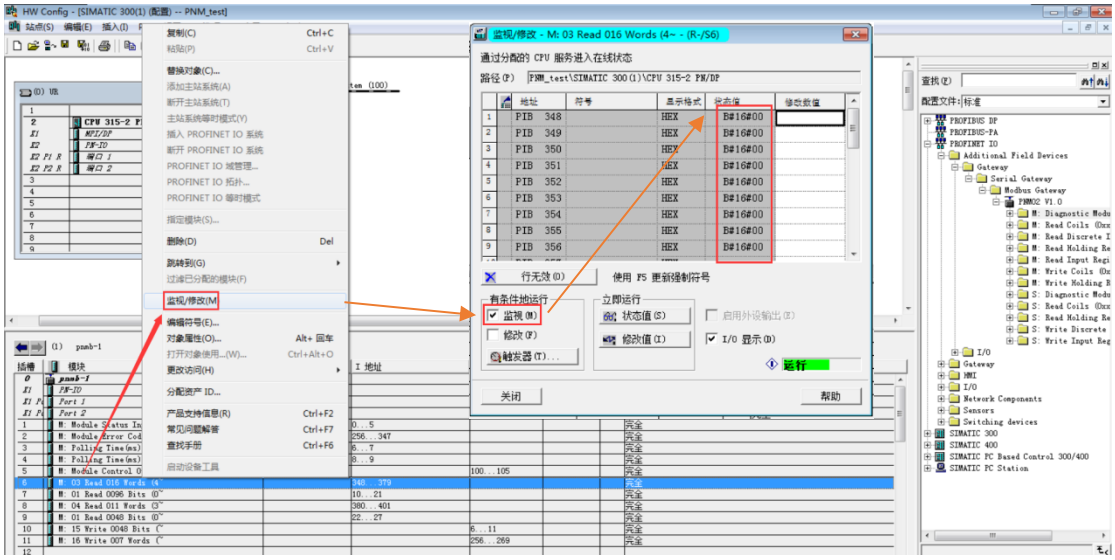
当 6 号插槽配置如下时，接在 COM1 口上的站号为 1 的 Modbus 从站，4 区 40001 至 40017 寄存器的数据将被读入至 PLC 的 I 区 IW348 至 IW378。（对于写数据的命令同理，只是数据对应于 PLC 内部的 Q 区）



上述例程中，在 PLC 程序中进行如下操作即可将接在 COM1 口上的站号为 1 的 Modbus 从站，4 区 40001 的数据赋值给 MW0。（写数据的命令同理，赋值给对应的 Q 区地址即可）



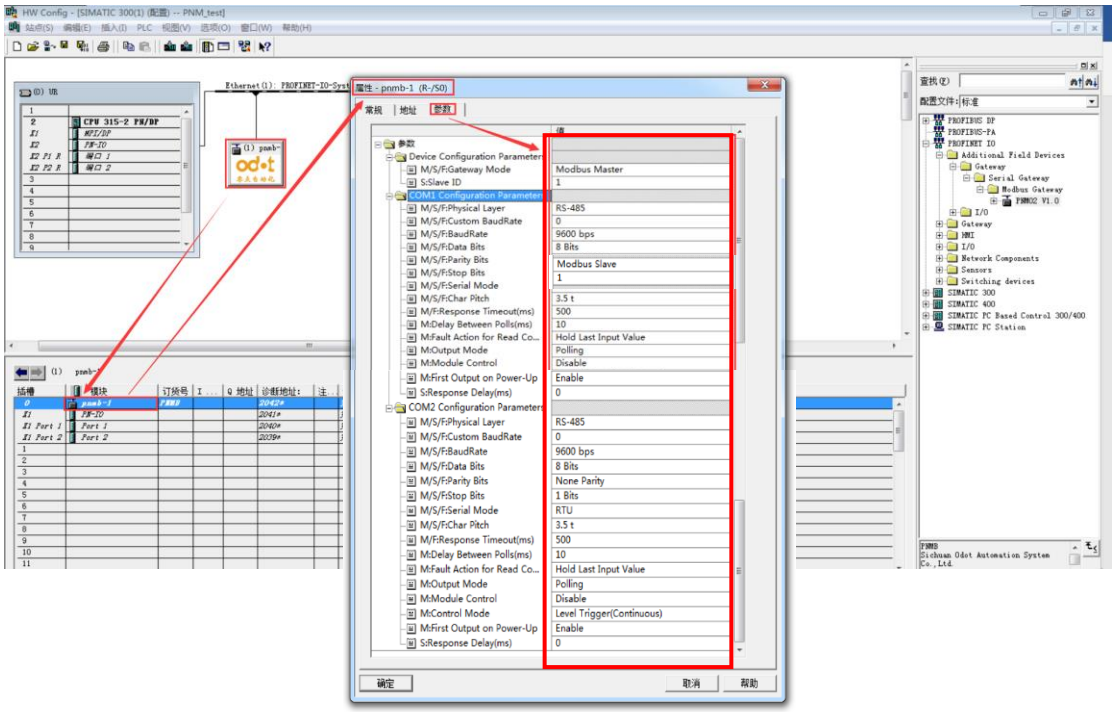
上述例程中，选中 6 号插槽右击，点击“监视/修改”选项，在“监视/修改”页面勾选“监视”，即可实时监视通讯数据，该功能可方便调试（如果是写数据的命令，可通过点击“修改值”按键，即可将数据写入到 Modbus 从站设备）。



5.2 MODBUS 从站模式的配置

1→7 参照 5.1(主站模式)的 1→7。

8、选中 ODOT-PNM02 设备图标，在软件下方的模块插槽信息显示部分，双击第一个插槽，在弹出的属性窗口中，选中参数选项卡，修改 ODOT-PNM02 模块参数。



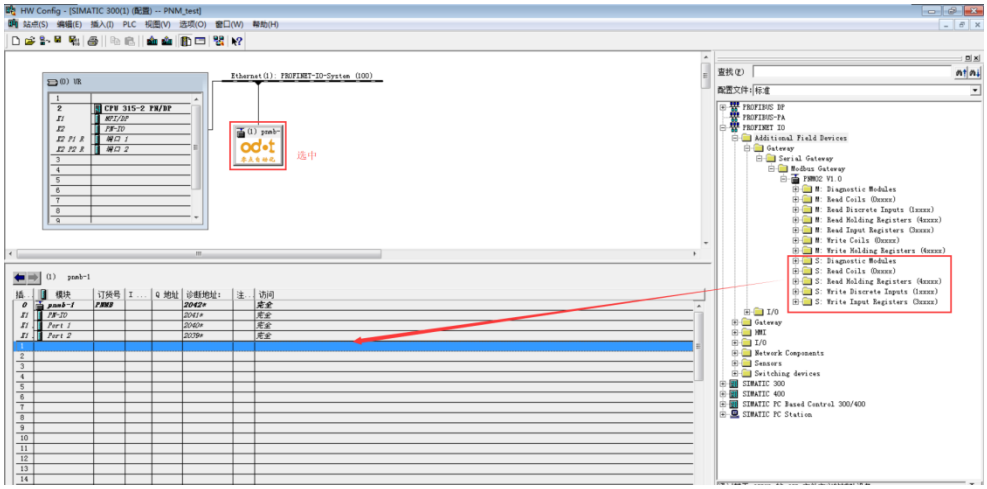
双击网关进入设备视图，选中网关，在常规参数下设置模块参数。

M/S/F :网关工作模式（Gateway Mode）：选择为 **Modbus 从站模式（Modbus Slave）**。

S:从站 ID 号：设为 1（网关作为 Modbus RTU/ASCII 的从站站号即为 1）

串口 1 和串口 2 参数参考主站模式注释。

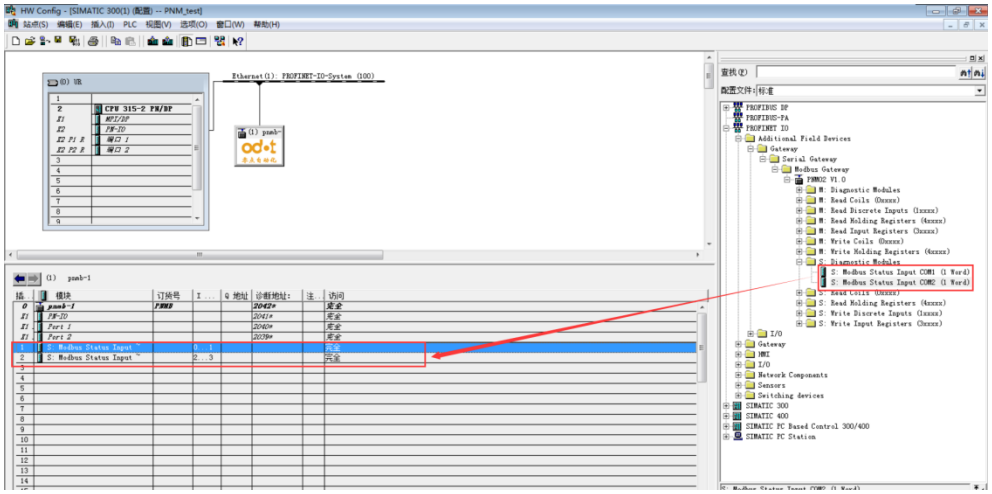
9、选中 ODOT-PNM02 设备图标，在软件下方的模块插槽信息显示部分，选中插槽，双击目录视图中 PNM02 下方模块文件夹下的模块，在插槽中插入模块（注：S 文件夹下的）。



S :诊断模块（Diagnostic Modules）：

S :**Modbus 从站输入状态**：表示当前串口的主站下发的数据包处理情况。

从站输入状态：仅可在最前插槽内插入 2 条命令。在如下的配置中，通过 IW0 和 IW2 的值，结合“Modbus 从站状态代码表”即可判断网关作为 Modbus 从站的当前状态。

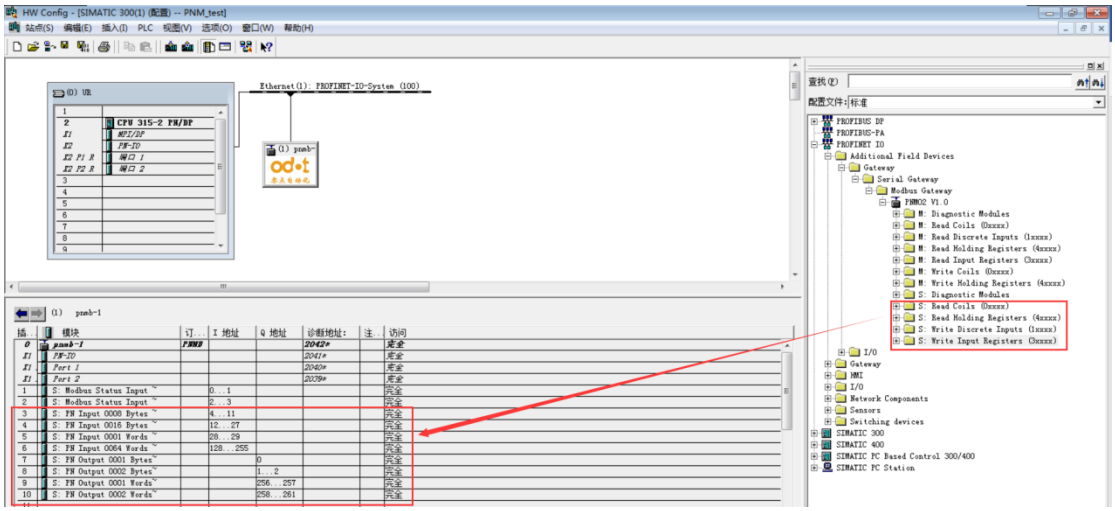


Modbus 从站状态代码表

错误代码	故障说明	故障排除方法
0x00	从站工作正常	无
0x01	非法功能码	从站不支持当前功能码，选择对应的功能码访问
0x02	非法数据地址	从站数据超出其地址范围，修改数据起始地址或数据长度
0x03	非法数据值	数据长度错误，数据长度超出最大允许值 125(Word)或 2000(Bit)，修改长度

0x07	奇偶校验错误	检查奇偶校验、波特率、停止位，检查硬件连接状态
0x09	CRC 校验错误	报文 CRC 计算错误，检查通讯参数等
0x0A	ID 号不匹配	当前接收报文与本设备 ID 不匹配
0x0E	接收报文长度错误	增大接收字符间隔
0x31	帧格式错误	检查通讯参数
0x32	ASCII 长度错误	ASCII 模式数据包长度错误
0x33	ASCII 值错误	数据中包含非 16 进制 ASCII 码

9、网关作为从站，支持 Modbus 功能码 01/02/03/04/15/16。将网关支持的 Modbus RTU/ASCII 地址命令添加到插槽中。



S :读保持寄存器（Read Holding Registers）支持 1~512words 可选

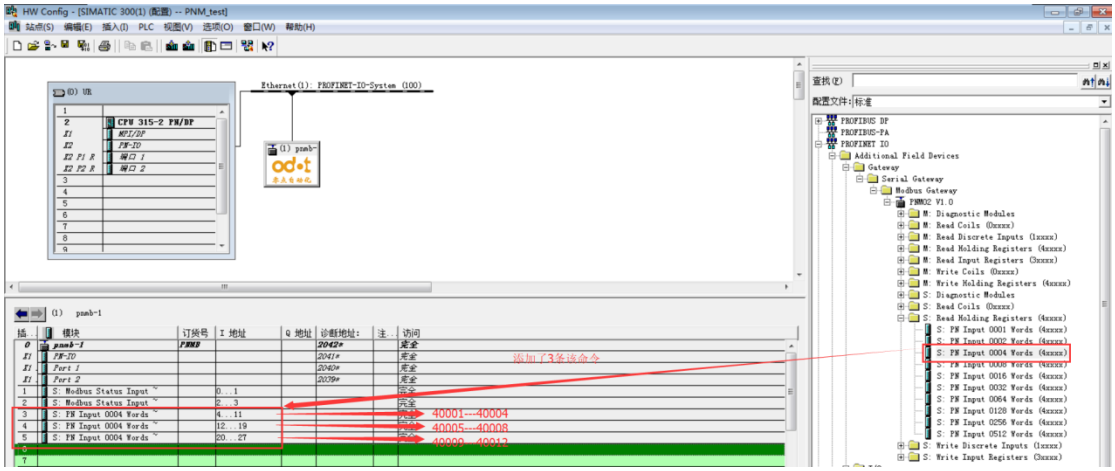
S :读线圈（Read Coils）支持 1~1024Bytes 可选

S :写离散量输入（Write Discrete Inputs）支持 1~1024Bytes 可选

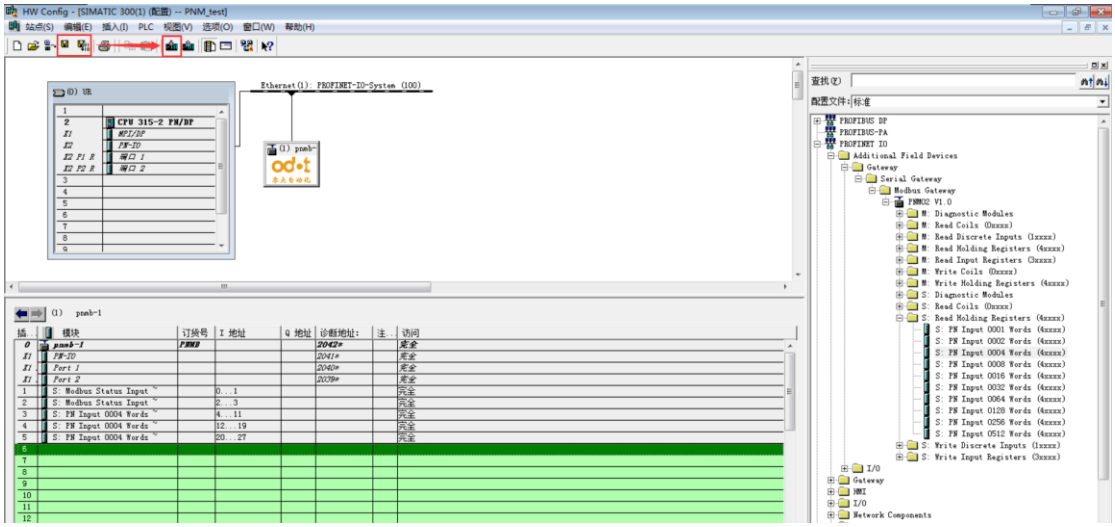
S :写输入寄存器（Write Input Registers）支持 1~125words 可选

10、添加完读写命令，不需要对读写命令进行模块参数设置。每条命令对应的 Modbus 地址范围依据如下规则自动生成：

命令按照所在插槽先后顺序，在同一个 Modbus 数据区的命令对应的 Modbus 地址从 0 开始，自动增加。示例如下：

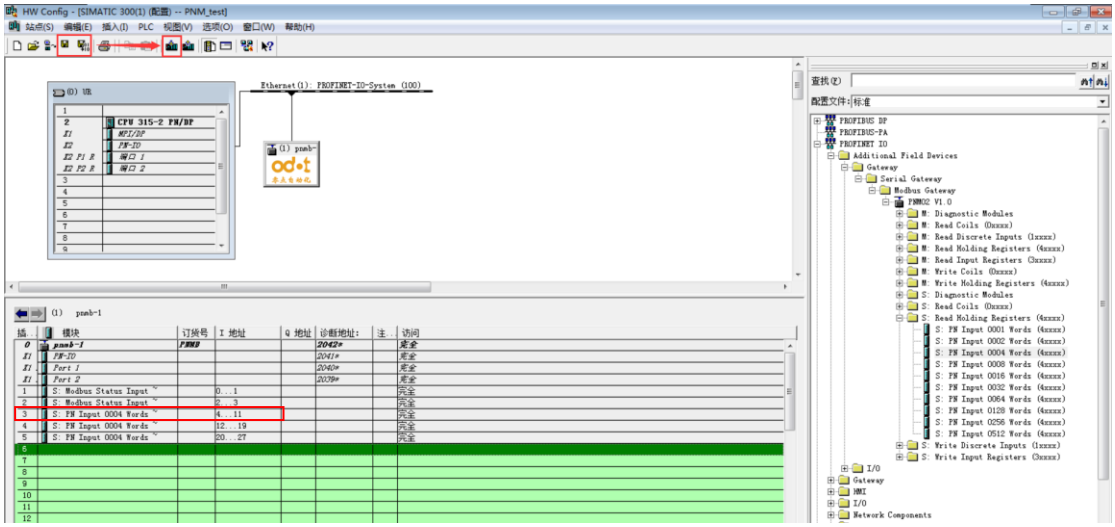


11、此时硬件组态已基本完成，保存编译，下载即可。

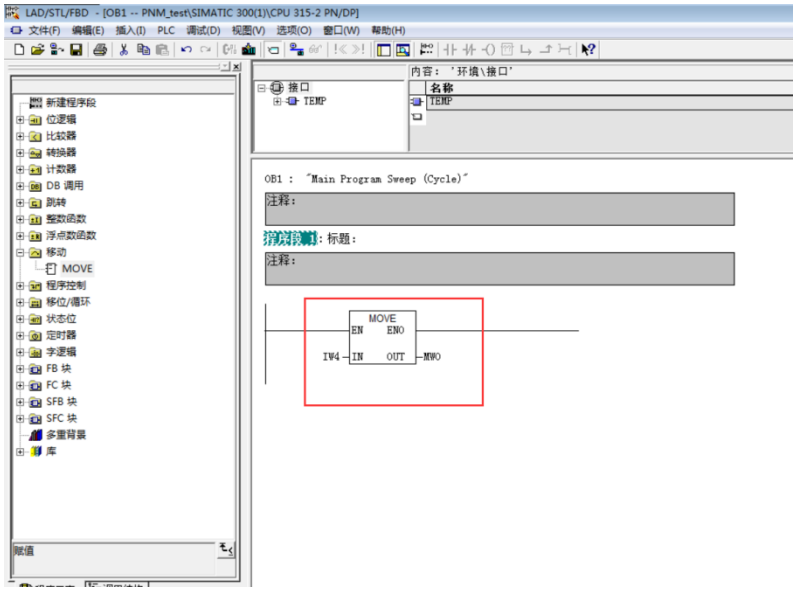


12、数据的监视与使用。

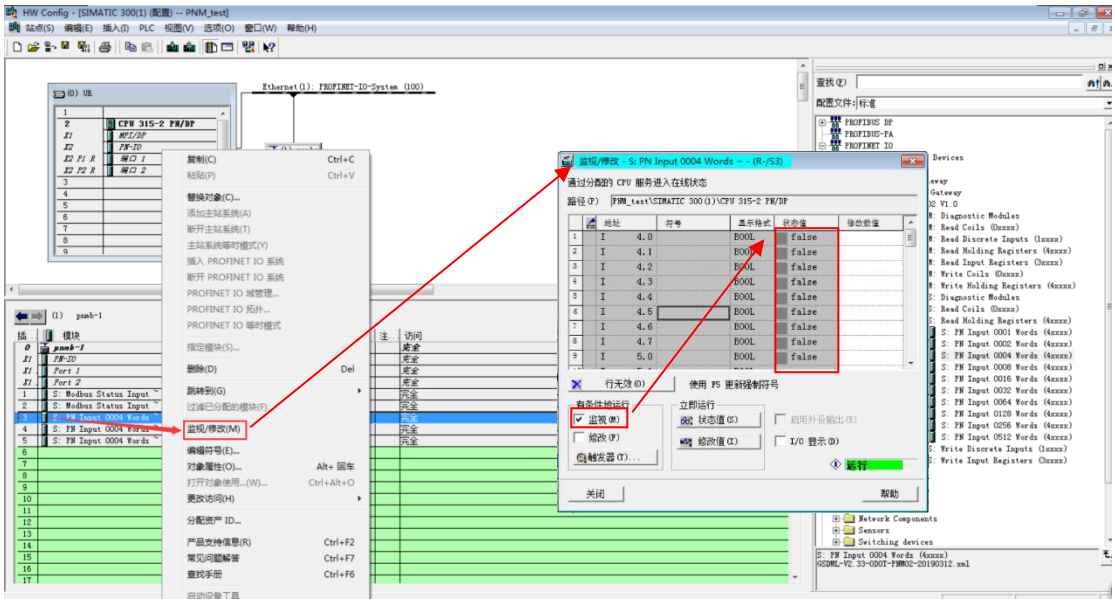
例如当 3 号插槽配置如下时，网关作为 Modbus RTU/ASCII 从站设备 4 区 40001 至 40004 寄存器的数据将被映射至 PLC 的 I 区 IW4 至 IW10。连接与网关 Com 口上的外部 Modbus RTU/ASC||主站发送写 40001 数据的命令，数据将通过网关传入到 PLC 的 IW4 中



上述例程中，在 PLC 程序中进行如下操作即可将 Modbus RTU/ASC||主站写入到 40001 中的数据的赋值到 MW0。



上述例程中，选中 3 号插槽右击，点击“监视/修改”选项，在“监视/修改”页面勾选“监视”，即可实时监视通讯数据，该功能可方便调试（如果是写数据的命令，可通过点击“修改值”按键，即可将数据写入）。

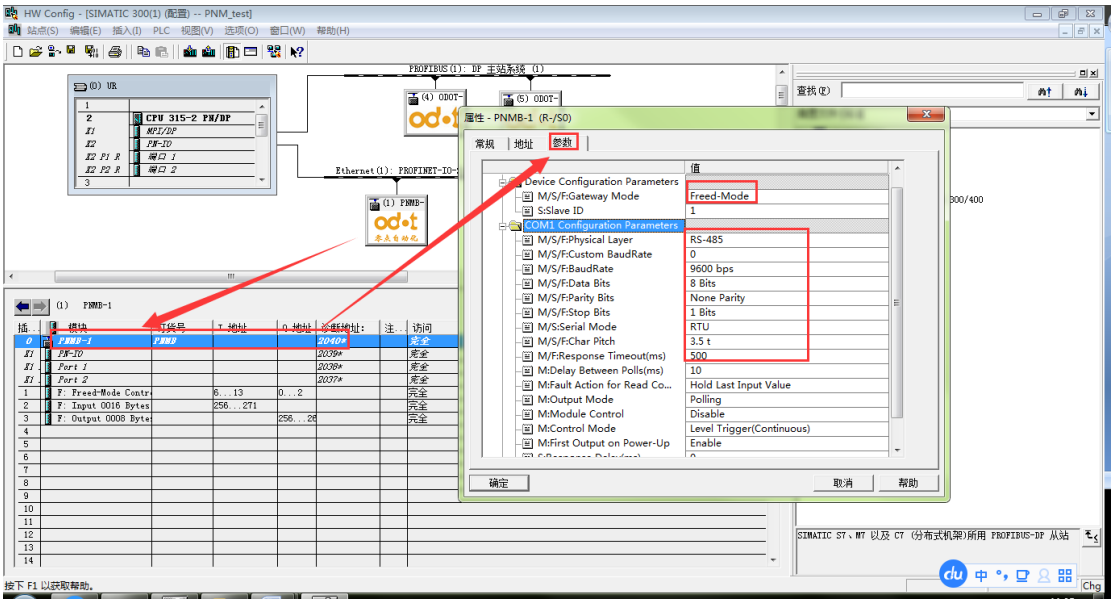


5.3 自由口透传模式的配置

1→7 参照 5.1(主站模式)的 1→7。

注：网关支持该功能的 GSD 文件是 20191008 及其以上版本

8、选中 ODOT-PNM02 设备图标，在软件下方的模块插槽信息显示部分，双击第一个插槽，在弹出的属性窗口中，选中参数选项卡，修改 ODOT-PNM02 模块参数。（设置带 F 前缀的模块参数）



设备配置参数：M/S/F:网关工作模式选择**自由口透传**模式。

串口 1 和串口 2 参数注释：

M/S/F :物理层：RS485/RS232/RS422 可选，**默认 RS485。**

M/S/F :自定义波特率：0,300-500000bps 可设，填 0，表示串口使用标准波特率，非 0，及数值在 300-500000 之间时，串口使用自定义波特率，下面的标准波特率选项无效。**默认 0。**注：少数客户的设备是非标波特率，就可以自定义。

M/S/F :波特率：串口波特率，300-500000bps 可选，**默认 9600bps。**

M/S/F :数据位：7 位、8 位可选，**默认 8 位。**

M/S/F :校验位：无、奇、偶、字符、空格校验可选，**默认无校验。**

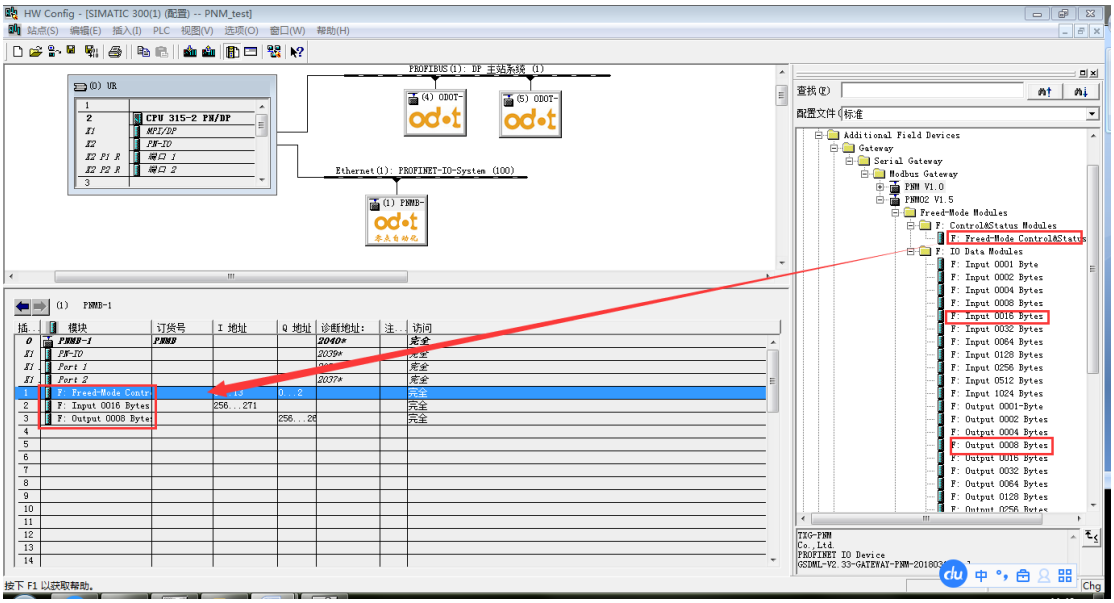
M/S/F :停止位：1 位、2 位，**默认 1 位。**

M/S/F :字符间隔：接收报文时的帧间隔检测时间，1.5t~2000t 可选，**默认 5t。**（t 为单个字符传送的时间，和波特率有关）。

M/F : 响应超时时间(ms)：主站发送命令后，等待从站响应的时间。1~65535

可选，**默认 500**。

11、选中 ODOT-PNM02 设备图标，在软件下方的模块插槽信息显示部分，选中插槽，双击右侧硬件目录视图中 PNM02 下方模块文件夹下的模块，在插槽中插入模块。（选择 F 开头的命令）



自由口透传模式下，分控制和状态模块、输入输出数据模块。

（1）控制和状态模块，需要设置串口号，透传通讯方式。透传通讯方式有主动上报模式和主从应答模式。

（2）输入输出数据模块，只需要设置串口号。

控制和状态模块的过程数据定义：

Profinet数据方向	数据名称	变量名称	数据类型	字节偏移	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	说明
输入数据	输出控制字反馈	Control_Word_Feedback	uint8_t	0	Reseverd		Received Reset	Error Reset	Reseverd			Trigger	
	串口状态	COM_Status	uint8_t	1	Reseverd		Timeout Error	Parity Error	Reseverd		Done	Busy	
	接收错误帧计数	Error_Counter	uint16_t	2									
	接收总数据帧计数	Received_Counter	uint16_t	4									
	当前接收帧字节长度	Received_Data_Len	uint16_t	6									
输出数据	输出控制字	Control_Word	uint8_t	0	Reseverd		Received Reset	Error Reset	Reseverd			Trigger	
	发送帧字节长度	Send_Data_Len	uint16_t	1									

输入数据说明：

1.Control_Word_Feedback 为输出控制字 Control_Word 的反馈值，输出控制字刷新到 PN 从站后，将更新到控制字反馈中。

2.主从应答模式下，串口发送数据时，Busy 位被置 1，Done 位被清零。

当在超时时间内串口接收到应答后，Busy 位清零，Done 完成位置 1，Received_Counter 计数值加 1，若接收帧有奇偶校验错误，则 Parity_Error 位被置 1，同时 Error_Counter 计数加 1。

当在超时时间内串口未接收到应答，Busy 位清零，Done 完成位置 1，同时设置 Timeout_Error 为 1，Error_Counter 错误计数值加 1。

3.在主动上报模式下，从站收到数据包时，Received_Counter 计数值加 1，若接收帧有奇偶校验错误，则 Parity_Error 位被置 1，同时 Error_Counter 计数加 1。

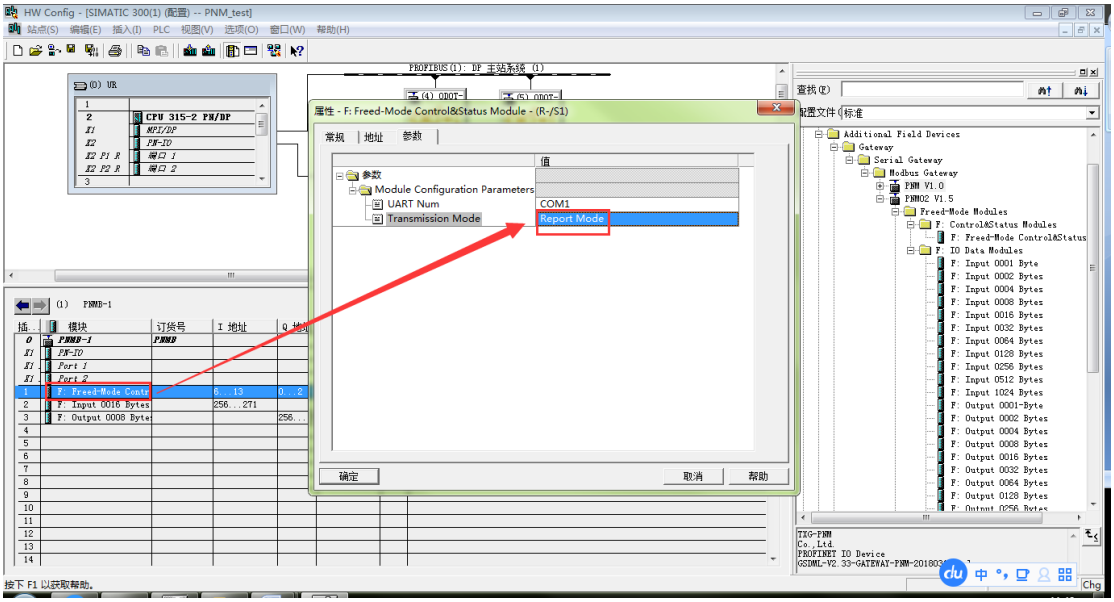
输出数据说明：

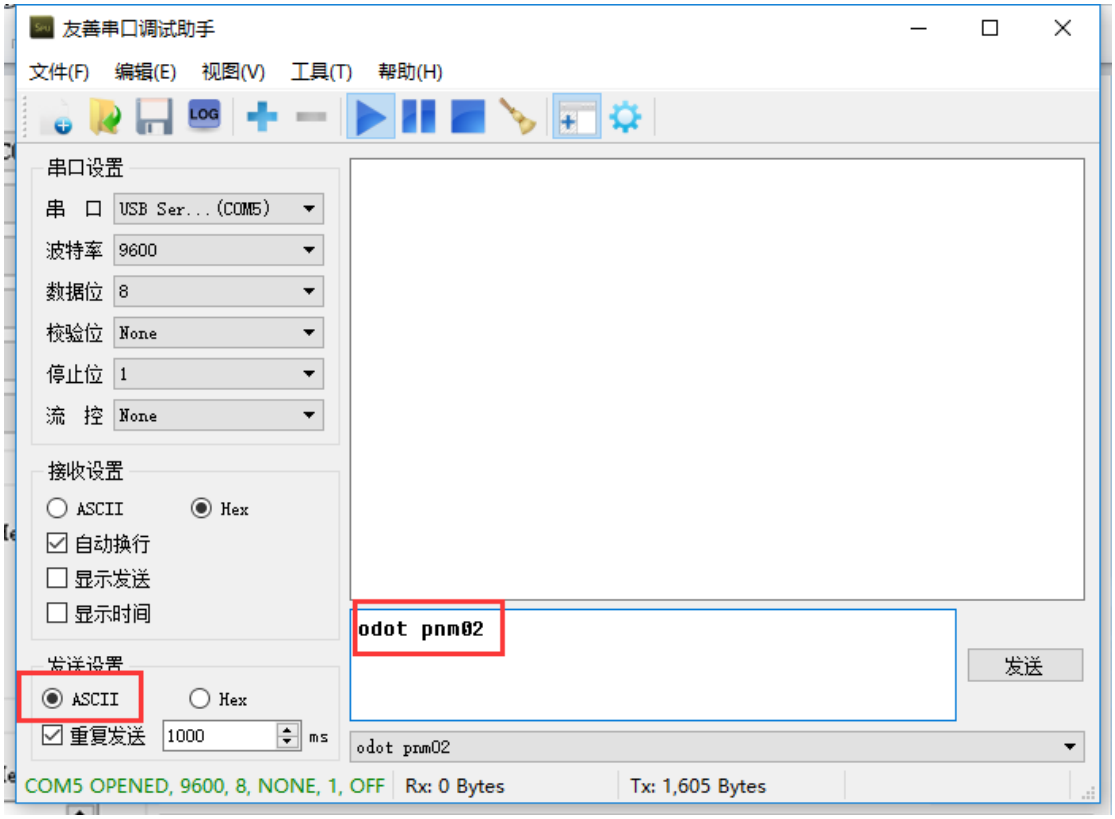
1.Received_Reset 上升沿时，接收计数值 Received_Counter 被清零，Error_Reset 上升延时，错误计数值 Error_Counter 被清零。

2.主动上报模式下，Trigger 位无效，Send_Data_Len 无效。

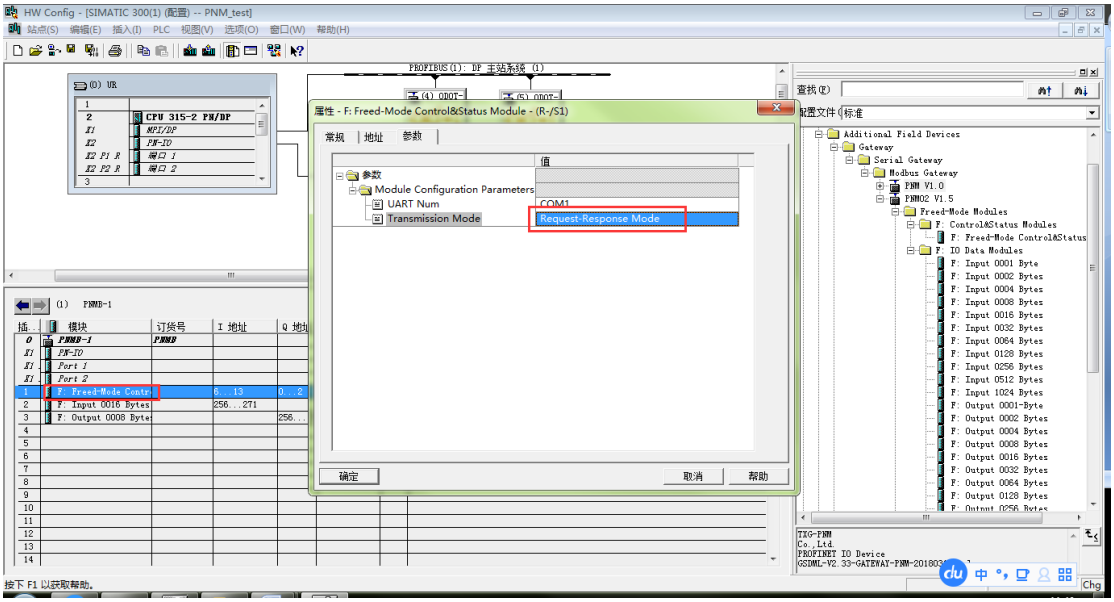
2.主从应答模式下，Trigger 上升延时触发一次串口数据发送，串口将按 Send_Data_Len 的数据长度发送数据包并等待应答处理。

（1）将网关设置为**主动上报**模式，网关串口 1 接调试串口工具模拟现场设备（比如扫码枪、称重仪表等）。可在控制和状态模块、输入输出数据模块监控到相应的值的变化。





（2）将网关设置为**主从应答**模式。当控制字 Trigger 为 0 无效时，网关保持主动上报形式，接收串口侧的数据。



当控制字 Trigger 为 0-1 脉冲激活时，网关发送数据到串口。注：Trigger 位激活一次，网关发送一次数据。

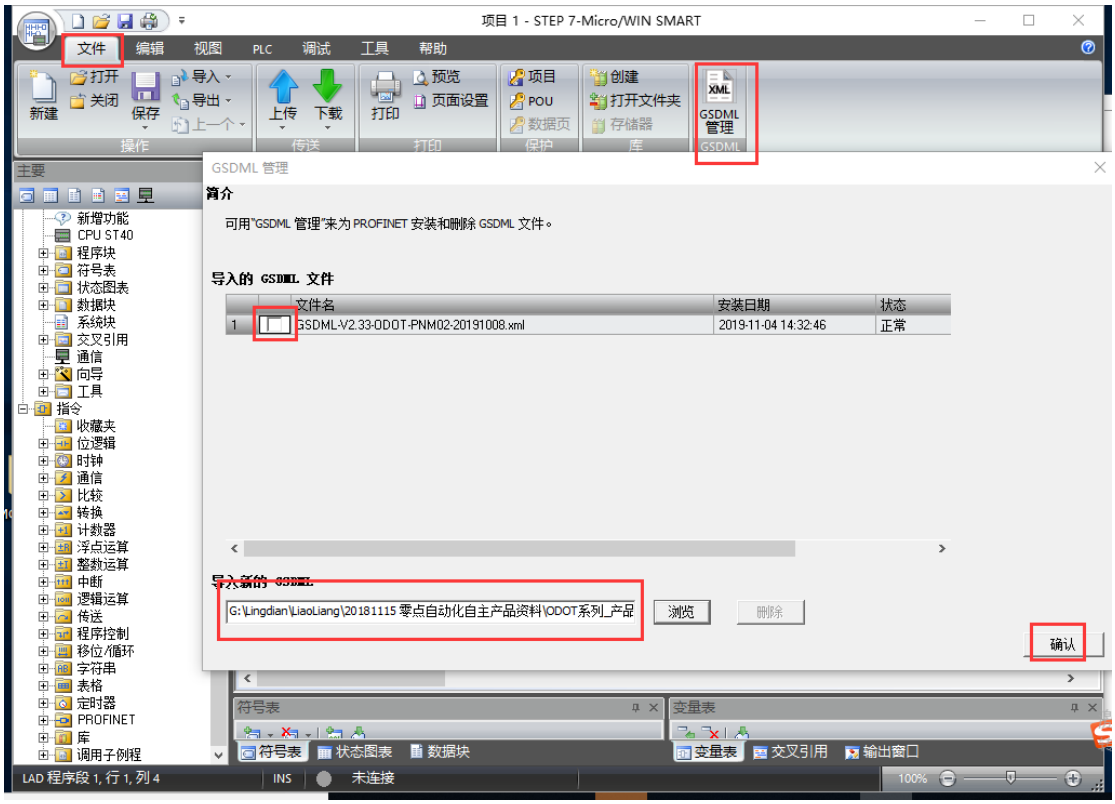
通过一系列的设置调试，PLC 通过网关将串口侧数据采集上来后存储在 PLC 地址区，工程人员自己解析上传报文数据格式，提取有效的数据进行编程处理。项目完成后，保存、编译，下载程序。

六、在西门子 STEP 7-MicroWIN SMART 中使用本模块

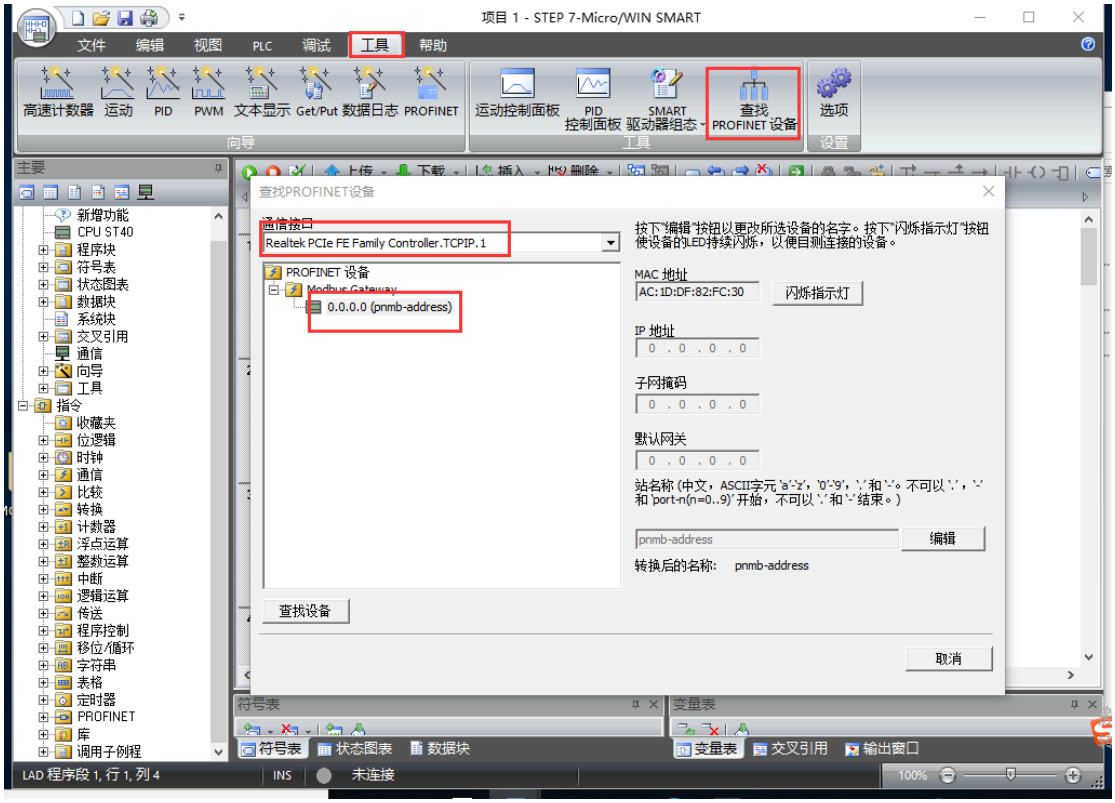
注：S7-200SMART CPU 固件版本在 V2.4 版本及以上才支持 PROFINET 通讯，STEP 7-MicroWIN SMART 编程软件版本在 V2.4 版本及以上才支持 PROFINET 通讯。若 CPU 或者编程软件版本低于 V2.4，又想要做 PROFINET 通讯，请在西门子网站升级 CPU 固件版本及下载高版本的编程软件。

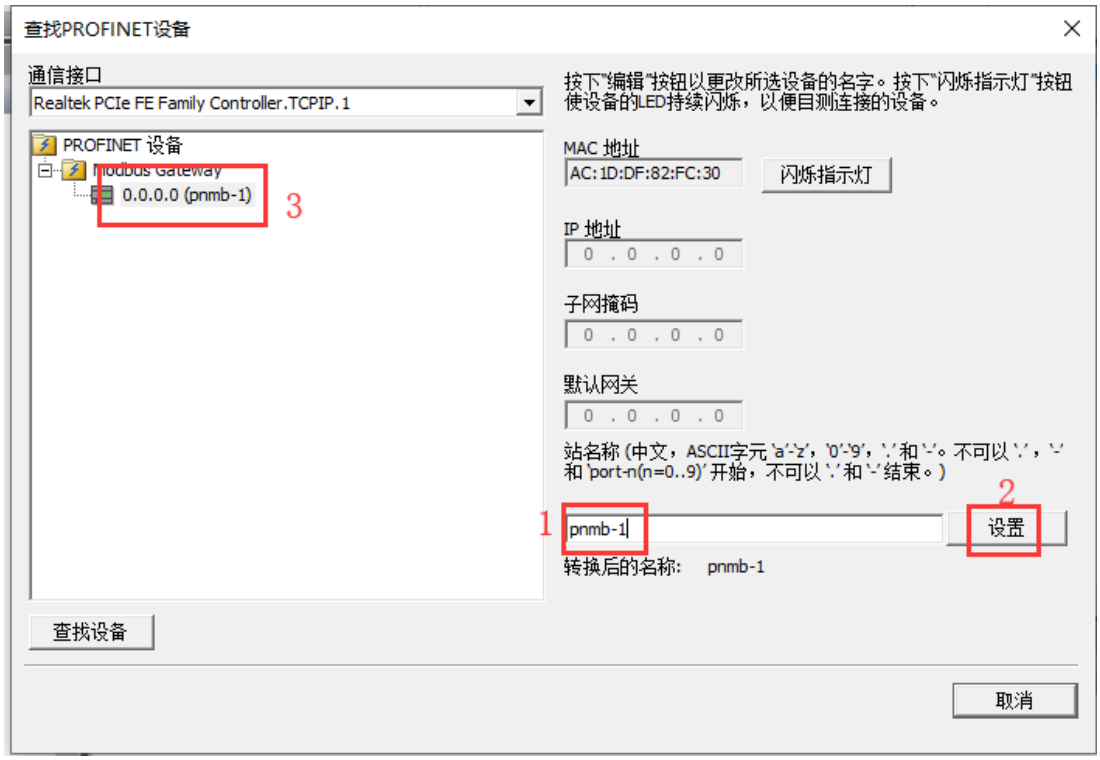
6.1 MODBUS 主站模式的配置

1、打开 STEP 7-MicroWIN SMART 软件，点击文件点击 GSDML 管理，在弹出的界面，找到 ODOT-PNM02 的 GSD 文件所在目录，点击确认。



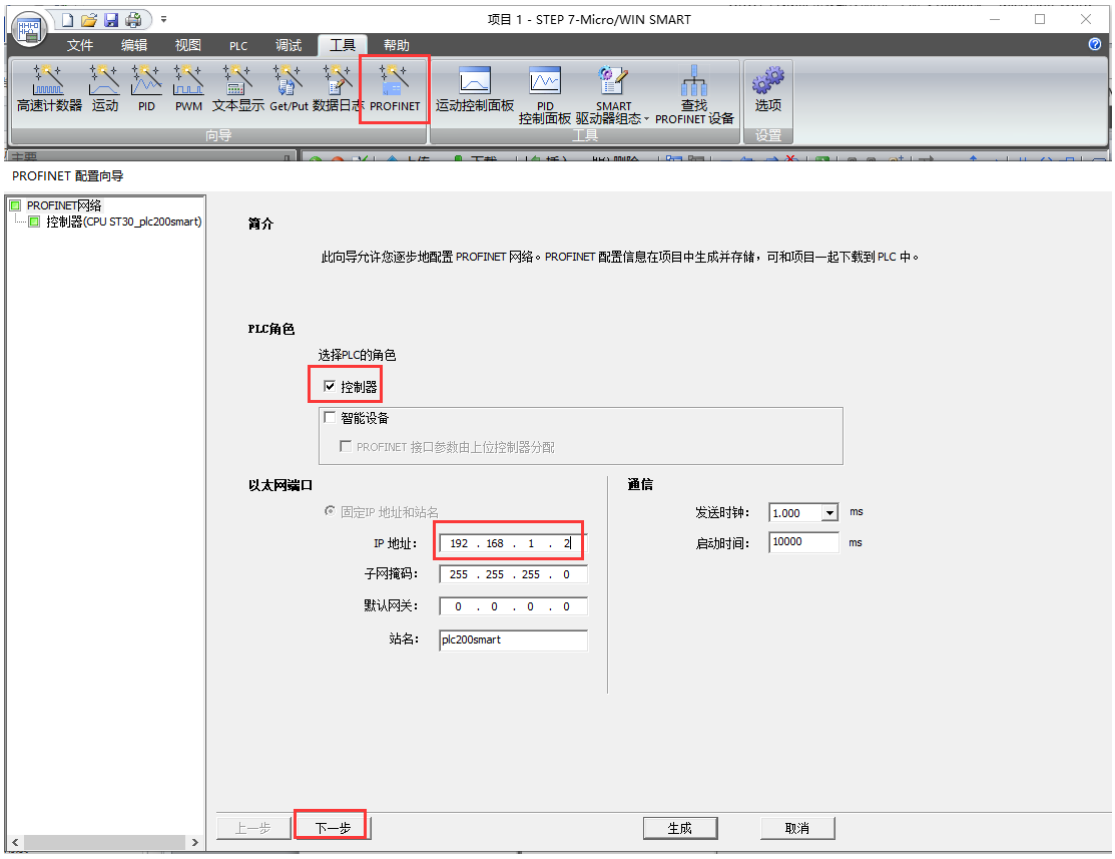
2、点击查找 PROFINET 设备，选择本机网卡，会自动扫描到所有的 PROFINET 设备，可查看网关的 IP 地址和设备名称。点击编辑，设置网关设备名称。





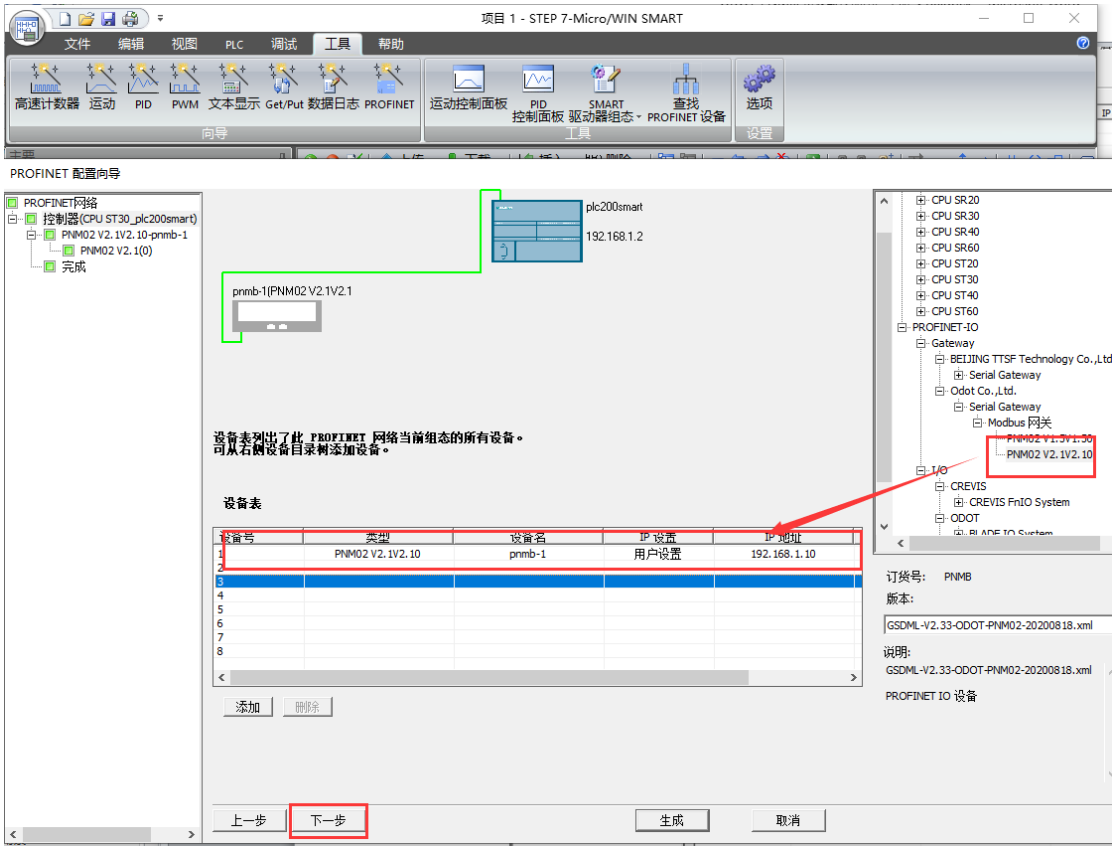
3、点击工具，点击 PROFINET，在弹出的 PROFINET 配置向导界面，选

择 PLC 角色为：控制器，设置 PLC 的 IP 地址，点击下一步。

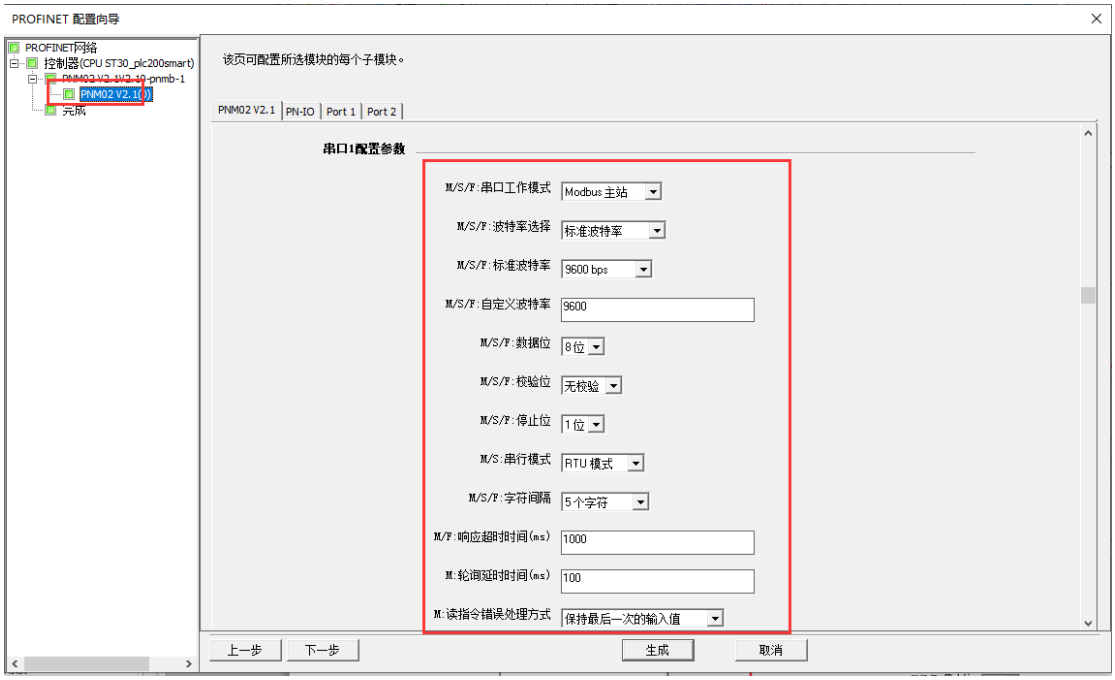


4、在弹出的界面，在右侧目录栏选中 PNM02，在左下角点击添加按钮，可将网关加入 PLC 的 PROFINET 总线。可修改网关的 IP 地址及设备名称。

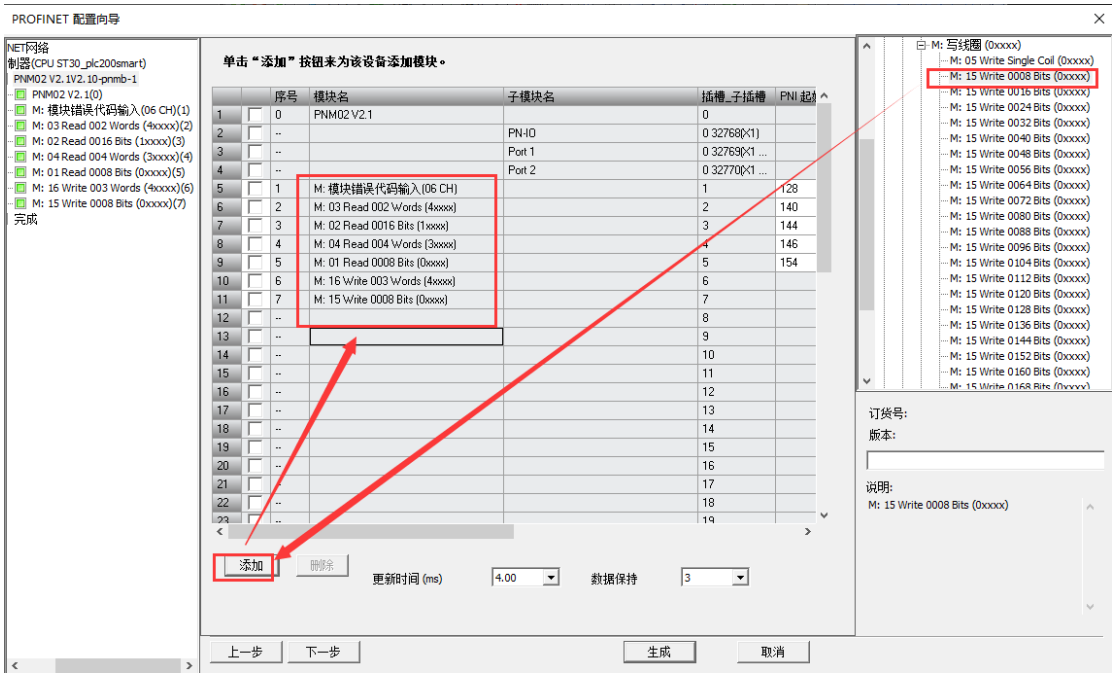
注：设备名称必须和前面扫描到或修改后的设备名称保持一致。



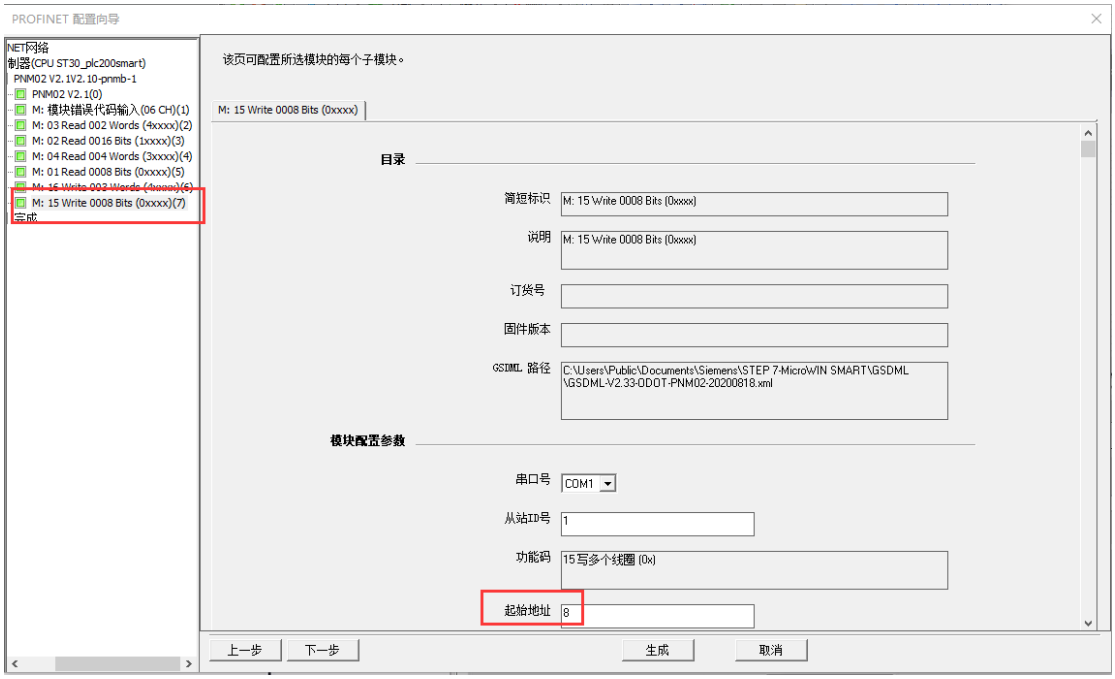
5、选中 PNM02，可修改网关工作模式和串口参数，此文档采用默认参数**主站模式**进行测试。



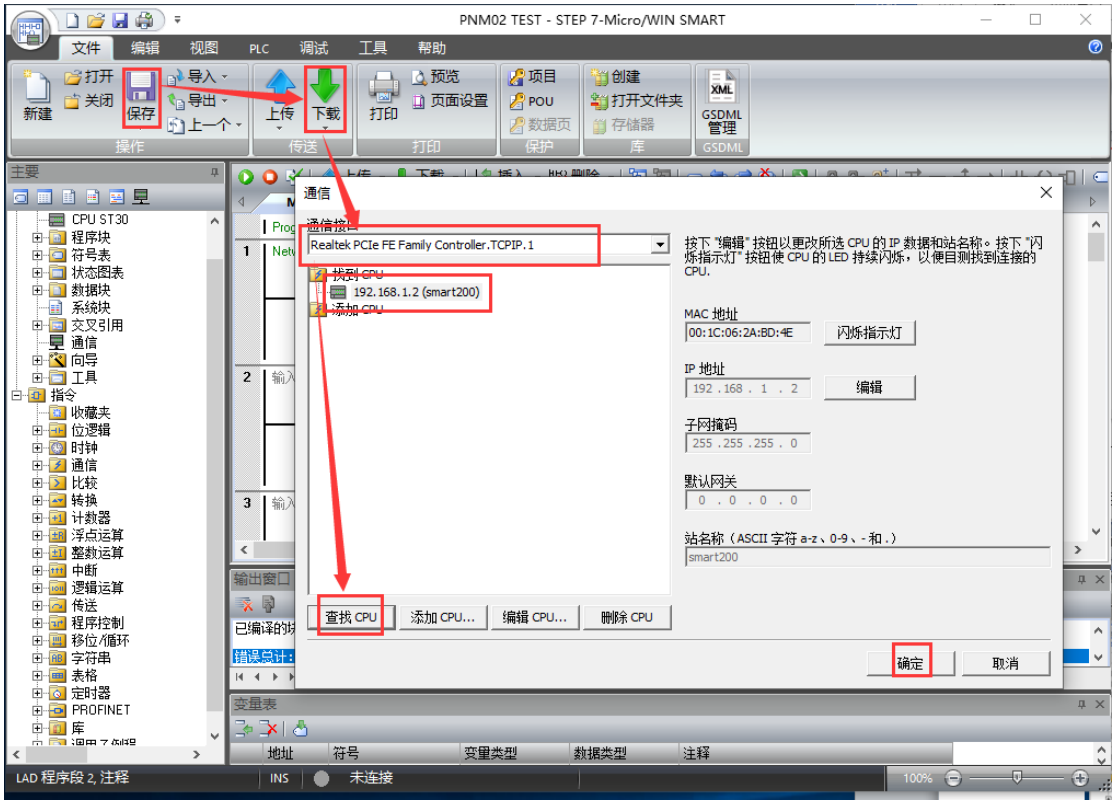
6、选中 PNM02 V2.12.10-pnmb-1,将右侧的主站模式下读写命令添加到插槽内。选中模块错误代码输入（06CH）点击添加。



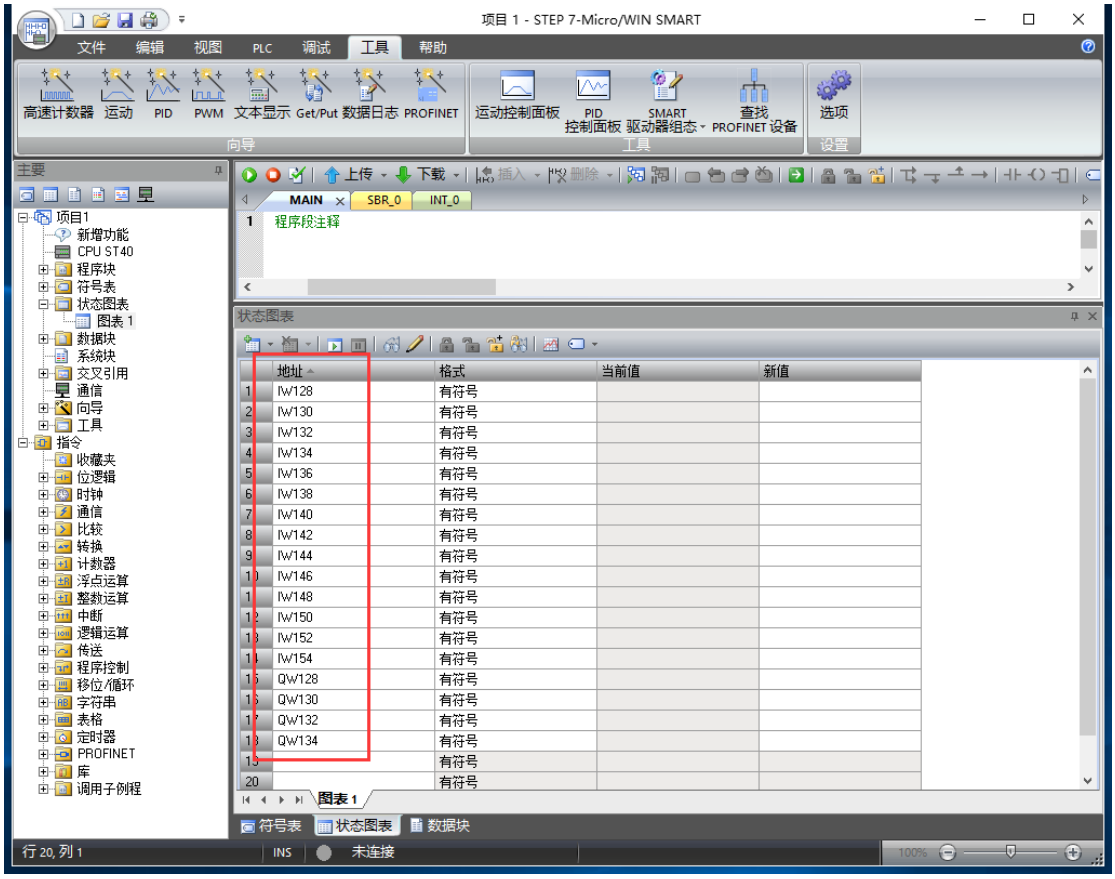
7、每条读或写命令，均可以修改串口号、从站 ID、起始地址参数。前四条命令采用默认值，选中第 5 条和第 6 条的写命令，起始地址分别改成 2 和 8。点击**生成**，完成对网关 PNM02 主站模式的配置。



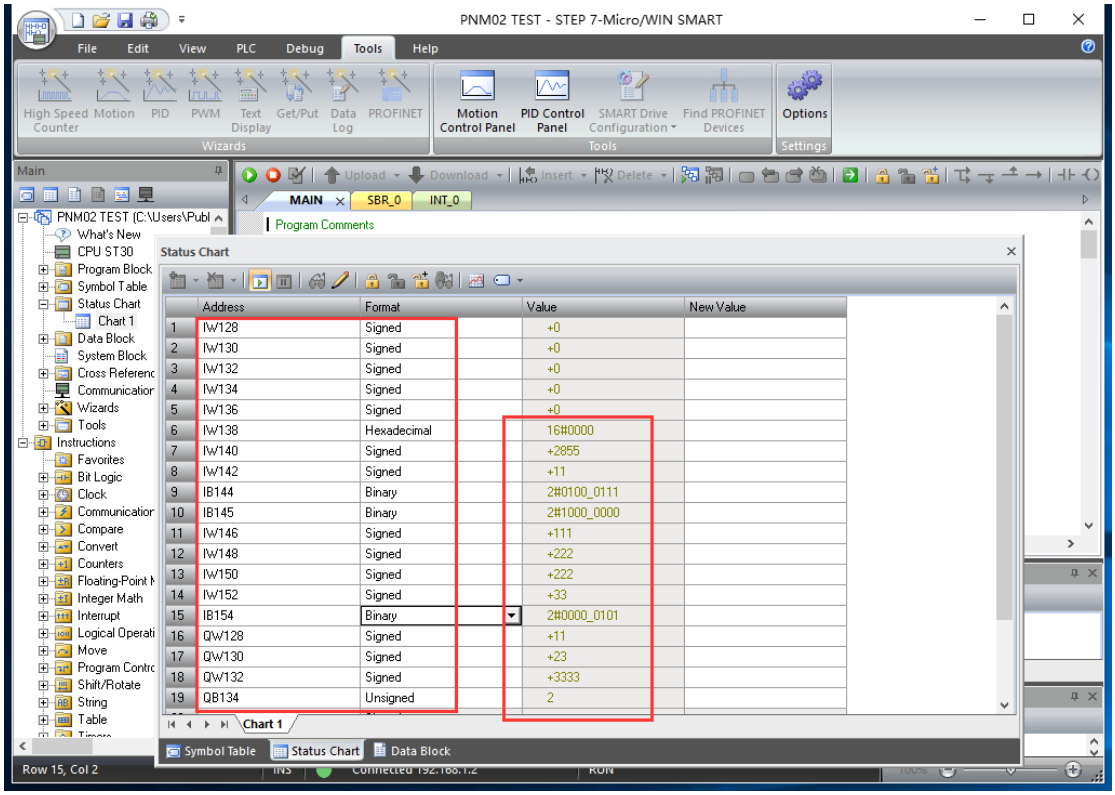
8、保存，编译，下载。

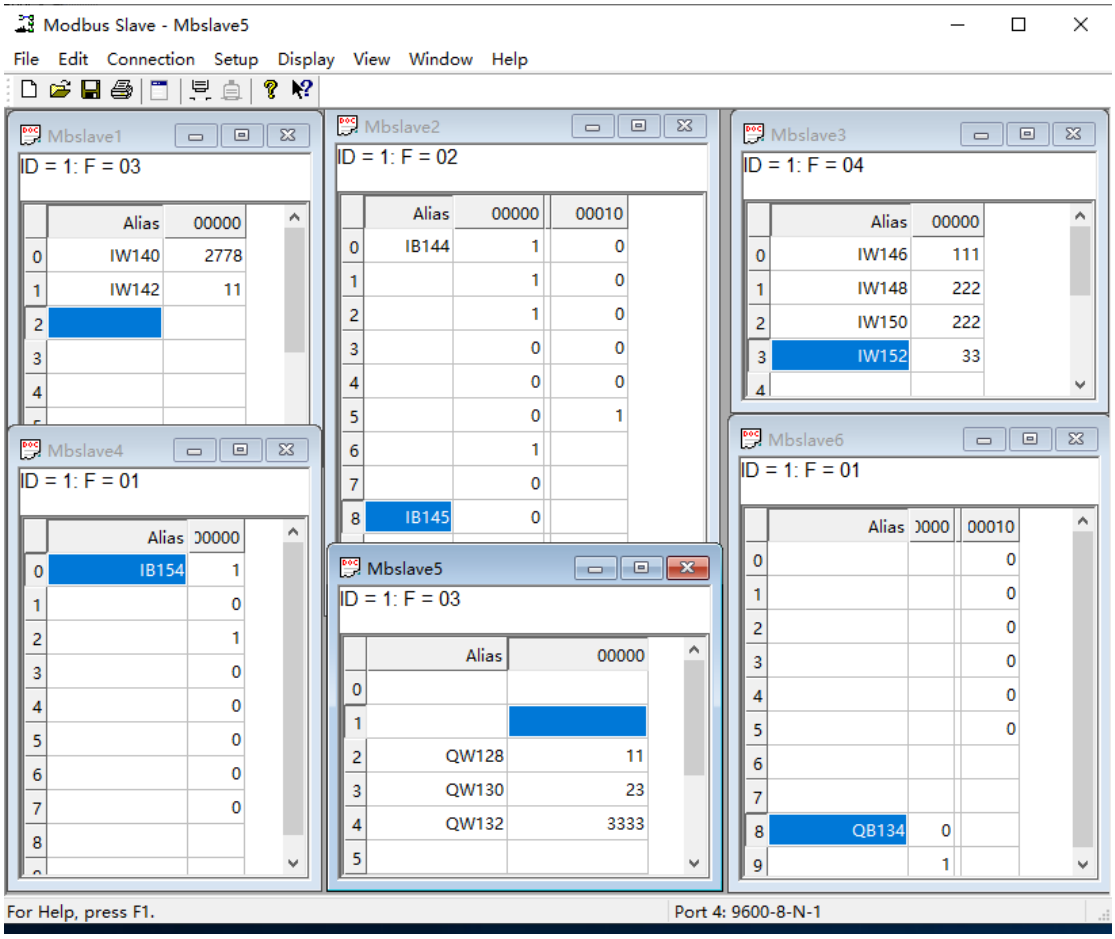


9、当程序运行时，可以使用状态图表来读、写监视和强制其中的变量。



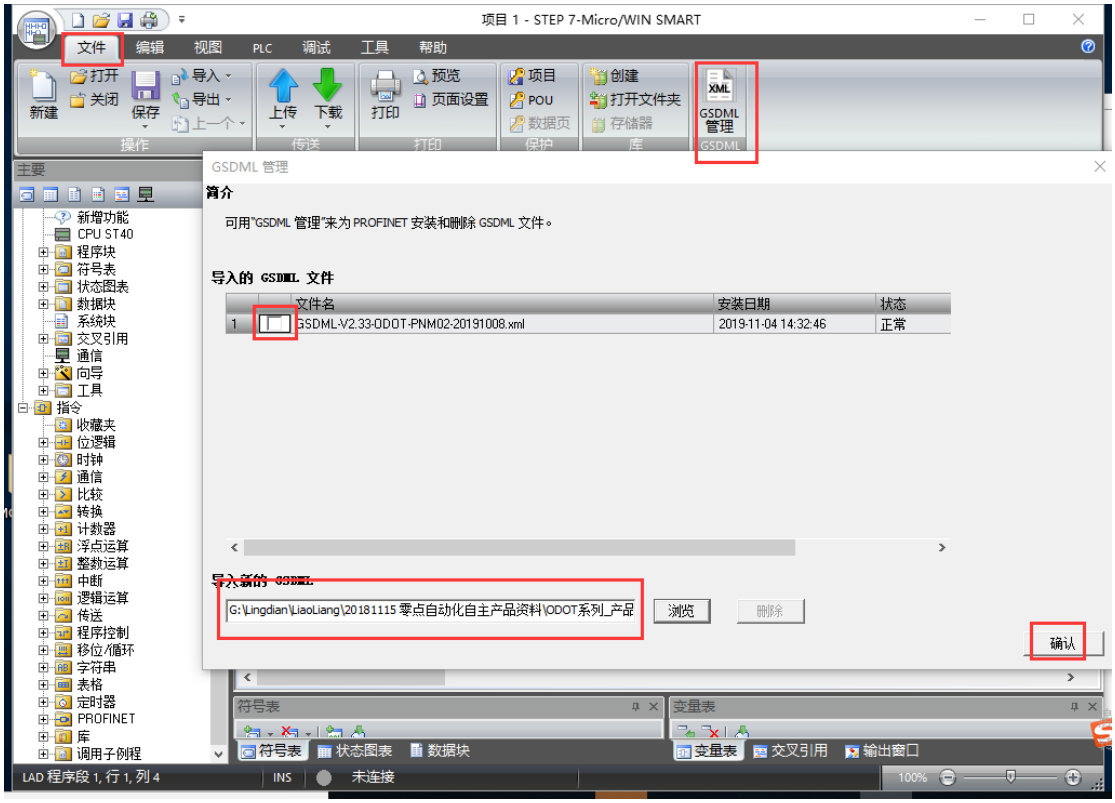
10、用 Modbus Slave 模拟现场底层 RS485 设备。STEP 7-Micro/WIN SMART 软件点击在线运行，点击状态图标监控按钮，可监控到 RS485 侧的数据。



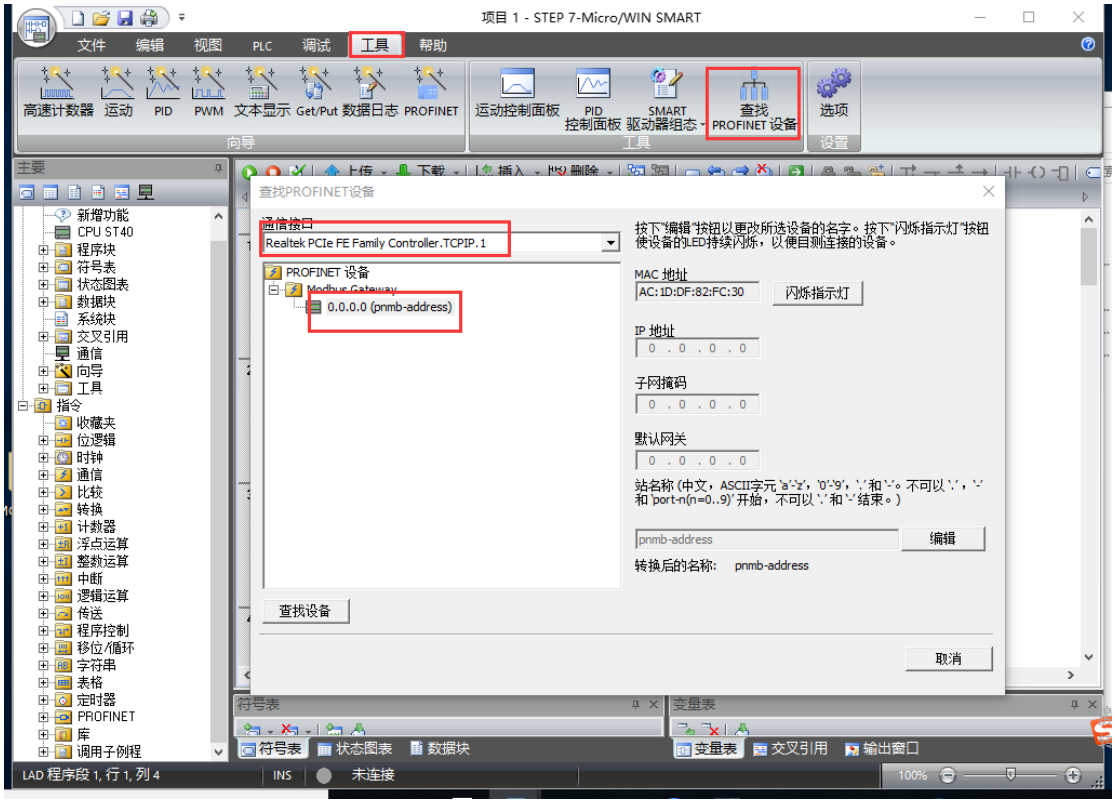

Modbus Slave - Mbslave5
File Edit Connection Setup Display View Window Help
Mbslave1
ID = 1: F = 03
Alias 00000
0 IW140 2778
1 IW142 11
Mbslave2
ID = 1: F = 02
Alias 00000 00010
0 IB144 1 0
1 1 0
2 1 0
3 0 0
4 0 0
5 0 1
6 1
7 0
8 IB145 0
Mbslave3
ID = 1: F = 04
Alias 00000
0 IW146 111
1 IW148 222
2 IW150 222
3 IW152 33
Mbslave4
ID = 1: F = 01
Alias 00000
0 IB154 1
1 0
2 1
3 0
4 0
5 0
6 0
7 0
Mbslave5
ID = 1: F = 03
Alias 00000
2 QW128 11
3 QW130 23
4 QW132 3333
Mbslave6
ID = 1: F = 01
Alias 00010
8 QB134 0
9 1
For Help, press F1.
Port 4: 9600-8-N-1

6.2 MODBUS 从站模式的配置

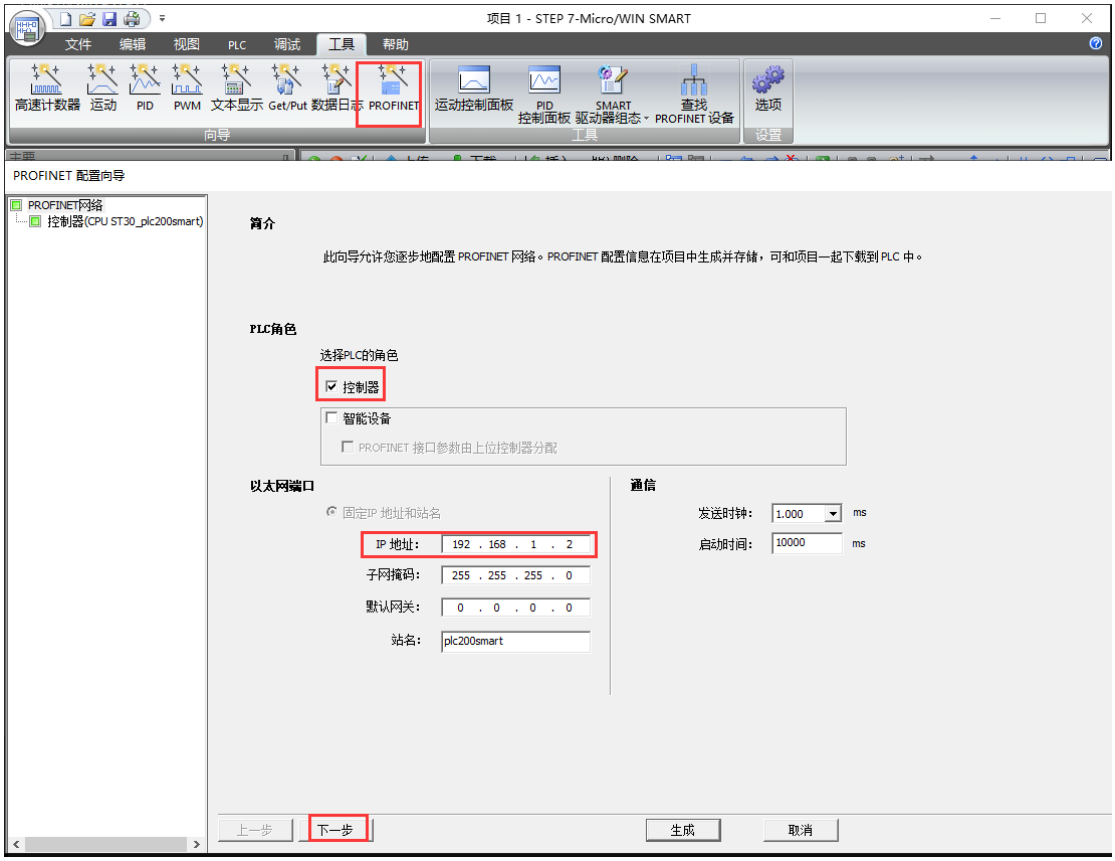
1、打开 STEP 7-MicroWIN SMART 软件，点击文件点击 GSDML 管理，在弹出的界面，找到 ODOT-PNM02 的 GSD 文件所在目录，点击确认。



2、点击查找 PROFINET 设备，选择本机网卡，会自动扫描到所有的 PROFINET 设备，可查看网关的 IP 地址和设备名称。点击编辑，设置网关设备名称。

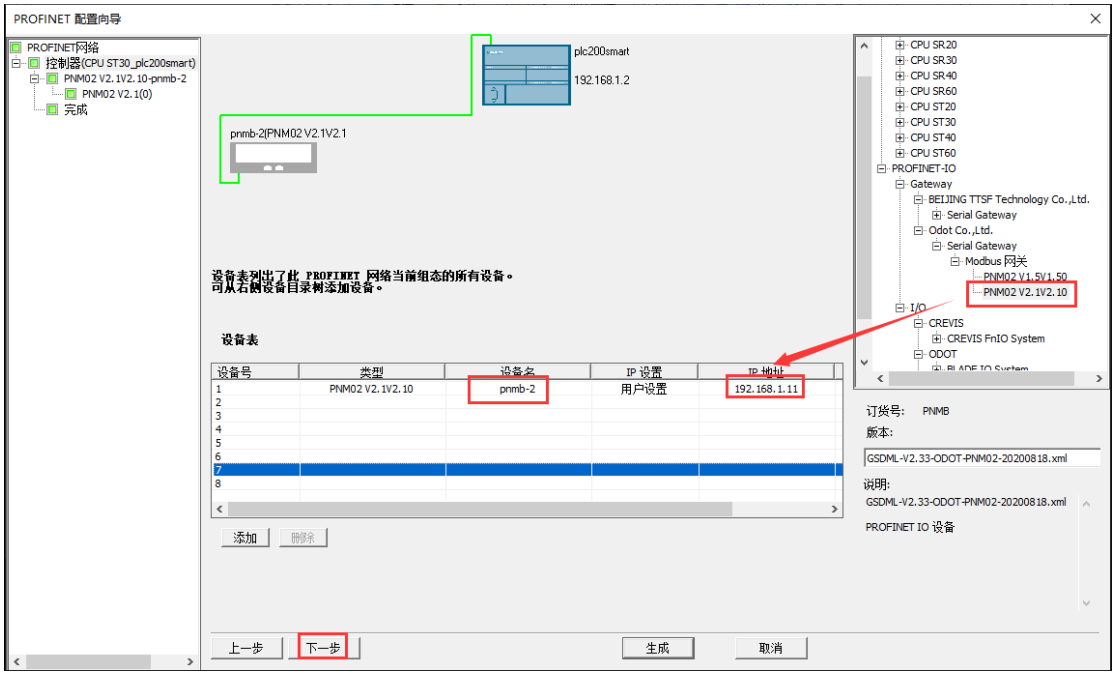


3、点击工具，点击 PROFINET，在弹出的 PROFINET 配置向导界面，选择 PLC 角色为：PROFINET 控制器，点击下一步。

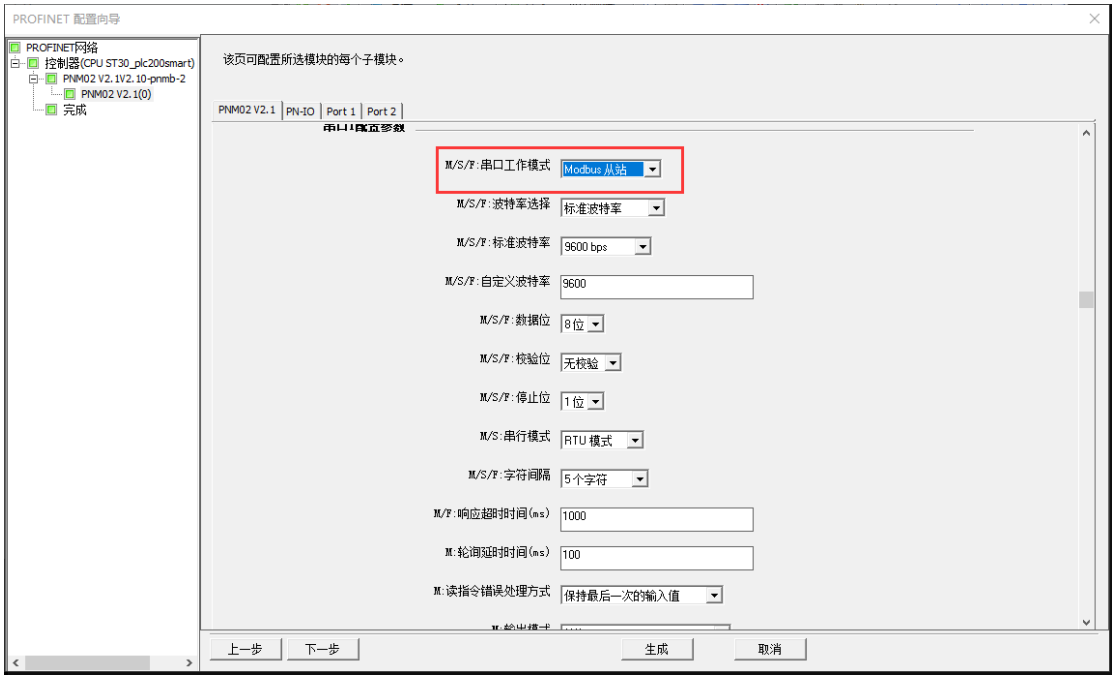


4、在弹出的界面，可修改 200 Smart 的 IP 地址。在右侧目录栏选中 PNM02，

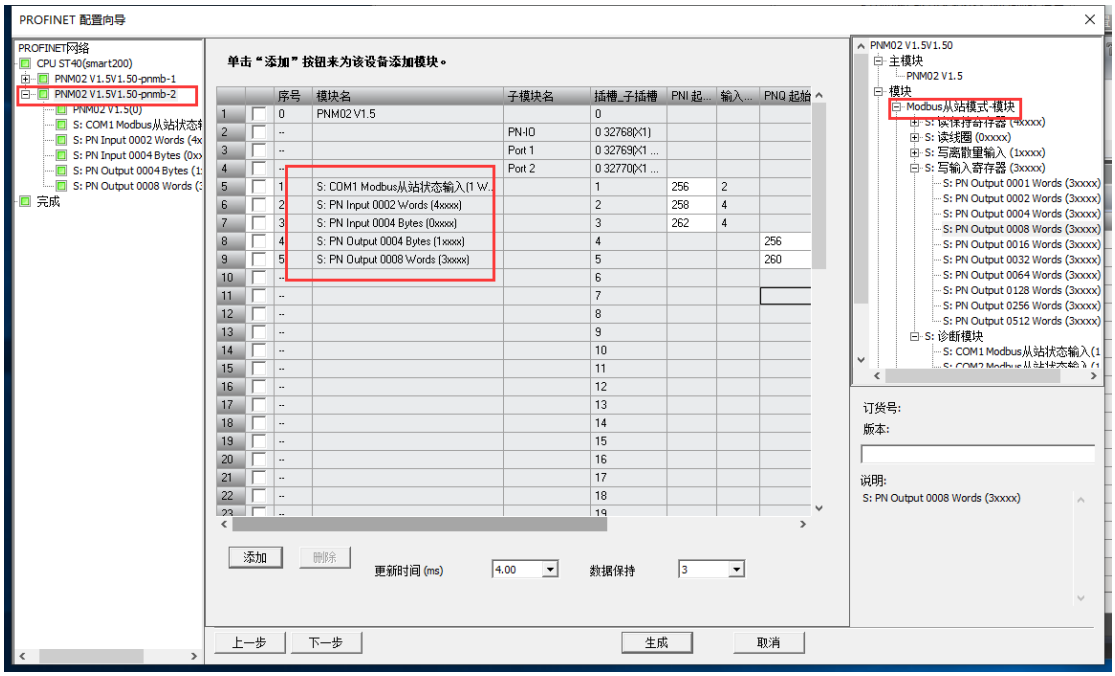
在左下角点击添加按钮，可将网关加入 PLC 的 PROFINET 总线。设置之前的设备名称 pnmb-2，分配网关的 IP 地址 192.168.1.11.



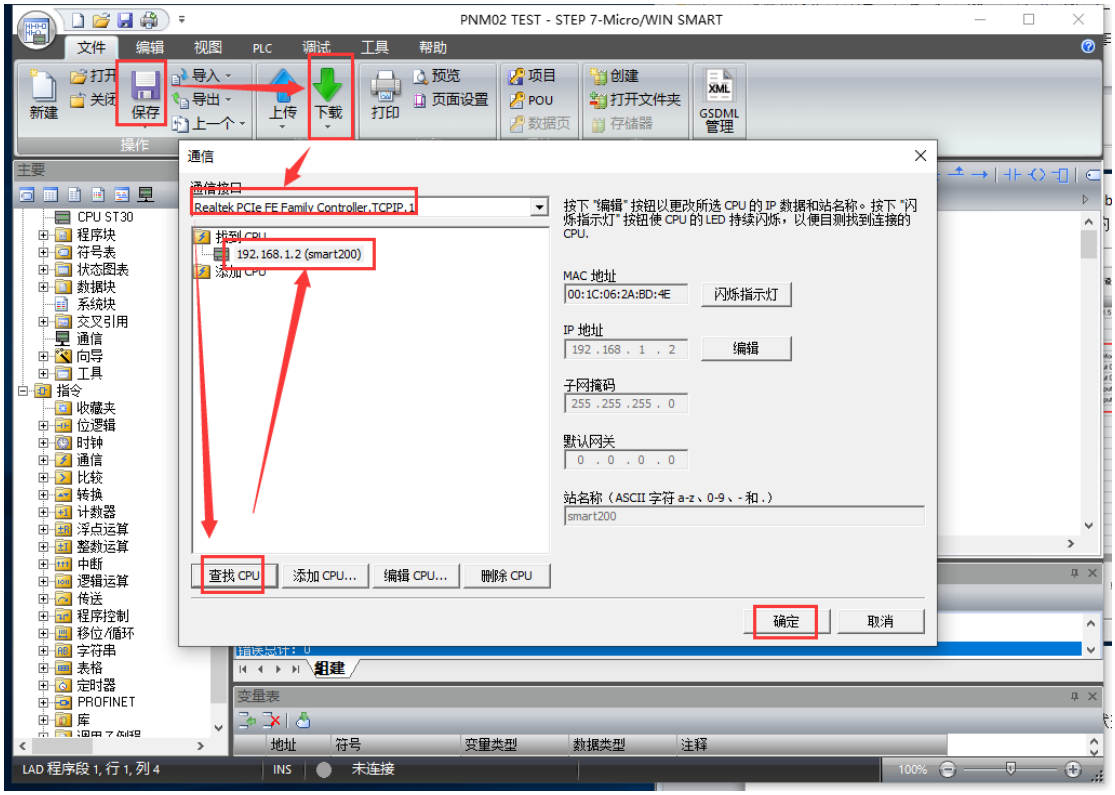
5、选中 PNM02，可修改网关工作模式和串口参数， 工作模式选择 Modbus 从站，站地址是 ID=6。



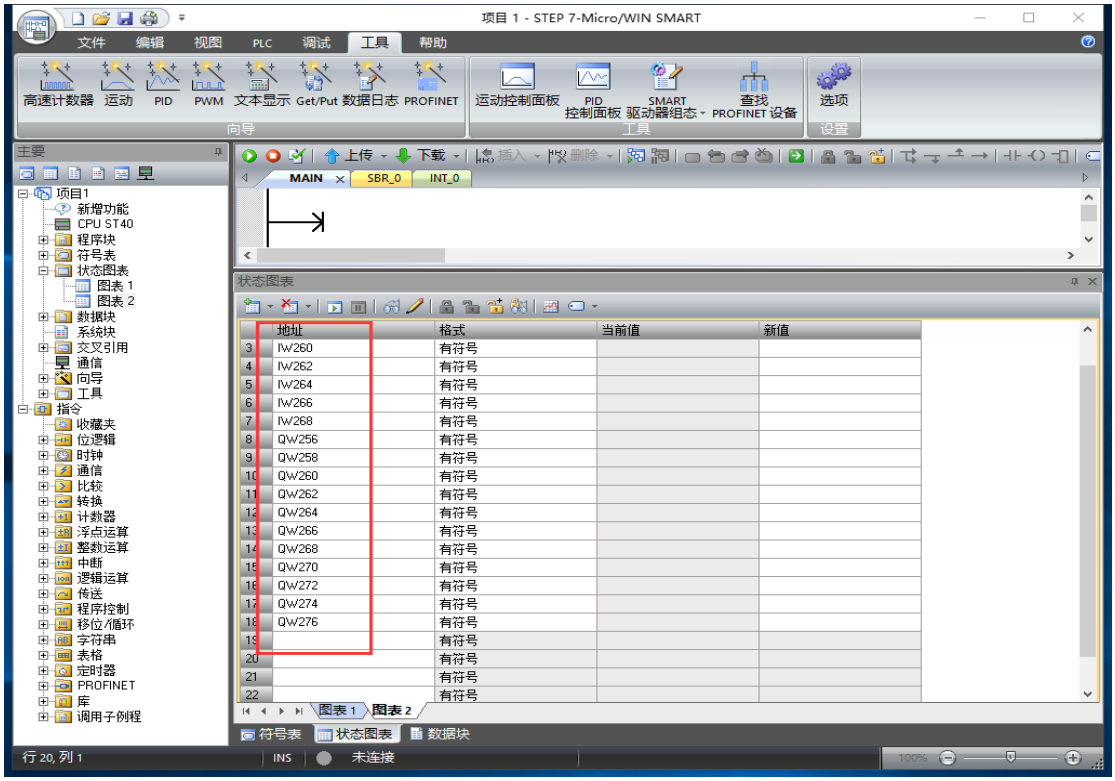
6、选中 PNM02-pnmb-2,将右侧的从站模式下读写命令添加到插槽内。点击**生成**，完成对网关 PNM02 从站模式的配置。



7、保存，编译，下载。



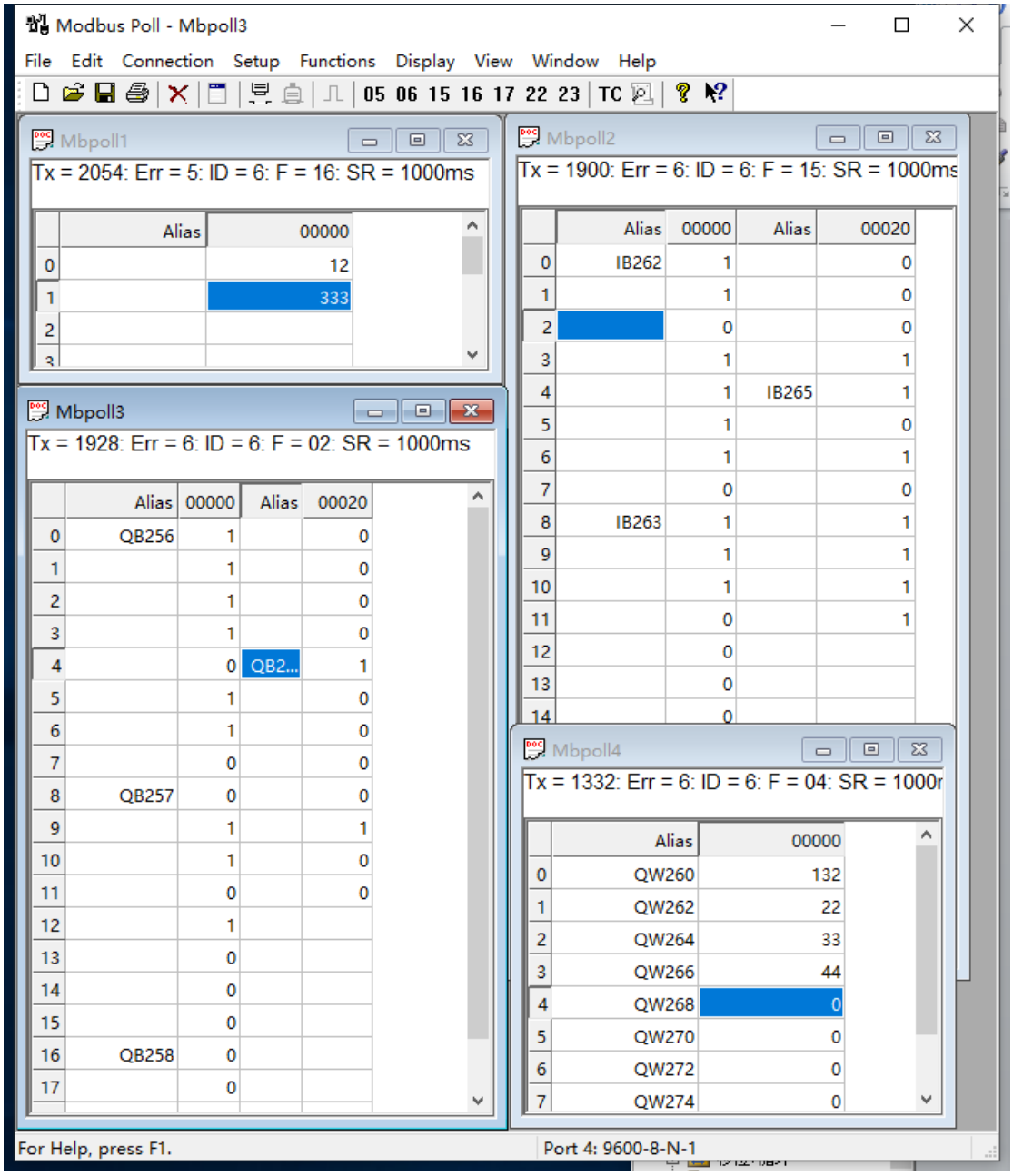
8、当程序运行时，可以使用状态图表来读、写监视和强制其中的变量。



9、用 Modbus Poll 模拟现场底层 RS485 主站设备。STEP 7-Micro/WIN SMART 软件点击在线运行，点击状态图标监控按钮，可监控到 RS485 侧的数据。

状态图表

	地址	格式	当前值	新值
1	IW256	有符号	+0	
2	IW258	有符号	+12	
3	IW260	有符号	+333	
4	IB262	二进制	2#0111_1011	
5	IB263	二进制	2#0000_0111	
6	IB264	二进制	2#1000_0000	
7	IB265	二进制	2#1111_0101	
8	QB256	二进制	2#0110_1111	
9	QB257	二进制	2#0001_0110	
10	QB258	二进制	2#0000_0000	
11	QB259	二进制	2#0010_0001	
12	QW260	有符号	+132	
13	QW262	有符号	+22	
14	QW264	有符号	+33	
15	QW266	有符号	+44	
16	QW268	有符号	+0	
17	QW270	有符号	+0	
18	QW272	有符号	+0	
19	QW274	有符号	+0	
20		有符号		
21		有符号		
22		有符号		
23		有符号		


Modbus Poll - Mbpoll3
File Edit Connection Setup Functions Display View Window Help
05 06 15 16 17 22 23 TC
Mbpoll1
Tx = 2054: Err = 5: ID = 6: F = 16: SR = 1000ms
Alias 00000
0 12
1 333
Mbpoll2
Tx = 1900: Err = 6: ID = 6: F = 15: SR = 1000ms
Alias 00000 Alias 00020
0 IB262 1 0
1 1 0
2 0 0
3 1 1
4 1 IB265 1
5 1 0
6 1 1
7 0 0
8 IB263 1 1
9 1 1
10 1 1
11 0 1
12 0
13 0
14 0
Mbpoll3
Tx = 1928: Err = 6: ID = 6: F = 02: SR = 1000ms
Alias 00000 Alias 00020
0 QB256 1 0
1 1 0
2 1 0
3 1 0
4 0 QB2... 1
5 1 0
6 1 0
7 0 0
8 QB257 0 0
9 1 1
10 1 0
11 0 0
12 1
13 0
14 0
15 0
16 QB258 0
17 0
Mbpoll4
Tx = 1332: Err = 6: ID = 6: F = 04: SR = 1000r
Alias 00000
0 QW260 132
1 QW262 22
2 QW264 33
3 QW266 44
4 QW268 0
5 QW270 0
6 QW272 0
7 QW274 0
For Help, press F1.
Port 4: 9600-8-N-1

6.3 MODBUS 自由口透传模式的配置

6.3.1 自由口透传模式简介

自由口透传模式下，分控制和状态模块、输入输出数据模块。

（1）控制和状态模块，需要设置串口号，透传通讯方式。透传通讯方式有主动上报模式和主从应答模式。

（2）输入输出数据模块，只需要设置串口号。

控制和状态模块的过程数据定义：

IO 模块数据方向	数据名称	变量名称	数据类型	字节偏移
输入数据	输出控制字-反馈	Control_Word_Feedback	uint16_t	0
	发送帧字节长度-反馈	Send_Data_Len_Feedback	uint16_t	2
	串口状态	COM_Status	uint16_t	4
	接收错误帧计数	Error_Counter	uint16_t	6
	接收总数据帧计数	Received_Counter	uint16_t	8
	当前接收帧字节长度	Received_Data_Len	uint16_t	10
输出数据	输出控制字	Control_Word	uint16_t	0
	发送帧字节长度	Send_Data_Len	uint16_t	2

变量定义：

变量名称	Bit15-6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Control_Word	Reserved	Received Counter Reset	Error Counter Reset	Timeout Error Reset	Parity Error Reset	Done Reset	Trigger
Send_Data_Len	Send_Data_Len						
COM_Status	Reserved			Timeout Error	Parity Error	Done	Busy
Error_Counter	Error_Counter						
Received_Counter	Received_Counter						
Received_Data_Len	Received_Data_Len						

输入数据说明：

7. Control_Word_Feedback 为输出控制字 Control_Word 的反馈值，输出

控制字刷新到模块后，将更新到控制字反馈中。

8. Send_Data_Len_Feedback 为发送帧字节长度 Send_Data_Len 的反馈值，发送帧字节长度刷新到模块后，将更新到发送帧字节长度反馈中。

9. 应答模式下，串口发送数据时，Busy 位被置 1。

3.1 当在超时时间内串口接收到应答后，Busy 位清零，Done 完成位置 1，Received_Counter 计数值加 1，若接收帧有奇偶校验错误，则 Parity_Error 位被置 1，同时 Error_Counter 计数加 1。Received_Data_Len 中保存当前接收帧的字节数。

3.2 当在超时时间内串口未接收到应答，Busy 位清零，Done 完成位置 1，同时设置 Timeout_Error 为 1，Error_Counter 错误计数值加 1，Received_Data_Len 值清零。

4.在主动上报模式下，从站收到数据包时，Received_Counter 计数值加 1，若接收帧有奇偶校验错误，则 Parity_Error 位被置 1，同时 Error_Counter 计数加 1。

输出数据说明：

3. Received_Counter_Reset 上升沿时，接收计数值 Received_Counter 被清零，
Error_Counter_Reset 上升延时，错误计数值 Error_Counter 被清零，
Timeout_Error_Reset 上升延时，Timeout_Error 被清零，
Parity_Error_Reset 上升延时，Parity_Error 被清零,
Done_Reset 上升延时，Done 被清零。

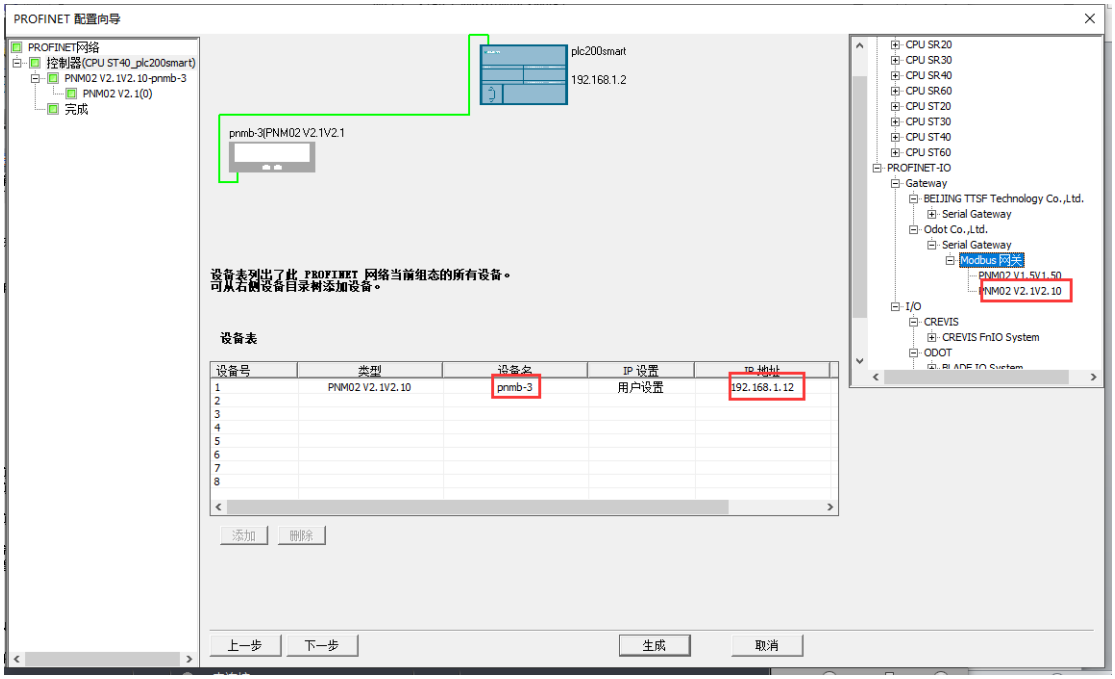
2.主动上报模式下，Trigger 位无效，Send_Data_Len 无效。

3.主从应答模式下，Trigger 上升延时触发一次串口数据发送，串口将按 Send_Data_Len 的数据长度发送数据包并等待应答处理。

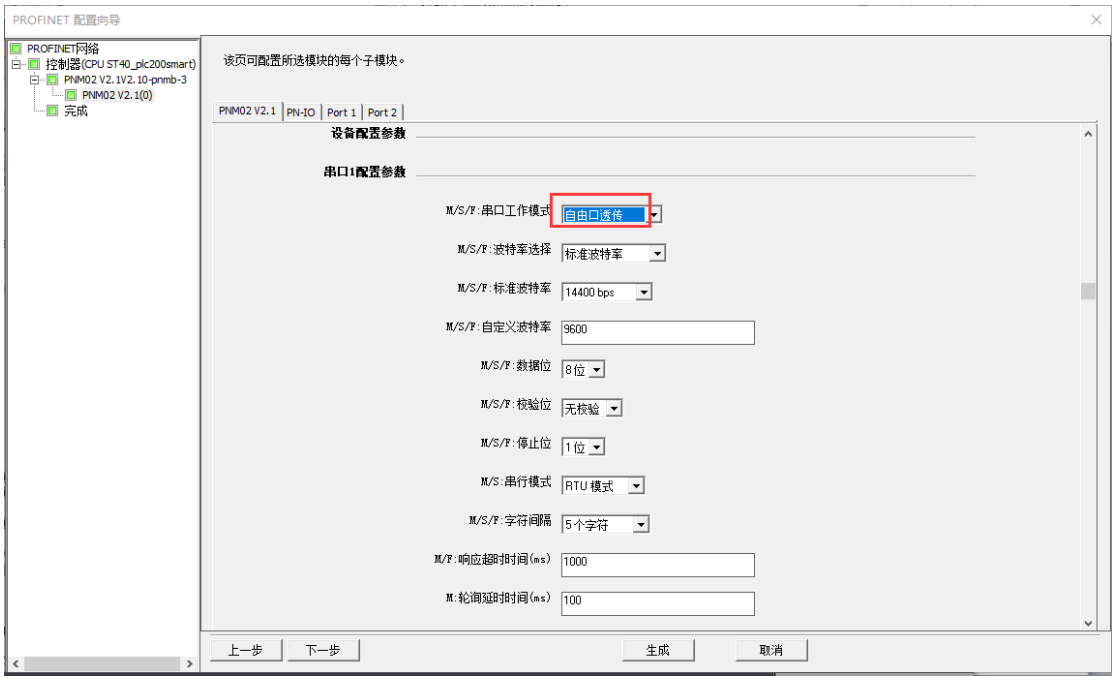
6.3.2 自由口透传模式测试应用

1、打开 STEP 7-MicroWIN SMART 软件， 点击查找 PROFINET 设备，选择本机网卡，会自动扫描到所有的 PROFINET 设备，可查看网关的 IP 地址和设备名称。点击编辑，设置网关设备名称。

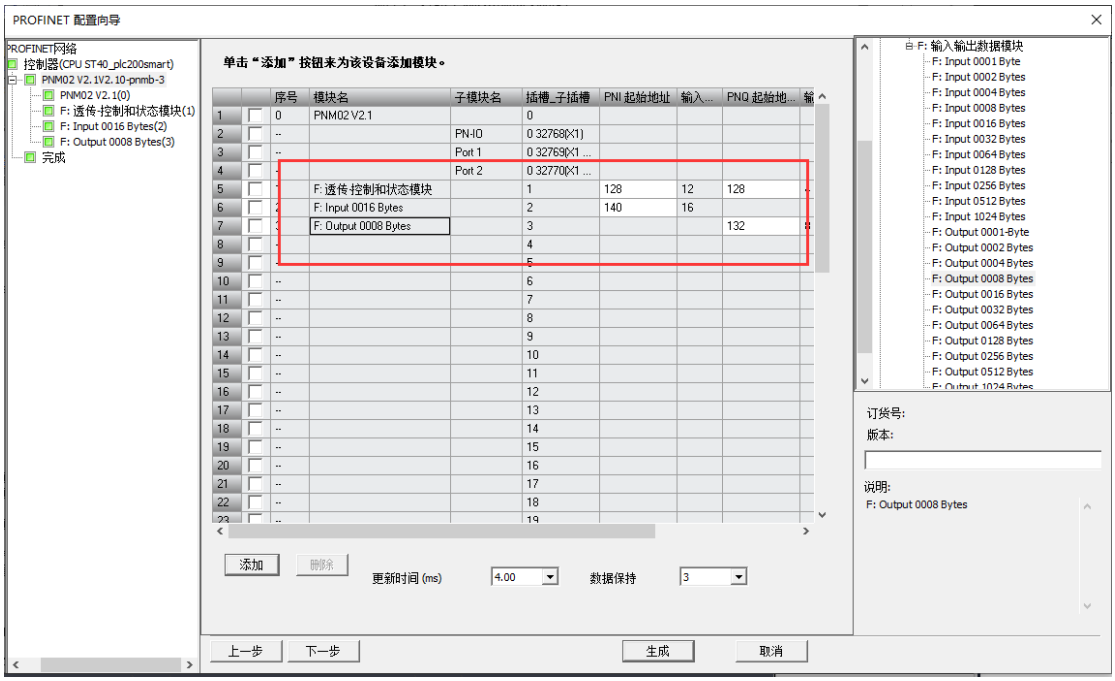
2、点击工具，点击 PROFINET，在弹出的 PROFINET 配置向导界面，选择 PLC 角色为：控制器，修改 200 Smart 的 IP 地址，点击下一步。在右侧目录栏选中 PNM02，在左下角点击添加按钮，可将网关加入 PLC 的 PROFINET 总线。设置之前的设备名称 pnmb-3，分配网关的 IP 地址 192.168.1.12.



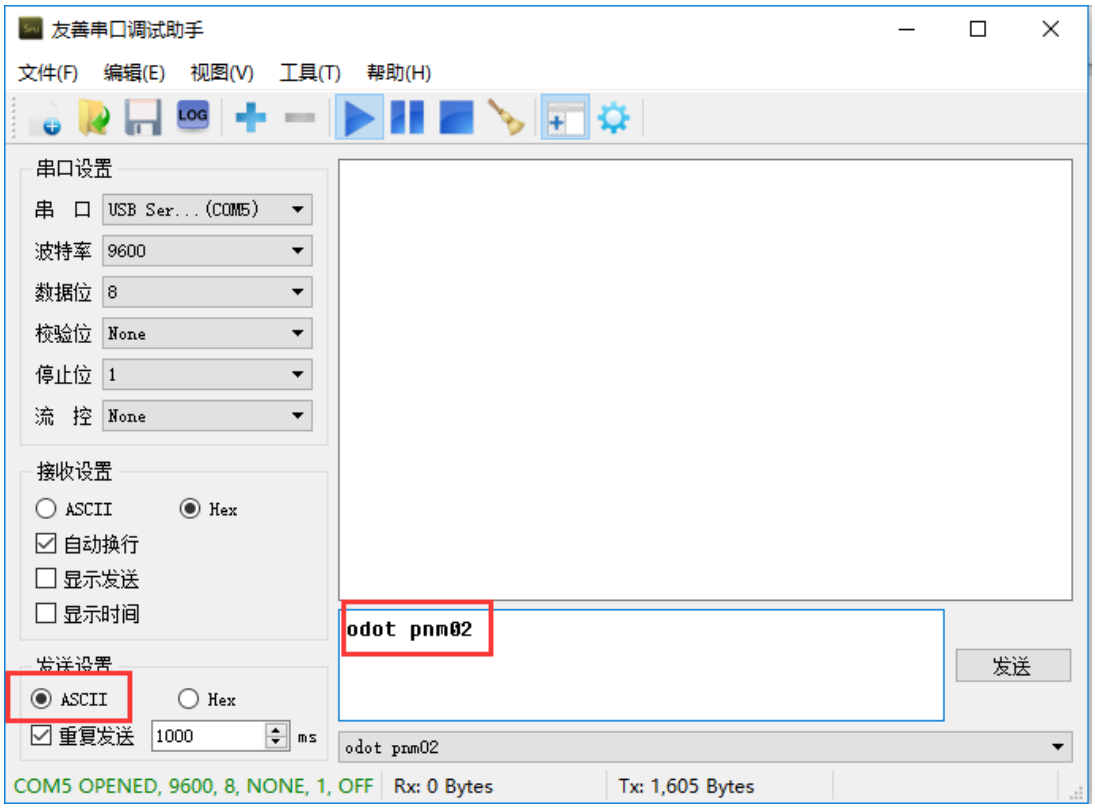
选中 PNM02,可修改网关工作模式和串口参数，工作模式选择自由口透传。

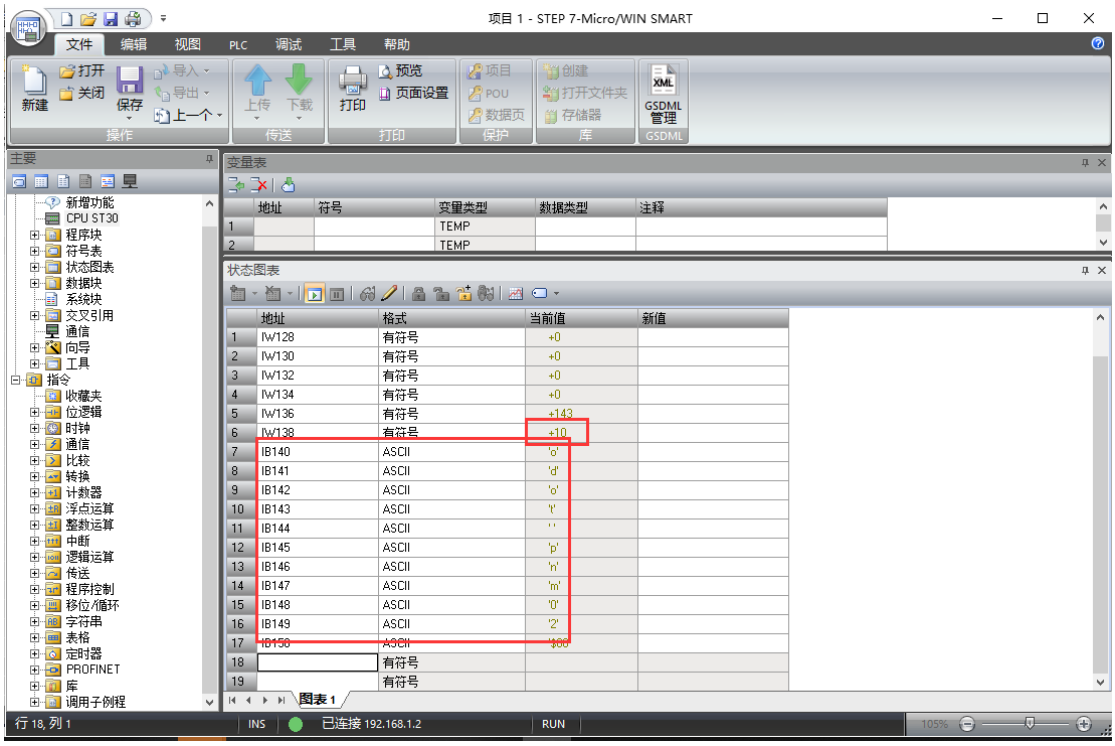


6、选中 PNM02-pnmb-2,将右侧的自由口透传模式下读写命令添加到插槽内。设置模块透传通讯方式为**主动上报模式**，点击**生成**，完成对网关 PNM02 自由口透传模式的配置。



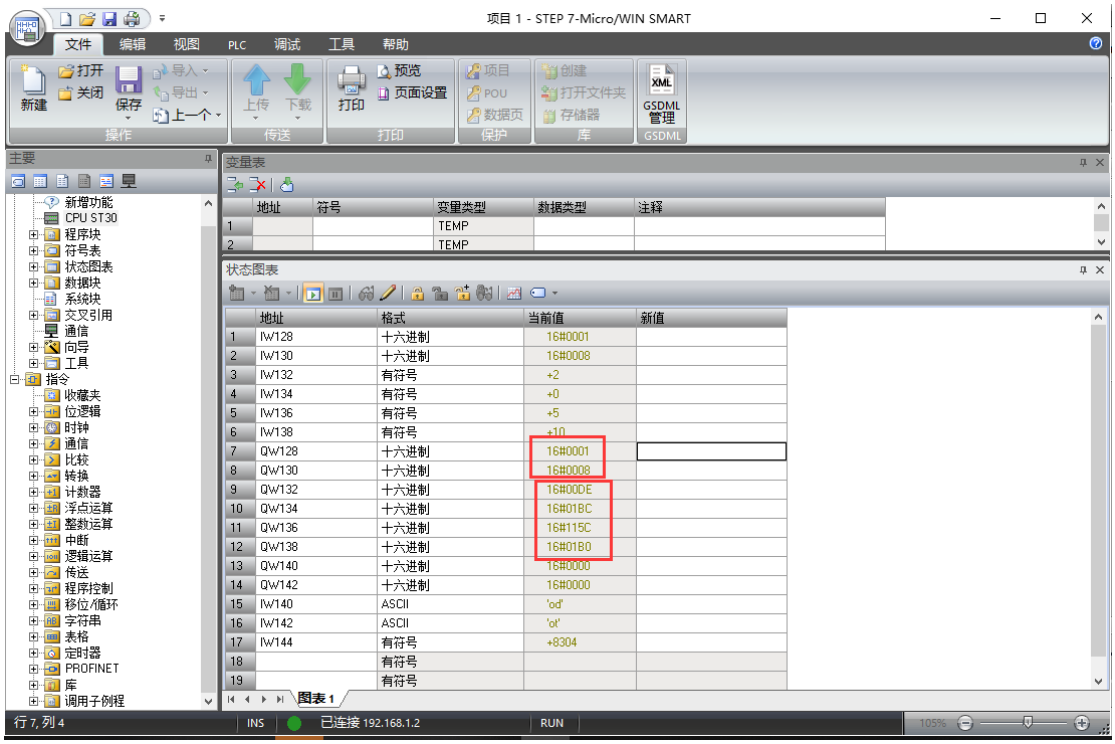
将网关设置为**主动上报**模式，网关串口 1 接调试串口工具模拟现场设备（比如扫码枪、称重仪表等）。可在控制和状态模块、输入输出数据模块监控到相应的值的变化。

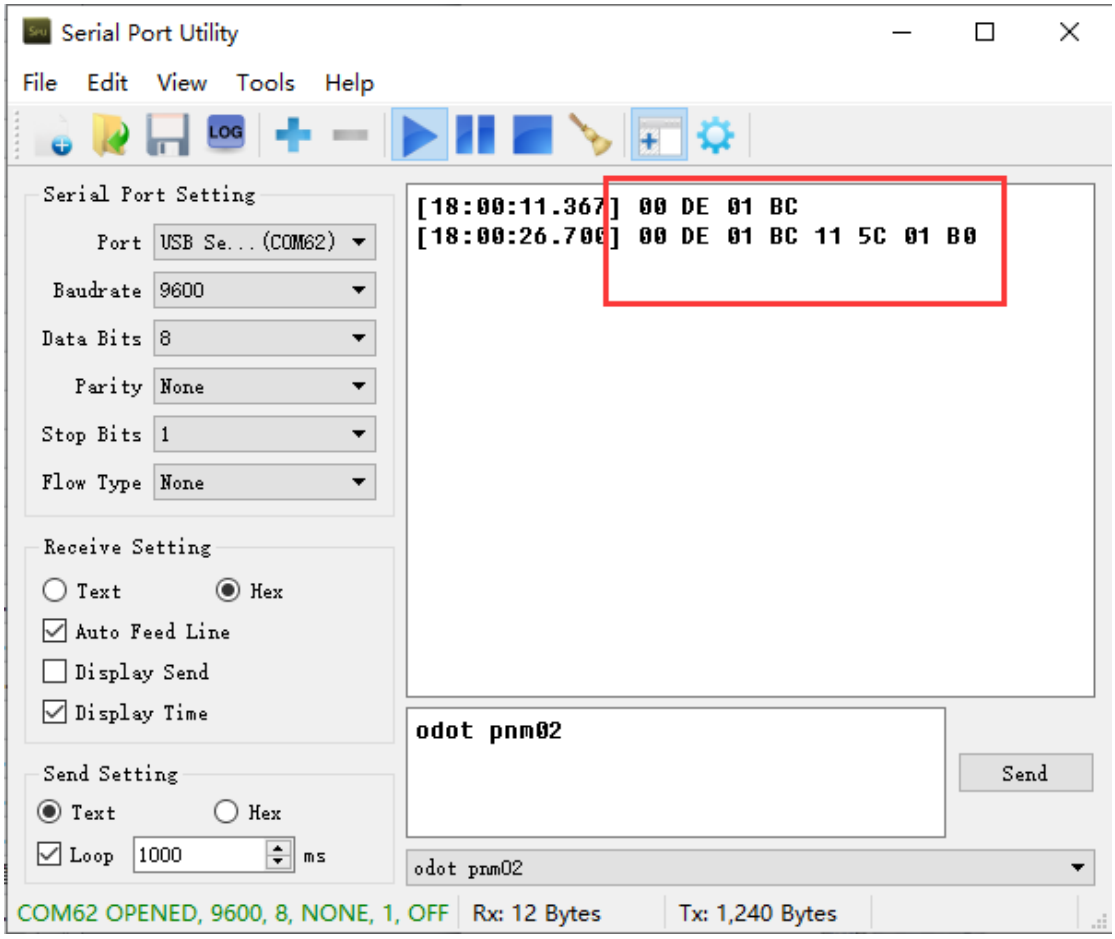

友善串口调试助手
文件(F) 编辑(E) 视图(V) 工具(T) 帮助(H)
串口设置
串 口 USB Ser...(COM5)
波特率 9600
数据位 8
校验位 None
停止位 1
流 控 None
接收设置
ASCII Hex
自动换行
显示发送
显示时间
发送设置
ASCII Hex
重复发送 1000 ms
odot pnm02
发送
odot pnm02
COM5 OPENED, 9600, 8, NONE, 1, OFF Rx: 0 Bytes Tx: 1,605 Bytes


项目 1 - STEP 7-Micro/WIN SMART
变量表
状态图表
地址 格式 当前值 新值
IW128 有符号 +0
IW130 有符号 +0
IW132 有符号 +0
IW134 有符号 +0
IW136 有符号 +143
IW138 有符号 +10
IB140 ASCII 'o'
IB141 ASCII 'd'
IB142 ASCII 'o'
IB143 ASCII 't'
IB144 ASCII ' '
IB145 ASCII 'p'
IB146 ASCII 'n'
IB147 ASCII 'm'
IB148 ASCII '0'
IB149 ASCII '2'
图表 1
行 18, 列 1 INS 已连接 192.168.1.2 RUN

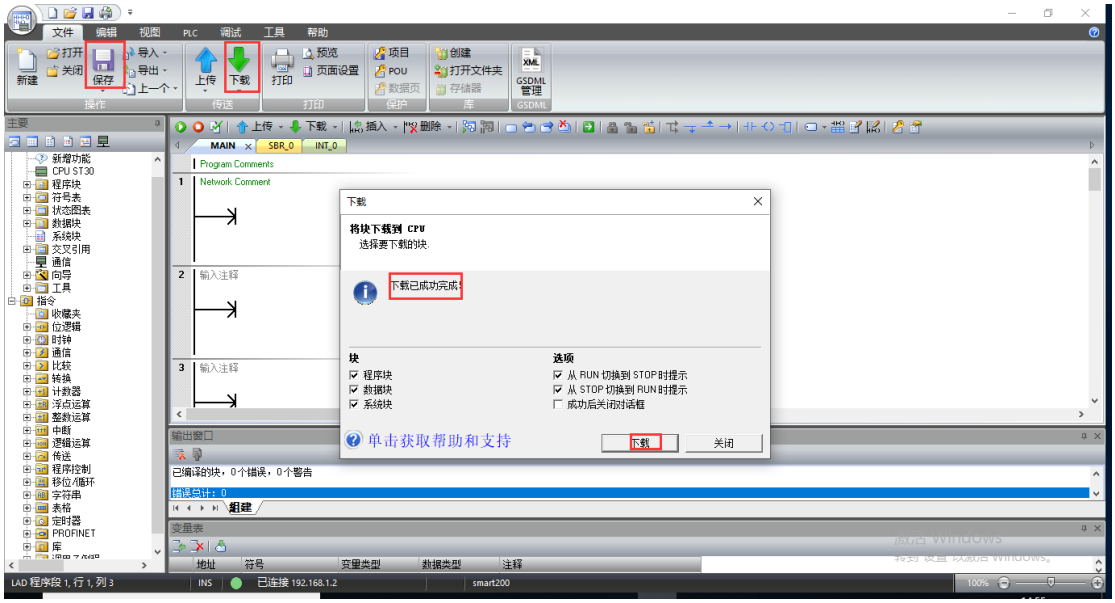
将网关设置为**主从应答**模式。

当控制字 Trigger 为 0-1 脉冲激活时，网关发送数据到串口。注：Trigger 位激活一次，网关发送一次数据。





通过一系列的设置调试，PLC 通过网关将串口侧数据采集上来后存储在 PLC 地址区，工程人员自己解析上传报文数据格式，提取有效的数据进行编程处理。项目完成后，保存、编译，下载程序。



七、固件升级

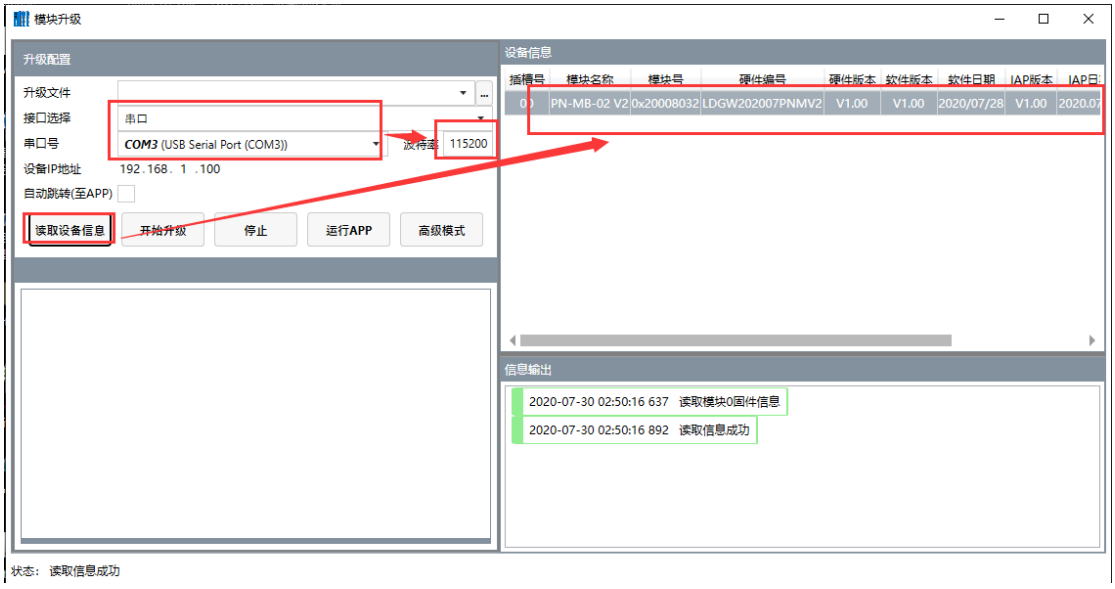
7.1 串口升级

当模块固件更新，需要给模块固件升级。升级需要在 IAP 模式进行。

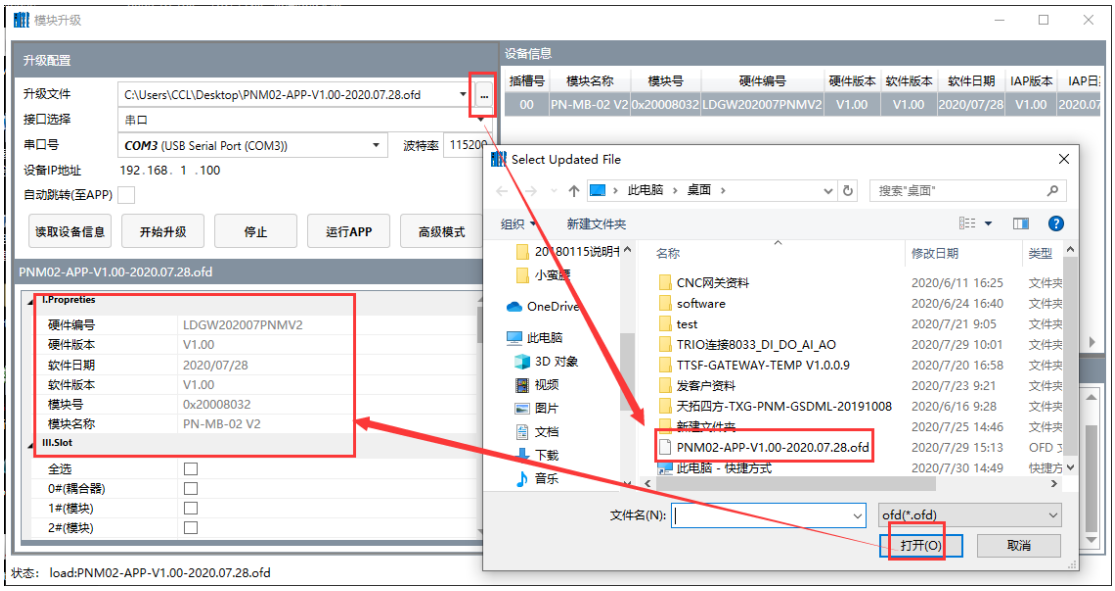
按住复位按钮后给模块上电 24Vdc，当当 DF 红绿指示灯交替闪烁时，表示进入 IAP 模块。使用 USB 转 485 转换器的 485 接口 A、B 接到网关串口 1 的 1TA+、1TB-端口，转换器的 USB 接口接到电脑的 USB 接口

安装升级软件：**Firmware Update Tool V1.0.0.8**

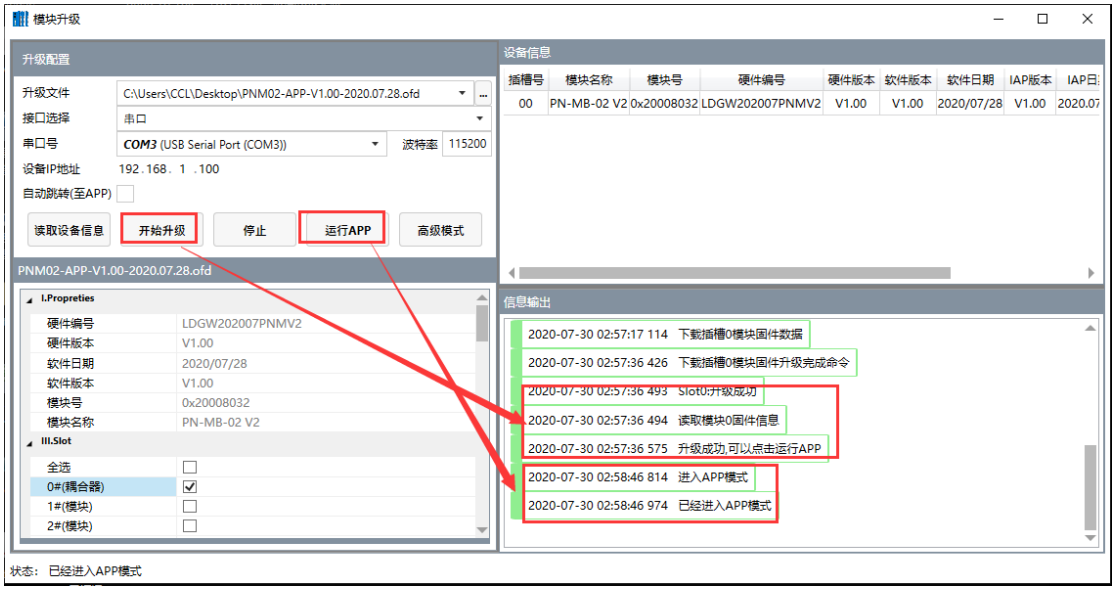
安装完成后，打开升级软件，接口选择串口，串口号可查看我的电脑—“设备管理器”，波特率设置为：115200。点击读取设备信息，可以读取到网关内部固件信息。



点击 ... ，在弹出的界面，选择新的固件文件，点击打开，会在左下角显示新固件信息。



选中 0#耦合器，打“√”，点击开始升级，完成后点击运行 APP。或者选中自动跳转（至 APP）点击开始升级。



进入 APP 模式时，所有指示灯会闪烁亮一次。

7.2 网口升级

网关支持网口升级。

当模块固件更新，需要给模块固件升级。升级需要在 IAP 模式进行。

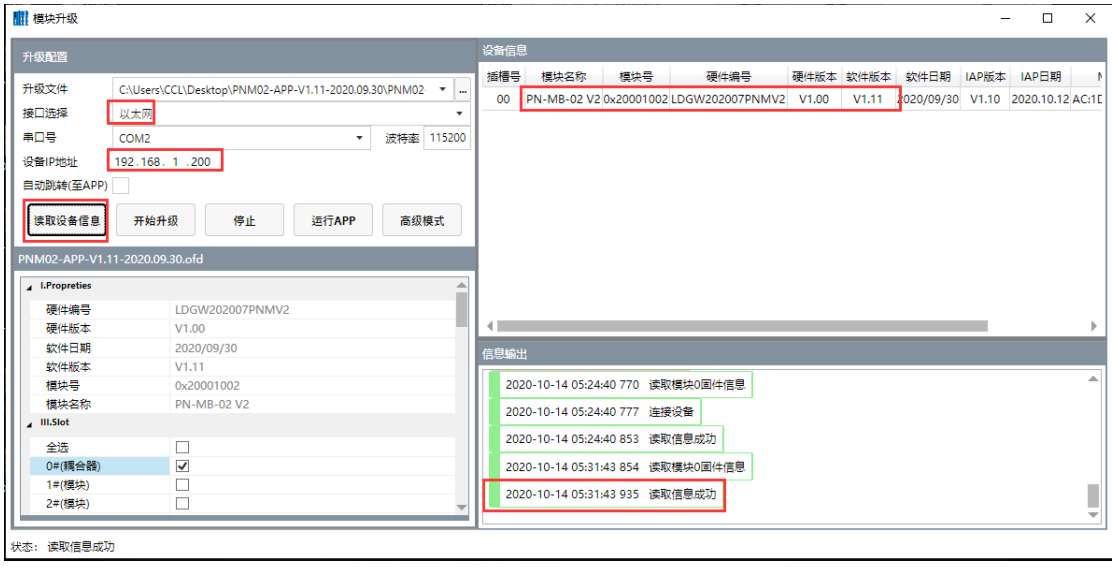
进入 IAP 升级模式有两种方式：

一：按住复位按钮后给模块上电 24Vdc，当 DF 红绿指示灯交替闪烁时，表示进入 IAP 升级模式。

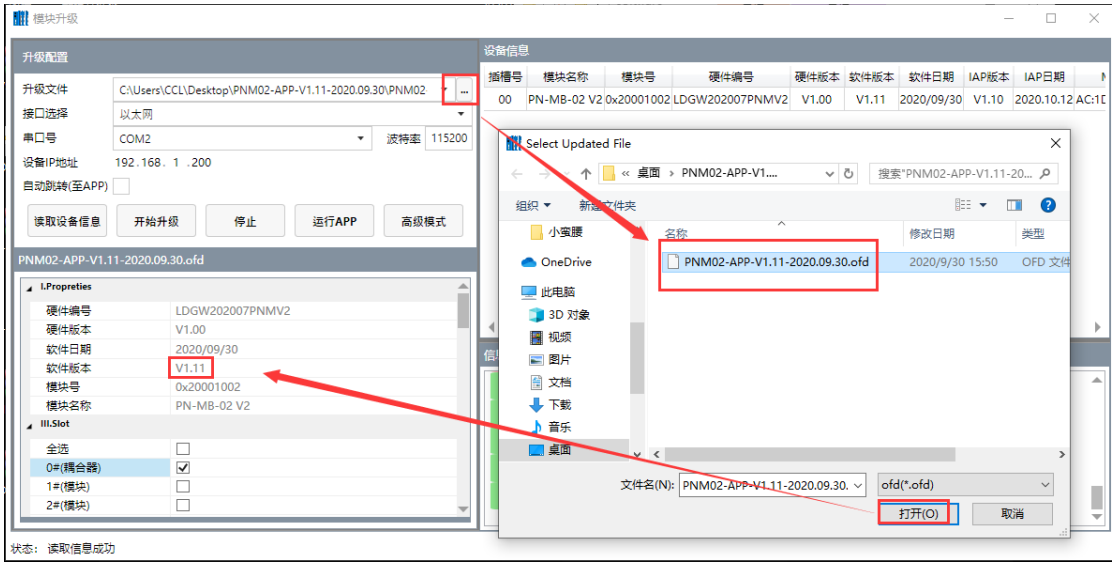
二：给网关设备名称设置为“start-bootloader”,即可进入 IAP 升级模式

安装升级软件：Firmware Update Tool V1.0.0.8

安装完成后，打开升级软件，接口选择网口，设备 IP 地址：192.168.1.200。点击读取设备信息，可以读取到网关内部固件信息。



点击 ... ，在弹出的界面，选择新的固件文件，点击打开，会在左下角显示新固件信息。



选中 0#耦合器，打“√”，点击开始升级，完成后点击运行 APP。或者选中自动跳转（至 APP）点击开始升级。

八、附录

8.1 Modbus-RTU 协议简介

对于您来说，您只需要了解 Modbus 有 4 个区对应的 8 条重要的功能码：4 条读、2 条写单个位或寄存器，2 条写多个位或者多个寄存器。(地址描述采用 PLC 地址)

8.1.1 Modbus存储区

Modbus 涉及到的控制器（或 Modbus 设备）存储区以 0XXXX、1XXXX、3XXXX、4XXXX 标识。

存储区标识	名称	数据类型	读/写	存储单元地址
0XXXX	输出线圈	位	读/写	00001~0XXXX, XXXX：与设备有关
1XXXX	离散量输入	位	只读	10001~1XXXX, XXXX：与设备有关
3XXXX	输入寄存器	字	只读	30001~3XXXX, XXXX：与设备有关
4XXXX	输出/保持寄存器	字	读/写	40001~4XXXX, XXXX：与设备有关

8.1.2 Modbus功能码

Modbus 报文相对比较固定，所以您只需要稍作了解，看几条报文之后就知道了它的结构，在需要的时候再具体查询。

（1）读取输出线圈状态

功能码：01H

主站询问报文格式：

地址	功能码	起始地址 高位	起始地址 低位	线圈数 高位	线圈数 低位	CRC
0x11	0x01	0x00	0x13	0x00	0x25	xxxx

功能：读从站输出线圈 0XXXX 状态。

注意：有些设备线圈起始地址为 00000，对应设备中 00001 地址，依次顺延。

本例：读 0x11 号从站输出线圈，寄存器起始地址为 0x13=19，线圈数为 0x0025H=37；因此，本询问报文功能是：读 0x11（17）号从站输出线圈 00019—00055，共 37 个线圈状态。

从站应答格式：

地址	功能码	字节计数	线圈状态 19-26	线圈状态 27-34	线圈状态 35-42	线圈状态 43-50	线圈状态 51-55	CRC
0x11	0x01	0x05	0xCD	0x6B	0xB2	0x0E	0x1B	xxxx

功能：从机返回输出线圈 0XXXX 状态

（2）读取离散量输入状态

功能码：02H

主站询问报文格式：

地址	功能码	起始地址高位	起始地址低位	线圈数高位	线圈数低位	CRC
0x11	0x02	0x00	0xC4	0x00	0x16	xxxx

功能：读从站输入线圈 1XXXX 状态。

注意：有些设备线圈起始地址为 10000，对应设备中 10001 地址，依次顺延。

本例：读 0x11 号从站输入线圈，起始地址为 0x00C4=196，线圈数为 0x0016=22.

因此，本询问报文功能是：读 0x11（17）号从站输入线圈 10196—10217，共 22 个离散量输入状态。

从站应答格式：

地址	功能码	字节计数	DI 10196-10203	DI 10204-10211	DI 10212-10217	CRC
0x11	0x02	0x03	0xAC	0xDB	0x35	xxxx

功能：从机返回输入线圈 1 XXXX 状态

（3）读取输出/保持寄存器

功能码：03H

主站询问报文格式：

地址	功能码	寄存器起始地址高位	寄存器起始地址低位	寄存器数高位	寄存器数低位	CRC
0x11	0x03	0x00	0x6B	0x00	0x03	xxxx

功能：读从站保持寄存器 4XXXX 值。

注意：有些设备寄存器起始地址 40000 对应设备中 40001 地址,依次顺延。

本例：读 0x11 号从站保持寄存器值，起始地址为 0x006BH=107，寄存器数为 0x0003；因此，本询问报文功能是：读 0x11（17H）号从站 3 个保持寄存器 40107—40109 的值；

地址	功能码	字节计数	寄存器 40107 高位	寄存器 40107 低位	寄存器 40108 高位	寄存器 40108 低位	寄存器 40109 高位	寄存器 40109 低位	CRC
0x11	0x03	0x06	0x02	0x2B	0x01	0x06	0x2A	0x64	xxxx

功能：从站返回保持寄存器的值：(40107)=0x022B，(40108)=0x0106，(40109)=0x2A64

（4）读取输入寄存器

功能码：04H

主站询问报文格式：

地址	功能码	寄存器起始地址高位	寄存器起始地址低位	寄存器数高位	寄存器数低位	CRC
0x11	0x04	0x00	0x08	0x00	0x01	xxxx

功能：读从站输入寄存器 3XXXX 值。

注意：有些设备中寄存器起始地址 30000 对应设备中 30001 地址，依次顺延。

本例：读 0x11 号从站输入寄存器值，起始地为 0x0008H，寄存器数为 0x0001；因此，本询问报文功能：读 0x11（17）号从站 1 个输入寄存器 30008 的值；

从站应答格式：

地址	功能码	字节计数	输入寄存器 30008 高位	输入寄存器 30008 低位	CRC
0x11	0x04	0x02	0x01	0x01	xxxx

功能：从站返回输入寄存器 30008 的值；（30008）=0x0101

（5）强置单个线圈

功能码：05H

主站询问报文格式：

地址	功能码	线圈地址高位	线圈地址低位	断通标志	断通标志	CRC
0x11	0x05	0x00	0xAC	0xFF	0x00	xxxx

功能：强置 0x01(17)号从站线圈 0XXXX 值。有些设备中线圈起始地址 00000 对应设备中 00001 地址，依次顺延。

断通标志=FF00，置线圈 ON。

断通标志=0000，置线圈 OFF。

例：起始地址为 0x00AC=172。强置 17 号从站线圈 0172 为 ON 状态。

应答格式：原文返回

功能：强置 17 号从机线圈 0172 ON 后原文返回

地址	功能码	线圈地址高位	线圈地址低位	断通标志	断通标志	CRC
0x11	0x05	0x00	0xAC	0xFF	0x00	xxxx

（6）预置单保持寄存器

功能码：06H

主站询问报文格式：

地址	功能码	寄存器起始地址高位	寄存器起始地址低位	寄存器数高位	寄存器数低位	CRC
0x11	0x06	0x00	0x87	0x03	0x9E	xxxx

功能：预置单保持寄存器 4XXXX 值。有些设备中线圈起始地址 40000 对应设备中 40001 地址，依次顺延。

例：预置 17 号从机单个保持寄存器 40135 值为 0x039E；

应答格式：原文返回

地址	功能码	寄存器起始地址高位	寄存器起始地址低位	寄存器数高位	寄存器数低位	CRC
0x11	0x06	0x00	0x87	0x03	0x9E	xxxx

功能：预置 17 号从机单保持寄存器 40135 值为 0x039E 后原文返回。

（7）强置多线圈

功能码：0FH

主站询问报文格式：

地址	功能码	线圈起始地址高位	线圈起始地址低位	线圈数高位	线圈数低位	字节计数	线圈状态 20-27	线圈状态 28-29	CRC
0x11	0x0F	0x00	0x13	0x00	0x0A	0x02	0xCD	0x00	xxxx

功能：将多个连续线圈 0XXXX 强置为 ON/OFF 状态。

注意：有些设备中线圈起始地址 00000 对应设备中 00001 地址，依次顺延。

本例：强置 0x11 号从站多个连续线圈，线圈起始地址为 0x0013=19，线圈数为 0x000A=10

因此，本询问报文功能是：强置 0x11（17）号从站 10 个线圈 00019—00028 的值； CDH→00019-00026; 00H→00027-00028；

从站应答格式：

地址	功能码	线圈起始地址高位	线圈起始地址低位	线圈数高位	线圈数低位	CRC
0x11	0x0F	0x00	0x13	0x00	0x0A	xxxx

（8）预置多寄存器

功能码：10H

主站询问报文格式：

地址	功能码	起始寄存器地址高位	起始寄存器地址低位	寄存器数高位	寄存器数低位	字节计数	数据高位	数据低位	数据高位	数据低位	CRC
0x11	0x10	0x00	0x87	0x00	0x02	0x04	0x01	0x05	0x0A	0x10	xxxx

功能：预置从站多个保持寄存器值 4XXXX。

注意：有些设备中保持寄存器起始地址 40000 对应设备中 40001 地址，依次顺延。

本例：预置 0x11 号从站多个保持寄存器值，寄存器起始地址为 0x0087=135，线圈数为 0x0002=2。

因此，本询问报文功能是：预置 0x11（17）号从站 2 个保持寄存器值；0105H→40135; 0A10H→40136.

应答格式：

地址	功能码	起始寄存器地址高位	起始寄存器地址低位	寄存器数高位	寄存器数低位	CRC
0x11	0x10	0x00	0x87	0x00	0x02	xxxx

8.2 串口网络拓扑结构简介

8.2.1 RS232

RS232 是工业控制的串行通信接口之一，它被广泛用于计算机串行接口与外设连接。RS232 使用一根信号线和一根信号返回线构成共地的传输形式，采用三线制的接线方式，可以实现全双工通讯，传输信号为单端信号，这种共地传输容易产生共模干扰，所以抗噪声干扰性弱，传输距离有限，RS232 接口标准

规定在码元畸变小于 4%的情况下最大传输距离标准值为 50 英尺（**约为 15 米**）（15m 以上的长距离通信，需要采用调制调解器），最大传输距离还与通讯波特率有关，在实际运用过程中，如果传输距离较远，请降低波特率。为减小信号在传输过程中受到外界的电磁干扰，请使用**屏蔽电缆**作为通讯电缆。

RS232 接口标准规定了在 TXD 和 RXD 上：

RS232 采用负逻辑传送信号，将-(3~15)V 的信号作为逻辑“1”；将+(3~15)V 的信号作为逻辑“0”；介于-3~+3V 之间的电压无意义，低于-15V 或高于+15V 的电压也无意义。

RS232 接口分类：

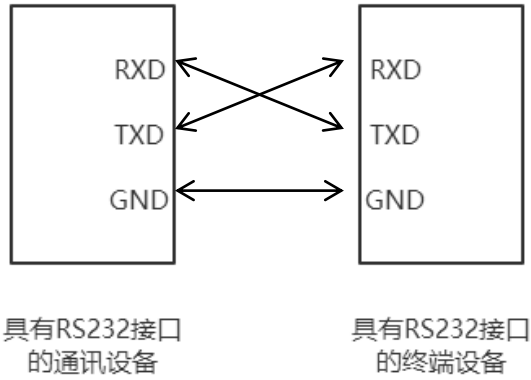
DB9 公头接口

左上角为 1，右下角为 9

9 针 RS232 串口（DB9）		
引脚	名称	作用
1	CD	载波检测
2	RXD	接收数据
3	TXD	发送数据
4	DTR	数据终端准备好
5	GND	信号地线
6	DSR	数据准备好
7	RTS	请求发送
8	CTS	清除发送
9	RI	振铃提示

由于 RS232 接口具有上述电气特性，所以其只能实现**点对点通讯**。

RS232 通讯接线示意图如图所示：



8.2.2 RS422

RS422 接口标准全称是“平衡电压数字接口电路的电气特性”，它定义了接口电路的特性。RS422 采用四线加地线（T+、T-、R+、R-、GND），全双工，差分传输，多点通信的数据传输协议。它采用平衡传输采用单向/非可逆，有使能端或没有使能端的传输线。由于接收器采用高输入阻抗和发送驱动器比 RS232 更强的驱动能力，故允许在相同传输线上连接多个接收节点，最多可接 10 个节点。即一个主设备(Master)，其余为从设备(Salve)，从设备之间不能通信，所以 RS-422 支持点对多的双向通信。

RS-422 的最大传输距离为 4000 英尺（约 1219 米），最大传输速率为 10Mb/s。其平衡双绞线的长度与传输速率成反比，在 100kb/s 速率以下，才可能达到最大传输距离。只有在很短的距离下才能获得最高速率传输。一般 100 米长的双绞线上所能获得的最大传输速率仅为 1Mb/s。

RS-422 需要接终端电阻，要求其阻值约等于传输电缆的特性阻抗。在短距离传输时可不需终接电阻，即一般在 300 米以下不需终接电阻。终接电阻接在传输电缆的最远端。

在进行一主多从组网连接时，**所有从站**的**发送端**通过**菊花链**的方式连接最后接入主站的**接收端**；所有从站的**接收端**通过**菊花链**的方式连接最后接入主站的**发送端**。

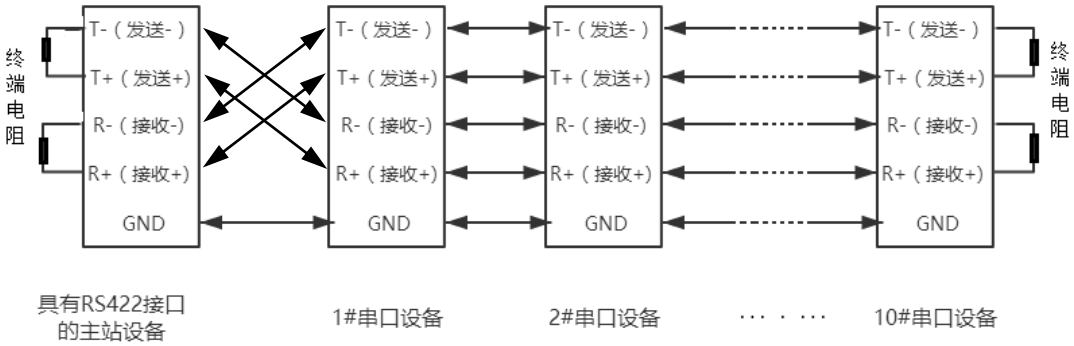
RS422 引脚定义：

RS422（9Pin）		作用	备注
3	R-	接收负	必连
2	T-	发送负	必连
7	R+	接收正	必连

8	T+	发送正	必连

左上角为 1，右下角为 9

RS422 通讯接线示意图如图所示：



8.2.2 RS485

由于 RS-485 是从 RS-422 基础上发展而来的，所以 RS-485 许多电气规定与 RS-422 相仿。如都采用平衡传输方式、都需要在传输线上接终接电阻等。RS-485 可以采用二线与四线方式，二线制可实现真正的多点双向通信。

RS485 是一个定义平衡数字多点系统中的驱动器和接收器的电气特性的标准，采用平衡驱动器和差分接收器的组合，抗共模干能力增强，即抗噪声干扰性好。由于 RS485 接口组成的半双工网络一般采用两线制的接线方式，采用差分信号传递数据，两线间的电压差为-(2~6)V 表示逻辑"0”，两线间的电压差为+(2~6)V 表示逻辑"1"。

RS485 信号**传输距离**与通讯波特率有关，波特率越高，传输距离越短，在波特率不高于 **100KbpS** 的情况下，理论最大通信距离约为 **1200 米**，在实际运用过程中，由于电磁干扰等因素，往往达不到最大通信距离，如果进行较远距离通讯，请**降低波特率**，为降低信号在传输过程中受到外界电磁干扰，请使用**双绞屏蔽电缆**作为通讯电缆。

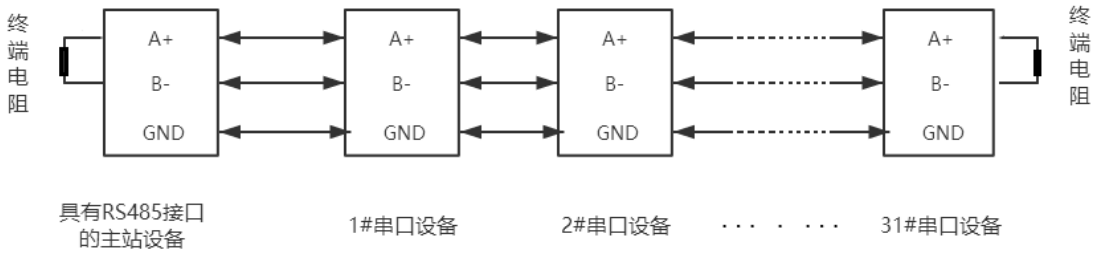
RS485 总线在不加中继的情况下最大支持 **32 个**节点，节点与节点之间采用“**菊花链**”的连接方式，在通讯电缆两端需加终端电阻，要求其阻值约等于传输电

缆的特性阻抗。在短距离传输时可不需终接电阻，即一般在 300 米以下不需终接电阻。终接电阻接在传输电缆的最两端。

RS485 9 针引脚定义：

针脚	名称	作用	备注
1	Data-/B-/485-	发送正	必连
2	Data+/A+/485+	接收正	必连
5	GND	地线	

RS485 通讯接线示意图如图所示：



四川零点自动化系统有限公司

地址：四川省绵阳市飞云大道 261 号综合保税区 204 厂房

电话：0816-2530577

传真：0816-6337503

邮编：621000

网址：www.odot.cn

零点微信公众号