MODBUS RTU 转 PROFINET 协议网关

HT3S-PNS-MDN

用户手册

V1.2



北京中科易联科技有限公司

目录

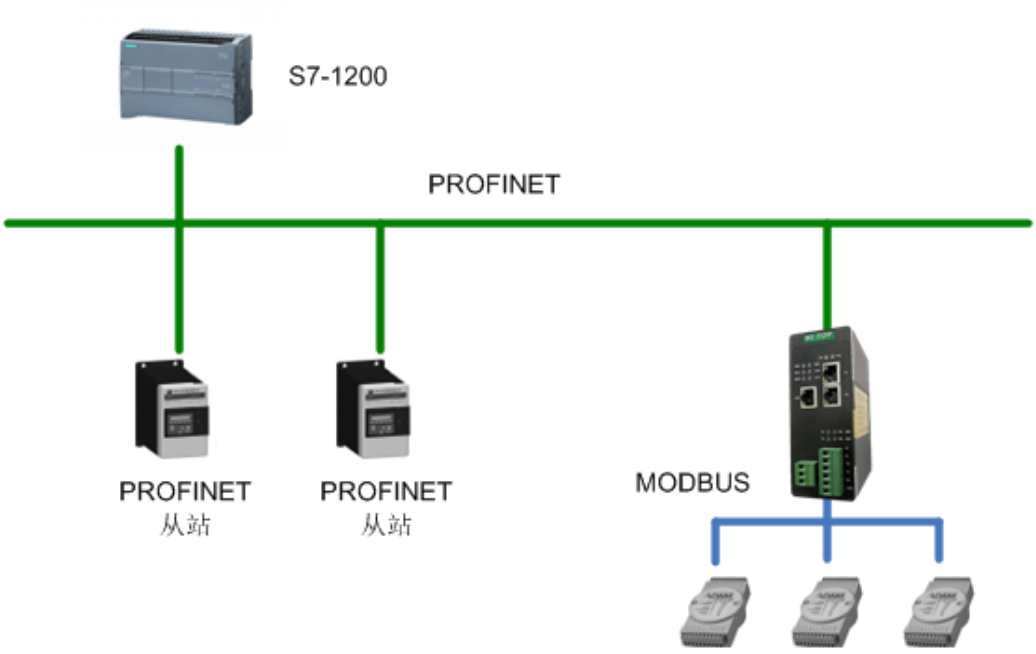
1. 产品概述 2
1.1 产品功能 2
1.2 技术参数 2
2. 产品外观 4
2.1 产品尺寸图 4
2.2 端子说明 4
2.3 指示灯 5
2.4 拨码说明 5
3. 硬件电气规范 6
3.1 电气参数 6
3.2 PROFINET 的电气连接 6
3.3 MODBUS 的电气连接 7
4. 协议及数据转换 8
4.1 协议转换原理 8
4.2 PROFINET 协议介绍 8
4.3 MODBUS 协议介绍 9
5. 软件配置及操作 16
5.1 通讯状态字及控制字 16
5.2 网关作为 MODBUS 主站 17
5.3 网关作为 MODBUS 从站 21

1. 产品概述

1.1 产品功能

HT3S-PNS-MDN 是一款 PROFINET 从站功能的通讯网关，主要功能是将各种 MODBUS-RTU 设备接入到 PROFINET 网络中，进行数据传输。

本网关连接到 PROFINET 总线中作为从站使用，连接到 MODBUS-RTU 总线中作为主站或从站使用。



1.2 技术参数

1.2.1 PROFINET 技术参数

● 网关作为 PROFINET 网络的 Device 设备（即从站），带 2 个 RJ45 以太网接口，支持 100BASE-TX，MDI/MDIX 自检测，集成以太网交换机，可以组成链式网络，支持环网冗余。

● 适应 PROFINET V2.3 协议，采用实时（RT）通讯功能，符合： GB/T 25105-2014《工业通信网络现场总线规范类型 10: PROFINET IO 规范》，IEC 61158-5-10：2007，IDT。

● 支持的数据长度：输入≤1400 字节，输出≤1400 字节，输入+输出≤2800 字节。

● 支持的插槽数量：最大 62 条。

● MODBUS 作为主站或从站时，使用不同的 GSD 文件。

1.2.2 MODBUS-RTU 技术参数

● 网关的 MODBUS 接口可通过拨码选择作为主站或从站，两种工作方式二选一工作。

● 网关的 MODBUS 接口可通过拨码选择 RS485 接口或 RS232 接口，两种接口二选一工作。

● 网关的 MODBUS 波特率支持： 2400、4800、9600、19.2K、38.4K、57.6K、115.2K，其它波特率可以定制。

● 网关的 MODBUS 字符格式及校验位：8 位无校验+1 停止位、8 位+偶校验+1 停止位、8 位+奇校验+1 停止位、8 位无校验+2 停止位。

● 网关作为 MODBUS 主站，支持 01H、02H、03H、04H、05H、06H、0FH、10H 号功能。

● 网关作为 MODBUS 从站，支持 02H、04H、0FH、10H 号功能。

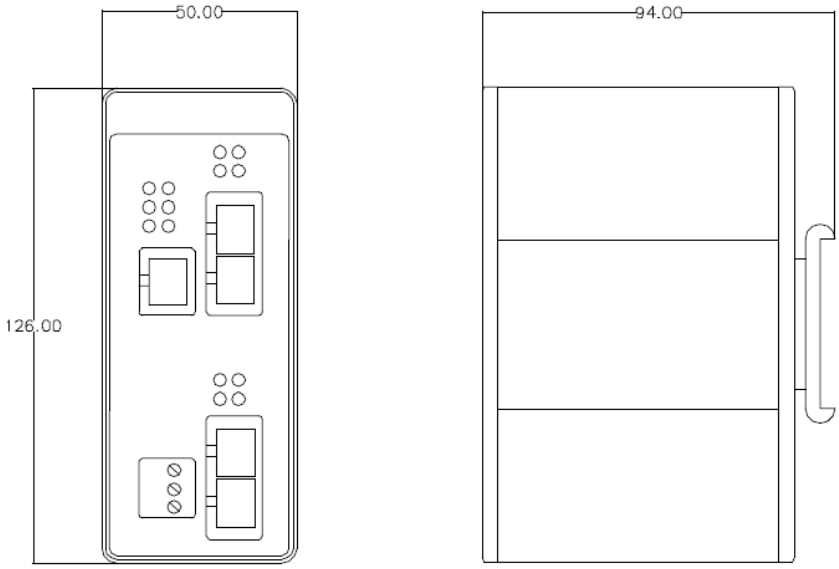
● 网关作为 MODBUS 主站，能带 Modbus 站点数：不确定，主要有两个条件的限制：

本产品网关最多能配置的 Modbus-RTU 报文数为 62 条；

支持的数据长度：输入≤1400 字节，输出≤1400 字节，输入+输出≤2800 字节。

2. 产品外观

2.1 产品尺寸图



2.2 端子说明



3PIN 端子 L+：电源 24V

3PIN 端子 M：电源 0V

3PIN 端子 PE：保护地

网口 LAN：网关下载口，本产品不使用

网口 P1：PROFINET 输入接口

网口 P2：PROFINET 输出接口

6PIN 端子 A+：485 信号 A

6PIN 端子 B-：485 信号 B

6PIN 端子 TR：485 终端电阻，TR 与 B 短接表示接入终端电阻

6PIN 端子 TX：232 发送信号

6PIN 端子 RX：232 接收信号

6PIN 端子 GND：232 口 GND

2.3 指示灯

标识	颜色	定义
PWR	绿色	网关内部电源正常
OK	黄色	PROFINET 通讯正常
FAL	红色	PROFINET 通讯断线
485-TX	绿色	485 接口正在发送数据
485-RX	绿色	485 接口正在接收数据
232-TX	绿色	232 接口正在发送数据
232-RX	绿色	232 接口正在接收数据

2.4 拨码说明



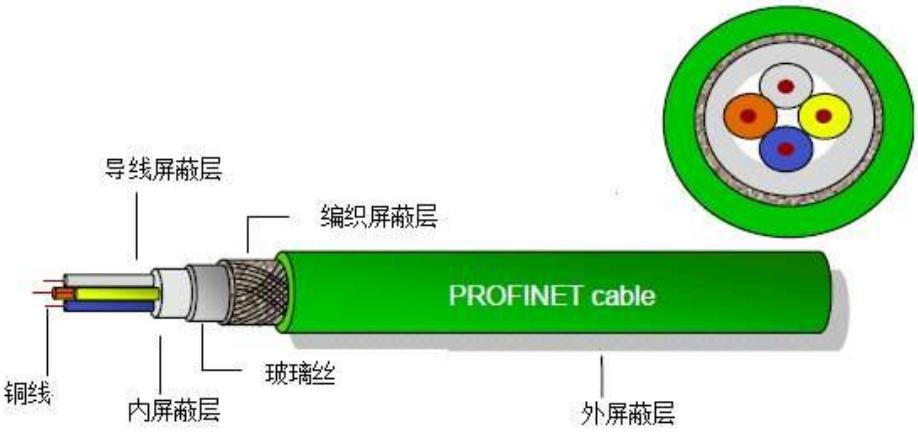
标识	拨位	定义
SW1 MODBUS 功能	Bit1	MODBUS 主从设置： ON：网关作为 MODBUS 主站工作 OFF：网关作为 MODBUS 从站工作
	Bit2	MODBUS 物理接口设置： ON：网关使用 485 接口工作 OFF：网关使用 232 接口工作
	其他	预留，全部拨到 OFF

3. 硬件电气规范

3.1 电气参数

- 电源：直流 24V/200mA（18V～30V 可用），使用中建议接好保护地 PE
- 工作环境：-40～75℃，湿度≤95%
- 防护等级：IP20
- 安装方式：35mm 导轨
- 重量：500g

3.2 PROFINET 的电气连接

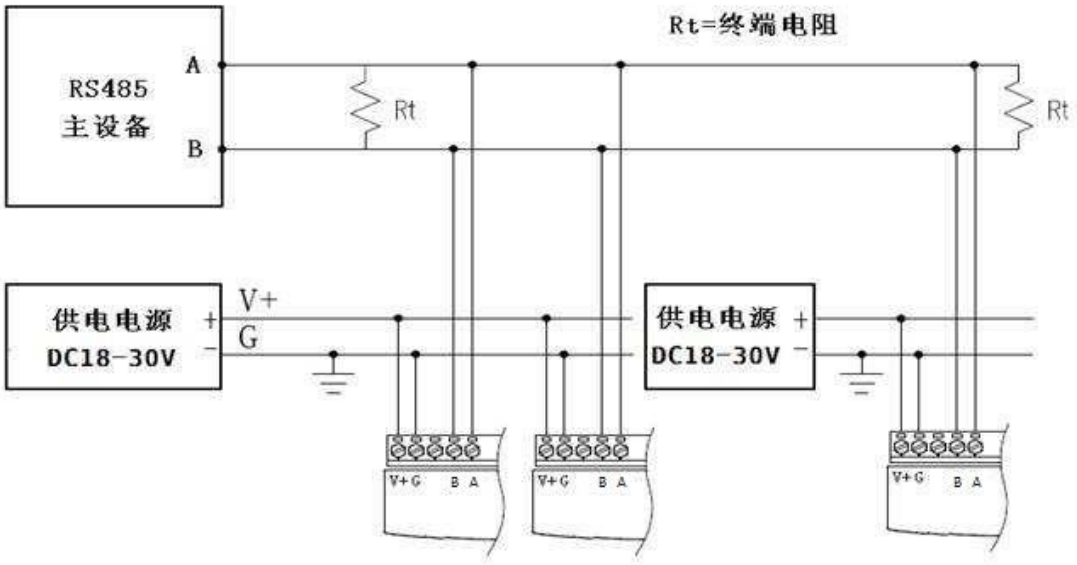


PROFINET 采用标准 4 芯屏蔽电缆。建议用户使用标准 PROFINET 插头及标准 PROFINET 电缆。有关 PROFINET 安装规范请用户参照有关 PROFINET 技术标准。



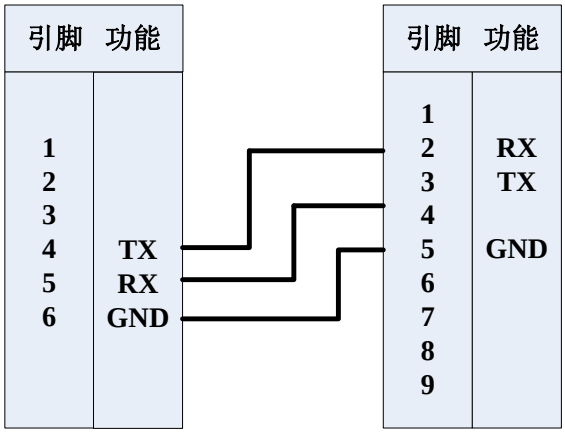
3.3 MODBUS 的电气连接

3.3.1 RS485 电气连接



使用 RS485 通讯时，所有设备的信号 A 连接到一起，信号 B 连接到一起。当需要使用终端电阻时，可以将网关端子的 B 与 TR 短接到一起。

3.3.2 RS232 电气连接

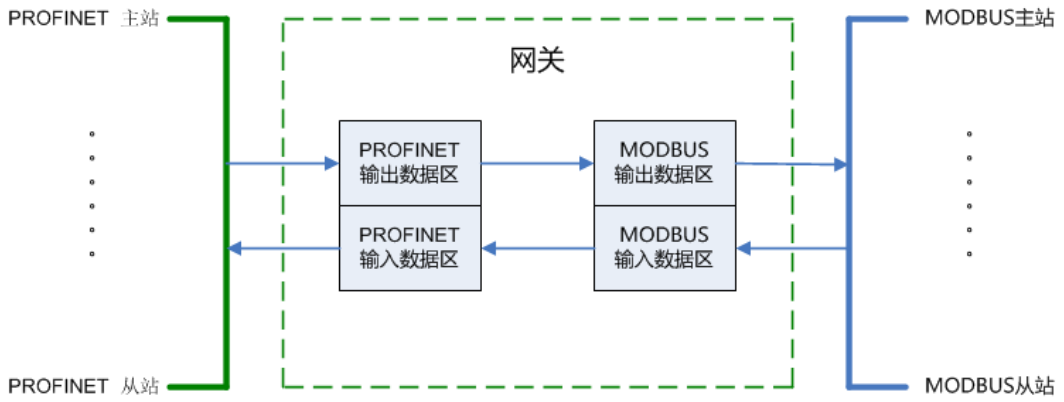


使用 RS232 通讯时，信号传输是单向的，请注意与对端设备的连接线序。网关的 TX 接对端设备的 RX，网关的 RX 接对端设备的 TXD，两端的 GND 连到一起。

4. 协议及数据转换

4.1 协议转换原理

网关分别从 PROFINET 一侧和 MODBUS 一侧读写数据，存入各自的缓冲区，网关内部将缓冲区的数据进行交换，从而实现两边数据的传输。



4.2 PROFINET 协议介绍

PROFINET 由 PROFIBUS 国际组织（PROFIBUS International，PI）推出，是新一代基于工业以太网技术的自动化总线标准。

PROFINET 为自动化通信领域提供了一个完整的网络解决方案，囊括了诸如实时以太网、运动控制、分布式自动化、故障安全以及网络安全等当前自动化领域的热点话题，并且，作为跨供应商的技术，可以完全兼容工业以太网和现有的现场总线（如 PROFIBUS）技术，保护现有投资。

PROFINET 网络中的每个模组都有以下的三个位址：

- MAC 位址。
- IP 地址。
- 设备名称，是在整个网络组态中对模组定义的逻辑名称。

由于 PROFINET 使用 TCP/IP，会用到 MAC 位址及 IP 地址，但若一设备更换为其他设备，其 MAC 地址会变动，而 IP 地址是动态定址下的结果，为了让网络上的某一设备有固定的名称，因此会使用设备名称。

为了分配 IP 地址、子网络遮罩及预设闸道，定义了以下的二种方式：

DCP(协定)（发现和配置协定）。

DHCP（动态主机设定协定）。

4.3 MODBUS 协议介绍

4.3.1 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	类型	读/写	存储单元地址
0XXXX	线圈	位	读/写	00000~0XXXX
1XXXX	输入线圈	位	只读	10000~1XXXX
3XXXX	输入寄存器	字	只读	30000~3XXXX
4XXXX	保持/输出寄存器	字	读/写	40000~4XXXX

4.3.2 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，在需要的时候再来具体查询。

4.3.2.1 读取输出状态(01H)

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
13H	01H	00H	11H(17)	00H	25H	xxxx

功能：读从站输出线圈0XXXX状态。

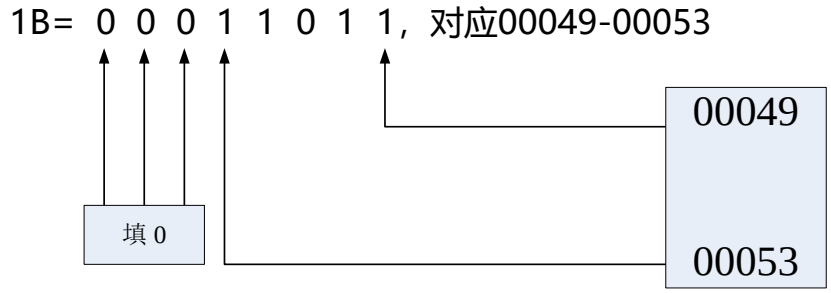
本例：读13H号从站输出线圈，寄存器起始地址=0011H=17，线圈数=0025H=37；因此，本询问报文功能是：读19（13H）号从站输出线圈00017-00053，共37个线圈状态。

从站应答格式：

地址	**功能码**	**字节计数**	**线圈状态 00017-00024**	**线圈状态 00025-00032**	**线圈状态 00033-00040**	**线圈状态 00041-00048**	**线圈状态 00049-00053**	**CRC**
13H	01H	05H	CDH	ABH	EFH	12H	1BH	xxxx

功能：从机返回输出线圈0XXXX状态

本例：1B=00011011，对应00049-00053



4.3.2.2 读取输入状态(02H)

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**
13H	02H	00H	12H(18)	00H	10H	xxxx

功能：读从站输入线圈1XXXX状态。

本例：读13H号从站输入线圈，起始地址=0012H=18，线圈数=0010H=16

因此，本询问报文功能是：读19（13H）号从站输入线圈10018—10033，共16个输入线圈状态；

从站应答格式：

地址	功能码	字节计数	线圈状态 10018-10025	线圈状态 10026-10033	CRC
13H	02H	02H	CDH	ABH	xxxx

功能：从机返回DI=1XXXX状态

4.3.2.3 读取保存寄存器(03H)

功能码：03H

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	寄存器数高位	寄存器数低位	CRC
13H	03H	00H	60H(96)	00H	02H	xxxx

功能：读从站保持寄存器4XXXX值。

本例：读13H号从站保持寄存器值，起始地址=0060H=96，寄存器数=0002；

因此，本询问报文功能是：读19（13H）号从站3个保持寄存器40096—40097的值；

从站应答格式：

地址	功能码	字节计数	寄存器 40096 高位	寄存器 40096 低位	寄存器 40097 高位	寄存器 40097 低位	CRC
13H	03H	04H	03H	00H	02H	2AH	xxxx

功能：从站返回保持寄存器的值：40096=0300H，40097=022AH

4.3.2.4 读取输入寄存器(04H)

功能码：04H

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	寄存器数高位	寄存器数低位	CRC
13H	04H	00H	05H	00H	01H	xxxx

功能：读从站输入寄存器3XXXX值。

本例：读13H号从站输入寄存器值，起始地=0005H=0005，寄存器数=0001；

因此，本询问报文功能：读19（13H）号从站1个保持寄存器30005的值；

从站应答格式：

地址	功能码	字节计数	寄存器 30005 高位	寄存器 30005 低位	CRC
13H	04H	02H	00H	00H	xxxx

功能：从站返回输入寄存器30005的值： 30005=0000H

4.3.2.5 强制单线圈(05H)

功能码：05H

询问格式：

地址	功能码	起始地址高位	起始地址低位	断通标志	断通标志	CRC
13H	05H	00H	11H(17)	FFH	00H	xxxx

功能：强置19号从站线圈0XXXX值。

断通标志=FF00，置线圈ON。

断通标志=0000，置线圈OFF。

例：起始地址=0011(H)=0017。强置17号从站线圈0172为 ON状态 。

从站应答格式：原文返回

地址	功能码	起始地址高位	起始地址低位	断通标志	断通标志	CRC
13H	05H	00H	11H(17)	FFH	00H	xxxx

功能：强置19号从站线圈0017=ON后原文返回

4.3.2.6 预置单保持寄存器(06H)

功能码：06H

询问格式：

地址	功能码	寄存器地址	寄存器地址	寄存器数	寄存器数	CRC

		高位	低位	高位	低位	
13H	06H	00H	15H	01H	01H	xxxx

功能：预置单保持寄存器4XXXX值。

例：预置19号从机单保持寄存器40021值=0x0101；

从站应答格式：原文返回

地址	功能码	寄存器地址高位	寄存器地址低位	寄存器数高位	寄存器数低位	CRC
13H	06H	00H	15H	01H	01H	xxxx

功能：预置19号从机单保持寄存器40021值=0x0101后原文返回。

4.3.2.7 强制多线圈(0FH)

功能码：0FH

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	线圈数高位	线圈数低位	字节计数	线圈状态17-24	线圈状态25	CRC
13H	0FH	00H	11H	00H	09H	02H	01H	01H	xxxx

功能：将多个连续线圈0XXXX强置为ON/OFF状态。

本例：强置13H号从站多个连续线圈，线圈起始地址=0011H=17，线圈数=0009H=9；

因此，本询问报文功能是：强置19（13H）号从站9个线圈00017-00025的值；

01H→00017-00024; 01H→00025；

从站应答格式：

地址	功能码	线圈地址高位	线圈地址低位	线圈数高位	线圈数低位	CRC
13H	0FH	00H	11H	00H	09H	xxxx

4.3.2.8 预置多寄存器(10H)

功能码：10H

主站询问报文格式：

地址	功能码	寄存器地址高位	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
13H	10H	00H	0AH	00H	02H	04H	01H	02H	01H	CDH	xxxx

功能：预置从站多个保持寄存器值4XXXX。

本例：预置13H号从站多个保持寄存器值，寄存器起始地址=000AH=00010，线圈数=0002H=2。因此，本询问报文功能是：预置19（13H）号从站2个保持寄存器值；

0102H→40010； 01CDH→40011

从站应答格式：

地址	功能码	寄存器地址高位	寄存器地址低位	寄存器数高位	寄存器数低位	CRC
13H	10H	00H	0AH	00H	02H	xxxx

4.3.3 MODBUS 异常码

(1) 从机接收到的主机报文，没有传输错误，但从机无法正确执行主机命令或无法作出正确应答，从机将以“异常应答”回答之。

(2) 异常应答报文格式

例：主机发请求报文，功能码01H：读1个04A1线圈值

地址	功能码	寄存器地址高位	寄存器地址低位	线圈数高位	线圈数低位	CRC
0AH	01H	04H	A1H	00H	01H	xxxx

由于从机最高线圈地址为0400，则04A1 超地址上限，从机作出异常应答如下（注意：功能码最高位置1）：

地址	功能码	寄存器地址高位	CRC
0AH	81H	02H	xxxx

(3) 异常码：

异常码	名称	说明
01	非法功能	所收到的报文功能对于被编址从机是不允许执行的。
02	非法数据地址	数据字段中的地址对于被编址的从机是禁止的。
03	非法数据	数据字段中的数值对于被编址的从机是禁止的。
04~07	保留	
08	奇偶校验错误	通讯报文中的奇偶校验出错。

5. 软件配置及操作

5.1 通讯状态字及控制字

当添加网关到 Profinet 总线上去的时候，有一个 Module 是自动添加上去的，这就是状态字以及控制字。

（1） 通信状态字

D7：奇偶校验	D6：CRC 校验	D5：等待超时	D4~D1：异常应答	D0：接收/发送
0：没有错误 1：奇偶校验错	0：没有错误 1：CRC 校验错	0：没有错误 1：等待超时	0：没有错误 其他：Modbus 访问异常	0：准备接收 1：准备发送

D0：MODBUS 正在发送或接收数据。

D4~D1：异常应答如果不为 0，说明你发出去的 Modbus 报文对于被访问设备来说是无效的，有可能是地址超限，或者写给设备的值是非法的。解决此问题的方法就是一定要弄清楚你要访问的数据是什么，寄存器地址是多少？被设置的值有没有范围限制等等。

D5：等待超时，可以将“总线空闲时间”设置的大一些。

D6：CRC 校验错，可能用户编写的 CRC 高低字节反了，或者在没有完整收到一帧报文也会出现 CRC 错，这时候我们可以通过串口调试助手软件监控一下报文。

D7：奇偶校验错，接口没有设置的一致。

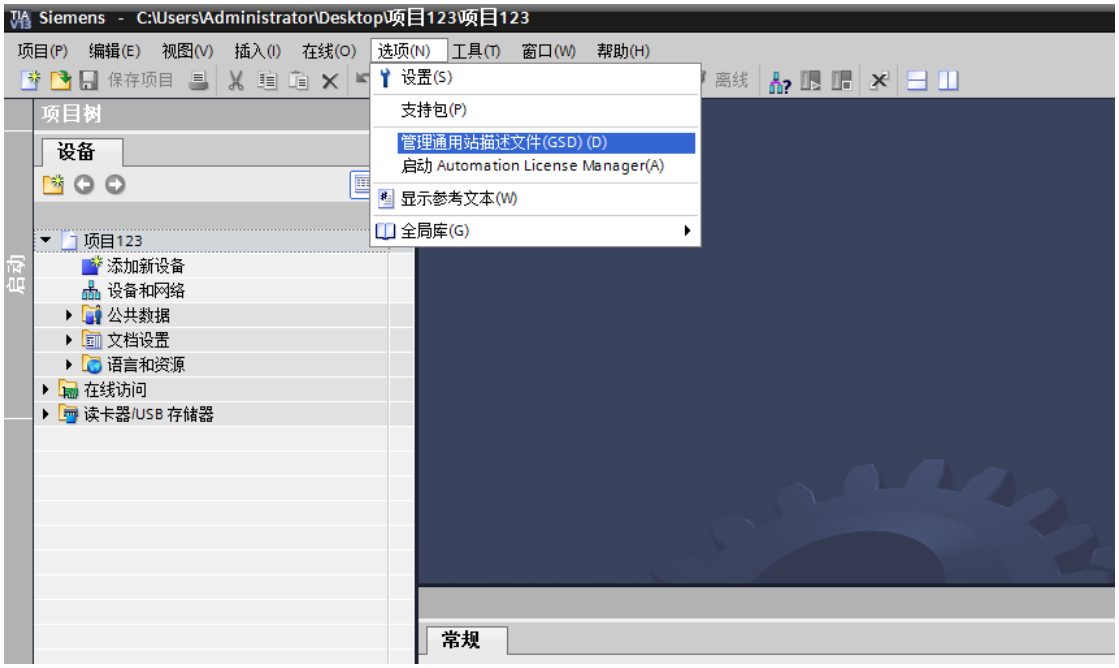
（2） 通信控制字

D7	D6	D5	D4-D3	D2	D1	D0
强制复位	停止等待	清除错误	保留	写允许	读允许	启动工作

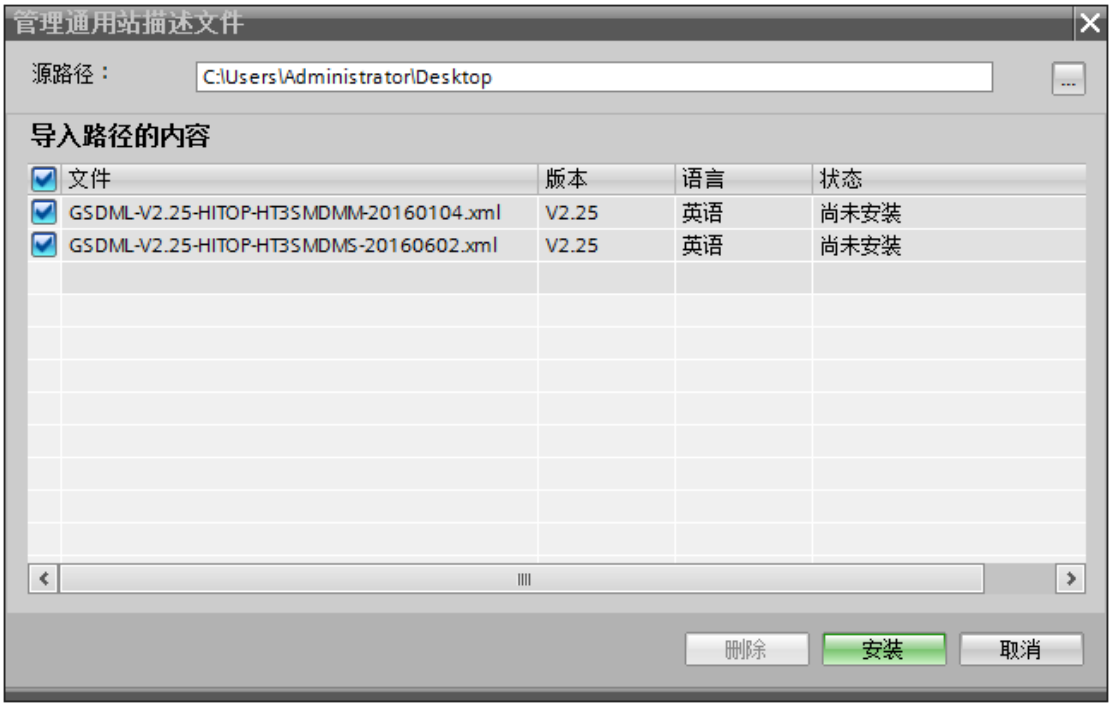
注意：在用户无特殊需求的情况下，不推荐使用其他功能，仅需要将 D0 位置 1，启动网关发送 Modbus 报文即可。

5.2 网关作为 MODBUS 主站

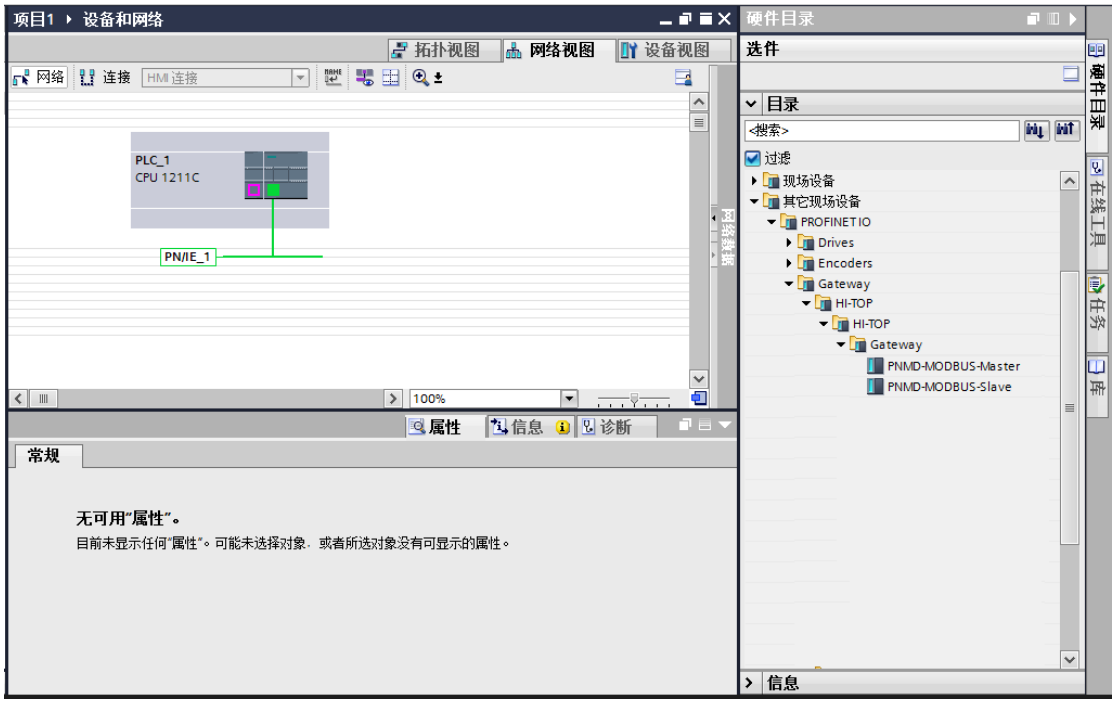
（1） 在博途中新建一个项目，通过“选项”——“管理通用站描述文件”添加网关的 GSD 文件。



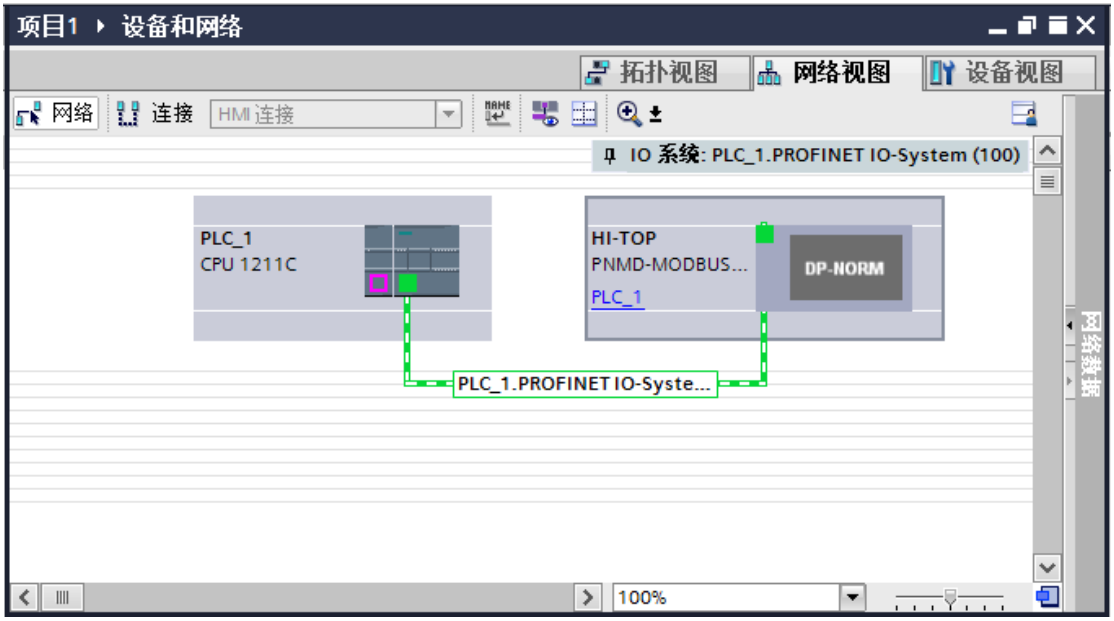
选择 GSD 文件所在的目录，点击安装：



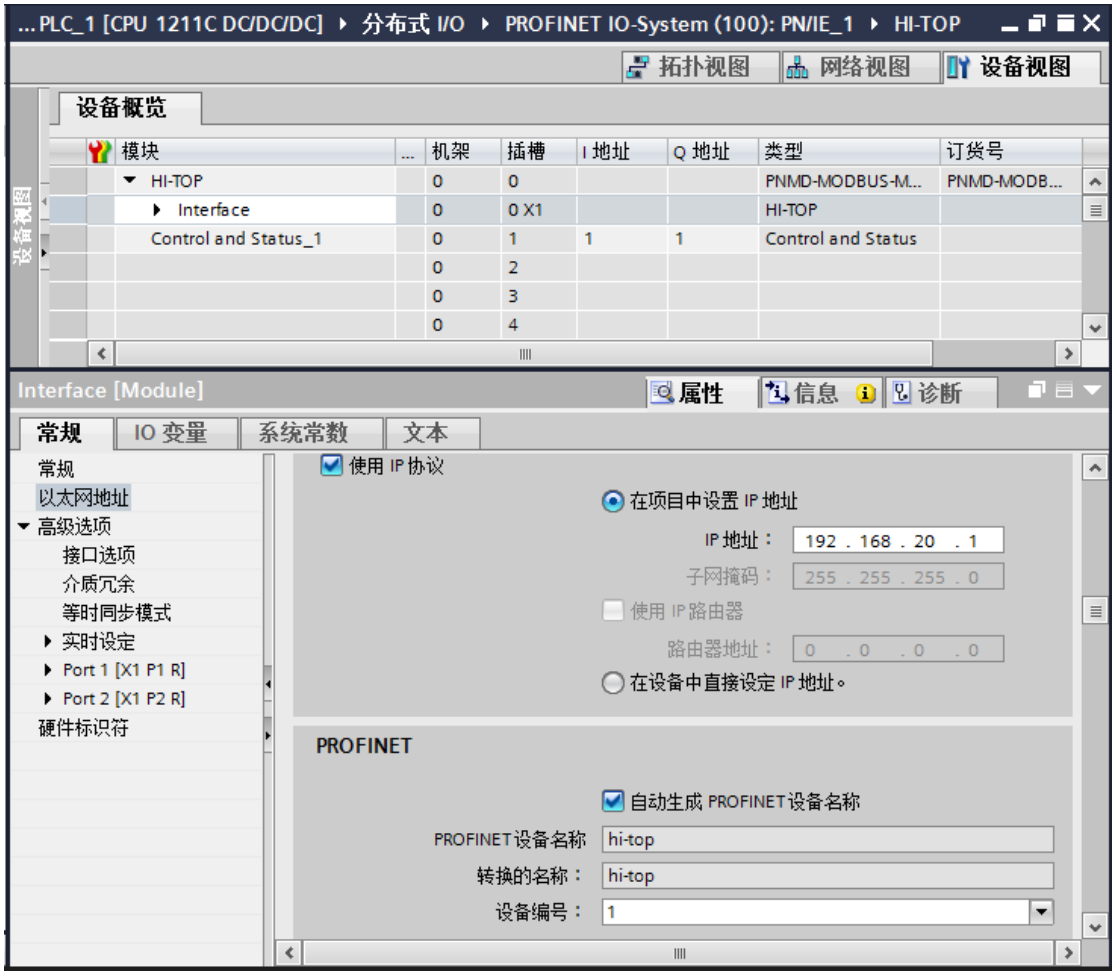
（2） 在“设备和网络”中添加网关



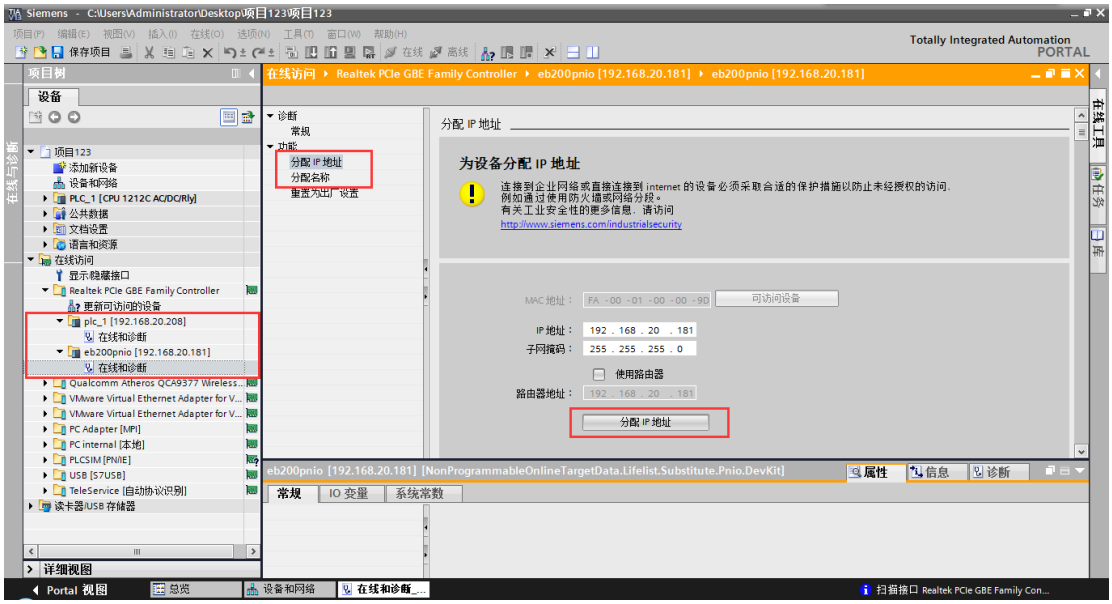
（3） 给网关分配 PLC，构建 Profinet 链接



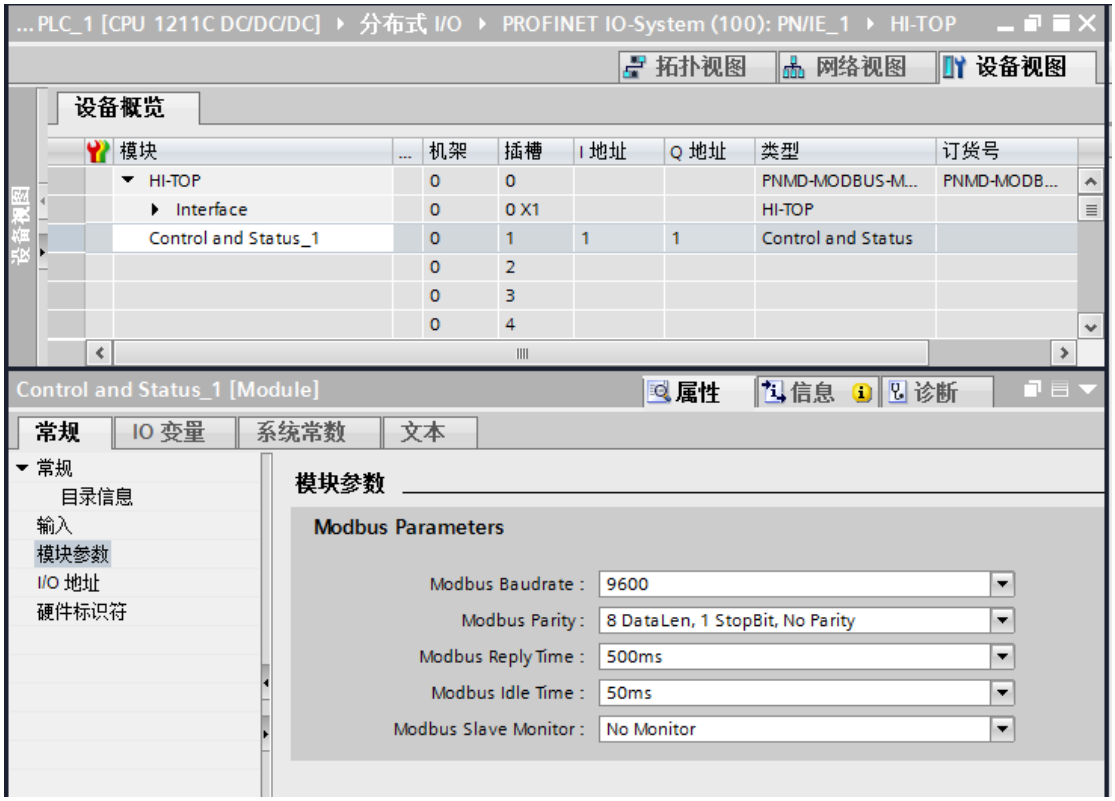
（4） 双击网关的图标，进入设备视图，设置网关的 IP 地址、子网掩码、设备名称。



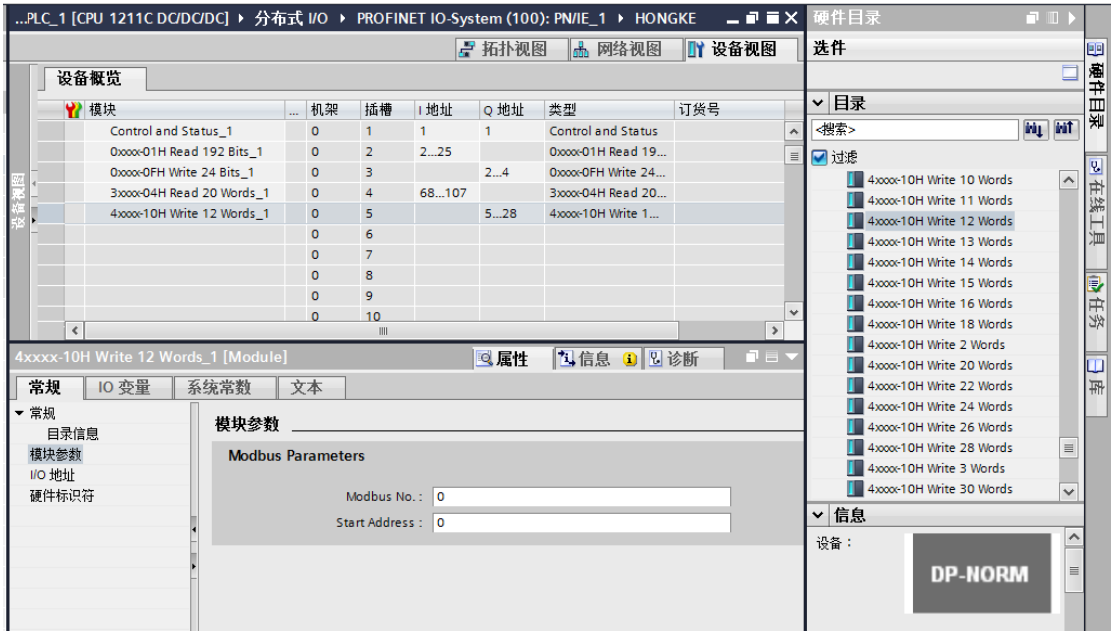
（5） 在线访问----修改实际 PLC 和网关的 IP 地址和名称（IP 地址要和实际的 PLC 地址在同一网段，名称要和网关一致）



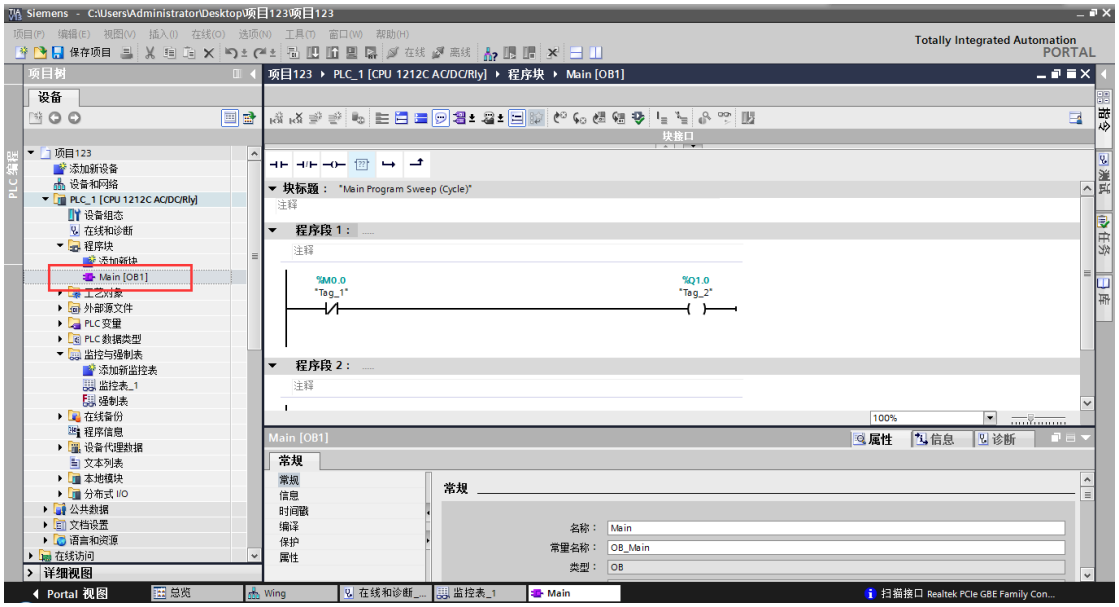
（6） 设置网关参数（包含 MODBUS 设备的波特率、发送间隔、等待应答时间、从站状态监测等信息，此处设置的参数要和被连设备实际参数一致）



（7） 配置 MODBUS 读写报文



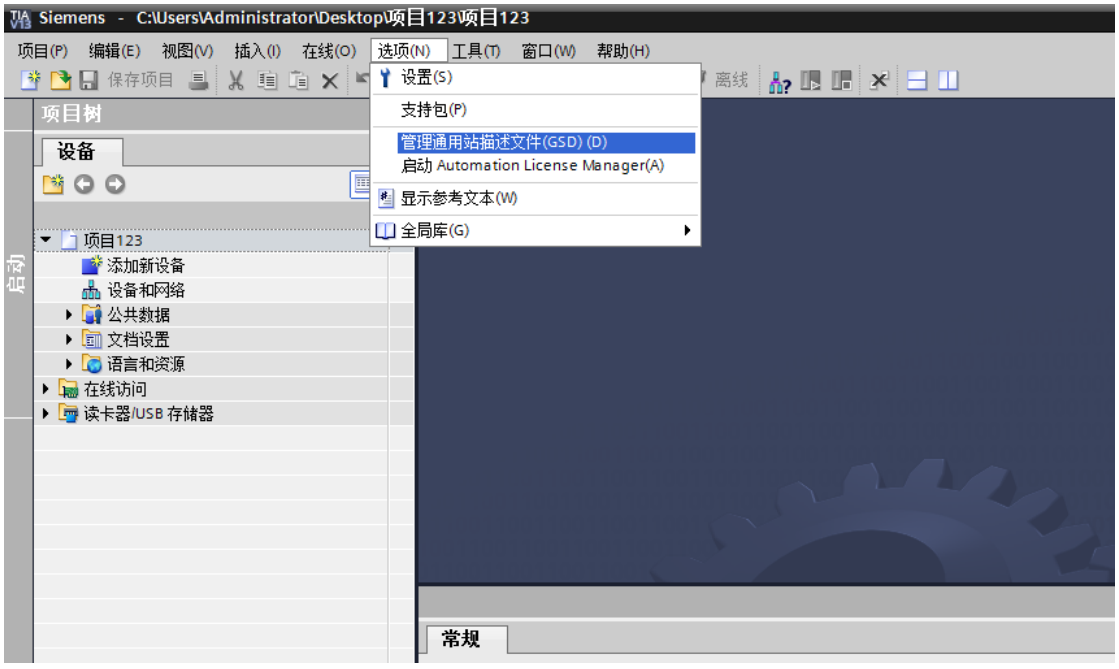
（8） 令网关控制字的最低位置 1



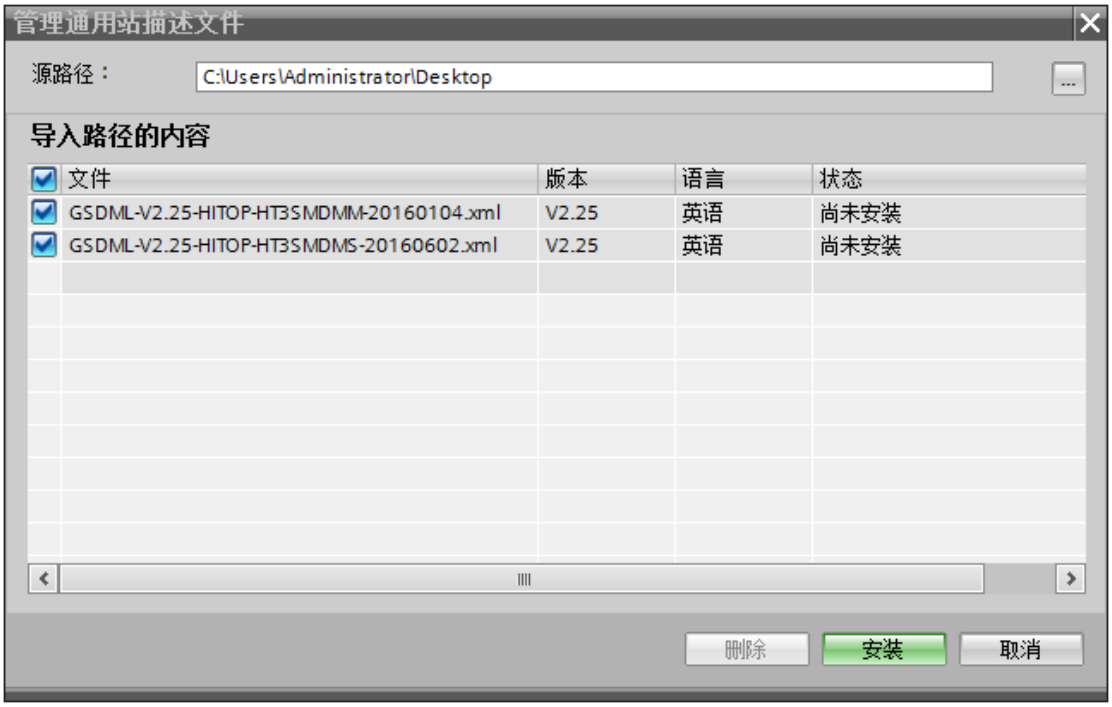
（9） 将程序编译下载即可实现 S7-1200 读写 MODBUS 设备的数据。

5.3 网关作为 MODBUS 从站

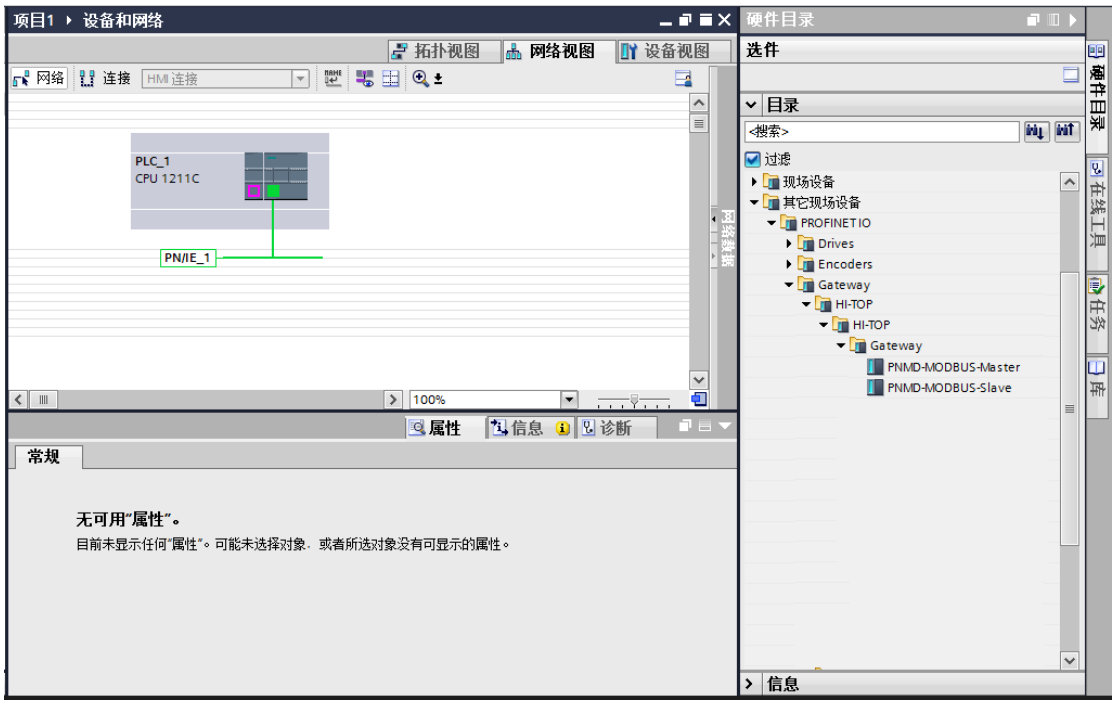
（1） 在博途中新建一个项目，通过“选项”——“管理通用站描述文件”添加网关的 GSD 文件。



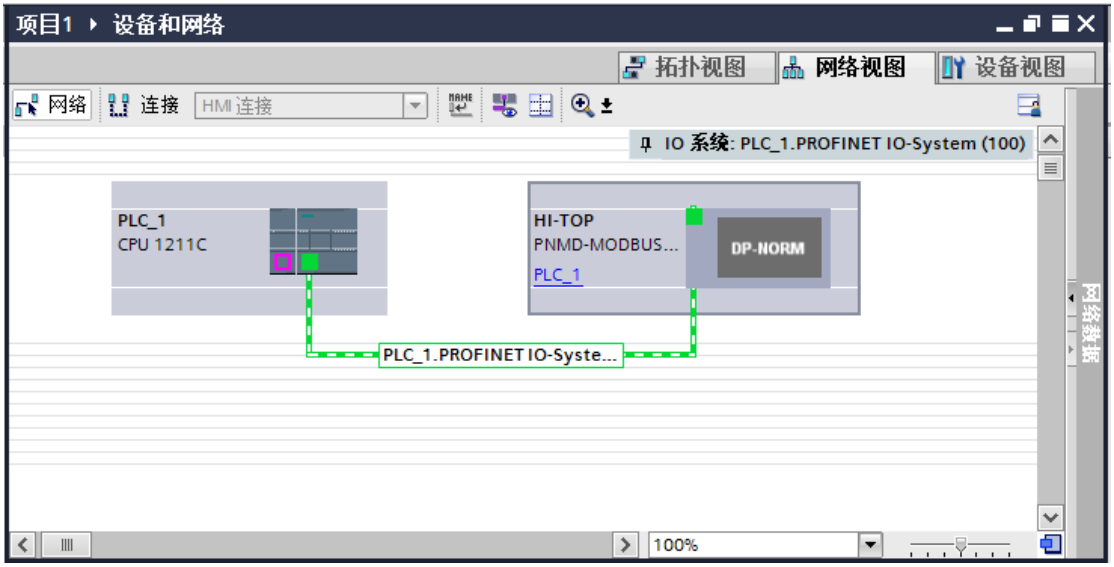
选择 GSD 文件所在的目录，点击安装：



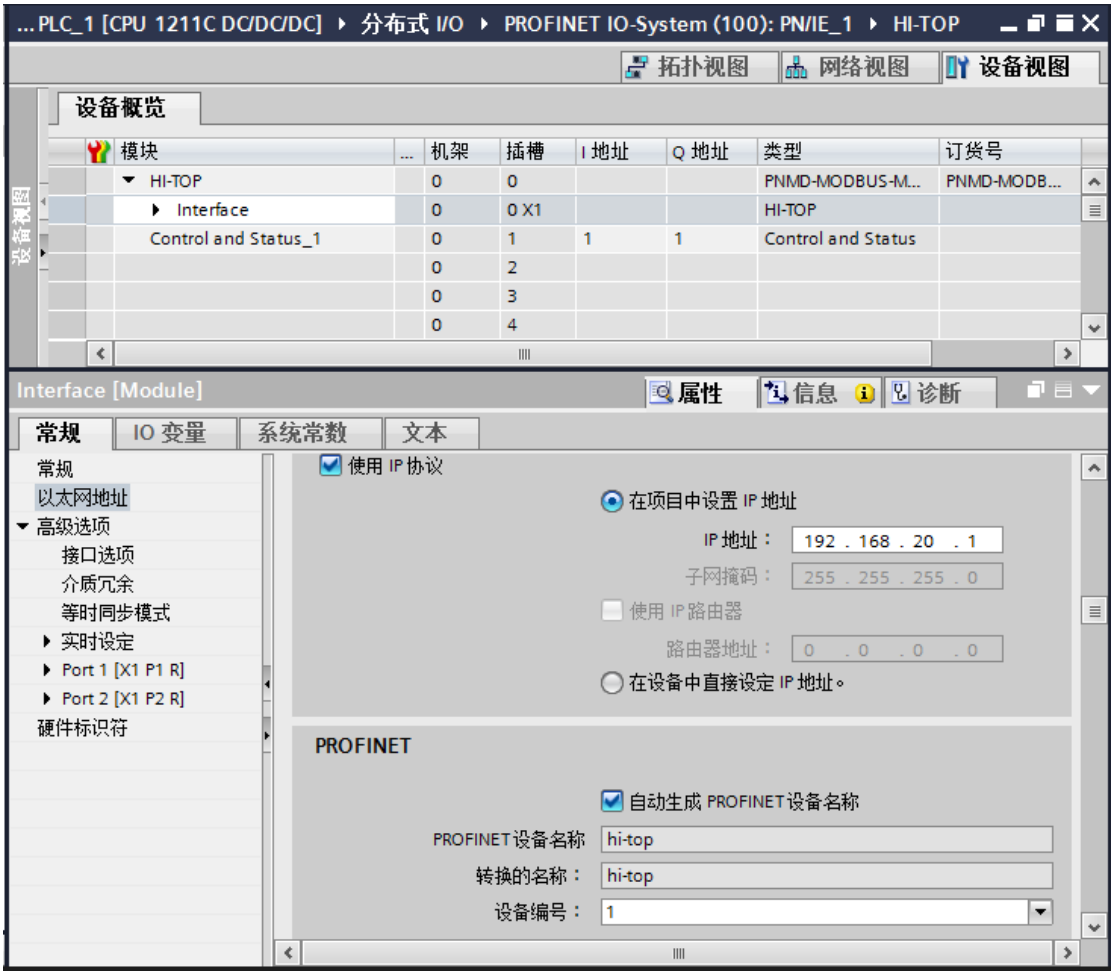
（2） 在“设备和网络”中添加网关



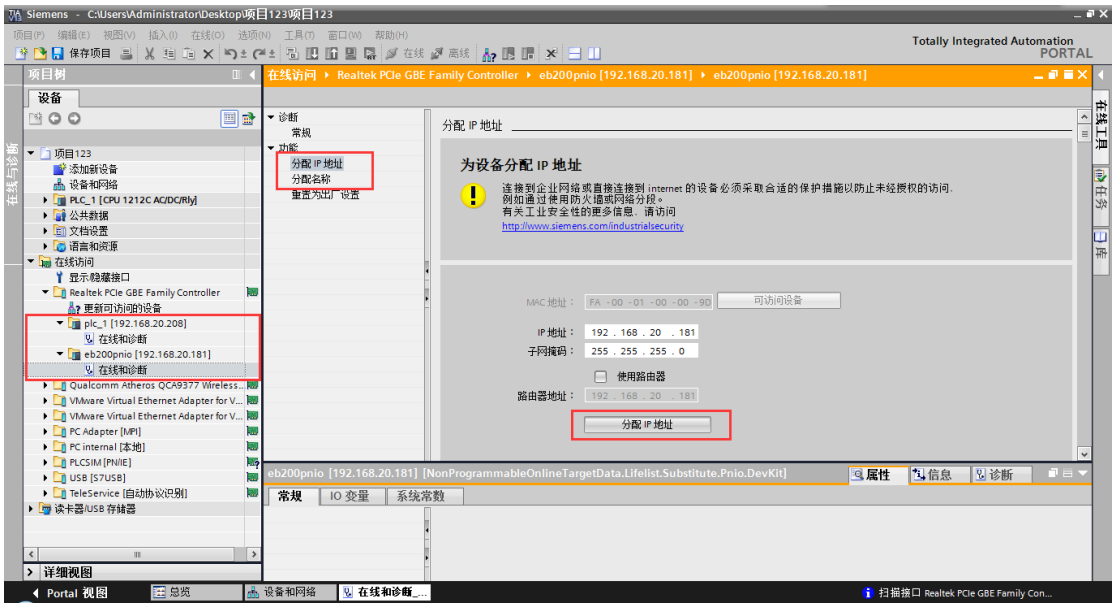
（3） 给网关分配 PLC，构建 Profinet 链接



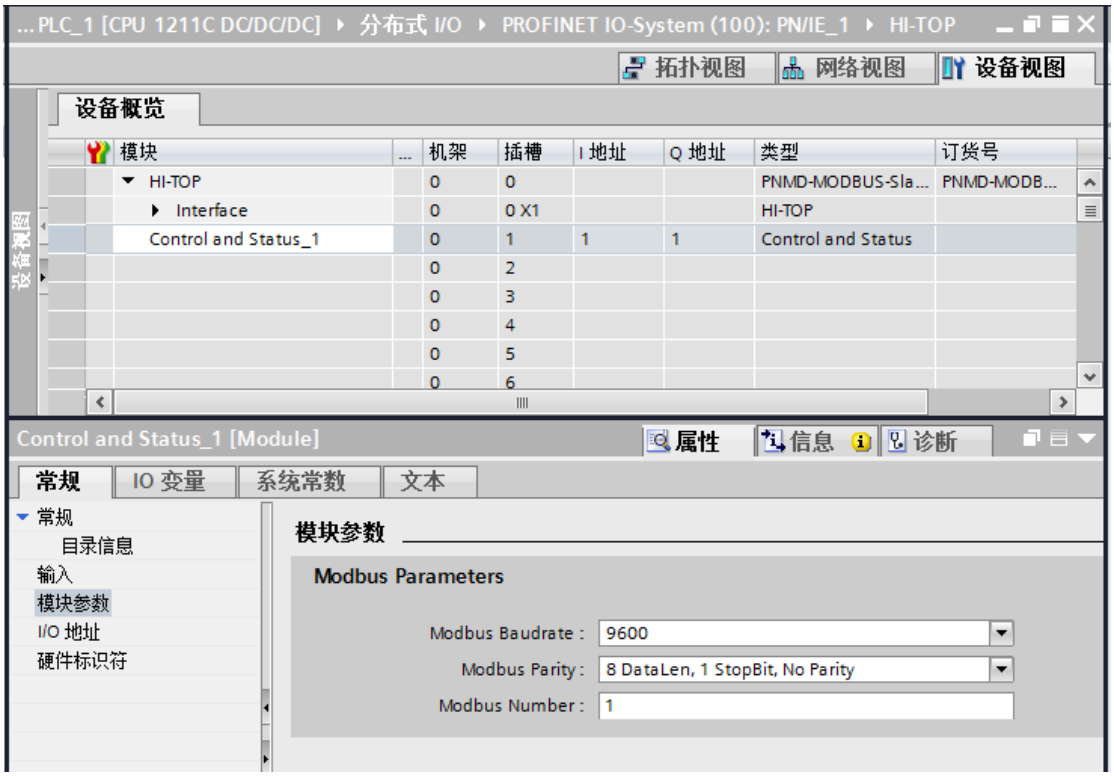
（4） 双击网关的图标，进入设备视图，设置网关的 IP 地址、子网掩码、设备名称。



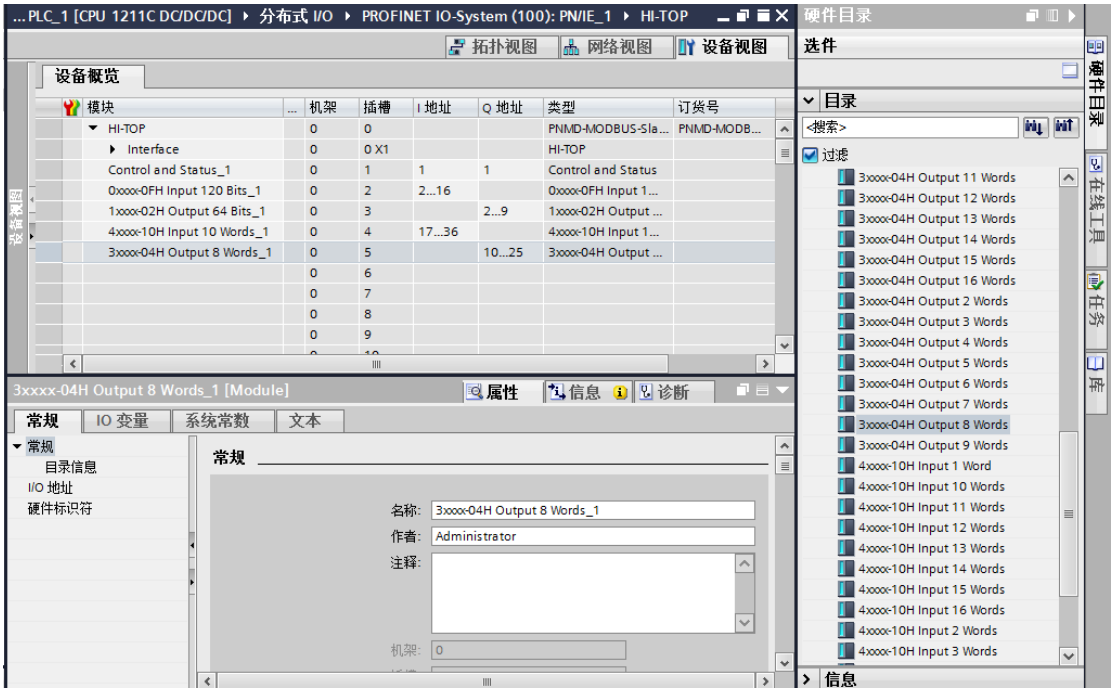
（5） 在线访问----修改实际 PLC 和网关的 IP 地址和名称（IP 地址要和实际的 PLC 地址在同一网段，名称要和网关一致）



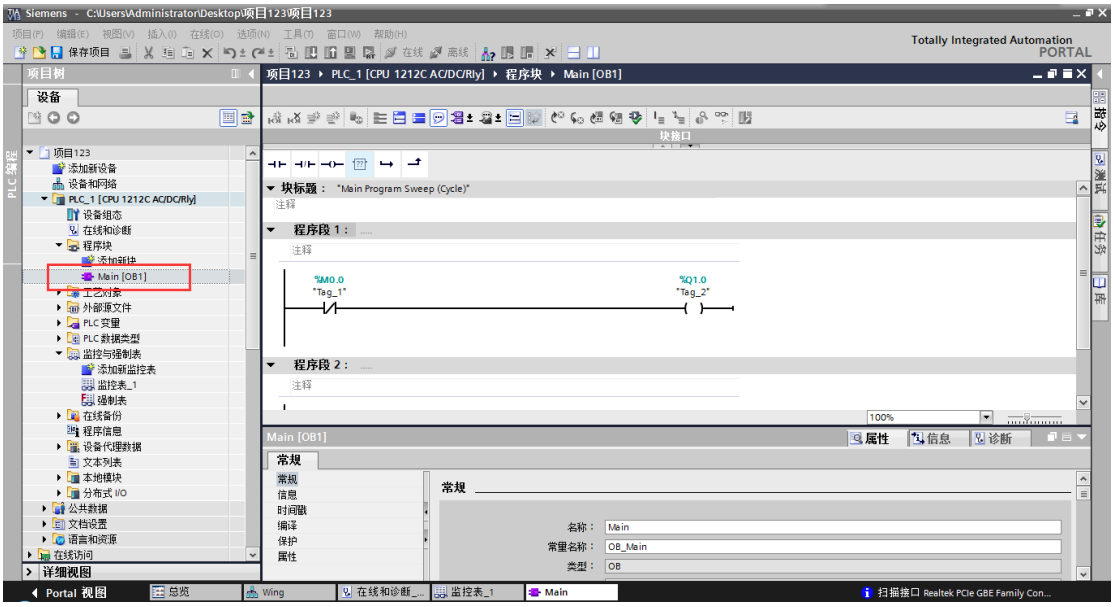
（6） 设置网关参数（包含 MODBUS 设备的波特率、校验位、站号等信息）



（7） 配置 MODBUS 数据区



（8） 令网关控制字的最低位置 1



（9） 将程序编译下载即可实现 S7-1200 读写 MODBUS 设备的数据。