PROFINET 到 MODBUS 协议网关

PN-G-MODBUS 产品手册

北京鼎实创新科技股份有限公司

2019-10

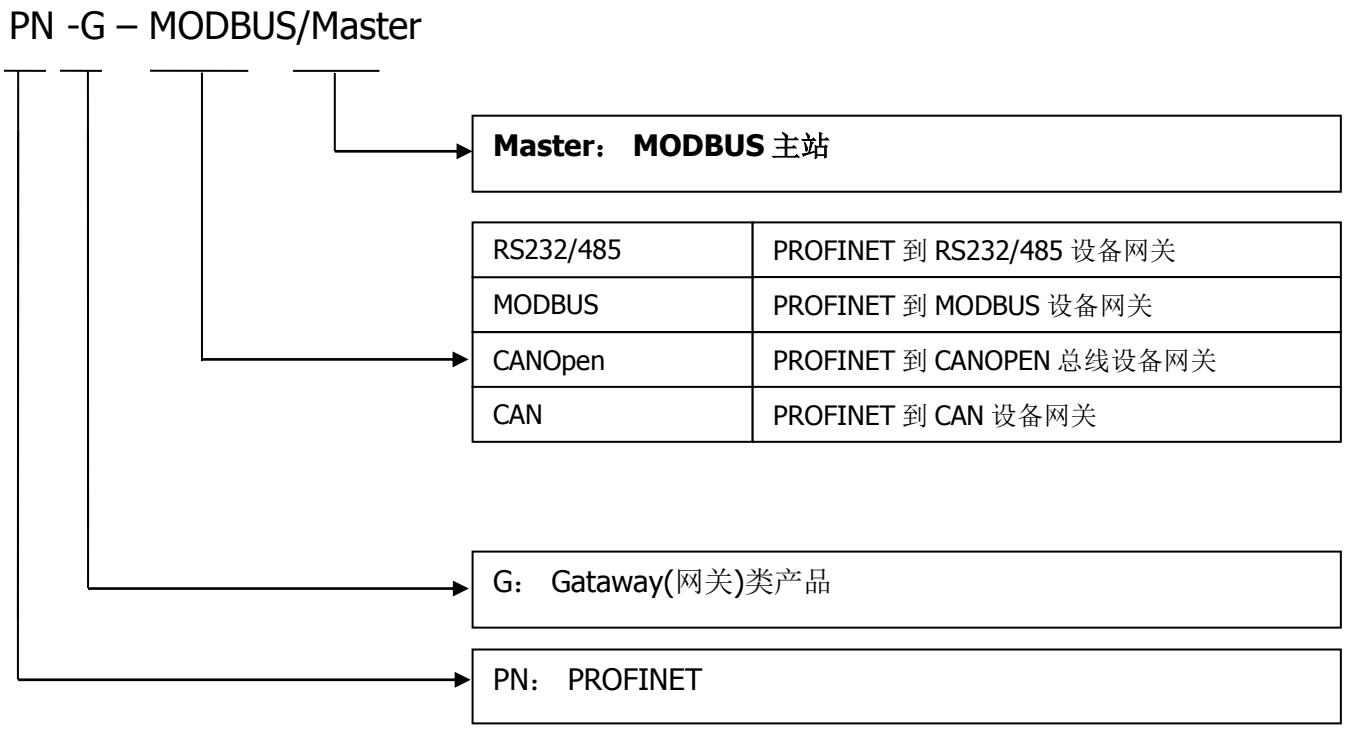
目录

第一章 产品概述

一、产品主要用途

1、产品系列

PN-G-MODBUS 接口（以下有时简称“接口”）是 PROFINET 网关 Gataway (网关)系列中的产品，本产品手册适合 PN-G-MODBUS 类型产品。



2. PROFINET 网关系列产品主要用途

将具有 RS232/485、 MODBUS、CAN 以及 CANOPEN 等专用通信协议的接口设备连接到 PROFINET 总线上，使设备成为 PROFINET 总线上的一个从站。见图 1-1，应用网关 PN-G-XXXX 将设备连接到 PROFIBUS 总线上。

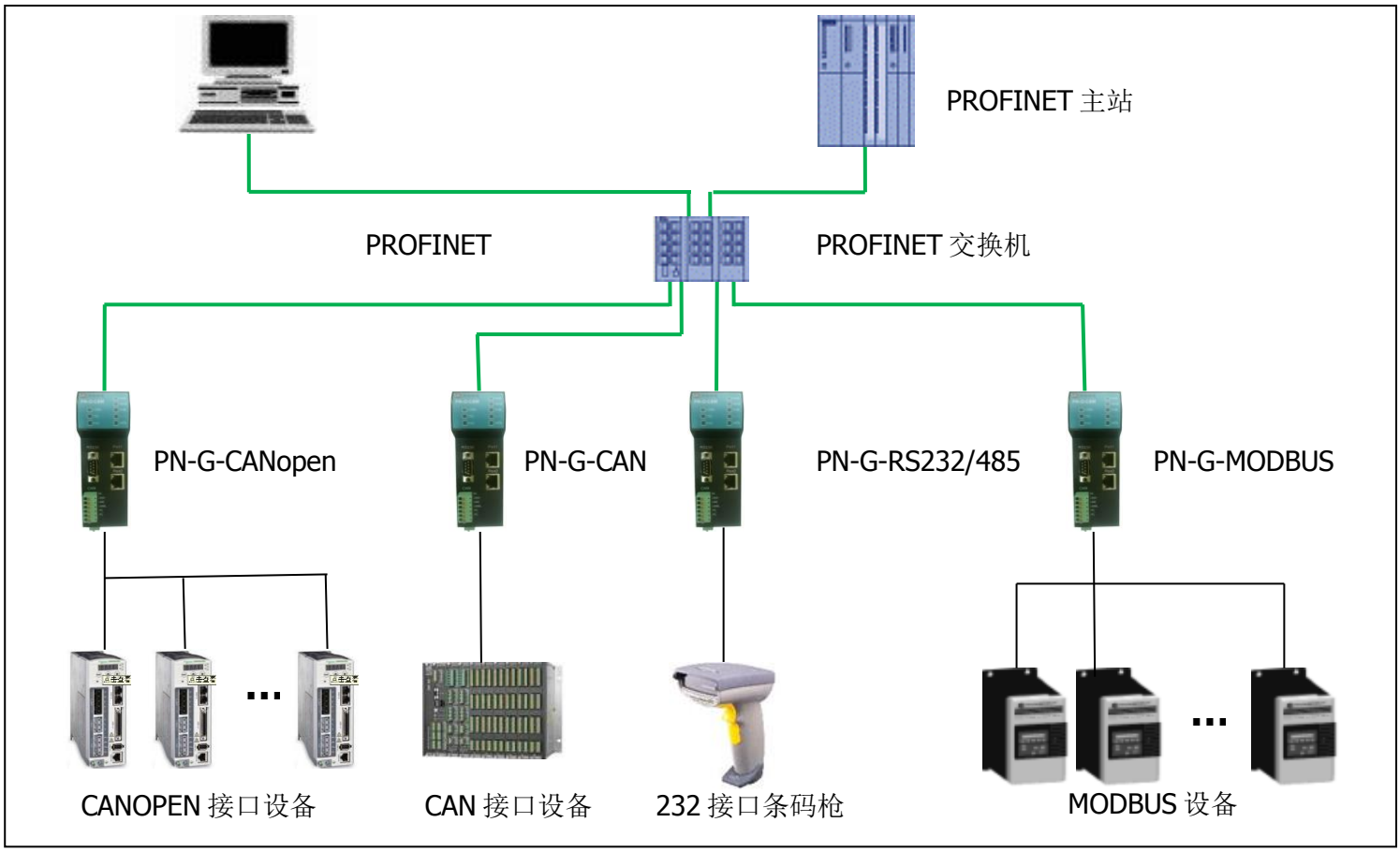


图 1-1 具有不通通讯协议的设备与 PROFINET 总线的连接

二、产品特点

▼**应用广泛：**凡具有 RS232/485 接口，标准 MODBUS RTU 协议的设备都可以使用本产品实现与现场总线 PROFINET 的互连。如：具有 MODBUS 协议接口的变频器、电机启动保护装置、智能高低压电器、电量测量装置、各种变送器、智能现场测量设备及仪表等等。

▼**应用简单：**用户不用了解 PROFINET 和 MODBUS 技术细节，用户只需参考本手册及提供的应用实例，根据要求完成配置，不需要复杂编程，即可在短时间内实现连接通信。

▼**透明通信：**用户可以依照 PROFINET 通信数据区和 MODBUS 通信数据区的映射关系，实现 PROFINET 到 MODBUS 之间的数据透明通信。

▼**通讯稳定可靠：**产品通过 PROFINET 认证、符合 EMC 标准 IEC61131-2，抗干扰能力强。

三、技术指标

1、PN-G-MODBUS 接口在 PROFINET 侧相当于 PROFINET 网络中的 Device（与 Controller 相对应），在 MODBUS 一侧既可做 MODBUS 主站，也可做 MODBUS 从站；接口通过 PROFINET 通信数据区和 MODBUS 数据区的数据映射实现 PROFINET 和 MODBUS 的数据透明通信。

2、两个 RJ45 以太网接口，支持 100BASE-TX，MDI/MDIX 自侦测, 集成以太网交换机，方便将 PROFINET 设备组成菊花链。

3、ROFINET/V2.2 协议，网关 PROFINET 侧采用实时（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。

4、电磁兼容指标：

EFT： level 4; class A

浪涌： level 2; class A

静电：level 3 ;class A

5、支持 Modbus RTU 协议,支持 01H、02H、03H、04H 、05H、06H、0FH、10H 功能码。

6、MODBUS 协议接口为标准 RS232 或 RS485 接口，半双工；

波特率：300、600、1200、 2400、4800、9600、19.2K、38.4K、57.6K 可选；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)可选。

7、最大输入/输出数据量：

① Input Bytes + Output Bytes ≤312 Bytes

② Max Input Bytes ≤312 Bytes

③ Max Output Bytes ≤312Bytes

8、可配置条数≤40 条

9、电源电压：24 VDC(±20%)，双路电源冗余供电。

10、额定功率 3W（24V/125mA）。

11、环境温度：

运输和存储：-40℃~+70℃

工作温度：-25℃~+55℃

12、工作相对湿度：5~95%（无结露）

13、外形尺寸：（宽）45mm×（高）125mm×（厚）118mm

14、安装方式：35mm 导轨

15、防护等级：IP20

16、重量：约 290g

第二章 产品外观、安装、启动

一、产品布局

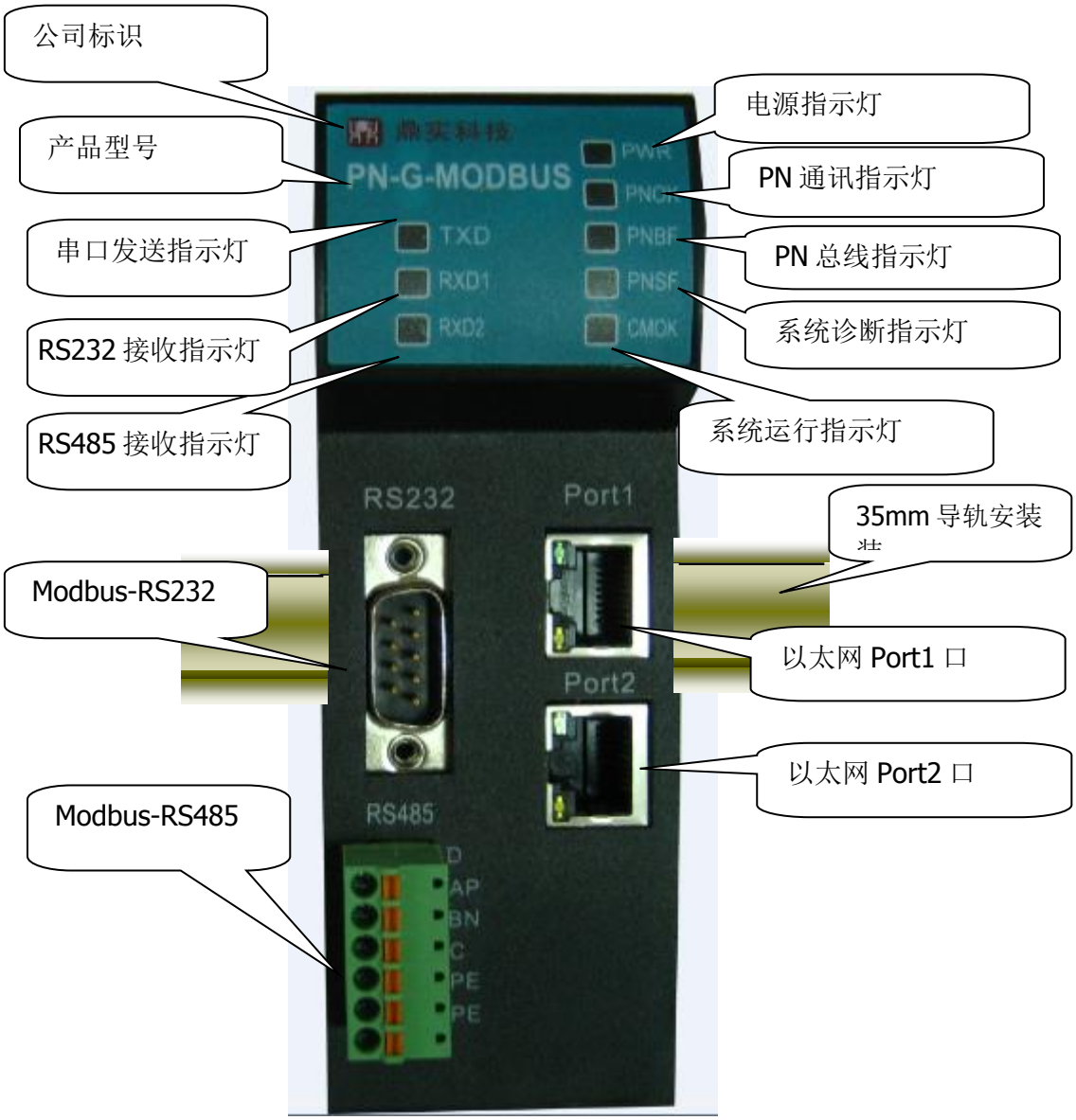


图 2-1 产品正

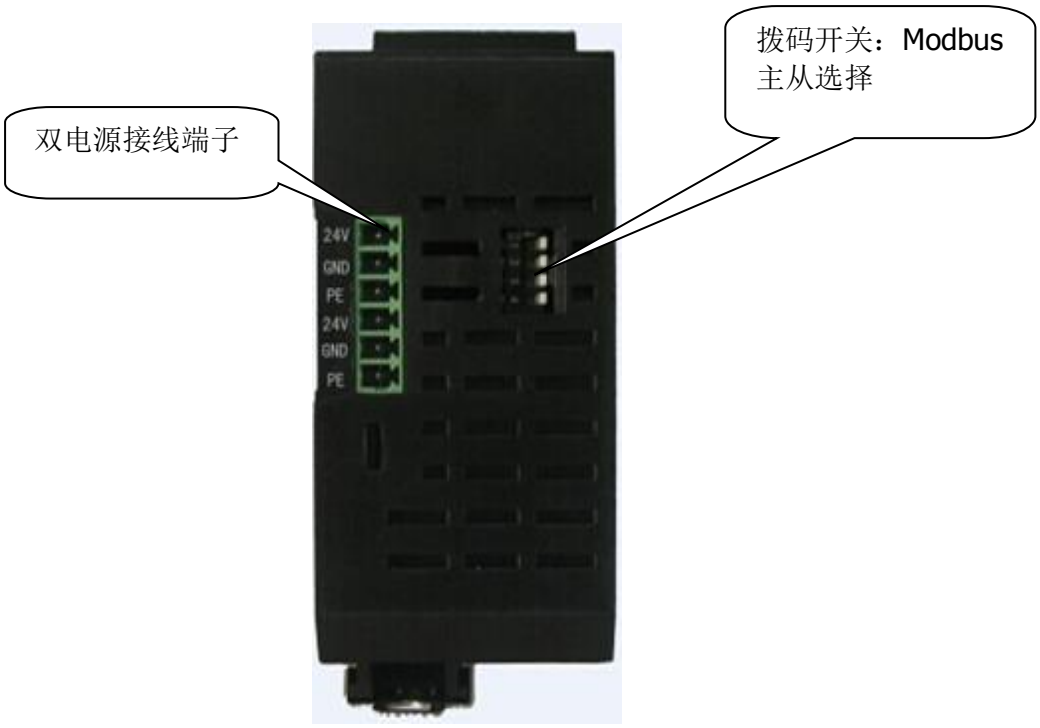


图 2-2 产品底部

二、外形尺寸

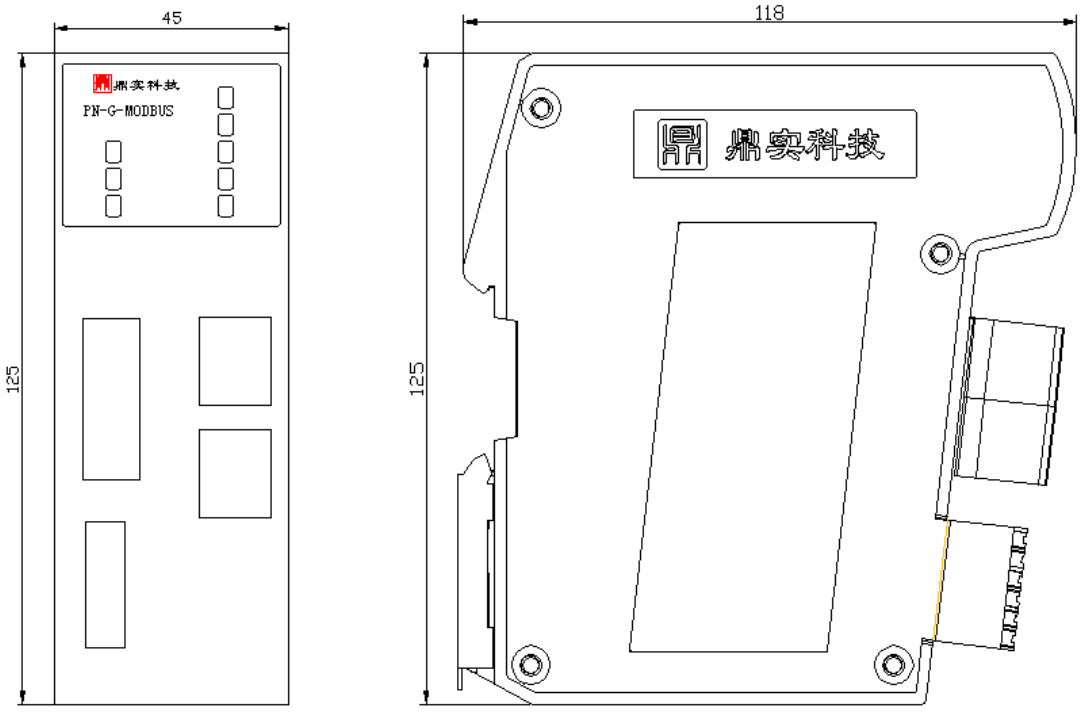


图 2-3 外形尺寸（单位：mm）

三、接口

1、电源

(1).采用双路电源冗余供电；

(2).电源拉偏 20%，可正常工作；

(3).额定功率 3W（24V/125mA）。

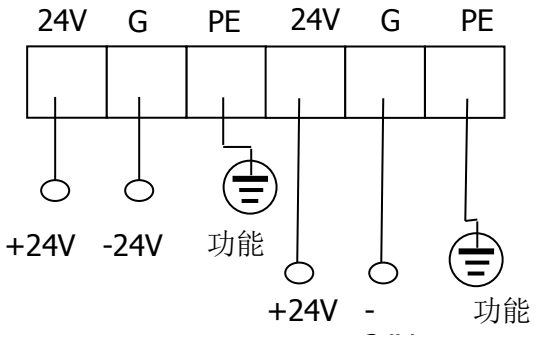


图 2-4 电源接口

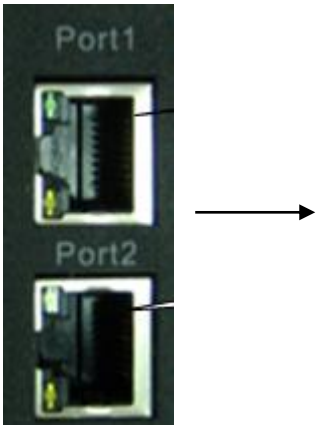
2、PN 端

(1).两个 RJ45 以太网接口，支持 100BASE-TX，MDI/MDIX 自侦测, 集成以太网交换机，方便将 PROFINET 设备组成菊花链；

(2).符合 PROFINET 的 C 类标准，支持 PROFINET2.3 版本；

(3).支持 PROFINET 的 NRT 和 RT 协议；

(4).在 PROFINET 接口端相当于 PROFINET 网络中的 Device（与 Controller 相对应），所有 Slot/subSlot 的输入输出数据总和不超过 312 字节。



1	Tx +
2	Tx -
3	Rx +
4	No Singal
5	No Singal
6	Rx -
7	No Singal
8	No Singal

图 2-5 PN 接口

3、串口端

(1).物理接口： 提供 RS232(DB9 针式接口) 和 RS485(6pin 接线端子)串行接口可选；

(2).可选接入终端电阻、PE 屏蔽。

功能	针号
	1
TXD	2
RXD	3
	4
GND	5
	6
	7
	8
	9

图 2-6 RS232 接口

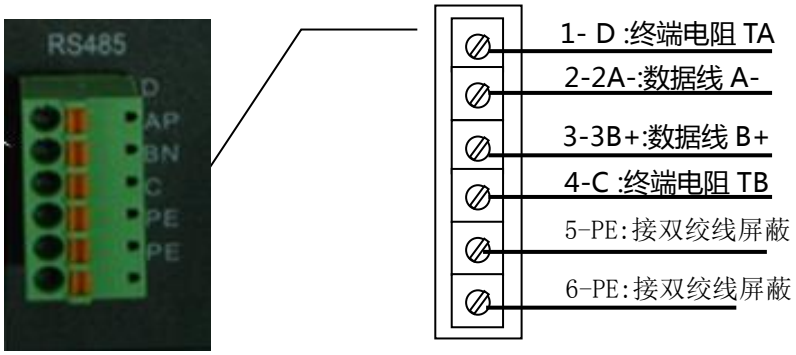


图 2-7 RS485 接口

***PN-G-MODBUS** 作为终端节点时，需要接入终端电阻，此设备内置终端电阻，只需要将端子 **Pin1-2** 和 **Pin3-4** 分别短接即可。**RS232** 接口与 **RS485** 接口不能同时使用。*

四、MODBUS 主从站设置

通过产品底部的拨码开关的第一位 SW1 来设置 PN-G-MODBUS 在 MODBUS 侧做主站还是从站。

SW1=OFF，为 MODBUS 主站模式，即产品做 MODBUS 主站，使用 GSD 文件名称为：“GSDML-V2.3-DingShi-Gateway-ModbusM43-xxxxxxxx.xml“；

SW1=ON，为 MODBUS 从站模式，即产品做 MODBUS 从站，使用 GSD 文件名称为：“GSDML-V2.3-DingShi-Gateway-ModbusS43-xxxxxxxx.xml “。

五、指示灯

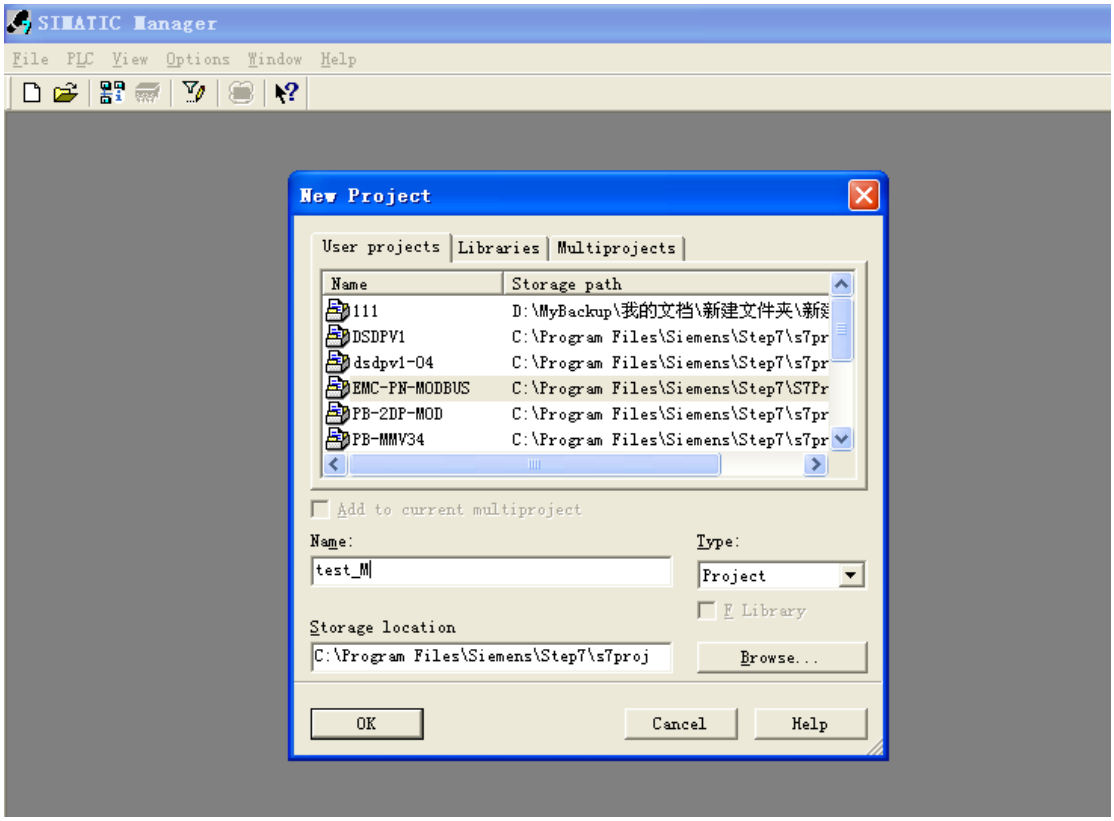
指示灯	状态	含义
TXD(串口发送指示灯)	闪亮	向现场设备发送数据
	灭	没有数据发送
RS232-RXD(RS232 接收指示灯)	闪亮	接收现场设备发送的数据
	灭	没有数据接收
RS485-RXD(RS485 接收指示灯)	闪亮	接收现场设备发送的数据
	灭	没有数据接收
PWR(电源指示灯)	亮	有电源
	灭	无电源
PNOK(PN 通讯指示灯)	亮	PN 控制器与此设备已进入数据交换状态
	灭	没有进入数据交换状态
PNBF(PN 总线指示灯)	常亮	没有总线链接
	闪亮	此设备与 PN 控制器之间正在建立链接
	灭	PN 控制器与此设备之间有一个活动的链接
SF(系统诊断指示灯)		预留
SYS(系统运行指示灯)	亮	系统运行正常
	灭	运行异常

第三章 STEP 7 V5.5 下配置 PN-G-MODBUS

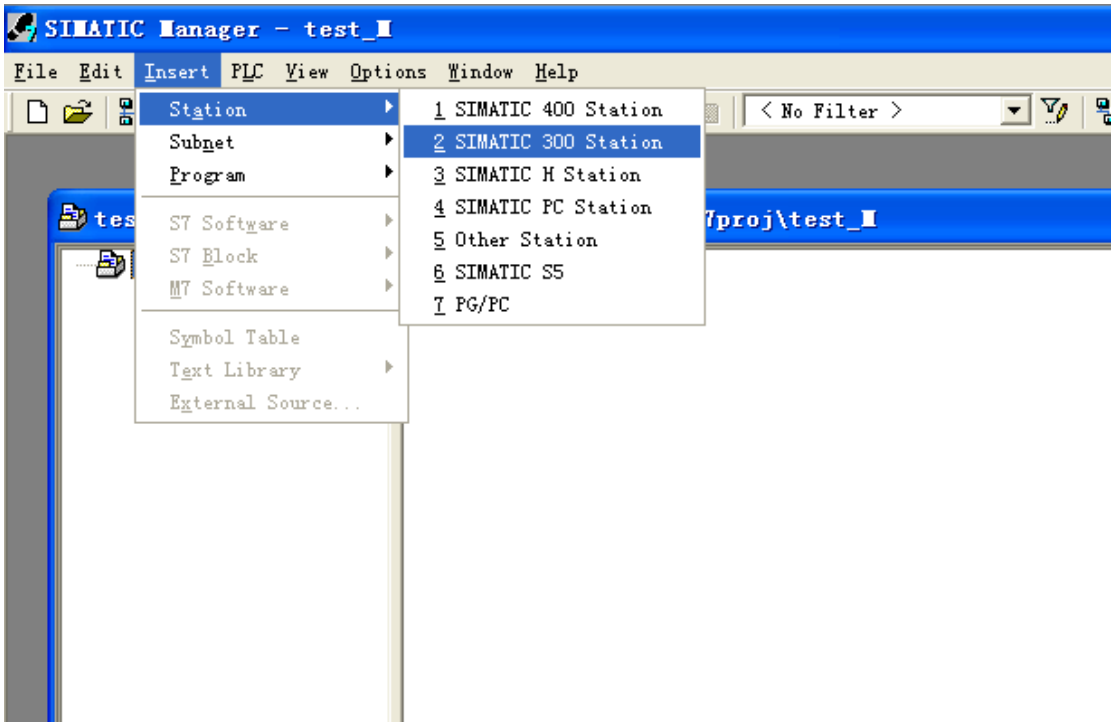
本章将以 SIEMENS 的 315-2 PN/DP 作为 PROFINET 的 Controller，使用 STEP 7 V5.5 作为组态软件，举例说明 PN-G-MODBUS 的配置方法。

一、MODBUS 主站配置

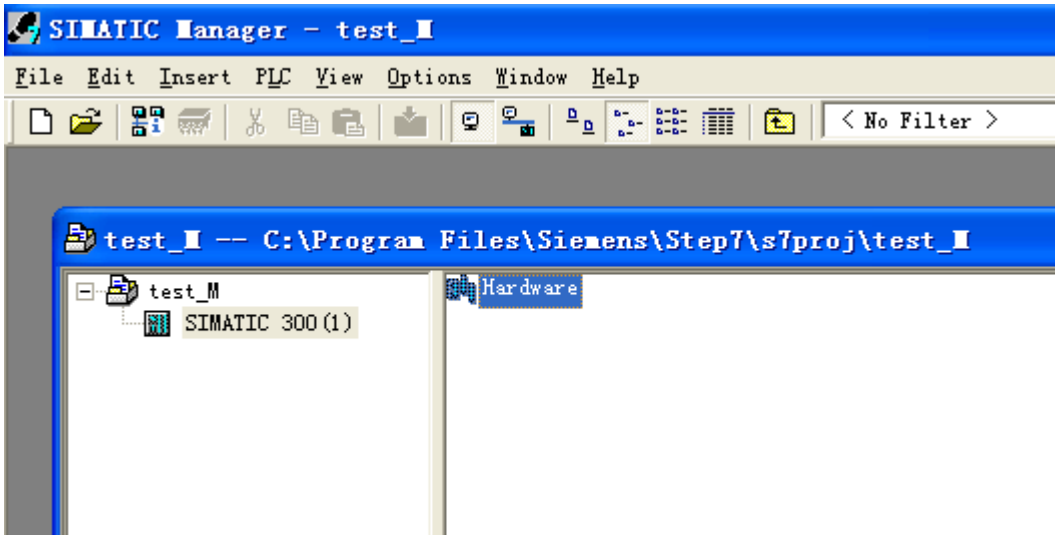
1、打开 STEP 7 软件，点击菜单栏 File→New，新建一个工程，命名为“test_M”。



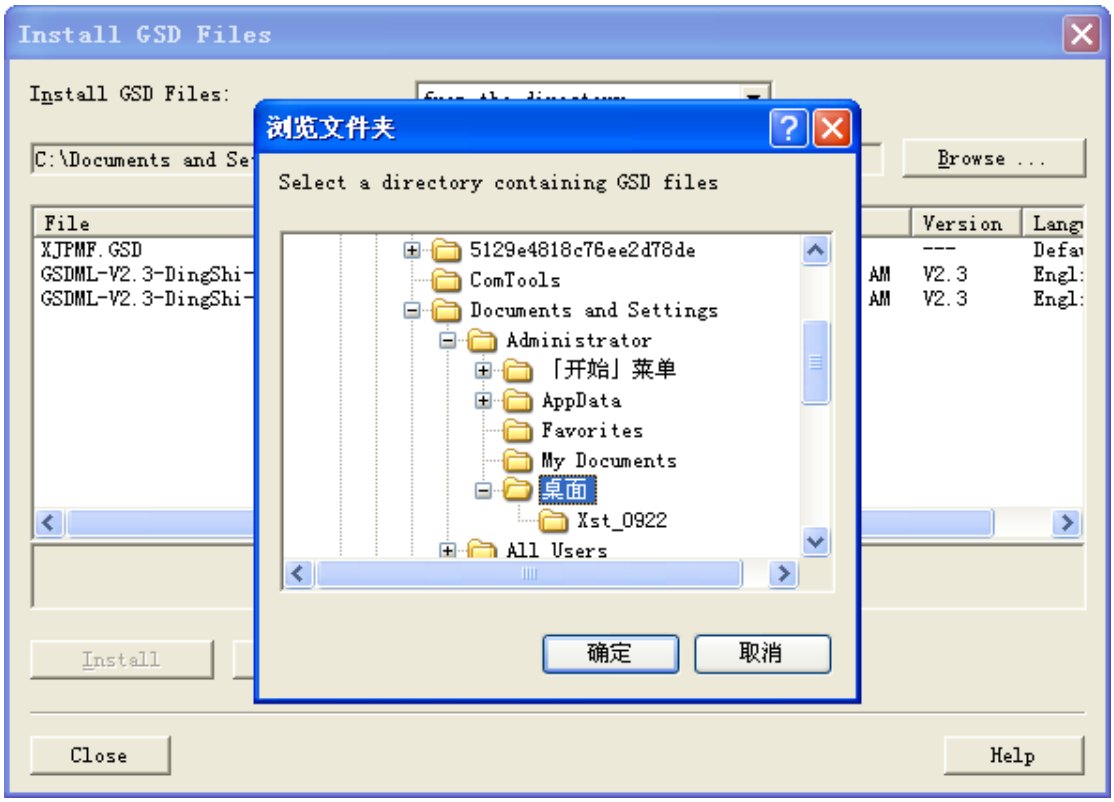
2、添加 300 站点，点击菜单栏 Insert→Station→SIMATIC 300 Station。

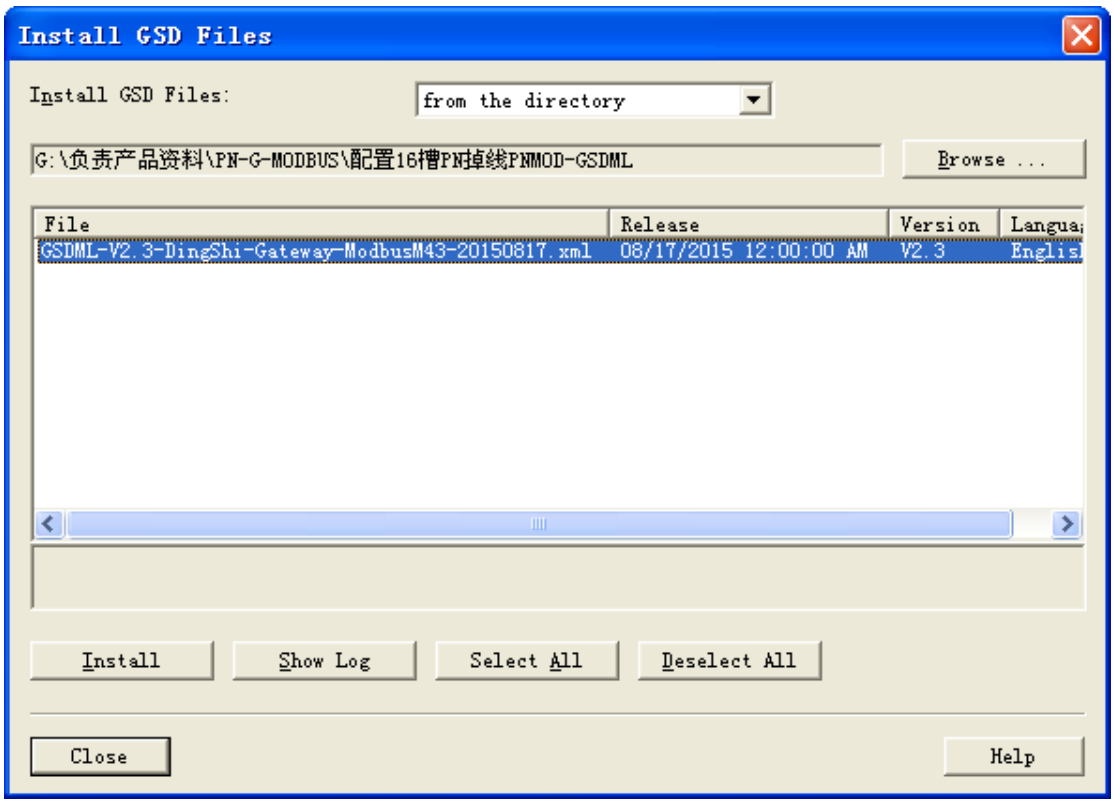


3、SIMATIC 300(1)→Hardware 双击，打开硬件组态。

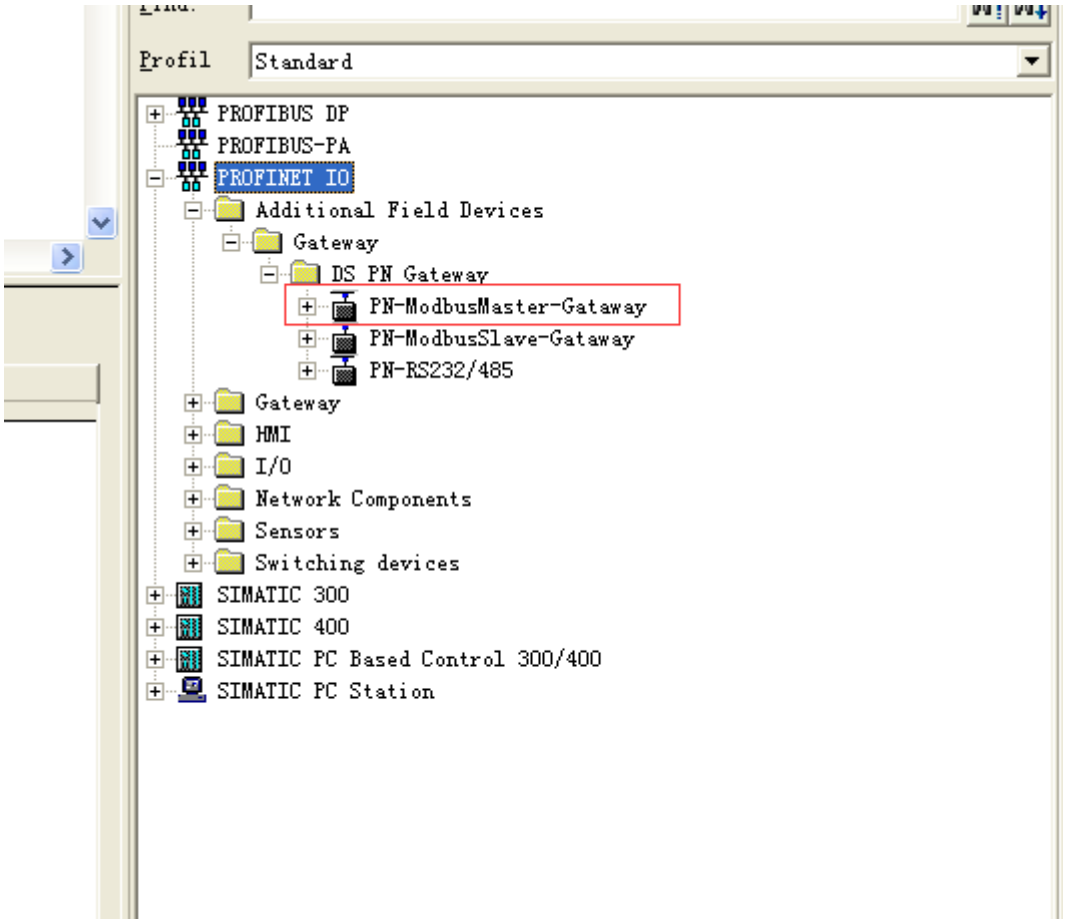


4、在硬件组态界面，点击 Option→Install GSD Files，选择路径，找到“GSDML-V2.3-DingShi-Gateway-ModbusM60-20170817.xml”，添加 GSD 文件。添加 GSD 文件成功后，点击 close 退出添加 GSD 对话框。

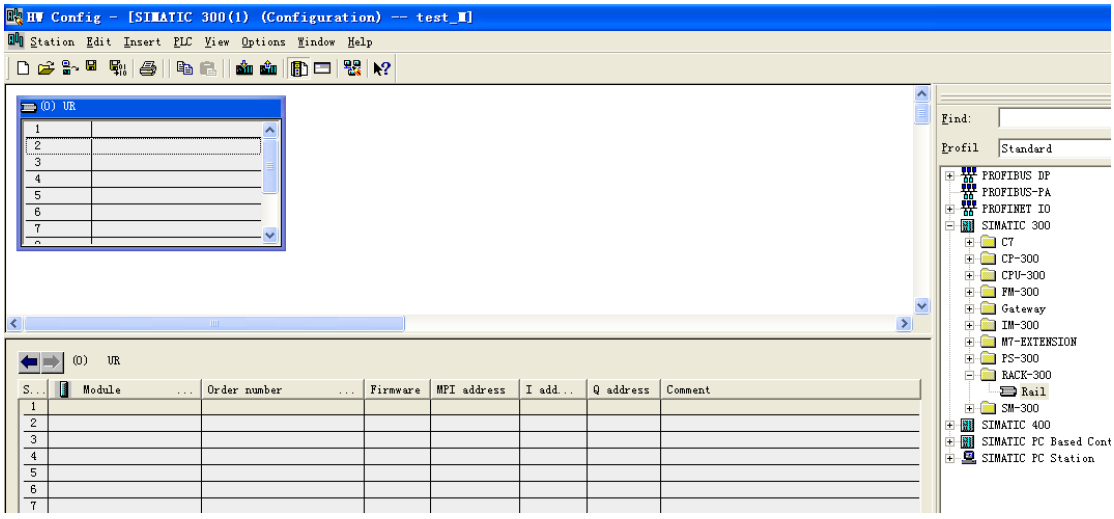




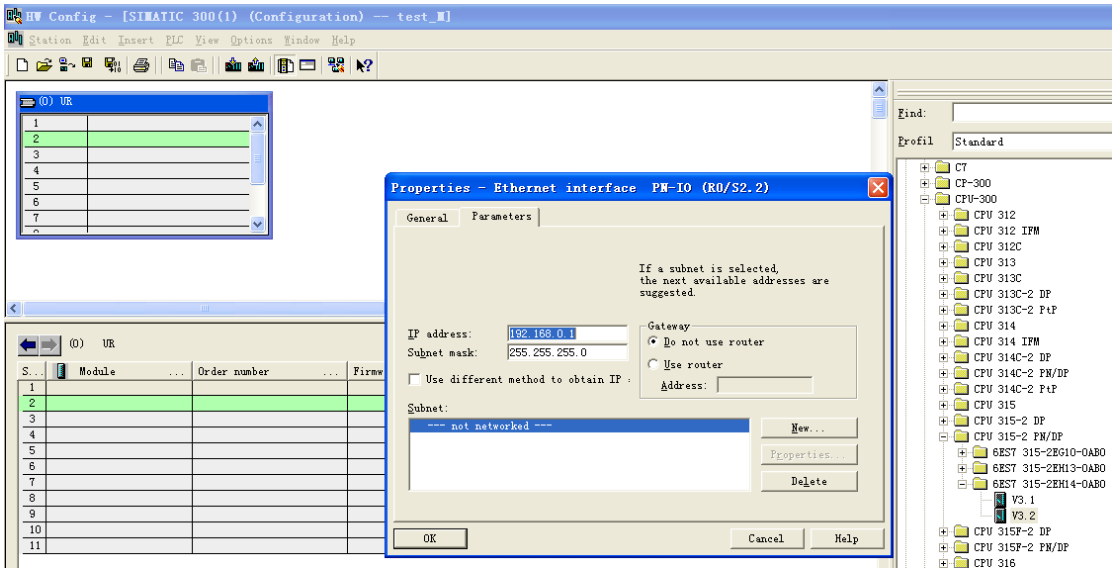
在设备目录里点开 PROFINET IO→Additional Field Devices→Gateway→DS PN Gateway，找到“PN-ModbusMaster-Gateway”，说明 GSD 文件添加成功。



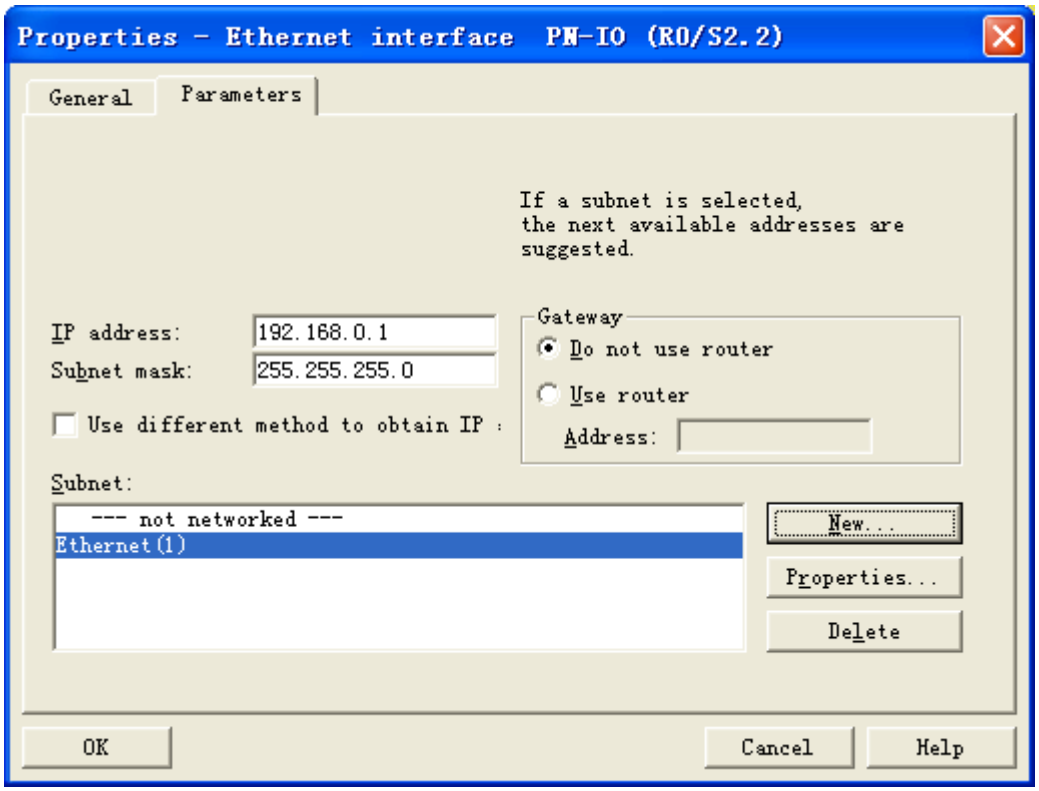
5、添加机架，在设备目录里点开 SIMATIC 300→RACK-300→Rail 双击

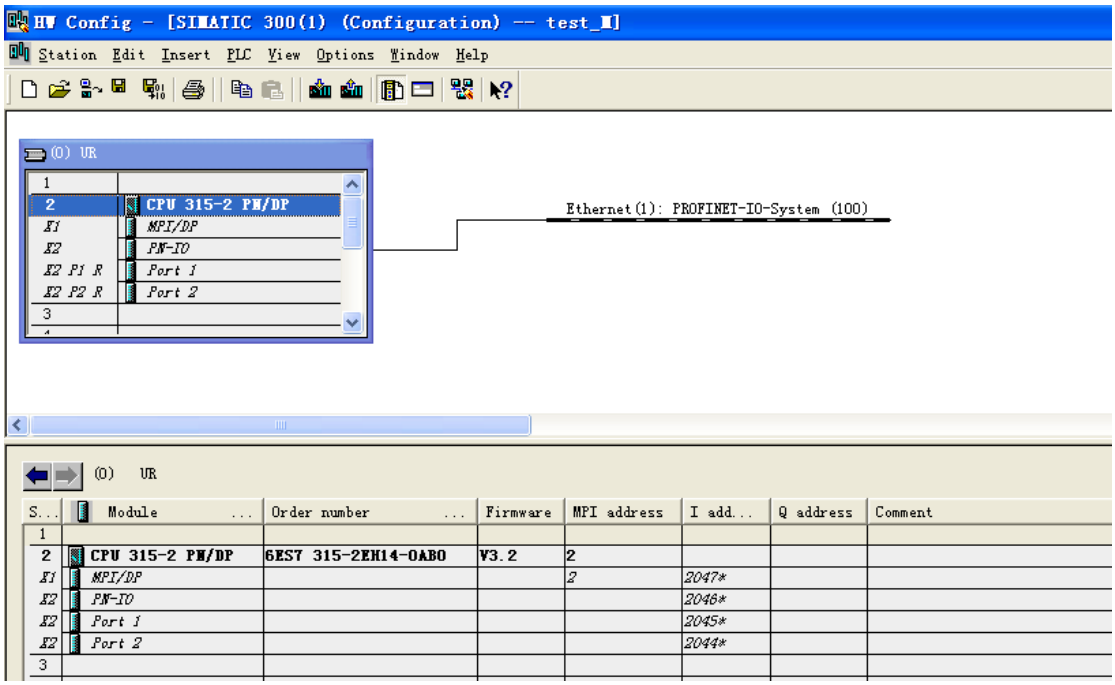


6、配置 CPU，本例以 315-2 PN/DP 为例，选择相应型号的 CPU。选中中机架 UR 2 槽，在设备目录中点开 SIMATIC 300→CPU-300→CPU 315 – 2 PN/DP→6ES7 315-2EH14-0AB0→V3.2 双击 ，并设置 CPU 的 IP 地址。

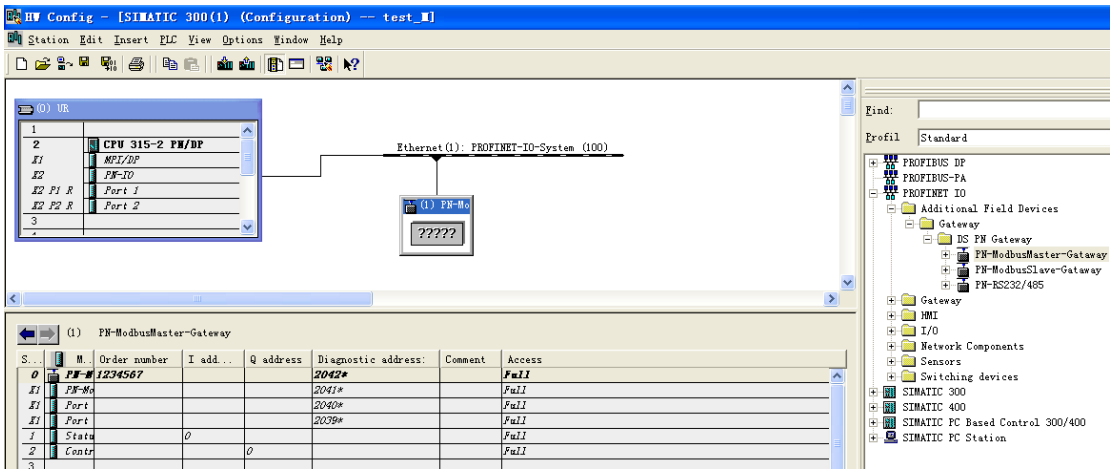


7、配置 PROFINET 总线网络，点击 New，在弹出的对话框中点击 OK，即配置了一条 PROFINET 总线。点击 OK 即可。

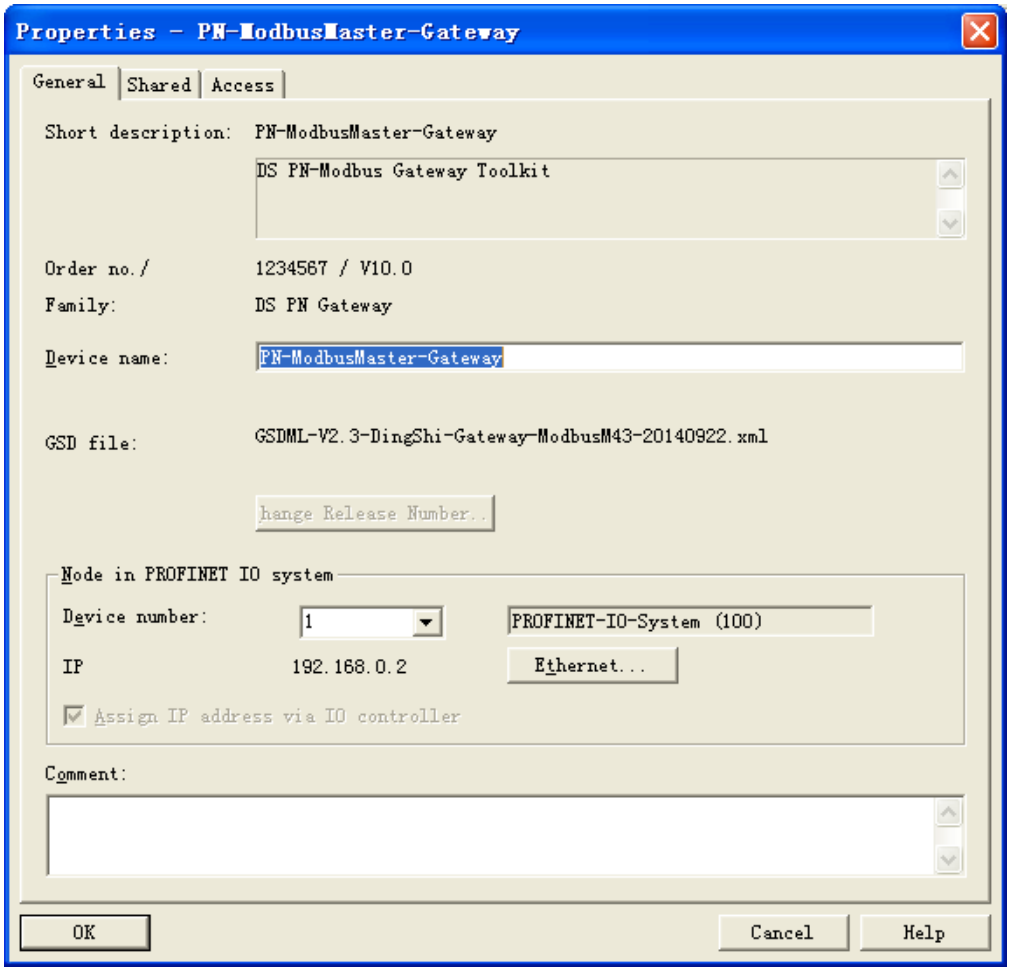


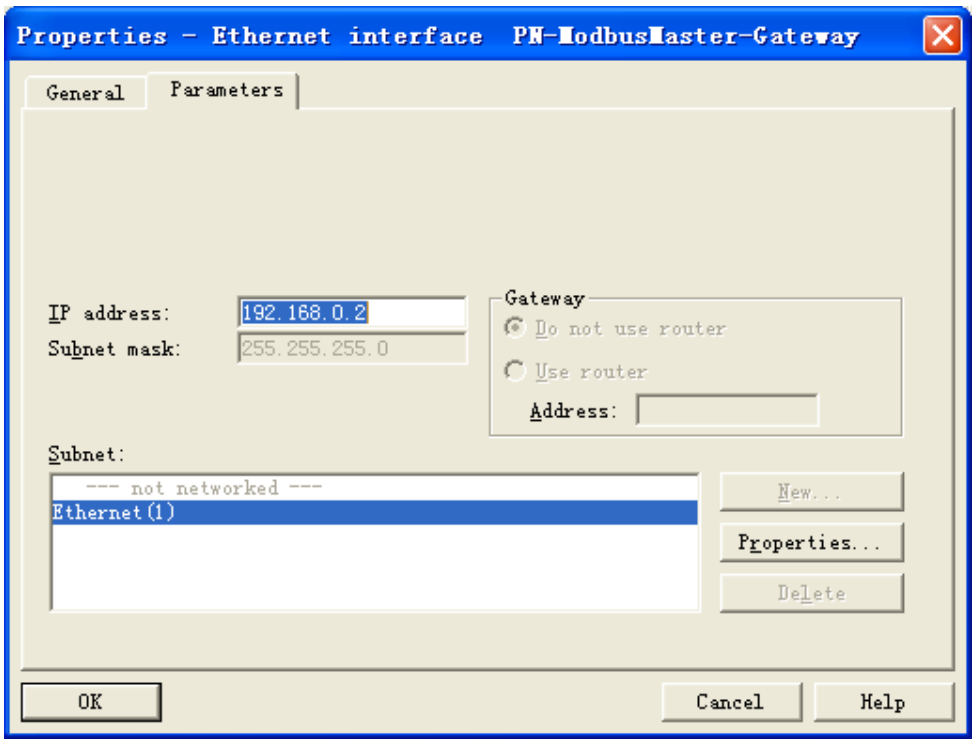


8、选中硬件组态中的总线，使其变成黑色，在设备目录里选择 PN-ModbusMaster-Gateway 双击，在总线上添加了 PN-G-MODBUS 设备。在该模块的配置栏可以看到，该模块会默认占用 2 个字节，一个字节输入，即 Status，1 bytes Input，为该模块的状态字；一个字节输出，即 Control，1 bytes Output，为该模块的控制字。关于状态字和控制字的定义我们会在下一节详细讲解。

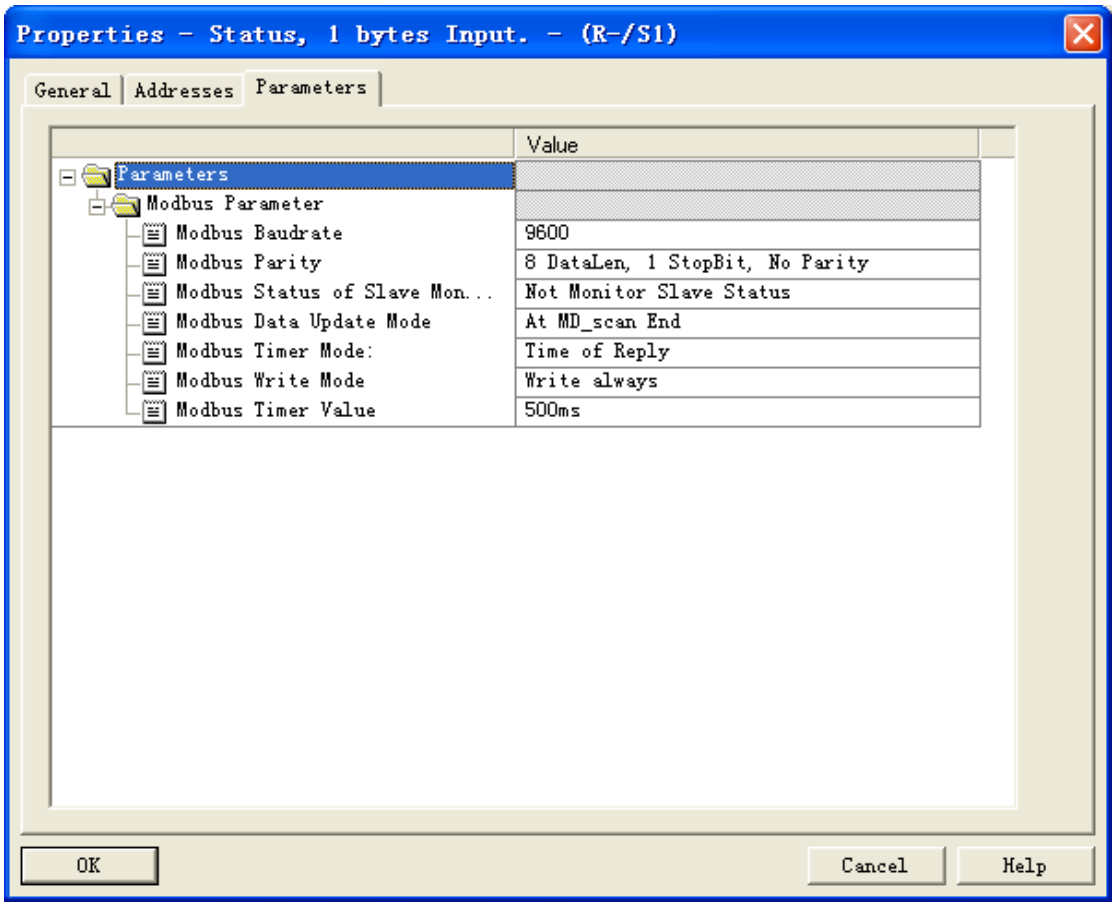


9、双击总线上的设备，弹出设备属性对话框，在 General 栏里可以配置设备号。点击 Ethernet，弹出的对话框参数栏里可以配置 IP 地址。IP 地址应与 PLC 设置在同意网段内。


Properties - PN-ModbusMaster-Gateway
General
Shared
Access
Short description:
PN-ModbusMaster-Gateway
DS PN-Modbus Gateway Toolkit
Order no./
1234567 / V10.0
Family:
DS PN Gateway
Device name:
PN-ModbusMaster-Gateway
GSD file:
GSDML-V2.3-DingShi-Gateway-ModbusM43-20140922.xml
hange Release Number..
Node in PROFINET IO system
Device number:
1
PROFINET-IO-System (100)
IP
192.168.0.2
Ethernet...
Assign IP address via IO controller
Comment:
OK
Cancel
Help


Properties - Ethernet interface PN-ModbusMaster-Gateway
General
Parameters
IP address:
192.168.0.2
Subnet mask:
255.255.255.0
Gateway
Do not use router
Use router
Address:
Subnet:
--- not networked ---
Ethernet(1)
New...
Properties...
Delete
OK
Cancel
Help

10、选中总线上的模块，在配置栏中双击插槽 1，即 Status，1 bytes Input，在弹出的对话框中的参数页面中可以配置 MODBUS 侧的通讯参数。



（1）、Modbus Baudrate：为 MODBUS 的波特率从 300 到 57.6K 可选。

（2）、Modbus Patity：为数据位、停止位、校检，可选。

（3）、Modbus Status of Slave Monitoring：选择有无从站状态监测。

（4）、Modbus Data Update Mode：配置 PROFIBUS 和 MODBUS 数据更新模式。

PROFIBUS 和 MODBUS 数据更新模式：是用户指定何时进行 PROFIBUS 数据区与 MODBUS 数据区的数据交换。

在每条 MD 回答后 At Evry MD End

在 MODBUS 扫描器完成每一条 MODBUS 通信命令后，就进行一次 PROFIBUS 和 MODBUS 数据区数据交换，这是缺省方式。

这种方式保证以最快速度传递 PROFIBUS 主站到 MODBUS 设备之间的数据。

在 MD 扫描结束后 At MD_scan End

在 MODBUS 扫描器完成整个一次 MODBUS 报文队列扫描后，进行一次 PROFIBUS 和 MODBUS 数据区数据交换。

这种方式保证了 MODBUS 通信数据的完整性。

（5）、Modbus Timer_mode：对发送时间控制。

“Time of Reply”：超时时间(Timer_Value)，即等待接收时间到后，马上发送下一条报文；

“Same Interval”： 按设置好的时间值(Timer_Value)定时发送，即按照设置的时间间隔周期性发送报文。

（6）、Modbus Write Mode：实现对写命令的控制功能。

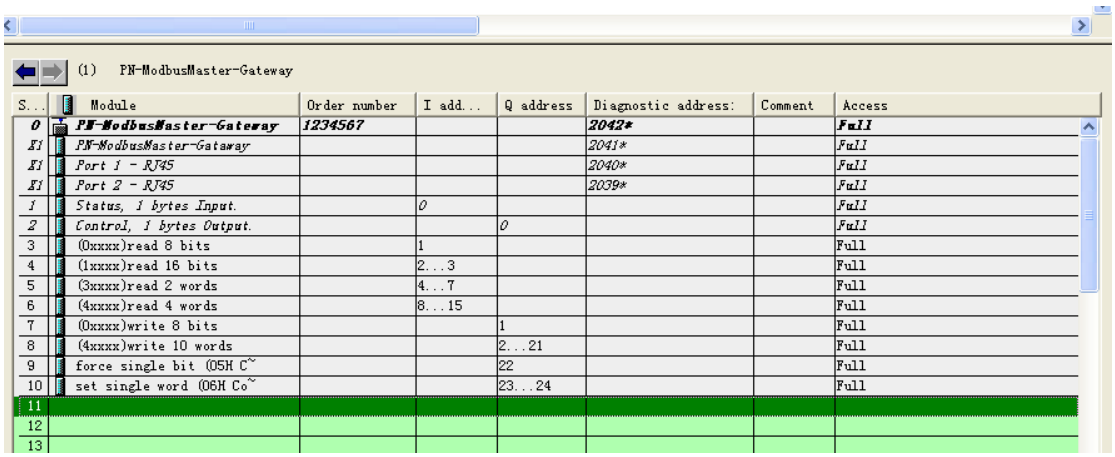
“Write always”： 总线桥启动后，写指令就发送；

“Write on change” 总线桥启动后，当写的数据有改变时才发送。

（7）、Modbus Timer_Value：选择时间值。如果“Timer_mode”选择了“Time of Reply”，则此处设置的时间值为等待从站应答的时间，超过这个时间，则认为从站无应答，发送下一条报文；如果“Timer_mode”选择了“Same Interval”，则此处设置的时间值为发送报文的时间间隔。

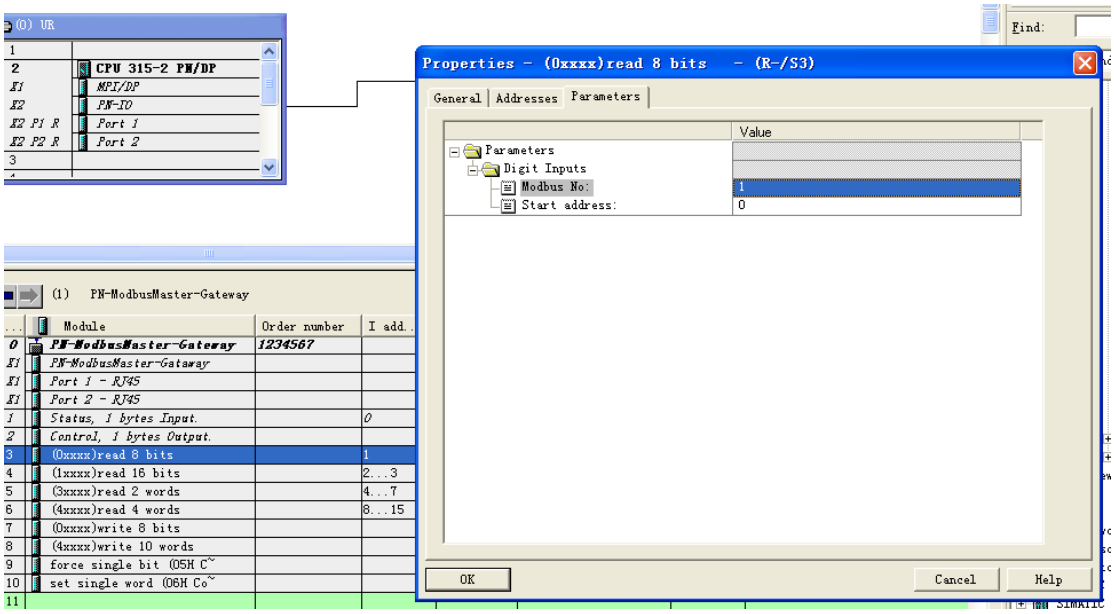
11、在设备目录里点开 PN-ModbusMaster-Gateway，分为 DI 和 DO 两个目录，DI 为输入，即读取 MODBUS 从站设备的数据；DO 为输出，即向 MODBUS 从站设备写入数据。点开 ID、DO，是不同数据长度的命令，开头的（0xxxx）、（1xxxx）、（3xxxx）和（4xxxx）代表该命令对应的 MODBUS 存储区，即分别为 0 区、1 区、3 区和 4 区。DO 目录里最后的 force single bit（05H Command）和 set single word（06H Command）分别对应 MODBUS 的 05H 功能码和 06H 功能码。用户可以根据实际情况自由配置，总数据量不能超过 312 bytes。

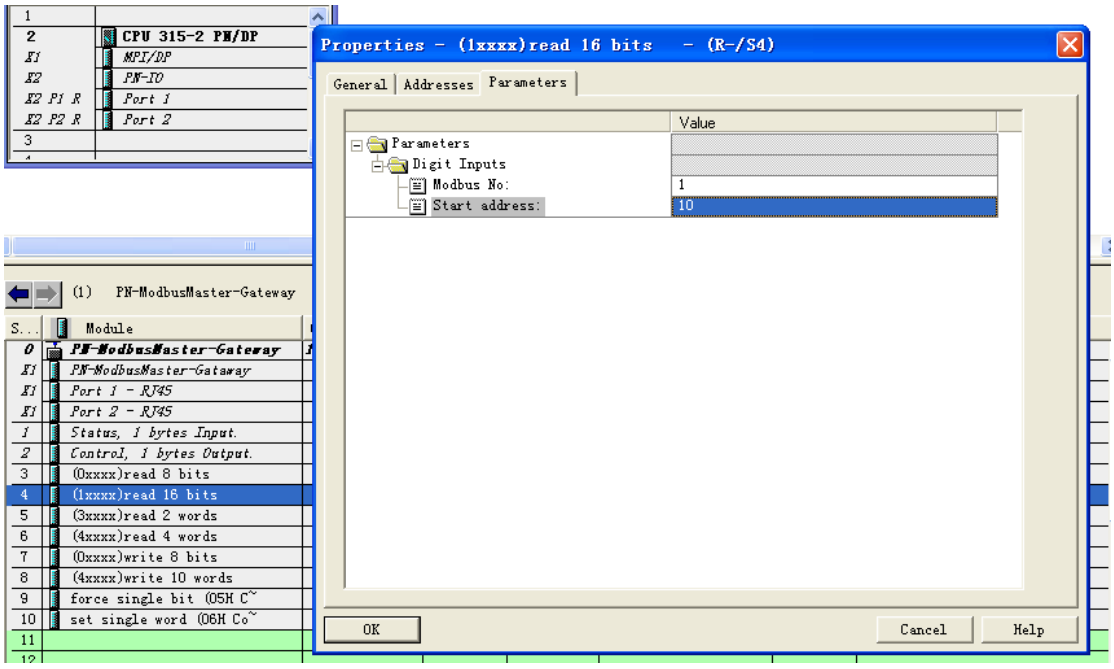
选中总线上的模块，点选配置栏第一个空插槽，即 3 号槽，双击设备目录里的命令即可添加到配置栏中。本例中插入（0xxxx）read 8 bits、（1xxxx）read 16 bits、（3xxxx）read 2 words、（4xxxx）read 4 words、（0xxxx）write 8 bits、（4xxxx）write 10 words、force single bit（05H Command）和 set single word（06H Command）。以上 8 条命令分别对应 MODBUS 的 01H、02H、04H、03H、0FH、10H、05H、06H 功能码（关于 MODBUS 功能码的说请看附录）

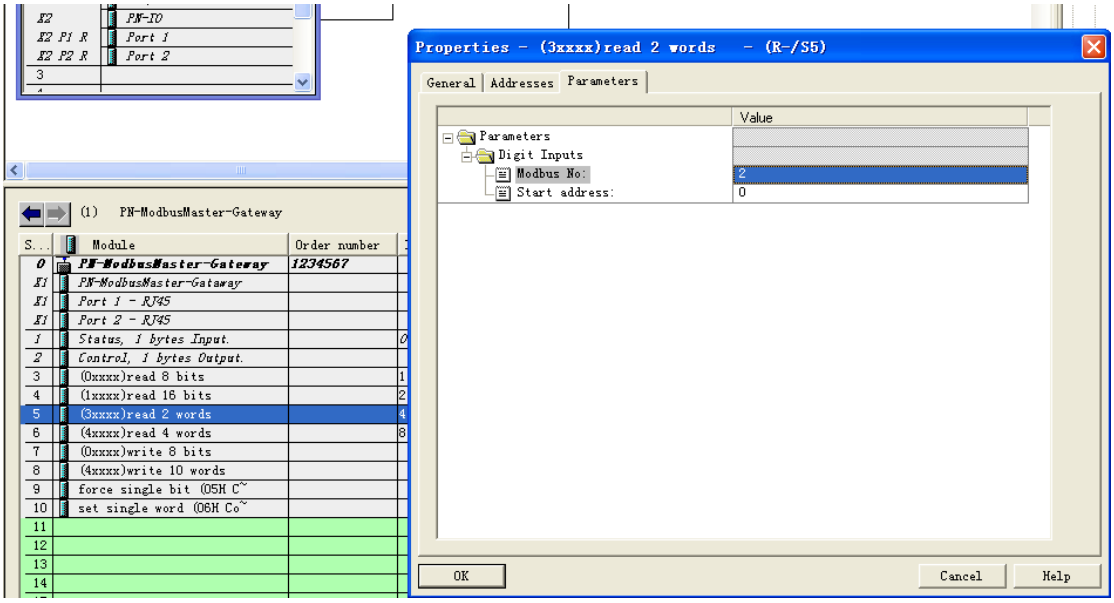


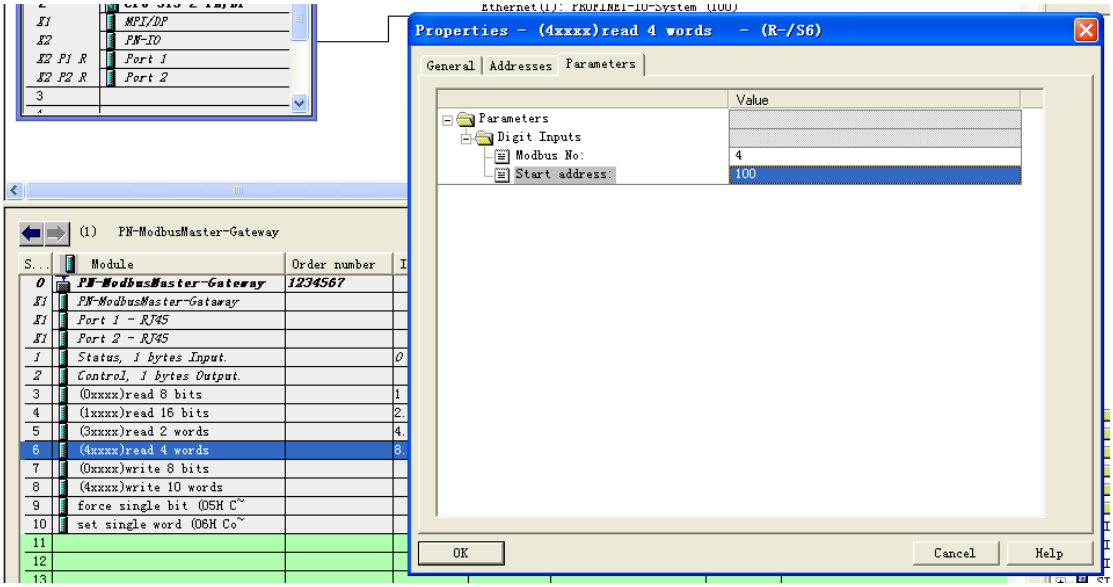
12、双击配置栏中第 3 号插槽（0xxxx）read 8 bits，弹出属性窗口，在参数页面中可以选择该条命令对应的 MODBUS 从站的站地址和寄存器起始地址（均为十进制数）。用户在实际使用中可根据实际情况自由配置。本例中各条命令的参数配置如下面几张图所示。

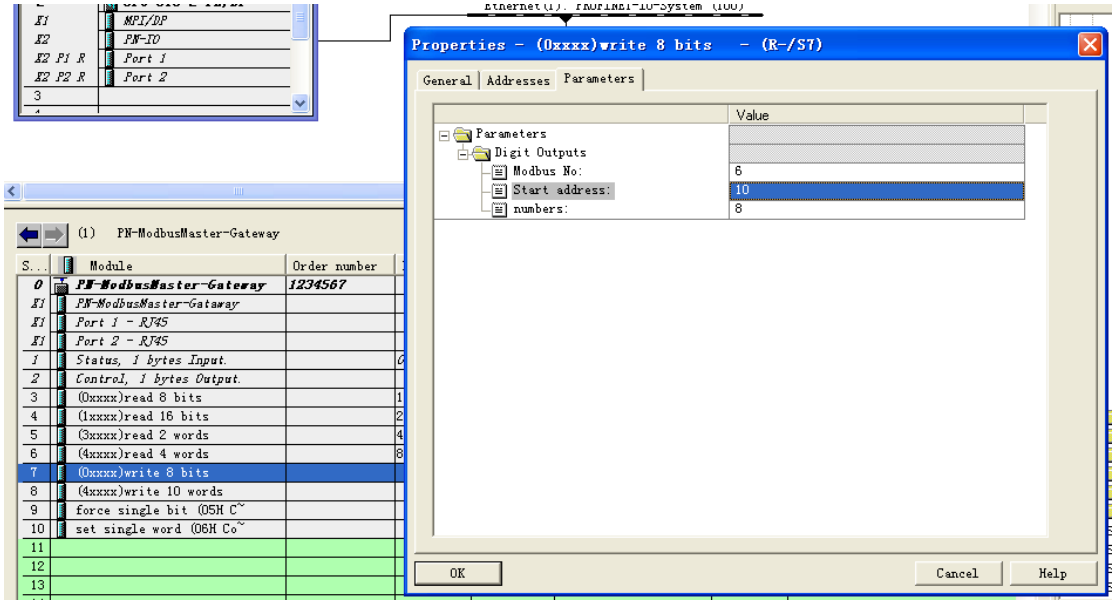
注意：本模块起始地址的计算从 0 开始，有些 MODBUS 设备寄存器起始地址的计算从 1 开始，这时需要填入的起始地址数应减 1。

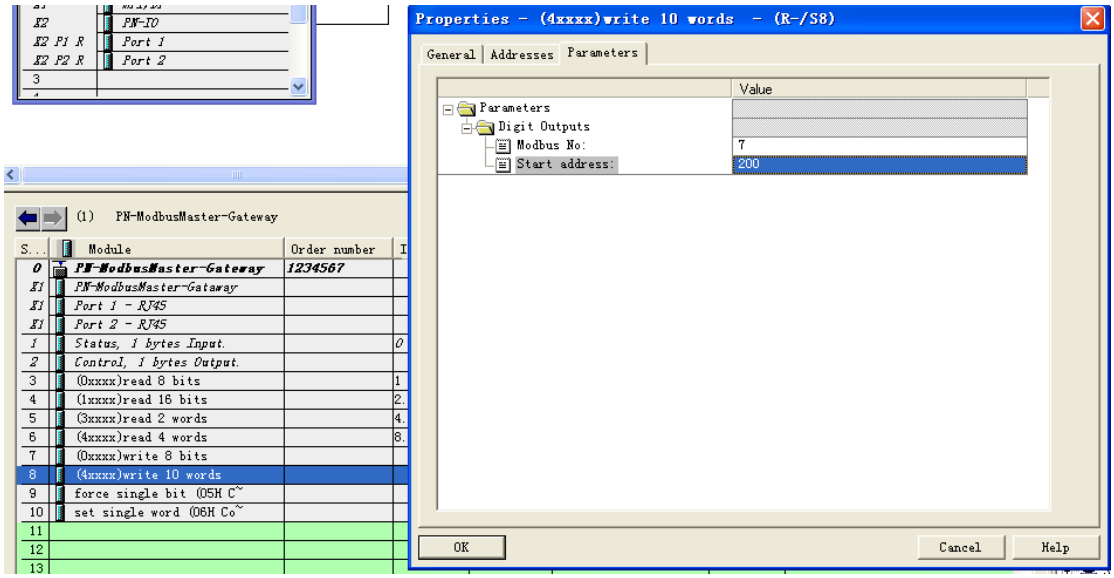


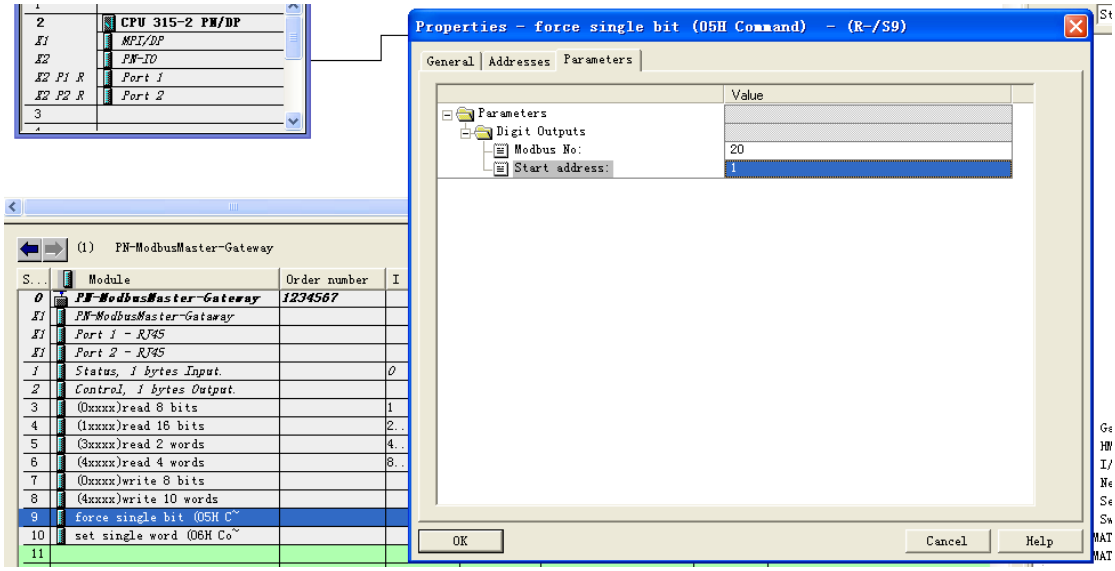


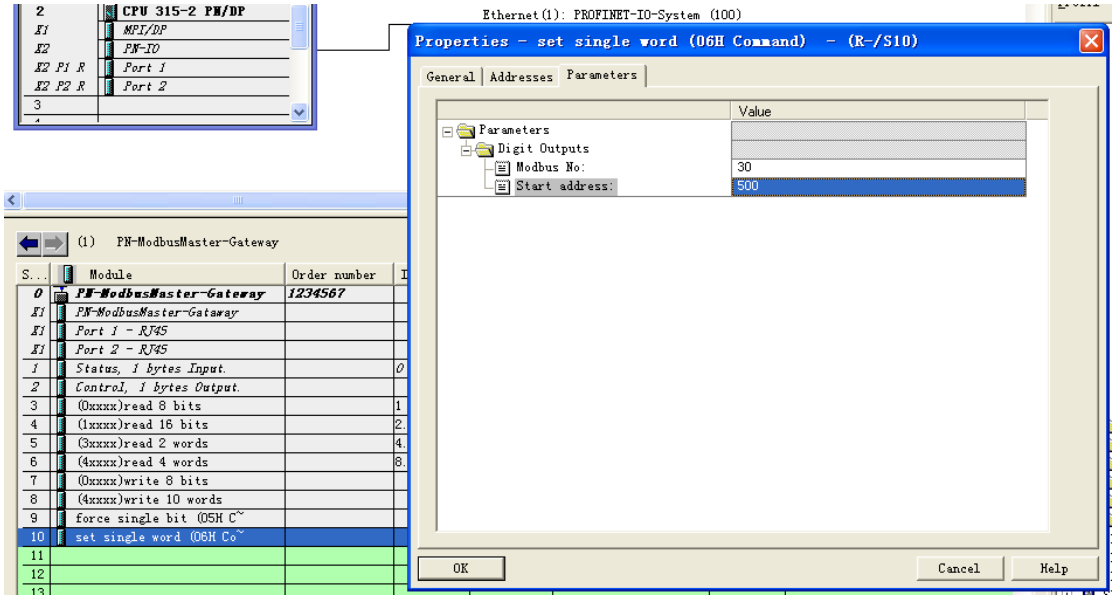

Properties - (3xxxx)read 2 words - (R-/S5)
General
Addresses
Parameters
Value
Parameters
Digit Inputs
Modbus No:
2
Start address:
0
OK
Cancel
Help
(1) PN-ModbusMaster-Gateway
Module
Order number
PN-ModbusMaster-Gateway
1234567
(0xxxx)read 8 bits
(1xxxx)read 16 bits
(3xxxx)read 2 words
(4xxxx)read 4 words
(0xxxx)write 8 bits
(4xxxx)write 10 words
force single bit (05H C~
set single word (06H Co~


Properties - (4xxxx)read 4 words - (R-/S6)
General
Addresses
Parameters
Value
Parameters
Digit Inputs
Modbus No:
4
Start address:
100
OK
Cancel
Help
(1) PN-ModbusMaster-Gateway
Module
Order number
PN-ModbusMaster-Gateway
1234567
(0xxxx)read 8 bits
(1xxxx)read 16 bits
(3xxxx)read 2 words
(4xxxx)read 4 words
(0xxxx)write 8 bits
(4xxxx)write 10 words
force single bit (05H C~
set single word (06H Co~


MPI/DP
PN-IO
Port 1
Port 2
Properties - (0xxxx)write 8 bits - (R-/S7)
General
Addresses
Parameters
Value
Parameters
Digit Outputs
Modbus No:
Start address:
numbers:
6
10
8
OK
Cancel
Help
(1) PN-ModbusMaster-Gateway
Module
Order number
PN-ModbusMaster-Gateway
1234567
PN-ModbusMaster-Gateway
Port 1 - RJ45
Port 2 - RJ45
Status, 1 bytes Input.
Control, 1 bytes Output.
(0xxxx)read 8 bits
(1xxxx)read 16 bits
(3xxxx)read 2 words
(4xxxx)read 4 words
(0xxxx)write 8 bits
(4xxxx)write 10 words
force single bit (05H C~
set single word (06H Co~

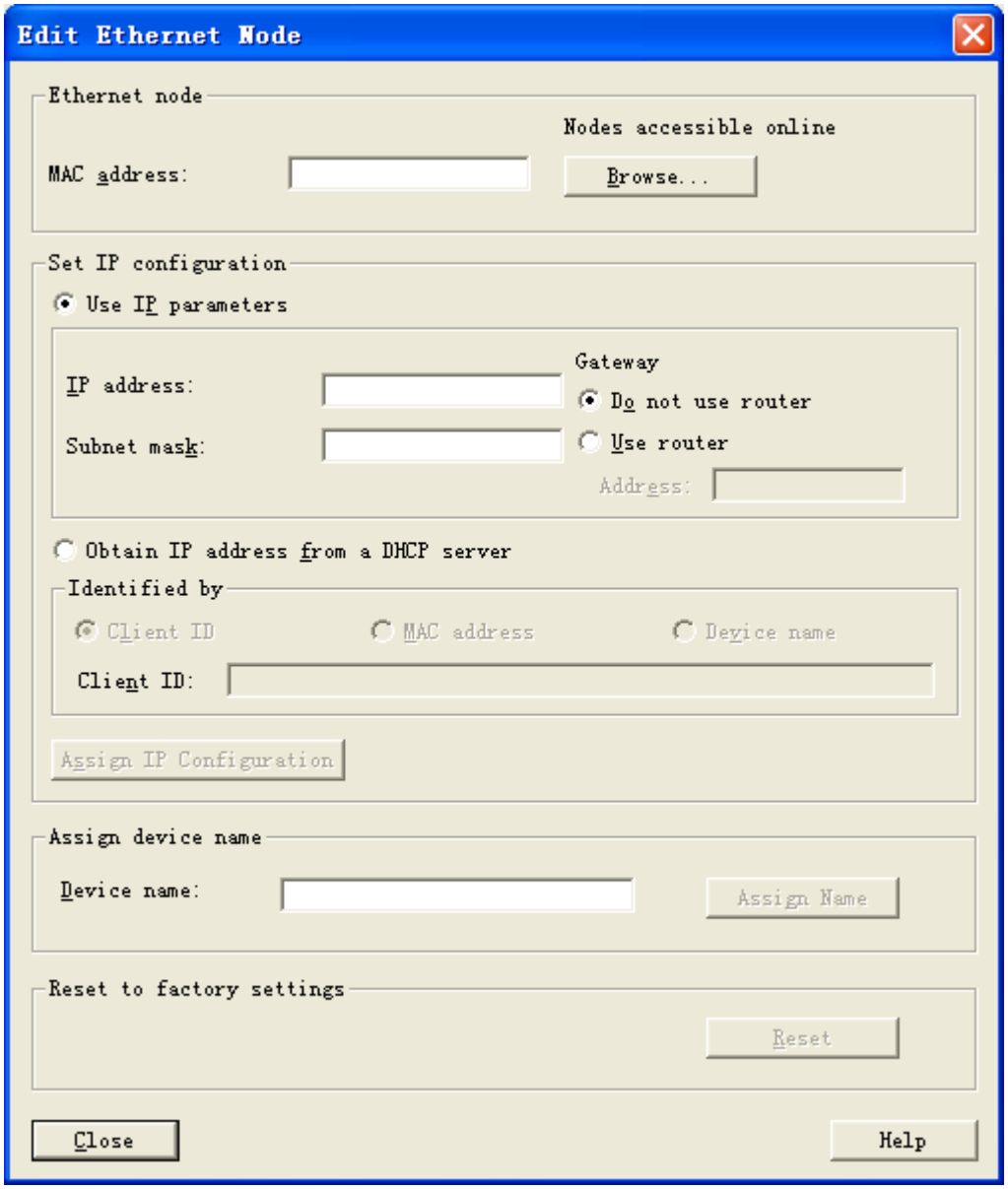

PN-IO
Port 1
Port 2
Properties - (4xxxx)write 10 words - (R-/S8)
General
Addresses
Parameters
Value
Parameters
Digit Outputs
Modbus No:
Start address:
7
200
OK
Cancel
Help
(1) PN-ModbusMaster-Gateway
Module
Order number
PN-ModbusMaster-Gateway
1234567
PN-ModbusMaster-Gateway
Port 1 - RJ45
Port 2 - RJ45
Status, 1 bytes Input.
Control, 1 bytes Output.
(0xxxx)read 8 bits
(1xxxx)read 16 bits
(3xxxx)read 2 words
(4xxxx)read 4 words
(0xxxx)write 8 bits
(4xxxx)write 10 words
force single bit (05H C~
set single word (06H Co~

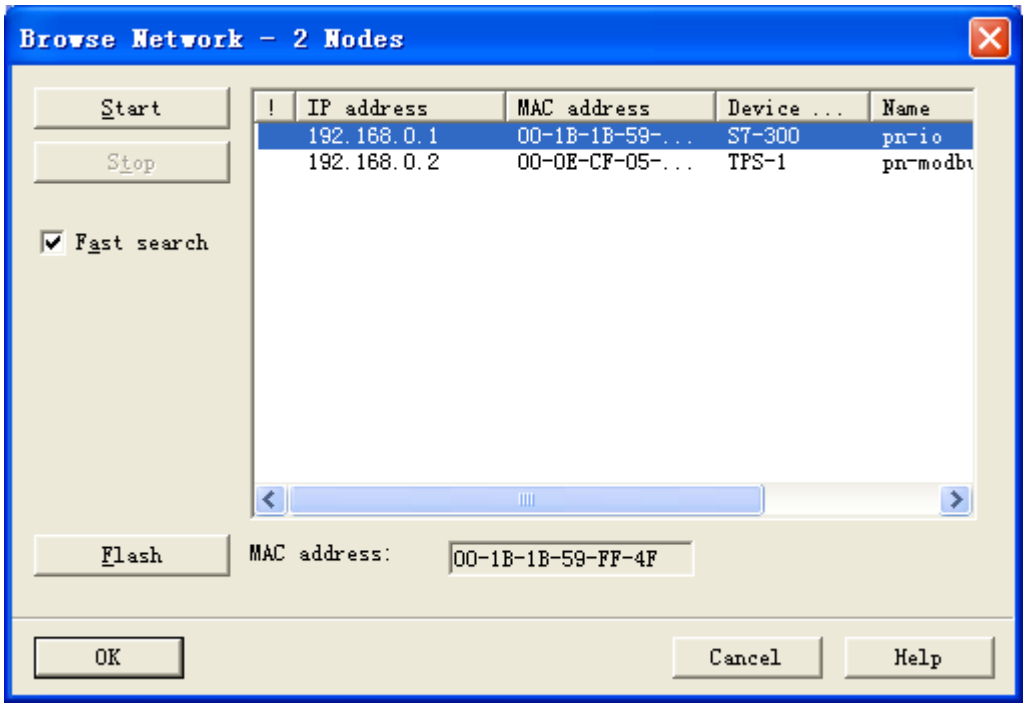




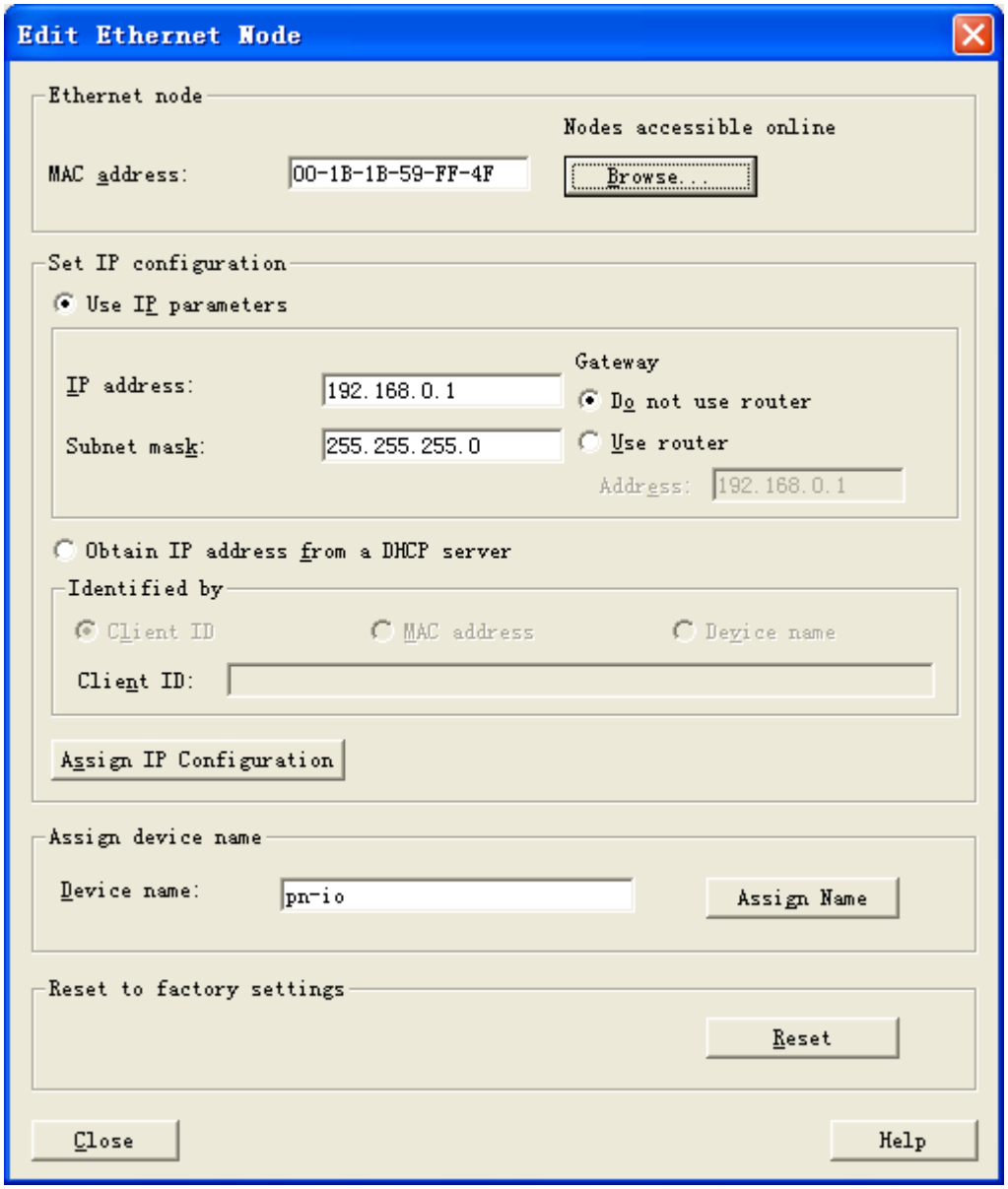
13、此时硬件组态已基本完成，在硬件组态界面的菜单栏中点击 Station→Save and Compile，进行存盘编译。将硬件及电源都连接好，将 PC 的 RJ45 接口与 PLC 的 PN 接口连接起来，打开 PC 的 IP 地址设置窗口，将 PC 的 IP 地址设成与 PLC 的 IP 在同一网段内即可。由于本例中 PLC 的 IP 地址为 192.168.0.1，所以将 PC 的 IP 地址设为 192.168.0.100。

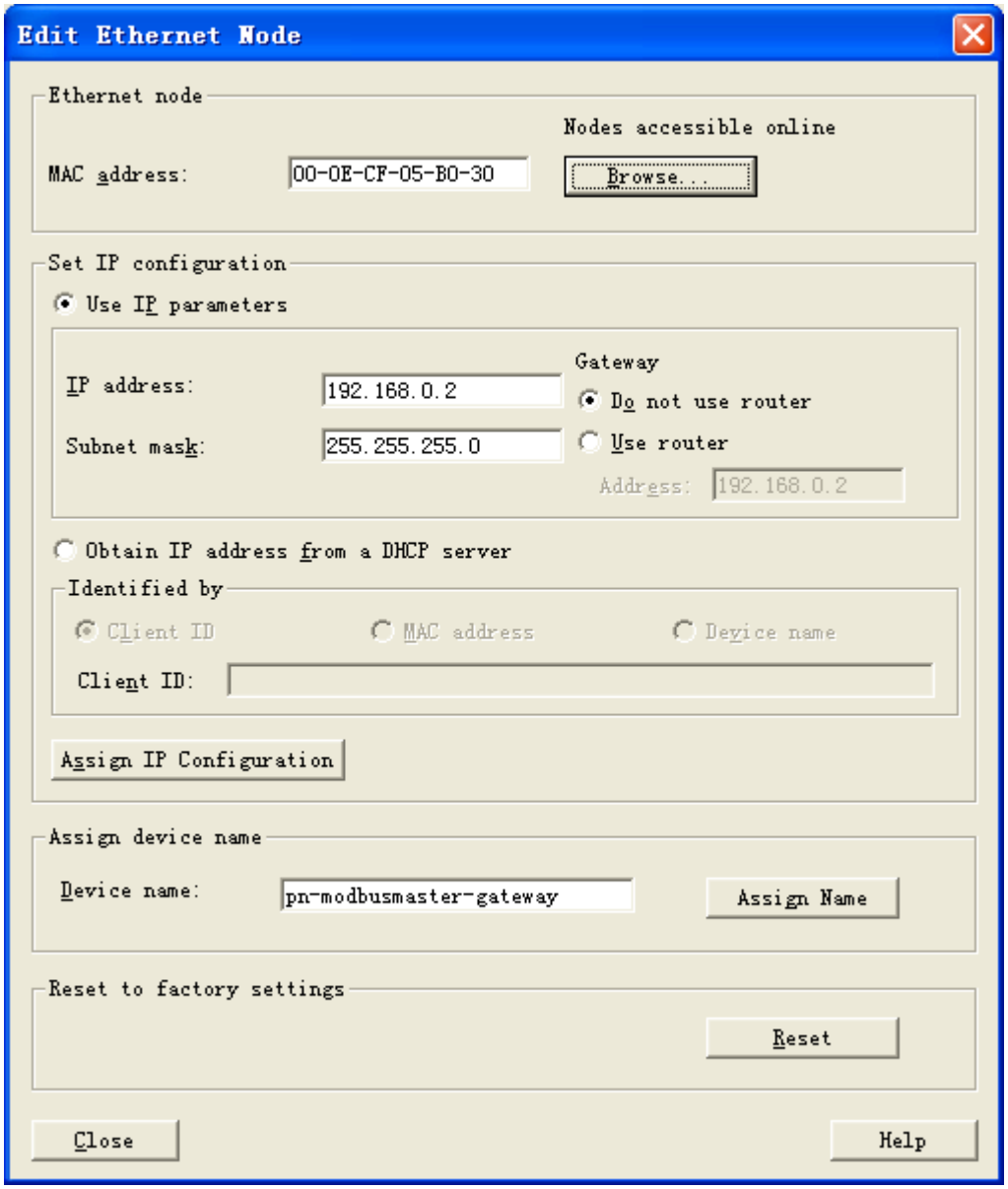
14、设置好 PC 的 IP 地址后，在 STEP 7 的硬件组态界面的菜单栏中点击 PLC→Ethernet→Edit Ethernet Node，在弹出的界面中点击 Browse 将会在弹出的对话框中显示当前与 PC 相连的以太网设备的 IP 地址、MAC 地址、设备类型及设备名称等信息。


Edit Ethernet Node
Ethernet node
Nodes accessible online
MAC address:
Browse...
Set IP configuration
Use IP parameters
IP address:
Gateway
Do not use router
Subnet mask:
Use router
Address:
Obtain IP address from a DHCP server
Identified by
Client ID
MAC address
Device name
Client ID:
Assign IP Configuration
Assign device name
Device name:
Assign Name
Reset to factory settings
Reset
Close
Help



15、在网络设备节点对话框中，点选第一个，点击 OK，将弹出该设备节点的一些相关信息，这里我们需要将该设备的 IP 地址和设备名称修改成与硬件组态的一致，修改好后，点击 Assign IP Configuration 和 Assign Name，将修改的参数分配到硬件中。其余设备的配置与之相同。


Edit Ethernet Node
Ethernet node
Nodes accessible online
MAC address:
00-1B-1B-59-FF-4F
Browse...
Set IP configuration
Use IP parameters
IP address:
192.168.0.1
Gateway
Do not use router
Subnet mask:
255.255.255.0
Use router
Address:
192.168.0.1
Obtain IP address from a DHCP server
Identified by
Client ID
MAC address
Device name
Client ID:
Assign IP Configuration
Assign device name
Device name:
pn-io
Assign Name
Reset to factory settings
Reset
Close
Help



16、在功能块 OB1 中，将控制字的最低位强制为 1，以启动模块工作。

17、将该工程下载到 PLC 中，即完成了本次配置。PN-G-MODBUS 模块会根据配置自动发送 MODBUS 报文。

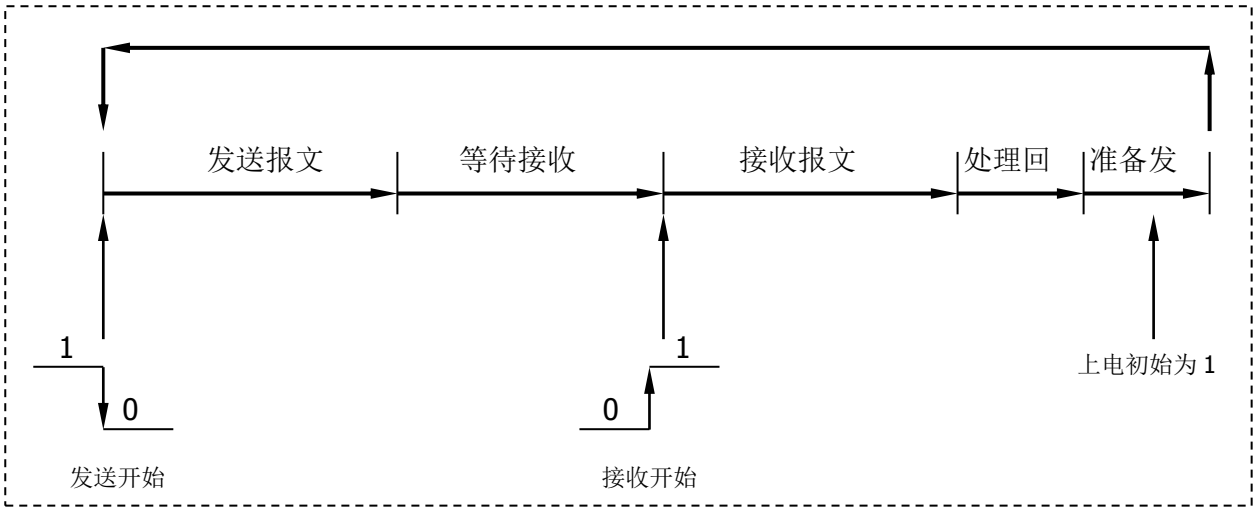
二、MODBUS 主站模式下的状态字及控制字

1、PN-G-MODBUS 模块在主站模式下的状态字

（1）、通信状态字格式

D7:oe_er	D6:CRC_er	D5:Tmdr_O	D4~D1:M_ER_CODE	D0:re_tr
奇偶校验错	CRC 校验错	等待 M 回答到时	MODBUS 异常应答码	接收/发送

（2）接收完毕/发送允许 D0：re_tr



re_tr=1: 接口正在接收或处理接收报文或准备发送的状态。本手册描述 PB-B-MM/V32 产品，只作 MODBUS 设备的主站。因此，接口上电后自动进入“接收/发送 re_tr=1”状态。

re_tr=0: 接口处在发送报文、等待接收状态。

（3）、MODBUS 异常应答码 M_ER_CODE

MODBUS 异常应答码：当接口发送一条 MODBUS 报文后，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时，从机将以“异常应答”回答之。详见“附录 MODBUS 技术简介—3. 异常应答”中的介绍。

注意:整个 MODBUS 报文队列有多条 MODBUS 报文，而只有一个通信状态字。因此，当多条 MODBUS 出现异常应答时，通信状态字中的异常应答码是滚动的。

（4）、等待 M 回答到时 Tmdr_O

总线桥发出 MODBUS 报文后，按配置的“等待回答时间 Time of Replay”等待 MODBUS 设备回答，如果等待时间到时，Tmdr_O=1。MODBUS 扫描器转向发送下一条 MODBUS 报文。

（5）、CRC 校验错 CRC_er

CRC_er=1：当接口接收到一条 MODBUS 回答报文，CRC 校验出现错误时，本产品认为 MODBUS 回答数据不可靠，废弃不用，不与 PROFINET 对应数据区交换。

（6）、奇偶校验错 oe_er

串口接收字符中发现字符奇偶校验错。此时，本产品认为 MODBUS 回答数据不可靠，废弃不用，不与 PROFINET 对应数据区交换。

2、PN-G-MODBUS 模块在主站模式下的控制字

（1）、通信控制字格式

D7: reset_M	D6: escape_M	D5: clear_er	D4-D3	D2:M_w_en	D1:M_r_en	D0:start_M
强置 MODBUS 扫描复位	停止等待	清错误标记	不用	MODBUS 写允许	MODBUS 读允许	启动 MODBUS 扫描

（2）、启动 MODBUS 扫描 D0:start_M

启动 MODBUS 扫描，MODBUS 扫描器从当前 MODBUS 扫描器指针开始，发送对应 MODBUS 报文。

（3）、MODBUS 读允许 D1:M_r_en

只发送 MODBUS 报文队列中的读类命令：即 01H、02H、03H、04H 命令。

（4）、MODBUS 写允许 D2:M_w_en

只发送 MODBUS 报文队列中的写类命令：即 05H、06H、0FH、10H 命令。

以上三个控制位（start_M、M_r_en、M_w_en）配合使用，主站可以完成“先读（设备状态）→判断→再写（控制设备）等更复杂的功能。

表 3-1 三个控制位（M_w_en、M_r_en、start_M）控制功能

D2：M_w_en MODBUS 写允许	D1：M_r_en MODBUS 读允许	D0：start_M 启动 MODBUS 扫描	功能
×	×	**0**	停止 MODBUS 扫描
0	**0**	**1**	启动 MODBUS 扫描，发送所有 MODBUS 读\写命令
1	**1**	**1**	
0	**1**	**1**	启动 MODBUS 扫描，只发送 MODBUS 读命令
1	**0**	**1**	启动 MODBUS 扫描，只发送 MODBUS 写命令

（5）、清错误标记 D5:clear_er

clear_er=1：总线桥清除通信状态字中错误标记位 D7～D1。

（6）、停止等待 D6:escape_M

escape_M=1：MODBUS 扫描器发出一条 MODBUS 报文后等待 MODBUS 设备回答。在此状态下, 如果 escape_M=1，扫描器停止等待, 继续扫描下一条 MODBUS 报文。该功能通常配合“等待回答时间 Time of Replay：无限期等待回答 Waiting……”的选择使用。

注意 1：如果 escape_M 保持为 1，那么，下一条 MODBUS 报文发出后，没有等待，立刻转向发送再下一条 MODBUS 报文。因此，escape_M 应配合 start_M 使用。如下指令系列所示：

↓

↓

MODBUS 扫描器处在无限期等待回答中……..

start_M=0;

escape_M=1;

escape_M=0;

start_M=1;

MODBUS 扫描器停止等待，转向发送下一条 MODBUS 报文……

↓

↓

（7）、强置 MODBUS 扫描复位 D7:reset_M

reset_M=1：强置 MODBUS 扫描器指针回到第一条 MODBUS 报文位置，MODBUS 扫描器处在复位状态。此时，启动 MODBUS 扫描 start_M 无效。

reset_M=0：“强置 MODBUS 扫描器复位”无效。

注意 2：reset_M 与 escape_M 同时作用无效。

reset_M	escape_M	功能
0	0	无作用

0	1	停止等待
1	0	强置 MODBUS 扫描复位
1	1	无作用

三、MODBUS 从站模式的配置

配置成 MODBUS 从站的方法基本与配置成主站的相同，只是使用的 GSD 文件名称为 GSDML-V2.3-DingShi-Gateway-ModbusS43-xxxxxxxx.xml 。并且将模块底部的第一个拨码开关拨到 ON 即可。在此就不多赘述。

四、MODBUS 主站模式下的状态字及控制字

作为 MODBUS 从站时的状态字和控制字与作为 MODBUS 主站时的有些区别。

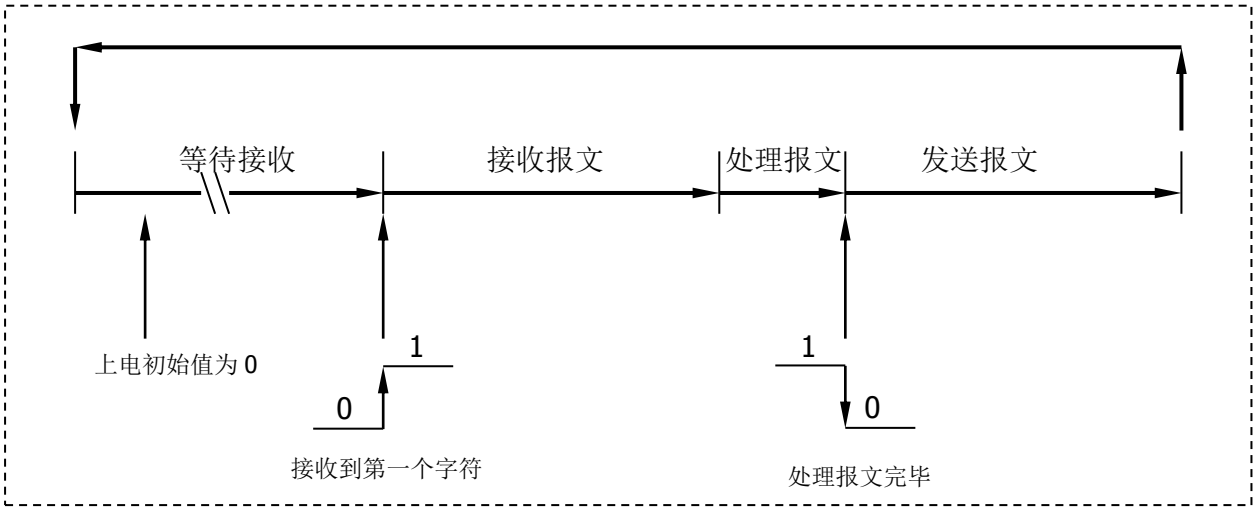
1、PN-G-MODBUS 模块在从站模式下的状态字

（1）、通信状态字格式

D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0：re_tr
奇偶校验错	CRC 校验错	不用	MODBUS 异常应答码	接收/发送

（2）、接收/发送：re_tr

接收/发送 re_tr 标识状态转换见图：



re_tr=1：接口正在接受报文或处理报文。

re_tr=0：接口处在发送报文、等待接收状态。

本手册描述产品 PB-B-MS 是 MODBUS 从站。因此，接口上电后自动进入等待接收状态 re_tr=0。

（3）、MODBUS 异常应答码:M_ER_CODE

MODBUS 异常应答码 M_ER_CODE：当接口发送一条 MODBUS 报文后，从站接收到的主机报文，没有传输错误，但从站无法正确执行主站命令或无法作出正确应答，从站将以“异常应答”回答之。详见“附录 MODBUS 技术简介--3. 异常应答”。

（4）、CRC 校验错：CRC_er

CRC_er=1：接口接收到 MODBUS 报文 CRC 校验出现错误。此时，接口认为此 MODBUS 报文数据不可靠、不响应执行命令，不作出回答。

CRC_er=0：没有 CRC 校验出现错误。

（5）、奇偶校验错 D7：oe_er

串口接收字符中发现字符奇偶校验错，此时接口认为此 MODBUS 报文数据不可靠、不响应执行命令，不作出回答。

2、PN-G-MODBUS 模块在从站模式下的控制字

（1）、通信控制字格式

D7：clear_er	D6—D1	D0：PB_O_EN
清错误标记	不用	PROFIBUS 输出有效

（2）、PROFIBUS 输出有效 D0：PB_O_EN

PB_O_EN =1：使 PROFIBUS 输出数据进入 MODBUS 1XXXX 和 3XXXX。

PB_O_EN =0：PROFIBUS 输出数据禁止进入 MODBUS 1XXXX 和 3XXXX，1XXXX 和 3XXXX 保持原数据（初始状态均为 0）；

（3）、清错误标记 D7：clear_er

clear_er=1：清除通信状态字中错误标记位 D7～D1

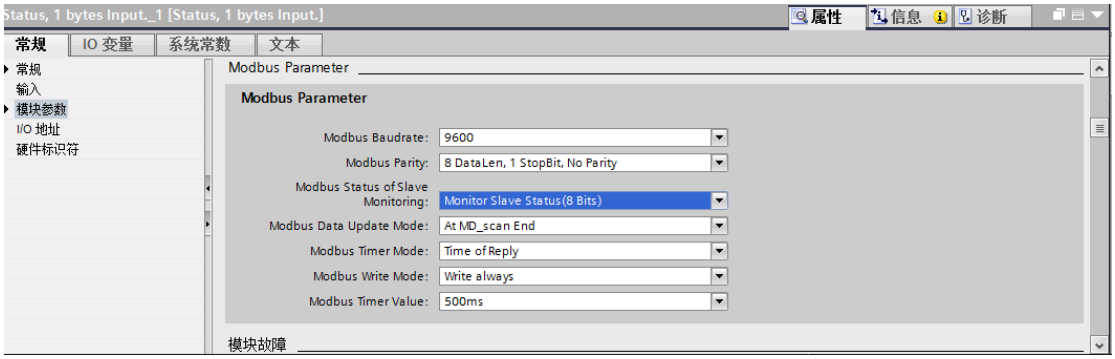
clear_er=0：无清除操作

五、MODBUS 主站模式下的从站状态监测

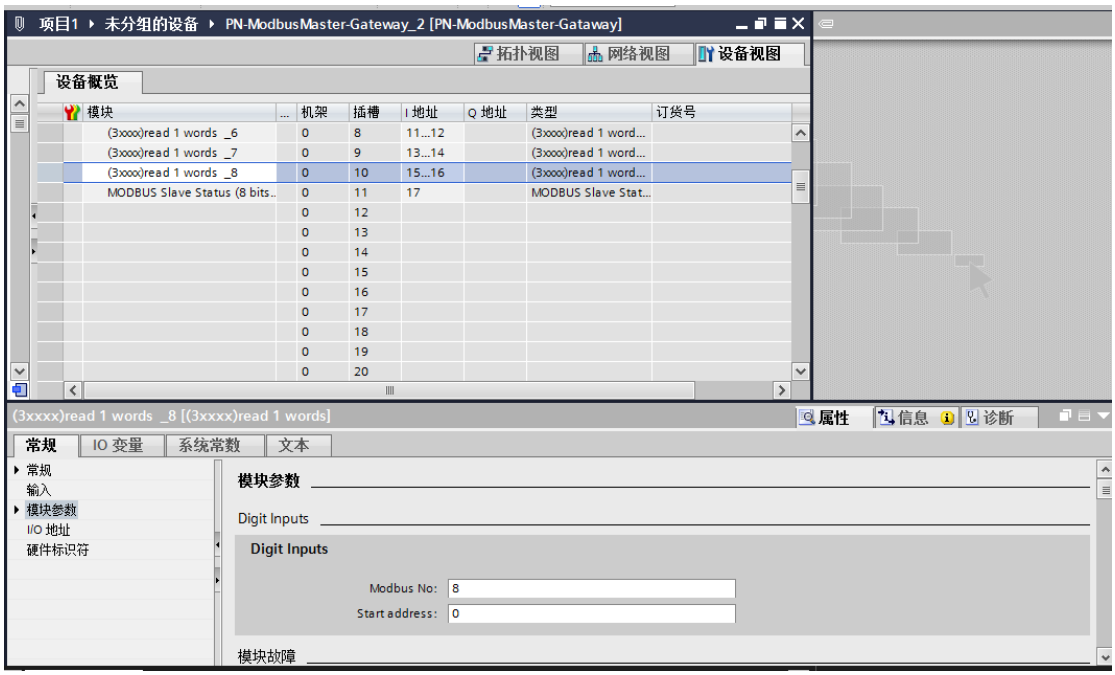
1、 MODBUS 从站通信状态（位）监测

在本例配置中有 8 个 MODBUS 从站（01H#、02H#、03H#、04H#、05H#、06H#、07H#、08H#）：在工程中可对 MODBUS 从站通信状态（位）进行监测。

第一步：选择“有从站状态监测（8 位）”，如下图所示。缺省时为：“无从站状态检测”。

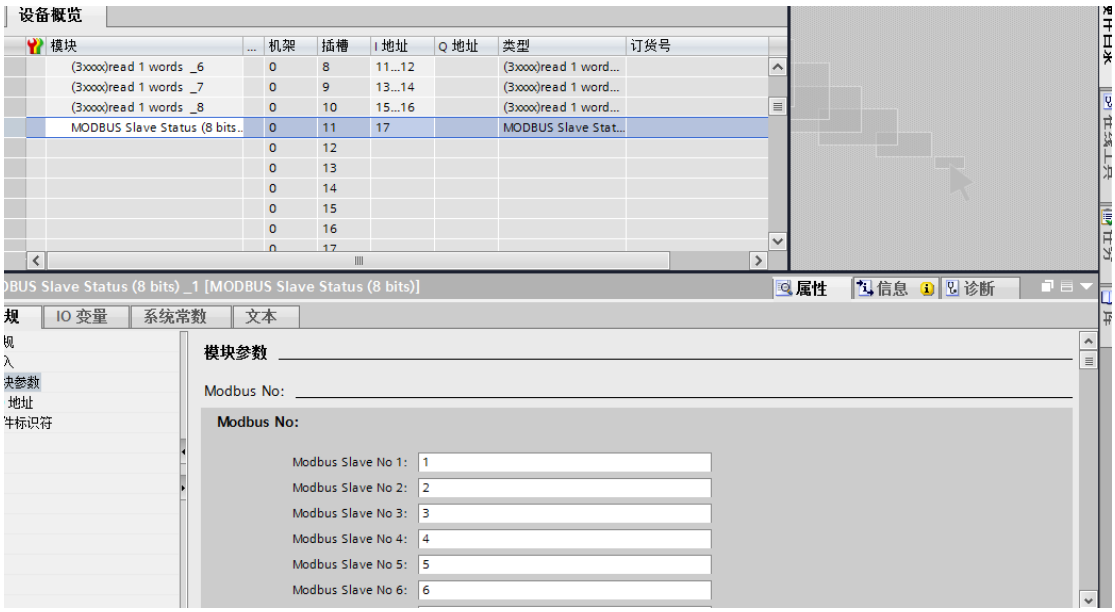


第二步：配置 MODBUS 报文。每个从站配置 1 条报文：读 1 个字 read 1 Words(3xxxx)，注意：每条报文都要设置 MODBUS 从站地址。如下图所示。



第三步：插入“MODBUS 从站状态表（8 位）”，键入 MODBUS 从站地址表：01、02、

03、04、05、06、07、08。（当被监测的从站少于 8 台时，多余位可随意设置）



注意：“MODBUS 从站状态表（8 位）”必须插在所有 MODBUS 报文最后。

第四步：程序运行后，可在 PROFINET 地址 IB17 中见到 MODBUS 从站 01H、02H、03H、04 H、05 H、06 H、07 H、08 H 的通信状态的显示：

IB1：

D7	D6	D5	D4	D3	D2	D1	D0
08H 站通信状态	07H 站通信状态	06H 站通信状态	05H 站通信状态	04H 站通信状态	03H 站通信状态	02H 站通信状态	01H 站通信状态

其中 D0 = 01H 站通信状态：

D0=0：MODBUS 主站（PN-G-MODBUS）向 01H 从站发送报文， 01H 从站根本没有接到可使其回答的 MODBUS 主站报文，或 01H 站超过了所配置等待回答时间 Time of Replay。

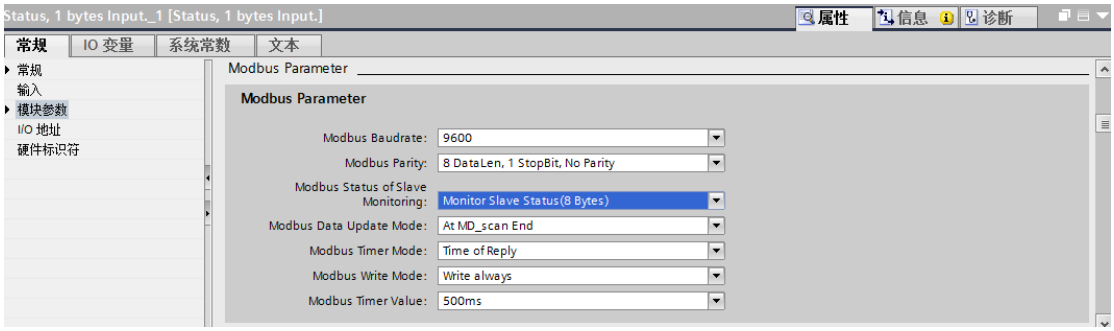
D0=1：01H 站在接收到 MODBUS 主站（PN-G-MODBUS）报文后在 Tsdr 时间之内作出了回答，并且 MODBUS 主站（PN-G-MODBUS）接收到的回答报文正确。

D1-D7：与上面 D0 作用相同。

2、 MODBUS 从站通信状态（字节）监测

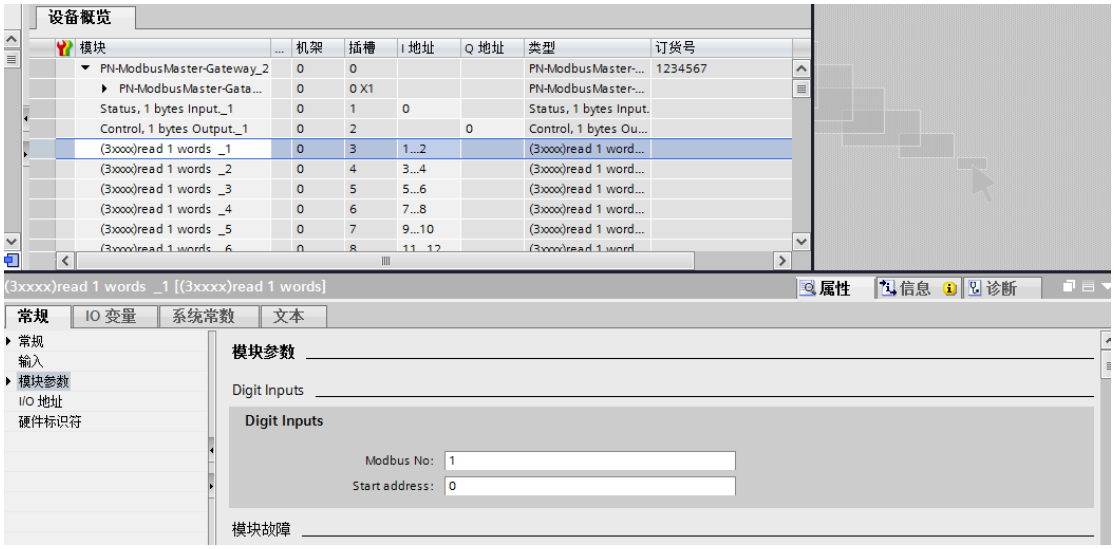
在举例中有 8 个 MODBUS 从站（01H#、02H#、03H#、04H#、05H#、06H#、07H#、08H#）,在工程中进行 MODBUS 从站通信状态（字节）的监测。

第一步：选择“有从站状态监测 8 Byte（字节）”。缺省时为：“无从站状态检测”。

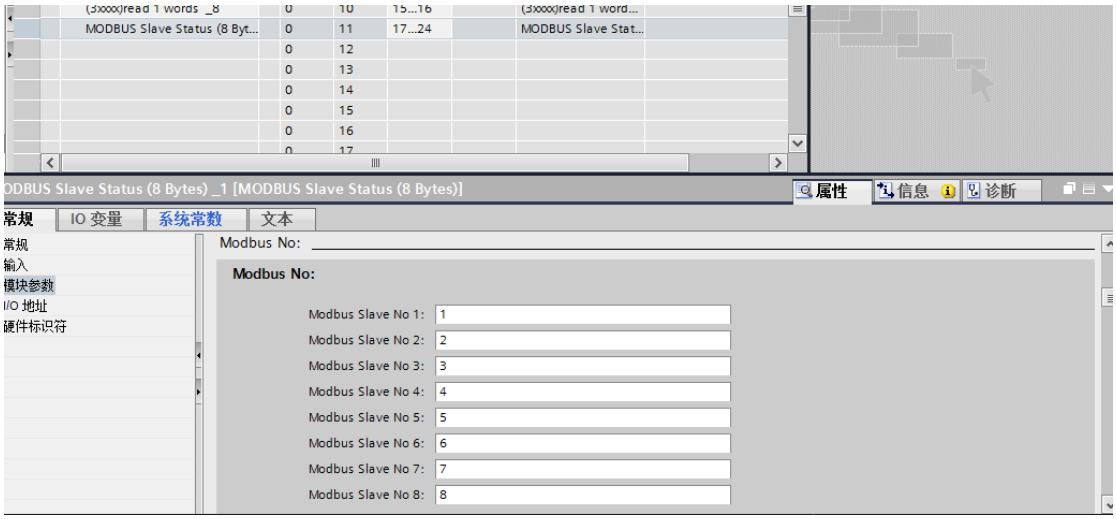


第二步：配置 MODBUS 报文。每个从站配置 1 条报文：读 1 个字 read 1 Words(3xxxx)。

注意：每条报文都要设置 MODBUS 从站地址。



第三步：插入“MODBUS 从站状态表（8 字节）”。键入 MODBUS 从站地址表：01、02、03、04、05、06、07、08。



注意：“MODBUS 从站状态表（8 位）”必须插在所有 MODBUS 报文最后。

第四步：运行程序后，在 PROFIBUS 主站地址 IB17~IB24 中，可显示对应 MODBUS 从站号 01、02、03、04、05、06、07、08 的通信状态字节。

IB17：对应 01H 号 MODBUS 从站的状态字节；

D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	MM 等待回答超时

其中：

D0=0：MODBUS 主站（PN-G-MODBUS）向 01H 号从站发送报文， 01H 从站根本没有接到可使其回答的 MODBUS 主站报文或者超过了配置等待回答时间 Time of Replay。

D0=1：01H 号从站接收到 MODBUS 主站（PN-G-MODBUS）报文后在 Tsdr 时间之内作出了回答，并且 MODBUS 主站（PN-G-MODBUS ）接收到的回答报文是正确的。

D4～D1：M_ER_CODE= MODBUS 异常应答码：

当 MODBUS 主站（PN-G-MODBUS）发送一条 MODBUS 报文后，01H 号从站接收到的主站报文，没有传输错误；但从站无法正确执行主站命令或无法作出正确应答；从站将以“异常应答”回答之。

D6：CRC_er =CRC 效验错

CRC_er=1：MODBUS 主站（PN-G-MODBUS）接收到一条 MODBUS 回答报文时 CRC 校验错误，此时，MODBUS 主站（PN-G-MODBUS）认为 MODBUS 回答数据不可靠、废弃不用，不与 PROFIBUS 对应数据区交换。

D7：奇偶校验错 oe_er

MODBUS 主站（PN-G-MODBUS）接收字符中发现字符奇偶校验错。此时，MODBUS 主站（PN-G-MODBUS）认为 MODBUS 回答数据不可靠、废弃不用，不与 PROFIBUS 对应数据区交换。

其它 MODBUS 状态字节：

IB18：对应 02H 号 MODBUS 从站的状态字节；

D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

IB19：对应 03H 号 MODBUS 从站的状态字节；

D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

IB20：对应 04H 号 MODBUS 从站的状态字节；

D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

IB21：对应 05H 号 MODBUS 从站的状态字节；

D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

IB22：对应 06H 号 MODBUS 从站的状态字节；

D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

IB23：对应 07H 号 MODBUS 从站的状态字节；

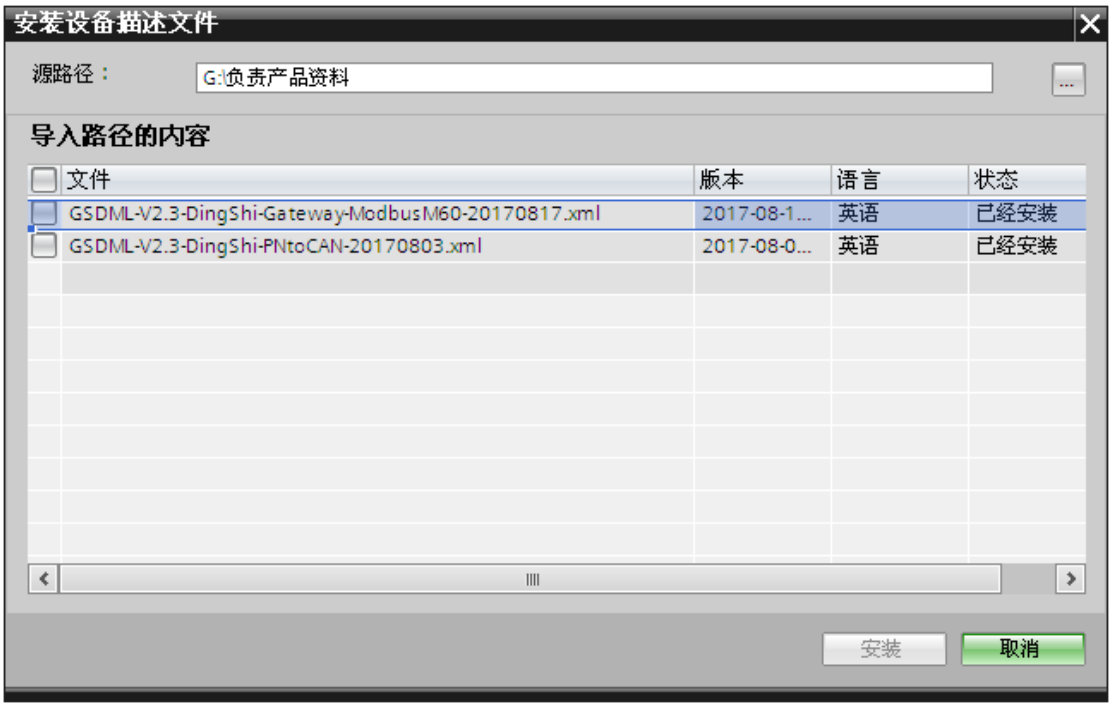
D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

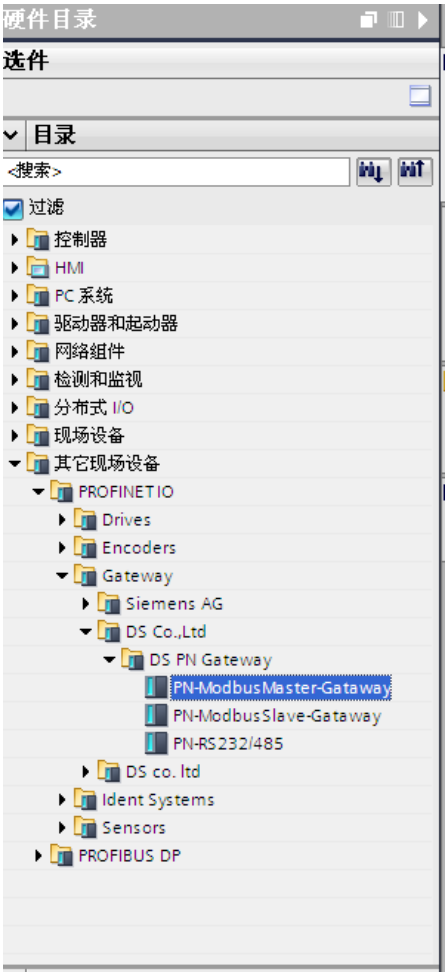
IB24：对应 08H 号 MODBUS 从站的状态字节；

D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

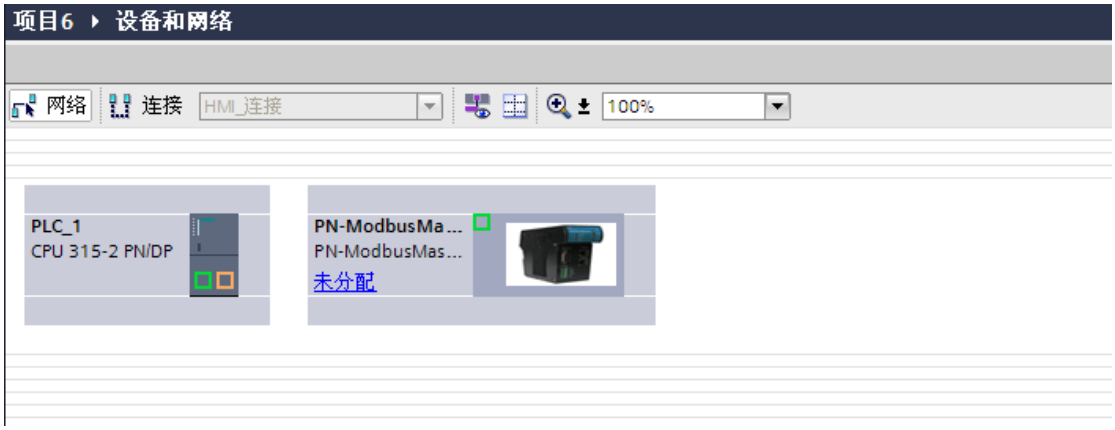
第四章 博途下 MODBUS 侧主站配置

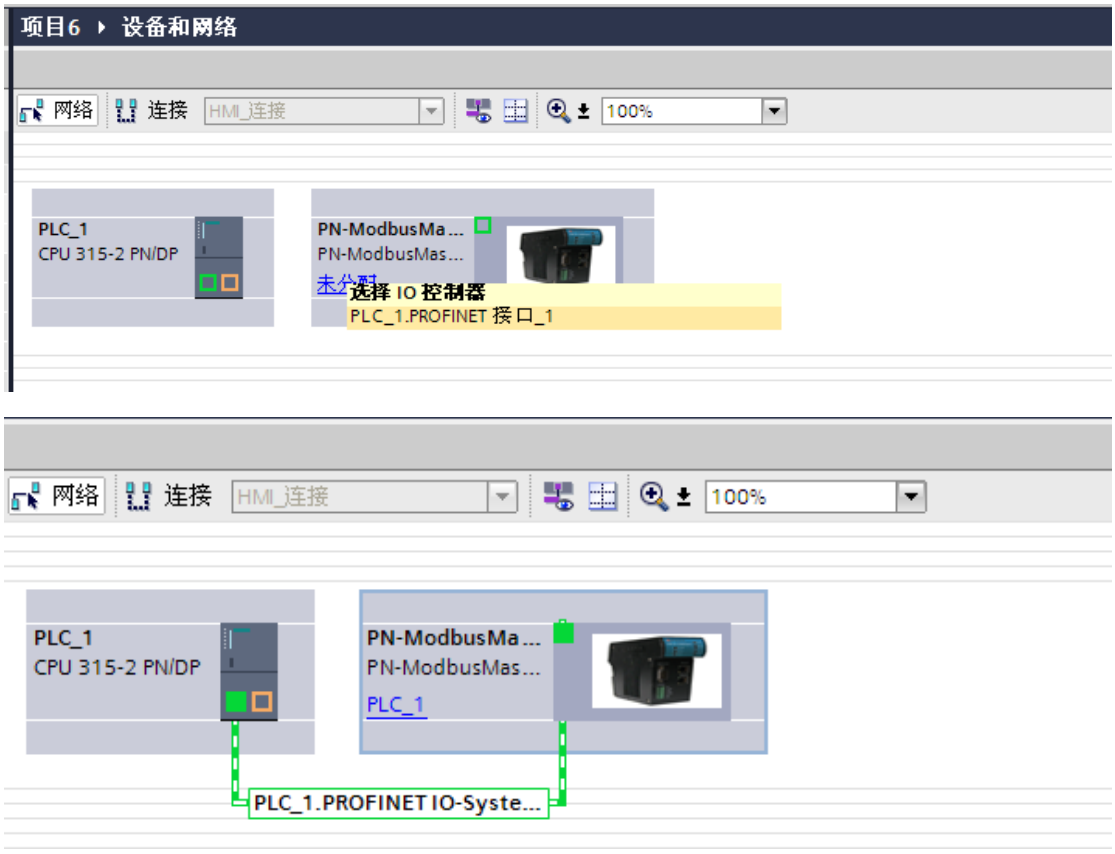
一、 *GSD 文件导入*



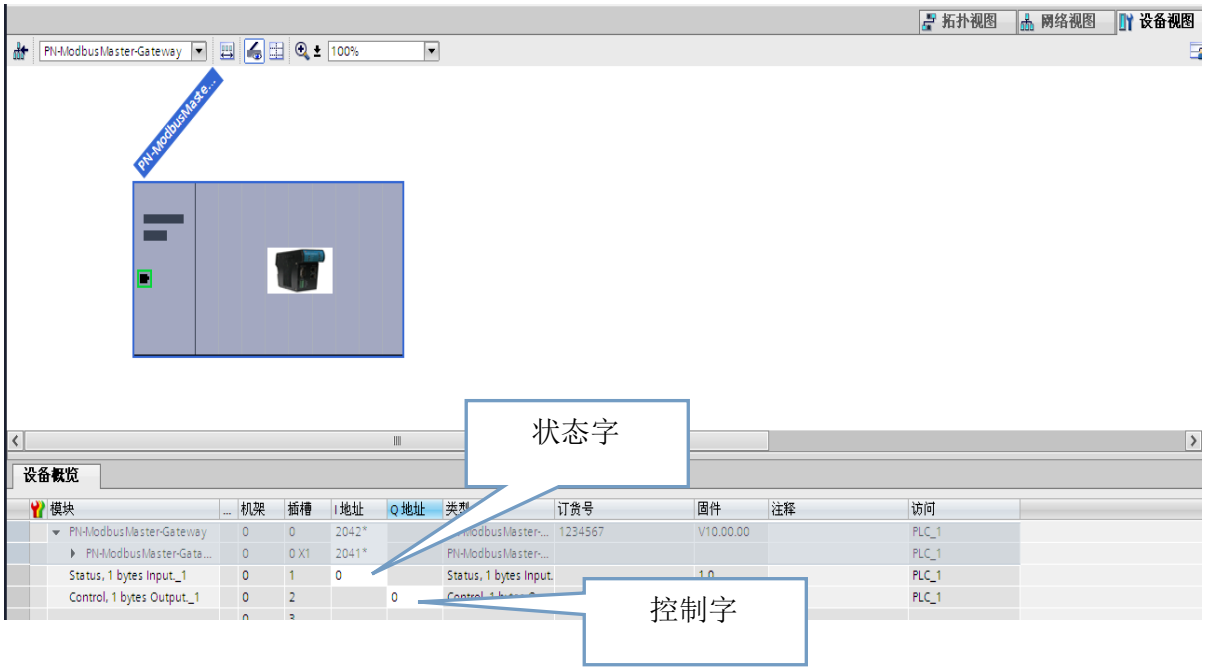


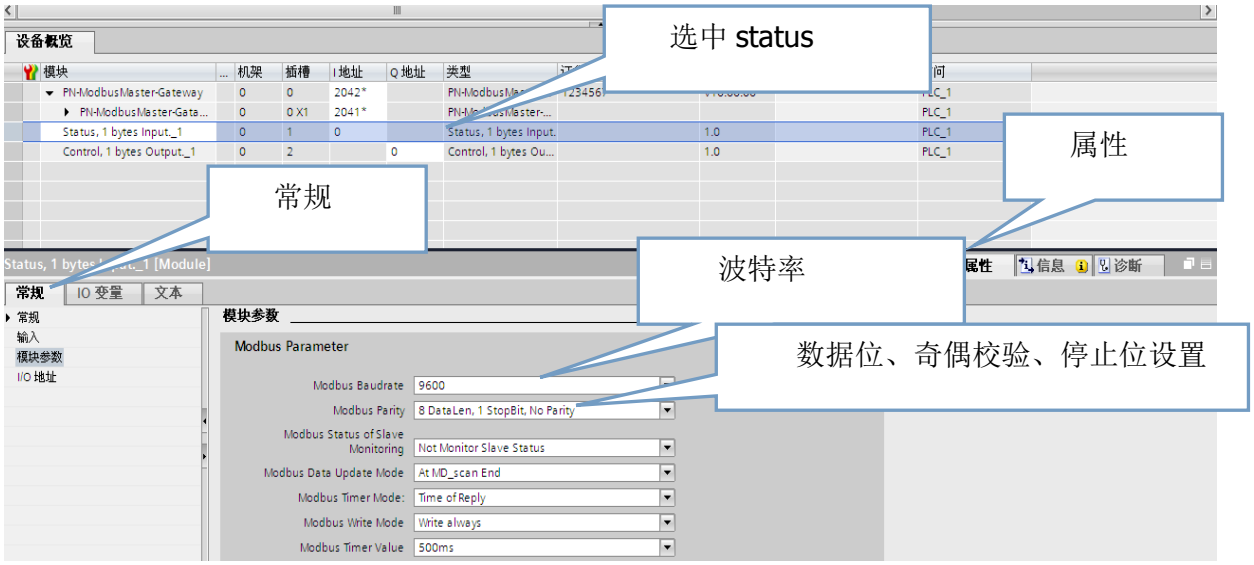
二、 *PN-G-MODBUS 模块添加*



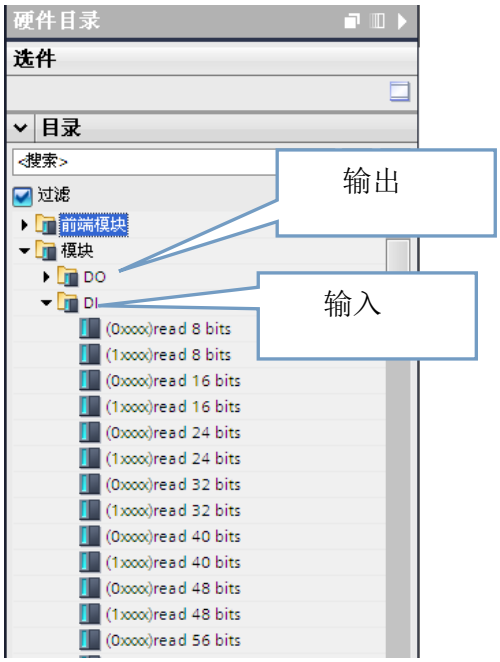


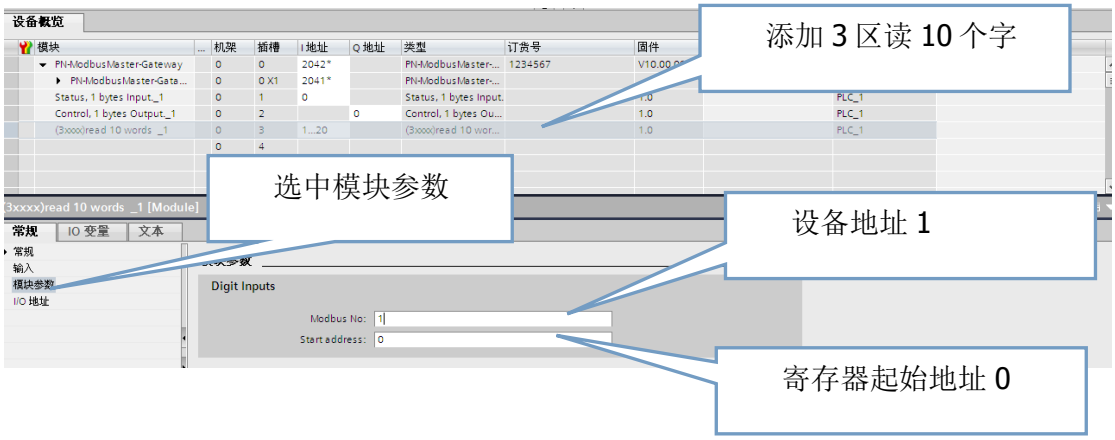
三、 *PN-G-MODBUS 模块 RTU 侧配置*

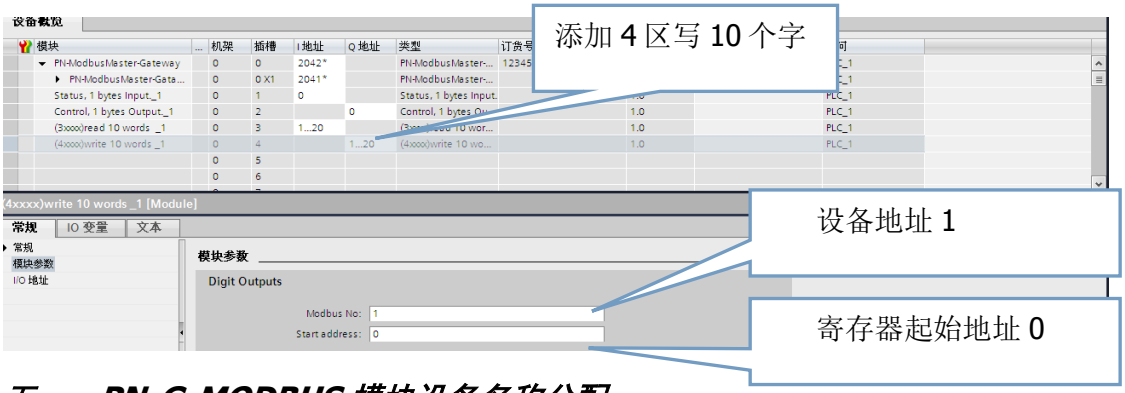




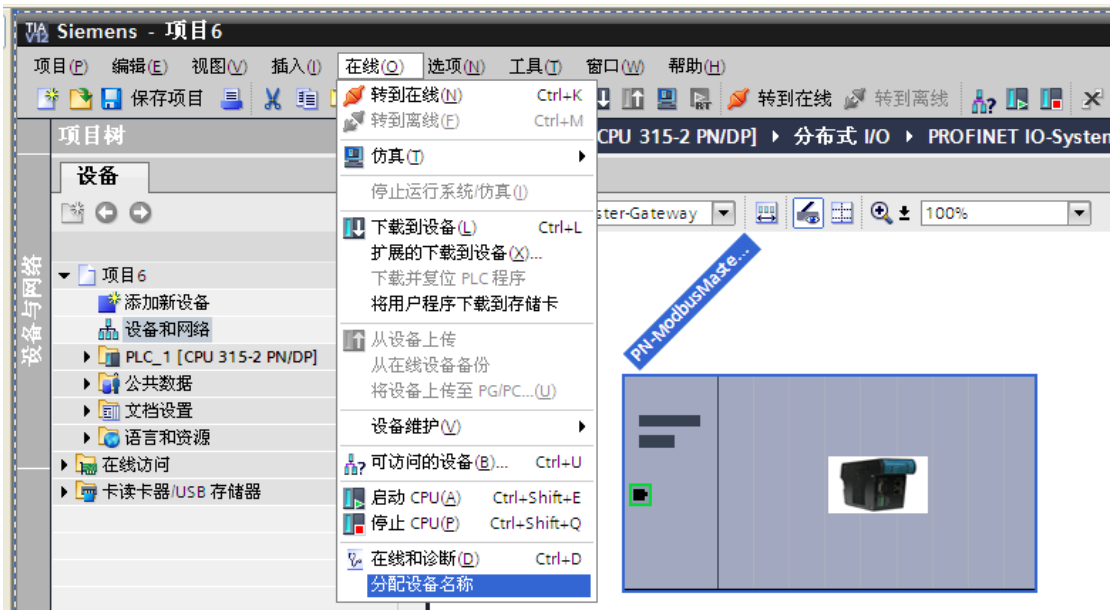
四、 PN-G-MODBUS 数据配置

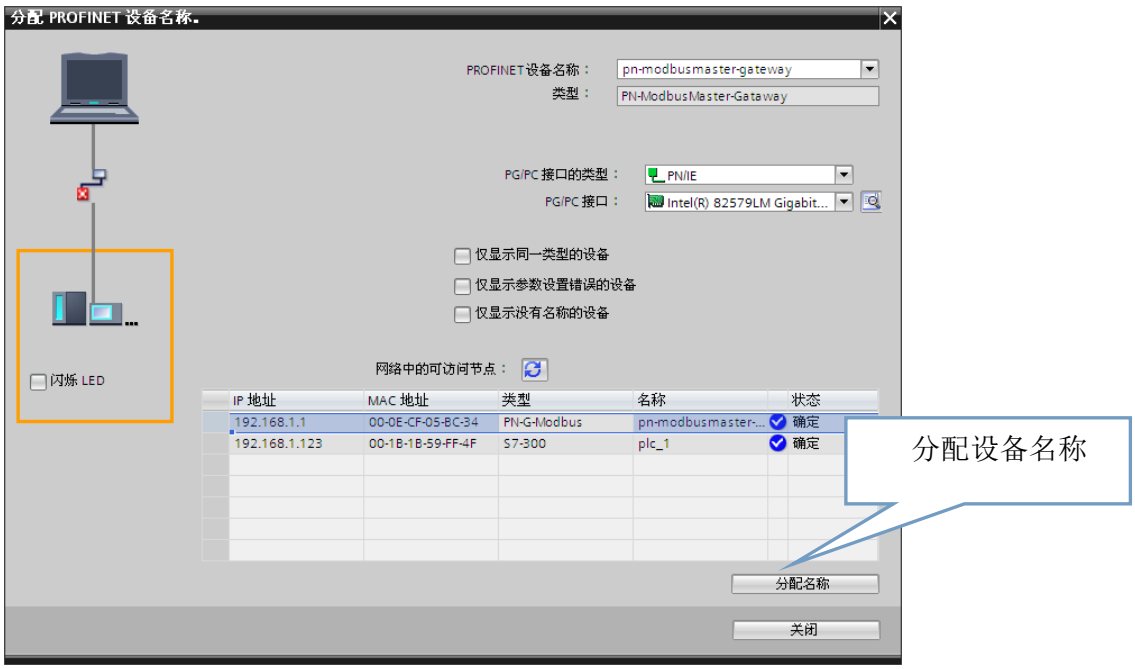






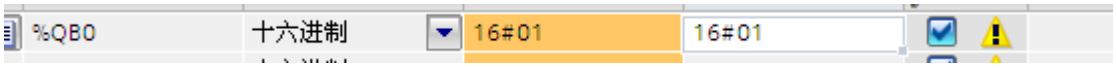
五、 PN-G-MODBUS 模块设备名称分配



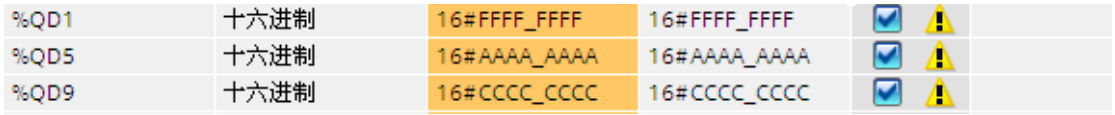


六、 *PN-G-MODBUS 数据测试*

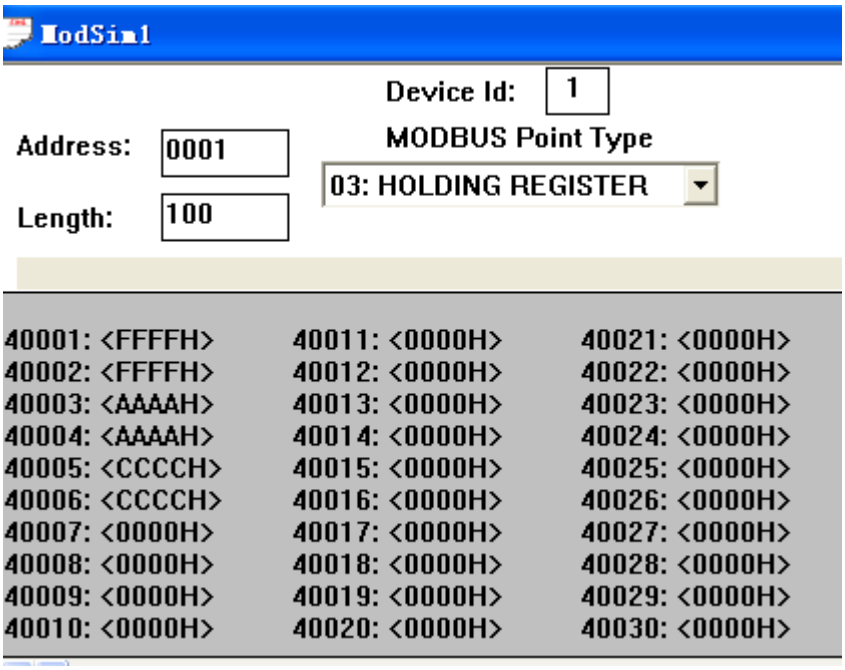
启动控制字：



博途 4 区写数据：

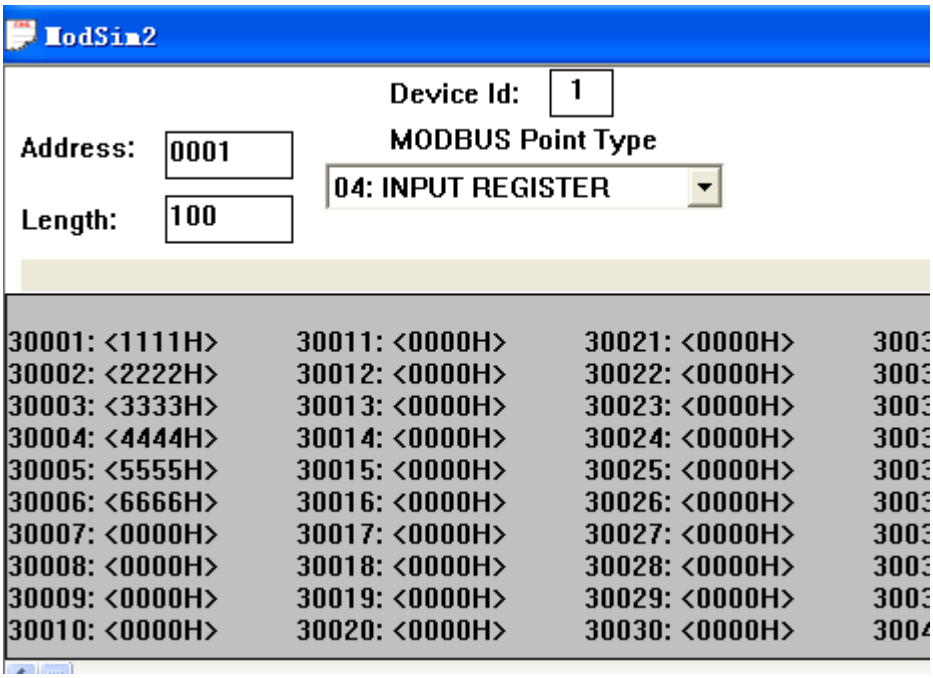


Modsim 监测数据：



博途读取 3 区数据：

%ID1	十六进制	16#1111_2222		
%ID5	十六进制	16#3333_4444		
%ID9	十六进制	16#5555_6666		

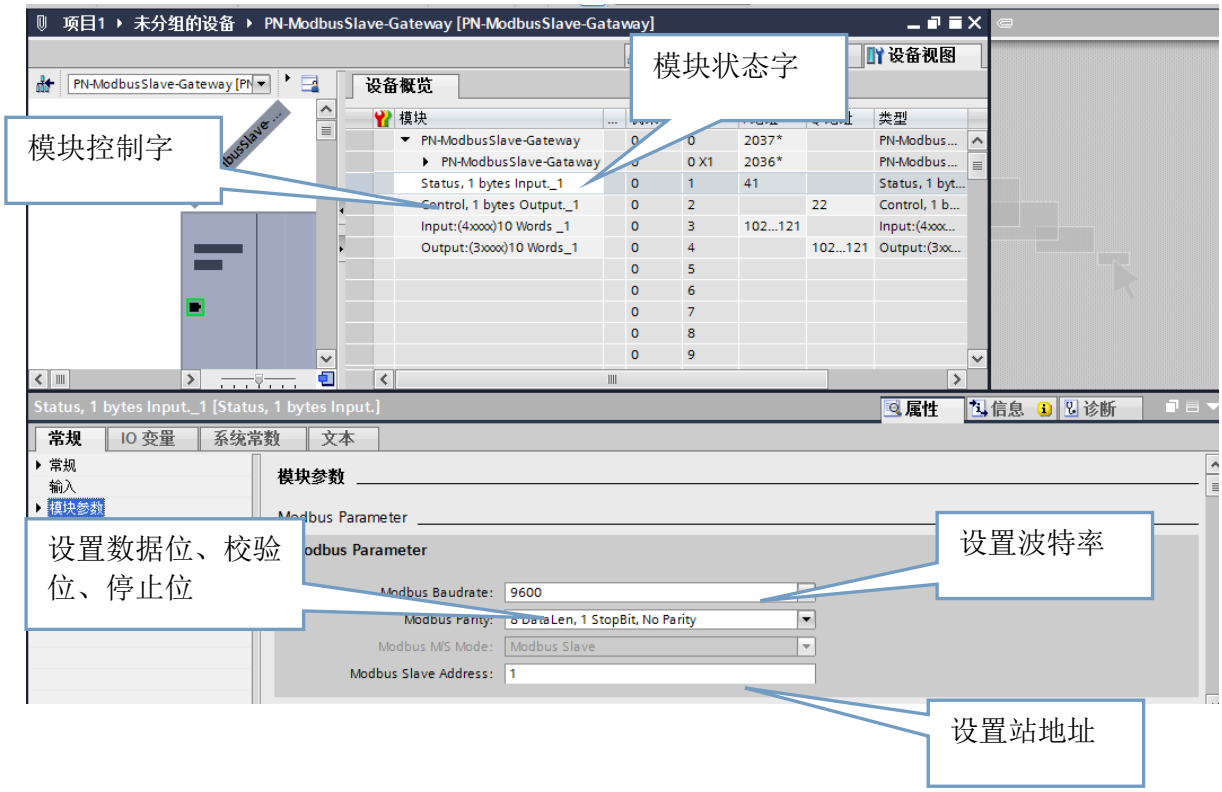


第五章 博途下 MODBUS 侧从站配置

一、从站模式配置

将模块底部拨码 bit1 拨至 on，模块重新上电，模块将以从站模式运行，同时工程需使用 GSDML-V2.3-DingShi-Gateway-ModbusS43-xxxxxxxx.xml。

二、modbus 通讯参数配置



三、从站模式下控制字、状态字含义

（1）、通信状态字格式

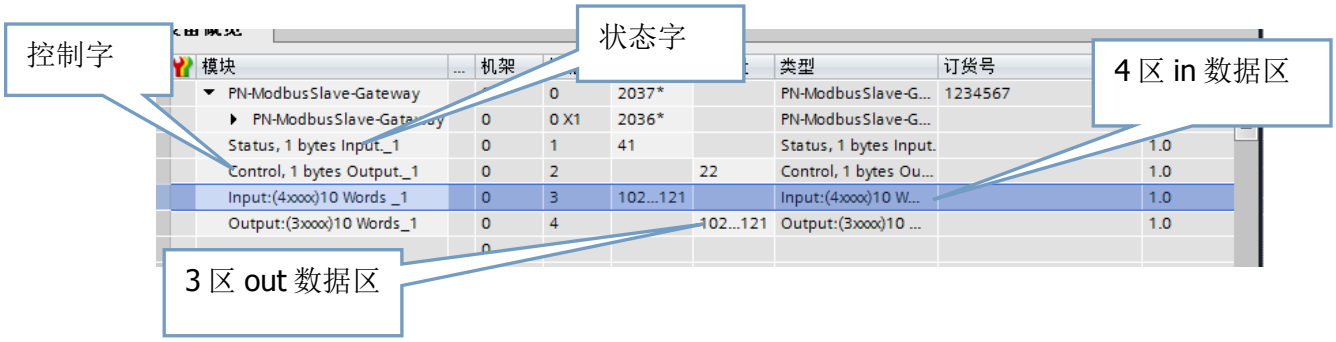
D7：oe_er	D6：CRC_er	D5	D4~D1：M_ER_CODE	D0：re_tr
奇偶校验错	CRC 校验错	不用	MODBUS 异常应答码	接收/发送

（2）、通信控制字格式

D7：clear_er	D6—D1	D0：PB_O_EN
清错误标记	不用	PROFIBUS 输出有效

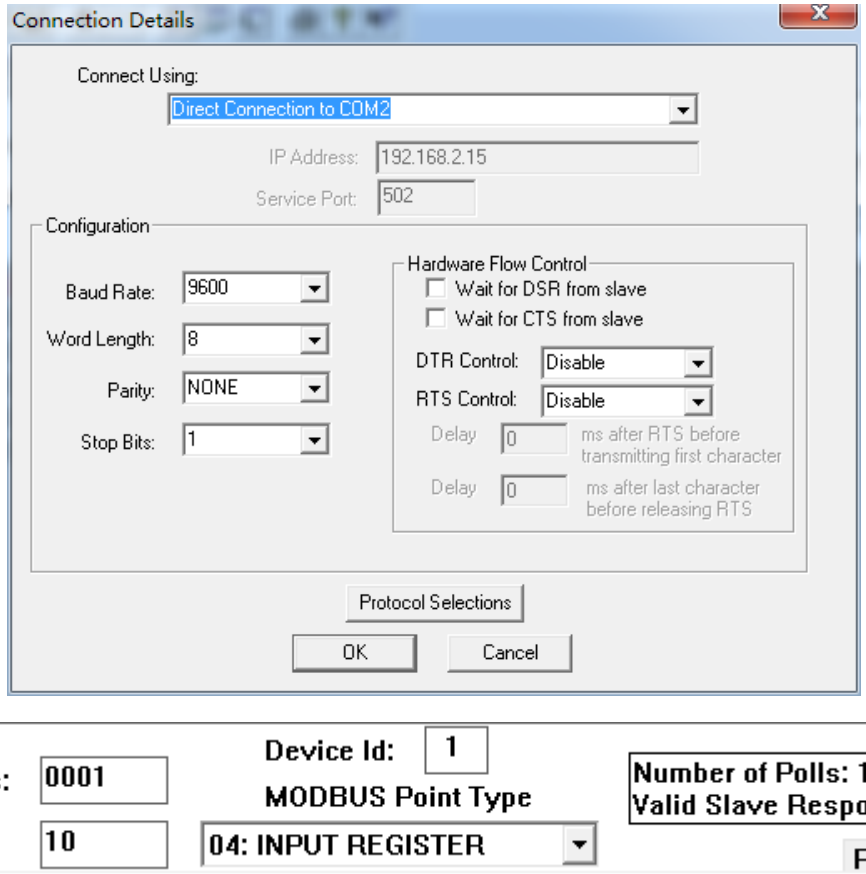
四、数据区配置

数据区地址均从地址 0 开始，modbus 从站寄存器地址根据插槽序号从小到大连续映射，假如 out 数据区及 in 数据区配置的均为 4 区，则 I/Q 区数据区数据将会同步一致。建议 out 配置在 3 区，in 配置在 4 区。

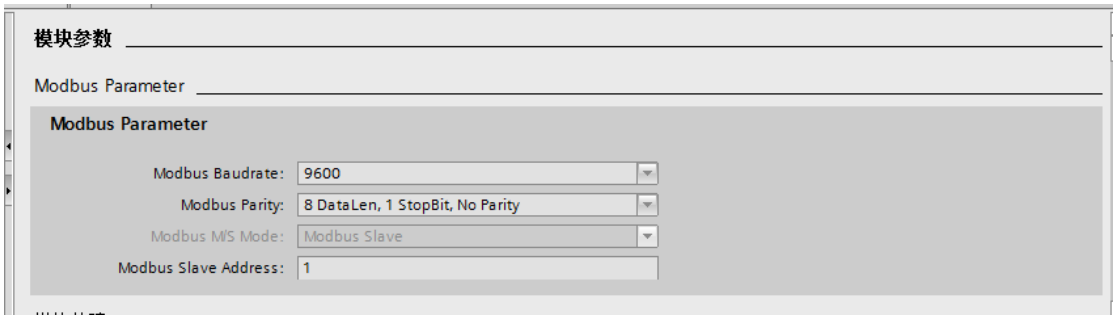


五、通讯参数及数据映射对应表

PC 机通过调试助手 modscan32 模拟 modbus 主站，与模块的 485 接口相连，调试助手 Modscan32 串口通讯参数：



Modscan32 通讯参数

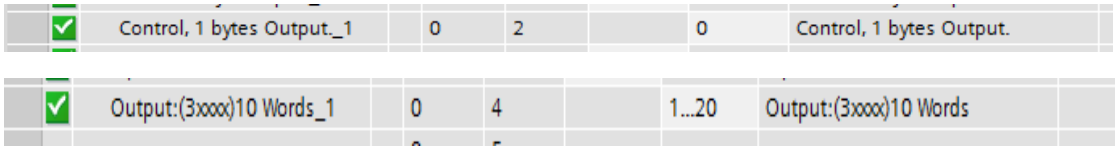


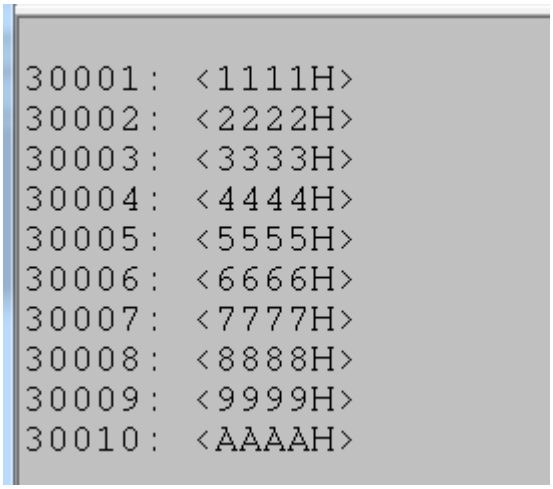
模块串口参数

模块串口参数必须与主站串口参数一致，否则通讯不成功。

输出数据区：

注意输出数据区 OUT 受到控制字控制，需将控制字最低位置 1 输出有效，样例中 Q0.0 置 1.





i	名称	地址	显示格式	监视值	修改值		注释
		%QB0	十六进制	16#01	16#01	☑ ⚠	
		%QW1	十六进制	16#1111	16#1111	☑ ⚠	
		%QW3	十六进制	16#2222	16#2222	☑ ⚠	
		%QW5	十六进制	16#3333	16#3333	☑ ⚠	
		%QW7	十六进制	16#4444	16#4444	☑ ⚠	
		%QW9	十六进制	16#5555	16#5555	☑ ⚠	
		%QW11	十六进制	16#6666	16#6666	☑ ⚠	
		%QW13	十六进制	16#7777	16#7777	☑ ⚠	
		%QW15	十六进制	16#8888	16#8888	☑ ⚠	
		%QW17	十六进制	16#9999	16#9999	☑ ⚠	
		%QW19	十六进制	16#AAAA	16#AAAA	☑ ⚠	
						☐	

输入数据区：

✓	Input:(4xxxx)10 Words _1	0	3	1...20		Input:(4xxxx)10 Words

```
40001:  <AAAAH>
40002:  <BBBBH>
40003:  <CCCCH>
40004:  <DDDDH>
40005:  <EEEEH>
40006:  <FFFFH>
40007:  <1234H>
40008:  <5678H>
40009:  <1111H>
40010:  <2222H>
```

i	名称	地址	显示格式	监视值	修...
		%IW1	十六进制	16#AAAA	
		%IW3	十六进制	16#BBBB	
		%IW5	十六进制	16#CCCC	
		%IW7	十六进制	16#DDDD	
		%IW9	十六进制	16#EEEE	
		%IW11	十六进制	16#FFFF	
		%IW13	十六进制	16#1234	
		%IW15	十六进制	16#5678	
		%IW17	十六进制	16#1111	
		%IW19	十六进制	16#2222	
		<添加>			

第六章 有毒有害物质表

根据中国《电子信息产品污染控制管理办法》的要求出台

部件名称	有毒有害物质和元素					
	铅（Pb）	汞（Hg）	镉（Cd）	六价铬（Cr（VI））	多溴联苯（PBB）	多溴二苯醚（PBDE）
塑料外壳	0	0	0	0	0	0
电路板	X	0	0	0	0	0
铜螺柱	0	0	0	0	0	0
贴膜	0	0	0	0	0	0
插座/插头	X	0	0	0	0	0
拨码开关	X	0	0	0	0	0

0：表示在此部件所用的所有同类材料中，所含的此有毒或有害物质均低于 SJ/T1163-2006 的限制要求；

X：表示在此部件所用的所有同类材料中，至少一种所含的此有毒或有害物质高于 SJ/T1163-2006 的限制要求。

注明：引用的“环保使用期限”是根据在正常温度和湿度条件下操作使用产品而确定的。

附录：MODBUS 技术简介

1. MODBUS 通信协议

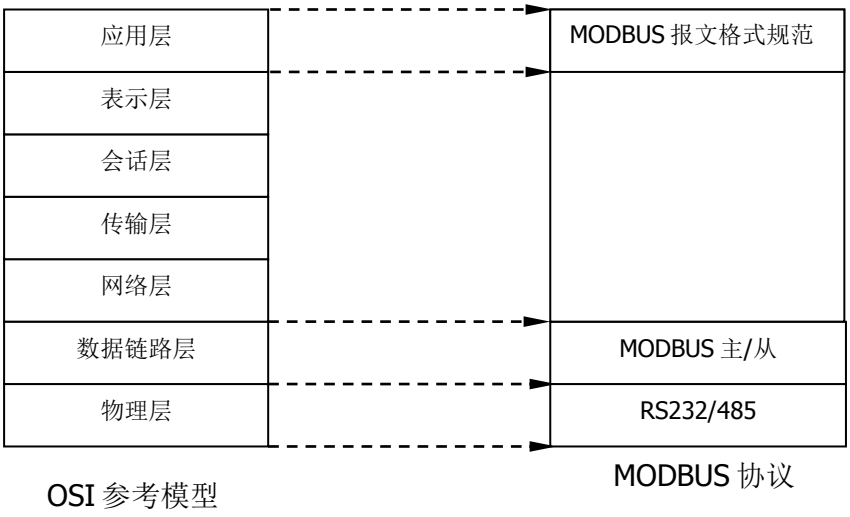
(1) Modbus 协议主要用于控制器之间的通信。通过此协议，两个控制器相互之间或控制器通过网络（例如以太网）和其它设备之间可以进行通信。目前有很多设备采用 MODBUS 的通信协议标准。

(2) 如果按照国际 ISO/OSI 的 7 层网络模型来说，标准 MODBUS 协议定义了通信物理层、链路层及应用层；

物理层：定义了基于 RS232 和 RS485 的异步串行通信规范；

链路层：规定了基于站号识别、主/从方式的介质访问控制；

应用层：规定了信息规范（或报文格式）及通信服务功能；



(3) 目前很多 MODBUS 设备应用都是基于 RS232/485，也有变化的 MODBUS 网络通信，只使用 MODBUS 的应用层（信息规范），而底层使用其它通信协议，如：底层使用以太网+TCP/IP 的 MODBUS 网络通信、底层使用无线扩频通信 MODBUS 网络等等。

2. MODBUS 协议要点

(1) MODBUS 是主/从通信协议。主站主动发送报文，只有与主站发送报文中呼叫地址相同的从站才向主站发送回答报文。

(2) 报文以 0 地址发送时为广播模式，无需从站应答，可作为广播报文发送，包括：

•修改线圈状态；

•修改寄存器内容；

•强置多线圈；

•预置多寄存器；

•询问诊断；

(3) MODBUS 规定了 2 种字符传输模式：ASCII 模式、RTU（二进制）模式；两种传输模式不能混用；

※ 本产品 PB-B-MODBUS 只能用于 RTU 模式。

特性	***RTU 模式***	***ASCII 模式***
编码	*二进制*	*ASCII（打印字符：0-9，a-z, A-Z）*
每个字符位数	*起始位:1 BIT*	*起始位:1 BIT*
	数据位:8 BITS	*数据位:7 BITS*
	奇偶校验位(可选):1 位	*奇偶校验位(可选):1 位*
	停止位:1 或 2	*停止位:1 或 2*
报文校验	*CRC(循环冗余校验)*	*LRC(纵向冗余校验)*

(4) 传输错误校验

→传输错误校验由奇偶校验、冗余校验检验。

→当校验出错时，报文处理停止，从机不再继续通信，不对此报文产生应答；

→通信错误一旦发生，报文便被视为不可靠；MODBUS 主机在一定时间过后仍未收到从站应答，即作出“通信错误已发生”的判断。

(5) 报文级（字符级）采用 CRC-16（循环冗余错误校验）

(6) MODBUS 报文 RTU 格式

小于 3.5 个字符的报文间隔时间	地址	功能码	数据	CRC 校验	小于 3.5 个字符的报文间隔时间
	1*byte	1*byte	N*bytes	2*bytes	

3. MODBUS 异常应答

(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 01：读 1 个 04A1 线圈值

从机地址	功能码	高位起始地址	低位起始地址	线圈数高位	线圈数低位	CRC
0A	01	04	A1	00	01	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）：

从机地址	功能码	异常码	CRC
0A	81	02	xxxx

(3) 异常应答码

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。若有询问命令发出，则本码表示在此之前无编程功能。*
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*	*数据字段中的值对于被编址的从机是禁止的。*
04	*相关设备故障*	*从机 PC 不能对报文或异常终止错误作出应答（见注 1）。*
05	*确认*	*从机 PC 已接受并正在处理长程序任务。应发出“探询”报文。查询该程序何时完成。若尚未完成，PC 会对“探询”报文发出否定应答（见注 2）。*
06	*忙碌、拒绝执行*	*收到报文无误，但 PC 已受约执行长程序命令。要求以后等 PC 有空时再传送。*
07	*否定*	*刚发送的编程功能无法执行，应发布“探询”报文以取得详细的设备错误信息。本码只对功能 13/14 有效（见注 2）。*
08	*存储器奇偶校验错误*	*扩展存储器的读数对正被访问的存储器数位进行检查。应在错误不会重复发生时进行复验。若所有复验均失败，应维修。*
注 1：对功能码 1—19，异常码 04 可表示：在应答设备发生不可校正的错误之前，只执行了有关询问报文的一部分。异常功能码 04 要求立即发布管理通告。		
注 2：只是在功能码 18 发生设备错误信息时，884 才支持异常功能码 05 和 06。至于异常码 05、06 和 07 之后发生的应答，可参阅具体设备手册的附录 A		

4. 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	00001~0XXXX， XXXX：与设备有关
1XXXX	输入线圈	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	保持/输出寄存器	字	读/写	40001~4XXXX， XXXX：与设备有关

5. MODBUS 功能

即 MODBUS 应用层，规定了 MODBUS 报文格式和服务功能。

(1) 读取输出状态

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
11	01	00	13(19)	00	25	XXXX

功能：读从站输出线圈 0XXXX 状态。

注意：报文中线圈起始地址 00000 对应设备中 00001 地址，其他顺延。

本例：读 11H 号从站输出线圈，起始地址=0013H=19，对应地址 00020；线圈数=0025H=37；末地址=00020+37-1=00056；

因此，本询问报文功能是：读 17（11H）号从站输出线圈 00020—00056，共 37 个线圈状态；

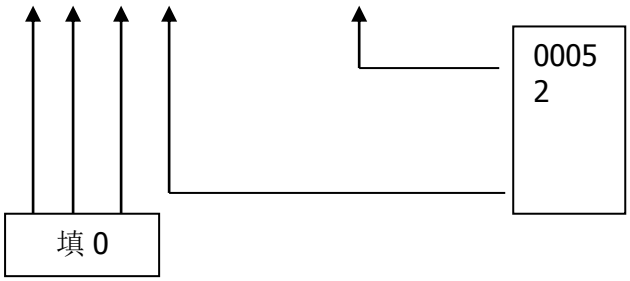
从站应答格式：

地址	功能码	字节计数	线圈状态 20-27	线圈状态 28-35	线圈状态 36-43	线圈状态 44-51	线圈状态 52-56	CRC
11	01	05	CD	6B	B2	0E	1B	XXXX

功能：从机返回输出线圈 0 XXXX 状态

本例：CD=11001101，对应 00020-00027；

1B= 0 0 0 1 1 0 1 1，对应 00052-00056；



（2）读取输入状态

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
11	02	00	C4	00	16	XXXX

本例：读 11H 号从站输入线圈，起始地址=00C4H=196，对应地址 10197；线圈数=0016H=22，末地址=10197+22-1=10218；

因此，本询问报文功能是：读 17（11H）号从站输入线圈 10197—10218，共 22 个输入线圈状态；

从站应答格式：

地址	功能码	字节计数	DI 10197-10204	DI 10205-10212	DI 10213-10218	CRC
11	02	03	AC	DB	35	xxxx

功能：从机返回 DI=1XXXX 状态

（3）读取保存寄存器

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
11	03	00	6B(107)	00	03	xxxx

功能：读从站保持寄存器 4XXXX 值。

注意：报文中寄存器起始地址 00000 对应设备中 40001 地址,其他顺延。

本例：读 11H 号从站保持寄存器值，起始地址=006BH=107，对应地址 40108；寄存器数=0003；末地址=40108+3-1=40110；

因此，本询问报文功能是：读 17（11H）号从站 3 个保持寄存器 40108—40110 的值；

从站应答格式：

地址	功能码	字节计数	寄存器 40108 高位	寄存器 40108 低位	寄存器 40109 高位	寄存器 40109 低位	寄存器 40110 高位	寄存器 40110 低位	CRC
11	03	06	02	2B	01	06	2A	64	XXXX

功能：从站返回保持寄存器 40108—40110 的值；(40108)=022BH，(40109)=0106H，(40110)=2A64H

(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
11	04	00	08	00	01	XXXX

功能：读从站输入寄存器 3XXXX 值。

注意：报文中寄存器起始地址 00000 对应设备中 30001 地址，其他顺延。

本例：读 11H 号从站输入寄存器值，起始地=0008H=0008，对应地址 30009；寄存器数=0001；末地址=30009；因此，本询问报文功能：读 17（11H）号从站 1 个保持寄存器 30009 的值；从站应答格式：

地址	功能码	字节计数	输入寄存器高位	输入寄存器低位	CRC
11	04	02	01	01	XXXX

功能：从站返回输入寄存器 30009 的值；（30009）=0101H

(5) 强置单线圈

功能码：05H

询问格式：

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
11	05	00	AC（172）	FF	00	XXXX

功能：强置 17 号从站线圈 0XXXX 值。报文中线圈起始地址 00000 对应设备中 00001 地址，其它顺延。

断通标志=FF00，置线圈 ON。

断通标志=0000，置线圈 OFF。

例：起始地址=00AC(H)=172，对应设备中的地址为 00173。强置 17 号从站线圈 0173 为 ON 状态 。

应答格式：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
11	05	00	AC（172）	FF	00	XXXX

功能：强置 17 号从机线圈 0173 ON 后原文返回

(6) 预置单保持寄存器

功能码：06H

询问格式：

地址	功能码	寄存器地址高位	寄存器地址低位	数据值高位	数据值低位	CRC
11	06	00	87 (135)	03	9E	XXXX

例：预置 17 号从机单保持寄存器 40136 值=0x039E；

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	数据值高位	数据值低位	CRC
11	06	00	87	03	9E	XXXX

功能：预置 17 号从机单保持寄存器 40136 值=0x039E 后原文返回。

（7）读取异常状态

功能码：07H

本产品 PB-B-MODBUS 暂不支持这一功能。

（8）回送校验

功能码：08H

本产品 PB-B-MODBUS 暂不支持这一功能。

（9）读取通信事件计数器

功能码：0BH

本产品 PB-B-MODBUS 暂不支持这一功能。

（10）读取通信事件计数器

功能码：0CH

本产品 PB-B-MODBUS 暂不支持这一功能。

（11）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
11	0F	00	13	00	0A	02	CD	00	XXXX

功能：将多个连续线圈 0XXXX 强置为 ON/OFF 状态。

注意：报文中线圈起始地址 00000 对应设备中 00001 地址，其他顺延。

本例：强置 11H 号从站多个连续线圈，线圈起始地址=0013H=19，对应地址 00020；线圈数=000AH=10；末地址=00020+10-1=00029；

因此，本询问报文功能是：强置 17（11H）号从站 10 个线圈 00020—00029 的值；CDH→00020-00027; 00H→00028-00029；

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
11	0F	00	13	00	0A	XXXX

（12）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
11	10	00	87	00	02	04	01	05	0A	10	XXXX

注意：报文中保持寄存器起始地址 40000 对应设备中 40001 地址，其他顺延。

本例：预置 11H 号从站多个保持寄存器值，寄存器起始地址=0087H=135，对应地址 40136，线圈数=0002H=2，末地址=40135+2-1=40137；

因此，本询问报文功能是：预置 17（11H）号从站 2 个保持寄存器值；0105H→40136; 0A10H→40137.

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
11	10	00	87	00	02	XXXXX

现场总线 PROFIBUS（中国）技术资格中心
北京鼎实创新科技股份有限公司
电话：010-82078264、010-62054940　　传真：010-82285084
地址：北京德胜门外教场口 1 号，5 号楼 A-1 室　邮编：100120
Web:www.c-profibus.com.cn　　Email: tangjy@c-profibus.com.cn