

# Modbus RTU/ASCII 转 Modbus TCP 协议转换器

## ODOT 系列网关 ODOT-S2E2

### 使用手册

*V1.9*

*2020.10.21*

## ODOT 系列网关 ODOT-S2E2



四川零点自动化系统有限公司

2014-09

版权©2014 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
2014-09-15	V1.00	发布版本	GJ
2014-12-05	V1.10	修改版本	GJ
2015-04-10	V1.20	修改版本	GJ
2016-07-14	V1.30	修改版本	LJP
2017-06-06	V1.5.0	修改版本	LJP
2018-06-01	V1.6.0	硬件改版	CCL
2019-11-08	V1.7.0	WINCC 应用 IP 地址修改	CCL
2020-08-10	V1.8.0	硬件改版	CCL
2020-10-21	V1.8.1	新增固件升级	CCL
2021-09-08	V1.9.0	诊断区修改	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。

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。四川零点自动化系统有限公司有权利在未通知用户的情况下修改本文档。

## 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。四川零点自动化系统有限公司有权利在未通知用户的情况下修改本文档。

## 固件信息

- 1、V1.4 及其以上固件版本支持 IAP 升级功能，用户可自己升级更高版本的固件。固件可咨询零点技术人员提供。
- 2、配置软件 MGCC ConfigV1.7 版本支持的固件版本为 V1.9 及以上。

## 软件下载

请登录零点自动化官网 [www.odot.cn](http://www.odot.cn)，在对应的产品页面点击下载。

## 目录

一、产品概述.....	7
1.1 产品功能.....	7
1.2 功能特点.....	7
1.3 技术参数.....	8
二、硬件说明.....	9
2.1 产品外观.....	9
2.2 指示灯说明.....	10
2.3 端子定义.....	11
2.4 复位开关.....	12
2.5 外接终端电阻.....	13
2.6 安装尺寸.....	14
三、如何使用网关.....	15
3.1 网关专用描述简介.....	15
3.1.1 串口工作模式.....	15
3.1.2 网关工作模式.....	15
3.1.3 网关数据存储区.....	15
3.1.4 系统诊断区.....	16
3.2 默认参数.....	19
3.3 网关 IP 地址修改.....	20
3.4 典型应用说明.....	23
3.4.1 实现 Modbus TCP 客户端与 Modbus RTU/ASCII 从站通讯.....	23
3.4.1.1 应用拓扑图.....	23
3.4.1.2 透传模式配置.....	23
3.4.1.3 映射模式配置.....	29
3.4.2 实现 Modbus TCP 客户端与 Modbus RTU/ASCII 主站通讯.....	36
3.4.2.1 应用拓扑图.....	36
3.4.2.2 简单配置.....	36

3.4.3 实现 Modbus RTU/ASCII 主站之间的通讯.....	42
3.4.3.1 应用拓扑图.....	42
3.4.3.2 简单配置.....	42
3.4.4 实现 Modbus TCP 客户端与 Modbus RTU/ASCII 主站同时访问一路 Modbus RTU/ASCII 从站.....	48
3.4.4.1 应用拓扑图.....	48
3.4.4.2 简单配置.....	48
四、在西门子 STEP7 的测试应用.....	56
4.1 网关 ODOT-S2E2 的配置.....	56
4.2 在西门子 STEP 7 的配置测试.....	57
五、在西门子 TIA V14 的测试应用.....	64
5.1 网关 ODOT-S2E2 的配置.....	64
5.2 软件 TIA V14 的配置测试.....	66
六、在上位机 WINCC V7.0 的测试应用.....	70
6.1 网关 ODOT-S4E2 的配置.....	70
6.2 上位机 WINCC 的配置测试.....	72
七、固件升级.....	76
八、附录.....	78
8.1 Modbus-RTU 协议简介.....	78
8.1.1 Modbus 存储区.....	78
8.1.2 Modbus 功能码.....	78
8.2 串口网络拓扑结构简介.....	85
8.2.1 RS232.....	85
8.2.2 RS422.....	86
8.2.3 RS485.....	88

# 一、产品概述

## 1.1 产品功能

本产品是四川零点自动化系统有限公司根据市场需求以及多年的经验而开发的一款 Modbus RTU/ASCII 到 Modbus TCP 的协议转换器。

凡是具有 RS485 接口并支持 Modbus RTU/ASCII 的从站设备都可以通过本网关连接到 Modbus TCP 网络，和 TCP 客户机通信。从而实现将低速串口设备连接到高速以太网中，实现数据的高速传输。网关有“透传”和“映射”两种不同的工作模式可选，可实现最大的系统兼容性。

## 1.2 功能特点

- ◆ 9-36V 宽电压输入，防反接保护。DC-DC 隔离电源，3000V 隔离电压。
- ◆ 2KV 网口隔离保护，10M/100Mbps 速率自适应，自动 MDI/MDIX 翻转。
- ◆ 体积小巧，仅 1 元硬币直径厚度，节省安装空间。
- ◆ 支持地址映射模式，实现对 TCP 客户端请求的快速响应。
- ◆ 支持多达 10 个 TCP 客户机访问。
- ◆ 映射模式支持功能码：0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x0F, 0x10。
- ◆ 透传模式支持所有公共功能码和自定义功能码。
- ◆ 6KB 超大数据缓存区，数据传输量更大。
- ◆ RS485 双串口实时刷新，扫描周期短，带载能力强。
- ◆ RTU 和 ASCII 的主、从站模式可选，适应性强。
- ◆ 看门狗可选择使能，看门狗时间可设定。
- ◆ 支持 IAP 下载，通过网口对产品中的固件程序进行更新升级。
- ◆ RS485 带浪涌保护，内置偏置电路，稳定性强。需外接终端电阻。
- ◆ 设备自带强大诊断功能，实时监控从设备通信状态。
- ◆ 支持一键复位功能，恢复出厂设置。
- ◆ 35mm 标准导轨安装。
- ◆ EMC 符合 EN 55022:2010 & EN55024:2010 国际标准。

## 1.3 技术参数

本产品相关技术参数如下表所示，请在本产品的参数范围内使用本产品，以便获得更好的性能。

环境参数	
工作温度范围	-40~85℃
存储温度范围	-55~125℃
工作湿度范围	5%~95% (无冷凝)
电源参数	
电源端口数量	1 路
输入电压范围	9~36VDC, 3KV 隔离电压
功耗	Max. 100mA@24V
以太网参数	
网关工作模式	透明传输模式、地址映射模式可选, Modbus TCP 协议
以太网端口数量	2 个 RJ45, 2KV 浪涌保护, 10M、100M 自适应速率
网络协议	ETHERNET、ARP、IP、TCP、ICMP
TCP 连接数量	最大 10 个
串口参数	
串口数量	双路 RS485
串行通信模式	RTU 模式和 ASCII 模式可选
串口终端电阻	需外置 120Ω 电阻
支持的波特率	1200~115200 bps
支持的校验模式	无校验、奇校验、偶校验
支持的从站数量	最大 62 个 (不带中继器)
映射模式协议功能码	0x01、0x02、0x03、0x04、0x05、0x06、0x0F、0x10
Modbus 数据存储区	0xxxx 区 (线圈): 8192 Bit 1xxxx 区 (离散量输入): 8192 Bit 3xxxx 区 (输入寄存器): 2048 Word 4xxxx 区 (保持寄存器): 2048 Word 3xxxx 区 (系统诊断区): 263 Word



## 二、硬件说明

### 2.1 产品外观



## 2.2 指示灯说明

设备共有五个 LED 状态指示灯，其符号定义及状态说明如“表 2.1”所示。

表 2.1 指示灯说明

符号	定义	状态	说明
PWR	电源指示	ON	电源接通
		OFF	电源未接通
ETH	网关状态指示	ON	TCP 网关通信错误
		OFF	TCP 网关通信正常
TX1	串口1发送指示灯	闪烁	串口1在发送数据
		OFF	串口1未发送数据
RX1	串口1接收指示灯	闪烁	串口1在接收数据
		OFF	串口1未接收数据
TX2	串口2发送指示灯	闪烁	串口2在发送数据
		OFF	串口2未发送数据
RX2	串口2接收指示灯	闪烁	串口2在接收数据
		OFF	串口2未接收数据

注：\*——正常通讯时，ODOT-S2E2网关指示灯的状态

## 2.3 端子定义

设备接线采用 3Pin 和 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。

电源端子定义

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

RS485 端子定义

序号	端子	定义
1	1B-	串口1 RS485-
2	1A+	串口1 RS485+
3	SGND	信号地
4	PE	接地
5	2B-	串口2 RS485-
6	2A+	串口2 RS485+
7	SGND	信号地
8	PE	接地
9-16	NC	空

## 2.4 复位开关



可采用回形针点击复位按钮，所有指示灯闪亮一次表示复位成功。网关复位成功，网关的技术参数如下：

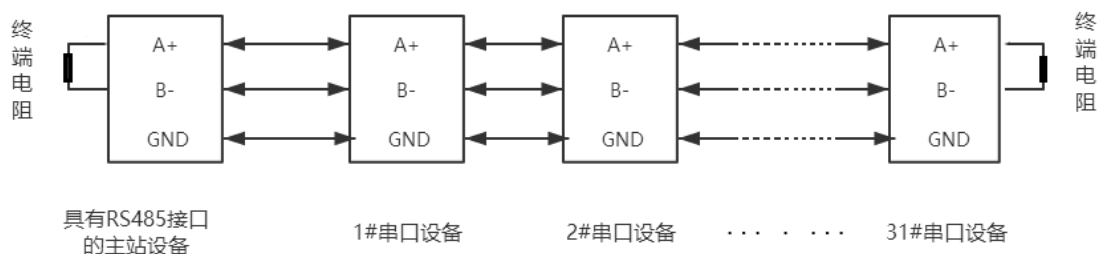
	参数名称	默认值
以太 网 侧	协议转换器 IP	192.168.1.254
	子网掩码	255.255.255.0
	局域网网关 IP	192.168.1.1
	Modbus TCP 数据端口	502
	配置端口	1024
	Modbus-TCP 看门狗时间	30S
	Modbus-TCP 看门狗是否使能	使能
	网关工作模式	透传模式
	网关站号	247
串 口 侧	串口工作模式	主站模式
	Modbus 协议类型	Modbus RTU
	串口波特率	9600bps
	校验位	无校验
	数据位	8位
	停止位	1位
	接收字符间隔	3.5t
	报文发送安格	0
	超时处理方式	数据保持
从站响应超时时间	500ms	

## 2.5 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。



## 2.6 安装尺寸



## 三、如何使用网关

### 3.1 网关专用描述简介

#### 3.1.1 串口工作模式

该网关的每个串口都具有两种工作模式：**主站模式**与**从站模式**

串口工作于主站模式时，该串口在不加中继的情况下最多可以连接 31 台 Modbus RTU/ASCII 从站设备；该模式主要用于 Modbus TCP 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；该模式可进行如下应用：

- (1) 实现 Modbus TCP 客户端与 Modbus RTU/ASCII 主站之间的数据通讯；
- (2) 实现 Modbus RTU/ASCII 主站之间的数据通讯；
- (3) 实现 Modbus TCP 客户端与 Modbus RTU/ASCII 主站同时与一路 Modbus RTU/ASCII 从站进行数据通讯；

#### 3.1.2 网关工作模式

网关有“透传”和“映射”两种工作模式可选，在出厂设置下为“透传”模式。“透传”模式下没有数据缓存，不用编辑从站地址映射表，网关在接收到 Modbus TCP 客户机的指令后直接将指令下发到 Modbus RTU/ASCII 从站设备，并等待从站设备响应，从站设备响应后再直接将数据返回给 TCP 客户机。“映射”模式采用**数据缓存**方式，需编辑从站地址映射表，网关上电后轮询各从站，并将数据存储于**数据缓存区**，网关在接收到 Modbus TCP 客户机的指令后，直接从**数据缓存区**读取数据，然后返回给 TCP 客户机。此方式可大大减少客户机访问从站时的等待时间，提高刷新速率。

#### 3.1.3 网关数据存储区

数据存储区分为五个部分，第一部分为“**线圈**” (DO) 存储区域，共 8192 点。第二部分为“**离散量输入**” (DI) 存储区域，共 8192 点。第三部分为“**输入寄存**

器” (AI) 存储区域, 共 2048 个字。第四部分为“保持寄存器” (A0) 存储区域, 共 2048 个字, 第五部分为“系统诊断”存储区域, 存储从站设备的工作状态, 共 263 个字。访问“系统诊断区”可获得从站的信息, 可用于设置从站断线报警等功能。数据存储区的分配及地址编码范围如“表 3.1”所示。

表 3.1 数据存储区地址表

序号	存储类别	说明	存储容量	地址范围
1	0区	线圈	8192 Bit	0x0000~0x1FFF
2	1区	离散量输入	8192 Bit	0x0000~0x1FFF
3	3区	输入寄存器	2048 Word	0x0000~0x07FF
4	4区	保持寄存器	2048 Word	0x0000~0x07FF
5	3区	系统诊断	263 Word	0x2000~0x2106

### 3.1.4 系统诊断区

系统诊断区分为两部分,

第一部分: 地址 0x2000-0x2003 共 4 个 word, 为“从站错误指示区”,

0x2000-0x2001 是 COM1 接口下的 31 个从站错误指示区。

0x2002-0x2003 是 COM2 接口下的 31 个从站错误指示区。

当从站通信出现错误时, 按照配置软件里组态的从站设备的地址大小, 从小到大相应从站的位被置 1。从站恢复正常后对应的错误指示位将自动清零。其数据编码格式如“表 3.2”所示。

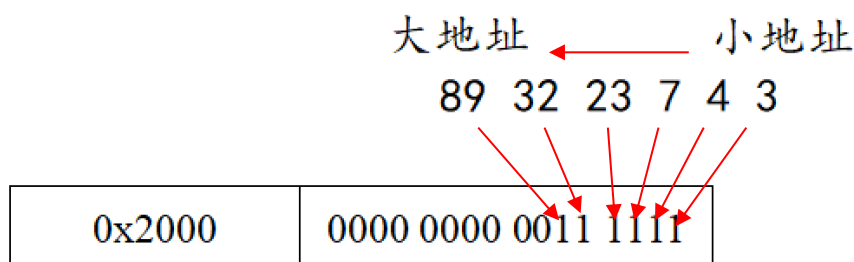
表 3.2 从站错误指示区编码格式

串口	Modbus 地址	数据(二进制显示)	备注
COM1	0x2000	0000 0000 0000 0000	按照组态的从站设备地址大小, 从小到大排序诊断显示。(不是按照站地址排序)
	0x2001	0000 0000 0000 0000	
COM2	0x2002	0000 0000 0000 0000	
	0x2003	0000 0000 0000 0000	

举例: COM1 接口配置了从站 32、3、4、7、23、89 共六个从站设备, 在 0x2000



地址低 6 位有效，若是这 6 个站均报错，相应诊断区数值为：



第二部分：地址 0x200F-0x208A 共 124 个 Word，为“从站状态指示”区，0x200F-0x204C（62 个 word）是 COM1 接口的从站站地址及错误代码显示，0x204D-0x208A（62 个 word）是 COM2 接口的从站站地址及错误代码显示，读取该区可获得从站的相应串口的站地址及当前工作状态，其数据编码格式如“表 3.3”所示。

表3.3从站状态指示区编码格式

Modbus 地址 (16进制)	Modbus 地址 (10进制)	高字节	低字节	备注
0x200F	8207	Byte1	Byte0	01指的是串口1 COM1接口的从站站地址及错误代码显示
		01	站地址	
0x2010	8208	Byte1	Byte0	
		功能码	错误代码	
...	...	...	...	
0x204B	8267	Byte1	Byte0	
		01	站地址	
0x204C	8268	Byte1	Byte0	
		功能码	错误代码	
0x204D	8269	Byte1	Byte0	02指的是串口2 COM2接口的从站站地址及错误代码显示
		02	站地址	
0x204E	8270	Byte1	Byte0	
		功能码	错误代码	
...	...	...	...	
0x2089	8329	Byte1	Byte0	
		02	站地址	
0x208A	8330	Byte1	Byte0	
		功能码	错误代码	

每一个从站诊断区有 2 个 Word 地址显示，均分为高低两个字节。

前一个 Word，Byte1 为高字节，指示当前从站所挂载串口号。Byte0 为低字节，指示从站站地址。

后一个 Word，Byte1 为高字节，指示当前执行的映射到从站的功能码。Byte0 为低字节，指示当前从站通信的错误代码。从站错误代码的具体含义如“表 3.4”所示。

表 3.4 从站错误代码说明

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
0x02	非法数据地址	设备数据超出其地址范围，参考从站手册
0x03	非法数据值	数据长度错误，数据长度超出最大允许值
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
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
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

## 3.2 默认参数

网关默认出厂配置如下：

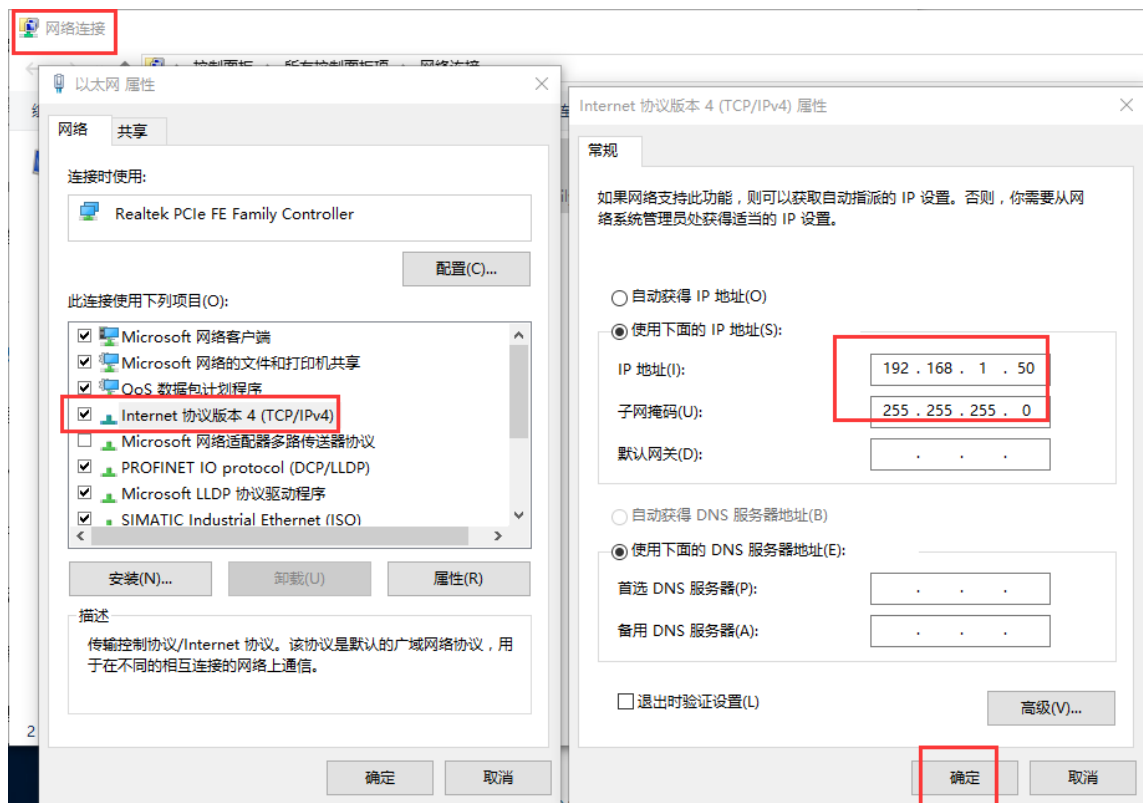
表 3.5 网关出厂默认配置

	参数名称	默认值
以太网侧	协议转换器 IP	192. 168. 1. 254
	子网掩码	255. 255. 255. 0
	局域网网关 IP	192. 168. 1. 1
	Modbus TCP 数据端口	502
	配置端口	1024
	Modbus-TCP 看门狗时间	30S
	Modbus-TCP 看门狗是否使能	使能
	网关工作模式	透传模式
	网关站号	247
串口侧	串口工作模式	主站模式
	Modbus 协议类型	Modbus RTU
	串口波特率	9600bps
	校验位	无校验
	数据位	8位
	停止位	1位
	接收字符间隔	3.5t
	报文发送安格	0
	超时处理方式	数据保持
	从站响应超时时间	500ms

注：网关出厂设置工作在透传模式下，可以免配置使用，此时 TCP 客户机所有的请求数据被发送到串口 1 上。若要配置网关的参数请使用软件“odot MGCC Config”进行配置，软件安装包位于随机光盘中，或拨打四川零点自动化系统有限公司咨询热线：400-0024-485。

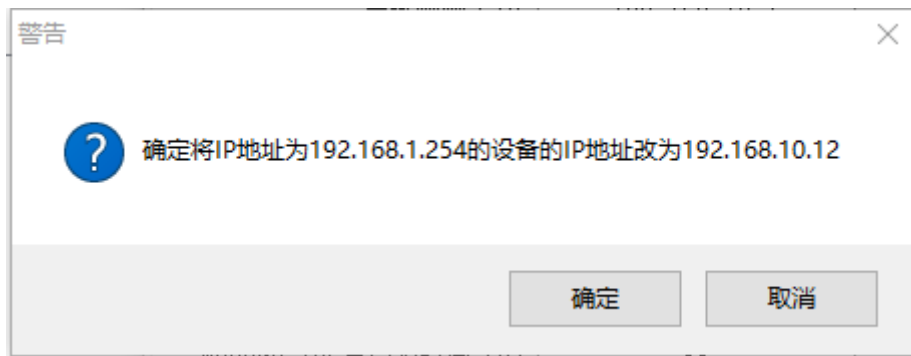
### 3.3 网关 IP 地址修改

首先给网关供电 24VDC，网线连接网关和电脑，将电脑的本机网卡 IP 地址改到 192.168.1.\*网段，然后打开配置软件 MGCC Config，点击上载网关配置，保证正常与网关通讯（能正常上载、下载网关配置）。

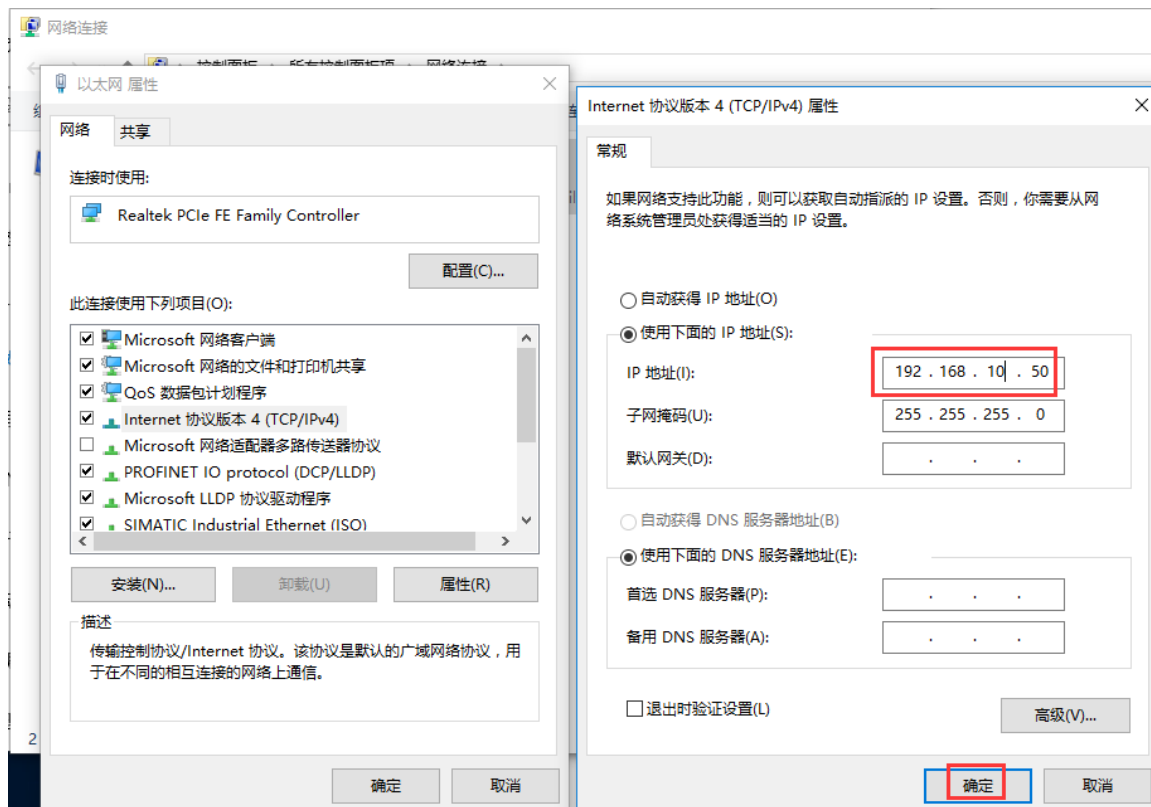


修改配置软件界面的网关 IP 地址为：192.168.10.12（跨网段），局域网网

关 IP 改为：192.168.10.1，修改完成后直接点击下载网关配置，会弹出一个警告框，确定是否修改 IP 地址，点击确定，在右下角可以看见下载成功。



IP 地址修改成功后，需要将本机电脑 IP 地址改到：192.168.10.\*网段。



在配置软件 MGCC Config 界面点击上载网关配置。上载成功后，可在右下角看见上载成功。



## 3.4 典型应用说明

### 3.4.1 实现 Modbus TCP 客户端与 Modbus RTU/ASCII 从站通讯站通讯

#### 3.4.1.1 应用拓扑图

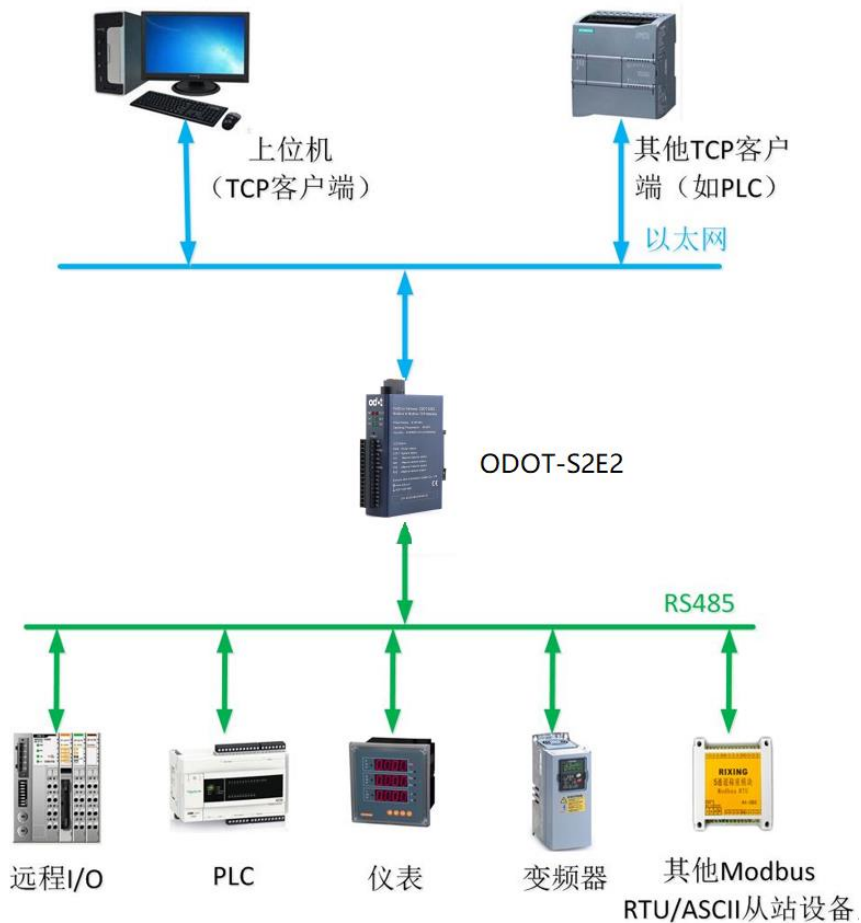


图 3.1 系统拓扑图

#### 3.4.1.2 透传模式配置

一. 打开软件配置软件“odot MGCC Config”，右击从站配置页面选择“添加设备”，添加“ODOT-S2E2”。

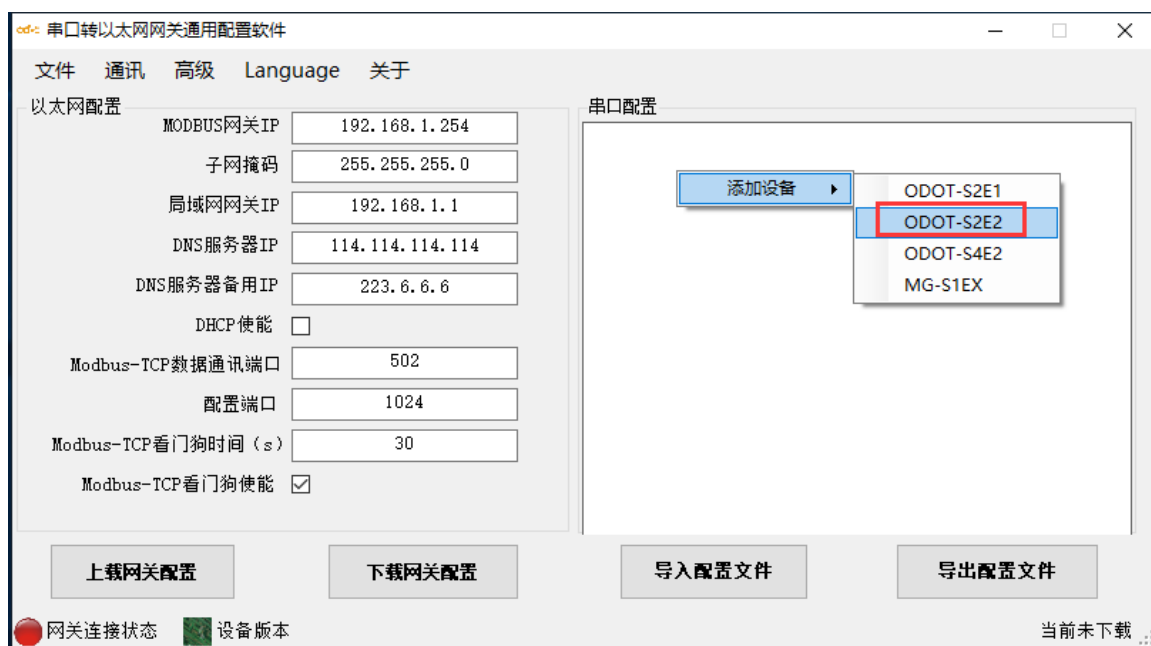


图 3.2 添加设备

二. 双击“ODOT-S2E2”，或右击“ODOT-S2E2”，选择“设备串口公共属性”，在弹出的设置页面将网关工作模式设置为“透传模式”。

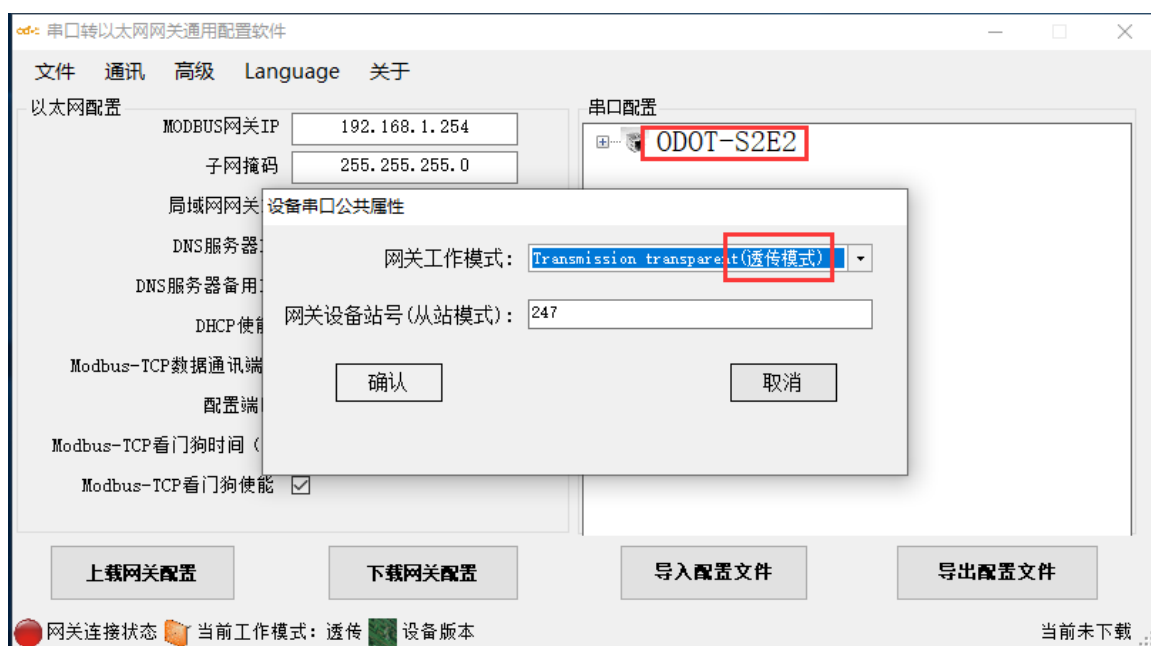


图 3.3 设置网关工作模式

三. 双击“COM1”或“COM2”或右击“COM1”或“COM2”并单击“串口属性”，弹出“串口设置”窗口，设置通讯参数后点击“确认”按钮保存并返回。

各参数含义如下：



### 工作模式：

用于设置网关在该串口所连接的网络中作为主站还是从站，默认为主站模式，此处设置为主站模式。

### Modbus协议类型：

用于设置网关在该串口所连接的网络中与其他设备通信所用协议的类型，Modbus RTU/ASCII 可选，请将该参数设置为与该串口所连接的设备一致。

### 波特率：

串口波特率，可选范围 1200~115200bps，默认 9600bps，请将该参数设置为与该串口所连接的设备一致。

### 校验位：

可选择无校验、奇校验、偶校验，默认无校验，请将该参数设置为与该串口所连接的设备一致。

### 停止位：

1 位、2 位停止位可选，默认 1 位停止位。请将该参数设置为与该串口所连接的设备一致。

### 接收字符间隔：

接收报文时的帧间隔检测时间， $1.5t \sim 200t$  可选，默认  $3.5t$  ( $t$  为单个字符传送的时间，和波特率有关)。一般情况下，不用更改此参数。

### 报文发送间隔：

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)，0ms-65535ms 可设，默认 0ms，建议设置 100ms，防止连接的设备因反应太慢而出现通讯故障。

### 超时处理方式：

读从站数据，如果从站响应超时的数据处理方式，可选择“数据清零”或“数据保持”。默认“数据保持”模式，此参数只对 Modbus 读命令有效，请根据实际需求设置此数值。

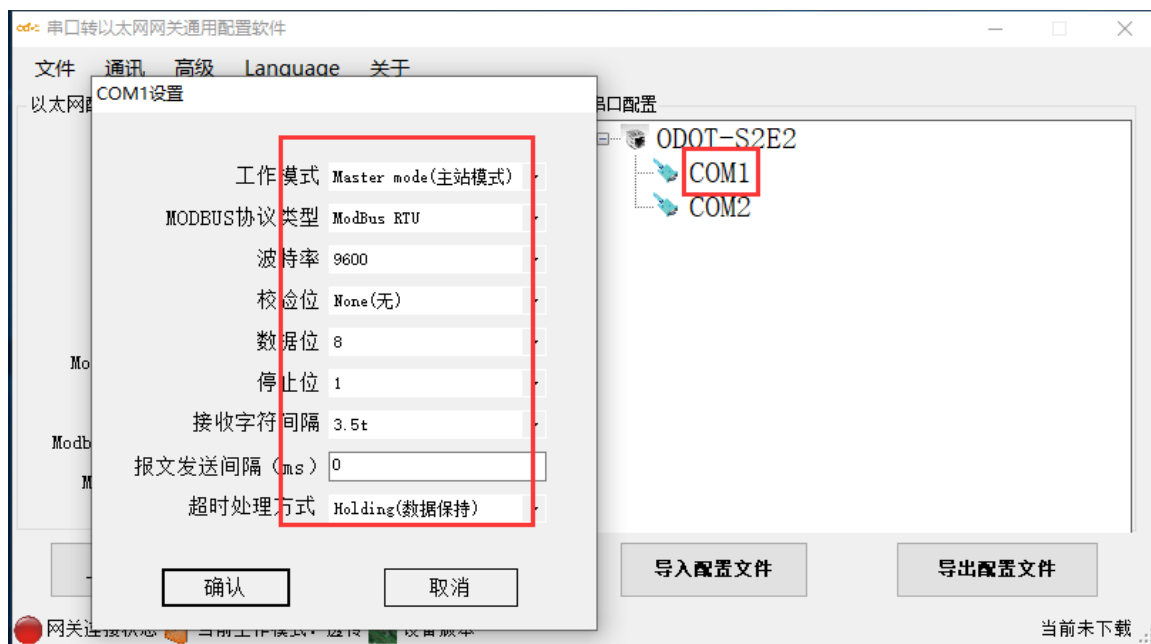


图 3.4 设置串口属性

四. 选中“COM1”或“COM2”，单击右键选择添加从站，输入“从站名称”，填入“从站站号”和从站“响应超时”时间，点击“确认”返回。设备上的各从站站号不能相同，不能与设备站号相同，且从站地址范围在 1-247 之间，同一串口下的从站名不能相同。“响应超时”时间需查看从设备的手册获取，建议设置在 500ms 以上，点击“确认”。

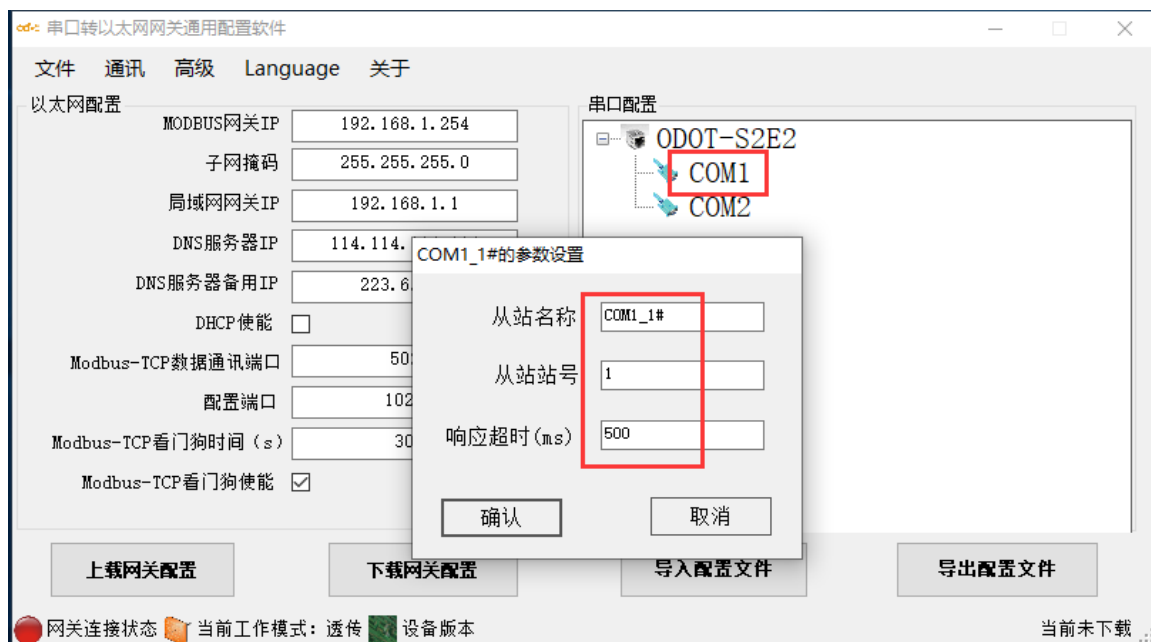


图 3.5 添加从站

五. 通过配置软件左半部分的“以太网配置”对网关的以太网参数进行配置。

部分参数含义如下：

Modbus 网关 IP：设备自身 IP 地址；

子网掩码：设备的子网掩码；

局域网网关 IP：设备所在网络的网关 IP 地址；

Modbus-TCP 数据通讯端口：一般为 502；

配置端口：配置软件通过设备的该端口下载配置到设备；

Modbus-TCP 看门狗时间：网关从接收到最后一条 Modbus TCP 报文到进行自动重启的时间间隔；注：网关自动重启动可以及时释放掉长期没有使用的连接资源；

Modbus-TCP 看门狗使能：是否使能看门狗功能。



图 3.6 设置设备以太网属性

六. 通过“通讯”——“通讯配置”设置想要下载的目标网关地址以及下载使用的通讯端口号，默认为网关出厂默认 IP 192.168.1.254 以及端口号 1024。



图 3.7 软件与网关的通讯配置

七. 单击“**下载网关配置**”按钮，下载配置参数到网关。下载成功后状态栏右下角显示“**下载成功**”提示，下载成功后网关自动重启，并进入到运行状态。如果下载失败，请检查电脑 IP 地址与网关 IP 地址是否在同一个网段，并检查网关 IP 地址是否设置正确，如果忘记网关 IP 地址，可以通过复位键对网关进行复位操作，复位后网关 IP 地址为出厂默认 IP 地址。单击“**导入配置文件**”和“**导出配置文件**”可导入和保存配置文件到本地磁盘。单击“**上载网关配置**”，可以将网关当前配置上传至软件。**注：进行下载、上载操作时，需保证电脑与网关在同一网段。**



图 3.8 下载网关配置

八. 完成上述设置后 Modbus TCP 客户端可使用 Modbus TCP 协议，通过网关 IP 地址 192.168.1.254、Modbus 数据通讯端口 502 以及从站站号 1 访问到站号为 1 的从站设备 16DI。

### 3.4.1.3 映射模式配置

一. 打开软件配置软件“odot MGCC Config”，右击从站配置页面选择“添加设备”，添加“ODOT-S2E2”。

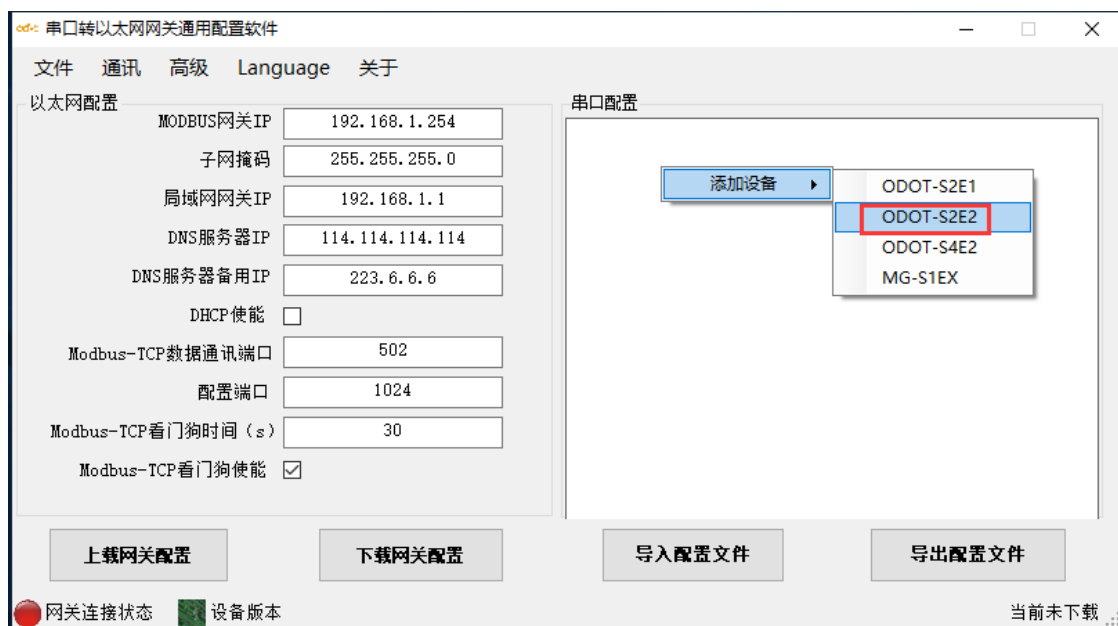


图 3.9 添加设备

二. 双击“ODOT-S2E2”，或右击“ODOT-S2E2”，选择“设备串口公共属性”，在弹出的设置页面将网关工作模式设置为“映射模式”。

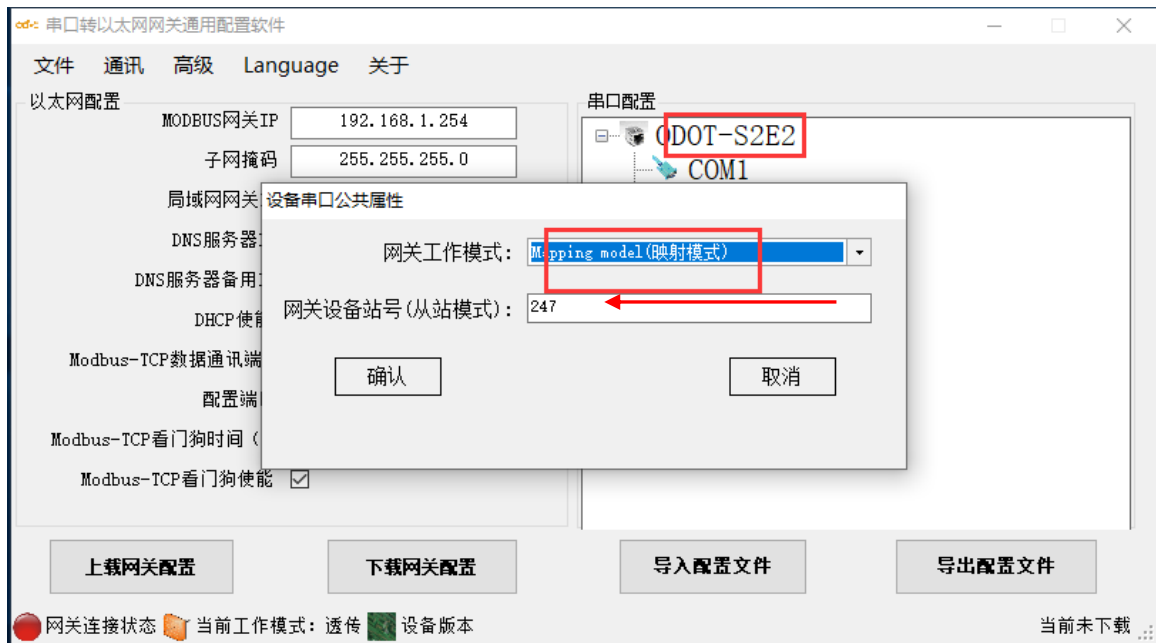


图 3.10 设置网关工作模式

三. 双击“COM1”或“COM2”或右击“COM1”或“COM2”并单击“串口属性”，弹出“串口设置”窗口，设置通讯参数后点击“确认”按钮保存并返回。

各参数含义如下：

**工作模式：**

用于设置网关在该串口所连接的网络中作为主站还是从站，默认为主站模式，此处设置为主站模式。

**Modbus 协议类型：**

用于设置网关在该串口所连接的网络中与其他设备通信所用协议的类型，Modbus RTU/ASCII 可选，请将该参数设置为与该串口所连接的设备一致。

**波特率：**

串口波特率，可选范围 1200~115200bps，默认 9600bps，请将该参数设置为与该串口所连接的设备一致。

**校验位：**

可选择无校验、奇校验、偶校验，默认无校验，请将该参数设置为与该串口所连接的设备一致。

**停止位：**

1 位、2 位停止位可选，默认 1 位停止位。请将该参数设置为与该串口所连接的设备一致。

#### 接收字符间隔：

接收报文时的帧间隔检测时间， $1.5t \sim 200t$  可选，默认  $3.5t$  ( $t$  为单个字符传送的时间，和波特率有关)。一般情况下，不用更改此参数。

#### 报文发送间隔：

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)， $0ms \sim 65535ms$  可设，默认  $0ms$ ，建议设置  $100ms$ ，防止连接的设备因反应太慢而出现通讯故障。

#### 超时处理方式：

读从站数据，如果从站响应超时的数据处理方式，可选择“数据清零”或“数据保持”。默认“数据保持”模式，此参数只对 Modbus 读命令有效，请根据实际需求设置此数值。

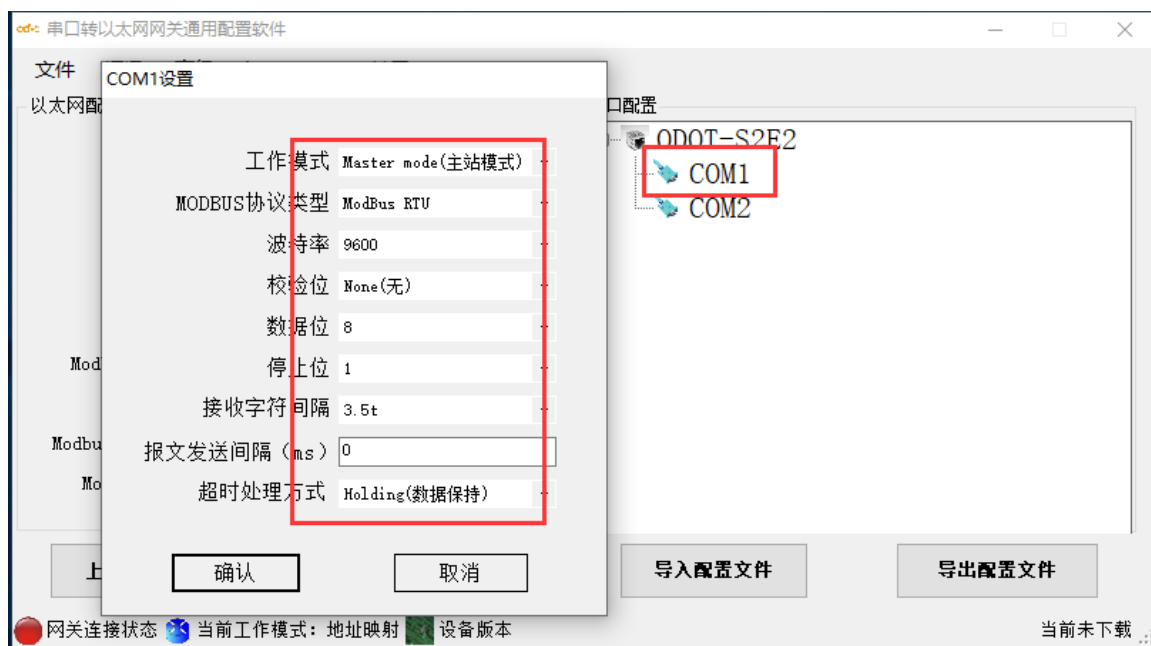


图 3.11 设置串口参数

四. 选中“COM1”或“COM2”，单击右键选择添加从站，输入“从站名称”，填入“从站站号”，根据从站设备的通讯手册配置 Modbus 功能码、从站数据起始地址、数据个数、网关映射区起始地址、响应超时时间、以及是否数变即发。同一个串口下的从站站号不能相同、不能与设备站号相同，且从站地址范围在

1-247 之间，同一串口下的从站名不能相同，数变即发含义为只有当数据发生变化时，网关才执行一次该命令，这个参数只对写命令有效。完成设置后点击“保存当前映射表编辑”。



图 3.12 添加从站



图 3.13 配置从站地址映射表

五. 通过配置软件左半部分的“以太网配置”对网关的以太网参数进行配置。

部分参数含义如下：

**Modbus 网关 IP:** 设备自身 IP 地址；

**子网掩码:** 设备的子网掩码；



局域网网关 IP：设备所在网络的网关 IP 地址；

Modbus-TCP 数据通讯端口：一般为 502；

配置端口：配置软件通过设备的该端口下载配置到设备；

Modbus-TCP 看门狗时间：网关从接收到最后一条 Modbus TCP 报文到进行自动重启的时间间隔；注：网关自动重启动可以及时释放掉长期没有使用的连接资源；

Modbus-TCP 看门狗使能：是否使能看门狗功能。



图 3.14 配置网关以太网参数

六. 通过“通讯”——“通讯配置”设置想要下载的目标网关地址以及下载使用的通讯端口号，默认为网关出厂默认 IP 192.168.1.254 以及端口号 1024。

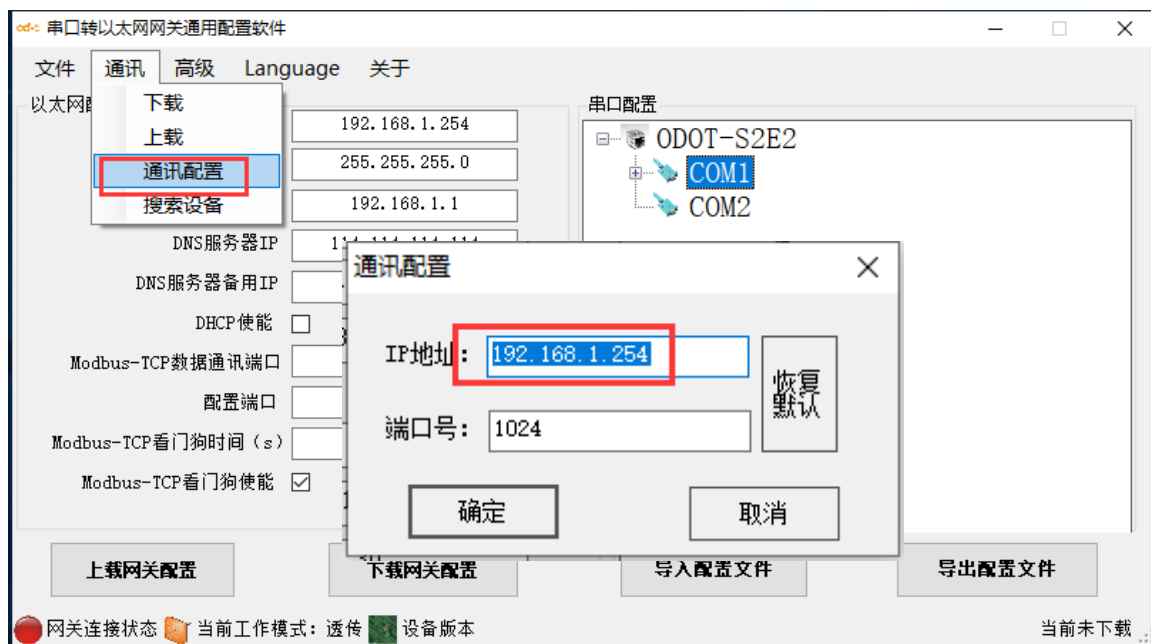


图 3.15 软件与网关通讯配置

七. 单击“**下载网关配置**”按钮，下载配置参数到网关。下载成功后状态栏右下角显示“**下载成功**”提示，下载成功后网关自动重启，并进入到运行状态。如果下载失败，请检查电脑 IP 地址与网关 IP 地址是否在同一个网段，并检查网关 IP 地址是否设置正确，如果忘记网关 IP 地址，可以通过复位键对网关进行复位操作，复位后网关 IP 地址为出厂默认 IP 地址。单击“**导入配置文件**”和“**导出配置文件**”可导入和保存配置文件到本地磁盘。单击“**上载网关配置**”，可以将网关当前配置上传至软件。**注：进行下载、上载操作时，需保证电脑与网关在同一网段。**



图 3.15 下载网关配置

八. 完成上述设置后 Modbus TCP 客户端可使用 Modbus TCP 协议, 通过网关 IP 地址 192.168.1.254、Modbus 数据通讯端口 502 以及从站站号 X ( $0 < X < 248$  且 X 不能为网关的设备站号) 访问到站号为 1 的从站设备 16DI。

### 3.4.2 实现 Modbus TCP 客户端与 Modbus RTU/ASCII 主站通讯

#### 3.4.2.1 应用拓扑图

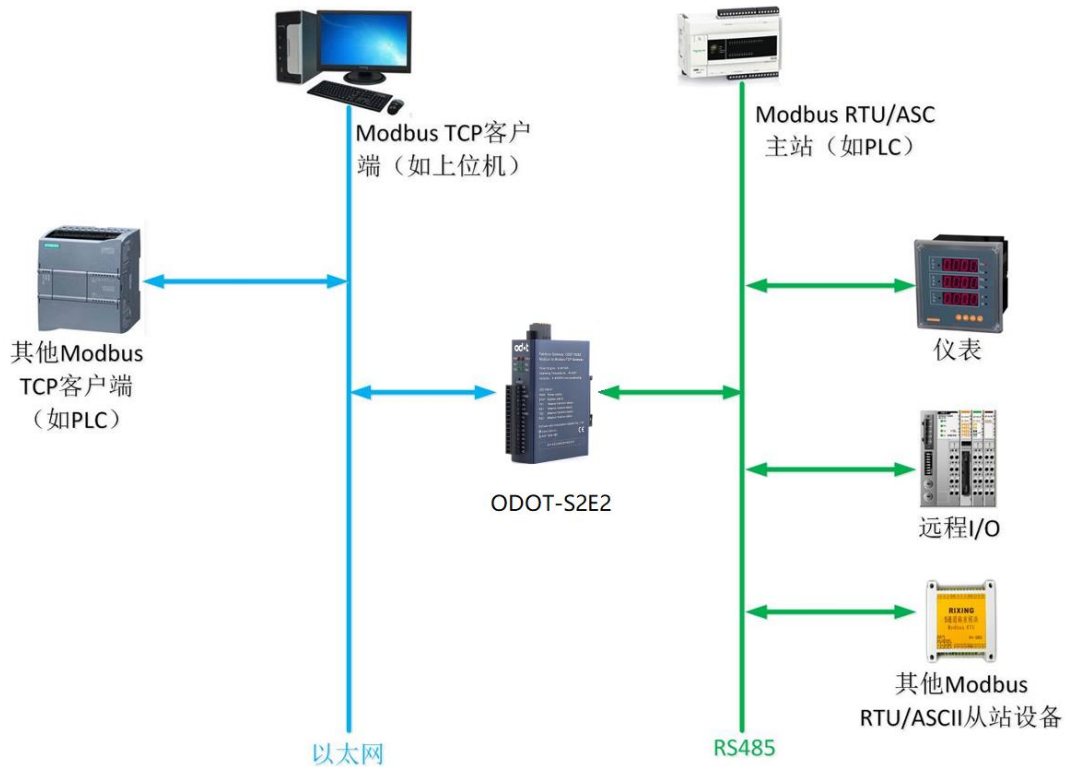


图 3.16 系统拓扑图

#### 3.4.2.2 简单配置

一. 打开软件配置软件“odot MGCC Config”，右击从站配置页面选择“添加设备”，添加“ODOT-S2E2”。

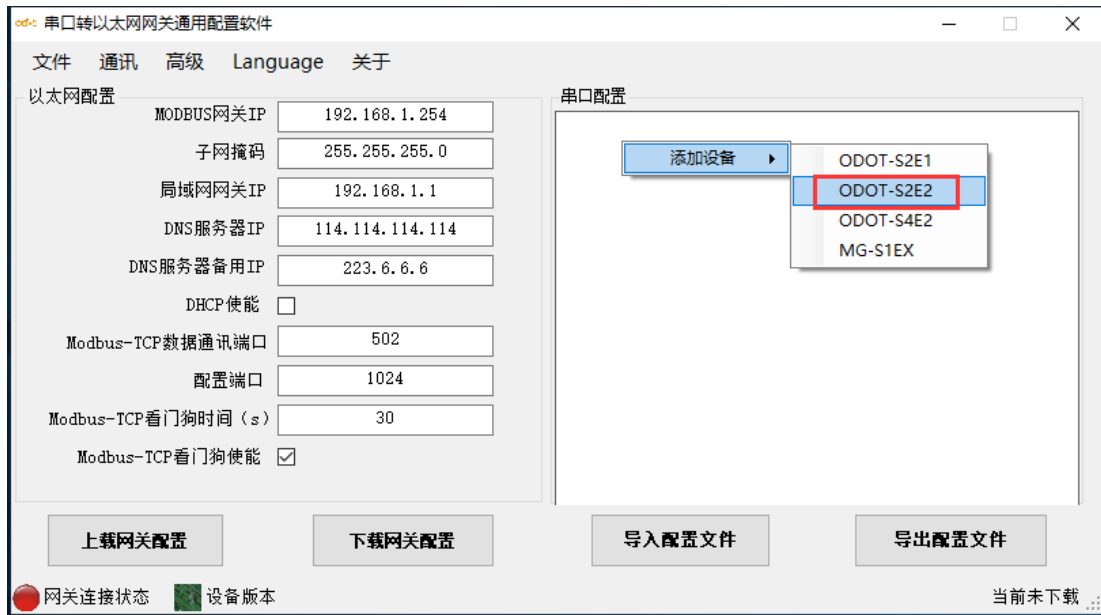


图 3.17 添加设备

二. 双击“ODOT-S2E2”，或右击“ODOT-S2E2”，选择“设备串口公共属性”，在弹出的设置页面设置网关作为 Modbus RTU/ASCII 从站的站号。

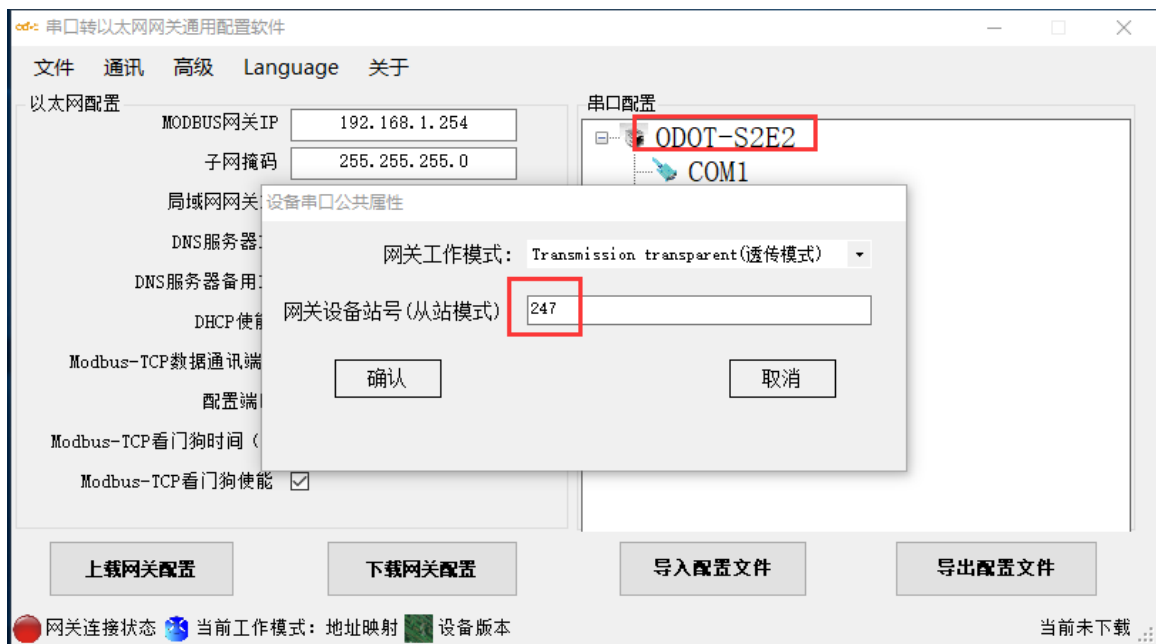


图 3.18 设置网关工作模式

三. 双击“COM1”或“COM2”或右击“COM1”或“COM2”并单击“串口属性”，弹出“串口设置”窗口，设置通讯参数，将串口工作模式设置为从站模式，点击“确认”按钮保存并返回。

各参数含义如下：

### 工作模式：

用于设置网关在该串口所连接的网络中作为主站还是从站，默认为主站模式，此处设置为从站模式。

### Modbus协议类型：

用于设置网关在该串口所连接的网络中与其他设备通信所用协议的类型，Modbus RTU/ASCII可选，请将该参数设置为与该串口所连接的设备一致。

### 波特率：

串口波特率，可选范围 1200~115200bps，默认 9600bps，请将该参数设置为与该串口所连接的设备一致。

### 校验位：

可选择无校验、奇校验、偶校验，默认无校验，请将该参数设置为与该串口所连接的设备一致。

### 停止位：

1 位、2 位停止位可选，默认 1 位停止位。请将该参数设置为与该串口所连接的设备一致。

### 接收字符间隔：

接收报文时的帧间隔检测时间， $1.5t \sim 200t$  可选，默认  $3.5t$  ( $t$  为单个字符传送的时间，和波特率有关)。一般情况下，不用更改此参数。

### 从站响应延迟：

网关作为 Modbus RTU/ASCII 从站，从接收到主站报文到发送回复报文的<sup>时间间隔</sup>，该参数和主站性能有关。

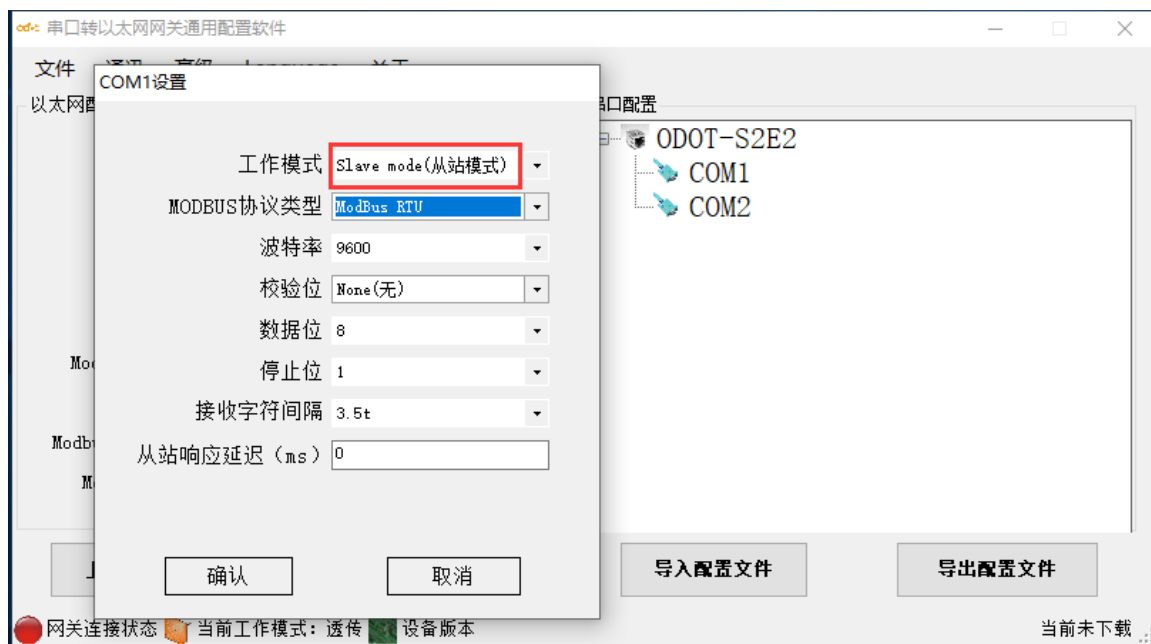


图 3.19 将对应的串口设置为从站模式

三. 通过配置软件左半部分的“以太网配置”对网关的以太网参数进行配置。

部分参数含义如下：

**Modbus 网关 IP：**设备自身 IP 地址；

**子网掩码：**设备的子网掩码；

**局域网网关 IP：**设备所在网络的网关 IP 地址；

**Modbus-TCP 数据通讯端口：**一般为 502；

**配置端口：**配置软件通过设备的该端口下载配置到设备；

**Modbus-TCP 看门狗时间：**网关从接收到最后一条 Modbus TCP 报文到进行自动重启的时间间隔；注：网关自动重启动可以及时释放掉长期没有使用的连接资源；

**Modbus-TCP 看门狗使能：**是否使能看门狗功能。



图 3.20 配置网关以太网参数

四. 通过“通讯”—“通讯配置”设置想要下载的目标网关地址以及下载使用的通讯端口号，默认为网关出厂默认 IP 192.168.1.254 以及端口号 1024。



图 3.21 软件与网关通讯配置

五. 单击“下载网关配置”按钮，下载配置参数到网关。下载成功后状态栏右下角显示“下载成功”提示，下载成功后网关自动重启，并进入到运行状态。如果下载失败，请检查电脑 IP 地址与网关 IP 地址是否在同一个网段，并检查网关 IP 地址是否设置正确，如果忘记网关 IP 地址，可以通过复位键对网关进行复



位操作，复位后网关 IP 地址为出厂默认 IP 地址。单击“导入配置文件”和“导出配置文件”可导入和保存配置文件到本地磁盘。单击“上载网关配置”，可以将网关当前配置上传至软件。**注：进行下载、上载操作时，需保证电脑与网关在同一网段。**



图 3.22 下载网关配置

六. 设置完成后，将网关通过以太网接入 Modbus TCP 网络，通过对应的串口（例程配置为 COM2）接入 Modbus RTU/ASCII 网络，网关在 Modbus TCP 网络中作为 Modbus TCP 服务器，在 Modbus RTU/ASCII 网络中作为从站，Modbus TCP 客户端可以通过 Modbus TCP 协议读写网关内部的**网关数据存储区**，Modbus RTU/ASCII 主站也可以通过 Modbus RTU/ASCII 协议读写网关内部**网关数据存储区**，网关充当一个数据中继的作用从而实现了 Modbus TCP 客户端与 Modbus RTU/ASCII 主站通讯。

### 3.4.3 实现 Modbus RTU/ASCII 主站之间的通讯

#### 3.4.3.1 应用拓扑图

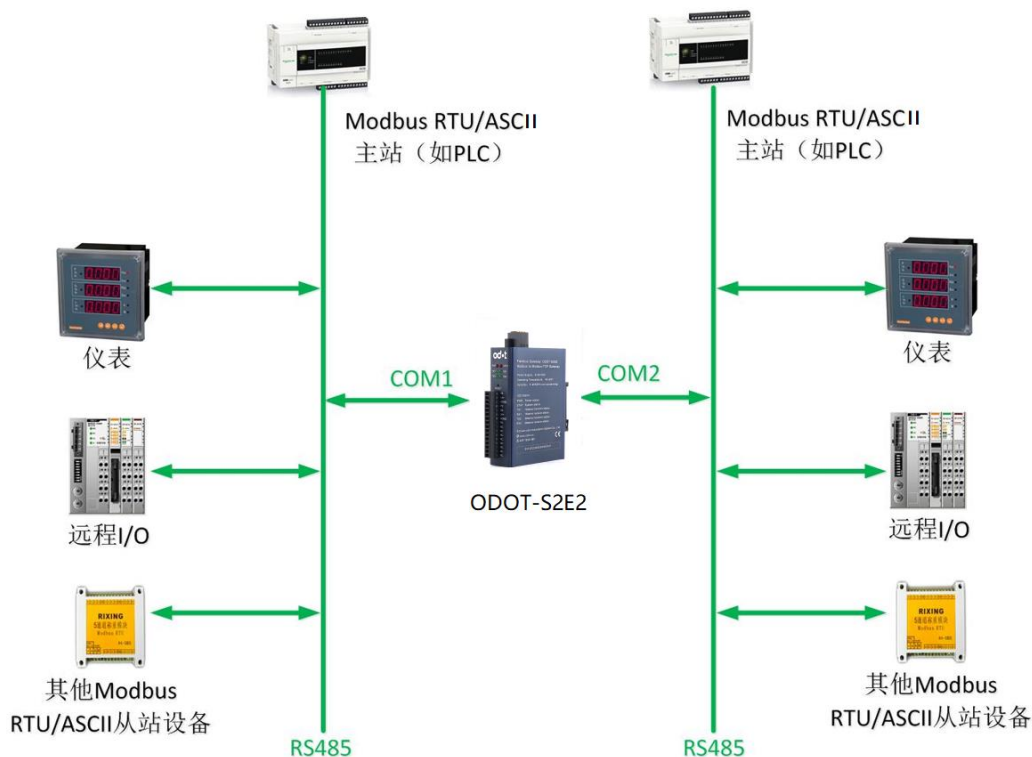


图 3.23 系统拓扑图

#### 3.4.3.2 简单配置

一. 打开软件配置软件“odot MGCC Config”，右击从站配置页面选择“添加设备”，添加“ODOT-S2E2”。

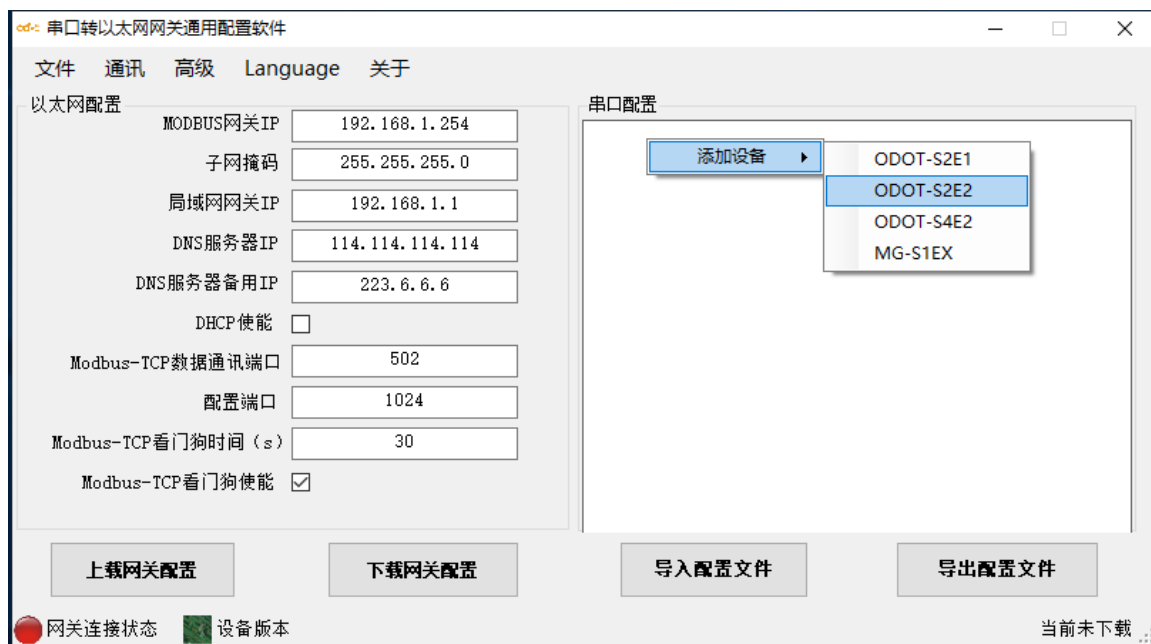


图 3.24 添加设备

二. 双击“ODOT-S2E2”，或右击“ODOT-S2E2”，选择“设备串口公共属性”，在弹出的设置页面设置网关作为 Modbus RTU/ASCII 从站的站号。



图 3.25 设置网关工作模式

三. 双击“COM1”、“COM2”或右击“COM1”、“COM2”并单击“串口属性”，弹出“串口设置”窗口，设置通讯参数，将两个串口的工作模式都设置为从站模式，点击“确认”按钮保存并返回。

各参数含义如下：

### 工作模式：

用于设置网关在该串口所连接的网络中作为主站还是从站，默认为主站模式，此处设置为**从站模式**。

### Modbus 协议类型：

用于设置网关在该串口所连接的网络中与其他设备通信所用协议的类型，Modbus RTU/ASCII 可选，请将该参数设置为与该串口所连接的设备一致。

### 波特率：

串口波特率，可选范围 1200~115200bps，默认 9600bps，请将该参数设置为与该串口所连接的设备一致。

### 校验位：

可选择无校验、奇校验、偶校验，默认无校验，请将该参数设置为与该串口所连接的设备一致。

### 停止位：

1位、2位停止位可选，默认1位停止位。请将该参数设置为与该串口所连接的设备一致。

### 接收字符间隔：

接收报文时的帧间隔检测时间， $1.5t \sim 200t$  可选，默认  $3.5t$  ( $t$  为单个字符传送的时间，和波特率有关)。一般情况下，不用更改此参数。

### 从站响应延迟：

网关作为 Modbus RTU/ASCII 从站，从接收到主站报文到发送回复报文的**时间间隔**，该参数和主站性能有关。

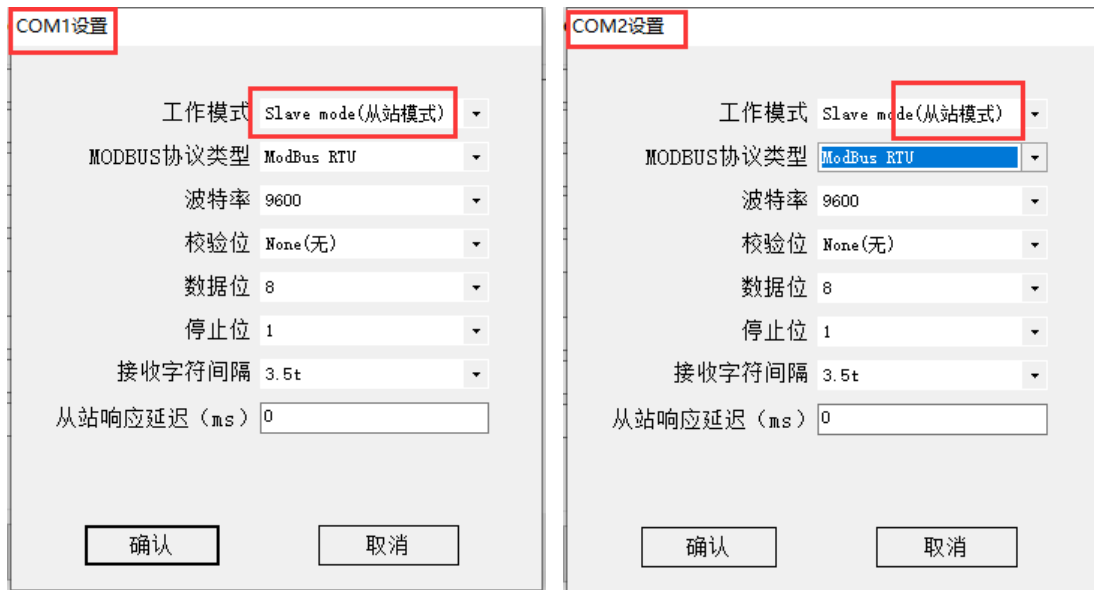


图 3.26 将对应的串口设置为从站模式

三. 通过配置软件左半部分的“以太网配置”对网关的以太网参数进行配置。

部分参数含义如下：

**Modbus 网关 IP：**设备自身 IP 地址；

**子网掩码：**设备的子网掩码；

**局域网网关 IP：**设备所在网络的网关 IP 地址；

**Modbus-TCP 数据通讯端口：**一般为 502；

**配置端口：**配置软件通过设备的该端口下载配置到设备；

**Modbus-TCP 看门狗时间：**网关从接收到最后一条 Modbus TCP 报文到进行自动重启的时间间隔；注：网关自动重启动可以及时释放掉长期没有使用的连接资源；

**Modbus-TCP 看门狗使能：**是否使能看门狗功能。



图 3.27 配置网关以太网参数

四. 通过“通讯”—“通讯配置”设置想要下载的目标网关地址以及下载使用的通讯端口号，默认为网关出厂默认 IP 192.168.1.254 以及端口号 1024。



图 3.28 软件与网关通讯配置

五. 单击“下载网关配置”按钮，下载配置参数到网关。下载成功后状态栏右下角显示“下载成功”提示，下载成功后网关自动重启，并进入到运行状态。如果下载失败，请检查电脑 IP 地址与网关 IP 地址是否在同一个网段，并检查网关 IP 地址是否设置正确，如果忘记网关 IP 地址，可以通过复位键对网关进行复

位操作，复位后网关 IP 地址为出厂默认 IP 地址。单击“导入配置文件”和“导出配置文件”可导入和保存配置文件到本地磁盘。单击“上载网关配置”，可以将网关当前配置上传至软件。**注：进行下载、上载操作时，需保证电脑与网关在同一网段。**



图 3.29 下载网关配置

六. 设置完成后，通过对应的串口分别接入两个不同的接入 Modbus RTU/ASCII 网络，网关在两个 Modbus RTU/ASCII 网络中均作为从站，两个网络中的 Modbus RTU/ASCII 主站均可以通过 Modbus RTU/ASCII 协议读写网关内部的网关数据存储区，网关充当一个数据中继的作用从而实现了 Modbus RTU/ASCII 主站之间通讯。

### 3.4.4 实现 Modbus TCP 客户端与 Modbus RTU/ASCII 主站同时访问一路 Modbus RTU/ASCII 从站

#### 3.4.4.1 应用拓扑图

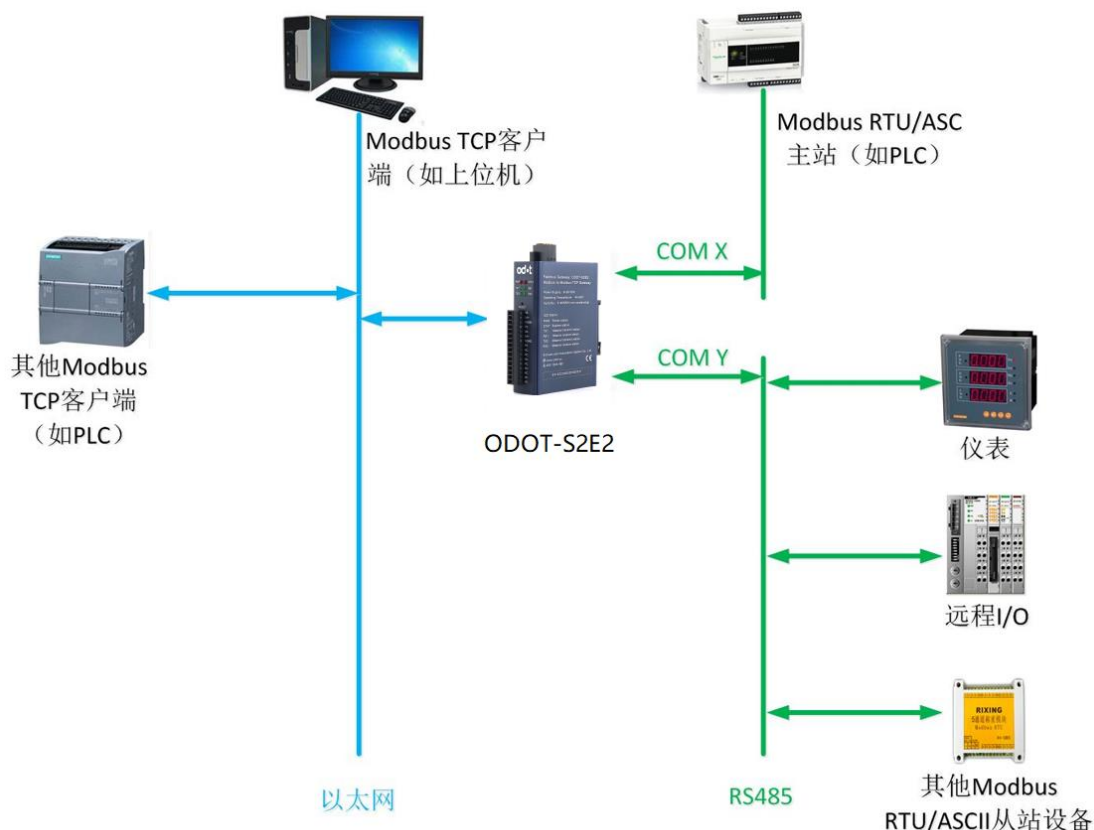


图 3.30 系统拓扑图

#### 3.4.4.2 简单配置

一. 打开软件配置软件“odot MGCC Config”，右击从站配置页面选择“添加设备”，添加“ODOT-S2E2”。



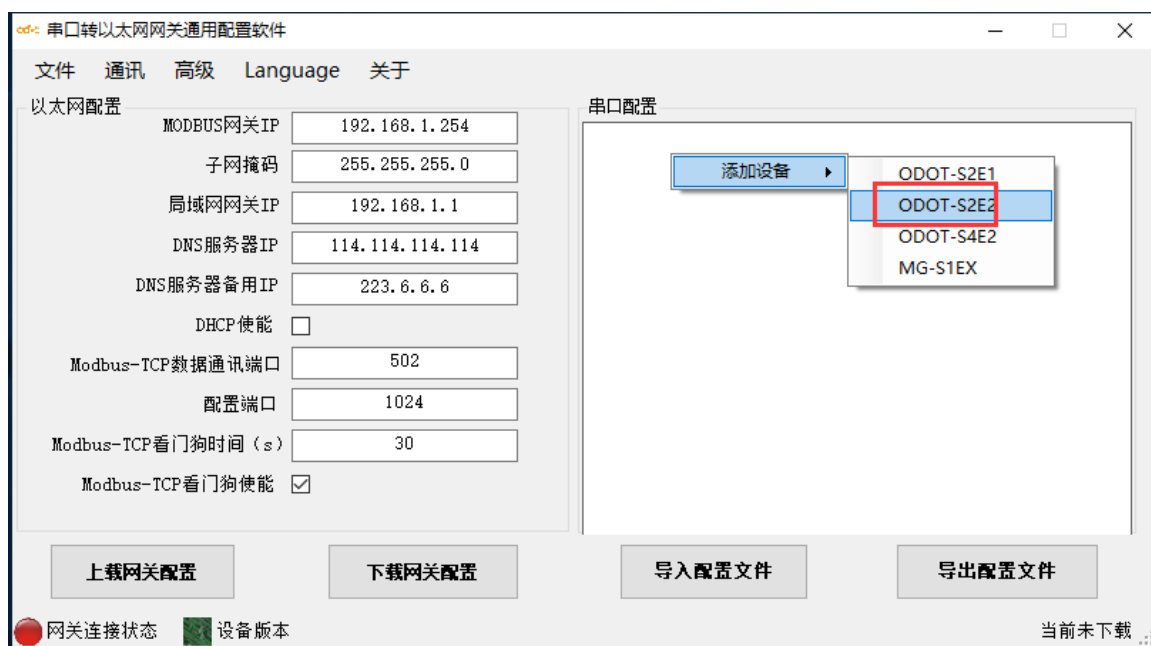


图 3.31 添加设备

二. 双击“ODOT-S2E2”，或右击“ODOT-S2E2”，选择“设备串口公共属性”，在弹出的设置页面将网关工作模式设置为“映射模式”。

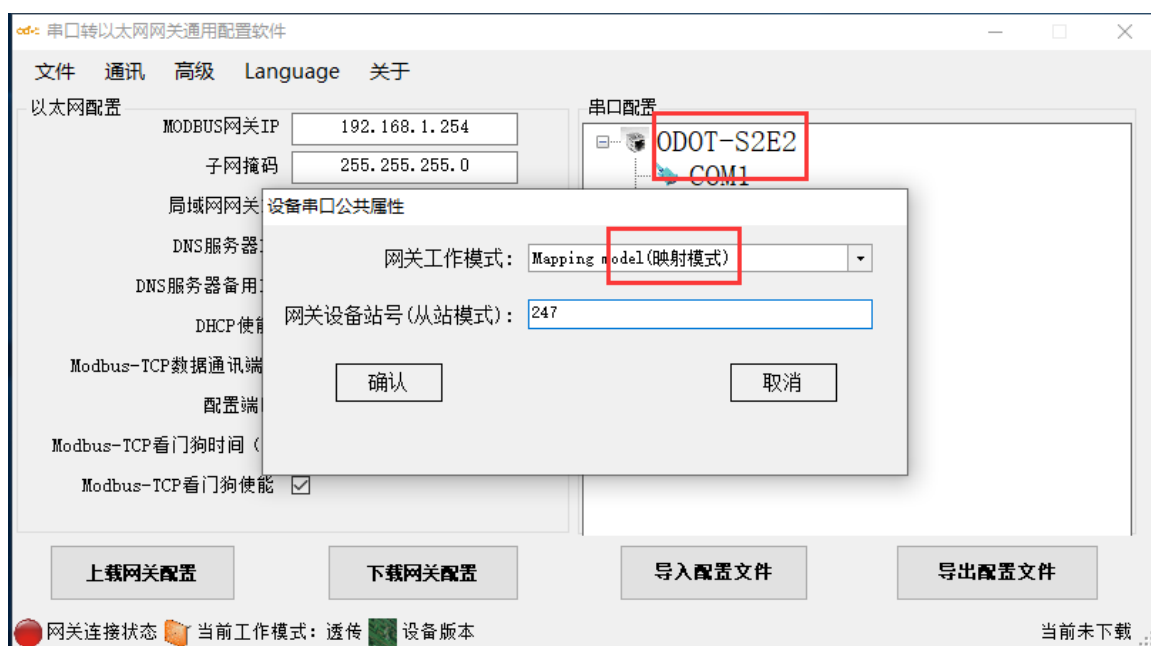


图 3.32 设置网关工作模式

三. 双击“COM1”或“COM2”或右击“COM1”或“COM2”并单击“串口属性”，弹出“串口设置”窗口，设置通讯参数后点击“确认”按钮保存并返回(此例选择 COM1)。

各参数含义如下：

**工作模式：**

用于设置网关在该串口所连接的网络中作为主站还是从站，默认为主站模式，此处设置为**主站模式**。

**Modbus 协议类型：**

用于设置网关在该串口所连接的网络中与其他设备通信所用协议的类型，Modbus RTU/ASCII 可选，请将该参数设置为与该串口所连接的设备一致。

**波特率：**

串口波特率，可选范围 1200~115200bps，默认 9600bps，请将该参数设置为与该串口所连接的设备一致。

**校验位：**

可选择无校验、奇校验、偶校验，默认无校验，请将该参数设置为与该串口所连接的设备一致。

**停止位：**

1 位、2 位停止位可选，默认 1 位停止位。请将该参数设置为与该串口所连接的设备一致。

**接收字符间隔：**

接收报文时的帧间隔检测时间， $1.5t \sim 200t$  可选，默认  $3.5t$  ( $t$  为单个字符传送的时间，和波特率有关)。一般情况下，不用更改此参数。

**报文发送间隔：**

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)，0ms-65535ms 可设，默认 0ms，建议设置 100ms，防止连接的设备因反应太慢而出现通讯故障。

**超时处理方式：**

读从站数据，如果从站响应超时的数据处理方式，可选择“数据清零”或“数据保持”。默认“数据保持”模式，此参数只对 Modbus 读命令有效，请根据实际需求设置此数值。

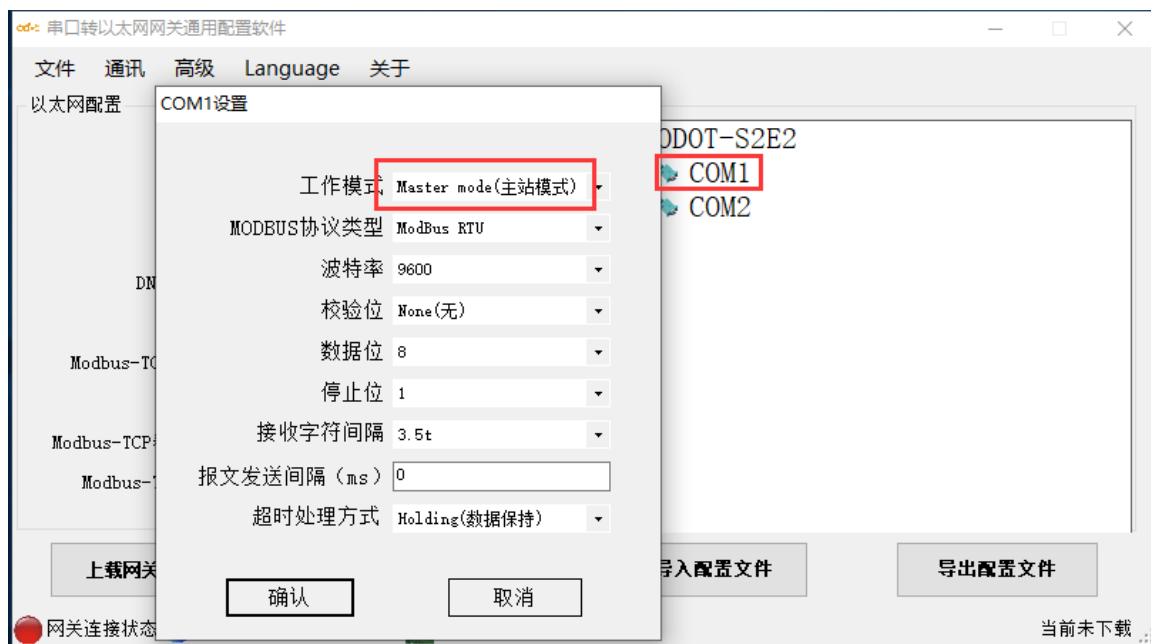


图 3.33 设置作为 Modbus RTU/ACII 主站的串口参数

四. 选中“COM1”或“COM2”（此例为 COM1），单击右键选择添加从站，输入“从站名称”，填入“从站站号”，根据从站设备的通讯手册配置 Modbus 功能码、从站数据起始地址、数据个数、网关映射区起始地址、响应超时时间、以及是否数变即发。同一个串口下的从站站号不能相同、不能与设备站号相同，且从站地址范围在 1-247 之间，同一串口下的从站名不能相同，数变即发含义为只有当数据发生变化时，网关才执行一次该命令，这个参数只对写命令有效。完成设置后点击“保存当前映射表编辑”。

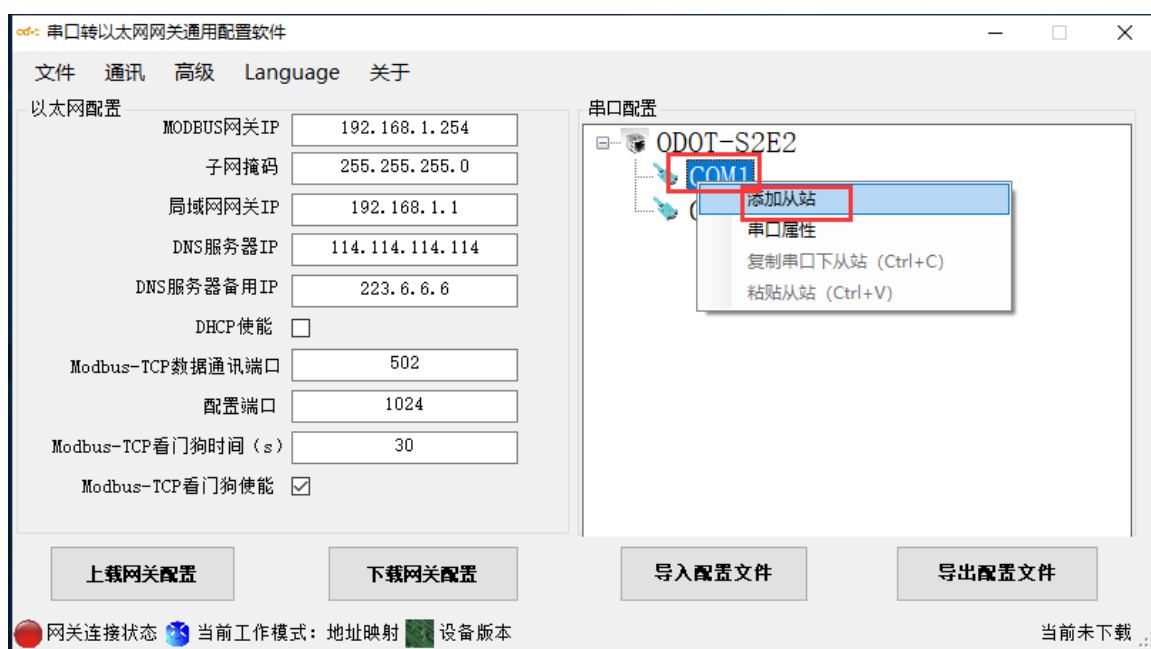


图 3.34 添加从站

COM1\_1#从站地址映射表\*

从站名称: COM1\_1#      从站站号 (1-247): 1

Modbus功能码	从站数据起始地址	数据个数	网关映射区起始地址	响应超时时间 (ms)	数变即发
03 (4x) Read Hold...	2	55	0	500	<input type="checkbox"/>
▶*				500	<input type="checkbox"/>

保存当前映射表编辑      关闭当前映射表编辑

图 3.35 配置从站地址映射表

五. 双击“COM1”或“COM2”或右击“COM1”或“COM2”并单击“串口属性”，弹出“串口设置”窗口，设置通讯参数，将串口工作模式设置为从站模式，点击“确认”按钮保存并返回（此例程选 COM2）。

各参数含义如下：

**工作模式：**

用于设置网关在该串口所连接的网络中作为主站还是从站，默认为主站模式，此处设置为从站模式。

**Modbus 协议类型：**

用于设置网关在该串口所连接的网络中与其他设备通信所用协议的类型，Modbus RTU/ASCII 可选，请将该参数设置为与该串口所连接的设备一致。

**波特率：**

串口波特率，可选范围 1200~115200bps，默认 9600bps，请将该参数设置为与该串口所连接的设备一致。

**校验位：**

可选择无校验、奇校验、偶校验，默认无校验，请将该参数设置为与该串口所连接的设备一致。

**停止位：**

1 位、2 位停止位可选，默认 1 位停止位。请将该参数设置为与该串口所连接的设备一致。

**接收字符间隔：**

接收报文时的帧间隔检测时间， $1.5t \sim 200t$  可选，默认  $3.5t$  ( $t$  为单个字符传送的时间，和波特率有关)。一般情况下，不用更改此参数。

**从站响应延迟：**

网关作为 Modbus RTU/ASCII 从站，从接收到主站报文到发送回复报文的时间间隔，该参数和主站性能有关。

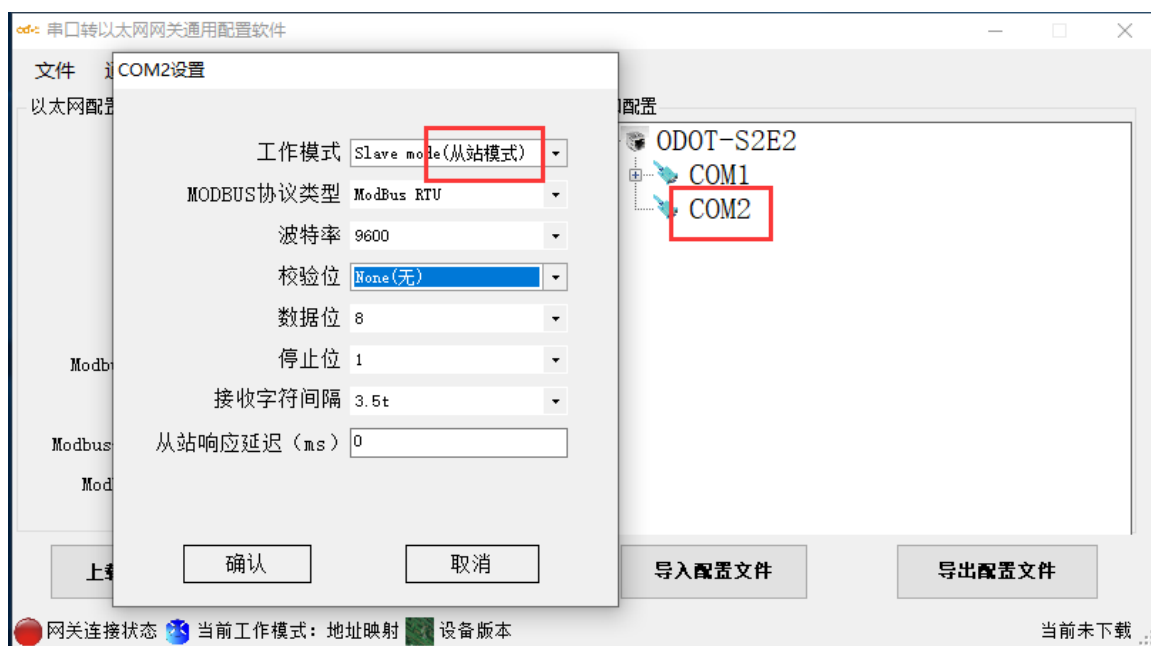


图 3.36 设置作为 Modbus RTU 从站的串口参数

六. 通过配置软件左半部分的“以太网配置”对网关的以太网参数进行配置。部分参数含义如下：

**Modbus 网关 IP：**设备自身 IP 地址；

**子网掩码：**设备的子网掩码；

**局域网网关 IP：**设备所在网络的网关 IP 地址；

**Modbus-TCP 数据通讯端口：**一般为 502；

**配置端口：**配置软件通过设备的该端口下载配置到设备；

**Modbus-TCP 看门狗时间：**网关从接收到最后一条 Modbus TCP 报文到进行自动重启的时间间隔；注：网关自动重启可以及时释放掉长期没有使用的连接资

源；

Modbus-TCP 看门狗使能：是否使能看门狗功能。



图 3.37 配置网关以太网参数

七. 通过“通讯”—“通讯配置”设置想要下载的目标网关地址以及下载使用的通讯端口号，默认为网关出厂默认 IP 192.168.1.254 以及端口号 1024。



图 3.38 软件与网关通讯配置

八. 单击“下载网关配置”按钮，下载配置参数到网关。下载成功后状态栏右下角显示“下载成功”提示，下载成功后网关自动重启，并进入到运行状态。

如果下载失败，请检查电脑 IP 地址与网关 IP 地址是否在同一个网段，并检查网关 IP 地址是否设置正确，如果忘记网关 IP 地址，可以通过复位键对网关进行复位操作，复位后网关 IP 地址为出厂默认 IP 地址。单击“导入配置文件”和“导出配置文件”可导入和保存配置文件到本地磁盘。单击“上载网关配置”，可以将网关当前配置上传至软件。**注：进行下载、上载操作时，需保证电脑与网关在同一网段。**



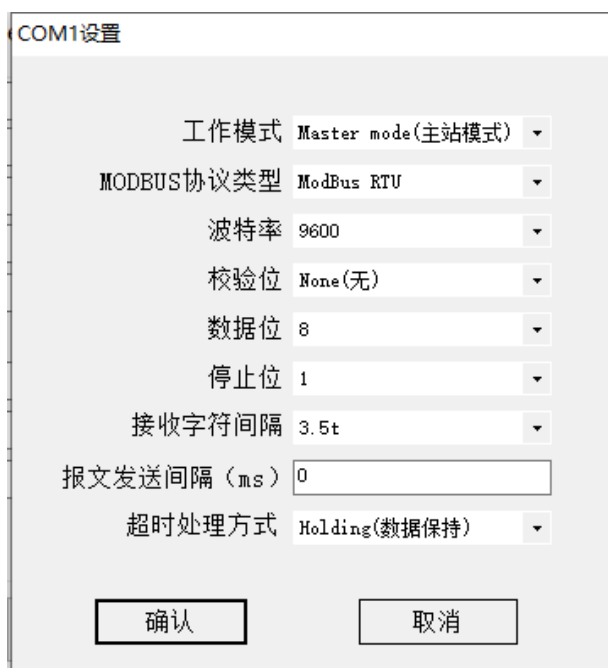
图 3.39 下载网关配置

九. 在本例程中，完成上述设置后，将 Modbus RTU/ASCII 从站连接至 COM1，Modbus RTU/ASCII 主站连接至 COM2，将 Modbus TCP 客户端通过以太网连接至网关，网关将从 COM1 自动刷新底层 Modbus RTU/ASCII 从站数据，Modbus RTU/ASCII 主站与 Modbus TCP 客户端通过访问网关内部的网关数据存储区间接实现对 Modbus RTU/ASCII 从站的访问。

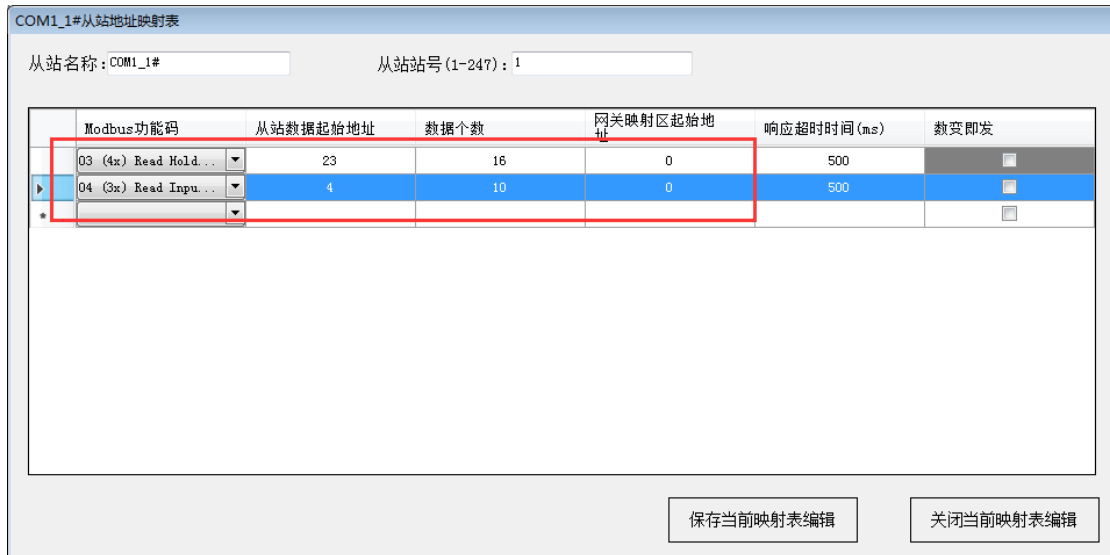
## 四、在西门子 STEP7 的测试应用。

### 4.1 网关 ODOT-S2E2 的配置

网关工作模式采用地址映射模式，网关 IP 地址设置为：192.168.1.4，RS485 侧 COM1 口参数：Modbus RTU 协议、9600、N、8、1，从站 ID=1，使用 03 号功能码读取 4 区 16 个数据，起始地址是 23，使用 04 号功能码读取 3 区 10 个数据，起始地址是 4。测试时用 Modbus slave 模拟现场 RS485 设备。



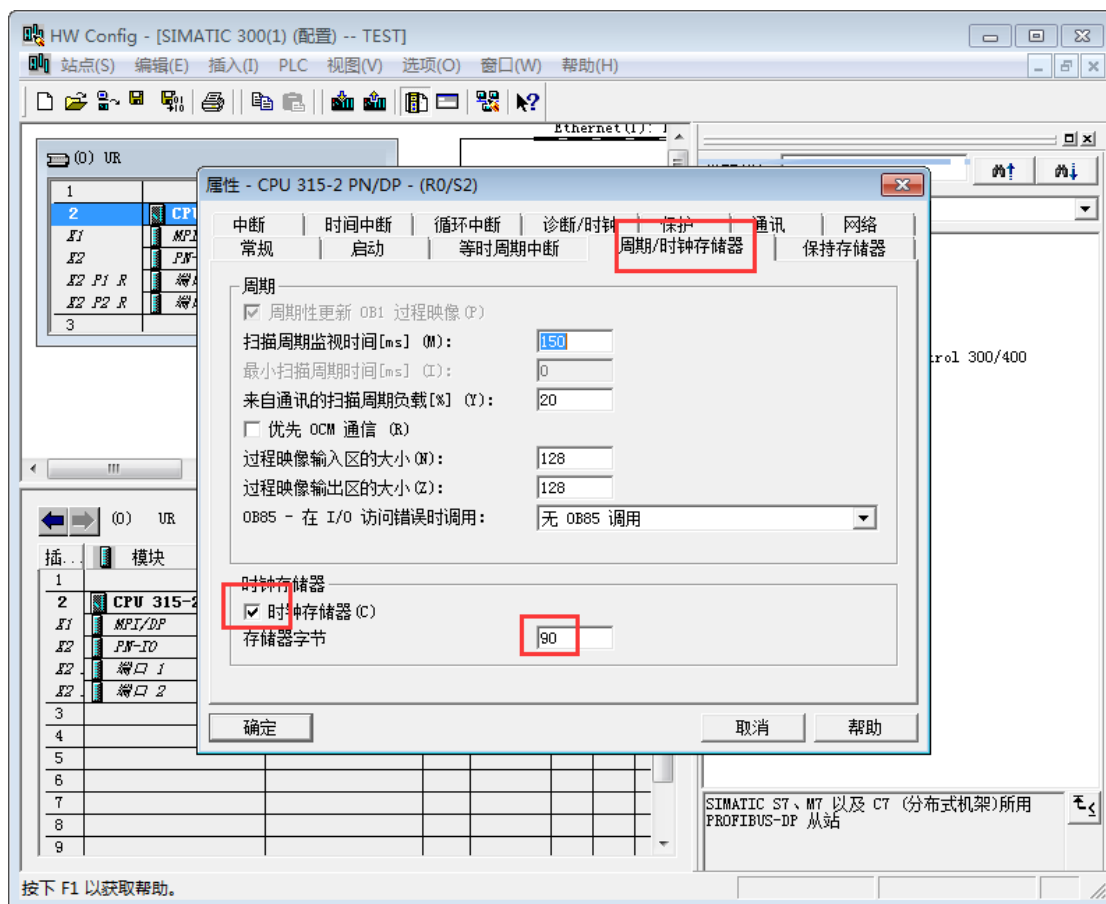




## 4.2 在西门子 STEP 7 的配置测试

本文档测试采用 S7-315-2 PN/DP PLC 作为主控制器，调用 MODBUS TCP 客户端功能块实现与网关的 MODBUS TCP 通讯。

1、打开 STEP 7 软件，新建一个工程，插入新对象，选择“SIMATIC 300 站点”，单击“SIMATIC 300”，然后双击右边的“硬件”，进入硬件组态界面。先放置导轨 Rail，再分别在 1、2 号槽位，放入电源模块和 CPU315-2 PN/DP 模块，双击 CPU 315-2 PN/DP，在弹出的对话框，选择周期/时钟存储器，激活时钟存储器，存储器字节填：90。



时钟存储字节的位	7	6	5	4	3	2	1	0
周期持续时间(s)	2.0	1.6	1.0	0.8	0.5	0.4	0.2	0.1
频率(Hz)	0.5	0.625	1	1.25	2	2.5	5	10

2、在新建项目可以直接复制零点公司提供的测试项目里的块。FB63、FB64、FB65、FB66、FB1024、FC4、FC11、FC21、FC37、FC38、DB60、DB1024、SFC20、SFC51。注：FB1024 功能块参考博图软件里的功能块 MB-Client。

DB60 数据块定义功能块 FB1024 参数。DB1024 定义通讯命令字符串，格式：从站地址\_ 功能码\_ 寄存器起始地址\_ 寄存器个数，采集数据地址区。

DB 参数 - [DB60 -- TEST\SIMATIC 300(1)\CPU 315-2 PN/DP]

地址	声明	名称	类型	初始值	实际值	备注
1	0.0	in	AUTH_NUM1	INT	0	
2	2.0	in	AUTH_NUM2	INT	0	
3	4.0	in	AUTH_NUM3	INT	0	
4	6.0	in	AUTH_NUM4	INT	0	
5	8.0	in	AUTH_NUM5	INT	0	
6	10.0	in	AUTH_NUM6	INT	0	
7	12.0	in	AUTH_NUM7	INT	0	
8	14.0	in	AUTH_NUM8	INT	0	
9	16.0	in	REQ_CONNECT	BOOL	FALSE	FALSE
10	16.1	in	REQ_STA	BOOL	FALSE	FALSE
11	16.2	in	DSCONNECT	BOOL	FALSE	FALSE
12	18.0	in	CONNECT_ID	INT	0	
13	20.0	in	IP_ODOT_1	INT	0	
14	22.0	in	IP_ODOT_2	INT	0	
15	24.0	in	IP_ODOT_3	INT	0	
16	26.0	in	IP_ODOT_4	INT	0	
17	28.0	in	Enable_NUM	INT	0	
18	30.0	in	COMMAND_STRING1	STRING [ 18 ]	''	'' 命令字符串
19	50.0	in	MB_DATA_PRT1	ANY	P#P 0.0 VOID 0	P#P 0.0 V...
20	60.0	in	COMMAND_STRING2	STRING [ 18 ]	''	'' 命令字符串
21	80.0	in	MB_DATA_PRT2	ANY	P#P 0.0 VOID 0	P#P 0.0 V...

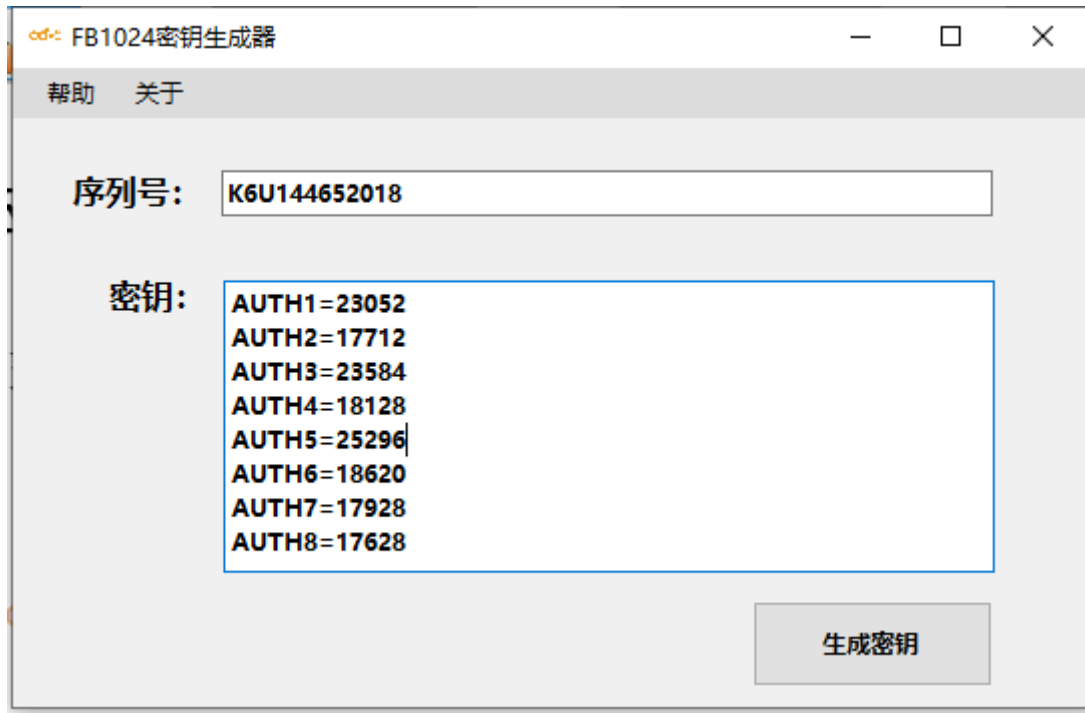
LAD/STL/FBD -- [DB1024 -- "ODOT" -- TEST\SIMATIC 300(1)\CPU 315-2 PN/DP...\DB1024]

地址	名称	类型	初始值	注释
0.0		STRUCT		
+0.0	COMMAND_STRING1	STRING[18]	'1_01_1_10'	通讯命令字符串, 格式: 从站地址_功能码_寄存器
+20.0	COMMAND_STRING2	STRING[18]	'2_02_2_20'	
+40.0	COMMAND_STRING3	STRING[18]	'3_03_3_30'	
+60.0	COMMAND_STRING4	STRING[18]	'4_04_4_40'	
+80.0	COMMAND_STRING5	STRING[18]	'5_05_5_50'	
+100.0	COMMAND_STRING6	STRING[18]	'6_06_6_60'	
+120.0	COMMAND_STRING7	STRING[18]	'15_15_15_150'	
+140.0	COMMAND_STRING8	STRING[18]	'16_16_16_100'	
+160.0	COMMAND_STRING9	STRING[18]	'20_16_16_100'	
+180.0	COMMAND_STRING10	STRING[18]	'21_16_16_100'	
+200.0	COMMAND_STRING11	STRING[18]	'22_16_16_100'	
+220.0	COMMAND_STRING12	STRING[18]	'23_16_16_100'	
+240.0	COMMAND_STRING13	STRING[18]	'24_16_16_100'	
+260.0	COMMAND_STRING14	STRING[18]	'25_16_16_100'	
+280.0	COMMAND_STRING15	STRING[18]	'26_16_16_100'	
+300.0	COMMAND_STRING16	STRING[18]	'27_16_16_100'	
+320.0	COMMAND_STRING17	STRING[18]	'28_16_16_100'	
+340.0	COMMAND_STRING18	STRING[18]	'29_16_16_100'	
+360.0	COMMAND_STRING19	STRING[18]	'30_16_16_100'	
+380.0	COMMAND_STRING20	STRING[18]	'31_16_16_100'	
+400.0	MB_DATA_PRT1	ARRAY[0..299]		第1条命令发送/接收到的数据存于此
*1.0		BYTE		
+700.0	MB_DATA_PRT2	ARRAY[0..299]		第2条命令发送/接收到的数据存于此
*1.0		BYTE		

程序元素 调用结构

1: 错误 2: 信息 3: 交叉参考 4: 地址信息 5: 修改 6: 诊断 7: 比较

按下 F1 以获取帮助。 离线 Abs < 5.2 插入 Chg



AUTH\_NUM1—AUTH\_NUM8: 授权码, 请联系厂家生成, 如果没有填入正确的授权码, 通讯会在正常运行一段时间后中断。通过 FB1024 密钥生成器输入序列号后 12 位生成。

REQ\_CONNECT: 建立连接使能, 上升沿有效。

REQ\_STAR: 发送 (接收) 数据使能, 上升沿有效。

DSCONNECT: 终止连接, “1” 为终止连接。

CONNECT\_ID: 通讯连接号。

IP\_DODT1: 服务器 IP 地址第 1 个字节数据。

IP\_DODT2: 服务器 IP 地址第 2 个字节数据。

IP\_DODT3: 服务器 IP 地址第 3 个字节数据。

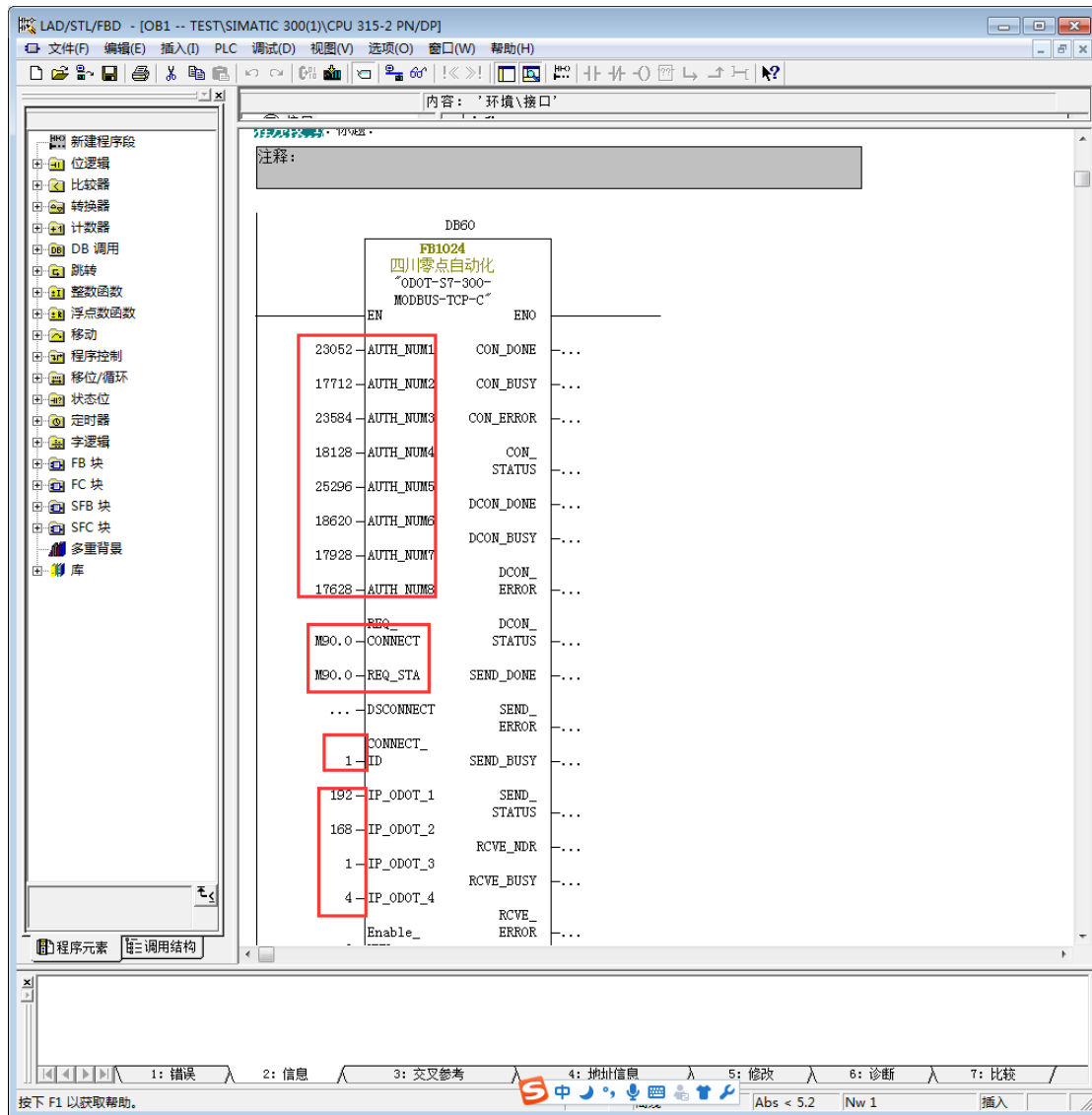
IP\_DODT4: 服务器 IP 地址第 4 个字节数据。

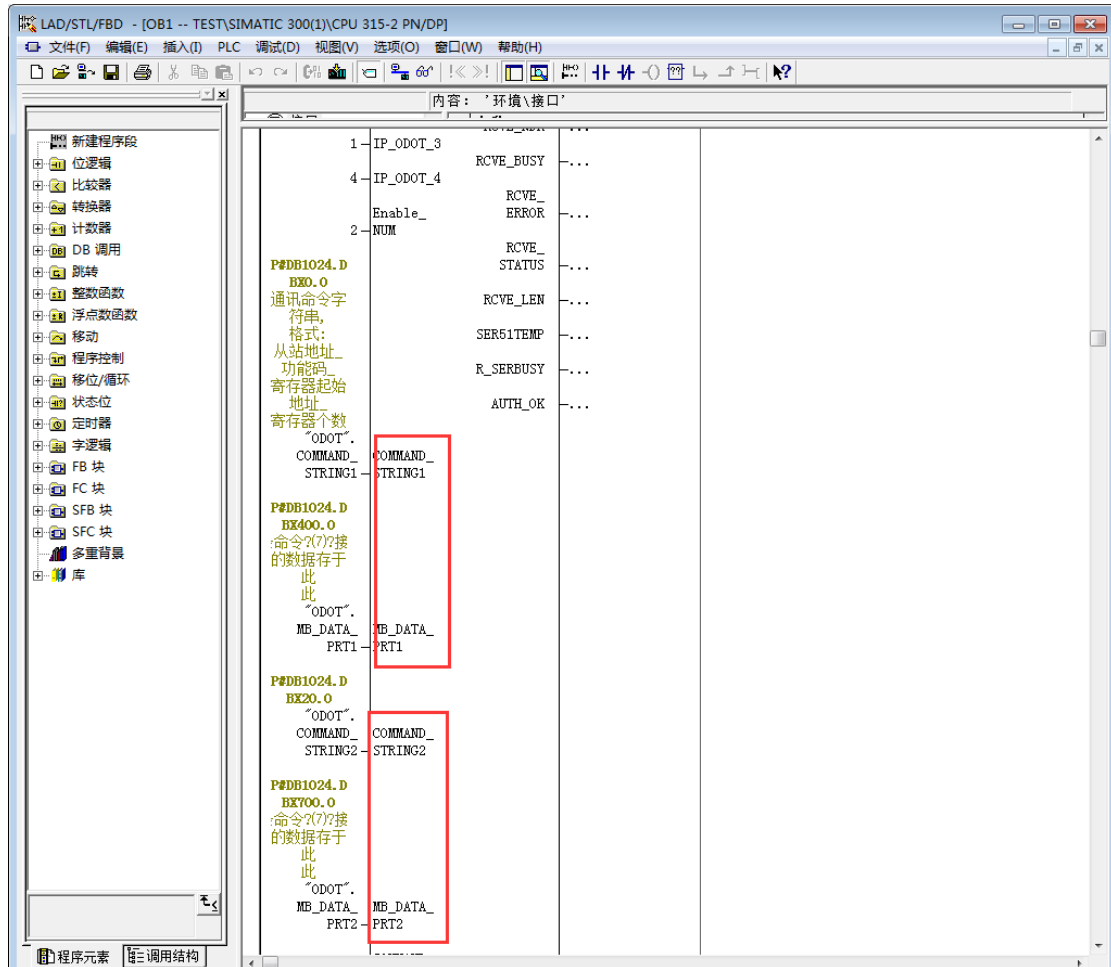
Enable\_NUM: 使能的命令条数, 例如想让 COMMAND\_STRING1 运行就填 1, 想让 COMMAND\_STRING1—COMMAND\_STRING20 运行就填 20。

COMMAND\_STRING1—COMMAND\_STRING20: 通讯命令字符串, 格式以及含义如下: 设备站号\_功能码\_寄存器起始地址\_寄存器个数; 例如设备站号为 1, 要使用 3 号功能码从四区寄存器地址为 0 的寄存器开始读取 10 个寄存器数据, 则对应的命令字符串如下: 1\_3\_0\_10。

MB\_DATA\_PRT1—MB\_DATA\_PRT20: 指向 COMMAND\_STRING1—COMMAND\_STRING20  
读取或写出数据的存储区的 ANY 指针。

3、打开 OB1，组态 FB1024 功能块。





4、保存、编译下载程序，进行监视。可监控 DB1024 里的数据与 Modbus Slave 里的数据保持一致。

The screenshot shows the 'Modbus Slave - [Mbslave1]' configuration window. The table below represents the data points configured in the window:

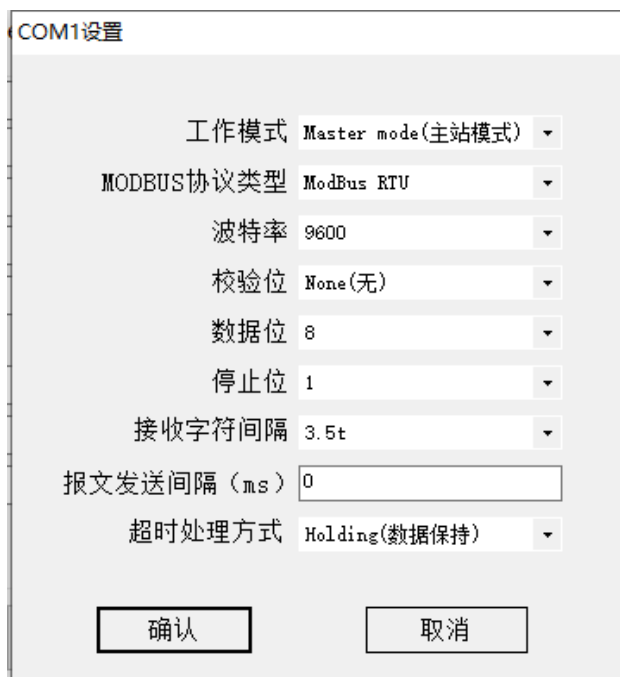
Address	Alias	Value
0		0
1		0
2		0
3		0x2A81
4		0x4321
5		0x4533
6		0x1545
7		0
8		0
9		0

The background table in the main window shows the mapping of these values to the '实际值' (Actual Value) column, with the value '1\_03\_0\_20' corresponding to address 3. A red box highlights this value in the background table.

## 五、在西门子 TIA V14 的测试应用

### 5.1 网关 ODOT-S2E2 的配置

网关工作模式采用地址映射模式，网关 IP 地址设置为：192.168.1.4，RS485 侧 COM1 口参数：Modbus RTU 协议、9600、N、8、1，从站 ID=1，使用 03 号功能码读取 4 区 6 个数据，起始地址是 23。测试时用 Modbus slave 模拟现场 RS485 设备。





COM1\_1#从站地址映射表

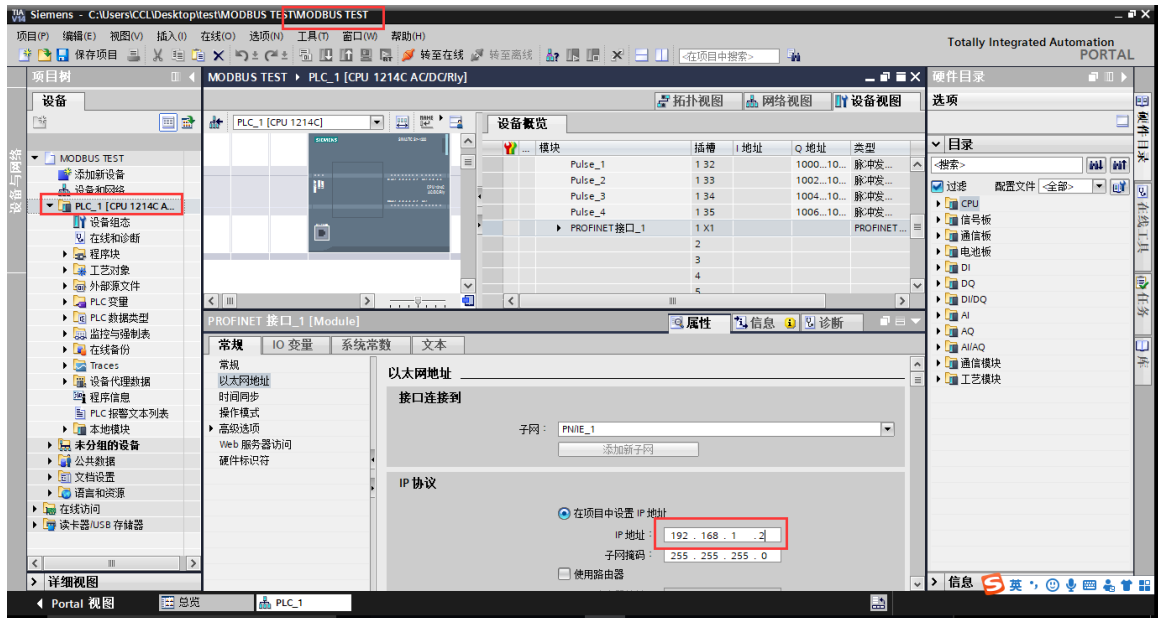
从站名称: COM1\_1#      从站站号(1-247): 1

Modbus功能码	从站数据起始地址	数据个数	网关映射区起始地址	响应超时时间(ms)	数变即发
▶ 03 (4x) Read Hold...	23	6	0	500	<input type="checkbox"/>
*					<input type="checkbox"/>

保存当前映射表编辑      关闭当前映射表编辑

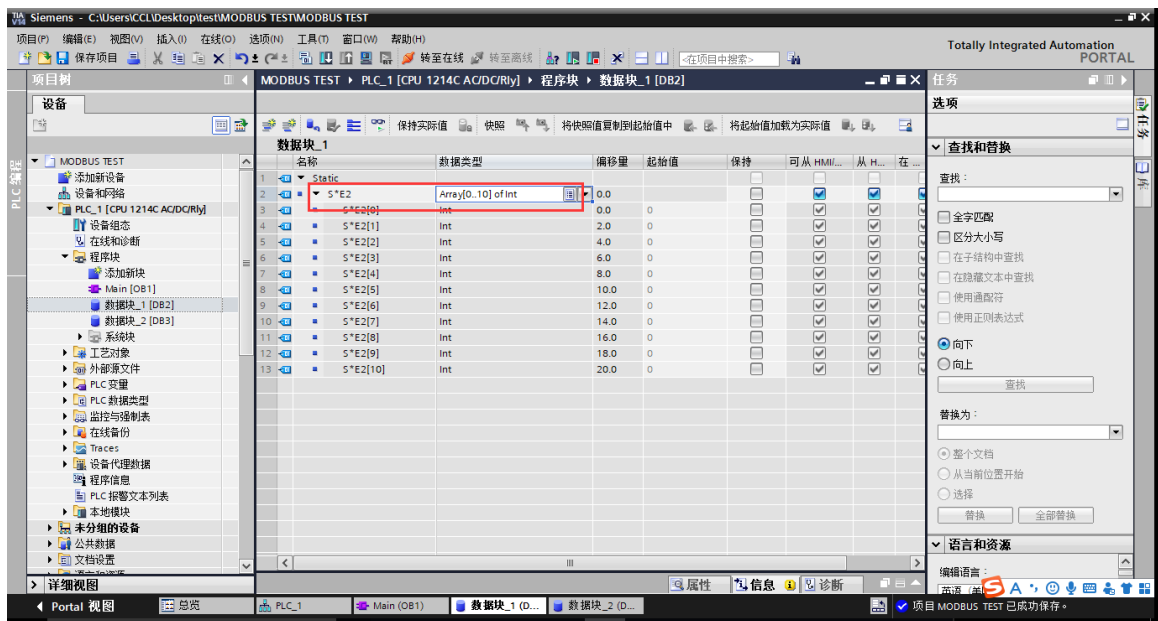
## 5.2 软件 TIA V14 的配置测试

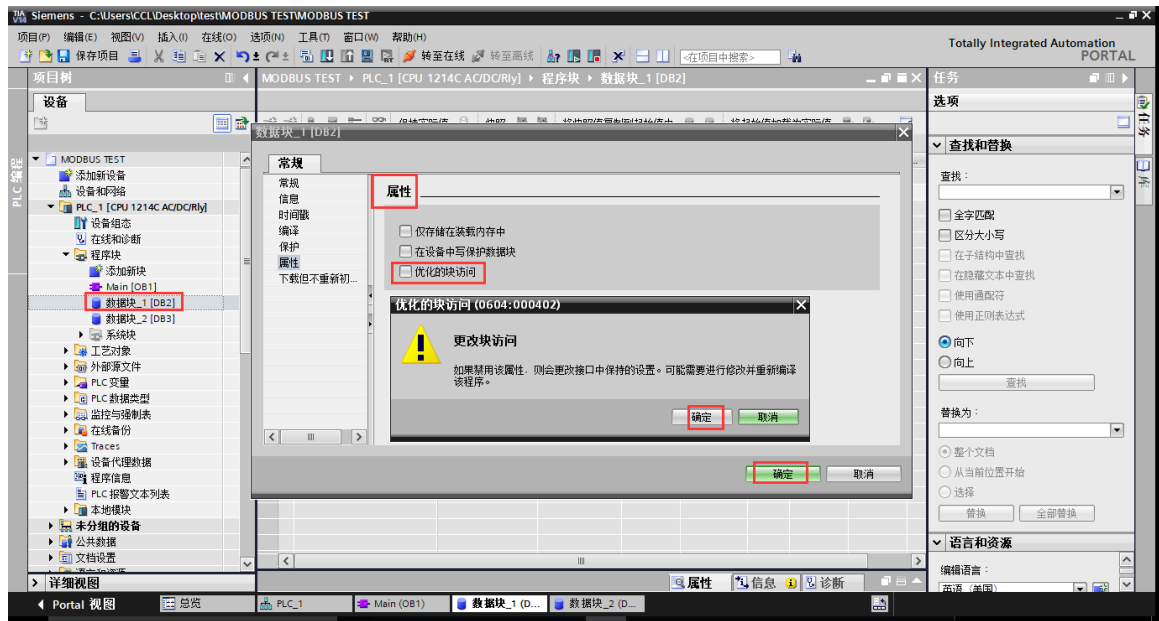
本文档测试采用 S7-1200PLC 作为主控制器。打开 TIA 软件，新建一个项目工程 MODBUS TEST，添加新设备 S7-1214 AC/DC/RLY。设置网口 IP 为：192.168.1.2。



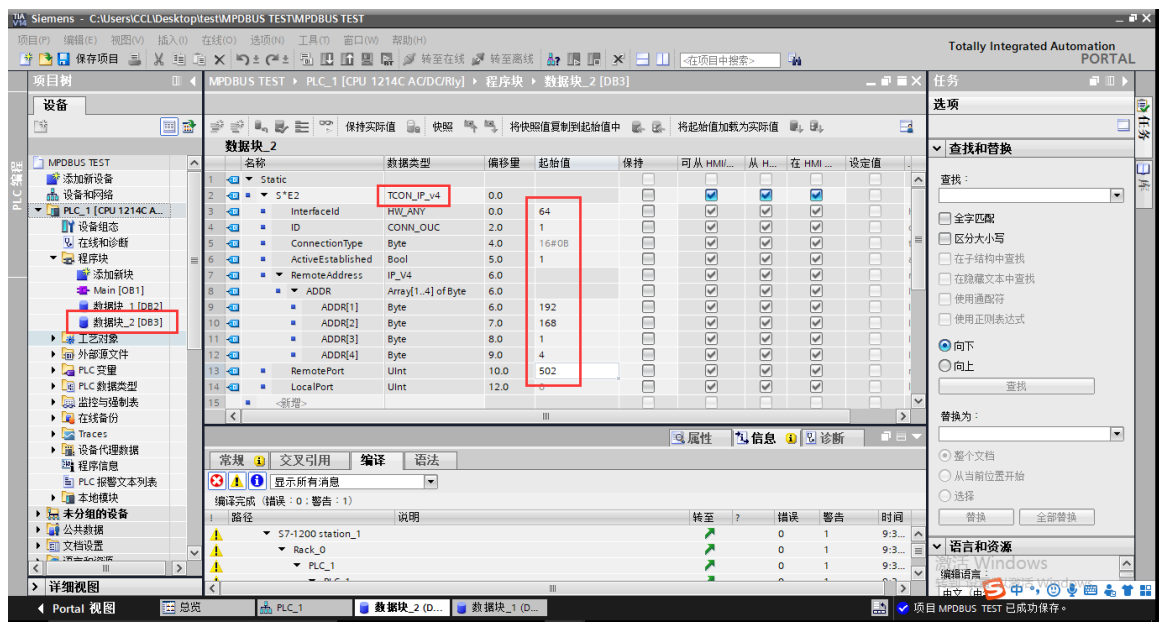
点击程序块，添加新块，建立数据块 DB2、DB3。

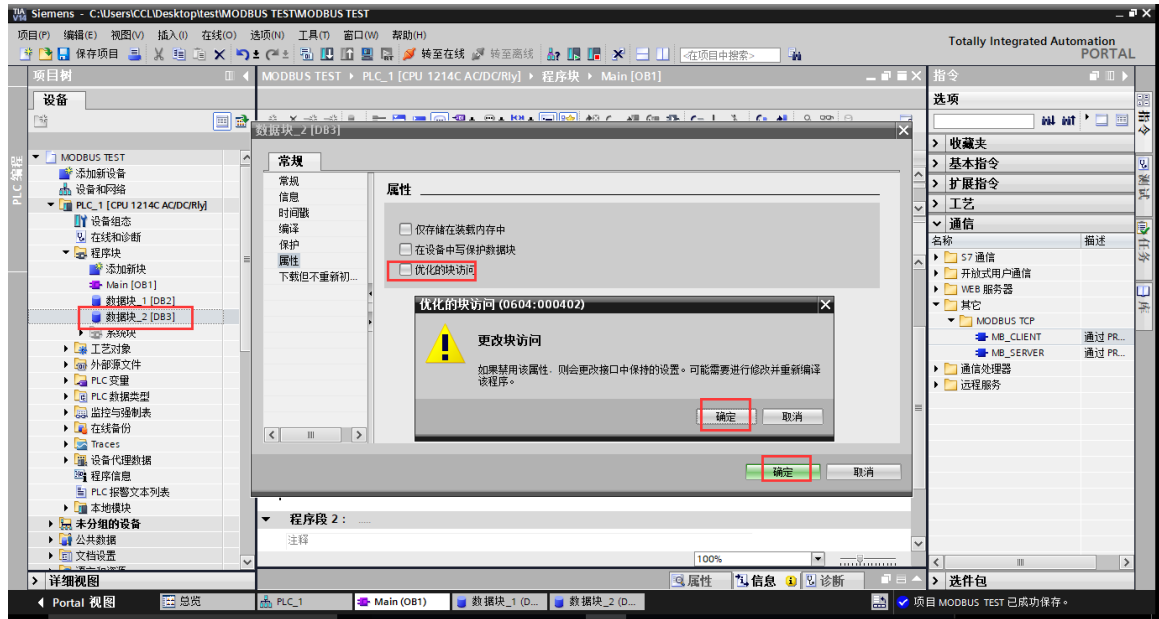
在 DB2 建立指向待从 Modbus 服务器接收数据的数据缓冲区，修改 DB2 属性里，去掉优化的数据块前面的 。选中 DB2，保存编译。



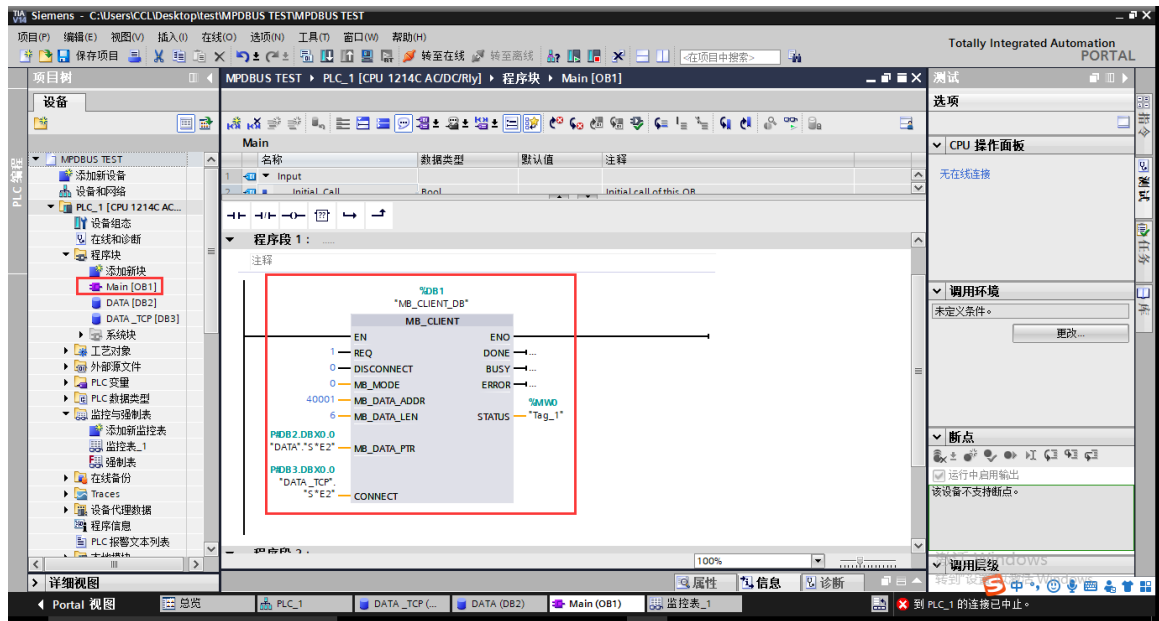


在 DB3 建立指定连接所需的所有地址参数。所填 IP 地址为网关的 IP 地址。  
修改 DB3 属性里，去掉优化的数据块前面的 。选中 DB3，保存编译。

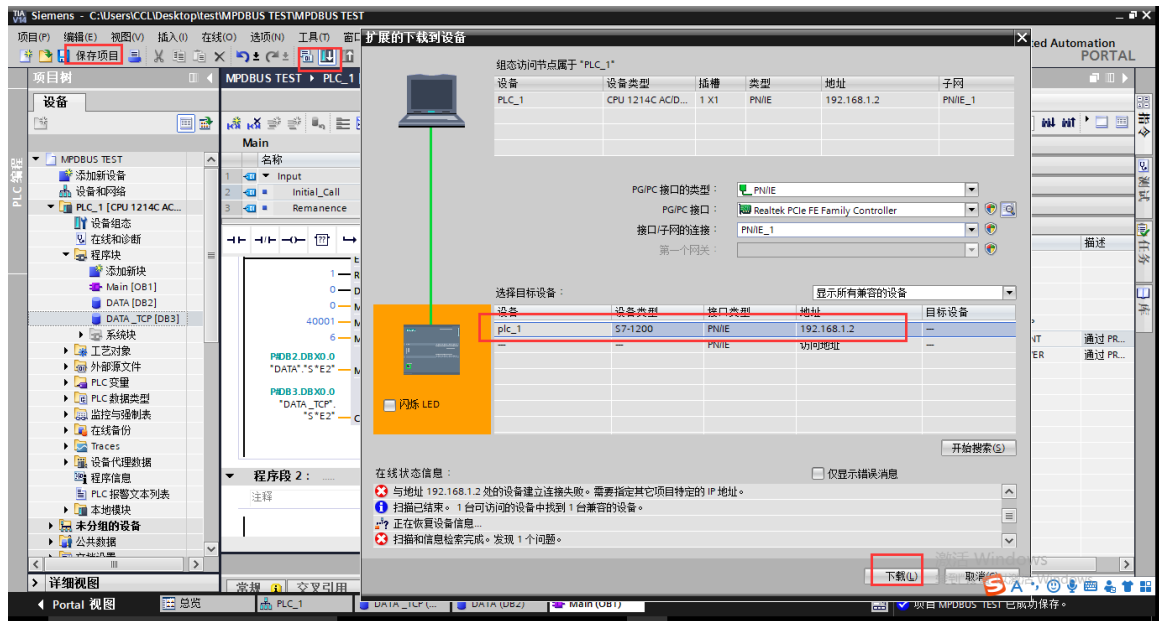




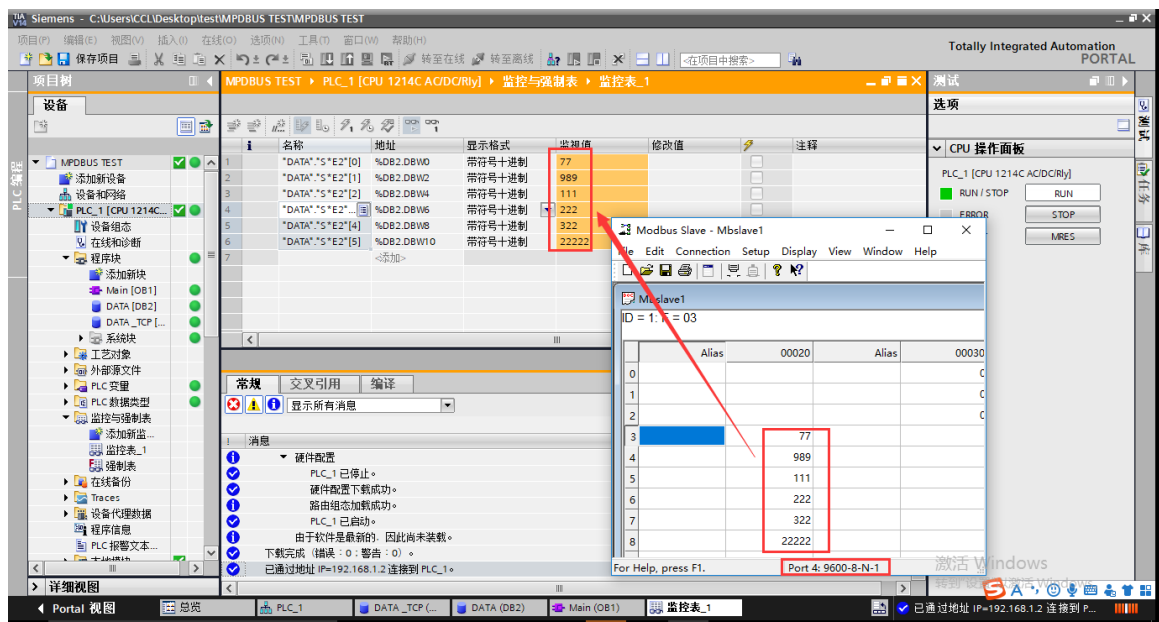
双击主程序块 Main[OB1]，在弹出的界面编程调用功能块 MB-CLIENT。



保存、编译、下载程序。



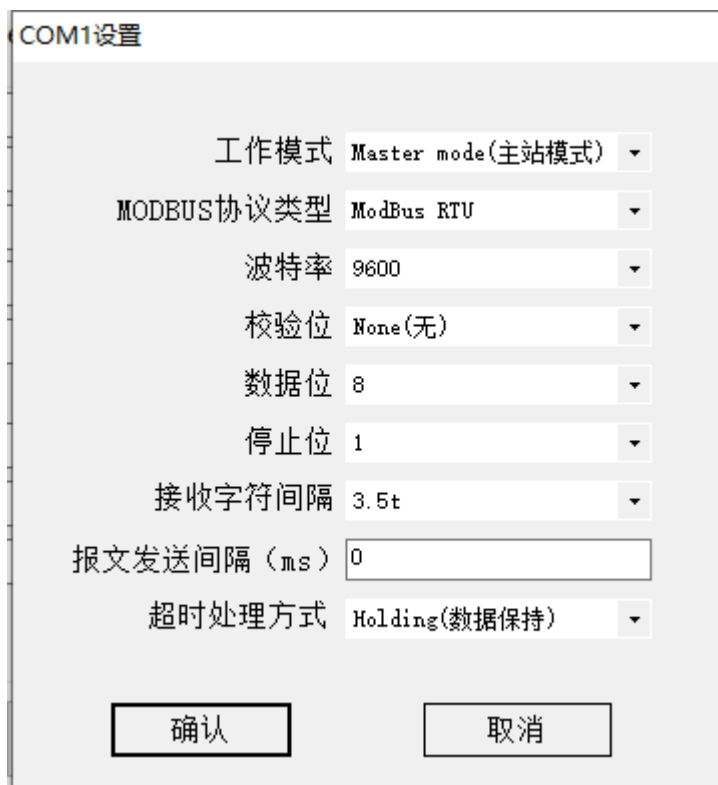
打开 Modbus Slave 软件模拟现场 RS485 设备，打开监控表，监控 DB2 里的数据，是否和 Modbus Slave 数据保持一致。

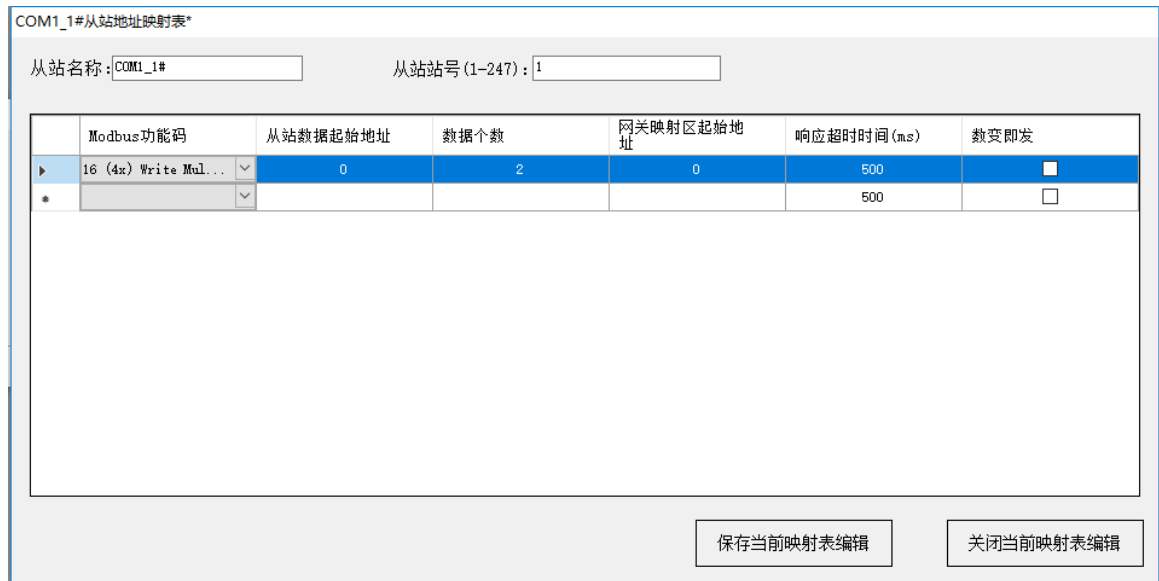


## 六、在上位机 WINCC V7.0 的测试应用

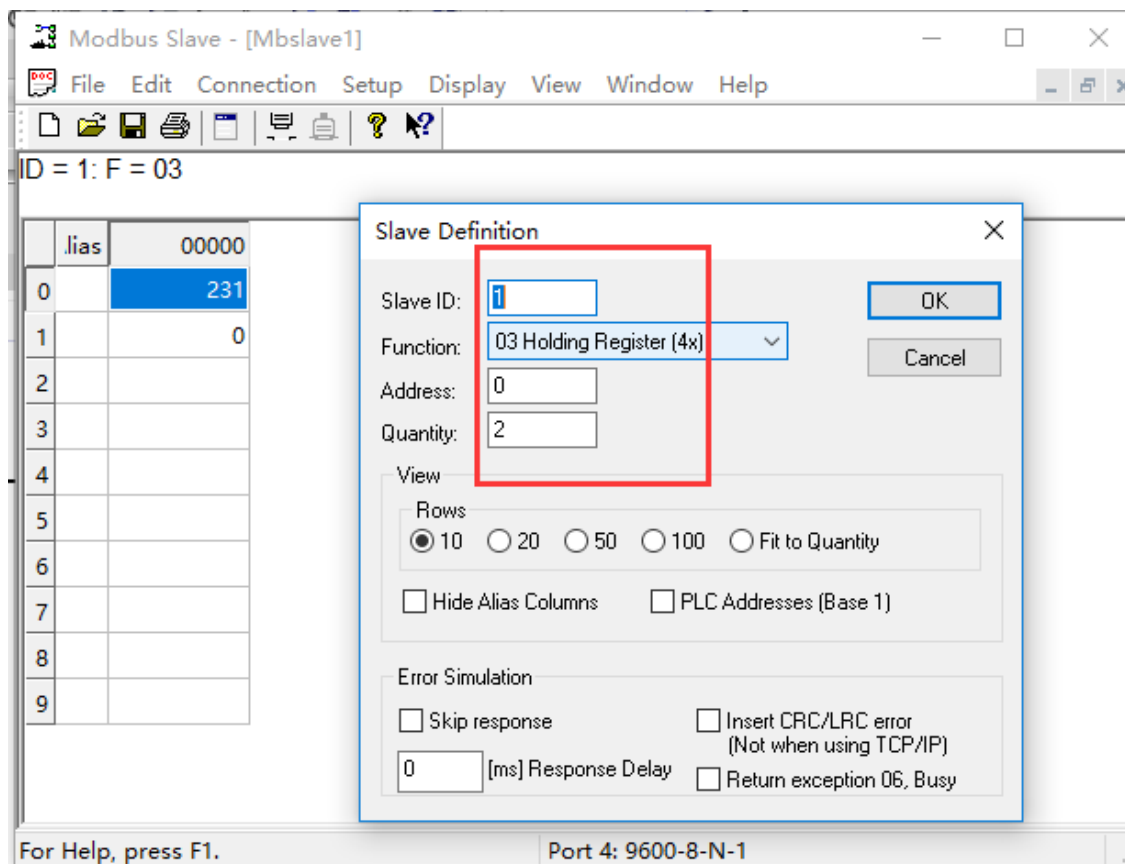
### 6.1 网关 ODOT-S4E2 的配置

网关 ODOT-S4E2 使用串口 1 进行测试,串口 1 采用默认串口参数(主站模式、地址映射模式、9600、N、8、1)。网关 MODBUS TCP 向串口 1 下挂 485 从站设备写值。





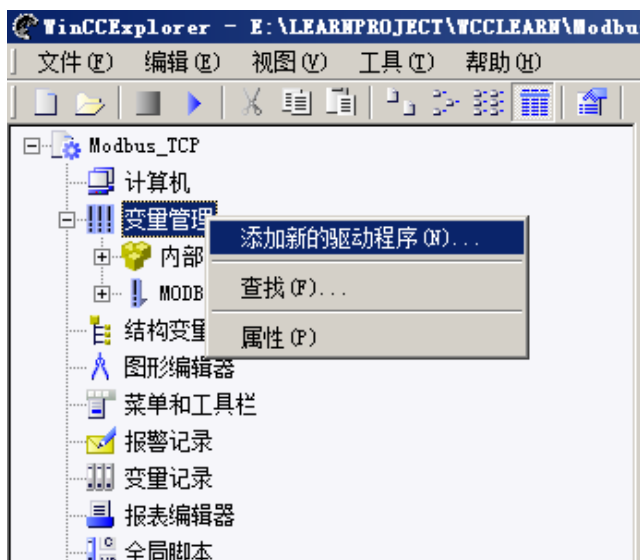
底层 485 从站设备采用 Modbus Slave 模拟从站。



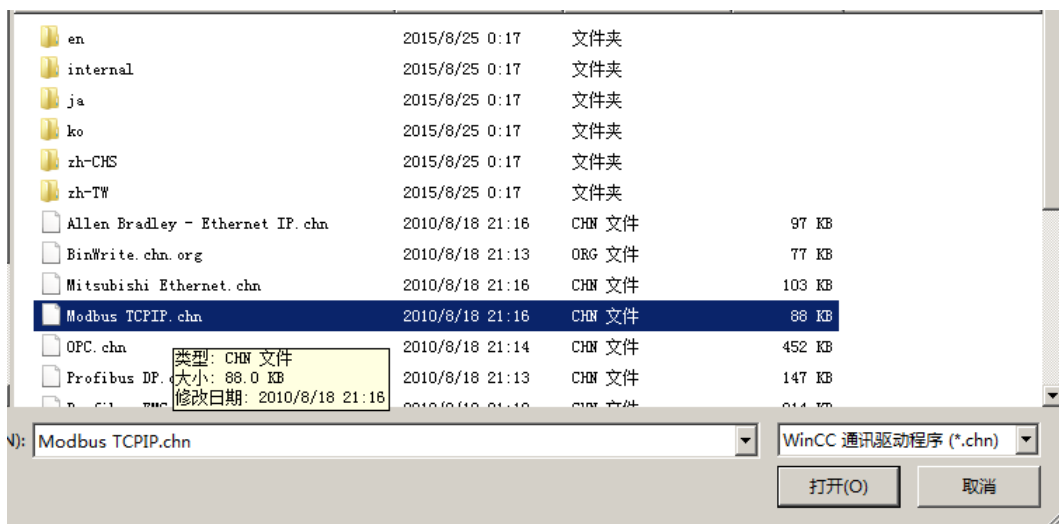
## 6.2 上位机 WINCC 的配置测试

本文档使用的 WINCC 版本为 7.0，请使用 7.0 及以上版本进行 MODBUS TCP 通讯。

打开 WINCC，建立一个新醒目 Modbus TCP。右击“变量管理”选择“添加新的驱动程序”。

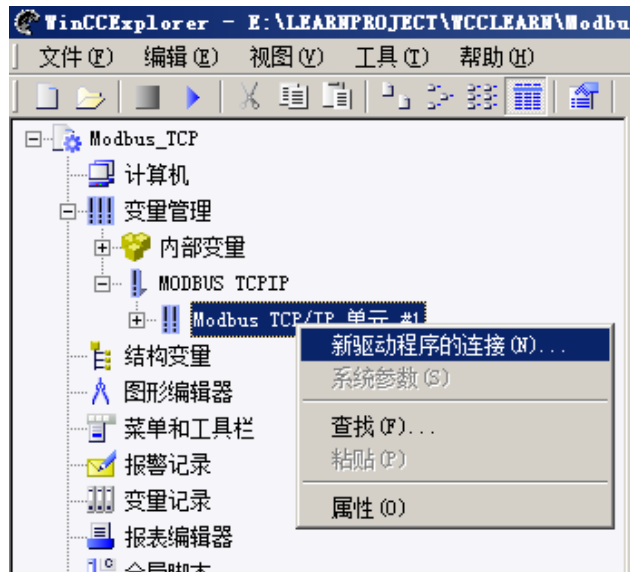


选择 Modbus TCPIP 驱动，点击“打开”。

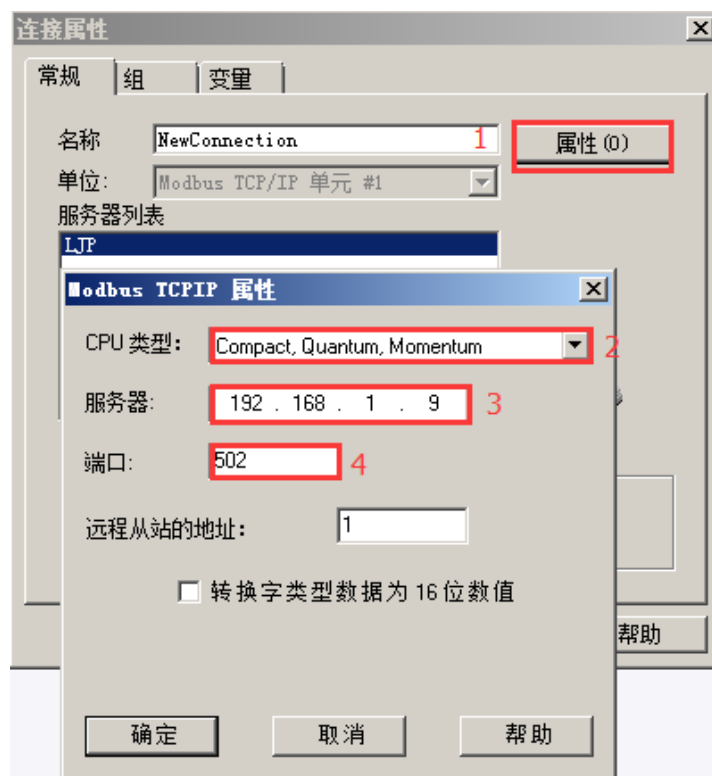


右击“Modbus TCPIP”，右击“Modbus TCPIP 单元#1”，点击“新驱动程序连接(N) ...”

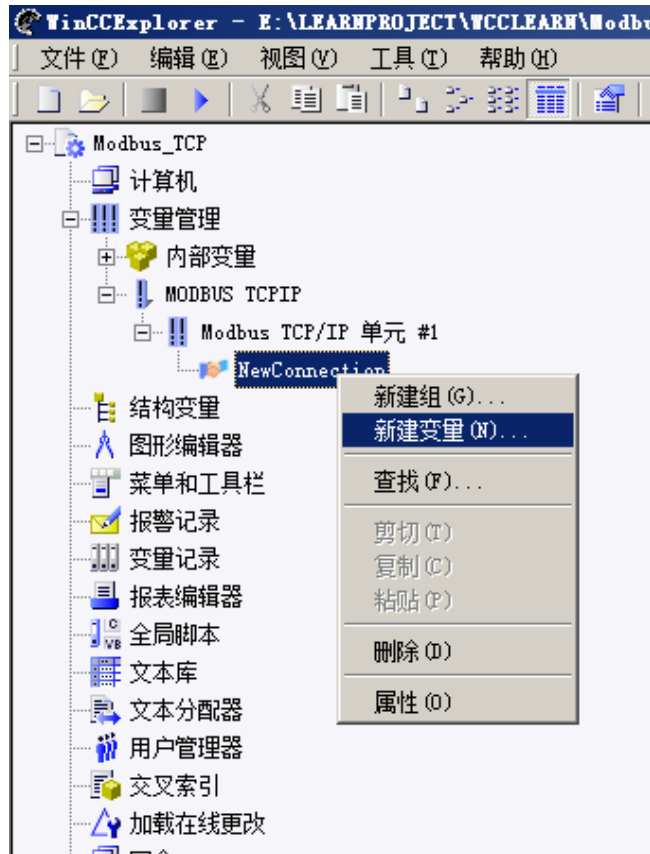




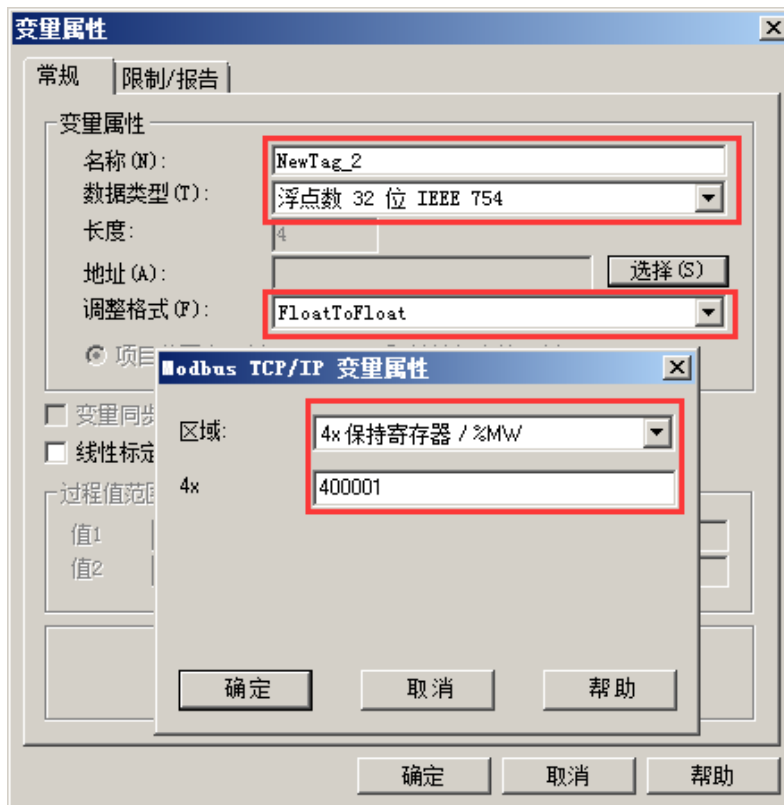
点击属性，选择 CPU 类型如下图“2”所示，填写 ODOT 网关或 I/O 模块 IP，端口选择 502（默认）。



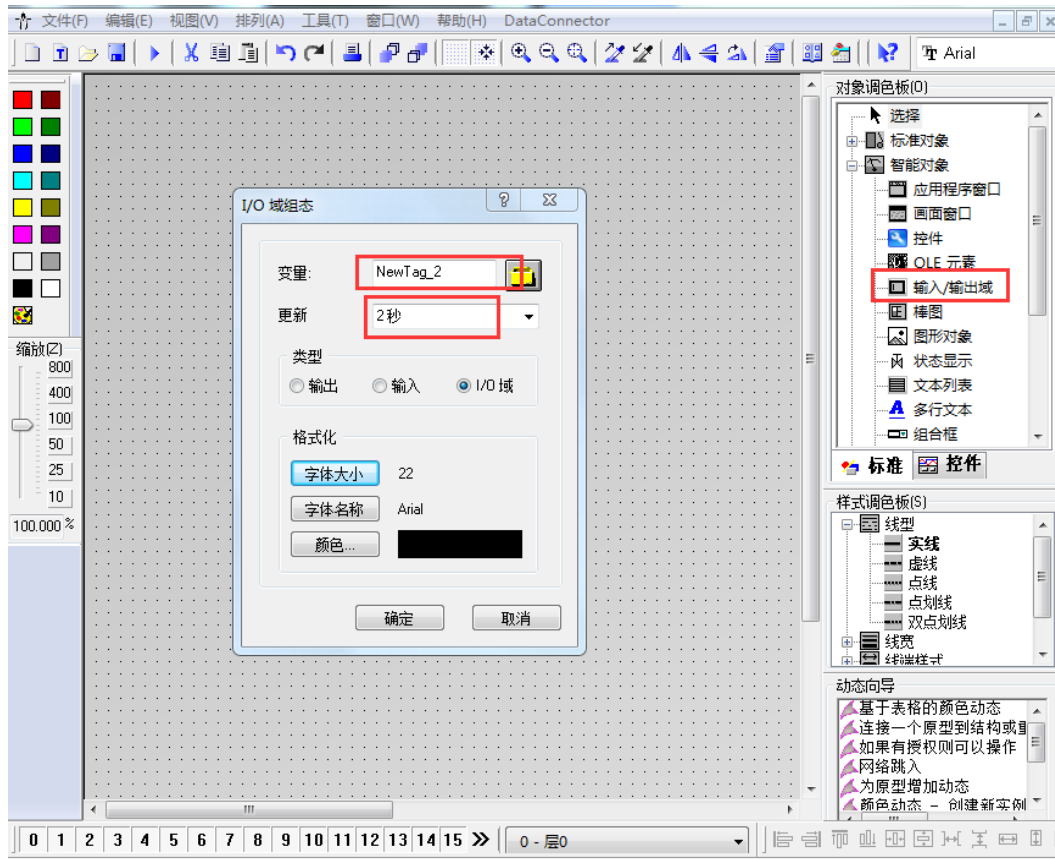
右击建立的连接，选择新建变量。



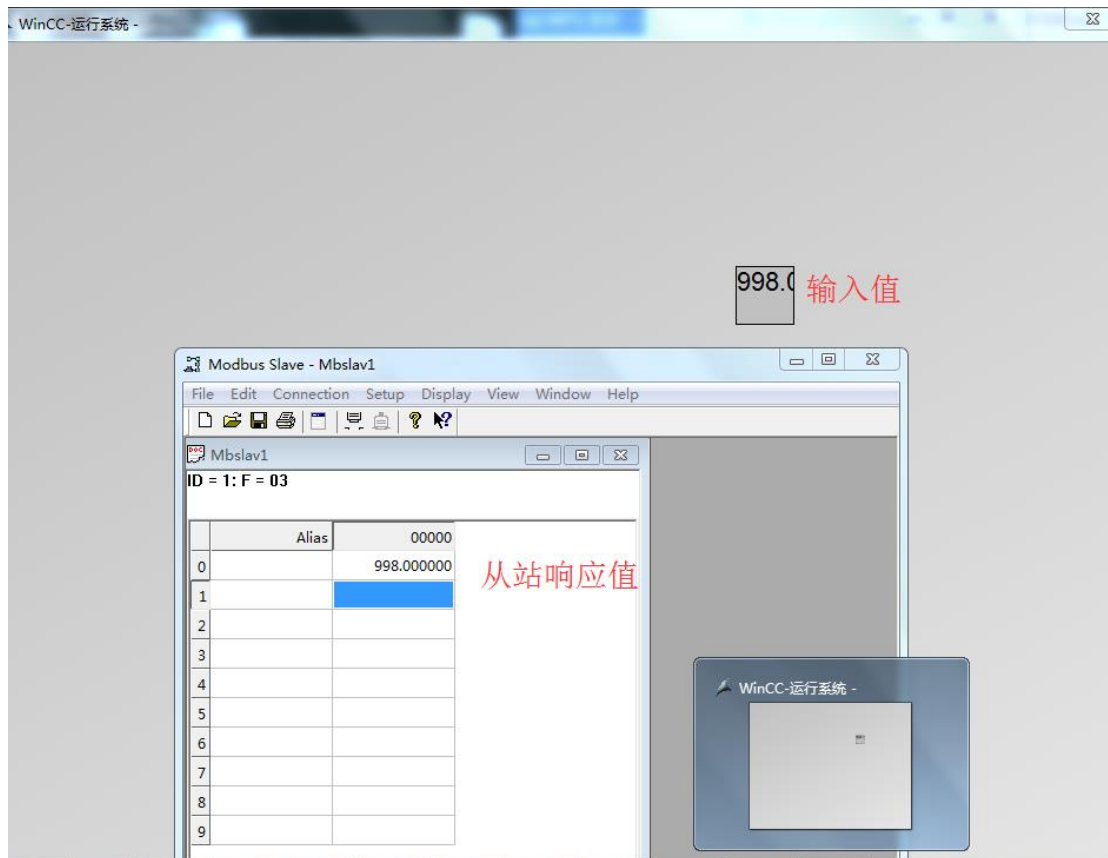
修改变量名称，选择数据类型及数据所在数据区以及地址。



打开画面编辑界面，选择输入/输出域对象，锁定刚才新建的变量。保存



WINCC 运行系统运行画面显示。

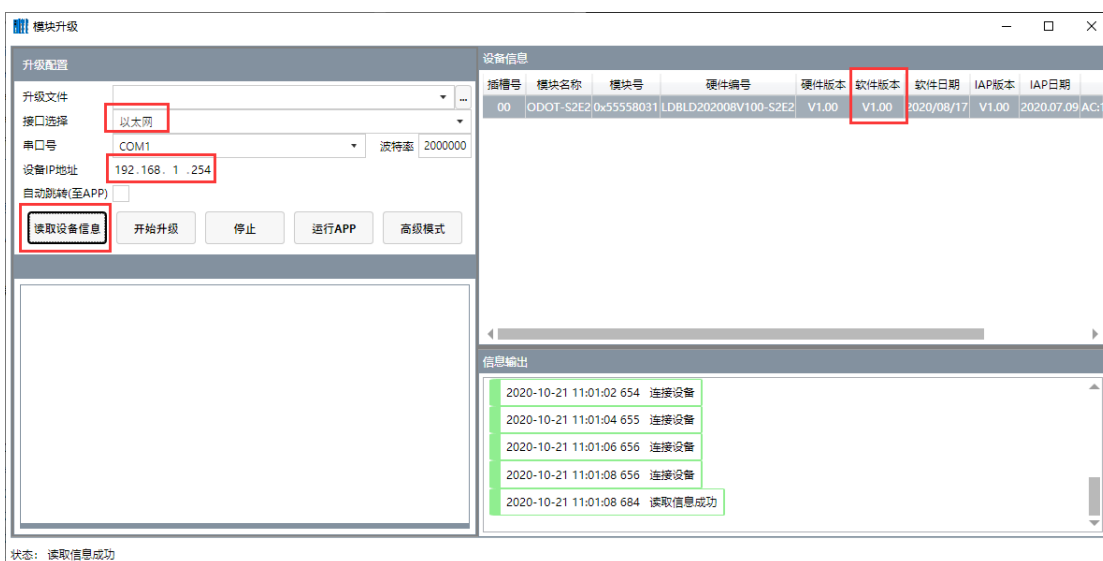



## 七、固件升级

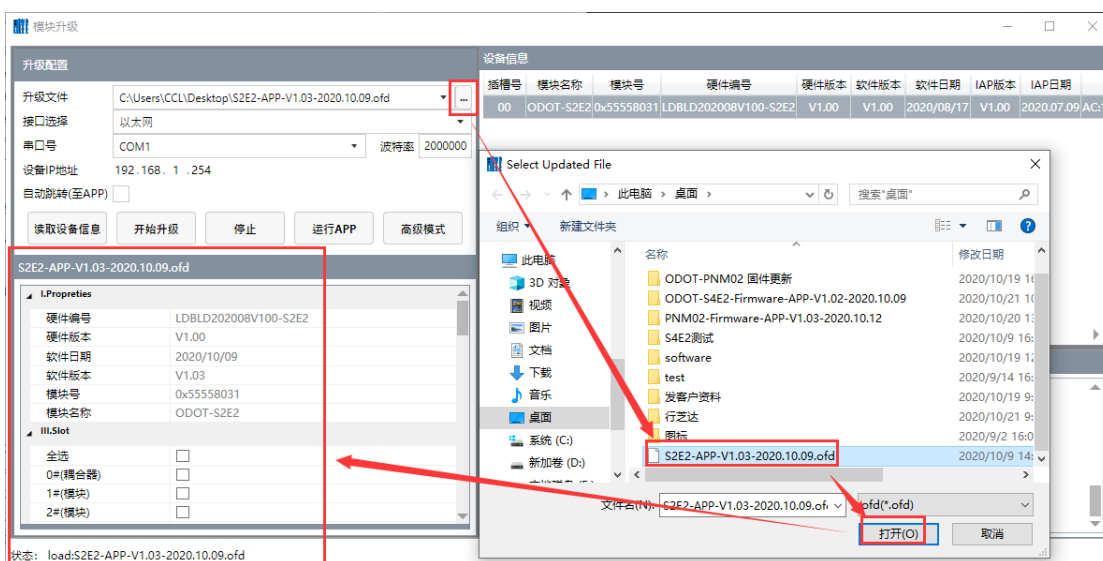
当模块固件更新，需要给网关固件升级，网关可以通过网口升级。给网关供电 24Vdc 电源，本机网卡 IP 地址和网关在同一网段（网关出厂默认地址是 192.168.1.254）。用一根网线连接电脑和网关。

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：192.168.1.254。点击读取设备信息，可以读取到网关内部固件信息。

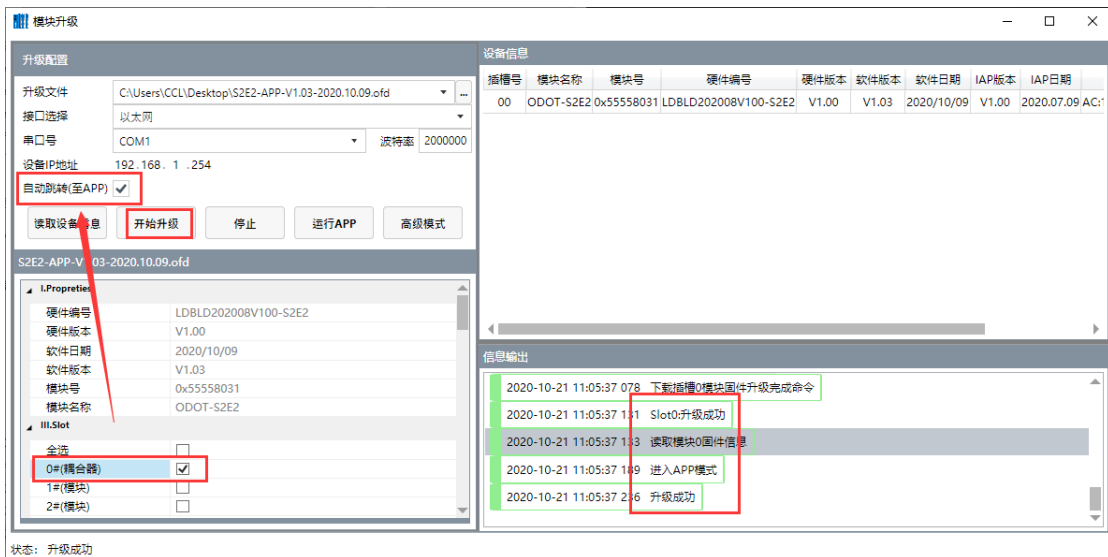
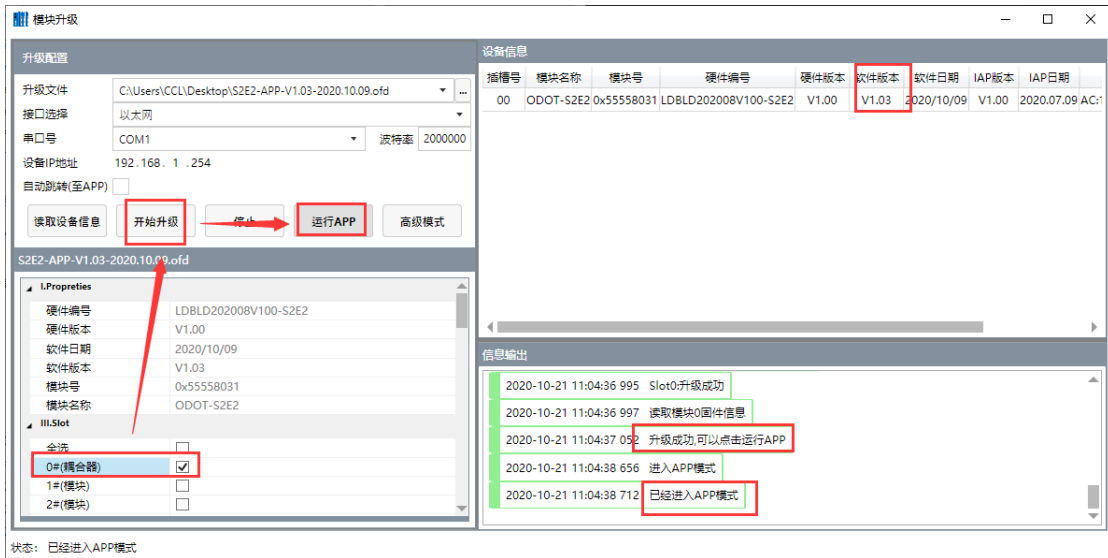


点击 , 在弹出的界面，选择新的固件文件，点击打开，会在左下角显示新固件信息。



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

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

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 17 号从机线圈 0172 ON 后原文返回

(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	xxx x

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 $-3\sim 15$ V 的信号作为逻辑“1”；将 $+3\sim 15$ V 的信号作为逻辑“0”；介于 $-3\sim +3$ V 之间的电压无意义，低于 $-15$ V 或高于 $+15$ V 的电压也无意义。

RS232 接口分类：

DB9 公头接口

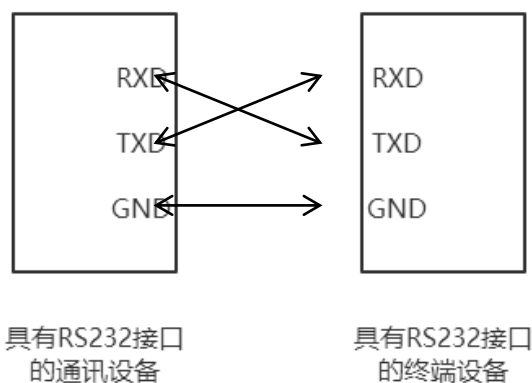


左上角为 1，右下角为 9

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 (Slave)，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。

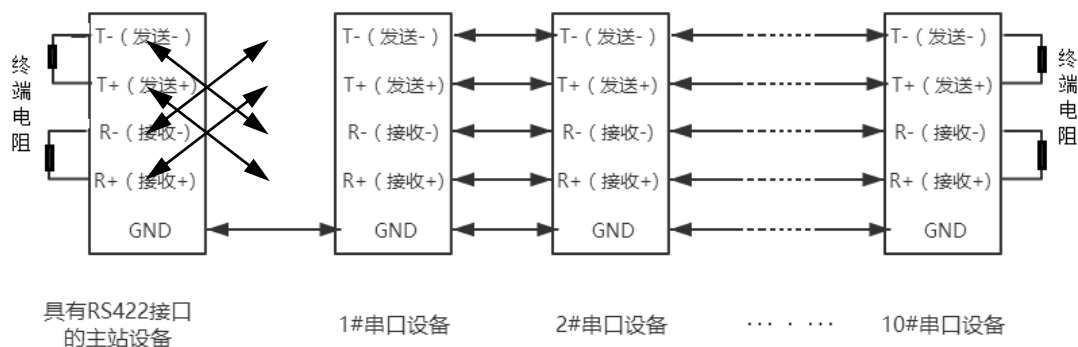
RS422 引脚定义:

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:



### 8.2.3 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端电阻等。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  $-(2\sim6)V$  表示逻辑"0"，两线间的电压差为  $+(2\sim6)V$  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。

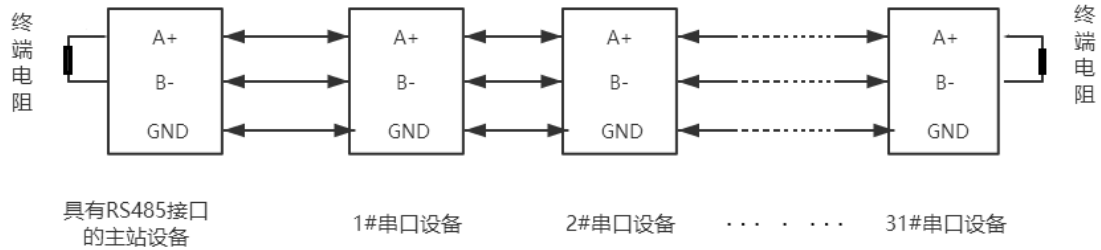
RS485 9 针引脚定义：



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