DL/T 645 到 Modbus 协议转换器

MG-S2EX

用户手册

V2.3

2020.10.21

DL/T 645 到 Modbus 协议转换器

四川零点自动化系统有限公司

2015-12

版权©2015 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
2015-12-15	V1.00	发布版本	GJ
2018-03-01	V2.00	硬件改版	CCL
2019-11-14	V2.10	配置软件截图 组态王里应用	CCL
2020-08-24	V2.2	硬件改版	CCL
2020-10-21	V2.3	新增固件升级章节	CCL

所有权信息

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

免责声明

本文档只用于辅助读者使用产品，本公司不对使用该文档中的信息而引起的损失或者错误负责。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。

备注：

1、配置软件 MG-S2EX V1.3 版本支持的固件版本为 V2.1 及以上。

2、配置软件 MG-S2EX V1.4 版本支持的固件版本为 V2.5 及以上。

3、V2.0 及以上固件版本支持 IAP 升级功能

4、配置软件 MG-S2EX V1.4 版本及其以上支持自动上传功能。

5、配置软件 MG-S2EX V1.4.5 版本支持的固件版本为 V1.14 及以上，新增串口 2 获取瞬时 A、B、C 相视在功率，前导码功能，序号检测错误代码。

软件下载

请登录零点自动化官网 www.odot.cn，在对应的产品页面点击下载。

免责条款

产品使用

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

免责范围

本公司不对以下情况导致的设备损坏或故障承担任何责任：

1、运输损坏：由于不当运输或包装造成的设备损坏；

2、自然因素：雷击、电压波动、进水或自然灾害（如火灾、洪水等）造成的损坏；

3、不当使用：超负荷、不规范操作、私自改装或使用不合格配件导致的损坏；

4、未授权维修：未经授权的维修或改动所导致的设备故障；

5、其他非产品原因：与设备本身无关的其他原因引起的损坏。

维修服务

1、对于上述原因导致的损坏，本公司将根据实际情况收取维修费用。

2、保修期外，本公司提供有偿维修服务，费用依据维修情况收取。

风险承担

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

目录

一、产品概述.....8
1.1 产品简介.....8
1.2 功能特点.....9
1.3 技术参数.....10
二、硬件说明.....11
2.1 产品外观.....11
2.2 指示灯说明.....12
2.3 端子定义.....13
2.4 复位开关.....14
2.5 外接终端电阻.....14
2.6 安装尺寸.....15
三、如何使用网关.....16
3.1 工作模式.....16
3.2 数据存储区.....16
3.3 系统诊断区.....17
3.4 网关 IP 地址修改.....21
3.5 网关参数配置.....23
3.5.1 实现 Modbus TCP 客户端与 Modbus RTU 从站和电表的通讯配置.24
3.5.2 实现 Modbus TCP 客户端与 Modbus RTU 主站和电表的通讯配置.34
3.5.3 实现 Modbus RTU 主站与电表的通讯配置.....37
四 在西门子 TIA V14 的测试应用.....40
4.1 网关 MG-S2EX 的配置测试.....40
4.2 软件 TIA V14 的配置测试.....42
五、在上位机组态王 V6.55 的测试应用.....46
5.1 网关 MG-S2EX 的配置.....46
5.2 上位机组态王的配置测试.....47

六、 固件升级.....52
七、 附录.....54
7.1 Modbus-RTU 协议简介.....54
7.1.1 Modbus 存储区.....54
7.1.2 Modbus 功能码.....54
7.2 串口网络拓扑结构简介.....60
7.2.1 RS232.....60
7.2.2 RS422.....61
7.2.3 RS485.....62

一、产品概述

1.1 产品简介

MG-S2EX 网关支持多种协议，如 DL/T645-1997 主站、DL/T645-2007 主站、Modbus-RTU 主站/从站、Modbus-TCP 服务器。可实现的协议转换功能包括 DL/T645-1997/2007 主站转 Modbus-TCP 服务器，Modbus-RTU 从站、Modbus-RTU 主站转 Modbus-TCP 服务器、DL/T645-1997/2007 主站转 Modbus-RTU 从站。

1.2 功能特点

- 19.2~28.8VDC 电压输入，防反接保护。
- 支持多种协议的相互转换。
- DC-DC 隔离电源，3000V 隔离电压。
- 双以太网口，带交换机功能，支持级联(线性拓扑)。
- 2KV 网口隔离保护，10M/100Mbps 速率自适应，支持 Auto MDI/MDIX。
- 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 5 个 TCP 客户机同时访问。
- 映射模式支持功能码：0x01,0x02,0x03,0x04,0x05,0x06,0x0F,0x10。
- 6KB 超大数据缓存区，数据传输量更大。
- RS485 带浪涌保护，内置偏置电路，稳定性强。需外接终端电阻。
- 数据包发送间隔可自由调节，使用更灵活。
- 设备自带强大诊断功能,实时监控从设备通信状态,快速排除通讯故障。
- 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。
- 配置参数可保存到本地文件，配置文件支持拖拽读取功能。
- 2007 版数据单个表可采集 74 个数据，1997 版可采集 42 个变量。

1.3 技术参数

本产品相关技术参数如“表 1”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。

表 1. 技术参数

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	19.2~28.8VDC，3KV 隔离电压
功耗	Max.100mA@24V
以太网参数	
网关工作模式	地址映射模式，Modbus TCP 协议
以太网端口数量	2 个 RJ45，10M/100Mbps、自适应速率，带交换机功能
网络协议	ETHERNET、ARP、IP、TCP、ICMP
TCP 连接数量	最大 5 个
串口参数	
串口数量	2 路 RS485
串行通信模式	RTU 模式和 DL/T645 模式
串口终端电阻	需外置 120Ω 电阻
支持的波特率	RTU 模式：1200~115200 bps DL/T645 模式：600~19200 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）
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）：8192 Word 4xxxx 区（保持寄存器）：8192 Word 3xxxx 区（系统诊断区）：264 Word

二、硬件说明

2.1 产品外观

2.2 指示灯说明

设备共有 6 个 LED 状态指示灯，其符号定义及状态说明如“表 2”所示。

表 2. 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
SF	系统故障指示	ON	TCP 网关通信错误
		OFF	TCP 网关通信正常
TX1	串口 1 发送指示	ON	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	ON	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	ON	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	ON	串口 2 在接收数据
		OFF	串口 2 未接收数据

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。

上侧电源端子定

序号	端子	定义
1	PE	接地端子
2	V-	电源输入负
3	V+	电源输入正

正面串口端子定义

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：

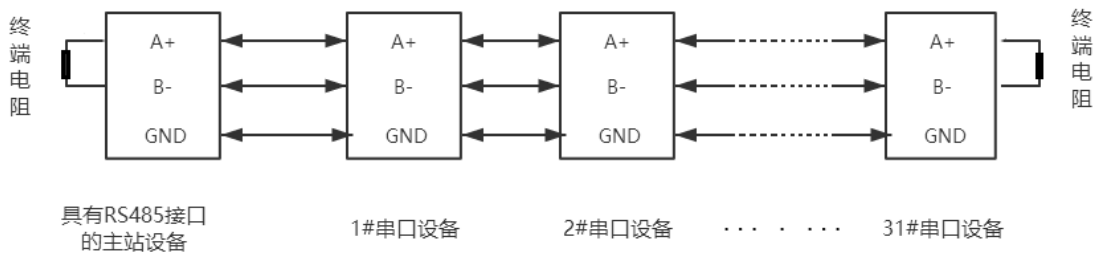
参数名称		默认值
以太网	协议转换器 IP	192.168.1.254
	子网掩码	255.255.255.0
	局域网网关 IP	192.168.1.1
	Modbus TCP 数据端口	502
	配置端口	1024

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

Fieldbus Gateway: MG-S2EX
Modbus to Modbus-TCP Gateway
Power Supply: 19.2-28.8VDC
Operating Temperature: -40~85℃
Humidity: 5~95%RH(non-condensing)
LED Status
PWR Power status
STAT Syatem status
TX1: 1# serial transmit status
RX2: 1# serial recelve status
TX2: 2# serial transmit status
RX2: 2# serial recelve status
Sichuan Odot Automation System Co.,Ltd.
www.odot.cn
400 1024 485
SN:20211208WG0147
PWR
STAT
TX1
RX1
TX2
RX2
RESET
1B-
1A+
SGND
PE
2B-
2A+
SGND
PE
NC
100mm
30mm
80mm

三、如何使用网关

3.1 工作模式

网关有多种工作模式用以实现不同协议之间的相互转换，不同工作模式下各端口支持的协议类型如下表所示。

工作模式	串口 1 协议	串口 2 协议	以太网协议
工作模式 1	Modbus-RTU 主站	DL/T645 主站	Modbus-TCP 服务器
工作模式 2	Modbus-RTU 从站	DL/T645 主站	Modbus-TCP 服务器
工作模式 3	Modbus-RTU 从站	DL/T645 主站	

3.2 数据存储区

Modbus 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”存储区域，共 8192 个字。第四部分为“保持寄存器”存储区域，共 8192 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 264 个字。在工作模式 1 下访问“系统诊断区”可获得 Modbu-RTU 网络中各从站的信息，可用于设置 Modbus 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 5”所示。

表 5.Modbus 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	8192 Word	0x0000~0x1FFF
4	4 区	保持寄存器	8192 Word	0x0000~0x1FFF
5	3 区	系统诊断	264 Word	0x2000~0x2107

3.3 系统诊断区

系统诊断区在工作模式 1 下数据有效，其他模式无用。系统诊断区分为两部分，第一部分：地址 0x2000-0x200F 共 16 个 word 即 256 个位，为“从站错误指示区”，其中编号为 1-246 的位分别对应地址为 1-246 的从站，编号 248-256 的位保留。当从站通信出现错误时，从站地址对应的位被置 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 6”所示。

表 6. 从站错误指示区编码格式

地址 0x2000	BIT	Bit15	Bit14	Bit13	Bit12	Bit11	Bit10	Bit9	Bit8
	位编号	16	15	14	13	12	11	10	9
	BIT	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
	位编号	8	7	6	5	4	3	2	1
地址 0x2001	BIT	Bit15	Bit14	Bit13	Bit12	Bit11	Bit10	Bit9	Bit8
	位编号	32	31	30	29	28	27	26	25
	BIT	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
	位编号	24	23	22	21	20	19	18	17
.									
.									
.									
地址 0x200F	BIT	Bit15	Bit14	Bit13	Bit12	Bit11	Bit10	Bit9	Bit8
	位编号	x	x	x	x	x	x	x	x
	BIT	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
	位编号	x	x	246	245	244	243	242	241

第二部分：地址 0x2010-0x2105 共 246 个 Word，为串口 1“从站状态指示”区，读取该区可获得从站的当前工作状态，其数据编码格式如“表 7”所示。

表 7. 从站状态指示区编码格式

地址 0x2010	从站 1	Byte1	Byte0
		功能码	错误代码
地址 0x2011	从站 2	Byte1	Byte0
		功能码	错误代码
.			
.			
地址 0x2105	从站 246	Byte1	Byte0
		功能码	错误代码

每一个 Word 分为高低两个字节，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 8”所示。

表 8. 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，请参考从站手册选择对应的功能码模块
0x02	非法数据地址	设备数据超出其地址范围，参考从站手册修改数据起始地址或数据长度
0x03	非法数据值	数据长度错误，数据长度超出最大允许值 125(Word)或2000(Bit)，修改长度
0x04	数据处理错误	检查数据值范围是否符合从站要求
0x05	应用层长度不匹配	增大接收字符间隔，检查通信参数设置
0x06	协议 ID 错误	检查发送端报文
0x07	缓存地址错误	设备内部错误
0x08	位偏移错误	设备内部错误

0x09	从站 ID 号不匹配	增大超时时间，检查硬件连接状态，检查通信参数设置
0x0A	CRC 错误	CRC 错误，检查通讯线路
0x0B	LRC 错误	LRC 错误，检查通讯线路
0x0C	应答功能码不匹配	检查硬件连接状态
0x0D	应答地址不匹配	检查硬件连接状态
0x0E	应答数据长度不匹配	检查硬件连接状态
0x0F	通信超时	增大超时时间，检查硬件连接状态，检查通信参数设置
0x10	ASCII 模式起始符错误	‘:’冒号起始符错误
0x11	ASCII 模式结束符错误	CR/LF 回车换行结束符错误
0x12	ASCII 模式非字符数据	数据中包含非16进制 ASCII 码
0x13	ASCII 模式字符数错误	从站应答长度错误

第三部分：地址 0x2106-0x2107 共 2 个 Word，为串口 2“从站状态指示”和“错误代码”区。当从站通信出现错误时，串口 2 下电表对应的序号位被置 1。从站恢复正常后对应的错误指示位将自动清零。读取该区可获得从站的当前工作状态，其数据编码格式如 “表 9”所示。错误代码“表 10”所示。

表 9. 电表从站状态指示区编码格式

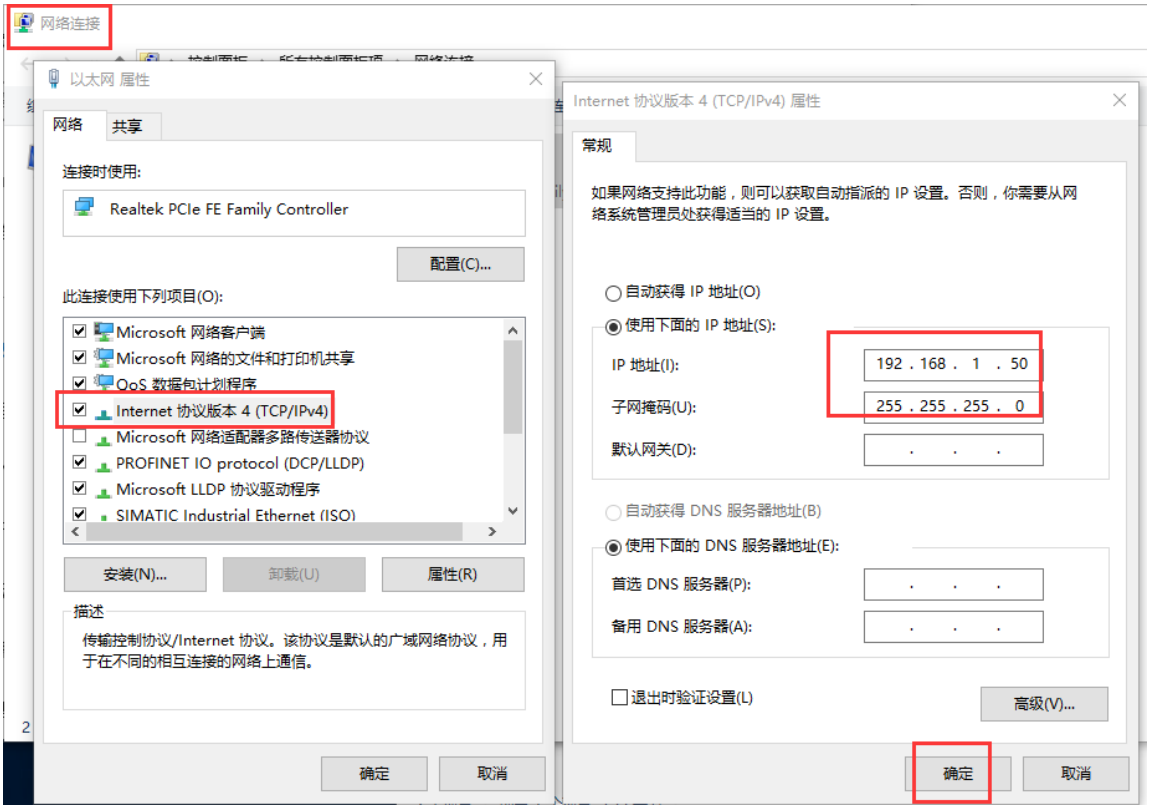
地址 0x2106	Word0
	串口 2 下所挂电表序号
地址 0x2107	Word0
	错误代码

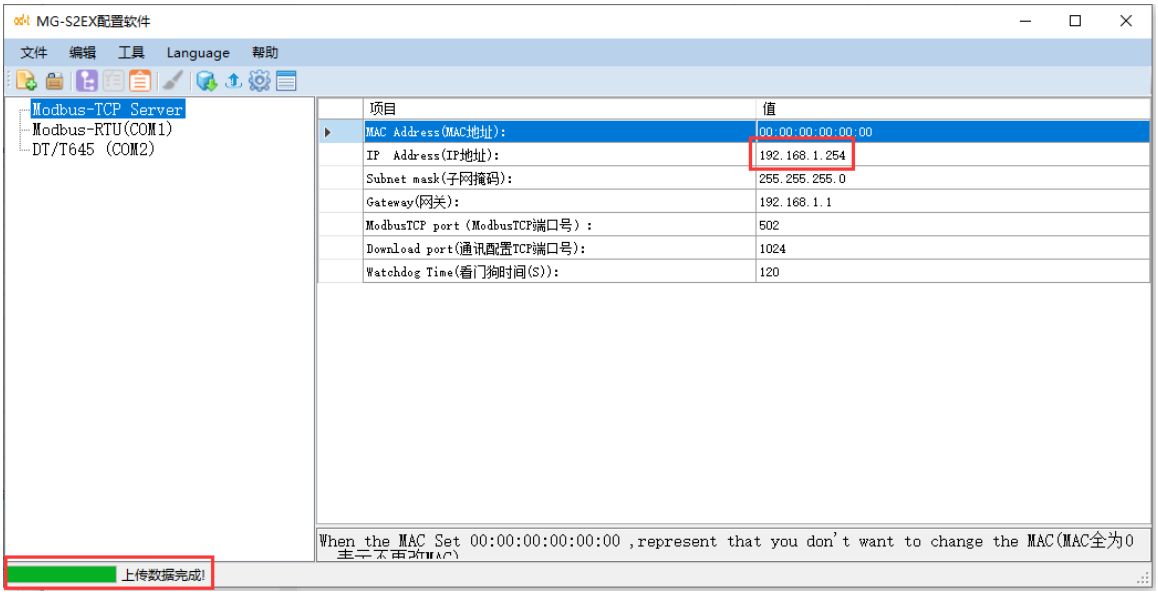
表 10. 电表从站错误代码说明如下图

错误代码	说明
0x00	从站工作正常
0x07	奇偶校验错误
0x09	帧 CS 校验错误
0x0B	响应超时
0x80	异常响应代码
0x81	帧格式错误，帧起始符合结束符错误
0x82	序号不匹配

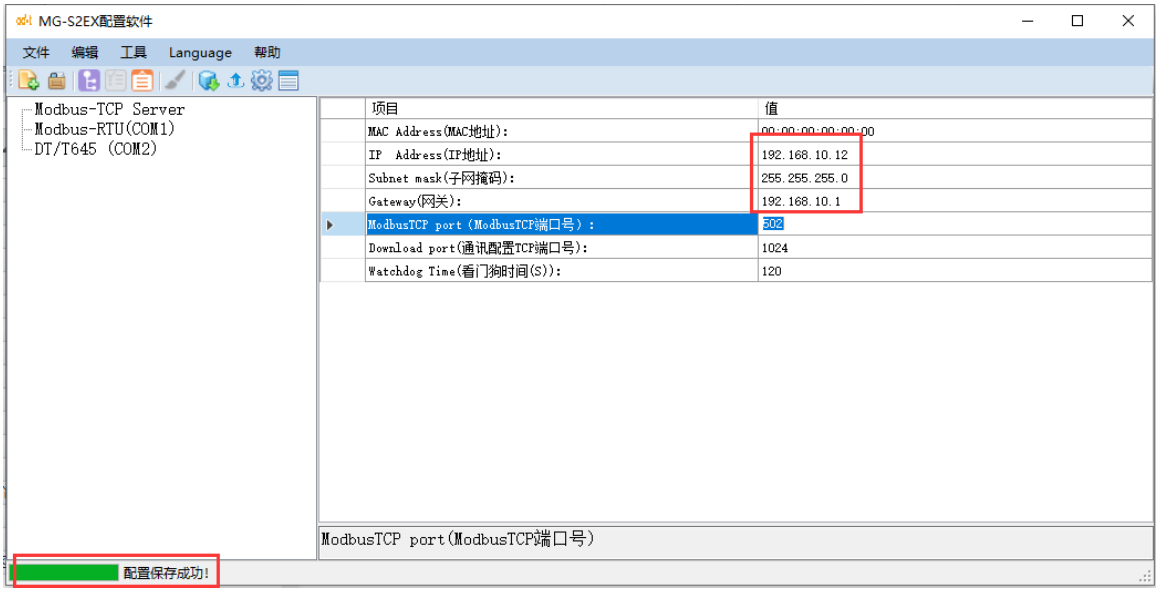
3.4 网关 IP 地址修改

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‘MG-S2EX 配置软件’，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）。。

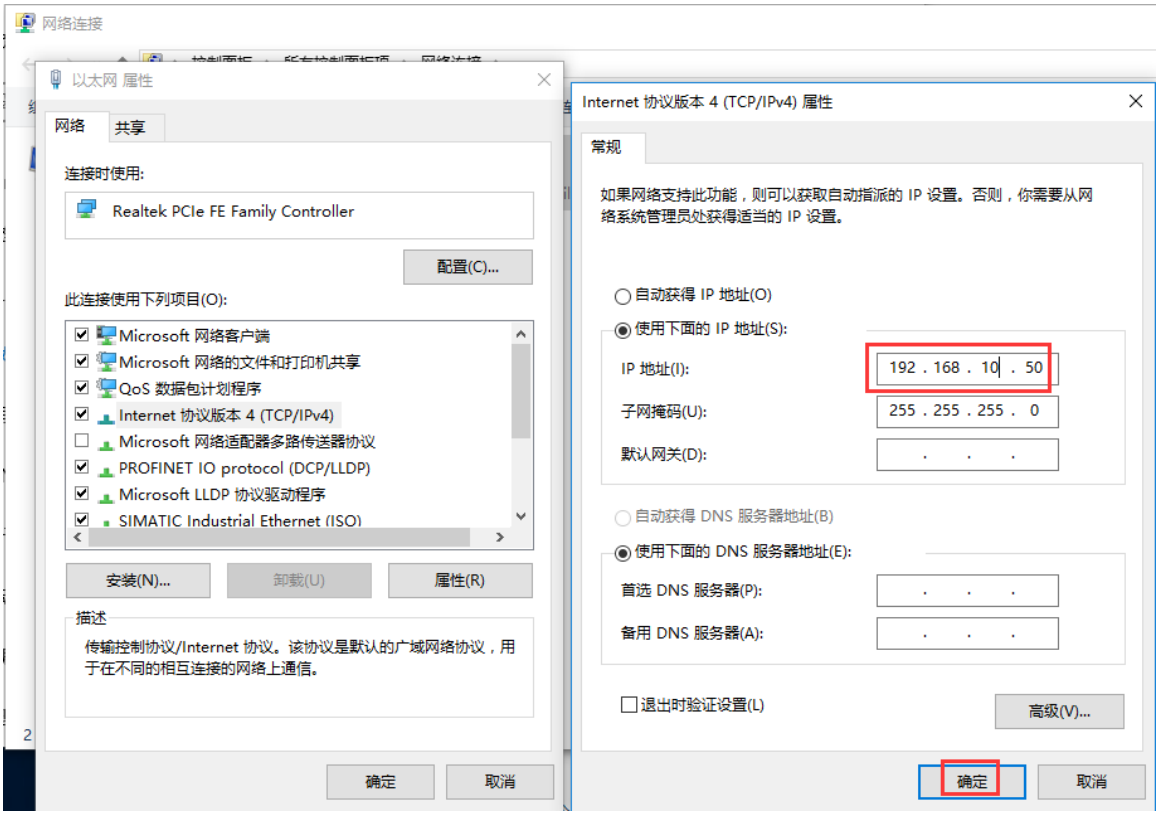




修改配置软件界面的网关 IP 地址为：192.168.10.12（跨网段），局域网网关 IP 改为：192.168.10.1，修改完成后直接点击下载网关配置，在右下角可以看见配置保存成功。

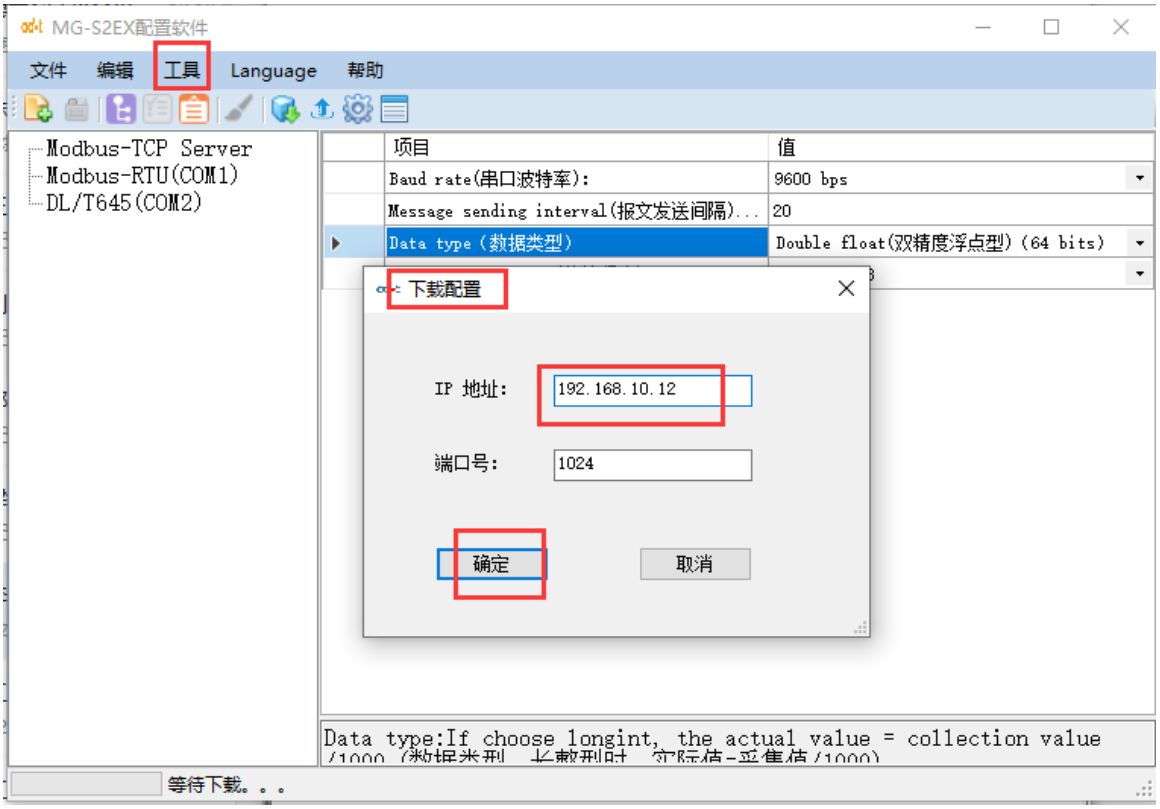


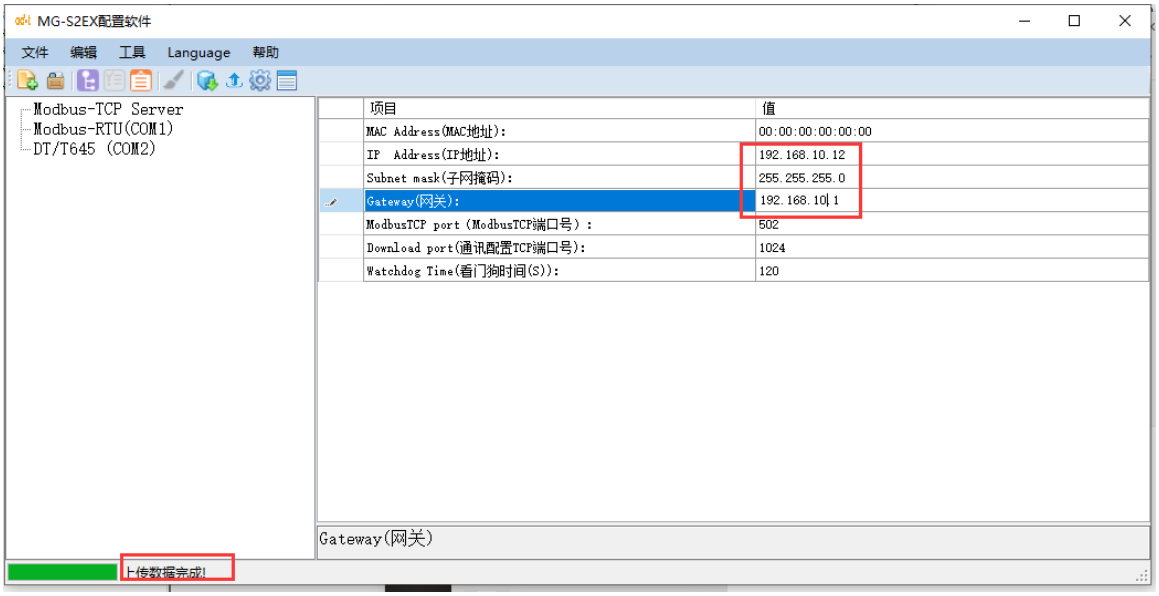
IP 地址修改成功后，需要将本机电脑 IP 地址改到：192.168.10.*网段。



在配置软件‘MG-S2EX 配置软件’界面点击工具——通讯配置，修改网关 IP 地址为硬件内部 IP 地址。点击确定。点击上载按钮，上载成功后，可在左下角

看见上传数据成功。





3.5 网关参数配置

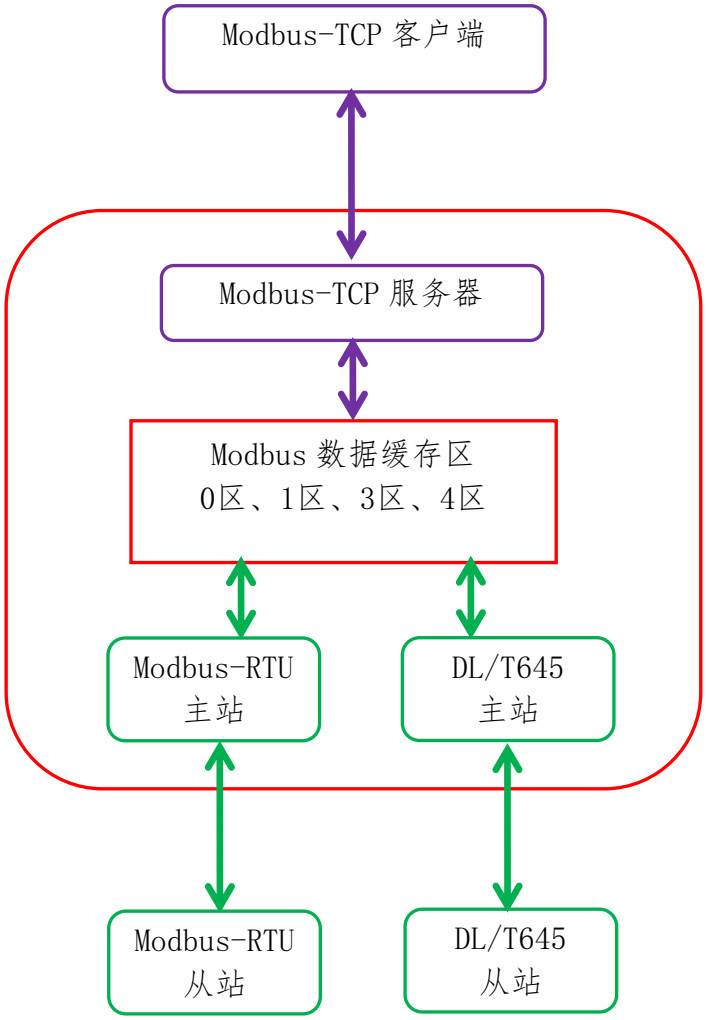
网关的工作模式见说明 3.1 工作模式，网关出厂设置为“工作模式 1”。配

置网关的参数请使用“MG-S2EX 配置软件”，软件安装包在官网上下载，或可拨打技术支持热线 400-1024-485 咨询。

注：在测试时请将本机网卡 IP 地址改到：192.168.1.*网段。

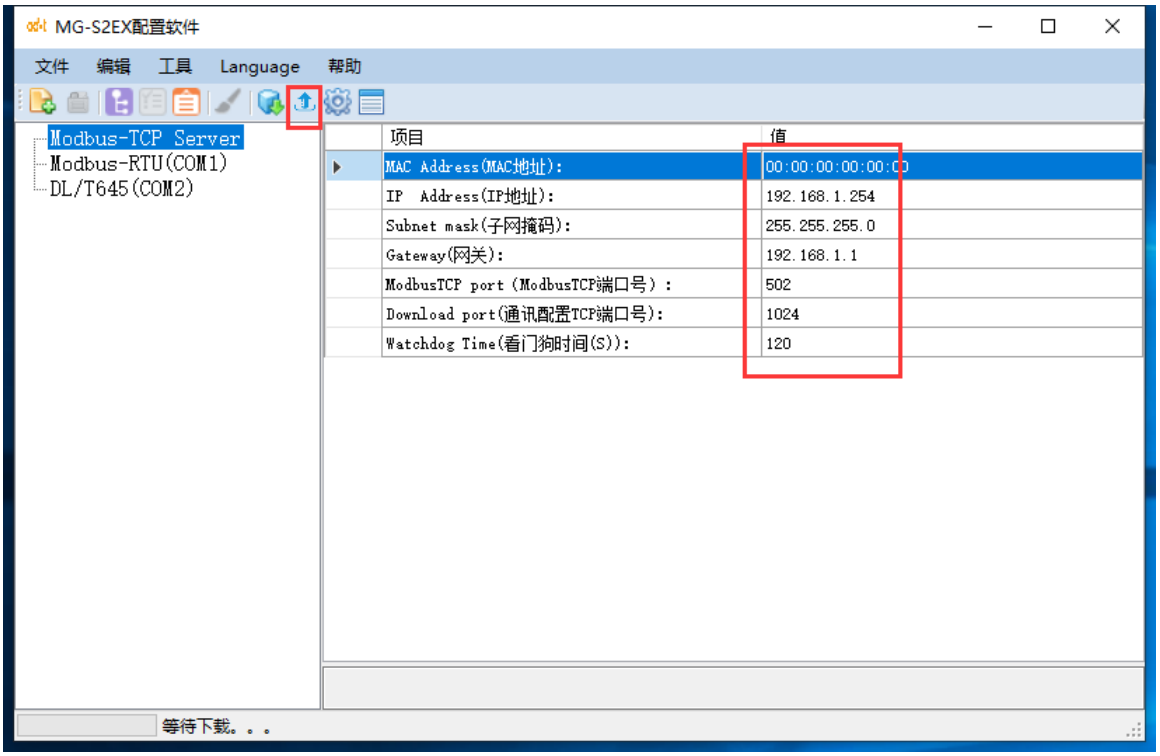
3.5.1 实现 Modbus TCP 客户端与 Modbus RTU 从站和电表的通讯配置

工作模式 1 时，串口 1 为 Modbus-RTU 主站，可连接标准 Modbus-RTU 从站设备。串口 2 为 DL/T645 主站，可连接支持该协议的电能表，DL/T645 支持 1997 和 2007 两个版本。2007 版数据单个表可采集 65 个数据，1997 版可采集 42 个数据。Modbus-RTU 主站和 DL/T645 主站读取到的数据均存入 Modbus-TCP 服务器存储区中。其数据交换原理如下图所示：

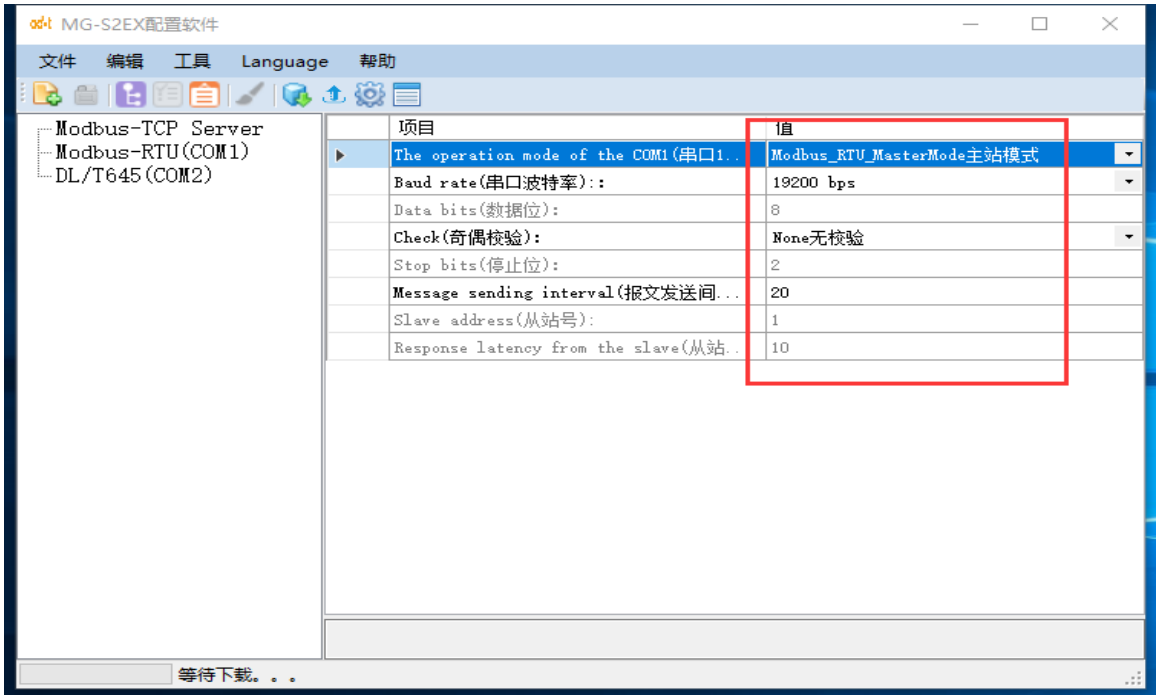


工作模式 1 的配置流程如下：

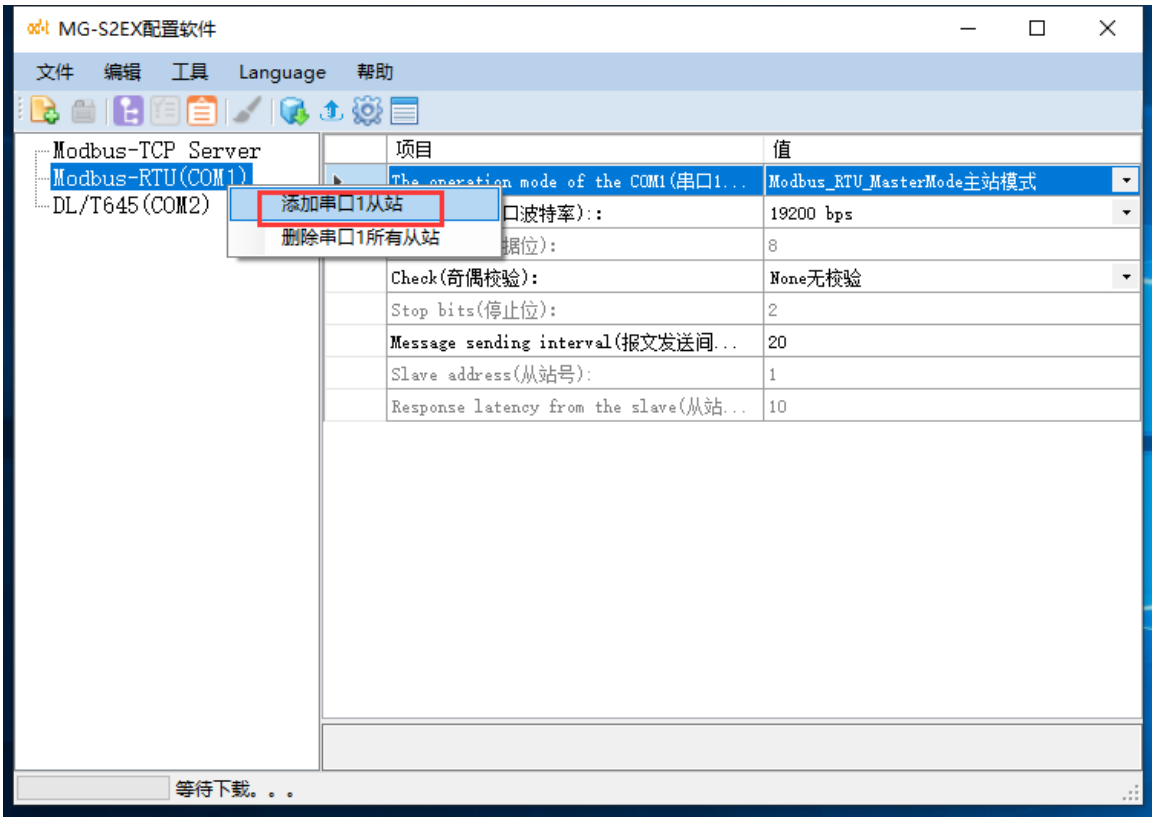
a. 双击安装文件夹中的“MG_S2EX Config.exe”文件，打开配置软件。点击 可自动上传网关默认参数（注：默认 IP 地址是 192.168.1.254，若是不能上载请先 ping 一下 IP 地址或者按一下复位按钮）。



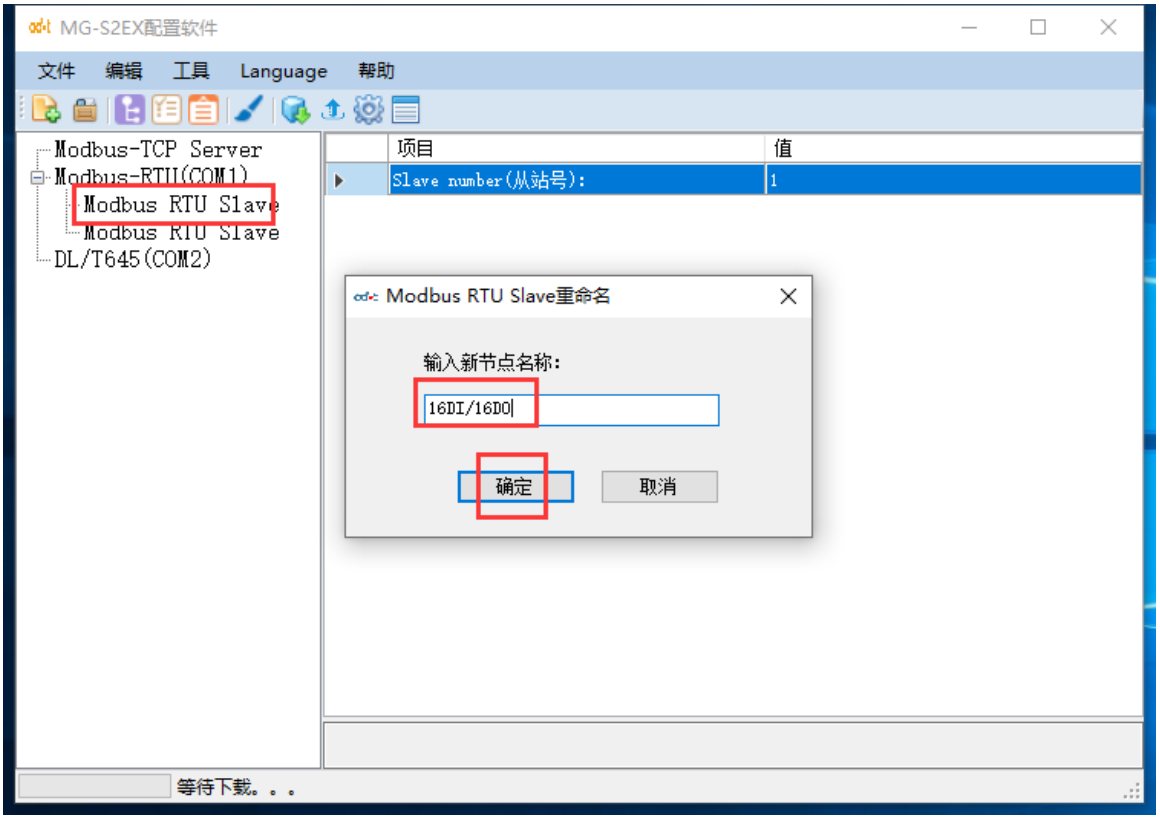
b. 配置 Modbus 主站参数，串口工作模式选“Modbus_RTU_MasterMod 主站模式”，设置波特率、校验、报文发送间隔等参数。报文发送间隔需根据从站具体而定，建议设在 10ms 以上。

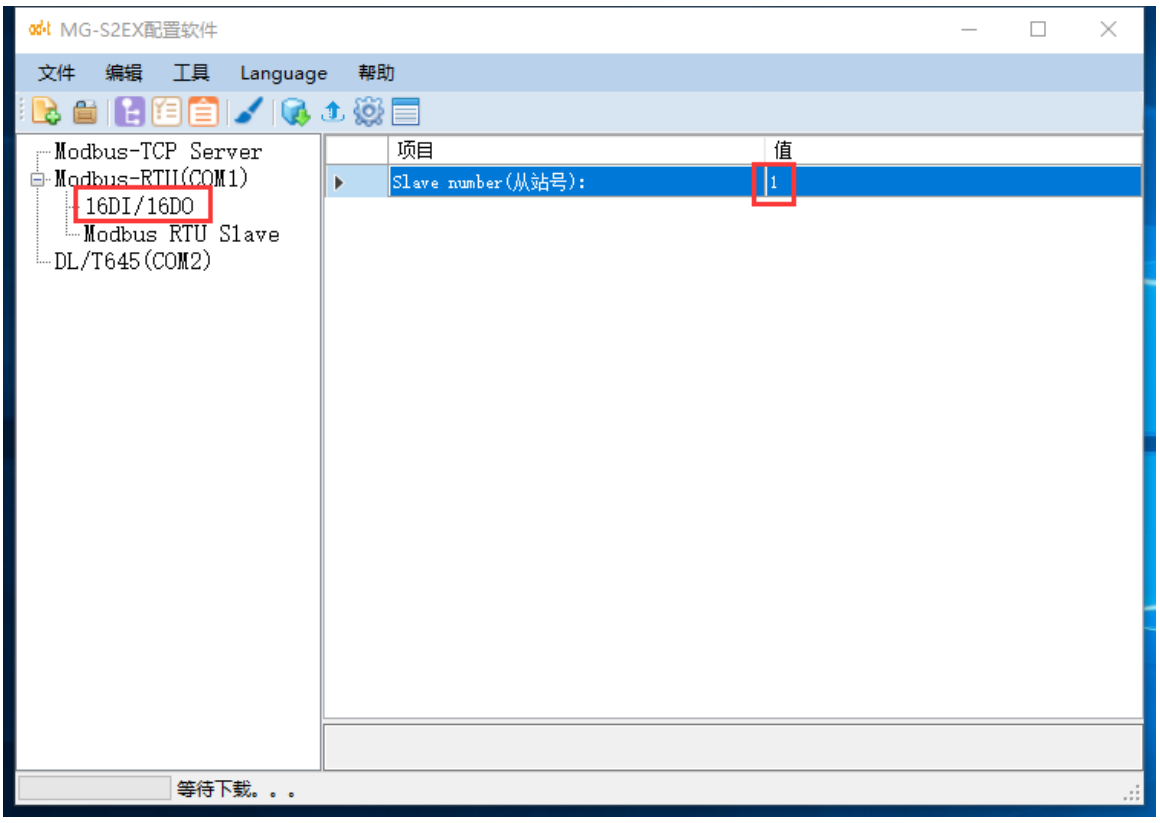


c. 选中串口 1，单击右键添加串口 1 从站。

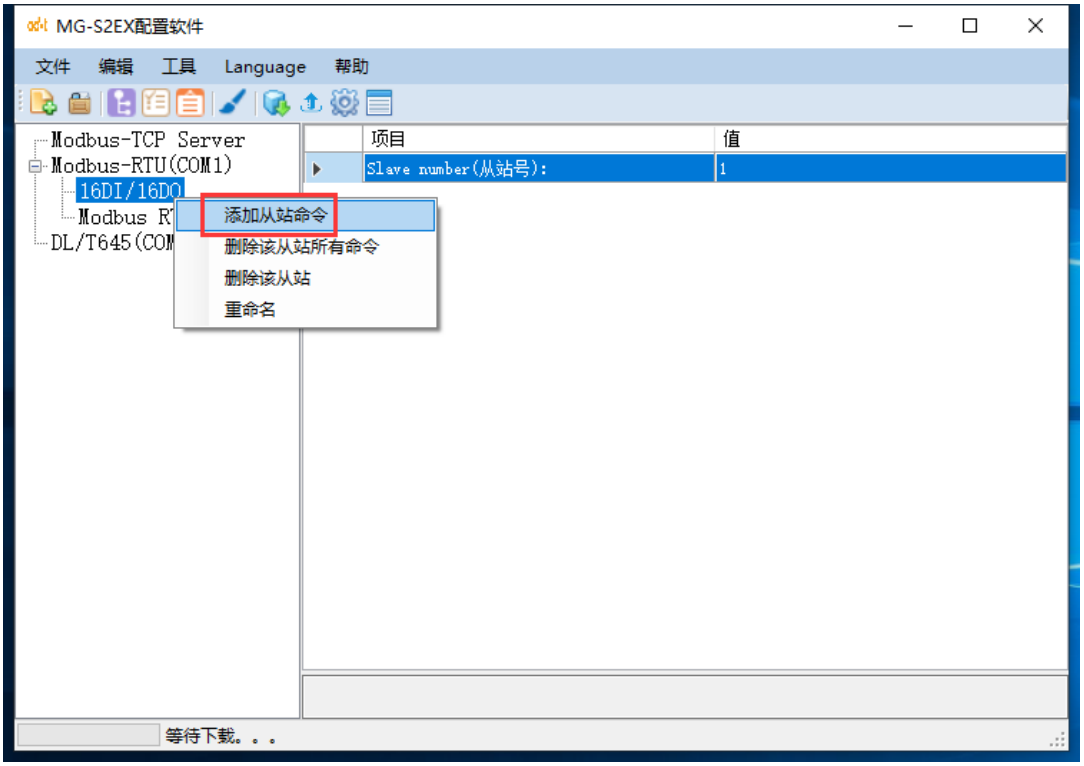


d. 右键重命名或双击修改从站名称为 16DI/16DO，填写 Modbus 从站号 ID=1，需与从站所设置地址一致。

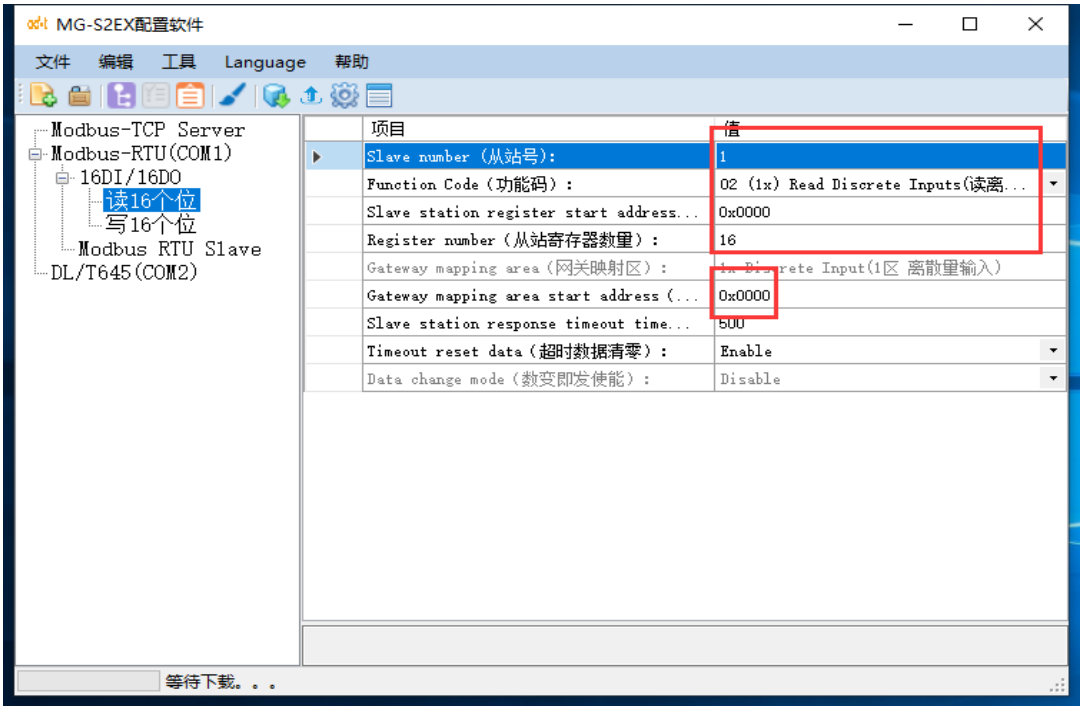




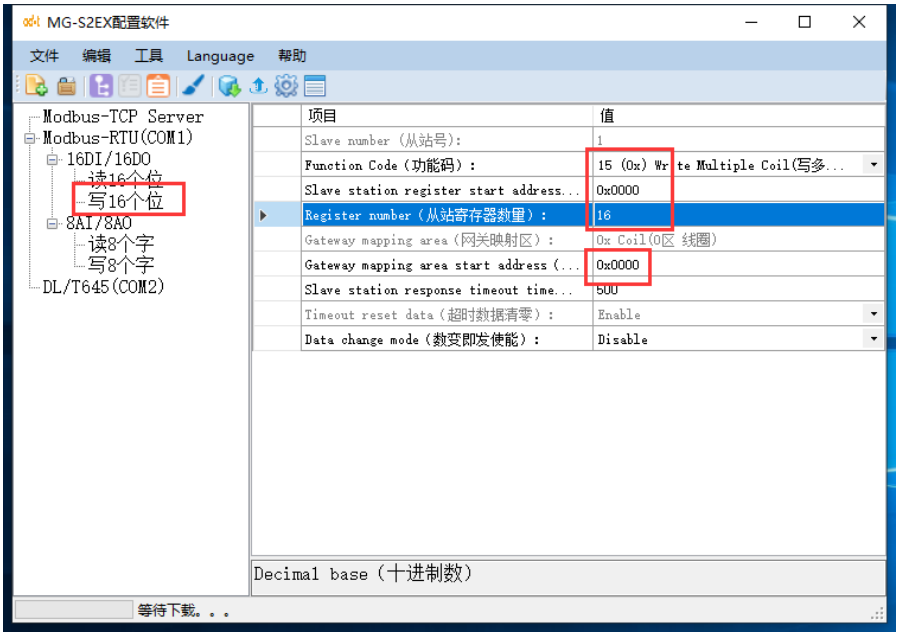
选中从站“16DI/16DO”，单击右键添加从站命令。



f. 修改命令名称，选择“读 16 个位”命令，设置对应的功能码、设置从站起始地址、设置读取数量、设置网关映射地址、设置超时时间、超时处理方式等参数。测试读取 1 区数据。

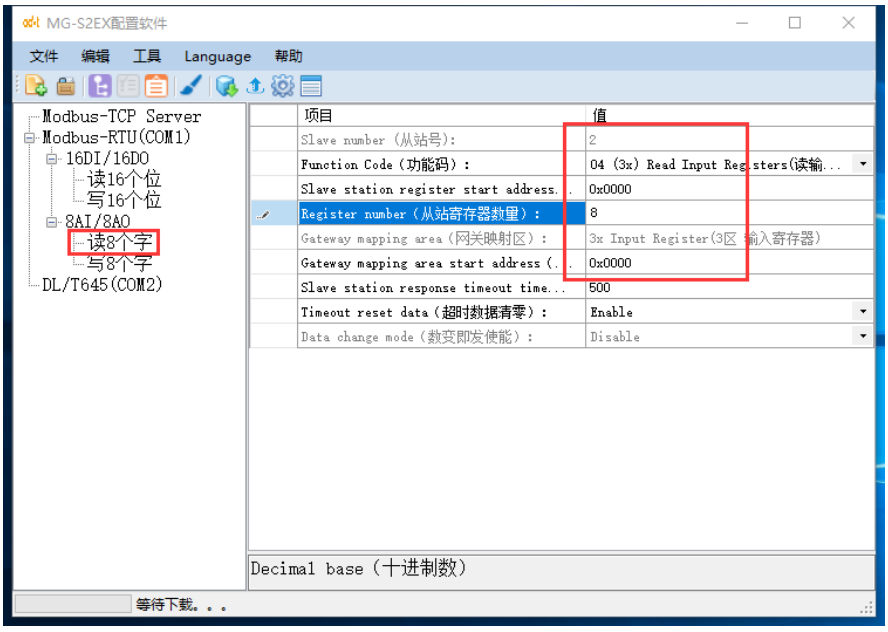


g. 选择“写 16 个位”命令，设置对应的功能码、设置从站起始地址、设置从站写入数量、设置网关映射地址、设置超时时间、数变即发使能等参数。测试写入 0 区数据。

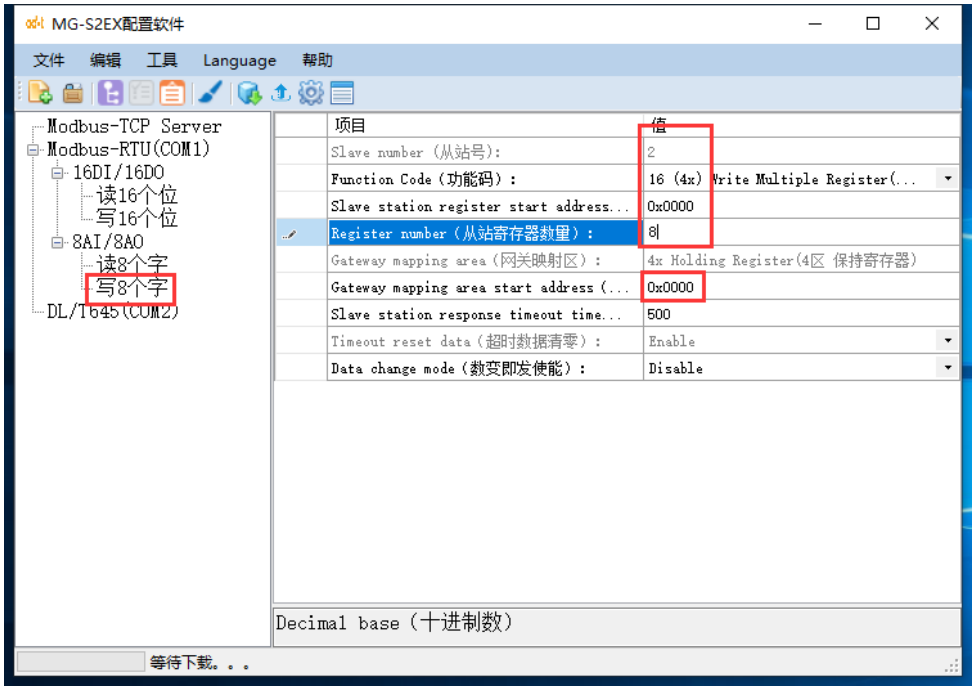


h. 新增从站修改名称为 8AI/8AO，参照 16DI/16DO 步骤，选中从站“8AI/8AO”，单击右键添加从站命令。

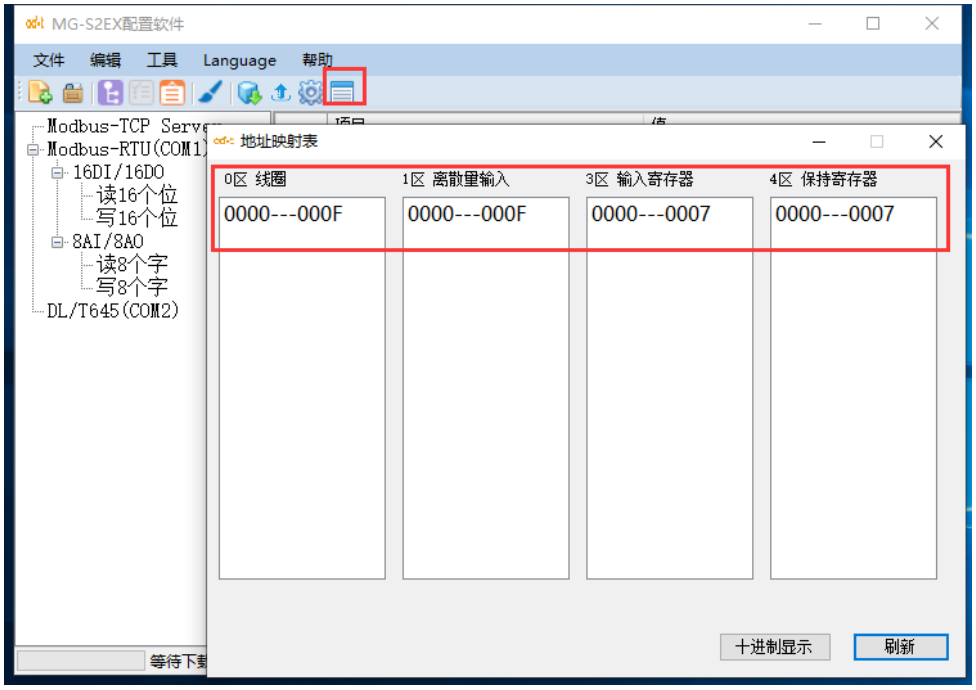
选择“读 8 个字”命令，设置对应的功能码、设置从站起始地址、设置读取数量、设置网关映射地址、设置超时时间、超时处理方式等参数。测试读取 3 区数据。



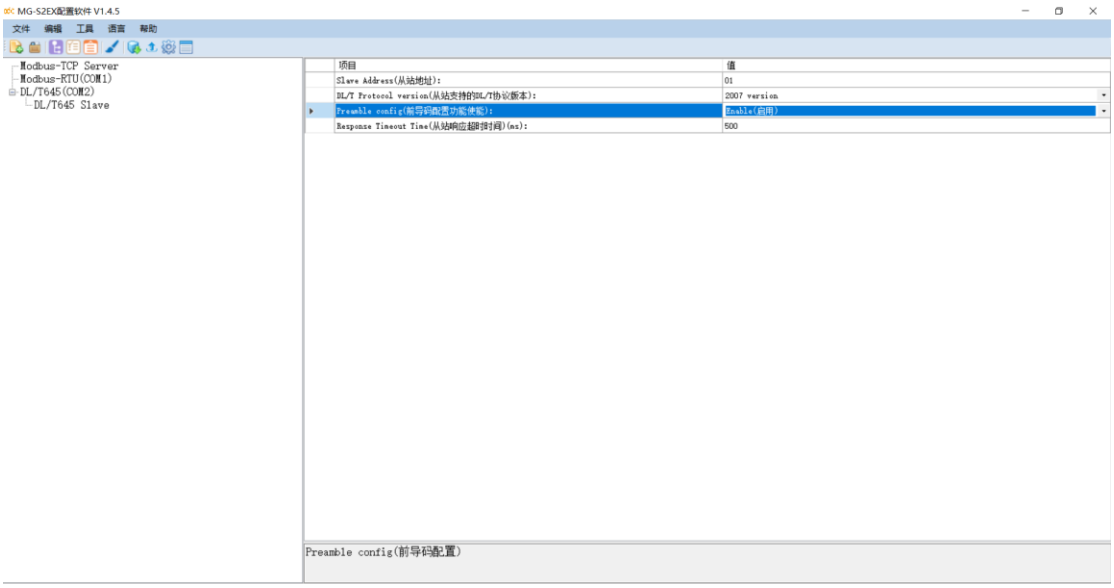
i. 选择“写 8 个字”命令，设置对应的功能码、设置从站起始地址、设置从站写入数量、设置网关映射地址、设置超时时间、数变即发使能等参数。测试写入 4 区数据。



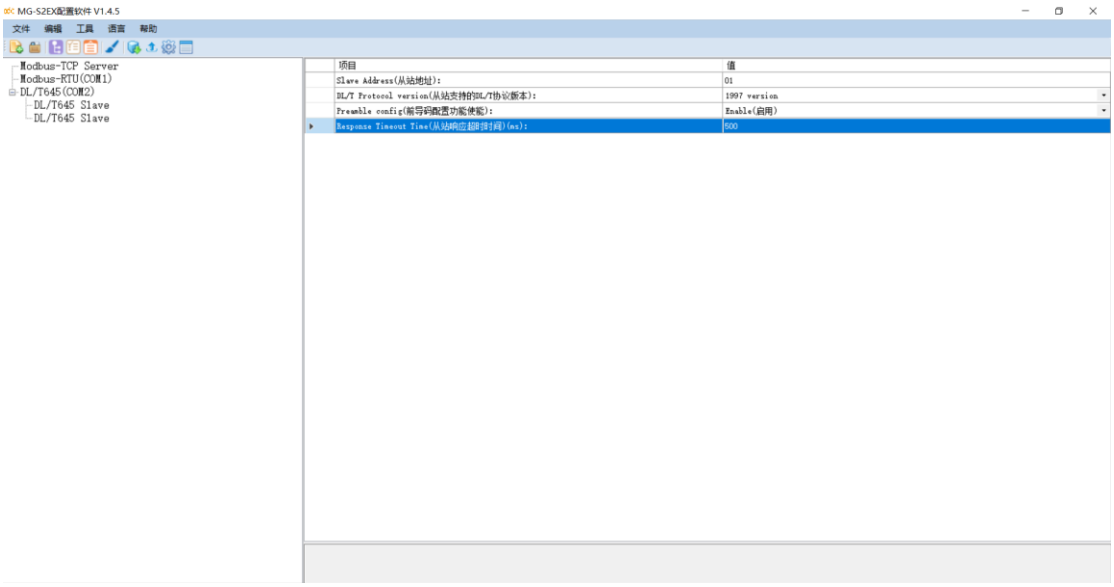
j. 单击工具栏“地址映射表按钮”，可显示 Modbus-TCP 各个缓存区网关映射地址使用情况，缓存区地址不能重叠。



k.选中串口2(COM2)，右键添加DL/T645从站，修改从站名称。设置电表1地址、选择支持的DL/T645协议版本、设置前导码配置功能(0：启用，1：禁止)、设置超时时间。

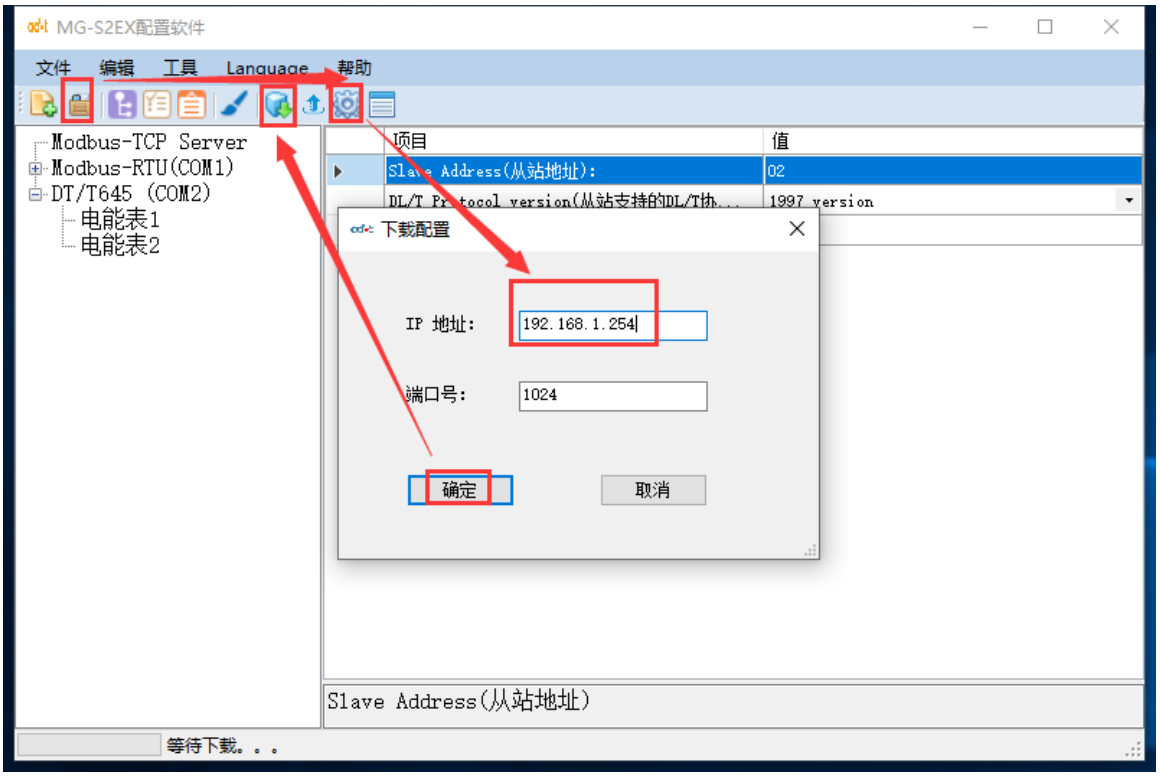


1.设置电表2地址、选择支持的DL/T645协议版本、设置前导码配置功能(0：启用；1：禁用）、设置超时时间。



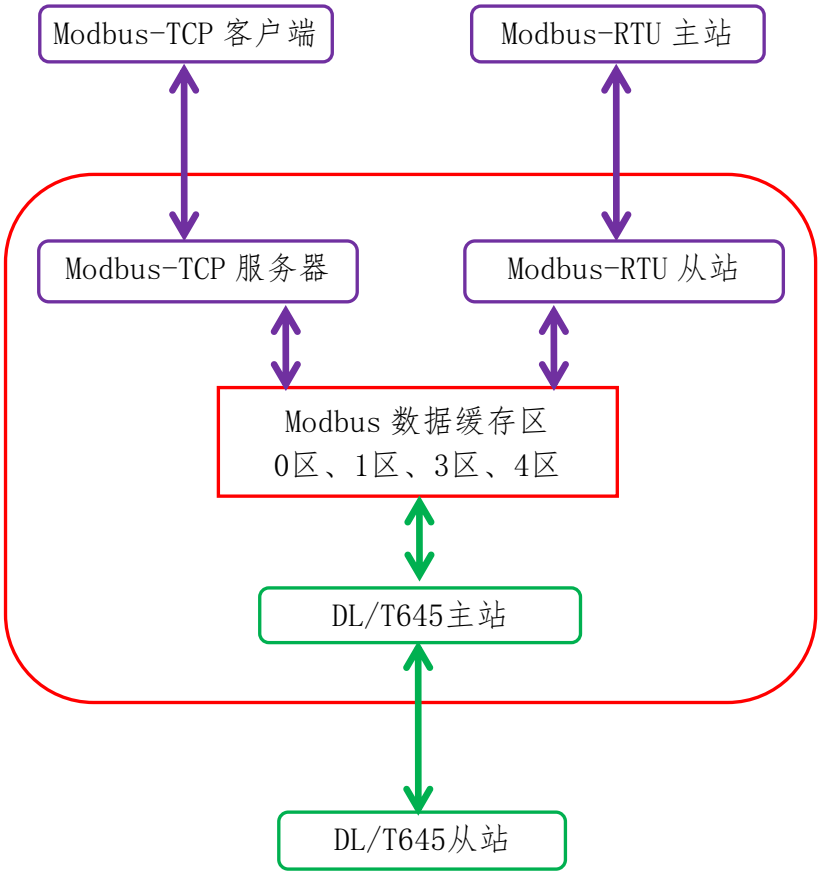
m. 双击电能表 1，弹出电能表数据采集选择框，电能表中读取的数据被映射到 Modbus-TCP 服务器的 3xxxx 存储区，每一个电能表数据被转换成 1 个浮点数，占用 3xxxx 区两个字空间。选择需要采集的数据项，填写 3xxxx 区映射地址，地址不能与串口 1 上所占用的地址重叠。单击“查看地址表”按钮，可实时查看被占用的映射地址区。同理，设置电能表 2 的数据采集项。MG-S2EX Config V1.4.5 版本新增 2007 协议数据采集项：瞬时 A 相视在功率、瞬时 B 相视在功率、瞬时 C 视在功率。

n. 单击工具栏“保存”按钮保存配置文件。单击工具栏“下载配置”按钮，设置当前 IP 地址及配置端口号。单击工具栏“下载”按钮下载配置参数。



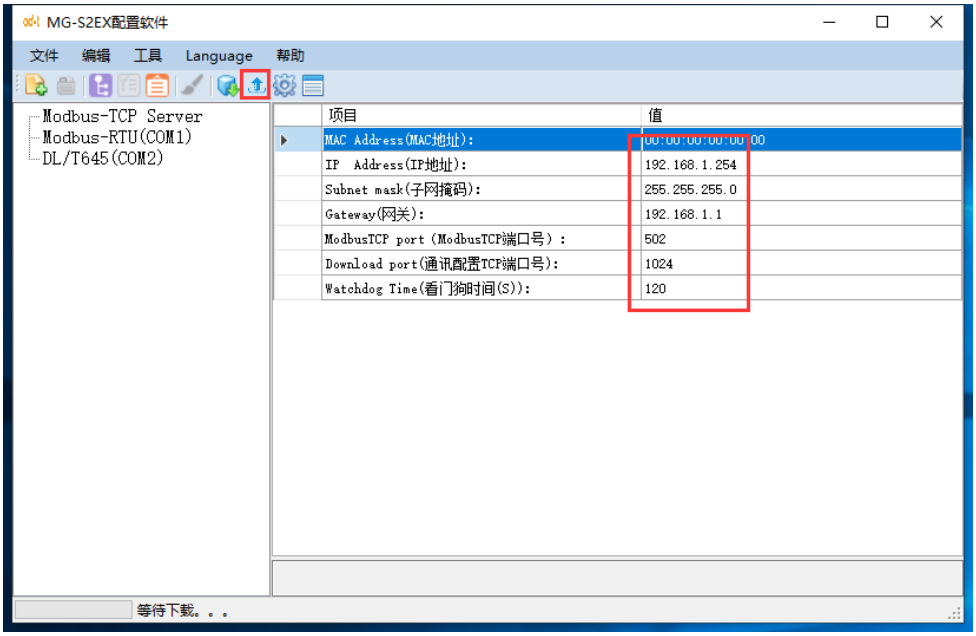
3.5.2 实现 Modbus TCP 客户端与 Modbus RTU 主站和电表的通讯配置

工作模式 2 时，串口 1 为 Modbus-RTU 从站，可连接标准 Modbus-RTU 主站设备。串口 2 为 DL/T645 主站，可连接支持该协议的电能表，DL/T645 支持 1997 和 2007 两个版本。DL/T645 主站读取到的数据存入网关 Modbus 存储区中，Modbus-RTU 从站和 Modbus-TCP 服务器共享 Modbus 存储区，存储区可同时被访问。其数据交换原理如下图所示。

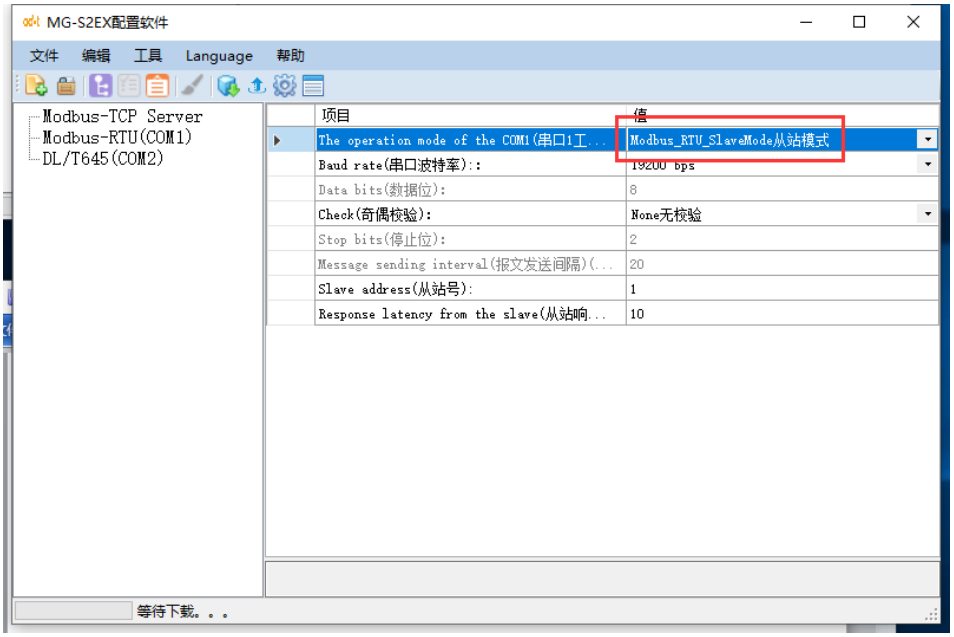


工作模式 2 的配置流程如下：

a. 打开配置软件，点击 可自动上传网关默认参数（注：默认 IP 地址是 192.168.1.254，若是不能上载请先 ping 一下 IP 地址或者按一下复位按钮）。

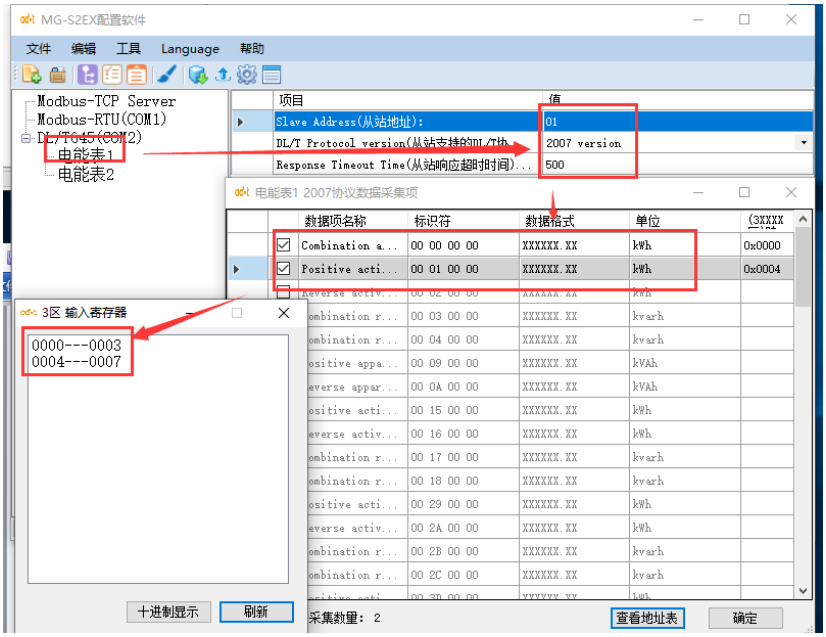


b. 设置 Modbus-RTU 从站参数，串口工作模式选“Modbus-RTU 从站模式”，设置波特率、校验位、从站号、从站响应延迟等参数。

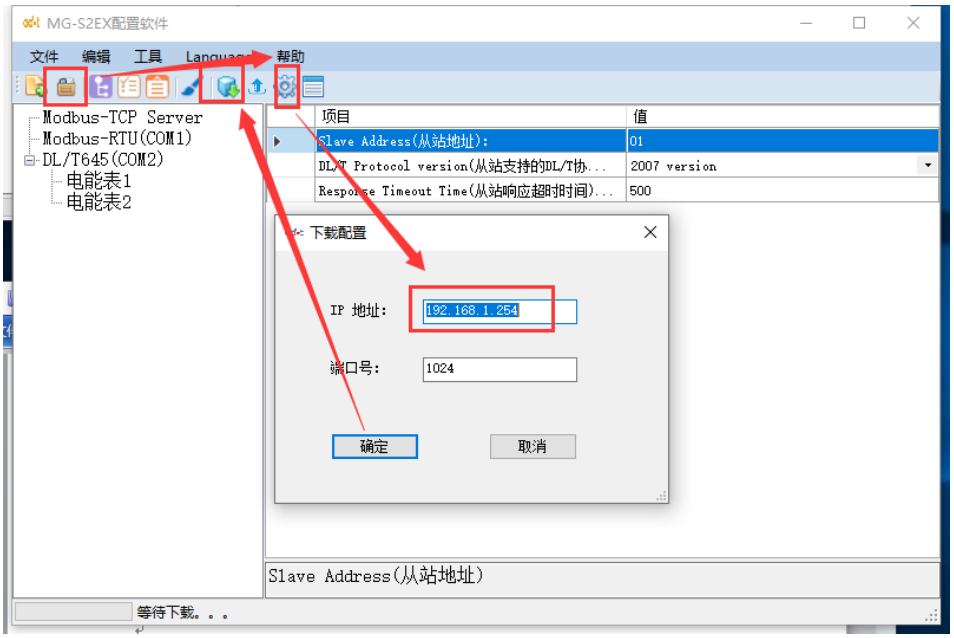


c. 在串口 2 上添加 DL/T645 从站、修改从站名称、设置前导码配置功能（0：启用；1：禁止）、设置从站地址，设置 DL/T 协议版本和超时时间。双击电能表，

设置数据采集项及映射地址，“确定”后保存返回。

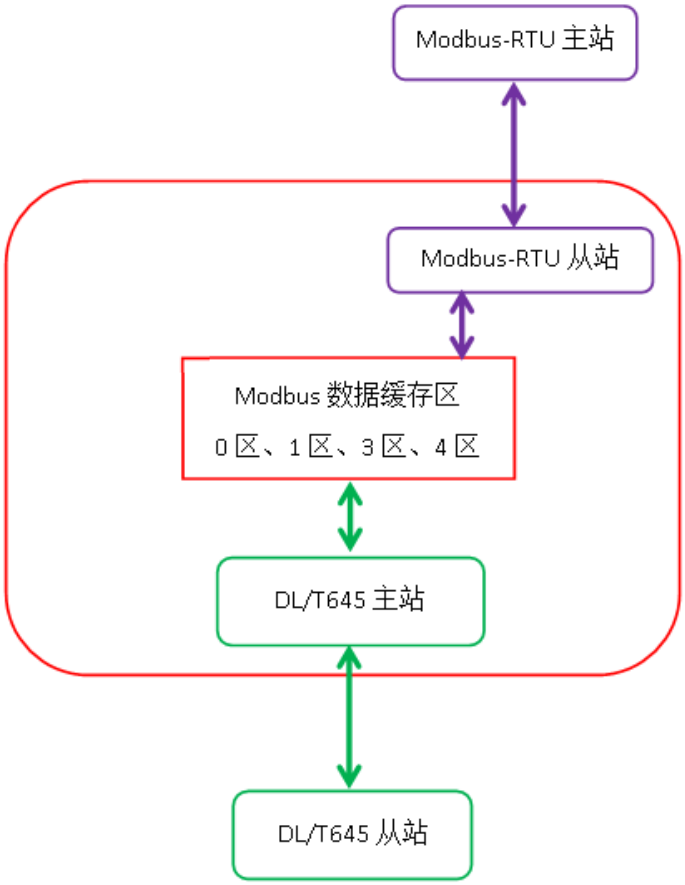


d. 单击工具栏“保存”按钮保存配置文件。单击工具栏“下载配置”按钮，设置当前 IP 地址及配置端口号。单击工具栏“下载”按钮下载配置参数。



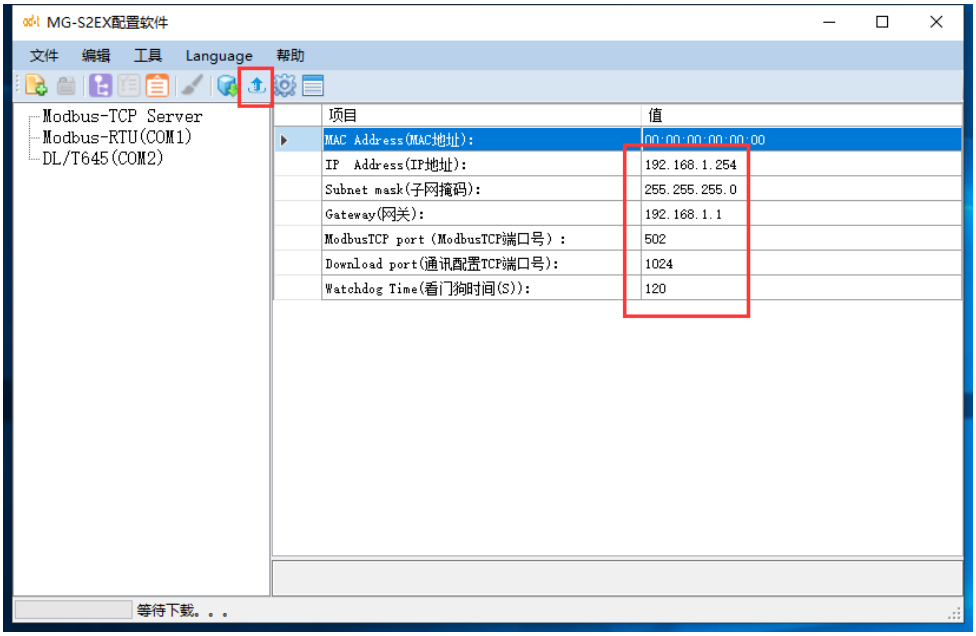
3.5.3 实现 Modbus RTU 主站与电表的通讯配置

工作模式 3 时，串口 1 为 Modbus-RTU 从站，可连接标准 Modbus-RTU 主站设备。串口 2 为 DL/T645 主站，可连接支持该协议的电能表，DL/T645 支持 1997 和 2007 两个版本。DL/T645 主站读取到的数据存入网关 Modbus 存储区中，Modbus-RTU 从站共享 Modbus 存储区，Modbus RTU 主站可访问 Modbus 存储区读写数据。

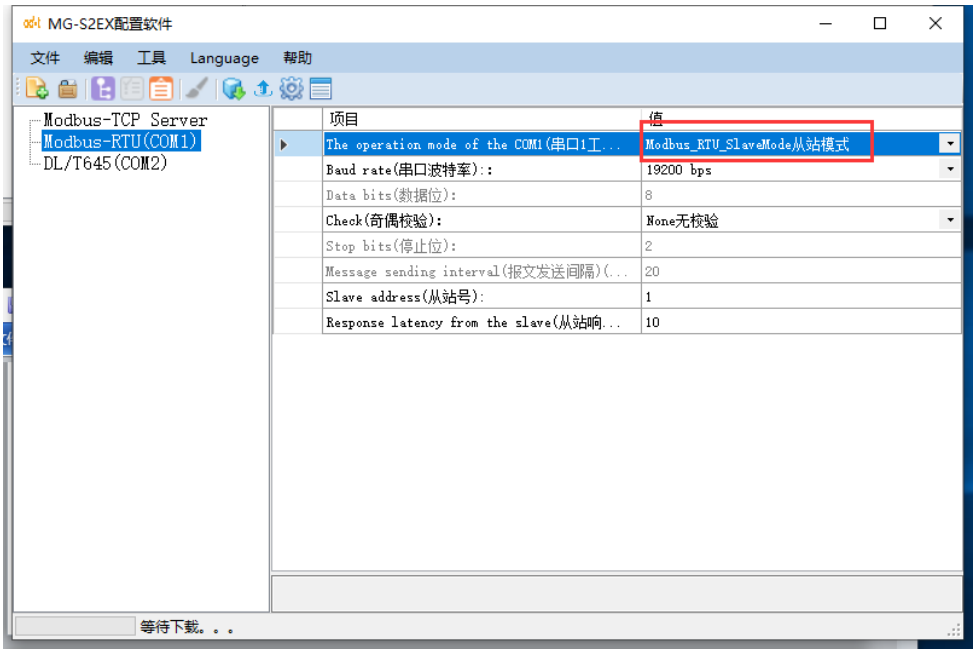


工作模式 3 的配置流程如下：

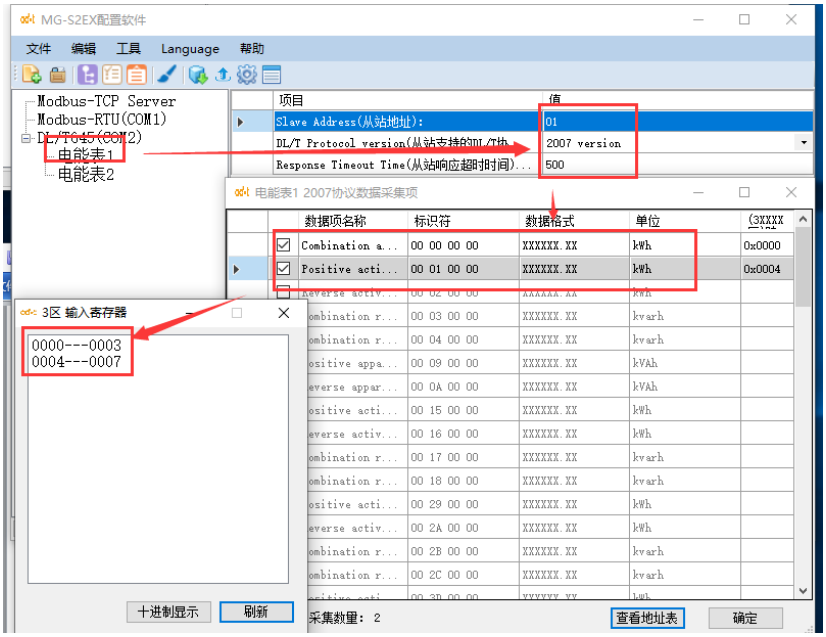
a. 打开配置软件，点击 可自动上传网关默认参数（注：默认 IP 地址是 192.168.1.254，若是不能上载请先 ping 一下 IP 地址或者按一下复位按钮）。



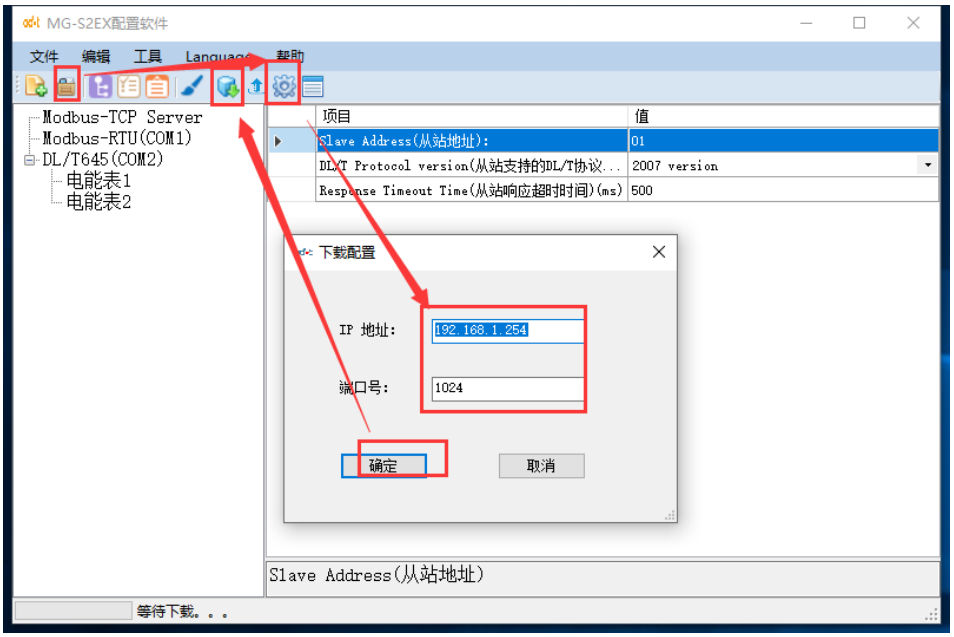
b. 设置 Modbus-RTU 从站参数，串口工作模式选“Modbus-RTU 从站模式”，设置波特率、校验位、从站号、从站响应延迟等参数。



c. 在串口 2 上添加 DL/T645 从站，修改从站名称，设置从站地址，设置前导码配置功能（0：启用，1：禁止），设置 DL/T 协议版本和超时时间。双击电能表，设置数据采集项及映射地址，“确定”后保存返回。



d. 单击工具栏“保存”按钮保存配置文件。单击工具栏“下载配置”按钮，设置当前 IP 地址及配置端口号。单击工具栏“下载”按钮下载配置参数。

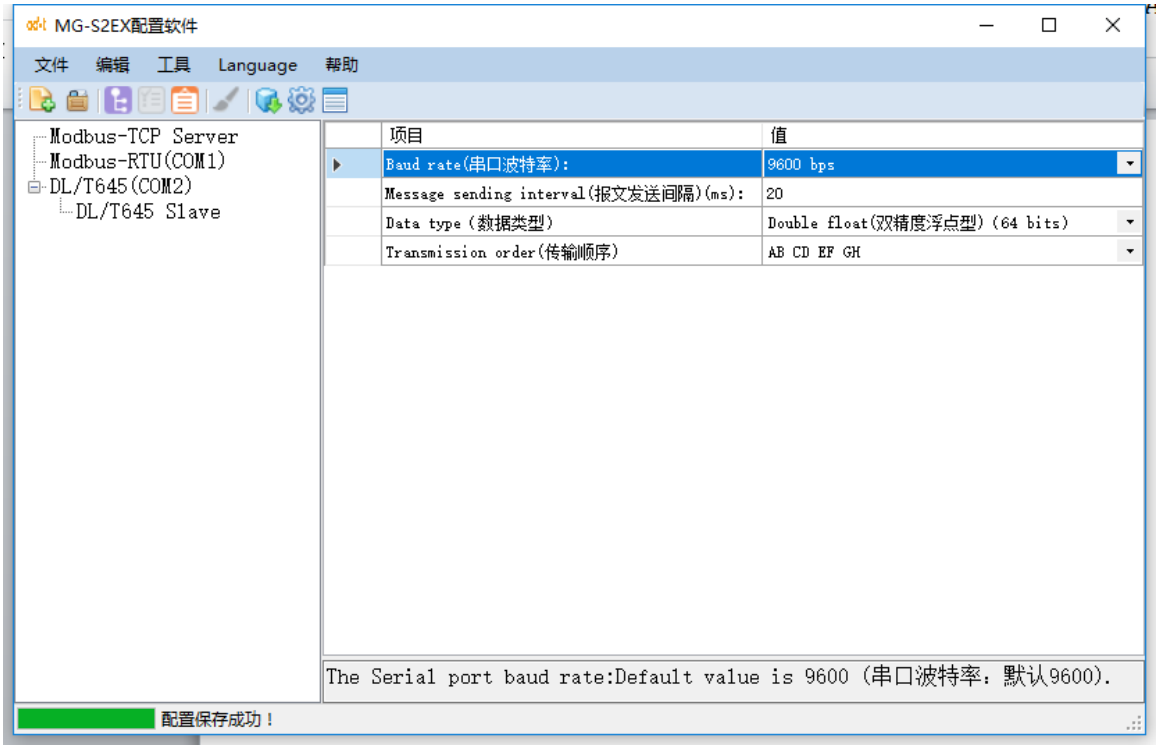


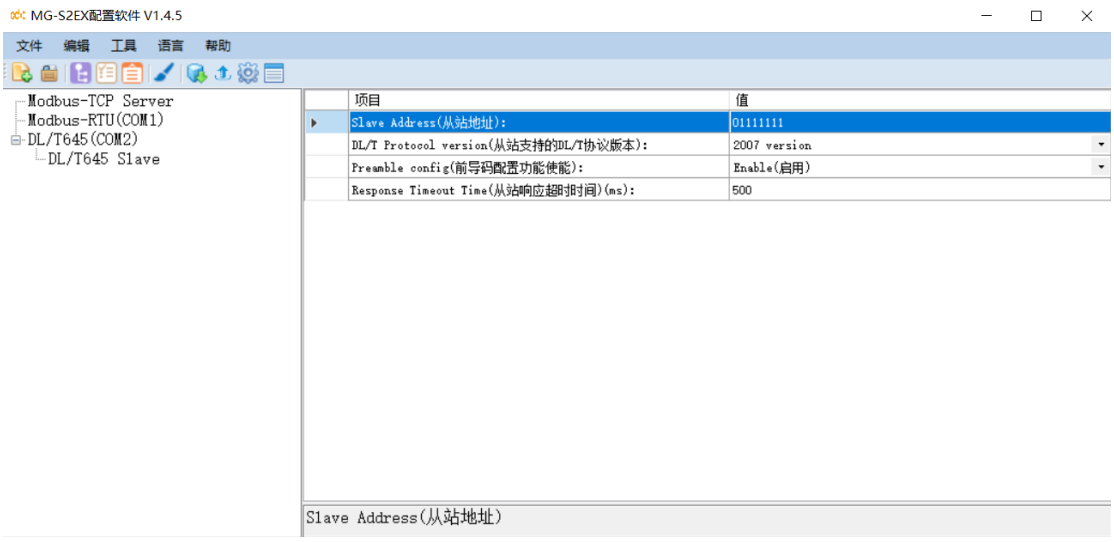
e. 这样就可以实现串口 1 读取串口 2 电表的数据。

四 在西门子 TIA V14 的测试应用

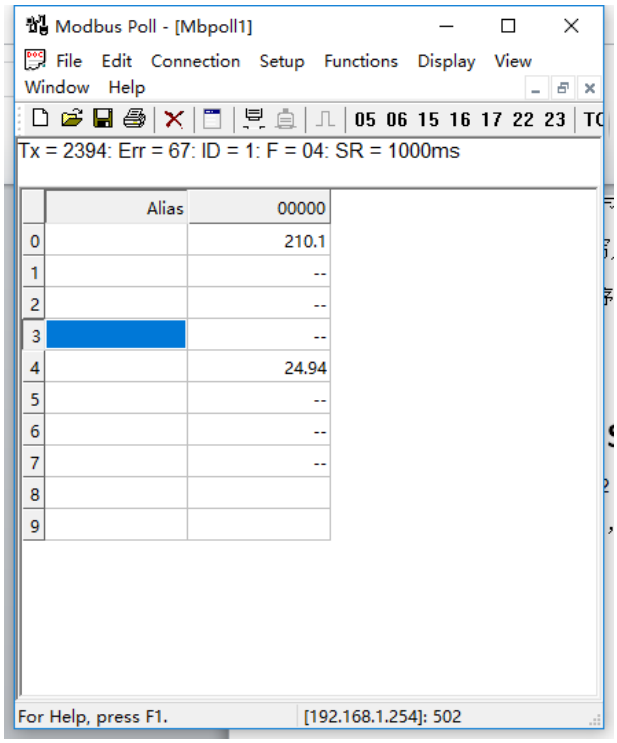
4.1 网关 MG-S2EX 的配置测试

A、网关工作模式采用地址映射模式，网关 IP 地址设置为：192.168.1.254，RS485 侧 COM2 口接安科瑞的电表，电表串口参数：电表 ID=01111111，9600、DL/T645 2007，前导码配置功能使能。



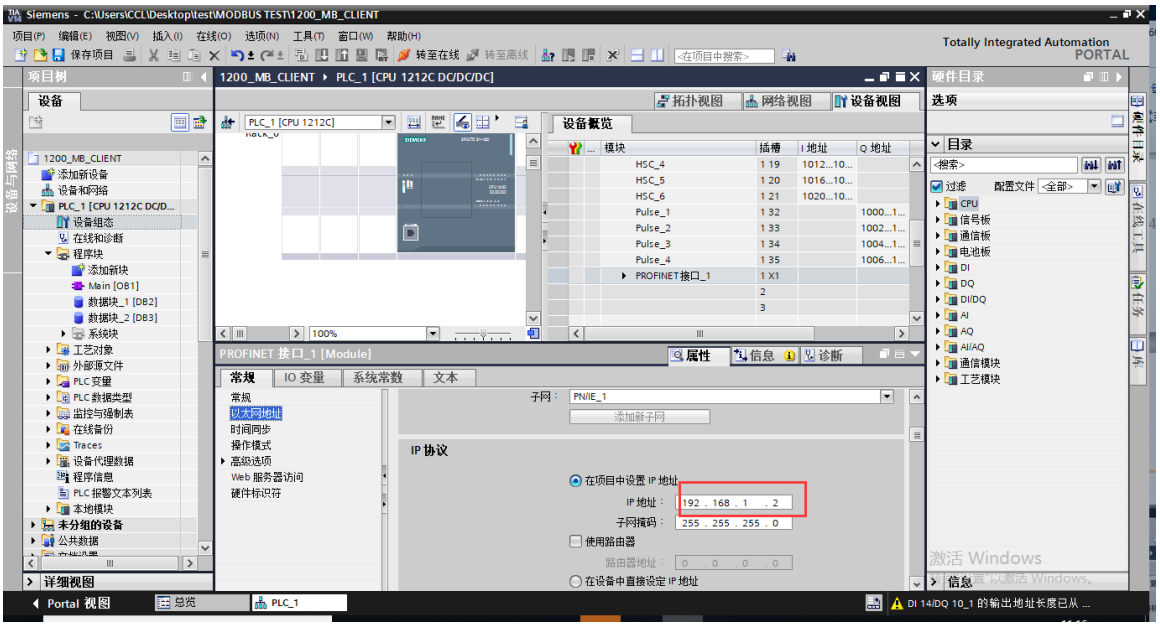


B、配置完成，点击下载，会在软件的左下角显示配置保存成功。可使用 Modbus Poll 软件以 Modbus TCP 的方式读取电表参数，见下图。



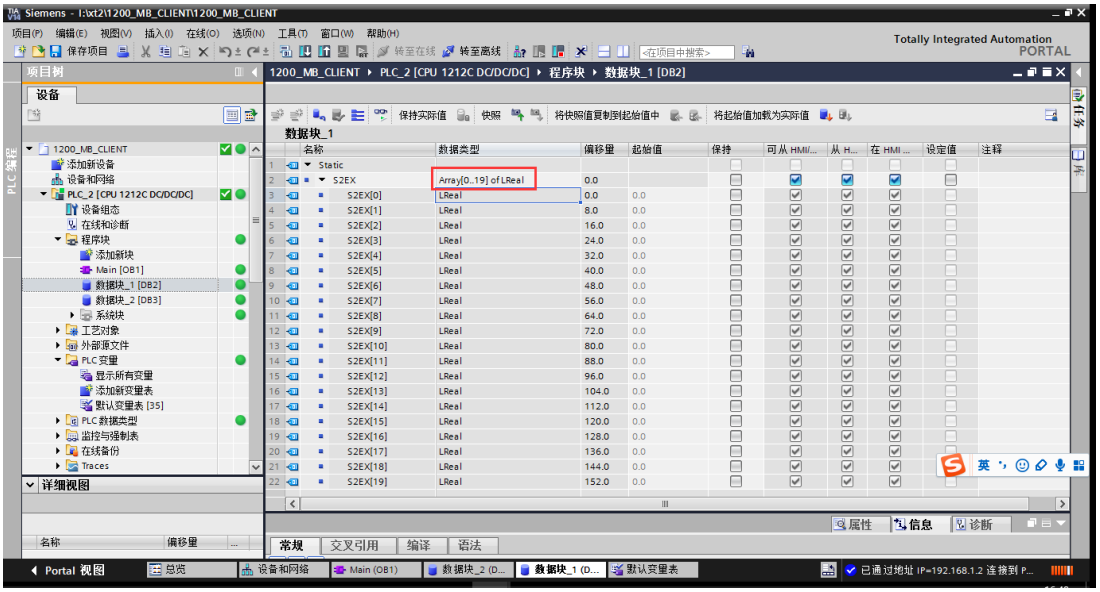
4.2 软件 TIA V14 的配置测试

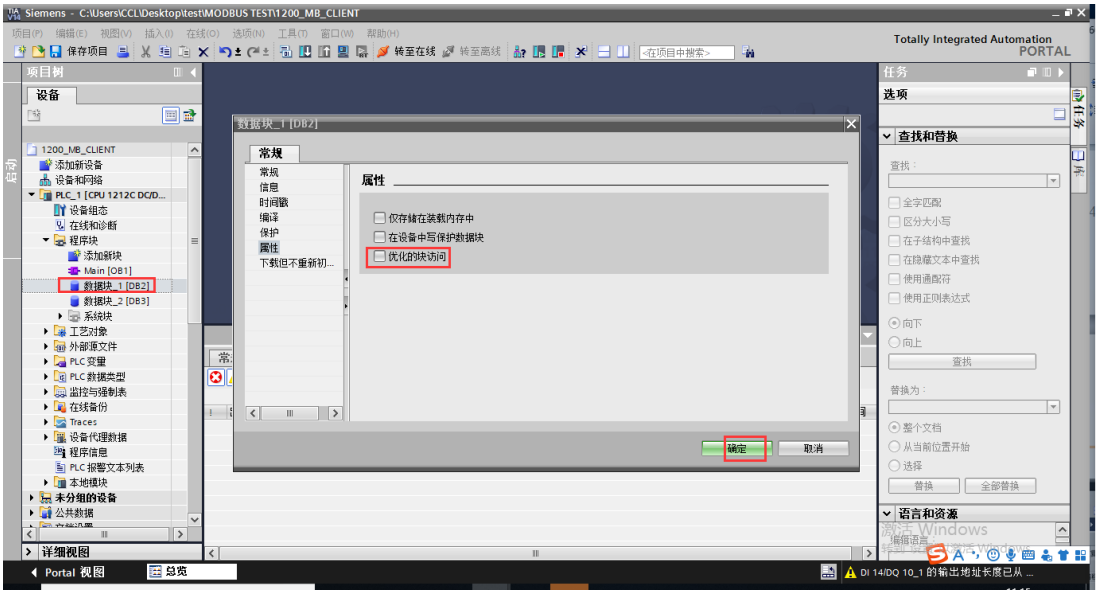
本文档测试采用 S7-1200PLC 作为主控制器。打开 TIA 软件，新建一个项目工程 1200-MB-CLIENT。添加新设备 S7-1212 DC/DC/DC。设置网口 IP 为：192.168.1.2。



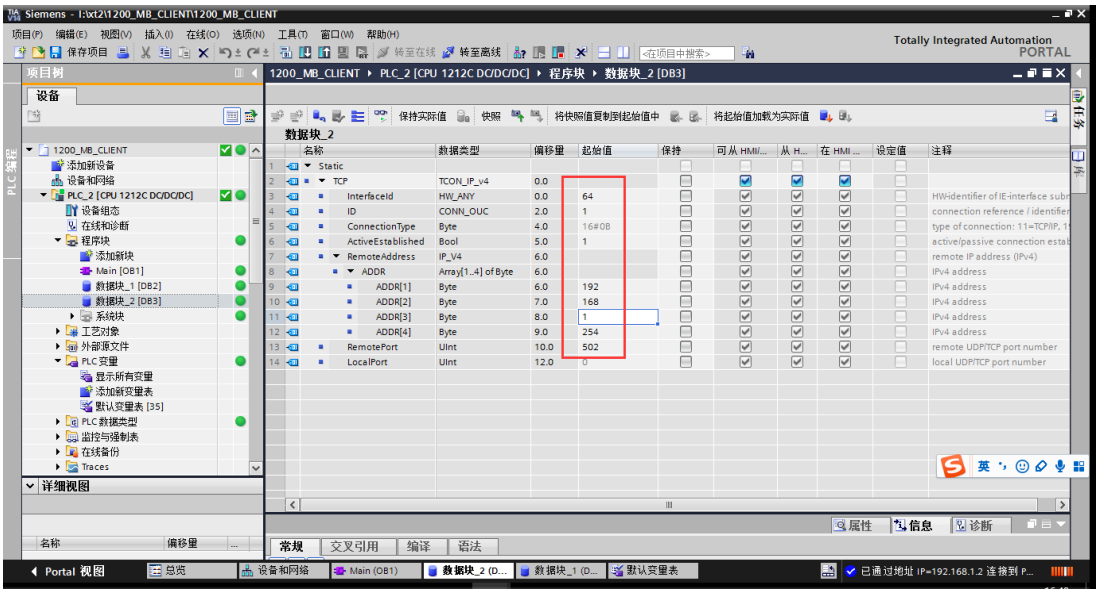
点击程序块，添加新块，建立数据块 DB2、DB3。

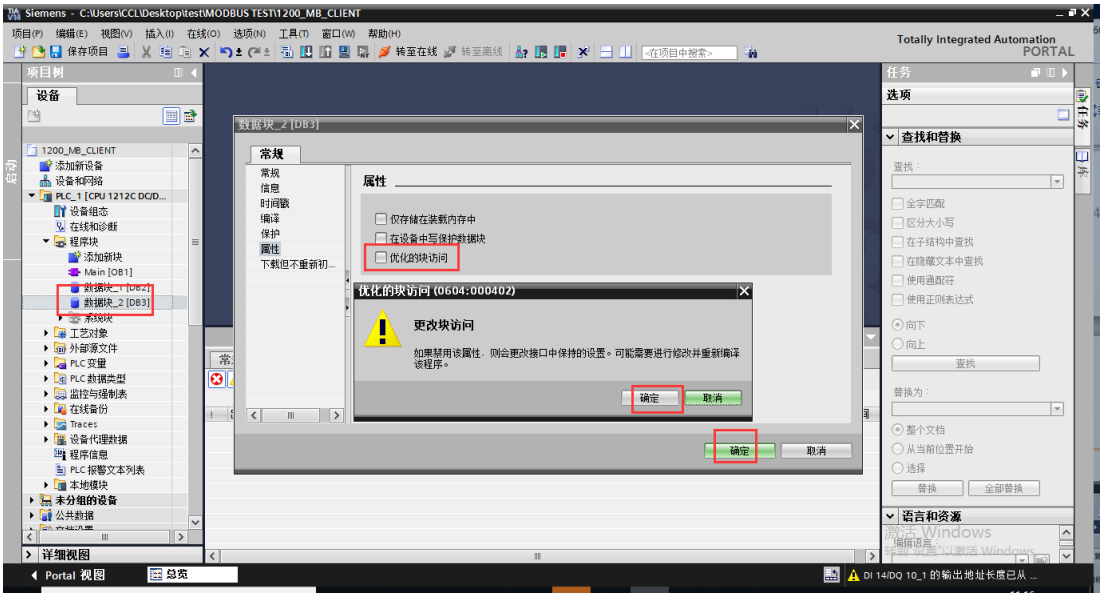
在 DB2 建立指向待从 Modbus 服务器接收数据的数据缓冲区，修改 DB2 属性里，去掉优化的数据块前面的√。选中 DB2，保存编译。



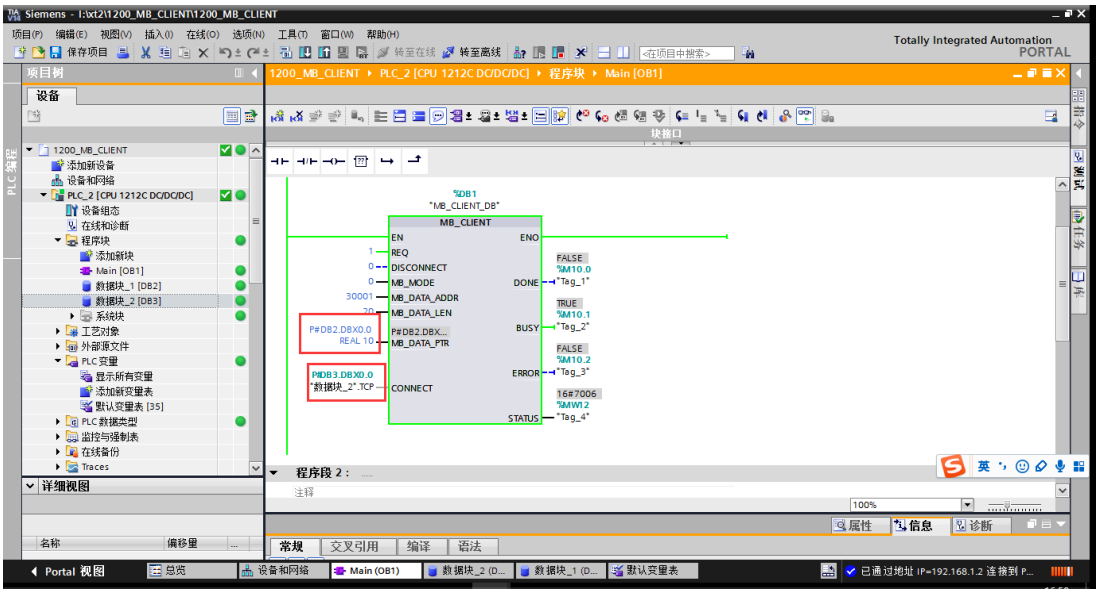


在 DB3 建立指定连接所需的所有地址参数。所填 IP 地址为网关的 IP 地址。修改 DB3 属性里，去掉优化的数据块前面的√。选中 DB3，保存编译。

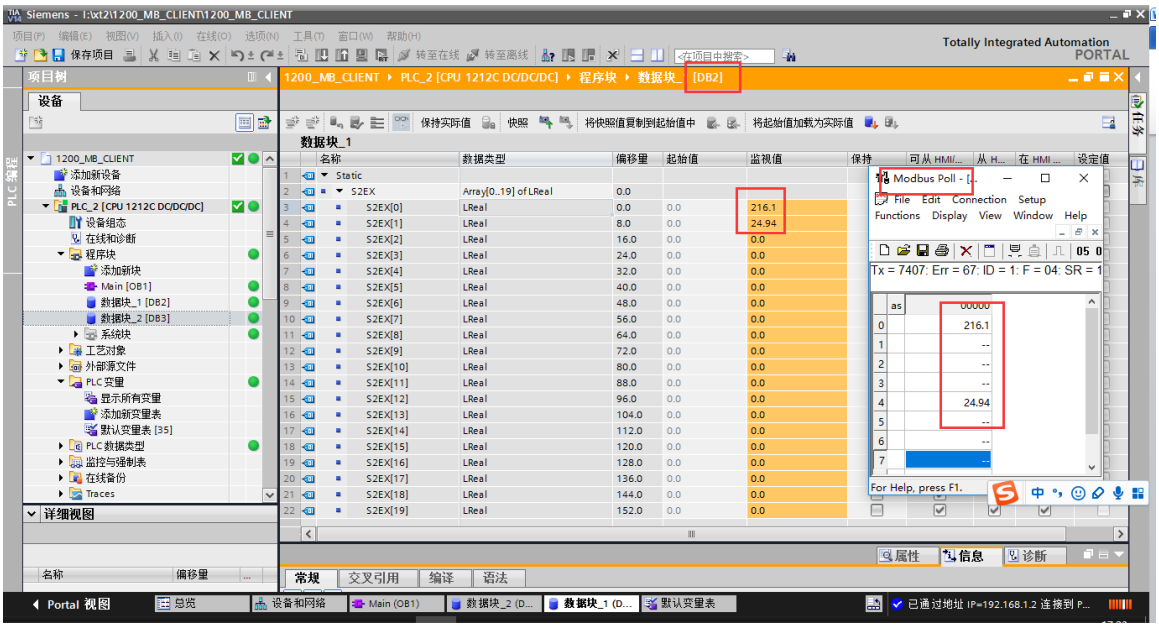




双击主程序块 Main[OB1]，在弹出的界面编程**调用功能块 MB-CLIENT。**通过查看帮助文档修改各个参数，使得功能块正常运行。



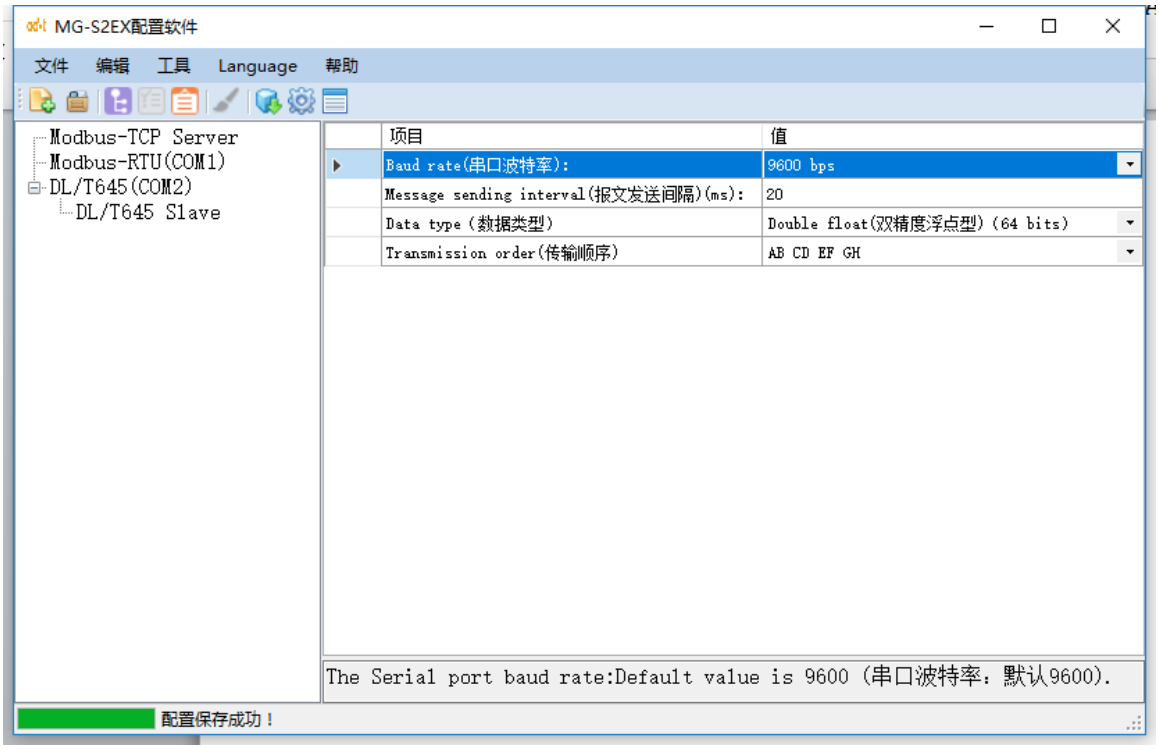
配置好后，保存编译下载，可在 DB2 里直接监视到电表数据。

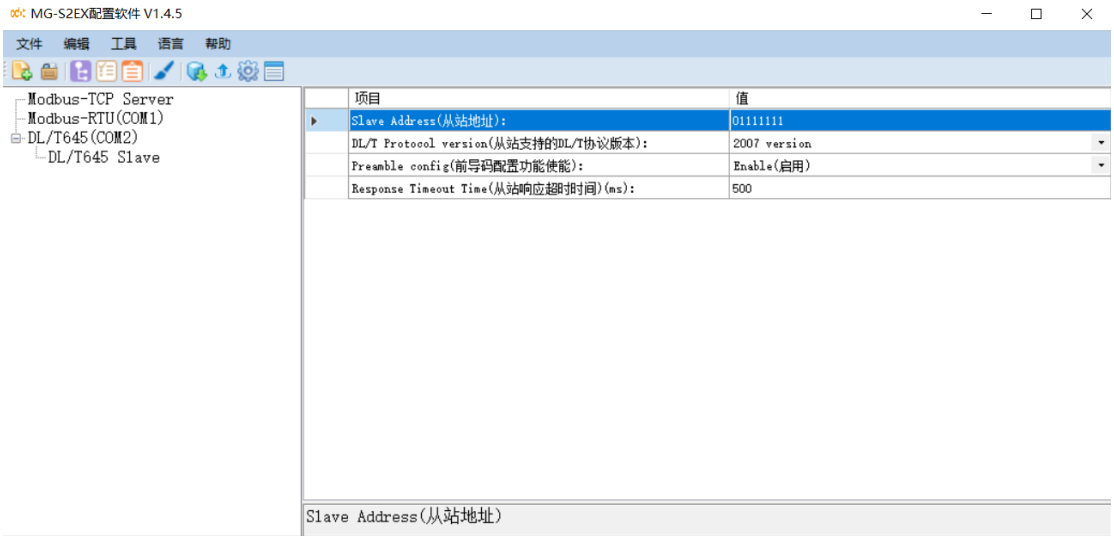


五、在上位机组态王 V6.55 的测试应用

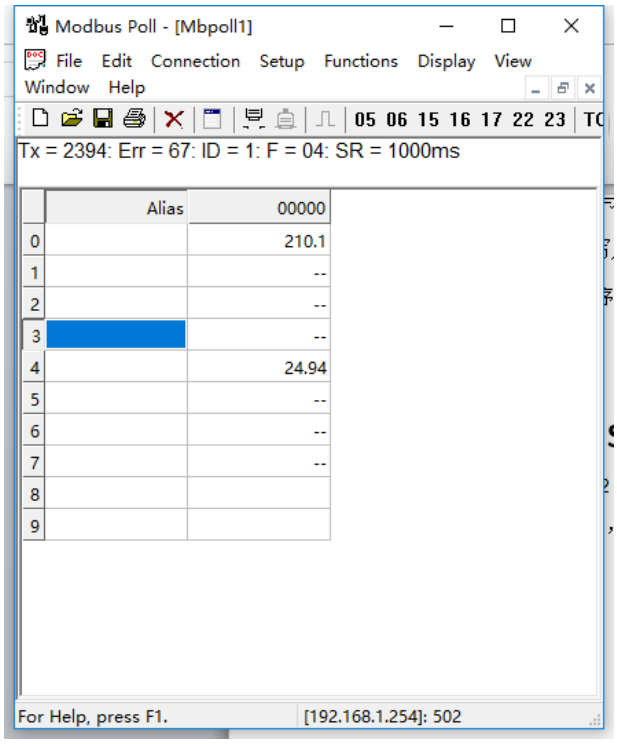
5.1 网关 MG-S2EX 的配置

A、网关工作模式采用地址映射模式，网关 IP 地址设置为：192.168.1.254，RS485 侧 COM2 口接安科瑞的电表，电表串口参数：电表 ID=01111111，9600、DL/T645 2007，前导码配置功能使能。



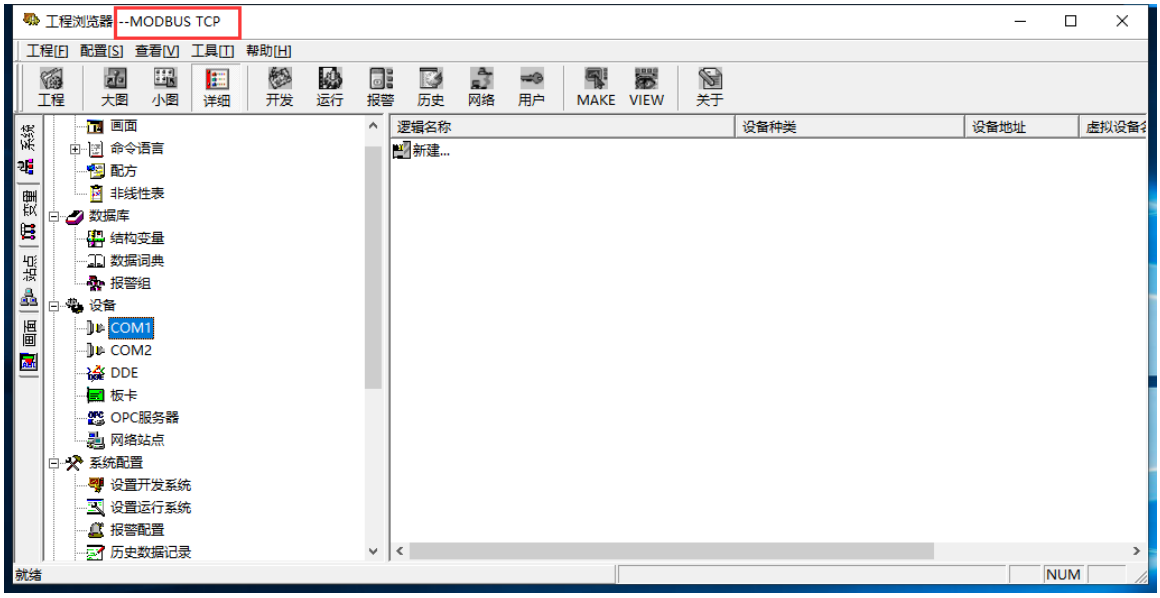


B、配置完成，点击下载，会在软件的左下角显示配置保存成功。可使用 Modbus Poll 软件以 Modbus TCP 的方式读取电表参数，见下图。

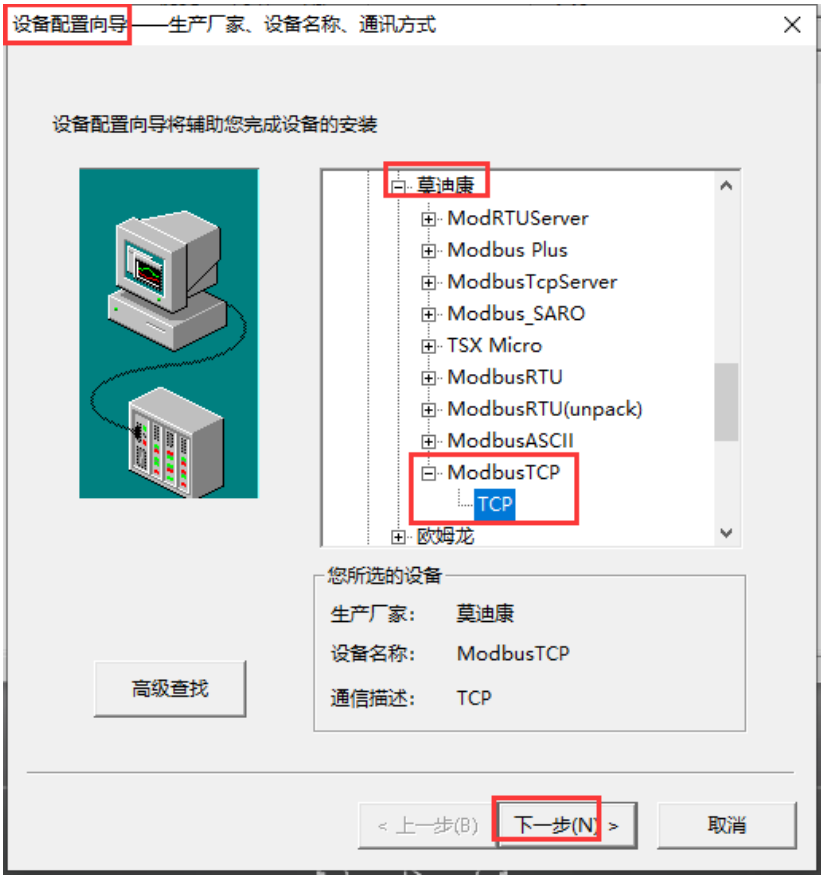


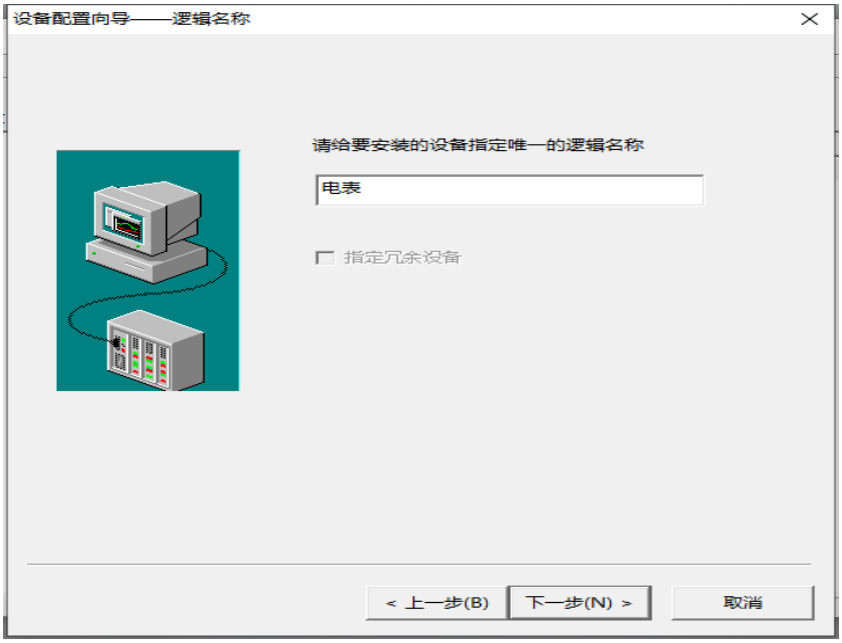
5.2 上位机组态王的配置测试

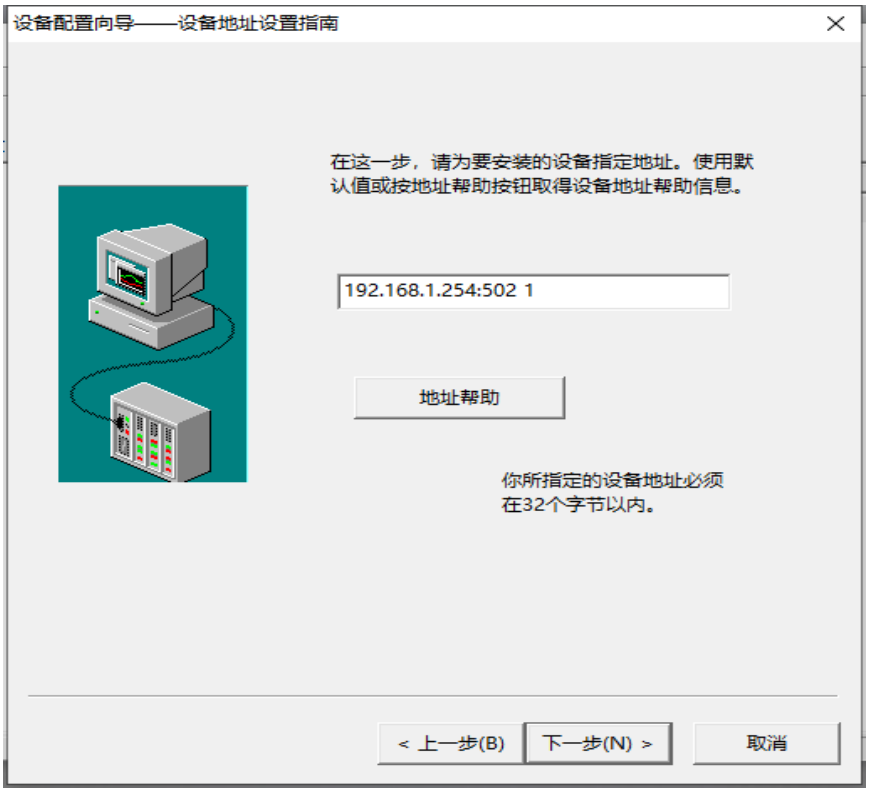
打开组态王 V6.55 软件，新建工程 MODBUS TCP，双击进入工程浏览器。



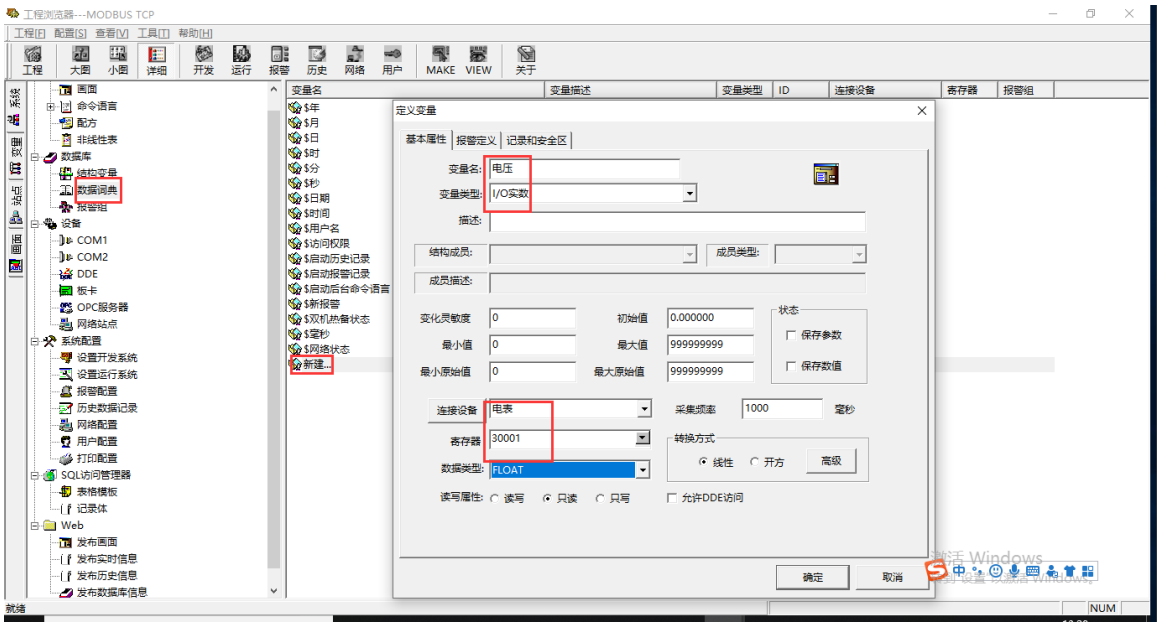
点击设备，双击右侧新建设备配置向导，点击 PLC—莫迪康—Modbus TCP—TCP，点击下一步，给要采集数的设备命名‘电表’。点击下一步——下一步，填写网关的 IP 地址：192.168.1.254:502 1(可点击地址帮助填写地址),点击下一步直到完成配置。



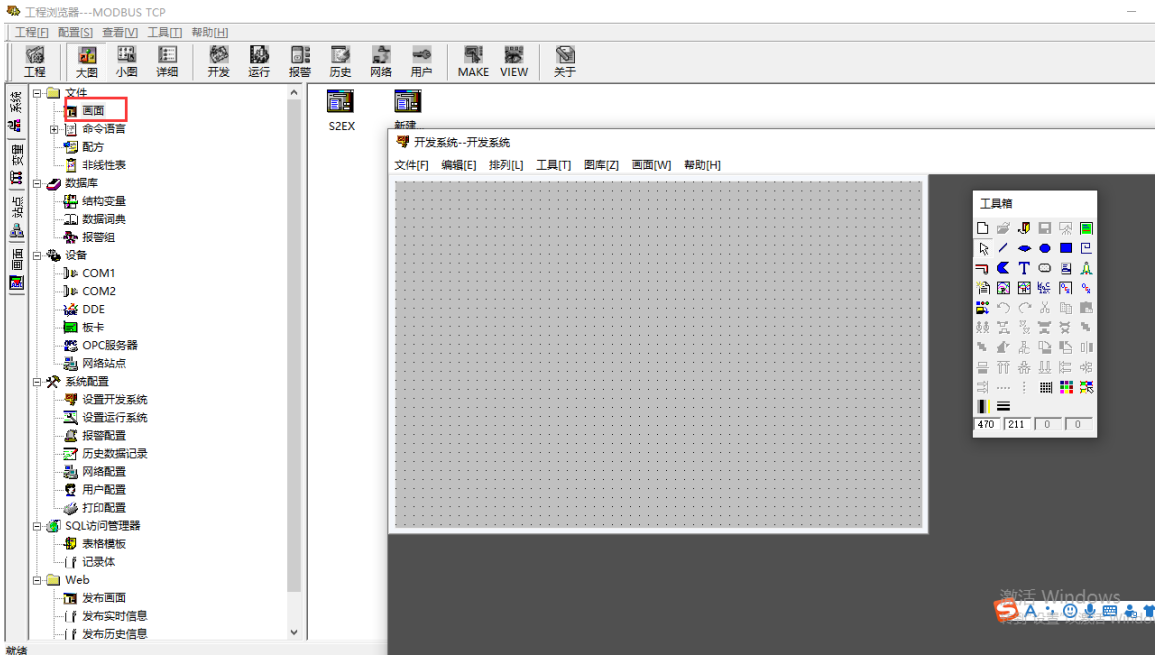




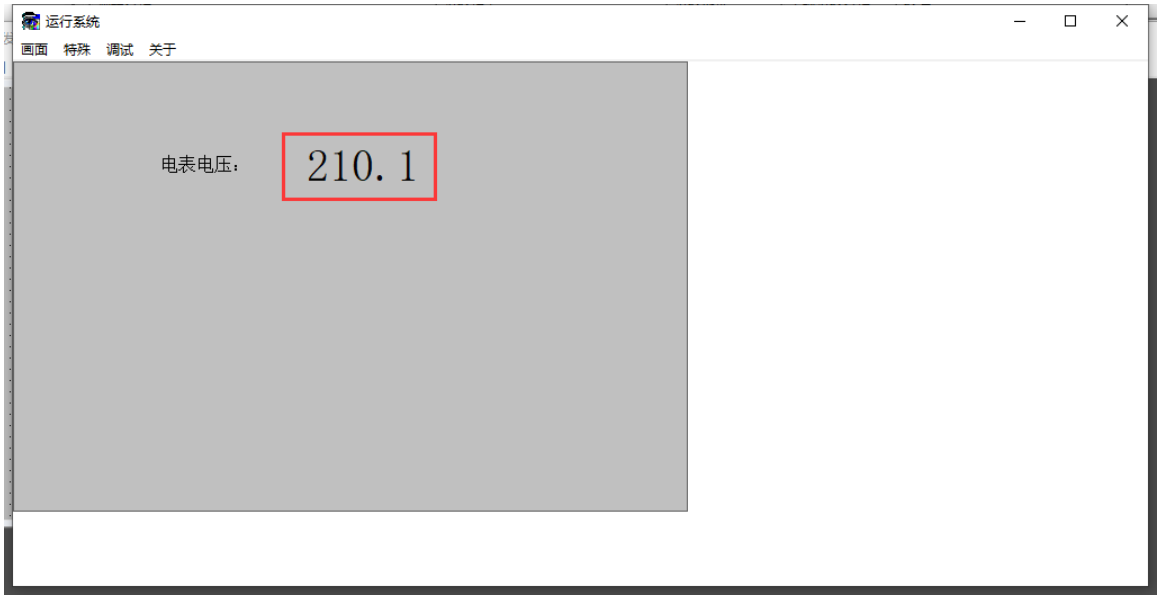
点击数据库下的数据词典，点击新建变量



点击画面，新建画面 S2EX，建立变量电表电压。画面编辑完成后保存。



点击文件，切换到 View,在运行系统，打开刚才建立的画面。可以监控到电表的数据。

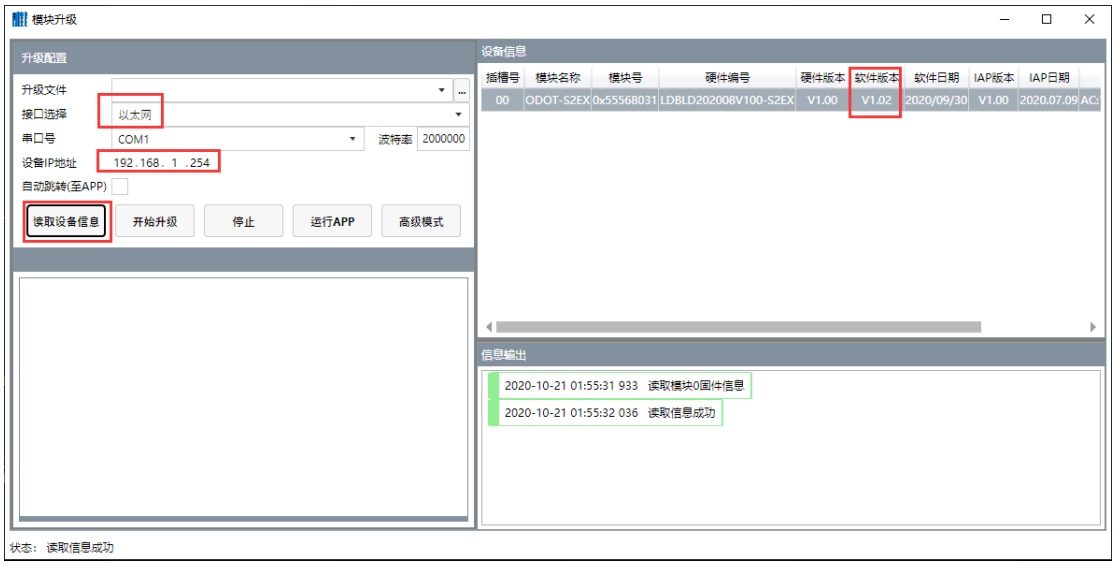


六、 固件升级

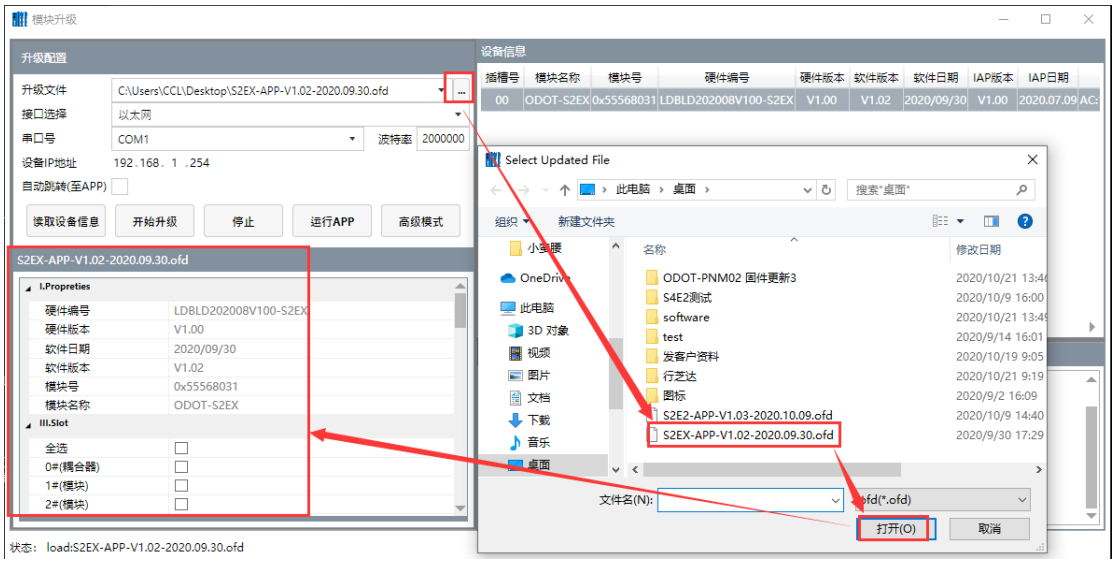
当模块固件更新时，需要给网关固件升级，网关可以通过网口升级。给网关供电 24Vdc 电源，本机网卡 IP 地址和网关在同一网段（网关出厂默认地址是 192.168.1.254）。用一根网线连接电脑和网关。

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。

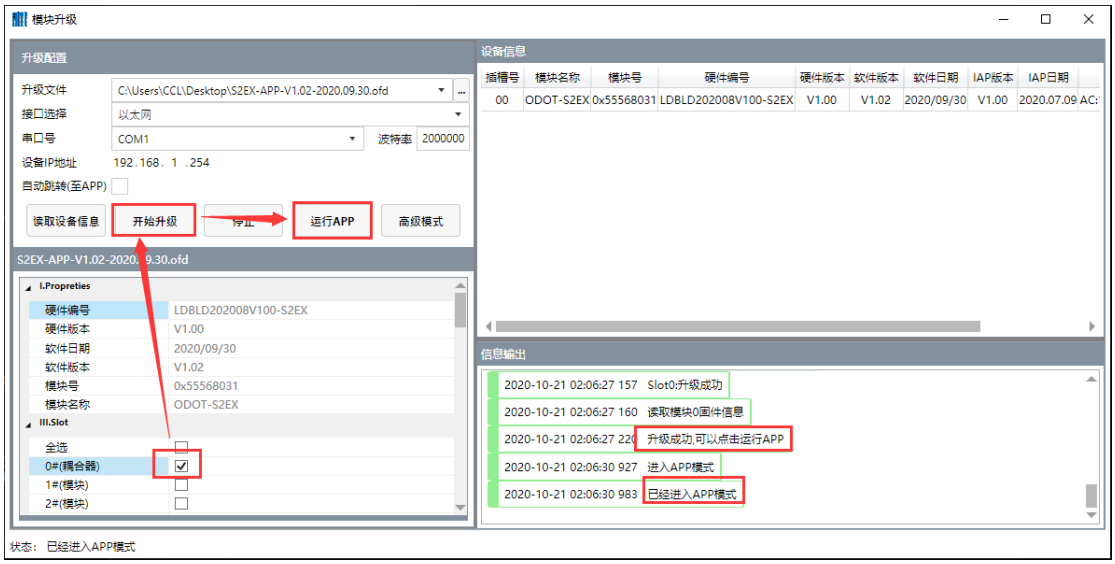


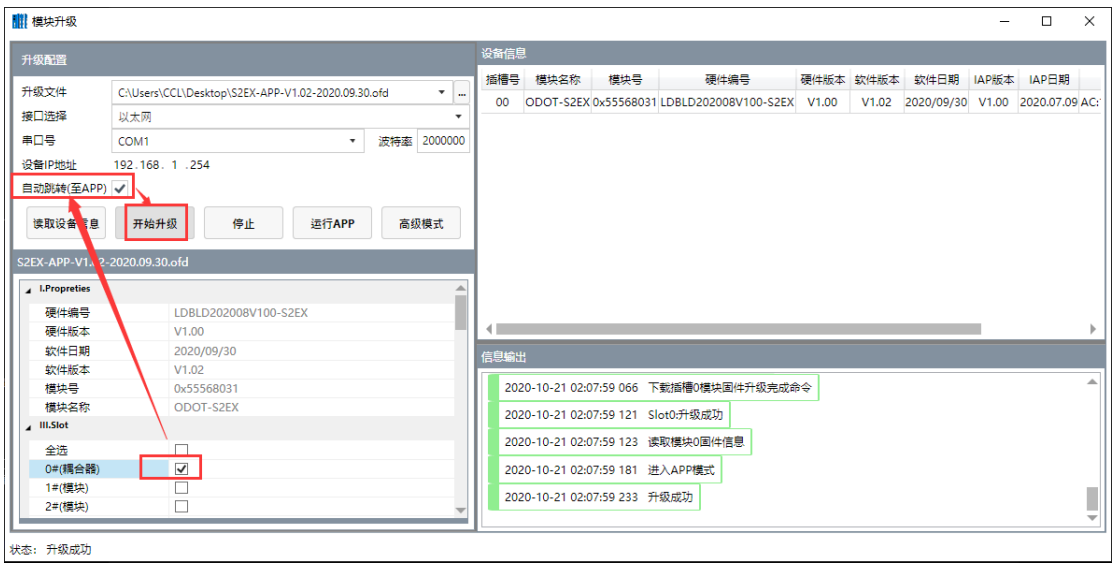
点击 ，在弹出的界面，选择新的固件文件，点击打开，会在左下角显示新固件信息。



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。





七、 附录

7.1 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)。

7.1.1 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

7.1.2 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	xxxx

功能：预置从站多个保持寄存器值4XXXX。

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

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

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

应答格式：

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

7.2 串口网络拓扑结构简介

7.2.1 RS232

RS232 是工业控制的串行通信接口之一，它被广泛用于计算机串行接口与外设连接。RS232 使用一根信号线和一根信号返回线构成共地的传输形式，采用三线制的接线方式，可以实现**全双工**通讯，传输信号为单端信号，这种共地传输容易产生共模干扰，所以抗噪声干扰性弱，传输距离有限，RS232 接口标准规定在码元畸变小于 4%的情况下最大传输距离标准值为 50 英尺（**约为 15 米**）（15m 以上的长距离通信，需要采用调制调解器），最大传输距离还与通讯波特率有关，在实际运用过程中，如果传输距离较远，请降低波特率。为减小信号在传输过程中受到外界的电磁干扰，请使用**屏蔽电缆**作为通讯电缆。

RS232 接口标准规定了在 TXD 和 RXD 上：

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

RS232 接口分类：

DB9 公头接口

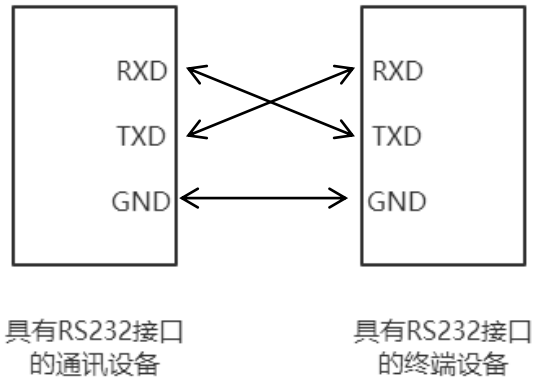
左上角为 1，右下角为 9

9 针 RS232 串口（DB9）		
引脚	名称	作用
1	CD	载波检测
2	RXD	接收数据
3	TXD	发送数据
4	DTR	数据终端准备好

5	GND	信号地线
6	DSR	数据准备好
7	RTS	请求发送
8	CTS	清除发送
9	RI	振铃提示

由于 RS232 接口具有上述电气特性，所以其只能实现**点对点通讯**。

RS232通讯接线示意图如图所示：



7.2.2 RS422

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

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

RS-422 需要接终端电阻，要求其阻值约等于传输电缆的特性阻抗。在短距

离传输时可不需终接电阻，即一般在 300 米以下不需终接电阻。终接电阻接在传输电缆的最远端。

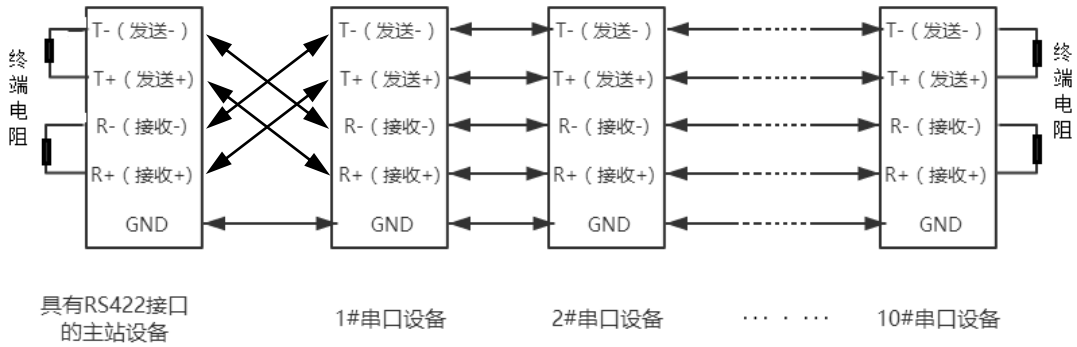
在进行一主多从组网连接时，**所有从站**的**发送端**通过**菊花链**的方式连接最后接入主站的**接收端**；所有从站的**接收端**通过**菊花链**的方式连接最后接入主站的**发送端**。

RS422 引脚定义：

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

左上角为 1，右下角为 9

RS422通讯接线示意图如图所示：



7.2.3 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接电阻等。RS-485 可以采用二线与四线方式，二线制可实现真正的多点双向通信。

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

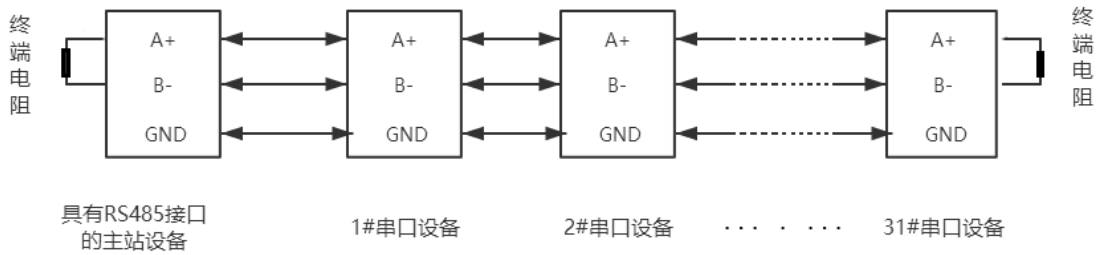
RS485 信号**传输距离**与通讯波特率有关，波特率越高，传输距离越短，在波特率不高于 **100KbpS** 的情况下，理论最大通信距离约为 **1200 米**，在实际运用过程中，由于电磁干扰等因素，往往达不到最大通信距离，如果进行较远距离通讯，请**降低波特率**，为降低信号在传输过程中受到外界电磁干扰，请使用**双绞屏蔽电缆**作为通讯电缆。

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

RS485 9 针引脚定义：

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

RS485通讯接线示意图如图所示：



四川零点自动化系统有限公司

地址：四川省绵阳市飞云大道 261 号综合保税区 204 厂房

电话：0816-2530577

传真：0816-6337503

邮编：621000

网址：www.odot.cn

零点微信公众号