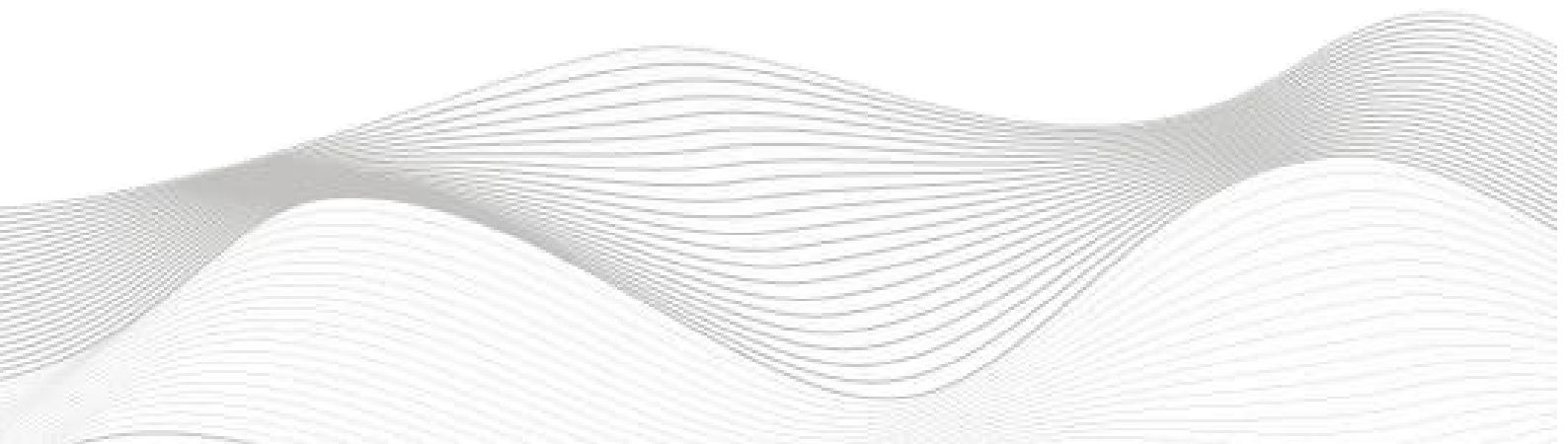




# 技术笔记

## SRX-MT与西门子S7-1200的连接 应用

关键词：MODBUS TCP/IP ， S7-1200， SRX-MT



# 修订记录

变更内容:	
2023-01-18 创建本文档。	
编制: 刘小锋	审核:
2023 年 1 月 18 日	2023 年 1 月 18 日

## 目录

SRX-MT与西门子S7-1200的连接 .....	1
1. SRX-MT原理概述 .....	4
2. 调试环境 .....	4
3. 技术实现 .....	4
3.1 硬件连接 .....	4
3.2 模块参数及IP地址配置 .....	5
3.2.1 LAEConfig软件界面介绍 .....	5
3.2.2 扫描网络中的硬件 .....	5
3.2.3 修改模块的IP地址 .....	6
3.2.4 修改模块的参数 .....	6
3.2.5 下载模块的参数 .....	7
3.3 示例工程建立 .....	7
3.3.1 新建工程打开 TIA Portal 软件， 选择“创建新项目” .....	8
3.3.2 CPU的添加与连接 .....	8
3.3.3 在主程序中调用MB_CLIENT指令 .....	10
3.2.4 添加2个全局数据块，数据类型TCON_IP_v4 .....	11
3.2.5 MB_MODE、MB_DATA_ADDR、MB_DATA_LEN、 Modbus TCP 功能码等之间的关系 .....	12
3.2.6 程序编写 .....	12
3.4 程序编译下载 .....	14

举例说明：西门子S7-1200，模块1：SRX-1616-MT16点数字量输入，16点数字量输出；模块2：SRX-0808-MT，8点数字量输入，8点数字量输出。

## 1. SRX-MT原理概述

S7-1200PLC可以通过Modbus-TCP通信连接SRX-MT远程IO模块，通过在博图软件中设置并编程，即可通过简易连接进行远程IO控制。

模块：SRX-3200-MT\*1；SRX-0032P-MT\*1

功能码：本例演示30001(读输入寄存器)，40001(写多个保持寄存器)

## 2. 调试环境

- 博途 TIA Portal V14 及以上版本
- LA-config软件

## 3. 技术实现

### 3.1 硬件连接

1. 正确连接 S7-1200PLC 与远程 IO 模块电源。
2. 将测试对象 PLC 的RJ45接口，通过专用以太网电缆接入到远程 IO 模块的以太网口上。



### 3.2 模块参数及IP地址配置


#### 3.2.1 LAEConfig软件界面介绍

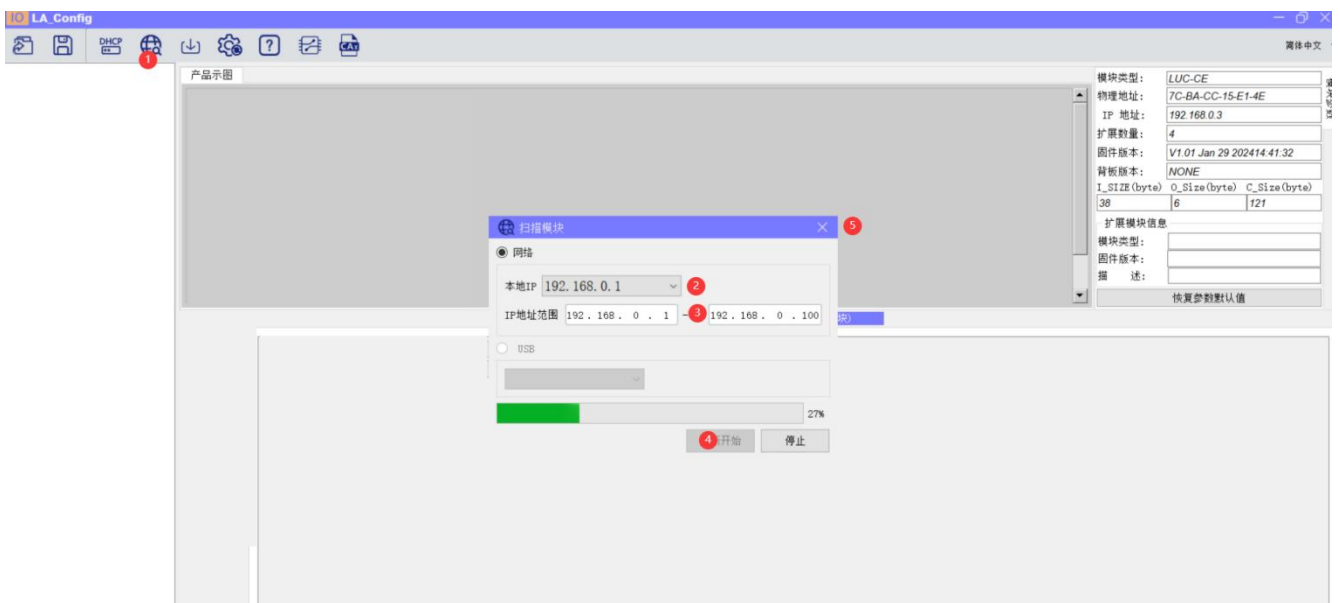


本软件界面包含了：工具栏，模块信息树形目录，参数设定区，模块信息显示区等等。




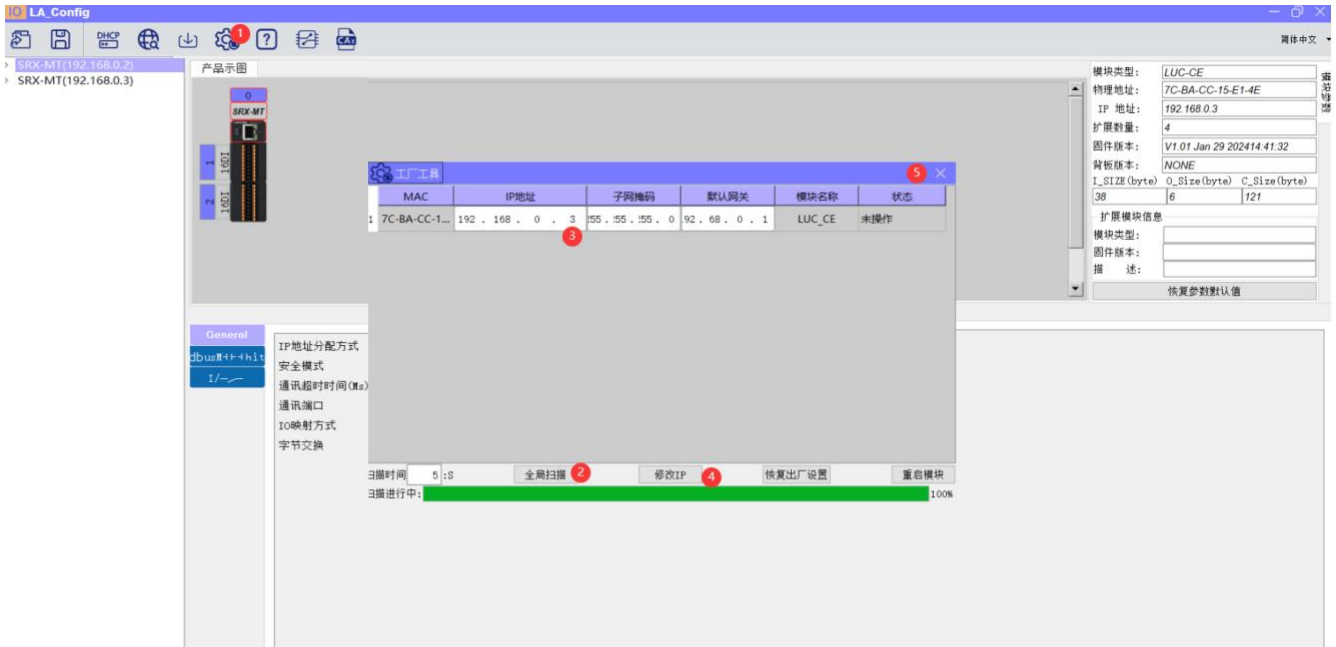
#### 3.2.2 扫描网络中的硬件

点击  扫描模块按钮，设置需要扫描的IP地址范围（在显示区中），并且是**电脑的网络IP参数要与设置的在同一网段内**。点击“开始”进入扫描阶段。就会在设置的IP范围内，把扫描上来的模块显示出来。



### 3.2.3 修改模块的IP地址

点击工具栏中的  按钮，点击全局扫描，选中IP地址进行修改，点击修改IP地址。进入分配IP地址的过程，分配是否成功可以在后面的状态列中显示出来。




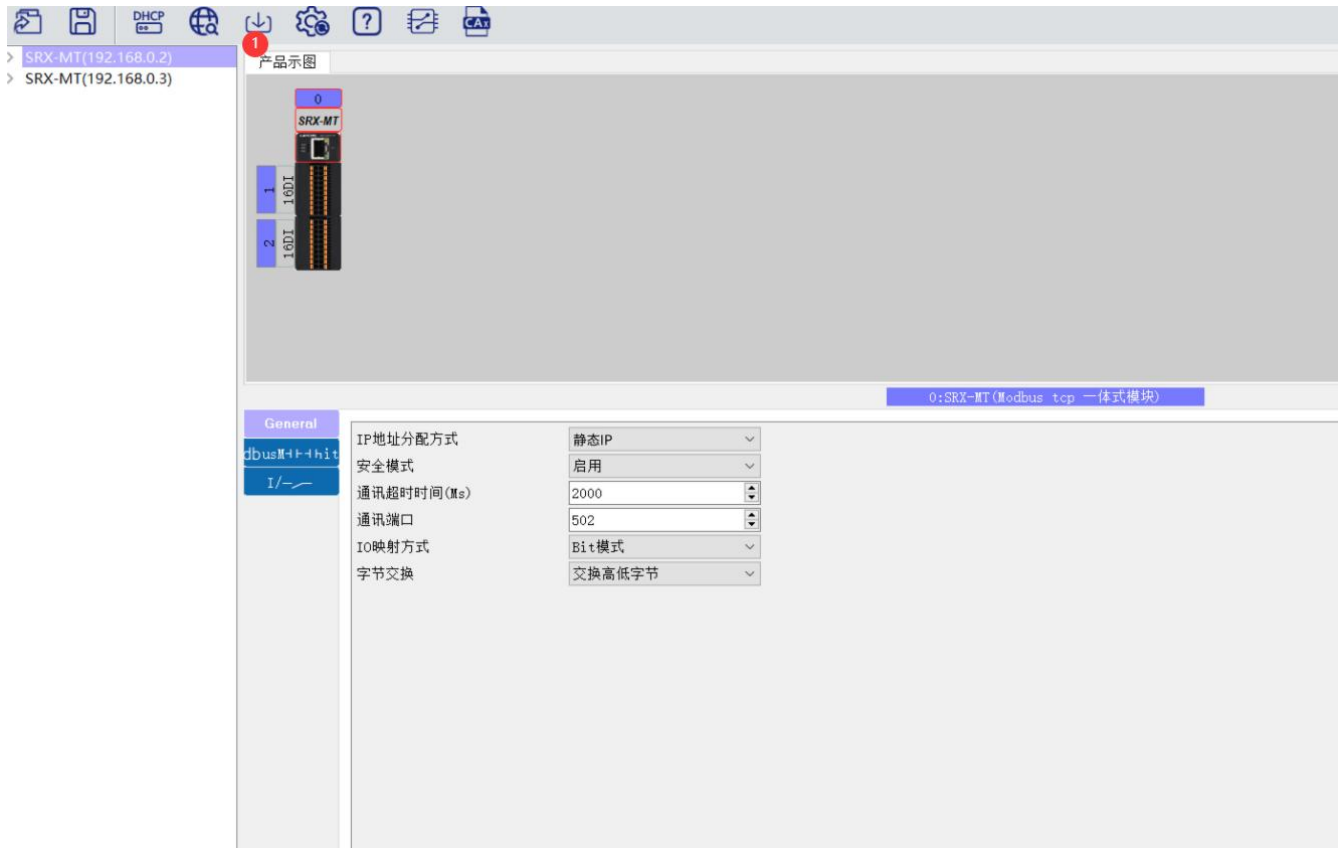
### 3.2.4 修改模块的参数

修改耦合器LUC-MT参数：单击SRX-MT模块，点击静态IP, 安全模式启用，通讯端口502, IO映射方式为REG模式。



### 3.2.5 下载模块的参数

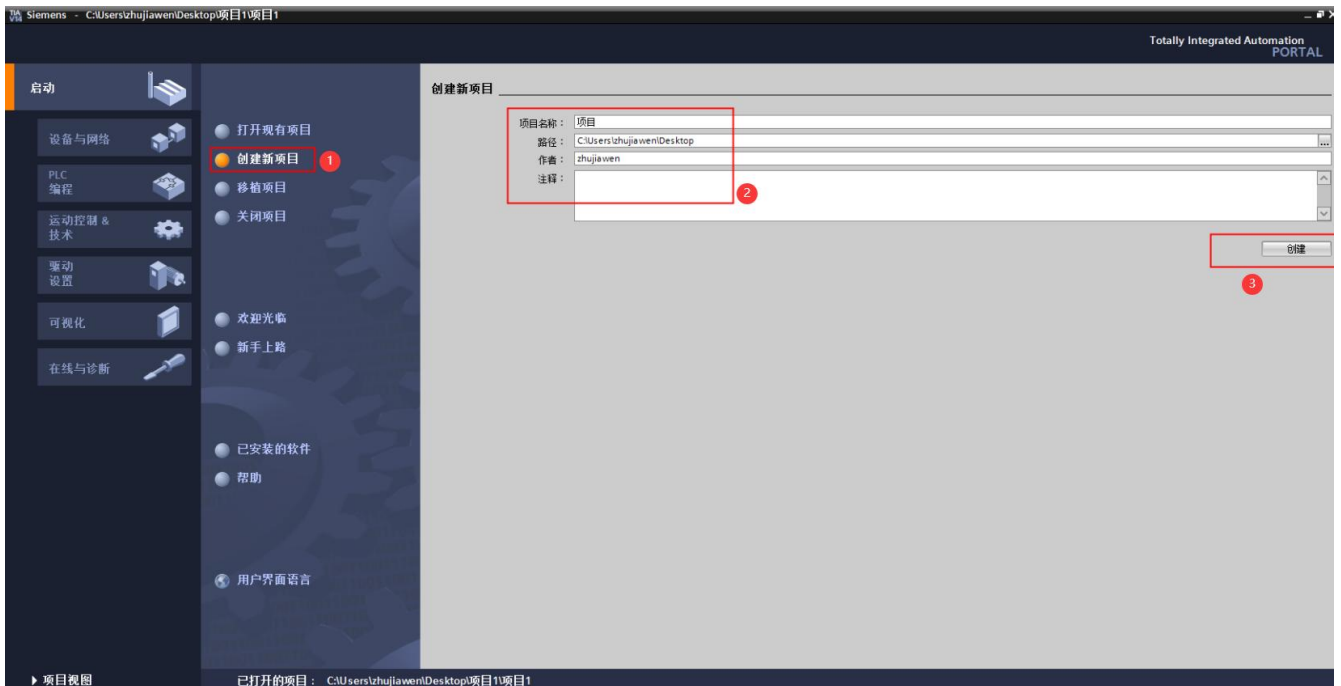
在参数设定区设定模块参数。设置完成之后点击  可以下载模块参数。



### 3.3 示例工程建立

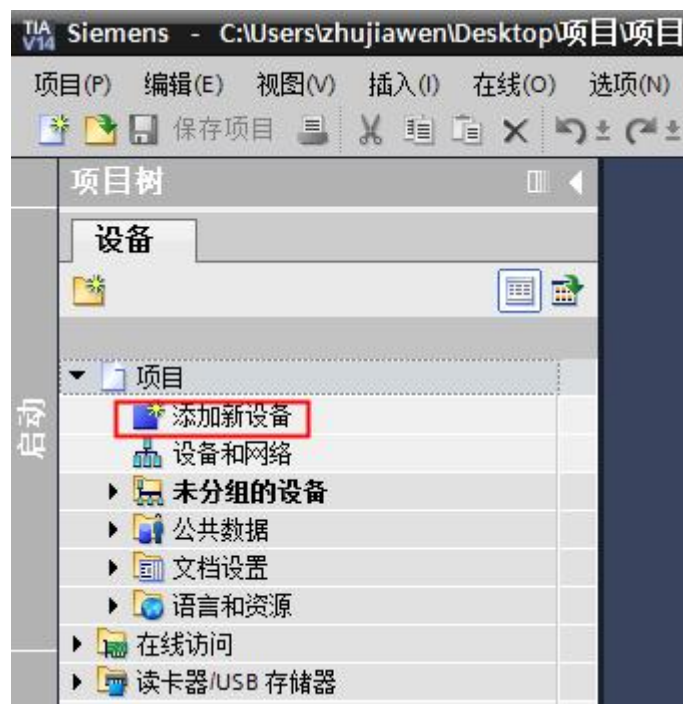
### 3.3.1 新建工程打开 TIA Portal 软件， 选择“创建新项目”

并填写项目名称、 路径、 版本、 作者等相关信息， 点击创建即可：



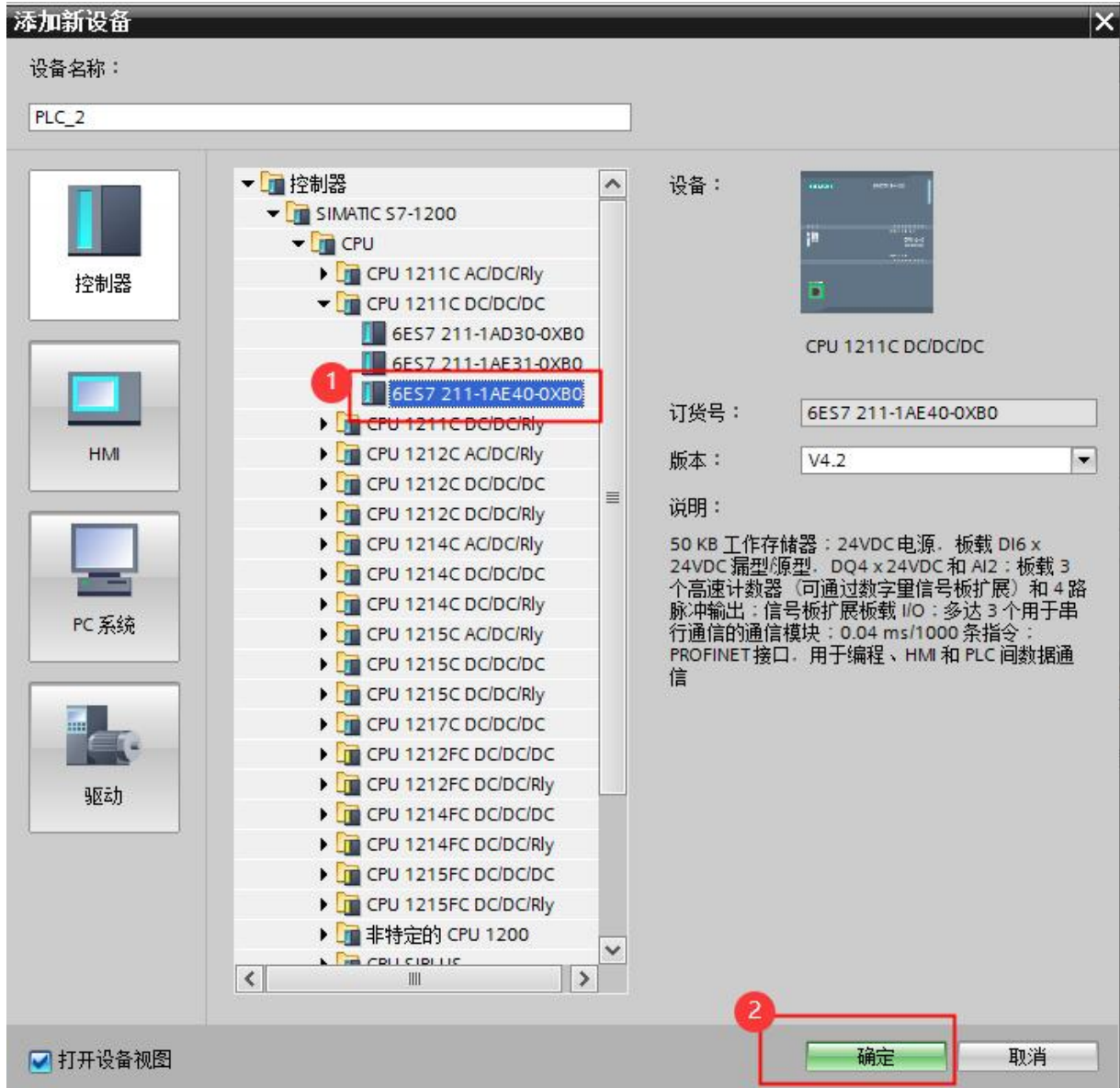
### 3.3.2 CPU的添加与连接

1. 点击界面左边的“项目”， 出现下级目录， 并双击“添加新设备”：



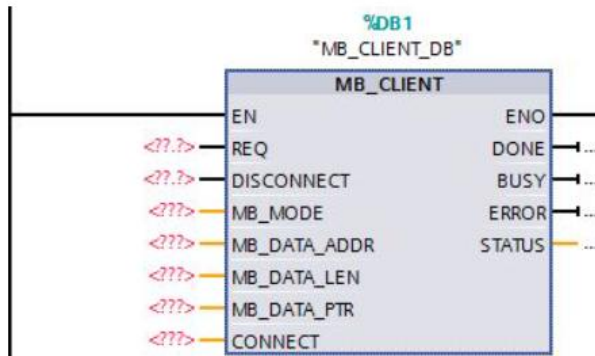


2. 弹出“添加新设备”窗口，进行“控制器→SIMATIC S7-1200→CPU→CPU 1211C DC/DC/DC→6ES7 211-1AE40-0XB0”操作, 点击确定：



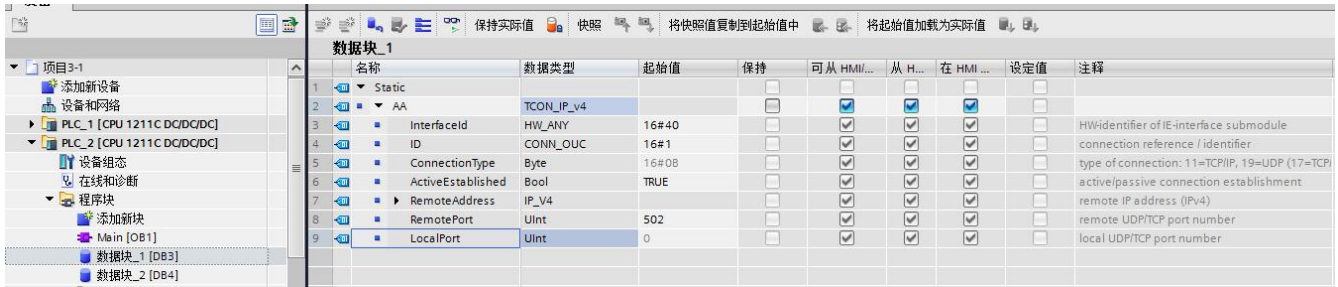
### 3.3.3 在主程序中调用MB\_CLIENT指令

名称	描述	版本
▸ S7 通信		V1.3
▸ 开放式用户通信		V4.0
▸ WEB 服务器		
▾ 其他		
▾ MODBUS TCP		V4.0
▣ MB_CLIENT	通过 PROFINET 进...	V4.0
▣ MB_SERVER	通过 PROFINET 进...	V4.0
▸ 通信处理器		
▸ 远程服务		V1.9



参数	说明
REQ	与服务器之间的通信请求，上升沿有效。
DISCONNECT	通过该参数，可以控制与 Modbus TCP 服务器建立和终止连接。0：建立连接；1：断开连接。
MB_MODE	选择 Modbus 请求模式（读取、写入或诊断）。具体参见表 4。
MB_DATA_ADDR	由“MB_CLIENT”指令所访问数据的起始地址。具体参见表 4。
MB_DATA_LEN	数据长度：数据访问的位或字的个数。具体参见表 4。
MB_DATA_PTR	指向 Modbus 数据寄存器的指针。
CONNECT	指向连接描述结构的指针。使用 TCON_IP_v4 数据类型。
DONE	最后一个作业成功完成，立即将输出参数 DONE 置位为“1”。
BUSY	作业状态位：0：无正在处理的“MB_CLIENT”作业；1：“MB_CLIENT”作业正在处理。
ERROR	错误位：0：无错误；1：出现错误，错误原因查看STATUS。
STATUS	指令的详细状态信息。

### 3.2.4 添加2个全局数据块，数据类型TCON\_IP\_v4



参数	说明
Interfaceld	网口硬件标识符，对于本体网口为 64，即16#40。
ID	连接 ID，取值范围 1~4095
Connection Type	连接类型。TCP 连接默认为：16#0B
ActiveEstablished	建立连接。主动为 1（客户端），被动为 0（服务器）。
ADDR	服务器侧的 IP 地址
RemotePort	远程端口号
LocalPort	本地端口号

本文远程服务器的 IP 地址为 192.168.0.2和192.168.0.3远程端口号设为 502

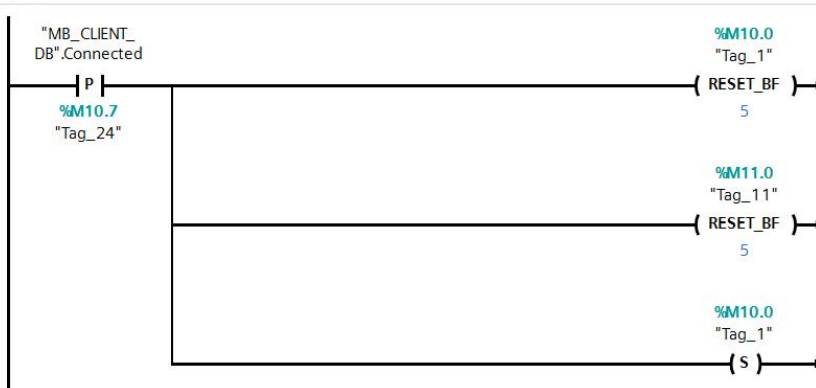
### 3.2.5 MB\_MODE、MB\_DATA\_ADDR、MB\_DATA\_LEN、Modbus TCP 功能码等之间的关系

MB_MODE	MB_DATA_ADDR	MB_DATA_LEN	Modbus TCP 功能码	操作和数据
0	1 - 9999	1 - 2000	01	• 读取输出位 • 每个请求 1 - 2000 个位
0	10001 - 19999	1 - 2000	02	• 读取输入位 • 每个请求 1 - 2000 个位
0	• 40001 - 49999 (等同于 400001 - 409999) • 400001 - 465535	1 - 125	03	• 读取保持寄存器 • 每个请求 1 - 125 个字
0	30001 - 39999	1 - 125	04	• 读取输入字 • 每个请求 1 - 125 个字
1	10001 - 19999	1	05	• 写入输出位 • 每个请求 1 个位
1	• 40001 - 49999 (等同于 400001 - 409999) • 400001 - 465535	1	06	• 写入保持寄存器 • 每个请求 1 个字
1	10001 - 19999	2 - 1968	15	• 写入多个输出位 • 每个请求 2 - 1968 个位
1	• 40001 - 49999 (等同于 400001 - 409999) • 400001 - 465535	2 - 123	16	• 写入多个保持寄存器 • 每个请求 2 - 123 个字
2	10001 - 19999	1 - 1968	15	• 写入输出位 • 每个请求 1 - 1968 个位
2	• 40001 - 49999 (等同于 400001 - 409999) • 400001 - 465535	1 - 123	16	• 写入保持寄存器 • 每个请求 1 - 123 个字
11			11	• 读取服务器的状态字和事件计数器: • 状态字反映了处理的状态 (0 - 未处理, 0xFFFF - 正在处理) • Modbus 请求或执行时, 事件计数器的递增, 如果执行 Modbus 功能时出错, 则服务器将发送消息, 但不会递增事件计数器。
80		1	08	• 通过诊断代码 0x0000 检查服务器状态 (返回循环测试 - 服务器返回请求): • 每次调用 1 个字
81		1	08	• 通过诊断代码 0x000A 读取服务器的事件计数器: • 每次调用 1 个字
101	0 - 65535	1 - 2000	01	• 读取输出位 • 每个请求 1 - 2000 个位
102	0 - 65535	1 - 2000	02	• 读取输入位 • 每个请求 1 - 2000 个位
103	0 - 65535	1 - 125	03	• 读取保持寄存器 • 每个请求 1 - 125 个字
104	0 - 65535	1 - 125	04	• 读取输入字 • 每个请求 1 - 125 个字
105	0 - 65535	1	05	• 写入输出位 • 每个请求 1 个位
106	0 - 65535	1	06	• 写入保持寄存器 • 每个请求 1 个字
115	0 - 65535	1 - 1968	15	• 写入输出位 • 每个请求 1 - 1968 个位
116	0 - 65535	1 - 123	16	• 写入保持寄存器 • 每个请求 1 - 123 个字

### 3.2.6 程序编写

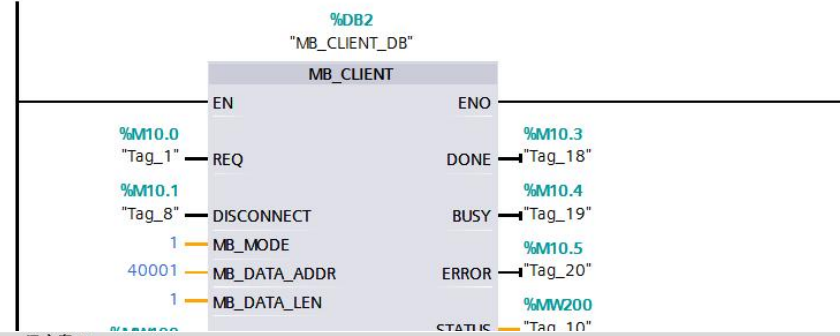
程序段 1: 连接建立后复位 MB\_CLIENT 指令的控制位和状态位, 置位请求信号 reqM10.0

注释



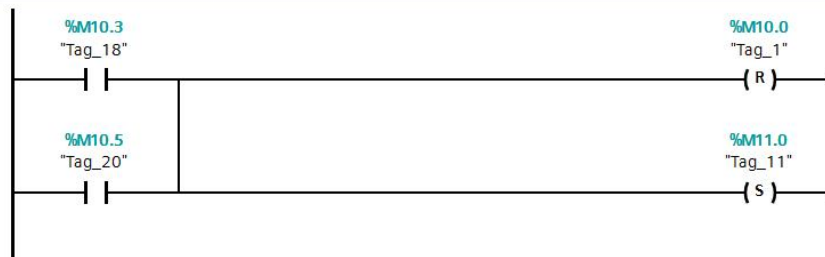
程序段 2 : Modbus TCP Client 1

- 1、Req使用上升沿触发
- 2、MB\_MODE设置模式为读参数模式,MB\_MODE=1设置模式为写参数模式
- 3、MB\_DATA\_ADDR=40001,表示寄存器数据地址从40001开始(保持寄存器),Iaeconfig软件设置中IO映射方式改成REG模式。
- 4、MB\_DATA\_LEN=1,表示1个字。
- 5、Connect使用数据块TCON\_IP\_v4接通,不通过指令断开连。



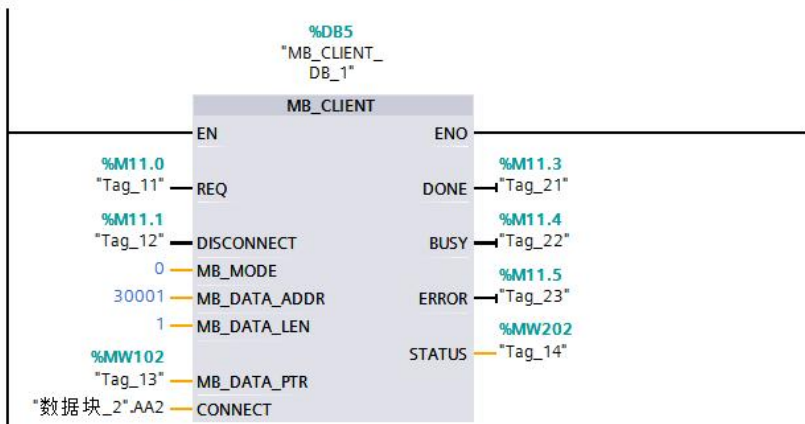
程序段 3 : 读写轮询1

注释



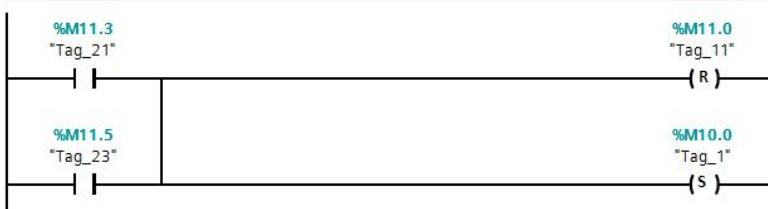
程序段 4 : Modbus TCP Client 2

- 1、Req使用上升沿触发
- 2、MB\_MODE设置模式为读参数模式,MB\_MODE=0设置模式为写参数模式
- 3、MB\_DATA\_ADDR=30001,表示寄存器数据地址从30001开始(输入寄存器),Iaeconfig软件设置中IO映射方式改成REG模式。
- 4、MB\_DATA\_LEN=1,表示1个字。
- 5、Connect使用数据块TCON\_IP\_v4接通,不通过指令断开连。



程序段 5 : 读写轮询2

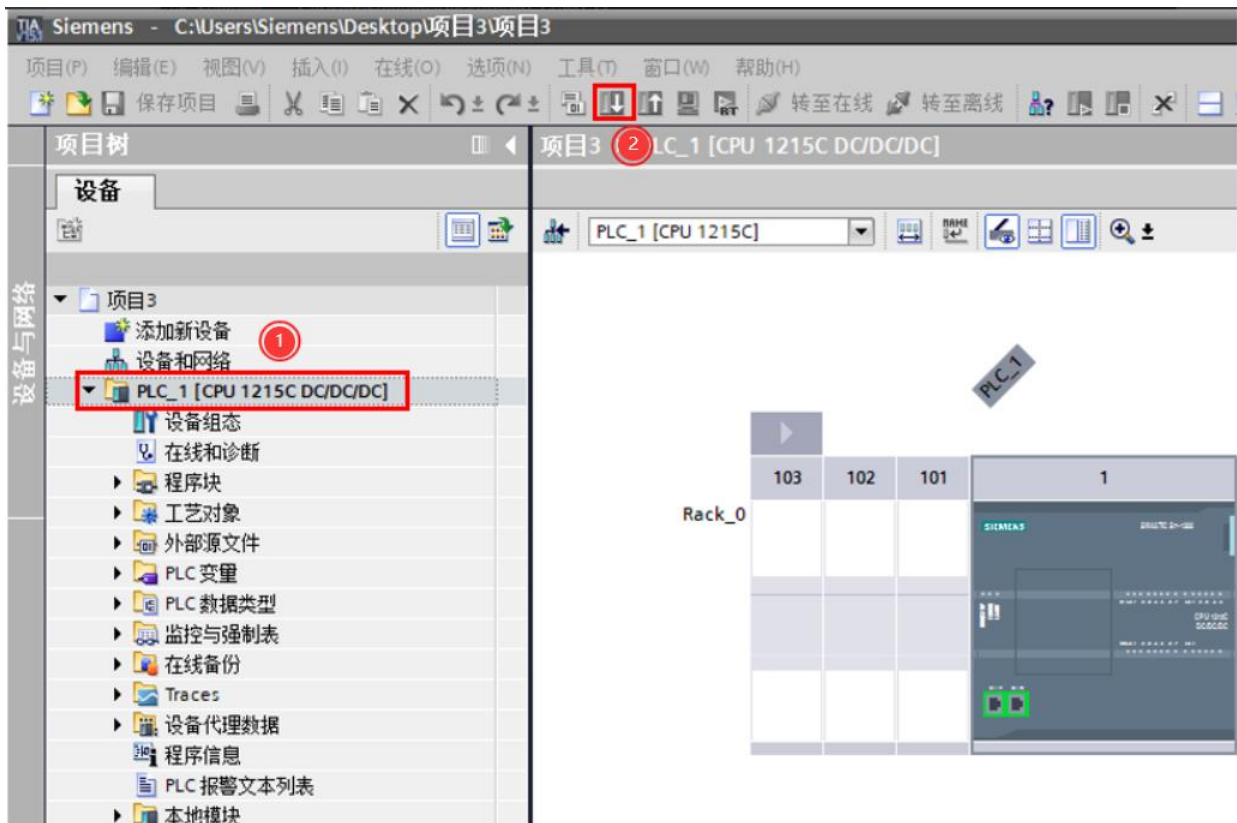
注释



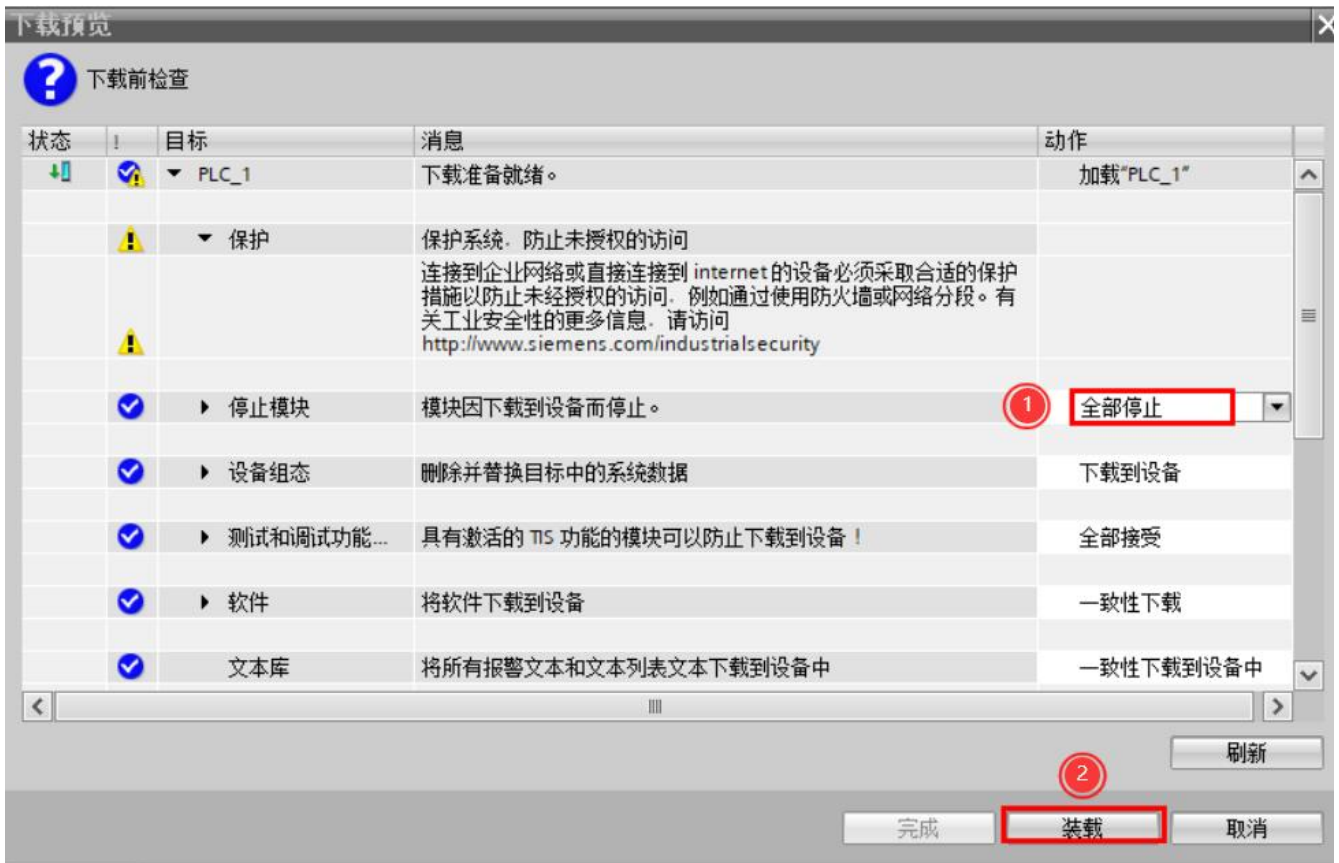


### 3.4 程序编译下载

1. 在项目树中，选中需要下载的项目文件夹，然后执行菜单命令"在线\下载到设备"或直接点击工具栏上的图标"下载到设备"



2. 如果需要下载修改过的硬件组态且CPU处于运行模式时，需要把CPU转为停止模式



官方网站



先进自动化控制及工业网络技术



**无锡凌科自动化技术有限公司** [www.latcos.cn](http://www.latcos.cn) 公司电话：**0510-85888030**  
公司地址：**江苏省无锡市惠山区清研路 3 号华清创智园 7 号楼 701 室**