RVNet-S7

西门子 SIMATIC®　S7 系列 PLC 以太网通讯处理器

使用手册

1.RVNet 产品选型

1.1 系列和型号

RVNet 产品主分为两个系列：**RVNet（基本版）**、**RVNet Plus（高级版）**。

- **RVNet（基本版）**包括三个型号：RVNet-S7200 直通型、RVNet-S7200 桥接型、RVNet-S7300。
  - RVNet-S7200 直通型：适用于西门子 S7200 系列、SMART 系列等 PLC 控制系统的的以太网通讯；其 X2 的扩展接口可以连接支持多主站通讯的触摸屏（西门子品牌、PROFACE 品牌）和通讯电缆（西门子原装）。
  - RVNet-S7200 桥接型：适用于西门子 S7200 系列、SMART 系列等 PLC 控制系统的的以太网通讯；其 X2 的扩展接口可以连接不支持多主站通讯的触摸屏（国产触摸屏品牌：威纶通、步科、昆仑通泰、海泰克等）。
  - RVNet-S7300：适用于西门子 S7200/300/400 系列等 PLC 控制系统和西门子 840D、840D SL 数控系统的以太网通讯；其 X2 的扩展接口可以连接支持多主站通讯的触摸屏（西门子品牌、PROFACE 品牌）和通讯电缆（西门子原装）。
- **RVNet Plus（高级版）**包括四个型号：RVNet-S7200 Plus 直通型、RVNet-S7200 Plus 桥接型、RVNet-S7300 Plus 直通型、RVNet-S7300 Plus 桥接型。
  - RVNet-S7200 Plus 直通型：适用于西门子 S7200 系列、SMART 系列等 PLC 控制系统的的以太网通讯；其 X2 的扩展接口可以连接支持多主站通讯的触摸屏（西门子品牌、PROFACE 品牌）和通讯电缆（西门子原装）。
  - RVNet-S7200 Plus 桥接型：适用于西门子 S7200 系列、SMART 系列等 PLC 控制系统的的以太网通讯；其 X2 的扩展接口可以连接不支持多主站通讯的触摸屏（国产触摸屏品牌：威纶通、步科、昆仑通泰、海泰克等）。
  - RVNet-S7300 Plus 直通型：适用于西门子 S7200/300/400 系列等 PLC 控制系统和西门子 840D、840D SL 数控系统的以太网通讯；其 X2 的扩展接口可以连接支持多主站通讯的触摸屏（西门子品牌、PROFACE 品牌）和通讯电缆（西门子原装）。
  - RVNet-S7300 Plus 桥接型：适用于西门子 S7200/300/400 系列等 PLC 控制系统和西门子 840D、840D SL 数控系统的以太网通讯；其 X2 的扩展接口支持 Modbus 功能（支持 Modbus 主站功能和 Modbus 从站功能），实现 PLC 与其他 Modbus 设备的通讯。

1.2 系列对比

名称	功能	RVNet 基本版	RVNet Plus 高级版
参数设置和诊断	参数设置、诊断	WEB 浏览器、NetDevice	
	参数密码保护	支持	
	初始化 IP 地址	192.168.1.188	
	恢复出厂设置	支持（模块侧面复位按钮，长按至 Bus 灯熄灭后重新点亮）	
S7 总线接口	协议模式	PPI/MPI 从站/MPI 主从站/PROFIBUS	
	波特率	自适应/手动设定	
		9.6K – 6Mbps	

	S7-200/300/400 混合总线网络	可同时访问所有站点	
	S7-200 之间存在网络读写的总线网络	支持并可访问任意站点，选择 MPI 从站模式	
以太网接口	以太网连接数	32	
	协议支持	S7TCP、ModbusTCP、RVNetS7	
PLC 数据交换	PLC 之间的数据交换	不支持	支持
Modbus 通讯	PLC 与 Modbus 设备通讯	不支持	支持

2.RVNet 功能应用

功能一：编程调试

RVNet-S7 模块支持对 PLC 控制系统的编程调试（MicroWIN、STEP7、博图软件）。详见《第五章：编程调试》。

功能二：SCADA 以太网通讯

RVNet-S7 模块支持和市面上几乎所有的 SCADA 监控组态软件以太网通讯，例如：WINCC、组态王、MCGS、力控、杰控、易控、INTOUCH、IFIX、LABVIEW 等。详见《第六章：SCADA 以太网通讯》

功能三：OPC 通讯

RVNet-S7 模块支持和市面上主流的 OPC Server 以太网通讯，例如：KEPWARE OPC、PC ACCESS OPC 等。另外，基于 RVNetS7 协议，我们开发了完全免费的 RVNetS7 OPC 服务器，最多可连接 1023 台设备，适用于大规模的设备联网项目的数据采集。详见《第七章：OPC 通讯》

功能四：触摸屏以太网通讯

RVNet-S7 模块支持和市面上主流的触摸屏以太网通讯，例如：西门子 KTP/TP 系列、西门子 SmartIE 系列连 S7300、威纶通、步科、昆仑通态等。详见《第八章：触摸屏以太网通讯》。

功能五：ModbusTCP 通讯

RVNet-S7 模块内部集成了 ModbusTCP 服务器功能，上位机软件（ModusTCP 客户端）可直接按照地址映射表去访问 PLC 控制系统的内部寄存器地址的数据，地址映射表可以使用默认的也可以自由定义映射关系，使得通讯变得更加灵活。详见《第九章：ModbusTCP 通讯》。

功能六：高级语言编程

RVNet-S7 模块提供开放的以太网协议（RVNetS7 协议）供工程师开发通讯程序软件使用。详见《第十章：RVNetS7 协议规范》。

功能七：PLC 数据交换

RVNet-S7 模块（仅 RVNet Plus（高级版）支持该功能，RVNet（基本版）不支持）支持与西门子 S7-1200、S7-1500、SMART 200PLC 实现交换数据。详见《第十一章：PLC 数据交换》。

功能八：Modbus 通讯

RVNet-S7 模块（仅 RVNet-S7300 Plus 桥接型支持该功能支持 Modbus 功能，可作为 Modbus 主站或者 Modbus 从站，实现 PLC 与其他 Modbus 设备的通讯。详见《第十二章：Modbus 通讯》。

3.RVNet 安装、诊断

3.1 安装

1、将西门子 PLC 控制器上电；
2、将 RVNet-S7 模块插入到 PLC 的 DB9 通讯口，并拧紧螺栓加以固定；
3、用一根网线连接 RVNet-S7 模块和电脑。

3.2 诊断

1、RVNet-S7 模块的红色电源指示灯 Pwr 灯将立即常亮；
2、RVNet-S7 模块的绿色总线指示灯 Bus 灯应在 3 秒内常亮，Bus 灯常亮表明 RVNet-S7 模块已自动锁定了 PLC 通讯口的波特率，此状态为未通讯时的正常状态，也是正常通讯的前提；
3、RVNet-S7 模块的 RJ45 端口的绿色 Link 灯应常亮，Link 灯常亮表明 RVNet 已经建立了以太网连接。

注意：

当 RVNet-S7 模块插在 PLC 的 PPI 通讯口，并且处于未通讯的状态时发现 Bus 灯非【常亮】状态（即无法锁定 PLC 通讯口的波特率），一般为以下情况：

PLC 的通讯口被设置成了自由口通讯，解决方法：将 PLC 的拨码开关打到 STOP 状态，再次尝试连接。

当 RVNet-S7 模块插在 PLC 的 PROFIBUS 通讯口，并且处于未通讯的状态时发现 Bus 灯非【常亮】状态（即无法锁定 PLC 通讯口的波特率），一般为以下情况：

1、 新的 PLC 的 PROFIBUS 口默认是未启用状态，解决方法：通过 MPI 通讯口对 PROFIBUS 通讯口进行配置并且下载硬件配置；

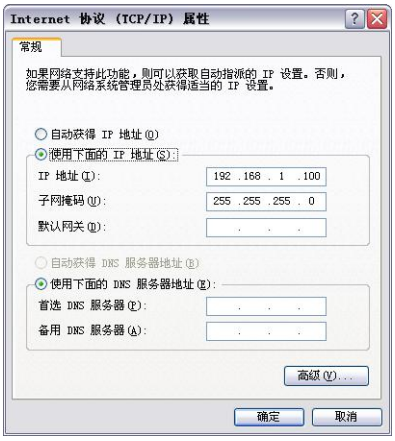
2、 PROFIBUS 通讯口的波特率高于 6M bps，解决方法：RVNet-S7 模块在 PROFIBUS 通讯口下支持的最高波特率为 6M bps，将 PROFIBUS 通讯口的波特率设置为 6M bps 以下。

4.RVNet 参数设定

当需要对 RVNet-S7 的参数进行修改（比如修改 IP 地址）时，可以通过登录 Web 网页或者使用 NetDevice 软件来实现。
一般情况下，只要保证 RVNet-S7 和电脑的 IP 地址在同一网段，其它参数无需设置，就可以正常通讯了。

4.1Web 页面的登录、查看

1.将电脑的本地网卡的 IP 设置成 192.168.1.100。如下图所示：



2.电脑上运行 Internet Explorer 浏览器，在地址栏输入：192.168.1.188（这是 RVNet-S7 的出厂 IP 地址），然后按回车键，浏览器应能显示 RVNet-S7 的内部 Web 网页，如下图所示：

3.登录后显示的首页，如下图所示：

设备基本信息：由出厂时预置。

S7 总线接口参数：显示当前设置的 S7 接口各项参数。

S7 总线接口状态：包括当前 RVNet-S7 所处的 S7 总线协议模式、S7 总线状态、主从站地址表及自动波特率的执行情况。

以太网接口参数：显示当前设置的以太网接口参数。

4.1.1 串行总线接口参数

RVNet 站地址：RVNet-S7 的自身站地址，默认为 0。这个地址不能和 S7 总线上其他设备的站地址相同，必须唯一。

S7 总线最高站地址：指定 S7 总线上可能的最高站地址，默认为 31；RVNet-S7 会根据这个参数去

搜寻网络上可能存在的 PLC 设备。

站点通讯重试次数：当通讯发生错误时 RVNet-S7 进行重试的次数，默认为 3。

地址间隔刷新系数：这个系数影响 RVNet-S7 查找其他设备的速度，默认为 10。

S7 总线协议模式：设置 RVNet-S7 运行的协议模式：

当 RVNet 插在 S7200 的 PPI 通讯口上时：选择 PPI 模式；

当 RVNet 插在有网络读写通讯的 S7200 的 PPI 通讯口上或者插在 EM277 上时：选择 MPI 从站模式；

当 RVNet 插在 S7300 的 MPI 通讯口上时：选择 MPI 主从站模式；

当 RVNet 插在 S7300 的 PROFIBUS 通讯口时：选择 PROFIBUS 模式。

S7 总线波特率自动检测：默认为【开启】，【开启】状态下无需设置【S7 总线——>波特率】，将自动识别 PLC 通讯口的波特率。

扩展总线接口波特率自动检测：默认为【开启】，【开启】状态下无需设置【扩展总线(HMI 端)——>波特率】，将自动识别 HMI 通讯口的波特率，仅对桥接型模块有意义。

高级设置：

S7 总线——>波特率：只当【S7 总线波特率自动检测】状态为【关闭】时，需要根据连接的 PLC 通讯口的波特率手动设置该参数。

扩展总线(HM 端)——>波特率：只当【扩展总线接口波特率自动检测】状态为【关闭】时，需要根据连接的 HMI 通讯口的波特率手动设置该参数，仅对桥接型模块有意义。

当更改以上参数后请点击[确认]按钮，RVNet-S7 将复位并重新启动。请回到地址栏重新刷新首页并查看 S7 接口参数设置是否有效。

4.1.2 以太网接口参数

设置 RVNet-S7 的 IP 地址、掩码和网关（即路由器的地址）；

S7TCP 默认目标 PLC 地址：默认为 2，这个参数只有当组态王、WINCC 等组态软件采用 S7TCP 驱动和 PLC 通讯时，需要设置这个参数与 PLC 的站地址保持一致。

通讯目标 PLC 地址由槽号决定：通过插槽号决定与不同 PLC 通讯，默认为【关闭】，即采用【S7TCP 默认目标 PLC 地址】参数通讯。

高级设置：

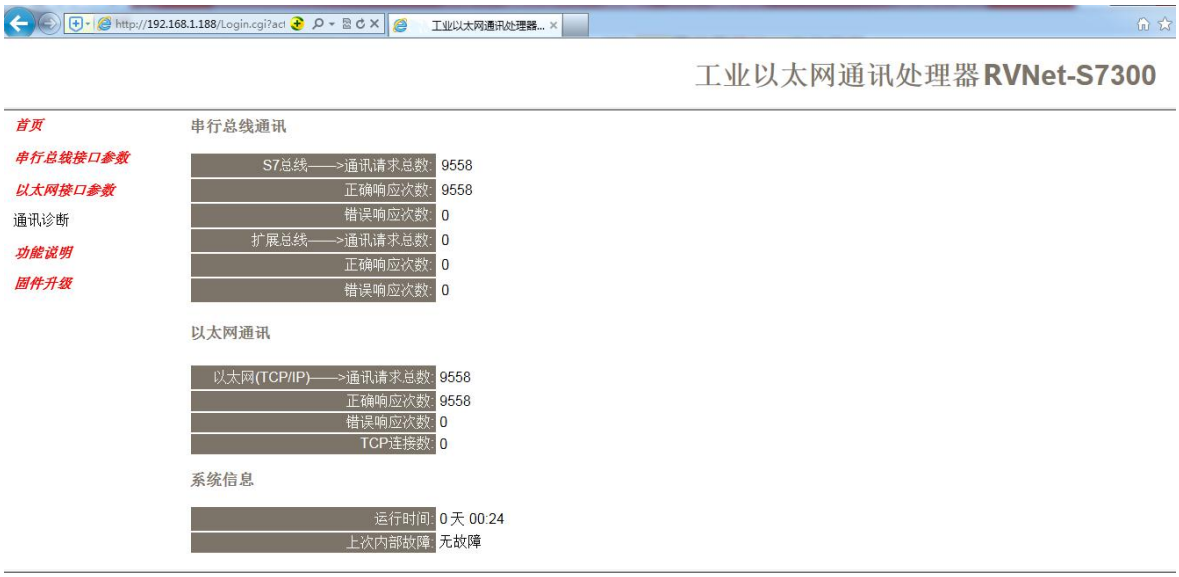
S7TCP 服务器端口号：默认为 102，建议默认。

ModbusTCP 端口号：默认为 502，建议默认。

RVNetS7 协议端口号：默认为 1099，建议默认。

当更改以上参数后请点击[确认]按钮，RVNet-S7 将复位并重新启动。如改了 IP 地址，请回到地址栏重新键入新的 IP 地址刷新首页并查看以太网接口参数设置是否有效。

4.1.3 通讯诊断



S7 总线——>通讯请求总数：所有发送到 PLC 的通讯请求数目；
正确响应次数：PLC 正确响应这些请求的数目；
错误响应次数：PLC 发出的错误响应数目；
注：对于 S7-300/400 通讯，一个通讯请求可能会产生多个正确的响应。因此正确响应次数和错误响应次数之和会大于通讯请求总数。

扩展总线——>通讯请求总数：HMI 发送到 RVNet-S7 的通讯请求数目；
正确响应次数：RVNet-S7 正确响应这些请求的数目；
错误响应次数：RVNet-S7 发出的错误响应数目；
以太网(TCP/IP)——>通讯请求总数：以太网客户机发送到 RVNet-S7 的通讯请求数目；
正确响应次数：RVNet-S7 正确响应这些请求的数目；

错误响应次数：RVNet-S7 发出的错误响应数目；

TCP 连接数：所有以太网客户机连接数；

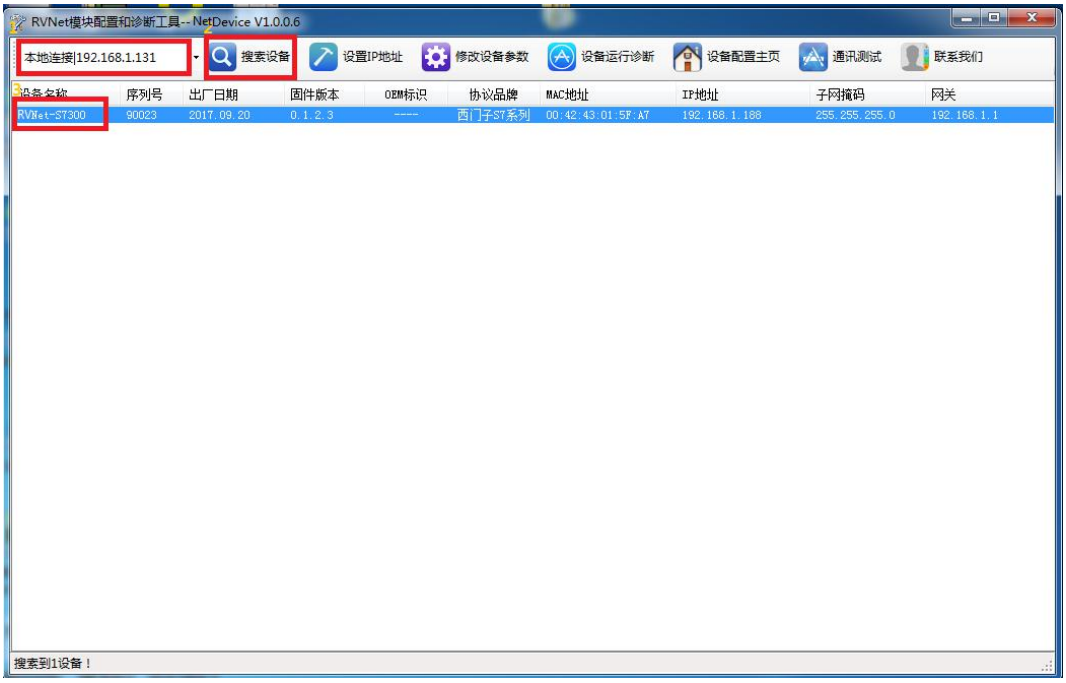
运行时间：RVNet-S7 上电后的运行时间；

上次内部故障：RVNet-S7 的系统故障，正常情况下不应该产生故障；

4.2NetDevice 软件使用

4.2.1 搜索设备

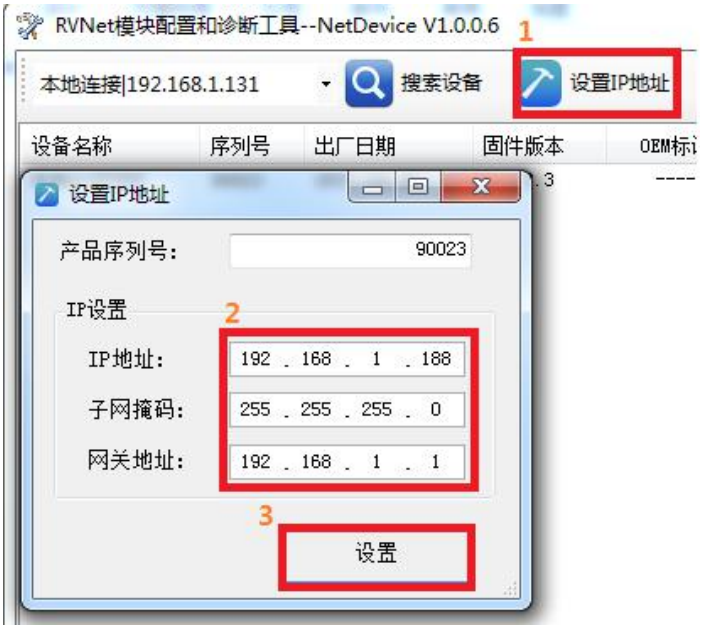
运行 NetDevice 软件，如下图：



1.搜索设备之前请选择好连接 RVNet-S7 模块的【网络接口】;
如果电脑和模块是通过网线连接的，请选择【本地连接】;
如果电脑和模块是通过无线连接的，请选择【无线网络连接】。
2.点击【搜索设备】按钮，可以把网络上的 RVNet-S7 模块搜索出来，此时我们可以看到模块的一些基本信息，包括：序列号、出厂日期、固件版本、IP 地址、子网掩码、网关等信息。

4.2.2 设置 IP 地址

首先，我们需要修改 RVNet-S7 模块的 IP 地址来保证与电脑的 Ip 地址在同一网段。
点击【设置 IP 地址】按钮，在弹出的对话框中，对【IP 地址】、【子网掩码】、【网关】进行修改，修改完成后，点击【设置】按钮进行参数保存。



4.2.3 修改设备参数

正常情况下，不需要对 RVNet-S7 模块进行参数的修改就已经可以正常通讯了。

4.2.3.1S7 总线接口参数配置

1.点击【修改设备参数】按钮，在弹出的对话框中，可以查看【S7 总线接口参数配置】——【S7 总线接口】参数，如果修改了其中的参数，需要点击【下载参数】按钮才能生效。

RVNet 站地址：RVNet-S7 的自身站地址，默认为 0。这个地址不能和 S7 总线上其他设备的站地址相同，必须唯一。

S7 总线最高站地址：指定 S7 总线上可能的最高站地址，默认为 31；RVNet-S7 会根据这个参数去搜寻网络上可能存在的 PLC 设备。

站点通讯重试次数：当通讯发生错误时 RVNet-S7 进行重试的次数，默认为 3。

地址间隔刷新系数：这个系数影响 RVNet-S7 查找其他设备的速度，默认为 10。

S7 总线协议模式：设置 RVNet-S7 运行的协议模式：

当 RVNet 插在 S7200 的 PPI 通讯口上时：选择 PPI 模式；

当 RVNet 插在有网络读写通讯的 S7200 的 PPI 通讯口上或者插在 EM277 上时：选择 MPI 从站模式；

当 RVNet 插在 S7300 的 MPI 通讯口上时：选择 MPI 主从站模式；

当 RVNet 插在 S7300 的 PROFIBUS 通讯口时：选择 PROFIBUS 模式。

S7 总线通讯波特率：推荐选择自动识别，如果你知道 PLC 通讯口的波特率，也可以手动设定波特率。

2.点击【修改设备参数】按钮，在弹出的对话框中，可以查看【S7 总线接口参数配置】——【扩展总线接口】参数，如果修改了其中的参数，需要点击【下载参数】按钮才能生效。

波特率：推荐选择自动识别，如果你知道触摸屏通讯口的波特率，也可以手动设定波特率。
注意：此界面配置只对桥接型模块有效。

4.2.3.2 以太网接口参数配置

1.点击【修改设备参数】按钮，在弹出的对话框中，可以查看【以太网接口参数配置】——【以太网接口参数】参数，如果修改了其中的参数，需要点击【下载参数】按钮才能生效。

IP 地址、子网掩码、网关地址分别为 RVNet-S7 的 ip 地址、子网掩码、网关。

2.点击【修改设备参数】按钮，在弹出的对话框中，可以查看【以太网接口参数配置】——【S7TCP 服务器】参数，如果修改了其中的参数，需要点击【下载参数】按钮才能生效。

S7TCP 服务器端口号：默认为 102，建议默认。

S7TCP 默认目标 PLC 地址：默认为 2，这个参数只有当组态王、WINCC 等组态软件采用 S7TCP 驱动和 PLC 通讯时，需要设置这个参数与 PLC 的站地址保持一致。

通讯目标 PLC 地址由槽号决定：通过插槽号决定与不同 PLC 通讯，默认为【关闭】，即采用【S7TCP 默认目标 PLC 地址】参数通讯。

4.2.3.3Modbus 映射表

点击【修改设备参数】按钮，在弹出的对话框中，可以查看【Modbus 映射表】参数，如果修改了其中的参数，需要点击【下载参数】按钮才能生效。

1.RVNet-S7 内置了默认地址映射表，映射规则为全区域映射（0~65535）：

- 线圈 Coil（000001~）映射为 PLC 的 Q 区；
- 输入 Input（100001~）映射为 PLC 的 I 区；
- 输入寄存器 InputRegsiter 映射为 PLC 的 M 区；
- 保持寄存器 HoldingRegsiter 映射为 PLC 的 DB1 数据块（S7200 的 V 区）。

2.除了默认的地址映射外，我们也可以自定义地址映射关系，我们推荐使用【自动分配映射关系（推荐）】来配置地址映射表，在此之前，我们需要手动删除默认的地址映射表。

1）选中映射块，点击【删除映射块】来删除映射块；

2）点击【自动分配映射地址（推荐）】，添加自定义映射块。

3）我们大致可以按照以下思路来完成自定义映射块的编辑：

◆ 根据你所要读写的 PLC 数据是以字为单位还是以位为单位，访问类型为只读还是读写来选择【映射到 Modbus 区域】;

Modbus 区域	数据类型	功能号	最大指令数
Coil 000001~	位	FC1（读线圈）	S7-200：119 S7-300：784
		FC5（写线圈）	1
Input 100001~	位	FC2（读输入）	S7-200：119 S7-300：784
InputRegsiter 300001~	字（2 字节）	FC4（读输入寄存器）	S7-200：16 S7-300：111
HoldingRegsiter 400001~	字（2 字节）	FC3（读保持寄存器） FC16（写保持寄存器）	111
		FC6（写单一保持寄存器）	1

◆ 选择你所要读写的 PLC 的数据区域及地址偏移。

举例：读写 DB1.DBW0

举例：读写 M0.0

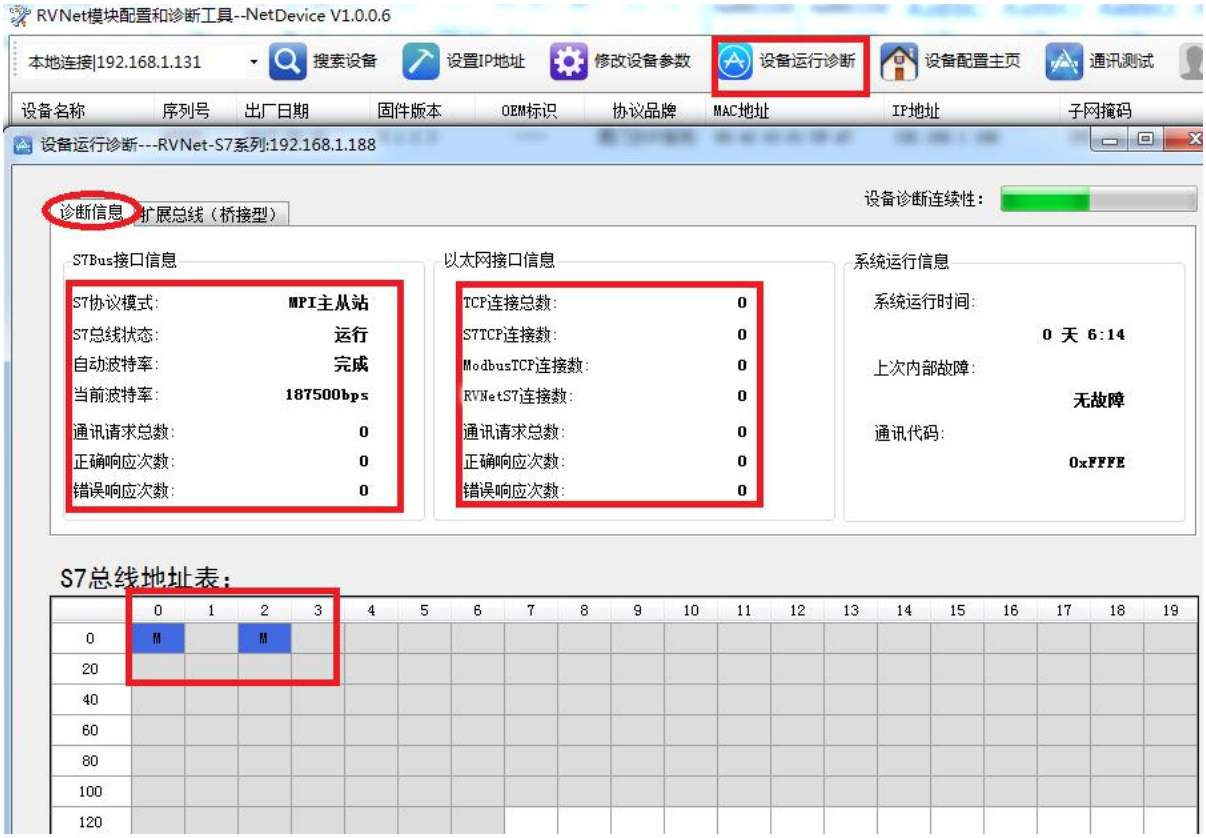
举例：只读 DB2.DBX10.0

举例：只读 DB3.DBW100

4）映射表编辑完成后，可以通过地址查询确定对应关系，比如要查询 DB1.DBW0 对应的 modbus 地址：点击【映射地址查询】，按如下设置，点击【查询】按钮，可以查询到对应的 Modbus 映射地址。

4.2.3.4 设备运行诊断

点击【设备运行诊断】按钮，可以查看 RVNet-S7 当前的运行情况：S7Bus 接口信息、以太网接口信息、S7 总线地址表等。



S7 总线地址表：

M：表示主站（Master）

S：表示从站（Slave）

S7 总线地址表显示当前 S7 总线上的站点信息：0 表示 RVNet-S7 的站地址；2 表示 S7300 的站地址。

4.2.3.5 通讯测试

点击【通讯测试】按钮，在弹出的对话框中，依次点击【发送】，把【循环】打上勾，点击【发送】。

这里我们读取了 PLC 的 MB0~MB19 共 20 个字节的数据，如果通讯正常，则会返回 MB0~MB19 共 20 个字节的数据（最直观的方法：如果接收次数和正确次数一直是累加的话，表面通讯正常），可以借此来判断 RVNet-S7 模块、PLC、上位机之间的以太网连接是否正常。

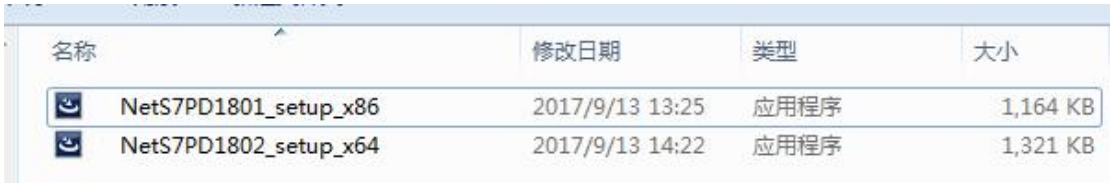
5.编程调试

5.1 驱动安装

安装编程驱动之前，计算机必须首先安装过西门子 MicroWIN 软件、STEP7 软件或者博途软件，控制面板中应有“设置 PG/PC 接口”图标，如下图：

设置 PG/PC 接口 (32 位)

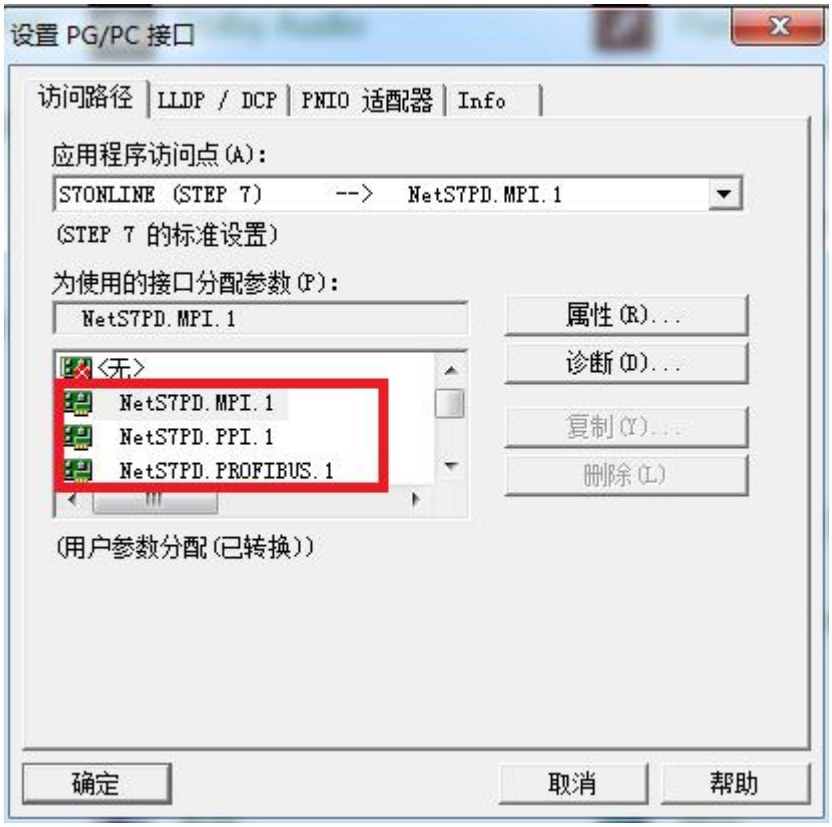
如果计算机的操作系统是 32 位的，请安装 32 位编程驱动；如果计算机的操作系统是 64 位的，请安装 64 位编程驱动。安装的时候，请右击驱动程序，以【管理员身份运行】安装，安装完成后，请重启计算机。驱动安装程序如下图：



【RVNetS7PD1801_setup_x86】为 32 位编程驱动；

【RVNetS7PD1802_setup_x64】为 64 位编程驱动。

重启计算机之后，进入控制面板，打开【设置 PG/PC 接口】，可以看到新增的通讯接口：



5.2MicroWIN 编程调试

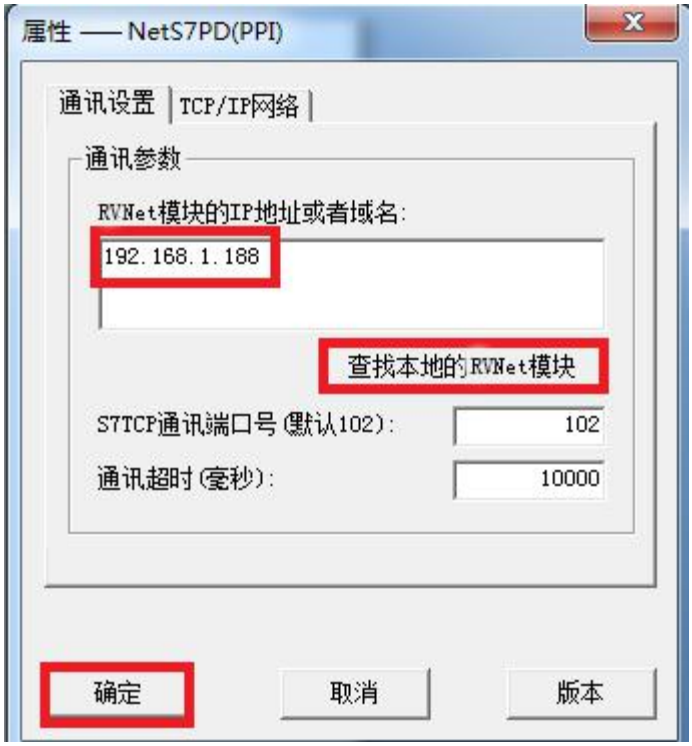
RVNet-S7 模块对 MicroWIN 编程调试有两种方法：通过 RVNet 编程驱动，或者通过西门子的以太网驱动。

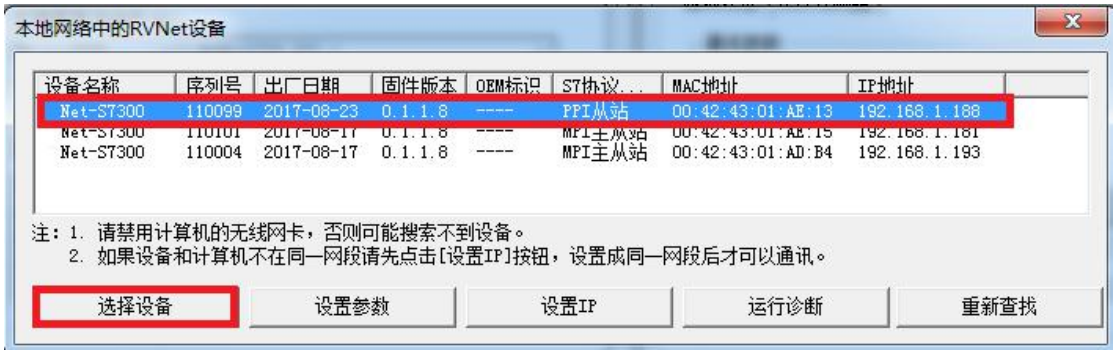
5.2.1 通过 RVNet 编程驱动

1.打开 MicroWIN 软件，点击左侧导航栏的【设置 PG/PC 接口】图标；

2.在【为使用的接口分配参数】中选择 RVNetS7PD.PPI.1，确保【应用程序访问点】为 Micro/WIN —>RVNetS7PD.PPI.1,点击【属性】按钮；

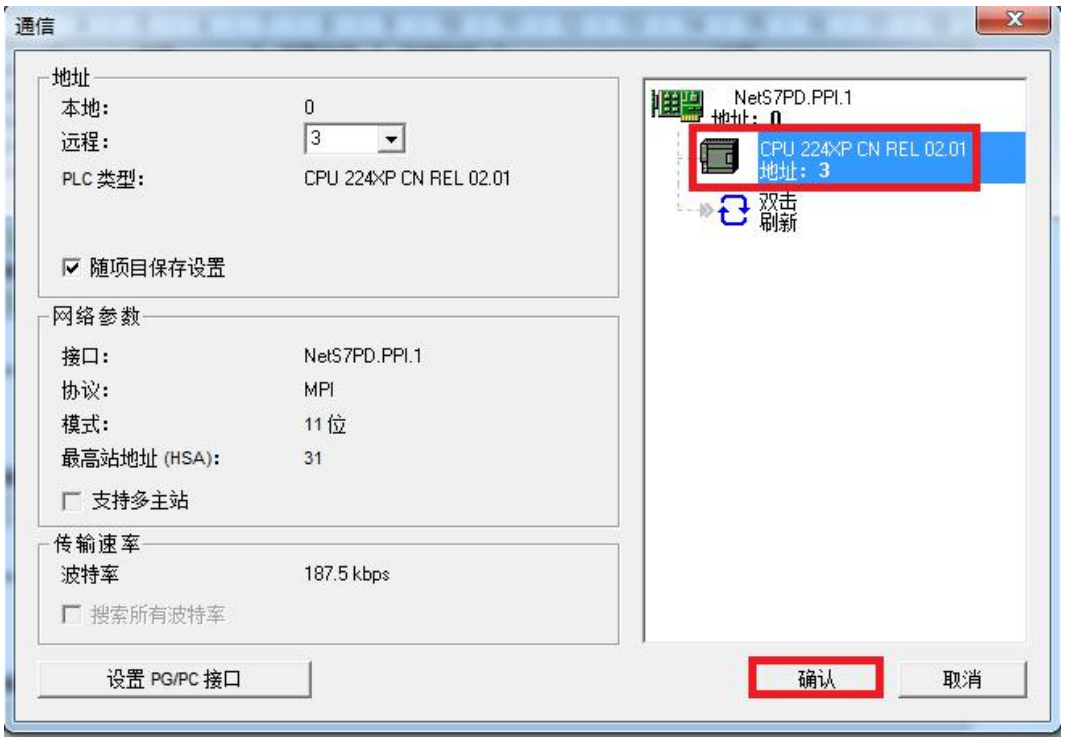
3.如果知道 RVNet 的 IP 地址，在【RVNet 模块的 IP 地址或域名】中直接输入 RVNet 的 IP 地址，点击【确定】按钮；
如果不知道 RVNet 的 IP 地址，可以点击【查找本地的 RVNet 模块】，选择要连接的 RVNet 模块，点击【选择设备】按钮。





4.点击左侧导航栏的【通信】图标；

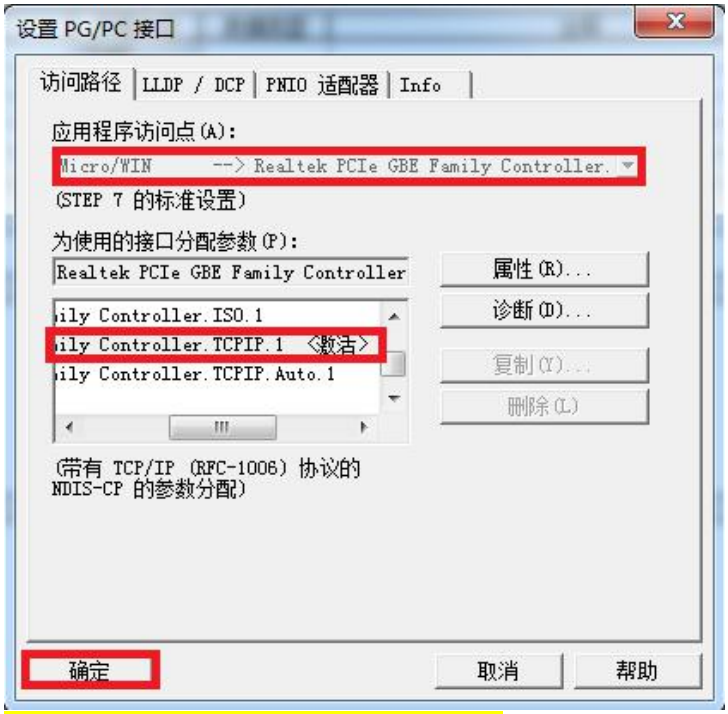
5.鼠标双击【双击刷新】图标，选中刷新到的 PLC，点击【确认】按钮。



5.2.2 通过西门子以太网驱动

1.打开 MicroWIN 软件，点击左侧导航栏的【设置 PG/PC 接口】图标；

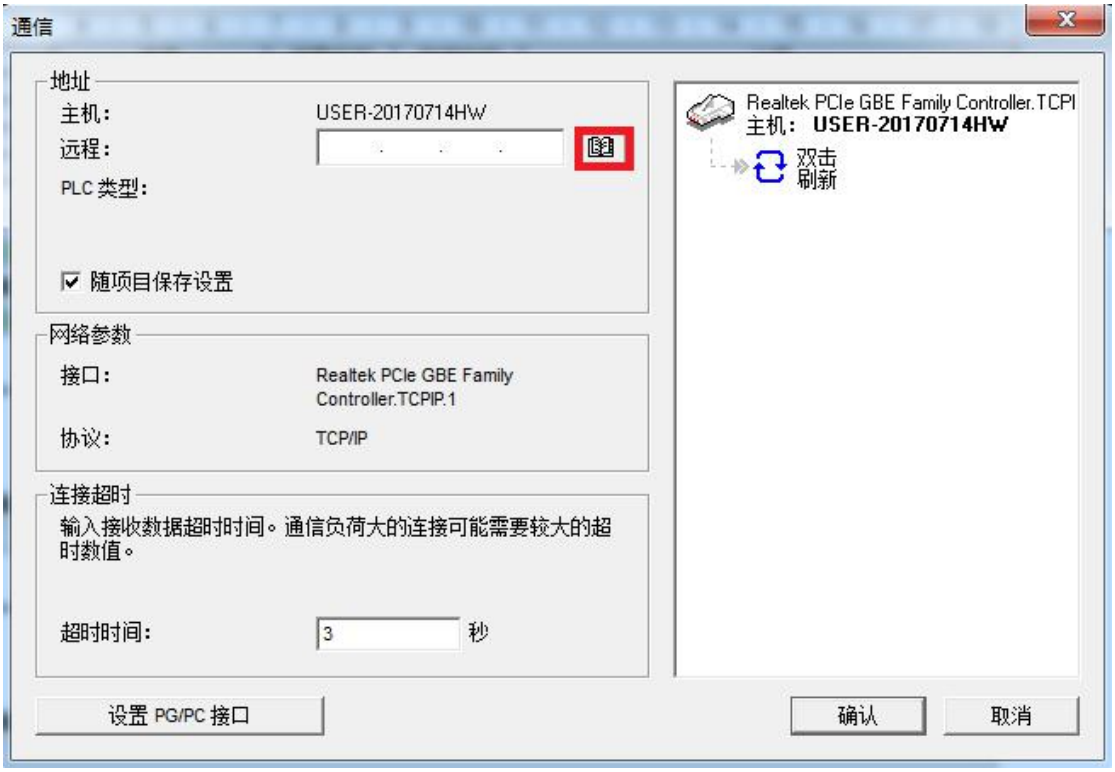
2.在【为使用的接口分配参数】中选择计算机的网卡，确保【应用程序访问点】为 Micro/WIN—>计算机网卡,点击【确定】按钮；



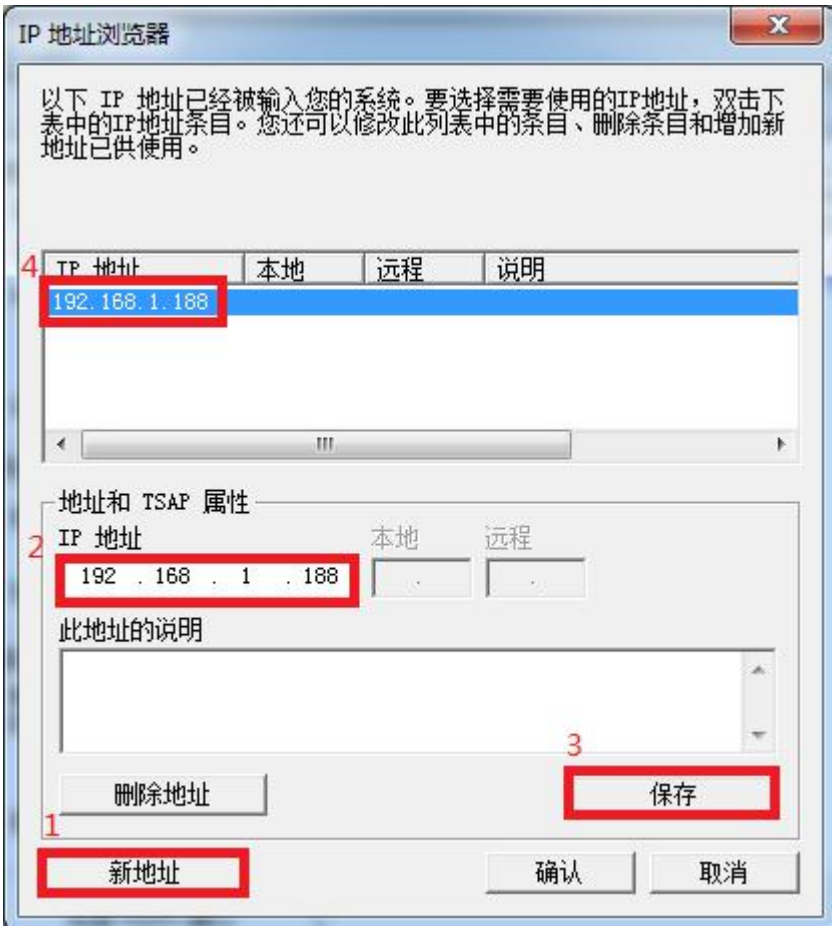
注意：请选择后缀为 TCPIP 的计算机网卡

3. 点击左侧导航栏的【通信】;

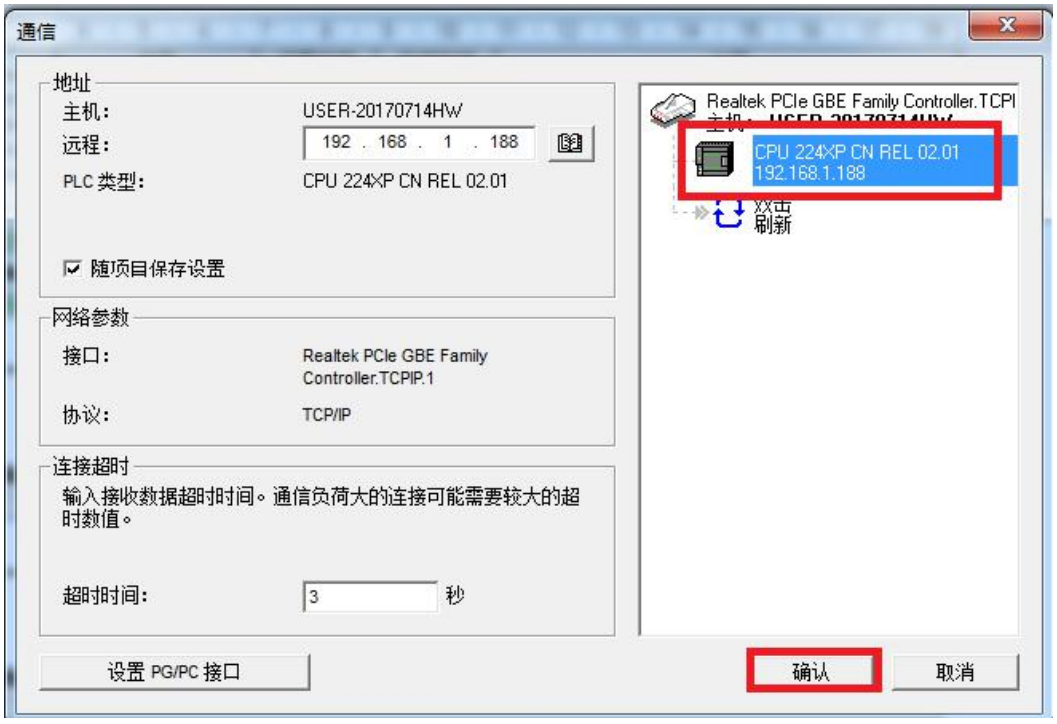
4.点击如下图标，打开 IP 地址浏览器;



5.点击【新地址】按钮，在【IP 地址】中输入 RVNet 的 IP 地址，点击【保存】按钮，双击保存后的 IP 地址；



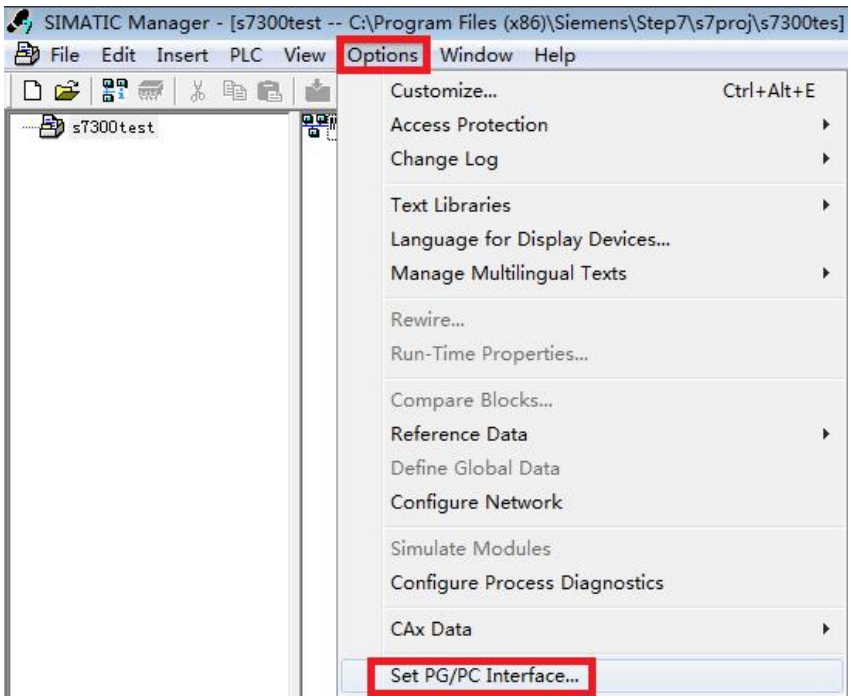
6. 鼠标双击【双击刷新】图标，选中刷新到的 PLC，点击【确认】按钮。



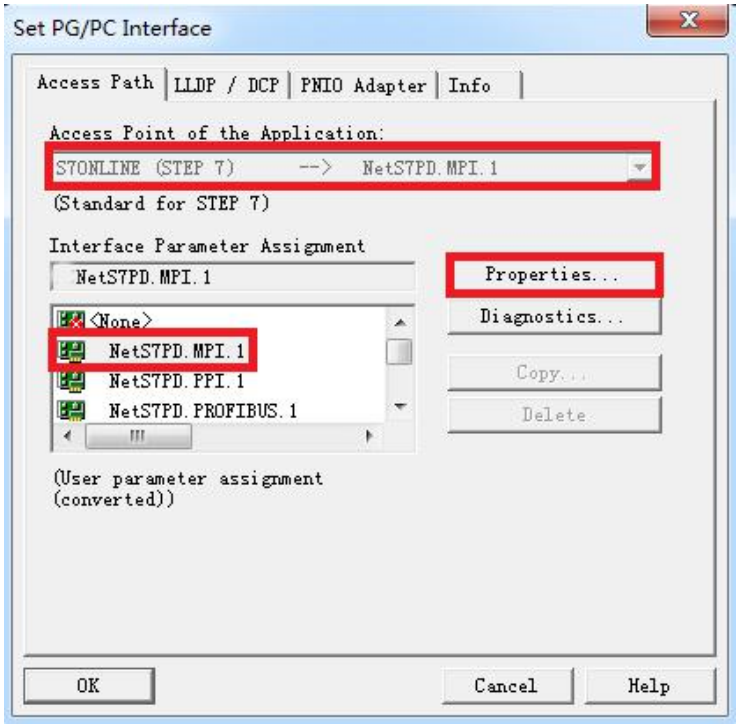
注意：通过西门子的以太网驱动时请设置【S7TCP 默认目标 PLC 地址】为当前 PLC 通讯口的站地址。

5.3Step7 编程调试

1.打开 STEP7 软件，新建项目，选择菜单栏的【Options】，点击【Set PG/PC Interface】;



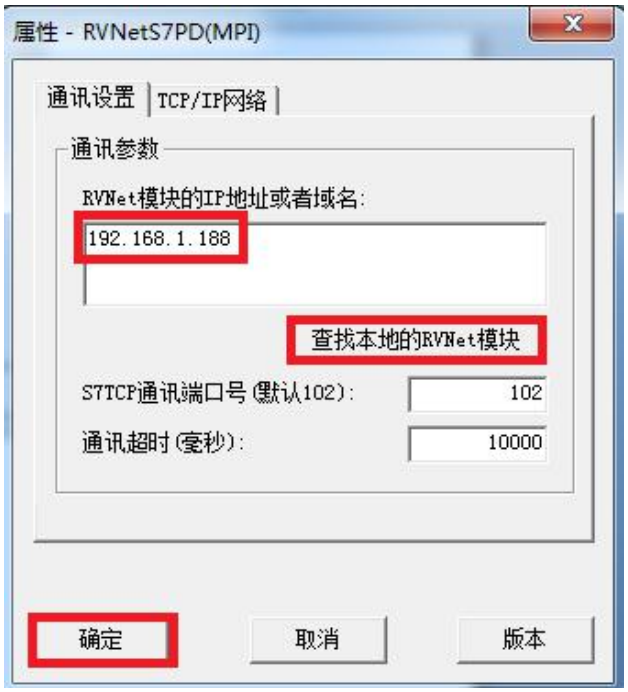
2.【Interface Parameter Assignment】设置为 RVNetS7PD.MPI.1，确保【Access Point of the Application】为 S7ONLINE（STEP7）—> RVNetS7PD.MPI.1，点击【Properties】按钮;

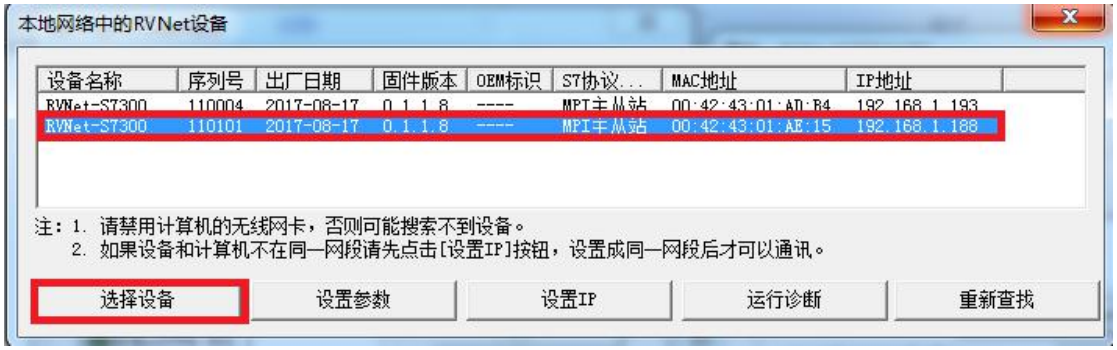


注意：如果 RVNet-S7 模块插在 PLC 的 MPI 口，【Interface Parameter Assignment】设置为 RVNetS7PD.MPI.1；如果 RVNet-S7 模块插在 PLC 的 PROFIBUS 口，【Interface Parameter Assignment】设置为 RVNetS7PD.PROFIBUS.1。

3.如果知道 RVNet 的 IP 地址，在【RVNet 模块的 IP 地址或域名】中直接输入 RVNet 的 IP 地址，点击【确定】按钮；

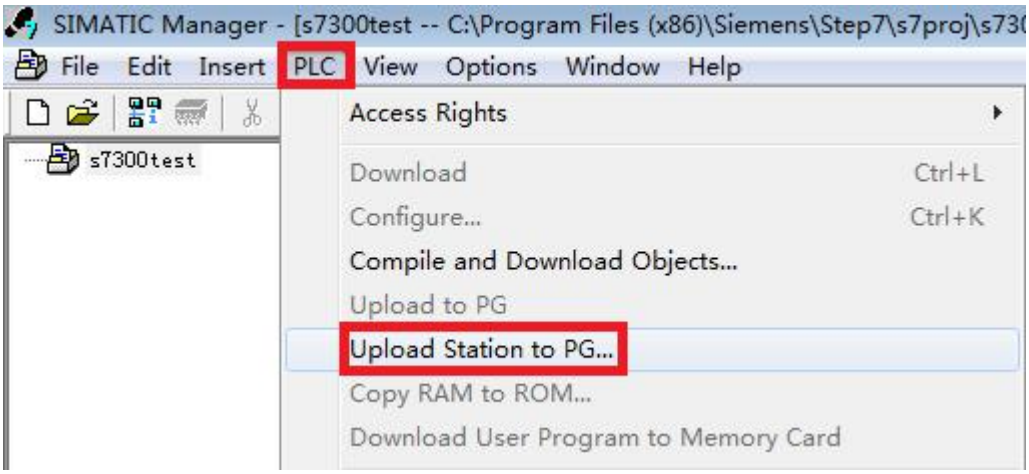
如果不知道 RVNet 的 IP 地址，可以点击【查找本地的 RVNet 模块】，选择要连接的 RVNet 模块，点击【选择设备】按钮。



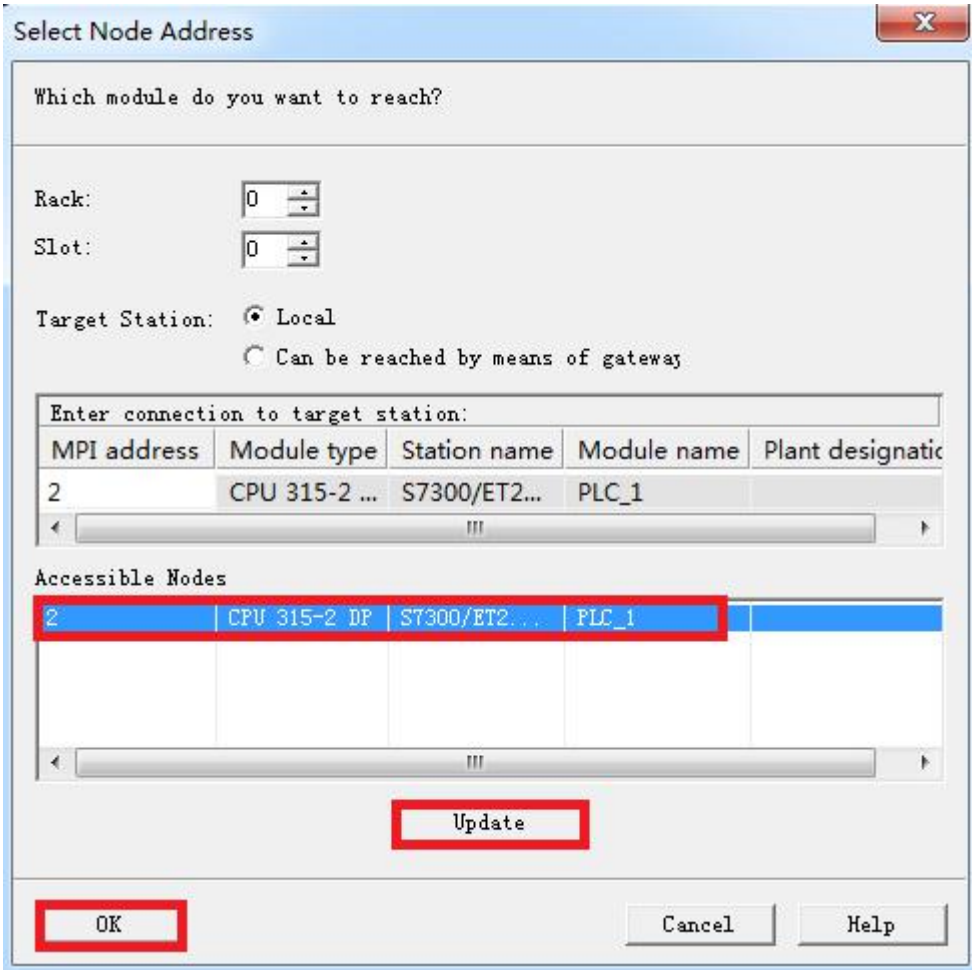


上载程序：

1.选择菜单栏的【PLC】，点击【Upload Station to PG...】；



2.在弹出的对话框中，点击【Update】按钮，选中要连接的 PLC 节点，点击【OK】按钮。



5.4 博途编程调试

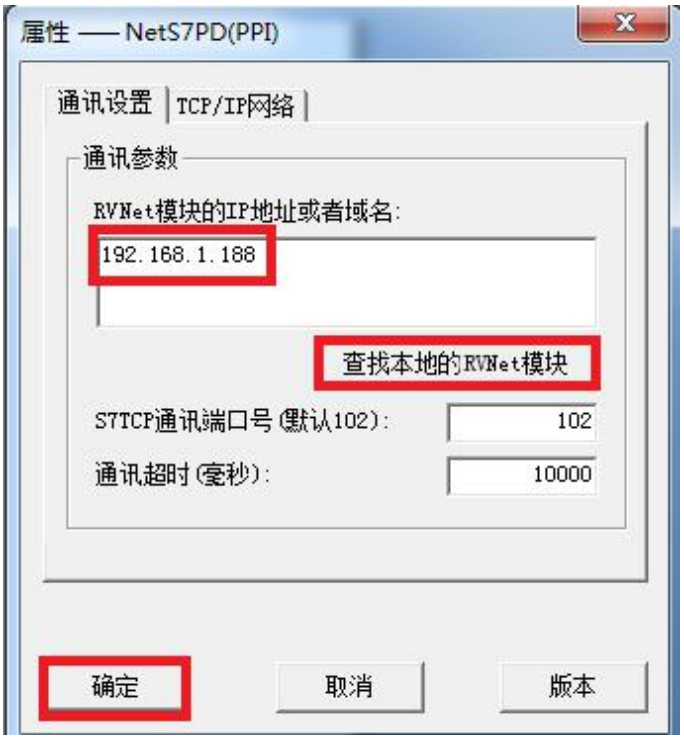
首先应设置好 PG/PC 接口参数：

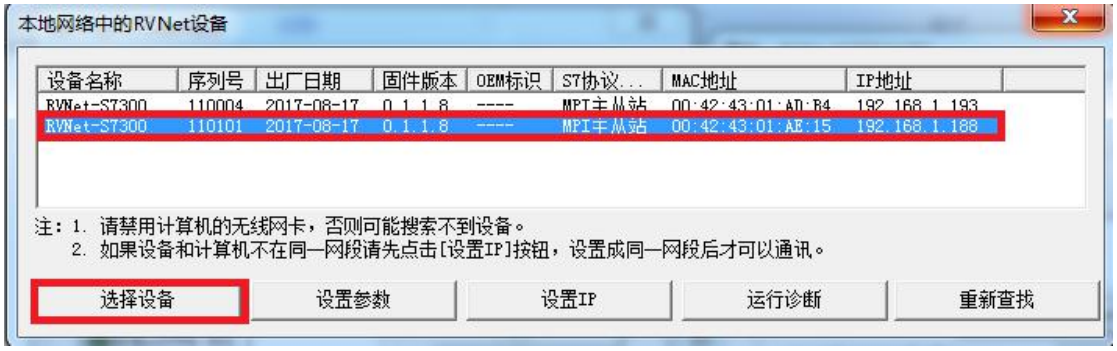
1.打开控制面板中的【设置 PG/PC 接口】图标；

2. 【为使用的接口分配参数】设置为 RVNetS7PD.MPI.1，【应用程序访问点】设置为 S7ONLINE（STEP7）—> RVNetS7PD.MPI.1，点击【属性】按钮；

3. 如果知道 RVNet 的 IP 地址，在【RVNet 模块的 IP 地址或域名】中直接输入 RVNet 的 IP 地址，点击【确定】按钮；

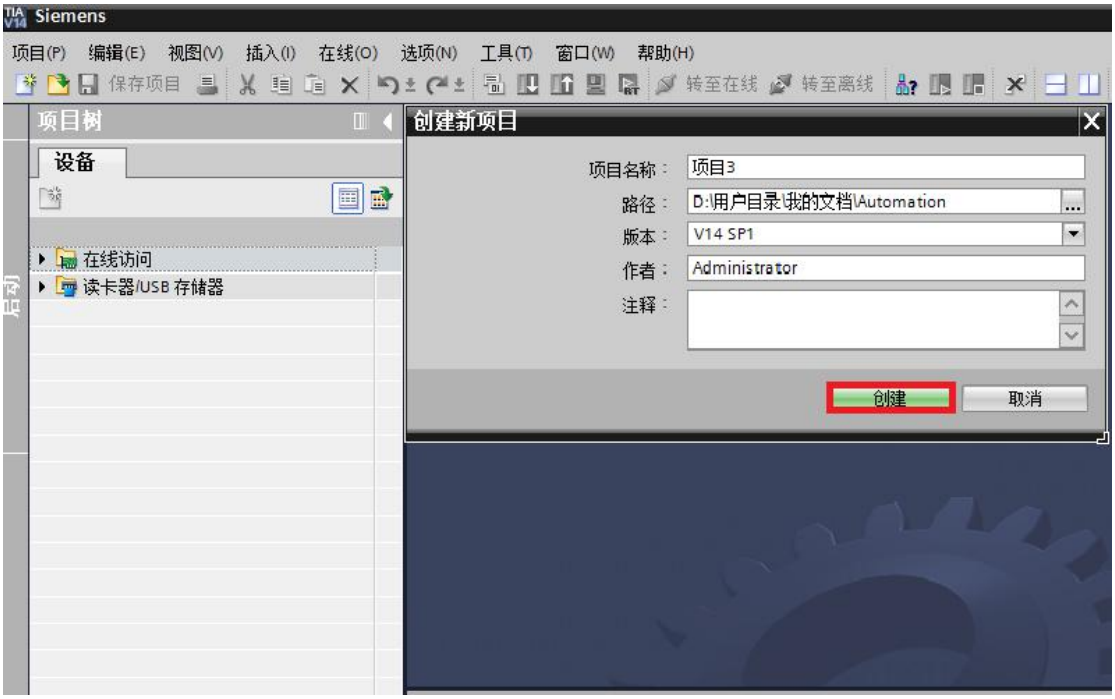
如果不知道 RVNet 的 IP 地址，可以点击【查找本地的 RVNet 模块】，选择要连接的 RVNet 模块，点击【选择设备】按钮。



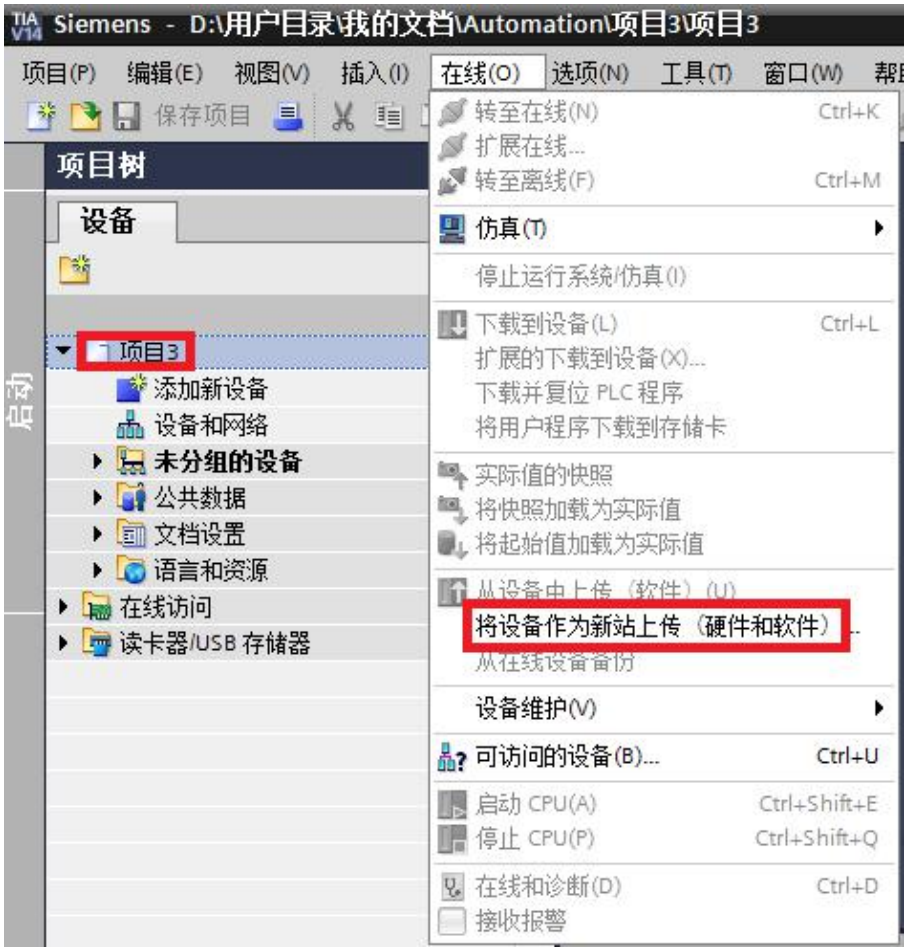


注意：如果 RVNet 插在 PLC 的 MPI 接口，请在 PG/PC 接口选择 NetS7PD.MPI.1,并在其属性参数里设置好 RVNet 的 IP 地址；如果 RVNet 插在 PLC 的 PROFIBUS 接口，请在 PG/PC 接口选 NetS7PD.PROFIBUS.1,并在其属性参数里设置好 RVNet 的 IP 地址；

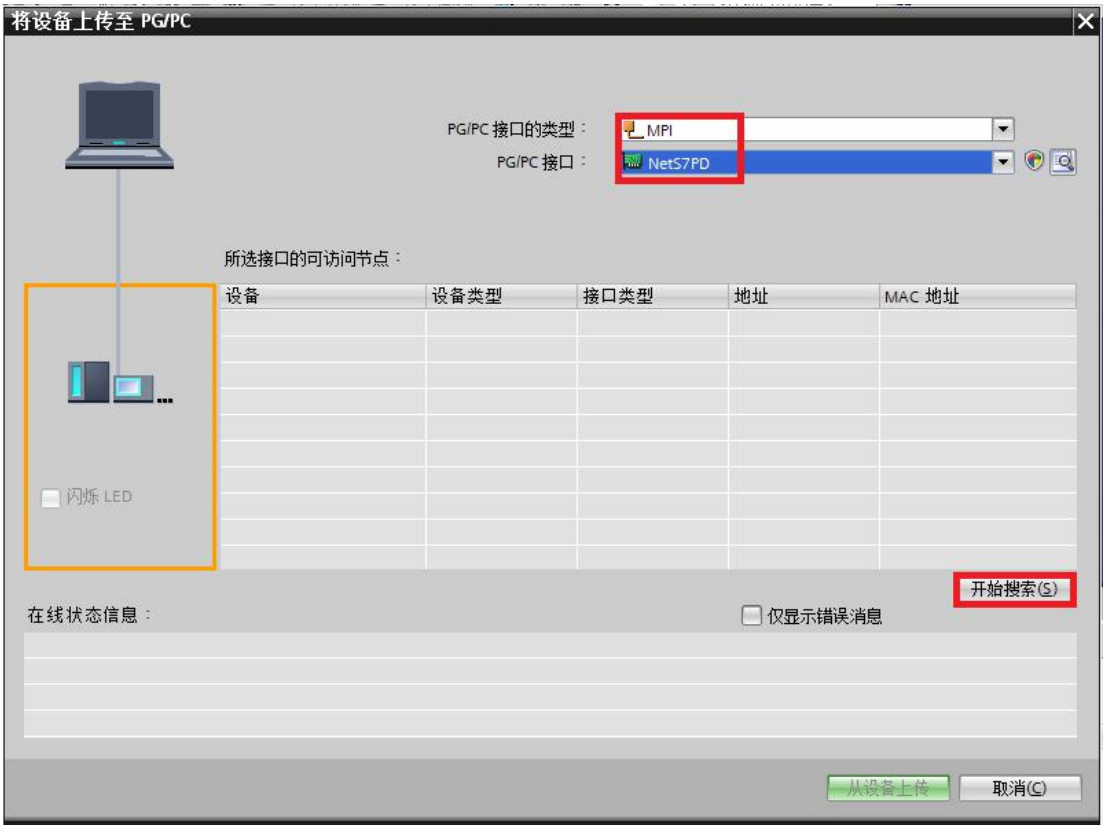
1.以【项目视图】打开博途软件，并新建项目；



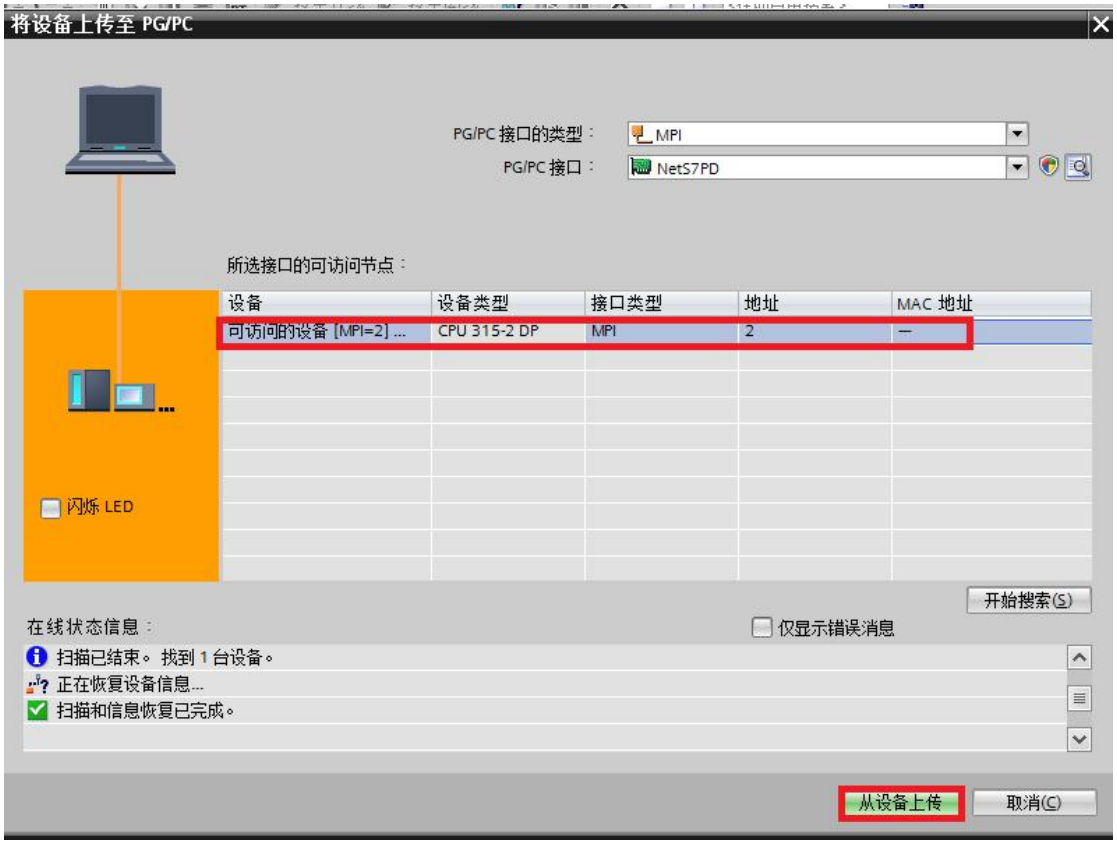
2.选中【项目 3】，选择菜单栏的【在线】，点击【将设备作为新站上传（硬件和软件）】；



3.【PG/PC 接口的类型】选择 MPI，【PG/PC 接口】选择 RVNetS7PD，点击【开始搜索】按钮；



4.选中搜索到的 PLC，点击【从设备上传】按钮，可以上载 PLC 的程序。



6.SCADA 以太网通讯

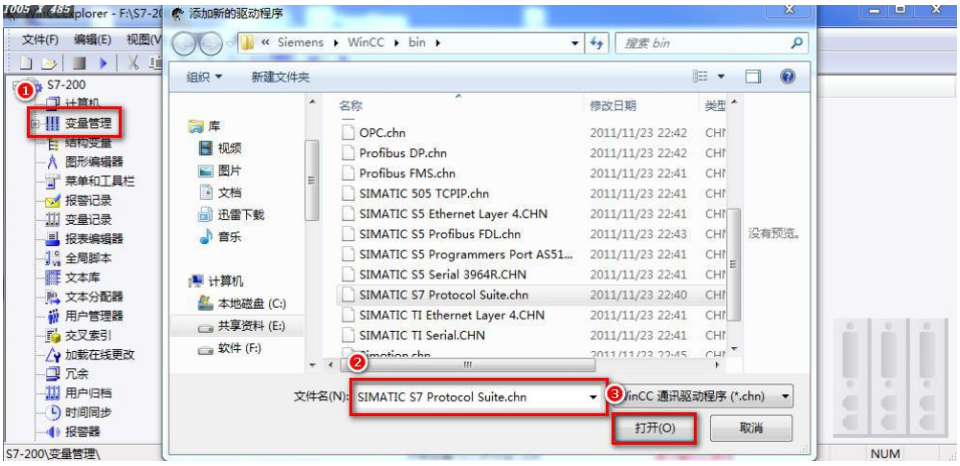
6.1WINCC 通讯

6.1.1 连接 S7200

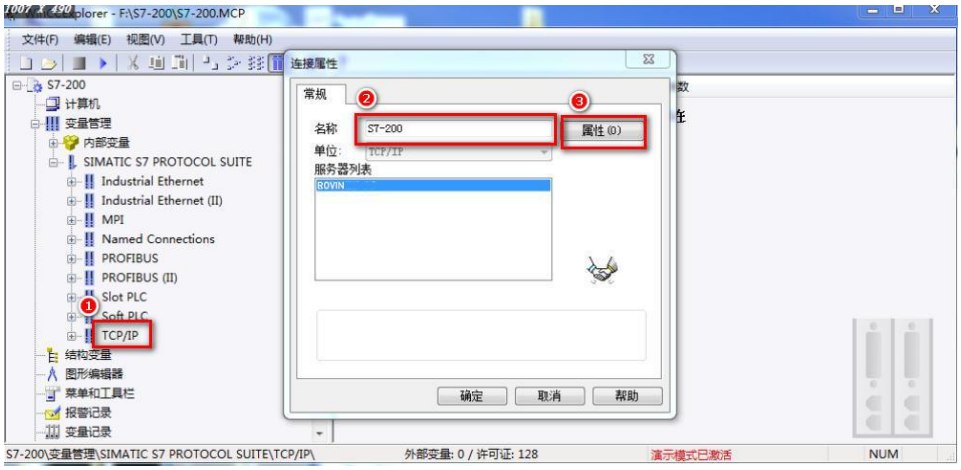
西门子 S7-200 采用 RVNet-S7200 连接 WINCC，可以采用：WINCC 的 TCP 驱动、OPC 驱动。

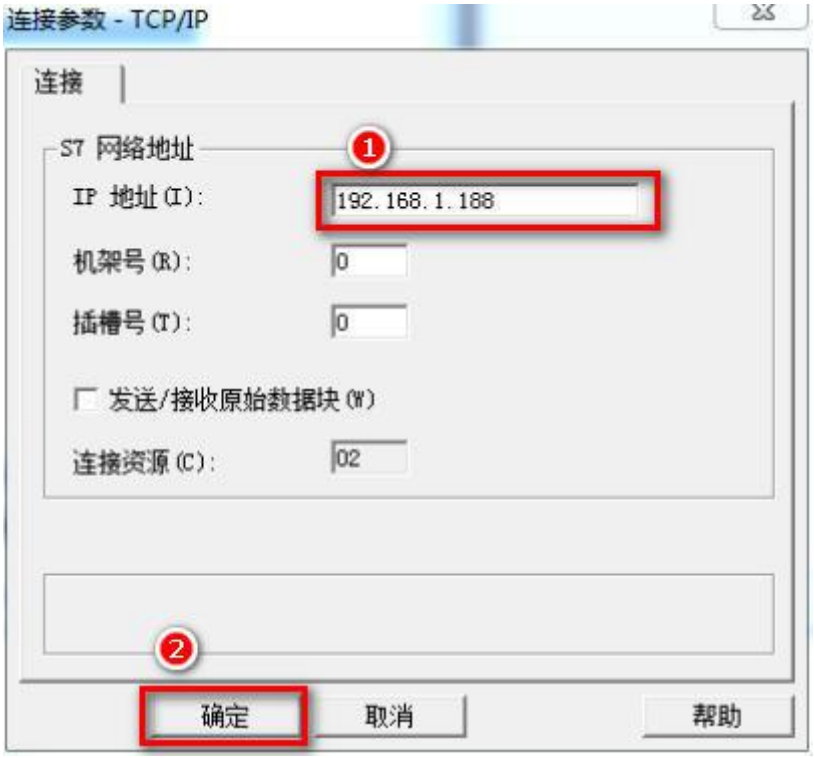
6.1.1.1 采用 WINCC 自带的 TCP/IP 驱动

1、 打开 WINCC 软件，新建一个项目，右击【变量管理】，选择【添加新的驱动程序】，选择【SIMATIC S7 Protocol Suite.chn】文件；



2、 右击【TCP/IP】连接，选择【新驱动程序的连接】，定义一个连接名，点击【属性】，在【IP 地址】处填入 RVNet-S7200 的 IP 地址，点击【确定】;





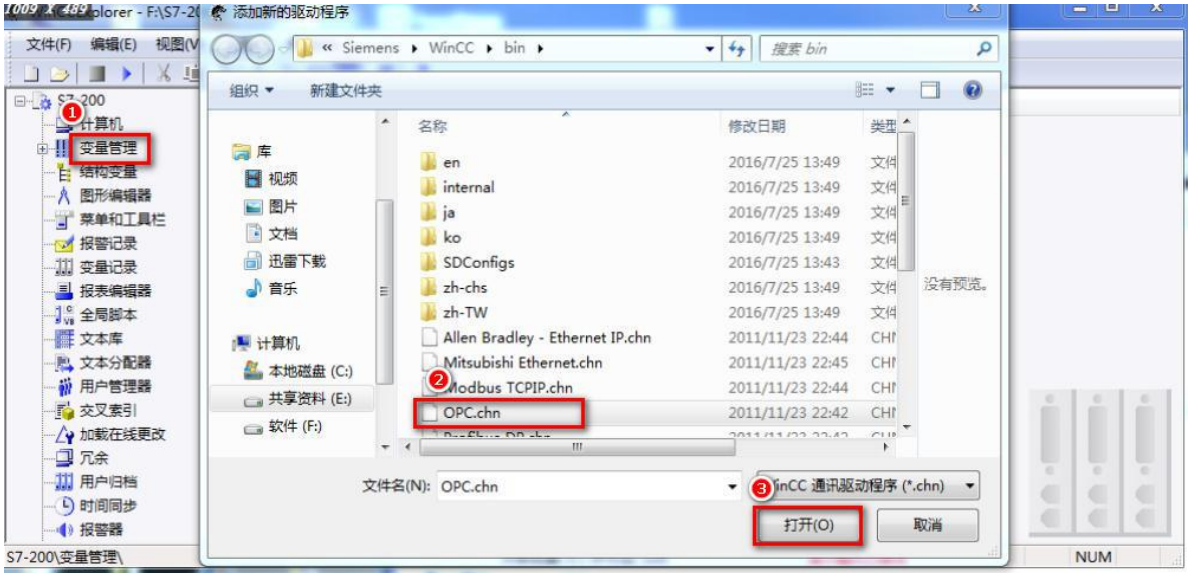
3、右击工程栏【变量管理】组下的 【TCP/IP】连接，选择【系统参数】，在【单位】选项中的【逻辑设备名称(D)】中选择“TCP/IP->（计算机网卡）”。

注意：

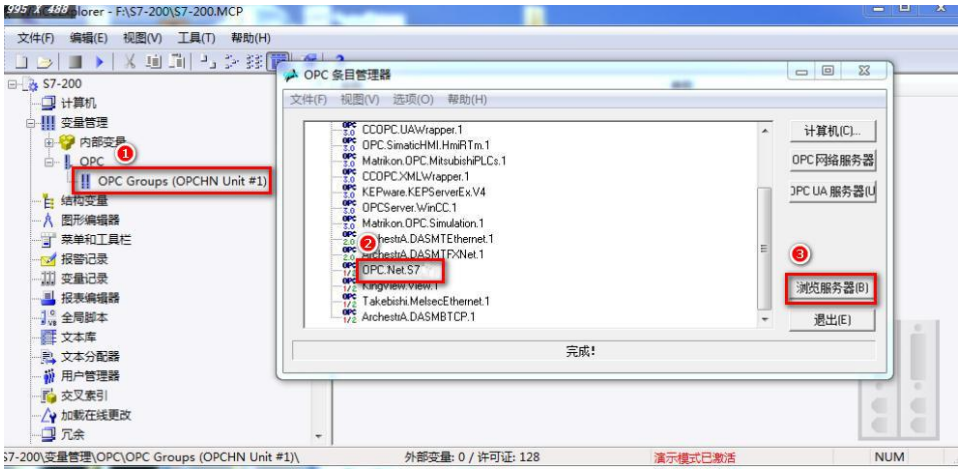
不要选带 auto 的网卡。

6.1.1.2 采用 RVNetS7OPC 服务器

1、 打开 WINCC 软件，新建一个项目；右击【变量管理】，选择【添加新的驱动程序】，选择【OPC.chn】文件，如下图：

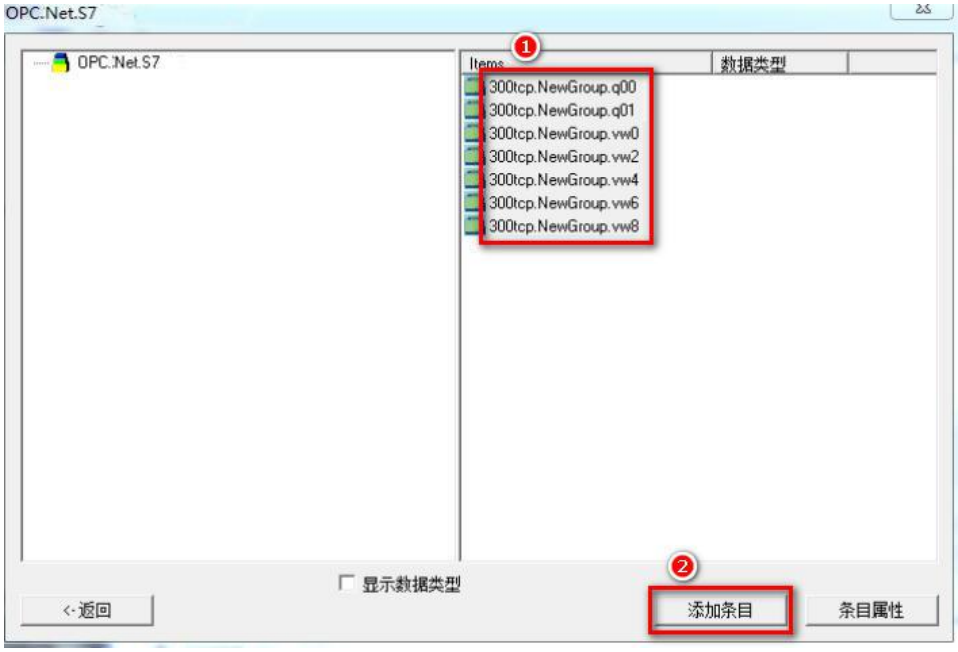


2、右击【OPC Groups】，选择【系统参数】，打开【OPC 条目管理器】， 选择【OPC.RVNet.S7】，



3、点击【浏览服务器】，弹出如下窗口，将【读访问】与【写访问】都打上勾；

4、点击【下一步】，搜索 OPC 服务器内部的变量，全选变量，点击【添加条目】，将变量添加到 WINCC 中。

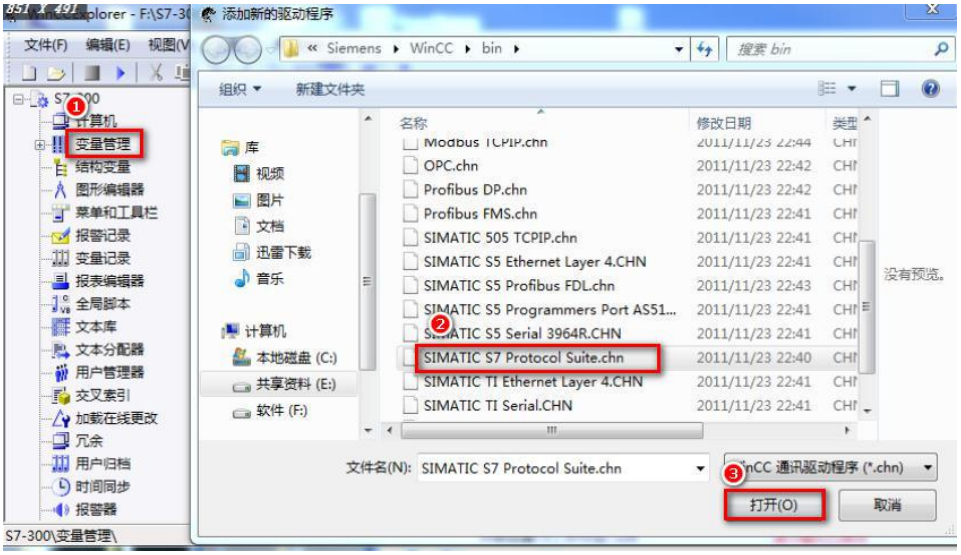


6.1.2 连接 S7300

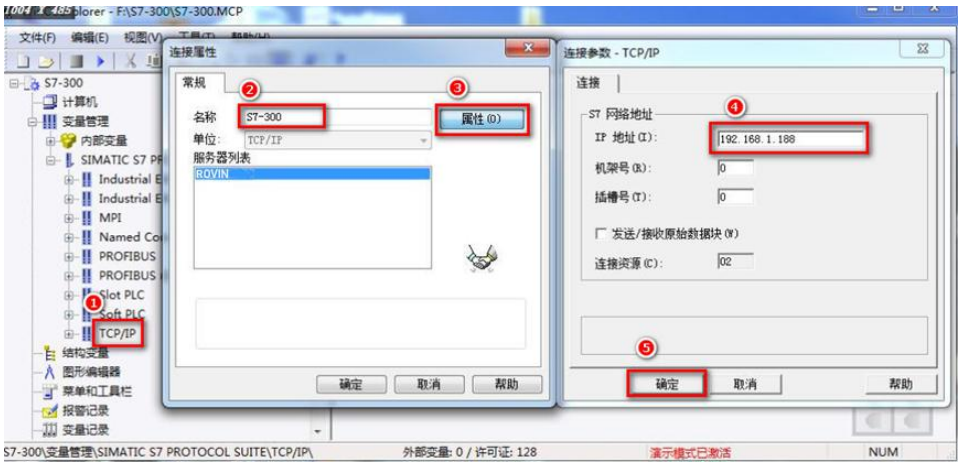
西门子S7-300/400 采用RVNet-S7300 连接WINCC，可以采用：WINCC的TCP驱动、OPC驱动。

6.1.2.1 采用 WINCC 自带的 TCP/IP 驱动

1、新建 WINCC 项目，选中项目的【变量管理】，点击鼠标右击，选择快捷菜单【添加新的驱动程序】，在弹出的对话框中选择【SIMATIC S7 PROTOCOL SUITE】;



2、右击【TCP/IP】，选择【新驱动程序的链接】。在弹出的连接属性对话框输入连接名字，点击【属性】按钮，在弹出的属性对话框中的【IP 地址】设置为 RVNet-S7300 的 IP 地址；



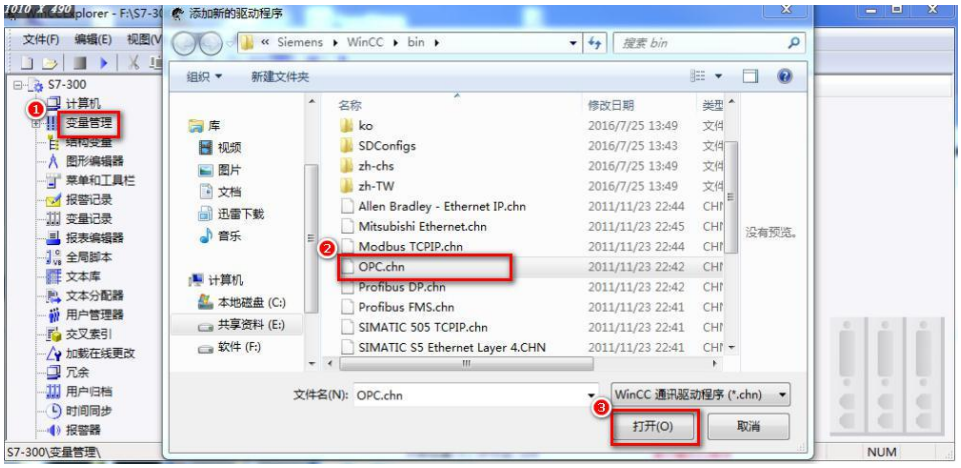
3、 右击【TCP/IP】，选择【系统参数】，在【单元】属性页中的【逻辑设备名称】设置为“TCP/IP->（计算机网卡）”。

注意：

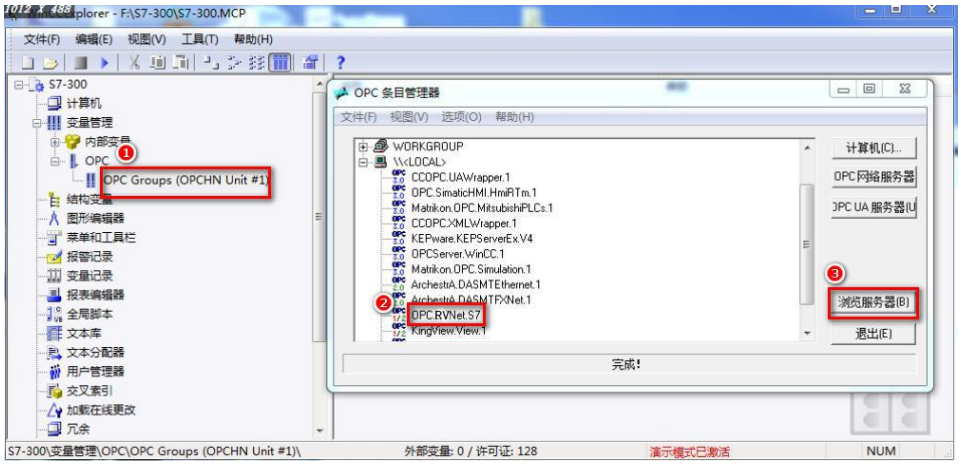
不要选带 auto 的网卡。

6.1.2.2 采用 RVNetS7OPC

1、打开 WINCC 软件，新建一个项目；右击【变量管理】，选择【添加新的驱动程序】，选择【OPC.chn】；



2、右击【OPC Groups】，选择【系统参数】，打开【OPC 条目管理器】，选择【OPC.RVNet.S7】，点击【浏览服务器】；



3、在弹出的对话框中，将【读访问】和【写访问】的勾打上；

4、点击【下一步】，搜索 OPC 服务器变量，全选变量，点击【添加条目】，将变量添加到 WINCC 中；

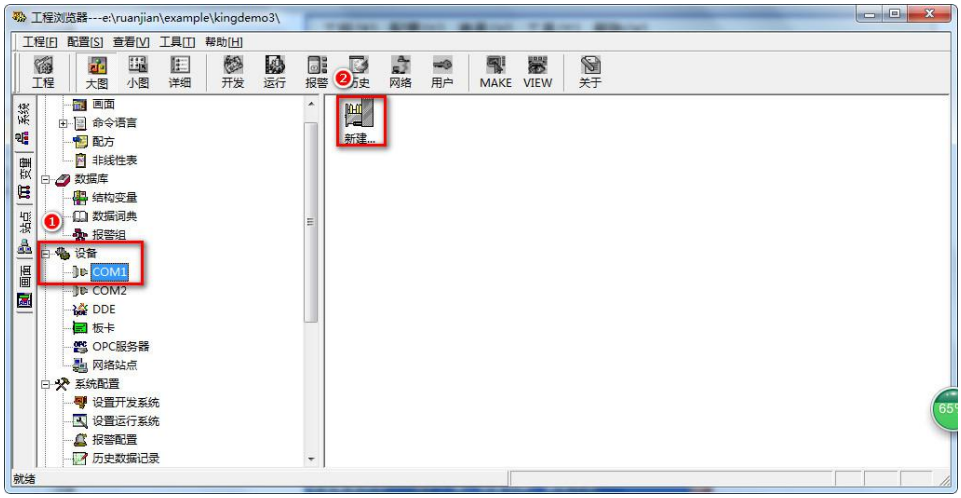
6.2 组态王通讯

6.2.1 连接 S7200

西门子 S7-200 通过 RVNet-S7200 连接组态王，可以采用：西门子 S7TCP 驱动、OPC 驱动。

6.2.1.1 采用 S7TCP 驱动

1、打开组态王软件，鼠标单击 开发 打开组态王工程浏览器——设备（COM1），双击右侧【新建】;

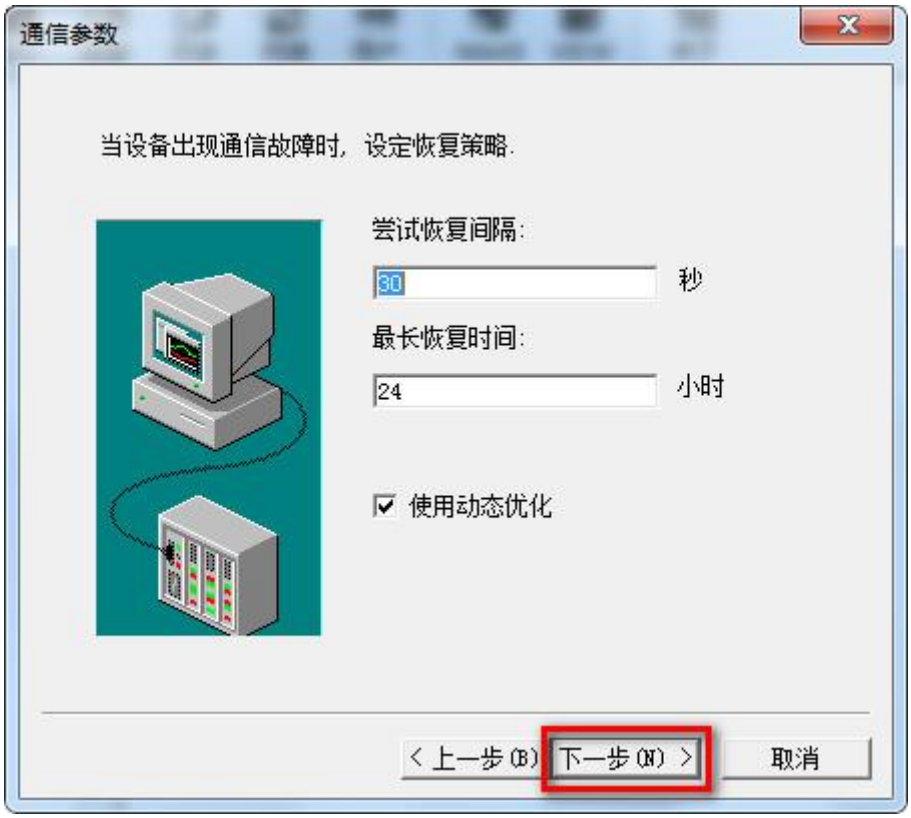


2、打开 PLC 分组，然后打开西门子分组，选择 S7-200 系列(TCP)下的 TCP 驱动

3、填入设备名称，点击【下一步】;

4、填入 RVNet-S7200 的 IP 地址：CPU 槽号（默认为 0）；例如 192.168.1.188:0；

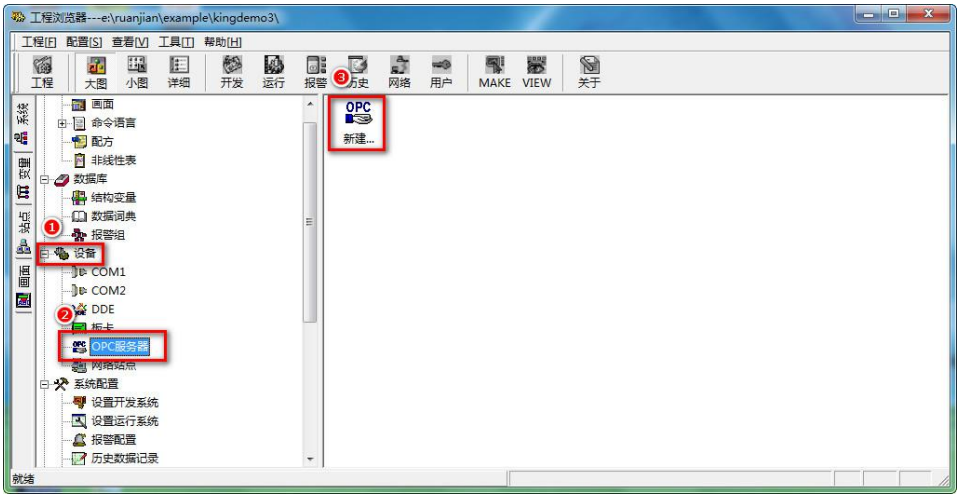
5、根据向导默认参数，点击【下一步】；



6、 完成参数设置。

6.2.1.2 采用 RVNetS7OPC

1、打开组态王软件，鼠标单击 开发 打开组态王工程浏览器——设备（OPC 服务器），双击右侧“新建”



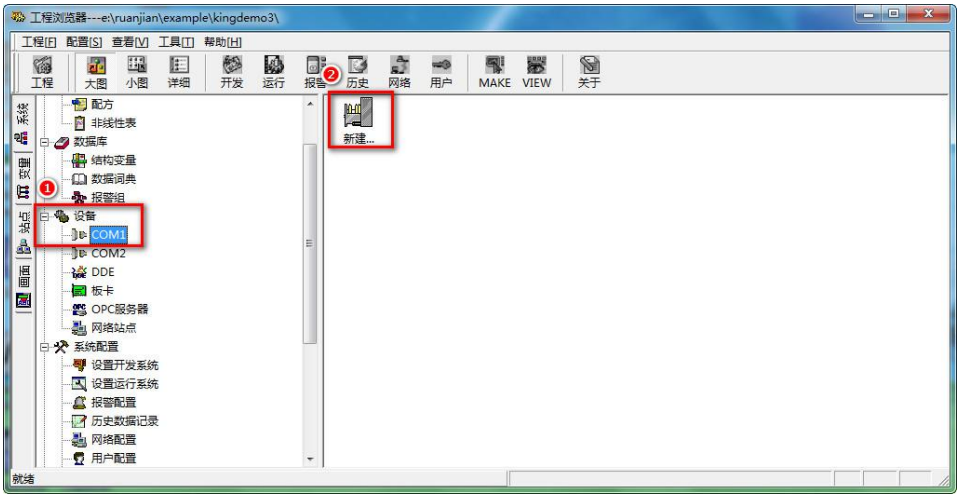
2、选择“OPC.RVNet.S7”,确定

6.2.2 连接 S7300

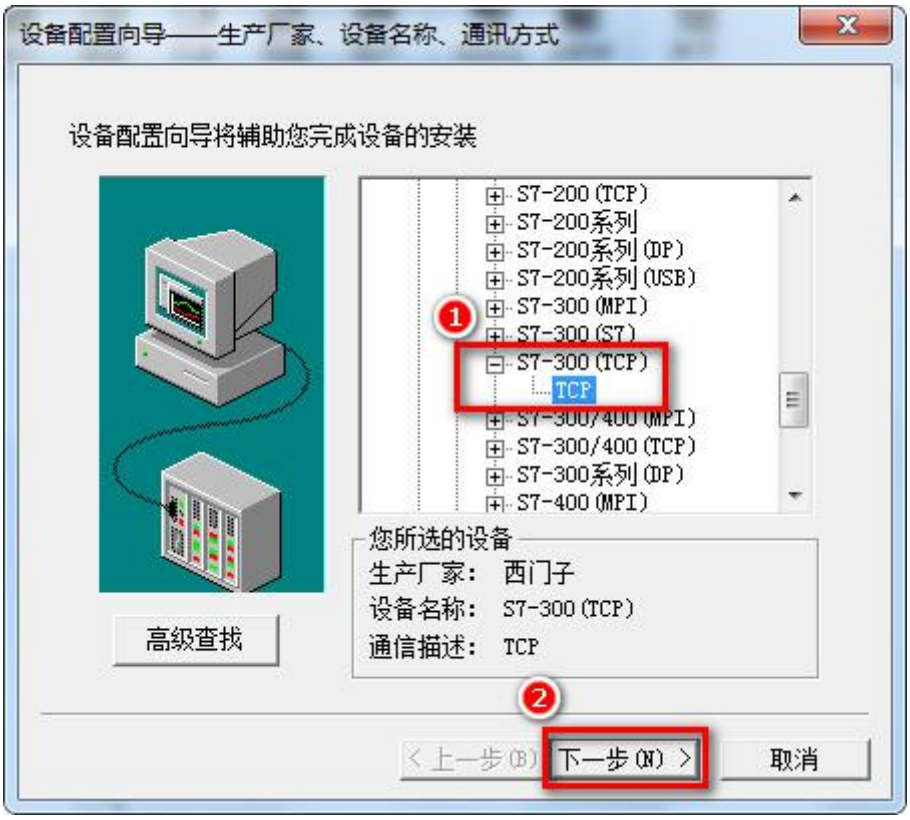
西门子S7-300/400 采用RVNet-S7300 连接组态王，可以采用：S7TCP驱动、OPC驱动。

6.2.2.1 采用 S7TCP 驱动

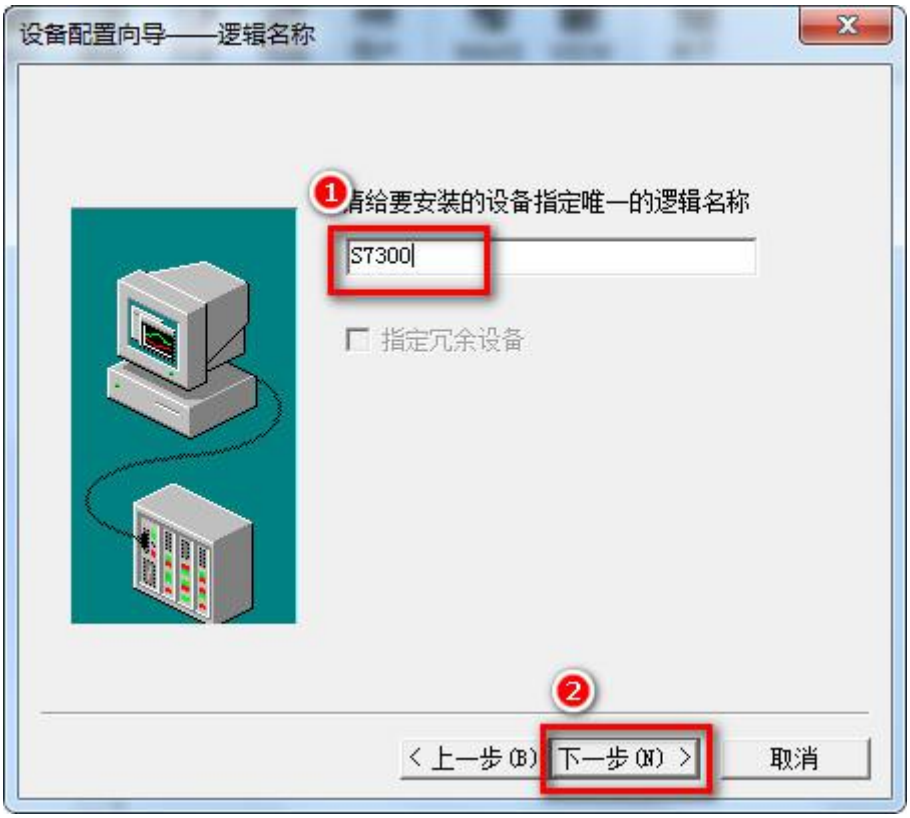
1、打开组态王工程浏览器——设备（COM1），双击右侧“新建”



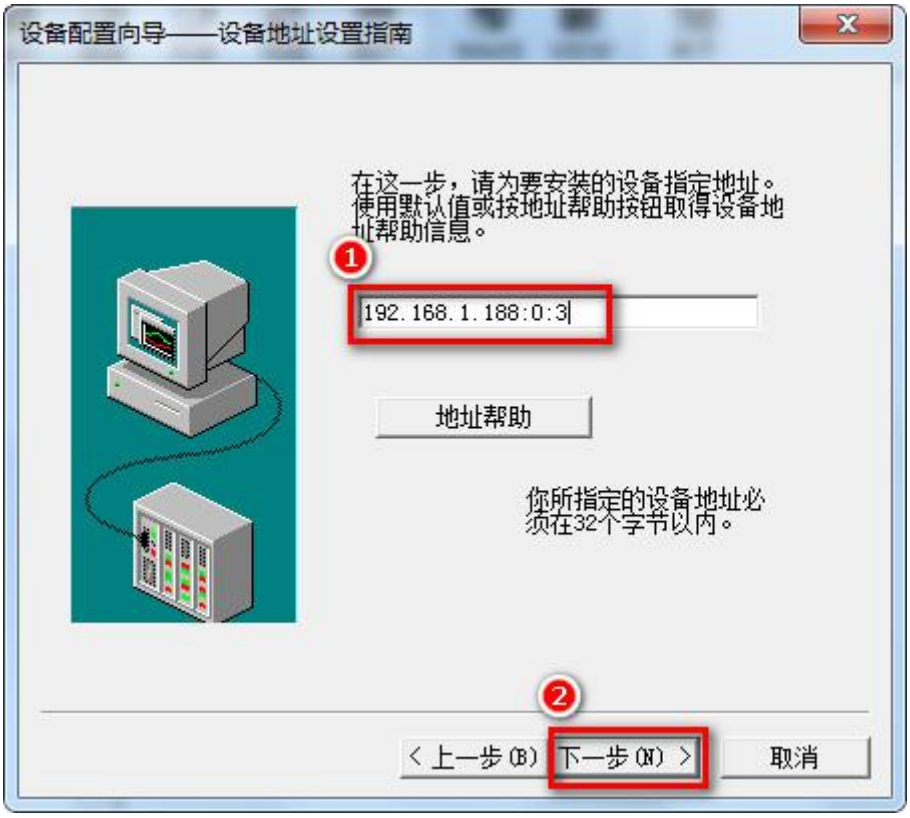
2、选择西门子 S7-300 系列 TCP 驱动，点击【下一步】;



3、填入设备名称；



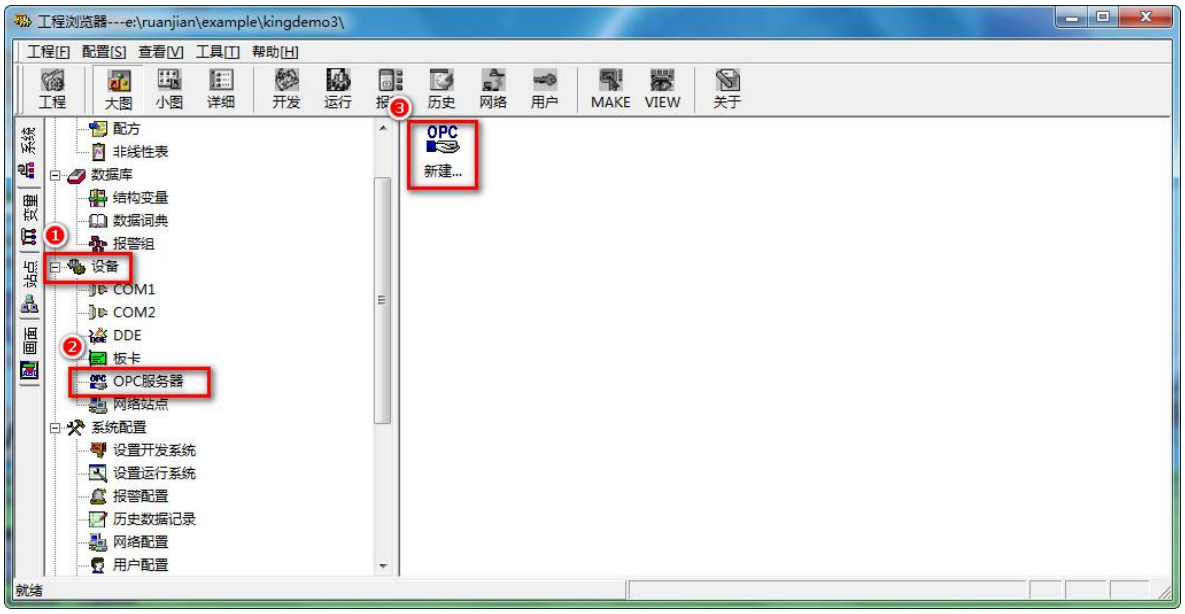
4、填入 RVNet-S7300 的 IP 地址：CPU 机架号：CPU 槽号（默认为 3）；



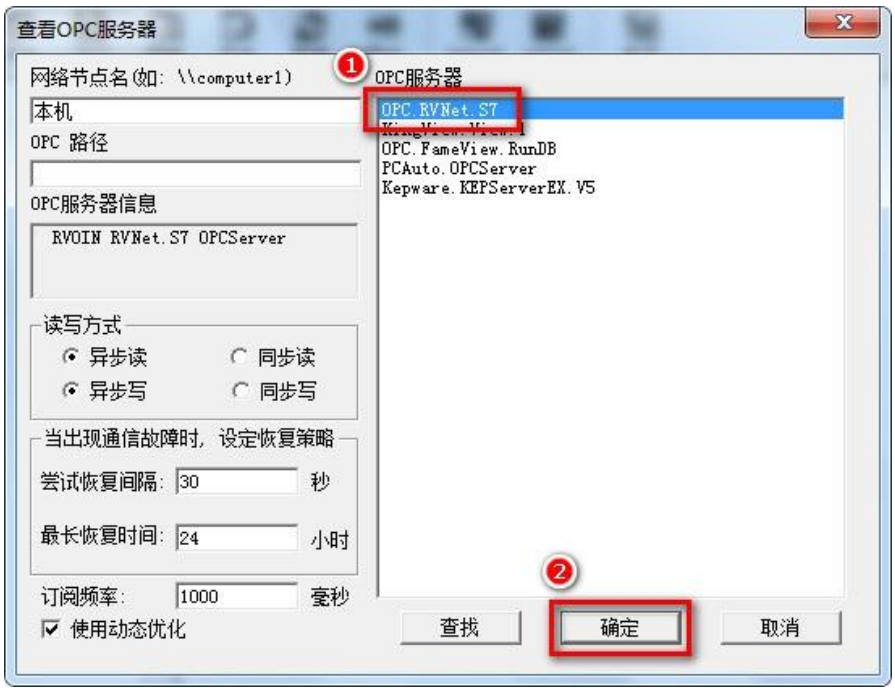
6、完成参数设置

6.2.2.2 采用 RVNetS7OPC

1、打开组态王工程浏览器——设备（OPC 服务器），双击右侧【新建】;



2、选择【OPC.RVNet.S7】,确定



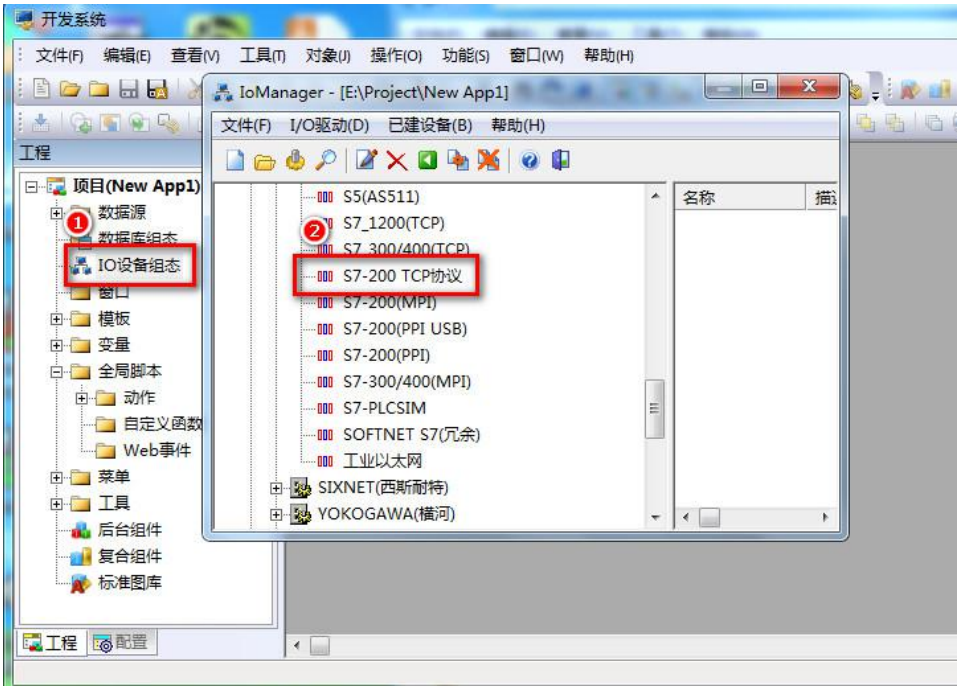
6.3 力控通讯

6.3.1 连接 S7200

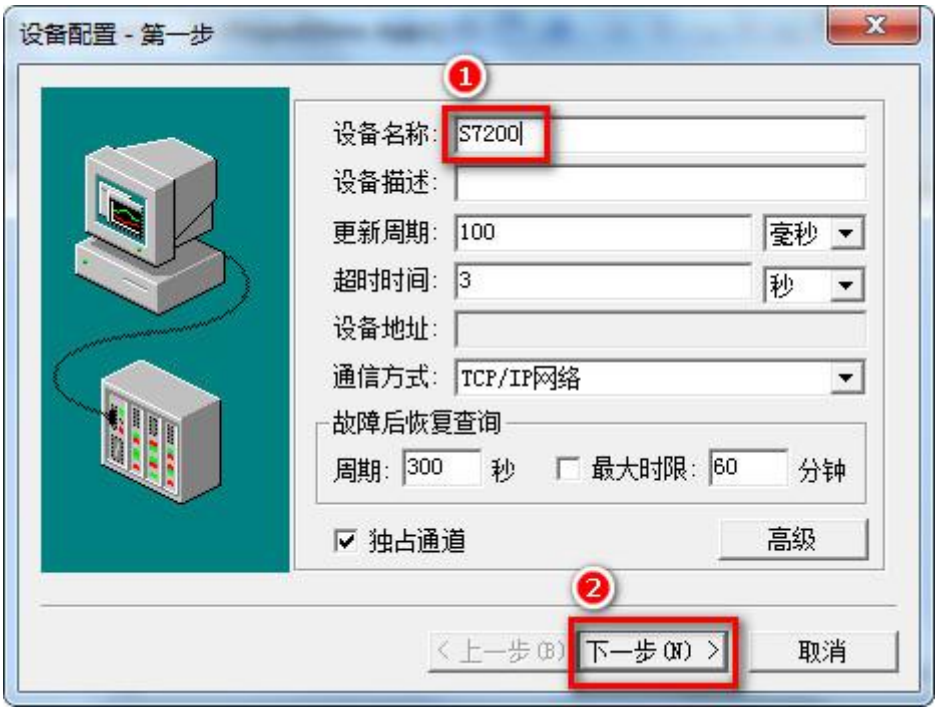
西门子 S7-200 通过 RVNet-S7200 连接 ForceControl，可以采用：西门子 S7TCP 驱动、OPC 驱动。

6.3.1.1 采用 S7TCP 驱动

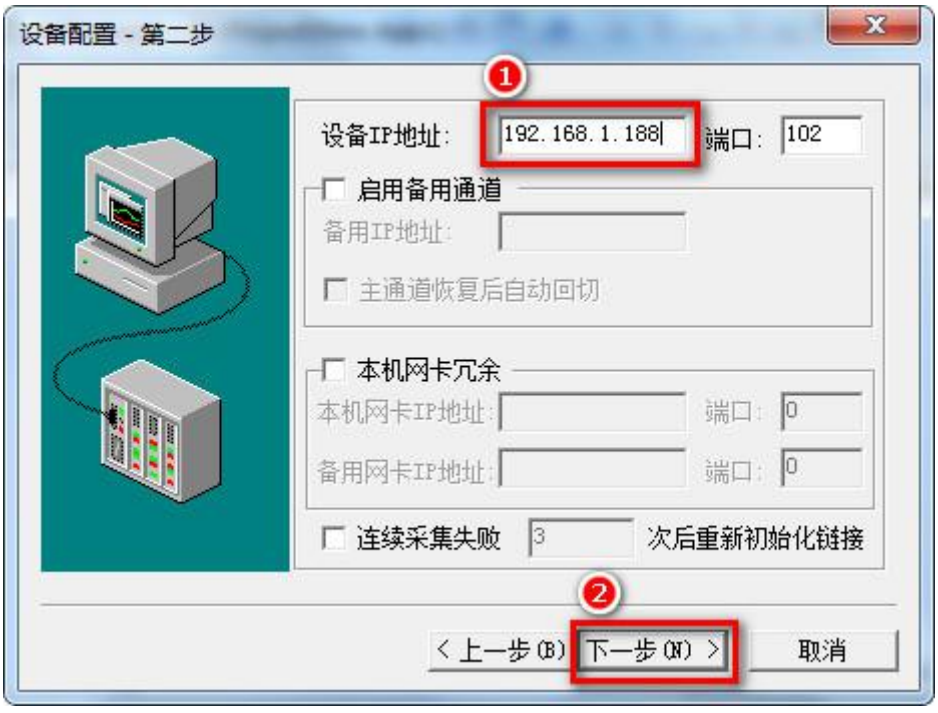
1、打开力控开发系统——IO 设备组态，选择【PLC-SIEMENS（西门子）—S7-200 TCP 协议】;



2、填入设备名称，点击【下一步】;

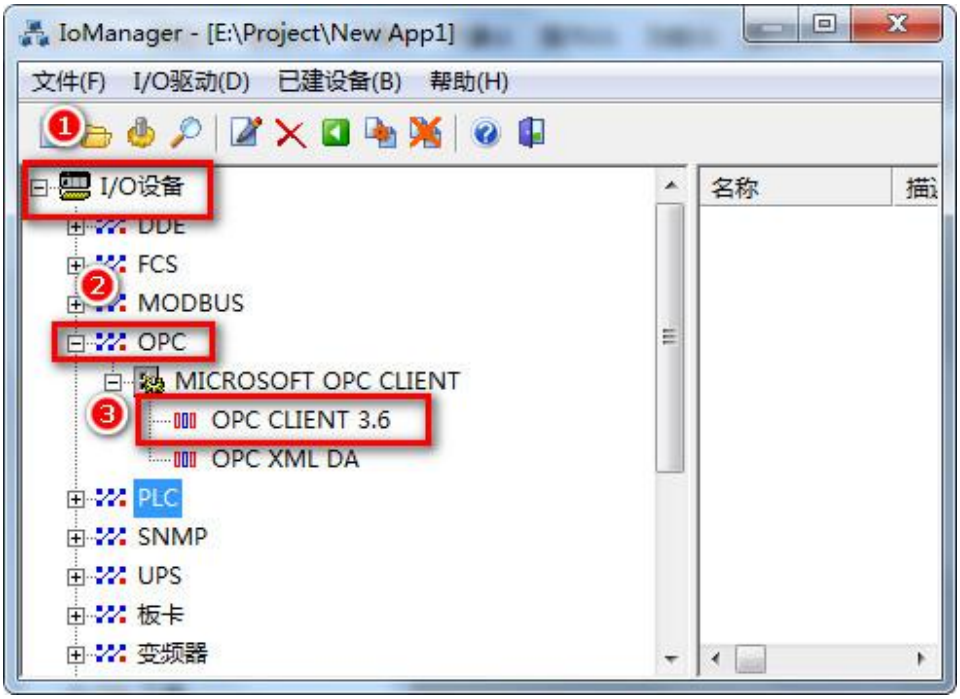


3、填入 RVNet-S7200 的 IP 地址，端口（默认为 102），完成设置。



6.3.1.2 采用 RVNetS7OPC

1、打开力控开发系统——IO 设备组态，选择【OPC—MICROSOFT OPC CLIENT—OPC CLIENT 3.6】;



2、填入设备名称，点击【下一步】;

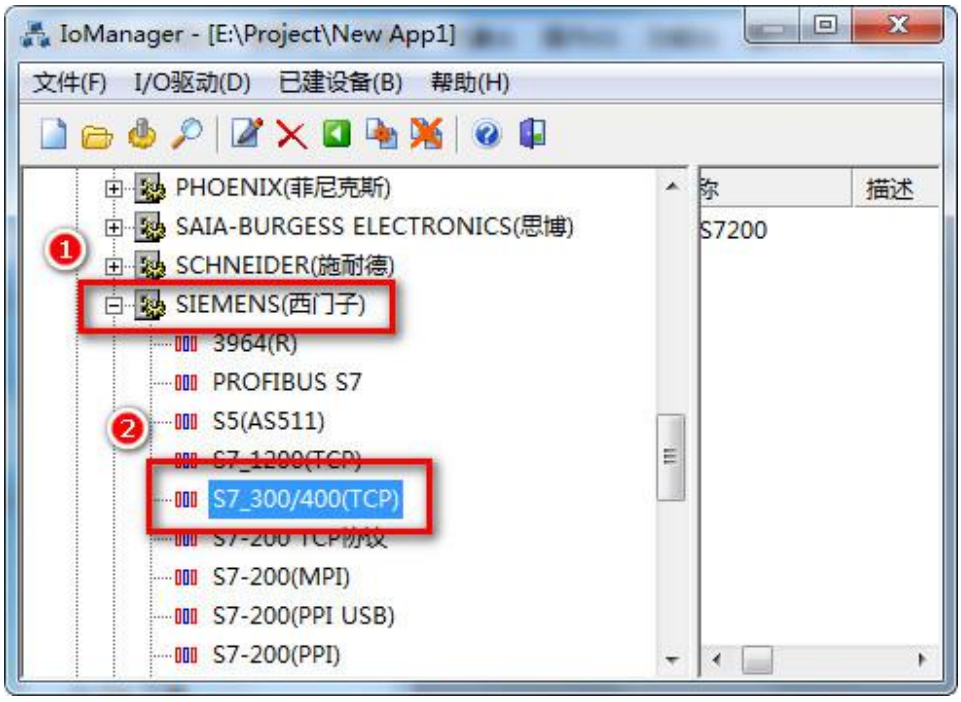
3、选择【OPC.RVNet.S7】，点击完成。

6.3.2 连接 S7300

西门子 S7-300/400 采用 RVNet-S7300 连接 ForceControl，可以采用：S7TCP 驱动、OPC 驱动。

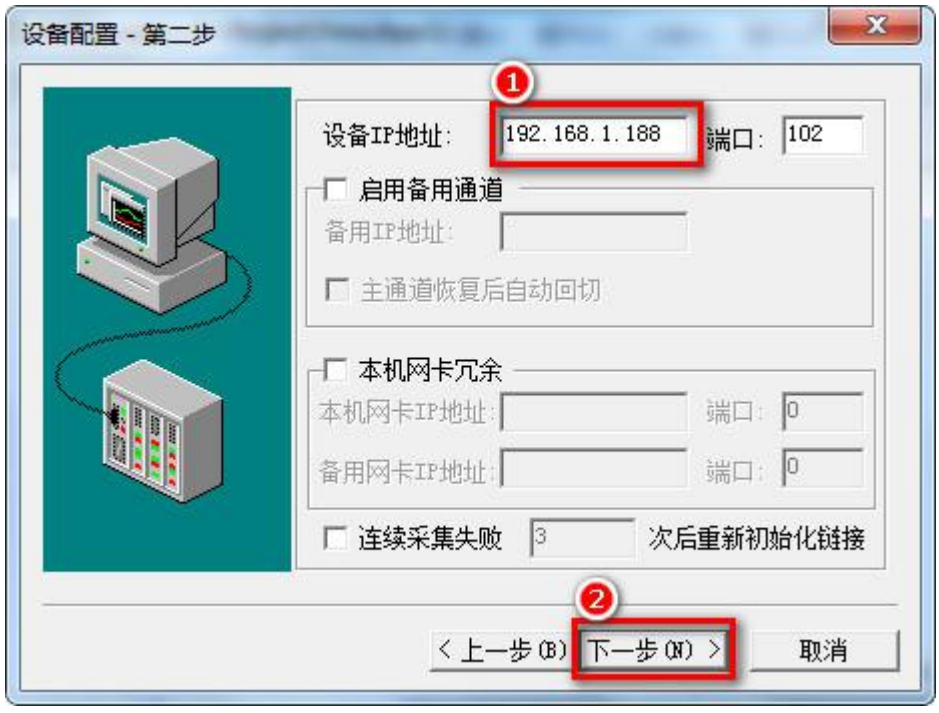
6.3.2.1 采用 S7TCP 驱动

1、打开力控开发系统——IO 设备组态，选择【PLC-SIEMENS（西门子）—S7 系列 TCP 协议】；



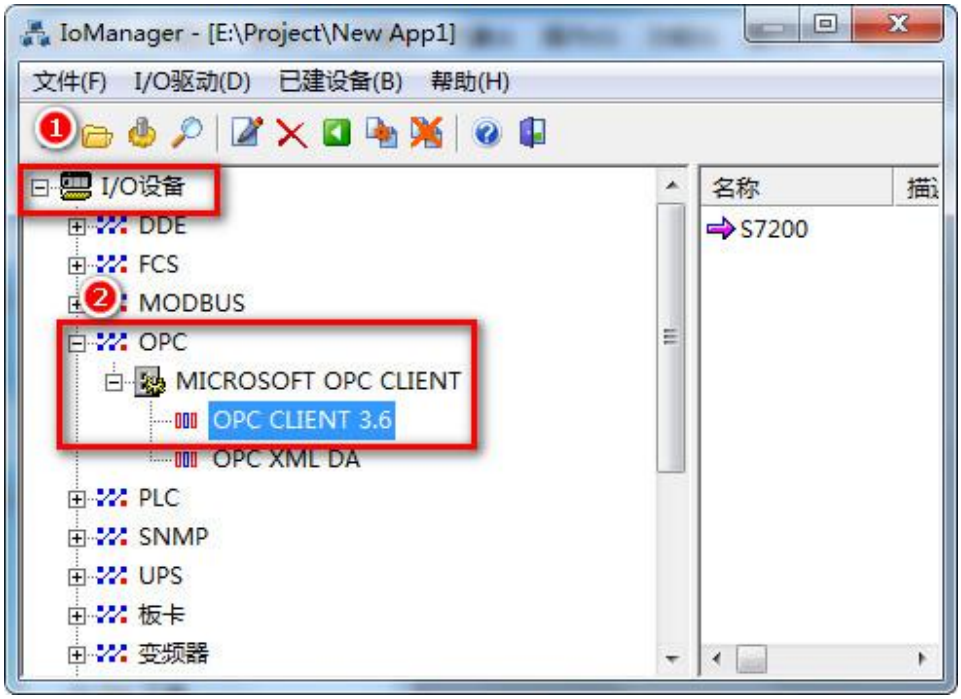
2、填入设备名称，点击【下一步】;

3、填入 RVNet-S7300 的 IP 地址，端口（默认为 102），完成设置。



6.3.2.2 采用 RVNetS7OPC

1、打开力控开发系统——IO 设备组态，选择【OPC—MICROSOFT OPC CLIENT—OPC CLIENT 3.6】;



1、 填入设备名称，点击【下一步】;

2、 选择【OPC.RVNet.S7】，完成设置。

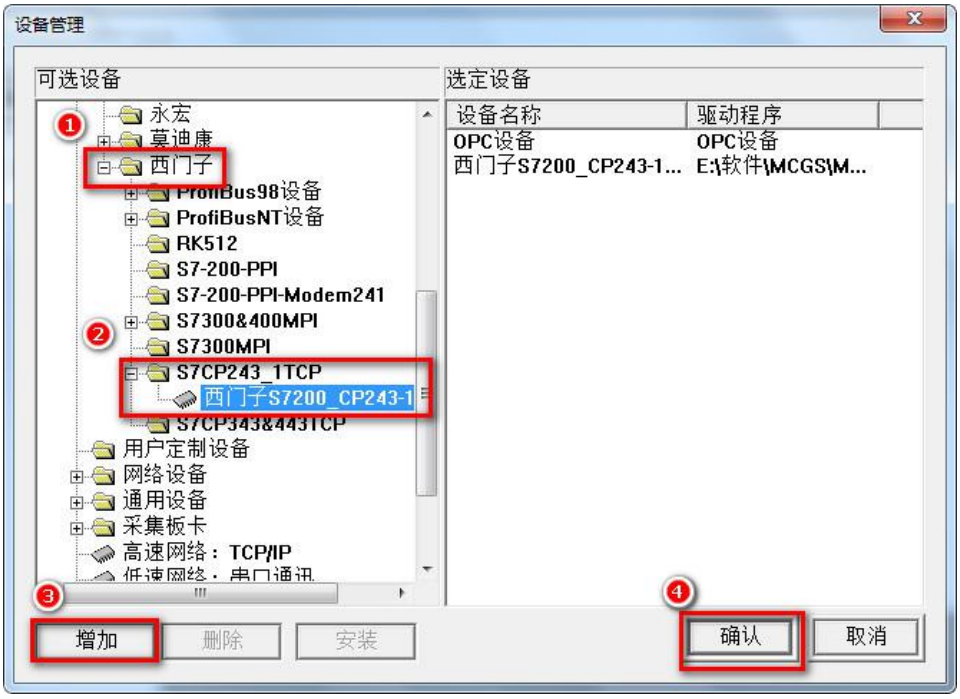
6.4MCGS 通讯

6.4.1 连接 S7200

西门子 S7-200 通过 RVNet-S7200 连接 MCGS，可以采用：西门子 S7TCP 驱动、OPC 驱动。

6.4.1.1 采用 S7TCP 驱动

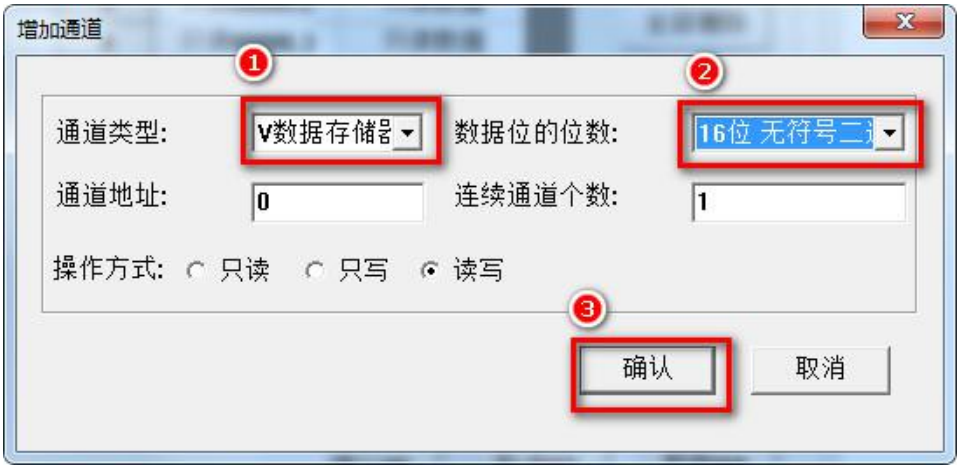
1、打开昆仑通态 MCGS 组态环境——设备窗口，选择【PLC-西门子-S7CP243_1TCP】;



2、在设备属性设置中，将计算机的 IP 地址填入【本地 IP 地址】，RVNet-S7200 的 IP 地址填入【远

端 IP 地址】,【远端端口号】填入 102；

3.点击【设置设备内部属性】进行变量的新建；

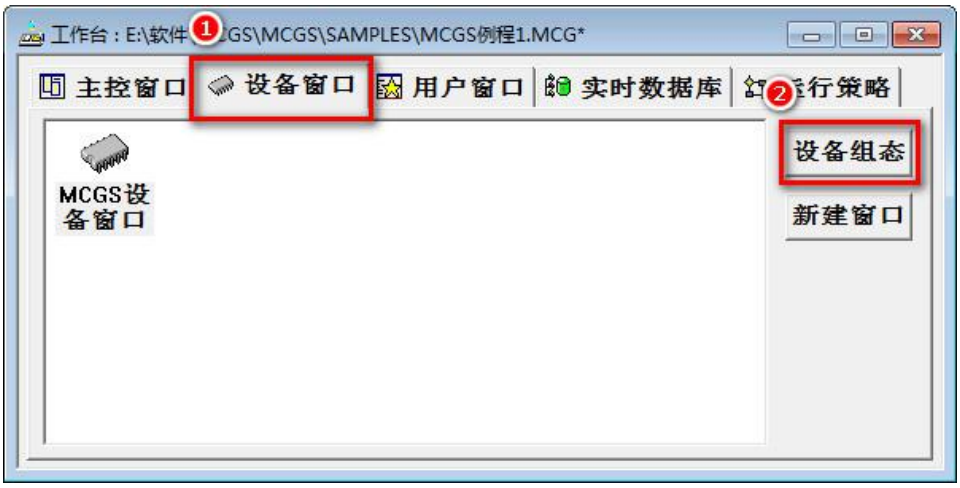


4、新建变量后点击【快速连接变量】;

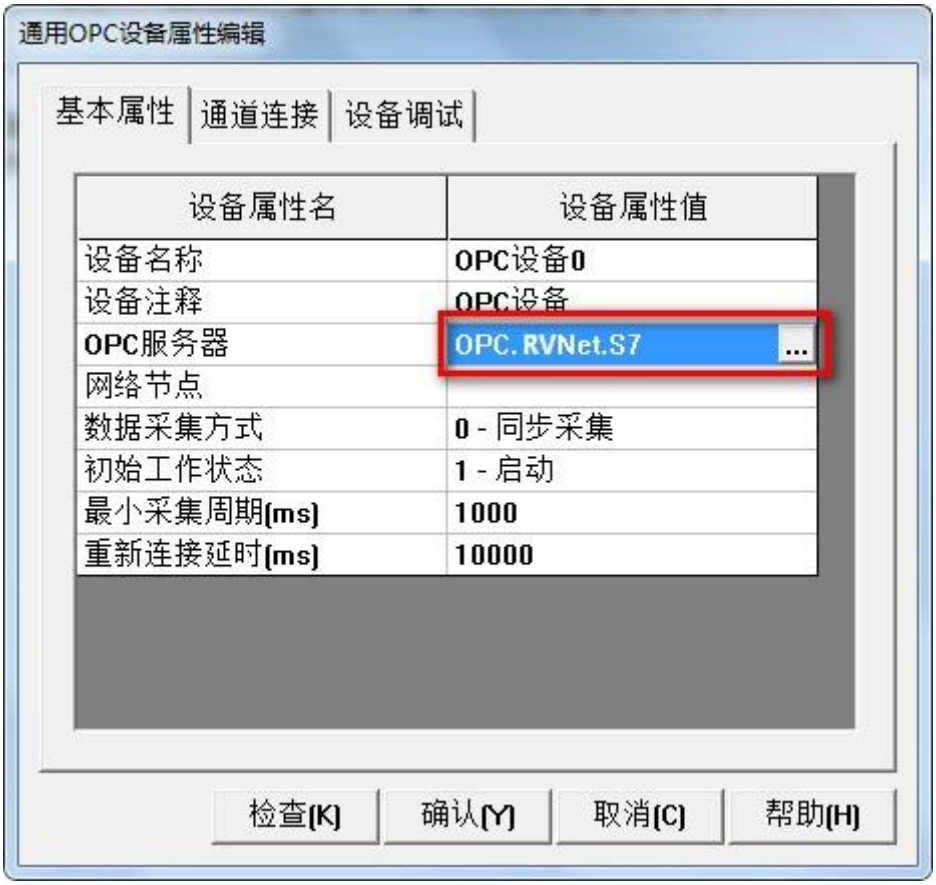
3、 再点击【设备调试】，进行变量的监视；

6.4.1.2 采用 RVNetS7OPC

1、打开昆仑通态 MCGS 组态环境——设备窗口，选择 OPC 服务器；



2、选择【OPC.RVNet.S7】,确定；

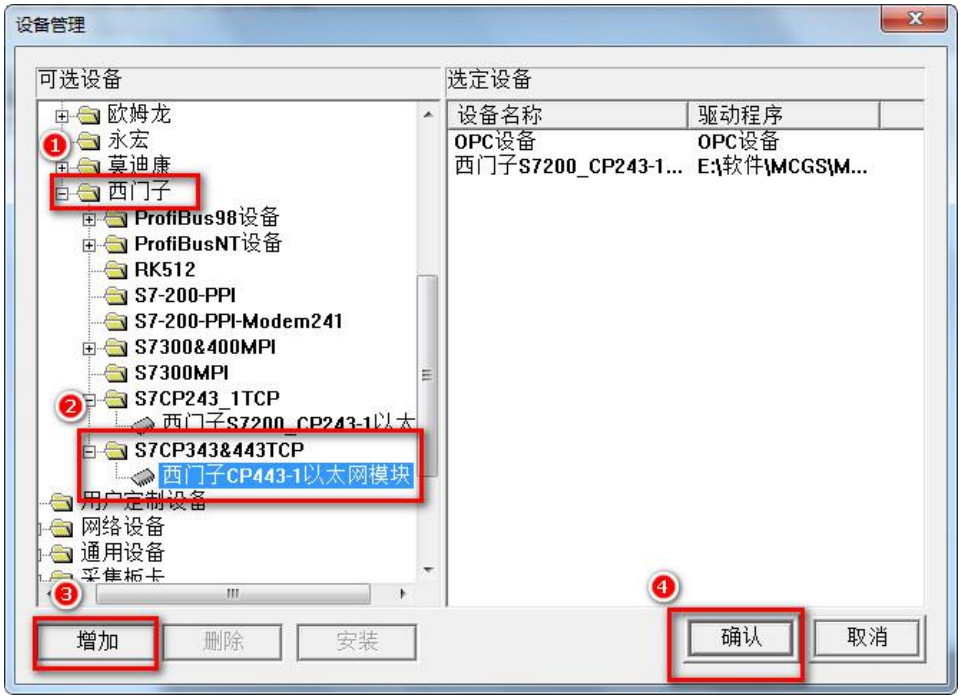


6.4.2 连接 S7300

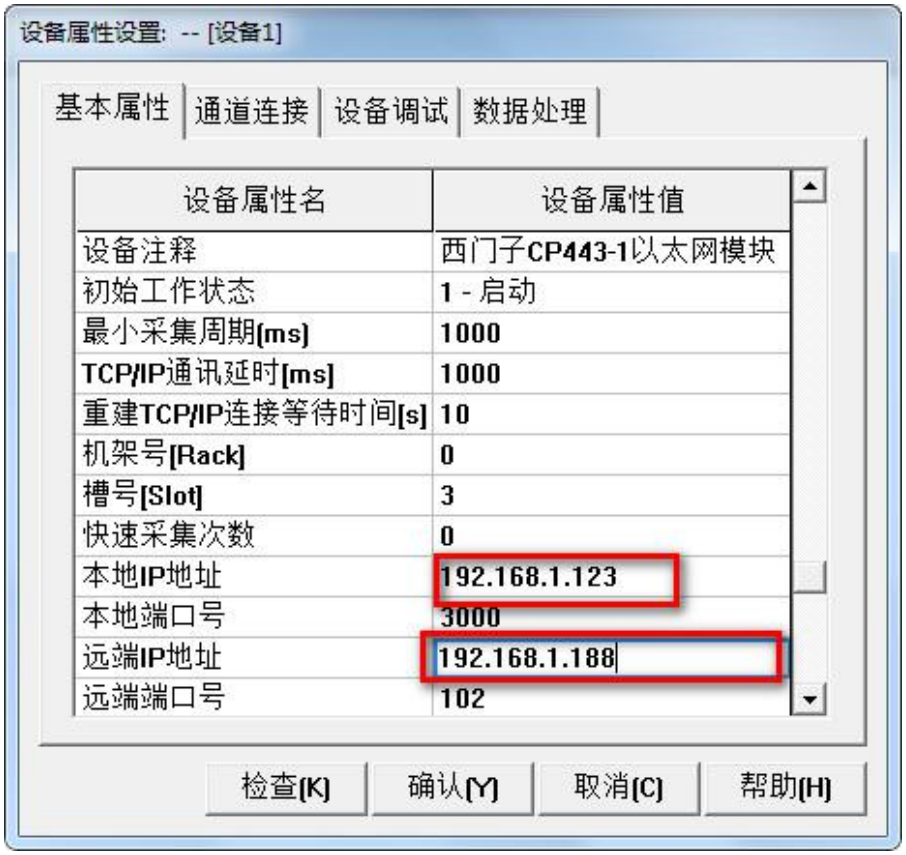
西门子 S7-300/400 采用 RVNet-S7300 连接 MCGS，可以采用：S7TCP 驱动、OPC 驱动。

6.4.2.1 采用 S7TCP 驱动

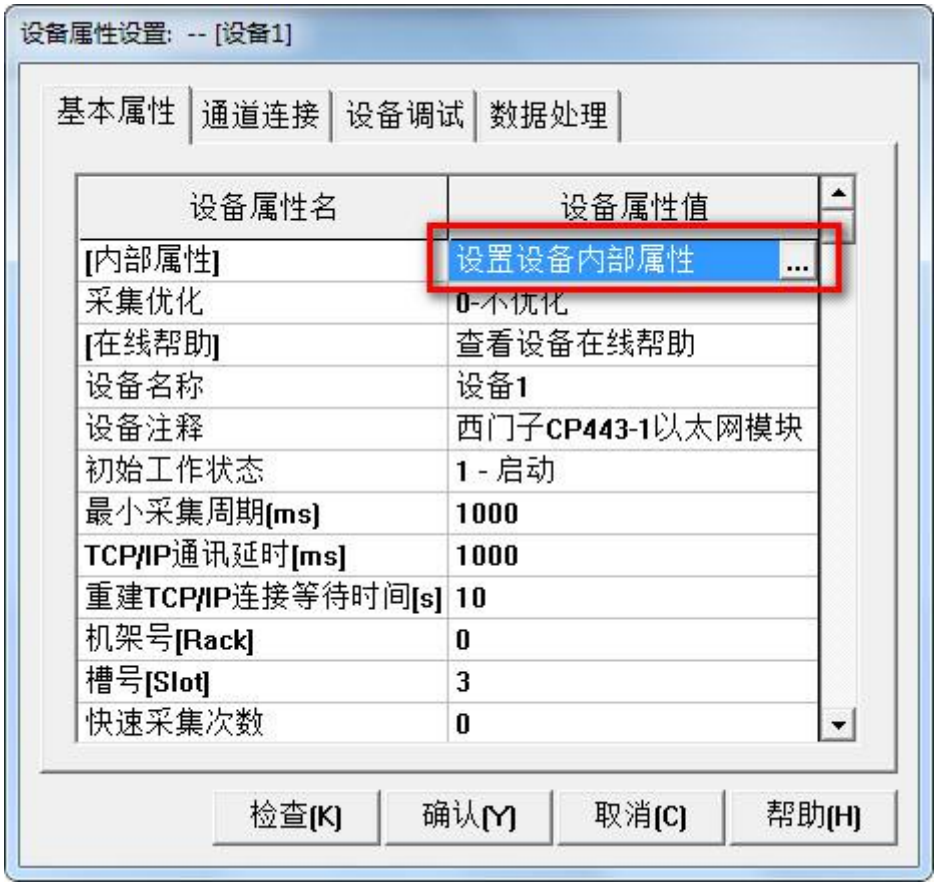
1、打开昆仑通态 MCGS 组态环境——设备窗口，在设备管理器中选择【PLC-西门子-S7CP343&443TCP-西门子 CP443-1 以太网模块】;

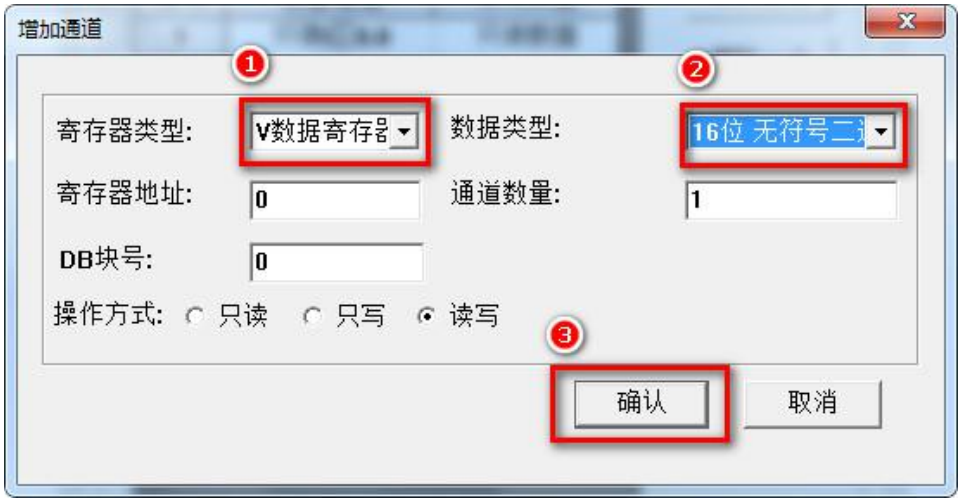


2、在设备属性设置中，将计算机的 IP 地址填入【本地 IP 地址】，RVNet-S7300 的 IP 地址填入【远端 IP 地址】,【远端端口号】填入 102；



3、点击【设置设备内部属性】，弹出设置窗口，点击【增加通道】进行变量的新建；



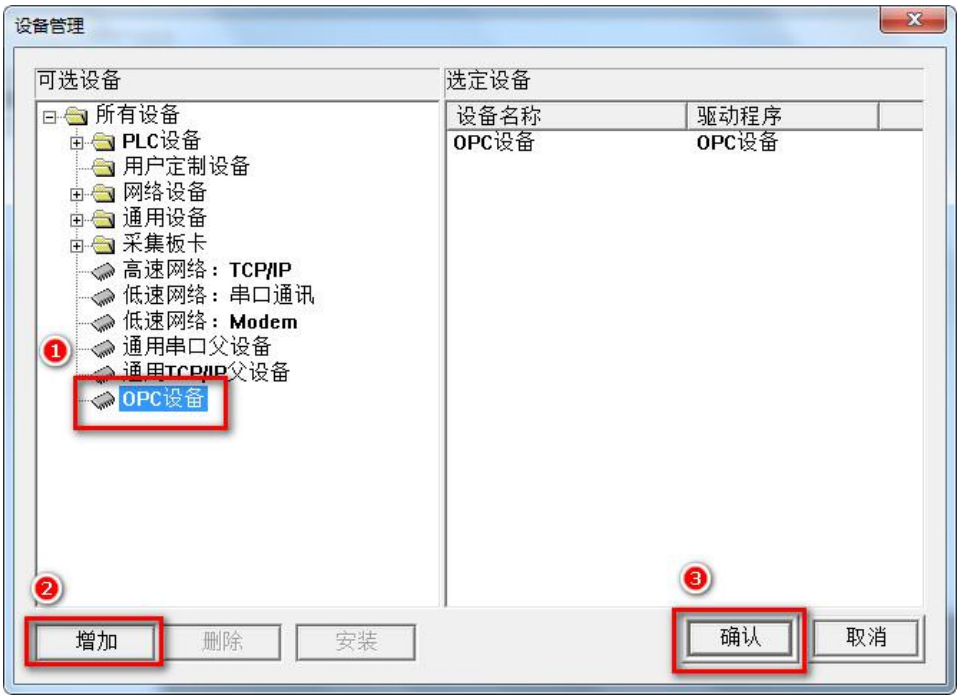


4、新建变量后点击“快速连接变量”，再点击“启动设备调试”，进行变量的监视。

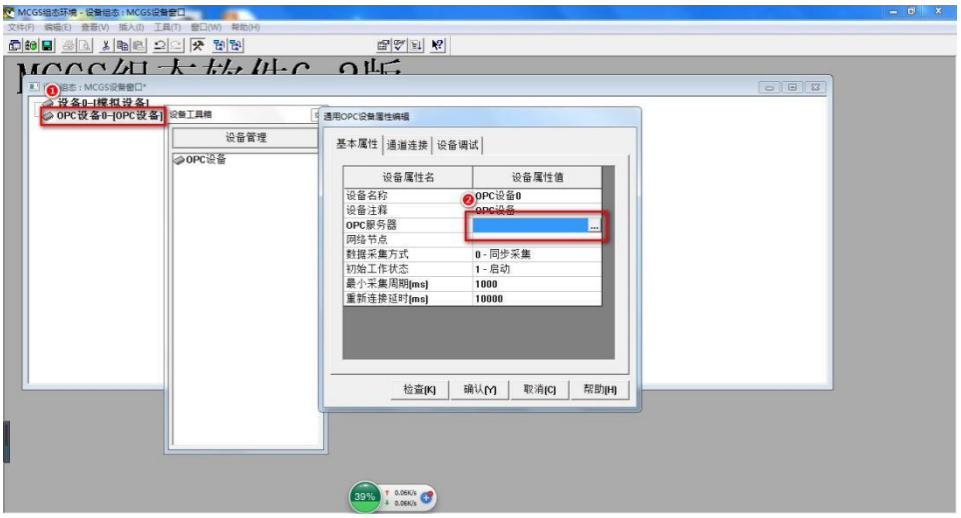
索引	连接变量	通道名称	通道处理	调试数据	采集周期
0000		通讯状态		0	1
0001	Data01	读写Q区0.1		1	1
0002	Data02	读写M区0.0		1	1
0003	Data03	读写DB1:VUB0		41538.0	1

6.4.2.2 采用 RVNetS7OPC

1、打开昆仑通态 MCGS 组态环境——设备窗口，选择 OPC 服务器；



2、双击【OPC 设备 0-[OPC 设备]】，弹出如下窗，选择【OPC.RVNet.S7】,确定。



6.5 杰控通讯

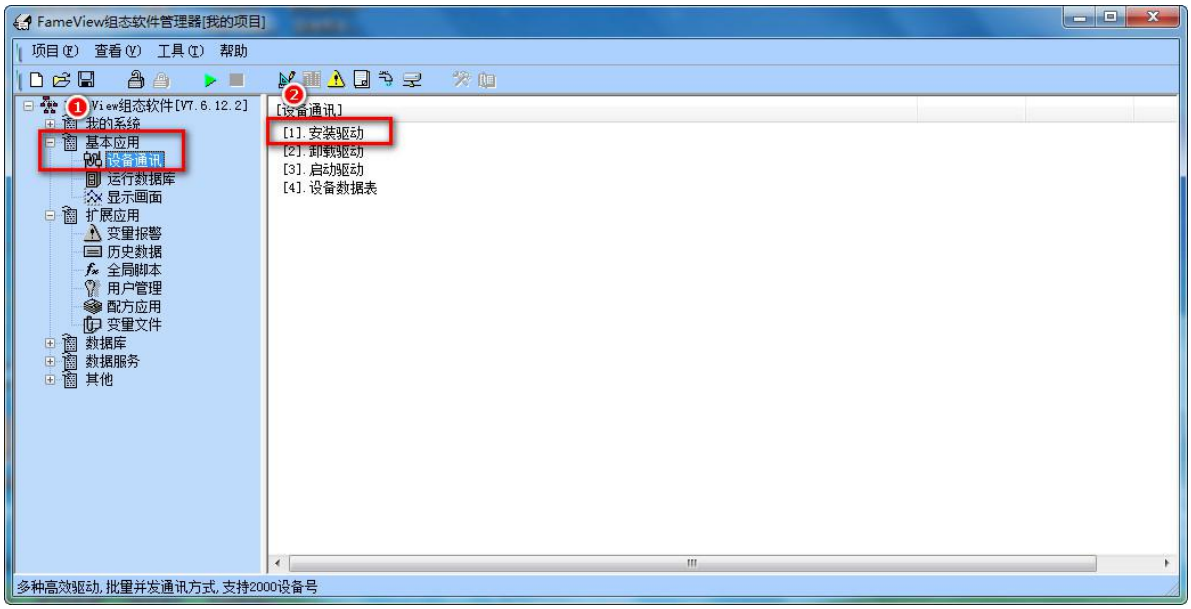
6.5.1 连接 S7200

西门子 S7-200 通过 RVNet-S7200 连接 FrameView，可以采用：西门子 S7TCP 驱动、OPC 驱动。

6.5.1.1 采用西门子 S7TCP 驱动

1、安装驱动程序：

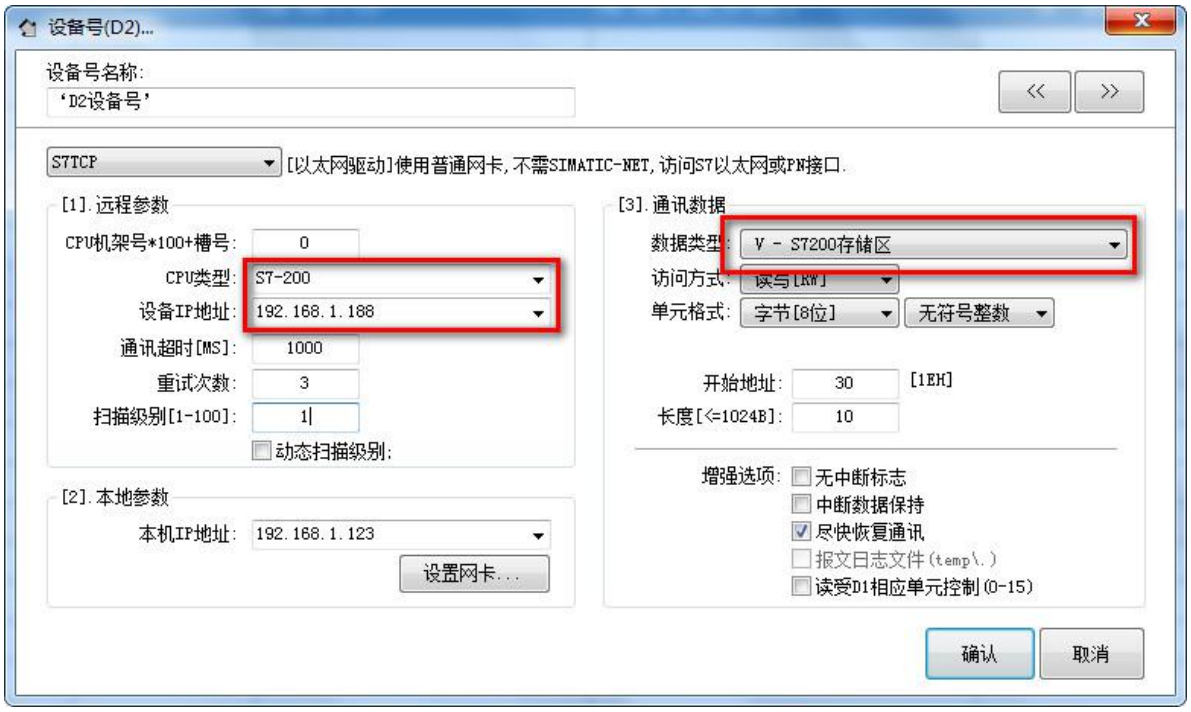
选择【基本应用】下【设备通讯】，执行【1.安装驱动程序】，显示下面对话框：



从西门子下选择【S7TCP】驱动，点击【安装】按钮进行安装。

2、定义设备数据表

选择【基本应用】下【设备通讯】，执行【4.设备数据表】显示设备数据表定义界面。双击【D2设备号】，通过下面的对话框进行定义：



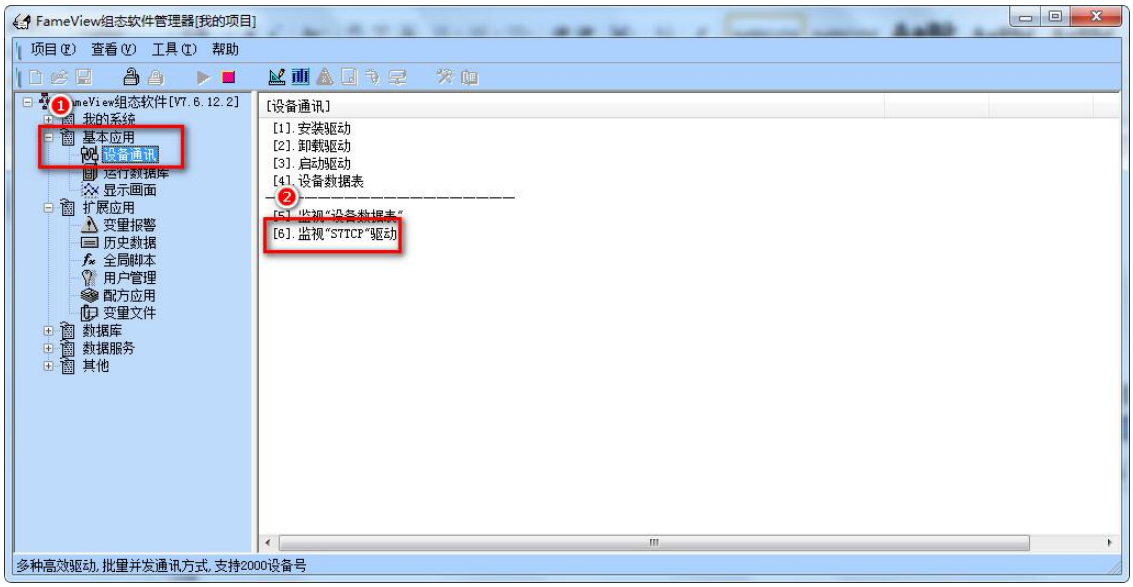
【CPU 类型】选择 S7-200，【设备 IP 地址】填入 RVNet-S7200 的 IP 地址；

这里我们定义了 S7-200PLC 的 VB30~VB39，一共 10 个字节的数据。

3、监视设备通讯

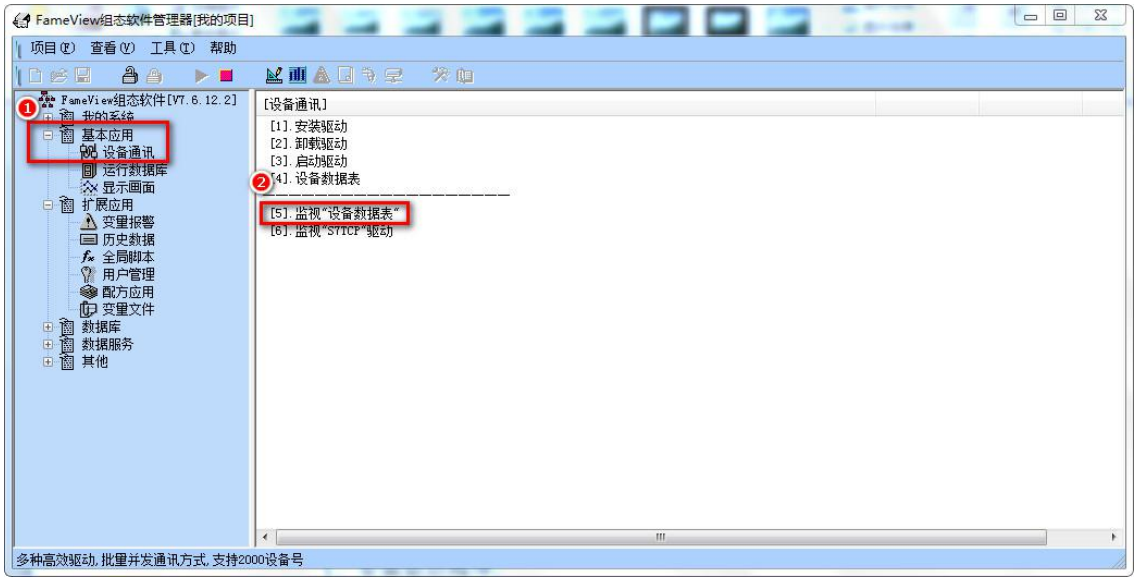
启动监视系统后，能监视驱动程序通讯状态。

选择【基本应用】下的【设备通讯】，执行【6.监视“S7TCP”驱动】，界面如下：



4、监视设备数据表

选择【基本应用】下的【设备通讯】，执行【5.监视“设备数据表”】

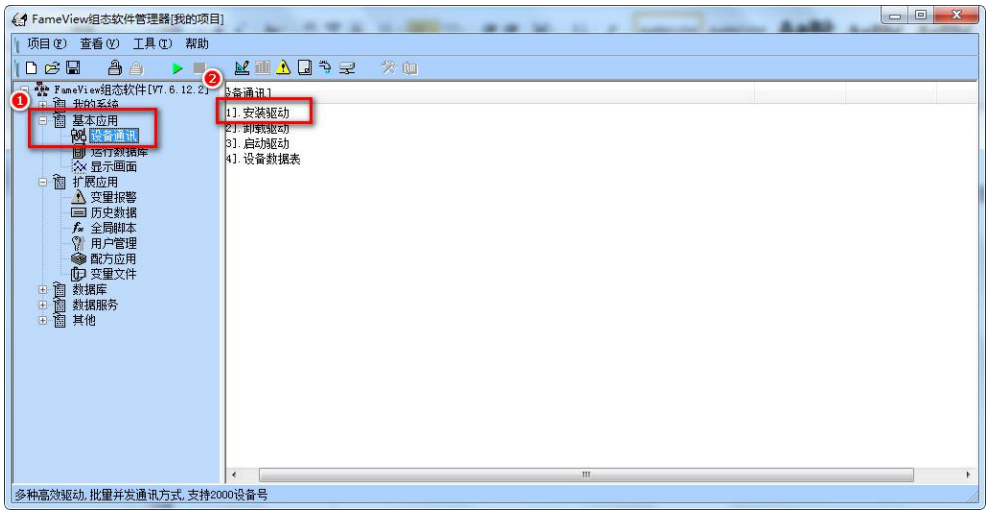


在【D2】那一行显示了你预先定义的 10 个字节的数据。

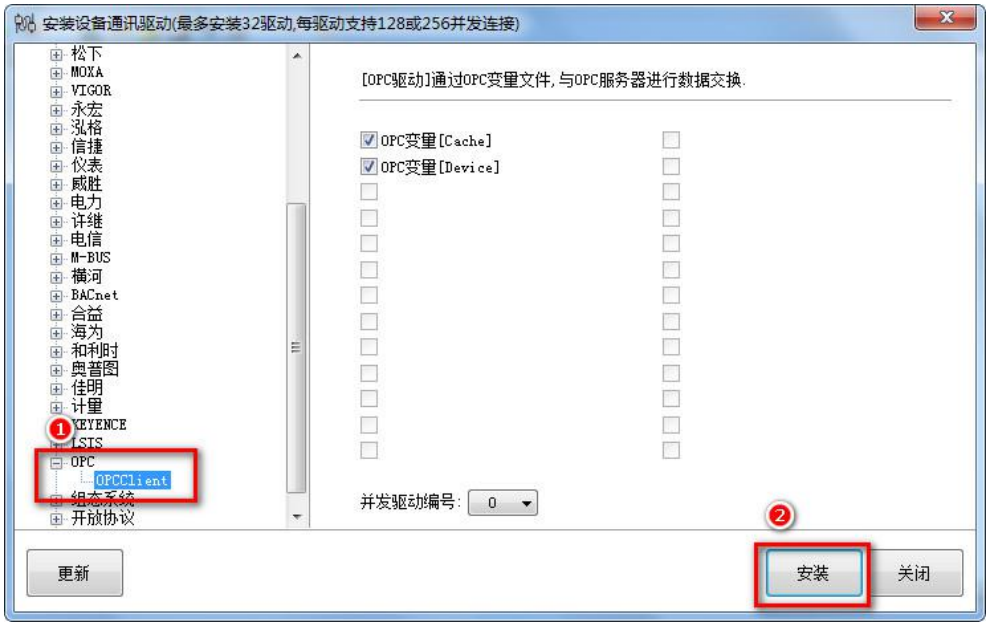
6.5.1.2 采用 RVNetS7OPC

1、安装驱动程序

选择【基本应用】下【设备通讯】，执行【1.安装驱动程序】，显示下面对话框：

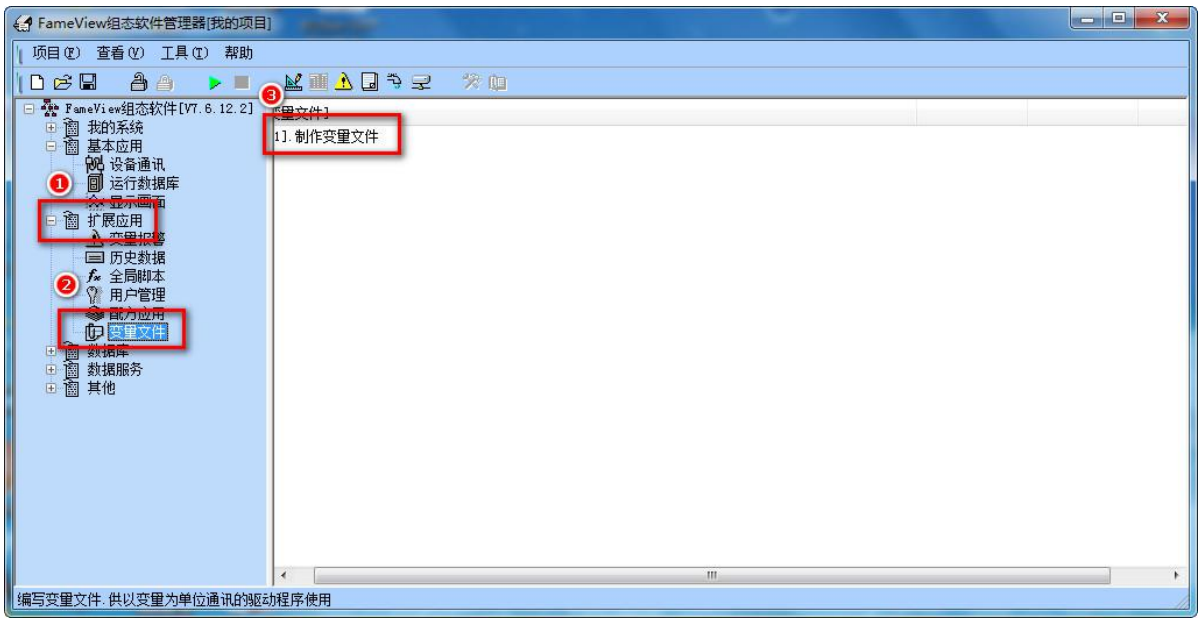


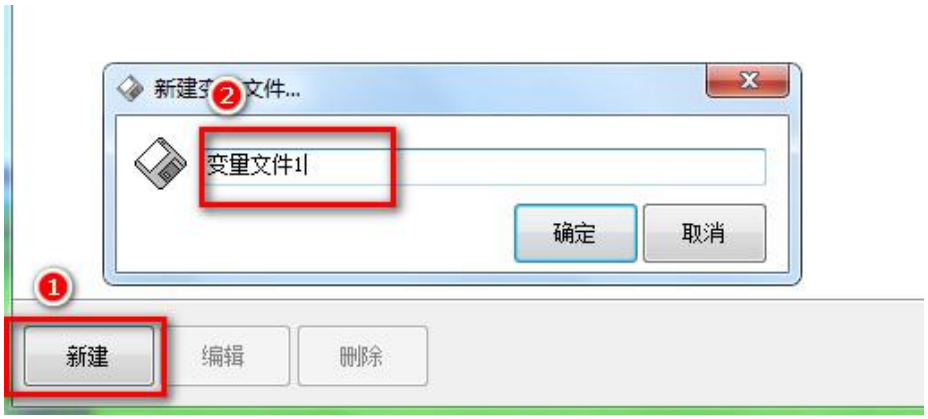
从 OPC 下选择【OPCClient】驱动，点击【安装】按钮进行安装。



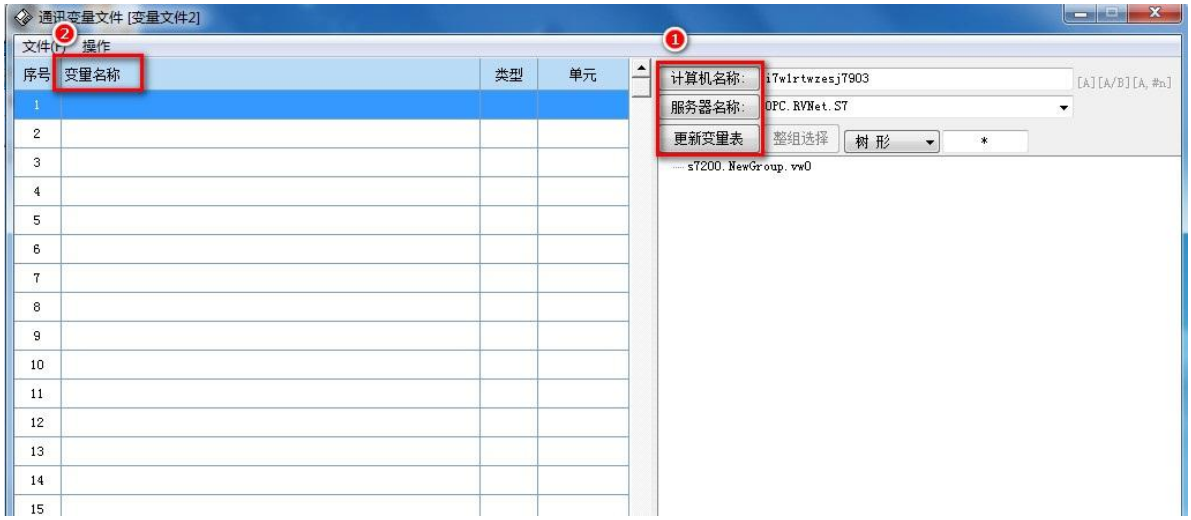
2、制作变量文件

选择【扩展应用】下【变量文件】，执行【1.制作变量文件】，选择新建，进行变量选择 ，如下面对话框：





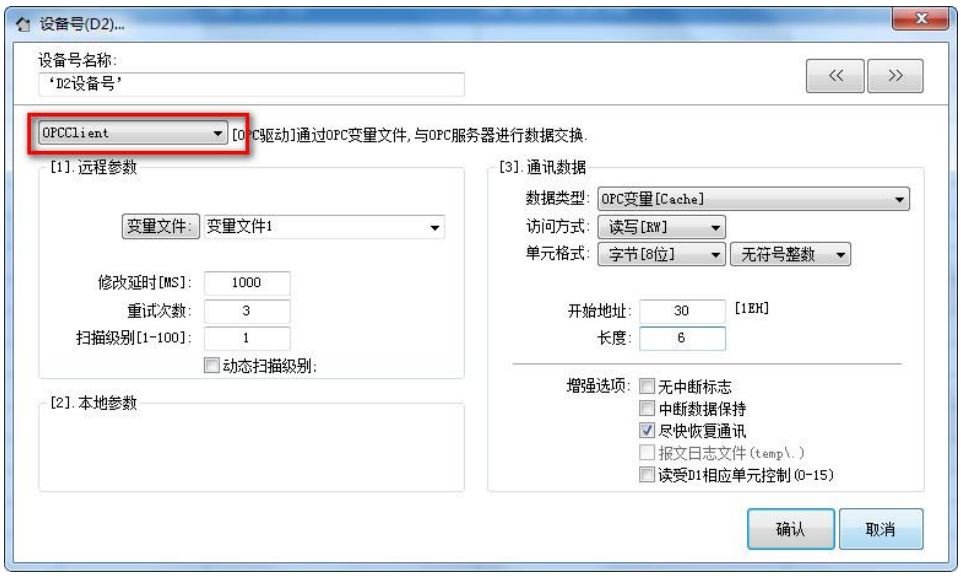
选择正确的计算机名称，服务器名称选择“OPC.RVNet.S7”,点击【更新变量表】，双击变量，将变量添加到变量名称列表中，最后进行保存；



3、定义设备数据表

选择【基本应用】下【设备通讯】，执行【4.设备数据表】显示设备数据表定义界面。

双击 D2 设备号，通过下面的对话框进行定义：



在【变量文件】中选择上面已编辑好了的变量表，【通讯数据】中的“开始地址”和“长度”对应了我变量表里的定义数据（VW30~VW36　6 个字节的数据长度）。

4、监视设备通讯

启动监视系统后，能监视驱动程序通讯状态。

选择【基本应用】下的【设备通讯】，执行【6.监视“OPCClient”驱动】，界面如下：

5、监视设备数据表

选择【基本应用】下的【设备通讯】，执行【5.监视“设备数据表”】，界面如下：

在【D2】那一行显示了你预先定义的 6 个字节的数据。

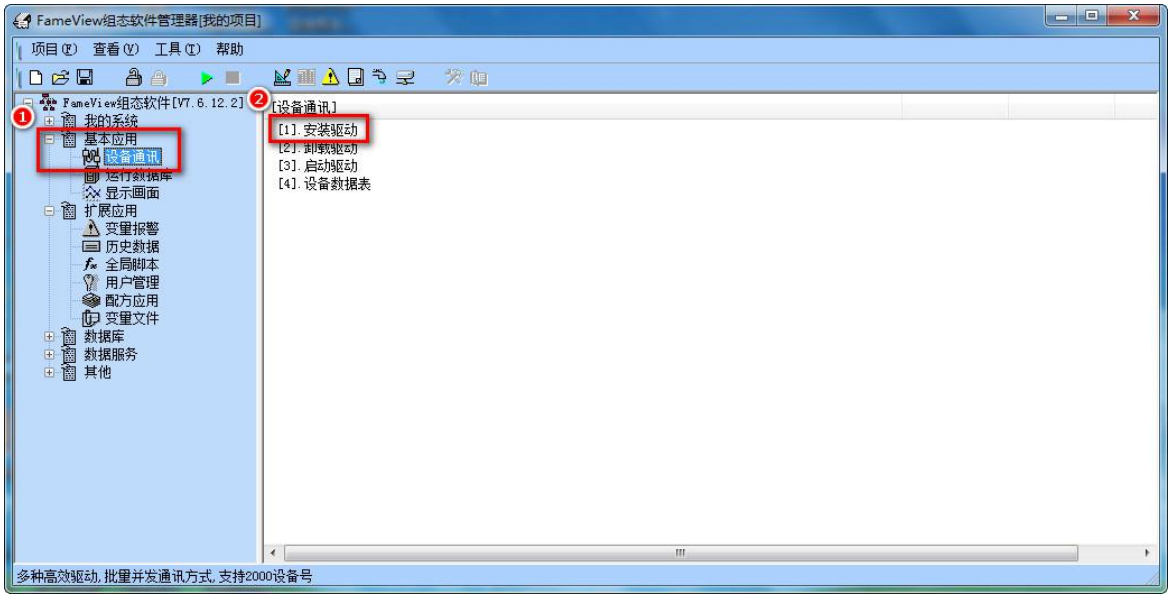
6.5.2 连接 S7300

西门子 S7-300/400 通过 RVNet-S7300 连接 FrameView，可以采用：西门子 S7TCP 驱动、OPC 驱动。

6.5.2.1 采用西门子 S7TCP 驱动

1、安装驱动程序

选择【基本应用】下【设备通讯】，执行【1.安装驱动程序】，显示下面对话框：

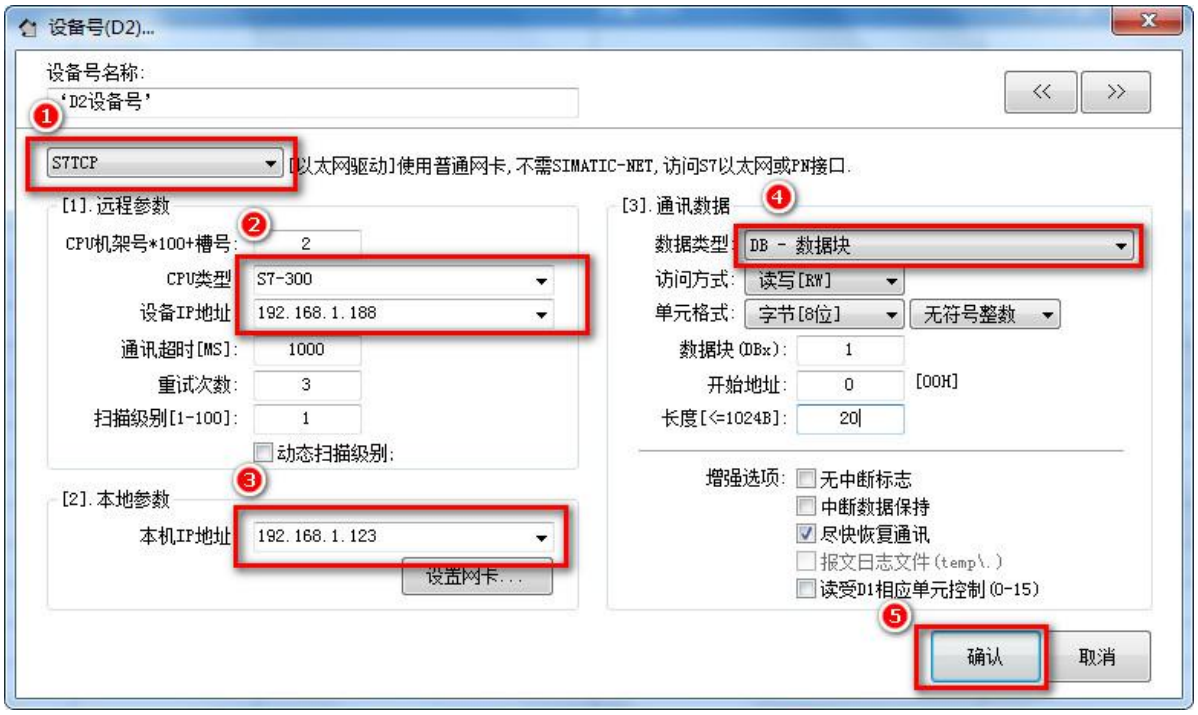


从西门子下选择【S7TCP】驱动，点击【安装】按钮进行安装。

2、定义设备数据表

选择【基本应用】下【设备通讯】，执行【4.设备数据表】显示设备数据表定义界面。

双击 D2 设备号，通过下面的对话框进行定义：



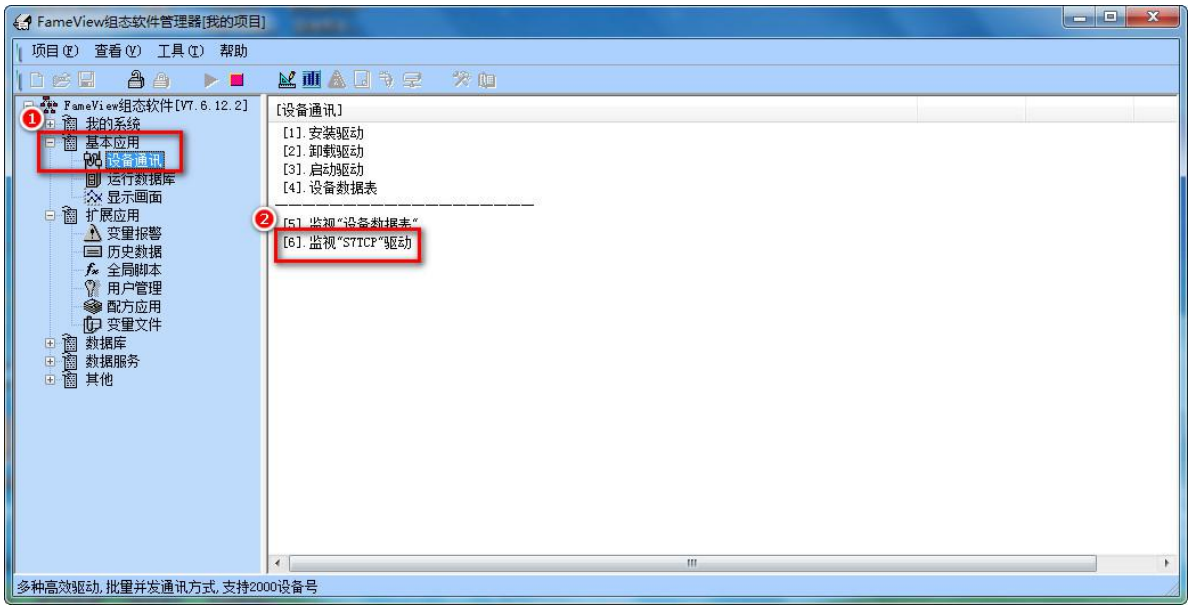
【CPU 类型】选择 S7-300，【设备 IP 地址】填入 RVNet-S7300 的 IP 地址；

这里我们定义了 S7-300PLC 中 DB1.DBB0~DB1.DBB19，一共 20 个字节的数据。

3、监视设备通讯

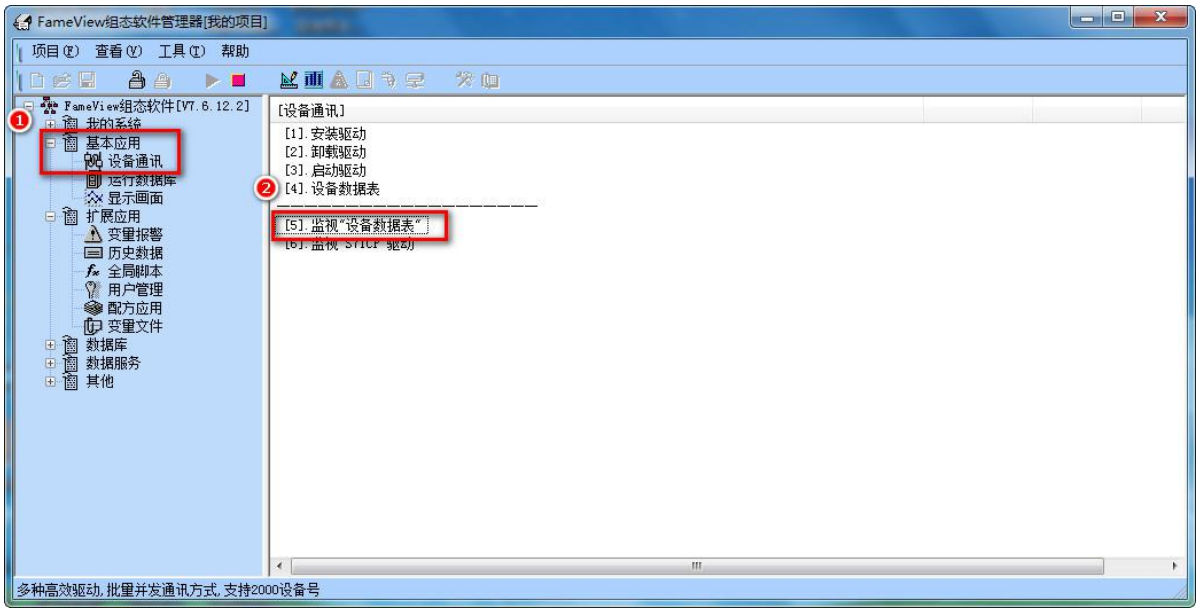
启动监视系统后，能监视驱动程序通讯状态。

选择【基本应用】下的【设备通讯】，执行【6.监视"S7TCP"驱动】:



4、监视设备数据表

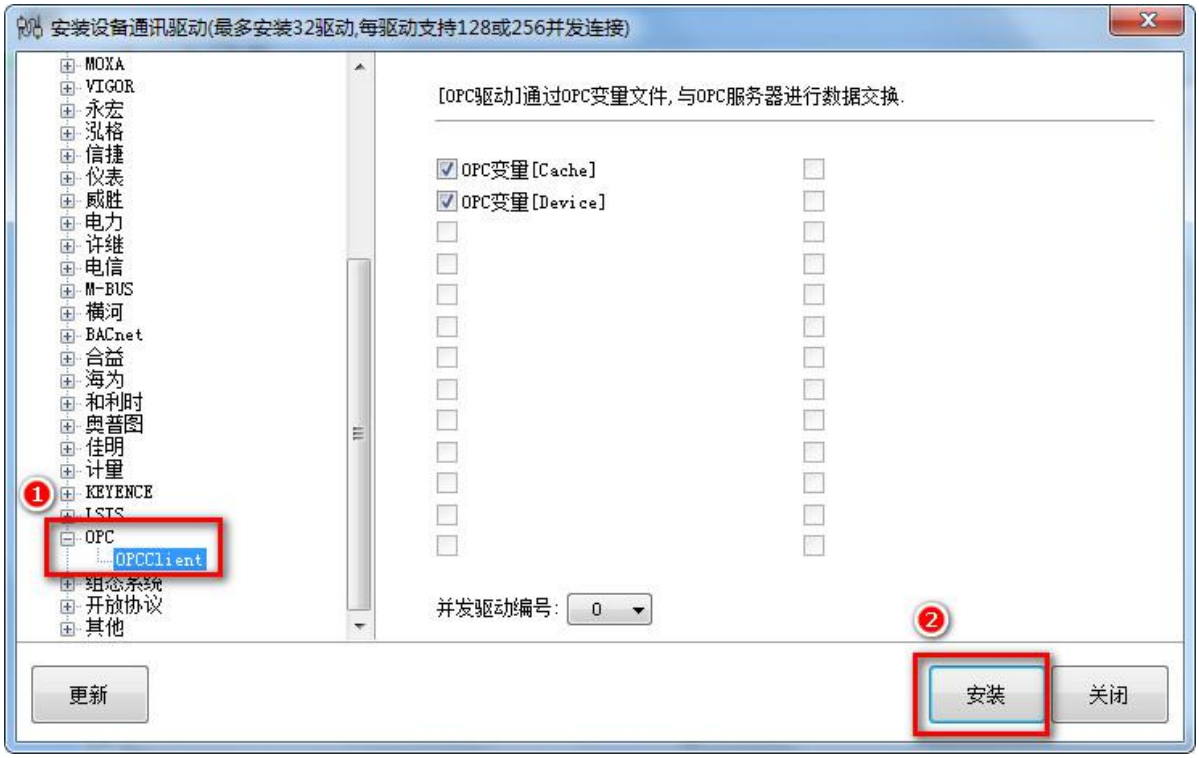
选择【基本应用】下的【设备通讯】，执行【5.监视"设备数据表"】:



6.5.2.2 采用 RVNetS7OPC

1、安装驱动程序

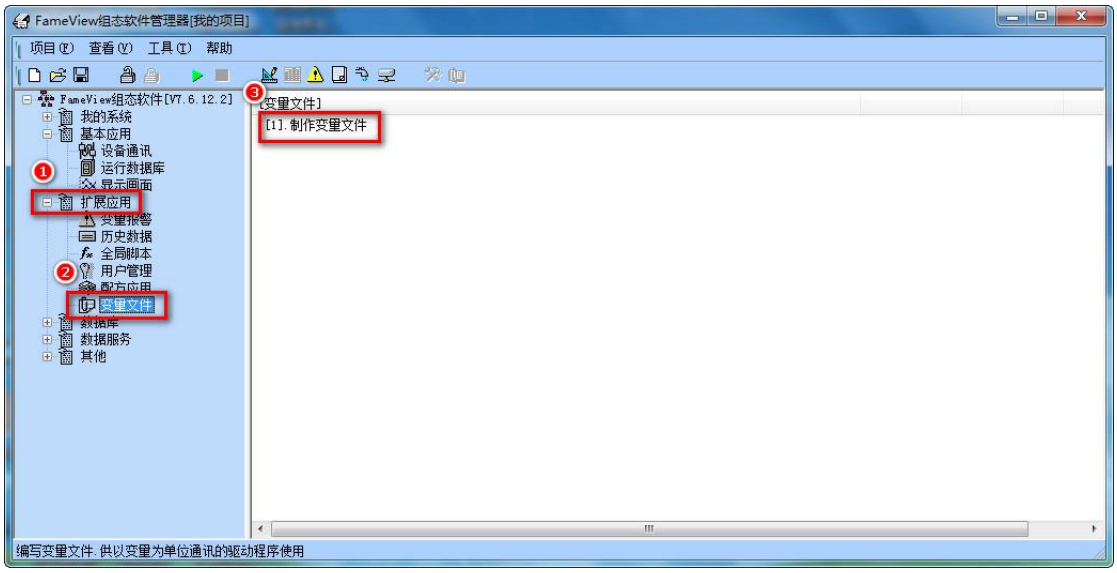
选择【基本应用】下【设备通讯】，执行【1.安装驱动程序】，显示下面对话框：



从 OPC 下选择“OPCClient”驱动，点击【安装】按钮进行安装。

2、制作变量文件

选择【扩展应用】下【变量文件】，执行【1.制作变量文件】，选择新建，进行变量选择 ，如下面对话框：

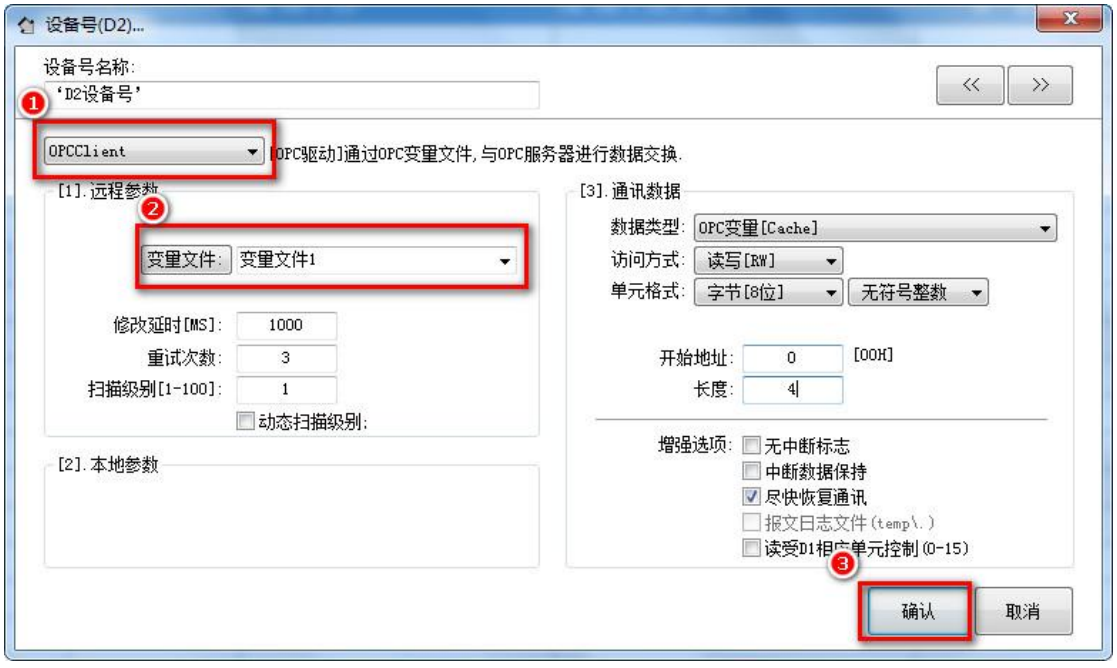


选择正确的计算机名称，服务器名称选择【OPC.RVNet.S7】,点击【更新变量表】，双击变量，将变量添加到变量名称列表中，最后进行保存。

3、定义设备数据表

选择【基本应用】下【设备通讯】，执行【4.设备数据表】显示设备数据表定义界面。

双击 D2 设备号，通过下面的对话框进行定义：

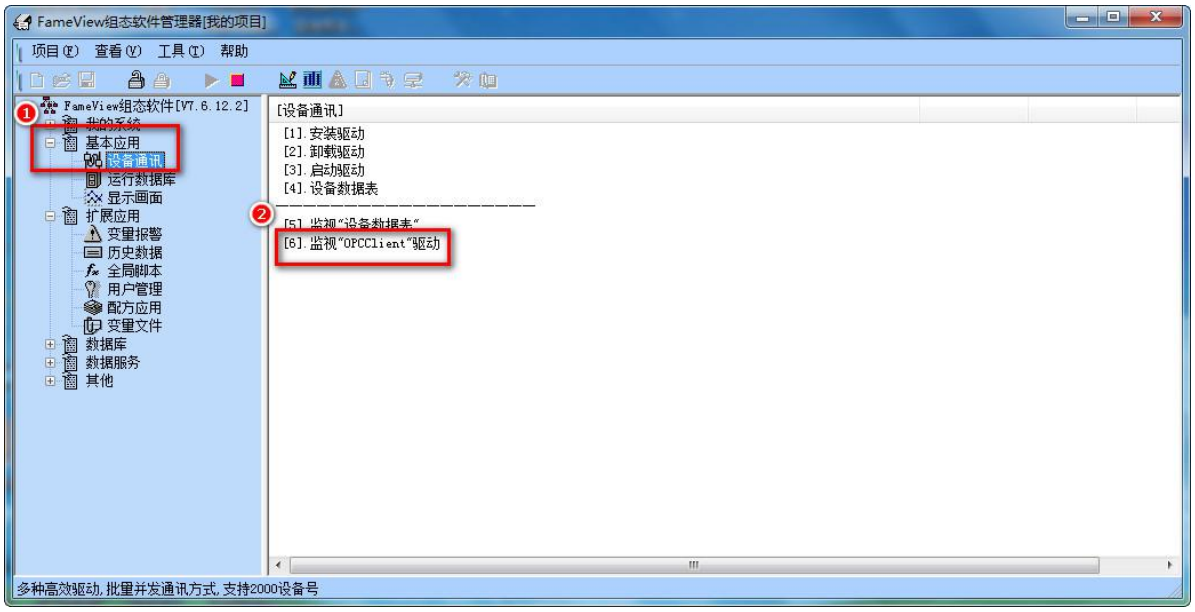


在【变量文件】中选择上面已编辑好了的变量表，【通讯数据】中的“开始地址”和“长度”对应了我变量表里的定义数据（DB1.DBW0 和 DB1.DBW2　4 个字节的数据长度）。

4、监视设备通讯

启动监视系统后，能监视驱动程序通讯状态。

选择【基本应用】下的【设备通讯】，执行【6.监视“OPCClient”驱动】，界面如下：



5、监视设备数据表

选择【基本应用】下的【设备通讯】，执行【5.监视“设备数据表”】，界面如下：

在【D2】那一行显示了你预先定义的 4 个字节的数据。

6.6IFIX 通讯

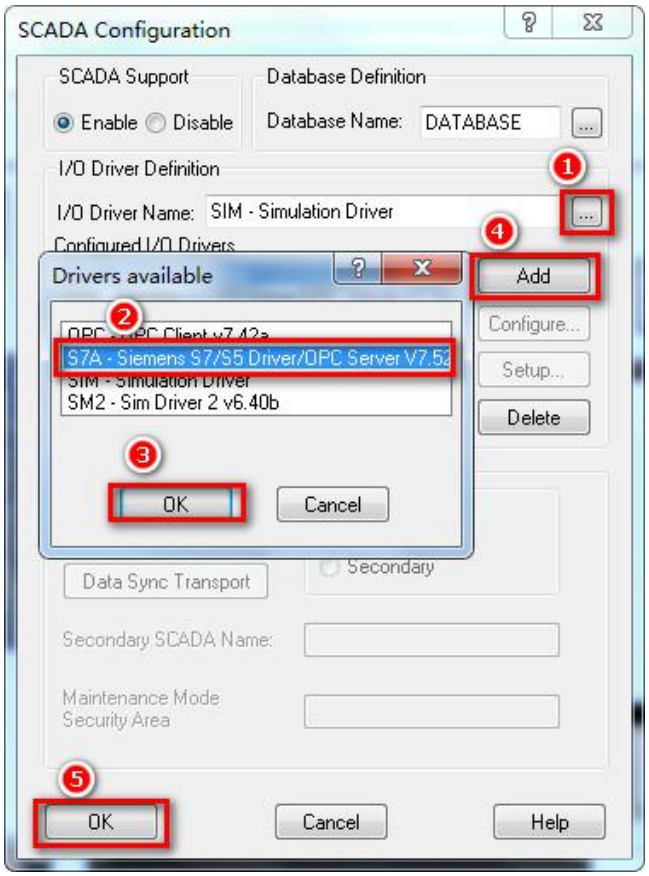
6.6.1 连接 S7200

西门子 S7-200 通过 RVNet-S7200 连接 iFIX，可以采用：iFIX 的 S7TCP 驱动、OPC 驱动。

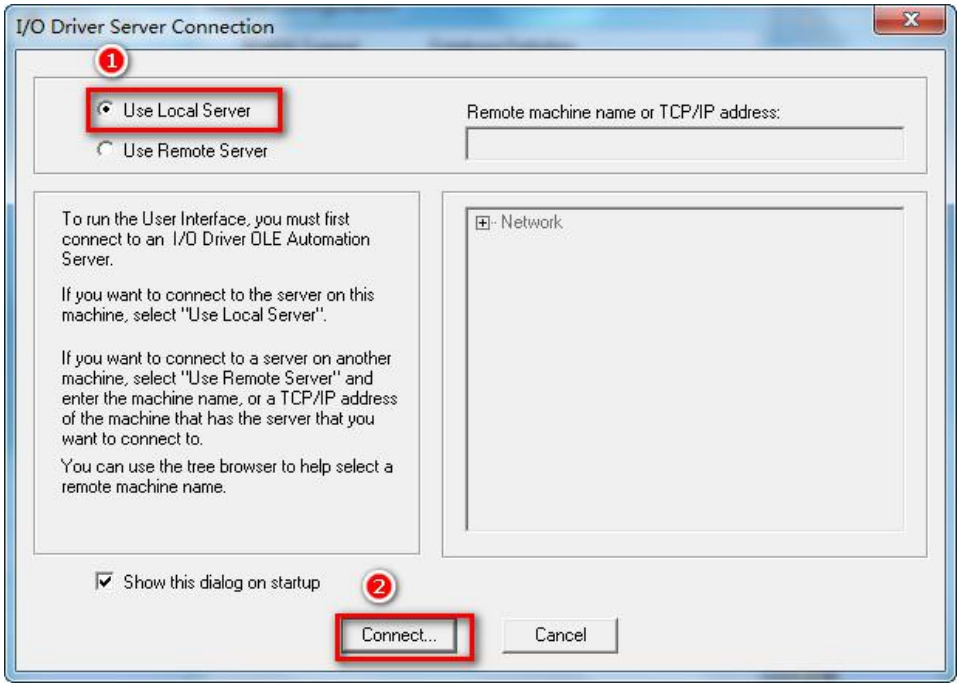
6.6.1.1 采用 S7TCP 驱动

1、安装西门子 S7TCP 驱动程序【S7A】，在【SCU-FIX】中配置 S7A 驱动：

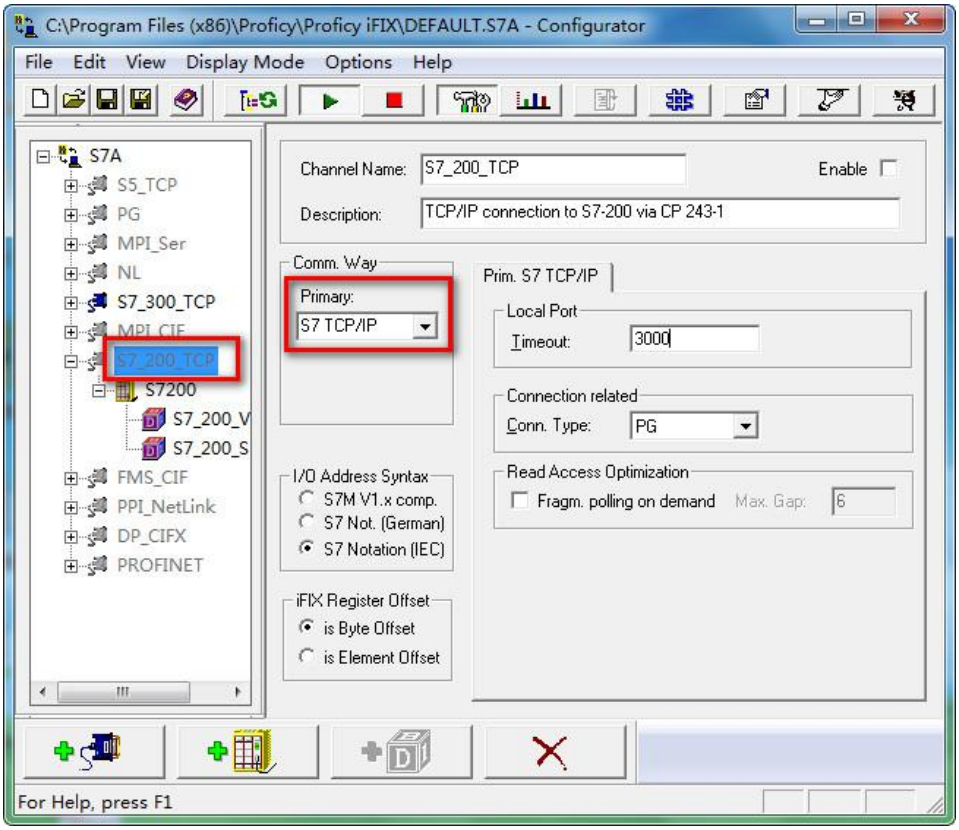

SCU - FIX
File Configure Help
Configuration File for Node FIX
NODE: FIX
PDB: DATABASE
Version: 5.5 (Build 8120)
SIM


SCADA Configuration
SCADA Support
Enable Disable
Database Definition
Database Name: DATABASE
I/O Driver Definition
I/O Driver Name: SIM - Simulation Driver
Configured I/O Drivers
Drivers available
Add
Configure...
Setup...
Delete
S7A - Siemens S7/S5 Driver/OPC Server V7.52
SM2 - Sim Driver 2 v6.40b
OK
Cancel
Data Sync Transport
Secondary
Secondary SCADA Name:
Maintenance Mode Security Area
OK
Cancel
Help

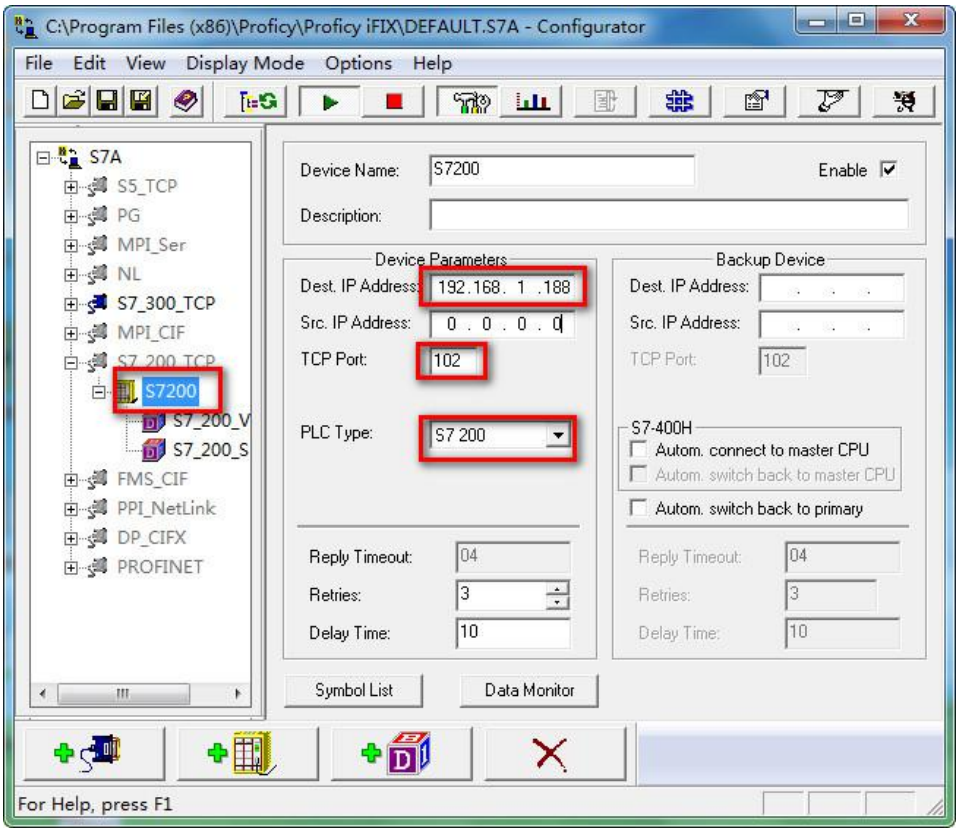

SCU - FIX
File Configure Help
Configuration File for Node FIX
NODE: FIX
PDB: DATABASE
Version: 5.5 (Build 8120)
SIM
S7A


I/O Driver Server Connection
1
Use Local Server
Use Remote Server
Remote machine name or TCP/IP address:
To run the User Interface, you must first connect to an I/O Driver OLE Automation Server.
If you want to connect to the server on this machine, select "Use Local Server".
If you want to connect to a server on another machine, select "Use Remote Server" and enter the machine name, or a TCP/IP address of the machine that has the server that you want to connect to.
You can use the tree browser to help select a remote machine name.
Network
Show this dialog on startup
2
Connect...
Cancel

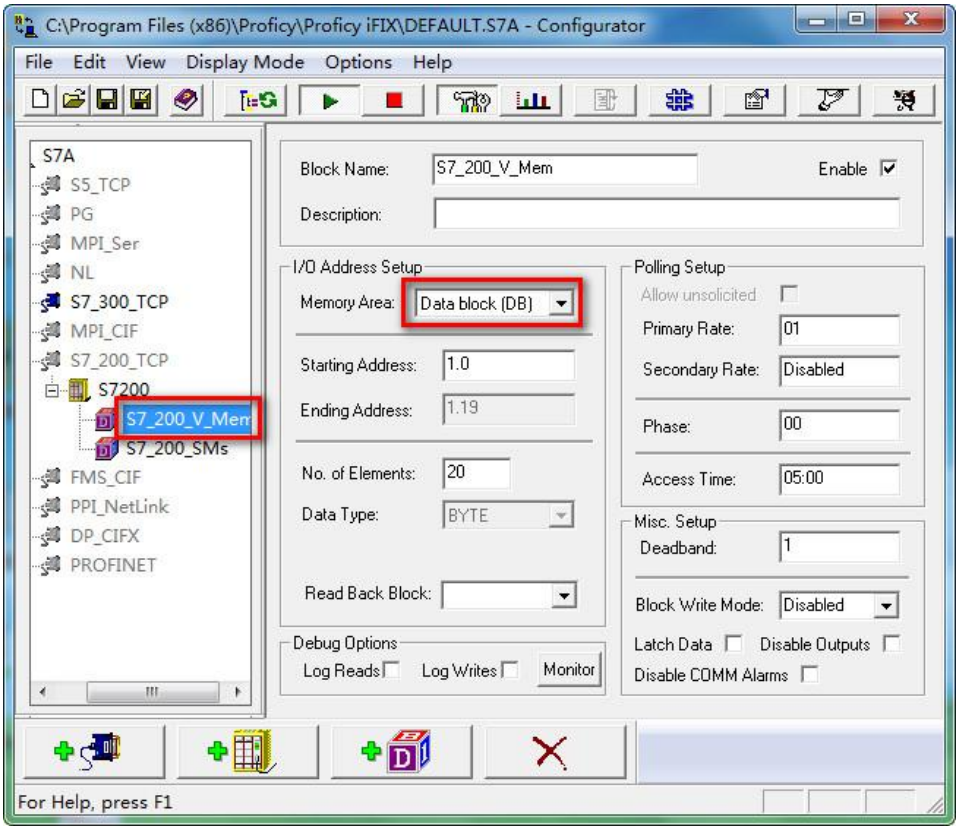
2、选择【S7_200_TCP】,【Primary】中选择S7TCP/IP；



3、 【Dest IP Address】中填入RVNet-S7200的IP地址，【Tcp Port】中填入：102； 【PLC Type】选择：S7200；其他参数默认；

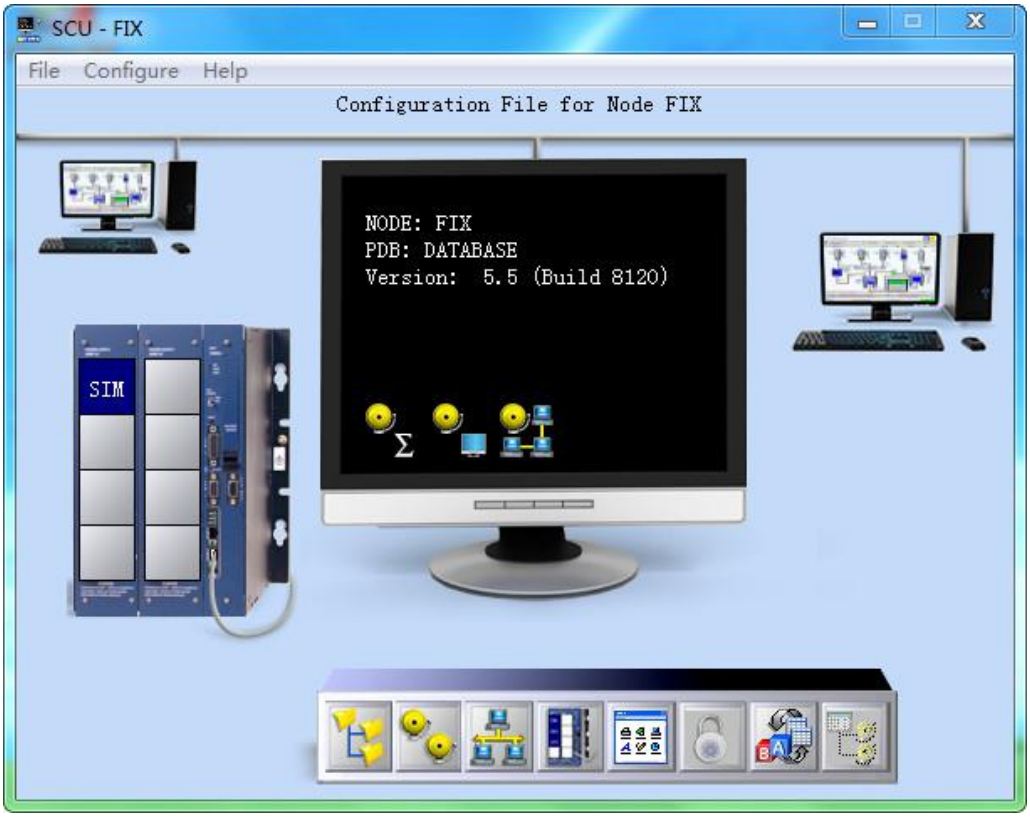


4、根据实际项目，建立各个区的变量(S7200的V区数据对应DB1，其他区的数据相同)。



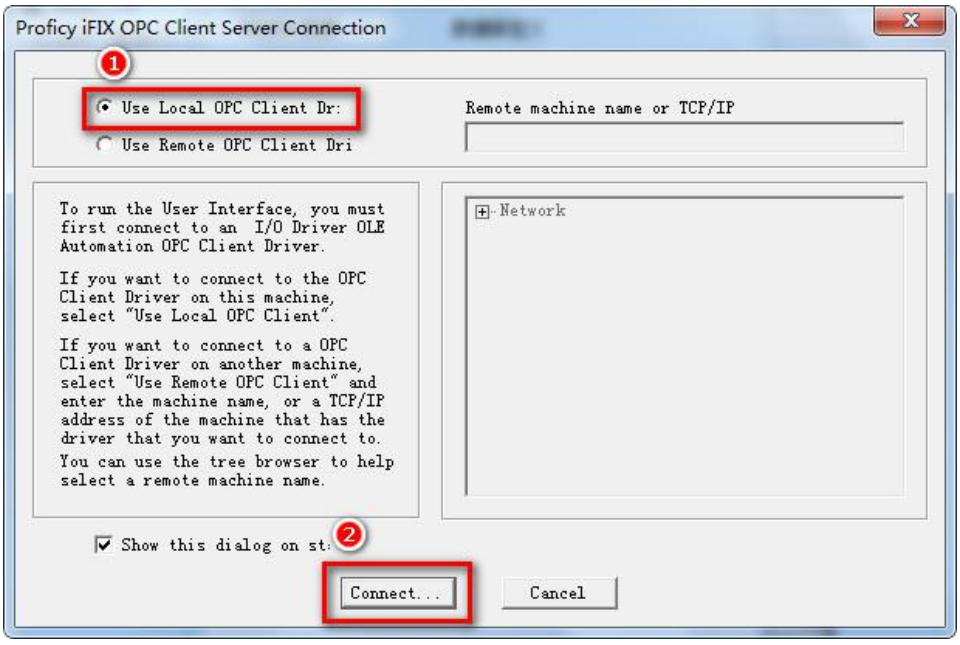
6.6.1.2 采用 RVNetS7OPC

3、 打开 iFIX 的系统配置（SCU-FIX）,点击下图底部第四个图标；

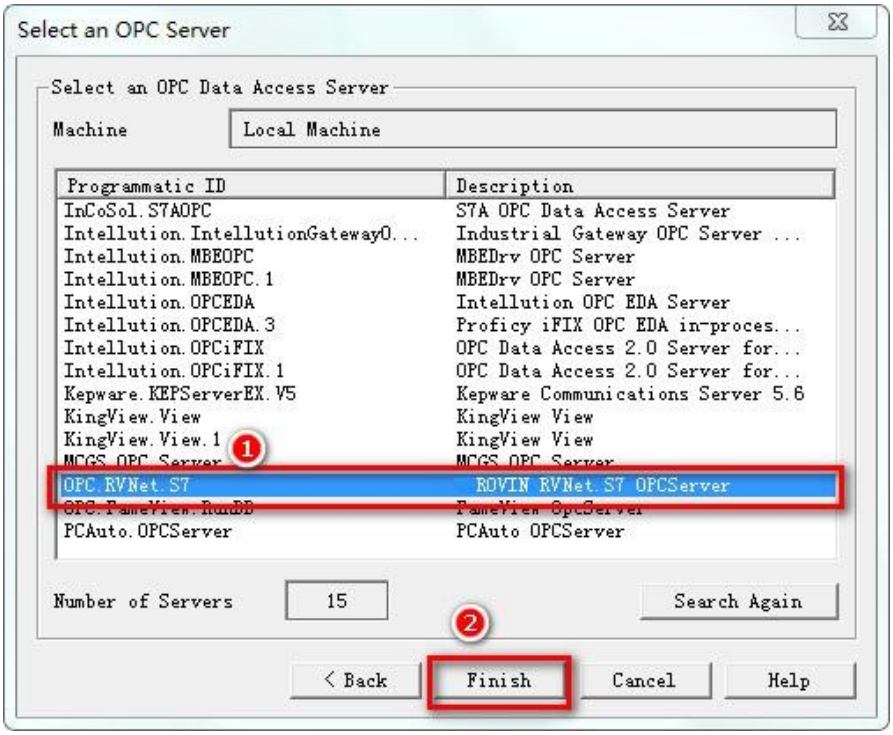


2、 按下图选择【OPC Client】驱动，确定后点击【添加】;

3、点击【配置】，选择本地连接【Use Local OPC Client Driver】,【Connet…】连接 OPC server



4、点击【Add OPC Server】，选择 【OPC.RVNet.S7】,【Finish】;

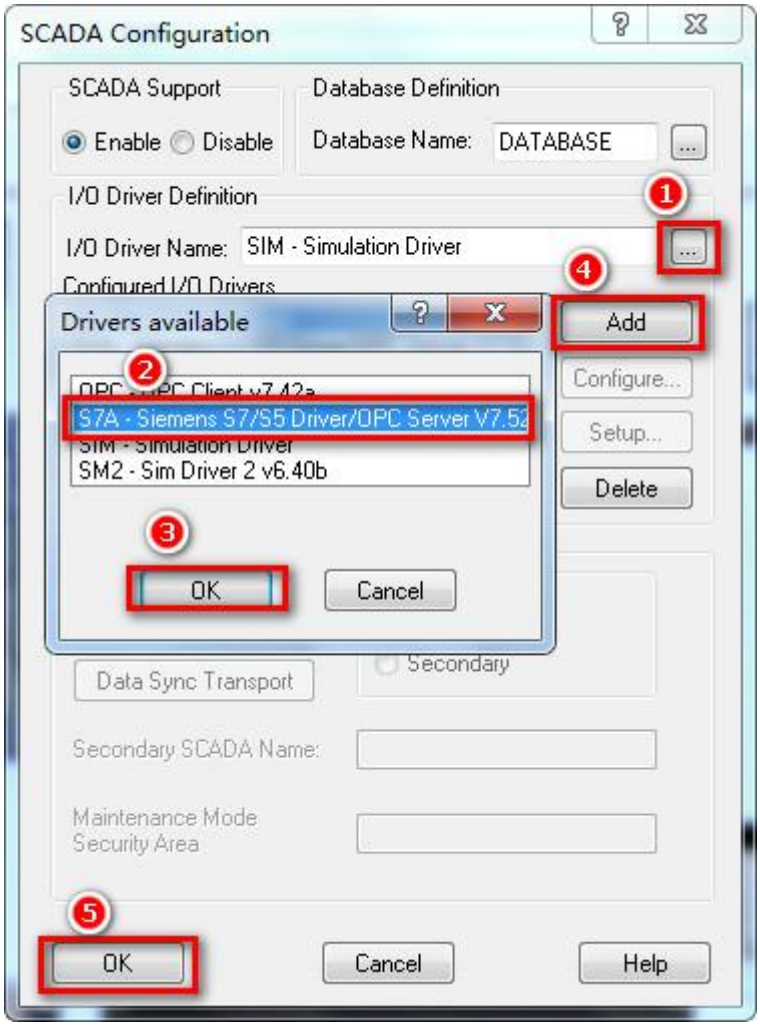


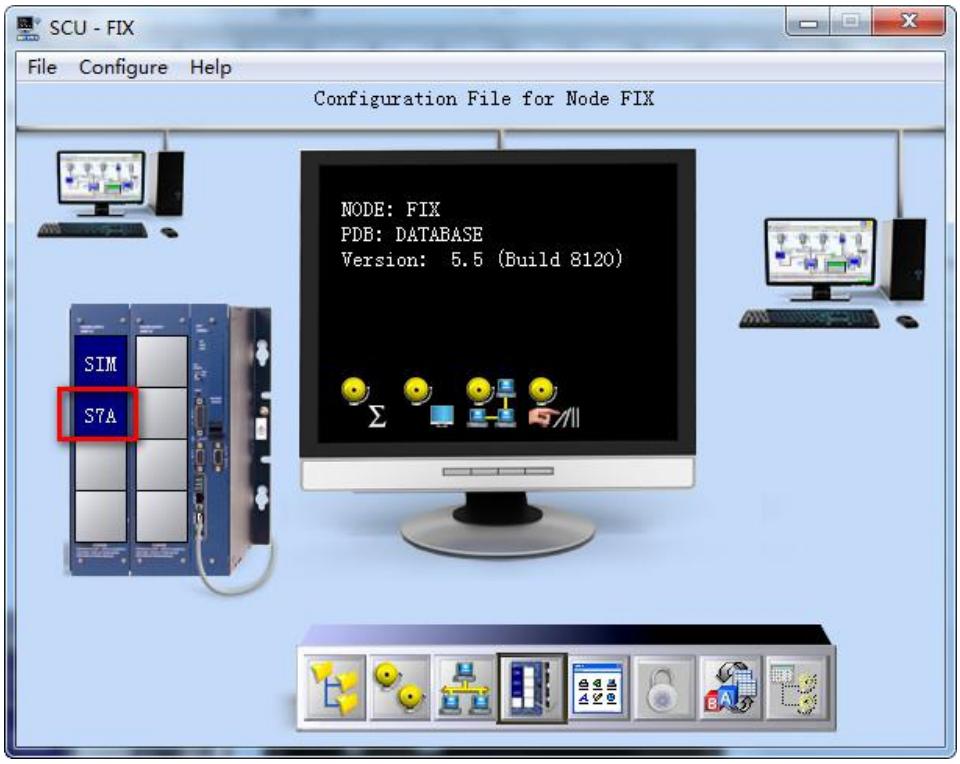
6.6.2 连接 S7300

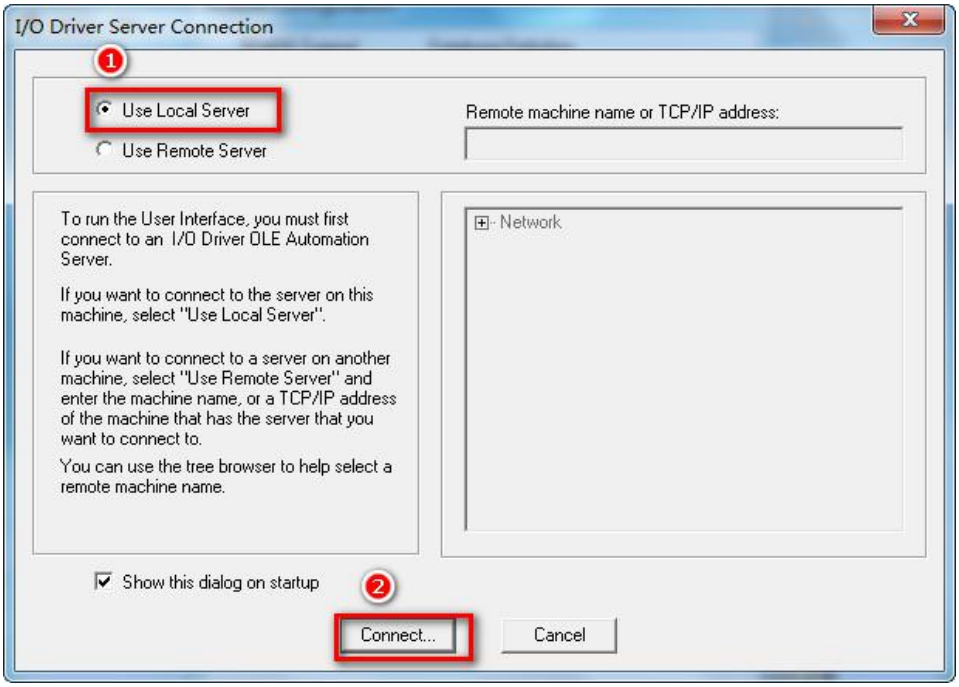
西门子 S7-300/400 采用 RVNet-S7300 连接 iFIX，可以通过：S7TCP 驱动、OPC 驱动。

6.6.2.1 采用 S7TCP 驱动

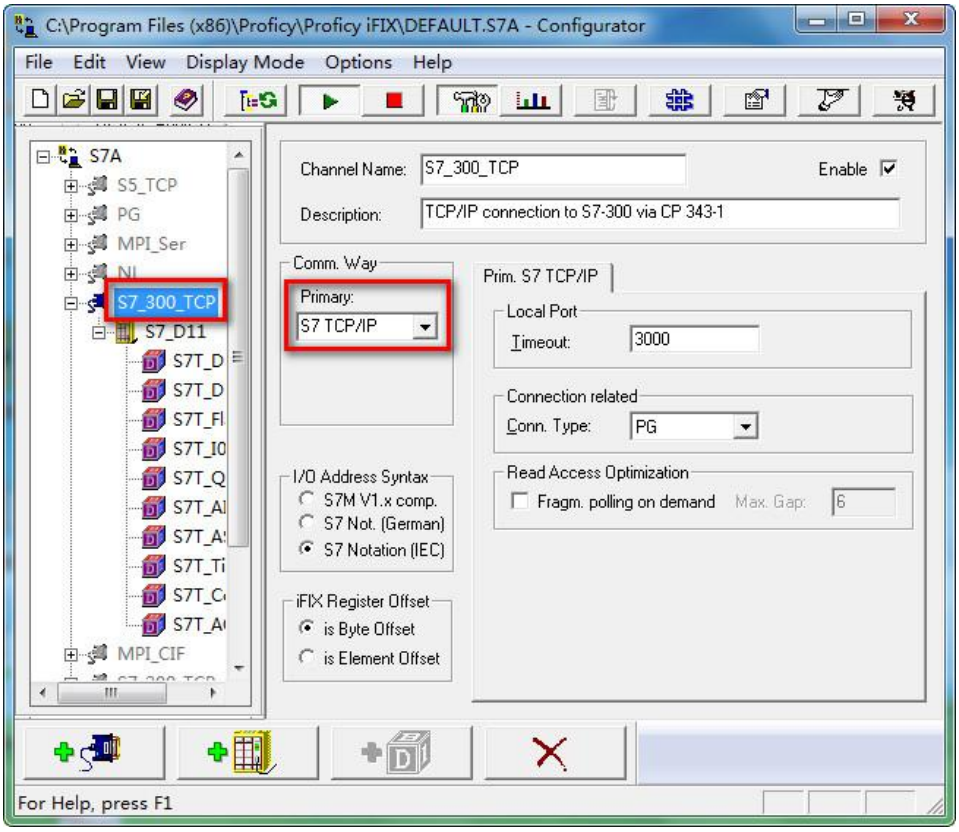
1、安装西门子 S7TCP 驱动程序【S7A】，在【SCU-FIX】中配置 S7A 驱动，如图：


SCADA Configuration
SCADA Support
Enable
Disable
Database Definition
Database Name:
DATABASE
I/O Driver Definition
I/O Driver Name:
SIM - Simulation Driver
Configured I/O Drivers
Drivers available
S7A - Siemens S7/S5 Driver/OPC Server V7.52
SM2 - Sim Driver 2 v6.40b
OK
Cancel
Add
Configure...
Setup...
Delete
Data Sync Transport
Secondary
Secondary SCADA Name:
Maintenance Mode
Security Area
OK
Cancel
Help
1
2
3
4
5

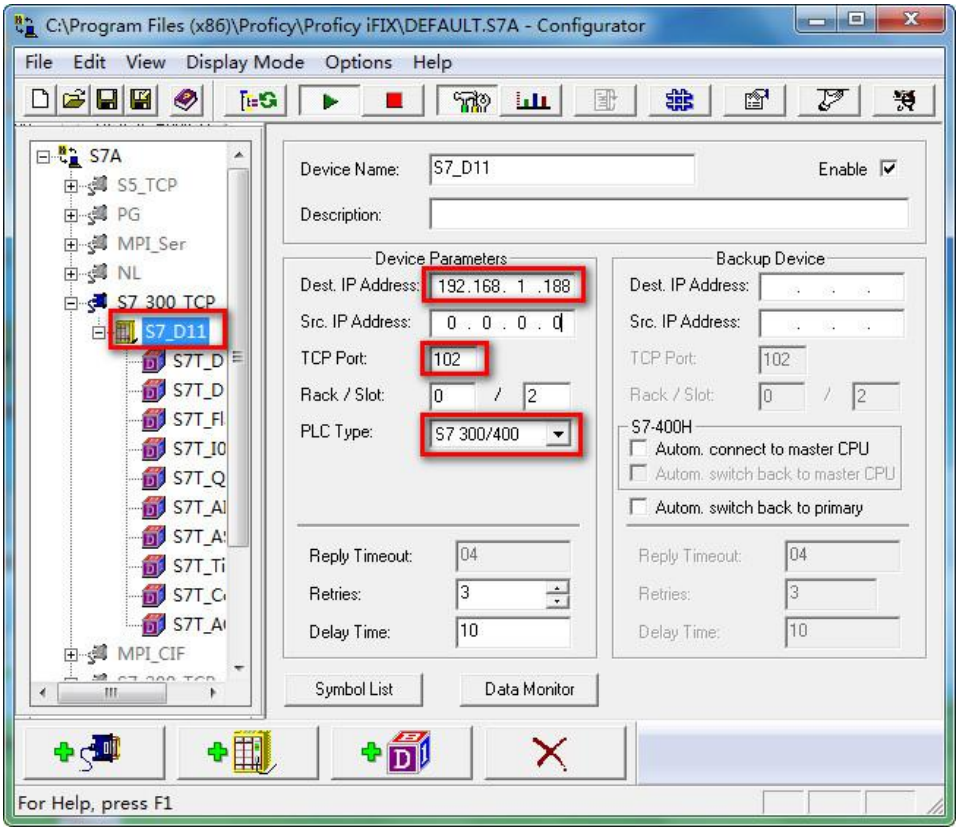

SCU - FIX
File
Configure
Help
Configuration File for Node FIX
NODE: FIX
PDB: DATABASE
Version: 5.5 (Build 8120)
SIM
S7A



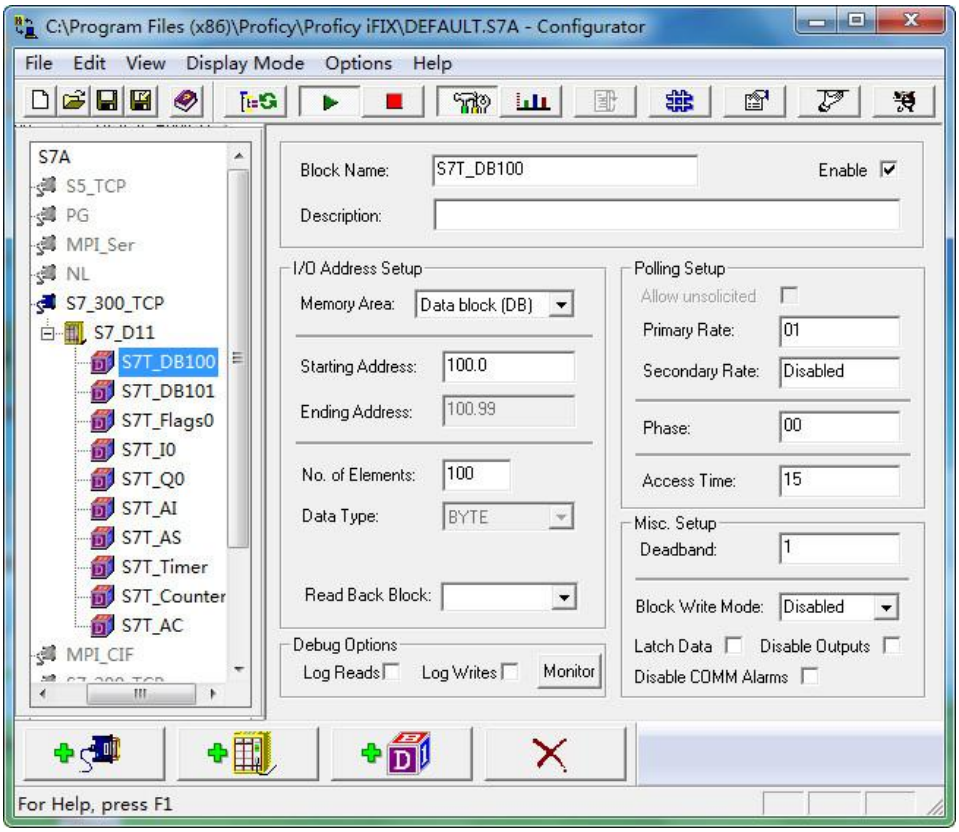
2、选择【S7_300_TCP】，在【Primary】中选择S7TCP/IP；



3、【Dest IP Address】，填入RVNet-S7300的IP地址，【Tcp Port】中填入：102，【PLC Type】中选择：S7300/400，其他参数默认。

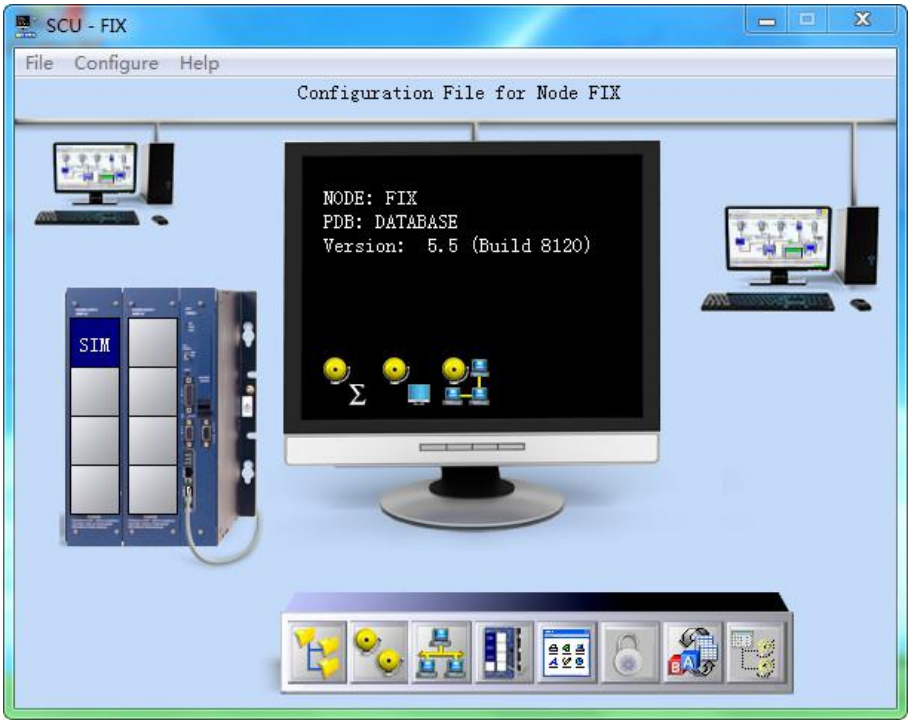


4、 根据实际项目，建立各个区的变量：

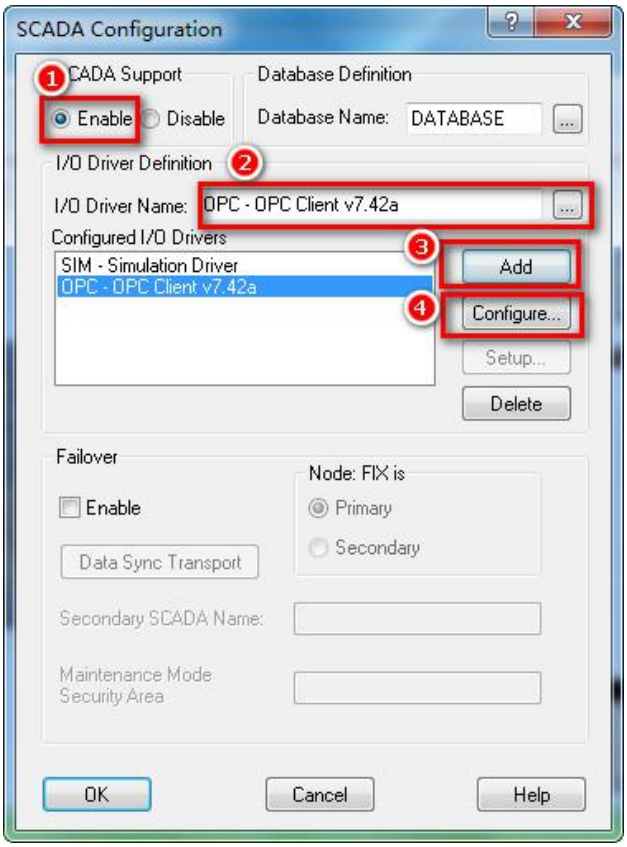


6.6.2.2 采用 RVNetS7OPC

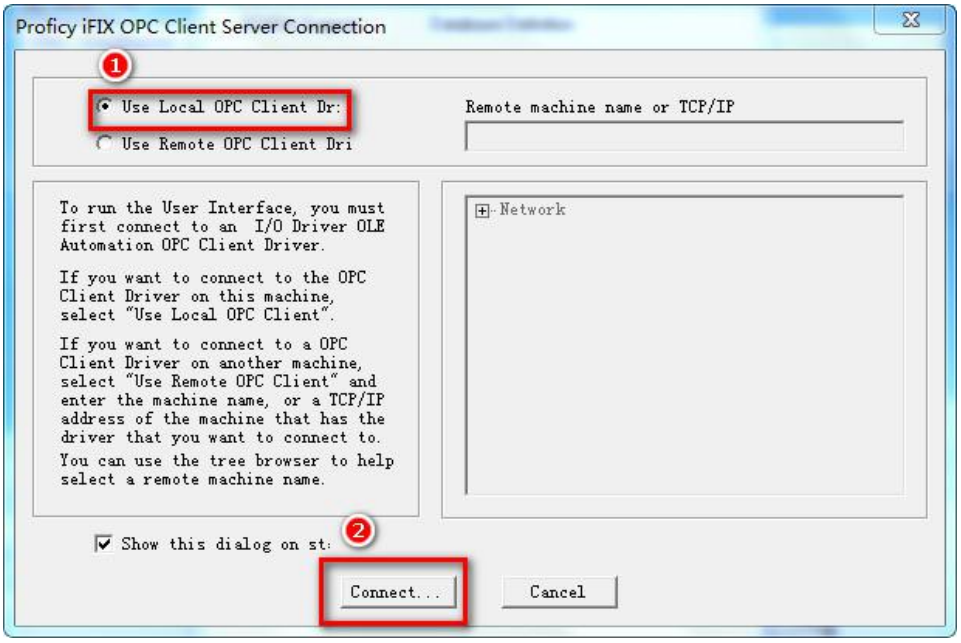
1、打开 IFIX 的系统配置（SCU-FIX），点击下图底部第四个图标；



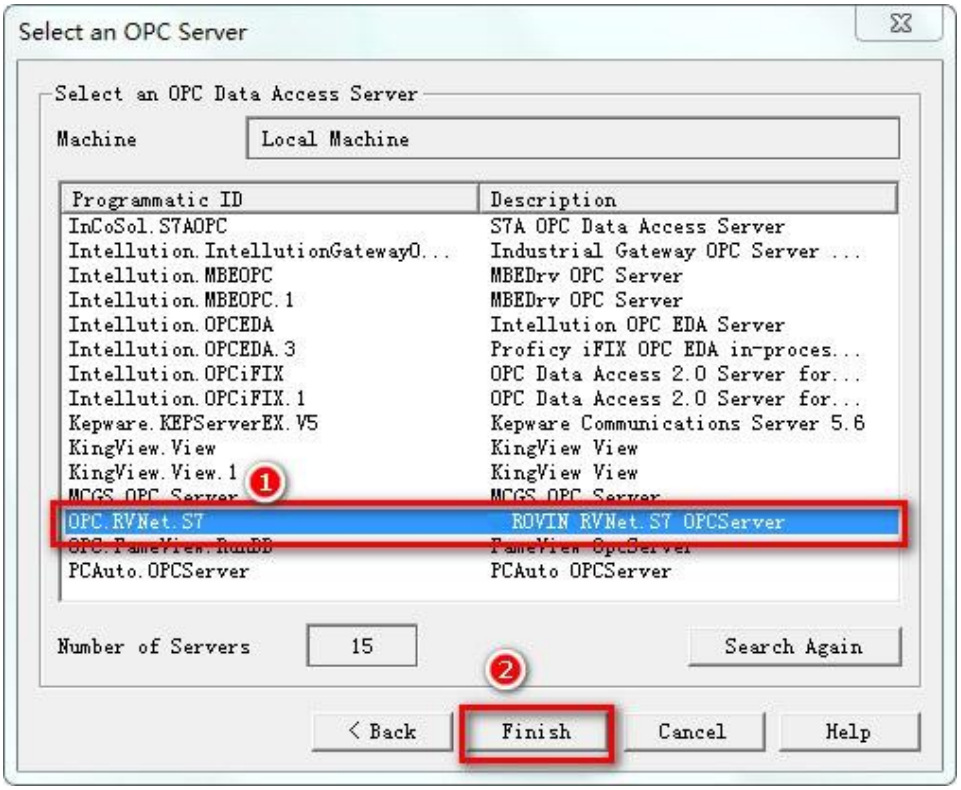
2、选择【OPC Client】驱动；



3、点击【配置(Configure)】，选择本地连接【Use Local OPC Client Driver】，点击【Connet…】连接OPC server；



4、点击【Add OPC Server】，选择 【OPC.RVNet.S7】，点击【Finish】;



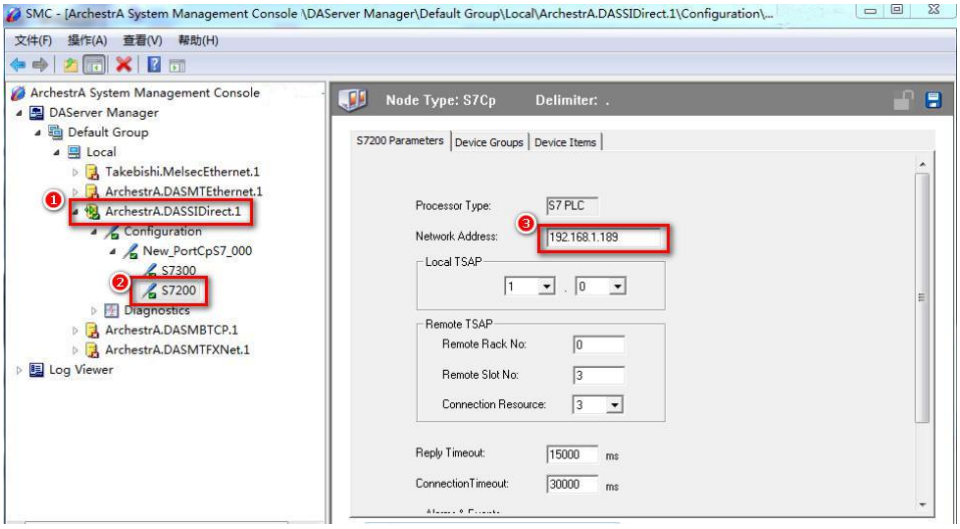
6.7INTOUCH 通讯

6.7.1 连接 S7200

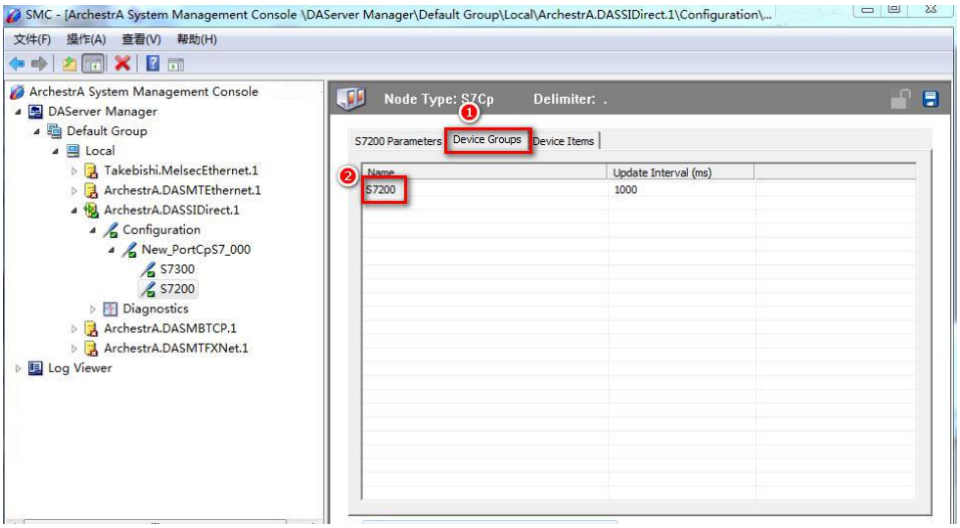
RVNet-S7200 连接 INTOUCH，有两种方式： 西门子 S7TCP 驱动、OPC 驱动。

6.7.1.1 通过西门子 S7TCP 驱动

1、安装西门子S7TCP驱动程序“DASSIDirect”：运行 【开始菜单/程序/Wonderware/System Management Console（SMC）程序】,在DAServer Manager下，找到【DASSIDirect】，如图：
2、右击【Configuration】，在菜单中选择【Add PortCpS7 Object】，右击【New_PortCpS7_000】并选择【Add S7Cp Object】，加入一个S7200的站点；只需要将RVNet-S7200的IP地址填入，其他参数默认；



3、选择【Device Group】属性页，右击点击【Device Group】对话框中的空白地方，选择【Add】，添加一个 Device Group，将【Topic_0】改为需要的名称，比如“S7200”，这个名称需要在INTOUCH中使用；



4、右击【ArchestrA.DASSIDirect】，选择【Activate Server】来启动此 DA Server；

5、打开 INTOUCH 软件，【工具/配置/访问名】，添加访问名来对应 DA Server 中的 S7TCP 站点中的 Device Group。S7200TCP:在【访问名】中填入“S7200TCP”，在【应用程序名】中填入“DASSIDirect”，【主题名】中填入“S7200”；

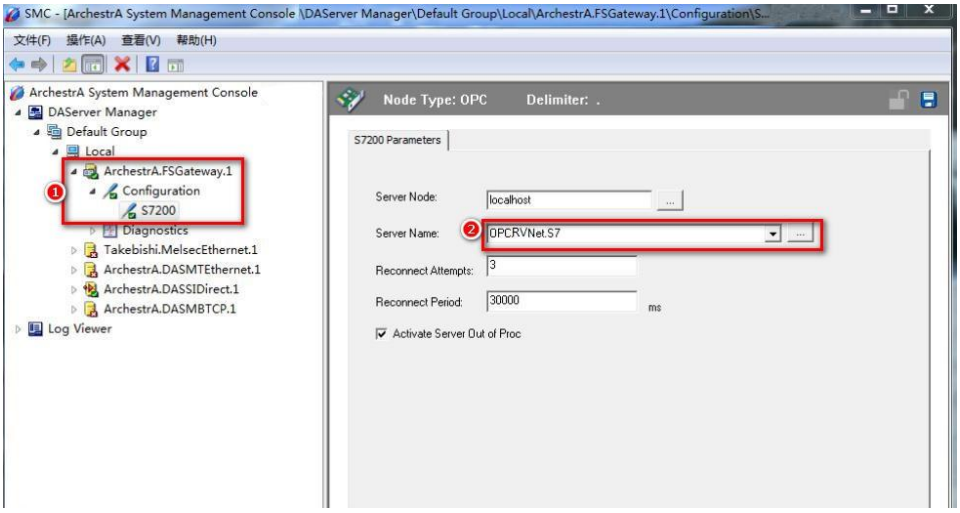
6、选择【标记名字典】，新建 S7200 的变量，填入【标记名】，如：“bbb”；点击【访问名】选择“S7200TCP”；在【项目】中，填入 S7PLC 的地址，如“DB1,w0”，对应 VW0；

4、 通讯在“窗口”中，引用建立的变量，即可以建立 S7PLC 和 INTOUCH 监控画面的通讯。

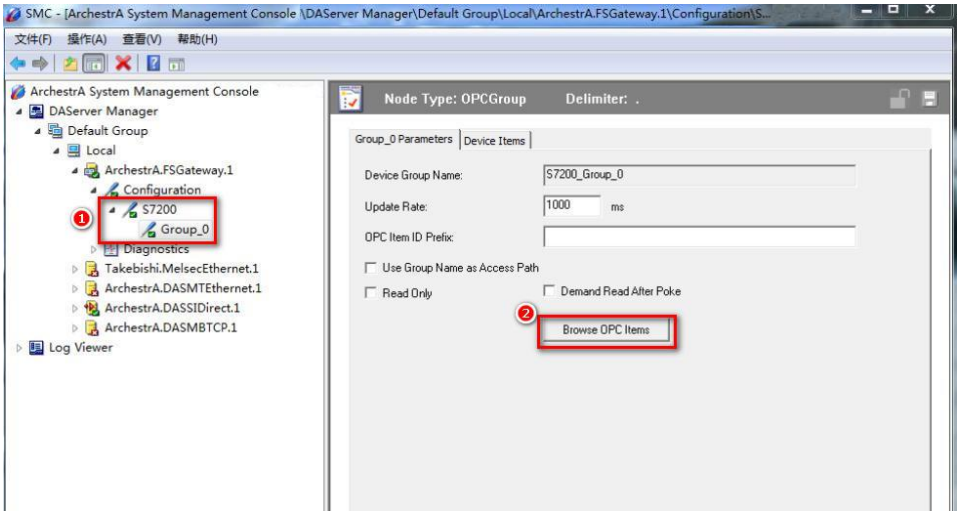
6.7.1.2 通过 RVNetS7OPC

1、安装驱动程序“Factory Suite Gateway”；运行 SMC 程序，在 DAServer Manager 下，找到【FSGateway】；

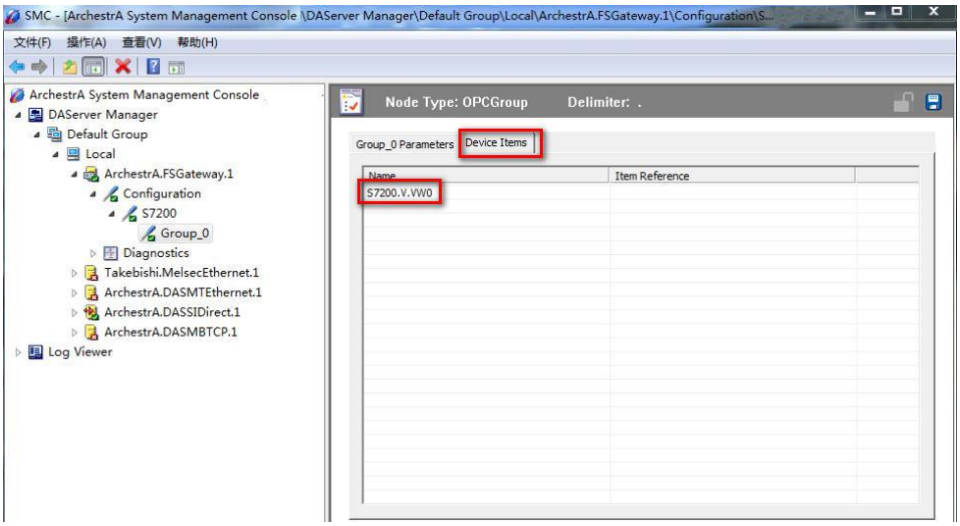
2、右击【Configuration】，在菜单中选择【Add OPC Object】； 在【New_OPC_000】的【Server Name】中，选择 “OPC.RVNet.S7”。



3、右击【S7200】并选择【Add OPC Group Object】,在【Device Group Name】中输入设备组名称，如：“S7200_Group_0”,需要在INTOUCH中使用。



4、点击按钮【Browse OPC Items】，弹出如下窗口，导入OPC.RVNet.S7中组态的变量，可以在【Device Items】中查看导入的变量。



5、右击【ArchestrA. FSGateway】，选择【Activate Server】来启动此 DA Server；

6、打开 INTOUCH 软件，选择【工具/配置/访问名】，添加一个访问名来对应 DA Server 中的 RVNetOPC 站点中的 OPC Group。在“访问名”中填入“S7200_OPC”，在【应用程序名】中填入“FSGateway”，在【主题名】中填入“S7200_Group_0”（注：和 SMC 中的【Device Group Name】对应。）

7、选择【标志名字典】，新建 S7200 的变量，填入【标注名】，如：“aaa”；选择【访问名】，如“S7200_OPC”；在【项目】中，填入 S7PLC 的地址，如“S7200.V.Vw0”，对应 SMC 中【Device Items】。

8、 通讯在【窗口】中，引用建立的变量，即可以建立 S7PLC 和 INTOUCH 监控画面的通讯。

6.7.2 连接 S7300

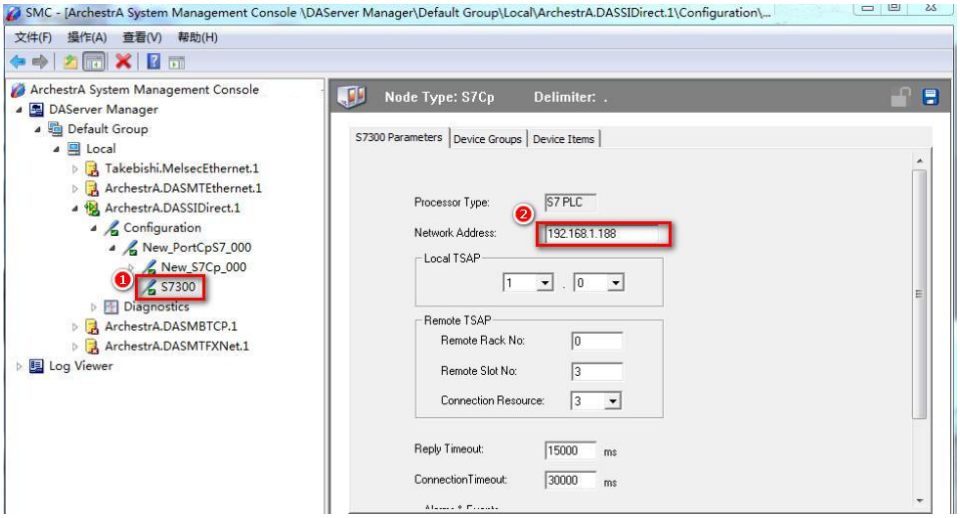
RVNet-S7300 连接 INTOUCH，有两种方式： 西门子 S7TCP 驱动、OPC 驱动。

6.7.2.1 通过西门子 S7TCP 驱动

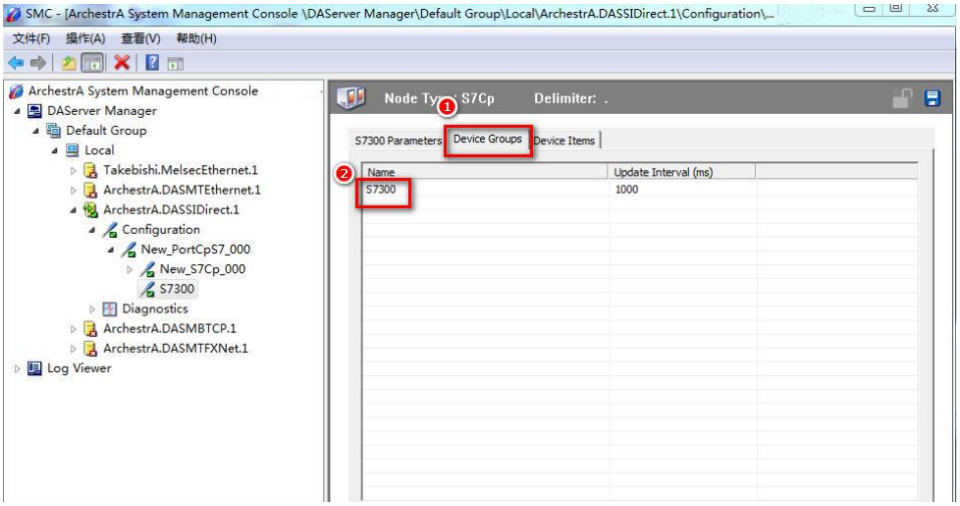
1、安装西门子S7TCP驱动程序“DASSIDirect”：运行 【开始菜单/程序/Wonderware/System

Management Console（SMC）程序】,在DAServer Manager下，找到【DASSIDirect】;

2、右击【Configuration】，在菜单中选择【Add PortCpS7 Object】，右击【New_PortCpS7_000】并选择【Add S7Cp Object】，加入一个S7300的站点；只需要将RVNet-S7300的IP地址填入，其他参数默认；



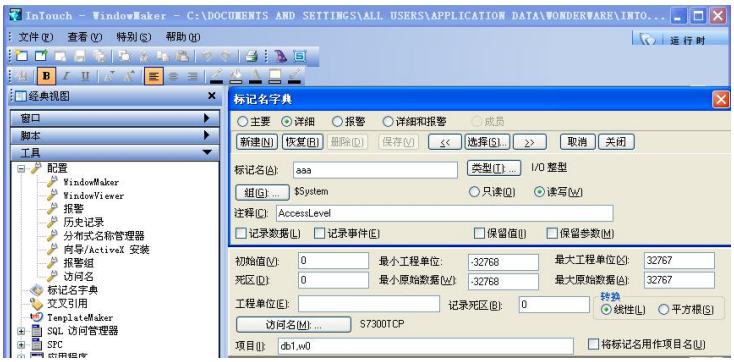
3、选择【Device Group】属性页，右击点击【Device Group】对话框中的空白地方，选择【Add】，添加一个 Device Group，将【Topic_0】改为需要的名称，比如“S7300”，这个名称需要在INTOUCH中使用；



4、右击【ArchestrA.DASSIDirect】，选择【Activate Server】来启动此 DA Server；

5、打开 INTOUCH 软件，【工具/配置/访问名】，添加访问名来对应 DA Server 中的 S7TCP 站点中的 Device Group。S7300TCP:在【访问名】中填入“S7300TCP”，在【应用程序名】中填入“DASSIDirect”，【主题名】中填入“S7300”；

6、选择【标记名字典】，新建 S7300 的变量，填入【标记名】，如："aaa"；点击【访问名】选择"S7300TCP"；在【项目】中，填入 S7PLC 的地址，如"db1,w0"，对应 DB1.DBW0；

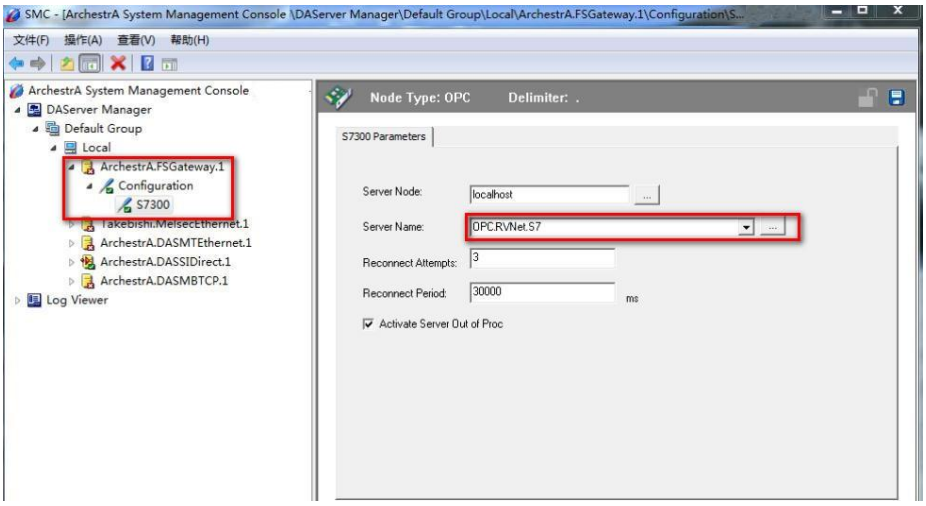


5、 通讯在"窗口"中，引用建立的变量，即可以建立 S7PLC 和 INTOUCH 监控画面的通讯。

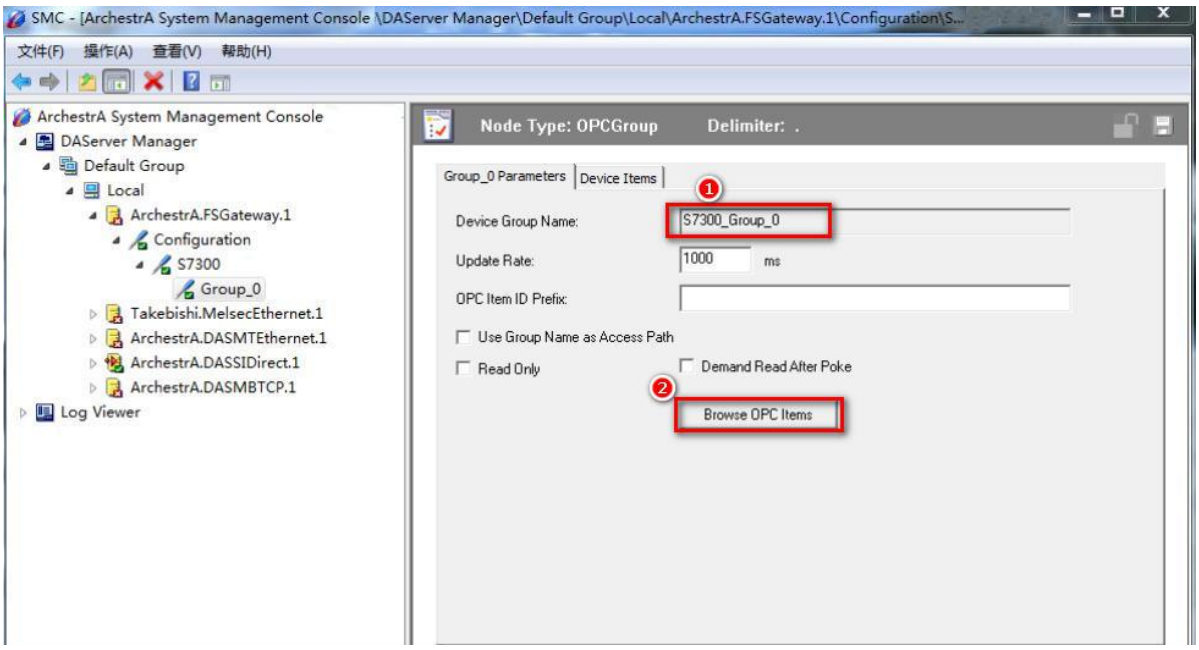
6.7.2.2 通过 RVNetS7OPC

1、安装驱动程序【Factory Suite Gateway】，运行 SMC 程序，在 DAServer Manager 下，找到【FSGateway】；

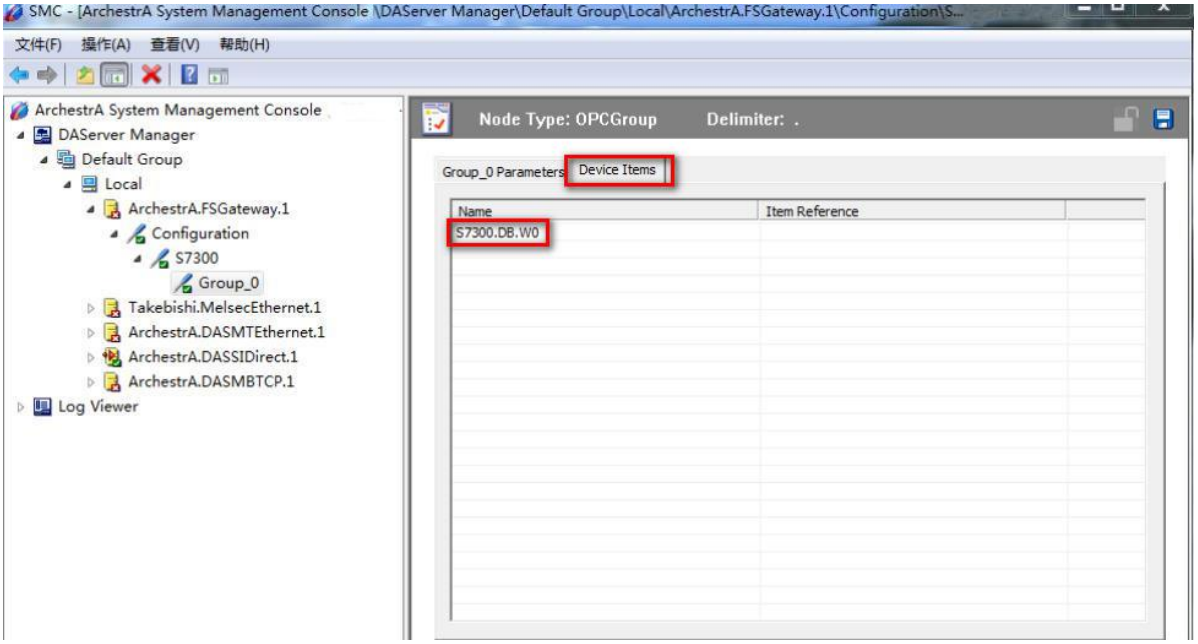
2、右击【Configuration】，在菜单中选择【Add OPC Object】， 在【New_OPC_000】的【Server Name】中，选择"OPC.RVNet.S7"。



3、右击【S7300】并选择【Add OPC Group Object】,在【Device Group Name】中输入设备组名称，如：“S7300_Group_0”,需要在INTOUCH中使用。



4、点击按钮【Browse OPC Items】，弹出如下窗口，导入OPC.RVNet.S7中组态的变量，可以在【Device Items】中查看导入的变量。



5、右击【ArchestrA. FSGateway】，选择【Activate Server】来启动此 DA Server；

6、打开 INTOUCH 软件，选择【工具/配置/访问名】，添加一个访问名来对应 DA Server 中的 RVNetOPC 站点中的 OPC Group。在“访问名”中填入“S7300_OPC”，在【应用程序名】中填入“FSGateway”，在【主题名】中填入“S7300_Group_0”（注：和 SMC 中的【Device Group Name】对应。）

7、选择【标志名字典】，新建 S7300 的变量，填入【标注名】，如："ddd"；选择【访问名】，如"S7300_OPC"；在【项目】中，填入 S7PLC 的地址，如"S7300.DB. W0"，对应 SMC 中【Device Items】。

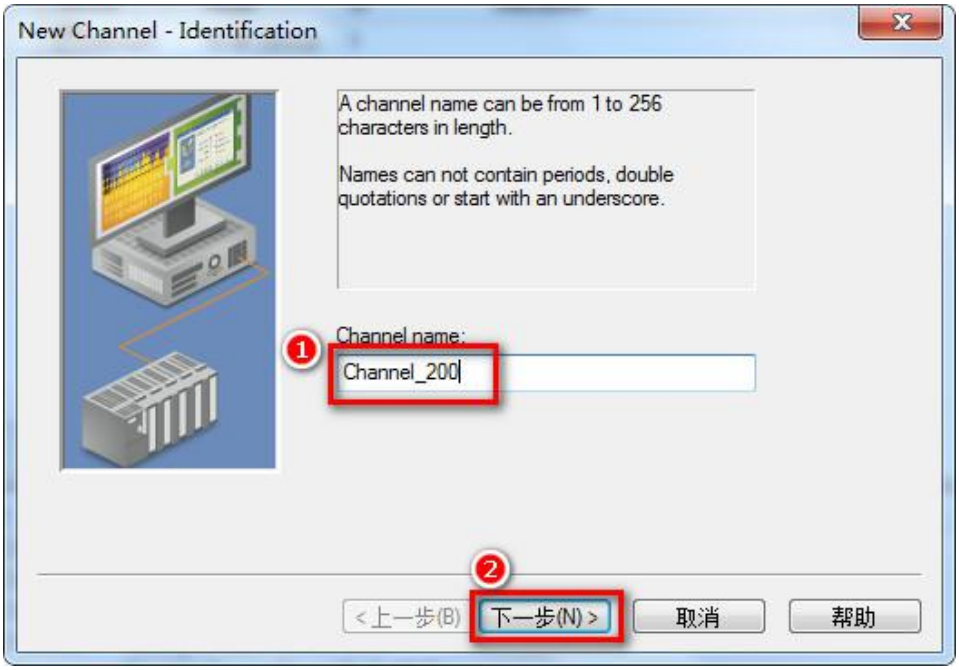
9、 通讯在【窗口】中，引用建立的变量，即可以建立 S7PLC 和 INTOUCH 监控画面的通讯。

6.8LABVIEW 通讯

6.8.1 连接 S7200

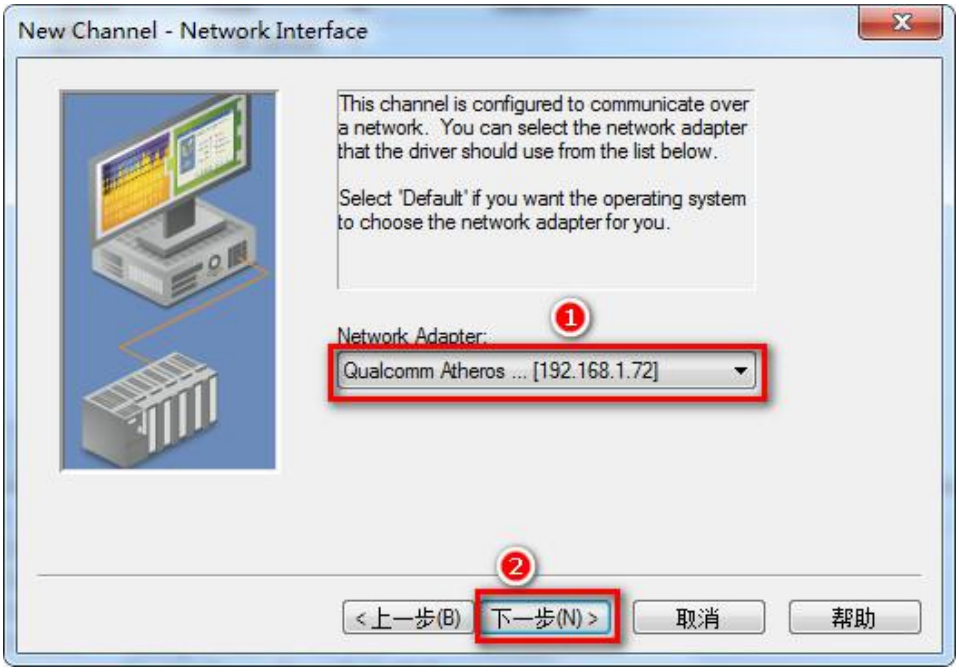
通过 NI OPC Servers 连接

1. 打开 NI OPC Servers 软件。
2. 新建一个 Channel，这里取名"Channel_200"，点击【下一步】;

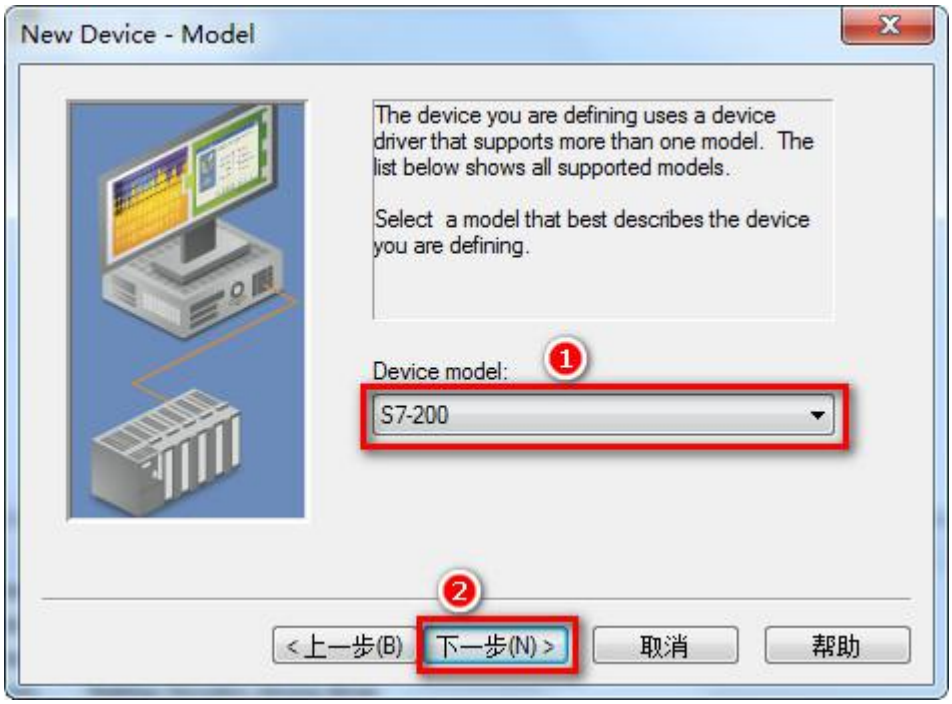


3. 在【Device driver】中选择【Siemens TCP/IP Ethernet】,点击【下一步】。

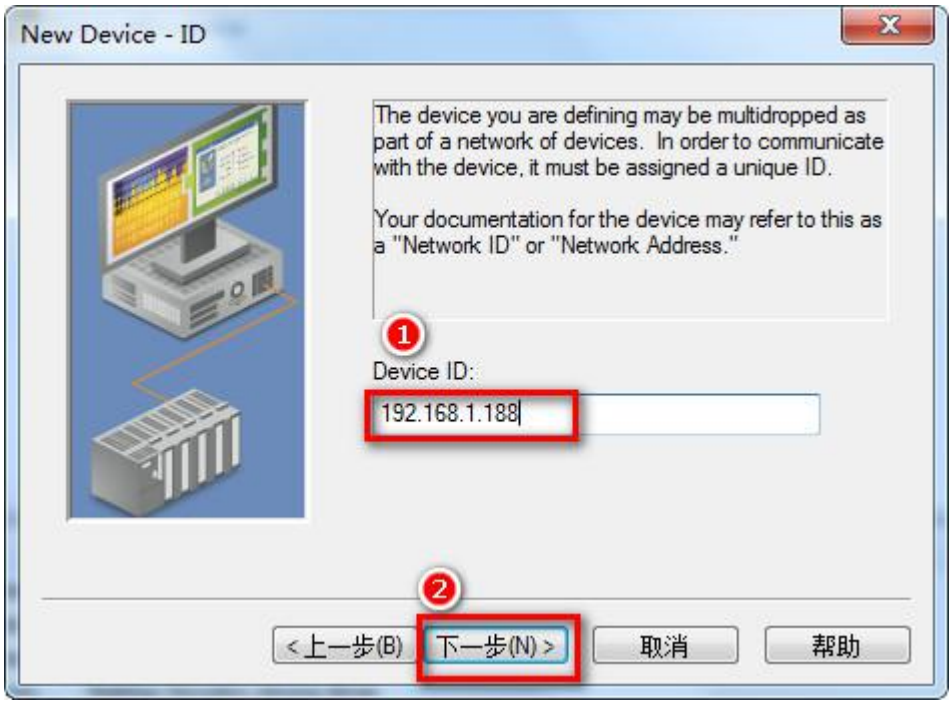
4. 在【Network Adapter】中选择你的网卡信息，点击【下一步】。



5. 选择默认参数，点击【下一步】直到【完成】。
6. 在刚建立的 Channel 下新建一个 Device,点击【下一步】，在【Device model】下选择【S7 200】，点击【下一步】。



7. 在【Device ID】下面填入 RVNet-S7200 的 IP 地址，点击【下一步】，其它参数默认直至完成。

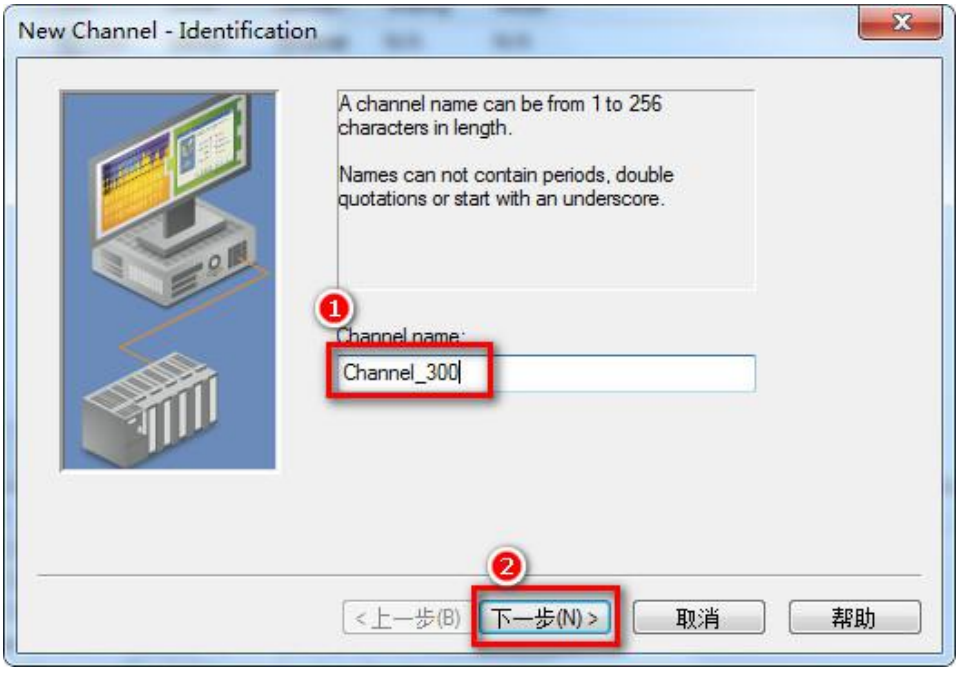


8. 选择默认参数，点击【下一步】直到【完成】。

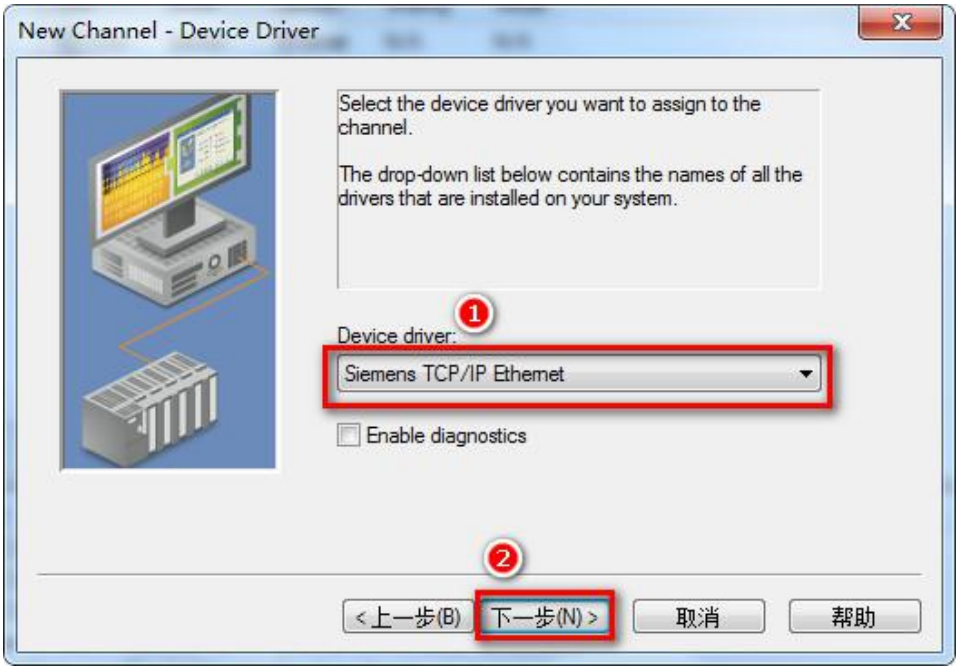
6.8.2 连接 S7300

通过 NI OPC Servers 连接

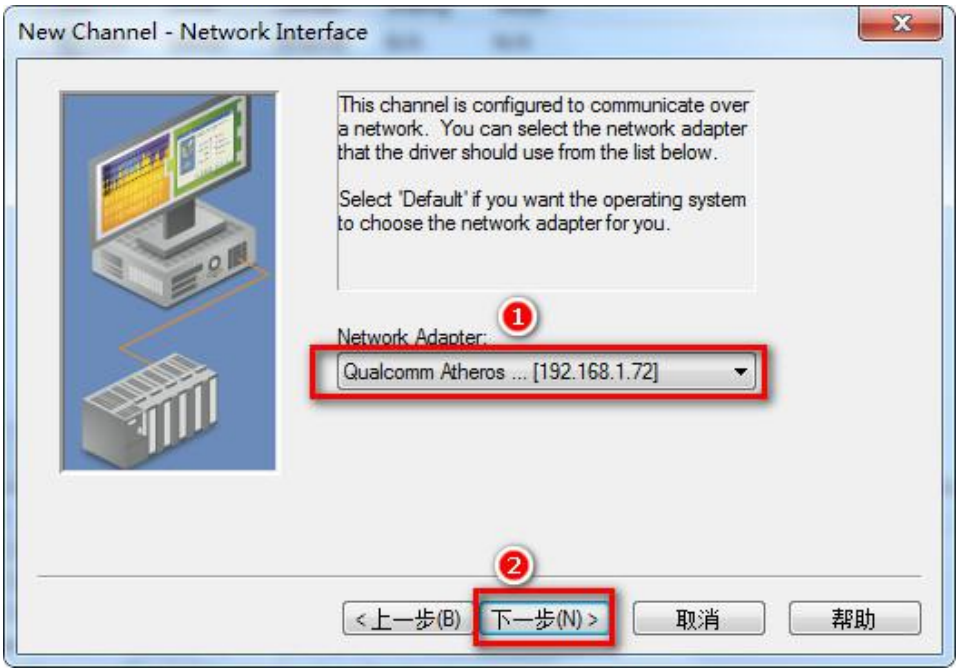
1、打开 NI OPC Servers 软件。新建一个 Channel,这里取名“Channel_300”,点击【下一步】;



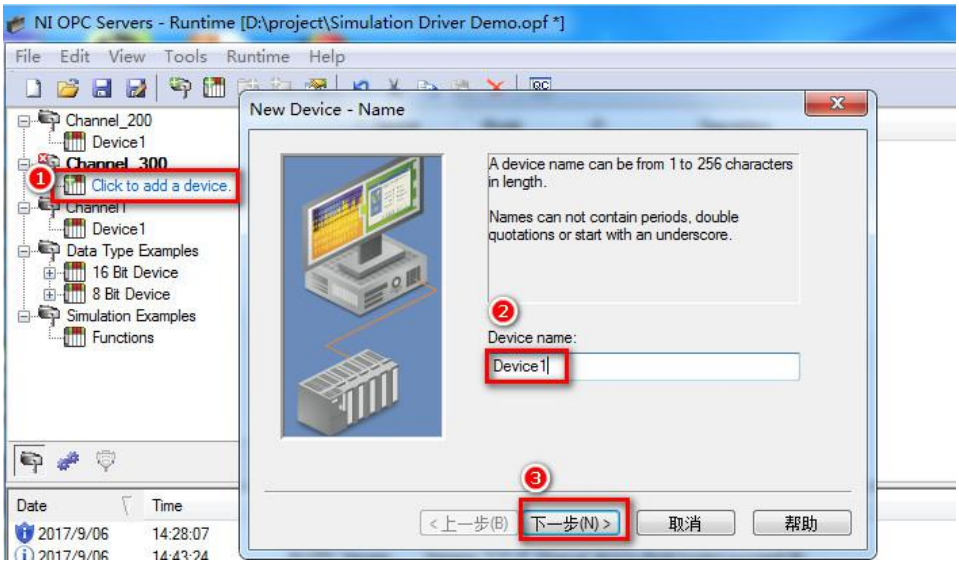
2、 在【Device driver】中选择【Siemens TCP/IP Ethernet】,点击【下一步】;



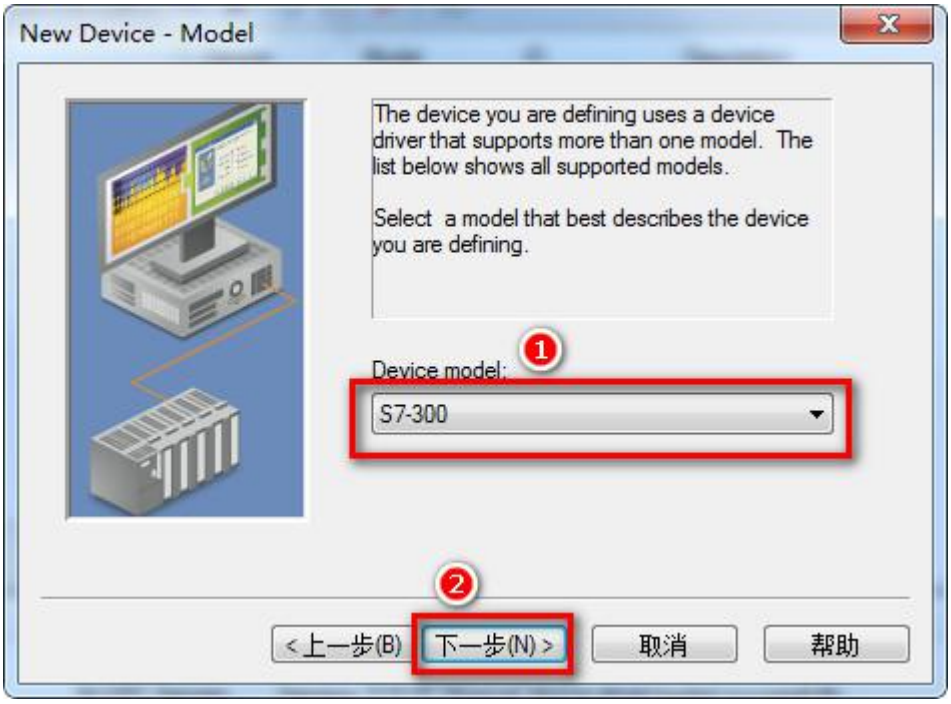
3、 在【Network Adapter】中选择你的网卡信息，点击【下一步】，根据向导完成参数设置；



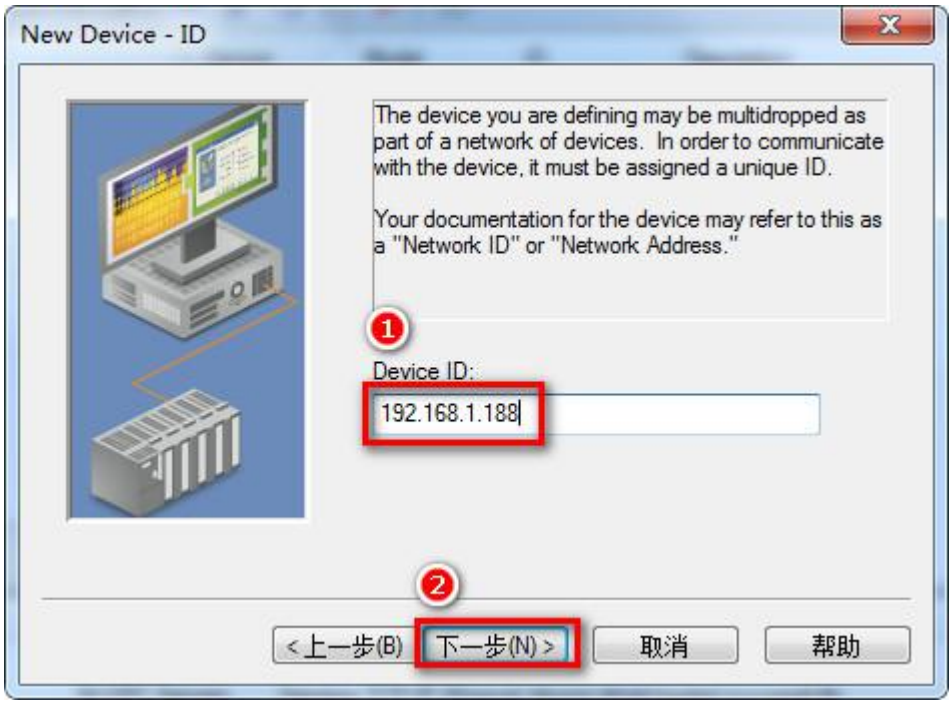
4、 在刚建立的 Channel 下新建一个 Device,这里取名“Device1”,点击【下一步】;



5、 在【Device model】下选择【S7 300】，点击【下一步】;



6、 在【Device ID】下面填入 RVNet-S7300 的 IP 地址，点击【下一步】，其它参数默认，直至完成。

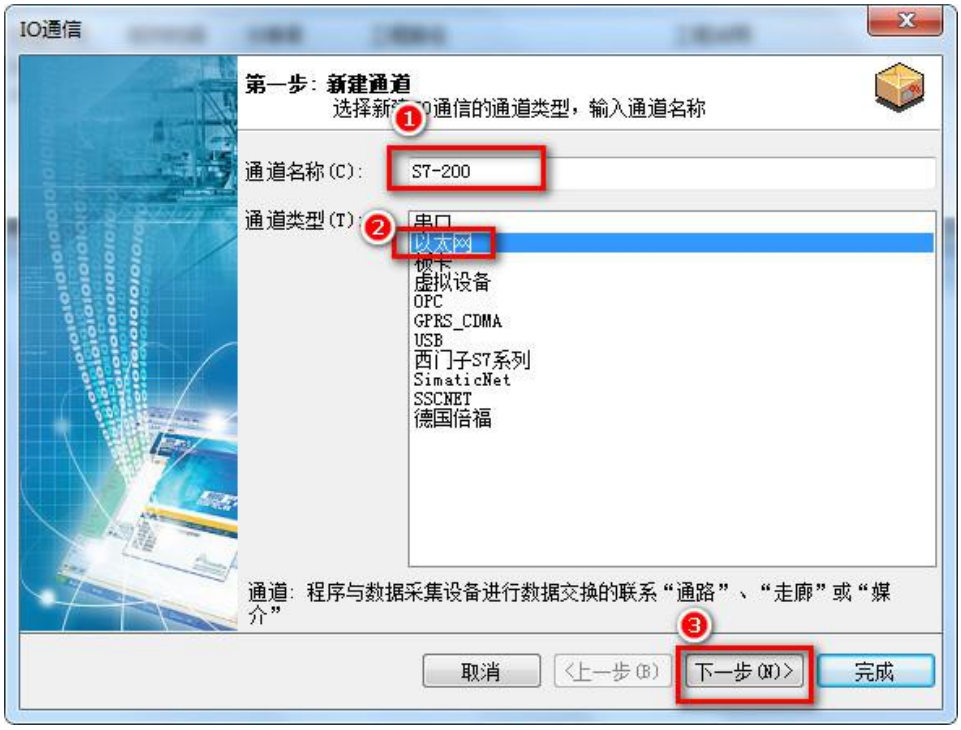


6.9 易控通讯

6.9.1 连接 S7200

通过西门子以太网驱动连接。

1、右击工程目录下的【IO 设备】，点击【新建】，输入通道名称，通道类型选择【以太网】通讯方式；



2、配置通道-远程节点中【IP 地址】填入 RVNet-S7200 的 IP 地址，【IP 端口】填入 102，点击【测试】，完成配置；

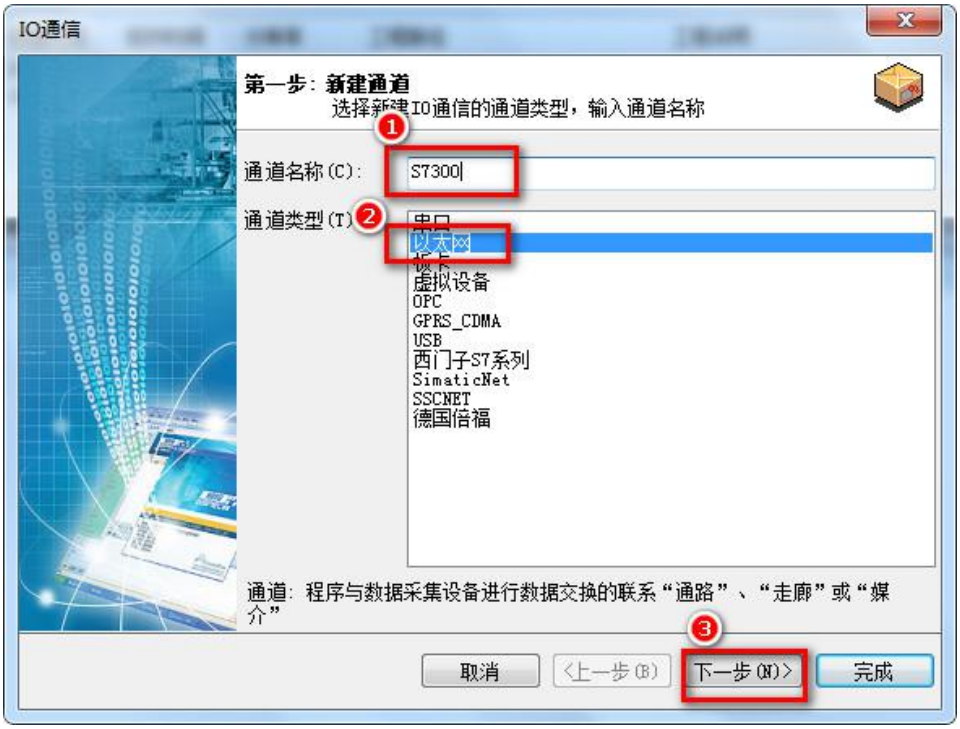
3、新建设备-在 PLC 中选择【西门子—S7200 以太网】，填入设备名称；【设备地址】填入 PLC 的站地址。

4、打开工程菜单【IO 通信】组下的【S7200 以太网】，添加变量和测试监控。

6.9.2 连接 S7300

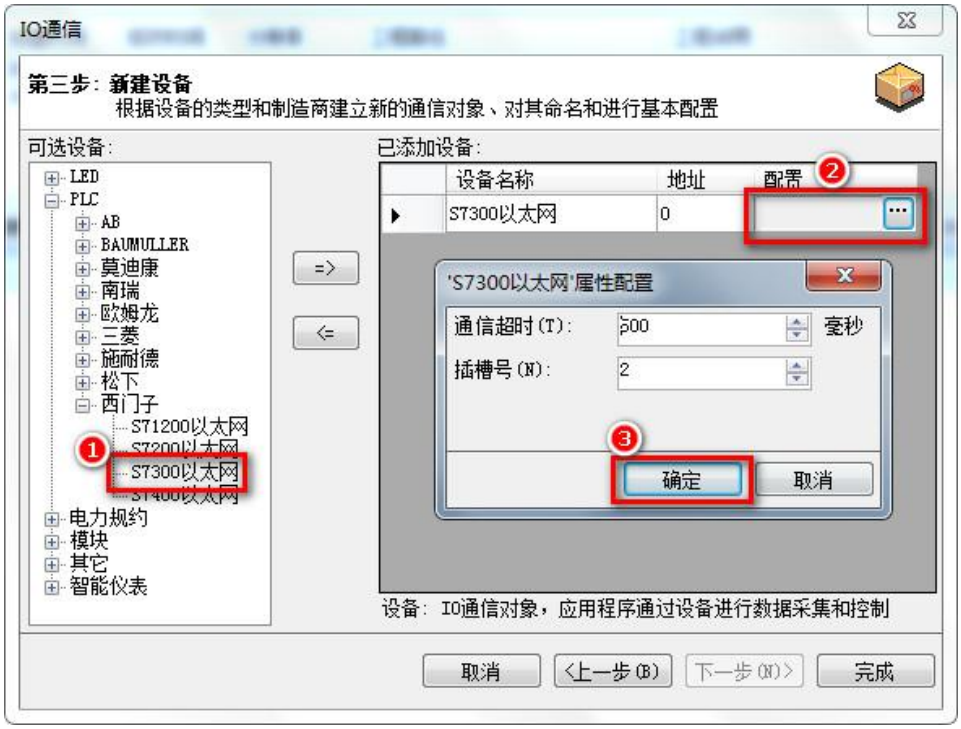
通过西门子以太网驱动连接

1、新建通道，选择【以太网】通讯方式，填入通道名称；



2、配置通道-远程节点中【IP 地址】填入 RVNet-S7300 的 IP 地址，【IP 端口】填入 102，点击【测试】，完成配置；

3）新建设备-在 PLC 中选择【西门子-S7300 以太网】，填入设备名称；



4）添加变量和测试监控；

7.OPC 通讯

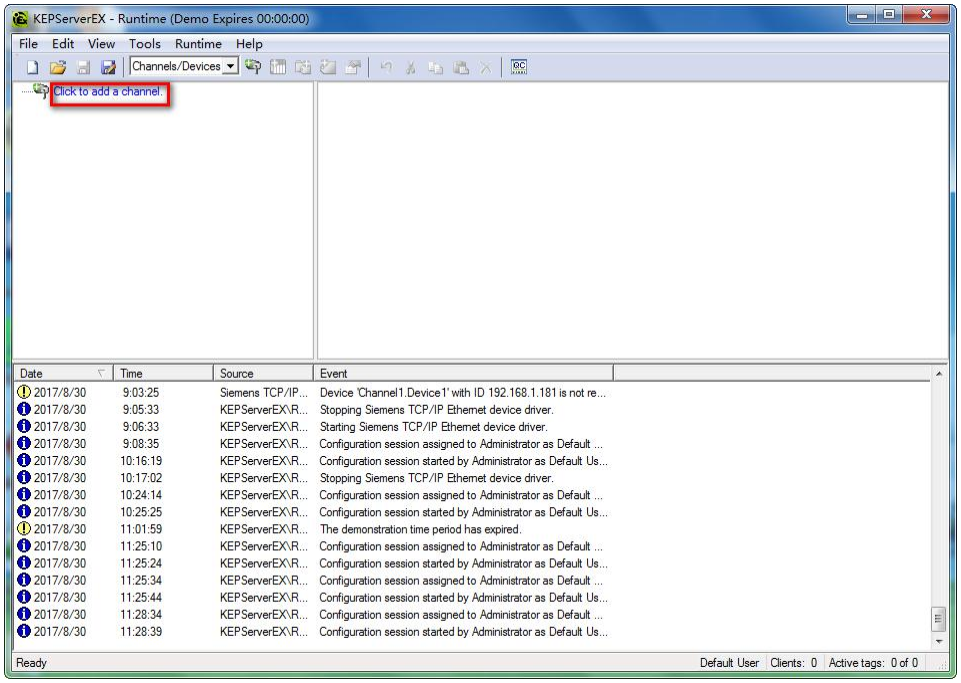
7.1Kepware OPC 通讯

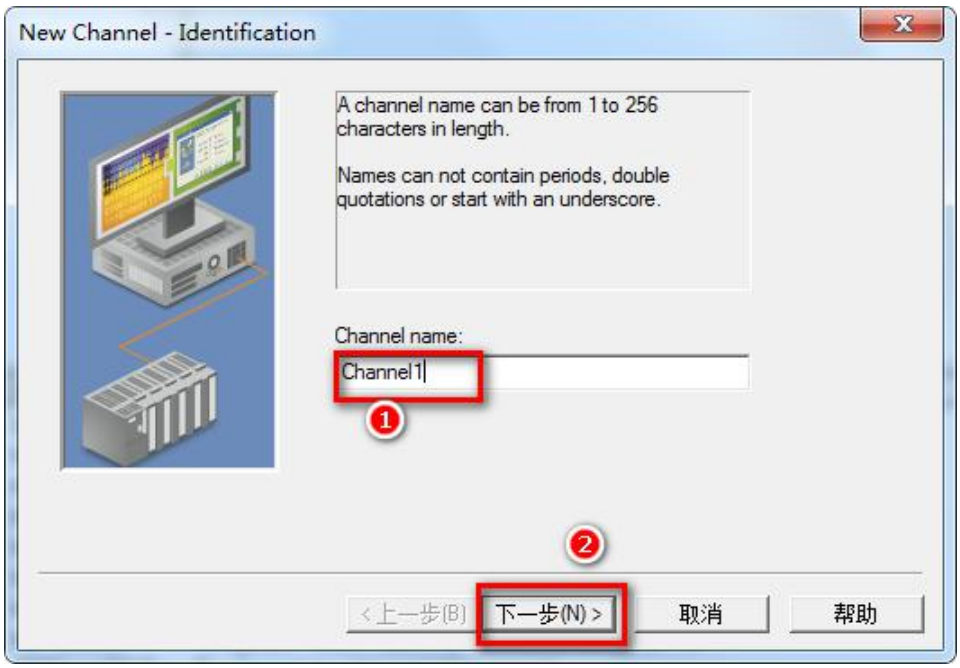
7.1.1 连接 S7200

西门子 S7-200 通过 RVNet-S7200 连接 KepWare OPC，可以采用西门子 S7TCP 驱动。

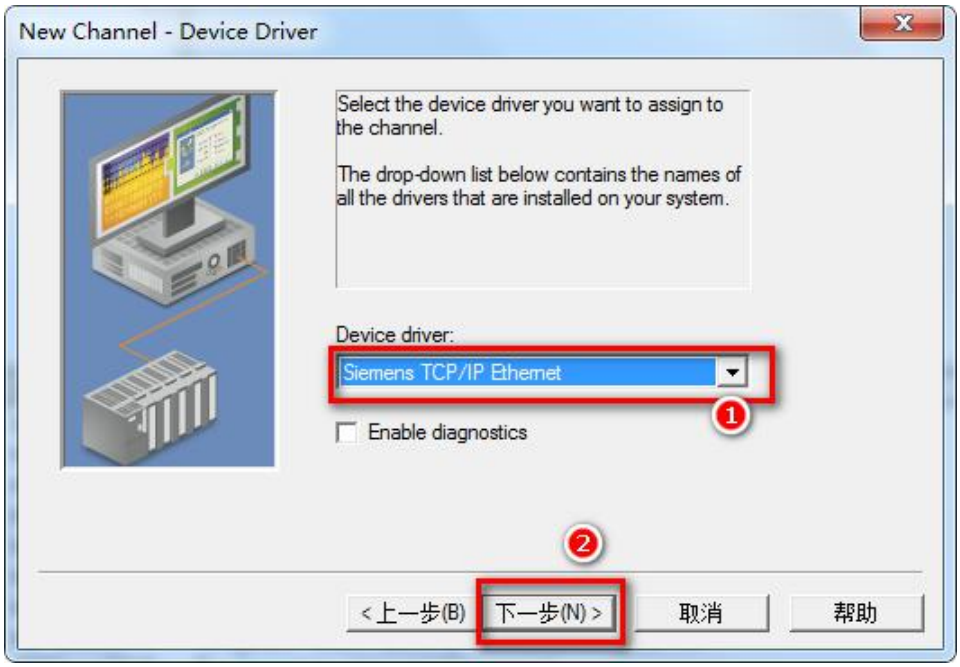
7.1.1.1 添加通道

1、打开 Kepware OPC Configuration，增加一个通道，填入通道名称，点击【下一步】;

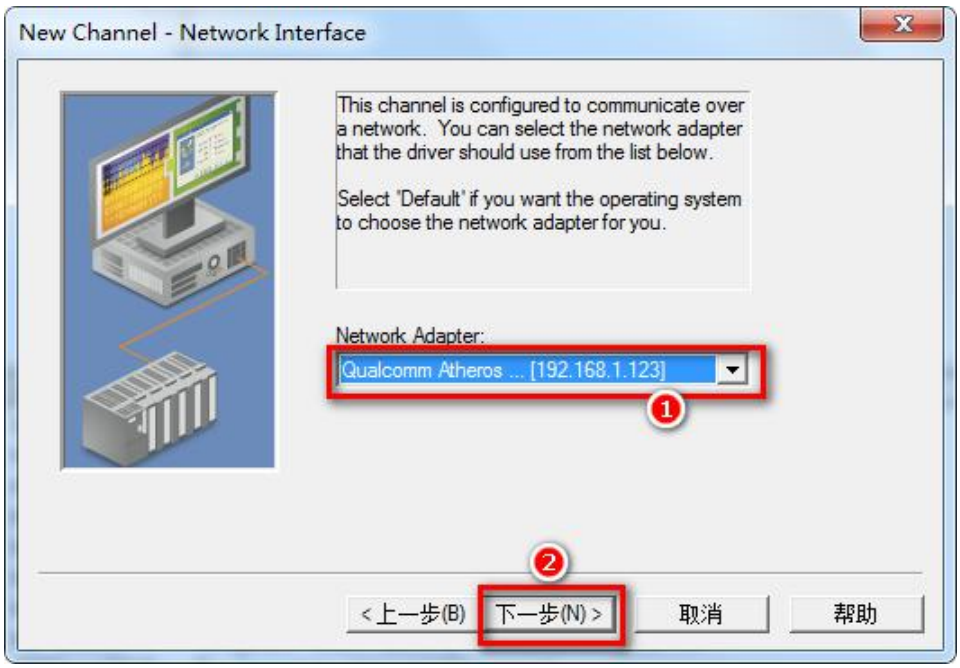




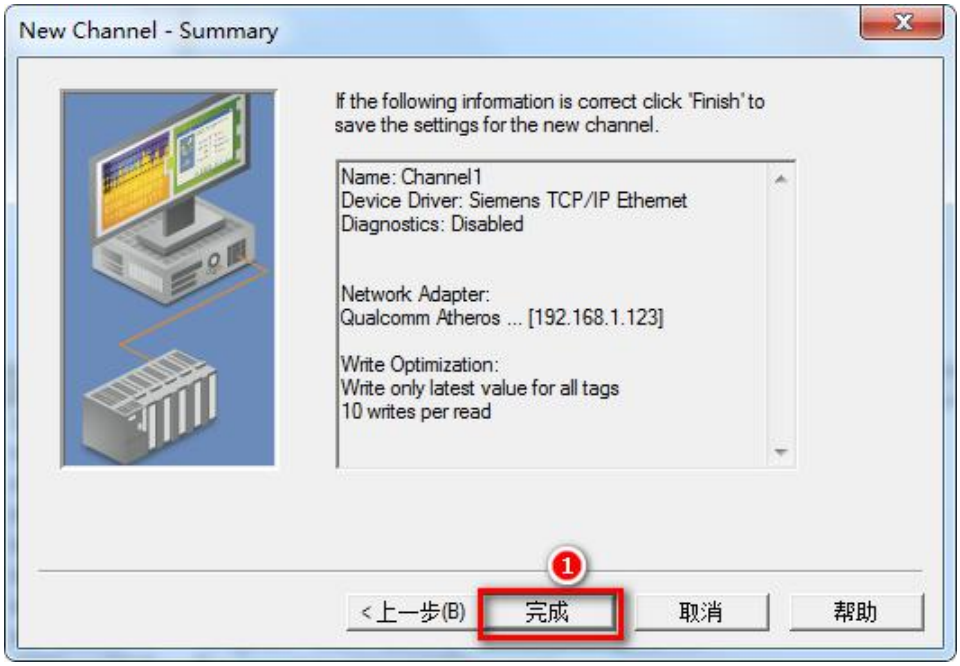
2、【Device driver】选择【Siemens TCP/IP Ethernet】驱动，点击【下一步】;



3、【Network Adapter】选择计算机网卡；

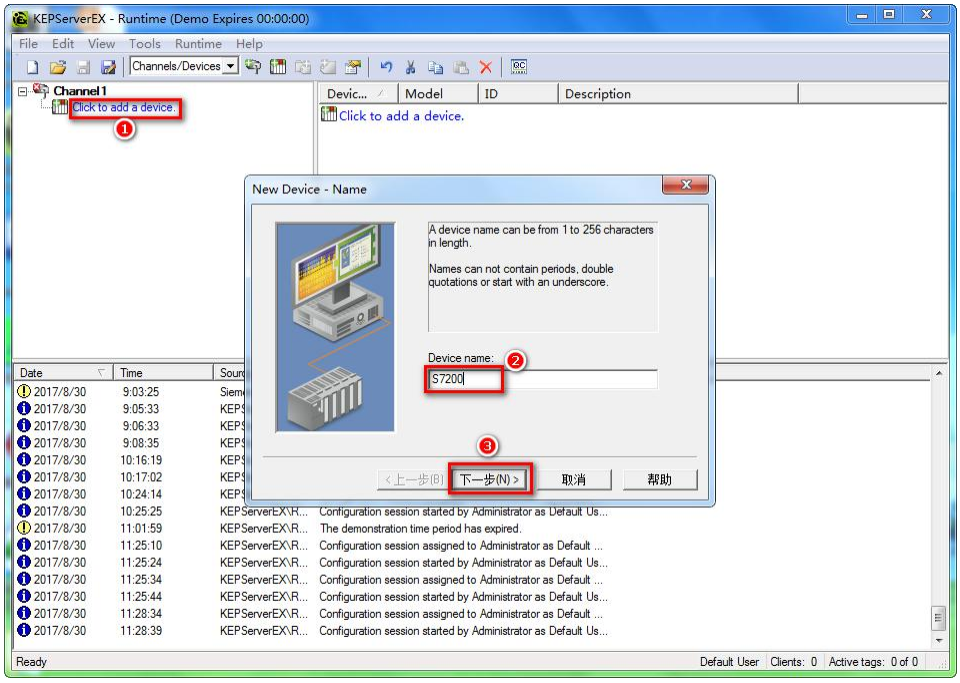


4、根据需要选择模式（可默认），依照向导完成通道参数设置；

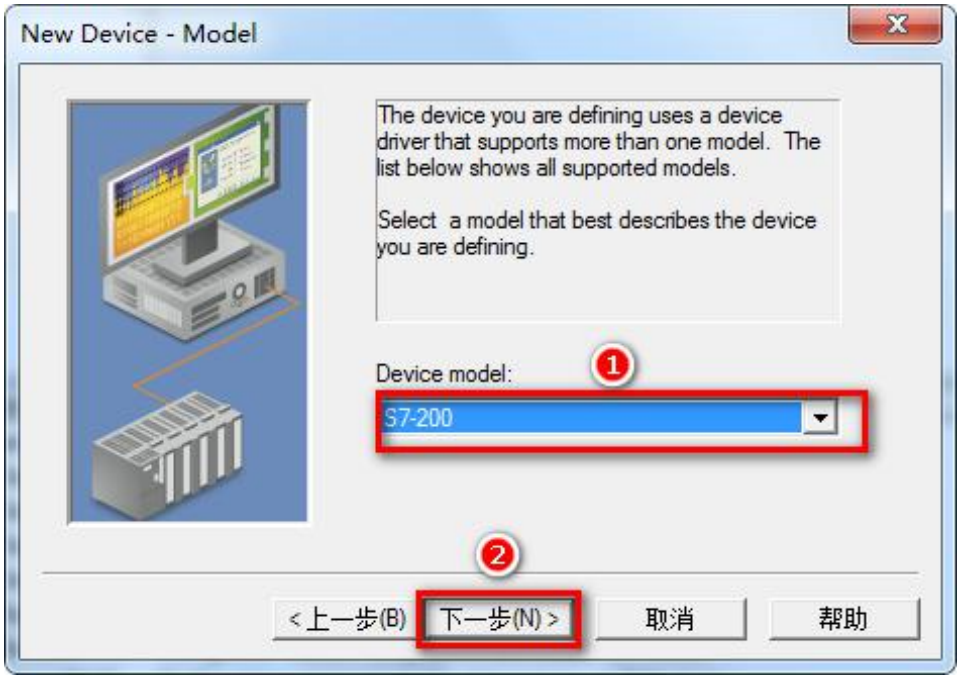


7.1.1.2 添加设备

1、增加设备，填入设备名称，点击【下一步】;

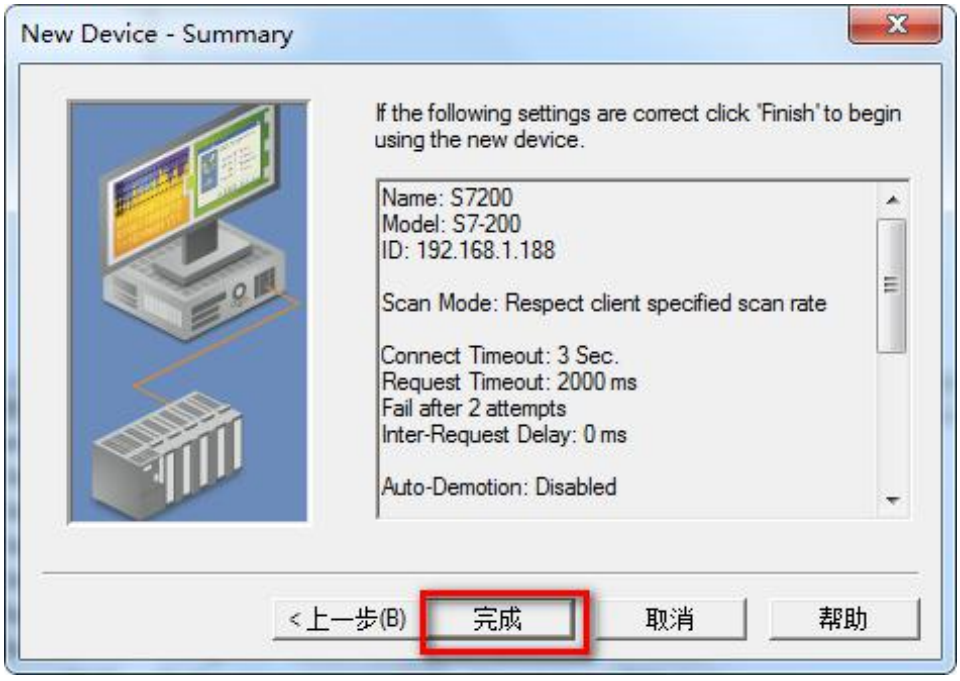


2、【Device model】选择 S7-200;



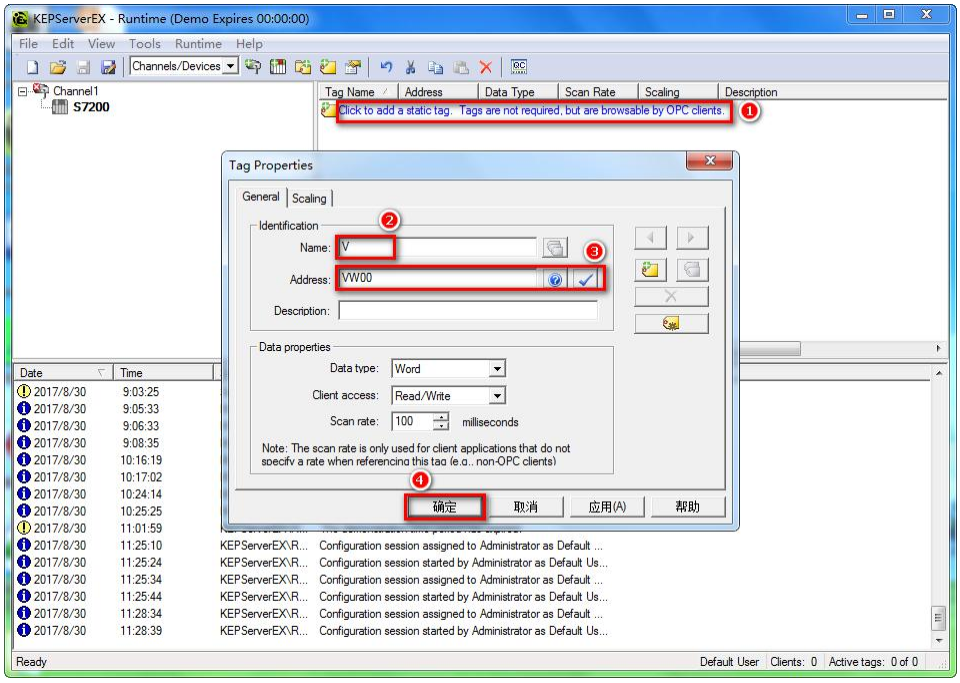
3、【Device ID】填入 RVNet-S7200 的 IP 地址，点击【下一步】;

4、依照向导完成设置。



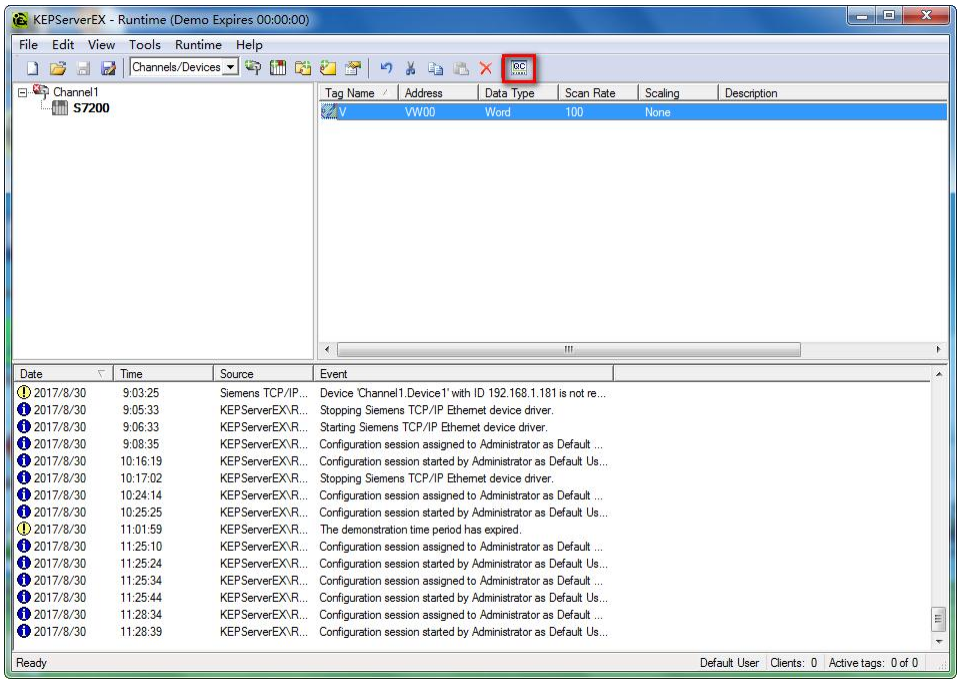
7.1.1.3 添加标签

1、按下图单击框①，弹出 Tag Properties 窗口，在框②设置变量，点击框③的  选择变量，单击  ，然后点击确定；



7.1.1.4 变量测试

1、在 OPC 客户端验证数据通讯。

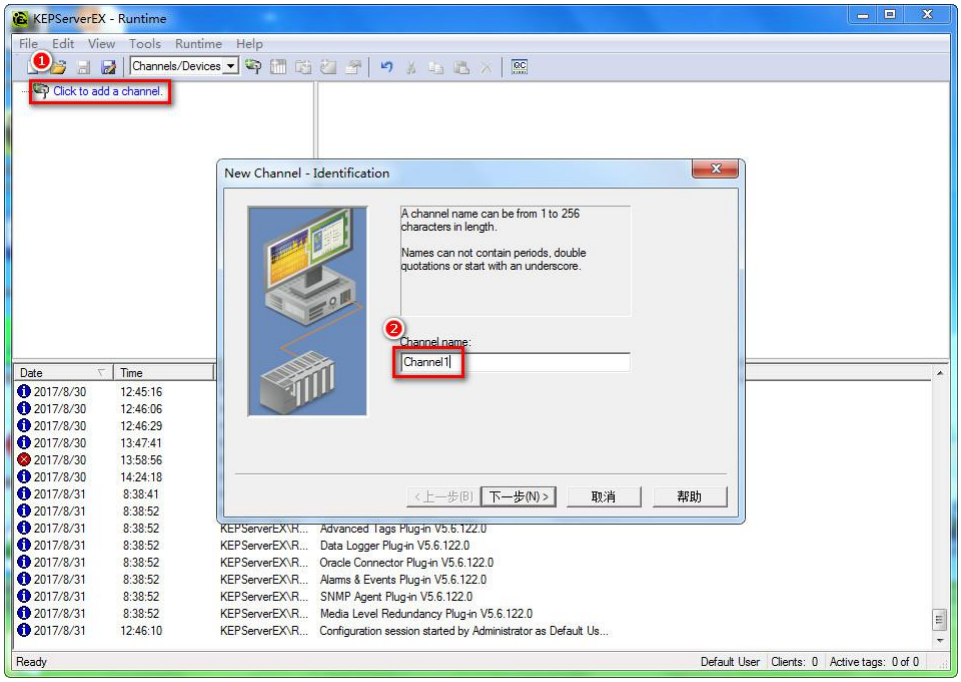


7.1.2 连接 S7300

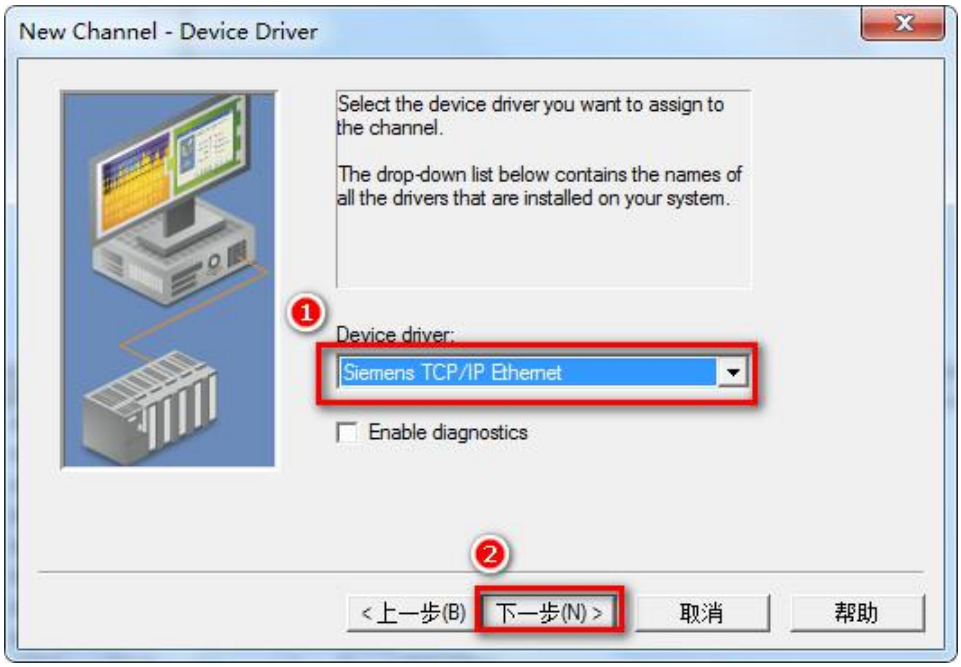
西门子 S7-300/400 通过 RVNet-S7300 连接 KepWare OPC，可以采用西门子 S7TCP 驱动。

7.1.2.1 添加通道

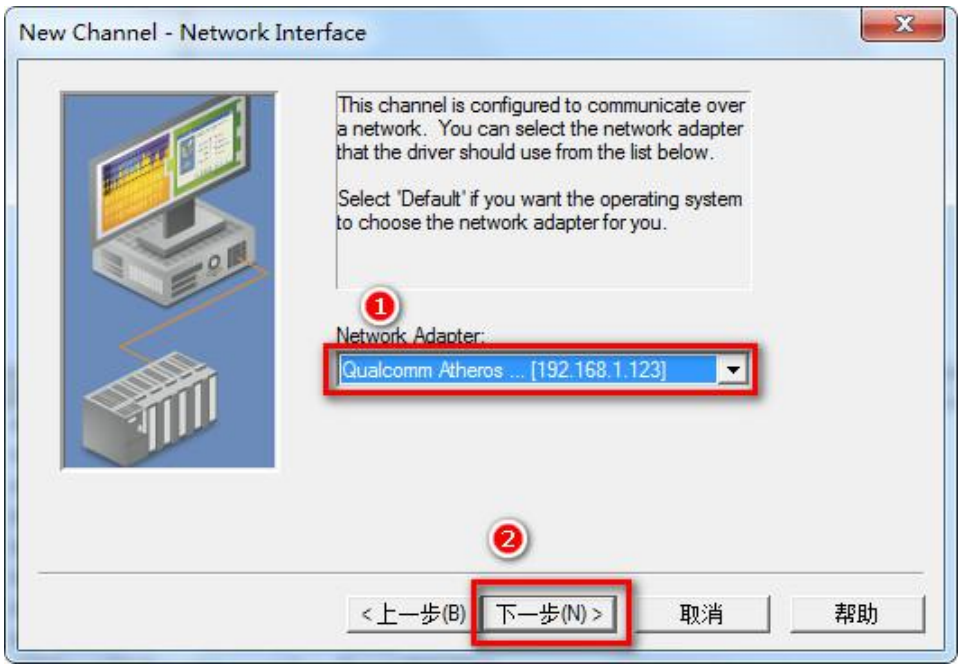
1、打开 Kepware OPC Configuration，增加一个通道，填入通道名称，点击【下一步】;



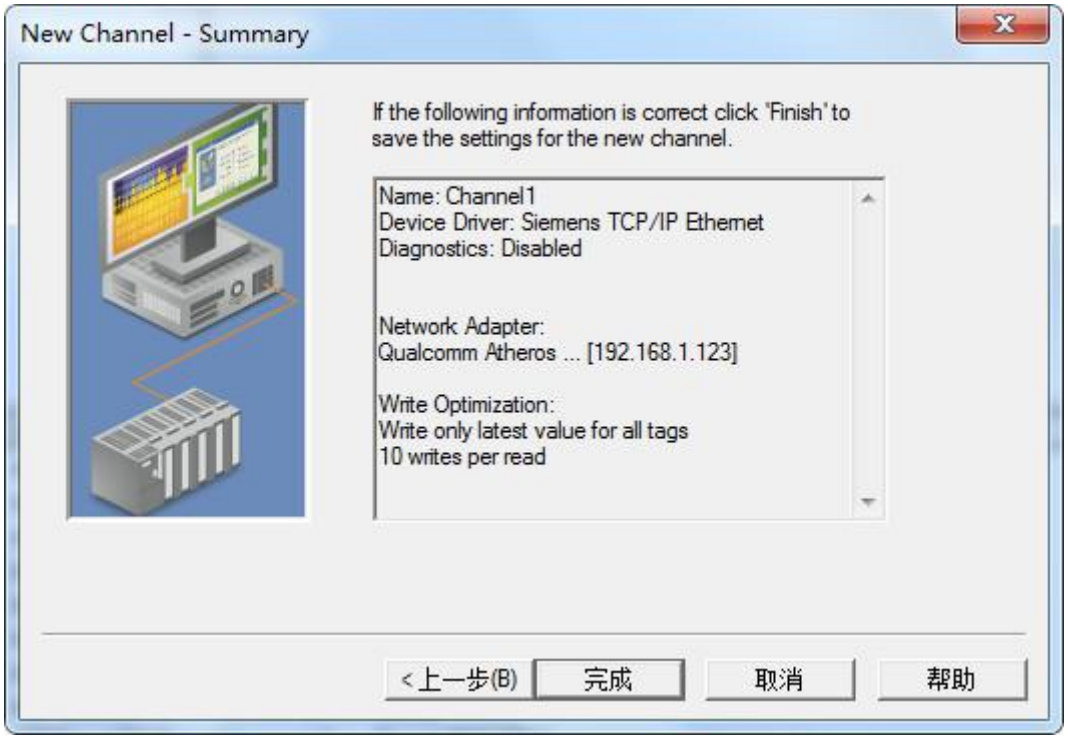
2、选择【Siemens TCP/IP Ethernet】驱动，点击【下一步】;



3、【Network Adapter】选择计算机网卡；

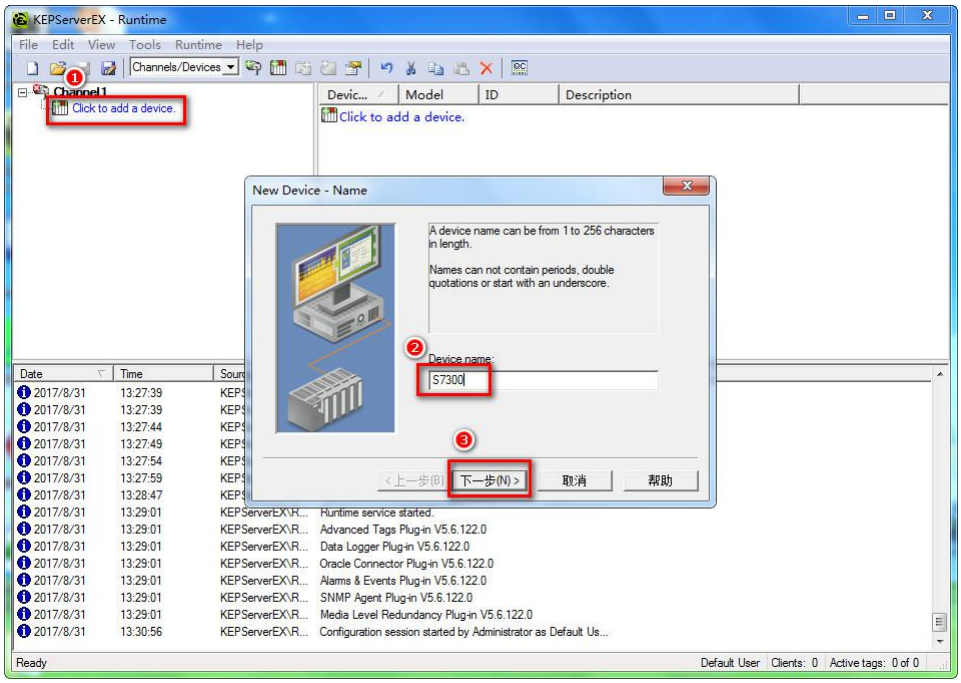


4、根据需要选择模式（可默认），完成通道参数设置；

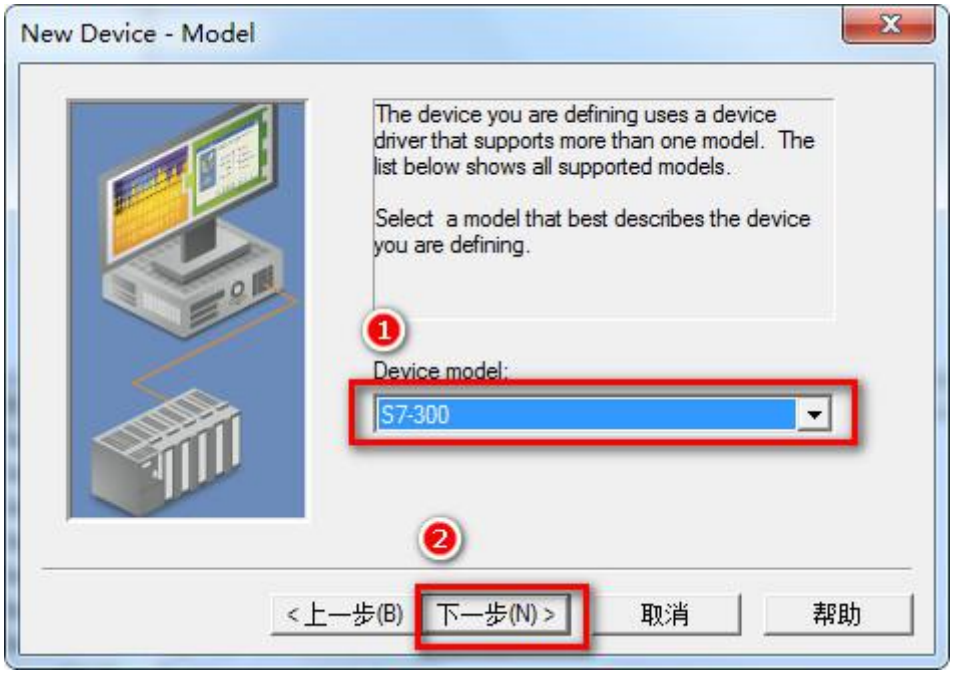


7.1.2.2 添加设备

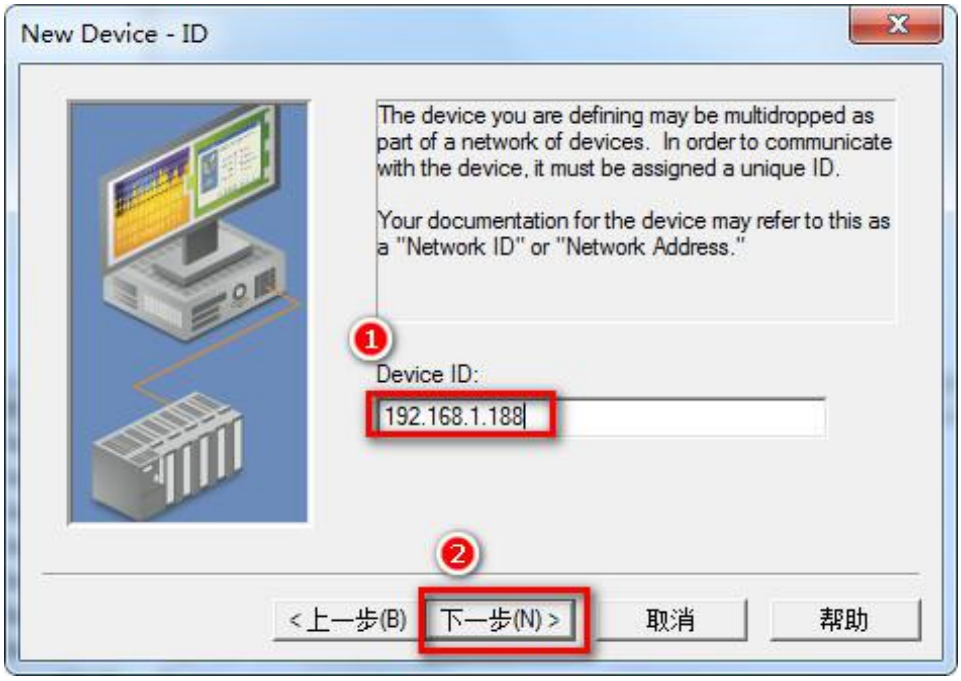
1、增加设备，填入设备名称，点击【下一步】;



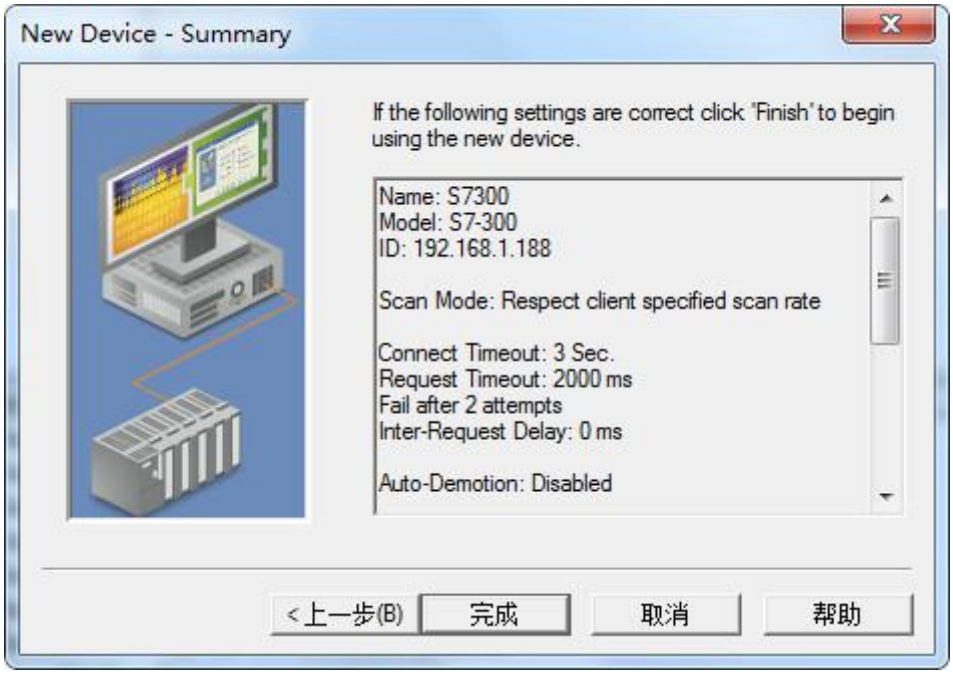
2、【Device model】选择 S7-300，下一步；



3、【Device ID】填入 RVNet-S7300 的 IP 地址，下一步；



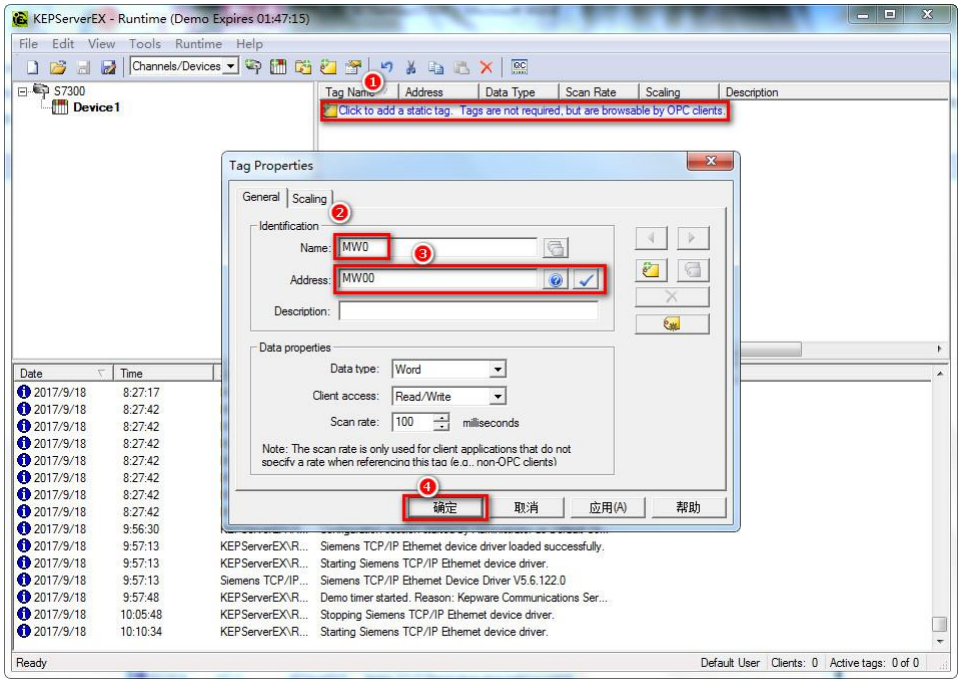
4、其他参数可以默认，完成设备设置。



7.1.2.3 添加变量

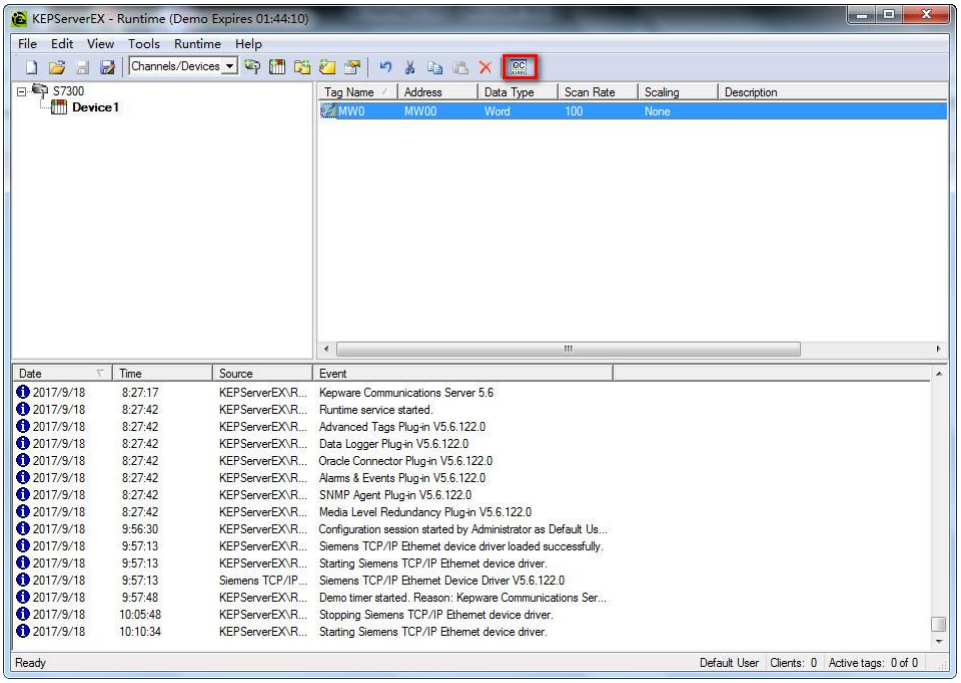
1、按下图单击框①，弹出 Tag Properties 窗口，在框②设置变量，点击框③的 选择变量，单击 ，

然后点击确定；



7.1.2.4 变量测试

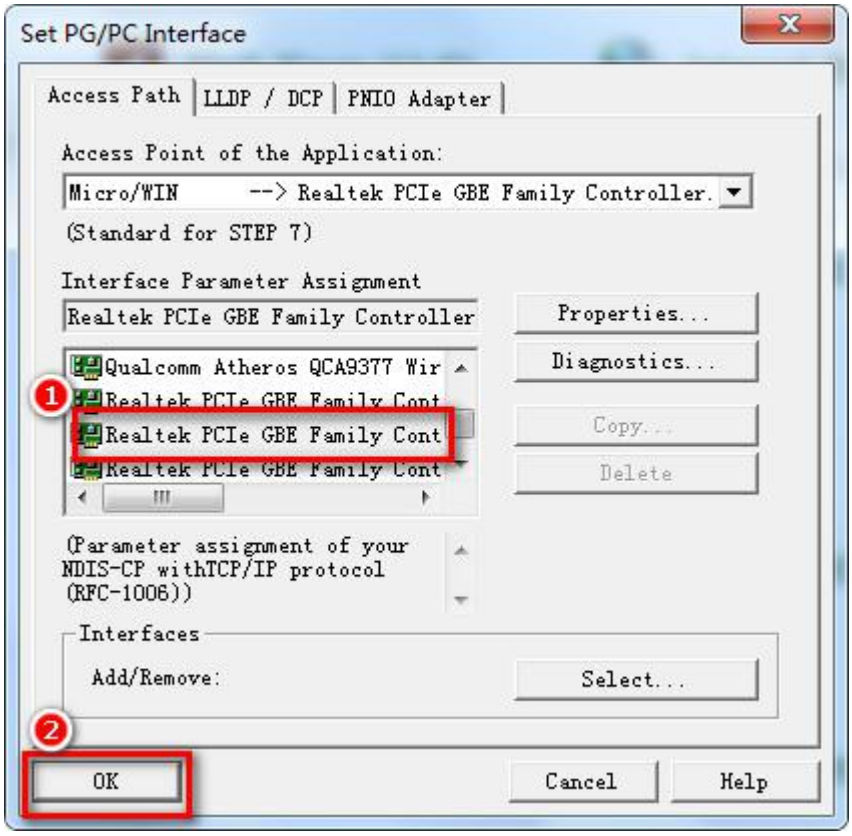
1、 在 OPC 客户端验证通讯。



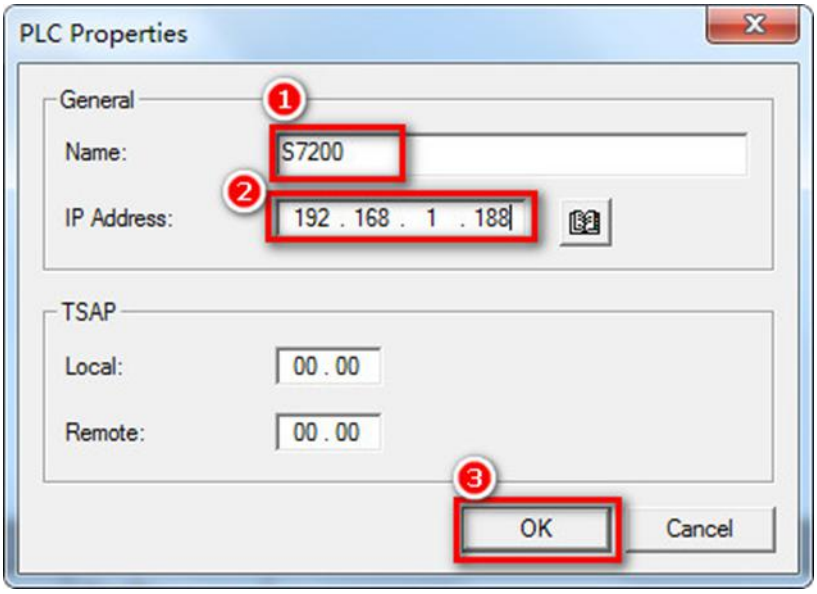
7.2PC Access 通讯

1、 通过控制面板或者 MicroWIN 软件，打开【设置 PG/PC 接口】，选择 MicroWIN 指向网卡;

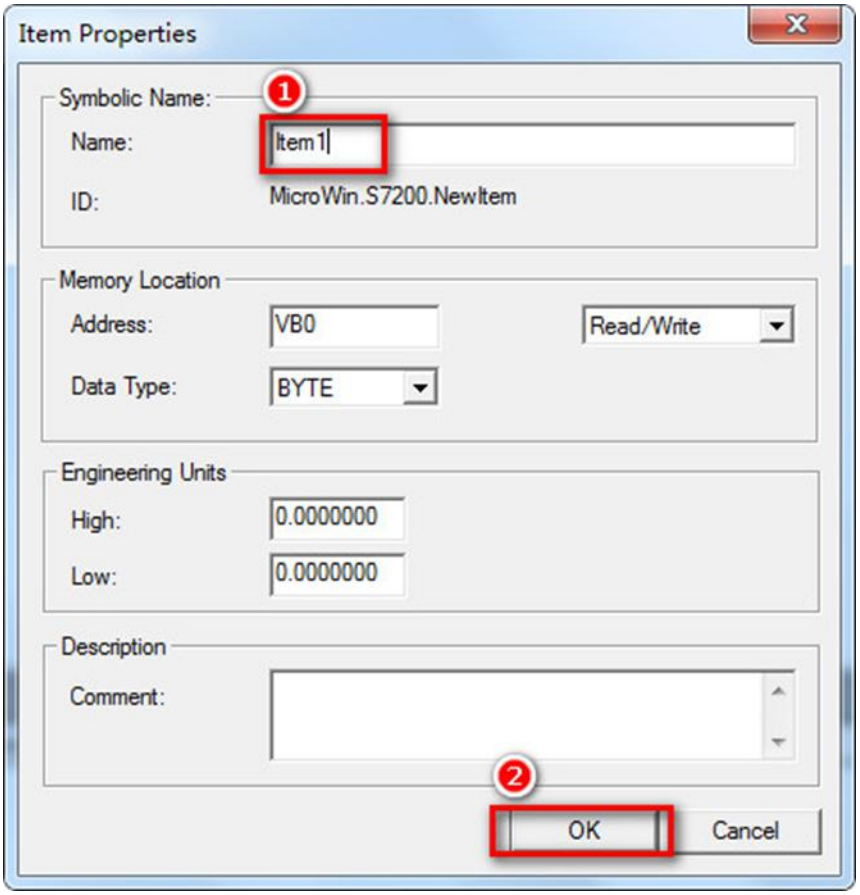
注：不要选带 auto 的网卡。



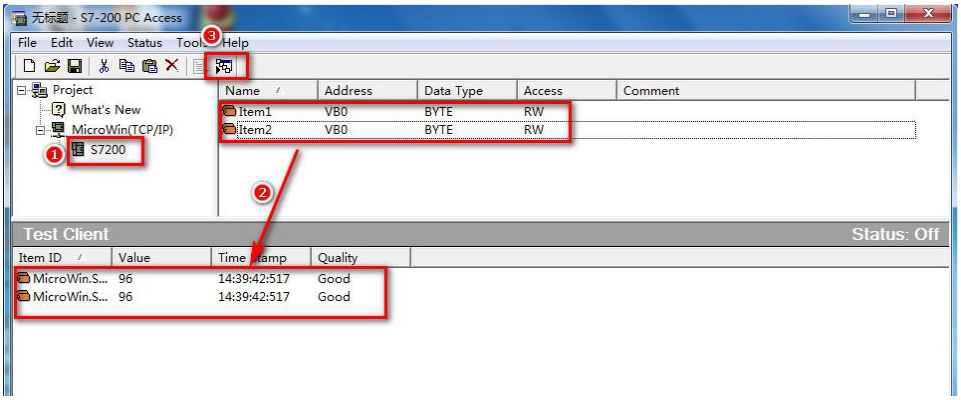
2、打开 S7-200 PC Access 软件,右击 Project 组下的【MicroWin（TCP/IP）】新建一个 PLC 连接，填入 RVNet-S7200 的 IP 地址，点击【OK】;



3、新建变量（项目）;



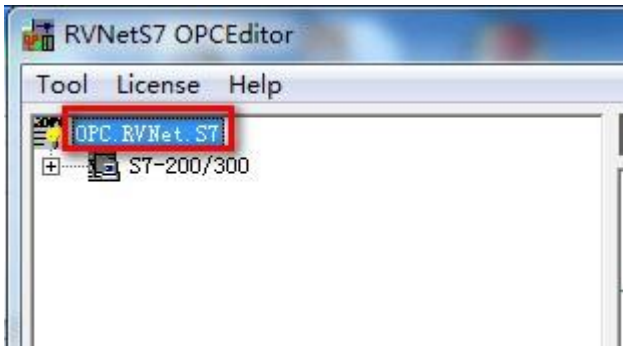
4、变量测试，将变量拖入测试区域，点击测试客户机;



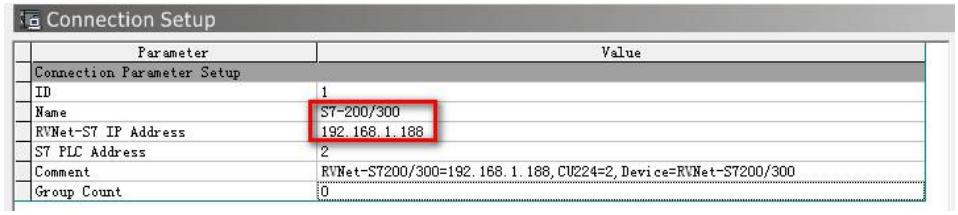
7.3RVNetS7OPC 通迅

7.3.1 配置 OPC 参数

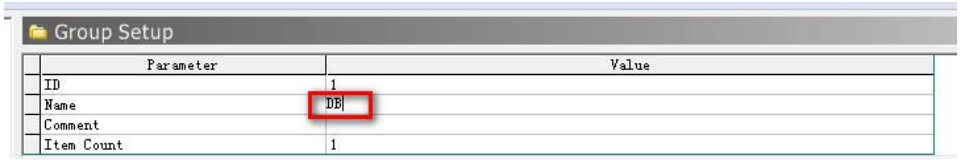
1、打开 RVNetS7 OPCEditor，右击【OPC.RVNet.S7】，选择【New Connection】添加新的连接;



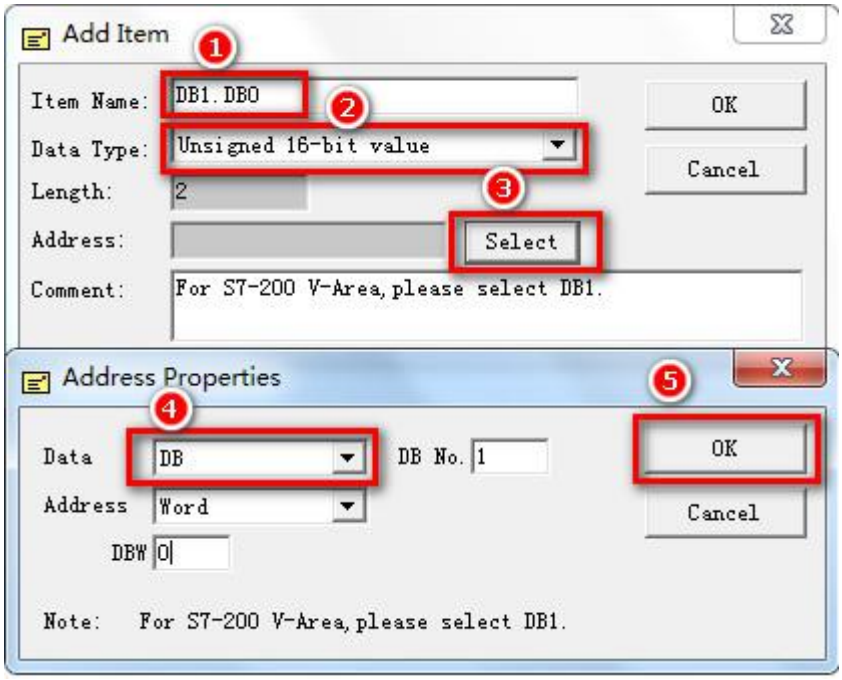
2、点击【New Connection】，在如下窗口填写连接设备的名称，如：S7-200/300，输入 RVNet-S7 模块的 IP 地址，【S7 PLC Address】中填入 PLC 的站地址;



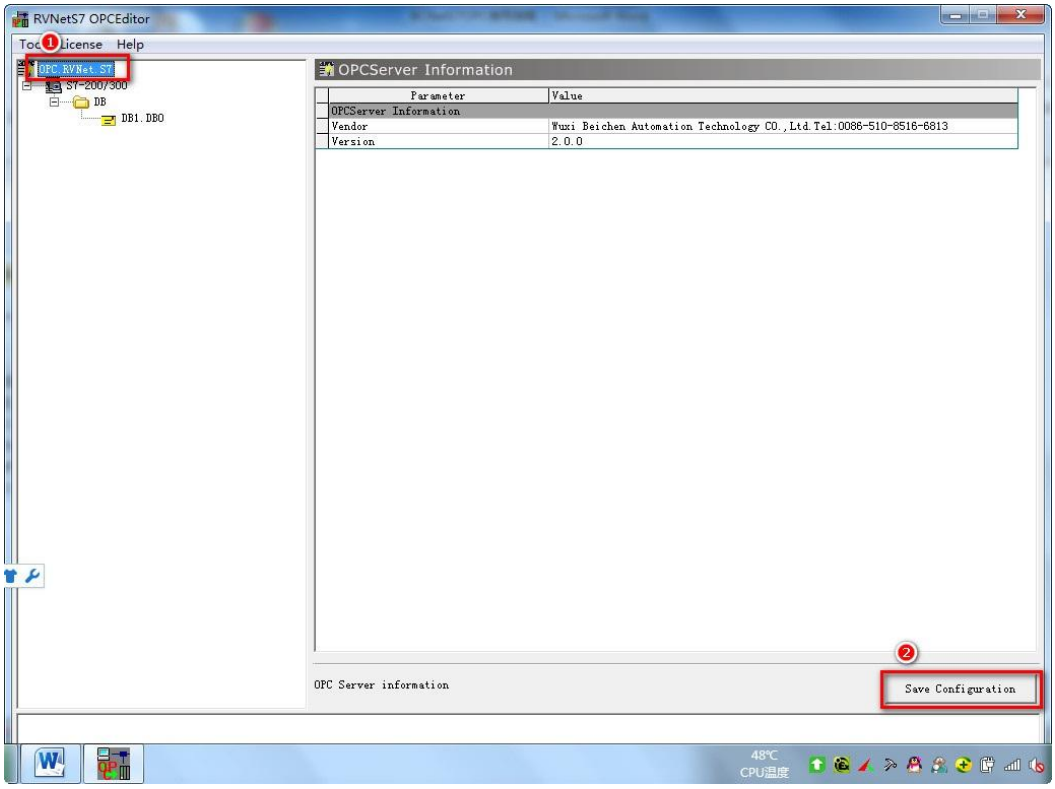
3、右击【S7-200/300】点击【New Group】，在如下的窗口填入组名，如：DB;



4、右击菜单栏下【DB】点击【New Item】建立变量，按下图完成 Item 的配置;

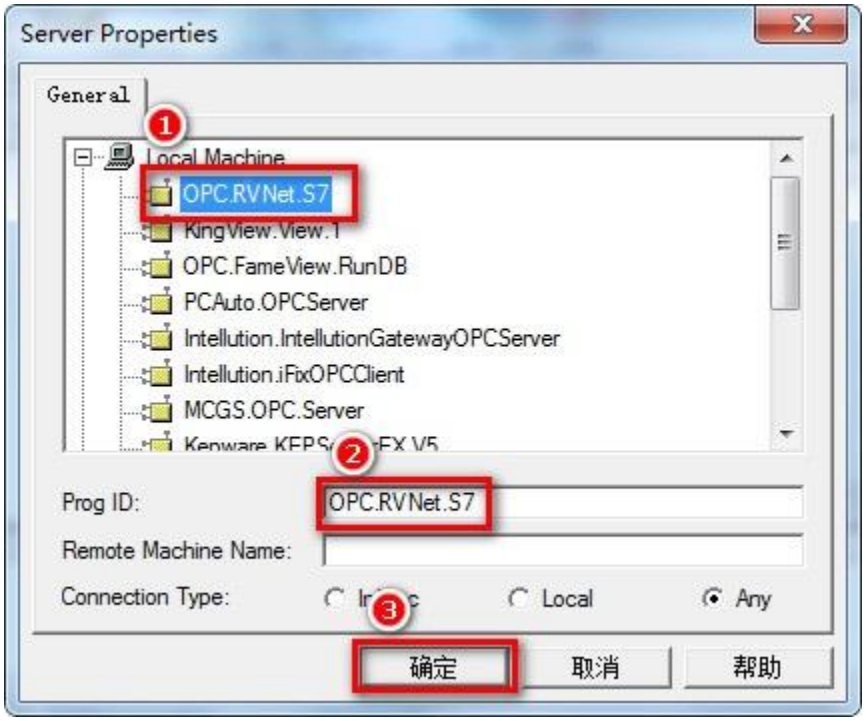


5、选择菜单栏的【OPC.RVNet.S7】，点击【Save Configuration】，完成设置;



7.3.2 测试 OPC 变量

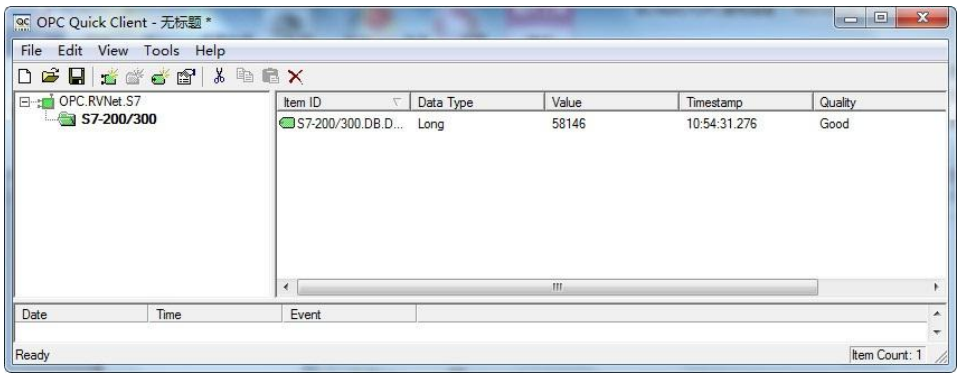
1、运行 OPC Quick Client 软件，选择菜单【Edit->New Server Connection】，在对话框中选择【OPC.RVNet.S7】后点击【确定】按钮，如下图：



2、鼠标右击菜单栏的【OPC.RVNet.S7】，点击【New Group...】,输入组名，如：S7-200/300，点击确定；

3、选择需要测试的变量，点击【Add Leaves】，点击  调整变量类型，点击【OK】。

4、测试画面如下：

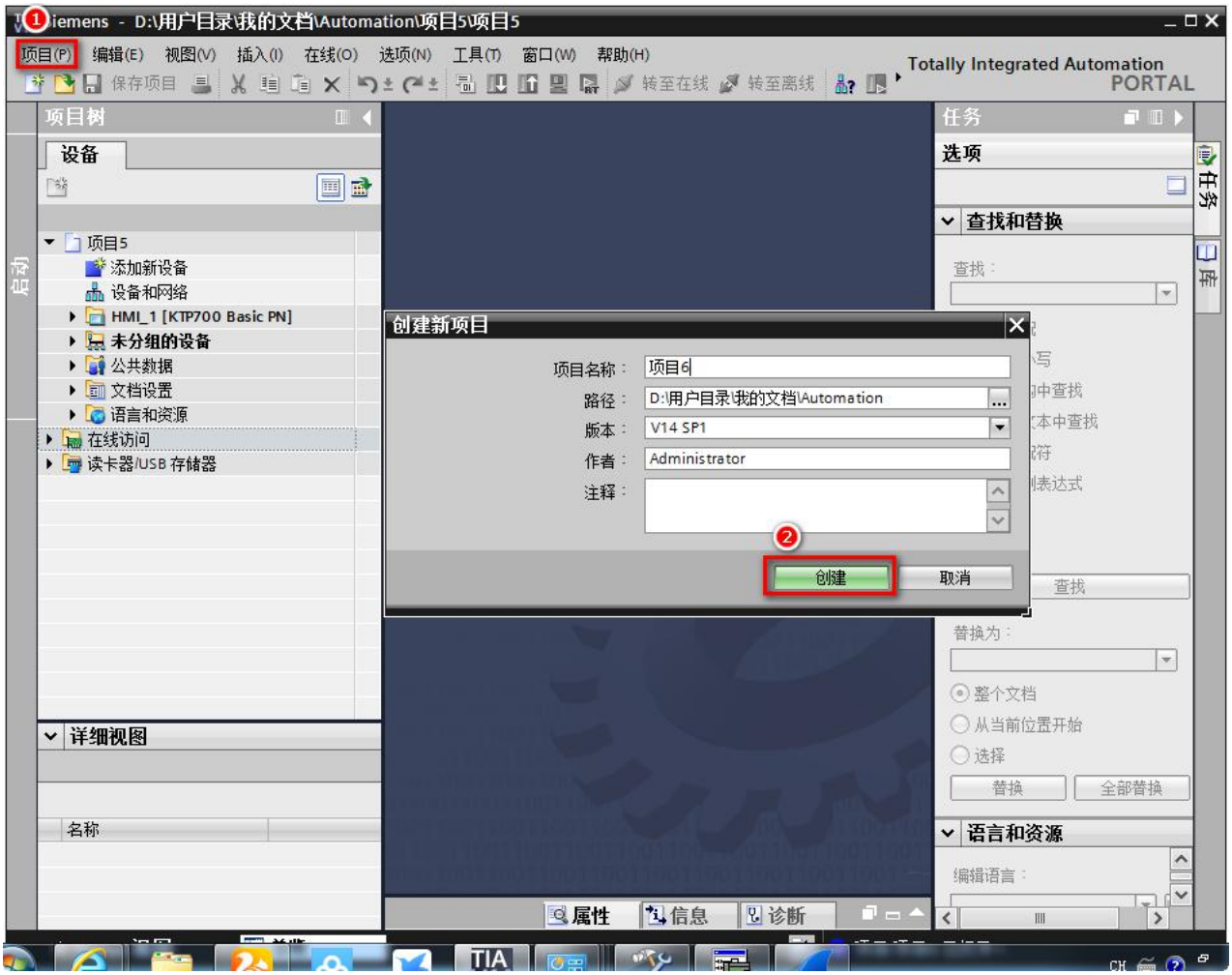


8.触摸屏以太网通讯

8.1 西门子 KTP/TP 系列触摸屏通讯

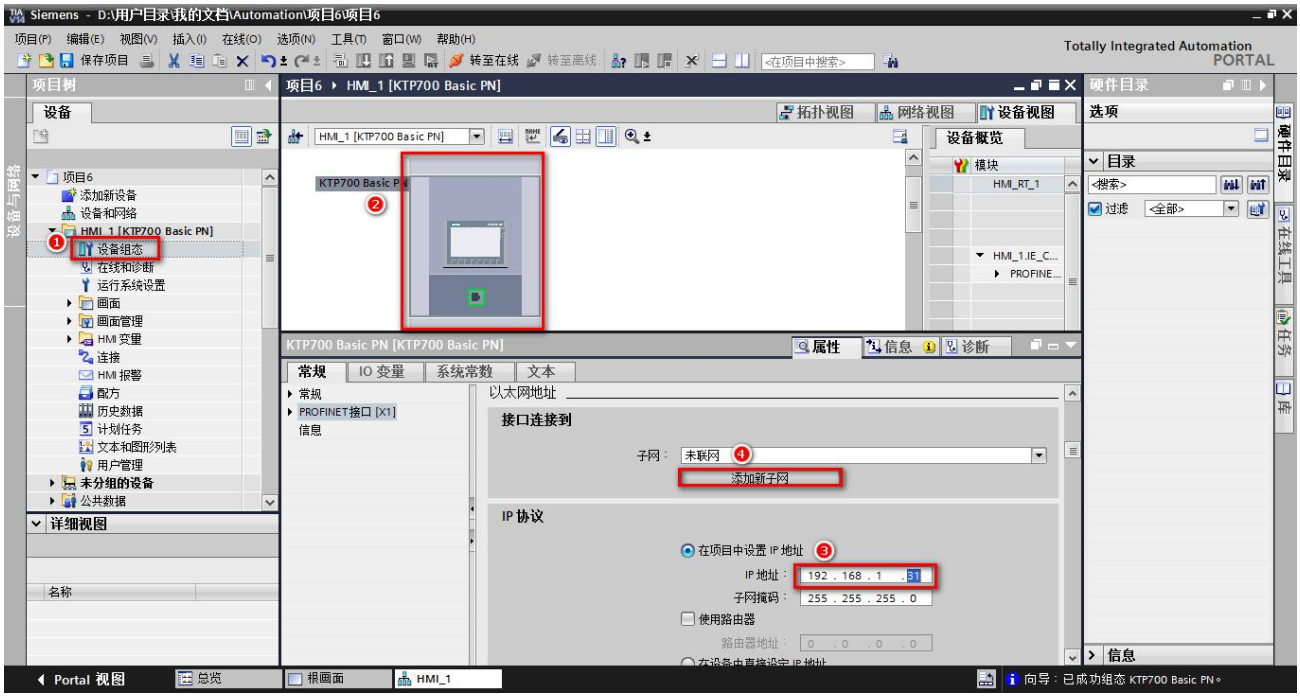
RVNet-S7 模块可以和西门子的 KTP/TP 系列触摸屏以太网通讯，这里以 KTP700 为例介绍参数设置。

1、新建项目；

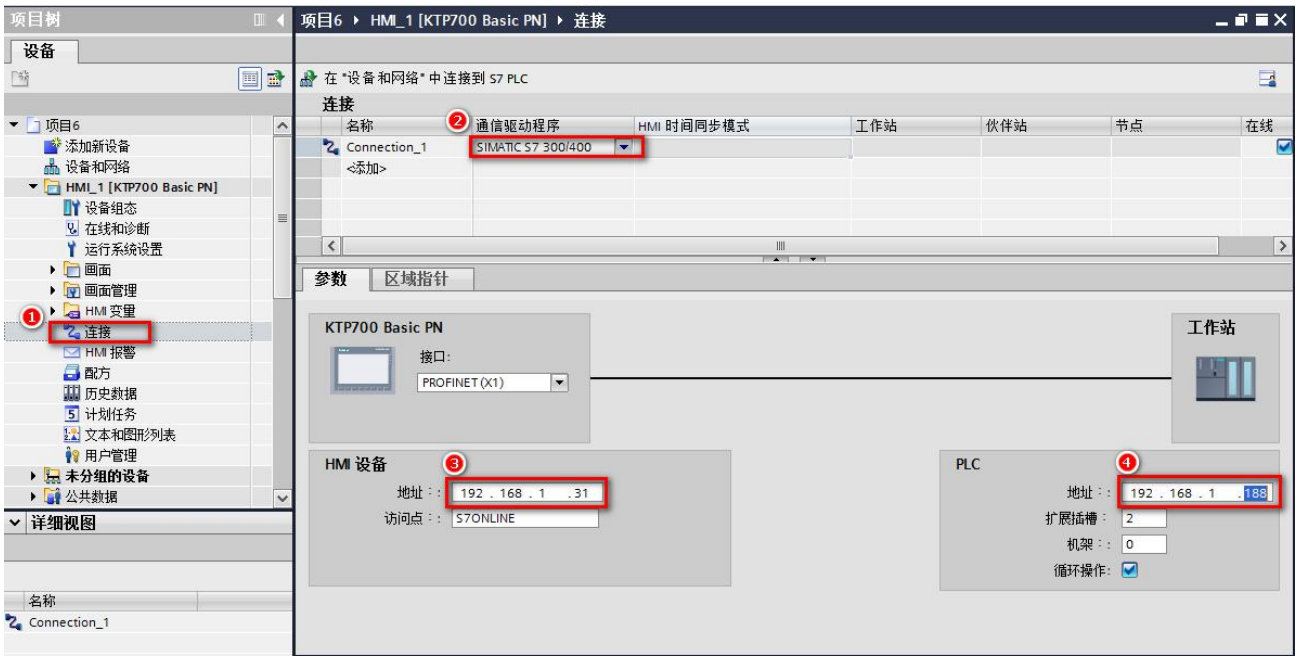


2、添加触摸屏设备；

3、给触摸屏分配 IP 地址（必须和 RVNet 模块的 IP 地址在同一网段）；



4、新建【连接】，在【通信驱动程序】中选择 SIMATIC S7 300/400，在【HMI 设备】-【地址】填入触摸屏的 IP 地址，在【PLC】-【地址】填入 RVNet 模块的 IP 地址。

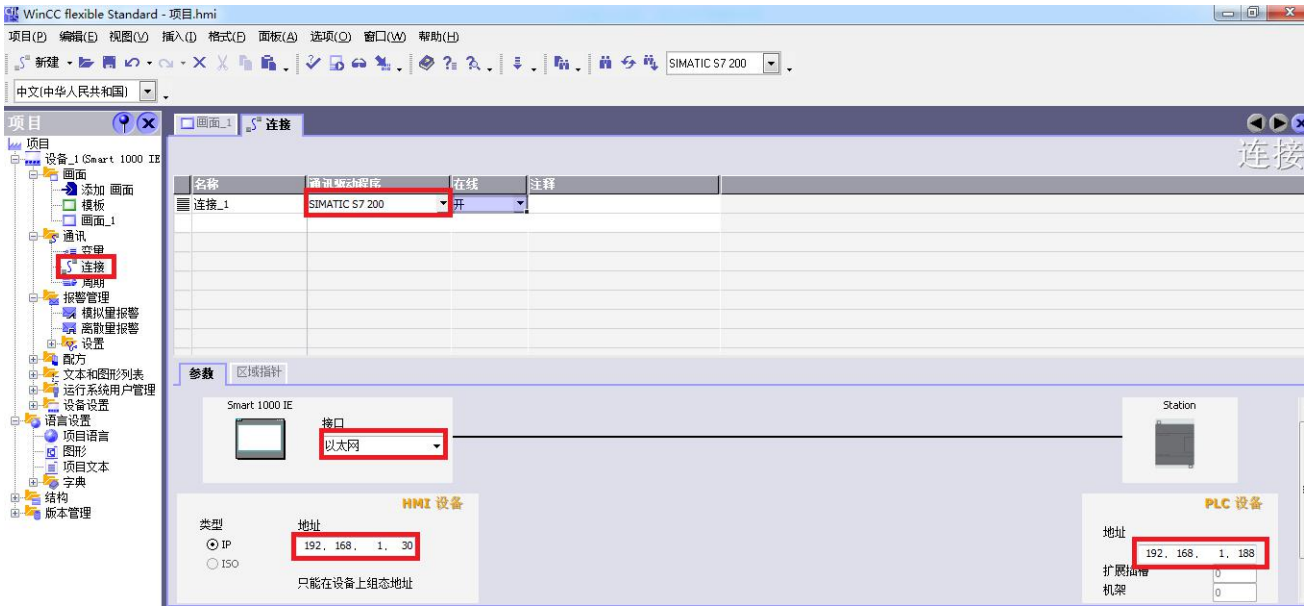


8.2 西门子 SmartIE 系列触摸屏连 S7300

SmartIE 触摸屏通过 RVNet-S7300 可以实现与西门子 S7300 的以太网通讯。

1.运行 WinCC flexible 软件，选择 SmartIE 系列触摸屏型号并新建项目；

2.双击【连接】，新建通讯连接，在【通讯设备通讯】中选择 SIMATIC S7 200，【接口】选择以太网，HMI 设备—【地址】输入触摸屏的 IP 地址，PLC 设备—【地址】输入 RVNet-S7300 的 IP 地址；



3.建立变量

SmartIE 触摸屏通过 RVNet-S7300，可访问 S7300 的 DB1 数据块、M 区、Q 区、I 区。

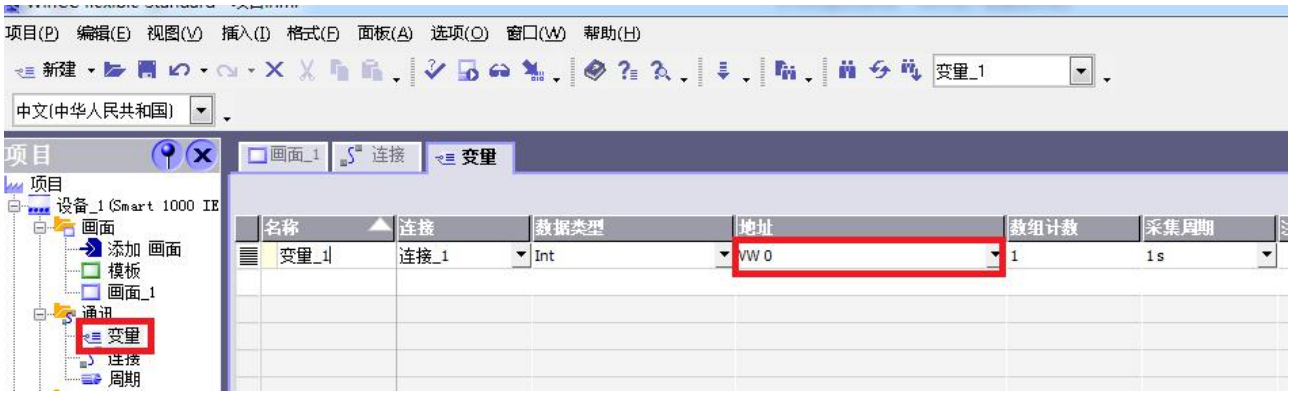
注意：软件中新建的变量与 PLC 的数据区对应关系：

V 区对应 S7300 的 DB1 数据块；

M 区对应 S7300 的 M 区；

Q 区对应 S7300 的 Q 区；

I 区对应 S7300 的 I 区；



这里的 VW0 对应 S7300 的 DB1.DBW0。

9.ModbusTCP 通讯

RVNet-S7 模块内集成 ModbusTCP 通讯服务器，因此 ModbusTCP 客户机，如支持 ModbusTCP 的组态软件、OPC 服务器、PLC 以及实现 ModbusTCP 客户机的高级语言开发的软件等，可以直接访问 S7 系列 PLC 的内部数据区。Modbus 协议地址在 RVNet 内部已经被默认映射至 S7 系列 PLC 的地址区，实现功能号包括：FC1、FC2、FC3、FC4、FC5、FC6 和 FC16，如果不采用默认的地址映射关系，也可以自定义地址映射关系，详见《第四章中的：Modbus 映射表》。

ModbusTCP 协议帧定义：

事务处理标识符	事务处理标识符	协议标识符	协议标识符	长度字段（高字节）	长度字段（低字节）	从站地址	功能号	数据地址（高字节）	数据地址（低字节）	指令数（高字节）	指令数（低字节）
0x0	0x0	0x0	0x0	0x0	后面的字节数						

9.1 默认地址映射表

Modbus	S7 系列 PLC	数据类型	计算公式	功能号	最大指令数
从站地址	S7 站点地址	字节	相等	-	-
00001~	Q0.0~	位	Q***m.n*** = 00001 + ***m****8 + ***n***	FC1（读线圈）	S7-200：119 S7-300：784
				FC5（写线圈）	1
10001~	I0.0~	位	I***m.n*** = 10001 + ***m****8 + ***n***	FC2（读输入）	S7-200：119 S7-300：784
30001~	MW0	字（2 字节）	MW***m***= 30001 + ***m***/2，***m*** 为偶数	FC4（读输入寄存器）	S7-200：16 S7-300：111
40001~	DBx.DBW0	字（2 字节）	DB***x***.DBW***m*** = 40001 + ***m***/2，***m*** 为偶数（***x*** 由参数指定，S7-200 的 V 区为 DB***1***）（见 S7 总线接口参数）	FC3（读乘法寄存器） FC16（写乘法寄存器）	111
				FC6（写单一乘法寄存器）	1

9.2ModScan32 测试

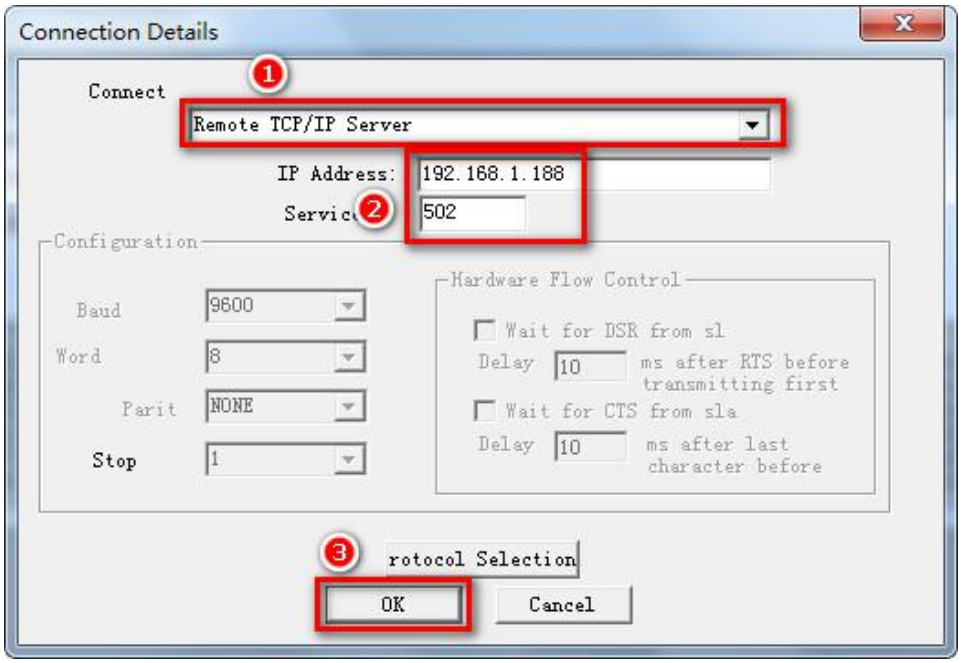
1. 运行 ModScan32 软件。

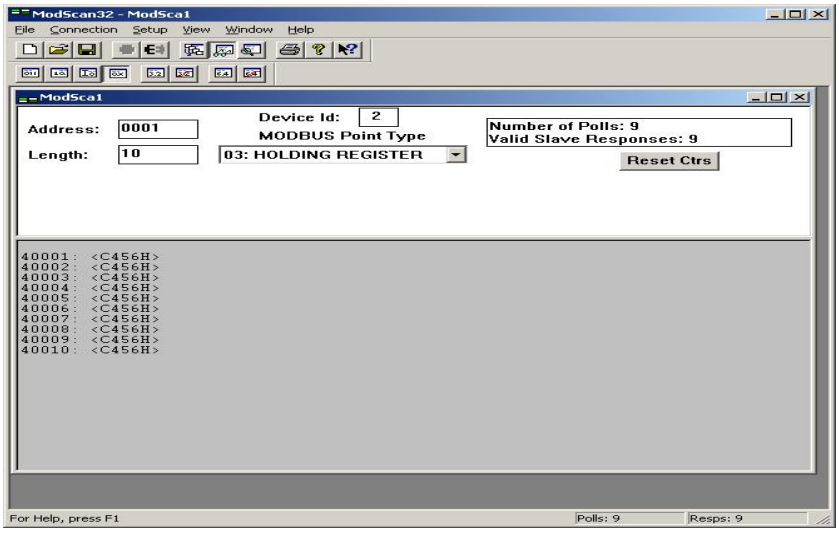
2. 选择菜单 Connection/Connect，选择 Remote TCP/IP Server，输入 RVNet-S7 的 IP 地址，Service 端口为 502；点击[OK]按钮。

3. 在子窗口“ModSca1”中设置 Device ID 为 S7-200PLC 的站地址（如 2），功能号选择 03:HOLDING REGISTER，Address = 00001，Length = 10。

4. 子窗口数据区显示 40001-40010 的 16 进制数据，其对应于 S7-200 的 VW0-VW18 数值。

5. 双击子窗口数据区的数据可以修改数值。


Connection Details
Connect
1
Remote TCP/IP Server
IP Address:
192.168.1.188
Servic
2
502
Configuration
Baud
9600
Word
8
Parit
NONE
Stop
1
Hardware Flow Control
Wait for DSR from sl
Delay
10
ms after RTS before transmitting first
Wait for CTS from sla
Delay
10
ms after last character before
3
rotocol Selection
OK
Cancel


ModScan32 - ModSca1
File Connection Setup View Window Help
ModSca1
Address:
0001
Length:
10
Device Id:
2
MODBUS Point Type
03: HOLDING REGISTER
Number of Polls: 9
Valid Slave Responses: 9
Reset Ctrs
40001: <C456H>
40002: <C456H>
40003: <C456H>
40004: <C456H>
40005: <C456H>
40006: <C456H>
40007: <C456H>
40008: <C456H>
40009: <C456H>
40010: <C456H>
For Help, press F1
Polls: 9
Resps: 9

10.RVNetS7 协议规范

10.1 通讯模式

RVNet-S7 模块在以太网上作为服务器运行，远程计算机作为客户机通过 TCP/IP 协议连接到 RVNet-S7 并向其发送和接收数据来实现与 S7PLC 的通讯。RVNetS7 协议的服务端口号为 1099。

10.2 报文定义

RVNetS7 协议的以太网通讯报文由固定的 8 个字节的报文头、8 个字节的扩展报文头和可选的最大 200 个字节的用户数据组成，无论是发送报文还是接收报文都遵循此结构；如下表：

节	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	接收方识别 ID
	1	msg.tx	byte	发送方识别 ID
	2	msg.ln	byte	扩展报文头和用户数据总
	3	msg.nr	byte	报文 ID
	4	msg.a	byte	响应号
	5	msg.f	byte	错误号
	6	msg.b	byte	命令号
	7	msg.e	byte	扩展号
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址
	9	msg.data_area	byte	数据区
	10,11	msg.data_adr	word	数据地址
	12	msg.data_idx	byte	数据索引号
	13	msg.data_cnt	byte	数据字节个数
	14	msg.data_type	byte	数据类型
	15	msg.function	byte	功能号
用户数据	16~215	msg.d[0~199]	byte array	最大 200 个字节的用户数据

其中：

1. 对于客户机（计算机）的识别 ID 为 0xFF（十进制数 255），服务器（RVNet-S7 模块）的识别 ID 为 0x03（十进制数 3）；因此：

   1) 客户机发送数据命令帧到服务器：msg.rx=0x03,msg.tx=0xFF；

   2) 服务器发送数据响应帧到客户机：msg.rx=0xFF,msg.tx=0x03；

   3) 客户机应该对接收报文的 msg.rx 和 msg.tx 进行检查以确定是否是 RVNet-S7 的响应报文；

2. 扩展报文头和用户数据区总长度 msg.ln 为扩展报文头和用户数据之字节数和，因此：

   1) 客户机发送读数据命令帧到服务器：msg.ln=0x08；无用户数据；

2) 客户机发送写数据命令帧到服务器：msg.ln=0x08+待写数据字节长度；

3) 服务器发送读数据响应帧到客户机：msg.ln=0x08+返回数据字节长度；

4) 服务器发送写数据响应帧到客户机：msg.ln=0x08；无用户数据；

5) 客户机应该根据接收报文的 msg.ln 来判断该报文的完整性；

3. 报文 ID msg.nr 标识每对发送/接收报文的对应信息。为了接收到正确的应答报文，客户机应在每次发送报文前将 msg.nr 自动增 1，然后判断接收报文的 msg.nr 是否与发送报文的 msg.nr 一致，如果一致说明接收报文为当前发送报文的响应帧；

4. 响应号 msg.a 在客户机发送报文中为 0x00；在服务器发送报文中应为发送报文的命令号 msg.b；客户机在接收报文数据时应判断接收报文的 msg.a 是否等于发送报文的 msg.b，如果一致再处理数据；

5. 错误号 msg.f 在客户机发送报文中为 0x00；在服务器发送报文中为错误号，如果 msg.f=0x00 表明客户机的请求被服务器正确处理；客户机应该检查接收报文的 msg.f，如果非 0 则应重试或者检查发送命令；

6. 命令号 msg.b 在客户机发送报文中为指定命令代号（见后描述），在服务器发送报文中为 0x00；

7. 扩展号 msg.e 总为 0x00；

8. 8 字节扩展报文头的定义见文档后续每个命令报文的详细描述；

9. 用户数据区在客户机发送读数据命令时长度为 0，即无用户数据区；在客户机发送写数据命令时储存待写数据；在服务器发送读数据响应帧时储存读取的数据；在服务器发送写数据响应帧时长度为 0，即无用户数据区；

10.3 读 DB 块数据

注意：对于 S7-200，V 区对应 DB1 数据块；

客户机发送读数据命令：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0x03
	1	msg.tx	byte	0xFF
	2	msg.ln	byte	0x08
	3	msg.nr	byte	客户机给定
	4	msg.a	byte	0x00
	5	msg.f	byte	0x00
	6	msg.b	byte	0x31（读写 DB 块）

	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	读起始字节地址的高 8 位值，=起始地址/256
	10,11	msg.data_adr	word	DB 块号,0~65534；S7-200 的 V 区为 0x0001（DB1）
	12	msg.data_idx	byte	读起始字节地址的低 8 位值，=起始地址%256
	13	msg.data_cnt	byte	需要读取的数据字节个数，最大为 200
	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x01（读数据）

服务器发送读数据响应帧：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0xFF
	1	msg.tx	byte	0x03
	2	msg.ln	byte	0x08+读取数据字节数
	3	msg.nr	byte	与客户机给定一致
	4	msg.a	byte	0x31（读写 DB 块）
	5	msg.f	byte	0x00（非 0 代表有错误）
	6	msg.b	byte	0x00
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	读起始字节地址的高 8 位值，=起始地址/256
	10,11	msg.data_adr	word	DB 块号,0~65534；S7-200 的 V 区为 0x0001（DB1）
	12	msg.data_idx	byte	读起始字节地址的低 8 位值，=起始地址%256
	13	msg.data_cnt	byte	已经读取的数据字节个数，小于等于 200

	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x01（读数据）
用户数据（最大 200 字节）	16~ 16+(读取数据字节数-1)	msg.d[0~(读取数据字节数-1)]	byte array	读取的数据

举例：客户机读取 S7-300（站地址为 2）的 DB1.DBB100~DBB119 共 20 个字节

客户机发送（16 进制）：

03	FF	08	01	00	00	31	00	02	00	00	01	64	14	05	01

服务器发送（16 进制）：

FF	03	1C	01	31	00	00	00	02	00	00	01	64	14	05	01
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00												

绿色数据为读取的 DB1.DBB100~DBB119 共 20 个字节数据；

红色数据为起始地址 DB1.DBB100（0x0064）；

10.4 写 DB 块数据

注意：对于 S7-200，V 区对应 DB1 数据块；

客户机发送写数据命令：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0x03
	1	msg.tx	byte	0xFF
	2	msg.ln	byte	0x08+写数据字节数
	3	msg.nr	byte	客户机给定
	4	msg.a	byte	0x00
	5	msg.f	byte	0x00
	6	msg.b	byte	0x31（读写 DB 块）
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	写起始字节地址的高 8 位值，=起始地址/256

	10,11	msg.data_adr	word	DB 块号,0~65534；S7-200 的 V 区为 0x0001（DB1）
	12	msg.data_idx	byte	写起始字节地址的低 8 位值，=起始地址%256
	13	msg.data_cnt	byte	需要写入的数据字节个数，最大为 200
	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x02（写数据）
用户数据（最大 200 字节）	16~16+(写入数据字节数-1)	msg.d[0~(写入数据字节数-1)]	byte array	写入的数据

服务器发送写数据响应帧：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0xFF
	1	msg.tx	byte	0x03
	2	msg.ln	byte	0x08
	3	msg.nr	byte	与客户机给定一致
	4	msg.a	byte	0x31（读写 DB 块）
	5	msg.f	byte	0x00（非 0 代表有错误）
	6	msg.b	byte	0x00
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	写起始字节地址的高 8 位值，=起始地址/256
	10,11	msg.data_adr	word	DB 块号,0~65534；S7-200 的 V 区为 0x0001（DB1）
	12	msg.data_idx	byte	写起始字节地址的低 8 位值，=起始地址%256
	13	msg.data_cnt	byte	已经写入的数据字节个数，小于等于 200

	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x02（写数据）

举例：客户机向 S7-300（站地址为 2）的 DB1.DBD1000 写入数据 0x01020304，共 4 个字节

客户机发送（16 进制）：

03	FF	0C	01	00	00	31	00	02	03	00	01	E8	04	05	02
01	02	03	04												

服务器发送（16 进制）：

FF	03	08	01	31	00	00	00	02	03	00	01	E8	04	05	02

绿色数据为写入的 DB1.DBD1000 共 4 个字节数据；

红色数据为起始地址 DB1.DBD1000（0x03E8）；

10.5 读 M 区数据

客户机发送读数据命令：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0x03
	1	msg.tx	byte	0xFF
	2	msg.ln	byte	0x08
	3	msg.nr	byte	客户机给定
	4	msg.a	byte	0x00
	5	msg.f	byte	0x00
	6	msg.b	byte	0x33（读写 M 区）
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	无用，0x00
	10,11	msg.data_adr	word	M 区起始地址，0~65534 [10] = 起始地址/256 [11] = 起始地址%256
	12	msg.data_idx	byte	无用，0x00
	13	msg.data_cnt	byte	需要读取的数据字节个数，最大为 200

	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x01（读数据）

服务器发送读数据响应帧：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0xFF
	1	msg.tx	byte	0x03
	2	msg.ln	byte	0x08+读取数据字节数
	3	msg.nr	byte	与客户机给定一致
	4	msg.a	byte	0x33（读写 M 区）
	5	msg.f	byte	0x00（非 0 代表有错误）
	6	msg.b	byte	0x00
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	无用，0x00
	10,11	msg.data_adr	word	M 区起始地址，0~65534 [10] = 起始地址/256 [11] = 起始地址%256
	12	msg.data_idx	byte	无用，0x00
	13	msg.data_cnt	byte	已经读取的数据字节个数，小于等于 200
	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x01（读数据）
用户数据（最大 200 字节）	16~ 16+(读取数据字节数-1)	msg.d[0~(读取数据字节数-1)]	byte array	读取的数据

举例：客户机读取 S7-300（站地址为 2）的 MB10~MB15 共 6 个字节

客户机发送（16 进制）：

03	FF	08	01	00	00	33	00	02	00	00	0A	00	06	05	01

服务器发送（16 进制）：

FF	03	0E	01	33	00	00	00	02	00	00	0A	00	06	05	01
00	00	00	00	00	00										

绿色数据为读取的 MB10~MB15 共 6 个字节数据；

红色数据为起始地址 MB10（0x000A）；

10.6 写 M 区数据

客户机发送写数据命令：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0x03
	1	msg.tx	byte	0xFF
	2	msg.ln	byte	0x08+写数据字节数
	3	msg.nr	byte	客户机给定
	4	msg.a	byte	0x00
	5	msg.f	byte	0x00
	6	msg.b	byte	0x33（读写 M 区）
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	无用，0x00
	10,11	msg.data_adr	word	M 区起始地址，0~65534 [10] = 起始地址/256 [11] = 起始地址%256
	12	msg.data_idx	byte	无用，0x00
	13	msg.data_cnt	byte	需要写入的数据字节个数，最大为 200
	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x02（写数据）
用户数据（最大 200 字节）	16~ 16+(写入数据字节数	msg.d[0~(写入数据字节数-1)]	byte array	写入的数据

	-1)			

服务器发送写数据响应帧：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0xFF
	1	msg.tx	byte	0x03
	2	msg.ln	byte	0x08
	3	msg.nr	byte	与客户机给定一致
	4	msg.a	byte	0x33（读写 M 区）
	5	msg.f	byte	0x00（非 0 代表有错误）
	6	msg.b	byte	0x00
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	无用，0x00
	10,11	msg.data_adr	word	M 区起始地址，0~65534 [10] = 起始地址/256 [11] = 起始地址%256
	12	msg.data_idx	byte	无用，0x00
	13	msg.data_cnt	byte	已经写入的数据字节个数，小于等于 200
	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x02（写数据）

举例：客户机向 S7-300（站地址为 2）的 MW20 写入数据 0x0102，共 2 个字节

客户机发送（16 进制）：

03	FF	0A	01	00	00	33	00	02	00	00	14	00	02	05	02
01	02														

服务器发送（16 进制）：

FF	03	08	01	33	00	00	00	02	00	00	14	00	02	05	02

绿色数据为写入的 MW20 共 2 个字节数据；

红色数据为起始地址 MW20（0x0014）；

10.7 读 I、Q 区（输入/输出信号）数据

客户机发送读数据命令：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0x03
	1	msg.tx	byte	0xFF
	2	msg.ln	byte	0x08
	3	msg.nr	byte	客户机给定
	4	msg.a	byte	0x00
	5	msg.f	byte	0x00
	6	msg.b	byte	0x34（读写 I、Q 区）
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	数据区 0x00：I 区 0x01：Q 区
	10,11	msg.data_adr	word	I、Q 区起始地址，0~65534 [10] = 起始地址/256 [11] = 起始地址%256
	12	msg.data_idx	byte	无用，0x00
	13	msg.data_cnt	byte	需要读取的数据字节个数，最大为 200
	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x01（读数据）

服务器发送读数据响应帧：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0xFF
	1	msg.tx	byte	0x03
	2	msg.ln	byte	0x08+读取数据字节数

	3	msg.nr	byte	与客户机给定一致
	4	msg.a	byte	0x34（读写 I、Q 区）
	5	msg.f	byte	0x00（非 0 代表有错误）
	6	msg.b	byte	0x00
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	数据区 0x00：I 区 0x01：Q 区
	10,11	msg.data_adr	word	I、Q 区起始地址，0~65534 [10] = 起始地址/256 [11] = 起始地址%256
	12	msg.data_idx	byte	无用，0x00
	13	msg.data_cnt	byte	已经读取的数据字节个数，小于等于 200
	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x01（读数据）
用户数据（最大 200 字节）	16~ 16+(读取数据字节数-1)	msg.d[0~(读取数据字节数-1)]	byte array	读取的数据

举例 1：客户机读取 S7-300（站地址为 2）的 IB0 共 1 个字节

客户机发送（16 进制）：

03	FF	08	01	00	00	34	00	02	00	00	00	00	01	05	01

服务器发送（16 进制）：

FF	03	09	01	34	00	00	00	02	00	00	00	00	01	05	01
00															

绿色数据为读取的 IB0 共 1 个字节数据；

红色数据为起始地址 IB0（0x0000）；

举例 2：客户机读取 S7-300（站地址为 3）的 QB1~QB2 共 2 个字节

客户机发送（16 进制）：

03	FF	08	01	00	00	34	00	03	01	00	01	00	02	05	01

服务器发送（16 进制）：

FF	03	0A	01	34	00	00	00	03	01	00	01	00	02	05	01	00	00

绿色数据为读取的 QB1~QB2 共 2 个字节数据；

红色数据为起始地址 QB1（0x0001）；

10.8 写 I、Q 区（输入/输出信号）数据

客户机发送写数据命令：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0x03
	1	msg.tx	byte	0xFF
	2	msg.ln	byte	0x08+写数据字节数
	3	msg.nr	byte	客户机给定
	4	msg.a	byte	0x00
	5	msg.f	byte	0x00
	6	msg.b	byte	0x34（读写 I、Q 区）
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	数据区 0x00：I 区 0x01：Q 区
	10,11	msg.data_adr	word	I、Q 区起始地址，0~65534 [10] = 起始地址/256 [11] = 起始地址%256
	12	msg.data_idx	byte	无用，0x00
	13	msg.data_cnt	byte	需要写入的数据字节个数，最大为 200
	14	msg.data_type	byte	0x05（字节）

	15	msg.function	byte	0x02（写数据）
用户数据（最大 200 字节）	16~ 16+(写入数据字节数-1)	msg.d[0~(写入数据字节数-1)]	byte array	写入的数据

服务器发送写数据响应帧：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0xFF
	1	msg.tx	byte	0x03
	2	msg.ln	byte	0x08
	3	msg.nr	byte	与客户机给定一致
	4	msg.a	byte	0x34（读写 I、Q 区）
	5	msg.f	byte	0x00（非 0 代表有错误）
	6	msg.b	byte	0x00
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	数据区 0x00：I 区 0x01：Q 区
	10,11	msg.data_adr	word	I、Q 区起始地址，0~65534 [10] = 起始地址/256 [11] = 起始地址%256
	12	msg.data_idx	byte	无用，0x00
	13	msg.data_cnt	byte	已经写入的数据字节个数，小于等于 200
	14	msg.data_type	byte	0x05（字节）
	15	msg.function	byte	0x02（写数据）

举例：客户机向 S7-300（站地址为 2）的 QB0 写入数据 0xFF，共 1 个字节

客户机发送（16 进制）：

03	FF	09	01	00	00	34	00	02	01	00	00	00	01	05	02

FF

服务器发送（16 进制）：

FF	03	08	01	34	00	00	00	02	01	00	00	00	01	05	02

绿色数据为写入的 QB0 共 1 个字节数据；

红色数据为起始地址 QB0（0x0000）；

10.9 读 DB、M、I、Q 的位值

注：RVNetS7 协议只支持对一个位的读取。

客户机发送读位命令：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0x03
	1	msg.tx	byte	0xFF
	2	msg.ln	byte	0x08
	3	msg.nr	byte	客户机给定
	4	msg.a	byte	0x00
	5	msg.f	byte	0x00
	6	msg.b	byte	和字节操作定义一致
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	和字节操作定义一致
	10,11	msg.data_adr	word	和字节操作定义一致
	12	msg.data_idx	byte	和字节操作定义一致
	13	msg.data_cnt	byte	无用 = 0x00
	14	msg.data_type	byte	高四位值：位偏移 0-7 低四位值：= 4（位）
	15	msg.function	byte	0x01（读数据）

服务器发送读位响应帧：

	字节	参数	类型	注释
8 字节报	0	msg.rx	byte	0xFF

文头	1	msg.tx	byte	0x03
	2	msg.ln	byte	0x09
	3	msg.nr	byte	与客户机给定一致
	4	msg.a	byte	和字节操作定义一致
	5	msg.f	byte	0x00（非 0 代表有错误）
	6	msg.b	byte	0x00
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	和字节操作定义一致
	10,11	msg.data_adr	word	和字节操作定义一致
	12	msg.data_idx	byte	和字节操作定义一致
	13	msg.data_cnt	byte	无用 = 0x00
	14	msg.data_type	byte	高四位值：位偏移 0-7 低四位值：= 4（位）
	15	msg.function	byte	0x01（读数据）
用户数据（1 字节）	16	msg.d[0]	byte	读取的位值 0x00：OFF 0x01：ON

举例：客户机读取 S7-300（站地址为 2）的 Q0.5 的位值

客户机发送（16 进制）：

03	FF	08	01	00	00	34	00	02	01	00	00	00	00	54	01

服务器发送（16 进制）：

FF	03	09	01	34	00	00	00	02	01	00	00	00	00	54	01	00

绿色数据为读取的 Q0.5 的位值，即 OFF；

红色数据为起始地址 QB0（0x0000），0x54 的高 4 位（=5）为位偏移；

10.10 写 DB、M、I、Q 的位值

注：RVNetS7 协议只支持对一个位的写入（输入 I 区是写不了的，取决于外部信号）。

客户机发送写位命令：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0x03
	1	msg.tx	byte	0xFF
	2	msg.ln	byte	0x09
	3	msg.nr	byte	客户机给定
	4	msg.a	byte	0x00
	5	msg.f	byte	0x00
	6	msg.b	byte	和字节操作定义一致
	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	和字节操作定义一致
	10,11	msg.data_adr	word	和字节操作定义一致
	12	msg.data_idx	byte	和字节操作定义一致
	13	msg.data_cnt	byte	无用 = 0x00
	14	msg.data_type	byte	高四位值：位偏移 0-7 低四位值：= 4（位）
	15	msg.function	byte	0x02（写数据）
用户数据（1 字节）	16	msg.d[0]	byte	写入的位值 0x00：OFF 0x01：ON

服务器发送写位响应帧：

	字节	参数	类型	注释
8 字节报文头	0	msg.rx	byte	0xFF
	1	msg.tx	byte	0x03
	2	msg.ln	byte	0x08
	3	msg.nr	byte	与客户机给定一致
	4	msg.a	byte	和字节操作定义一致
	5	msg.f	byte	0x00（非 0 代表有错误）
	6	msg.b	byte	0x00

	7	msg.e	byte	0x00
8 字节扩展报文头	8	msg.device_adr	byte	远程（PLC）站地址 0-31
	9	msg.data_area	byte	和字节操作定义一致
	10,11	msg.data_adr	word	和字节操作定义一致
	12	msg.data_idx	byte	和字节操作定义一致
	13	msg.data_cnt	byte	无用 = 0x00
	14	msg.data_type	byte	高四位值：位偏移 0-7 低四位值：= 4（位）
	15	msg.function	byte	0x02（写数据）

举例：客户机置位 S7-300（站地址为 2）的 Q0.5

客户机发送（16 进制）：

03	FF	09	01	00	00	34	00	02	01	00	00	00	00	54	02	01

服务器发送（16 进制）：

FF	03	08	01	34	00	00	00	02	01	00	00	00	00	54	02

绿色数据为写入的 Q0.5 的位值，即 ON；

红色数据为起始地址 QB0（0x0000），0x54 的高 4 位（=5）为位偏移；

10.11 错误号 msg.f

0x00：无错误；

0xA1~0xAC：PLC 忙或应答错误（S7 总线通讯错误）；

0x88~0x8E：PLC 非法地址访问（读写的地址在 PLC 中不存在）；

通常访问非法地址的错误号是 0x8C。

11.PLC 数据交换

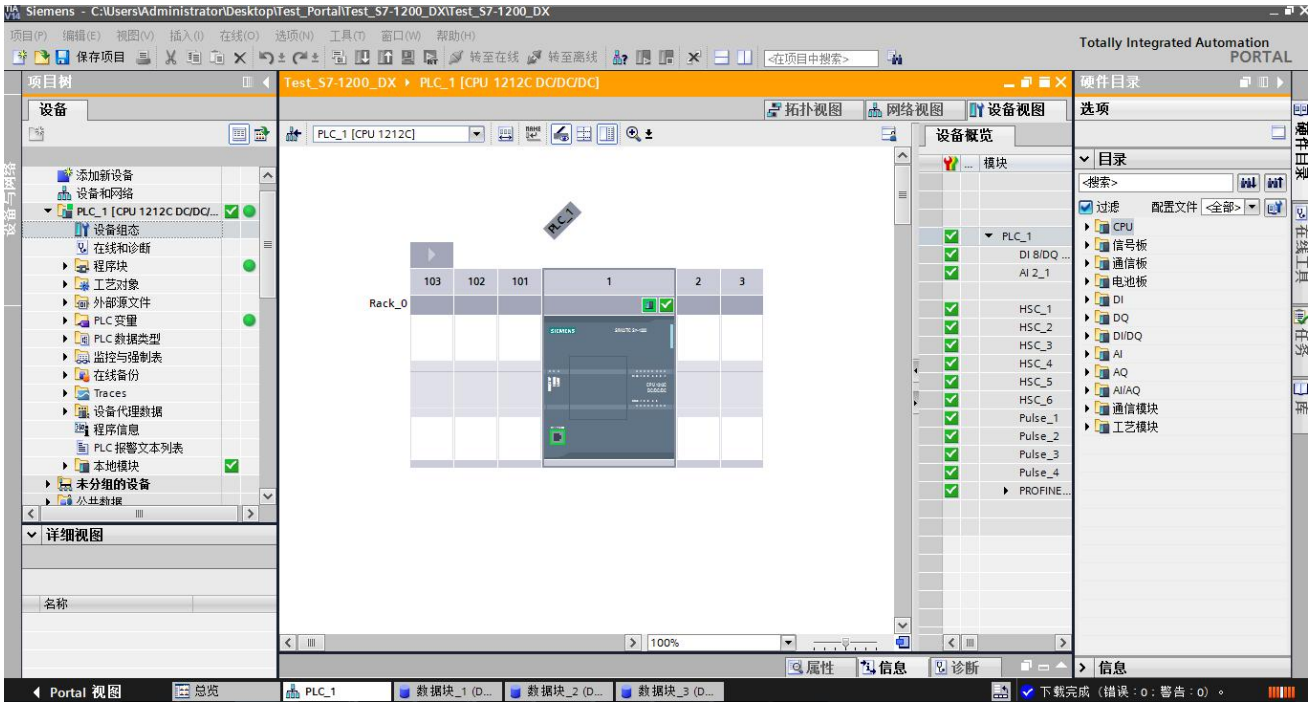
11.1 S7300 通过 RVNet-S7300 Plus 和 S7-1200/1500 等西门子 PLC 数据交换

本示例以 S7-1200(CPU 1212C DC/DC/DC)与 S7-300(CPU315-2DP)为例交换数据，S7-1500、SMART 200 与之步骤类似，不做重复介绍。

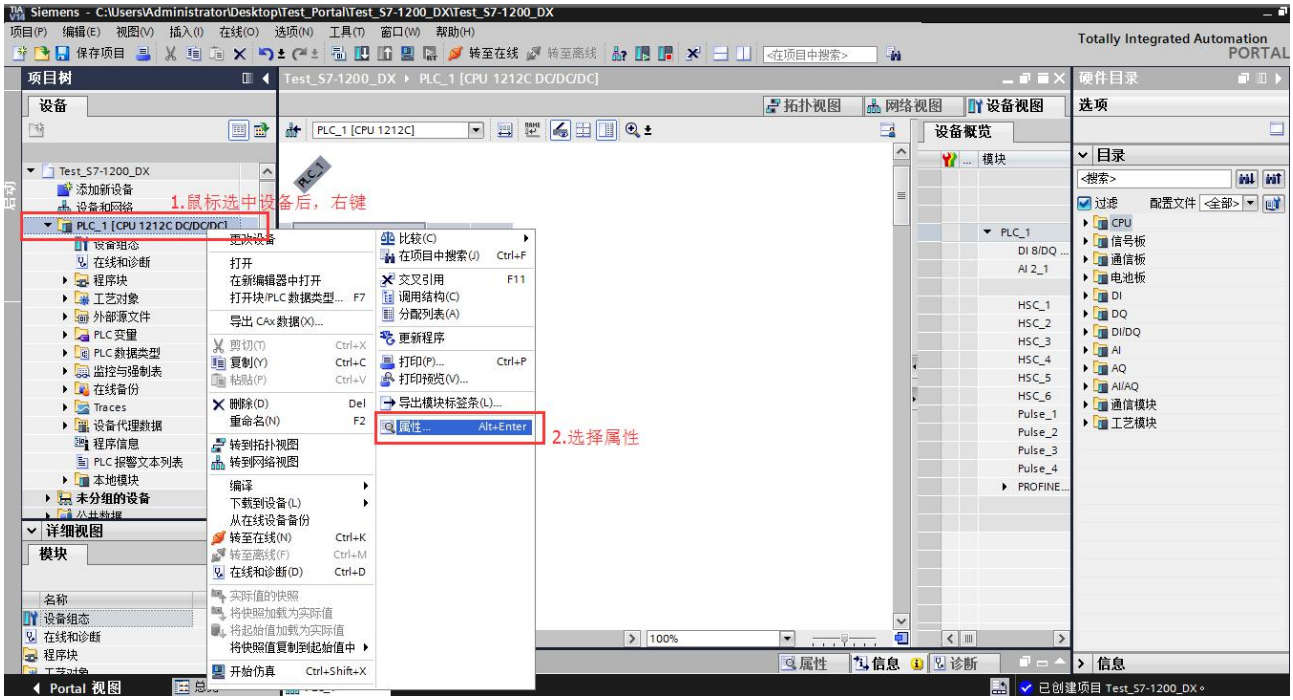
RVNet 的 DB9 公口（X1）连接 S7-300 的 MPI 口/DP 口，S7-1200 自带以太网口与 RVNet 的以太网口通过交换机连接，RVNet 通过 NetDevice 工具配置交换命令，实现实时高效的 S7-300 和 S7-1200 数据交换。

11.1.1 配置 S7-1200

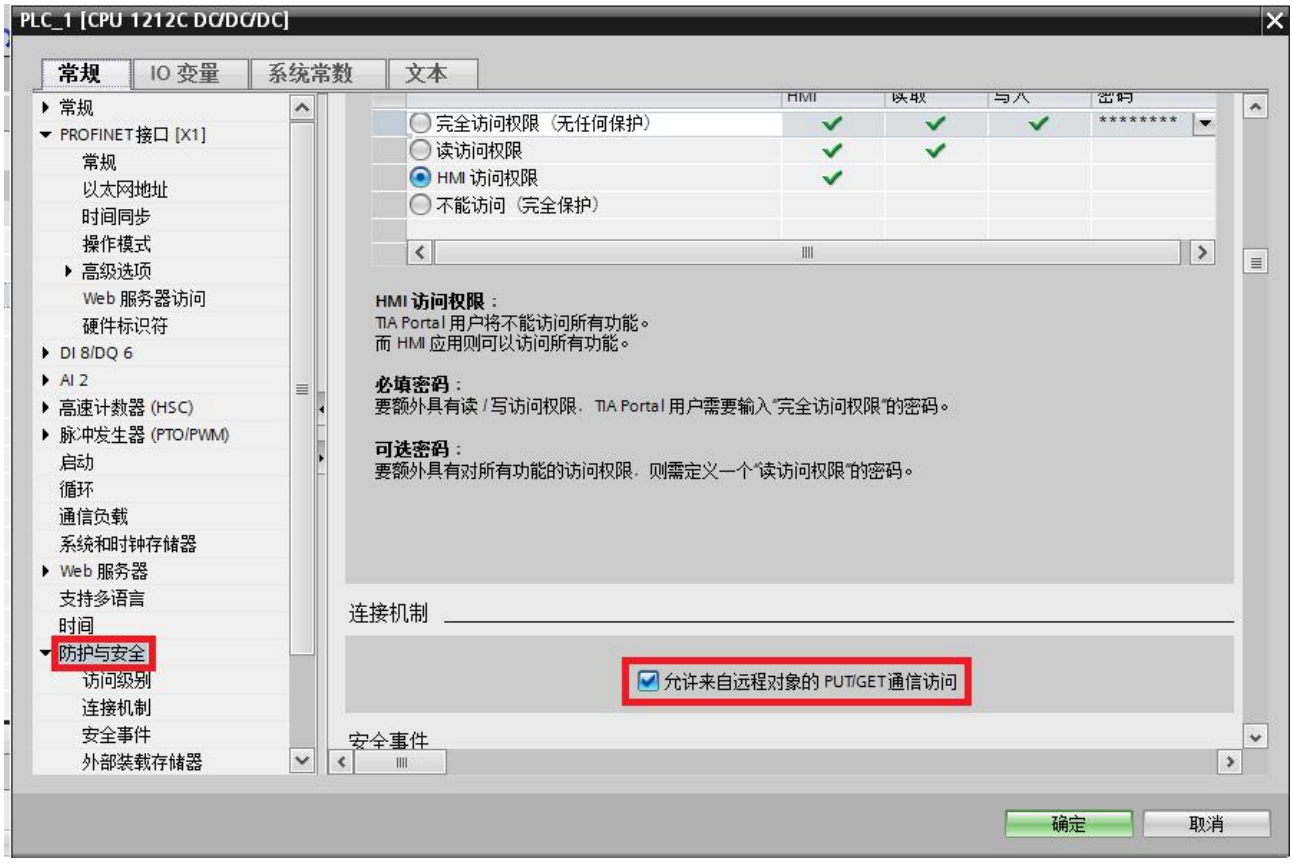
1、打开 TIA portal V14，新建项目，组态，连接 PLC；



2、选择 CPU，右键点击 PLC，选择【属性】；



3、配置属性；

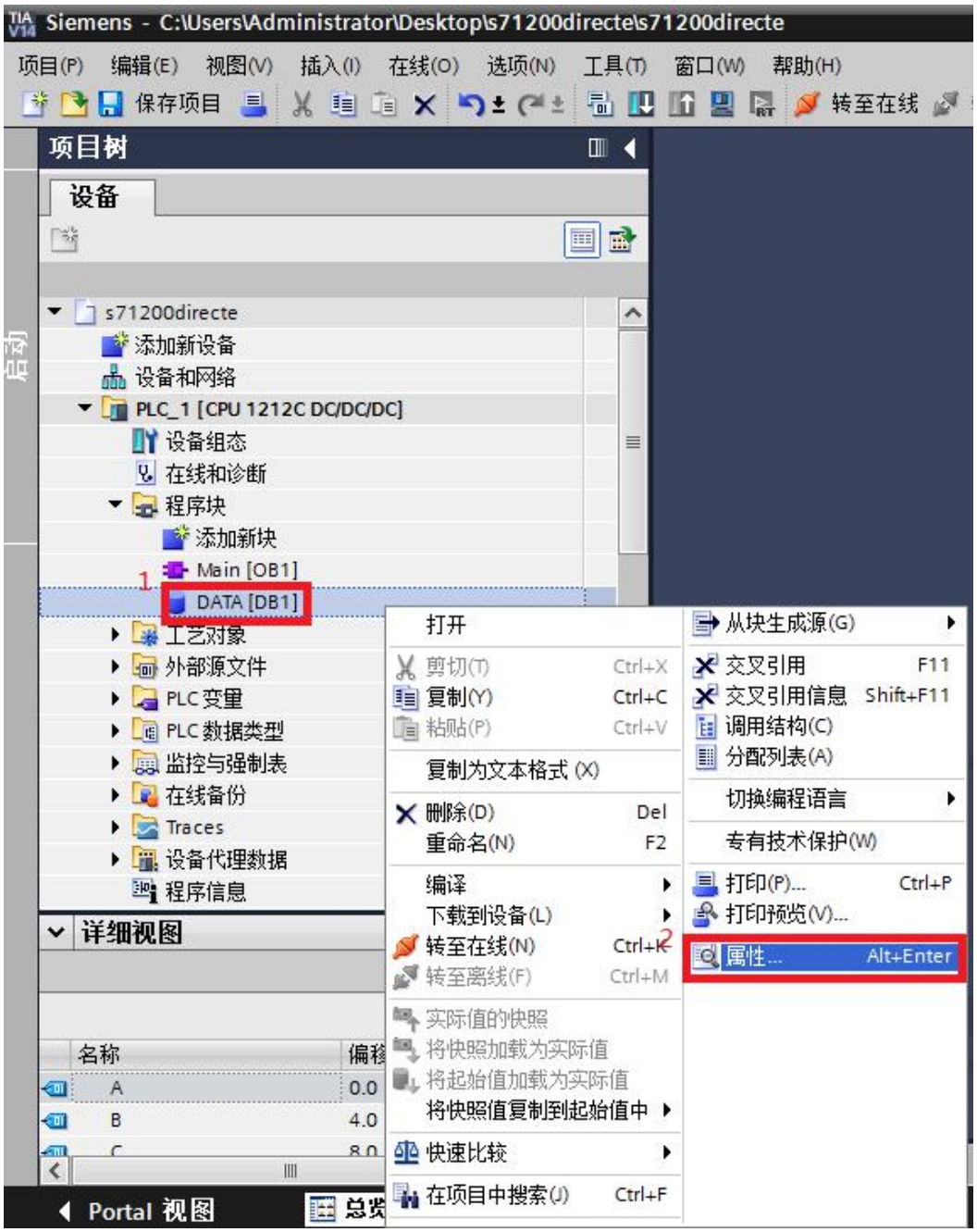


➢ 选择【防护与安全】;

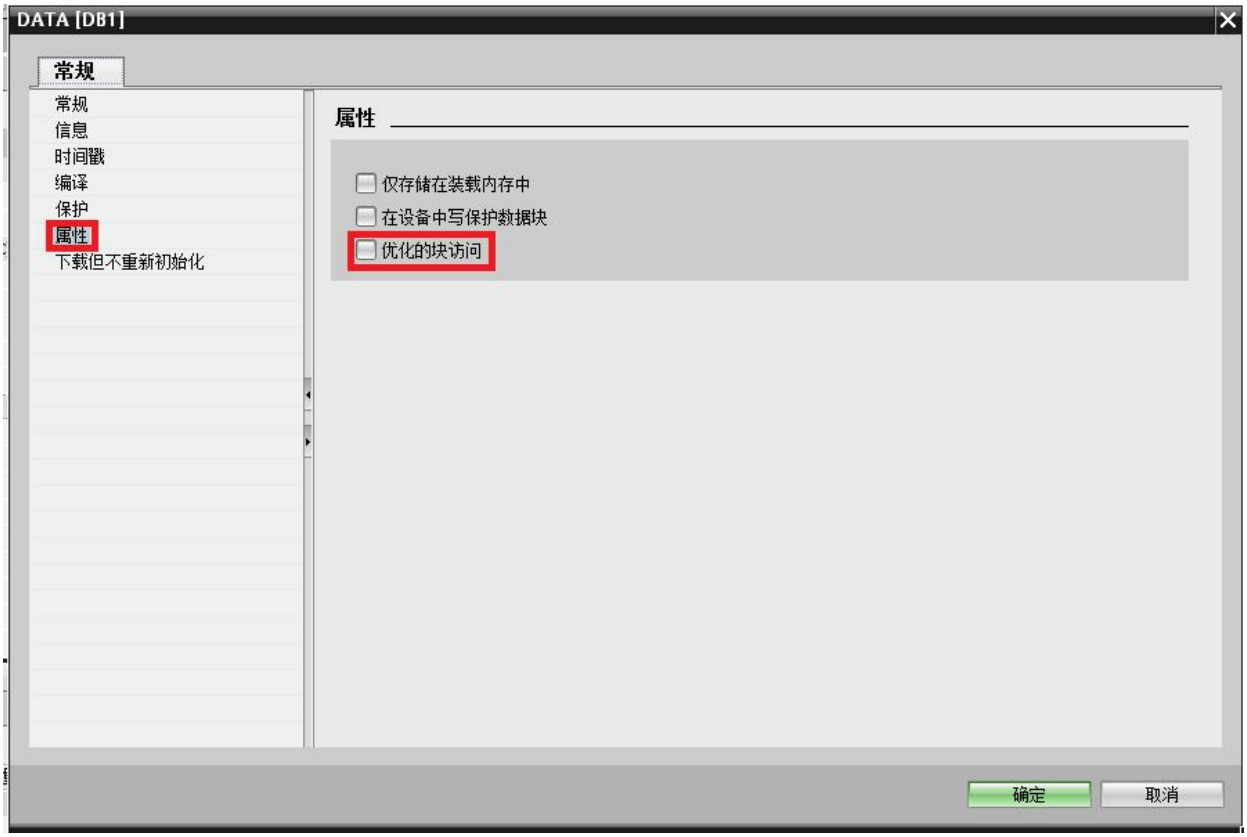
- **打钩【允许来自从远程对象的 PUT/GET 通信访问】;**
- 点击确认下载;

注意：当你需要对 DB 数据块的数据做数据交换的时候，还需要对 DB 数据块做如下设置：

1. 选择 DB 数据块，右键点击 DB 数据块，选择【属性】;

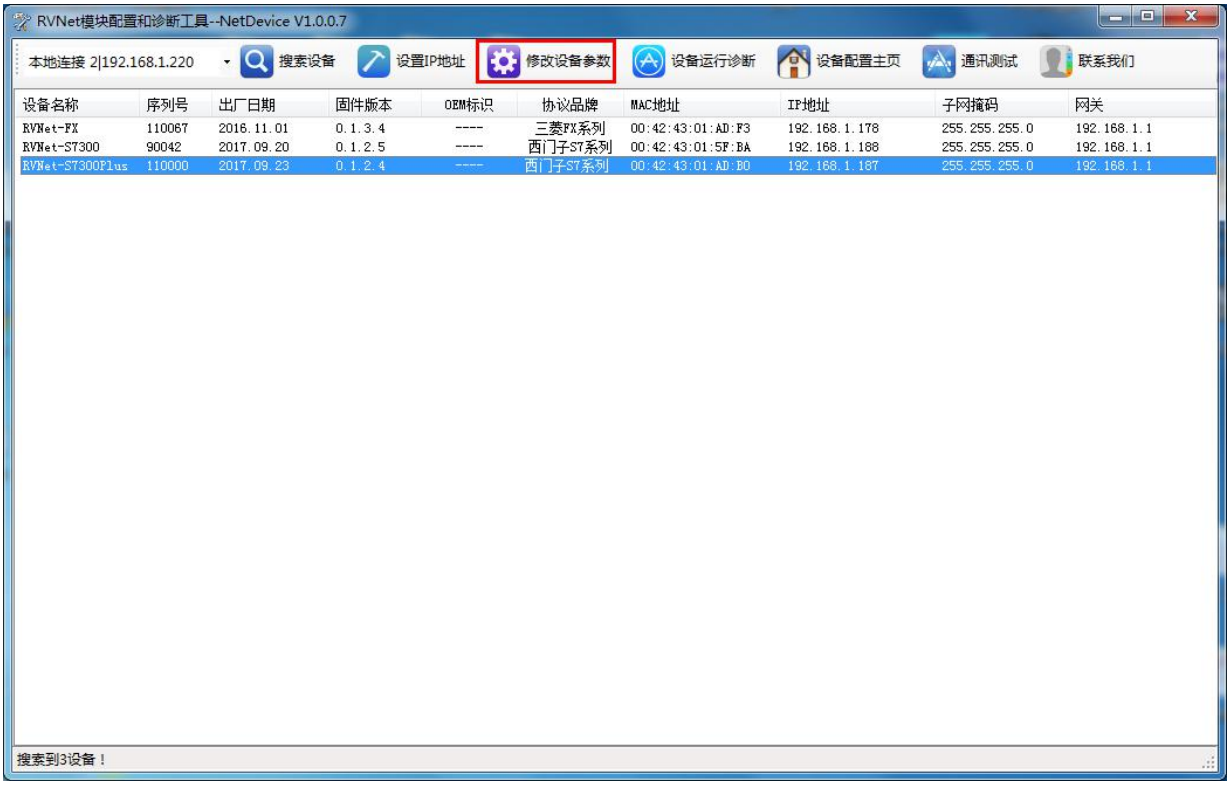


2.选择【属性】，右击【属性】，【优化的块访问】请不要打钩。



11.1.2 配置 RVNet 模块数据交换命令

1、打开 NetDevice，搜索到 RVNet-S7300Plus 后，选择【修改设备参数】;



2、新建客户机

- 点击数据交换，右键创建新的客户机 0；
- 【远程服务器的 IP 地址】为 S7-1200 的 IP 地址，例如：192.168.1.178；远程服务器的通讯端口号，默认为 102；连接超时时间默认为 10S；
- 本地/远程 TSAP

  本地 TSAP 可任意填写，远程 TSAP：包含两个字节，第一个字节标识访问的资源，01 是 PG,02 是 OP，03 是 S7 单边(服务器模式)，10(hex)及以上是 S7 双边通讯。第二个字节是访问点，可能是 CPU 的槽号，CP 的槽号等等。

本地 TSAP	远程 TSAP
任意	01 00/01
任意	02 00/01
任意	03 00/01

- 点击确认，创建客户机。

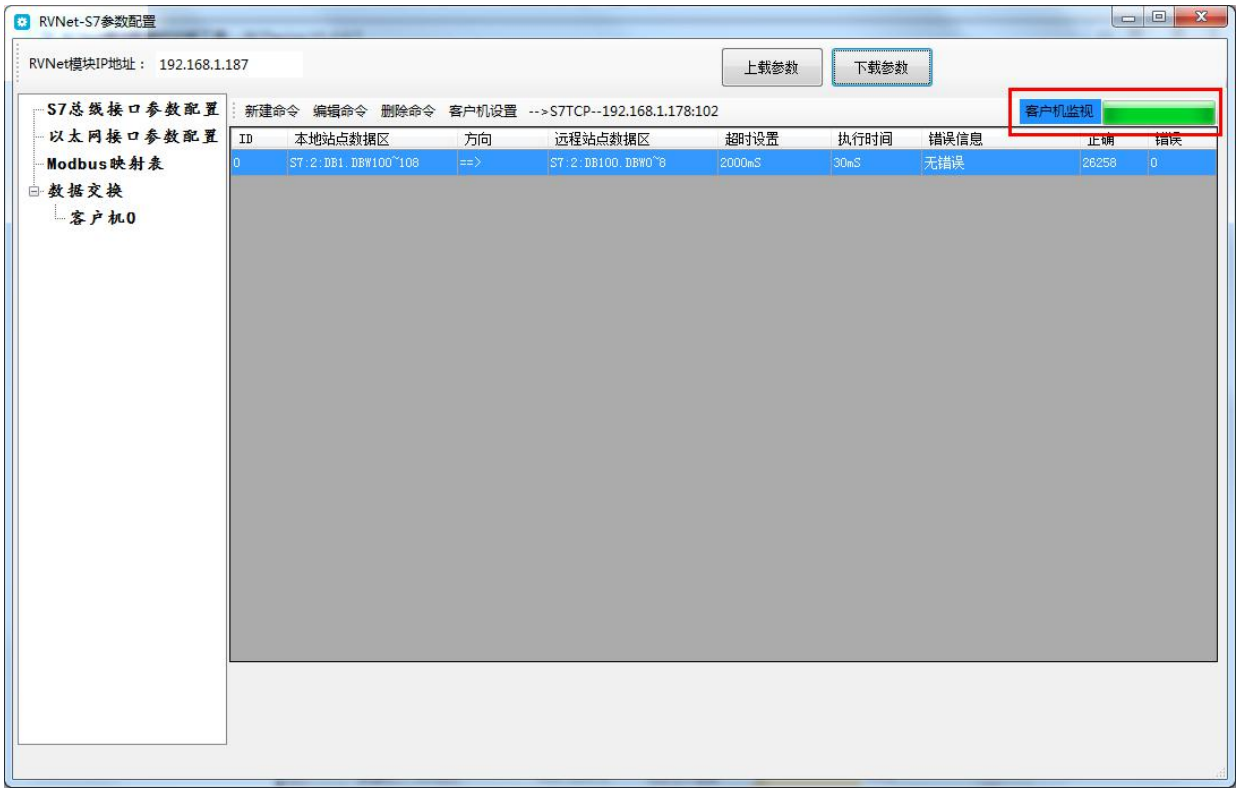
3、在客户机中配置数据交换命令

- 点击新建命令

  例如需要新建命令：S7-1200 的 DB100.DBW0~DB100.DBW8 读取 S7-300 的 DB1.DBW100~DB1.DBW108，总共 5 个字的数据；

- 选择[本地→远程]，在【设置传输的数据类型和个数】输入需要传输数据的个数和类型，例如：传输 5 个字；传输超时设置为 2S；
- 本地站点(S7-300)设置 RVNet 所在总线的 PLC 的站地址，数据区域选择 DB 块，DB 号为 1，字节偏移为 100，位偏移忽略；
- 远程站点(S7-1200)的 PLC 地址无需设置，数据区域选择 DB 块，DB 号为 100，字节偏移为 0，位偏移忽略；
- 点击【检查】按钮可进行规则检查，点击【确认】按钮即可生成命令；

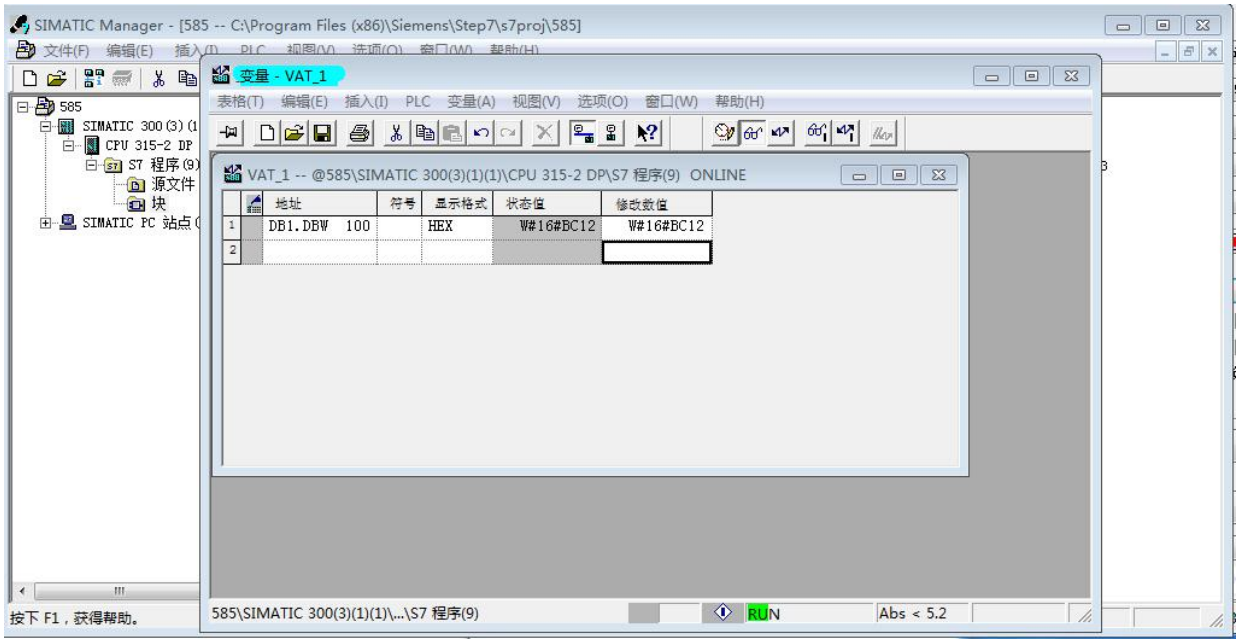
4、客户机监视



点击客户机监视按钮，【错误信息】为无错误，且【正确】有数据跳动，说明通信成功。

11.1.3 验证数据交换

1、打开 SIMATIC Manager 变量表，对 DB1.DBW100 进行数据修改为 BC12H;



2、打开 TIA portal V14 变量监控与强制表，对 DB100.DBW0 进行数据监视，值为 BC12H;

11.2 S7200 通过 RVNet-S7200Plus 和 SMART200 PLC 数据交换

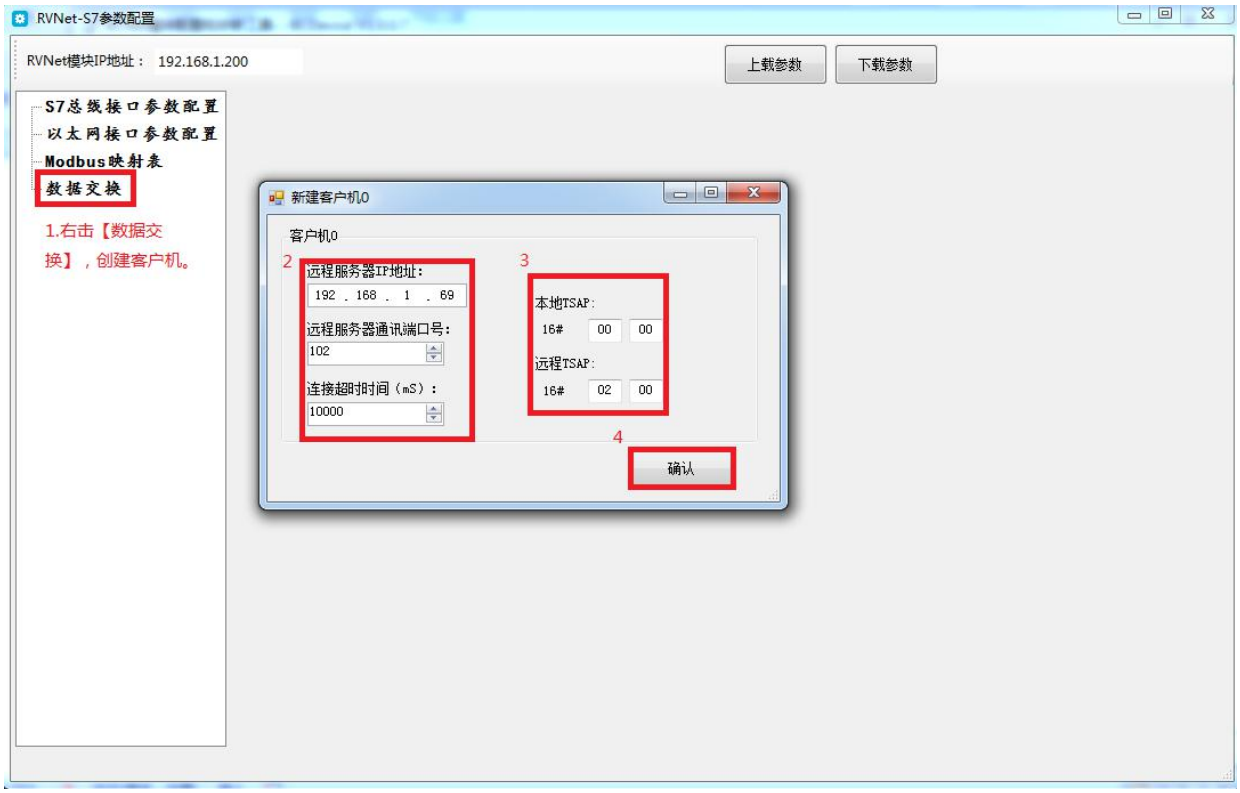
本示例以 S7-200(CPU224XP)与 SMART200 为例介绍如何实现两者之间的交换数据。

RVNet 的 DB9 公口（X1）连接 S7-200 的 PPI 口，SMART200 自带以太网口与 RVNet 的以太网口通过交换机连接，RVNet 通过 NetDevice 工具配置交换命令，实现实时高效的 S7-200 和 SMART200 的数据交换。

11.2.1 配置 RVNet 模块数据交换命令

1、打开 NetDevice，点击【搜索设备】，搜索到 RVNet-S7200Plus 后，点击【修改设备参数】;

2、新建客户机



- 点击数据交换，右键创建新的客户机 0；
- 远程服务器的 IP 地址为 SMART200 的 IP 地址，这里设置为 192.168.1.69；

远程服务器的通讯端口号，默认为 102；连接超时时间默认为 10S；

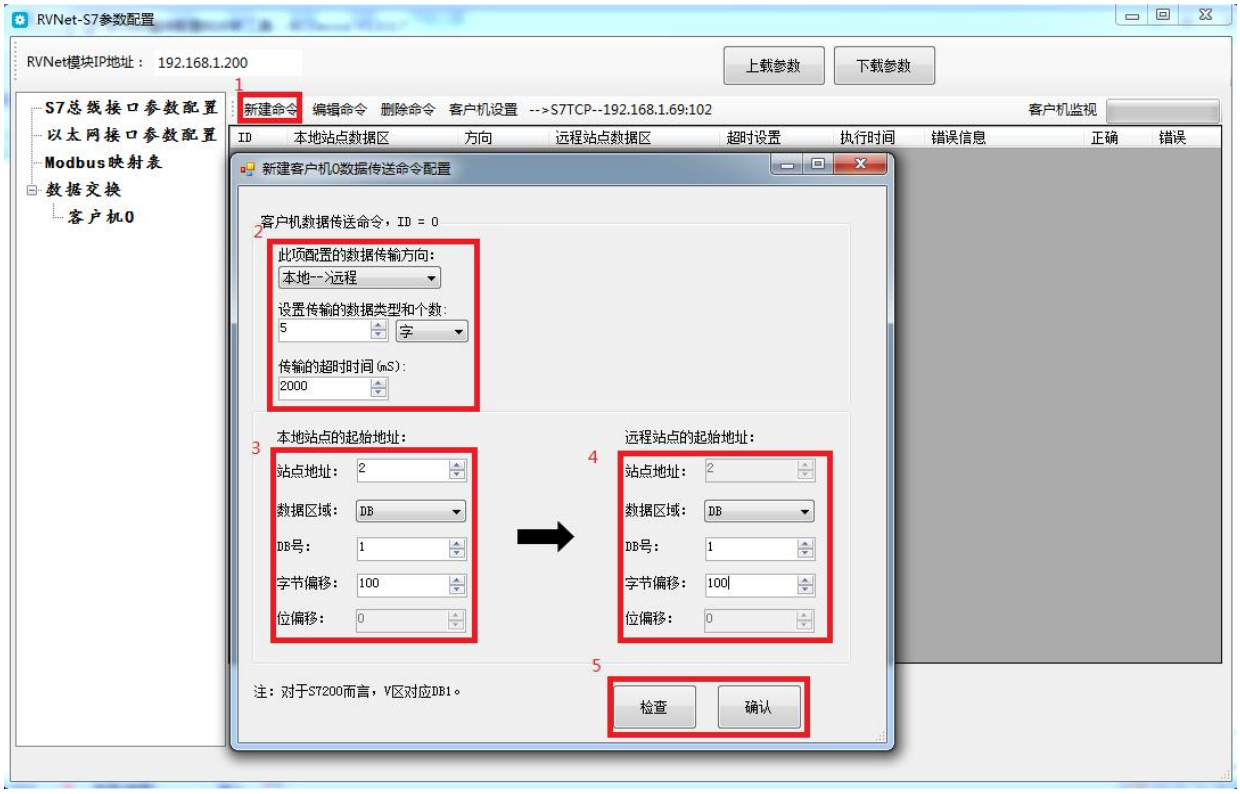
- 本地/远程 TSAP

本地 TSAP 可任意填写，远程 TSAP：包含两个字节，第一个字节标识访问的资源，01 是 PG,02 是 OP，03 是 S7 单边(服务器模式)，10(hex)及以上是 S7 双边通讯。第二个字节是访问点，可能是 CPU 的槽号，CP 的槽号等等。

➢ 本地 TSAP	➢ 远程 TSAP
➢ 任意	➢ 01 00/01
➢ 任意	➢ 02 00/01
➢ 任意	➢ 03 00/01

- 点击确认，创建客户机。

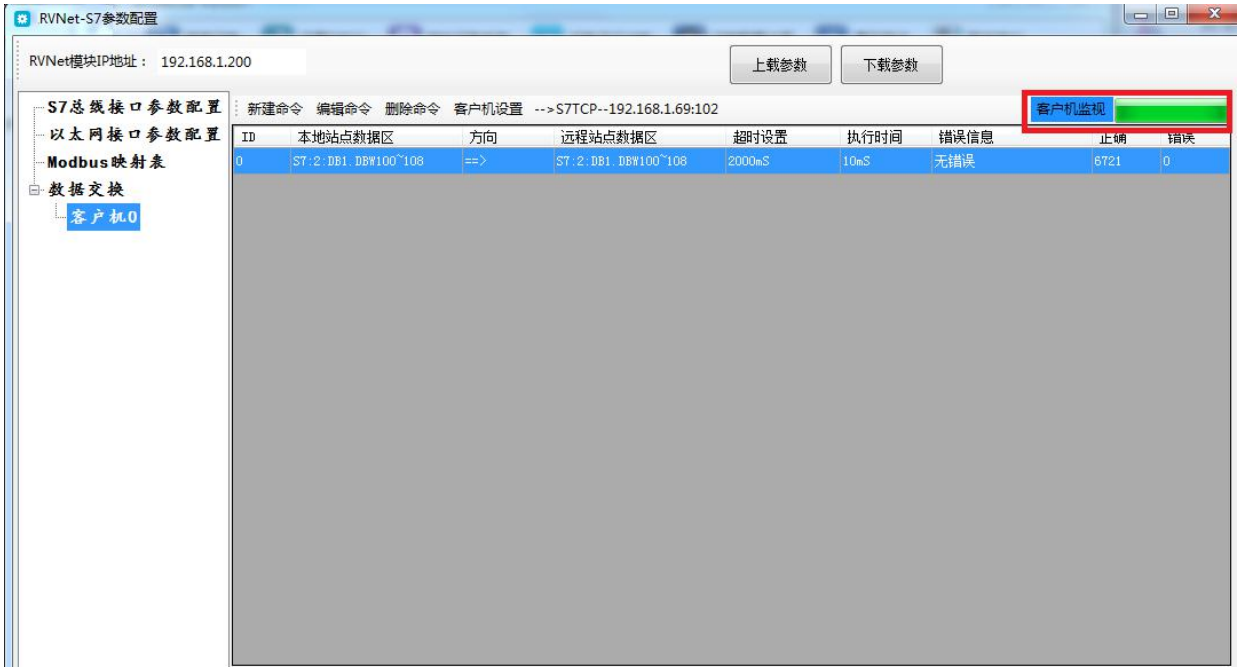
3、在客户机中配置数据交换命令



- 点击新建命令（SMART200 的 VW100~VW108 读取 S7-200 的 VW100~VW108）；
- 选择[本地→远程]，传输 5 个字；传输超时设置层 2S；

- 本地站点(S7-200)设置 RVNet 所在总线的 PLC 的站地址，数据区域选择 DB 块，DB 号为 1（对于 S7200 而言，V 区对应 DB1），字节偏移为 100，位偏移忽略；
- 远程站点(SMART200)的 PLC 地址无需设置，数据区域选择 DB 块，DB 号为 1,(对于 SMART200 而言,V 区对应 DB1)字节偏移为 100，位偏移忽略；
- 点击【检查】按钮可进行规则检查，点击【确认】按钮即可生成命令；

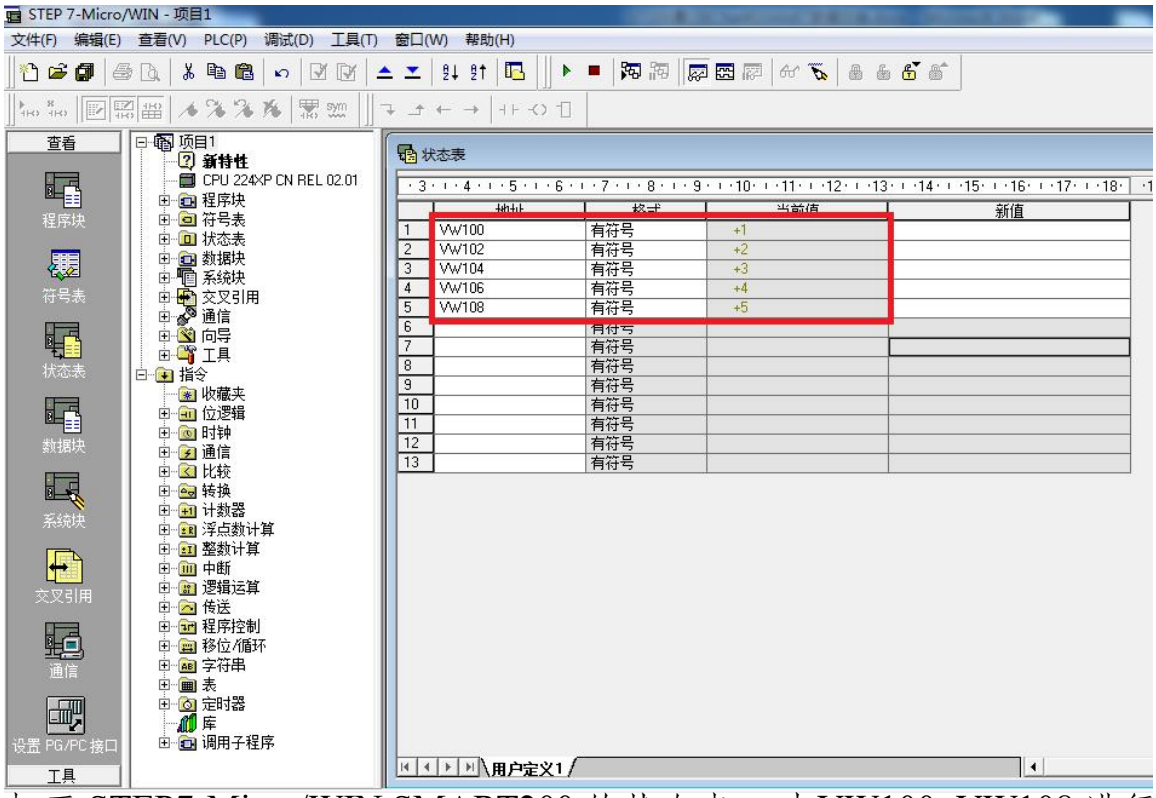
4、客户机监视



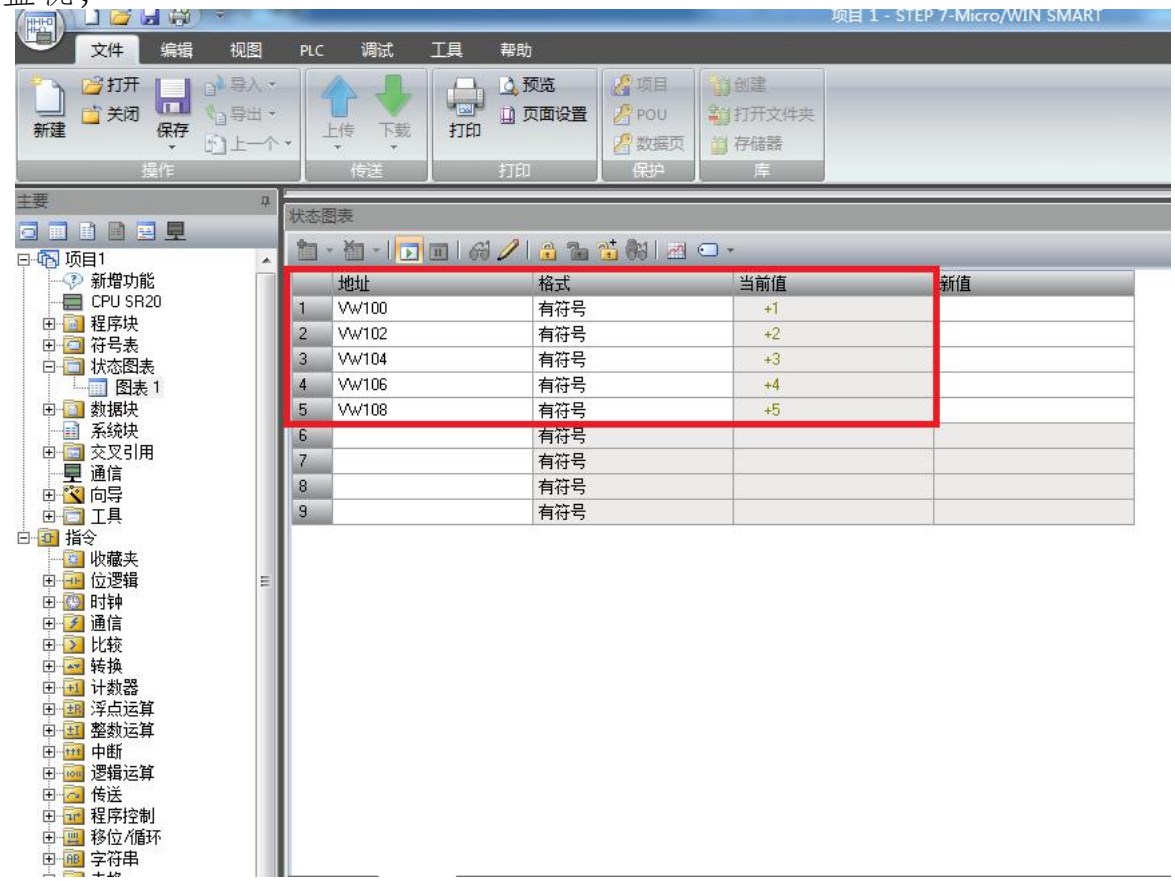
点击客户机监视按钮，【错误信息】为无错误，且【正确】有数据跳动，说明通信成功。

11.2.2 验证数据交换

1、打开 STEP7-Micro/WIN 的状态表，将 VW100~VW108 的数据分别修改为 1、2、3、4、5;



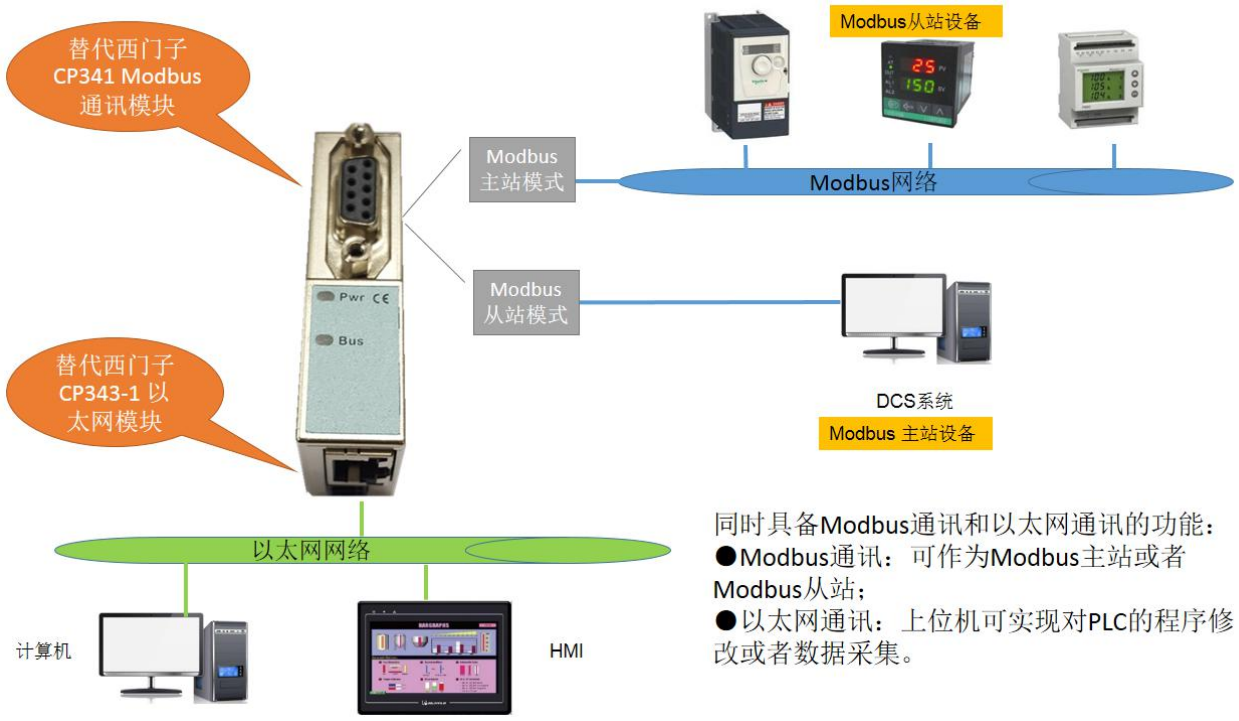
2、打开 STEP7-Micro/WIN SMART200 的状态表，对 VW100~VW108 进行数据监视；



3、两者数据完全一致。

12.Modbus 通讯

RVNet-S7Plus 桥接型模块支持 Modbus 功能，可作为 Modbus 主站或者 Modbus 从站，实现 PLC 与其他 Modbus 设备的通讯。



12.1Modbus 主站功能

12.1.1 功能和应用

RVNet 的扩展母口作为 Modbus 主站运行，连接外部 Modbus 仪表，根据预置命令在西门子 PLC 和 Modbus 仪表之间交换数据。应用于西门子 PLC 和 Modbus 仪表进行通讯。

RVNet 可最多配置 72 条数据交换命令，可以传送的数据类型包括位、字节和字。单条命令最多一次传送连续的 100 个字（寄存器），对 Modbus 站点数目并无限制。

12.1.2 通讯线连接

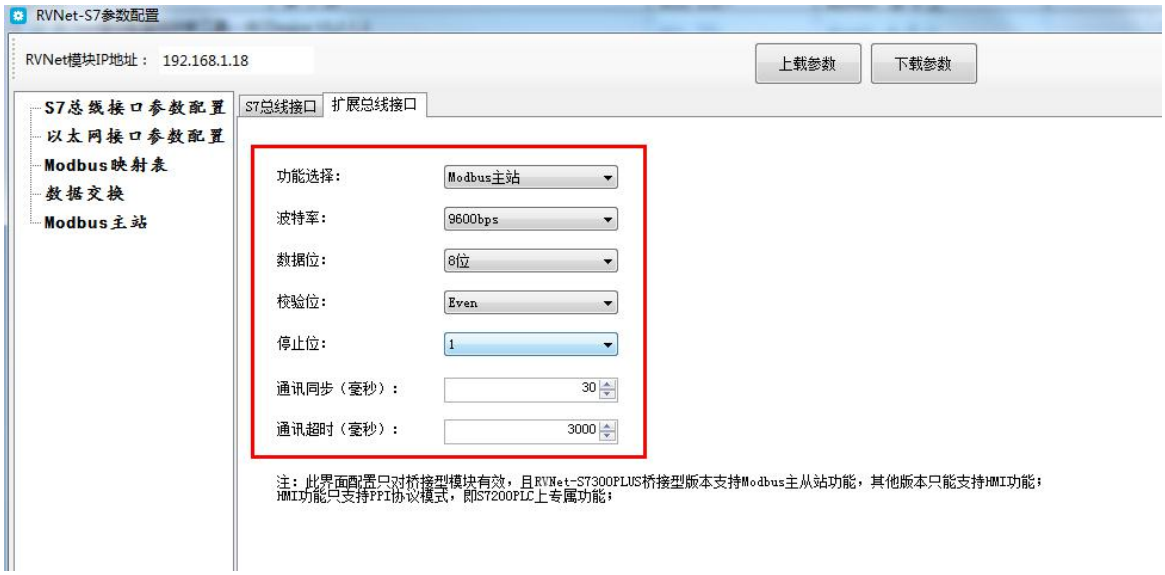
RVNet 的扩展总线接口连接外部 Modbus 仪表，桥接模式下 RVNet 扩展总线接口的针脚定义：

RVNet 扩展通讯口引脚 DSUB9 母口	定义	说明
第 3 脚	RX/TX+	RS485 信号正
第 8 脚	RX/TX-	RS485 信号负
第 5 脚	GND	RS485 信号地

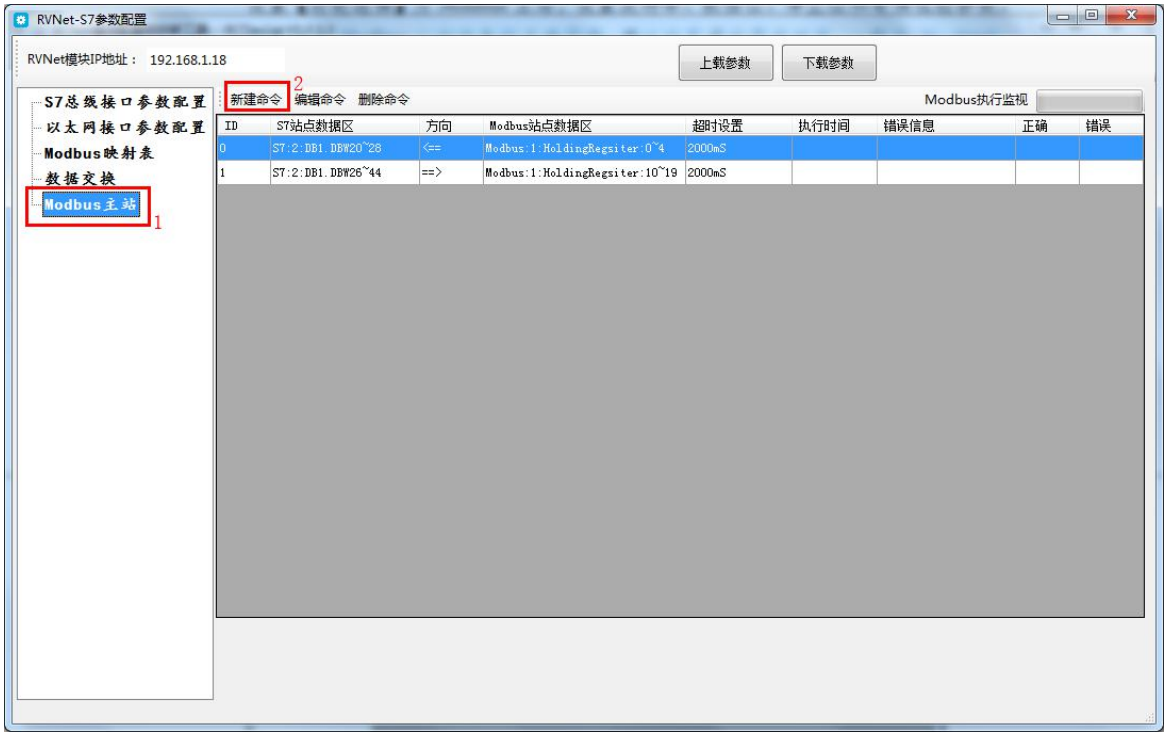
12.1.3 RVNet 配置

配置步骤：NetDevice 搜索→参数配置→扩展总线接口→Modbus 从站。

1. 电脑连接 RVNet 模块，运行 NetDevice（V1013 版本以上）配置软件，选择查找到的 NetDevice 模块，点击按钮栏【修改设备参数】按钮。
2. 在参数配置界面左侧选择【S7 总线接口参数配置】，右侧页面选择【扩展总线接口】，设置【功能选择】为 Modbus 主站，设置波特率、数据位、停止位和奇偶校验参数。如果为多 Modbus 从站设备的总线网络，建议设定通讯同步时间，一般为 30~50mS；



3. 在参数配置界面左侧选择【Modbus 主站】，右侧页面点击【新建命令】配置数据交换命令。



4. 编辑新建 Modbus 数据传送命令对话框，配置完成后点击【检查】查看有无错误，点击【确定】保存该命令。

如上：

1) 数据传送方向
   - Modbus→S7：读取 Modbus 仪表数据传送到西门子 PLC；
   - S7→Modbus：读取西门子 PLC 数据传送到 Modbus 仪表；

   传送的数据个数、数据类型和数据区域
   - 对于位传送，只能传送一个位，数据区域：COIL 和 INPUT；
   - 对于字节传送，最多连续的 200 个字节，数据区域：COIL 和 INPUT；字节传送只能是 Modbus→S7 方向。
   - 对于字传送，最多连续的 100 个字，数据区域：INPUT REG 和 HOLDING REG（输入寄存器和保持寄存器）。
2) S7 站点的起始地址:指定 PLC 的通讯口站地址和传送区域,对于 S7-200 的 V 区请选择 DB1。另外对于 S7-200 的 SM/AI 区只能读取，不能写入。
3) Modbus 站点的起始地址：指定 Modbus 站号和数据区起始地址。另外对于 INPUT REG 只能读取不能写入。

5. 命令示例

1) S7→Modbus 字传送：读取 PLC 地址为 2 的 DB10.DBW0~18 传送到 Mdobus 1 号站的 40001（HoldingRegsiter 保持寄存器 1）开始的 10 个字。

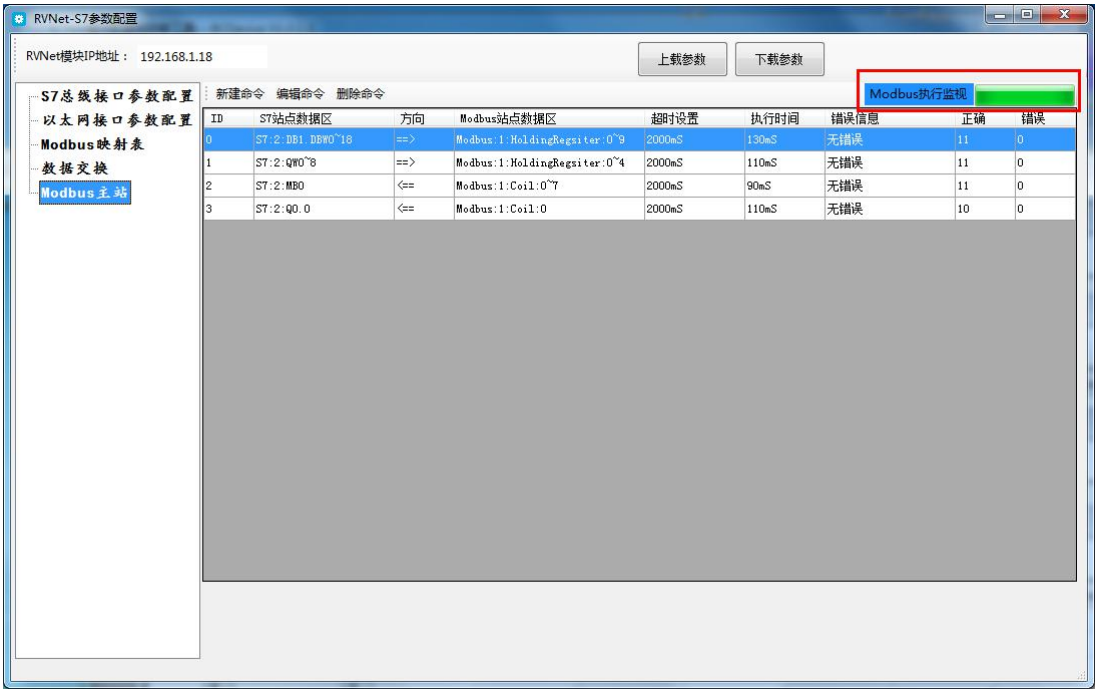
2) S7→Modbus 字传送：读取 PLC 地址为 2 的 QW0~18 传送到 Mdobus 1 号站的 40001（HoldingRegsiter 保持寄存器 1）开始的 10 个字。

3) Modbus→S7 字节传送：读取 Modbus 1 号站的 00001（Coil 线圈 1）~00008（Coil 线圈 8）之间的数据传送到 2 号 PLC 的 MB0。

4) Modbus→S7 位传送：读取 Modbus 1 号站的 00001（Coil 线圈 1）数据传送到 2 号 PLC 的 Q0.0。

ID	S7站点数据区	方向	Modbus站点数据区	超时设置	执行时间	错误信息	正确	错误
0	S7:2:DB10.DBW0~18	==>	Modbus:1:HoldingRegsiter:0~9	2000mS				
1	S7:2:QW0~18	==>	Modbus:1:HoldingRegsiter:0~9	2000mS				
2	S7:2:MB0	<==	Modbus:1:Coil:0~7	2000mS				
3	S7:2:Q0.0	<==	Modbus:1:Coil:0	2000mS				

6. 配置完成后点击【下载参数】按钮，将参数下载到 RVNet；设备重启运行后可对运行状态进行监视；



12.2.4 通讯测试

Modbus 仪表较常见的有各种智能温控仪，示例以集成 ModbusRTU 从站通讯口的温控器仪表为例，说明如何实现 RVNet 的 Modbus 主站数据通讯。

示例功能：将两台温控仪表的实际温度值（PV）分别读取到一台 S7-300 的 DB1.DBW100 和 DB1.DBW102 数据区；将 S7-300 的 DB1.DBW200 和 DB1.DBW202 数据作为温度设定值（SV）分别传送到两台温控仪表。

1. 接线：用 PROFIBUS 电缆连接两台温控器，将 PROFIBUS 网络插头插在 RVNet 的扩展总线接口上。如果自制通讯线，RVNet 扩展总线接口的 3 脚接 RS485+（接温控器 A 端口），8 脚接 RS485-（接温控器 B 端口），5 脚接 RS485 地。
2. 设置温控器参数为 Modbus 通讯协议，地址分别为 1 和 2，设置 9600bps 波特率，8 数据位，偶校验，一个停止位；
3. 配置 RVNet 参数，下载参数。
   1) 扩展总线接口参数：Modbus 主站，9600bps 波特率，8 位数据位，1 位停止位，偶校验。
   2) 配置 Modbus 主站命令：
   温控器的当前温度（PV 值）在保持寄存器 16#14，即保持寄存器的 20；设定值（SP 值）在保持寄存器的 16#28，即保持寄存器的 40。
   按示例要求配置如下命令：

新建命令 编辑命令 删除命令

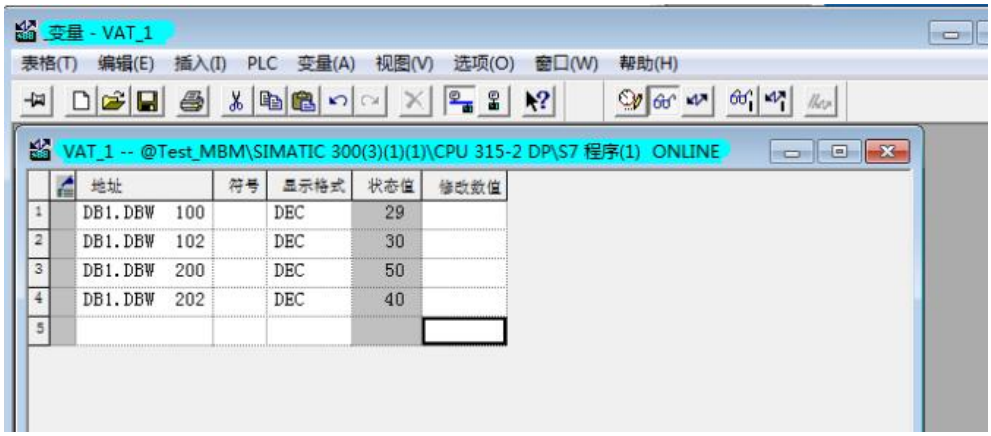
ID	S7站点数据区	方向	Modbus站点数据区	超时设置
0	S7:2:DB1.DBW100	<==	Modbus:1:HoldingRegsiter:20	2000mS
1	S7:2:DB1.DBW102	<==	Modbus:2:HoldingRegsiter:20	2000mS
2	S7:2:DB1.DBW200	==>	Modbus:1:HoldingRegsiter:40	2000mS
3	S7:2:DB1.DBW202	==>	Modbus:2:HoldingRegsiter:40	2000mS

4. 点击参数配置页面的【Modbus 执行监视】，查看命令执行信息。

新建命令 编辑命令 删除命令 Modbus执行监视

ID	S7站点数据区	方向	Modbus站点数据区	超时设置	执行时间	错误信息	正确	错误
0	S7:2:DB1.DBW100	<==	Modbus:1:HoldingRegsiter:20	2000mS	100mS	无错误	72	0
1	S7:2:DB1.DBW102	<==	Modbus:2:HoldingRegsiter:20	2000mS	100mS	无错误	72	0
2	S7:2:DB1.DBW200	==>	Modbus:1:HoldingRegsiter:40	2000mS	100mS	无错误	71	0
3	S7:2:DB1.DBW202	==>	Modbus:2:HoldingRegsiter:40	2000mS	100mS	无错误	71	0

5. 打开 Step7 软件，连接 RVNet，在监控表中输入 DB1.DBW100，DB1.DBW102，DB1.DBW200 和 DB1.DBW202，查看 DB1.DBW100/1002 是否为温控器的实际温度，修改 DB1.DBW200/2002 查看温控器设定温度是否一致。



6. 总结：

1) RVNet 的 Modbus 主站功能依据预先配置的数据交换命令自动执行 Modbus 仪表和 PLC 之间的数据传输，无须在 PLC 中编程；
2) RVNet 的 Modbus 主站通讯并不影响上位机的以太网通讯，上位机（如编程软件、监控组态软件、以太网触摸屏等）仍然可以通过以太网读写 PLC 数据；
3) 利用命令的连续数据区多字节/字传送可减少每个站点的命令数，从而增加可通讯站点；
4) 对于位传送，可以采用字节数据类型，连续的 8 个位值将直接传送到 PLC 中的一个字节地址；
5) 提高 PLC 的波特率（如 S7-200 设置为 187.5Kbps）和 RVNet 扩展通讯口的波特率（最高 256Kbps）可以加快 Modbus 数据交换的速度；如果 Modbus 通讯线较长应适当降低波特率；
6) 所有的 Modbus 站点需设置为站地址不一样，波特率、数据位和校验位应该相同并和 RVNet 扩展通讯口参数一致；

12.2Modbus 从站功能

12.2.1 功能和应用

RVNet-S7300PLUS 的扩展母口作为 ModbusRTU 从站运行，外部具备 ModbusRTU 主站的设备通过 Modbus 协议访问 RVNet 九针公口所连接的西门子 PLC 数据。应用于 DCS 系统或者触摸屏等通过 Modbus 总线读写西门子 PLC 数据。

12.2.2 通讯线连接

远程 Modbus 主站设备通过 RS485 总线连接到 RVNet 的扩展通讯口，桥接模式下 RVNet 扩展通讯口的针脚定义：

RVNet 扩展通讯口引脚 DSUB9 母口	定义	说明
第 3 脚	RX/TX+	RS485 信号正
第 8 脚	RX/TX-	RS485 信号负
第 5 脚	GND	RS485 信号地

12.2.3 RVNet 配置

配置步骤：NetDevice 搜索→参数配置→扩展总线接口→Modbus 从站。

1. 电脑连接 RVNet 模块，运行 NetDevice（V1013 版本以上）配置软件，选择查找到的 RVNet 模块，点击按钮栏【修改设备参数】按钮。
2. 在参数配置界面左侧选择【S7 总线接口参数配置】，右侧页面选择【扩展总线接口】，设置【功能选择】为 Modbus 从站，设置波特率、数据位、停止位和奇偶校验参数。
3. 配置 Modbus 映射，详见前章节介绍；

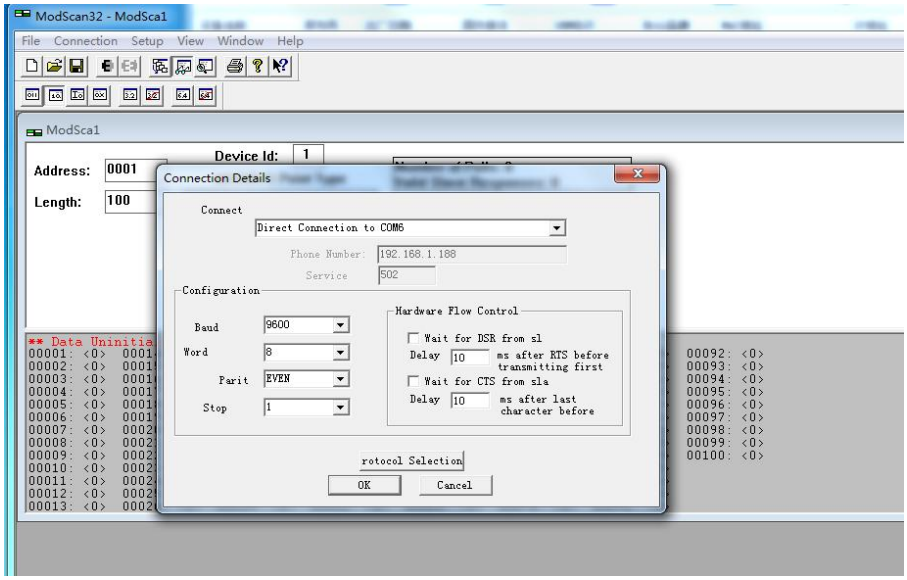
4. 设置好后点击【下载参数】按钮，将参数下载到 RVNet。

12.2.4 Modbus 测试

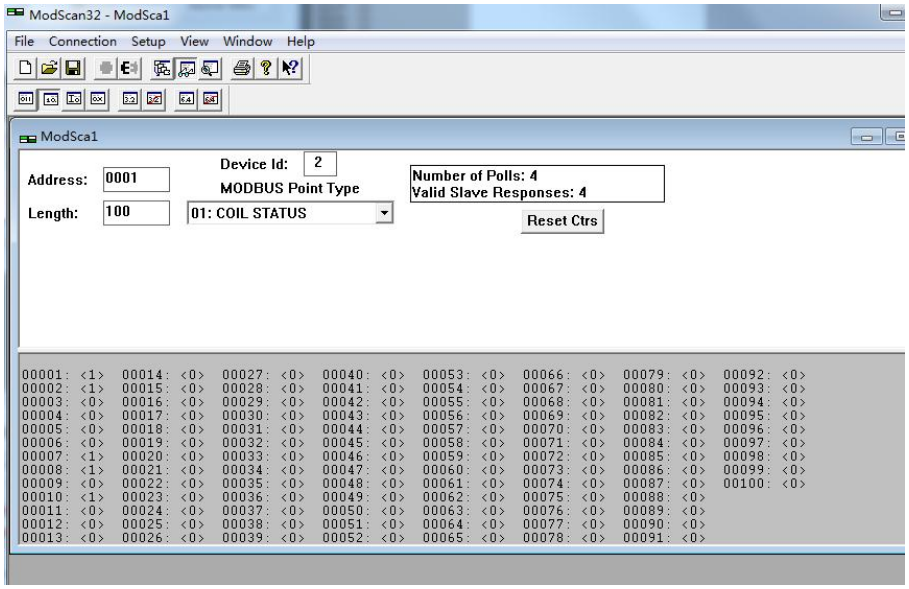
Modbus 测试可采用 ModScan 软件，该软件作 Modbus 主站，去连接 RVNet。

1. 采用一根 USB 转 RS485 的转换线，USB 端口接入计算机，RS485 端子连接一根 PROFIBUS 电缆和总线插头，将插头插入 RVNet 的扩展通讯口。

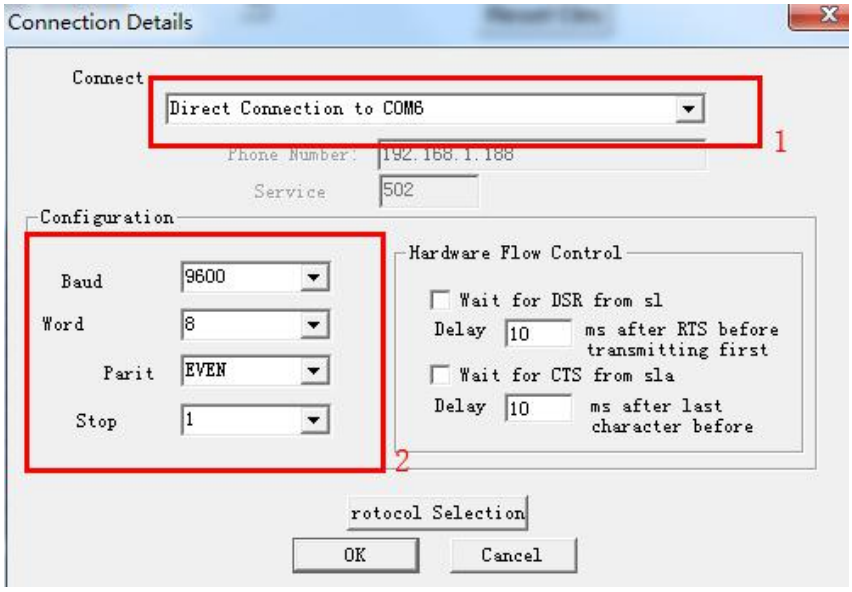
2. 在计算机上运行 ModScan.exe，点击“Connection”，设置相应的连接参数，此处 USB 连接的串口号为 COM6；



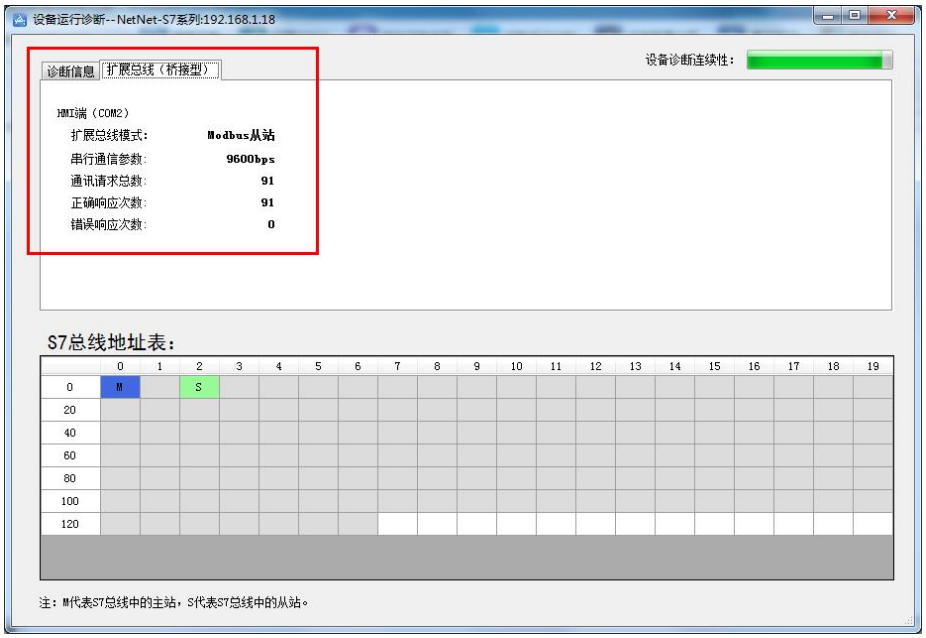
3. 将 Device Id 为西门子 PLC 的通讯口站地址，如 2。读取了线圈 00001 的 100 个线圈状态，查 Modbus 映射表可知为 Q0.0~Q12.4 的值；



4. 注意：1.选择 Direct Connection to COM（USB 转换器对应的 COM 口）；2.波特率、校验位等，这里的参数要和 RVNet 的扩展总线接口设置一致；



5. 用 NetDevice 诊断 RVNet 扩展总线的状态。



6. 总结：

1) RVNet 的 Modbus 从站功能根据预置 Modbus 映射表进行通讯，无须在 PLC 中编写程序；
2) 西门子 PLC 的通讯口站地址就是 Modbus 站地址；
3) RVNet 的 Modbus 从站通讯并不影响 RVNet 的以太网通讯，上位机（如编程软件、监控组态软件、监控组态软件、以太网触摸屏等）仍然可以通过以太网读写 PLC 数据。
4) 提高 PLC 的波特率（如 S7-200 设置为 187.5Kbps）和 RVNet 扩展通讯口的波特率（最高 256Kbps）可以加快 Modbus 数据采集的速度；如果 Modbus 通讯线较长应适当降低波特率。

13.产品技术指标

RVNet-S7 模块满足以下技术指标：

供电电源	24VDC±20%/100mA
工作环境	0-60 度，90%湿度，无结露
安装	西门子 S7PLC　DB9 通讯口直接安装
尺寸	65 x 33 x 17 mm
DB9 通讯口	TIA/EIA RS-485 兼容，ESD：±15KV，最多 32 个节点
DB9 通讯协议	西门子 S7 总线多主站协议，支持 PPI、MPI 从站、MPI 主从站和 PROFIBUS，支持波特率（bps）：9600、19200、45450、93750、187500、500K、1.5M、3M、6M
RJ45 以太网	IEEE 802.3 兼容，10/100M BT，1500Vrms，带 Link/Active 指示灯，支持 Auto-MDIX
以太网协议	S7TCP，RVNetS7，ModbusTCP，32 个 TCP/IP 连接
RoHS 生产	是
抗震动	4.5mm/30Hz/10Min
ESD	6KV
出厂老化	60 度老化箱运行 168 小时，通断电 50000 万次
通讯稳定性	持续一个月和 PLC 不间断通讯测试，1 亿 3 千万次通讯 0 错误

14.联系我们

名称：济南罗威智能科技有限公司

地址：山东省济南市高新区颖秀路 2755 号

邮编：250101

销售：0531-88689022

传真：0531-88689022

名称：青岛启源工业控制技术有限公司

地址：山东省青岛市城阳区德阳路 111 号

邮编：266107

销售：0532-68894021 83029299

传真：0532-83029299

技术支持：18753243991，garywei@dingtalk.com

网址：www.roviniot.com

微信公众号：