

TukBest TK 6000-MPI&PPI 西门子 S7 系列 PLC 以太网通讯处理器

V2.0 使用手册

南京图尔库智能科技有限公司

南京市浦口区泰西路 3 号金泰商务 4 层

电话：15996274156

邮箱：[404357550@qq.com](mailto:404357550@qq.com)

## 1. 产品选型

### 1.1 系列和型号

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

✚ **TukBest（基本版）** 包括三个型号：**TK 6000-PT 直通型**、**TK 6000-PB 桥接型**、**TK 6000-MT**。

┆ **TK 6000-PT 直通型**：适用于西门子 S7200 系列、SMART 系列等 PLC 控制系统的以太网通讯；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）。

┆ **TK 6000-PB 桥接型**：适用于西门子 S7200 系列、SMART 系列等 PLC 控制系统的以太网通讯；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、昆仑通态、海泰克等）。

┆ **TK 6000-MT**：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）。

✚ **TukBest（高级版）** 包括四个型号：**TK 6000-PTP 直通型**、**TK 6000-PBP 桥接型**、**TK 6000-MTP 直通型**、**TK 6000-MTCP 桥接型**。

┆ **TK 6000-PTP 直通型**：适用于西门子 S7200 系列、SMART 系列等 PLC 控制系统的以太网通讯；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）。

┆ **TK 6000-PBP 桥接型**：适用于西门子 S7200 系列、SMART 系列等 PLC 控制系统的以太网通讯；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）。

┆ **TK 6000-MTP 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）。

┆ **TK 6000-MTCP 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。

## 2. 功能应用

### 功能一：编程调试

TukBest 西门子系列模块支持对 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

TukBest 西门子系列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

TukBest 西门子系列 OPC Server 以太网通讯，例如：KEPWARE OPC、PC ACCESS OPC 等。详见《[第七章：OPC 通讯](#)》

## 功能四：触摸屏以太网通讯

TukBest 西门子系列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

TukBest 西门子系列模块内部集成了 ModbusTCP 服务器功能，上位机软件（ModbusTCP 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

TukBest 模块提供开放的以太网协议（TKNetS7 协议）供工程师开发通讯程序软件使用。

## 功能七：PLC 数据交换

TukBest 模块（仅 TukBest（高级版）支持该功能，TukBest（基本版）不支持）支持与西门子 S7-1200、S7-1500、SMART 200PLC 实现交换数据。

## 功能八：Modbus 通讯

TukBest 模块（仅 TK 6000-MTCP 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。

## 3. 安装、诊断

### 3.1 安装

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

## 3.2 诊断

- 1、上电后，TukBest 西门子系列模块的红色电源指示灯 **Pwr** 灯将立即常亮；
- 2、上电后，TukBest 西门子系列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、上电后，TukBest 西门子系列模块的 RJ45 端口的绿色 **Link** 灯应常亮，**Link** 灯常亮表明模块已经建立了以太网连接。

### 注意：

当模块插在 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：模块模块在 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。

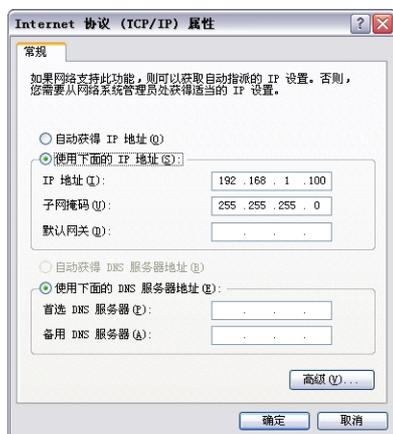
## 4. 参数设定

当需要对 TukBest 西门子系列模块的参数进行修改（比如修改 IP 地址）时，可以通过登录 Web 网页或者使用配置软件来实现。

一般情况下，只要保证模块和电脑的 IP 地址在同一网段，其它参数无需设置，就可以正常通讯了。

### 4.1 Web 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（出厂默认 IP 地址），然后按回车

键，浏览器应能显示 Web 网页，如下图所示：



3. 登录后显示的首页，如下图所示：

设备信息		设备基本信息	
设备名称:	TK 6000-MT&PT&PB	出厂日期:	2017-09-15
序列号:	18201	OEM标识:	---
固件版本:	0.1.2.3	MAC地址:	00-42-43-00-47-19

总线接口参数和状态:		S7总线接口参数		S7总线接口状态	
站地址:	0	S7总线状态:	运行	S7总线当前波特率:	锁定187500bps
S7总线最高站地址:	31	主站地址表:	0 2	从站地址表:	无
站点通讯重试次数:	3	扩展总线当前波特率:	未锁定		
地址间隔刷新系数:	10				
S7通讯协议模式:	MPI主从站				

以太网接口参数和状态:		以太网接口参数	
IP地址:	192.168.1.188	S7TCP服务器端口号:	102
掩码:	255.255.255.0	S7TCP默认目标PLC地址:	2
网关:	192.168.1.1	通讯目标PLC地址由槽号决定:	否

**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 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

<p><b>首页</b></p> <p>串行总线接口参数</p> <p><b>以太网接口参数</b></p> <p><b>通讯诊断</b></p> <p><b>功能说明</b></p> <p><b>固件升级</b></p>	<p><b>基本设置:</b></p> <p>修改以下各项参数, 点击[确认]按钮后设备将重启。</p> <table border="1"> <thead> <tr> <th></th> <th>设置</th> <th>描述</th> </tr> </thead> <tbody> <tr> <td>站地址:</td> <td>0</td> <td>范围: 0-126, 默认为0。</td> </tr> <tr> <td>S7总线最高站地址:</td> <td>31</td> <td>范围: 0-126, 默认为31。</td> </tr> <tr> <td>站点通讯重试次数:</td> <td>3</td> <td>范围: 0-8, 默认为3。</td> </tr> <tr> <td>地址间隔刷新系数:</td> <td>10</td> <td>范围: 1-100, 默认为10。</td> </tr> <tr> <td>S7通讯协议模式:</td> <td>MPI主从站</td> <td>S7总线通讯协议模式的选择, 支持PPI, MPI, Profibus DP等协议。</td> </tr> <tr> <td>S7总线波特率自动检测:</td> <td>开启</td> <td>支持对S7总线波特率的自动检测, 也可关闭后手动选择S7总线通讯波特率。</td> </tr> <tr> <td>扩展总线接口波特率自动检测:</td> <td>开启</td> <td>支持扩展总线接口的波特率自动检测, 仅当桥接型时设置有效。扩展接口可连接HMI触摸屏等设备。可关闭后手动选择扩展口波特率。</td> </tr> </tbody> </table> <p><b>高级设置:</b></p> <table border="1"> <thead> <tr> <th></th> <th>设置</th> <th>描述</th> </tr> </thead> <tbody> <tr> <td>S7总线——&gt;波特率:</td> <td>187500</td> <td>S7总线波特率选择, 可选9600、19200、187500等波特率。</td> </tr> <tr> <td>扩展总线(HMI端)——&gt;波特率:</td> <td>187500</td> <td>扩展总线的波特率选择, 可选9600、19200、187500波特率。</td> </tr> </tbody> </table> <p style="text-align: right;"><b>确认</b> 点击确认后TK 6000-MT&amp;PT&amp;PB将重启</p>		设置	描述	站地址:	0	范围: 0-126, 默认为0。	S7总线最高站地址:	31	范围: 0-126, 默认为31。	站点通讯重试次数:	3	范围: 0-8, 默认为3。	地址间隔刷新系数:	10	范围: 1-100, 默认为10。	S7通讯协议模式:	MPI主从站	S7总线通讯协议模式的选择, 支持PPI, MPI, Profibus DP等协议。	S7总线波特率自动检测:	开启	支持对S7总线波特率的自动检测, 也可关闭后手动选择S7总线通讯波特率。	扩展总线接口波特率自动检测:	开启	支持扩展总线接口的波特率自动检测, 仅当桥接型时设置有效。扩展接口可连接HMI触摸屏等设备。可关闭后手动选择扩展口波特率。		设置	描述	S7总线——>波特率:	187500	S7总线波特率选择, 可选9600、19200、187500等波特率。	扩展总线(HMI端)——>波特率:	187500	扩展总线的波特率选择, 可选9600、19200、187500波特率。
	设置	描述																																
站地址:	0	范围: 0-126, 默认为0。																																
S7总线最高站地址:	31	范围: 0-126, 默认为31。																																
站点通讯重试次数:	3	范围: 0-8, 默认为3。																																
地址间隔刷新系数:	10	范围: 1-100, 默认为10。																																
S7通讯协议模式:	MPI主从站	S7总线通讯协议模式的选择, 支持PPI, MPI, Profibus DP等协议。																																
S7总线波特率自动检测:	开启	支持对S7总线波特率的自动检测, 也可关闭后手动选择S7总线通讯波特率。																																
扩展总线接口波特率自动检测:	开启	支持扩展总线接口的波特率自动检测, 仅当桥接型时设置有效。扩展接口可连接HMI触摸屏等设备。可关闭后手动选择扩展口波特率。																																
	设置	描述																																
S7总线——>波特率:	187500	S7总线波特率选择, 可选9600、19200、187500等波特率。																																
扩展总线(HMI端)——>波特率:	187500	扩展总线的波特率选择, 可选9600、19200、187500波特率。																																

**站地址:** 模块自身站地址, 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。

**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; 模块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, 进行重试的次数, 默认为3。

**地址间隔刷新系数:** 这个系数影响查找其他设备的速度, 默认为10。

**S7总线协议模式:** 协议模式:

当插在S7200的PPI通讯口上时: 选择PPI模式;

当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;

当插在S7300的MPI通讯口上时: 选择MPI主从站模式;

当插在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(HMI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, 模块将复位并重新启动。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

以太网接口参数

通讯诊断

功能说明

固件升级

设置	描述
IP地址: 192 . 168 . 1 . 188	本地IP地址, 默认为192.168.1.178
掩码: 255 . 255 . 255 . 0	掩码地址, 默认为255.255.255.0。
网关: 192 . 168 . 1 . 1	网关地址, 默认为192.168.1.1。
S7TCP默认目标PLC地址: 2	指定S7TCP通讯的PLC地址, 如WINCC的TCP/IP通道, 默认为2。
通讯目标PLC地址由槽号决定: 关闭	开启后, S7TCP的目标PLC地址, 由槽号决定, 适用于S7300, S7通讯。

高级设置:

设置	描述
S7TCP服务器端口号: 102	S7TCP服务通讯端口号, 默认102。
ModbusTCP端口号: 502	ModbusTCP通讯端口号, 默认为502。

密码:	登入密码修改, 登入帐号为: admin。
确认密码:	登入密码修改确认, 登入帐号为: admin。

**确认** 点击确认后TK 6000-MT&PT&PB将重启

设置模块的 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。

当更改以上参数后请点击[确认]按钮，模块将复位并重新启动。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

首页

串行总线接口参数

以太网接口参数

通讯诊断

功能说明

#### 串行总线通讯

S7总线——>通讯请求总数:	9558
正确响应次数:	9558
错误响应次数:	0
扩展总线——>通讯请求总数:	0
正确响应次数:	0
错误响应次数:	0

#### 以太网通讯

以太网(TCP/IP)——>通讯请求总数:	9558
正确响应次数:	9558
错误响应次数:	0
TCP连接数:	0

#### 系统信息

运行时间:	0天 00:24
上次内部故障:	无故障

**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 发送到模块的通讯请求数目;

**正确响应次数:** 模块正确响应这些请求的数目;

**错误响应次数:** 模块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模块的通讯请求数目;

**正确响应次数:** 模块正确响应这些请求的数目;

**错误响应次数:** 模块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:** 上电后的运行时间;

**上次内部故障:** 模块的系统故障, 正常情况下不应该产生故障;

## 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。

【NetS7PD1801\_setup\_x86】为 32 位编程驱动；

【NetS7PD1802\_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：



### 5.2 MicroWIN 编程调试

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

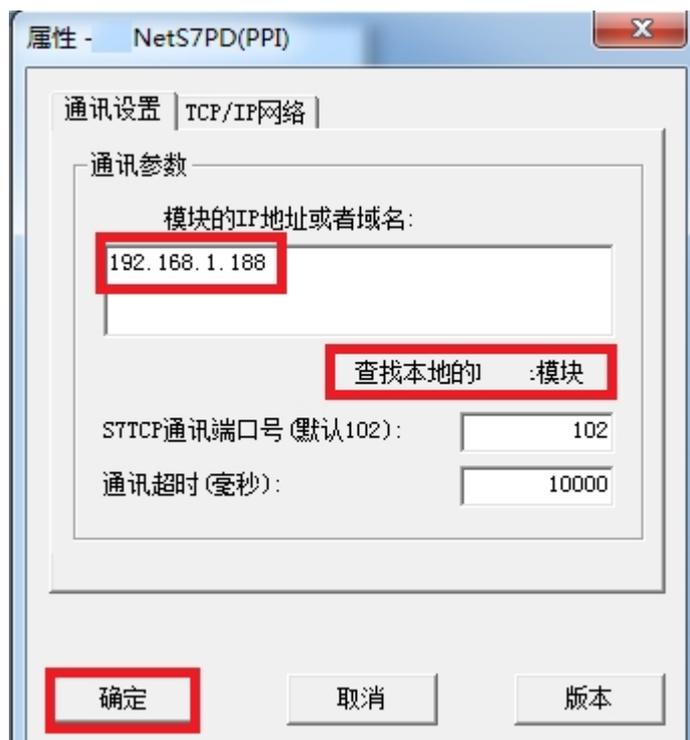
## 5.2.1 通过 TKNNet 编程驱动

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

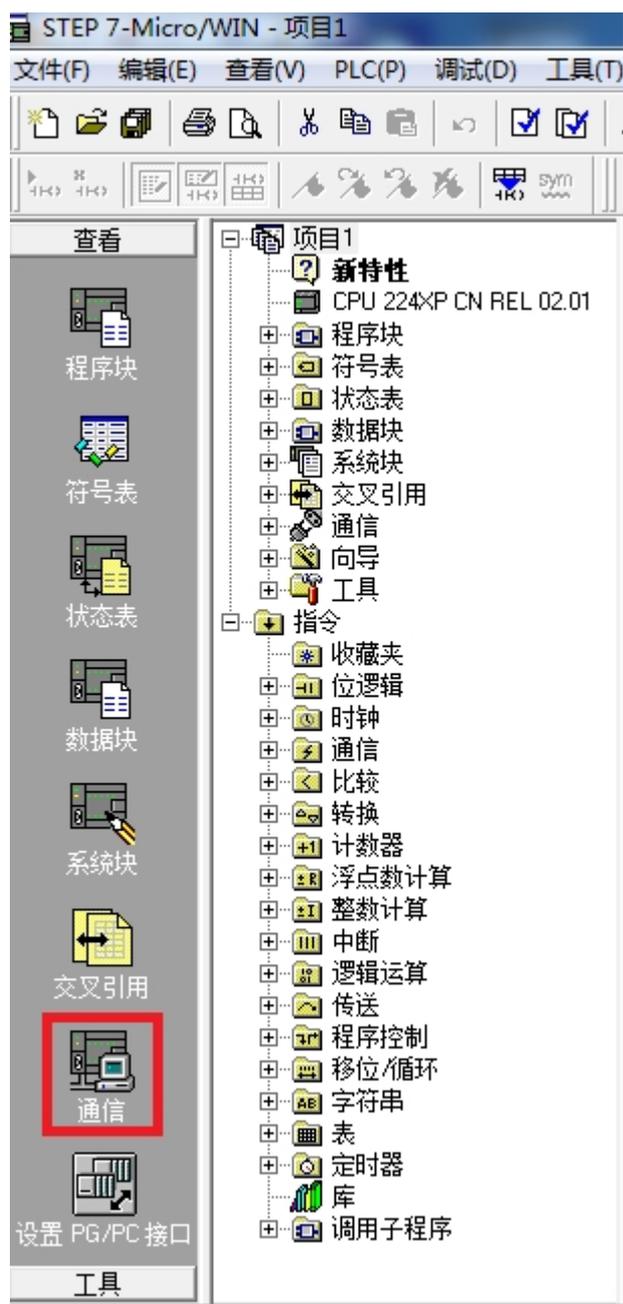


2.在【为使用的接口分配参数】中选择 NetS7PD.PPI.1，确保【应用程序访问点】为 Micro/WIN →NetS7PD.PPI.1,点击【属性】按钮；

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



4. 点击左侧导航栏的【通信】图标；

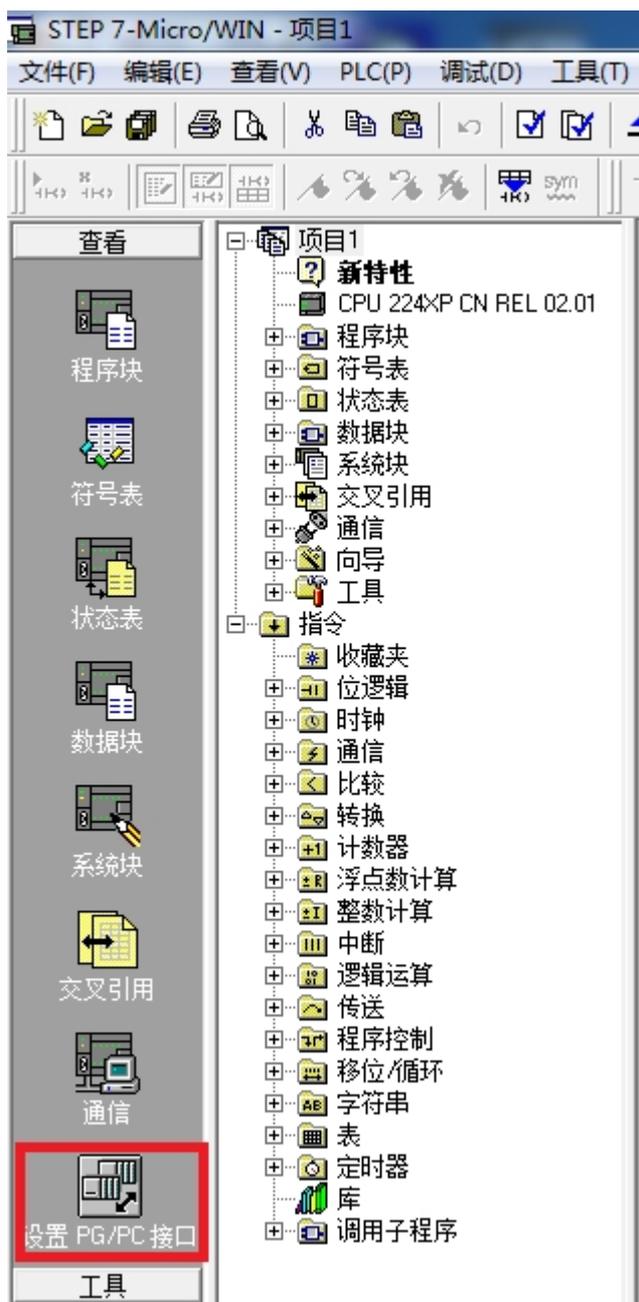


5. 鼠标双击【双击刷新】图标，选中刷新到的 PLC，点击【确认】按钮。

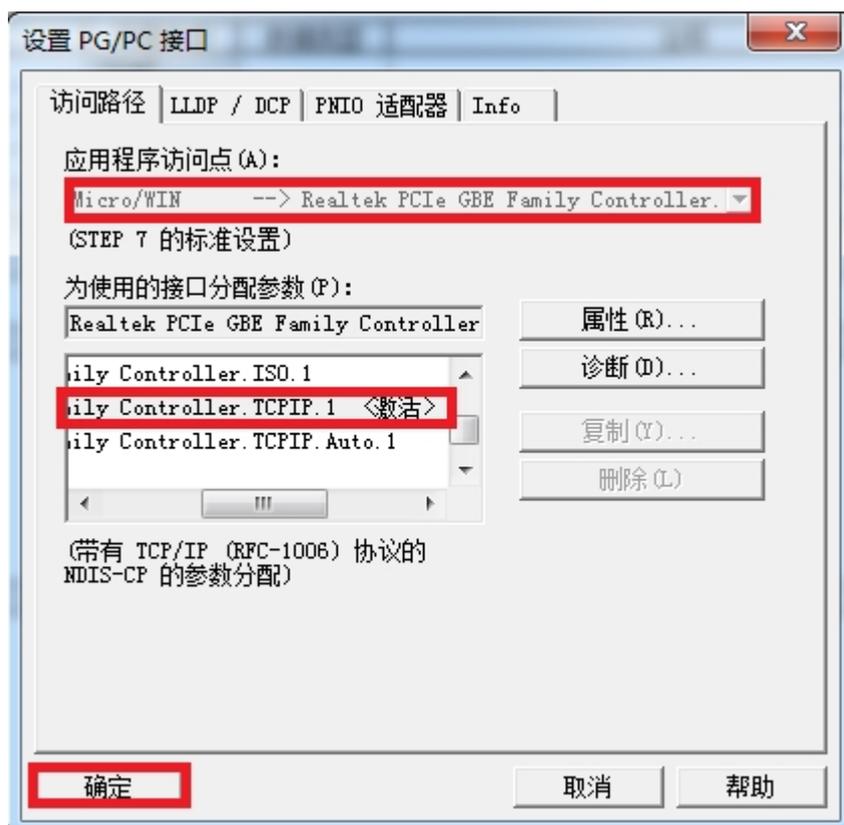


## 5.2.2 通过西门子以太网驱动

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

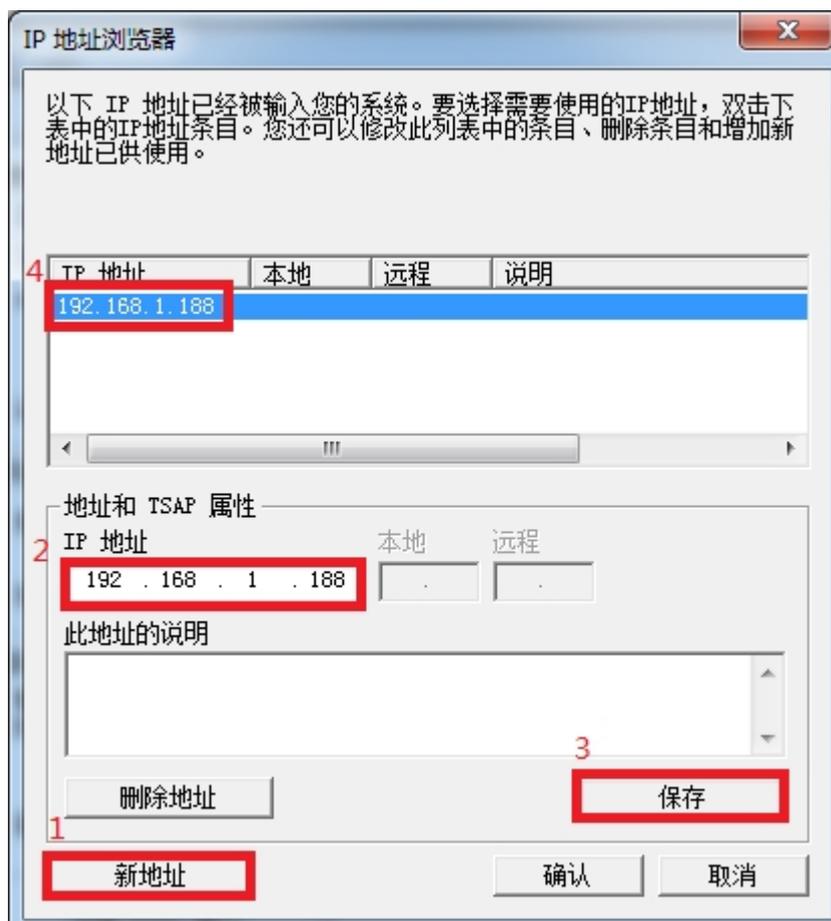
3. 点击左侧导航栏的【通信】;



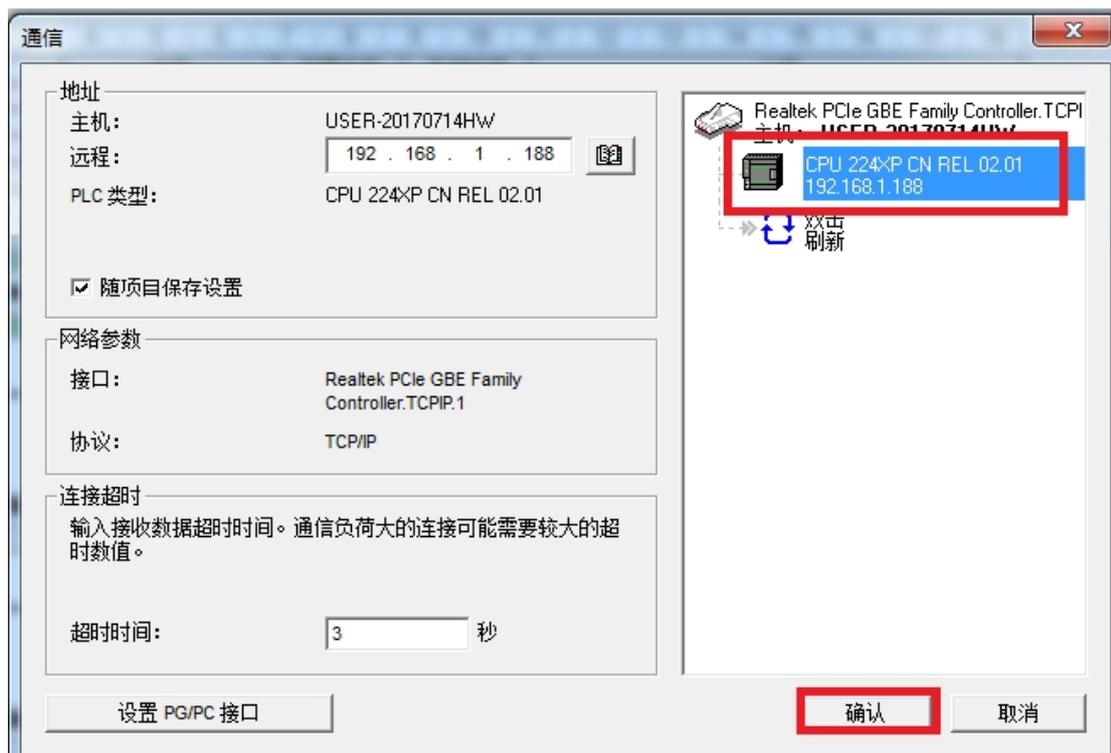
4. 点击如下图标，打开 IP 地址浏览器：



5. 点击【新地址】按钮，在【IP 地址】中输入模块的 IP 地址，点击【保存】按钮，双击保存后的 IP 地址；



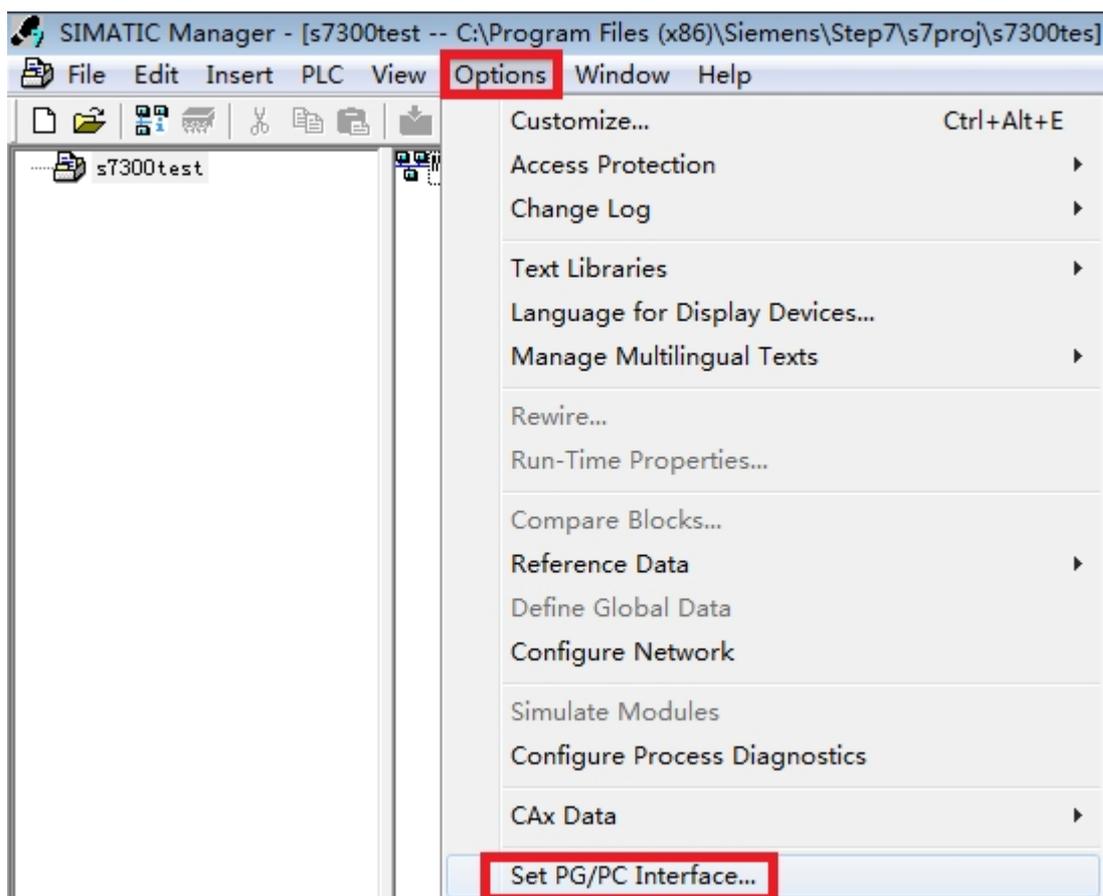
6. 鼠标双击【双击刷新】图标，选中刷新到的 PLC，点击【确认】按钮。



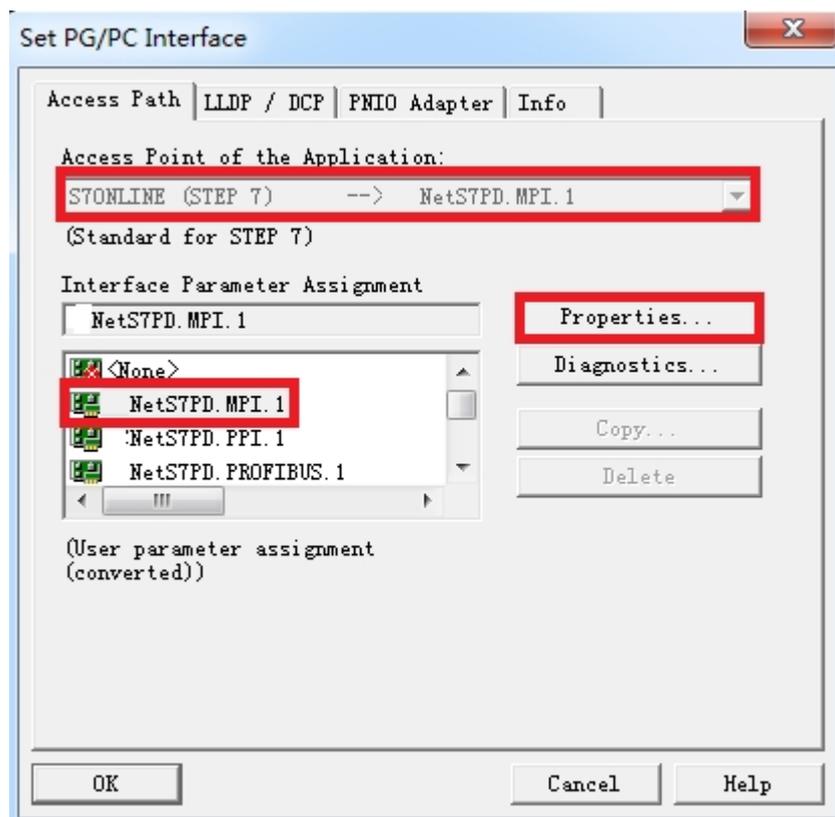
注意：通过西门子的以太网驱动时请设置【S7TCP 默认目标 PLC 地址】为当前 PLC 通讯口的站地址。

## 5.3 Step7 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】：



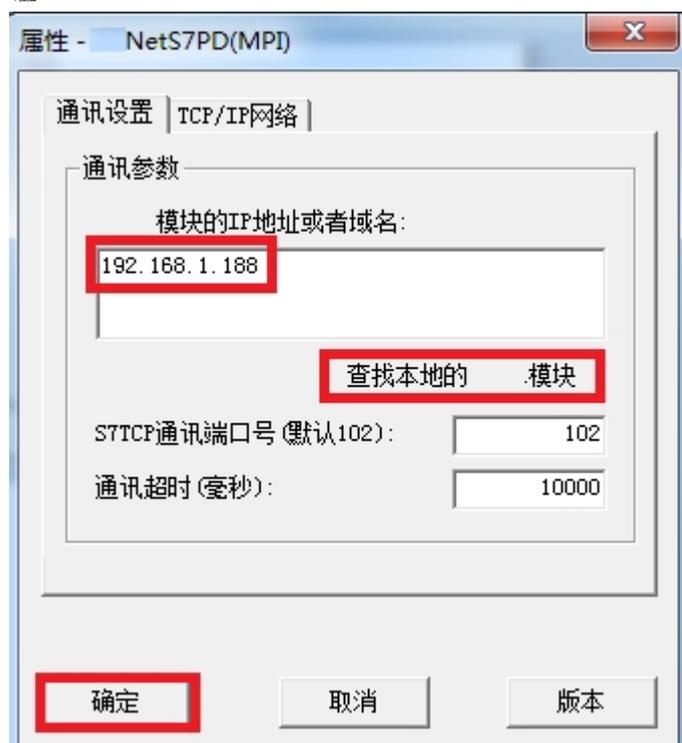
2. 【Interface Parameter Assignment】设置为 NetS7PD.MPI.1，确保【Access Point of the Application】为 S7ONLINE（STEP7）→ NetS7PD.MPI.1，点击【Properties】按钮；



注意：如果模块插在 PLC 的 MPI 口，【Interface Parameter Assignment】设置为 NetS7PD.MPI.1；如果模块插在 PLC 的 PROFIBUS 口，【Interface Parameter Assignment】设置为 NetS7PD.PROFIBUS.1。

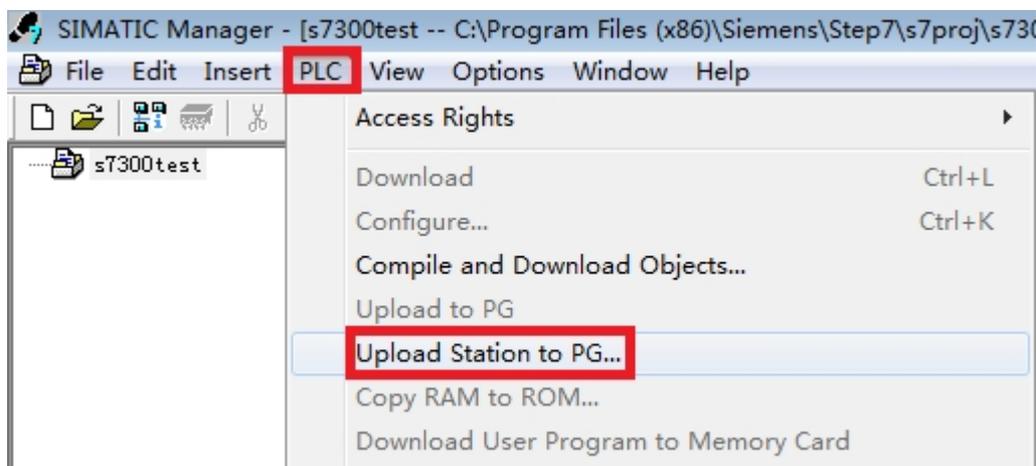
3.如果知道模块的 IP 地址，在【模块的 IP 地址或域名】中直接输入模块的 IP 地址，点击【确定】按钮；

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

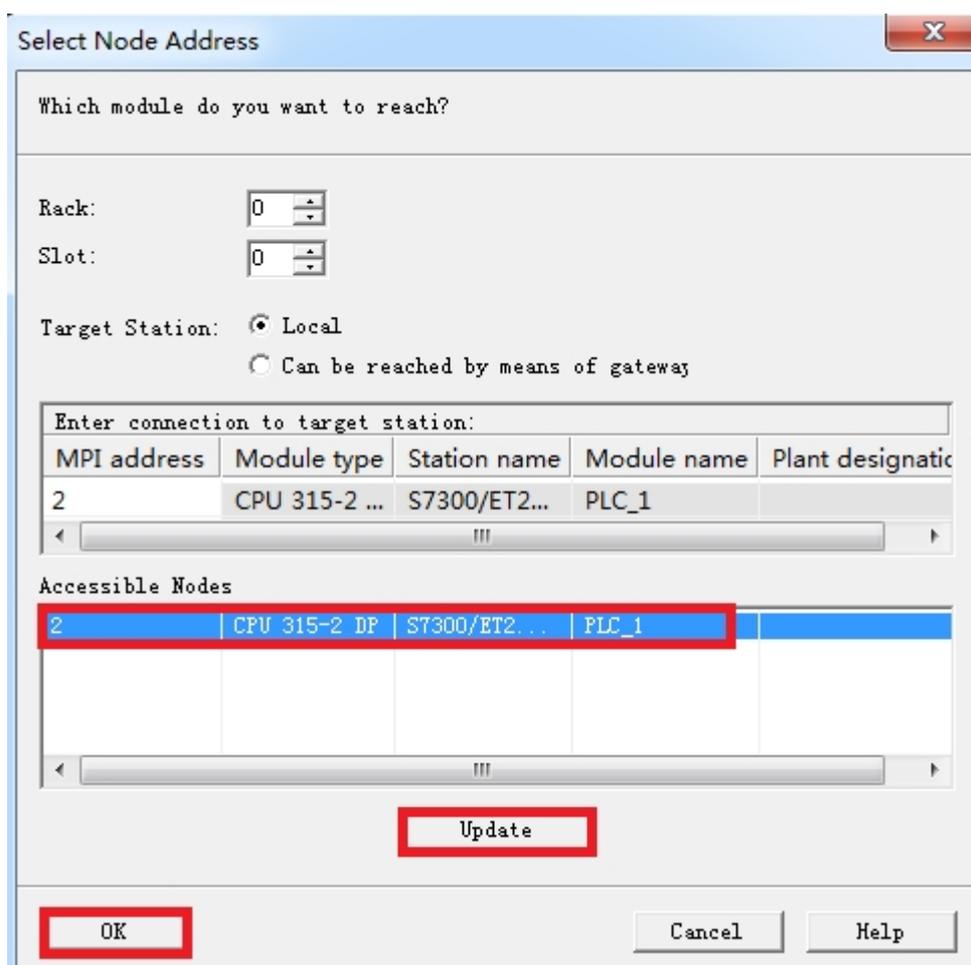


**上传程序：**

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

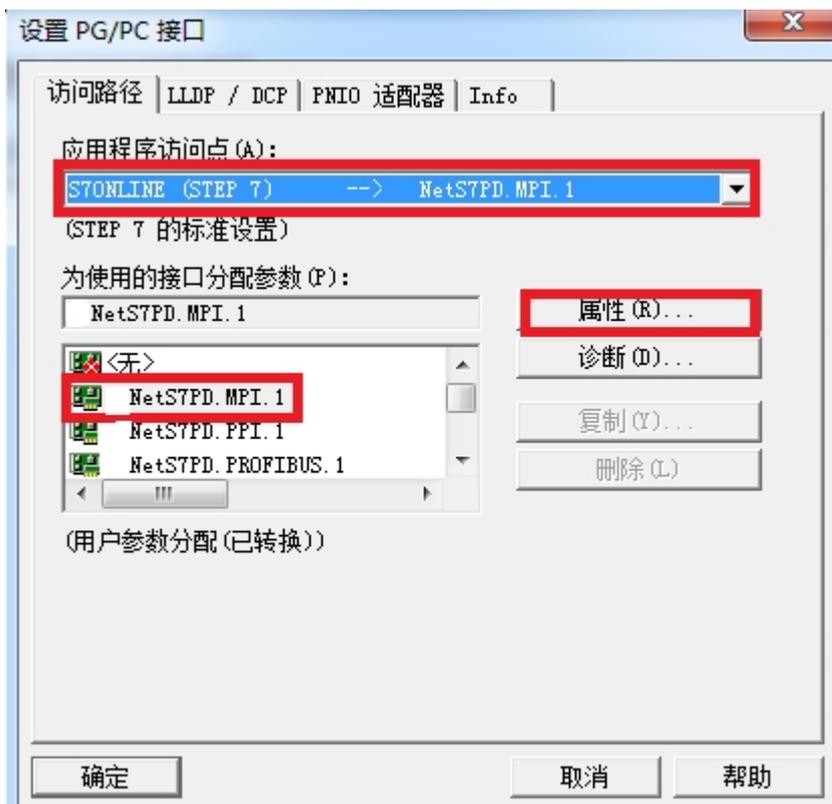
首先应设置好 PG/PC 接口参数：

1. 打开控制面板中的【设置 PG/PC 接口】图标：

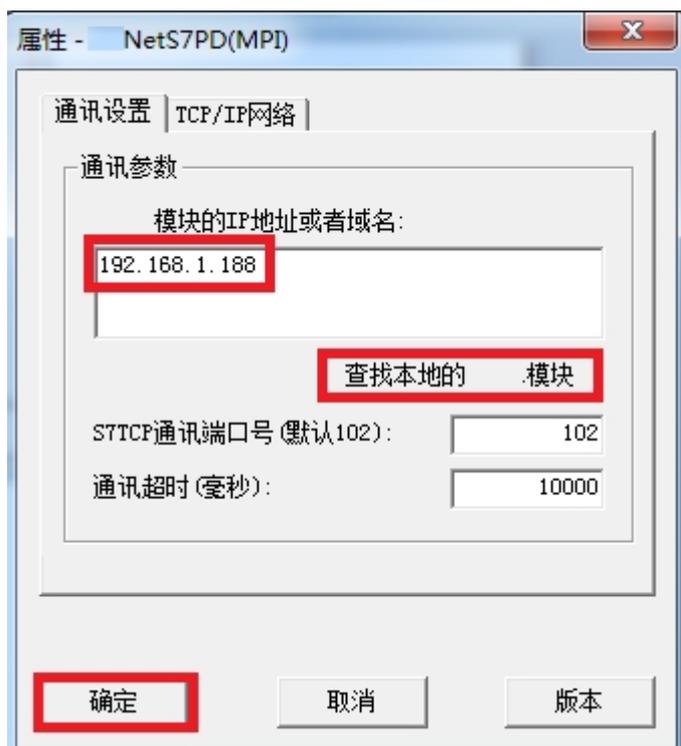


### 设置 PG/PC 接口 (32 位)

2. 【为使用的接口分配参数】设置为 NetS7PD.MPI.1, 【应用程序访问点】设置为 S7ONLINE (STEP7) → NetS7PD.MPI.1, 点击【属性】按钮；

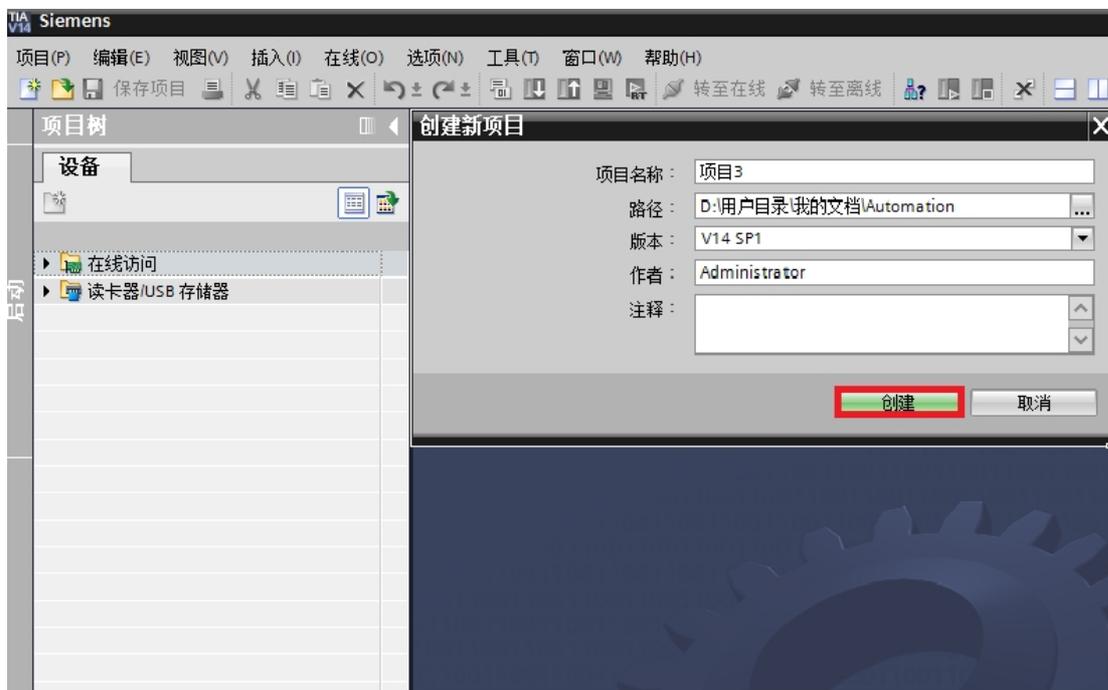


3. 如果知道模块的 IP 地址，在【模块的 IP 地址或域名】中直接输入模块的 IP 地址，点击【确定】按钮；如果不知道模块的 IP 地址，可以点击【查找本地的模块】，选择要连接的模块，点击【选择设备】按钮。



注意：如果插在 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模块的 IP 地址；如果插在 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模块的 IP 地址；

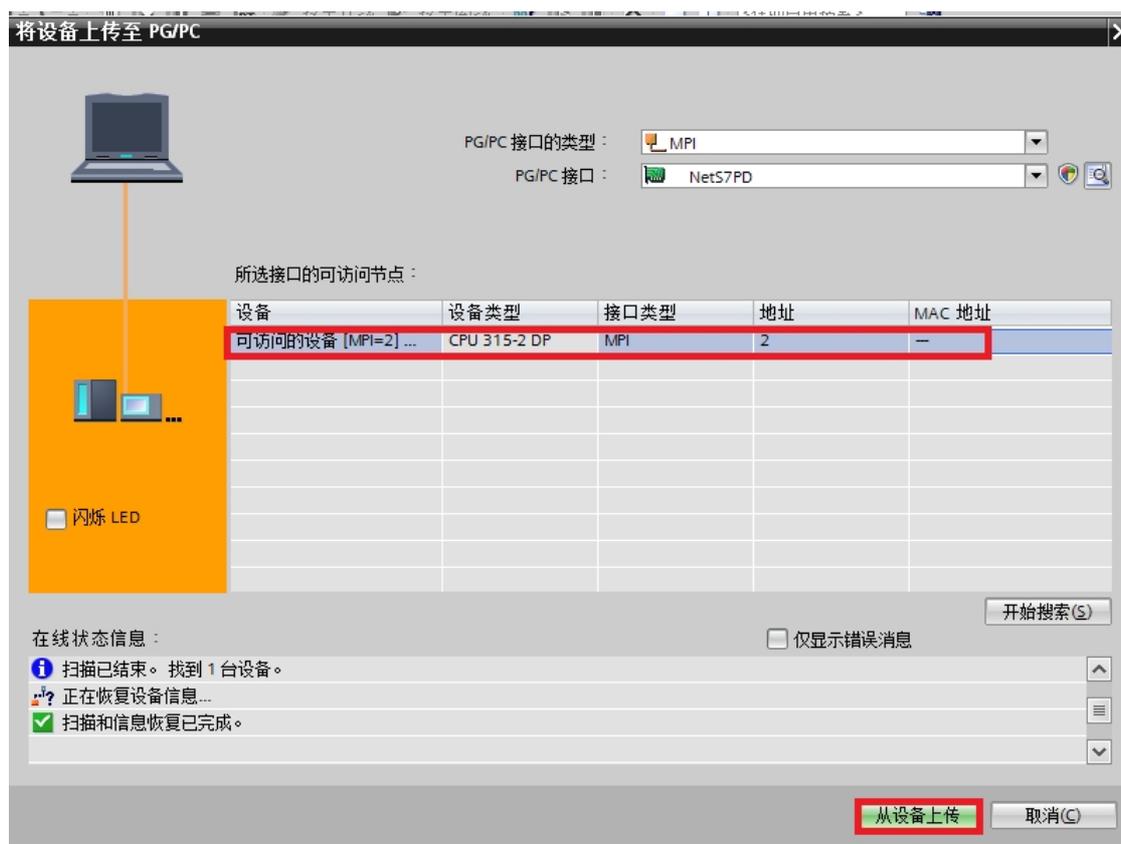
1.以【项目视图】打开博途软件，并新建项目；



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）】；



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. TK 6000-MT&PT&PB 模块 SCADA 以太网通讯

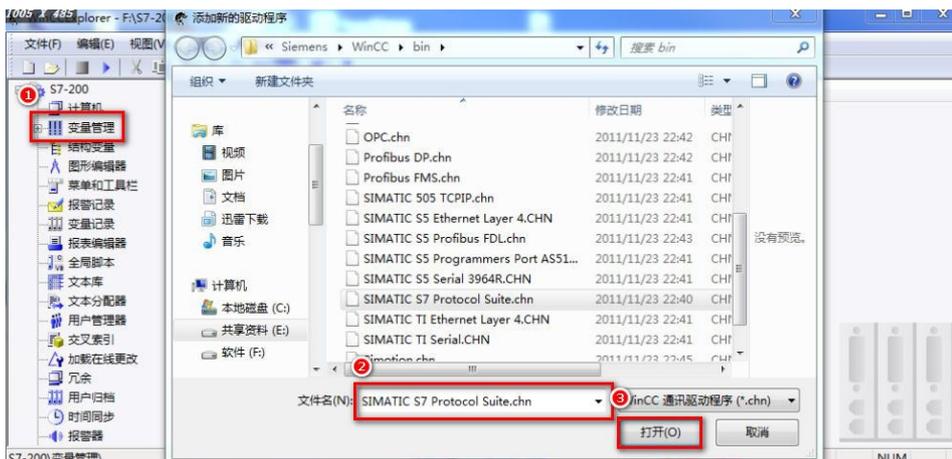
### 6.1 WINCC 通讯

#### 6.1.1 TK 6000-MT&PT&PB 模块连接 S7200

西门子 S7-200 采用模块连接 WINCC，可以采用：WINCC 的 TCP 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】处填入模块的 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。

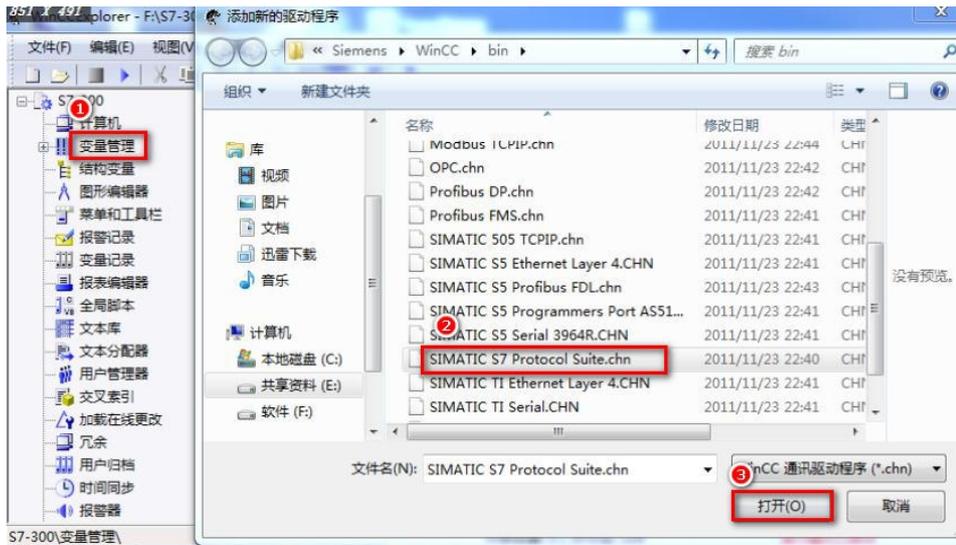


## 6.1.2TK 6000-MT 模块连接 S7300

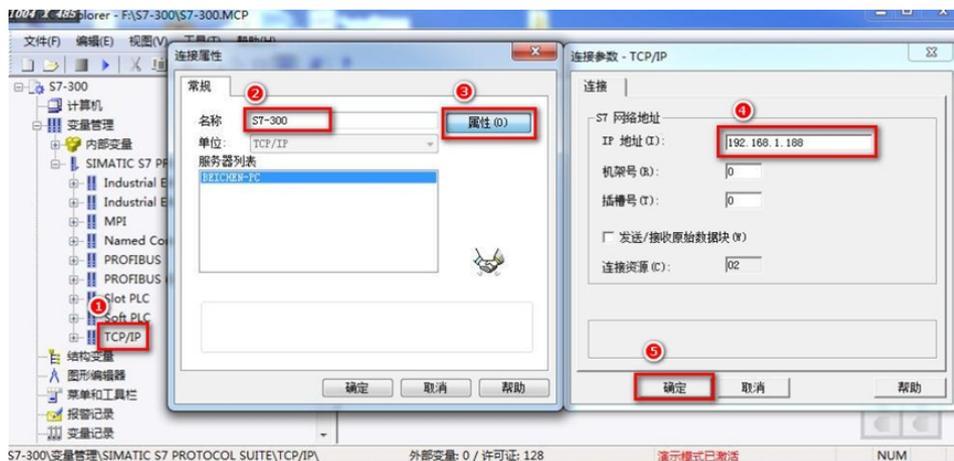
西门子S7-300/400 采用模块 连接WINCC，可以采用：WINCC的TCP驱动。

### 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】设置为模块的 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。



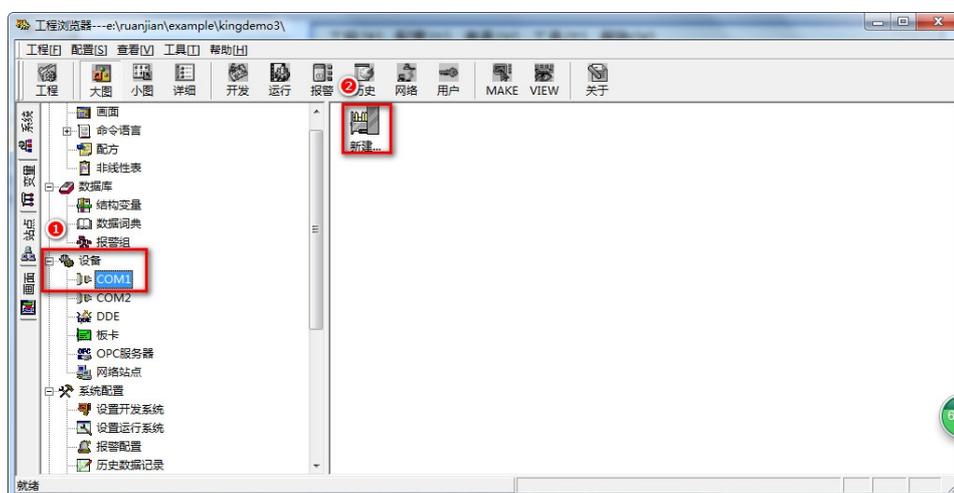
## 6.2TK 6000-MT&PT&PB 模块组态王通讯

### 6.2.1 连接 S7200

西门子 S7-200 通过模块连接组态王，可以采用：西门子 S7TCP 驱动。

#### 6.2.1.1 采用 S7TCP 驱动

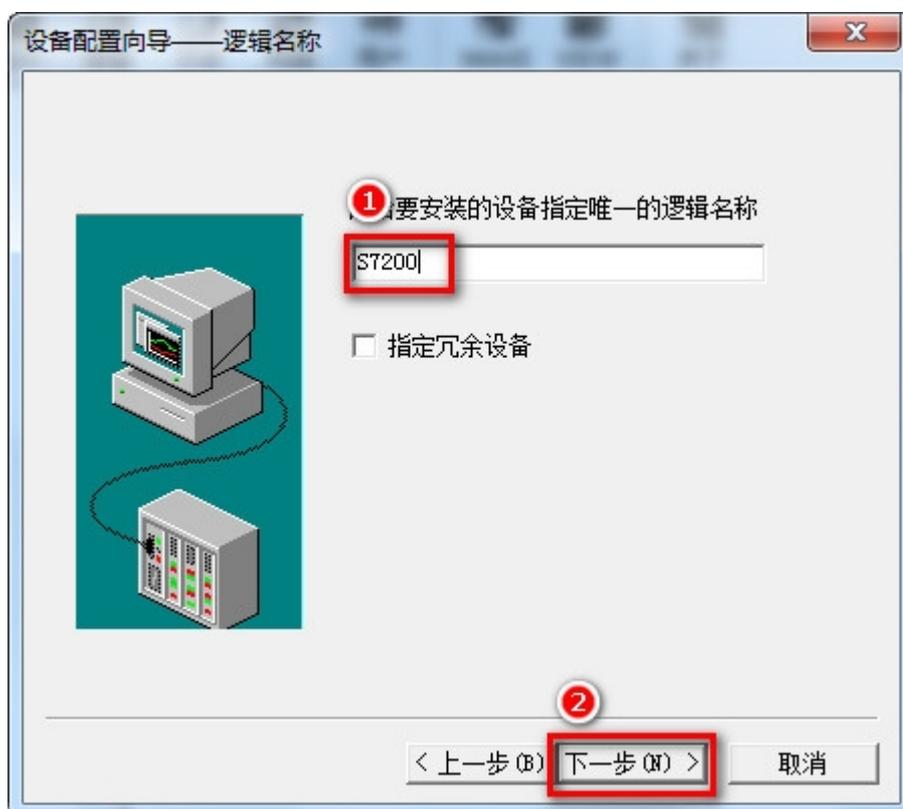
1、打开组态王软件，鼠标单击  打开组态王工程浏览器——设备 (COM1)，双击右侧【新建】：



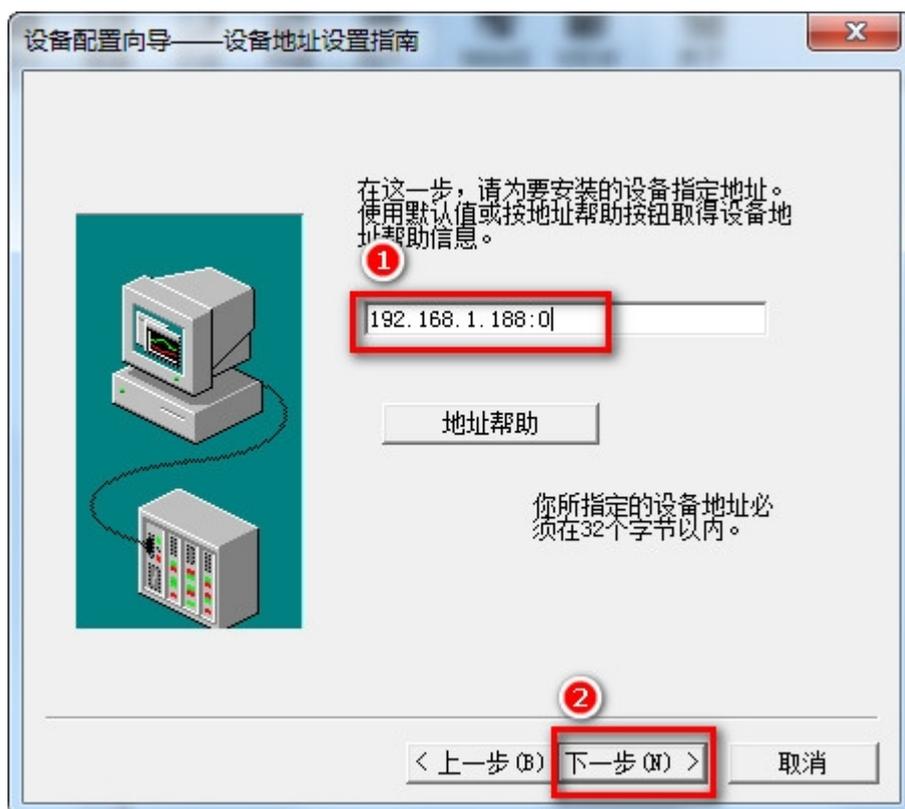
2、打开 PLC 分组，然后打开西门子分组，选择 S7-200 系列(TCP)下的 TCP 驱动



3、填入设备名称，点击【下一步】；



1、填入模块的 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。

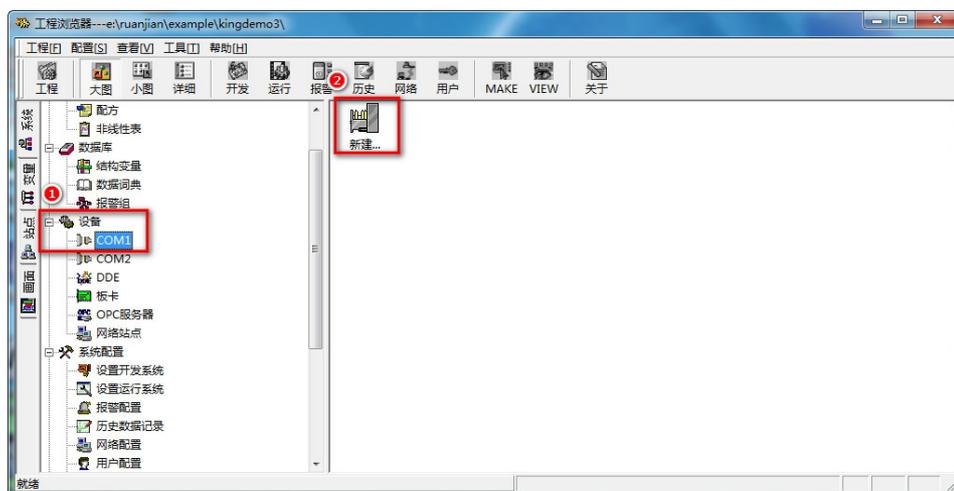


## 6.2.2 TK 6000-MT 模块连接 S7300

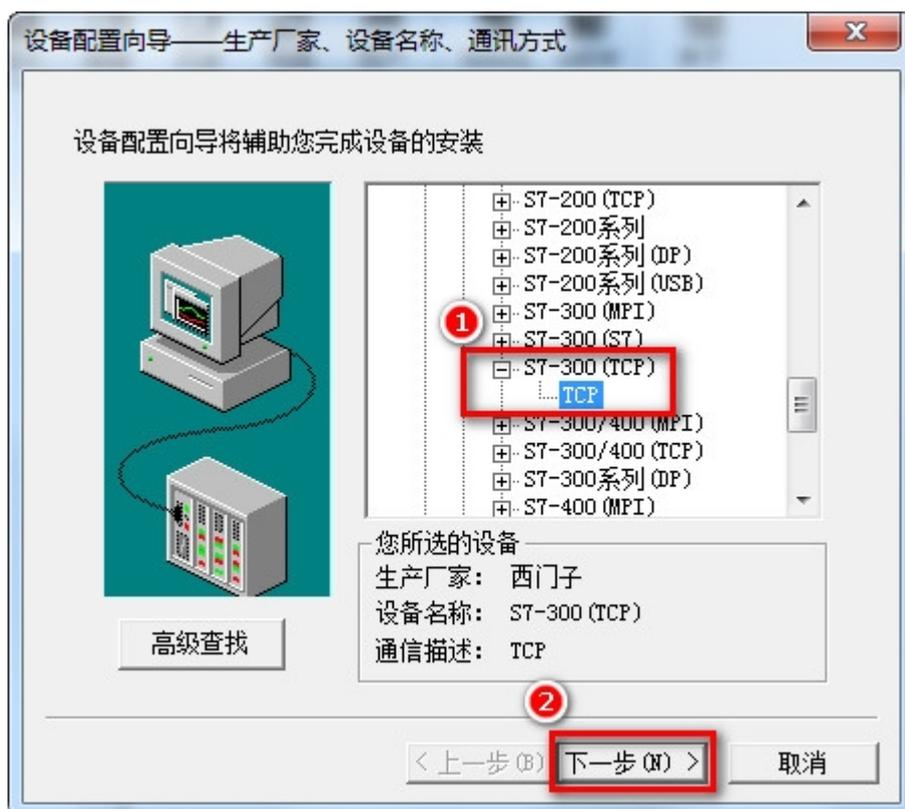
西门子S7-300/400 采用模块连接组态王，可以采用：S7TCP驱动。

### 6.2.2.1 采用 S7TCP 驱动

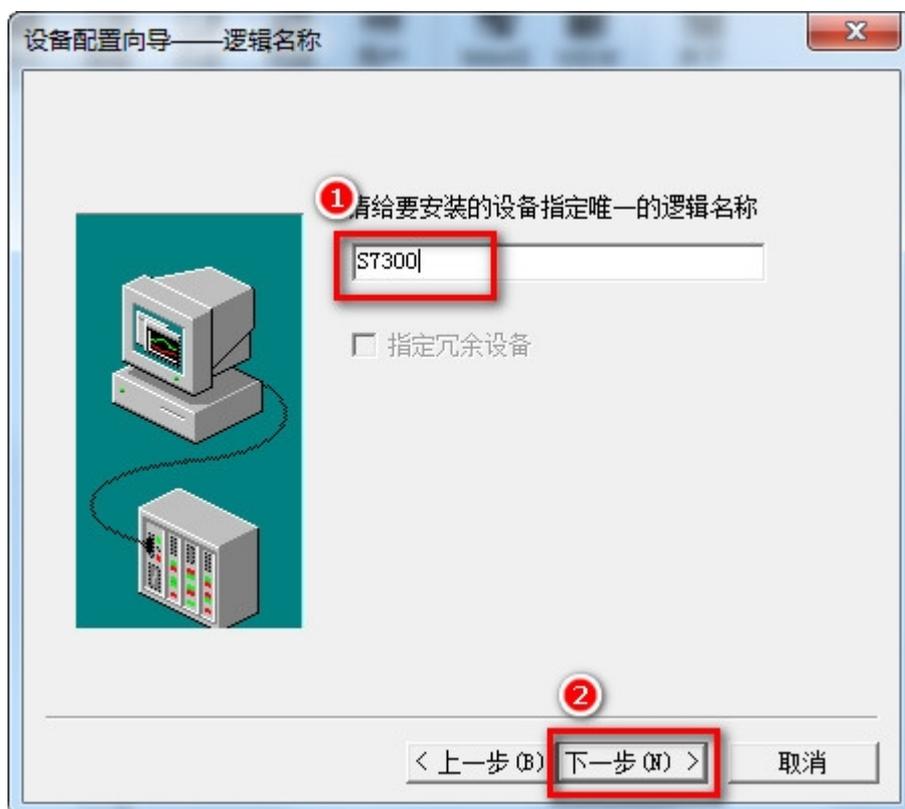
1、打开组态王工程浏览器——设备（COM1），双击右侧“新建”



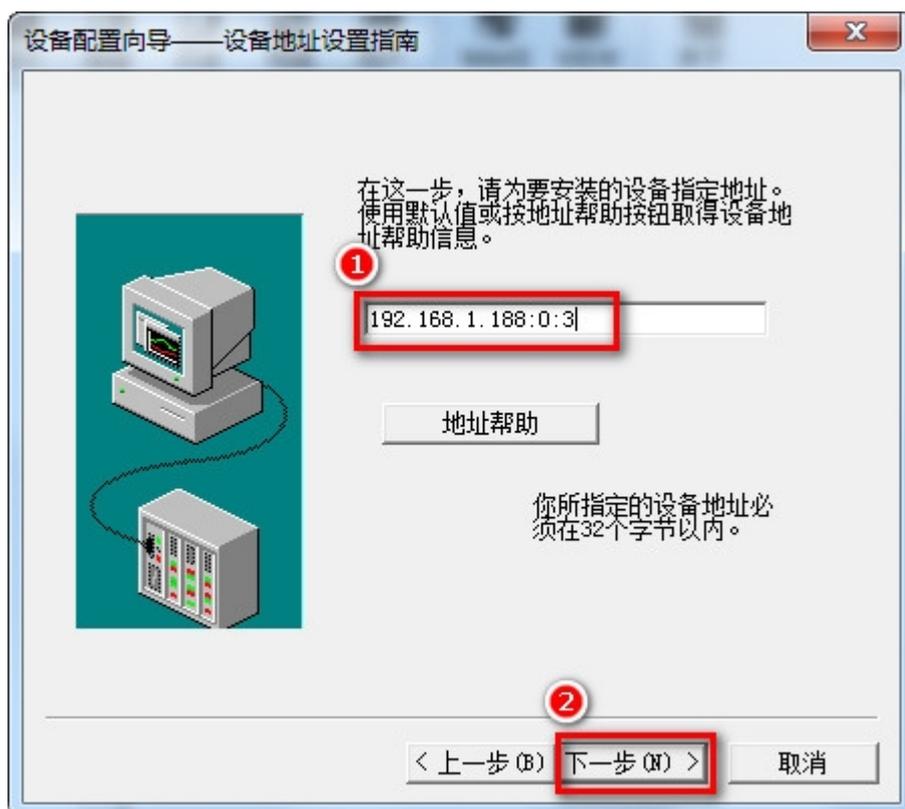
2、选择西门子 S7-300 系列 TCP 驱动，点击【下一步】；



3、填入设备名称；



4、填入模块的 IP 地址；CPU 机架号；CPU 槽号（默认为 3）；



## 6、完成参数设置



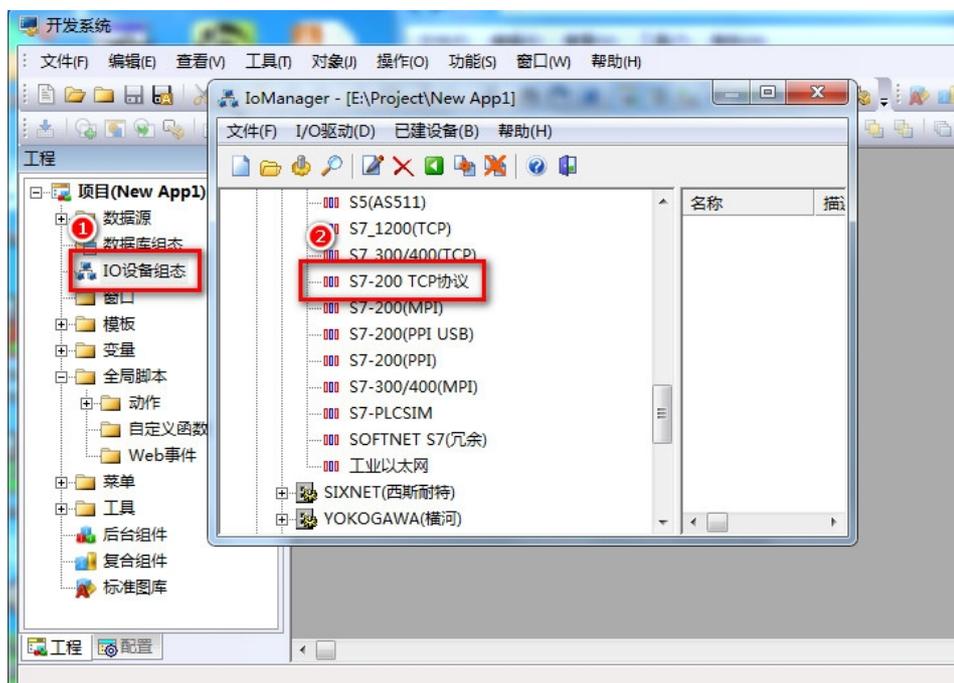
## 6.3TK 6000-MT&PT&PB 模块力控通讯

### 6.3.1TK 6000-MT&PT&PB 模块连接 S7200

西门子 S7-200 通过模块连接 ForceControl，可以采用：西门子 S7TCP 驱动。

#### 6.3.1.1 采用 S7TCP 驱动

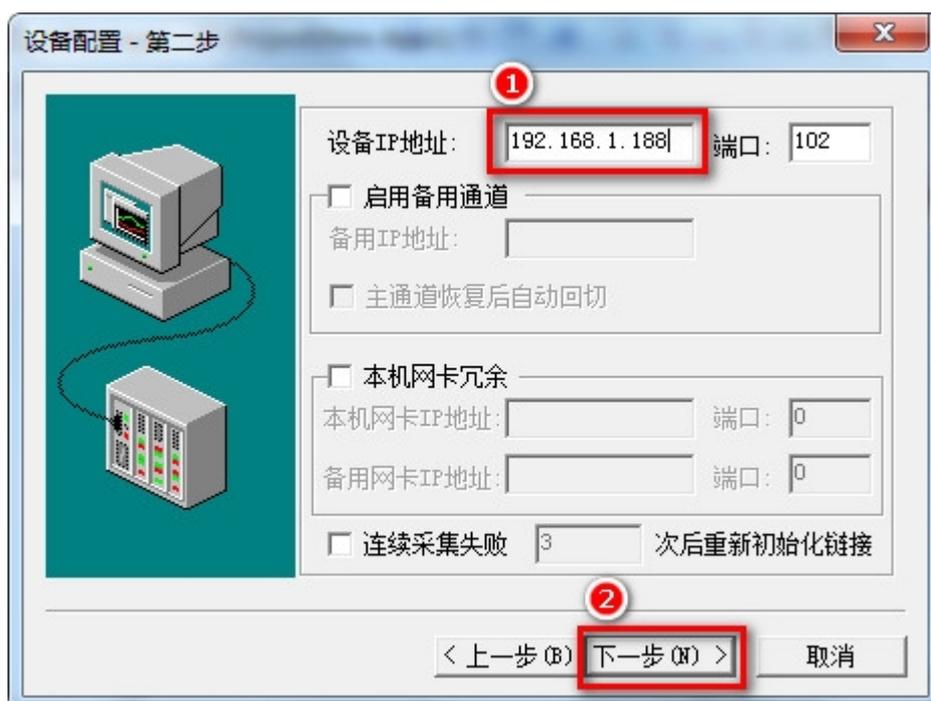
1、打开力控开发系统——IO 设备组态，选择【PLC-SIEMENS（西门子）—S7-200 TCP 协议】；



2、填入设备名称，点击【下一步】；



3、填入模块的 IP 地址，端口（默认为 102），完成设置。

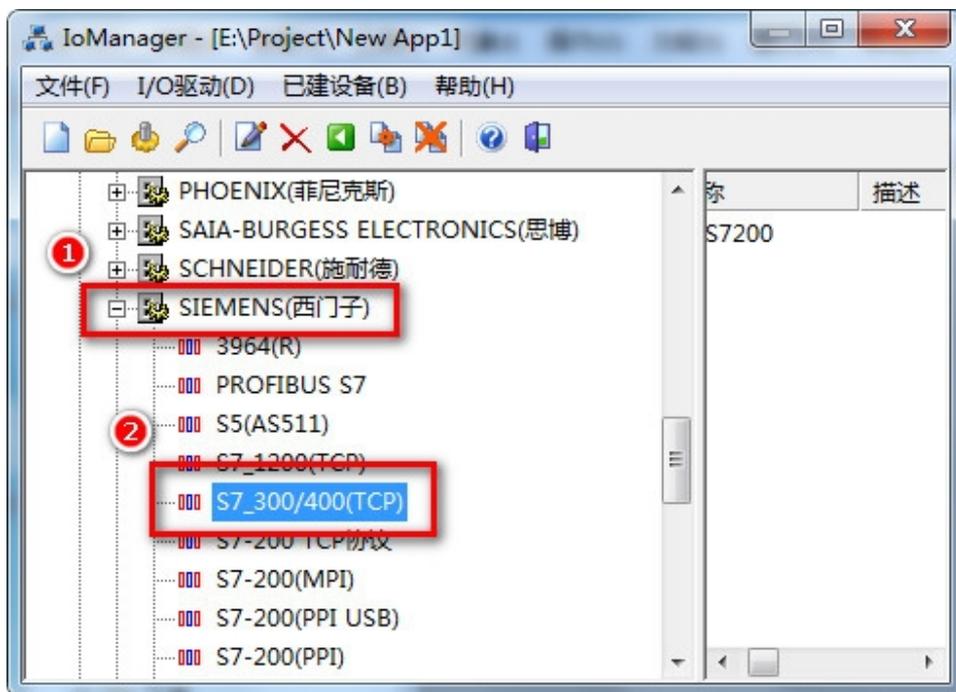


### 6.3.2 TK 6000-MT 模块连接 S7300

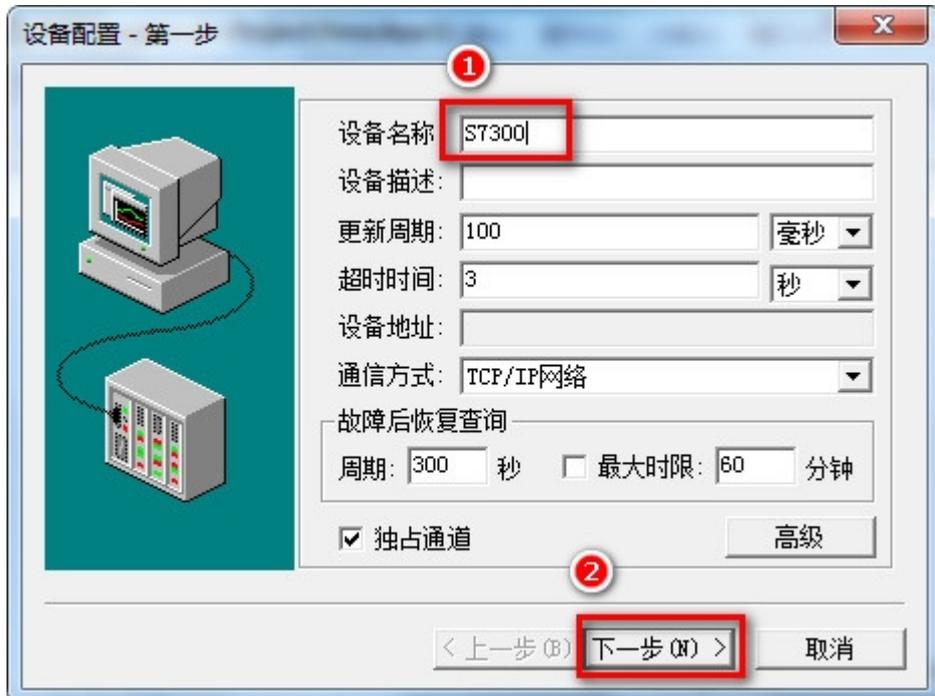
西门子 S7-300/400 采用 TK 6000-MT 模块连接 ForceControl，可以采用：S7TCP 驱动。

### 6.3.2.1 采用 S7TCP 驱动

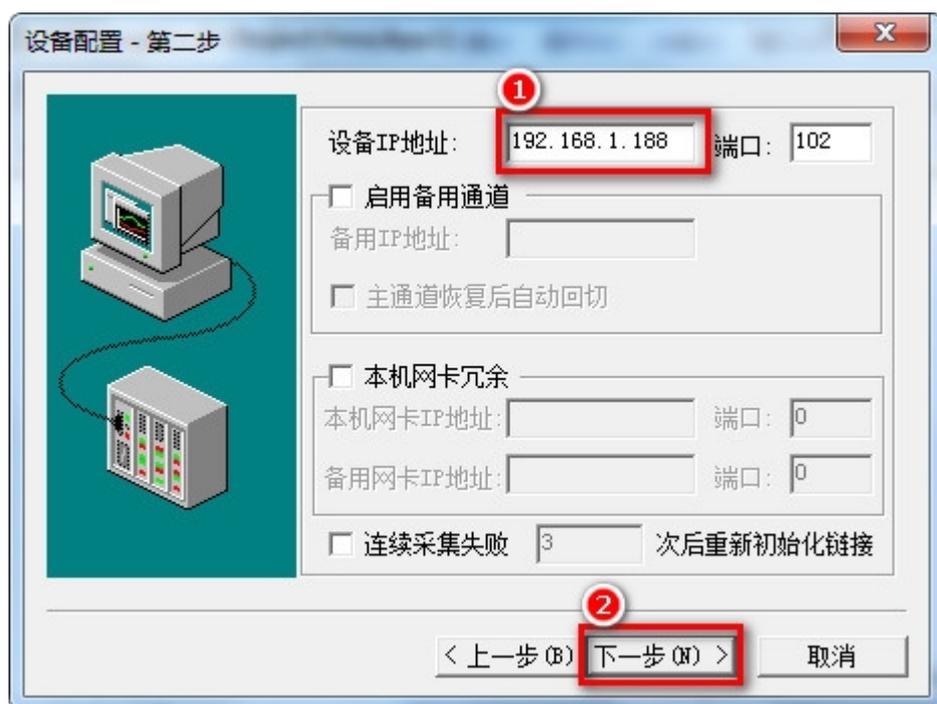
1、打开力控开发系统——IO 设备组态，选择【PLC-SIEMENS（西门子）—S7 系列 TCP 协议】；



2、填入设备名称，点击【下一步】；



3、填入模块的 IP 地址，端口（默认为 102），完成设置。



## 6.4 TK 6000-MT&PT&PB 模块 MCGS 通讯

### 6.4.1 连接 S7200

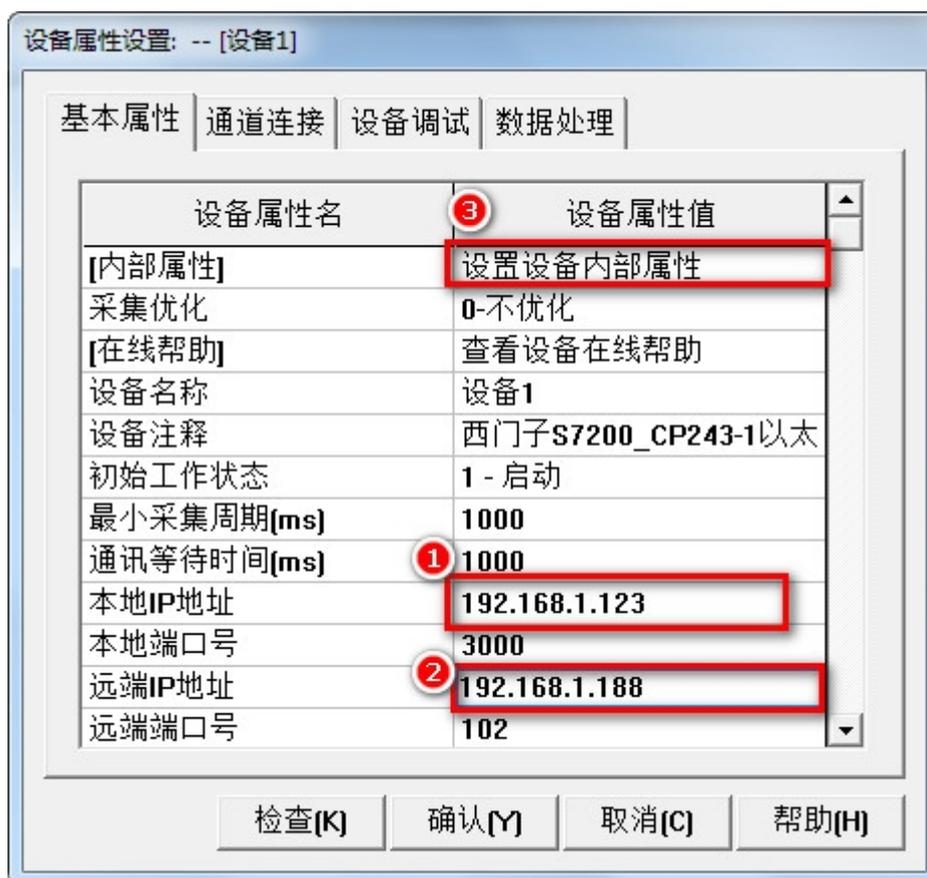
西门子 S7-200 通过模块连接 MCGS，可以采用：西门子 S7TCP 驱动。

#### 6.4.1.1 采用 S7TCP 驱动

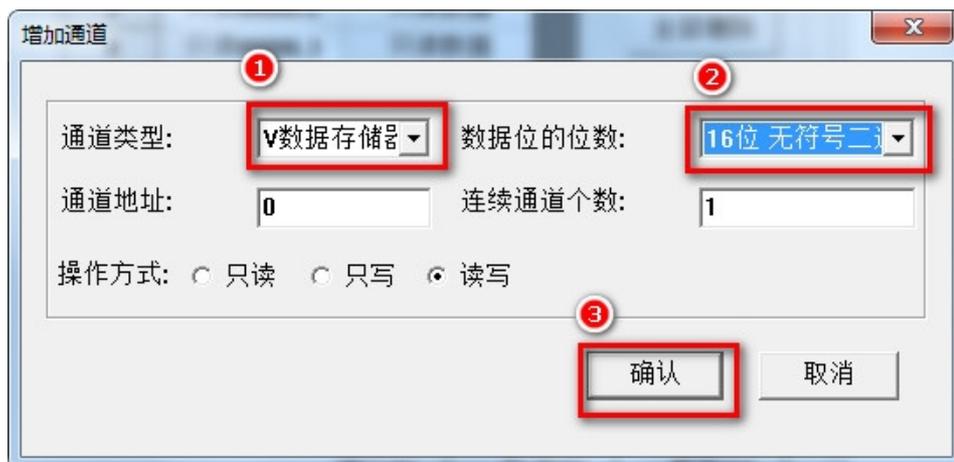
1、打开昆仑通态 MCGS 组态环境——设备窗口，选择【PLC-西门子-S7CP243\_1TCP】；



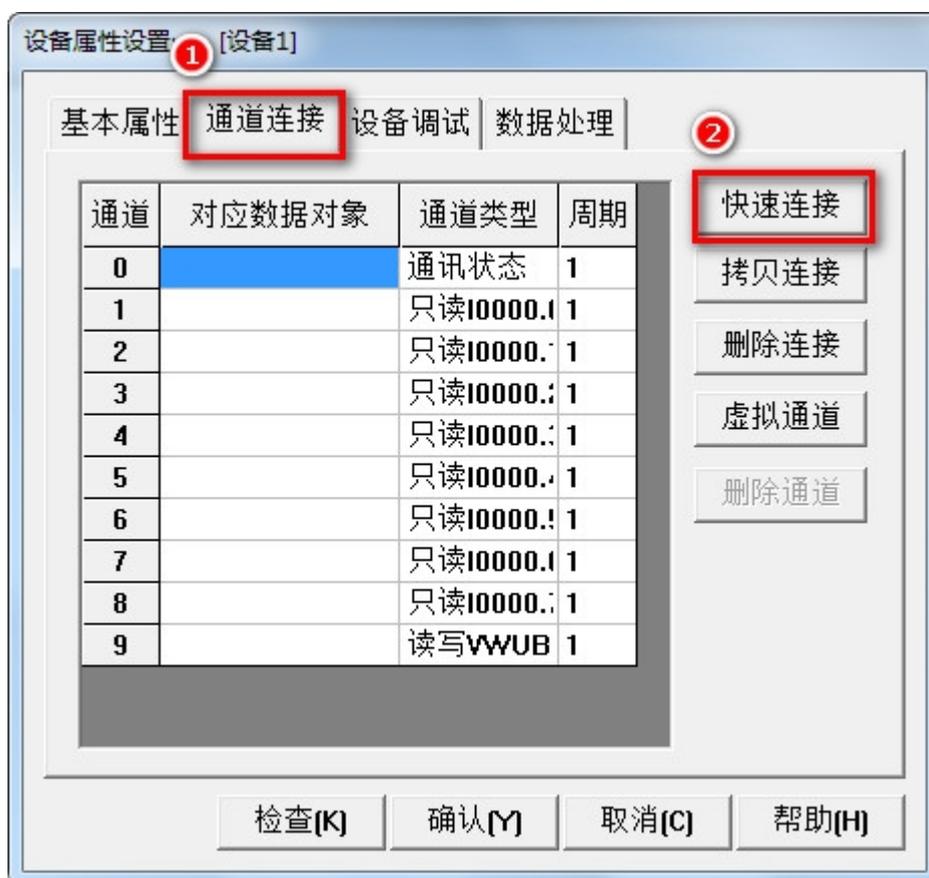
2、在设备属性设置中，将计算机的 IP 地址填入【本地 IP 地址】，模块的 IP 地址填入【远端 IP 地址】，【远端口号】填入 102；



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】:



2、再点击【设备调试】，进行变量的监视:

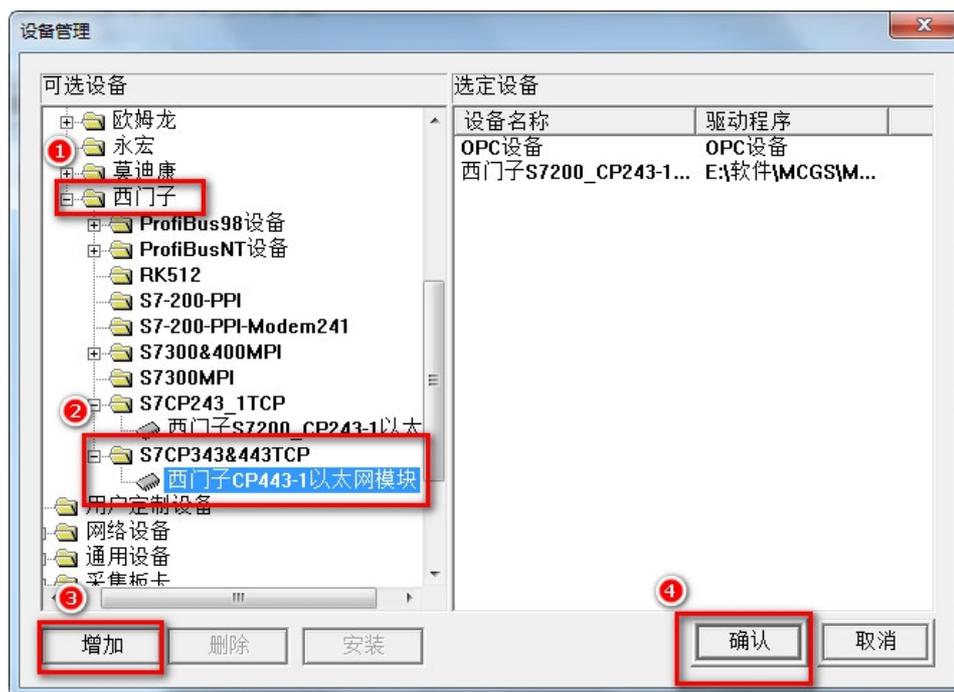


## 6.4.2 TK 6000-MT 模块连接 S7300

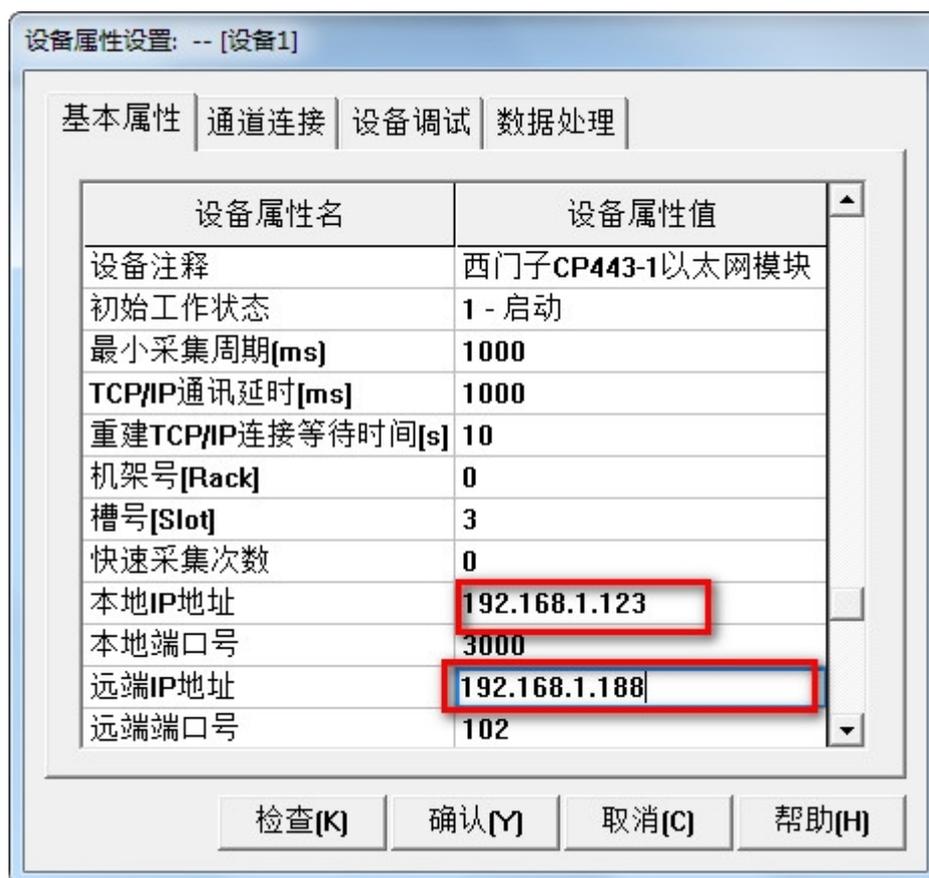
西门子 S7-300/400 采用模块连接 MCGS，可以采用：S7TCP 驱动。

### 6.4.2.1 采用 S7TCP 驱动

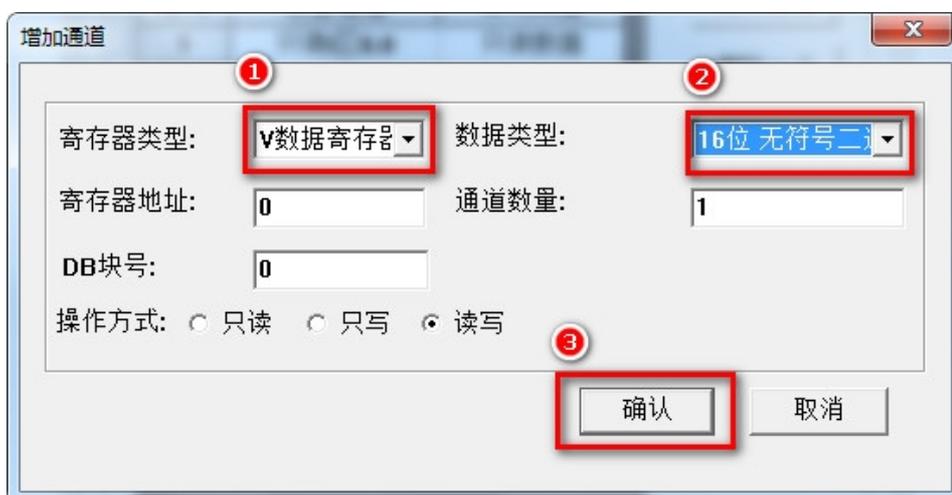
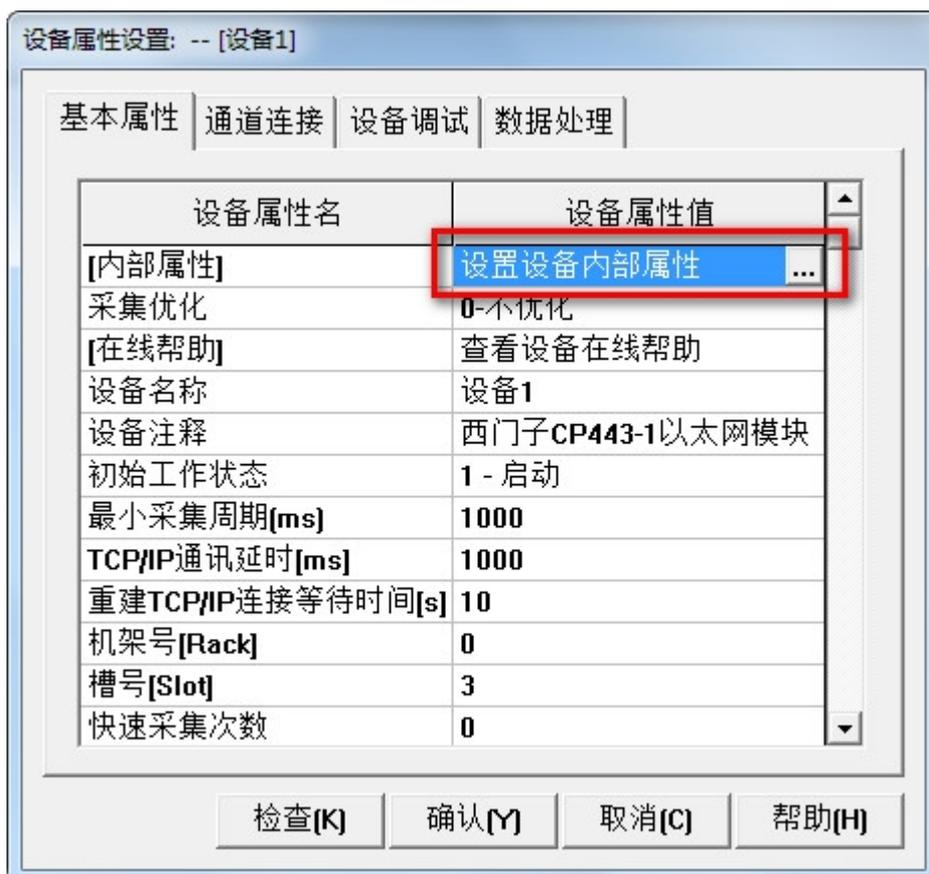
- 1、打开昆仑通态 MCGS 组态环境——设备窗口，在设备管理器中选择【PLC-西门子-S7CP343&443TCP-西门子 CP443-1 以太网模块】；



2、在设备属性设置中，将计算机的 IP 地址填入【本地 IP 地址】，模块的 IP 地址填入【远端 IP 地址】，【远端口号】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:WUB0		41538.0	1

## 6.5 TK 6000-MT&PT&PB 模块杰控通讯

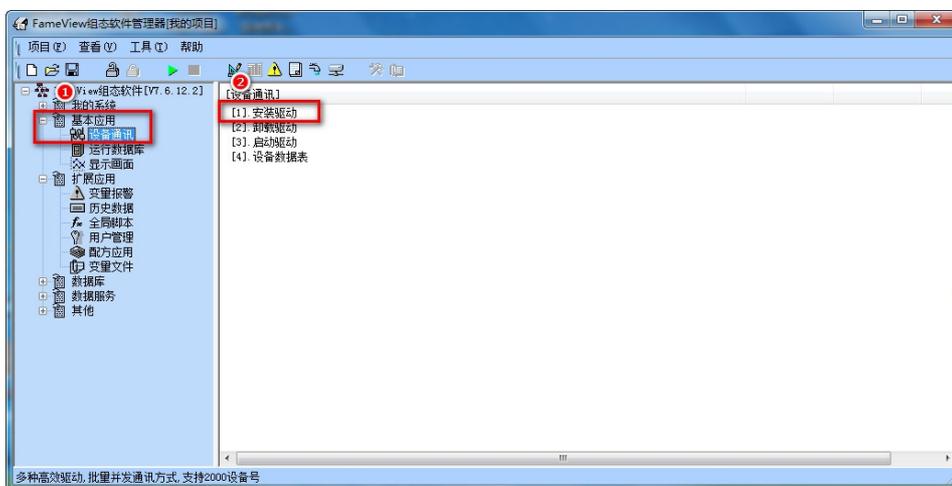
### 6.5.1 连接 S7200

西门子 S7-200 通过模块连接 FrameView，可以采用：西门子 S7TCP 驱动。

#### 6.5.1.1 采用西门子 S7TCP 驱动

##### 1、安装驱动程序：

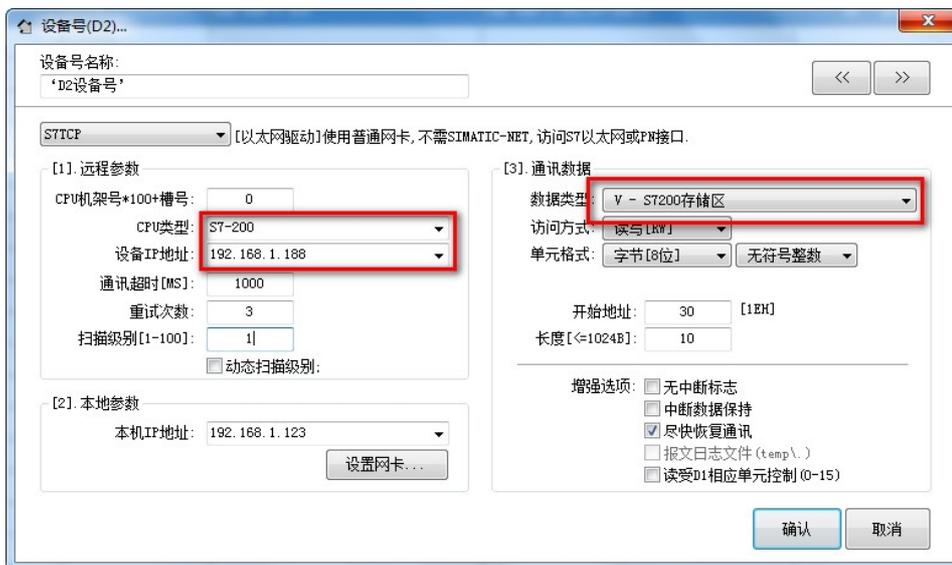
选择【基本应用】下【设备通讯】，执行【1.安装驱动程序】，显示下面对话框：



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：



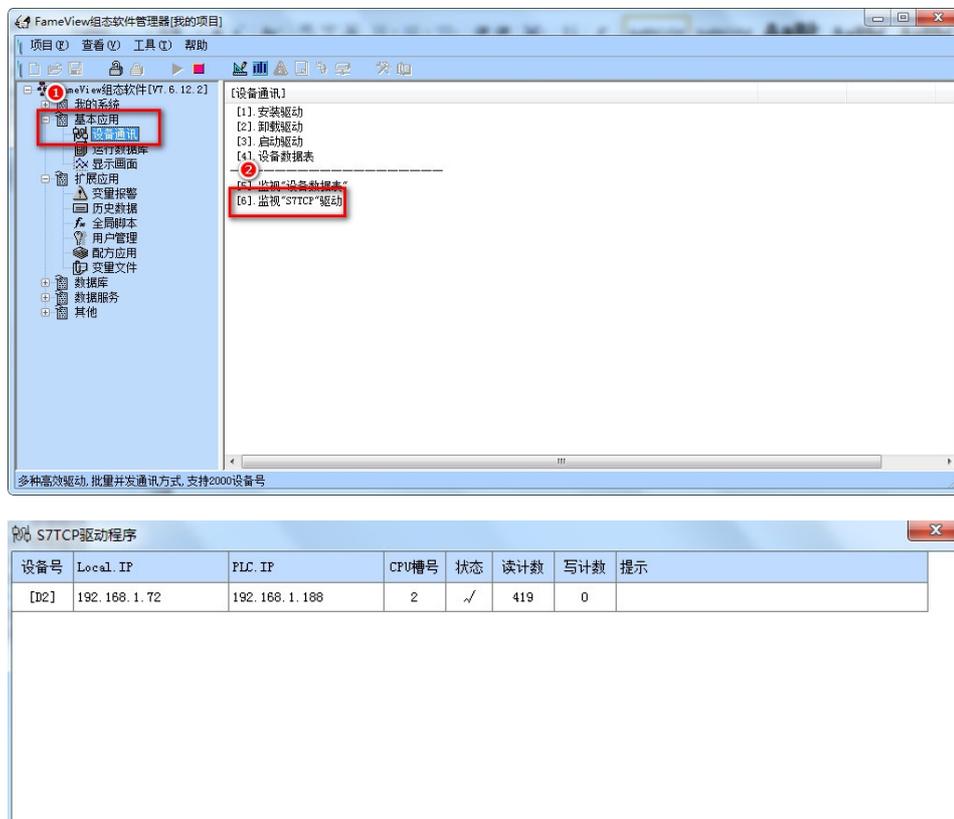
【CPU 类型】选择 S7-200，【设备 IP 地址】填入模块的 IP 地址；

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

### 3、监视设备通讯

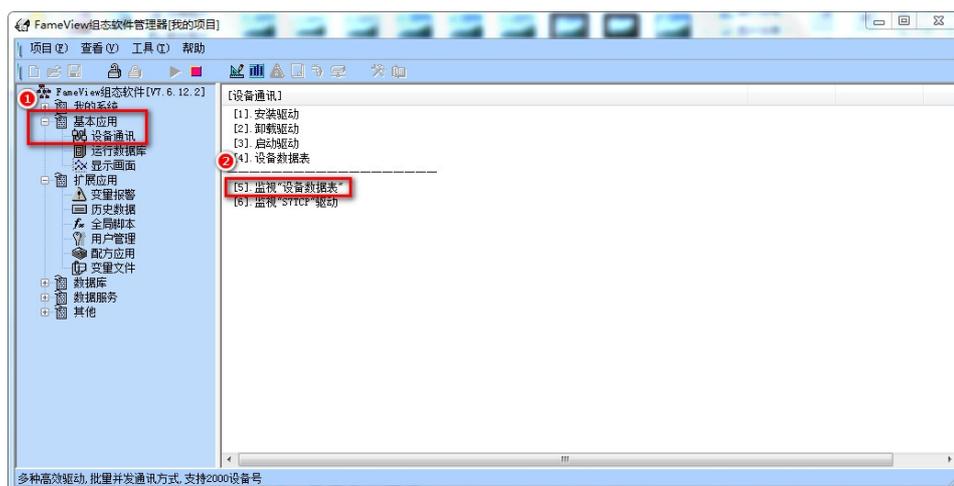
启动监视系统后，能监视驱动程序通讯状态。

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 个字节的的数据。

双字	DW0				DW1				DW2				DW3				DW4			
字	W0		W1		W2		W3		W4		W5		W6		W7		W8			
字节	B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16	B17		
[D1]	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
[D2]	38																			

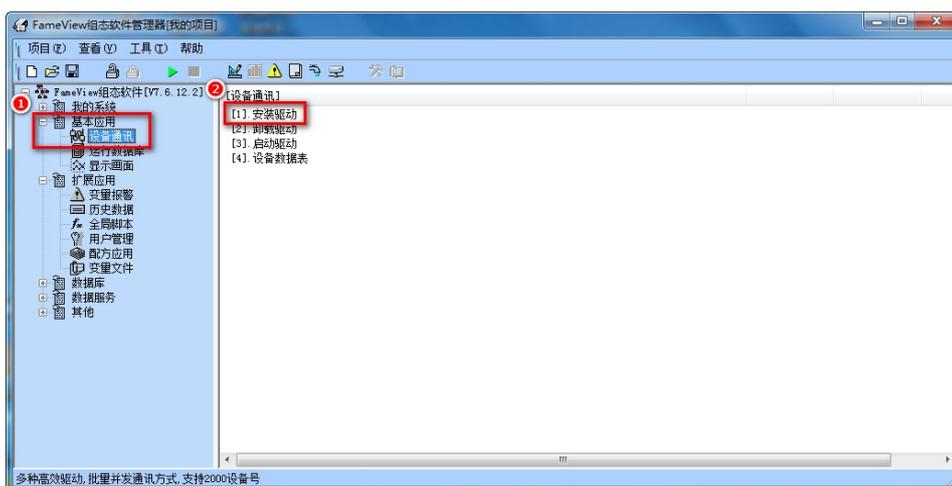
## 6.5.2 TK 6000-MT 模块连接 S7300

西门子 S7-300/400 通过模块连接 FrameView，可以采用：西门子 S7TCP 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：



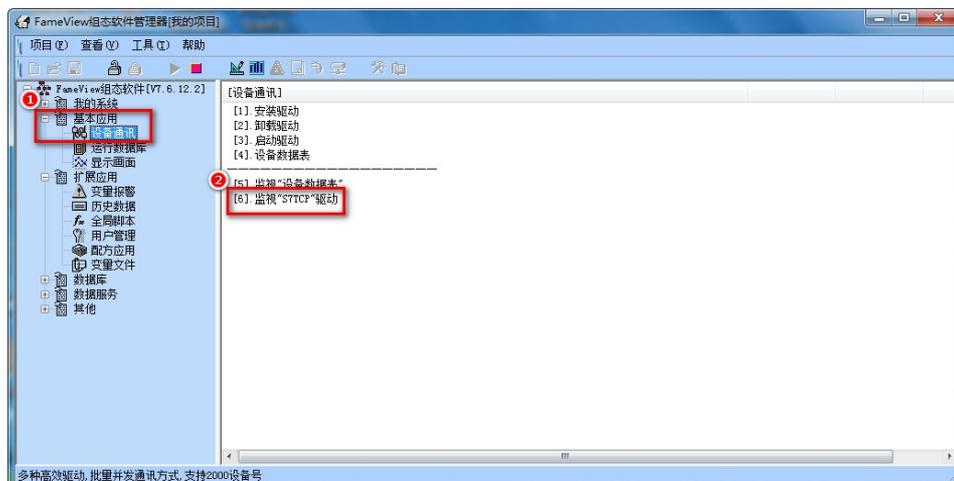
【CPU 类型】选择 S7-300，【设备 IP 地址】填入模块的 IP 地址；

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

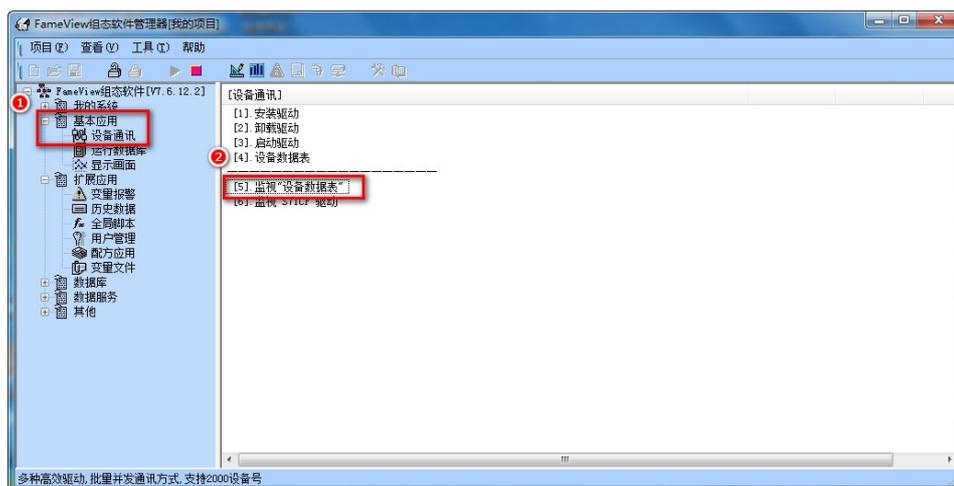
启动监视系统后，能监视驱动程序通讯状态。

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”】：



## 6.6TK 6000-MT&PT&PB 模块 IFIX 通讯

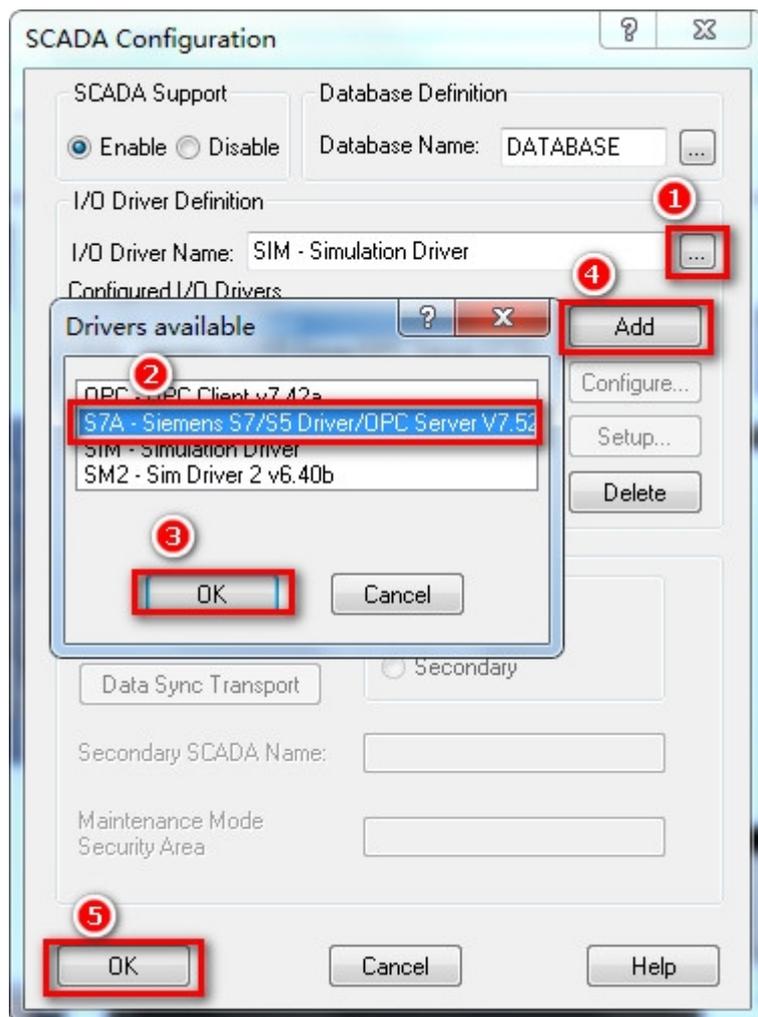
### 6.6.1 连接 S7200

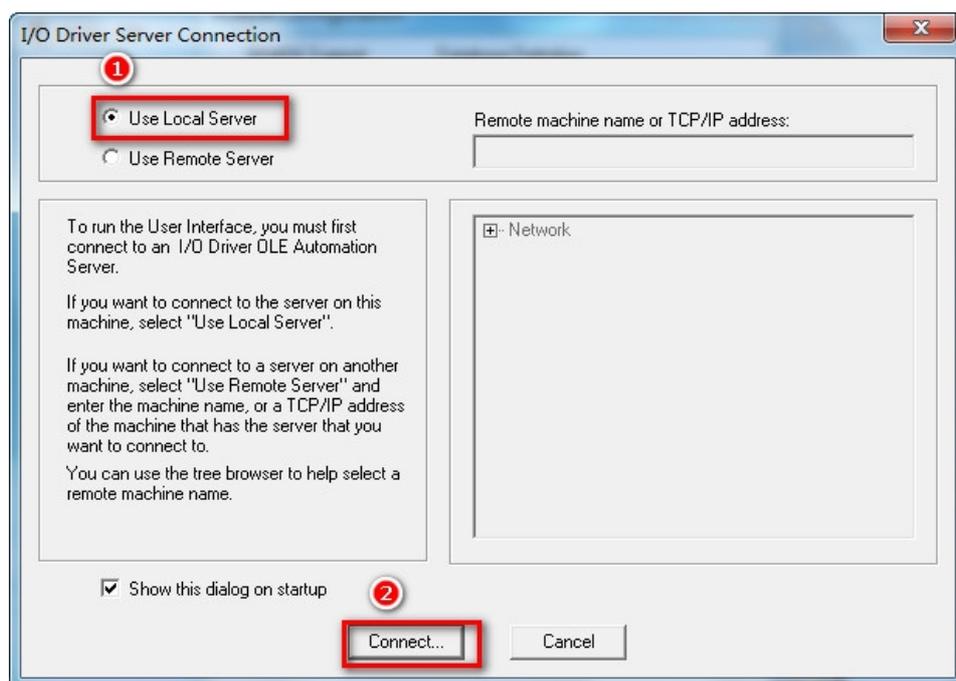
西门子 S7-200 通过模块连接 iFIX，可以采用：iFIX 的 S7TCP 驱动。

#### 6.6.1.1 采用 S7TCP 驱动

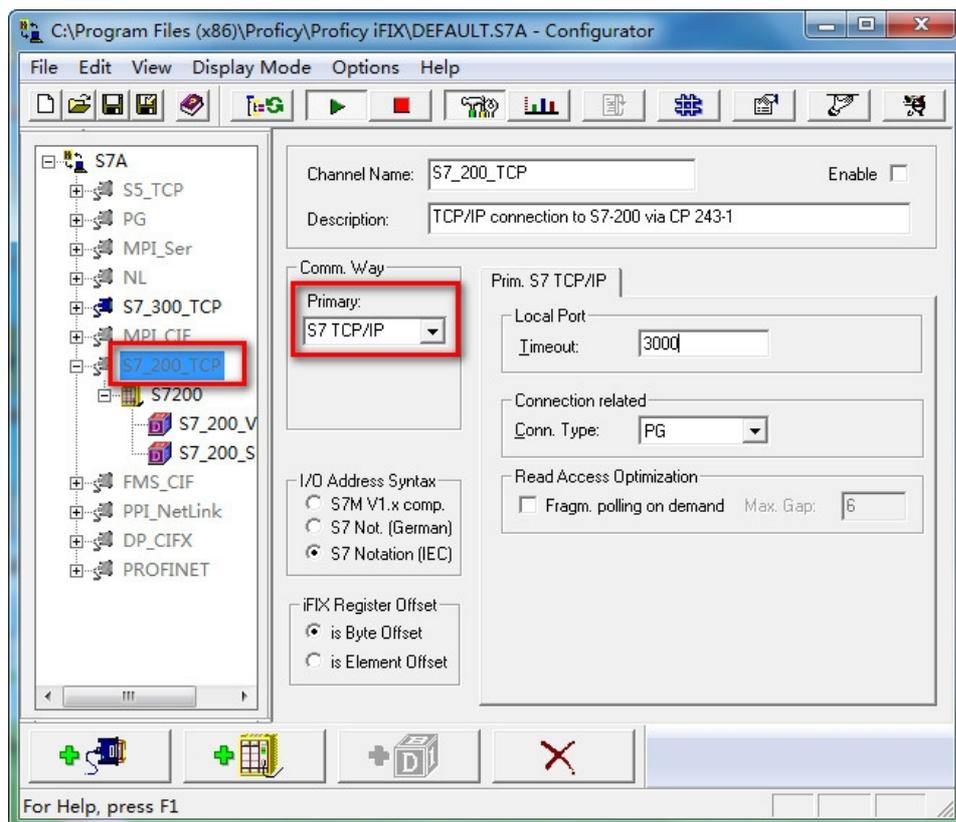
1、安装西门子 S7TCP 驱动程序【S7A】，在【SCU-FIX】中配置 S7A 驱动：



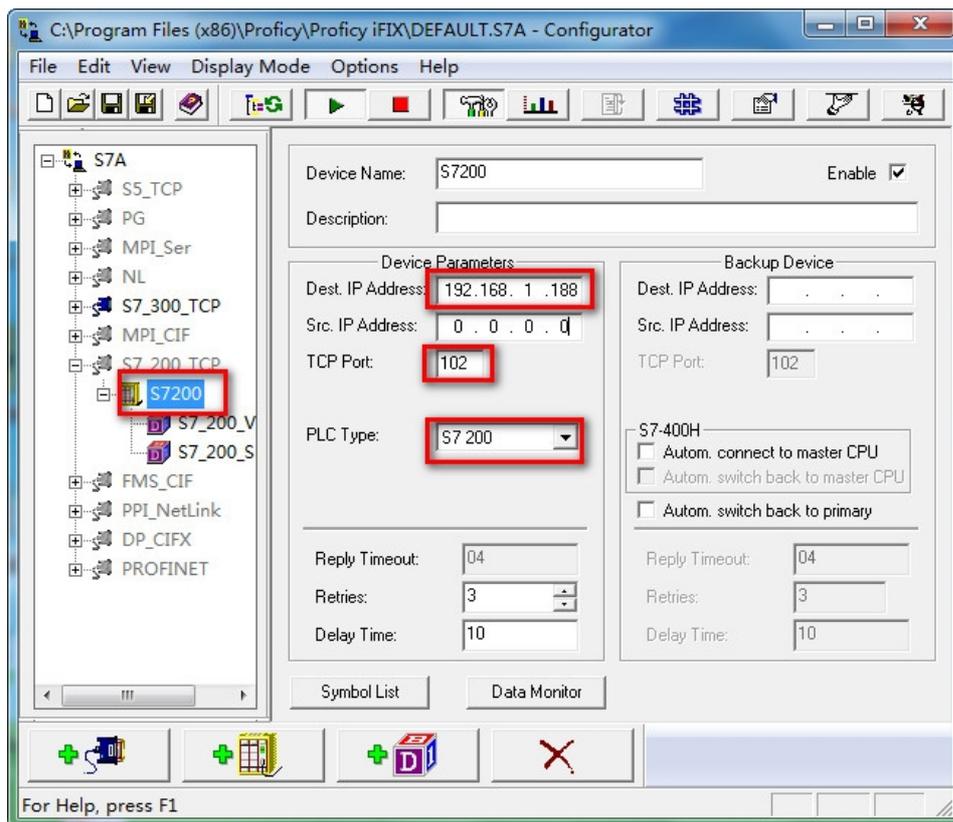




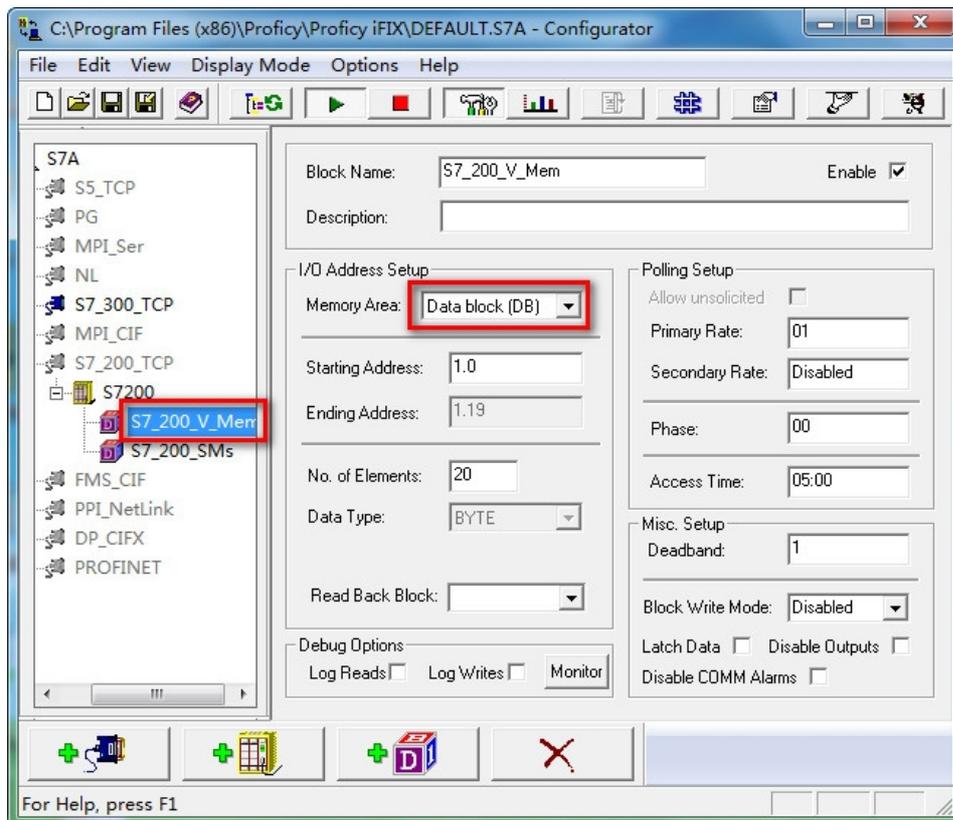
2、选择【S7\_200\_TCP】，【Primary】中选择S7TCP/IP；



3、【Dest IP Address】中填入模块的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)。



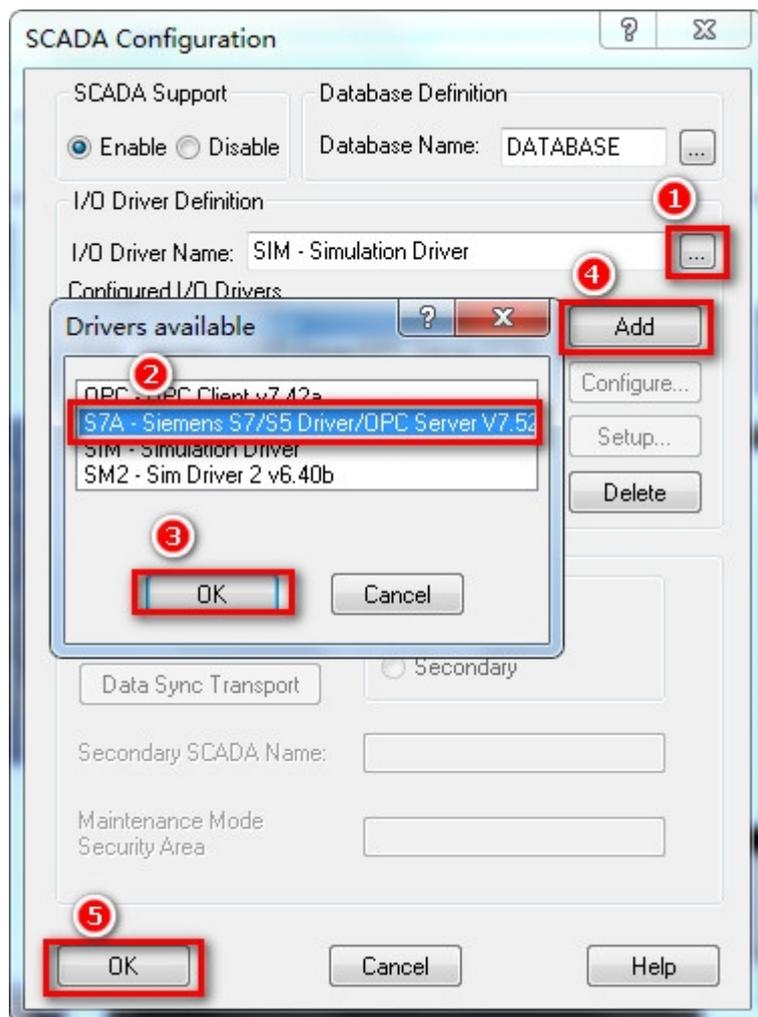
## 6.6.2TK 6000-MT 模块连接 S7300

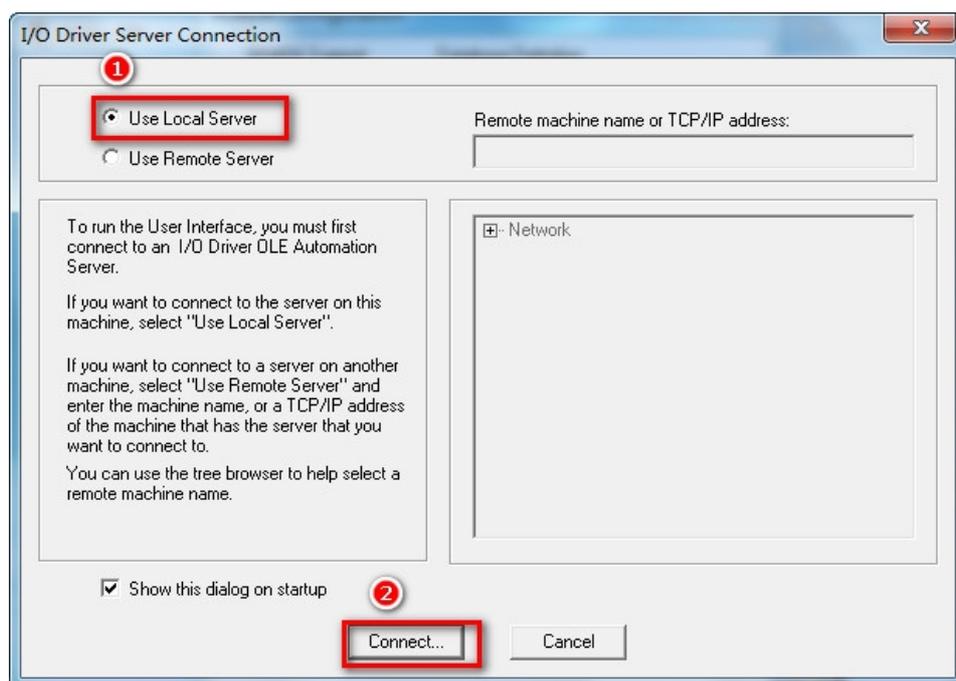
西门子 S7-300/400 采用模块 连接 iFIX，可以通过：S7TCP 驱动。

### 6.6.2.1 采用 S7TCP 驱动

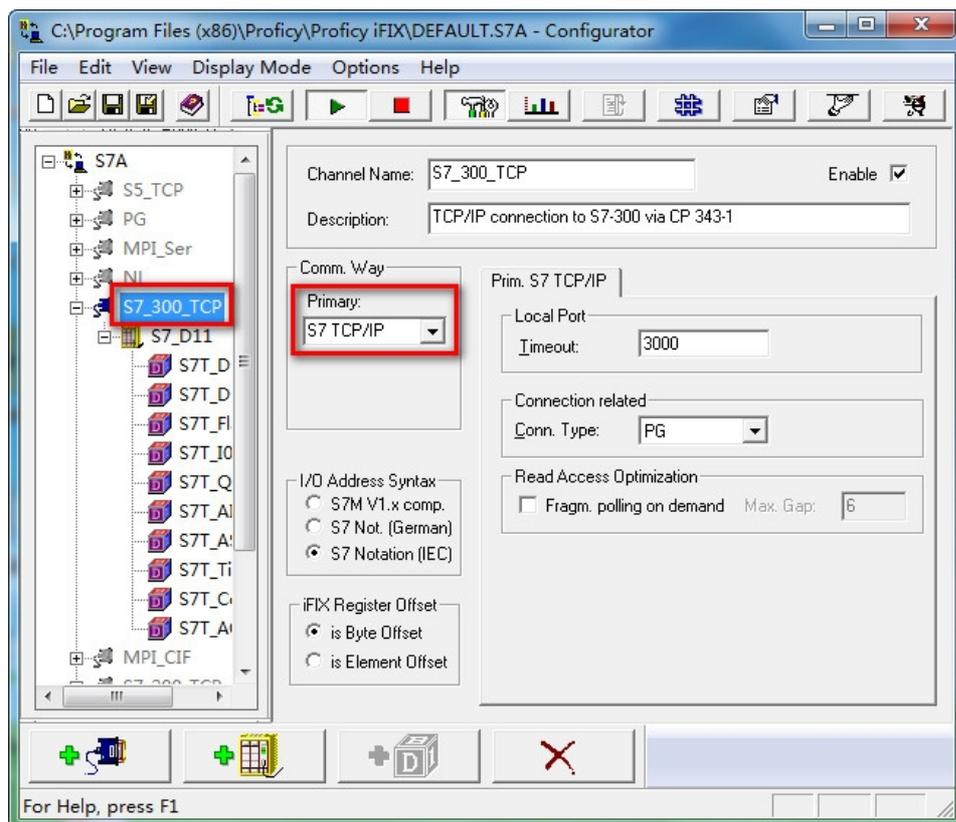
1、安装西门子 S7TCP 驱动程序【S7A】，在【SCU-FIX】中配置 S7A 驱动，如图：



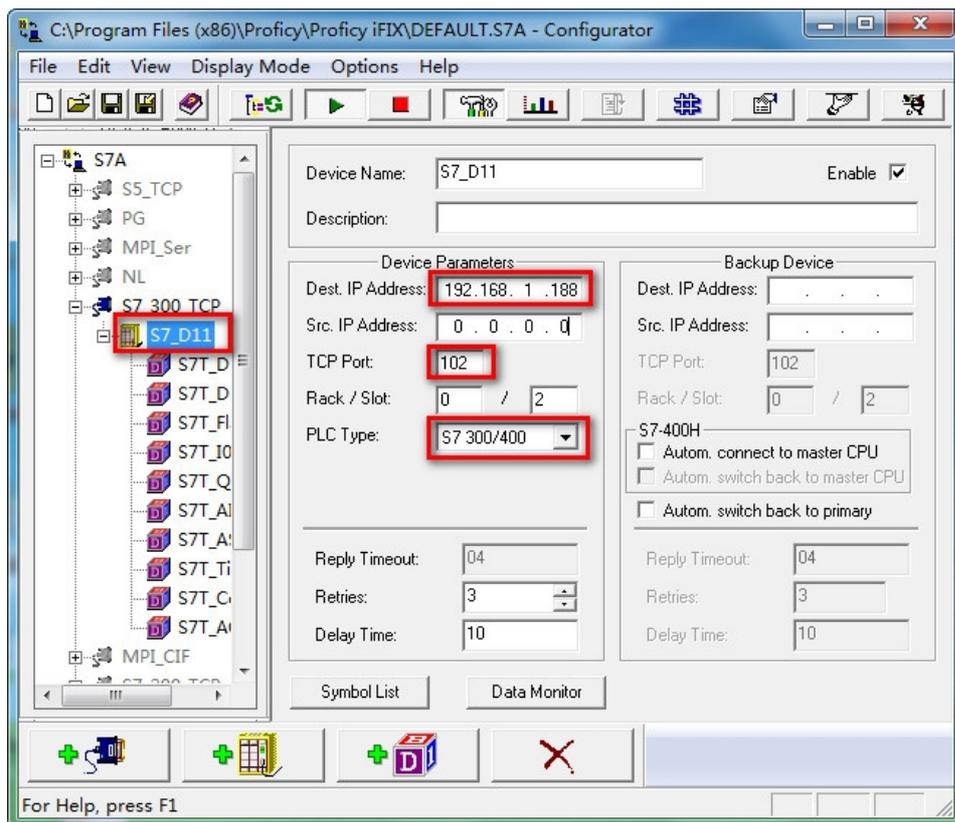




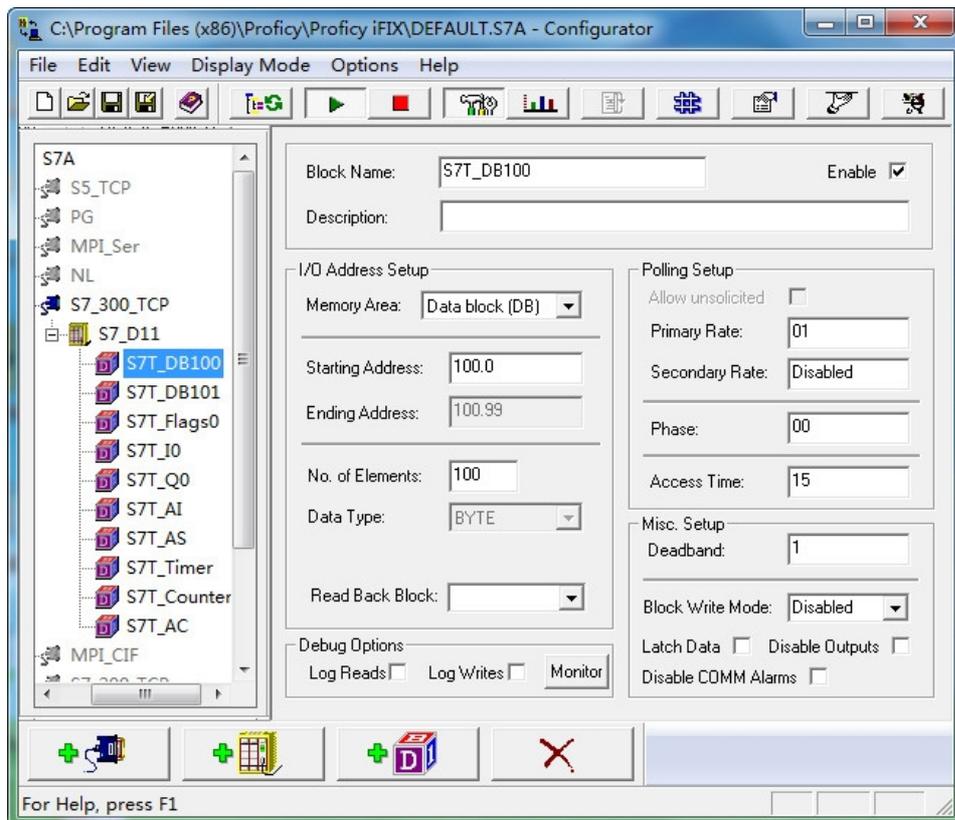
2、选择【S7\_300\_TCP】，在【Primary】中选择S7TCP/IP；



3、【Dest IP Address】，填入模块的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：



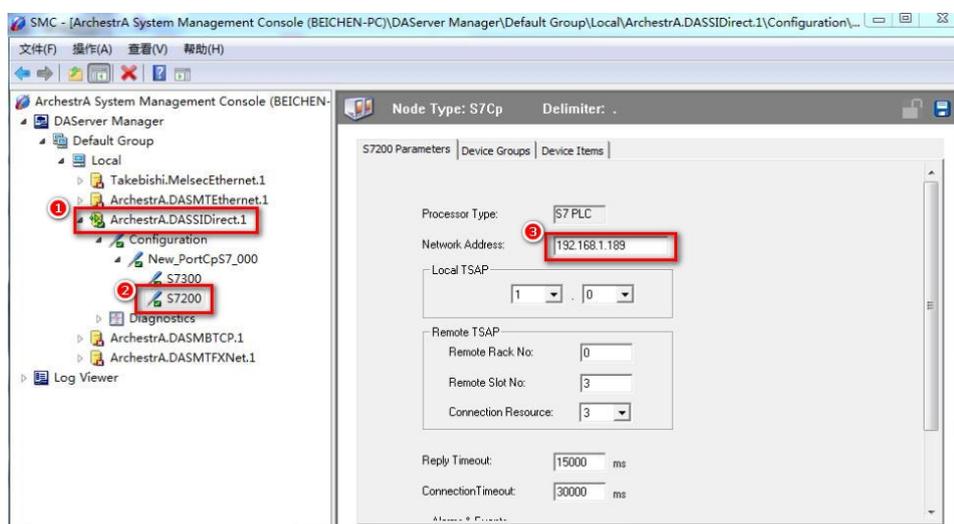
## 6.7 TK 6000-MT&PT&PB 模块 INTOUCH 通讯

### 6.7.1 连接 S7200

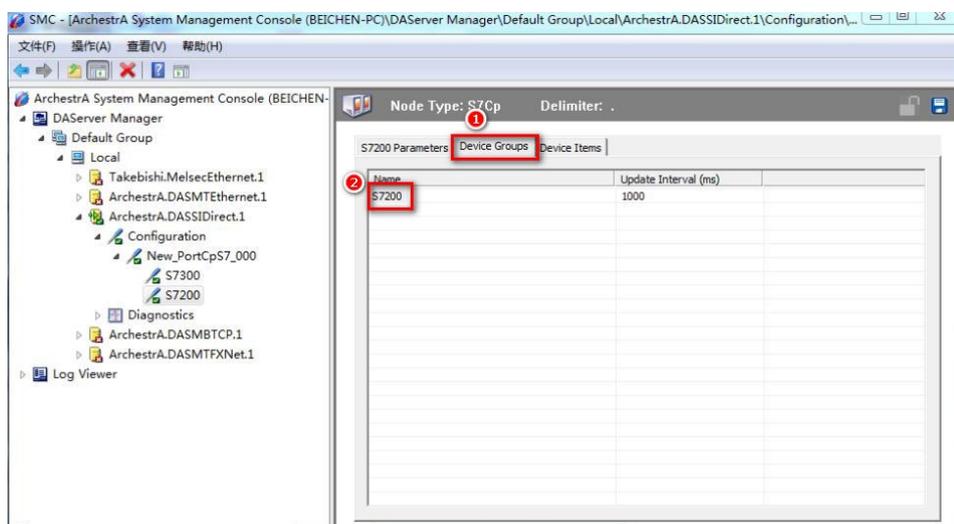
模块连接 INTOUCH，可以采用西门子 S7TCP 驱动。

#### 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；只需要将模块的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；



- 右击【ArchestrA.DASSIDirect】，选择【Activate Server】来启动此 DA Server；
- 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”；



- 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 VV0；



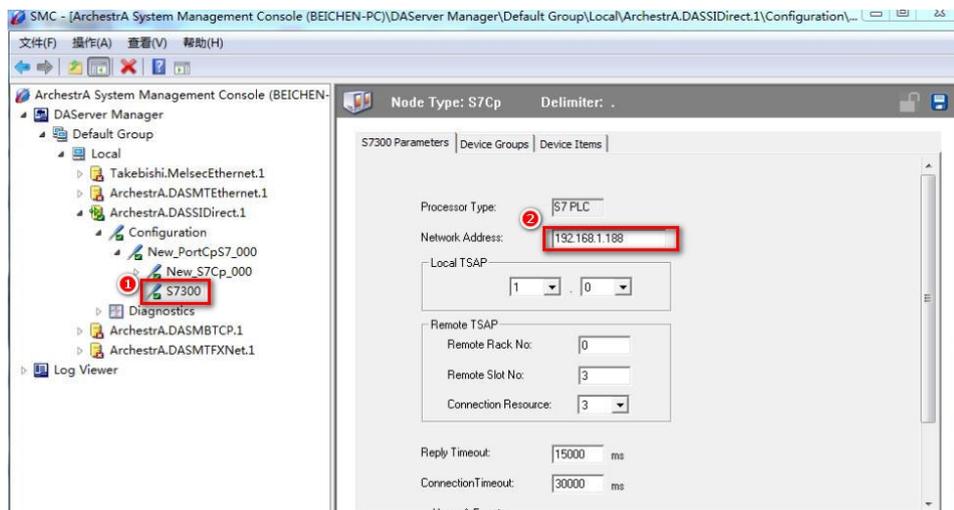
- 通讯在“窗口”中，引用建立的变量，即可以建立 S7PLC 和 INTOUCH 监控画面的通讯。

## 6.7.2TK 6000-MT 模块连接 S7300

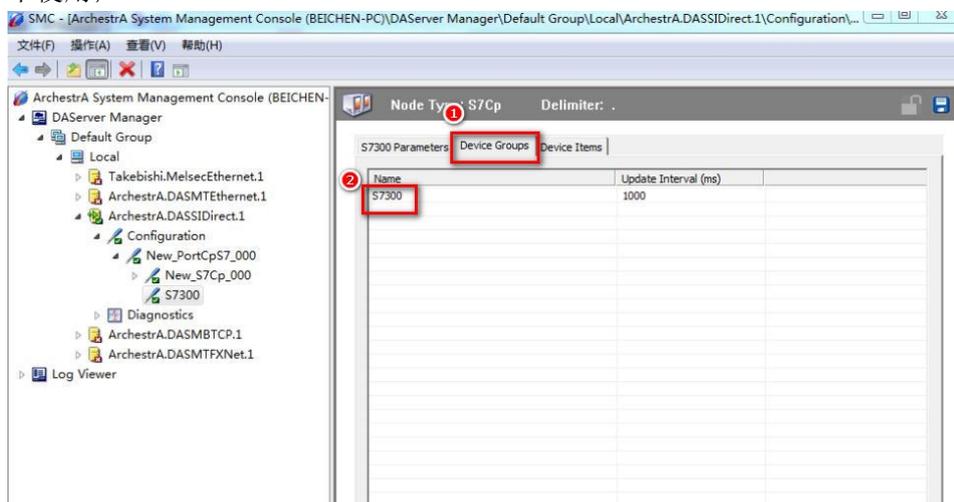
模块连接 INTOUCH，可以采用西门子 S7TCP 驱动。

### 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；只需要将模块的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；



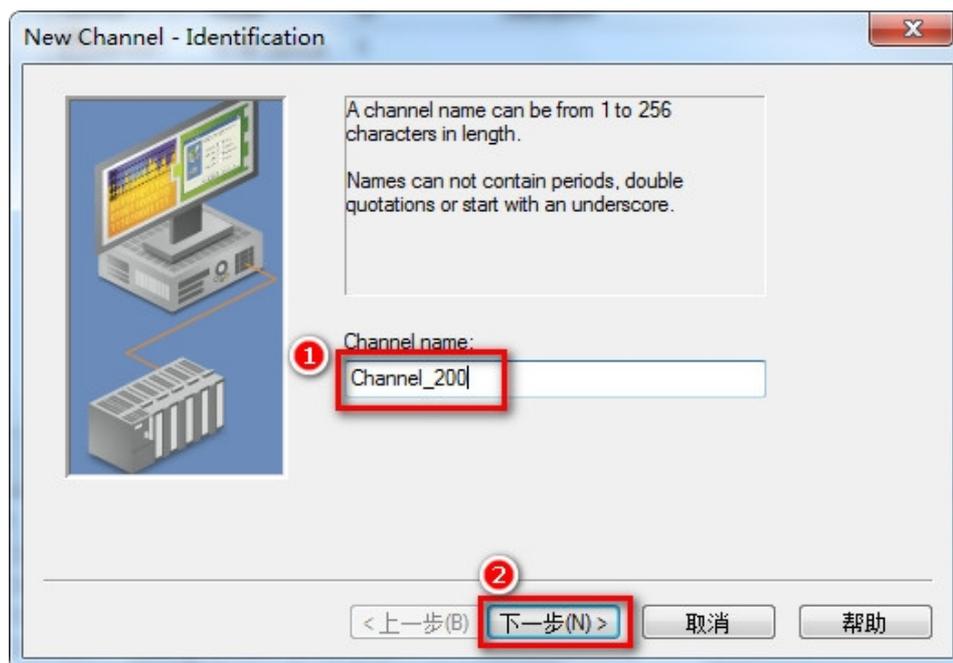
4、通讯在“窗口”中，引用建立的变量，即可以建立 S7PLC 和 INTOUCH 监控画面的通讯。

## 6.8 TK 6000-MT&PT&PB 模块 LABVIEW 通讯

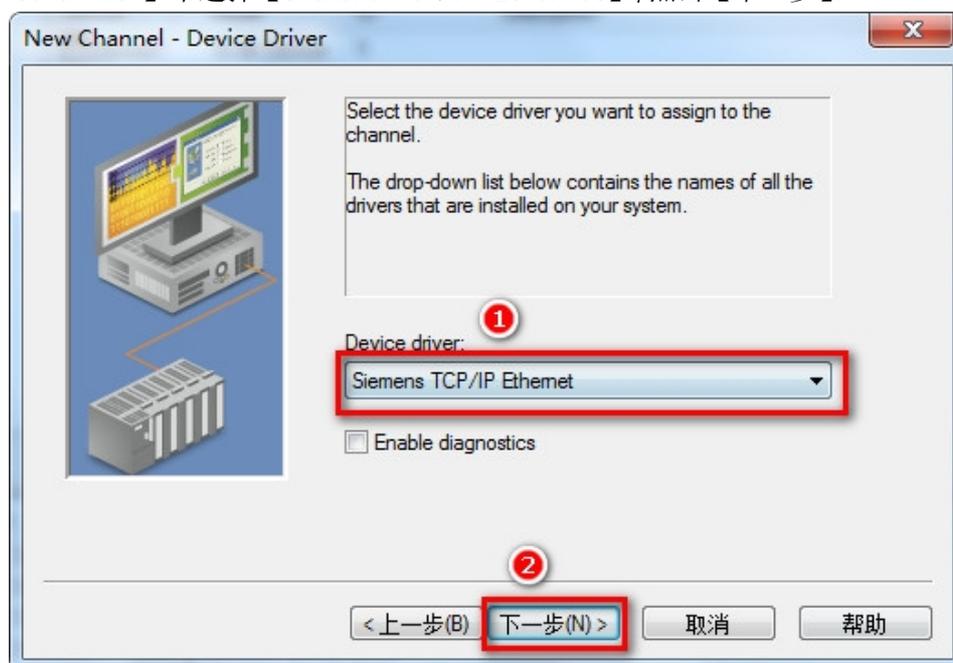
### 6.8.1 连接 S7200

通过 NI OPC Servers 连接

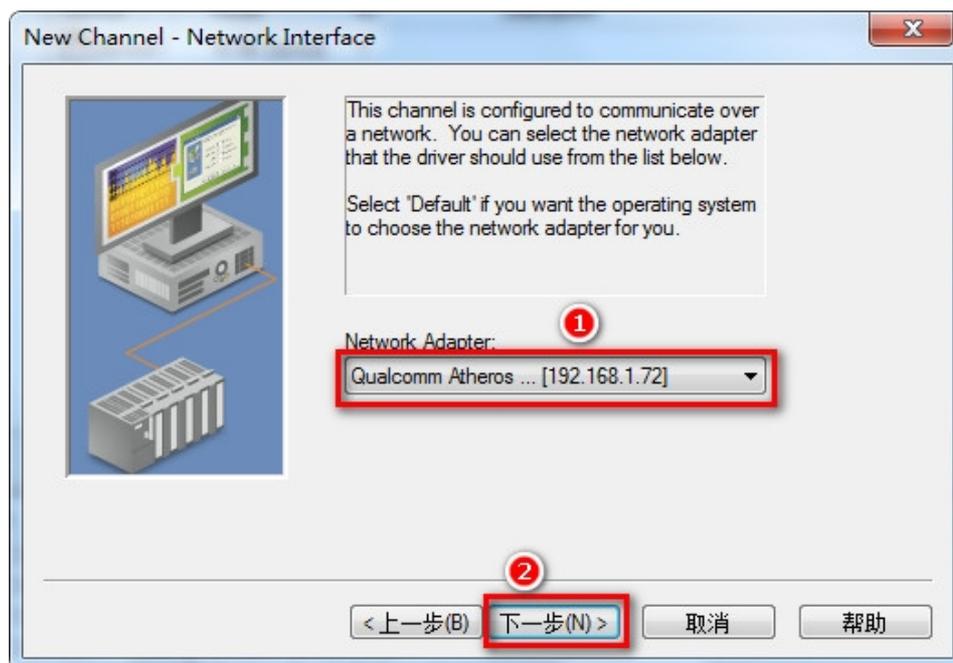
1. 打开 NI OPC Servers 软件。
2. 新建一个 Channel，这里取名“Channel\_200”，点击【下一步】；



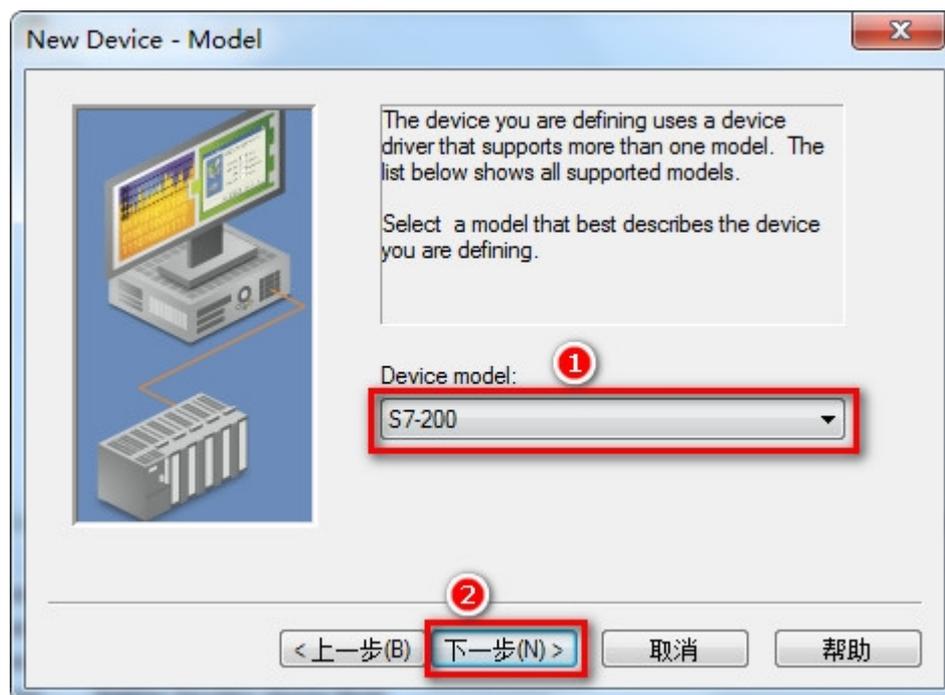
3. 在【Device driver】中选择【Siemens TCP/IP Ethernet】，点击【下一步】。



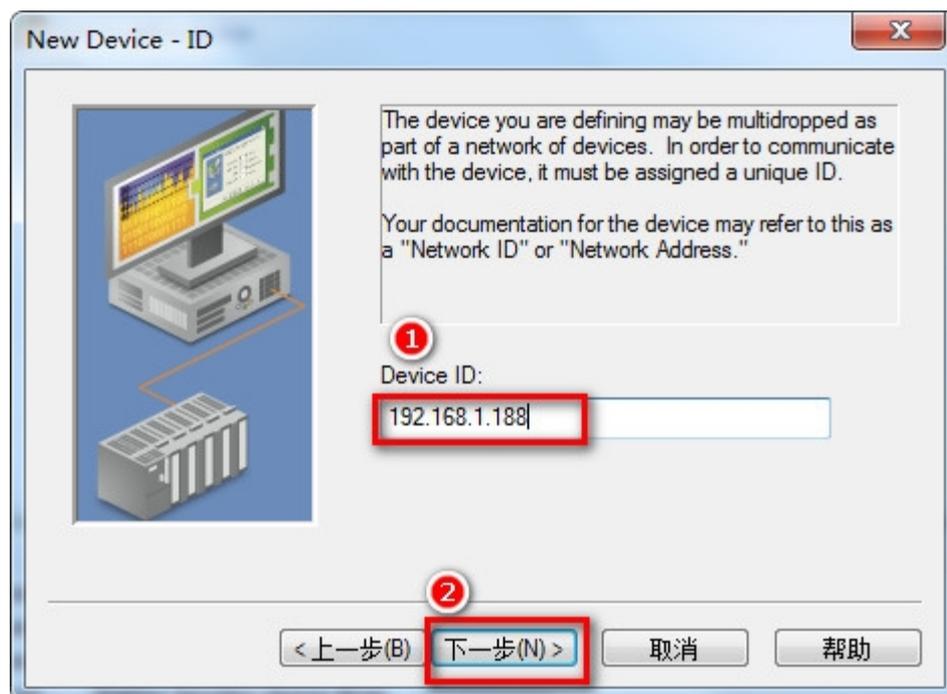
4. 在【Network Adapter】中选择你的网卡信息，点击【下一步】。



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】下面填入模块的 IP 地址，点击【下一步】，其它参数默认直至完成。

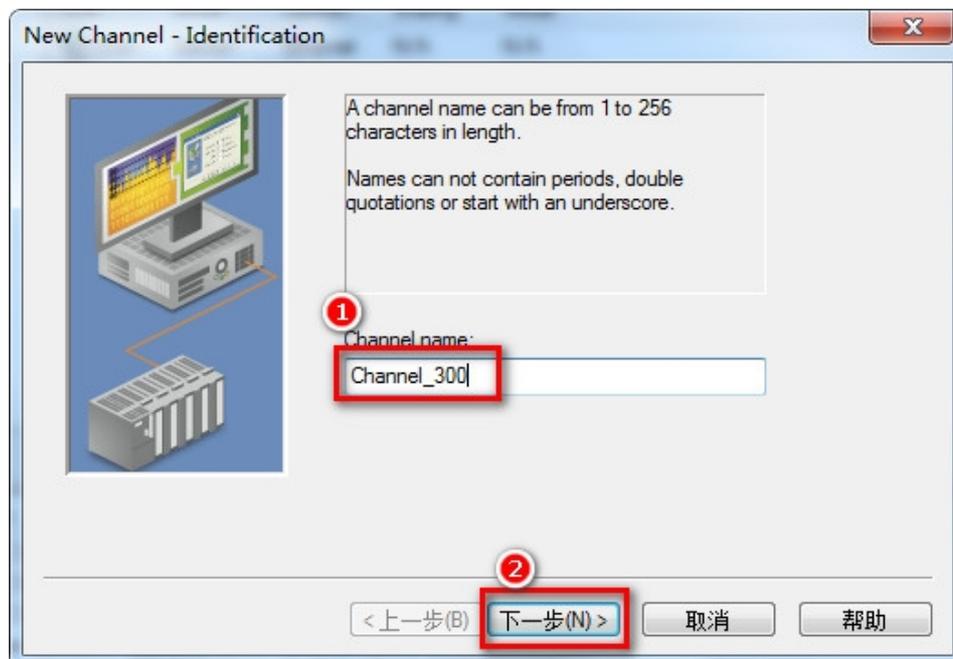


8. 选择默认参数，点击【下一步】直到【完成】。

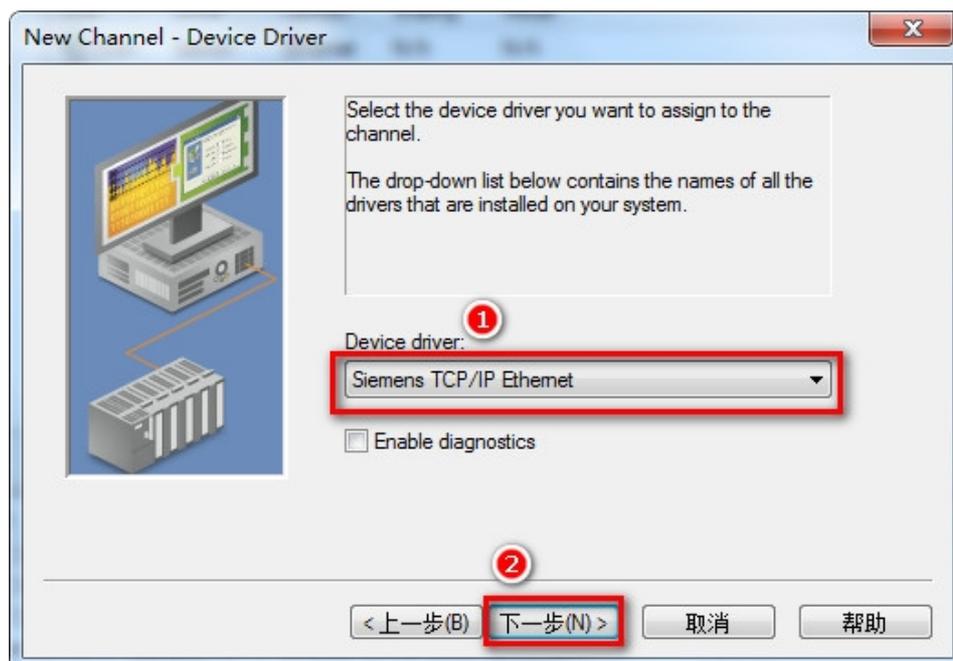
## 6.8.2 TK 6000-MT 模块连接 S7300

### 通过 NI OPC Servers 连接

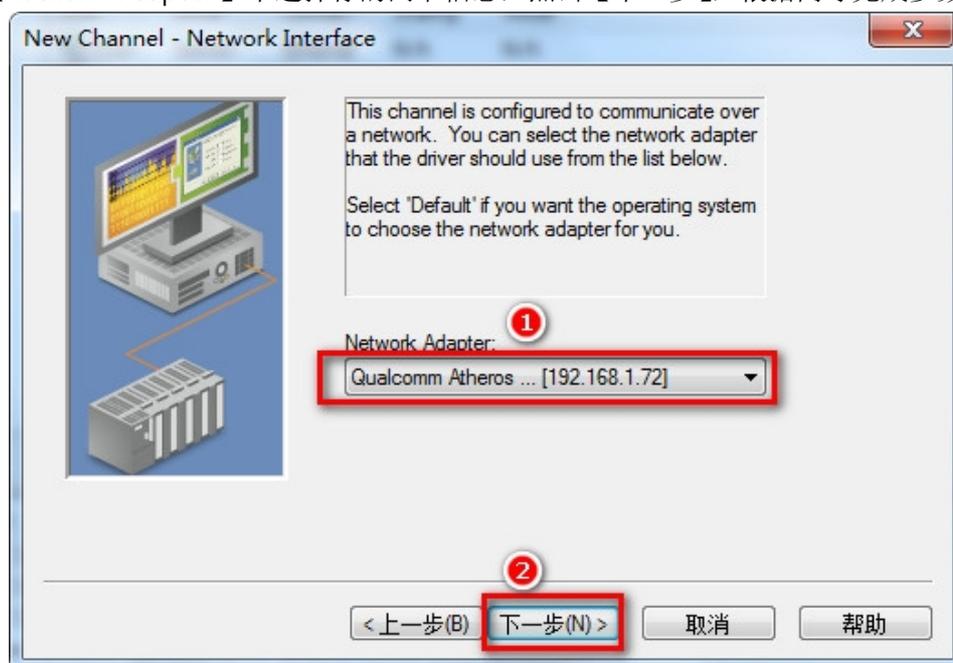
1、打开 NI OPC Servers 软件。新建一个 Channel，这里取名“Channel\_300”，点击【下一步】：



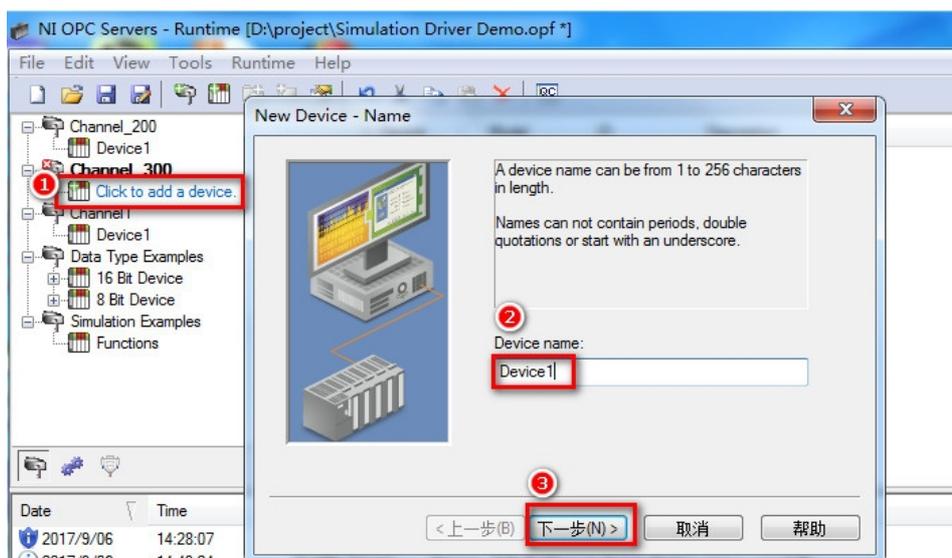
2、在【Device driver】中选择【Siemens TCP/IP Ethernet】，点击【下一步】：



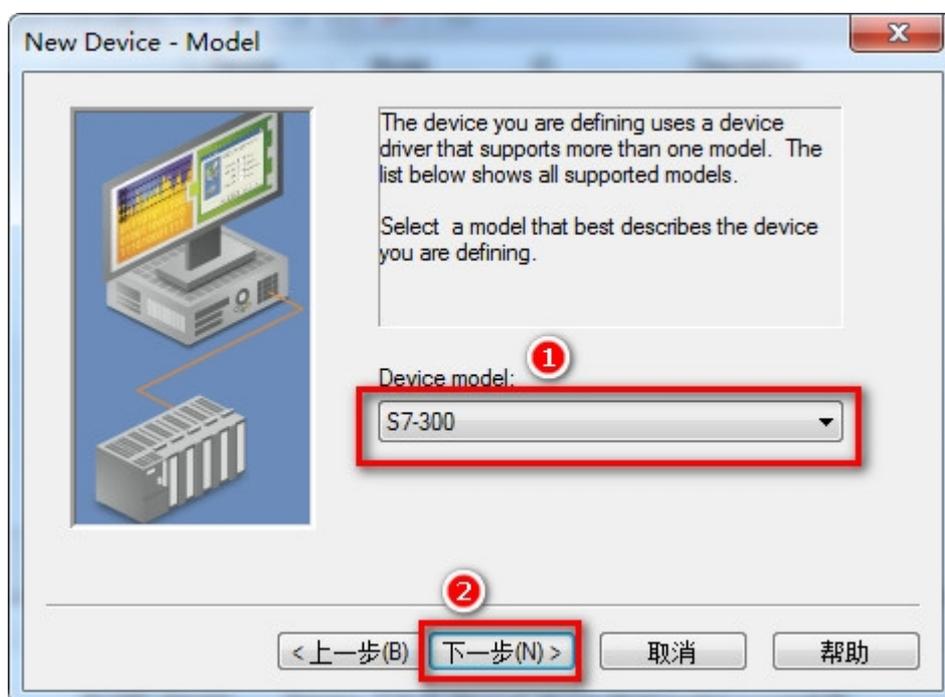
- 3、在【Network Adapter】中选择你的网卡信息，点击【下一步】，根据向导完成参数设置；



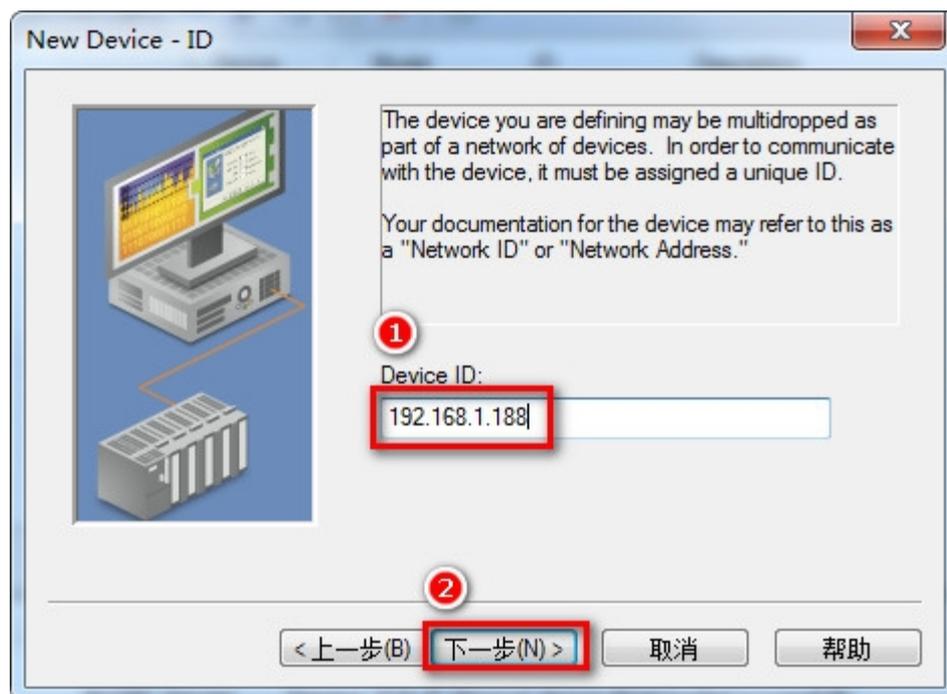
- 4、在刚建立的 Channel 下新建一个 Device, 这里取名“Device1”, 点击【下一步】；



5、在【Device model】下选择【S7 300】，点击【下一步】；



6、在【Device ID】下面填入模块的 IP 地址，点击【下一步】，其它参数默认，直至完成。

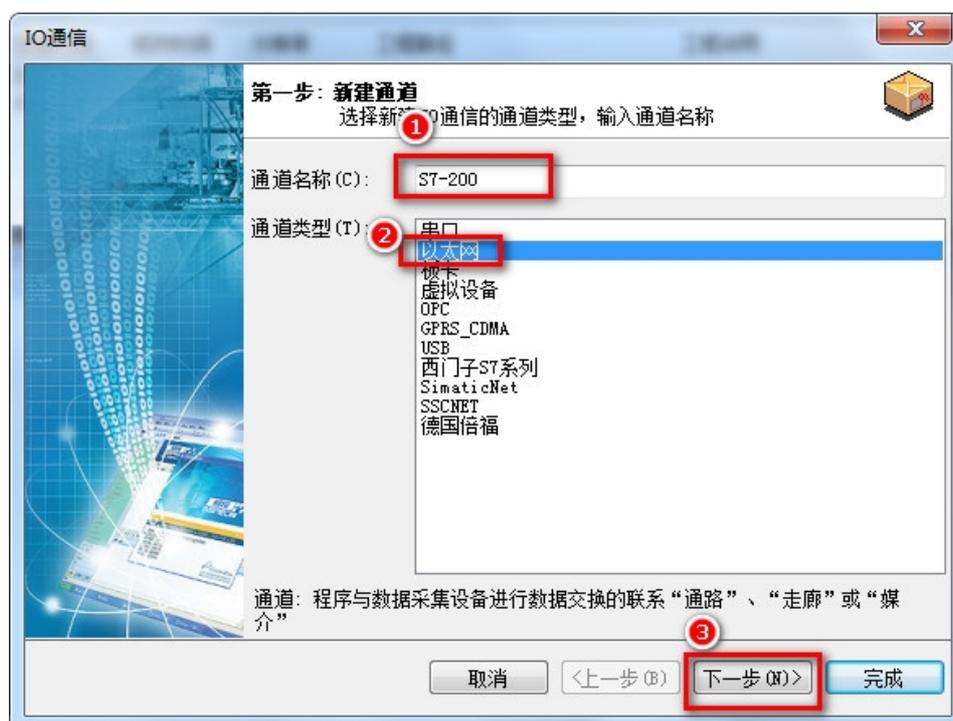


## 6.9 TK 6000-MT&PT&PB 模块易控通讯

### 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】填入模块的 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。



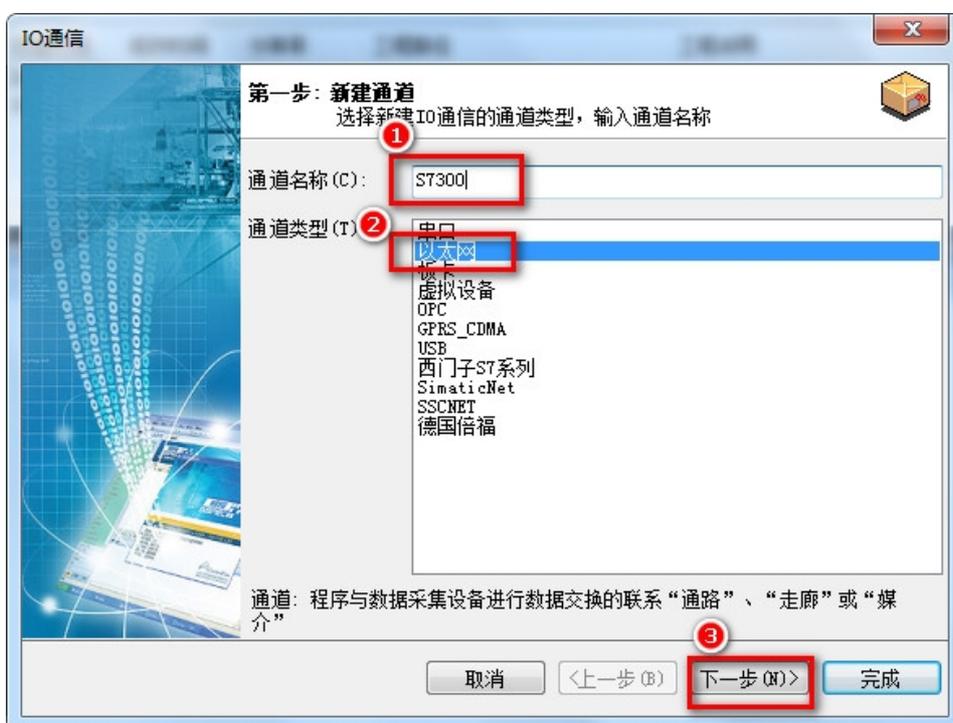
4、打开工程菜单【IO 通信】组下的【S7200 以太网】，添加变量和测试监控。



## 6.9.2 TK 6000-MT 模块连接 S7300

通过西门子以太网驱动连接

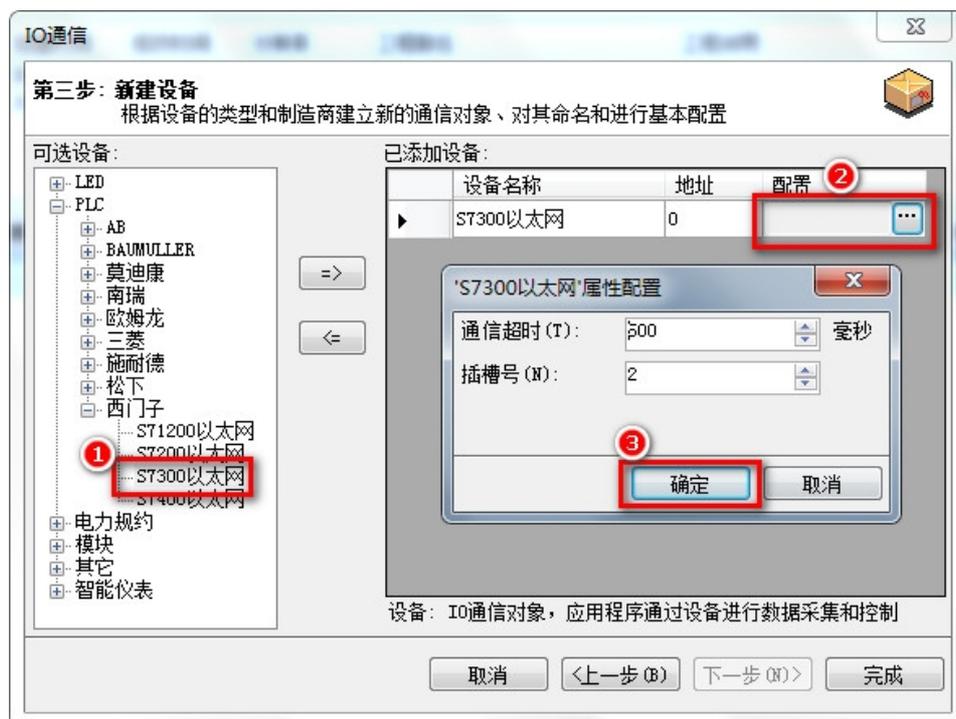
1、新建通道，选择【以太网】通讯方式，填入通道名称；



2、配置通道-远程节点中【IP地址】填入模块的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

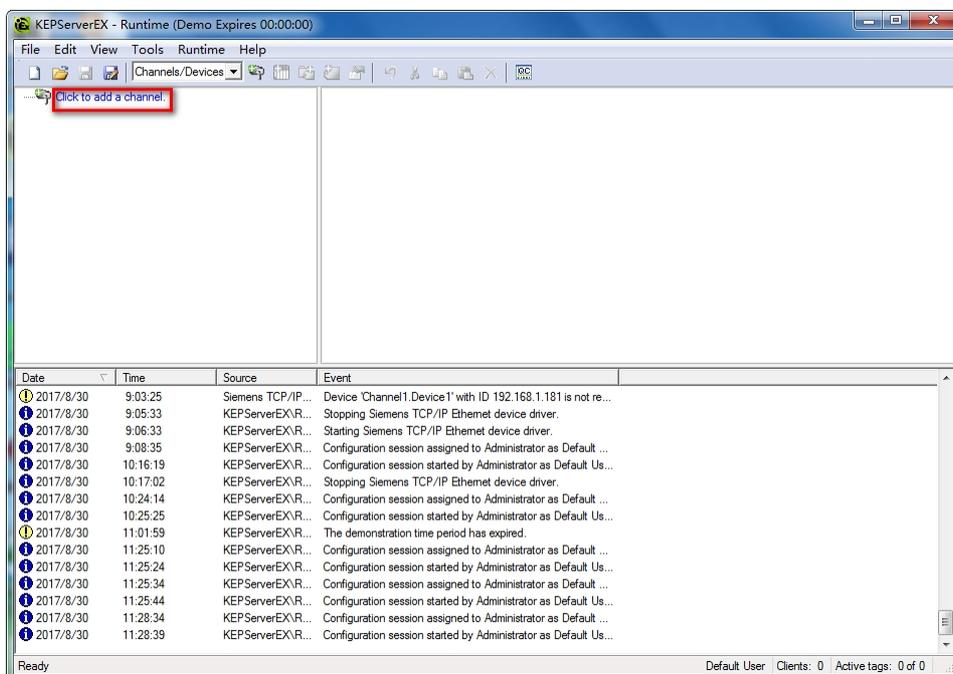
### 7.1 TK 6000-MT&PT&PB 模块 Kepware OPC 通讯

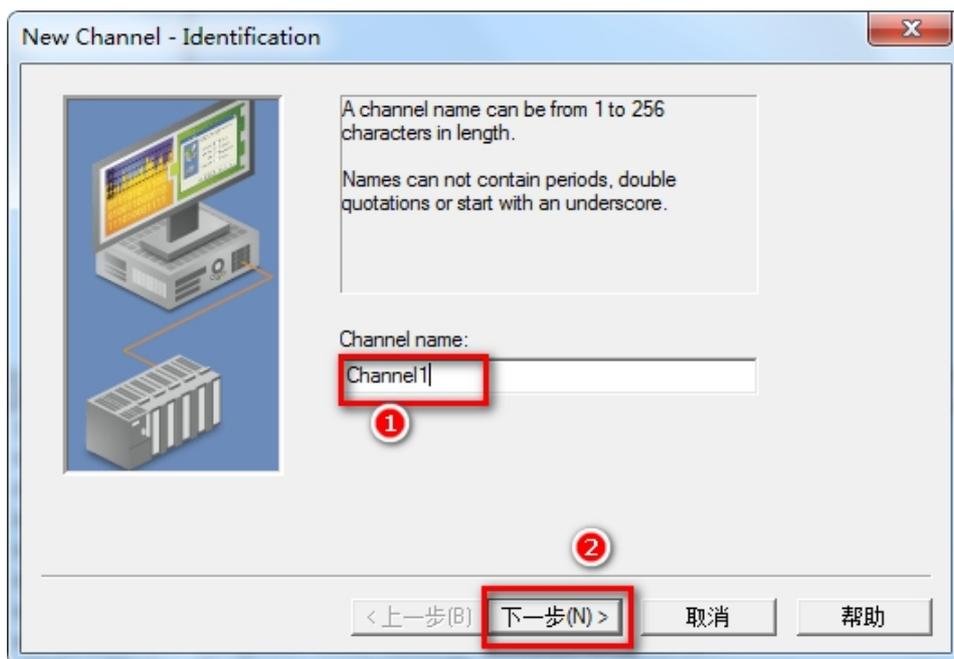
#### 7.1.1 连接 S7200

西门子 S7-200 通过模块连接 KepWare OPC，可以采用西门子 S7TCP 驱动。

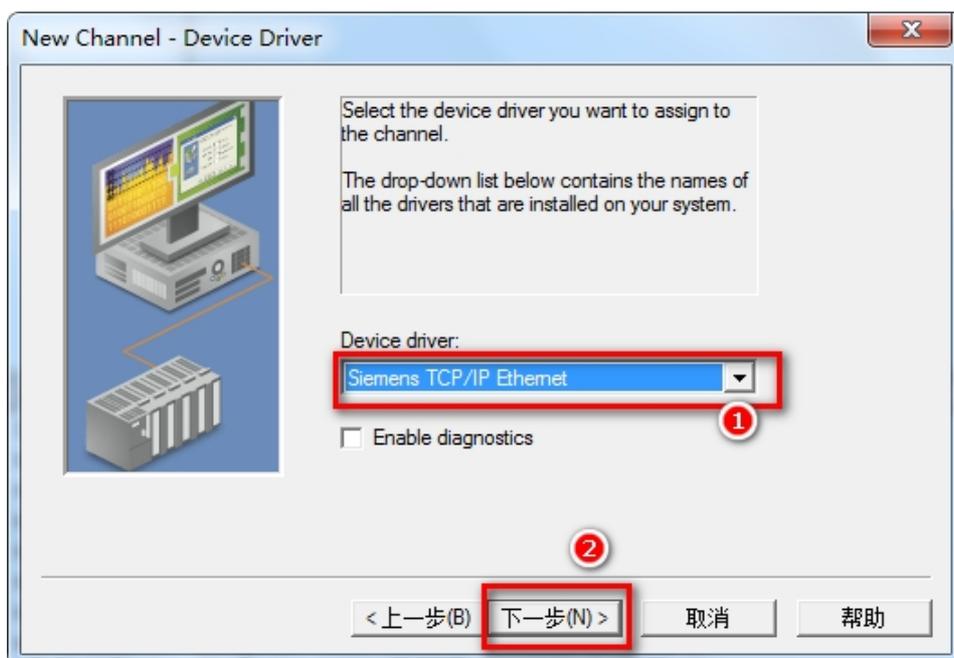
##### 7.1.1.1 添加通道

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

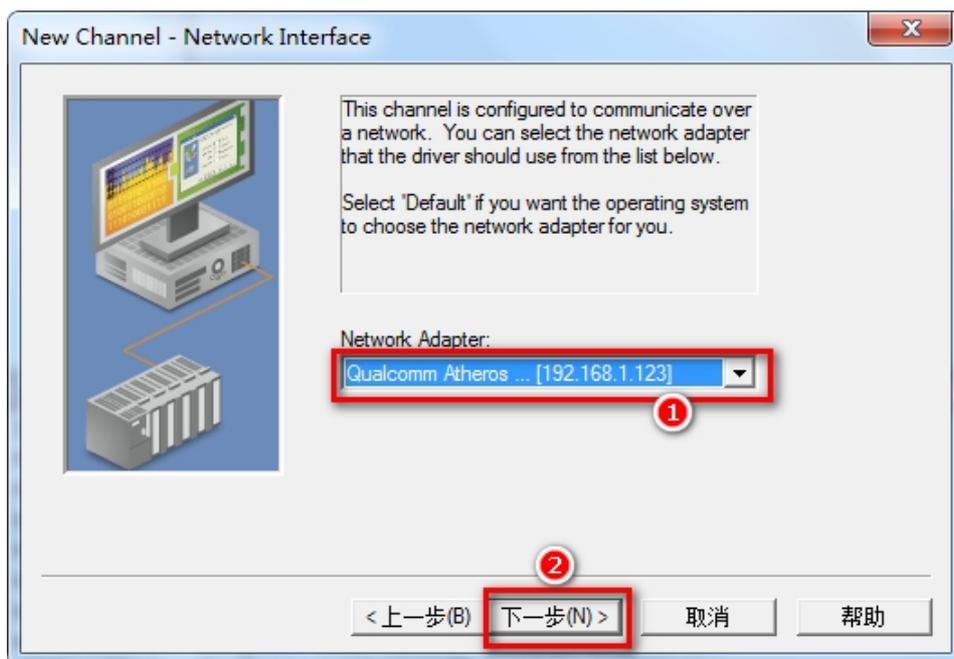




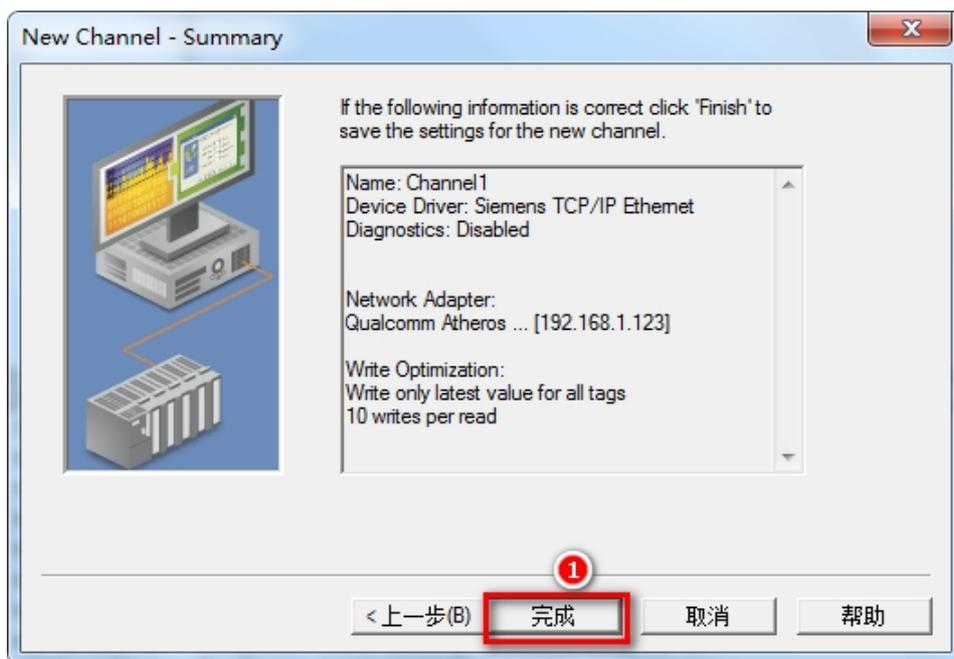
2、【Device driver】选择【Siemens TCP/IP Ethernet】驱动，点击【下一步】；



3、【Network Adapter】选择计算机网卡；

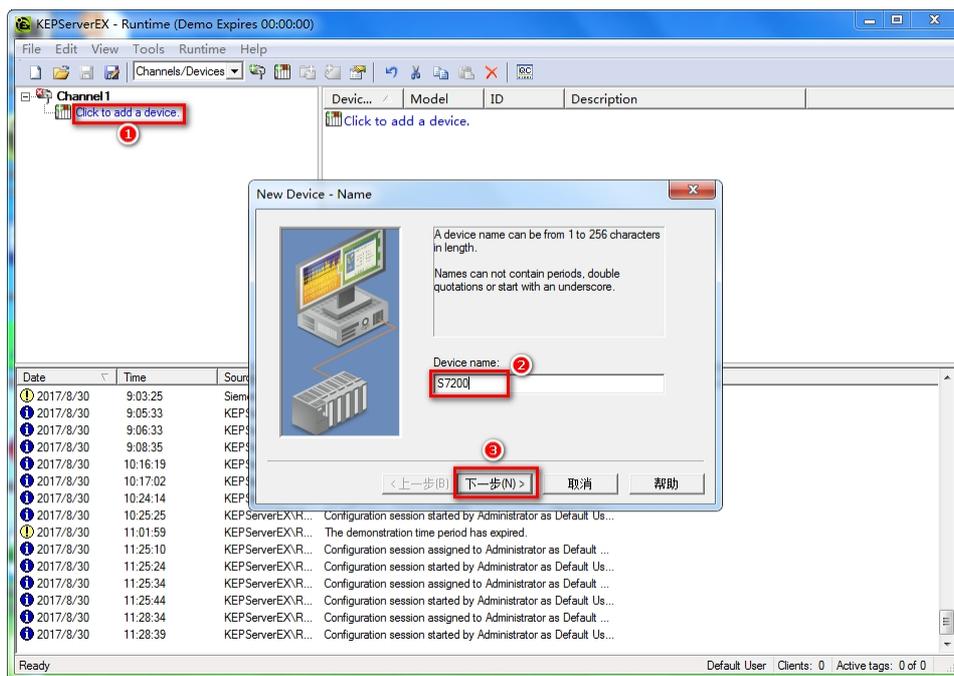


4、根据需要选择模式（可默认），依照向导完成通道参数设置；

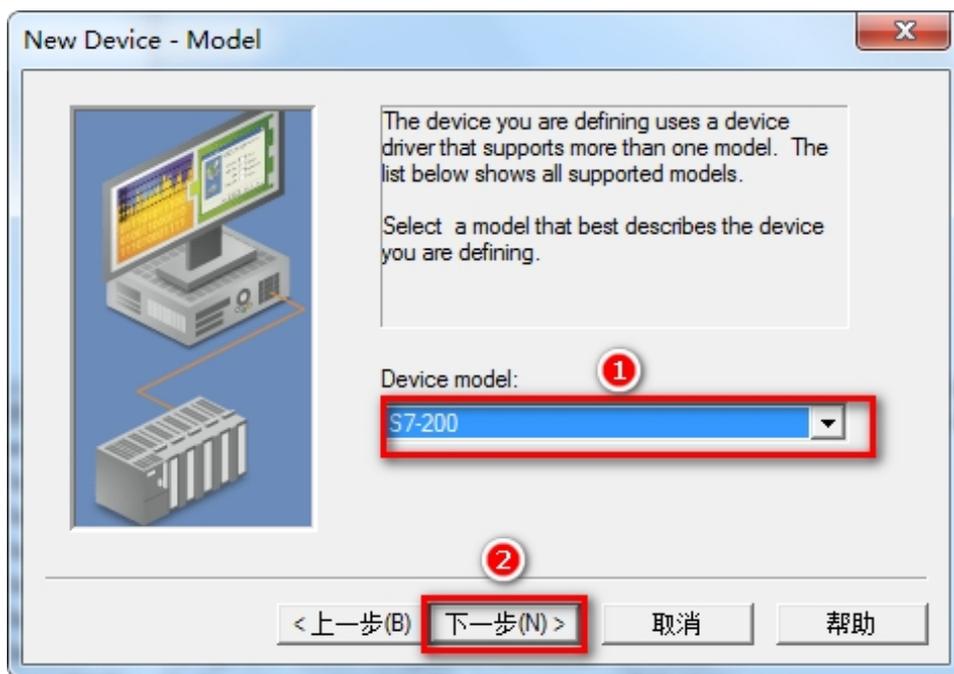


### 7.1.1.2 添加设备

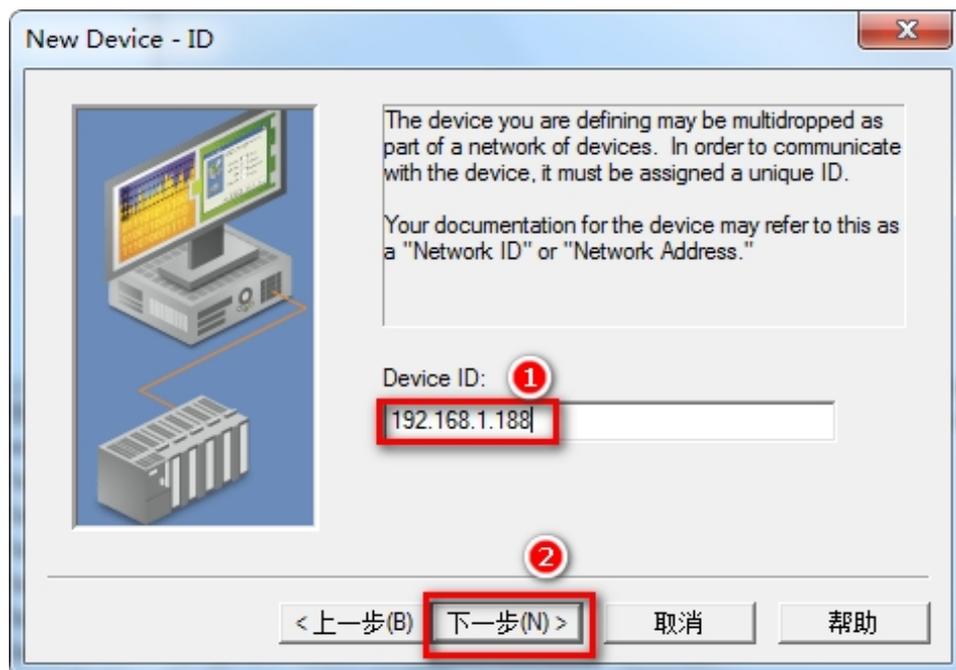
1、增加设备，填入设备名称，点击【下一步】；



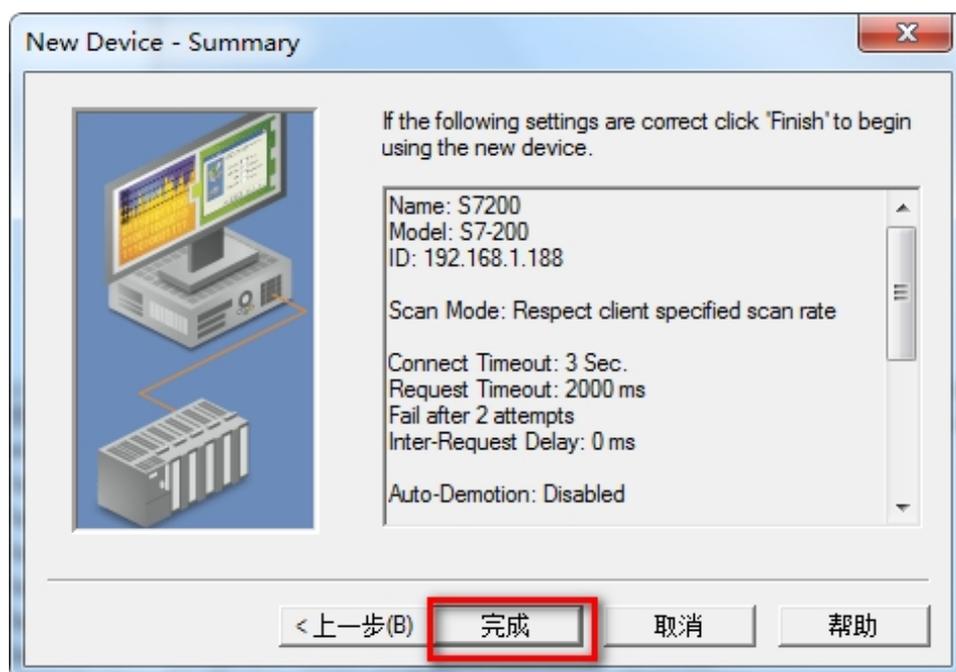
2、【Device model】选择 S7-200;



3、【Device ID】填入模块的 IP 地址，点击【下一步】;

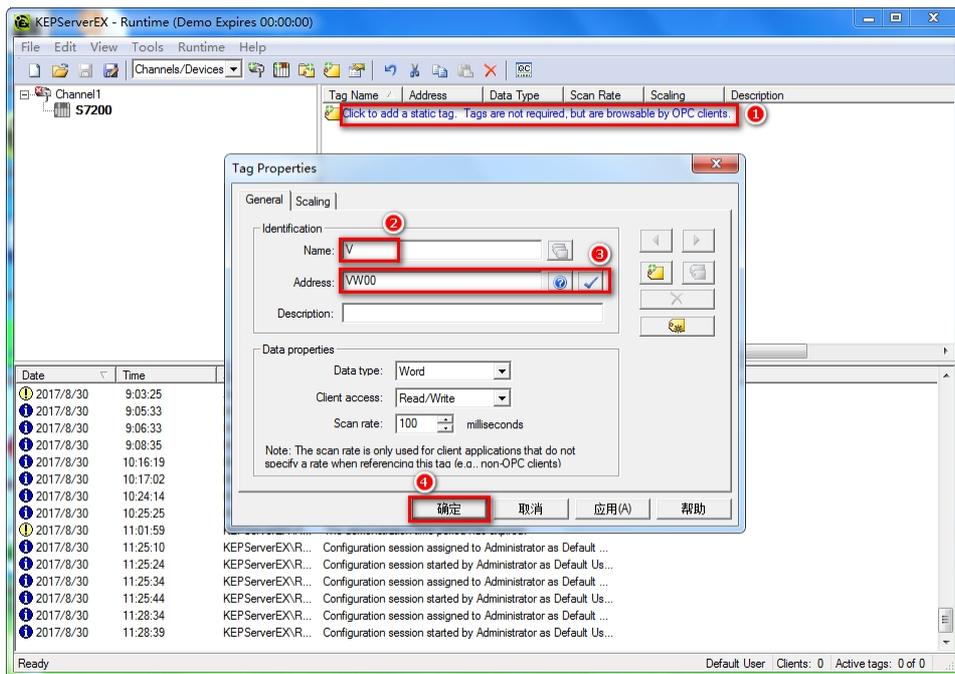


4、依照向导完成设置。



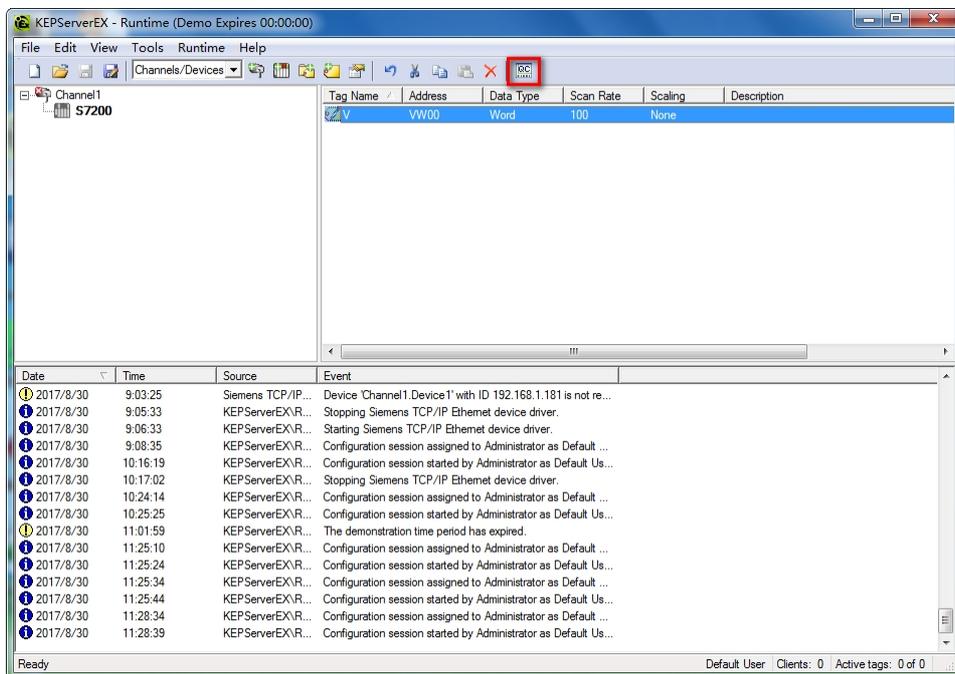
### 7.1.1.3 添加标签

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。

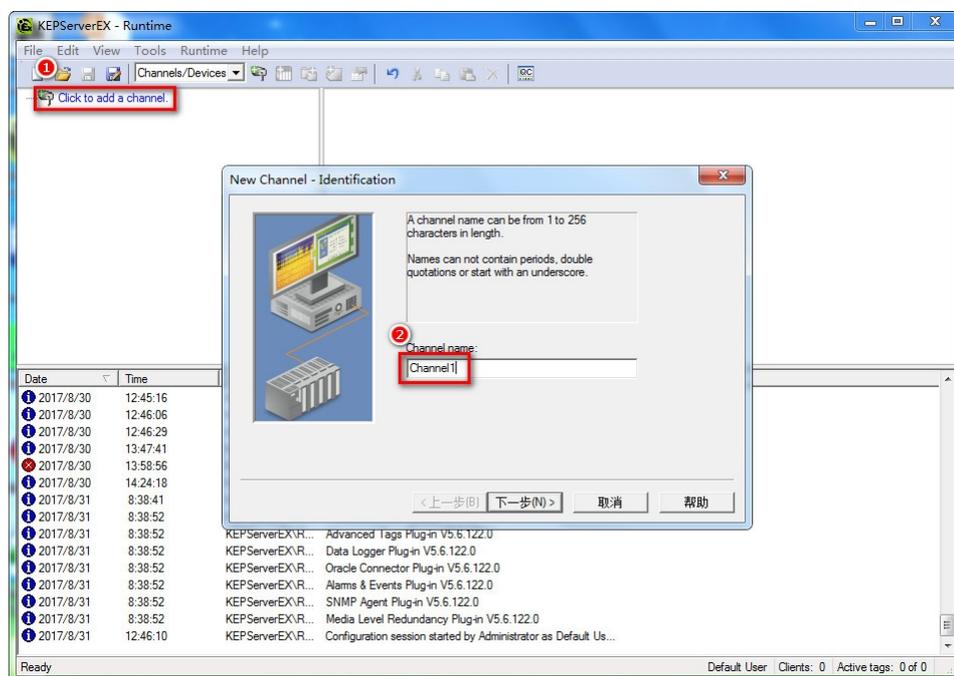


### 7.1.2 TK 6000-MT 模块连接 S7300

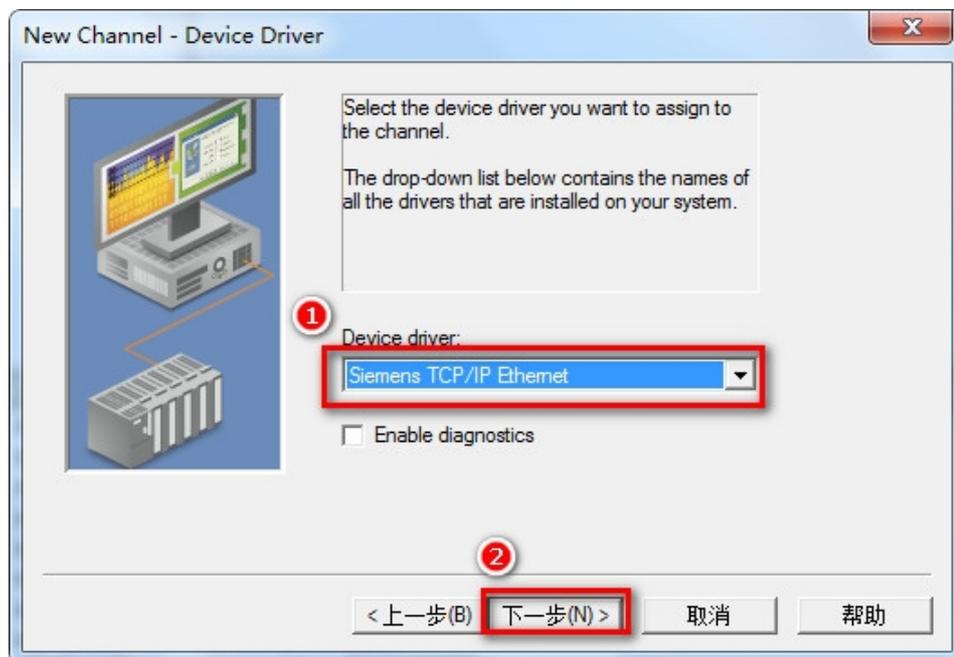
西门子 S7-300/400 通过模块连接 KepWare OPC，可以采用西门子 S7TCP 驱动。

## 7.1.2.1 添加通道

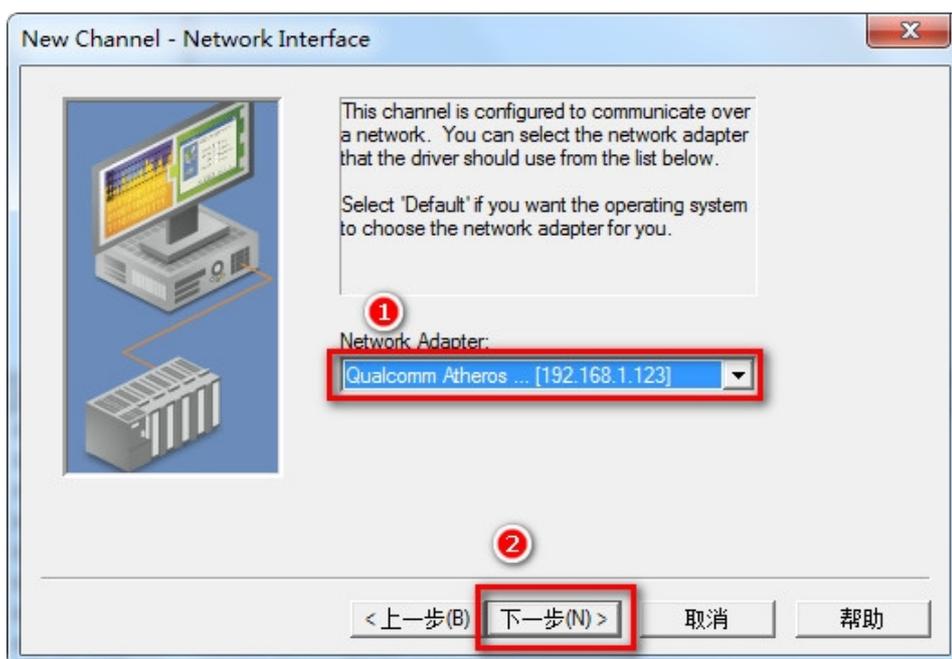
1、打开 Kepware OPC Configuration，增加一个通道，填入通道名称，点击【下一步】；



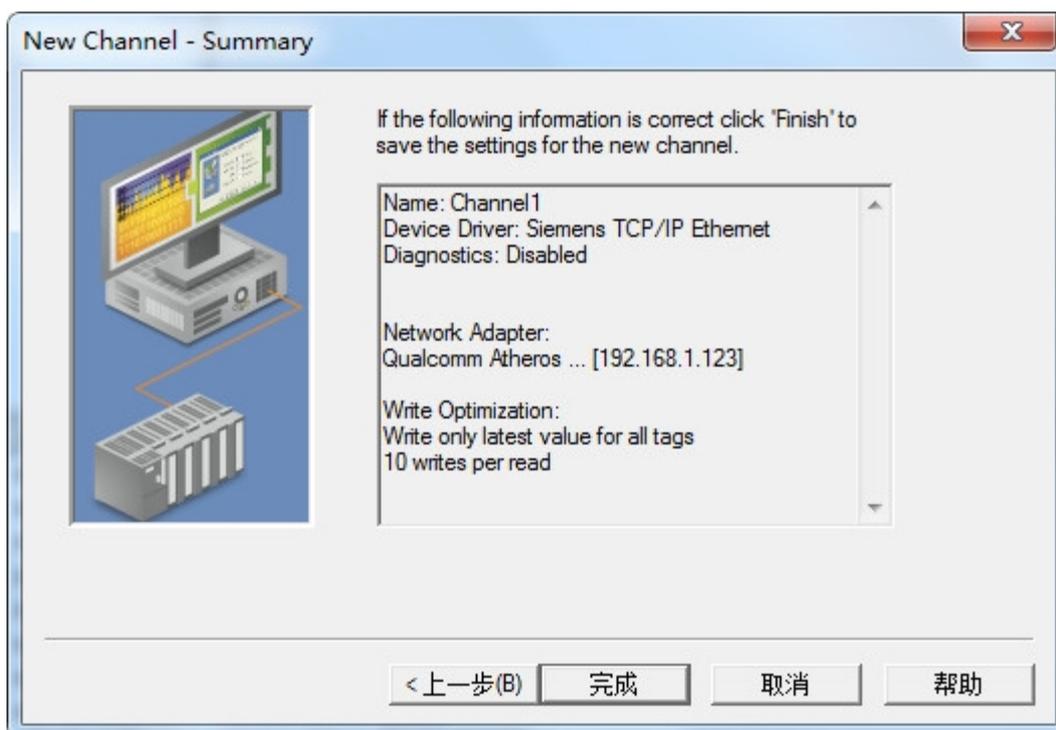
2、选择【Siemens TCP/IP Ethernet】驱动，点击【下一步】；



3、【Network Adapter】选择计算机网卡；

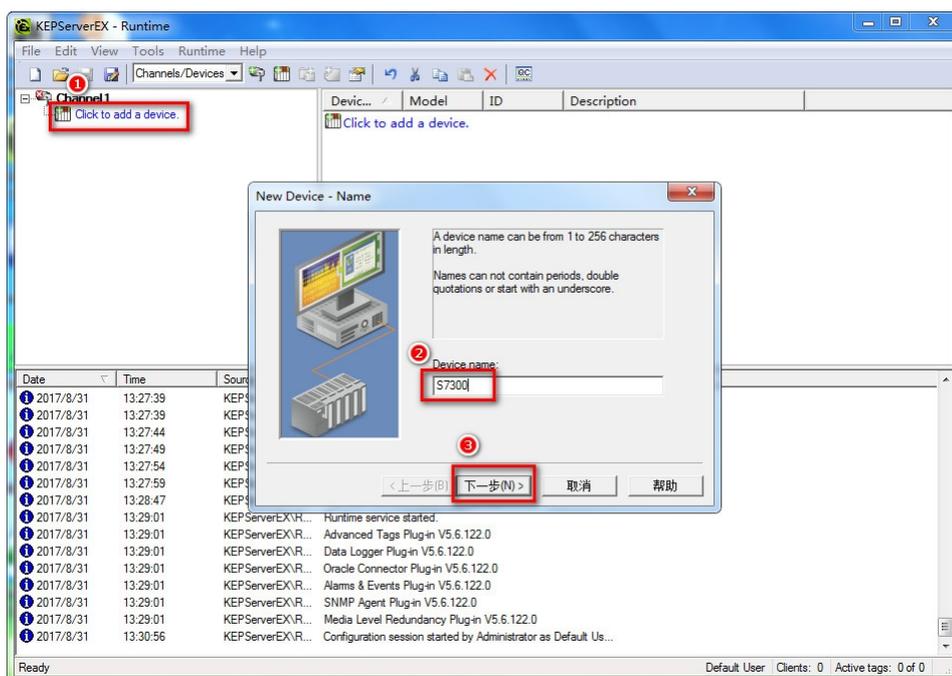


4、根据需要选择模式（可默认），完成通道参数设置；

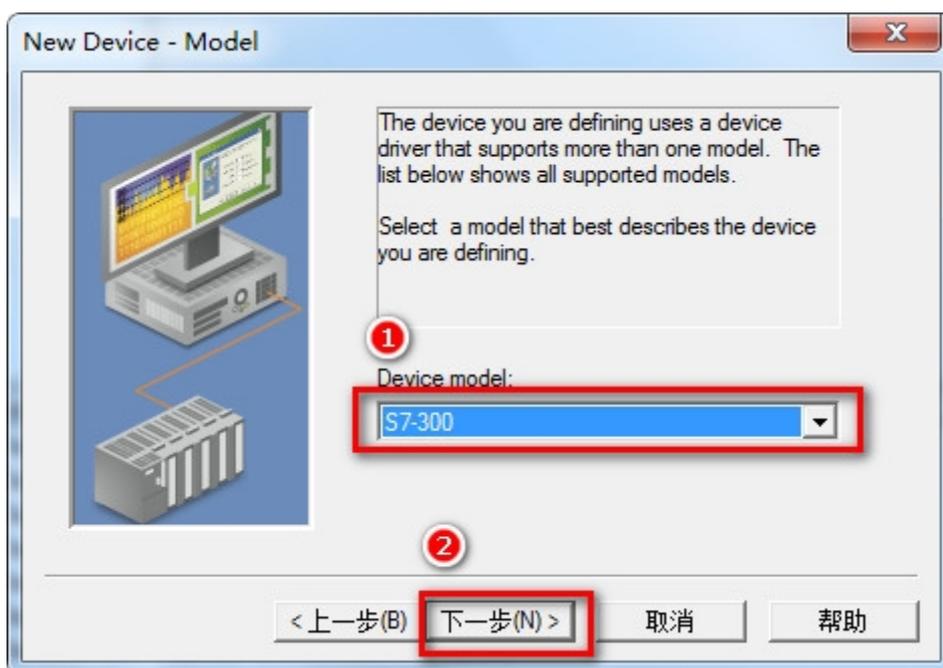


### 7.1.2.2 添加设备

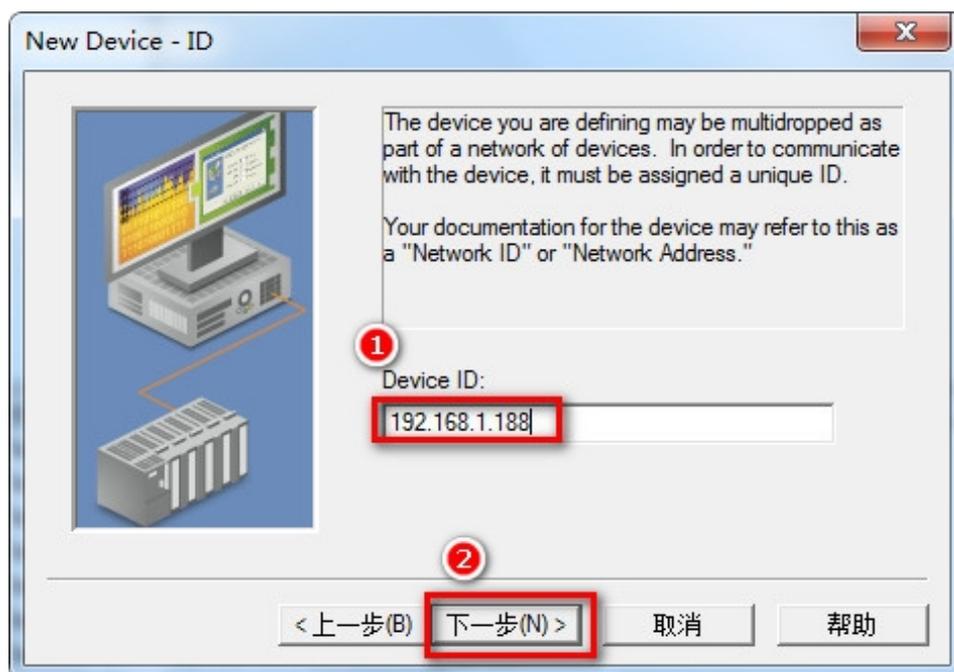
1、增加设备，填入设备名称，点击【下一步】；



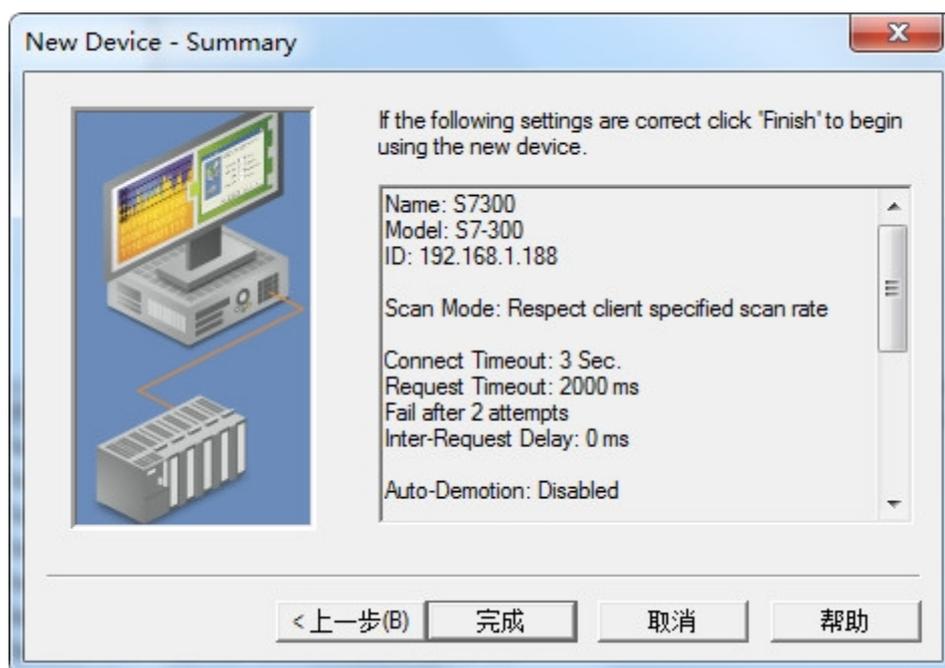
2、【Device model】选择 S7-300，下一步；



3、【Device ID】填入模块的 IP 地址，下一步；

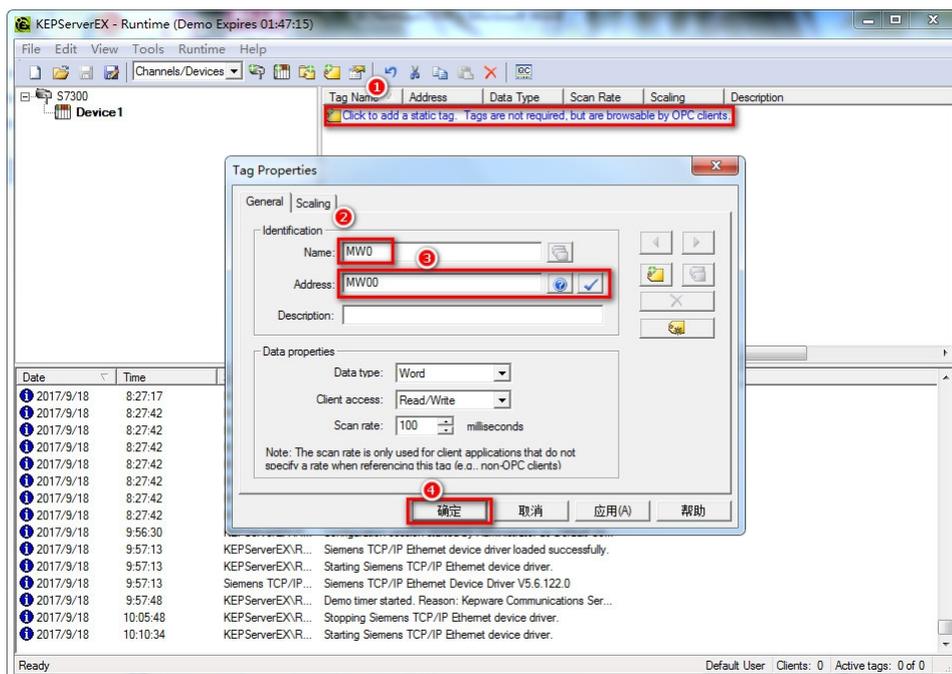


4、其他参数可以默认，完成设备设置。



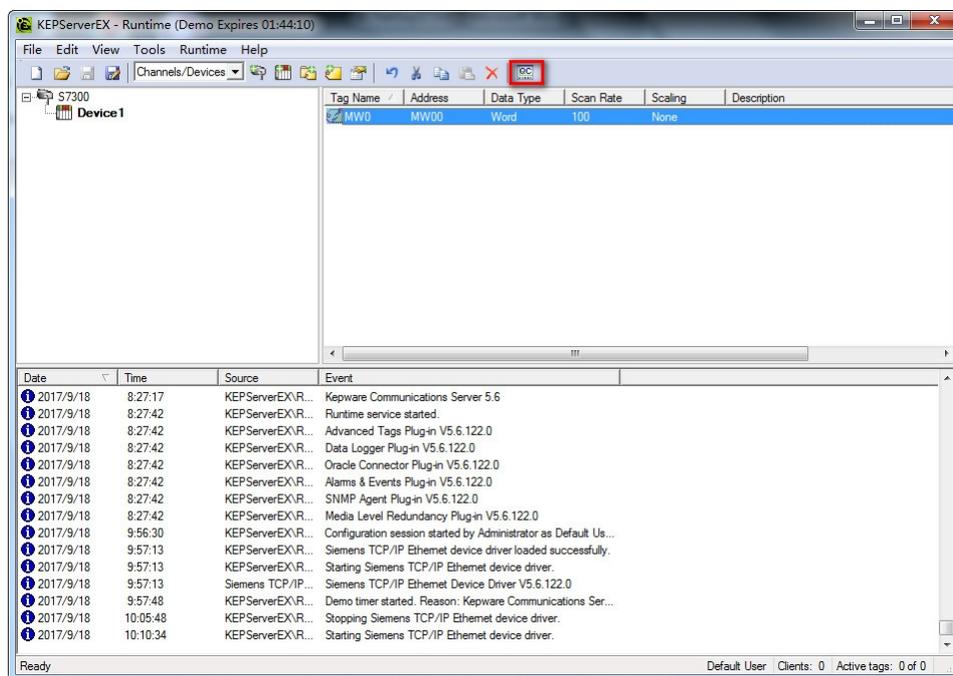
### 7.1.2.3 添加变量

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

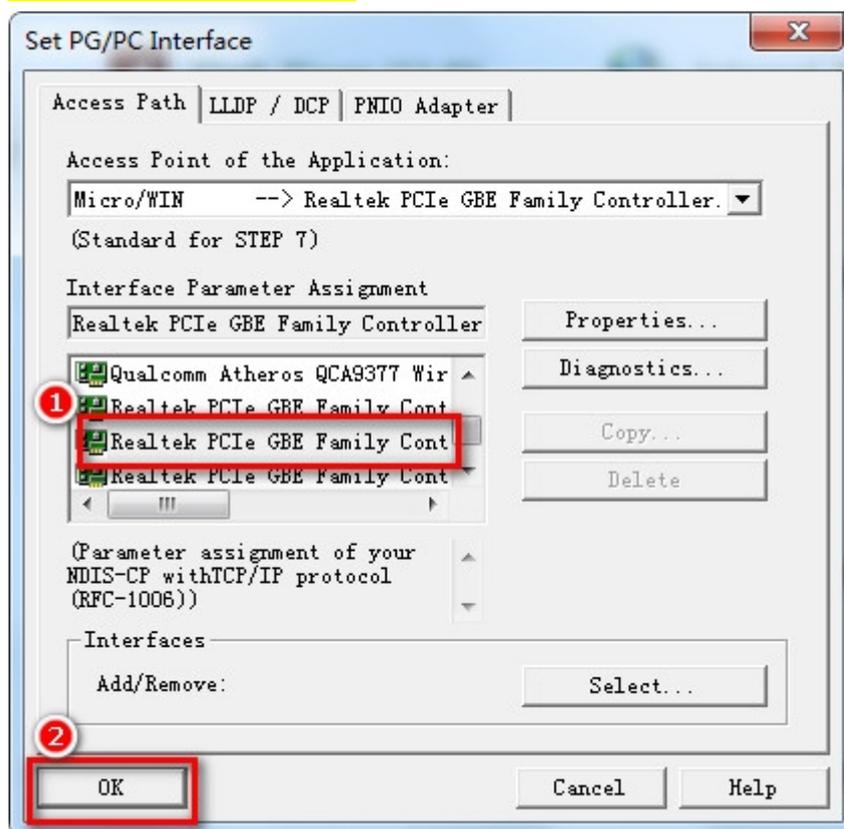
- 1、在 OPC 客户端验证通讯。



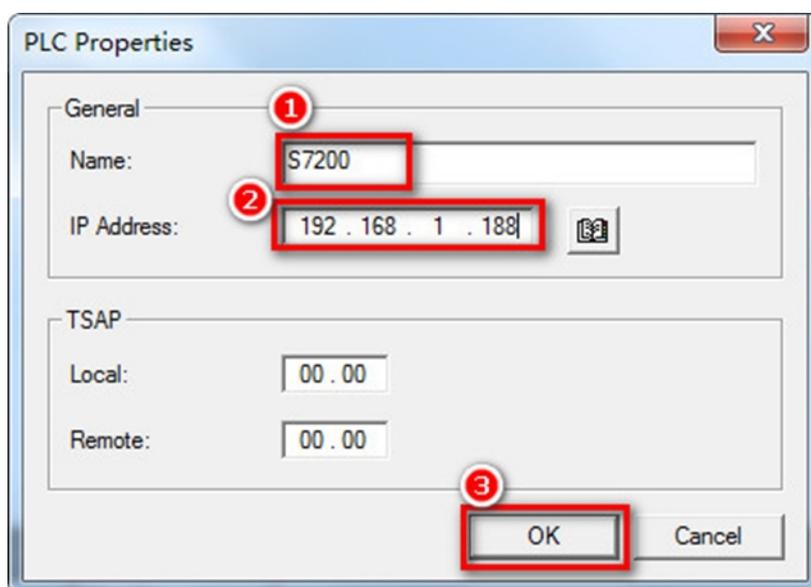
## 7.2 TK 6000-MT&PT&PB 模块 PC Access 通讯

- 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；

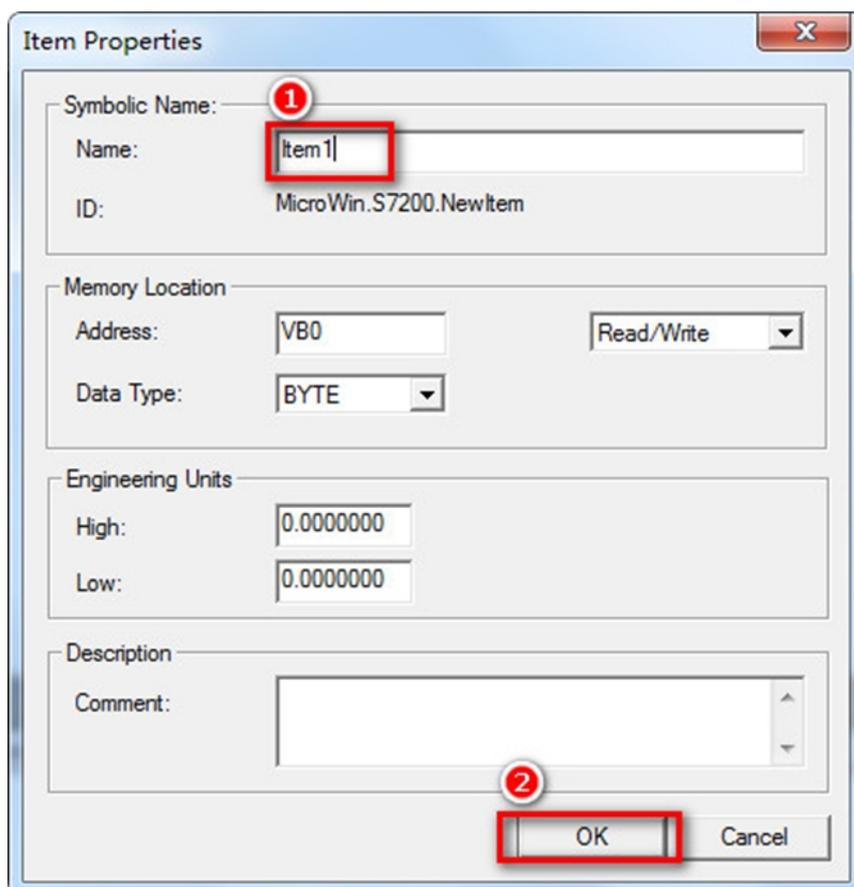
注：不要选带 auto 的网卡。



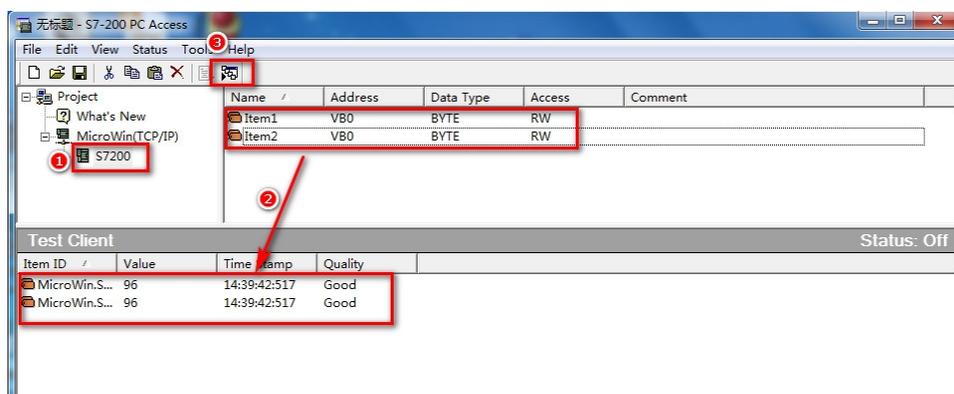
2、打开 S7-200 PC Access 软件,右击 Project 组下的【MicroWin (TCP/IP)】新建一个 PLC 连接,填入模块的 IP 地址, 点击【OK】:



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；

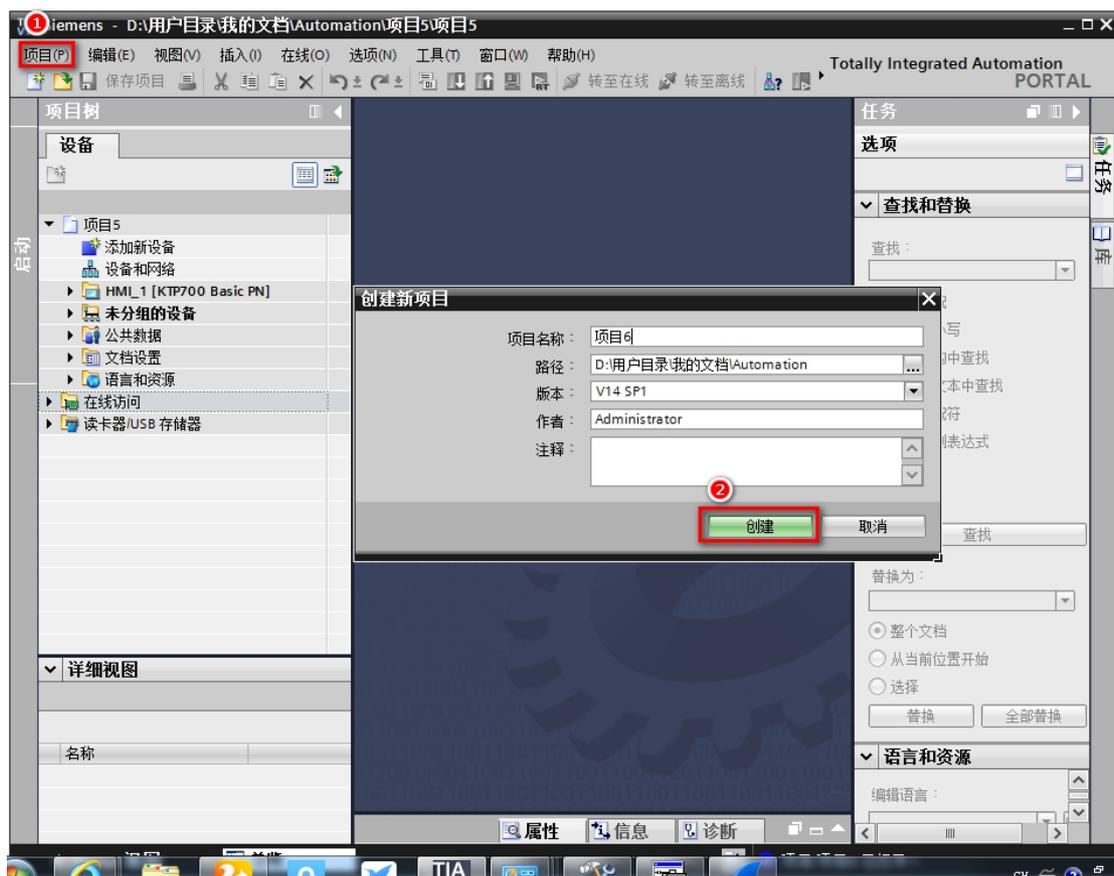


## 8. TK 6000-MT&PT&PB 模块触摸屏以太网通讯

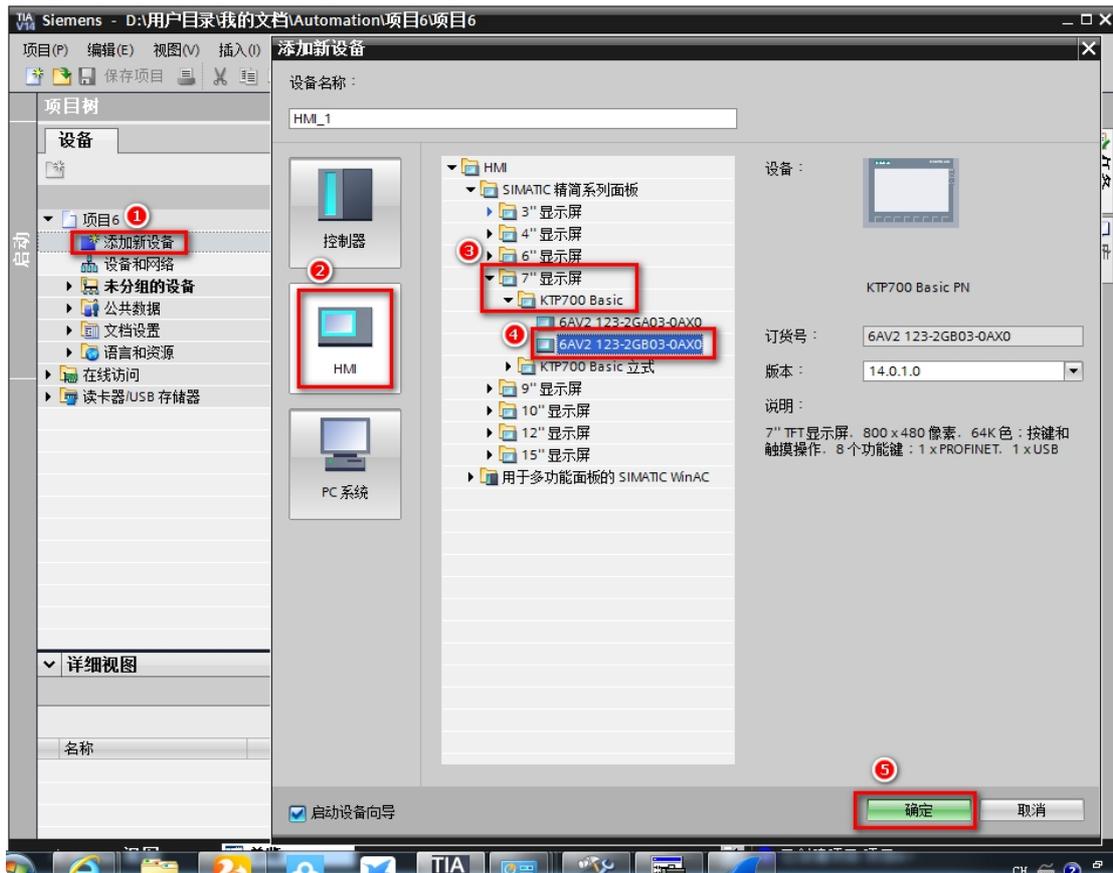
### 8.1 西门子 KTP/TP 系列触摸屏通讯

TK 6000-MT&PT&PB 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。

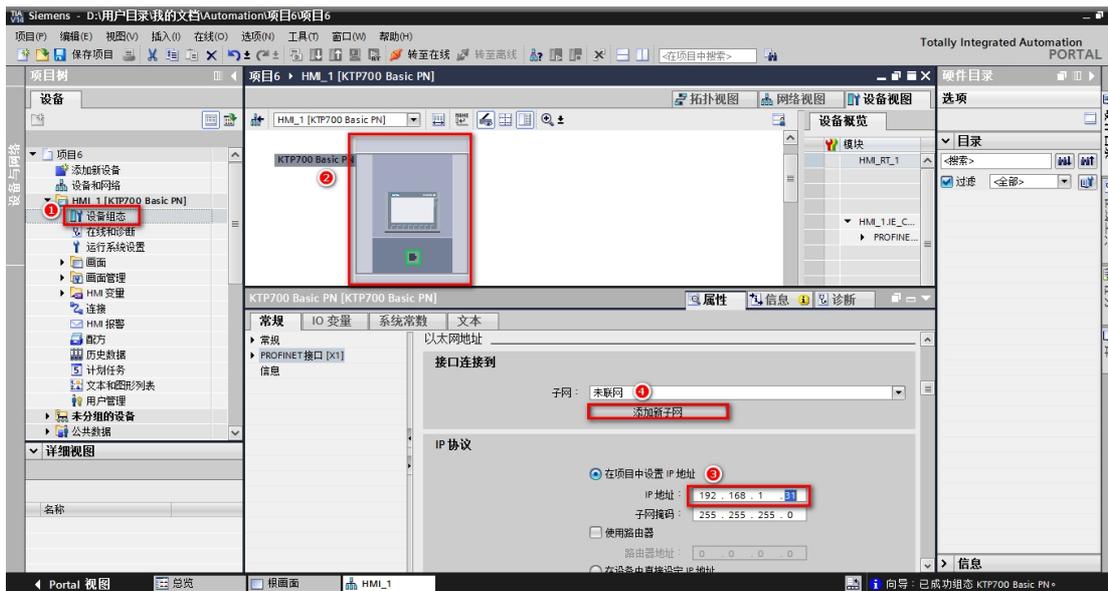
1、新建项目；



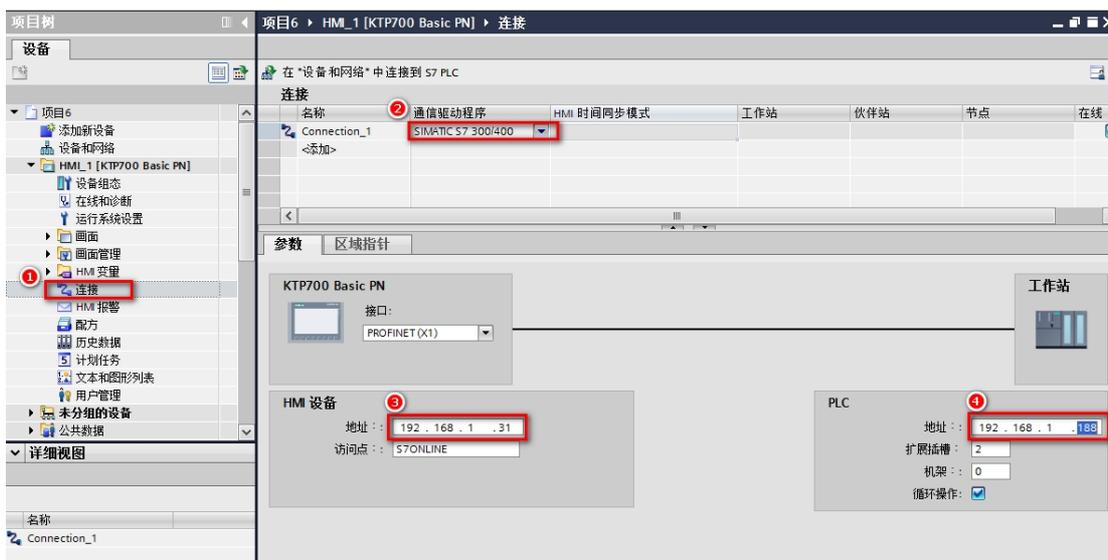
2、添加触摸屏设备；



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



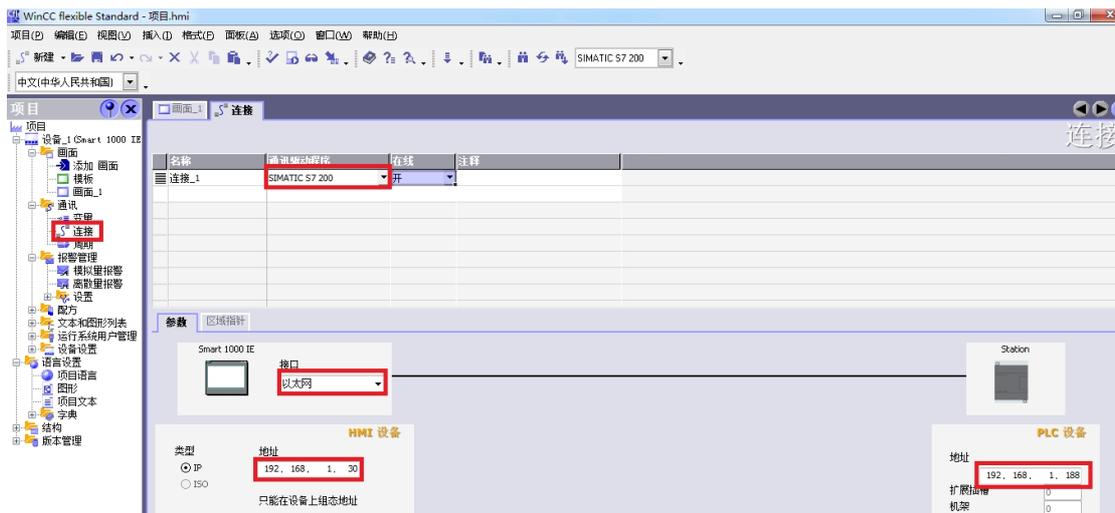
4、新建【连接】，在【通信驱动程序】中选择 SIMATIC S7 300/400，在【HMI 设备】-【地址】填入触摸屏的 IP 地址，在【PLC】-【地址】填入 TukBest 模块的 IP 地址。



## 8.2TK 6000-MT&PT&PB 模块西门子 SmartIE 系列触摸屏连 S7300

SmartIE 触摸屏通过模块可以实现与西门子 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】输入模块的 IP 地址；



### 3.建立变量

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

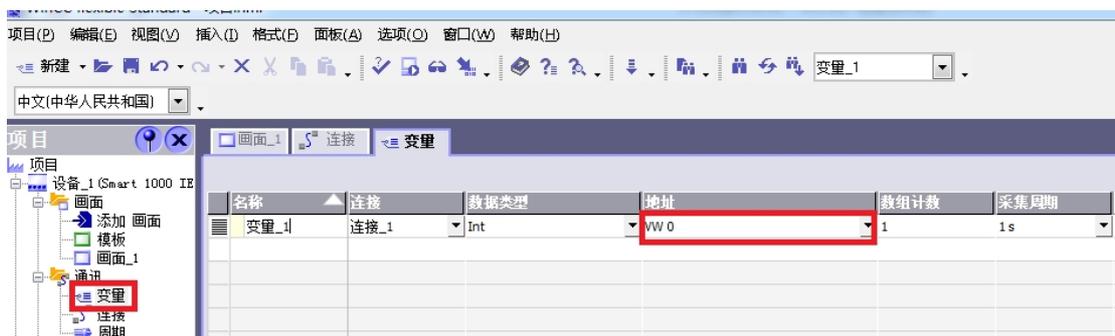
注意：软件中新建的变量与 PLC 的数据区对应关系：

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. TK 6000-MT&PT&PB 模块 ModbusTCP 通讯

TK 6000-MT&PT&PB 模块模块内集成 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 TukBest 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：

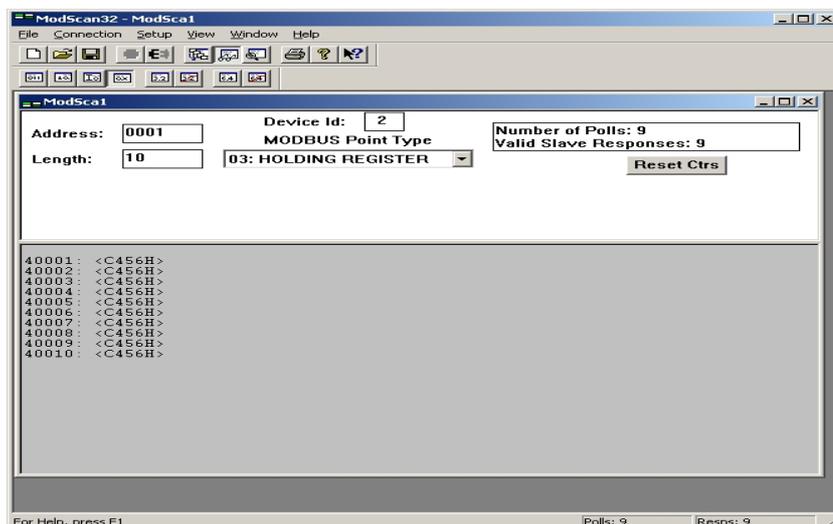
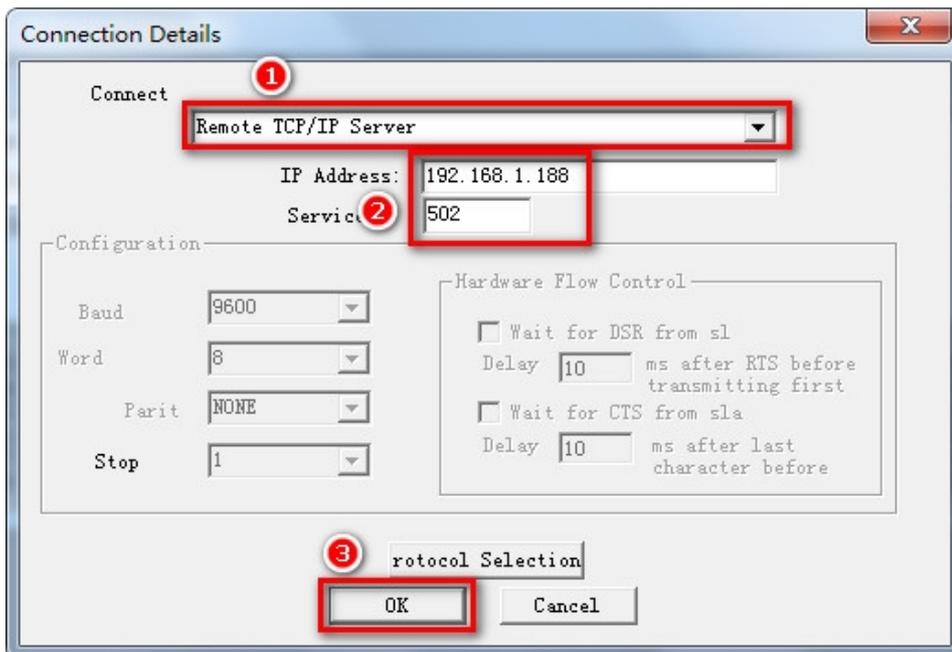
事务处 理标识 符	事务处 理标识 符	协 议 标 识 符	协 议 标 识 符	长度字段 (高字节)	长度字段 (低字节)	从站 地址	功 能 号	数据地址 (高字节)	数据地址 (低字节)	指 令 数 ( 高 字 节)	指 令 数 ( 低 字 节)
0x0	0x0	0x0	0x0	0x0	后面的字 节数						

## 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	$Qm.n = 00001 + m*8 + n$	FC1 (读线圈)	S7-200: 119 S7-300: 784
				FC5 (写线圈)	1
10001~	I0.0~	位	$Im.n = 10001 + m*8 + n$	FC2 (读输入)	S7-200: 119 S7-300: 784
30001~	MW0	字 (2 字节)	$MWm = 30001 + m/2$ , $m$ 为偶数	FC4 (读输入寄存器)	S7-200: 16 S7-300: 111
40001~	DBx.DBW0	字 (2 字节)	$DBx.DBWm = 40001 + m/2$ , $m$ 为偶数 ( $x$ 由参数指定, S7-200 的 V 区为 DB1) (见 <a href="#">S7 总线接口参数</a> )	FC3 (读乘法寄存器)	111
				FC16 (写乘法寄存器)	
				FC6 (写单一乘法寄存器)	1

## 9.2 ModScan32 测试

1. 运行 ModScan32 软件。
2. 选择菜单 Connection/Connect, 选择 Remote TCP/IP Server, 输入模块的 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。



## 10.TKNetS7 协议规范

### 10.1 通讯模式

TukBest 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 TukBest 并向其发送和接收数据来实现与 S7PLC 的通讯。TukBest 协议的服务端口号为 1099。

### 10.2 报文定义

TukBest 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. devi ce_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. functi on	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（TukBest 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 TukBest 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	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	8	msg. device_adr	byte	远程 (PLC) 站地址 0-31

展报文头	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

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	16~	msg. d[0~（写入	byte array	写入的数据

200 字节)	16+(写入数据字节数-1)	数据字节数-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_addr	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_addr	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：TukBest 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 字节报文头	0	msg. rx	byte	0xFF
	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 Q0 (0x0000), 0x54 的高 4 位 (=5) 为位偏移;

## 10.10 写 DB、M、I、Q 的位值

注：TukBest 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 Q0 (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。

## 附录：技术参数

产品型号	TK 6000-PT&PB
描述	西门子 S7-200 以太网通讯处理器
颜色	金属黑
状态显示	<u>Pwr</u> , Bus
以太网接口	Link/Active 指示灯, 线序自适应
接口类型	RJ45 母插座
传输速率	10/100Mbps
协议支持	西门子 S7TCP、 <u>ModbusTCP</u> 、OPC、TCP/IP 协议开放
TCP 连接数	最大 32
S7 接口	RS485
接口类型	DSUB 九针公
传输速率	9.6K、19.2K、187.5K, 波特率自适应
协议支持	PPI
人机接口	RS485
接口类型	DSUB 九针母
传输速率	9.6K、19.2K、187.5K
协议支持	S7 单主站协议
人机类型	西门子、MCGS、威纶、台达、步科等
编程软件	<u>MicroWIN</u>
组态软件	<u>WinCC</u> 、昆仑通态、组态王、力控、杰控、IFIX、INTOUCH、LABVIEW 等
OPC 软件	<u>KepWare OPC</u> 、TKNetS7 OPC
诊断和参数设置工具	IE 浏览器, 默认 192.168.1.188、 <u>TKNetPro</u> 、 <u>TK Device</u>
供电方式	PLC 通讯口直接取电
电压类型	24VDC/100mA
工作温度	0~60℃
工作湿度	95%非凝露
安装方式	即插即用
电磁兼容性	2014/30/EU
认证	CE 认证
尺寸 (L*W*H)	65*30*17mm
重量	60g

产品型号	TK 6000-MT
描述	西门子 S7-200/300/400 以太网通讯处理器
颜色	金属黑
状态显示	<u>Pwr</u> , Bus
以太网接口	Link/Active 指示灯, 线序自适应
接口类型	RJ45 母插座
传输速率	10/100Mbps
协议支持	西门子 S7TCP、 <u>ModbusTCP</u> 、OPC、TCP/IP 协议开放
TCP 连接数	最大 32
S7 接口	RS485
接口类型	DSUB 九针公
传输速率	9.6K、19.2K、187.5K、500K、1.5M、3M、6Mbps, 波特率自适应
协议支持	PPI/MPI/PROFIBUS
人机接口	RS485
接口类型	DSUB 九针母
传输速率	9.6K、19.2K、187.5K、500K、1.5M、3M、6Mbps
协议支持	S7 多主站协议
人机类型	西门子、MCGS、威纶、台达、步科等
编程软件	<u>MicroWIN</u> 、STEP7、博途
组态软件	<u>WinCC</u> 、昆仑通态、组态王、力控、杰控、IFIX、INTOUCH、LABVIEW 等
OPC 软件	<u>KepWare OPC</u> 、TKNetS7 OPC
诊断和参数设置工具	IE 浏览器, 默认 192.168.1.188、 <u>TK NetPro</u> 、 <u>TK Device</u>
供电方式	PLC 通讯口直接取电
电压类型	24VDC/100mA
工作温度	0~60°C
工作湿度	95%非凝露
安装方式	即插即用
电磁兼容性	2014/30/EU
认证	CE 认证
尺寸 (L*W*H)	65*30*17mm
重量	60g

南京图尔库智能科技有限公司

南京市浦口区泰西路 3 号金泰商务 4 层

电话：15996274156

传真：025-58193989

邮箱：[404357550@qq.com](mailto:404357550@qq.com)