RVNet-PN

西门子 SIMATIC®　S7 系列 PLC 以太网通讯处理器

使用手册

1.RVNet 产品简介

1.1 产品描述

RVNet 是一款高性能协议转换网关，是为满足日益增多的工厂设备信息化需求（设备网络监控和生产管理）而设计，用于西门子自带以太网接口的 PLC（S71200、S71500、S7300、S7200Smart 等）和西门子以太网模块（CP243-1、CP343-1 等）的以太网数据采集，非常方便构建生产管理系统。

RVNet 具备两个物理性接口，LAN1 和 LAN2 口分别具备独立的局域网能力。其中 LAN1 口为一个双 RJ45 接口，具备交换机功能，主要用于连接 PLC；LAN2 口为单端口 RJ45，主要用于上位机采集或者触摸屏的连接；

RVNet 可以实现近似于 NAT 的地址转换的功能，即可将 LAN1 口所连接 PLC 的 IP 地址和端口号，映射到 LAN2 口任意 IP 地址和端口号；方便解决了现场设备无法修改 IP 地址和端口号的问题；

RVNet 设计时充分考虑了工业现场环境的复杂性，从抗干扰角度进行了全方位的硬件设计，采用高性能工业级芯片、大容量 TVS、EMC 的 PCB Layout，这些赋予了 RVNet 强大工业应用能力。

1.2 功能简介

1、安装在 35mm 的导轨上，LAN1 为双端口的 RJ45，具备交换机功能，此端口连接 PLC；LAN2 为单端口 RJ45，可以连接触摸屏或上位机系统；RVNet 外接 24VDC 电源供电。
2、集成 WEB 服务器，通过网页可设置设备参数和运行诊断；也可以通过 NetDevice 工具进行配置；可以任意从 LAN1 或 LAN2 口进行配置。
3、实现 NAT 功能，将 LAN1 口所连接 PLC 的 IP 地址和端口号，映射到 LAN2 口的任意 IP 和端口号；
4、可实现 SmartIE 系列触摸屏连接 S71200、S71500 等 PLC；
5、LAN2 口可支持 ModbusTCP 服务器功能，可以将 LAN1 口连接的 PLC 映射成 LAN2 口的 ModbusTCP 服务器；
6、LAN2 口可支持 RVNetS7 协议服务器功能，可以将 LAN1 口连接的 PLC 映射成 LAN2 口的 RVNetS7 协议服务器，方便使用 RVNetOPC 功能；
7、支持可达 32 个的 LAN2/LAN1 的服务器/客户机并发模型，LAN2 口最多可支持 32 个上位机访问；
8、采用 RVNetS7 协议或者 ModbusTCP 的方式，皆可实现高级语言（如 VB、VC、C#等）编程，实现与 PLC 的数据通讯，方便开发生产管理系统。
9、支持 OPC 通道的 SCADA（上位组态软件）以 OPC 方式与 PLC 通讯。
10、支持用户侧通过以太网实现固件更新，免费提供集成更多功能的固件，一次购买硬件，永久升级。

2.RVNet 功能应用

功能一：编程调试

RVNet 模块支持对 PLC 控制系统的编程调试。详见《第五章：编程调试》。

功能二：SCADA 以太网通讯

RVNet 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、力控、杰控、等。详见《第六章：SCADA 以太网通讯》。

功能三：OPC 通讯

RVNet 模块支持和市面上主流的 OPC Server 以太网通讯，例如：KEPWARE OPC。详见《第七章：OPC 通讯》。

功能四：触摸屏以太网通讯

RVNet 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 S71200/1500、威纶通、步科等。详见《第八章：触摸屏以太网通讯》。

功能五：ModbusTCP 通讯

RVNet 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：NAT 地址转换

RVNet 可以实现近似于 NAT 的地址转换的功能，即可将 LAN1 口所连接 PLC 的 IP 地址和端口号，映射到 LAN2 口任意 IP 地址和端口号；方便解决了现场设备无法修改 IP 地址和端口号的问题。详见《第十章：NAT 地址转换》。

3.RVNet 安装、诊断

3.1 安装

1、将 RVNet 模块安装在 35mm 导轨上，并外接 24VDC 电源供电；
2、用一根网线连接 RVNet 模块的 LAN1 和 PLC；
3、用一根网线连接 RVNet 模块的 LAN2 和电脑。

3.2 诊断

1、RVNet 模块的红色电源指示灯 Pwr 灯将立即常亮；
2、正常通讯时，绿色 LAN1 和 LAN2 指示灯都将快速闪烁；

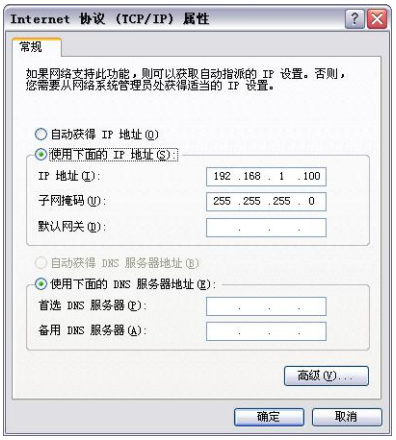
4.RVNet 参数设定

当需要对 RVNet-PN 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，我们通过 RVNet-PN 的 LAN2 口进行参数设定，只要保证 RVNet-PN 的 LAN2 口的 IP 地址和电脑的 IP 地址在同一网段。

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 的出厂 IP 地址），然后按回车键，浏览器应能显示 RVNet 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。

以太网连接及映射信息：显示当前模块以太网连接的 PLC 信息与状态、跨网段的映射信息。

以太网接口参数及功能设定：显示当前模块 LAN1 和 LAN2 接口的参数、LAN2 接口的功能设定。

4.1.1 LAN1 接口参数

设置 RVNet-PN 的 LAN1 接口的 IP 地址、掩码和网关（即路由器的地址）；

DHCP 功能：默认为关闭；开启情况下将自动获取 LAN1 接口的 IP 地址、掩码和网关；

高级设置：

要连接的 PLC 的 IP 地址：LAN1 接口连接的 PLC 的 IP 地址；必须保证 LAN1 接口的 IP 地址与连接的 PLC 的 IP 地址在同一网段；

密码、确认密码：修改模块的登录密码。

4.1.2 LAN2 接口参数

设置 RVNet-PN 的 LAN2 接口的 IP 地址、掩码和网关（即路由器的地址）；LAN2 接口的 IP 地址与连接的 PLC 的 IP 地址不一定要在同一网段（IP 地址可设置为其他网段）。

DHCP 功能：默认为关闭；开启情况下将自动获取 LAN2 接口的 IP 地址、掩码和网关；

高级设置：

LAN2 转发端口 1：LAN2 口的 TCP 服务器端口号，默认为 102；

LAN2 转发端口 2：LAN2 口的 UDP 服务器端口号，默认为 1002；

ModbusTCP 端口号：默认为 502；

SmartIE 屏连接功能：决定 LAN2 口是否支持 SmartIE 屏连接 S71200、S71500，默认为启用。

SmartIE 屏 Mapping：只有当【SmartIE 屏连接功能】为开启状态时才有意义，V 区对应的 DB 块号的转换关系由此参数决定。

4.1.3 通讯诊断

LAN1 接口通讯——>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；
TCP/UDP 存在数：所有连接 LAN1 口的以太网客户机连接数；

LAN2 接口通讯——>通讯请求总数：计算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/UDP 存在数：所有连接 LAN2 口的以太网客户机连接数；

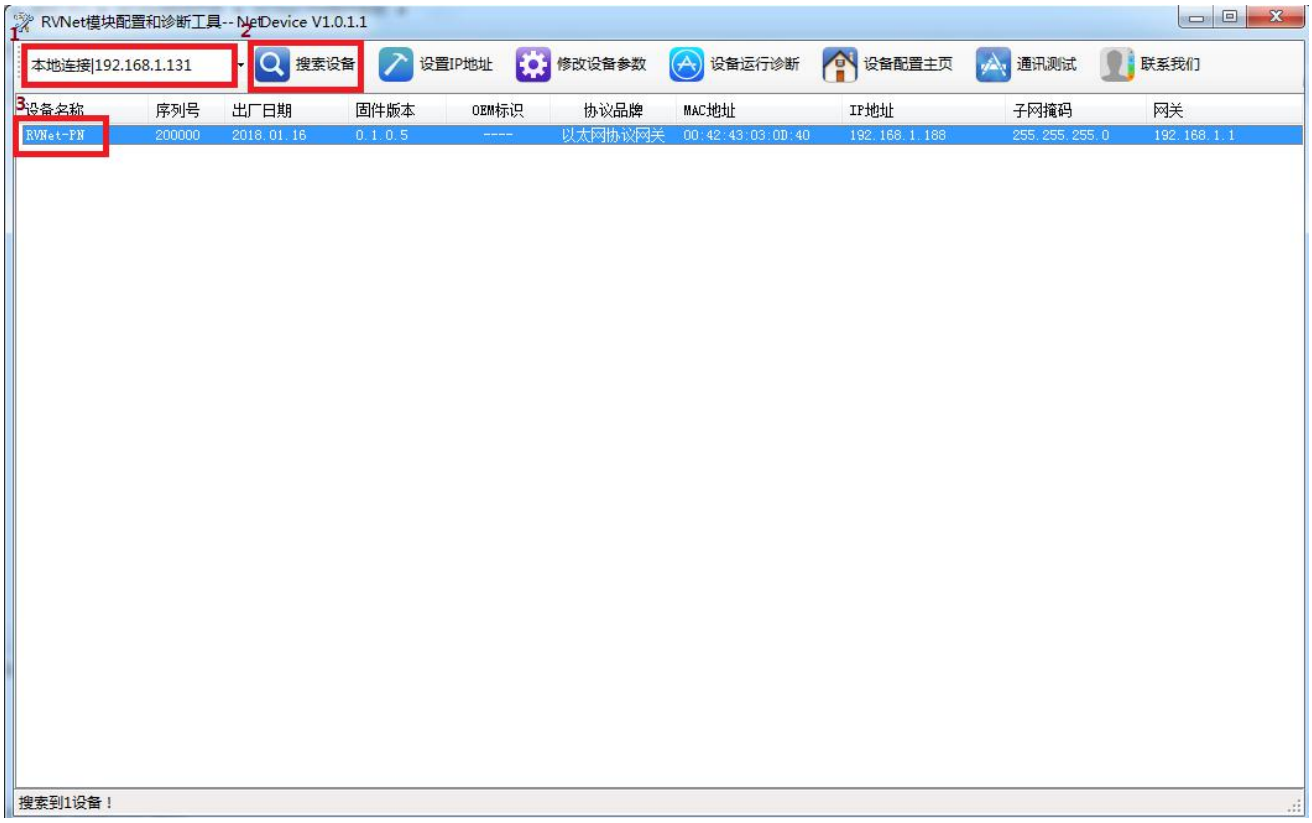
运行时间：RVNet 模块上电后的运行时间；

上次内部故障：RVNet 模块的系统故障，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 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【搜素设备】按钮，可以把网络上的 RVNet 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。

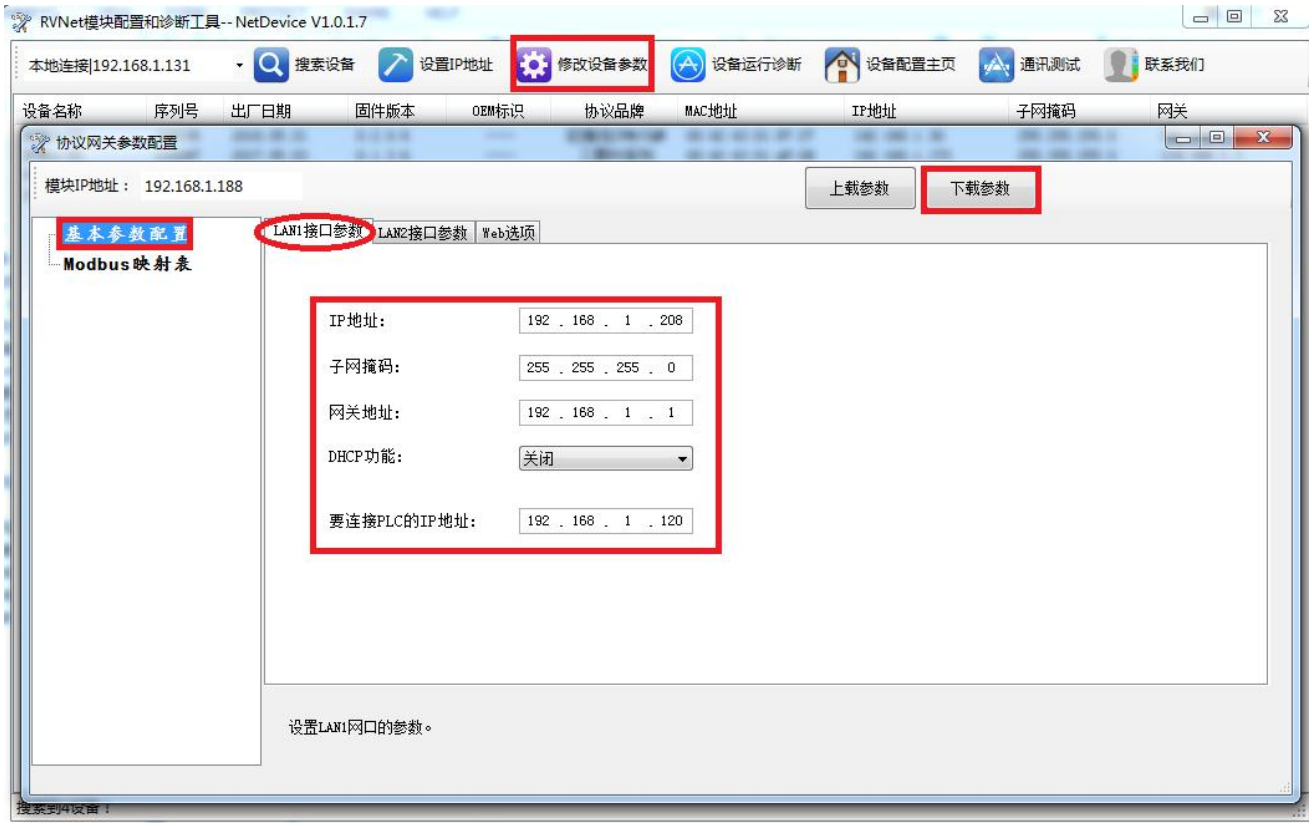
4.2.2 设置 IP 地址

首先，我们需要修改 RVNet 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

4.2.3.1 基本参数配置

1.点击【修改设备参数】按钮，在弹出的对话框中，可以查看【基本参数配置】——【LAN1 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 的 LAN1 接口的 ip 地址、子网掩码、网关。

DHCP 功能：默认为关闭；开启情况下将自动获取 LAN1 接口的 IP 地址、掩码和网关；

要连接 PLC 的 IP 地址：LAN1 接口连接的 PLC 的 IP 地址；必须保证 LAN1 接口的 IP 地址与连接的 PLC 的 IP 地址在同一网段。

2.点击【修改设备参数】按钮，在弹出的对话框中，可以查看【基本参数配置】——【LAN2 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 的 LAN2 接口的 ip 地址、子网掩码、网关。LAN2 接口的 IP 地址与连接的 PLC 的 IP 地址不一定要在同一网段（IP 地址可设置为其他网段）。

DHCP 功能：默认为关闭；开启情况下将自动获取 LAN2 接口的 IP 地址、掩码和网关；

LAN2 转发端口 1：LAN2 口的 TCP 服务器端口号，默认为 102；

LAN2 转发端口 2：LAN2 口的 UDP 服务器端口号，默认为 1002；

ModbusTCP 端口号：默认为 502；

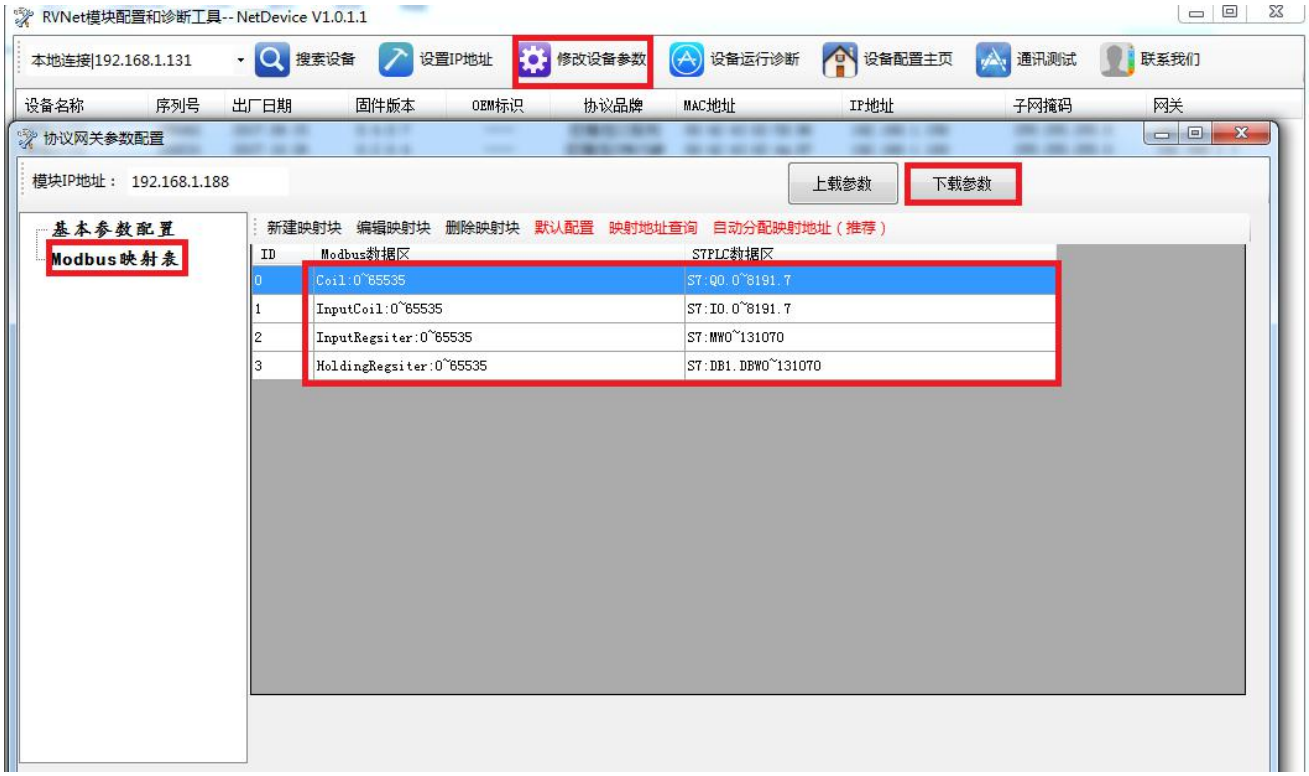
RVNetS7 协议端口号：默认为 1099。

SmartIE 屏连接功能：决定 LAN2 口是否支持 SmartIE 屏连接 S71200、S71500，默认为启用。

HMI_SmartIE_Mapping: 只有当【SmartIE 屏连接功能】为开启状态时才有意义，V 区对应的 DB 块号的转换关系由此参数决定。

4.2.3.2Modbus 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 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。

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
Coil 000001~	位	FC1（读线圈） FC5（写线圈）
Input 100001~	位	FC2（读输入）
InputRegsiter 300001~	字（2 字节）	FC4（读输入寄存器）
HoldingRegsiter 400001~	字（2 字节）	FC3（读保持寄存器） FC16（写保持寄存器） FC6（写单一保持寄存器）

◆ 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

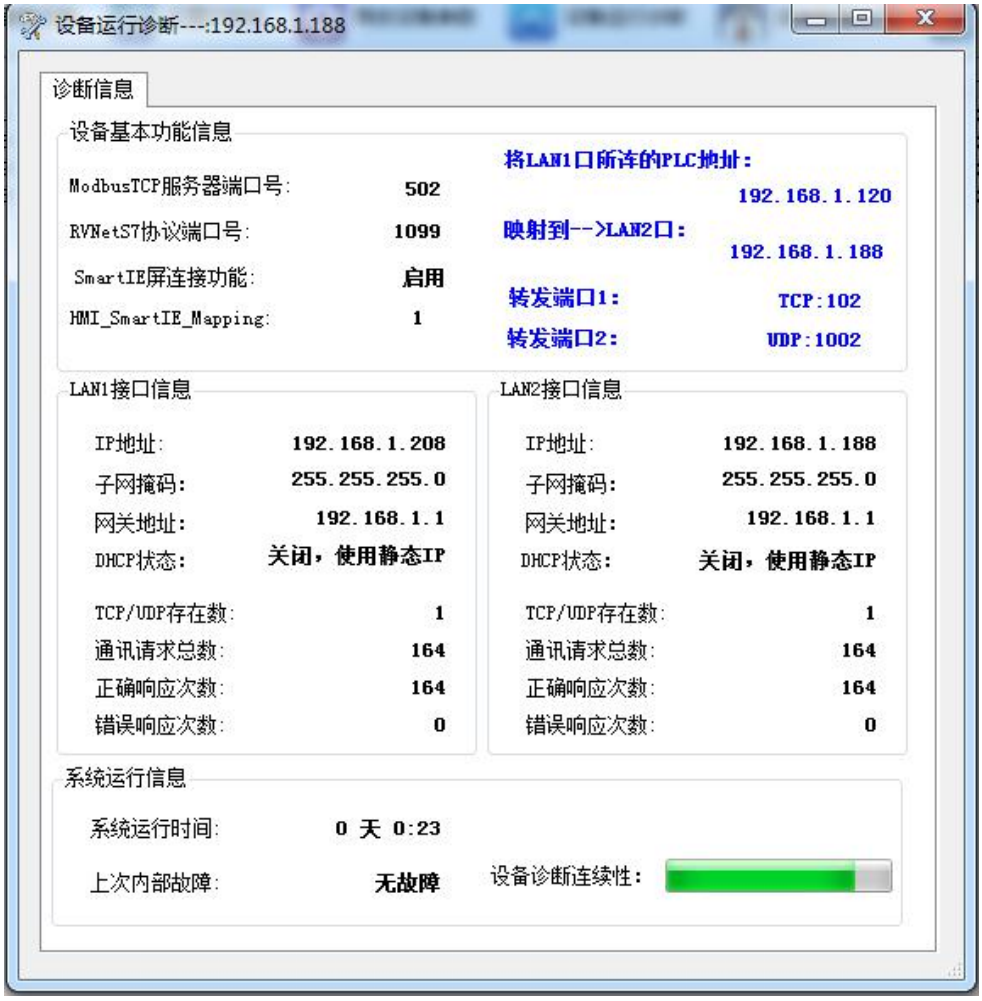
举例：只读 DB2.DBX10.0

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。

4.2.3.3 设备运行诊断

点击【设备运行诊断】按钮，可以查看 RVNet 模块当前的运行情况：设备基本功能信息、LAN1 接口信息、LAN2 接口信息、系统运行信息等。



4.2.3.4 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】。

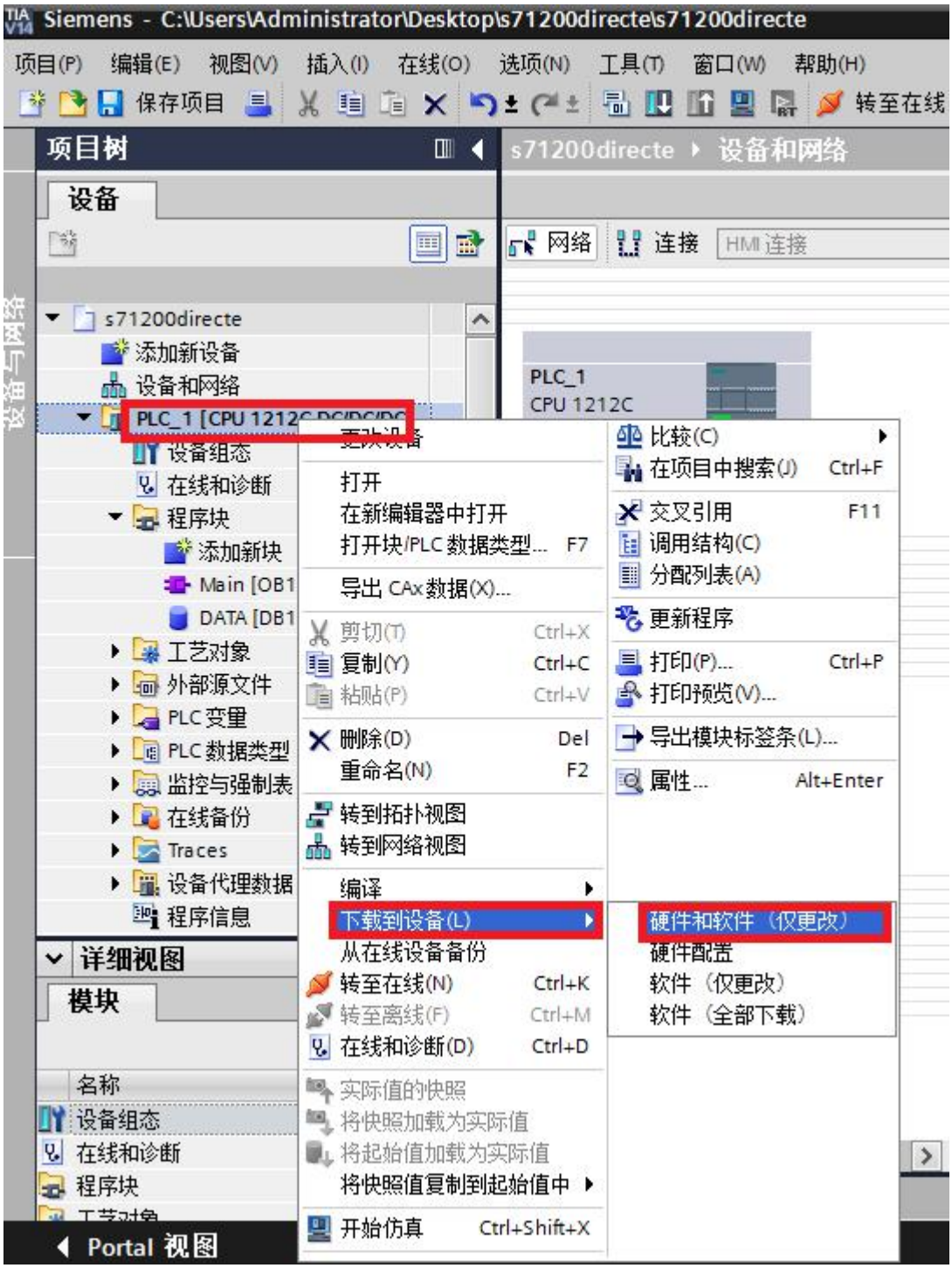
这里我们读取了 PLC 的 MB0 的数据，如果通讯正常，则会返回 MB0 的数据（最直观的方法：如果接收次数和正确次数一直是累加的话，表面通讯正常），可以借此来判断 RVNet 模块、PLC、上位机之间的以太网连接是否正常。

5.编程调试

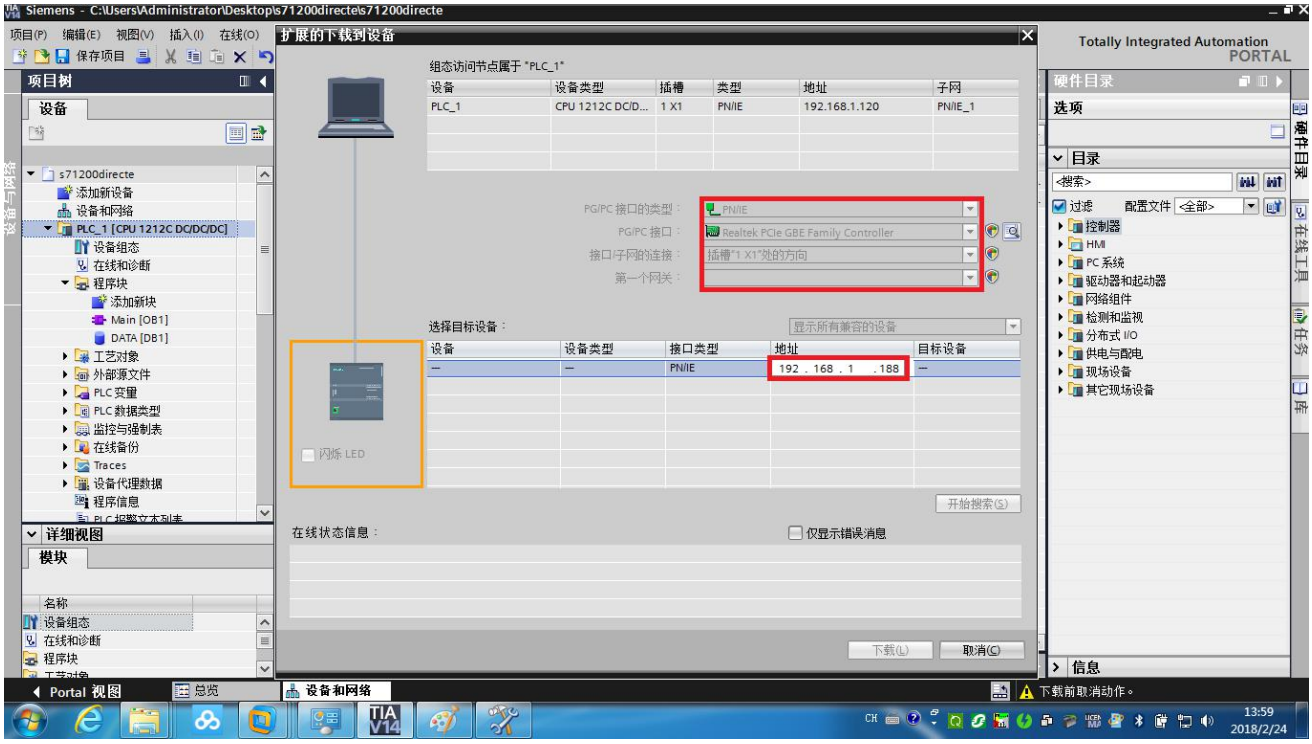
以下载 S7-1200PLC 的程序为例：

1.运行 TIA portal V14 软件并打开项目；

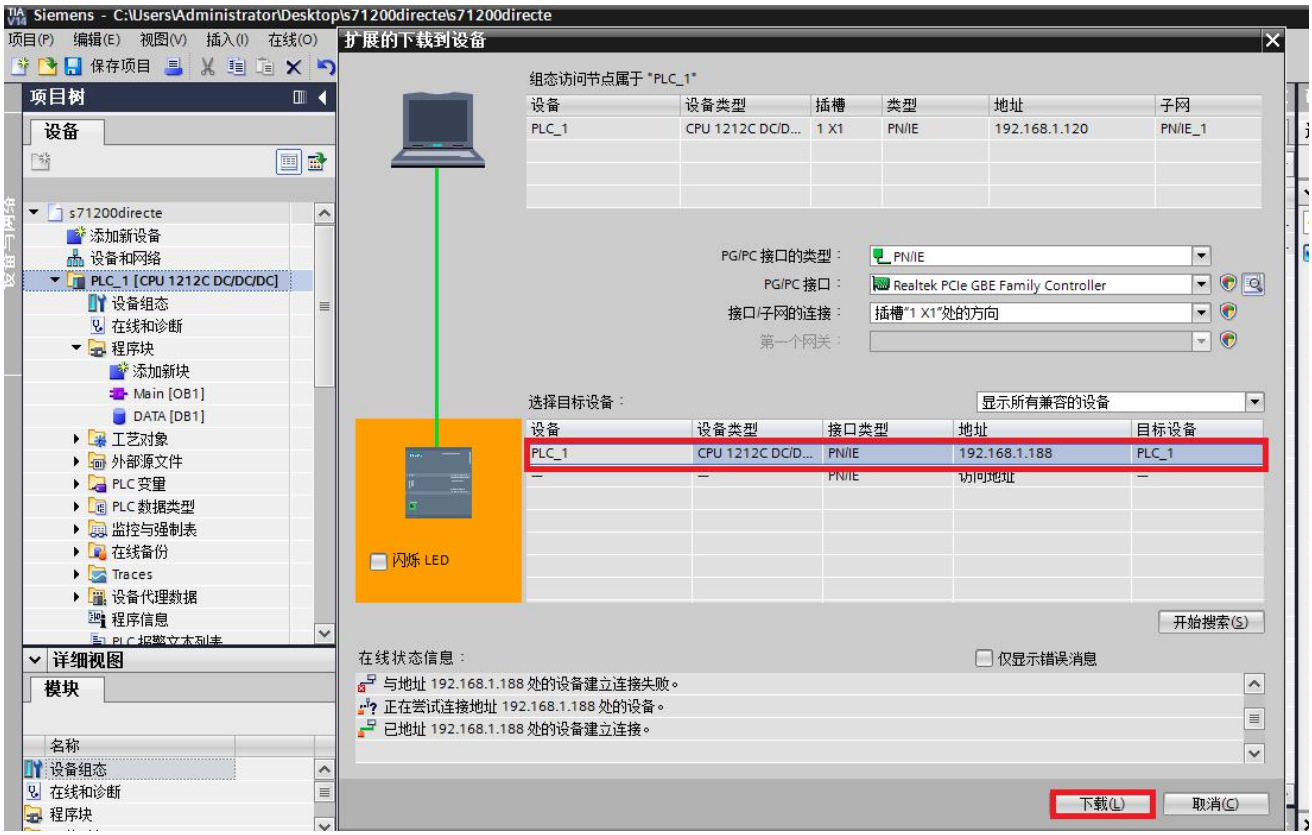
2.右击 PLC，选择【下载到设备】下的【硬件和软件（仅更改）】;



3.在【PG/PC 接口的类型】选择 PN/IE，【PG/PC 接口】选择你的计算机的网卡，在【访问地址】处手动填入 RVNet-PN 的 IP 地址，在空白处点击鼠标左键，即可搜索 PLC；



4.选中连接的 PLC，点击【下载】即可。

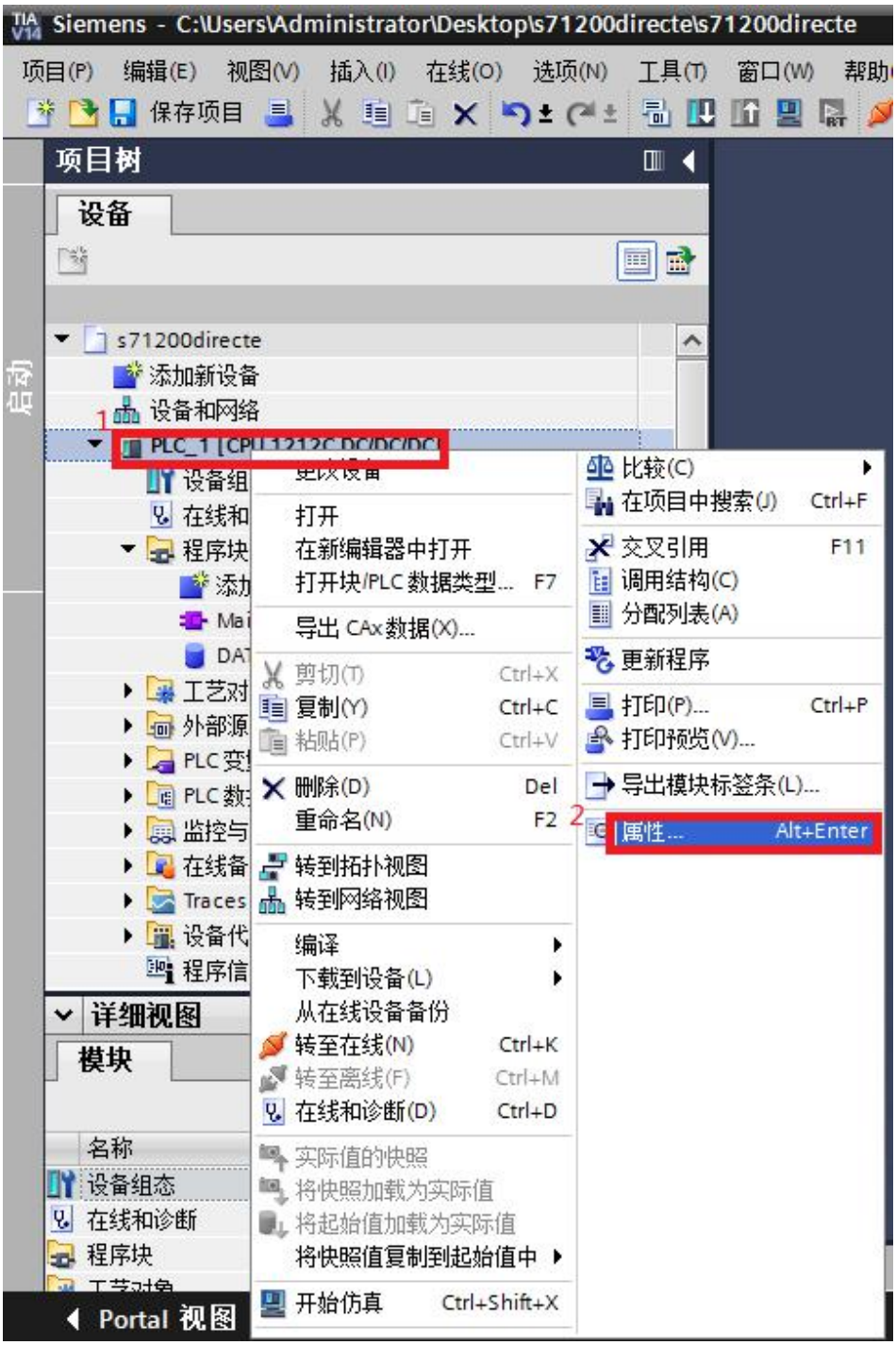


6.SCADA 以太网通讯

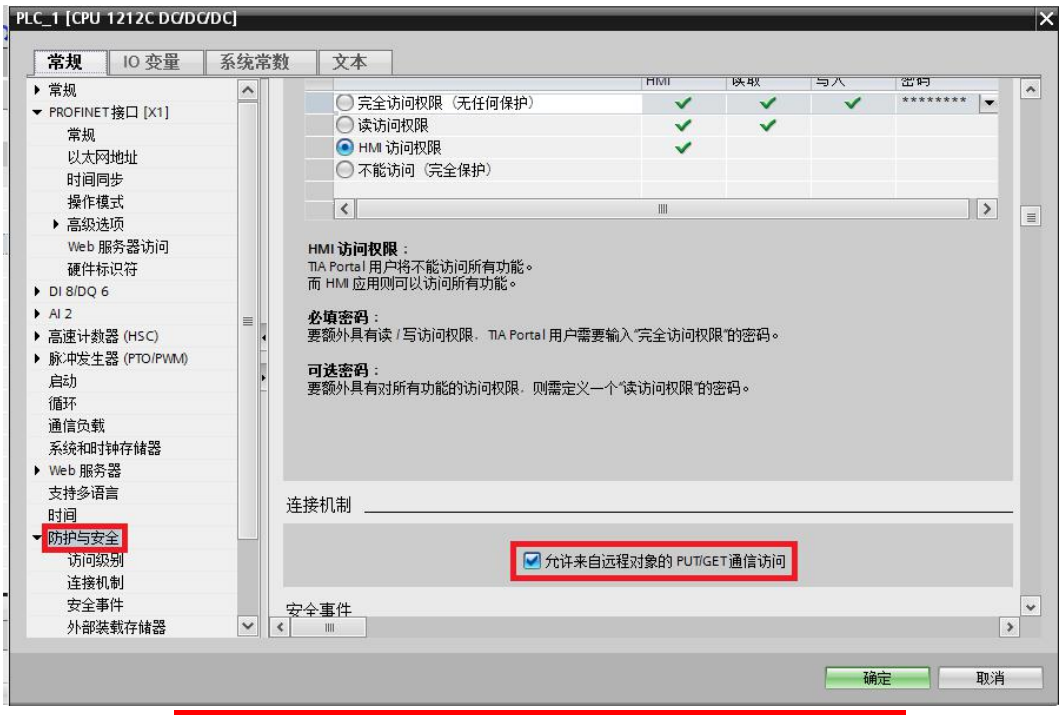
RVNet-PN 支持市面上常见的组态软件，比如组态王、力控、杰控、WINCC 等；

需要注意的是：除了西门子的 WINCC，其他组态软件需要访问 S71200、S71500 寄存器数据的时候，需要对 PLC 做如下设置：

1.运行 TIA portal V14 软件并打开项目；



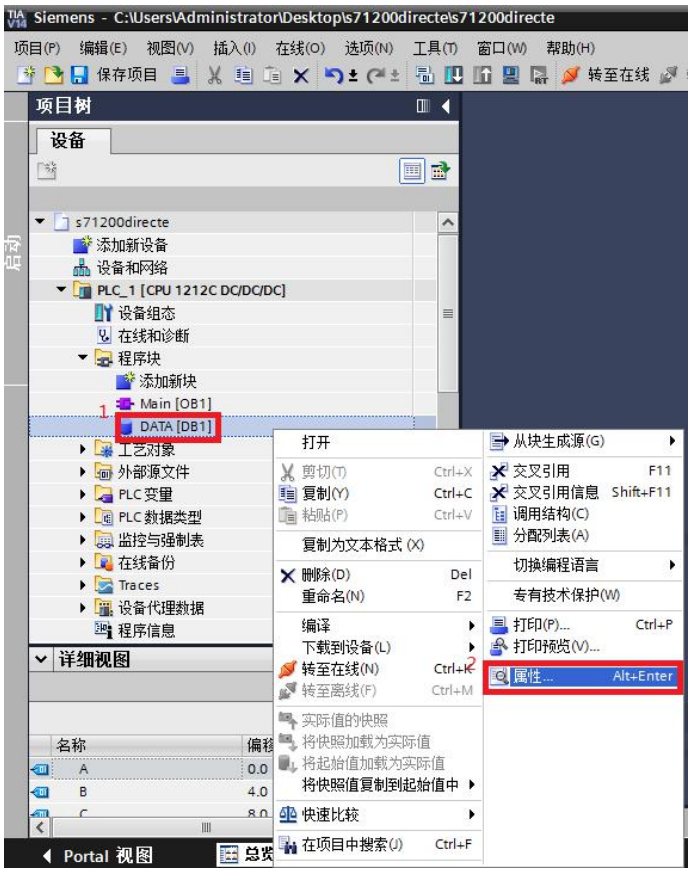
2.选中 PLC，右键点击 PLC，选择【属性】;



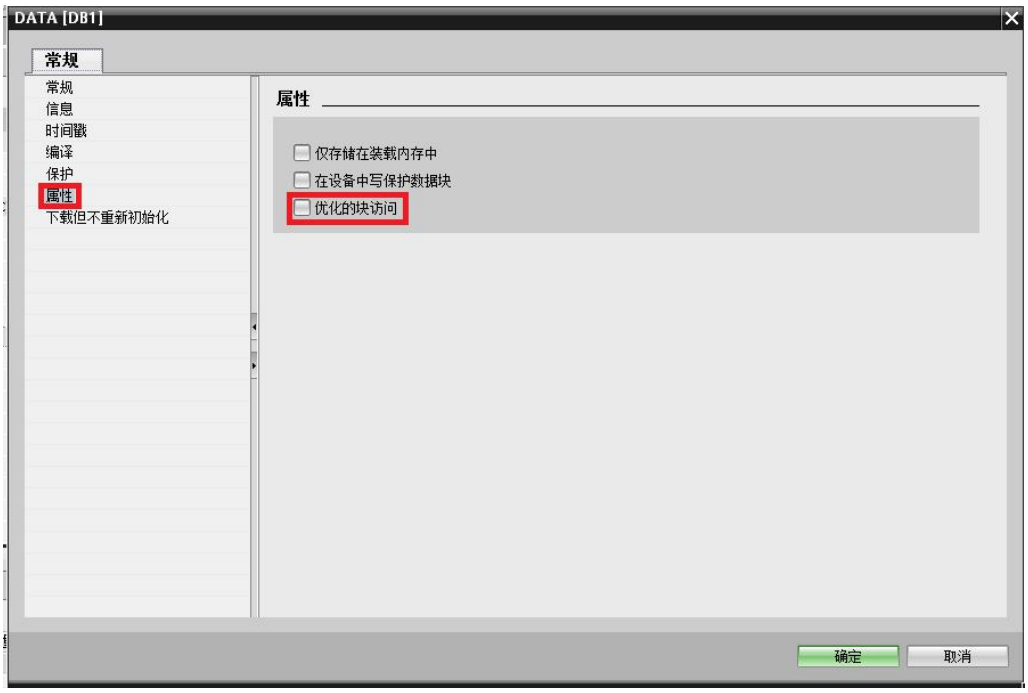
3. 选择【防护与安全】;【允许来自从远程对象的 PUT/GET 通信访问】必须要打钩。

当你需要访问 DB 数据块的数据时，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。

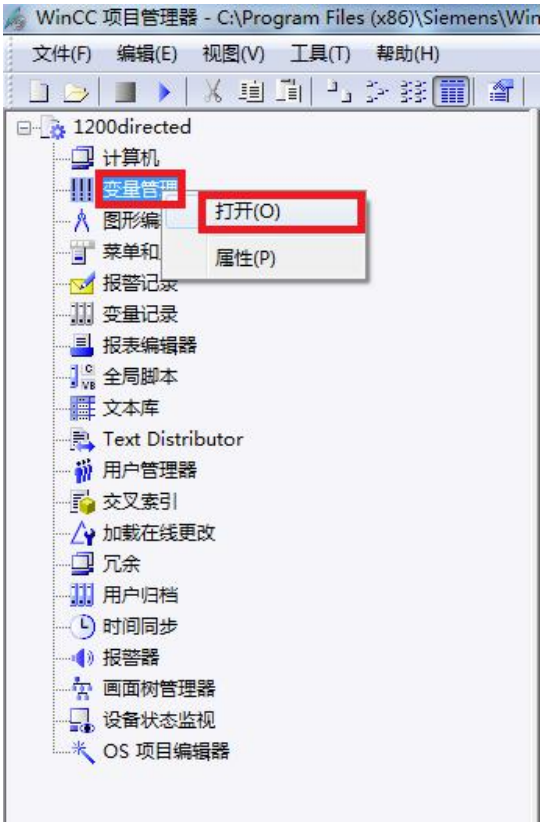


6.1WINCC 通讯

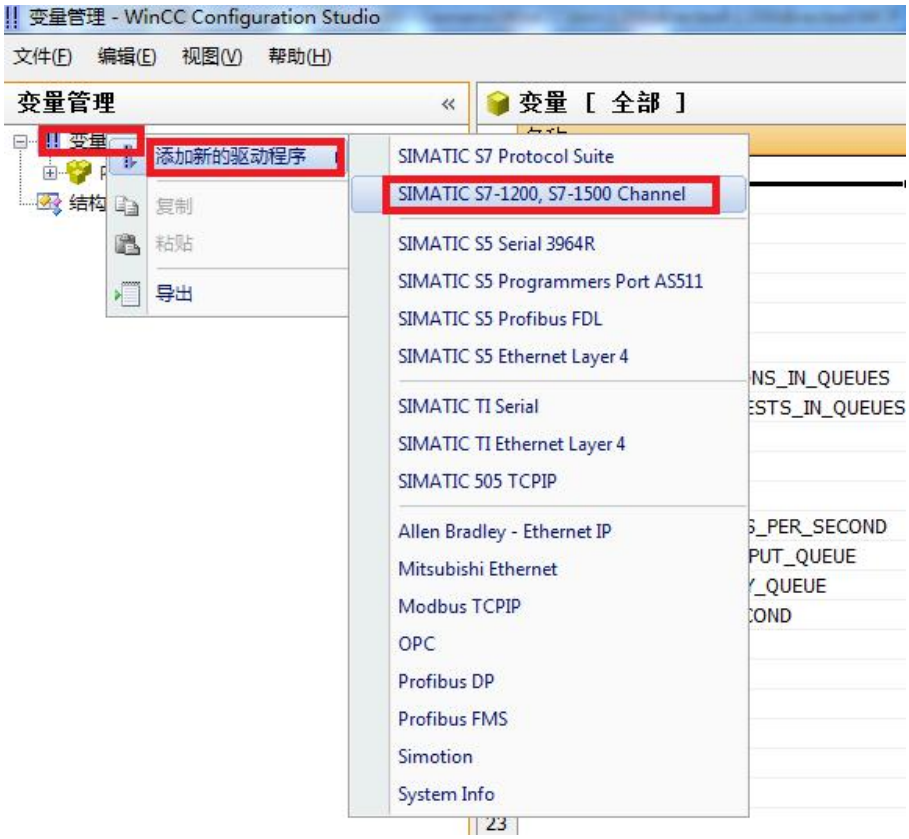
6.1.1 连接 S71200

西门子 S7-1200 通过 RVNet-PN 连接 WINCC，采用西门子 1200 的以太网驱动。

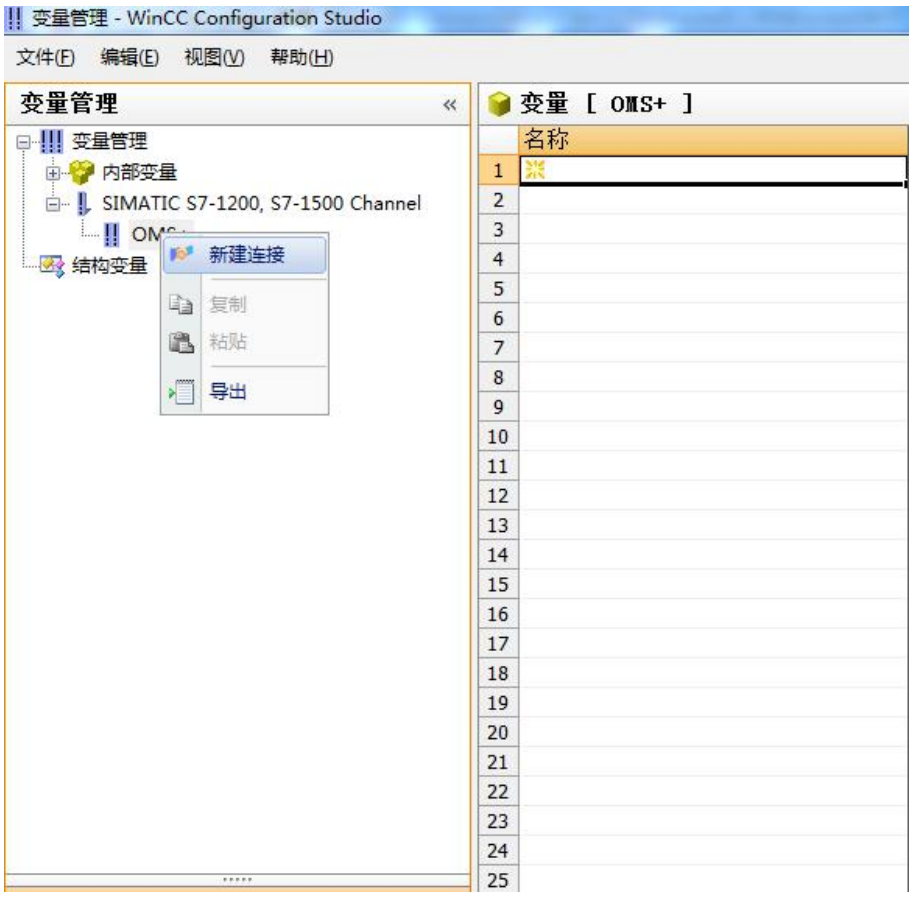
1、运行 WINCC 软件，右击【变量管理】，点击【打开】;



2、右击【变量管理】，选择【添加新的驱动程序】下的【SIMATIC S7-1200、S7-1500 Channel】;



3、右击【OMS+】，点击【新建连接】，新建一个通讯连接，例如 NewConnection_1；



4、右击新建的通讯连接，点击【连接参数】;

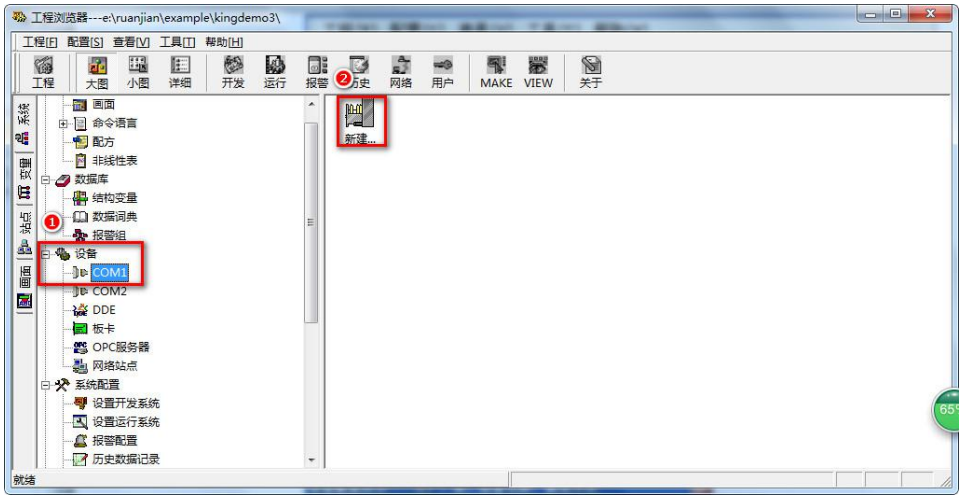
5、在弹出的对话框中，【IP 地址】填入 RVNet-PN 的 IP 地址，【访问点】选择 S7ONLINE，产品系列选择相应 PLC 的型号系列，例如 S7 1200。

6.2 组态王通讯

6.2.1 连接 S71200

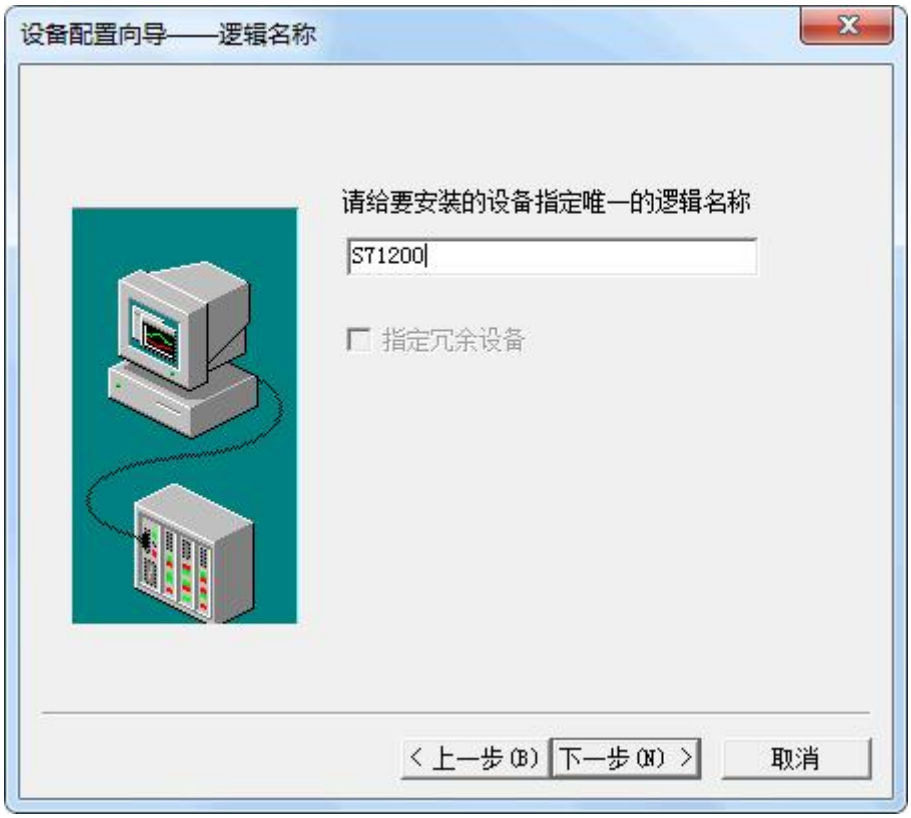
西门子 S7-1200 通过 RVNet-PN 连接组态王，采用西门子 S71200 的以太网驱动。

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】;

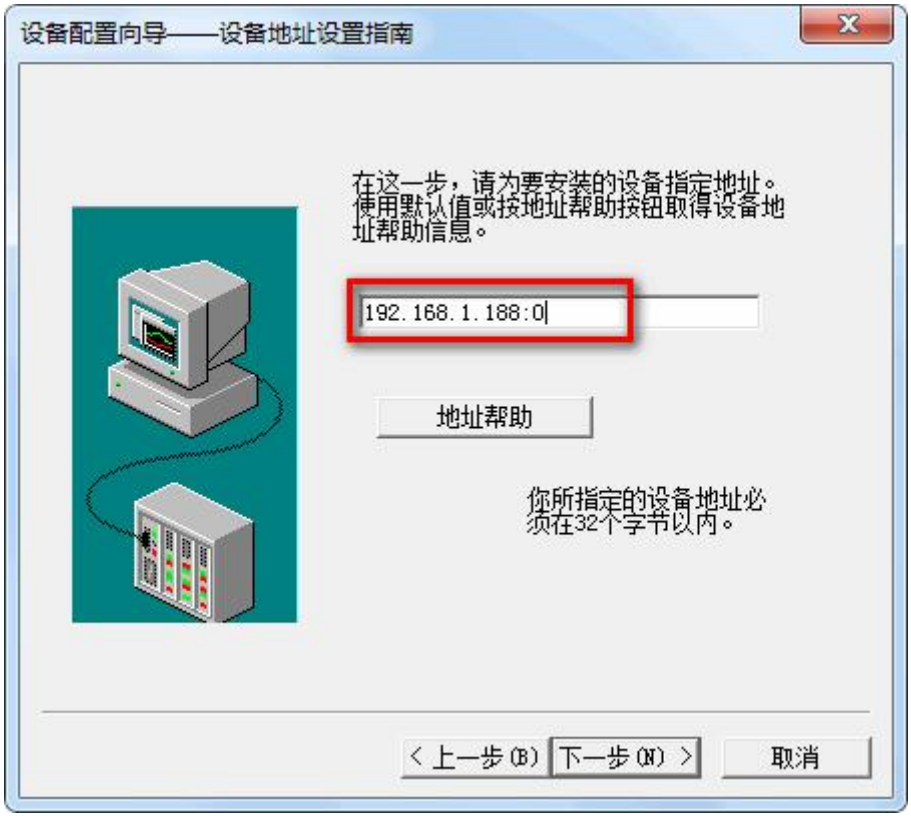


2、打开 PLC 分组，然后打开西门子分组，选择 S7-1200 系列(TCP)下的 TCP 驱动;

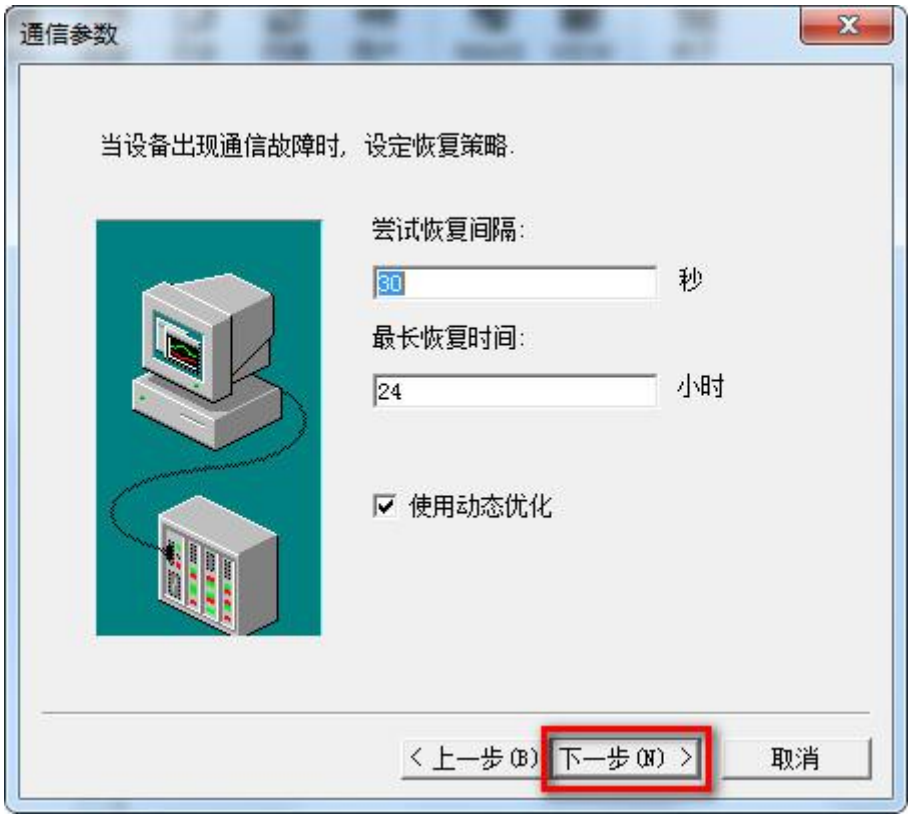
3、 填入设备名称，点击【下一步】;



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



4、 根据向导默认参数，点击【下一步】；


通信参数
当设备出现通信故障时，设定恢复策略.
尝试恢复间隔:
80
秒
最长恢复时间:
24
小时
使用动态优化
< 上一步(B)
下一步(N) >
取消

6、完成参数设置。

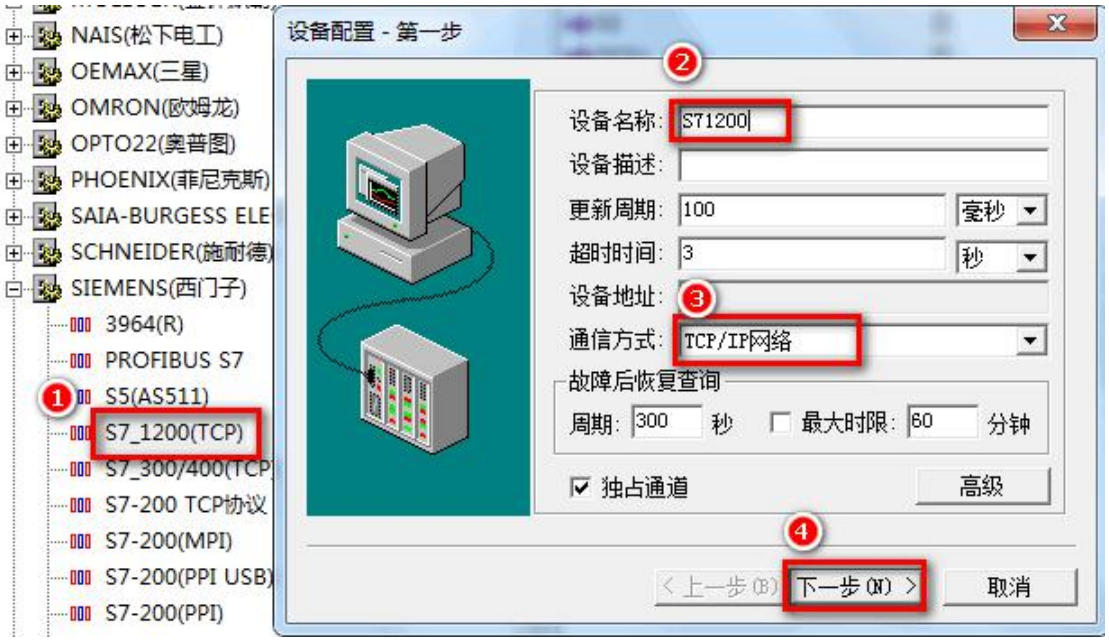

设备安装向导——信息总结
你所要安装的设备信息:
设备信息
新设备为 西门子 生产的 S7-1200 .
设备逻辑名: S71200
设备地址:192.168.1.188:0
通讯方式: TCP
自动建变量
< 上一步(B)
完成
取消

6.3 力控通讯

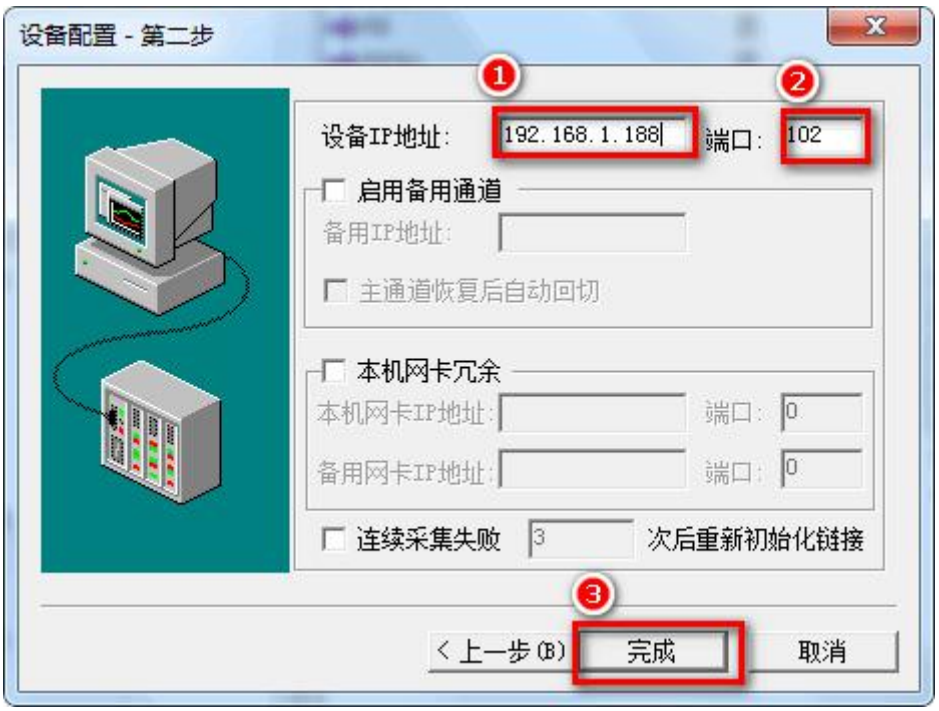
6.3.1 连接 S71200

西门子 S7-1200 通过 RVNet-PN 连接 ForceControl，采用西门子 S71200 的以太网驱动。

1、打开力控开发系统——IO 设备组态，选择【PLC-SIEMENS（西门子）—S7-1200 TCP 协议】，填入设备名称，点击【下一步】;



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



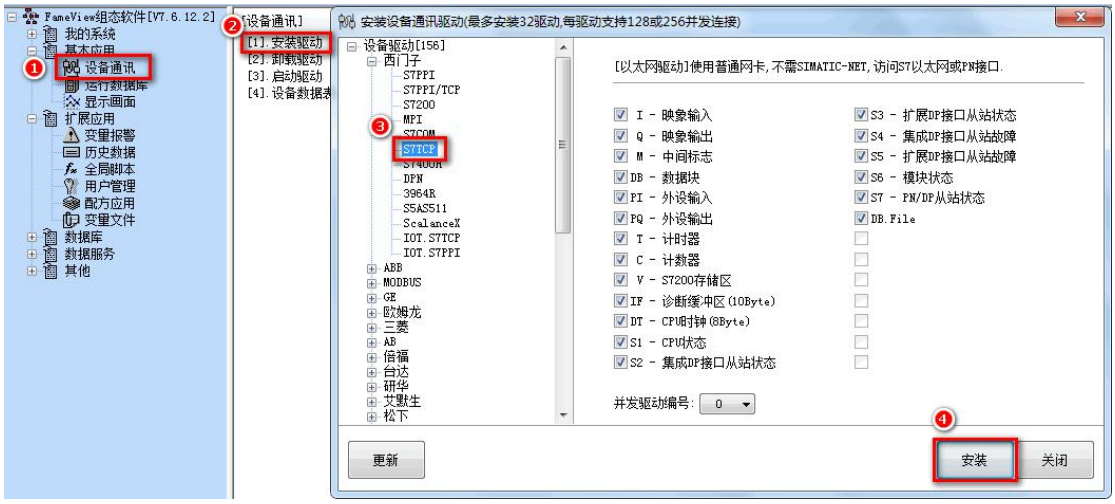
6.4 杰控通讯

6.4.1 连接 S71200

西门子 S7-1200 通过 RVNet-PN 连接 FrameView，采用西门子 S71200 的以太网驱动。

1、安装驱动程序：

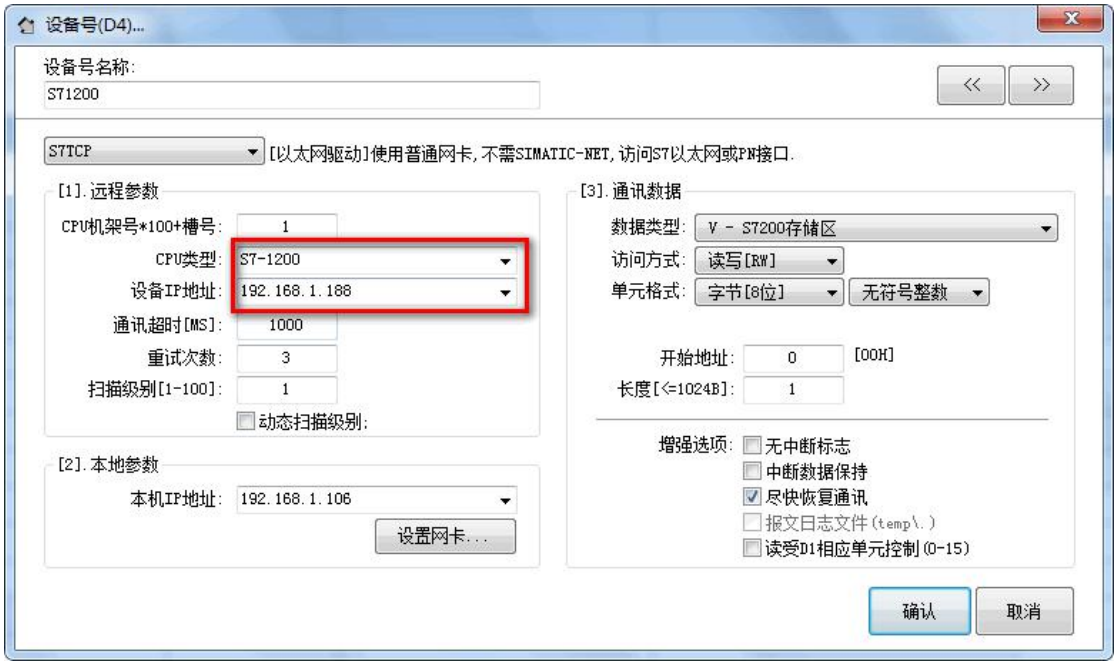
选择【基本应用】下【设备通讯】，执行【1.安装驱动程序】，显示下面对话框：



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 S7-1200，【设备 IP 地址】填入 RVNet-PN 的 IP 地址；

7.OPC 通讯

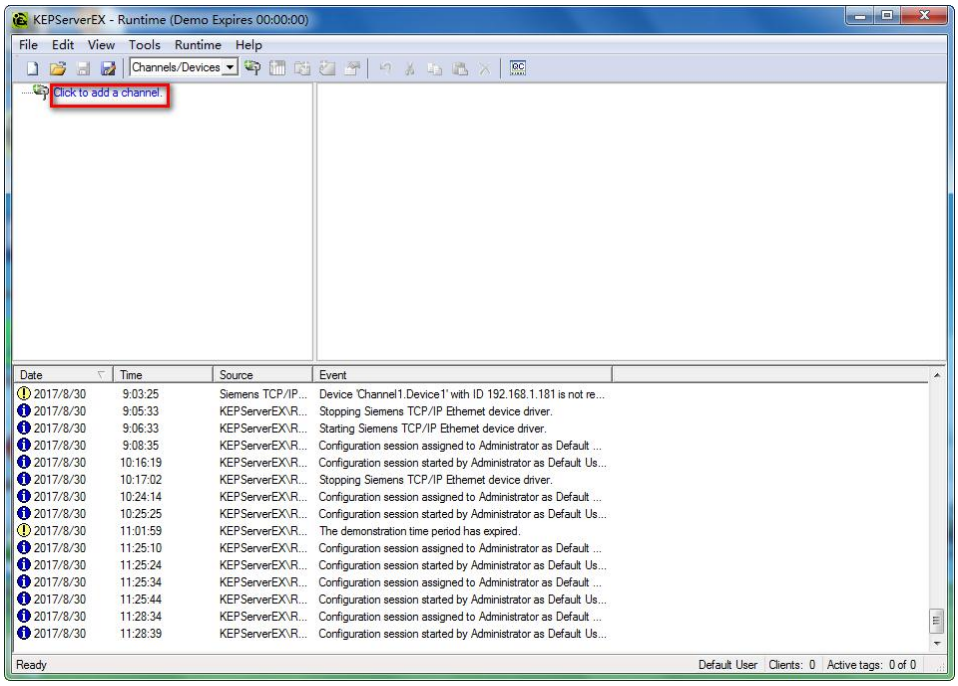
7.1Kepware OPC 通讯

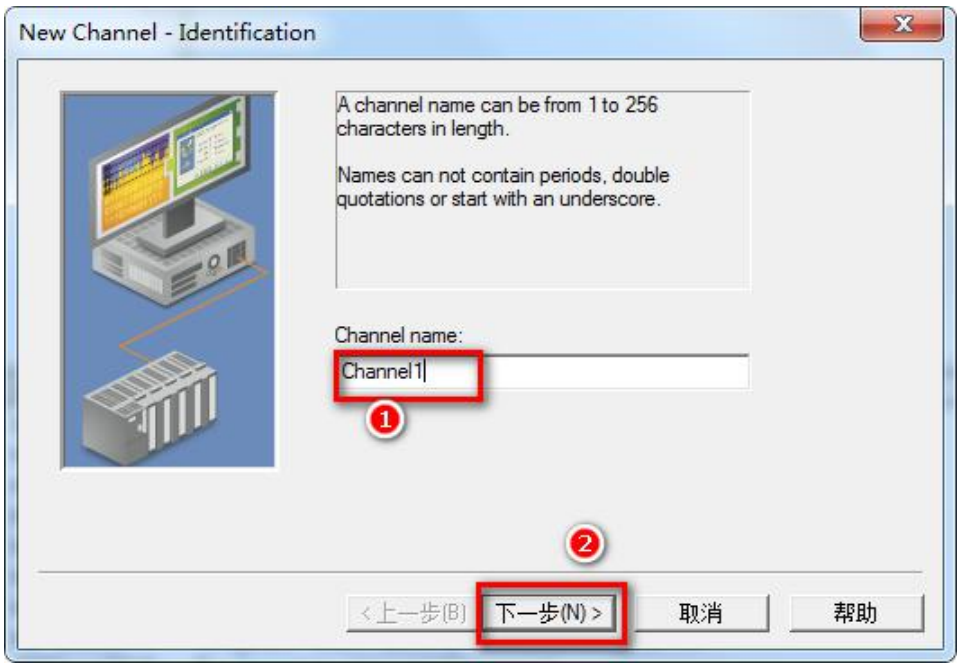
7.1.1 连接 S71200

西门子 S7-1200 通过 RVNet-PN 连接 KepWare OPC，采用西门子 S71200 的以太网驱动。

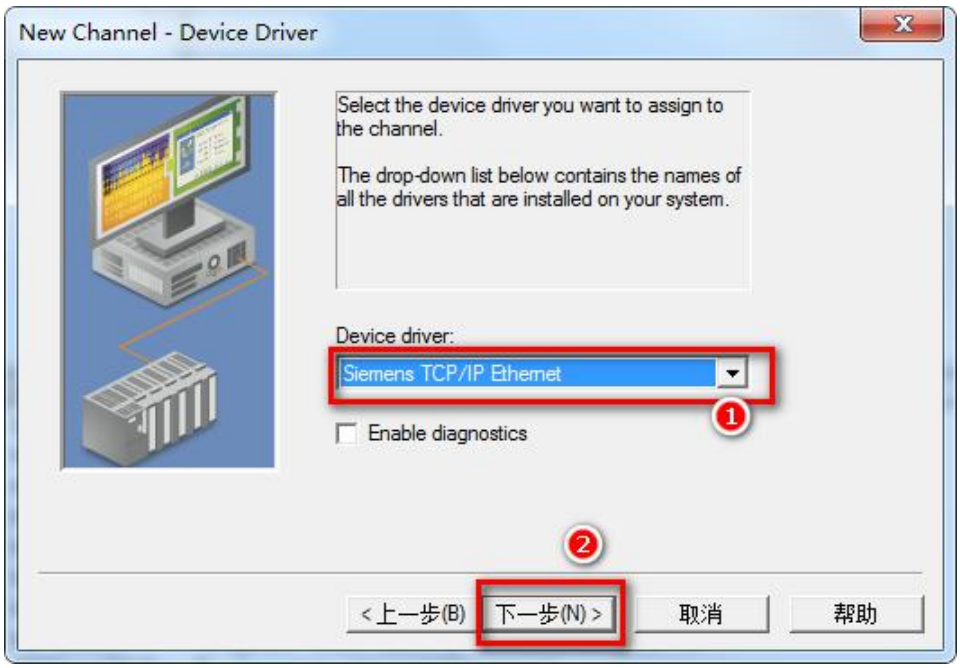
7.1.1.1 添加通道

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

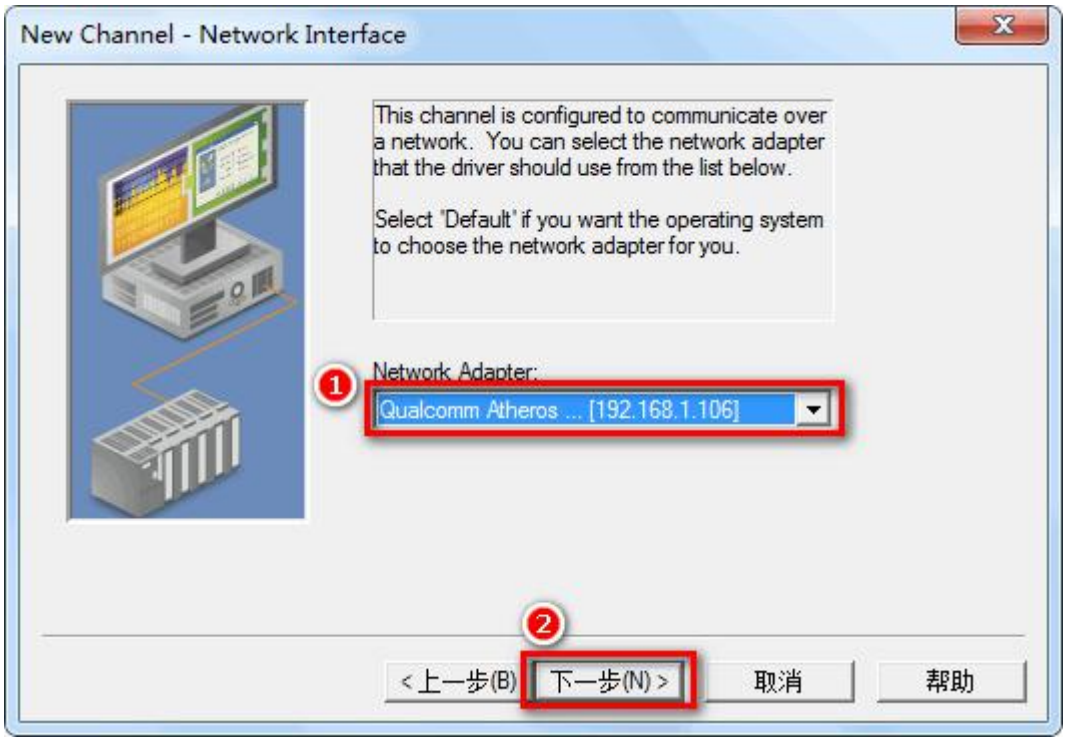




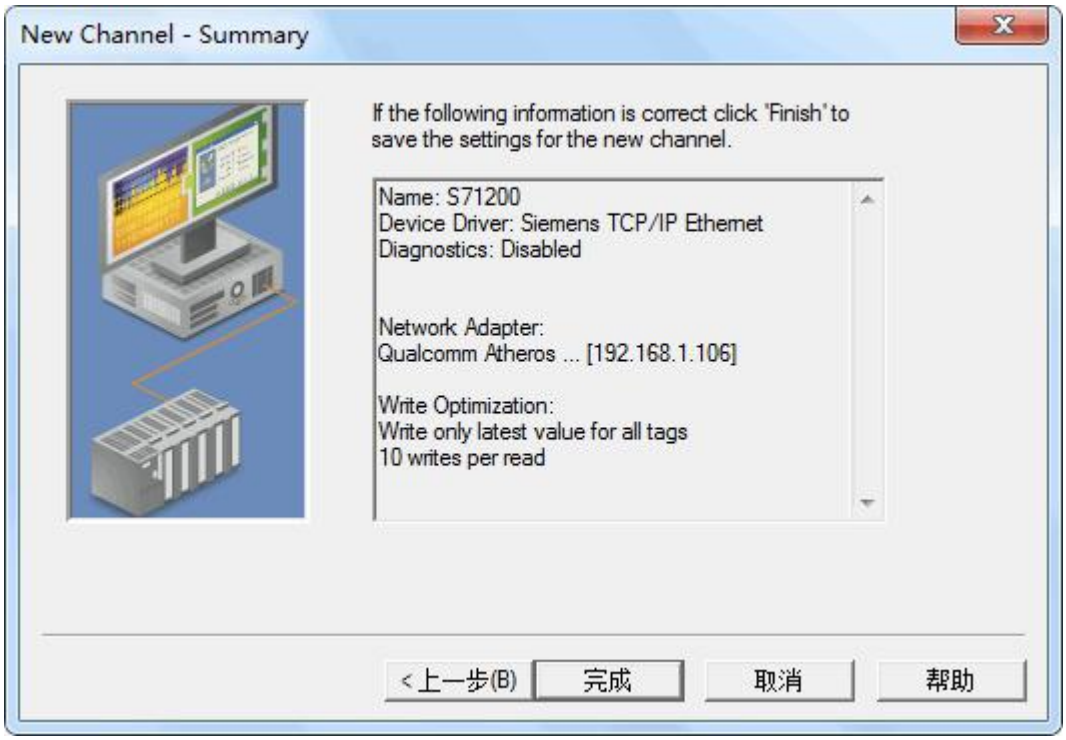
2、【Device driver】选择【Siemens TCP/IP Ethernet】驱动，点击【下一步】;



3、【Network Adapter】选择计算机网卡；

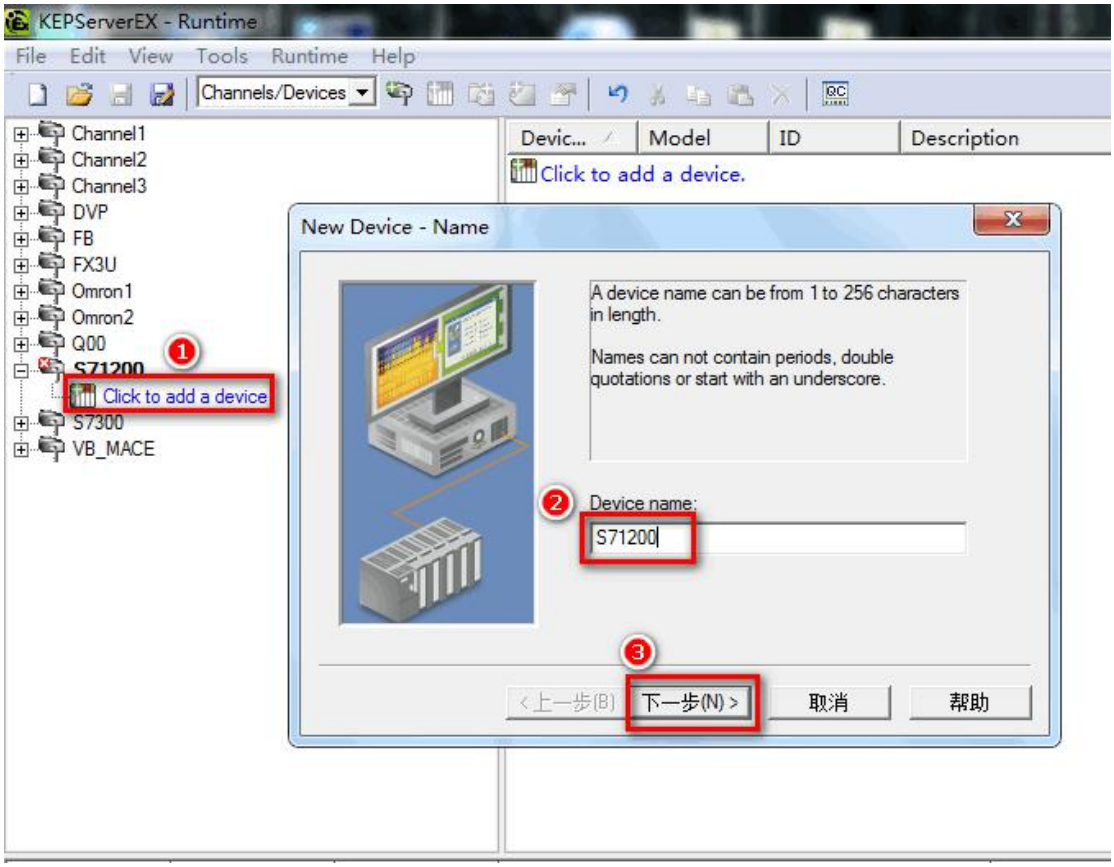


4、根据需要选择模式（可默认），依照向导完成通道参数设置；

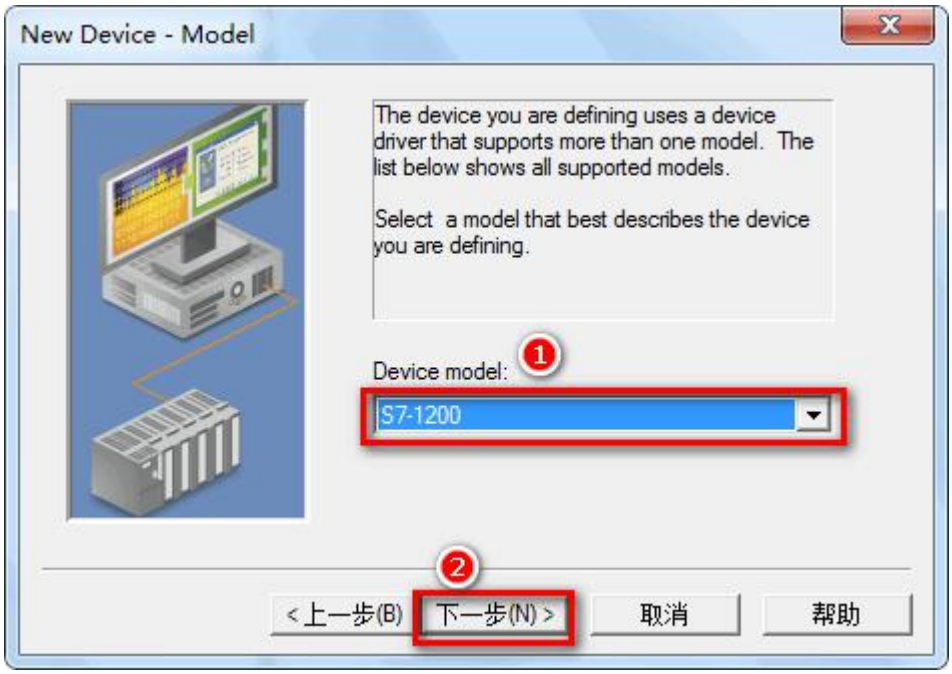


7.1.1.2 添加设备

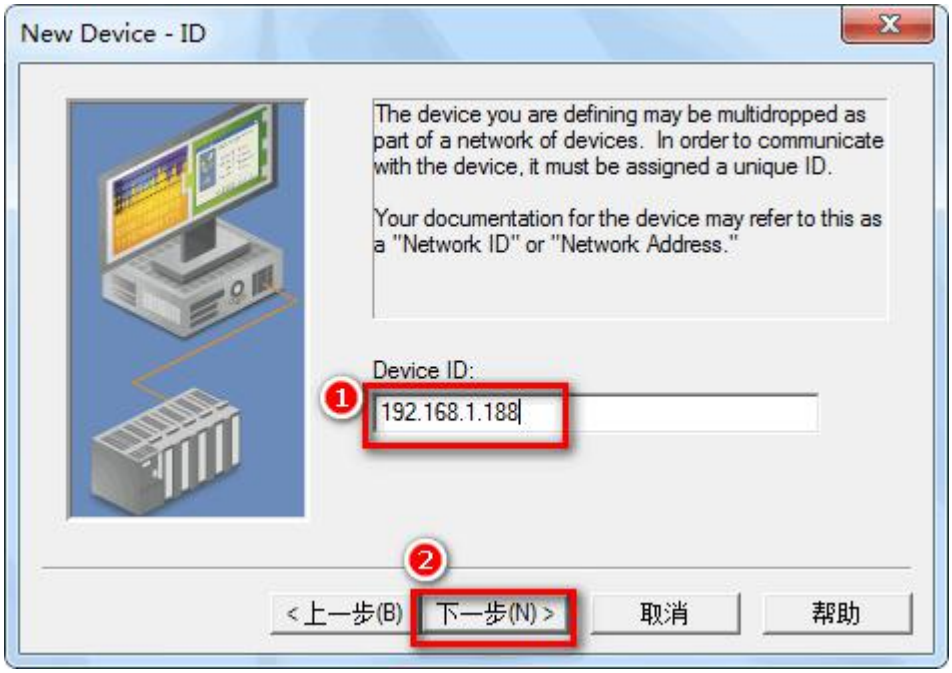
1、增加设备，填入设备名称，点击【下一步】;



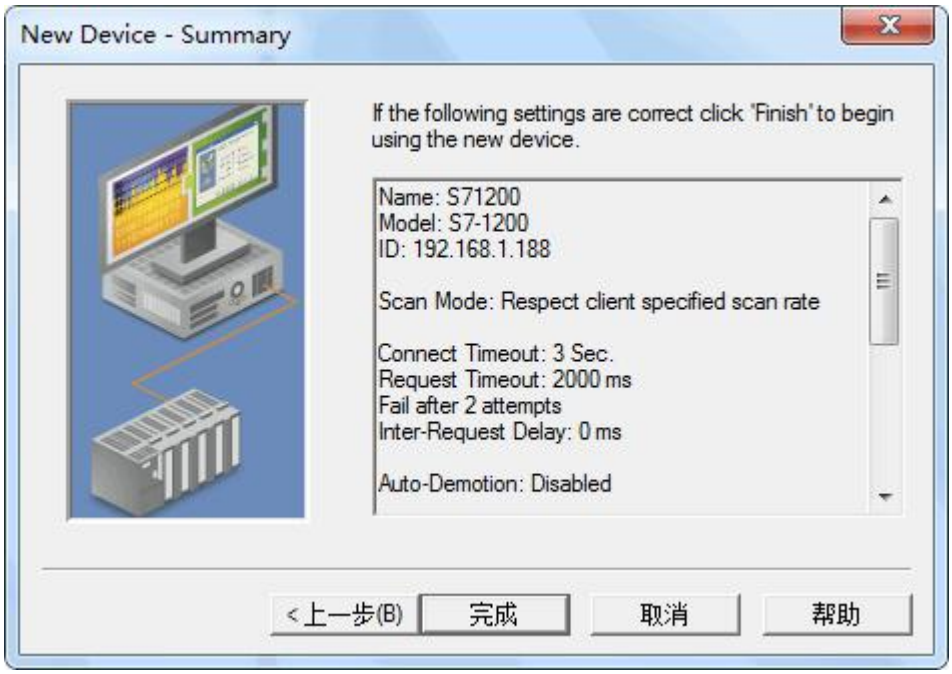
2、【Device model】选择 S7-1200；



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



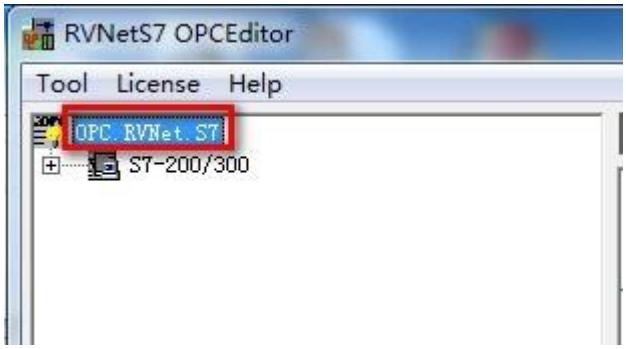
4、依照向导完成设置。



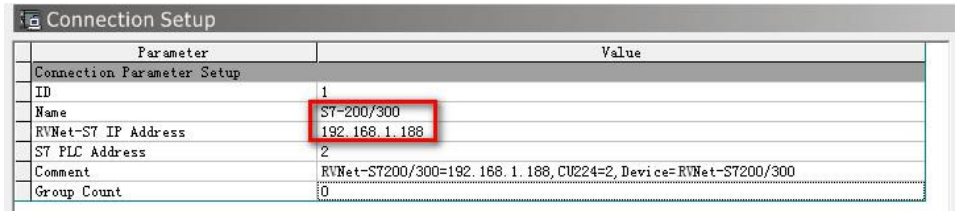
7.2RVNetS7OPC 通迅

7.2.1 配置 OPC 参数

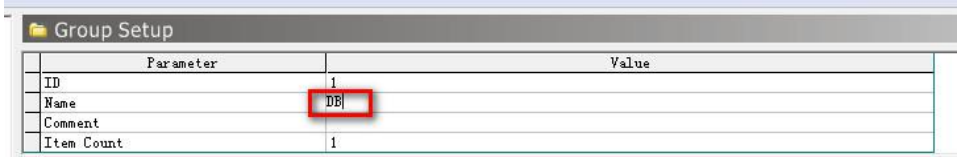
1、打开 RVNetS7 OPCEditor，右击【OPC.RVNet.S7】，选择【New Connection】添加新的连接；



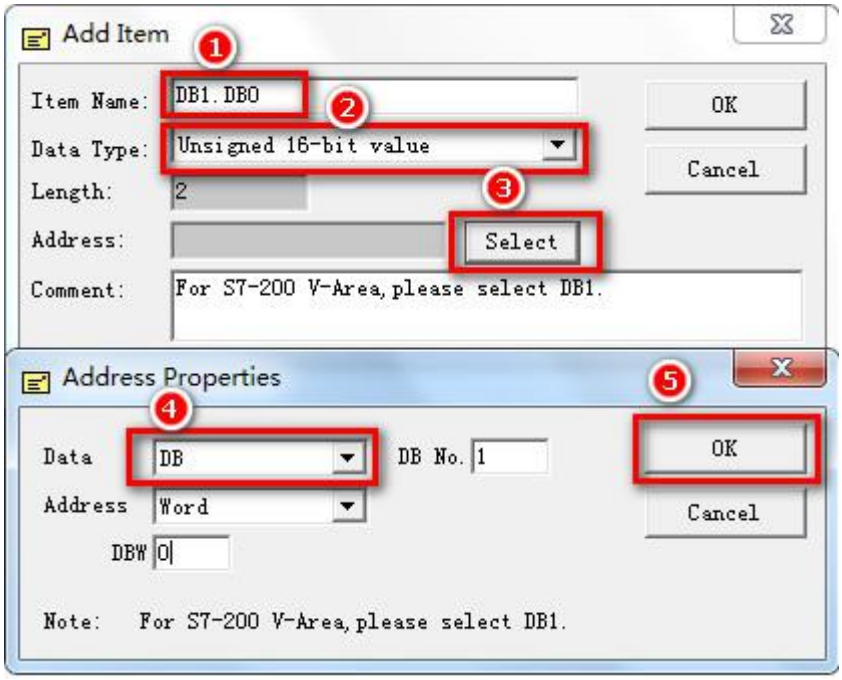
2、点击【New Connection】，在如下窗口填写连接设备的名称，如：S7-200/300，输入 RVNet-PN 的 IP 地址，【S7 PLC Address】填入默认值 2;



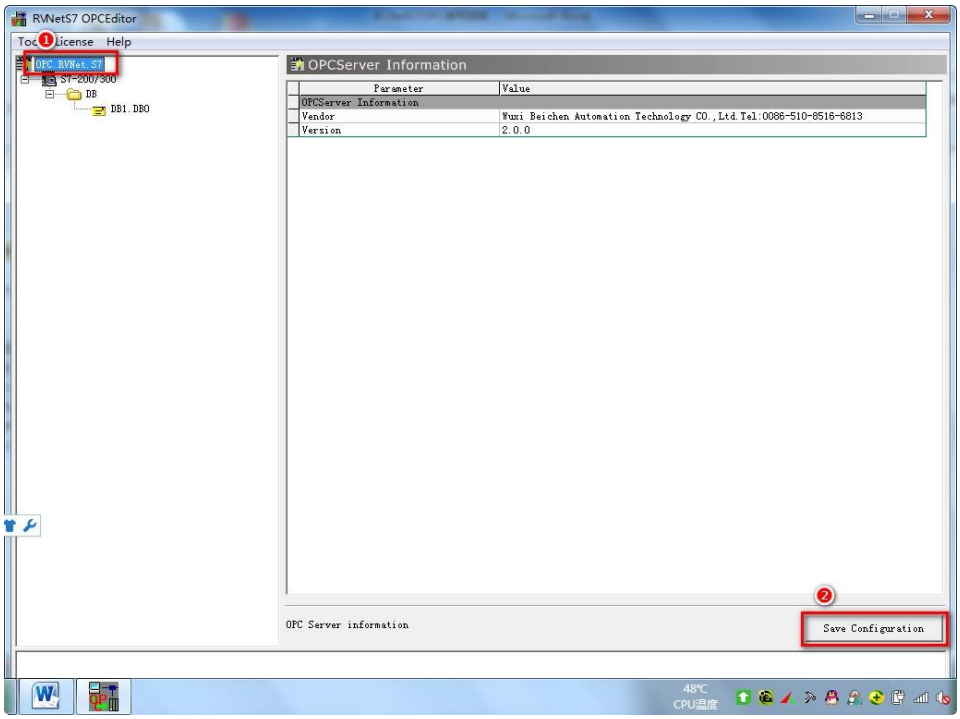
3、右击连接设备的名称【S7-200/300】点击【New Group】，新建组名，在如下的窗口填入组名，如：DB;



4、右击组名【DB】点击【New Item】建立变量，按下图完成 Item 的配置；

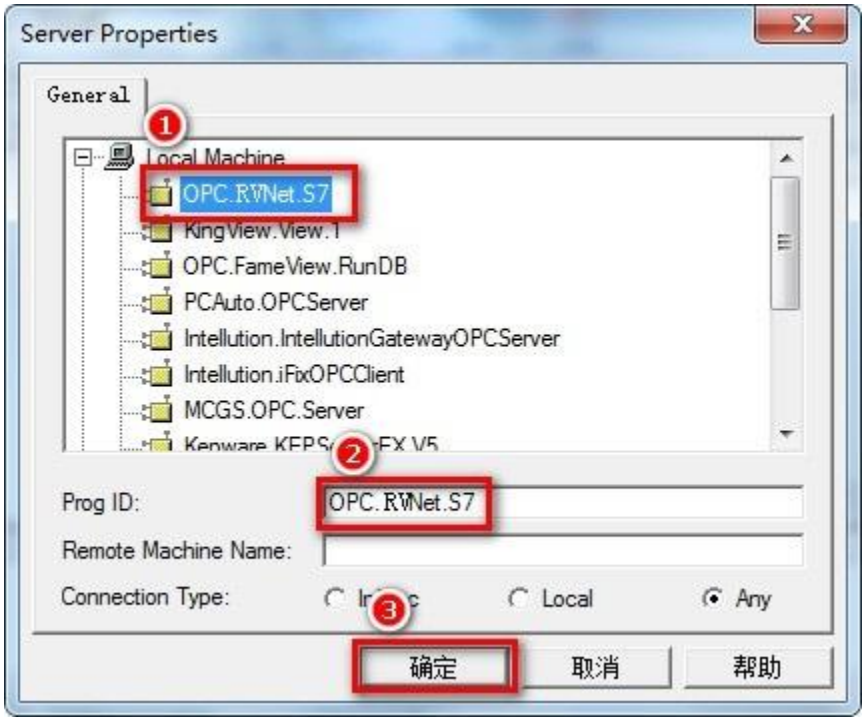


5、选择菜单栏的【OPC.RVNet.S7】，点击【Save Configuration】，完成设置；



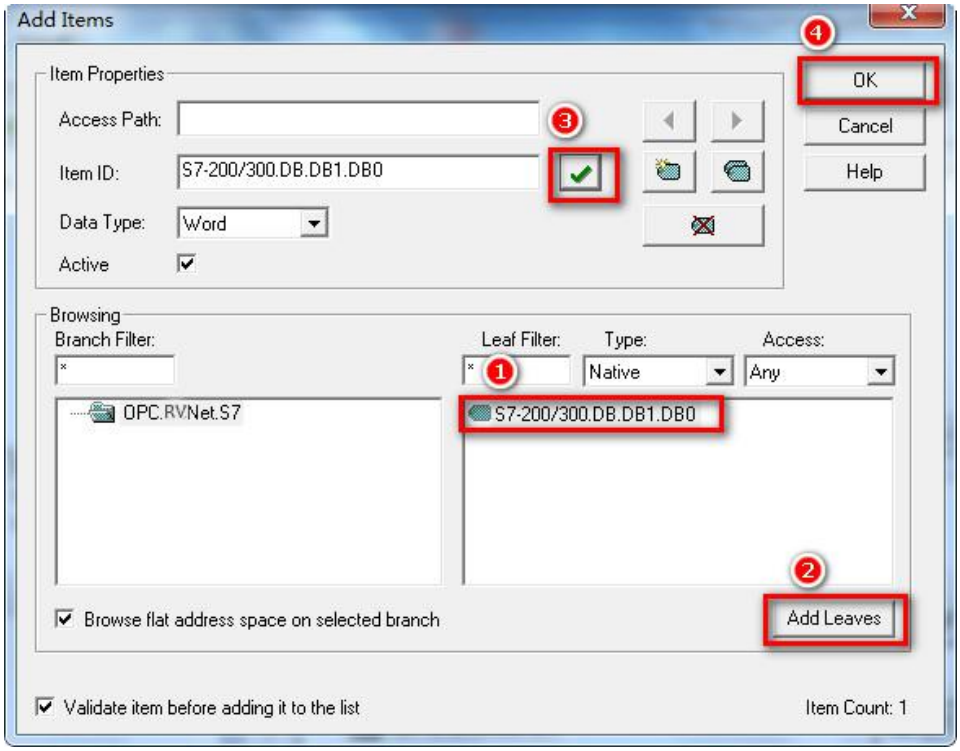
7.2.2 测试 OPC 变量

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：

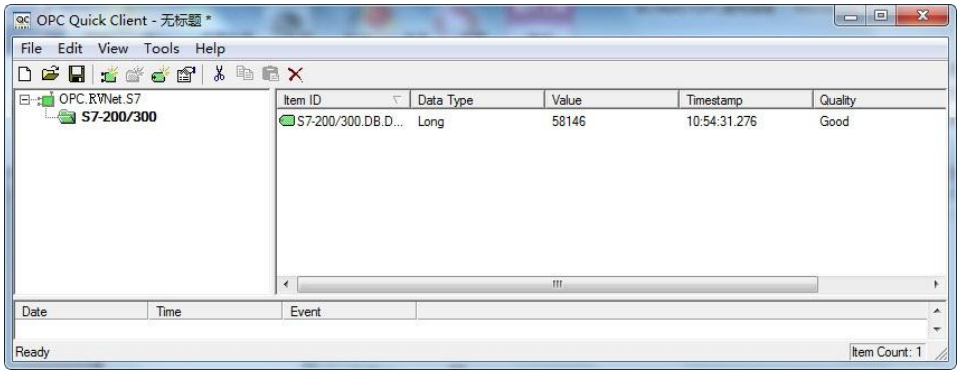


2、鼠标右击菜单栏的【OPC.RVNet.S7】，点击【New Group…】,输入组名，如：S7-200/300，点击确定；

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：

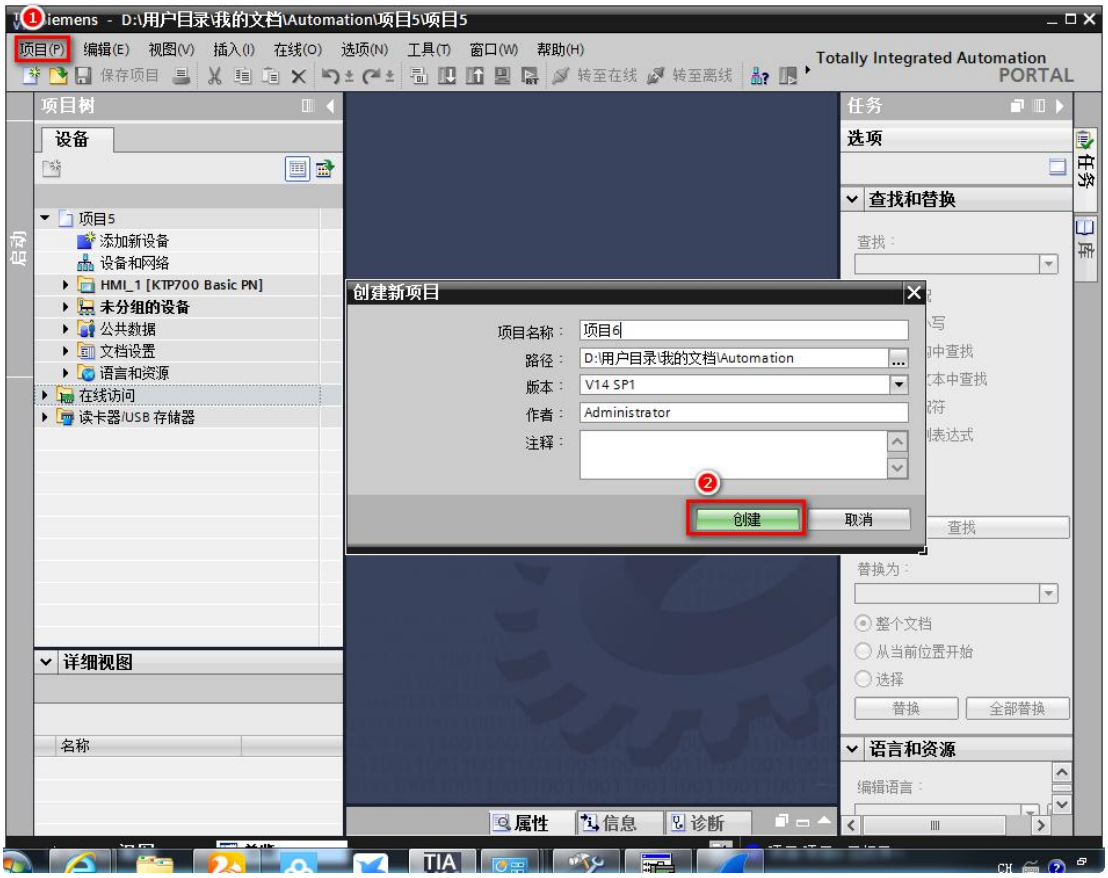


8.触摸屏以太网通讯

8.1 西门子 KTP/TP 系列触摸屏通讯

RVNet 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。

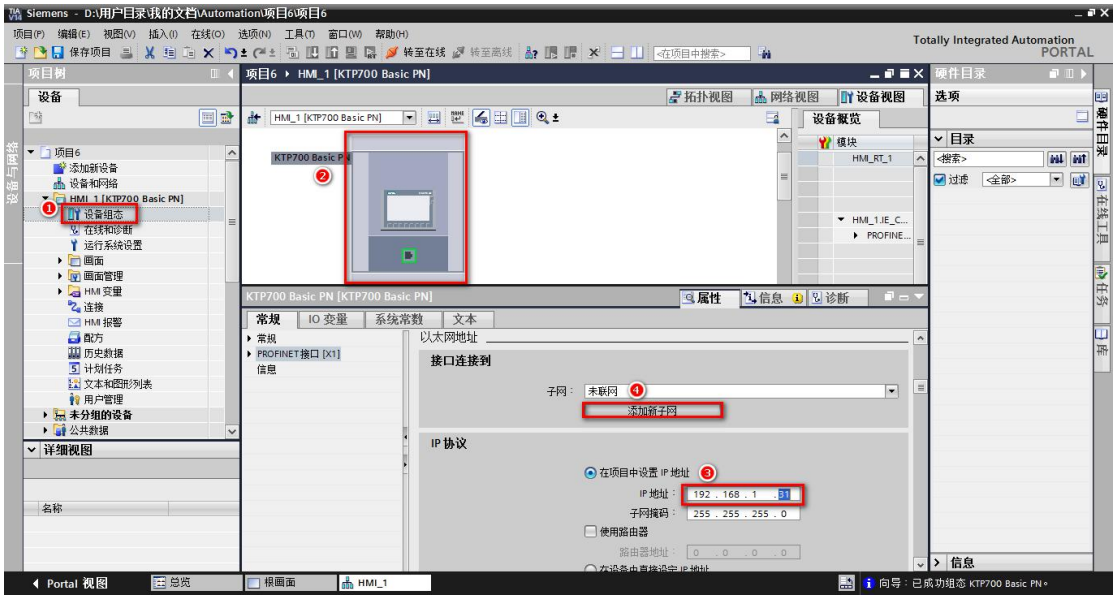
1、新建项目；


Siemens - D:\用户目录\我的文档\Automation\项目5\项目5
项目(P) 编辑(E) 视图(V) 插入(I) 在线(O) 选项(N) 工具(T) 窗口(W) 帮助(H)
Totally Integrated Automation PORTAL
项目树
设备
项目5
添加新设备
设备和网络
HMI_1 [KTP700 Basic PN]
未分组的设备
公共数据
文档设置
语言和资源
在线访问
读卡器/USB 存储器
详细视图
名称
创建新项目
项目名称： 项目6
路径： D:\用户目录\我的文档\Automation
版本： V14 SP1
作者： Administrator
注释：
创建
取消
任务
选项
查找和替换
查找：
替换为：
整个文档
从当前位置开始
选择
替换
全部替换
语言和资源
编辑语言：
属性
信息
诊断
TIA

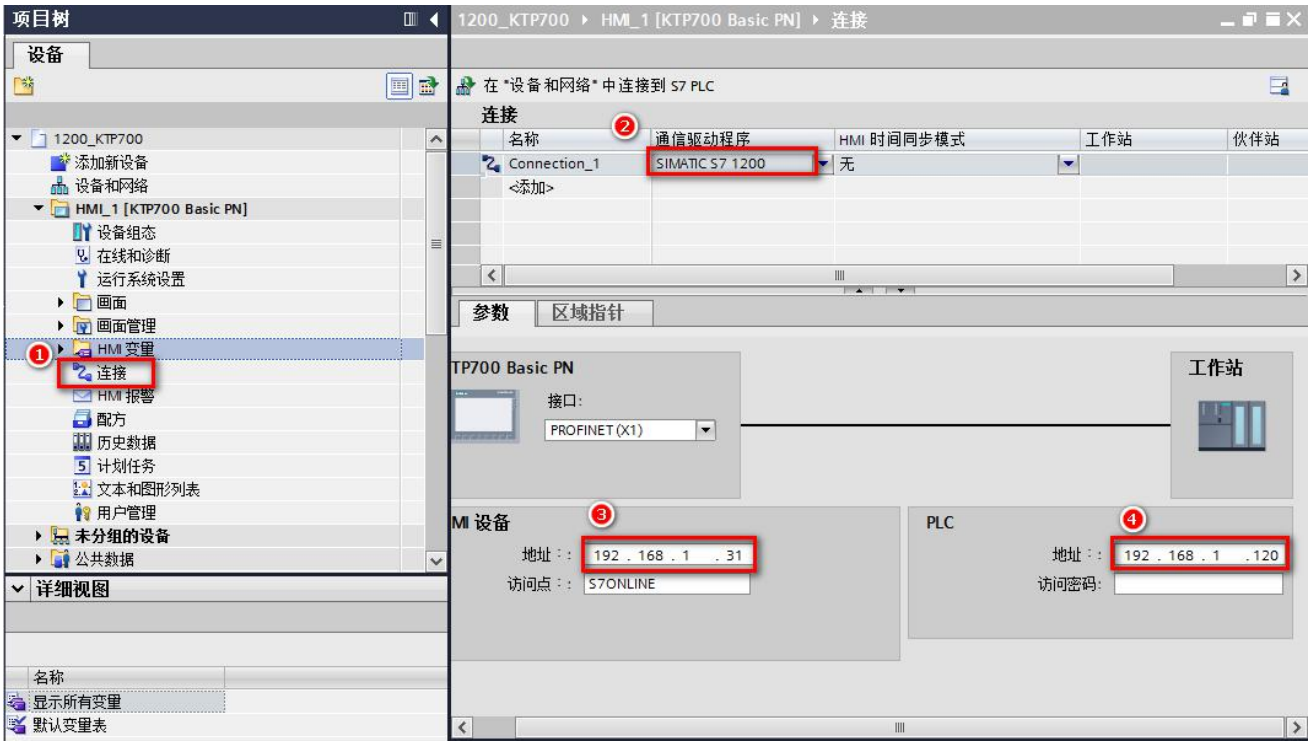
2、添加触摸屏设备；


Siemens - D:\用户目录\我的文档\Automation\项目6\项目6
项目(P) 编辑(E) 视图(V) 插入(I)
添加新设备
设备名称：
HMI_1
项目树
设备
项目6
添加新设备
设备和网络
未分组的设备
公共数据
文档设置
语言和资源
在线访问
读卡器/USB 存储器
详细视图
名称
控制器
HMI
PC 系统
HMI
SIMATIC 精简系列面板
3" 显示屏
4" 显示屏
6" 显示屏
7" 显示屏
KTP700 Basic
6AV2 123-2GB03-0AX0
6AV2 123-2GB03-0AX0
KTP700 Basic 立式
9" 显示屏
10" 显示屏
12" 显示屏
15" 显示屏
用于多功能面板的 SIMATIC WinAC
设备：
KTP700 Basic PN
订货号： 6AV2 123-2GB03-0AX0
版本： 14.0.1.0
说明：
7" TFT显示屏，800 x 480 像素，64K 色；按键和触摸操作，8 个功能键；1 x PROFINET，1 x USB
启动设备向导
确定
取消
TIA

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 1200，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。

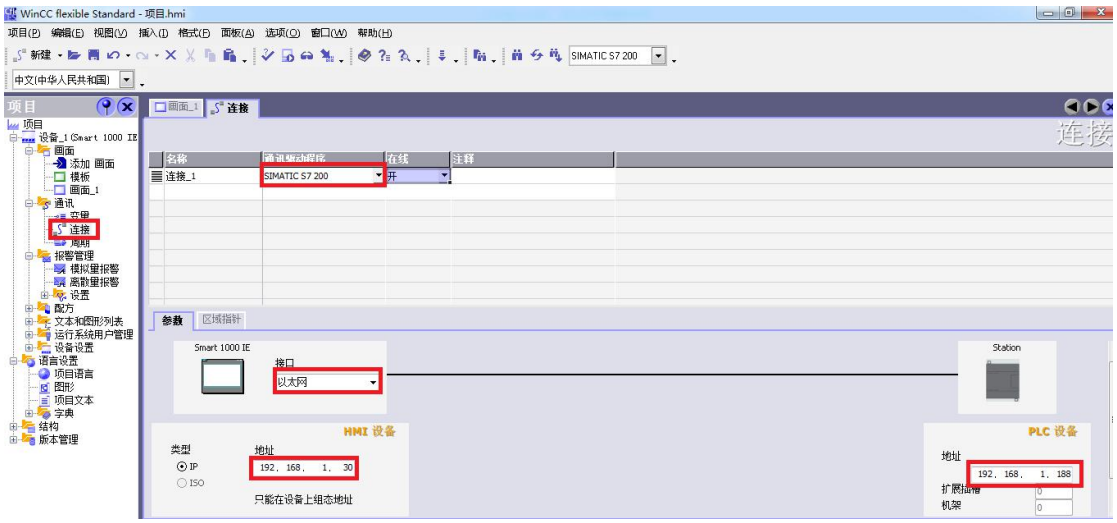


8.2 西门子 SmartIE 系列触摸屏连 S71200、S71500

SmartIE 触摸屏通过 RVNet-PN 可以实现与西门子 S71200、S71500 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-PN 的 IP 地址；



3.建立变量

SmartIE 触摸屏通过 RVNet-PN，可访问 S71200、S71500 的 DB 数据块、M 区、Q 区、I 区。

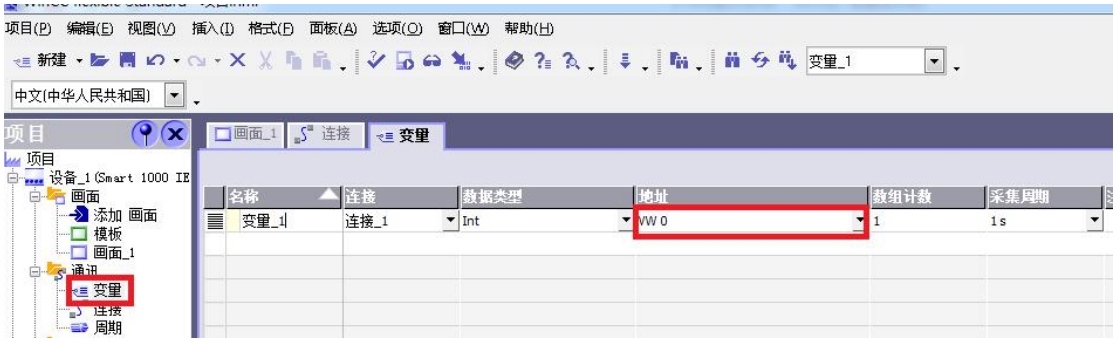
注意：软件中新建的变量与 PLC 的数据区对应关系：

V 区对应 PLC 的 DB 数据块；触摸屏的 V 区和 PLC 的 DB 数据块的对应关系与 RVNet 模块中的【SMARTIE 屏 Mapping】参数有关，具体关系如下：

当 Mapping=1 时：

V0—V32767 对应 DB1.DBX32767；
当 Mapping=2 时（DB 最大长度 10000）：
V0—V9999 对应 DB100.DBX0—DB100.DBX9999
V10000—V19999 对应 DB101.DBX0—DB101.DBX9999
V20000—V29999 对应 DB102.DBX0—DB102.DBX9999
V30000—V32767 对应 DB103.DBX0—DB103.DBX2767
当 Mapping=3 时（DB 最大长度 1000）：
V0—V999 对应 DB100.DBX0—DB100.DBX999
V1000—V1999 对应 DB101.DBX0—DB101.DBX999
V2000—V2999 对应 DB102.DBX0—DB102.DBX999
V3000—V3999 对应 DB103.DBX0—DB103.DBX999
……
V32000-V32767 对应 DB132.DBX0—DB132.DBX767

M 区对应 PLC 的 M 区；
Q 区对应 PLC 的 Q 区；
I 区对应 PLC 的 I 区；



当 Mapping=1 时：这里的 VW0 对应 PLC 的 DB1.DBW0；
当 Mapping=2 时：这里的 VW0 对应 PLC 的 DB100.DBW0；
当 Mapping=3 时：这里的 VW0 对应 PLC 的 DB100.DBW0

9.ModbusTCP 通讯

RVNet 模块内部集成 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）

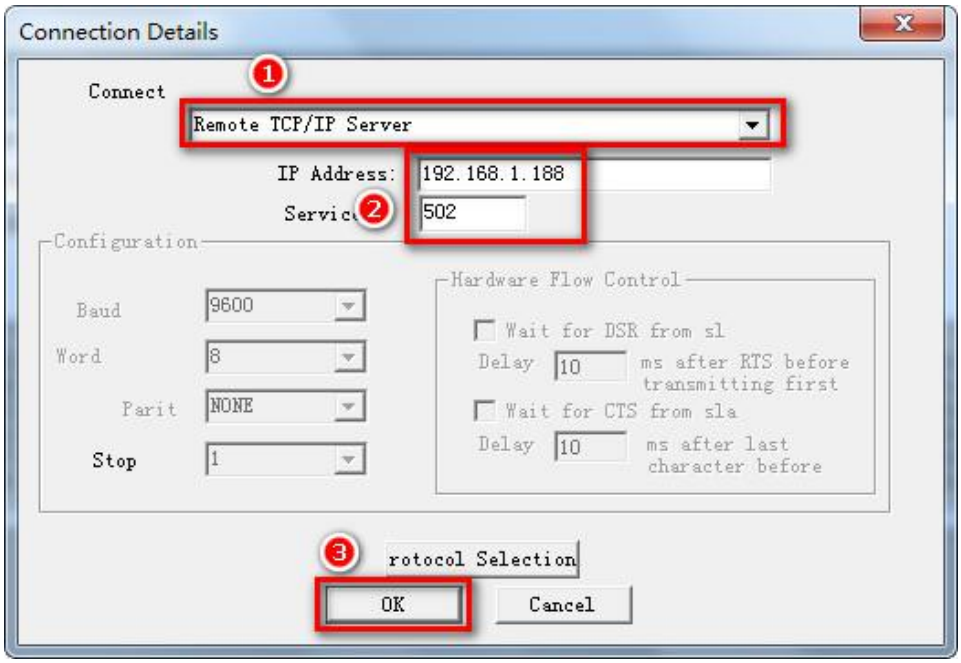
0x0	0x0	0x0	0x0	0x0	后面的字节数						

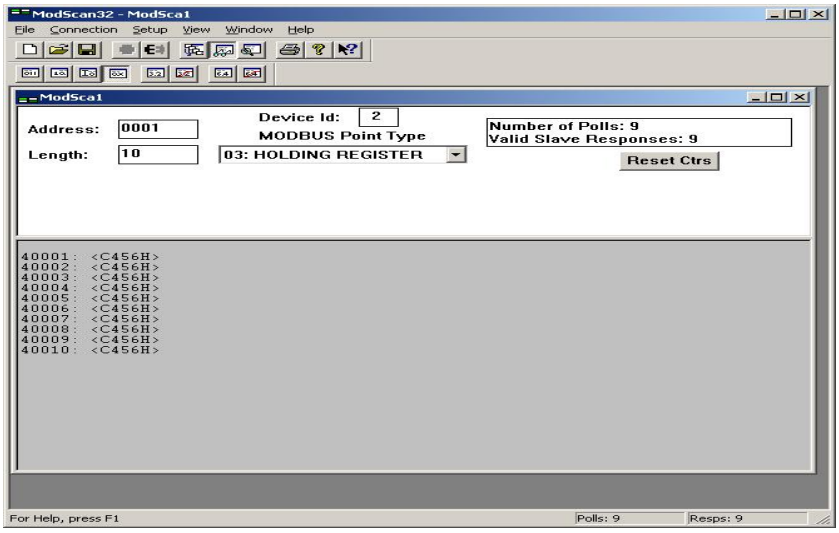
9.1 默认地址映射表

Modbus	S7 系列 PLC	数据类型	计算公式	功能号
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）
				FC5（写线圈）
10001~	I0.0~	位	I***m.n*** = 10001 + ***m****8 + ***n***	FC2（读输入）
30001~	MW0	字（2 字节）	MW***m***= 30001 + ***m***/2，***m*** 为偶数	FC4（读输入寄存器）
40001~	DB1.DBW0	字（2 字节）	DB***1***.DBW***m*** = 40001 + ***m***/2，***m*** 为偶数	FC3（读乘法寄存器） FC16（写乘法寄存器）
				FC6（写单一乘法寄存器）

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-PN 的 IP 地址，Service 端口为 502；点击[OK]按钮。
3. 在子窗口“ModSca1”中，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。
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.RVNet 协议规范

10.1 通讯模式

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

10.2 报文定义

RVNet 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
	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 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 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

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;
	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;
	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 PLC 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

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；
	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；
	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 PLC 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 PLC 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-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	0	msg.rx	byte	0xFF

文头	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 PLC 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	0	msg.rx	byte	0x03

文头	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 PLC 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 PLC 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 PLC 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：RVNet 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 PLC 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：RVNet 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 PLC 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）；

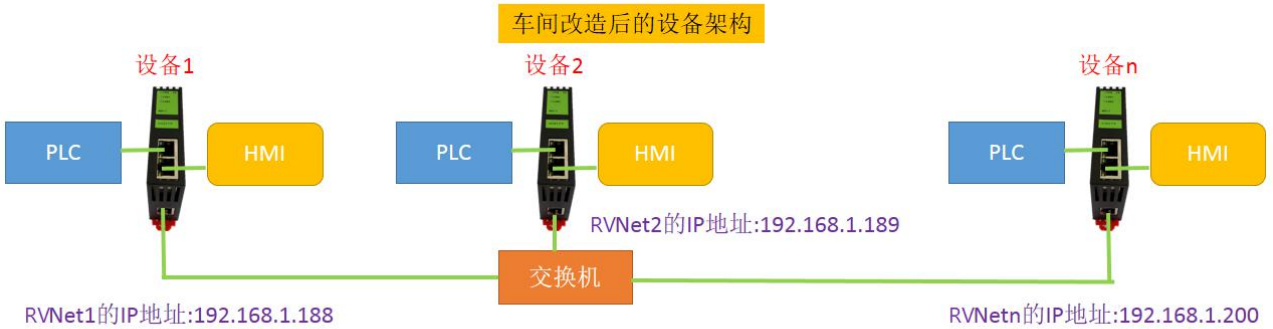
0x88~0x8E：PLC 非法地址访问（读写的地址在 PLC 中不存在）；

通常访问非法地址的错误号是 0x8C。

11.NAT 地址转换

RVNet 的 NAT 地址转换功能可应用在如下场景：

每套设备原本都是独立的系统，每个PLC的IP地址都是相同的，并且无法修改PLC的IP地址，如果现在需要增加一台计算机，实现对现场所有PLC的数据采集，简单的把PLC都连入交换机，显然由于IP地址冲突，此方案将无法实现。



在不改变原系统（PLC和HMI）设置的情况下，通过RVNet模块的NAT地址转换，可实现设备联网的方案需求。

12.产品技术指标

RVNet 模块满足以下技术指标：

产品型号	**RVNet-PN**
描述	西门子系列 PLC 以太网通讯处理器
颜色	金属黑
状态显示	Pwr，LAN1，LAN2
以太网接口 接口类型 传输速率 协议支持 TCP 连接数	IEEE 802.3 兼容，Link/Active 指示灯，线序自适应，支持 Auto-MDIX RJ45 母插座 10/100Mbps S7TCP、ModbusTCP、RVNetS7 等 32
LAN1 接口（连 PLC） 接口类型 传输速率 协议支持	Ethernet RJ45*2 10/100M TCP/IP、S7TCP
LAN2 接口（连上位） 接口类型 传输速率 协议支持	Ethernet RJ45*1 10/100M TCP/IP、S7TCP、ModbusTCP、RVNetS7
编程软件 组态软件 OPC 软件	Protal V14 WINCC、组态王、力控、杰控等 KepWare OPC

诊断和参数设置	IE 浏览器，默认 192.168.2.188(LAN1)、默认 192.168.1.188(LAN2) NetDevice 搜索配置工具
供电方式 电压类型	外接 24VDC 24VDC/100mA
工作温度	0~60℃
工作湿度	90%非凝露
安装方式	35mm 导轨安装
电磁兼容性	2014/30/EU
RoSH 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 30 天与 PLC 不间断通讯，1 亿 3 千万次通讯 0 错误
认证	CE 认证
尺寸（L*W*H）	90*24*65mm
重量	120g

13.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：