

PLC 与组态软件建立无线数据通信（串口）

目录

| | | |
|----|-----------------------------------|---|
| 一、 | 概述..... | 2 |
| 二、 | 通信协议：Modbus 协议 | 2 |
| 三、 | PLC 通过串口连接 DTU 与组态软件实现通信： | 3 |
| | 1. 设置 PLC 为 Modbus 从机模式..... | 3 |
| | 2. Plc 通过 485 接口连接计算机串口..... | 3 |
| | 3. 组态软件新建 I/O 设备和变量实现本地数据采集 | 4 |
| | 4. 设置 DTU 实现 4G/2G 无线通信..... | 6 |
| 四、 | 推而广之： | 8 |

一、 概述

组态软件是用于数据采集与过程控制的专用软件。作为工业自动控制系统监控层一级的软件平台和开发环境，使用灵活的组态方式，为用户提供快速构建工业自动控制系统通用软件工具。

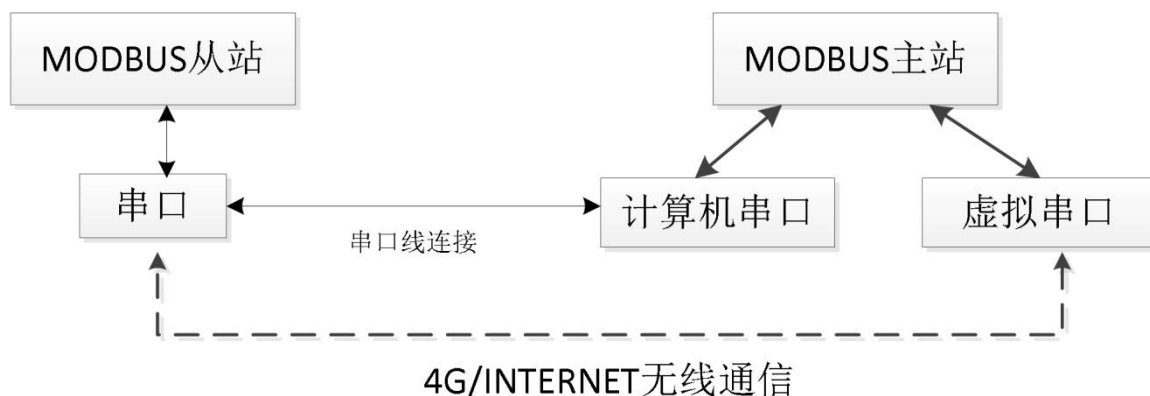
可编程逻辑控制器（Programmable Logic Controller，PLC），它采用一类可编程的存储器，用于其内部存储程序，执行逻辑运算、顺序控制、定时、计数与算术操作等面向用户的指令，并通过数字或模拟式输入/输出控制各种类型的机械动作或生产过程。

北京天同创新通信有限公司研发生产的 [4G DTU](#) 可以用于在组态软件和工业现场 PLC 之间建立可靠的基于 4G 网络的数据通信，实现无线远程监控和数据的采集。

二、 通信协议：Modbus 协议

使用 Comway 4G DTU 建立与组态软件的无线数据通信，理论上可以传输任何类型应用层数据报文，但无线通信相比有线通信的重要区别在于数据通信的延时较大且无规律，因此可以设置较长数据更新周期和通信延时的应用层数据协议更适合无线数据通信，所以 MODBUS 协议成为物联网业务的主流应用层数据协议。

PLC 的通信串口都支持 **Modbus RTU 通信协议**（欧姆龙可以选择 hostlink 协议），modbus rtu 协议的通信过程采取主从问答的方式，其采集周期可以灵活设置，适合 4G/2G 无线数据通信。

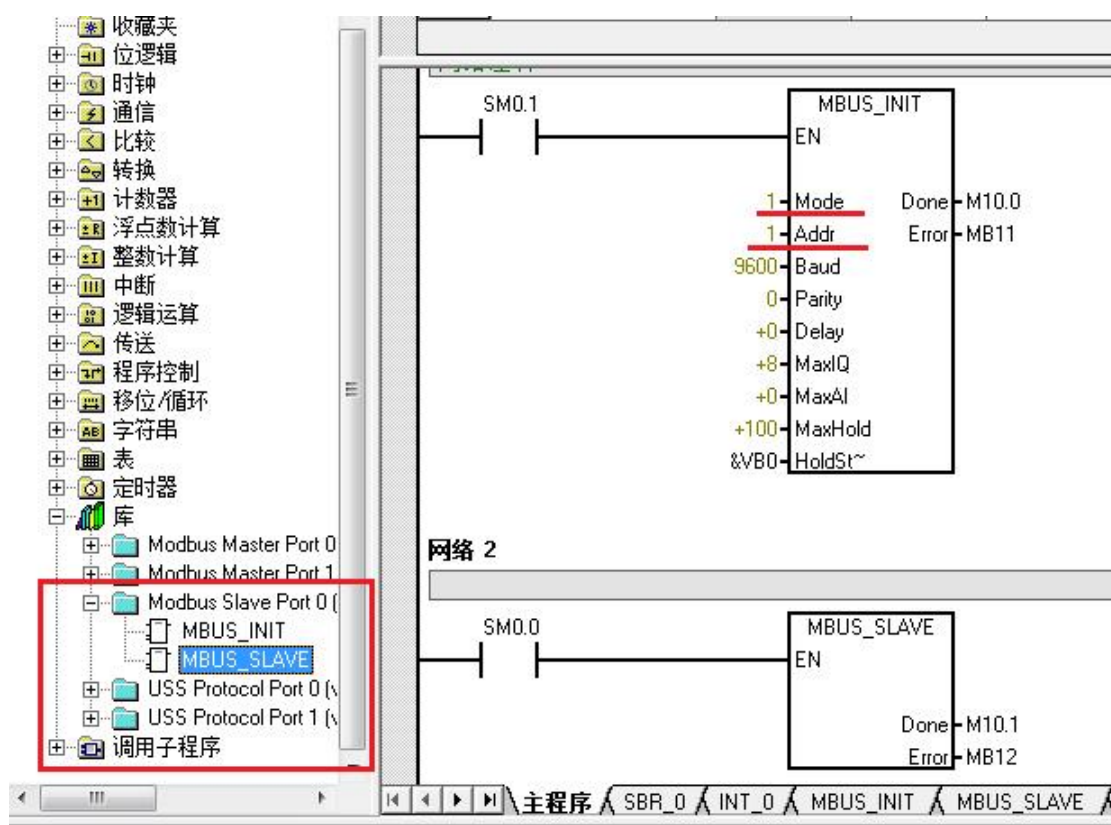


三、 PLC 通过串口连接 DTU 与组态软件实现通信：

以下以广泛使用的西门子 S7-200 通过 4G 网络连接组态王软件为例介绍实现的过程。

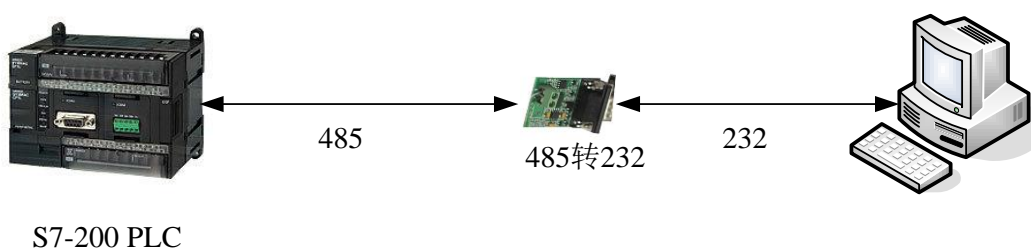
1. 设置 PLC 为 Modbus 从机模式

西门子 PLC S7-200 的 RS-485 串口设置为 **MODBUS 从机模式**，如下图所示，Modbus 设备地址为 1，串口波特率为 9600：



2. Plc 通过 485 接口连接计算机串口

S7-200 的串口为 DB9 接口，其中管脚 3 为 485 总线的 A，管脚 8 为 485 总线的 B，通过 485 转 232 接口与计算机的 RS-232 口连接。

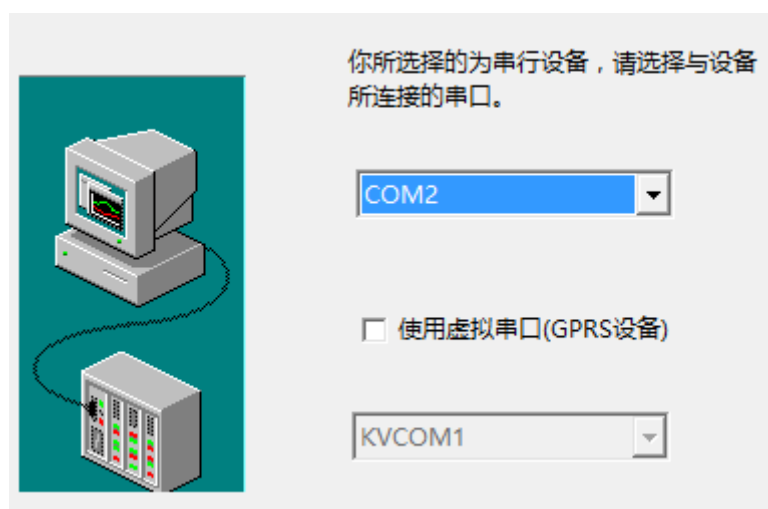


3. 组态软件新建 I/O 设备和变量实现本地数据采集

在组态软件新建 I/O 设备，如下图选择**莫迪康—Modbus Rtu--COM**。



通信端口选择与 PLC 连接的计算机串口，如下图示例中为 com2。



参考组态王软件 modbus 协议对应的寄存器变量地址，如下表所示：

| 寄存器格式 | 寄存器范围 | 读写属性 | 数据类型 | 变量类型 | 寄存器含义 |
|-------|---------|------|-------------|--------|-------------------|
| 0dddd | 1-65535 | 读写 | BIT | I/O 离散 | 逻辑线圈 (0XXXX) |
| 1dddd | 1-65535 | 读 | BIT | I/O 离散 | 输入位寄存器 (1XXXX) |
| 3dddd | 1-65535 | 读 | SHORT | I/O 整型 | 输入寄存器 (3XXXX) |
| | | | USHORT BCD | | |
| 4dddd | 1-65535 | 读写 | SHORT | I/O 整型 | 保持寄存器 (4XXXX) |
| | | | USHORT BCD | | |

在组态王软件的数据字典中新建 I/O 变量连接 I/O 设备，如下图示例即为新建 PLC 模拟量输入，寄存器地址：30001，注意采集周期设置为不低于 3000ms。



变量名: 模拟量输入

变量类型: I/O 整数

描述:

结构成员:

成员类型:

成员描述:

变化灵敏度: 0

初始值: 0

最小值: 0

最大值: 999999999

最小原始值: 0

最大原始值: 999999999

状态:

☐ 保存参数

☐ 保存数值

连接设备: 新IO设备

采集频率: 3000 毫秒

寄存器: 30001

数据类型: SHORT

转换方式:

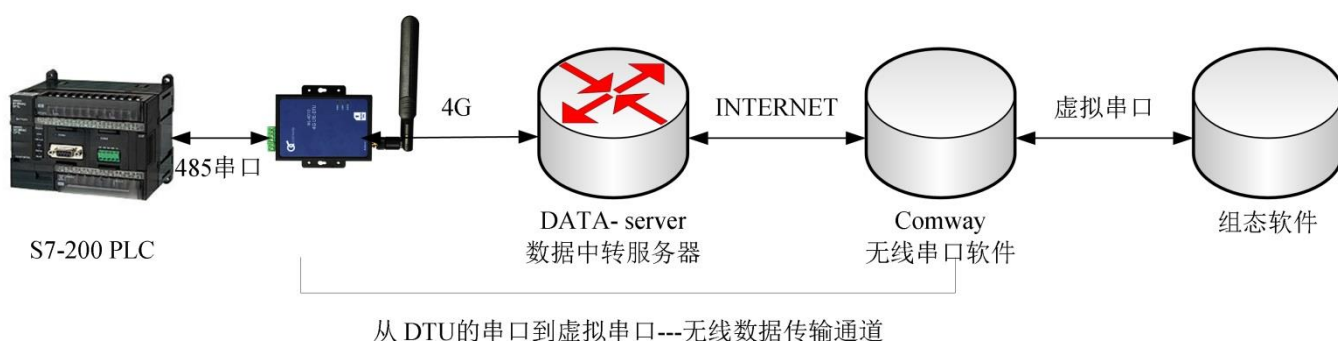
☒ 线性 ☐ 开方 高级

然后在组态王的画面中新建图形控件连接 I/O 变量，即可运行画面开始采集 PLC 的相关寄存器的数据，如数据显示正确，即完成组态软件和 PLC 通过本地串口以 Modbus RTU 方式数据通信过程。

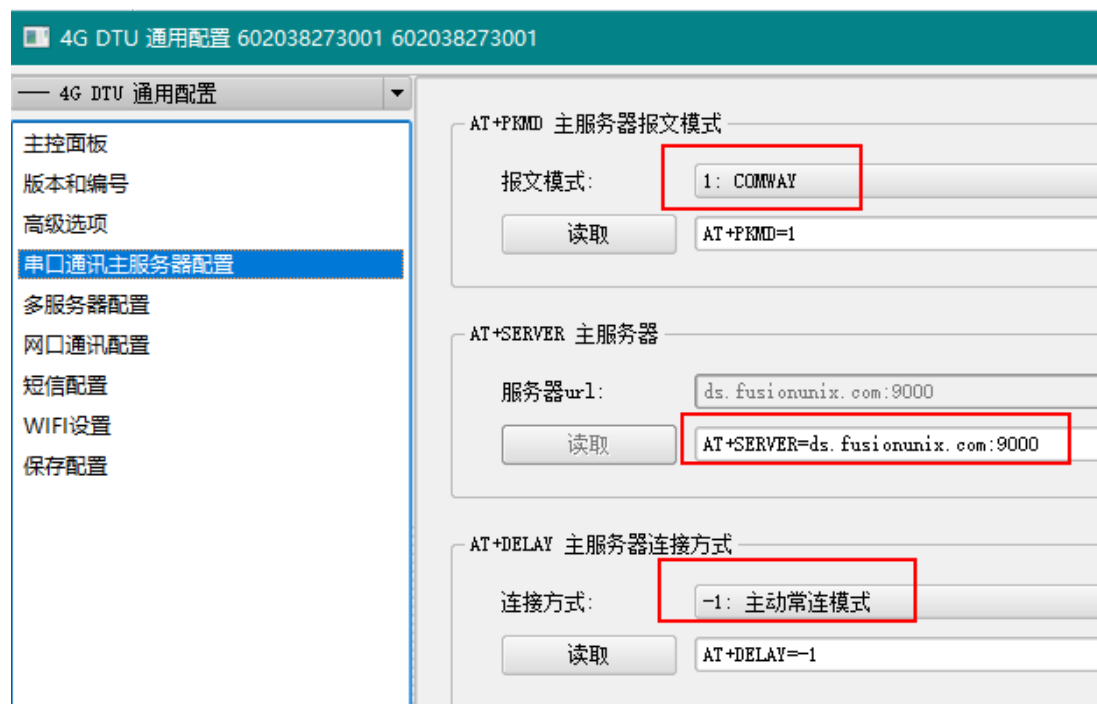
4. 设置 DTU 实现 4G/2G 无线通信

1) Comway 无线串口方式:

只要客户的计算机可以上网，安装 [Comway 无线串口软件](#) 即可通过 comway 通信平台实现无线数据通信，示意图如下：



在如下图串口通讯主服务器配置页面，需要选择 1: COMWAY 协议，默认服务器地址：**ds.fusionunix.com** 和端口号**(9000)**，DTU 模块 12 位条形码是出厂设定的唯一识别 ID 号。DTU 的串口参数需要与 PLC 的相关串口参数完全一致。

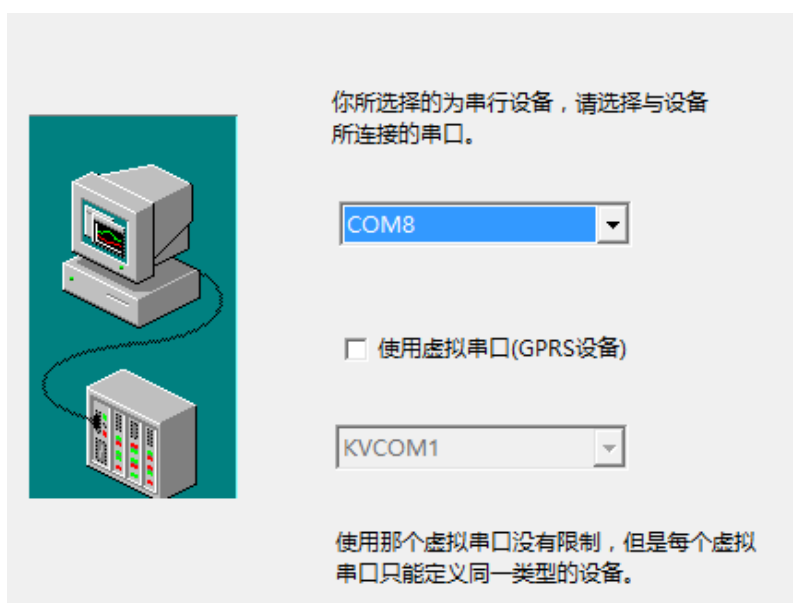


在计算机端安装 Comway 无线串口软件，DTU 插入 sim 卡上线后，将会在如下界面中显示 ONLINE，再映射 DTU ID 到添加的**虚拟串口 COM8**，如下图所示：



Comway 无线串口软件的具体安装和操作详见[相关说明](#)

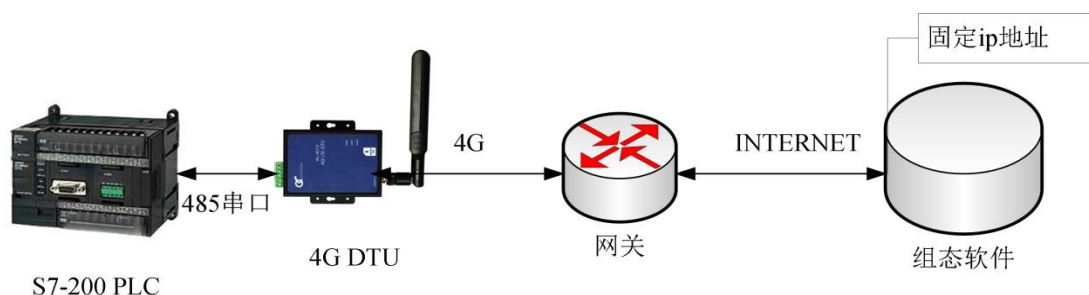
完成上述操作后，即可修改 I/O 设备在组态王软件中的通信端口，选择 comway 无线串口软件生成的**虚拟串口 com8**，如下图所示：



comway 无线串口软件在每个计算机上最多可以添加 128 个虚拟串口，而多个 DTU 可以映射到同一个虚拟串口（只要连接的设备的 modbus 地址不同），则组态软件可以同时与 500-1000 个 modbus 设备通过 DTU 建立 gprs 数据通信。

2) 固定 ip 或者动态域名方式：

中心服务器端具有公网固定 IP 地址或者安装动态域名软件，可以设置 4G DTU 通过 IP 地址或动态域名+端口访问组态软件，系统示意图如下图：



4G DTU 的通信协议可以设置为兼容桑荣协议或者兼容宏电协议，详见相关说明：

[COMWAY DTU 连接组态王配置说明](#)

[COMWAY DTU 连接三维力控配置说明](#)

四、 推而广之：

上述说明，详细介绍了 PLC 和组态软件建立无线数据通信的过程，推而广之，任何串口设备，如仪表、变送器和 RTU，只要在组态软件中有相关的设备驱动（即可以配合解析接收的数据的程序），均可通过 COMWAY DTU 建立无线数据通信。