

2026

ECS 工业通讯网关用户手册

V10.2



北京赛博利特科技有限公司

目录

| | | |
|----------|-----------------------------|-----------|
| 1 | 概述..... | 3 |
| 2 | 从这里开始 | 5 |
| 2.1 | 系统要求 | 5 |
| 2.2 | 包装清单 | 5 |
| 2.3 | 规格参数 | 6 |
| 2.4 | 产品选型 | 7 |
| 2.5 | 安装 ECS 主机 | 8 |
| 2.6 | 安装电源 | 8 |
| 2.7 | 接口说明 | 9 |
| 2.8 | ECS 工作原理 | 10 |
| 3 | 典型应用 | 10 |
| 4 | ECS 拓扑结构实例 | 11 |
| 4.1 | 连接的设备在同一网段 | 11 |
| 4.2 | ECS 连接的设备在不同网段..... | 11 |
| 4.3 | 网络设备与串口设备的互联互通..... | 12 |
| 4.4 | 串口设备之间的互联互通 | 12 |
| 4.5 | 复杂应用拓扑结构 | 13 |
| 5 | ECS 组态工具包（ECT） | 14 |
| 5.1 | 安装 ECS 组态工具包（ECT） | 14 |
| 5.2 | 安装 ECT 组态工具包 | 15 |
| 5.3 | 启动 ECT | 16 |
| 5.4 | 在多网卡计算机上启动 | 16 |
| 5.5 | 主界面 | 18 |
| 5.6 | 选择设备 | 19 |
| 5.7 | SYSTEM-系统界面 | 19 |
| 5.8 | NETWORK-网络 | 20 |
| 5.9 | MONITOR-在线监视模式 | 21 |
| 5.10 | 更新 ECS 固件 | 23 |
| 5.11 | 下载 ECS 组态配置 | 23 |
| 5.12 | 上传（备份）ECS 组态配置 | 24 |
| 6 | 组态配置 | 25 |

| | | |
|----------|---|-----------|
| 6.1 | 新建或打开已有组态 | 25 |
| 6.2 | 基本操作说明 | 26 |
| 6.3 | 设置通讯接口 | 28 |
| 6.4 | 设备管理 | 30 |
| 6.5 | 数据映射表 | 32 |
| 7 | 设备驱动说明 | 36 |
| 7.1 | LOGIX5000 系列控制器 | 36 |
| 7.2 | MODBUS TCP/RTU 系列设备 | 42 |
| 7.3 | 西门子 S7 系列 PLC | 50 |
| 7.4 | MITSUBISHI MELSEC Q 系列 PLC | 54 |
| 8 | 附录: | 58 |
| 8.1 | 子网掩码与 IP 地址及计算方法 | 58 |
| 8.2 | SIEMENS S7-1200/1500 通讯特殊设置 | 62 |
| 8.3 | SIEMENS S7-300 PLC 与 AB LOGIX 5000 系列 PLC 之间的数据交换 | 64 |
| 8.4 | CIP TEST TOOL 使用说明 | 69 |
| 8.5 | CIP 驱动心跳检测功能实现参考 | 71 |
| 8.6 | 心跳信号说明 | 72 |

1 概述

ECS 数据交换中心网关可提供安全可靠的数据连接与转换,使不同厂家的 PLC/DCS/数采系统实现互联互通并进行实时数据交换,低成本实现多网融合。

工业现场设备种类繁多,在企业自动化和信息化项目中,需要解决各种不同设备、系统之间的互联与集成。通讯方式和通讯协议的多样化问题一直存在,且越来越突出,工程技术人员需要投入大量的时间和精力解决不同系统之间的互联通信,已严重影响到自动化系统的性能、升级改造、工期、成本和系统稳定性等,解决自动化系统通信协议的转换及通信标准化的问题意义重大。

ECS 提供了完善的解决方案:使不兼容的协议之间互联互通,实现多网无缝融合,使不同协议之间实现实时的数据交换。

ECS 作为一款高性能工业通信网关,专用于解决自动化系统、企业信息化系统中各种不同通信标准、不同通信协议的系统之间的通信互联与互操作,简化实施过程,提高系统的性能,增加系统的稳定性,缩短项目工期,节约实施成本。

产品特点

- 用于 PLC/DCS/数采系统之间的数据交换
- 采用原生协议,无需编写通讯程序即可实现系统间的数据实时传输交换
- 无需添加专用模块即可接入第三方系统

- 系统间自动完成内部寄存器映射，实现数据同步
- 系统间数据交换支持双向读写操作
- 支持以太网(10/100/1000Mbps)及串口(RS232/485)设备之间的数据交换
- 配有简单易用的配置工具，同时具备通讯诊断功能

支持丰富通讯接口：

2 路以太网接口；

2~4 路串行通讯口（RS232、RS485）；

可提供更多类型接口的定制服务。

可连接不同的 PLC/DCS/数采系统

- Siemens Simatic S7 系列 PLC：S7-200/300/400, S7-200 Smart, S7-1200/1500, WinAC SoftPLC
- Rockwell Logix5000 系列 PLC：ControlLogix、CompactLogix、Softlogix
- Mitsubishi MELSEC Q 系列 PLC
- Modbus TCP 的设备(支持主从模式)
- Modbus RTU 的设备(支持主从模式)

支持的工业现场协议

- Siemens S7 ISO on TCP；
- AB Ethernet: CIP；
- Mitsubishi MELSEC MC ASCII*
- Modbus TCP Master/ Slave；

- Modbus RTU Master/ Slave;
- Modbus ASCII Master/ Slave;

2 从这里开始

2.1 系统要求

安装 ECS 配置工具包（ECT）需要的最低硬件和软件组件

电脑硬件配置

- 1GHz 或同等性能以上 CPU
- 最低 1GB 内存
- 最少 600MB 空闲磁盘空间
- 1024*768 或以上分辨率显示器

操作系统

- Windows 10(1709 版以上) /11 64-bit
- Win7/ Windows 10(1709 以下), 需要安装 OpenSSH 组件(可从 [ECT 下载页面](#) 下载)

2.2 包装清单

ECS 包装中包含的组件见随包装一起提供的包装清单, 在安装前请与包装清单确认是否完整。

2.3 规格参数

2.3.1 ECS-G2-02-04-204

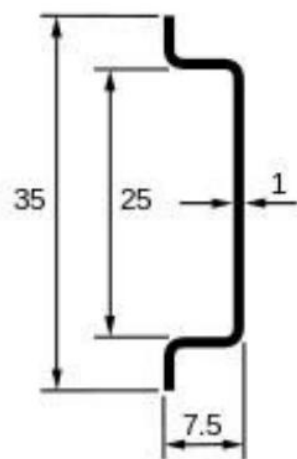
| 序号 | 项目 | 参数 |
|----|------------|---|
| 1 | 安装方式 | DIN 35mm 导轨/挂耳安装 |
| 2 | 以太网 | 2*RJ45 10/100Mbps |
| 3 | 以太网防护 | 支持 AUTO MDI/MDIX 双级抗雷防护 ◆ 支持 GB/T 17626.5-2008 标准中 10/700uS 测试的 3 级 2KV 防护 ◆ $\pm 15\text{kV}$ Human Body Model ◆ $\pm 15\text{kV}$ IEC61000-4-2 Air Discharge |
| 4 | 串口 (RS485) | 4*RS485 9600~115200bps |
| 5 | RS485 防护 | 支持收发数据指示灯, RS485 采用三级防护 ◆ 支持 GB/T 17626.5-2008 标准中 10/700uS 测试的最高等级 4KV 防护 ◆ $\pm 15\text{kV}$ Human Body Model ◆ $\pm 15\text{kV}$ IEC61000-4-2 Air Discharge |
| 6 | 串口 (RS232) | 2*RS232 9600~115200bps |
| 7 | RS232 防护 | 全独立隔离 RS232 接口 (2 个全隔离 RS232 接口分别与 COM3 和 COM4 端口上的 RS485 为复用关系) ◆ $\pm 15\text{kV}$ Human Body Model ◆ $\pm 15\text{kV}$ IEC61000-4-2 Air Discharge |
| 8 | 电源 | DC +9V ~ +48V, $\leq 5\text{W}$ |
| 9 | 电源防护 | ◆ GB/T 17626.5-2008 标准 4 级 (4KV) 8/20uS 雷击测试 ◆ 防反接保护 ◆ 过压保护 ◆ 抗脉冲群保护 ◆ 抗静电: ● $\pm 15\text{kV}$ Human Body Model ● $\pm 15\text{kV}$ IEC61000-4-2 Air Discharge |
| 10 | 硬件平台 | HTNICE GT665X |
| 11 | 外形尺寸 | 128 x 117 x 28 mm (W x H x D), |
| 12 | 重量 | 460g |
| 13 | 操作温度 | -40 ~ 85 °C |

2.4 产品选型

| 型号 | 网口数量 | 串口数量 | 串口支持类型 | | |
|------------------|------|------|--------|-------|-------|
| | | | RS232 | RS422 | RS485 |
| ECS-G2-02-04-204 | 02 | 04 | 2 | 0 | 4 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

2.5 安装 ECS 主机

ECS 可安装在 35mm 标准导轨上，也可通过挂耳安装



2.6 安装电源

ECS 支持 9VDC~48VDC 之间的基准电压, 连接电源时请确认所配电源规格型号。整机功耗 $\leq 5\text{W}$ 。



2.7 接口说明



2.8 ECS 工作原理

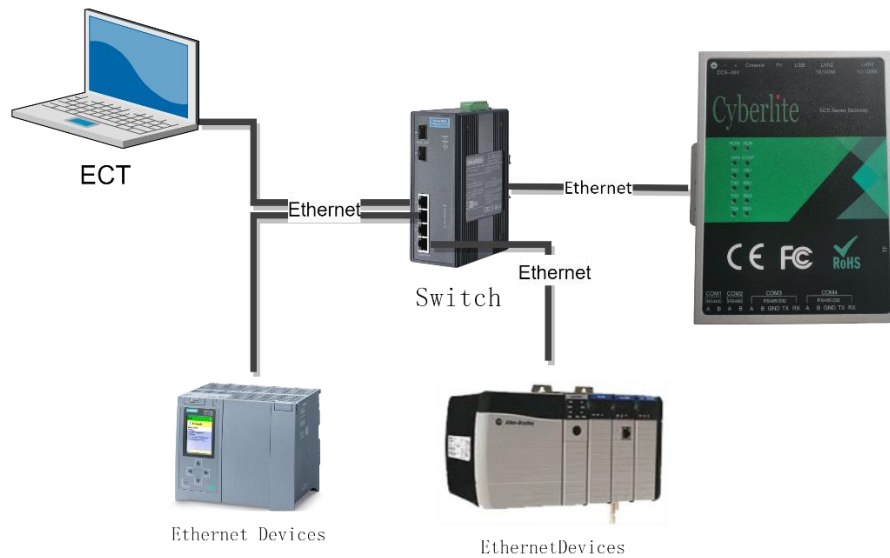
ECS 不同于普通的通讯网关仅仅是对各种网络协议做报文转换,普通网关只是解析出请求报文的内容,然后再转换为另一种协议,且只支持一种协议到另一种协议的被动转换。ECS 数据转换模式为主动模式, ECS 会根据创建的寄存器映射表实时的保持系统间数据的同步, ECS 可视为数据交换的中央枢纽,支持多种协议、多种链路同时进行系统级数据交换。

3 典型应用

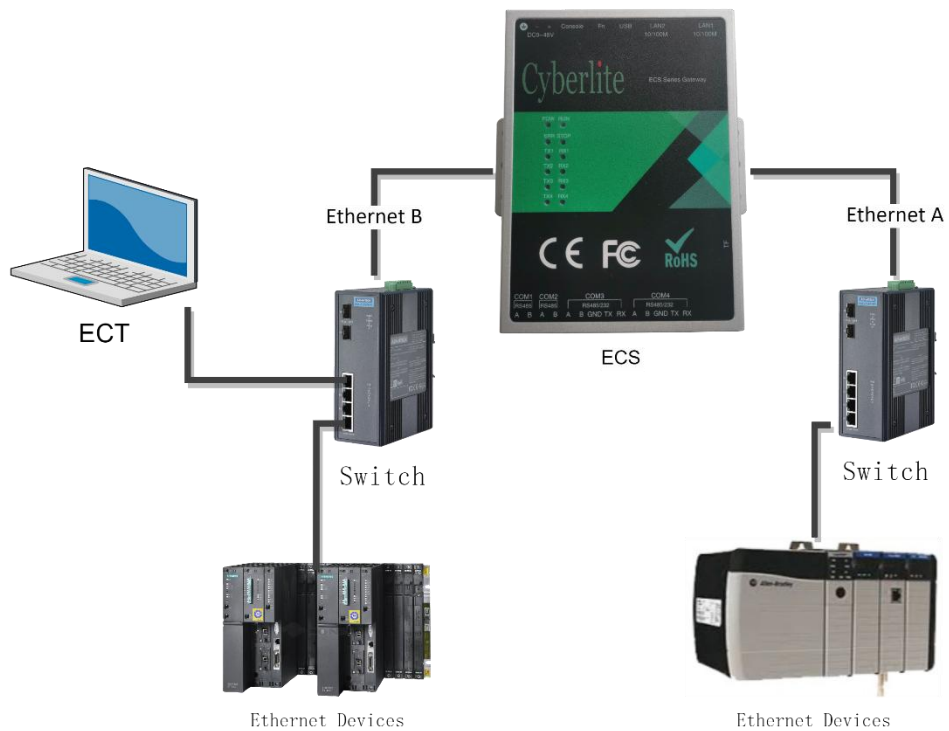
- 无需编程即可实现 PLC 与 PLC 之间的数据同步、交换;
- 无需编程即可为现有 PLC 系统添加第三方协议支持;
- 可不编程、不修改组态把旧系统接入到新的系统中;
- 统一现场多种协议;
- 数采网关;
- 串口设备接入以太网网络
- 分布式数据采集装置
- 工业协议转换网关
- 协议转换器
- 通讯服务器
- PLC 转换为标准 ModBus 设备 (RTU/TCP)

4 ECS 拓扑结构实例

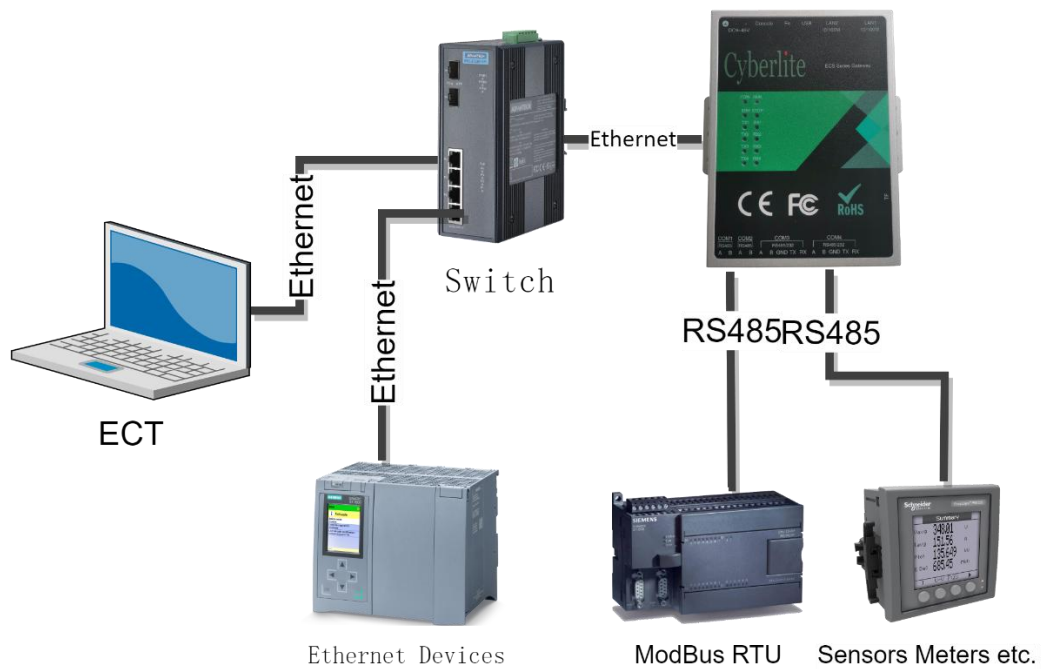
4.1 连接的设备在同一网段



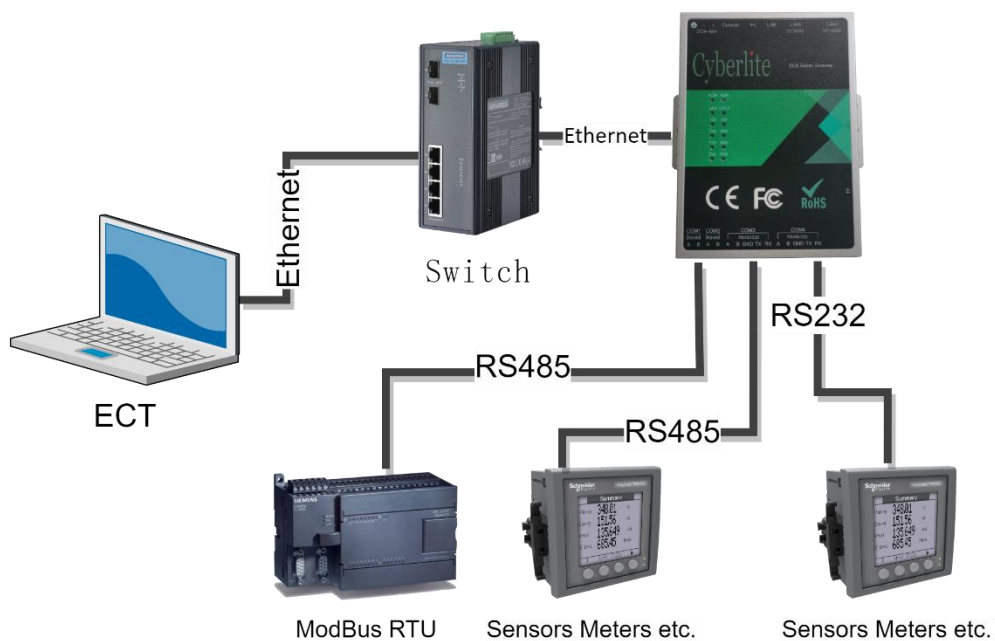
4.2 ECS 连接的设备在不同网段



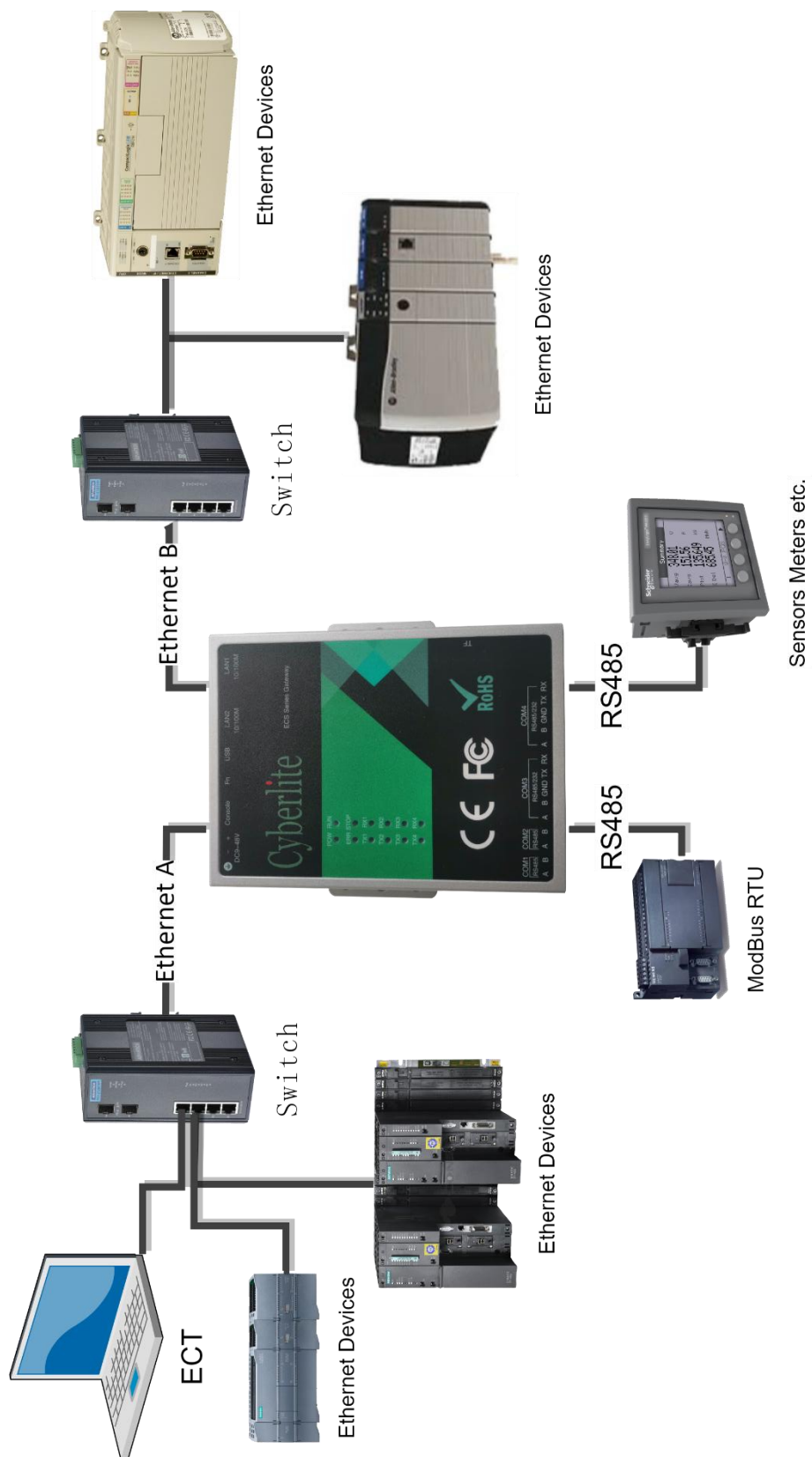
4.3 网络设备与串口设备的互联互通



4.4 串口设备之间的互联互通



4.5 复杂应用拓扑结构



5 ECS 组态工具包（ECT）

5.1 安装 ECS 组态工具包（ECT）

在对 ECS 主机组态前必须先安装 ECS 组态工具包---ECT。ECT 是 ECS 网关的集成化组态配置工具，ECT 提供以下功能：

- 离线组态；
- 管理网络上的 ECS 主机；
- 远程设置 ECS 主机；
- 下载离线状态下组态的 ECS 组态信息；
- 备份 ECS 主机的组态信息；
- 对 ECS 主机进行系统升级；
- 在线通讯诊断功能；

ECT 组态工具包可以通过以下途径获取：

1. 通过 [www.cyberlite.com.cn\getect](http://www.cyberlite.com.cn/getect) 下载最新版本。

注意：ECT 安装包完整版安装安装包和升级安装包，第一次在计算机上安装 ECT 需要选择完整安装包安装，在已安装 ECT 的计算机上安装 ECT 更新包只需下载升级安装包即可。

完整版安装包名称：ECT Install ver+版本号

升级版安装包名称：ECT SP Install ver+版本号

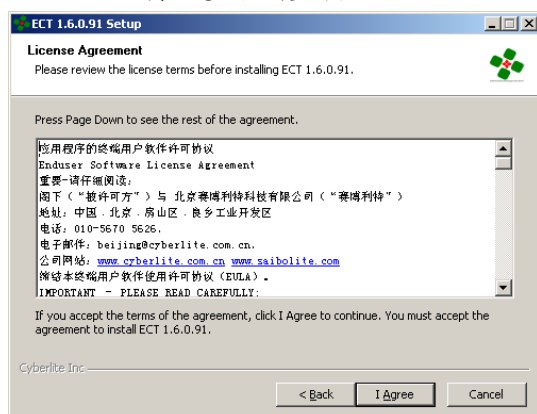
5.2 安装 ECT 组态工具包



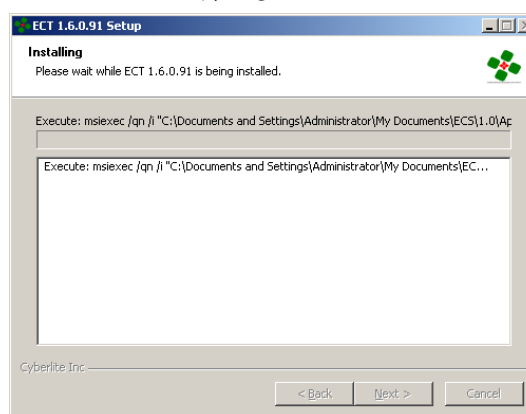
第 1 步双击安装包



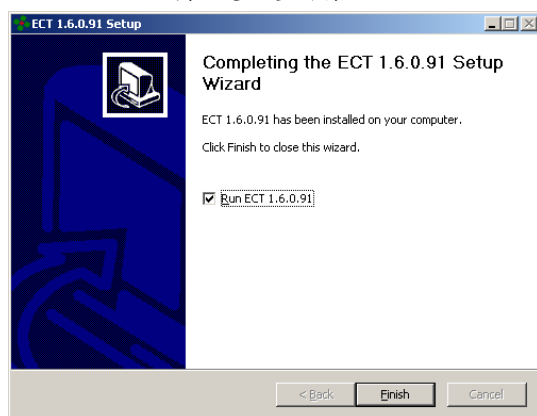
第 2 步



第 3 步 安装信息




第 4 步 安装中

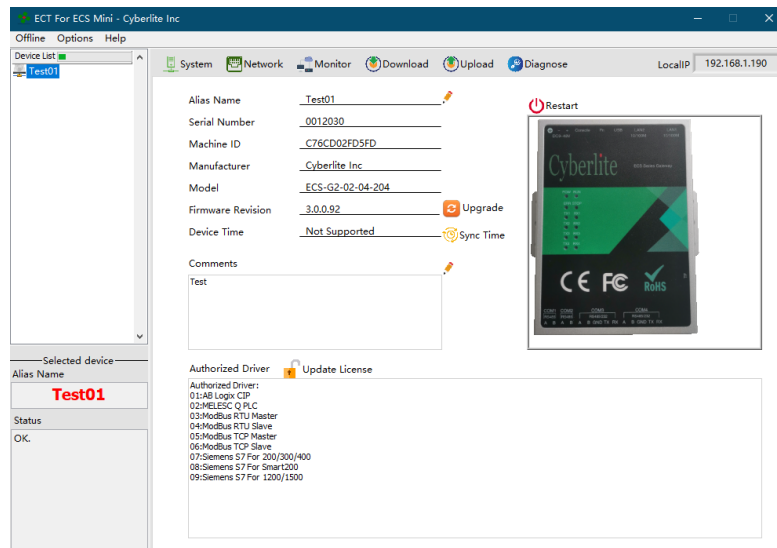


第 5 步 安装完成

注意：受制于不同版本 Windows 的差异，安装完成后如发现启动异常，请重启 Windows 后再次尝试。

5.3 启动 ECT

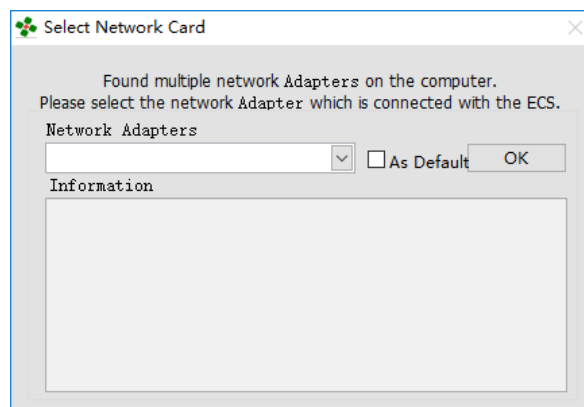
1. 在桌面找到 ECT 的快捷方式  ECT.exe
ECS Config Tool
Cyberlite
2. 开始-->程序-->Cyberlite-->ECT V3.exe



ECT 的主窗口分为两部分,左侧为网络上已存在的 ECS 设备列表,右侧为选中的 ECS 设备的详细信息。启动后,ECT 会自动搜索网络上已存在的 ECS 主机,并显示在 ECS 列表区。

5.4 在多网卡计算机上启动

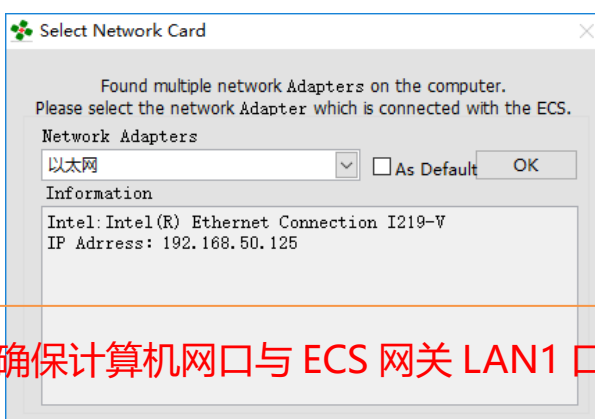
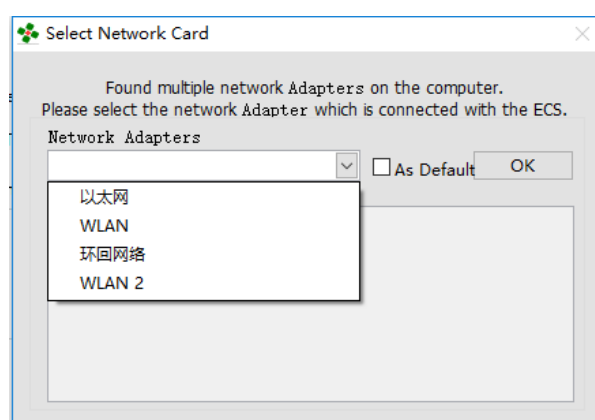
在安装有多个网卡的计算机上启动 ECT 需要选择用于通讯的网卡。



ECT 在启动时会自动检测计算机上是否安装了多个网卡，如存在多个网卡，ECT 将会弹出对话框，提示选择使用的网卡。

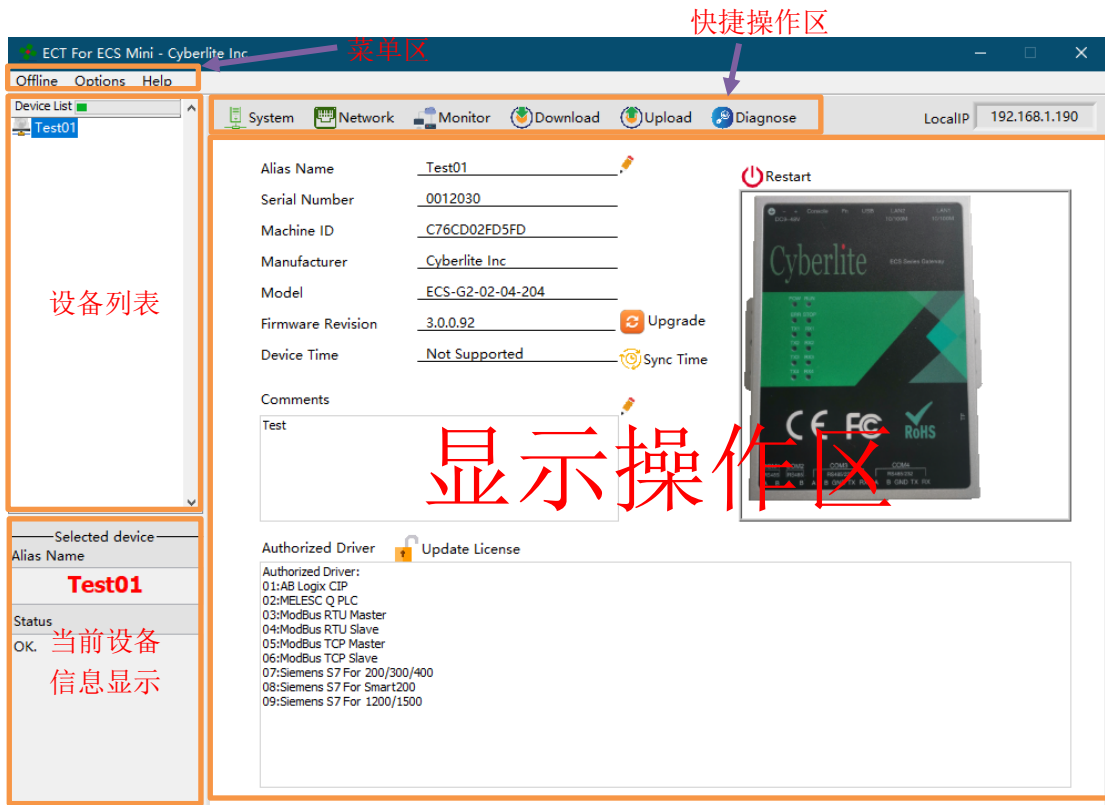
比如本例中，计算机上安装有多个网卡，计算机通过有线网卡经过交换机与 ECS 网关连接，在本例中需要选择【以太网】这个网关，在选择网卡后，网卡信息会显示出来，请确认该 IP 是否可网关是否在同一网段中，如不再同一网段中则需要修改网关或者计算机的 IP 设置，使网关和计算机处于同一网段中，否则无法启用【在线调试】。

【As Define】通过勾选此选项可设置当前选择的网卡为默认启动网卡，再次启动时将不再提示网卡选择对话框，根据默认设置自动选择，如需修改请通过菜单打开设置界面，菜单路径：【Option】→【Network Adapter】。



注意：需确保计算机网口与 ECS 网关 LAN1 口是相通的，
否则无法搜索到网络上的 ECS 网关设备

5.5 主界面



主界面区分为：

1、菜单区：菜单操作选项

1、Offline：离线组态菜单；

【New】：新建组态

【Open】：打开已有组态

2、Option：功能操作

【Network Adapter】：安装多网卡时网卡选择（安装多网卡时，ECT 启动时会自动弹出此对话框，但当设置了默认网卡，需更改网卡时需要在这里修改）

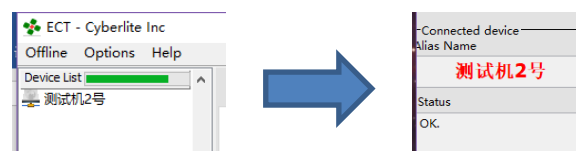
2、设备列表区：ECT 启动后会自动搜索已接入网络的 ECS 终端，并显示在该列表中，**双击列表中的设备名称即可选中设备**，选中

后即可对该设备进行设置操作。

- 3、 **当前设备信息显示区**：用于显示当前正在先选中设备的名称及实时状态信息显示。
- 4、 **快捷操作区**：用于切换设置选项、上传、下载配置文件、保持设置、重启设备等操作。
- 5、 **LocalIP**：当前用于与 ECS 通讯的网卡的 IP 地址
- 6、 **显示操作区**：用于显示设备的设置信息、修改设备设置以及在线诊断。

5.6 选择设备

通过双击设备列表中已搜索到的设备即可设置该设备为选中激活状态，即可对该设备进行设置修改或进入在线监视。同时当前设备区会显示设备名称和设备返回的状态信息。



5.7 System-系统界面

通过快捷操作区的 System 按键可切换到系统信息显示区。



AliasName: 设备别名, 默认别名为设备的出厂序列号, 可修改。

点击名称后面的【铅笔】图标即可编辑别名。

SerialNumber: 设备的出厂编号。

Machine ID: ECS 网关的硬件 ID, 设备唯一识别值。

Model: 设备的产品型号

Fireware Revision:设备的软件版本号。

DeviceTime: (部分型号可用)当前设备的时间, 可通过 SyncTime 来设置设备时间与当前计算机时间同步。

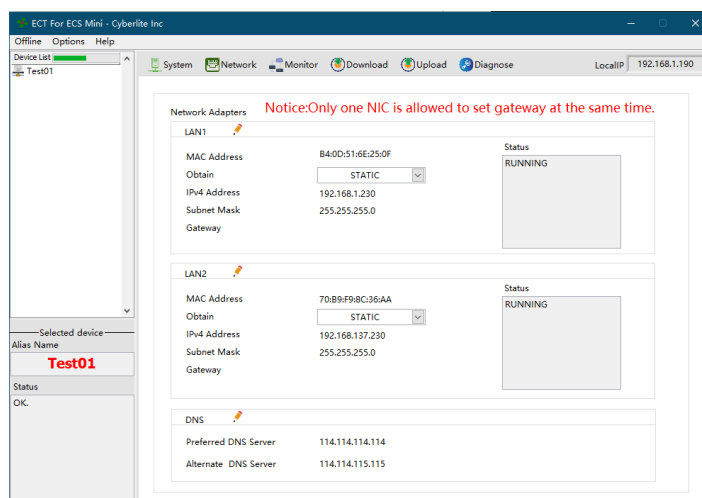
Coments: 设备描述信息。

Authorized Driver: 已授权的可用设备驱动。

Update License: 更新授权, 用于更新可用的设备驱动。

5.8 Network-网络

通过快捷操作区的 Network 按键可切换到 ECS 网络信息显示区, 可查看当前 ECS 网卡设置信息并可修改网卡设置。



通过【铅笔】图标即可进入编辑模式, 设置完成后点击保存, 修

改成功后 ECS 网关设备会自动重启，重启后生效。

有关 IP 与子网掩码的设置可参考附录 1

注意：只能设置一个默认网关，如果每个网卡都设置了默认网关，在跨网络通讯时会出现网络无法访问的现象。

5.9 Monitor-在线监视模式

通过快捷操作区的 Monitor 按键可切换到在线监视模式，可在在线监视网关的执行状态。



- 【ECSIP】：当前 ECS 用于与 ECT 连接的 IP
- 【Status】：当前 ECT 与 ECS 的连接状态，Conceded 表示已连接
- 【Refresh interval】：数据刷新闻隔，单位秒，默认 2 秒
- 【Mapping List】：当前 ECS 已创建的所有映射表。双击列表中的某个映射表可以激活所选的映射表，在右侧区域可用查看选中映射表的详细信息

【Mapping Table Name】：当选处于激活状态映射表的名称

【DataType】：当前选中的映射表传送的数据的数据类型

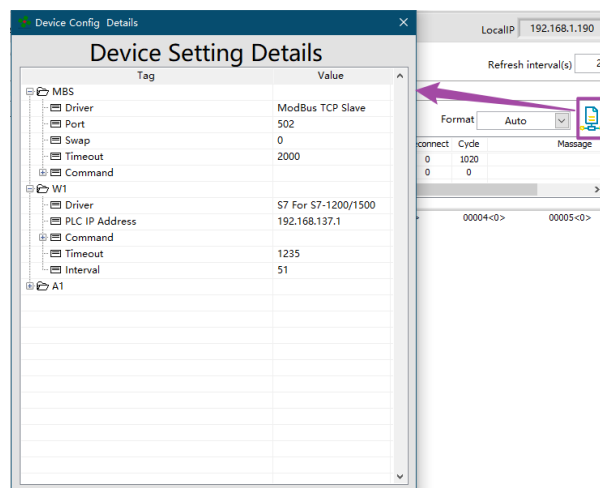
【Format】：设置数据区数据显示的格式，可选择显示十进制、十六进制、二进制

【设备信息区】：显示当前激活的映射表关联的设备的运行状态

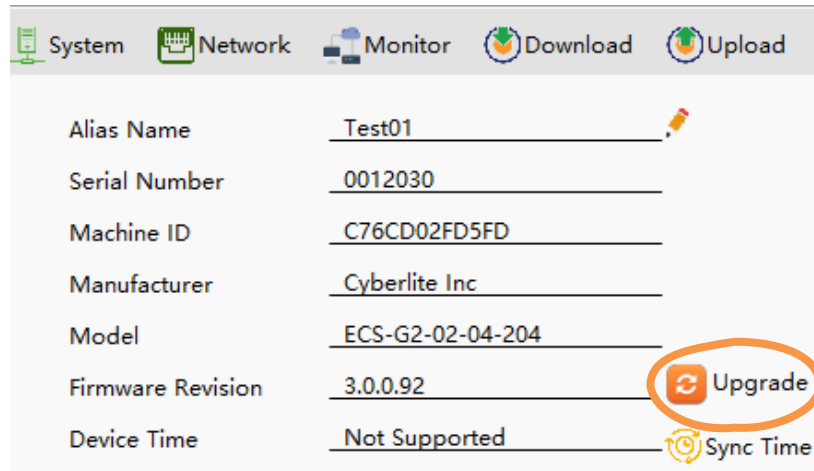
- ✓ Device：设备名称
- ✓ Connect：当前设备通讯状态
- ✓ Request：网关向 PLC 发送的读写总指令数
- ✓ Answer：PLC 正确响应网关请求的指令数
- ✓ Error Answer：错误响应数
- ✓ Reconnect：无响应或超时重连次数
- ✓ Cycle：当前设备轮询完所有映射表需要的时间，毫秒

【数据显示区】：显示当前映射表的实时数据

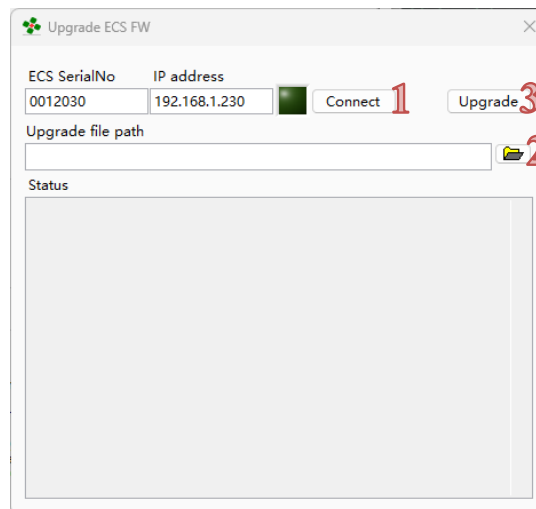
【查看设备组态配置】：通过打开查看设备设置详情按钮图标可打开设备设置显示窗口，用于查看当前设备的组态配置，用于配置信息的核验。



5.10 更新 ECS 固件



在 System 界面通过打开 ECS 固件升级界面。



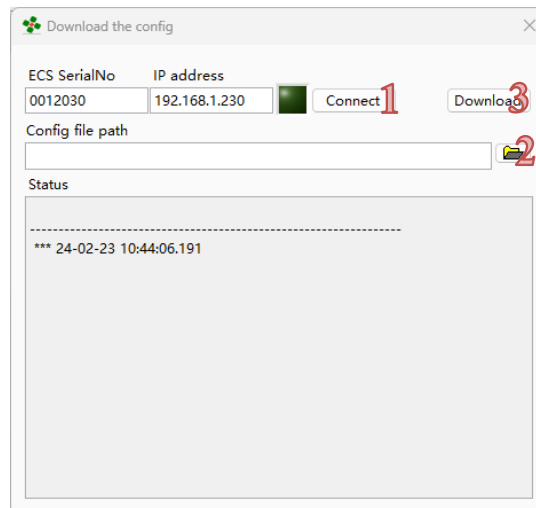
升级步骤：

- 1、点击【Connect】按钮连接设备
- 2、选择升级文件的存放路径，固件包的后缀名为 EUF
- 3、点击【Upgrade】按钮开始升级固件
- 4、升级完成后 ECS 会自动重启
- 5、重启完成后通过双击 Device List 中的设备名称，在 System 界面可以查看到最新的固件版本号。

5.11 下载 ECS 组态配置



通过【Download】快捷按钮可以启动 ECS 组态下载界面。



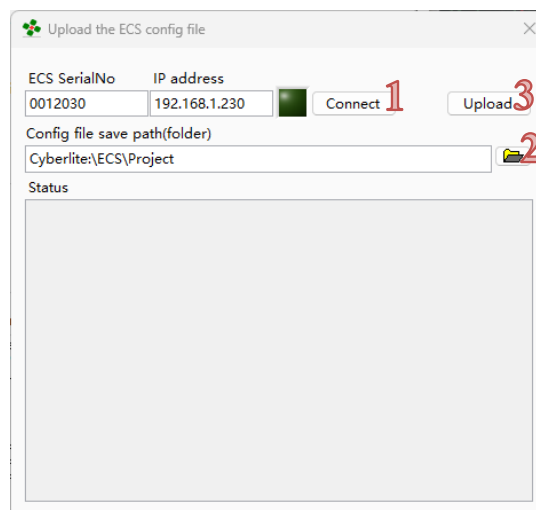
下载步骤:

- 1、 点击【Connect】按钮连接设备
- 2、 选择 ECS 组态文件的存放路径，固件包的后缀名为 ECS
- 3、 点击【Download】按钮开始下载
- 4、 下载完成后 ECS 会自动重启
- 5、 重启完成后 ECS 自动加载最新的组态配置并启动设备间的数据交换

5.12 上传（备份）ECS 组态配置



通过【Upload】快捷按钮可以启动 ECS 组态上传（备份）界面。



上传（备份）步骤:

- 1、 点击【Connect】按钮连接设备
- 2、 选择保持 ECS 组态文件的路径
- 3、 点击【Upload】按钮开始上载并保持在指定路径

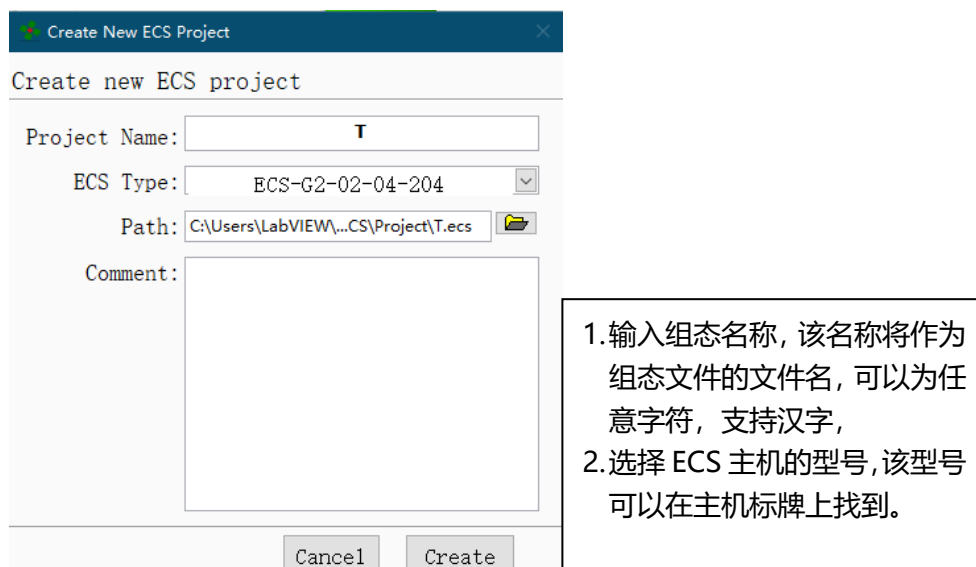
6 组态配置

在 ECS 主机投入使用之前，需要对 ECS 主机先进行配置，并将配置信息下载到 ECS 主机。可通过工具栏的快捷指令新建或打开已有的 ECS 配置文件对 ECS 进行配置。

6.1 新建或打开已有组态

在 ECS 主机未接入网络时可以通过工具栏的快捷命令启动离线组态工具——ECS Builder。

在 Offline 菜单中可以进行离线组态，【Offline】→【New】新建 ECS 组态，【Offline】→【Open】打开已有 ECS 组态。



图示：新建 ECS 组态



图示：打开已有的 ECS 组态

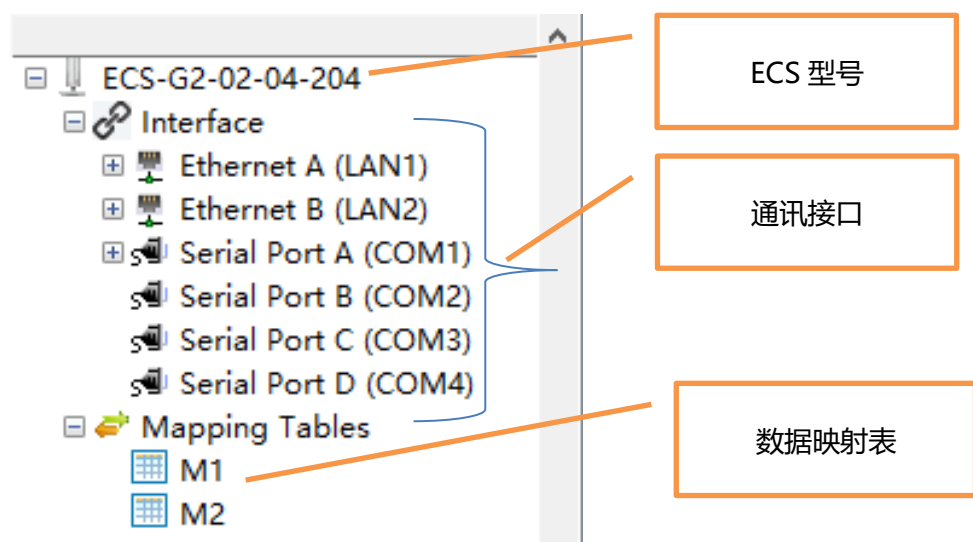
6.2 基本操作说明



图示：ECS bulier 操作界面

启动后的 ECS Builder 用户界面如图所示，操作界面工分为三个区域，分别为操作导航区（导航区）、详细信息显示区（信息区）和状态信息显示区（状态区）。

导航区



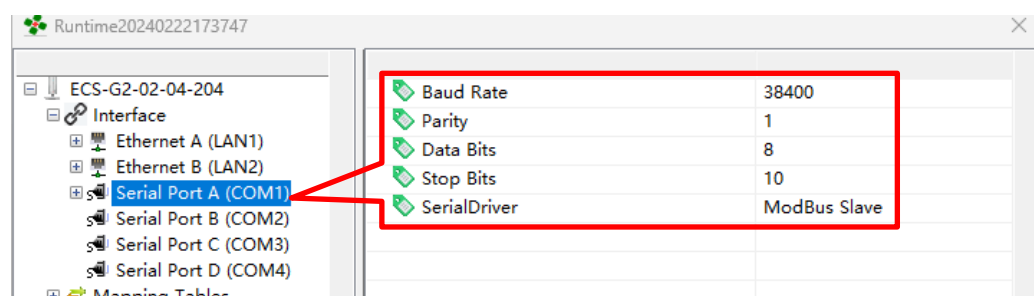
- **ECS 型号**: 新建组态是选择的 ECS 的型号;
- **通讯接口**: 当前型号 ECS 所支持的通讯接口
- **数据映射表**: 创建的所有 ECS 数据映射表都会在该区域显示。

导航区操作约定

导航区以树形列表的形式显示, 操作可分为鼠标左键单击 (单击) (在有些操作中称为“选中”), 鼠标左键双击 (双击) 和鼠标右键单击 (右键) 三种操作模式, 其具体操作约定如下:

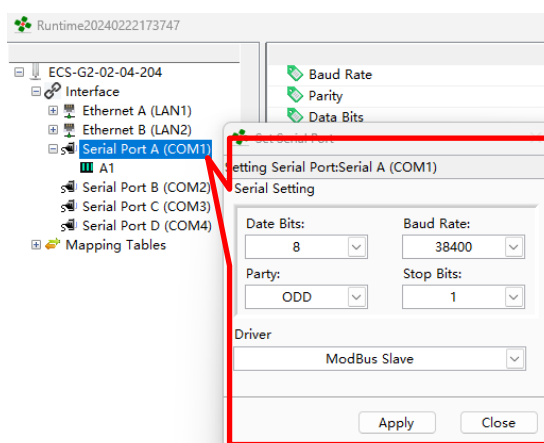
● 单击

单击树形导航列表中一个分项后, 右侧显示区将会显示该项包含的详细信息, 例如单击接口 Serial Port A, 将显示串口 A 口的配置信息;



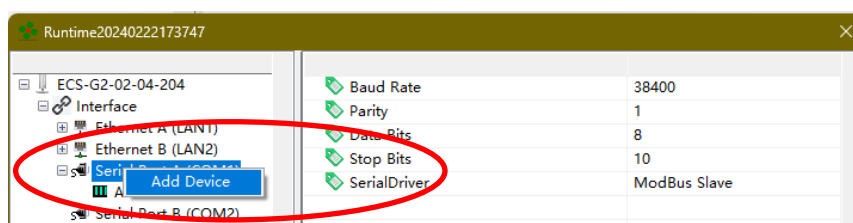
● 双击

双击树形导航列表中一个分项后，如该项包含设置信息，将会弹出该项的设置对话框，例如双击接口 Serial Port A，将弹出串口 A 口的配置对话框；



- **右键**

先通过**单击**操作选中树形导航列表中一个分项，然后在该分项上点击鼠标右键，将会弹出右键快捷指令，用于在指定通讯接口下添加或删除设备驱动以及新建或删除数据映射表等操作。

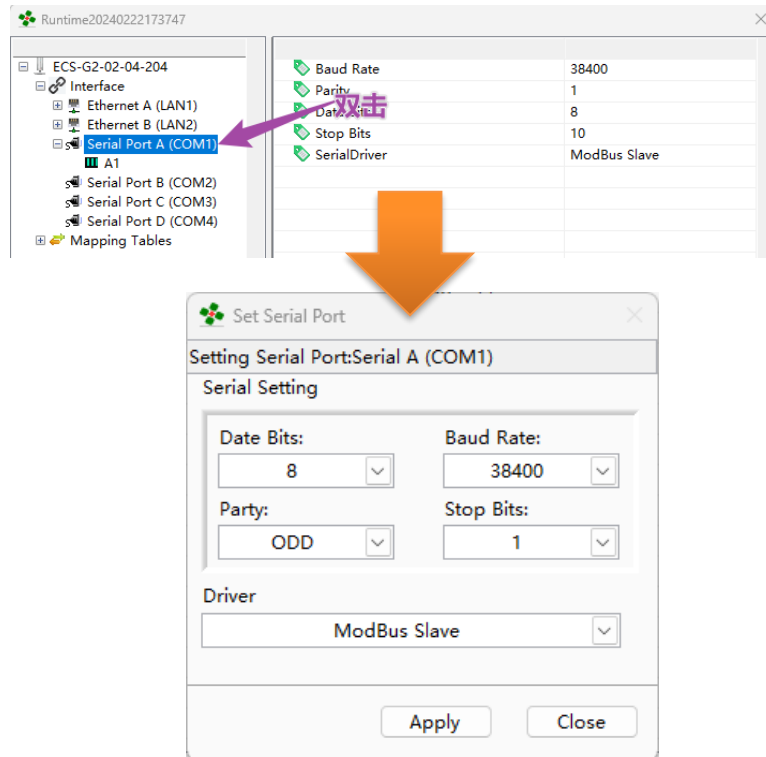


6.3 设置通讯接口

- **设置串行通讯口**

ECS 的串行通讯口支持 RS232、RS485、RS422，具体支持的接口类型取决于 ECS 的型号，详见 2.4 产品选型章节。

通过双击列表中串行通讯接口，即可弹出该串行接口的设置窗口



Data Bits: 数据位，支持 7、8 位数据格式；

Baud Rate: 传输波特率, 单位 bps, 支持 9600, 19200, 28800, 38400, 57600, 76800 以及 115200；

Party: 奇偶校验位, NONE, ODD, EVEN, MARK 和 SPACE；

Stop Bits: 停止位，支持 1bit, 1.5bits 和 2bits；

Driver: 选择串口下挂载的设备驱动

Apply: 更新设置；

Close: 保持现有设置并退出。

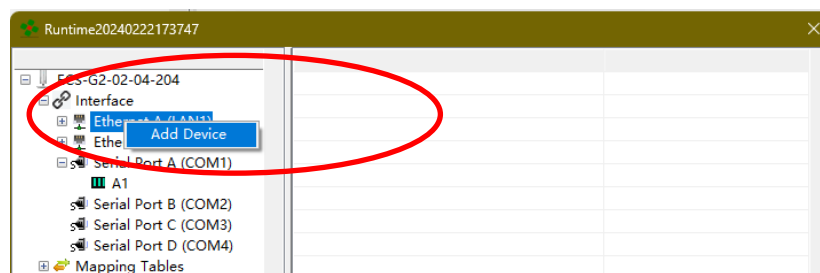
注意: 当串口为 RS485 模式时，ECS 支持在同一串口下挂载多个串行通讯设备，要求总线上串行设备的设置必须和 ECS 的设置保持一致。例如 Serial Port A 为 RS485 模式时，可连接多个通讯协议为 ModBus RTU 的设备，这些设备的波特率等串口参

数必须和 ECS Serial A 的设置保持一致，ECS 将通过通过轮询的方式与这些设备通讯。

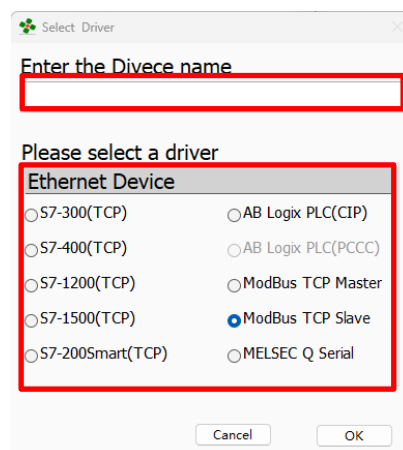
6.4 设备管理

● 添加设备

1. 确定与设备连接的通讯接口；
2. 选中通讯接口；
3. 在选中的通讯接口上单击右键，弹出快捷菜单；
4. 通过菜单 Driver→Add Driver 进入驱动选择窗口；



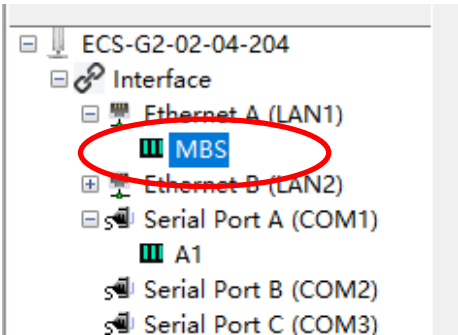
5. 选择对应的设备驱动，并为该设备命名；



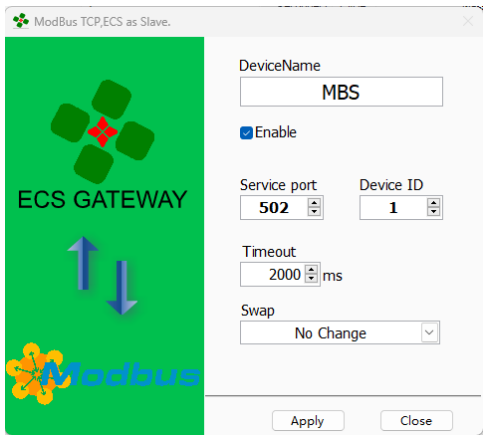
6. 通过 “OK” 确认添加新设备并退出，“Cancel” 取消添加新设备并退出。

● 设置、修改设备属性

添加设备后，会出现在对应的通讯接口下。选中并双击添加

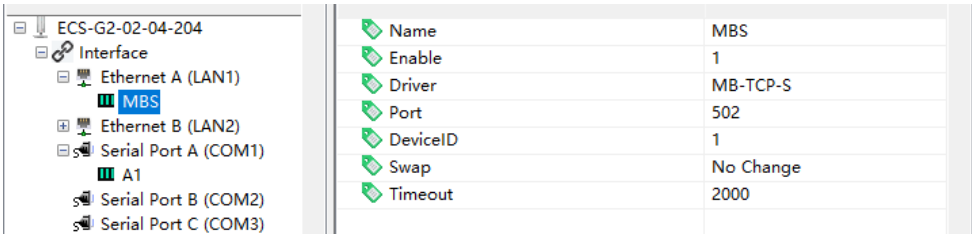


的设备即可弹出设备的设置窗口。不同的设备的设置内容有所不同，具体设置请参阅附录中具体驱动对应说明。



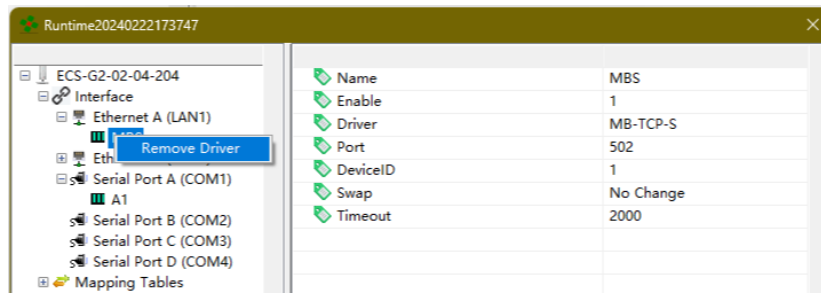
● 查看设置属性

可通过双击导航中的设备项在设置窗口中查看也可以通过单击设备项在右侧的信息区查看。



● 删除设备

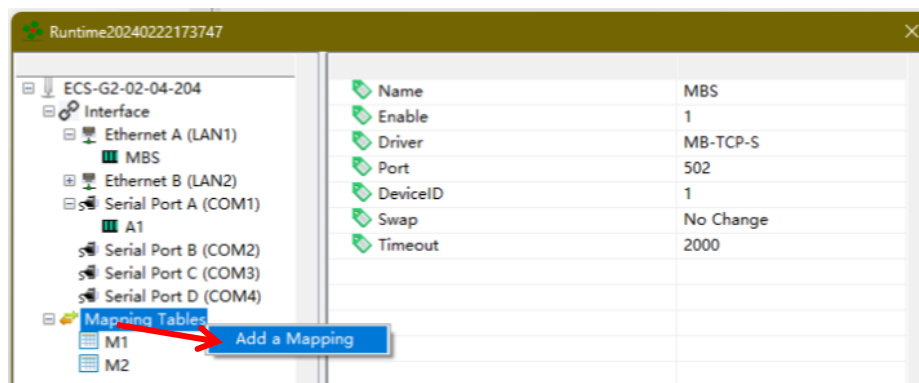
选中设备后，通过右键菜单 Driver→Remove Driver 删除已添加的设备。



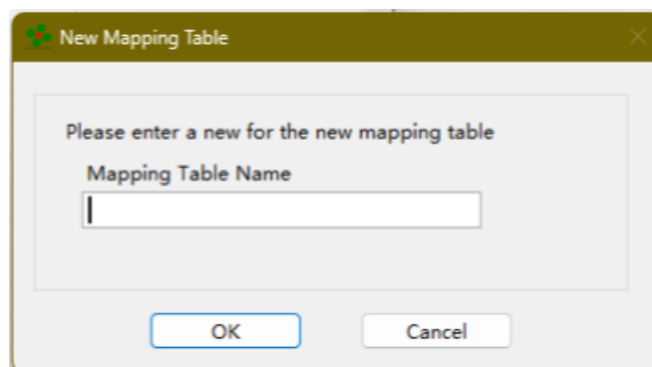
6.5 数据映射表

ECS 通过创建数据映射表将不同设备（PLC/DCS/数采系统等）的内部数据关联起来，并实时更新。从而实现不同系统之间的数据交换，实时同步。每个数据映射表都包含【数据源】、同步的【数据类型】和【数量】以及数据的【同步目标】，ECS 根据数据映射表的组态将一个或一组数据从数据源同步至数据目标。

● 新建数据映射表



1. 选中“Mapping Table”项；
2. 在“Mapping Table”上单击右键调出快捷操作指令；
3. 通过“Mapping Table” → “Add a Mapping”新建数据映射表；



4. 输入新建数据映射表的名称；可为任意字符，支持中文，不可重复；

● 组态数据映射表



1. **表名称**：新建时输入的表名；
 2. **数据源**：数据在数据源设备中的起始地址，可以是寄存器、也可以是变量名，具体设置详见附录具体设备驱动的使用说明；
- ◆ **Interface**：通讯接口，选择数据源设备所连接的通讯接口；

- ◆ **Driver:** 选择数据源所在的设备;
 - ◆ **DataArea/TagName:**寄存器或变量名;
 - ◆ **Starting:** 起始地址, 具体参照具体说明。
3. 数据传送设置: 数据传送的类型及数据长度
- ◆ **DataType:** 数据类型, **数据源与数据目标的数据类型应一致;**
 - ◆ **Quality:** 传送的数量。
4. **数据目的地:** 数据传输的目标地址, 可以是寄存器、也可以是变量名, 具体设置详见附录具体设备驱动的使用说明;
- ◆ **Interface:** 通讯接口, 选择数据目标设备所连接的通讯接口;
 - ◆ **Driver:** 选择数据目标所在的设备;
 - ◆ **DataArea/TagName:**寄存器或变量名;
 - ◆ **Starting:** 起始地址, 具体参照具体说明。

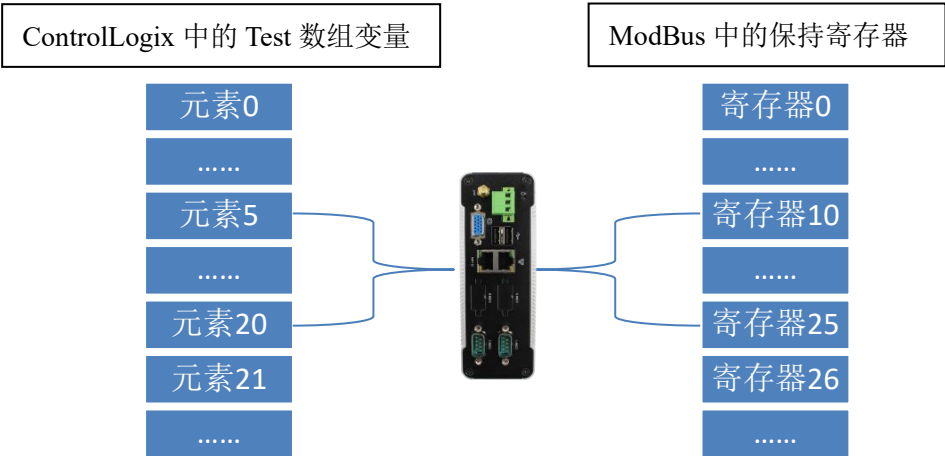
● 数据映射表举例

The screenshot shows a Windows-style dialog box titled "Create Register Convert Mapping Table". It contains the following fields and settings:

- Table Name:** Test
- Source Section:**
 - Interface: Ethernet A
 - Driver: AB
 - DataArea/Tag Name: Test
 - Starting: 5
- Transfer Section:**
 - Quantity: 15
 - DataType: I16
 - Legend: I:Signed integer, U:Unsigned integer
- Destination Section:**
 - Interface: Ethernet B
 - Driver: MB
 - DataArea/Tag Name: Holding Registers
 - Starting: 10
- Buttons:** Cancel, OK

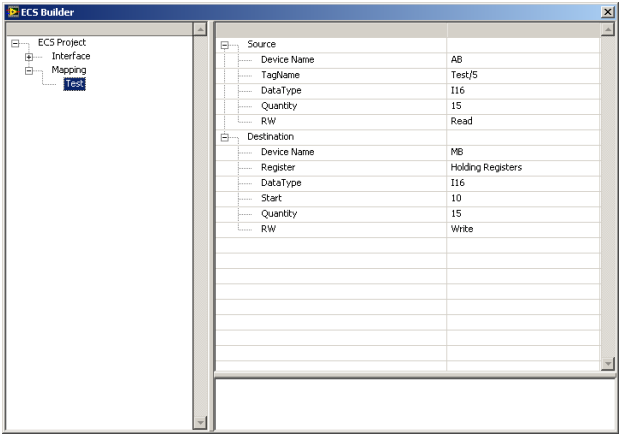
上图为一个数据映射表的组态实例, 表名为 Test, 将位于 Ethernet A 接口下的 ControlLogix 中数据类型为 16 位整型 (I16)

的数组的变量 Test 从第 6 个元素开始的 15 个元素的数据映射到位于 Ethernet B 接口下 ModBus 设备的 Holding Registers 从 10 开始的 15 个寄存器中。详见下图中图示分析：



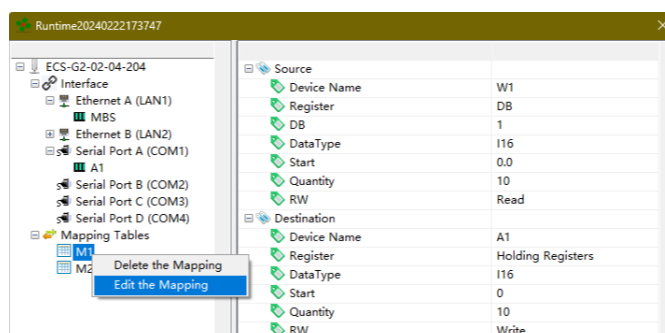
● **查看数据映射表详情**

在左侧树形导航中单击已创建的数据映射表的名称，在右侧的信息区将显示该映射表的详细信息。



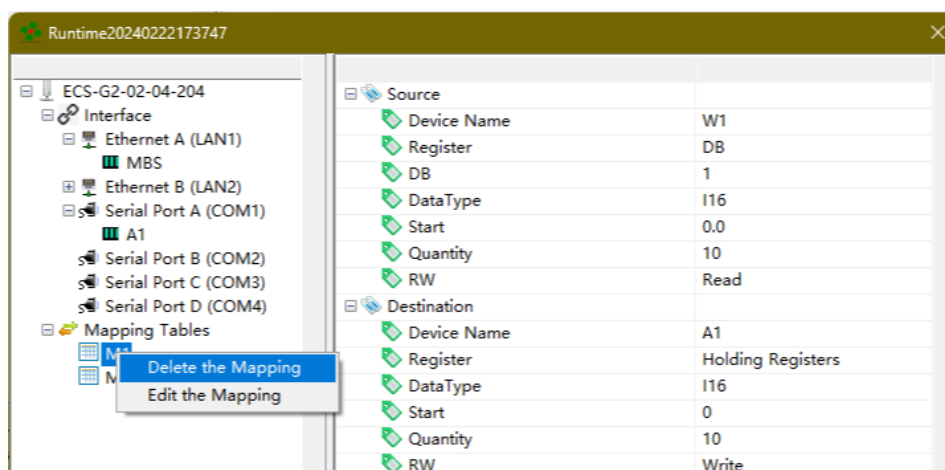
● **修改数据映射表**

通过此功能可以对已创建的映射表进行修改。先选中已创建的映射表，右键选择“ Edit the Mapping” 即可打开编辑界面



● 删除数据映射表

在左侧树形导航中选中已创建的数据映射表，在表名上点击鼠标右键，通过弹出的快捷菜单指令删除，如下图所示：



7 设备驱动说明

7.1 Logix5000 系列控制器

7.1.1 概述

Logix5000 系列控制器支持使用标准的以太网、TCP/IP 技术和一种名叫 CIP（Control and Information Protocol）的开放性应用层协议。CIP 也是 DeviceNet 和 ControlNet 网络的应用层协议。这个开放性的应用层协议使得面向自动化和控制应用的在 EtherNet/IP

上的工业自动化和控制设备的互操作性和互换性成为现实。

EtherNet/IP 同时支持 CIP 的时分的和非时分的消息传输服务。时分的消息交换基于生产者/消费者模型，在这个模型里一个传送者在网络上发送数据并被网络上的多个设备同时接收到。

7.1.2 ECS 中 Logix5000 系列控制器的驱动

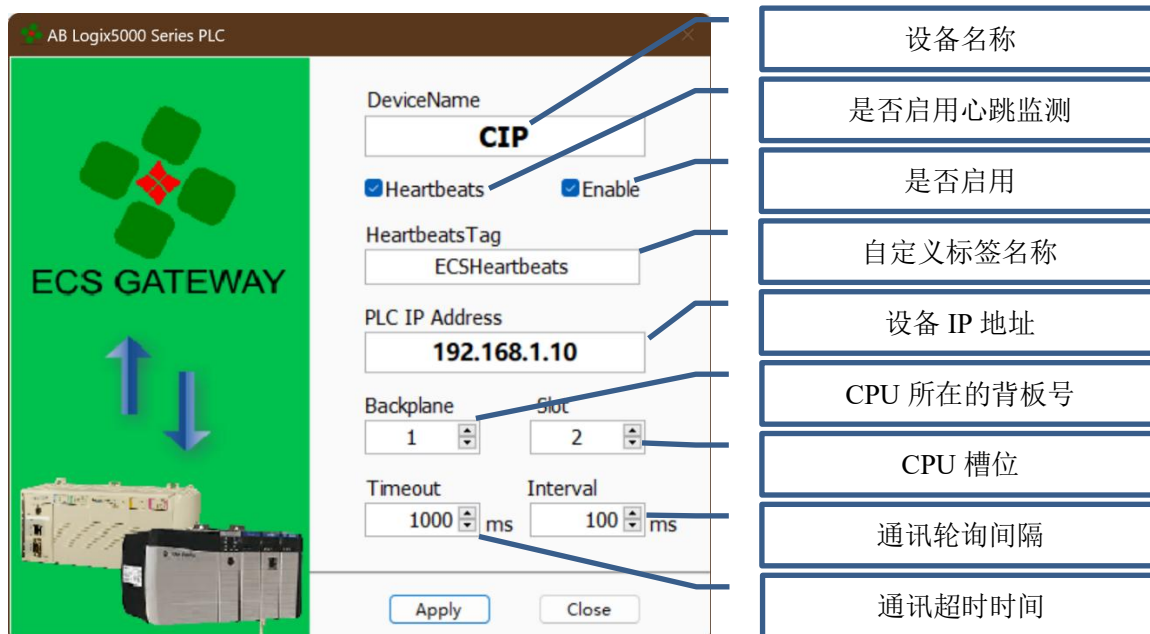
ECS 集成了与 AB 支持通用工业协议(CIP)的目标模块进行交互的驱动，通过标准以太网通信。

支持 AB 的 Logix5000 系列 PLC 包括：

- ControlLogix;
- CompactLogix;
- DriverLogix;
- FlexLogix;
- SoftLogix5800。

一个网口下可以挂载 9 台 Logix5000 系列 PLC，更多需求请连续我们索取特殊版本固件。

7.1.3 驱动设置



在相应接口下创建设备后，双击设备名称即可打开设备通讯属性设置窗口。如上图所示。

Enable:是否启用，不选中则在运行时不会建立与该设备的通讯连接；

Heartbeats:是否启用心跳信号。是否向 PLC 发送心跳信号，可用于判断网关与 PLC 之间连接是否正常，启用此功能需要在 PLC 中创建控制器标签（Controller Tag），标签名称为 HeartbeatsTag 设置的标签名，数据类型为 SINT 数组，大小为 10，该数组第 1 个数为心跳信号为脉冲信号（0/1 周期变化，周期约 2 秒），第 2~10 个数为预留通讯状态反馈，详见附录第 6 小节说明。附录第 5 小节为心跳检测的实例程序，用于检测网关与 PLC 通讯是否正常，也可根据实际需求自行编写相应的代码逻辑。

注意：如果 PLC 没有相关功能需求及没有创建自定义心跳标签（Tag）时不要启用该功能。

IP Address: Logix5000 控制器的 IP 地址;

Backplane: 背板号;

Slot: CPU 槽位;

Timeout: 通讯超时;

Interval: 通讯轮询间隔

Apply: 更新并保存设置;

Close: 保持原有设置并关闭窗口。

7.1.4 数据映射表设置

Logix5000 控制器将数据保存在标签中 (Tag)。标签就是实际工程中的变量，模拟量如水 位、压力、温度，数字量如开关启停、状态显示等。标签类型有**基本型 (Atomic 原子型)**、**结构体类型 (Structure)**、**数组型 (Array)**。

标签种类分为**程序标签** (局部) 和**控制器标签** (全局)。程序标签只能在所定义的程序内调用，不能被其他程序所调用。控制器标签可以在任意程序中调用。ECS 支持控制器标签和程序标签的读写操作，详见下文中的相关说明。

在与 Logix5000 通讯中**数据类型**信息至关重要，数据类型用于读操作、写操作以及用于描述结构体。Logix5000 系列控制器支持多种数据类型：

原子 (Atomic): 存储单一数值，类型包括 BOOL、DWORD (32-bit BOOL array)、SINT、INT、DINT、REAL、LINT 等；

结构体 (Structure)：多种不同数据类型的原子的聚合；

数组 (Array)：有相同数据类型原子连续排列组成的聚合。

The screenshot shows a dialog box titled "Create Register Convert Mapping Table". It has several sections: "Table Name" with the value "T1"; "Transfer" section with "Quantity" set to 1 and "DataType" set to I16; "Source" section with "Interface" set to Ethernet A, "Driver" set to CIP, "DataArea/Tag Name" set to I, and "Starting" set to 0; and "Destination" section which is empty. Red boxes are drawn around the "Quantity", "DataType", "DataArea/Tag Name", and "Starting" fields.

创建数据映射表时，Logix5000 控制器的设置项包含以下内

容：

- **数据类型：**DataType 选项。要与 Logix 5000 控制器里定义的数据类型保持一致，有关 ECS 中的数据类型与 Logix5000 控制器定义的数据类型的对应关系详见 “ECS 数据类型与 Logix PLC 数据类型对应关系”

| ECS 数据类型与 Logix PLC 数据类型对应关系 | | |
|------------------------------|---------------------------|----|
| ECS | Logix 5000 控制器 | 字节 |
| BOOL | BOOL | 1 |
| BOOL | DWORD (32-bit BOOL array) | 4 |
| I8 | SINT | 1 |
| I16 | INT | 2 |
| I32 | DINT | 4 |
| Float | REAL | 4 |
| I64 | LINT | 8 |

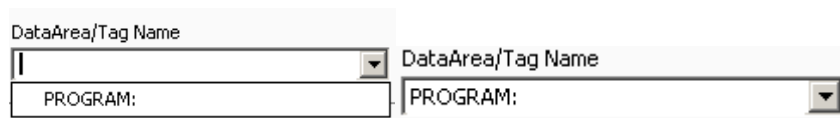
- **数据长度：**Quantity 选项。读写数组时的读写长度，读写标签为原子型或者为结构体中某一元素时为 1。标签为数组时，最大值小于该标签在控制器中定义的数组的大小**减去**

Starting 项后的**数值**。

注意：在 Logix5000 控制器中布尔数组其本质是 32 位整型数组，在通过偏移量进项区段写入时需规划合理的分组，写入时控制器会按照整型数据处理，规划不合理会造成数据被覆盖的风险。比如在设置了对布尔数组类型的标签起始地址为 5，长度为 3 的写入设置，在将数据写入控制器时，控制器会将数组的前 5 个写入 0。建议需要进项分段写入时以 32 个布尔量为一组进行规划。

- **标签名称：**DataArea/TagName 选项。为 Logix 5000 控制器中已定义的标签名。**标签名格式：**

- **原子型标签：**直接使用在控制器定义的名称。
- **结构体型标签：**结构体名.元素名
- **数组型标签：**数组名称。
- **程序标签：**ECS 支持程序标签的读写，标签的格式为：PROGRAM:程序名.标签名。PROGRAM:标识符可以通过 DataArea/TagName 下拉菜单选择。



The image shows a software interface with two identical dropdown menus side-by-side. Both are labeled 'DataArea/TagName'. The left dropdown menu is open, showing a list of options with 'PROGRAM:' selected. The right dropdown menu is closed, showing only the 'DataArea/TagName' label.

- **起始地址：**标签为数组时数据的其实索引。

7.2 Modbus TCP/RTU 系列设备

7.2.1 ModBus 概述

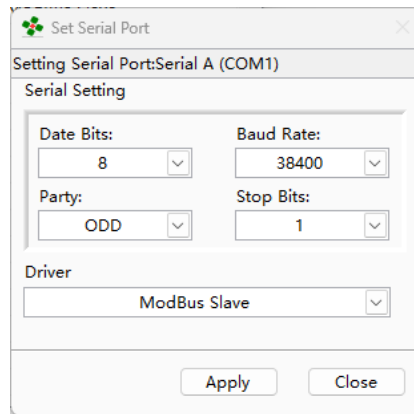
Modbus 通信协议为设备之间提供主从通信。Modbus 是一种通用语言，已经成为一通用工业标准。此协议支持传统的 RS-232、RS-422、RS-485 和以太网设备。许多工业设备，包括 PLC，DCS，智能仪表等都在使用 Modbus 协议作为他们之间的通讯标准。

关于 Modbus 的详细信息，请参考 Modbus 组织网站 (www.modbus.org)。

7.2.2 ECS 中的 Modbus 驱动

ECS 集成的 Modbus 驱动支持标准的 ModBus 通讯，包含下列不同主从通信类型的通信方法：

- Modbus RTU/ASCII - 支持 RS232、RS422、RS485 串行通讯接口。同一串行通讯总线上仅有一个 Modbus 主设备和一个或多个 Modbus 从设备连接。Modbus RTU/ASCII 驱动需要在串口设置中选择，如下图所示，一个串口下仅能挂载 1 个 Slave 类型的 ModBus 设备，选择 Master 类型驱动时最多可以挂载 256 个 ModBus 设备。同时挂载多台 ModBus 设备时建议增加 RS485 集线器。



- Modbus TCP - 通过标准以太网网络。

一个网口下可以挂载 9 个 ModBus 主站驱动，最多可连接 9 台从站设备，更多需求请连续我们索取特殊版本固件。

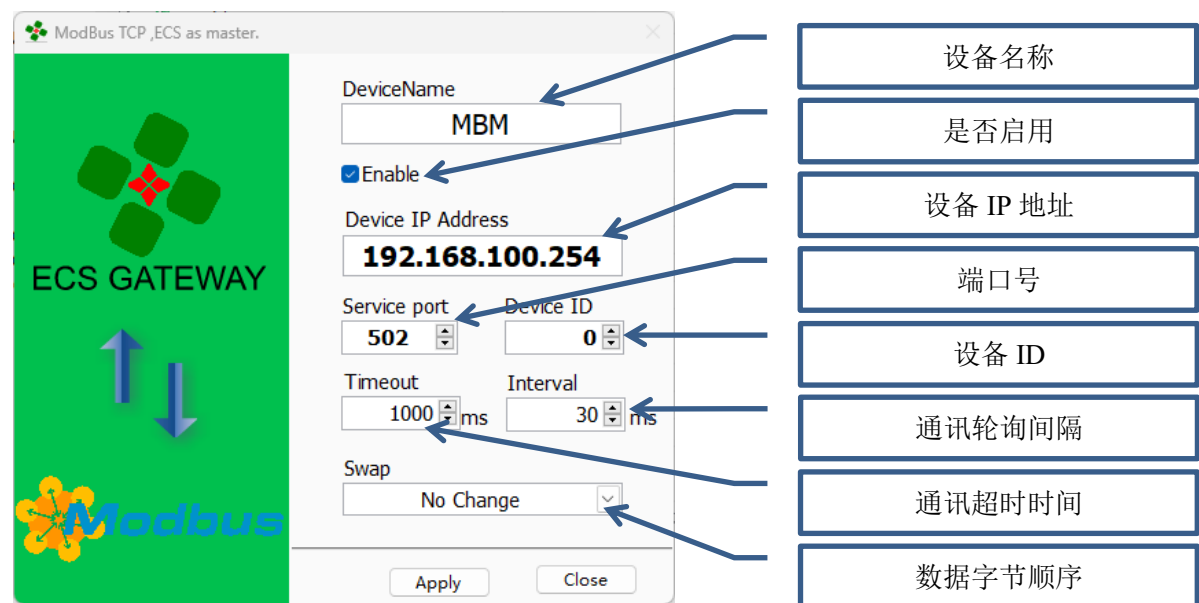
一个网口下仅可挂载 1 个 ModBus TCP Slave 驱动，Modbus 从站设备驱动同时支持 2 主站连接。

7.2.3 驱动设置

ECS 中 ModBus 的设备根据实际的设备驱动有四种情况：

- 1) **ModBus TCP Master**: ECS 做为 ModBus TCP 主站设备与其他 ModBus TCP 从站设备通讯。
- 2) **ModBus TCP Slave**: ECS 为 ModBus TCP 从站设备，等待响应网络上的 ModBus TCP 主站操作指令；
- 3) **ModBus RTU/ASCII Master**: ECS 做为 ModBus 主站设备与 ModBus 从站设备通过串行通讯连接；
- 4) **ModBus RTU/ASCII Slave**: ECS 做为 ModBus 从站设备与 ModBus 主站设备通过串行通讯连接。

7.2.3.1 ModBus TCP Master



Enable:是否启用设备，不选中则在运行时不会建立与该设备的通讯连接；

IP Address: ModBus TCP 从站设备的 IP 地址；

Service port: 服务端口号，默认为 502；

Device ID: 设备号，默认为 0；第三方设备通常将这个参数设为 0 或 1，组态后发现通讯异常时可尝试修改此参数；

Timeout: 通讯超时；

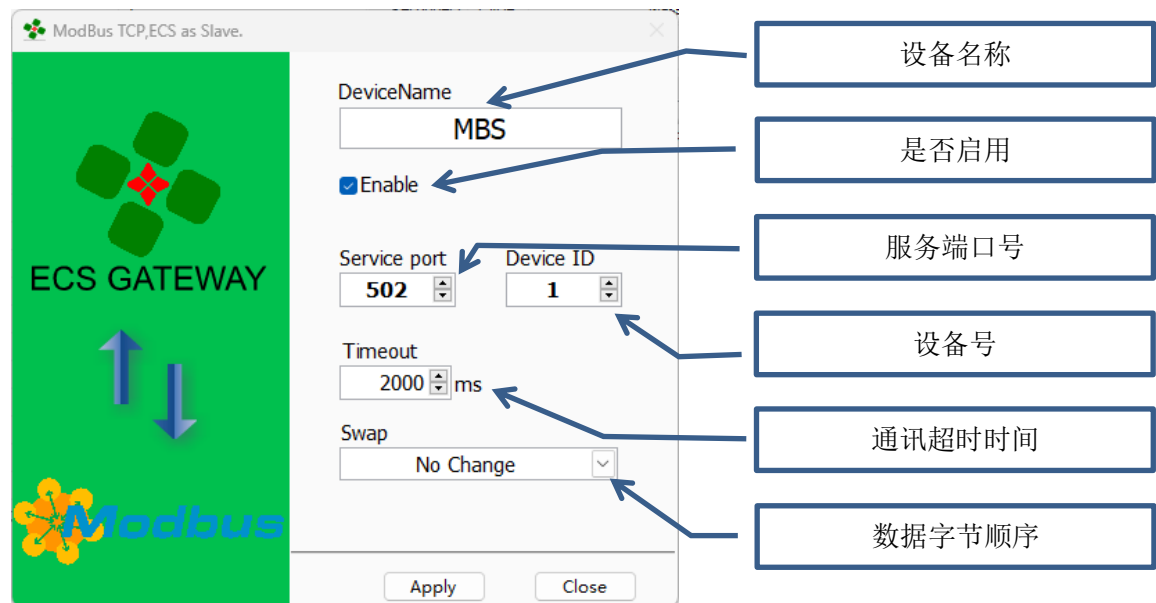
Interval: 通讯轮询间隔；

Swap: 数据字节顺序，可根据从站设置选择对应的格式；

Apply: 更新并保存设置；

Close: 保持原有设置并关闭窗口。

7.2.3.2 ModBus TCP Client



Enable:是否启用设备，不选中则在运行时不会建立与该设备的通讯连接；

Service port: 服务端口号，默认为 502；

Device ID: 设备号，默认为 0，第三方设备通常将这个参数设为 0 或 1，组态后发现通讯异常时可尝试修改此参数；

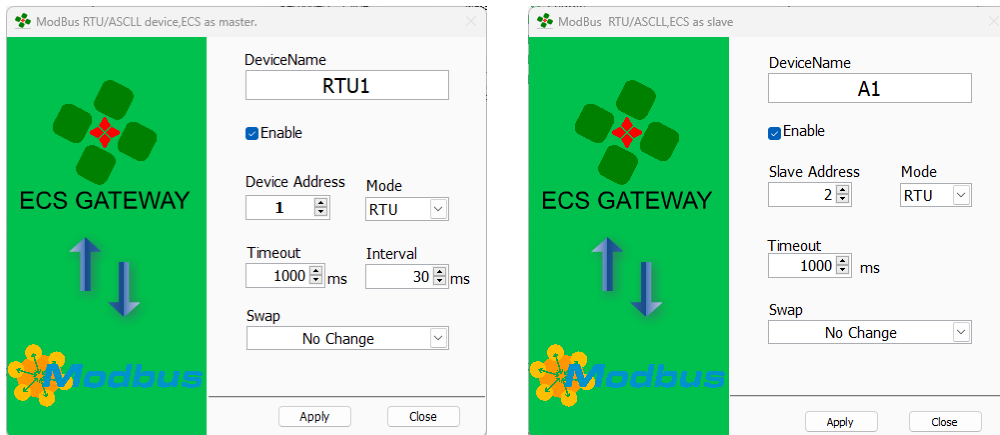
Timeout: 通讯超时；

Swap: 数据高低位转换类型，可根据从站设置选择对应的格式；

Apply: 更新并保存设置；

Close: 保持原有设置并关闭窗口。

7.2.3.3 ModBus RTU/ASCII Master(Slave)



ECS 做为 ModBus RTU/ASCII 主站设备或从站设备时的设置项相同，均包含：

Enable:是否启用设备，不选中则在运行时不会建立与该设备的通讯连接；

Slave Address: ECS 作为从站时分配的从站地址；

Device Address: ECS 作为主站时需要连接的从站设备的地址；

Mode: 传输模式，RTU 或者 ASCII；

Timeout: 通讯超时；

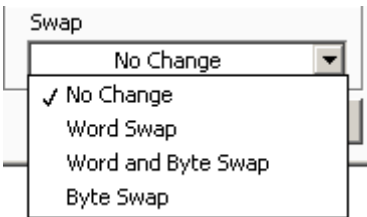
Interval: 通讯指令轮询间隔；

Swap: 数据高低位转换类型，可根据从站设置选择对应的格式；

Apply: 更新并保存设置；

Close: 保持原有设置并关闭窗口。

7.2.3.4 ModBus Swap



在 Modbus 规约驱动中，可以通过 SWAP 寄存器用于改变浮点数、32 位整型数的字节顺序，共有 4 种取值，分别为：

- 1) 当 SWAP= No Change 时，不做数据转换，
(1234=1234)
- 2) 当 SWAP= Word Swap 时，进行字交换 (1234=3421)
- 3) 当 SWAP=Word and Byte Swap 时，先进行字交换再进行字节交换 (1234=4321)
- 4) 当 SWAP=Byte Swap 时，进行字节交换 (1234=2143)

7.2.4 数据映射表设置

Modbus 的数据表格

数据表格是 ModBus 设备存储数据的数组或内存块。Modbus 的数据模型是基于数据表格的，详细信息如下：

| 数据表格 | 数据类型 | 访问 | 说明 | 注释 |
|--------------------------|---------------|----|-------|---|
| 离散输入 Discrete Input | 布尔 | 只读 | 输入状态 | Modbus 主设备和 Modbus 从设备均可读取离散输入。但只有 Modbus 从设备可修改离散输入。 |
| 线圈输出 Coils | 布尔 | 读写 | 输出状态 | Modbus 主设备和从设备均可读写线圈。 |
| 输入寄存器 Input Registers | 无符号 16 位整数 | 只读 | 模拟输入值 | Modbus 主设备和从设备均可读取输入寄存器。但只有 Modbus 从设备可修改输入寄存器。 |
| 保持寄存器 | 无符号 | 读写 | 模拟输出 | Modbus 主设备和从设备均可读写保持寄存器。 |

| | | | | |
|-------------------|--------|--|------|--|
| Holding Registers | 16 位整数 | | 内部数值 | |
|-------------------|--------|--|------|--|

Modbus 数据表格地址

Modbus 使用数据表格地址引用数据。每个数据表格都有其分配的地址。读写操作中，Modbus 允许主设备和从设备为每个数据表格最多选择 65536 个数据项。Modbus 数据表格地址为整数。地址是从零开始的，即每个数据表格的起始地址为 0。但某些设备使用以 1 开始的地址。验证每个设备的起始地址，以确可以获得择正确的数据项。

创建数据映射表时，ModBus 设备的设置项包含以下内容：

- **数据类型：**DataType 选项。有关 ECS 中的数据类型与 ModBus 定义的数据类型的对应关系详见下表

| ECS 数据类型与 ModBus 数据类型对应关系 | | |
|---------------------------|-------------|-------------|
| ECS | ModBus | Register |
| BOOL | 布尔型 | 线圈、输入状态 |
| I16 | 有符号 16 位整型数 | 输入寄存器、保持寄存器 |
| U16 | 无符号 16 位整型数 | 输入寄存器、保持寄存器 |
| I32 | 有符号 32 位整型数 | 输入寄存器、保持寄存器 |

| | | |
|-------|-------------|-------------|
| U32 | 无符号 32 位整型数 | 输入寄存器、保持寄存器 |
| Float | 单精度浮点型 | 保持寄存器 |

- **数据长度：**Quantity 选项。Modbus 设备可选择的最大连续

数据项取决于数据表格类型和待执行的操作。具体如下：

| 数据表 | 离散输入 Discrete Input | 线圈输出 Coils | 输入寄存器 Input Registers | 保持寄存器 Holding Registers |
|-----------------|------------------------|---------------|--------------------------|----------------------------|
| ModBus 设备为数据源时 | | | | |
| 最大连续数量 | 2000 | 2000 | 125 | 125 |
| ModBus 设备为数据目标时 | | | | |
| 最大连续数量 | 1968 | 1968 | 120 | 120 |

- **数据表：**DataArea/TagName 选项。支持标准 ModBus 数据表，离散输入状态 (Discrete Input)，线圈输出 (Coils)，输入寄存器 (Input Registers) 和保持寄存器 (Holding Registers)；
- **起始地址：**数据表的起始地址。

7.3 西门子 S7 系列 PLC

7.3.1 概述

西门子 PLC 常见的通讯方法有基于 PPI 通信, MPI 通信, ProfiBus 以及以太网通信等, ECS 中支持以太网通讯方式。

7.3.2 ECS 中西门子 S7 系列 PLC 驱动

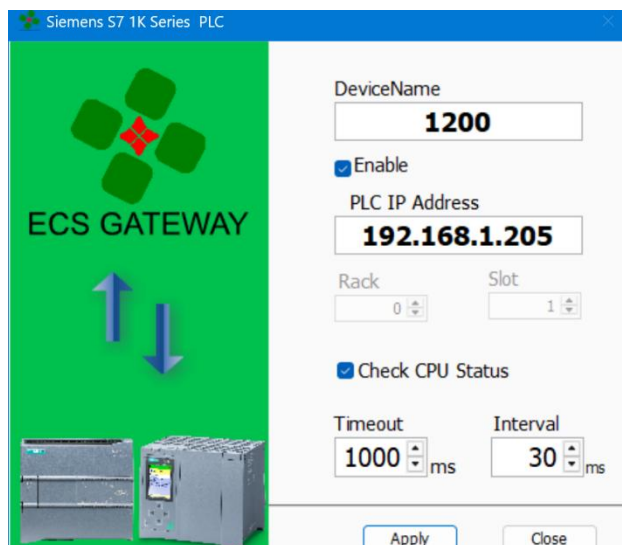
以太网通信

支持西门子的 S7 系列 PLC 的以太网 TCP 协议, 支持 CP243, CP343 和 CP443 扩展以太网通讯卡, 支持 S7-200Smart、S7-300/400、S7-1200、S7-1500 集成以太网通讯接口。

7.3.3 驱动设置

ECS 中集成了 S7 ISO-on-TCP 协议, 用于与 S7 站之间的数据交换, 站间通信是基于 IP 地址的, 数据块的数据传输适用于最大 8Kbytes 的数据。数据可以通过路由器(有路由功能的协议)传递。

7.3.3.1S7-TCP



Enable:是否启用设备，不选中则在运行时不会建立与该设备的通讯连接；

PLC IP Address: S7 系列 PLC (CP) 的 IP 地址；

Rack: 机架号；

Slot: 插槽号；

Check CPU Status*1: 是否启用监测 CPU 的运行状态；

Timeout: 通讯超时；

Interval: 通讯轮询间隔时间；

Apply: 更新并保存设置；

Close: 保持原有设置并关闭窗口。

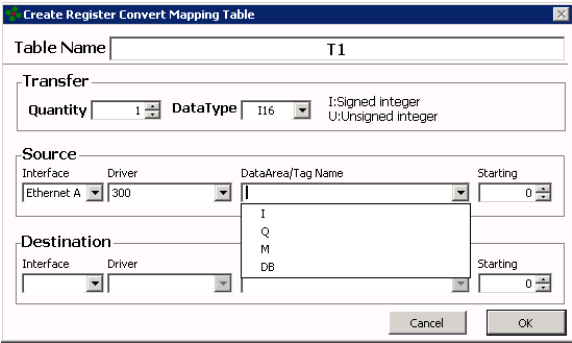
一个网口下可以挂载 9 台 S7-300/400/1200/1500/200Smart 系列 PLC，更多需求请连续我们索取特殊版本固件。

*1，在 ECS 与 PLC 通讯过程中如将 PLC 切换为 Stop，再切换回 RUN 模式时 ECS 会将需要同步到 PLC 数据强制更新，避免 BD

块在重启后被重置，造成与数据源的数据不同步。

注意：S7-1200/1500 的特殊设置参见附录 2

7.3.4 数据映射表设置



创建数据映射表时，S7 系列 PLC 的设置项包含以下内容：

- **数据类型：**DataType 选项。有关 ECS 中的数据类型与 S7-PLC 定义的数据类型的对应关系详见下表

| ECS 数据类型与 S7-PLC 数据类型对应关系 | | |
|---------------------------|------------------|-----------------|
| ECS | S7-PLC | PLC 符号 |
| BOOL | 位 (bit) | I、Q、M、V、DBX |
| I8 | 字节 (Byte) | IB、QB、MB、VB、DBB |
| U8 | 字节 (Byte) | IB、QB、MB、VB、DBB |
| I16 | 字 (Word) | IW、QW、MW、VW、DBW |
| U16 | 字 (Word) | IW、QW、MW、VW、DBW |
| I32 | 双字 (Double Word) | ID、QD、MD、VD、DBD |
| U32 | 双字 (Double Word) | ID、QD、MD、VD、DBD |
| Float | Real | MD、VD、DBD |

- **数据长度：**Quantity 选项。S7 系列 PLC 可选择的最大连续数据项取决于数据表格类型和待执行的操作。具体如下：

| 数据区 | I | Q | M | V | DB |
|-----------------|----------|----------|----------|-----|----------|
| ModBus 设备为数据源时 | | | | | |
| 最大连续数量 | 128Bytes | 128Bytes | 222Bytes | 125 | 164Bytes |
| ModBus 设备为数据目标时 | | | | | |
| 最大连续数量 | 128Bytes | 128Bytes | 212Bytes | 120 | 164Bytes |

- **系统存储器：**DataArea/TagName 选项。支持标准的 S7 地址有 I, Q, M, DB; DB 的格式为选择 DB 后直接在其后输入 DB 块的编号, 比如 DB20;
- **起始地址：**Starting 选项。数据的起始地址。数据类型为布尔型时的格式为 x.y.

S7 的地址有由 DataType+DataArea/TagName+Starting 共同组合构成, 如起始地址为 M10.0, 则 DataType 为 BOOL, DataArea/TagName 为 M, Starting 为 10.0.

7.4 Mitsubishi MELSEC Q 系列 PLC

7.4.1 概述

Mitsubishi Q PLC 默认支持 MELSEC Communication (MC) 协议，MC 协议报文传输格式分为 ASCII 和 Binary 两种格式。两种格式报文功能相同，只是采用 Binary 格式时比采用 ASCII 格式的数据传输量可减少 50%。

7.4.2 ECS 中的 MC 协议驱动

ECS 网关集成的三菱 MC 协议驱动兼容 3E 帧的文件格式，兼容 E71 系列网卡。支持对 Q 系列 PLC 内部 X、Y、M、V、B、D、W 等寄存器的读写操作。

7.4.3 PLC 设置准备工作

在将三菱 Q 系列 PLC 接入 ECS 网关前需要检查 PLC 设置项，以确保可以正常通讯。

1、 基础设置

如下图所示，需要设置【通信数据代码设置】为【ASCII 码通信】，同时将【允许 RUN 中写入(FTP 与 MC 协议)】选中。



图示：基础设置

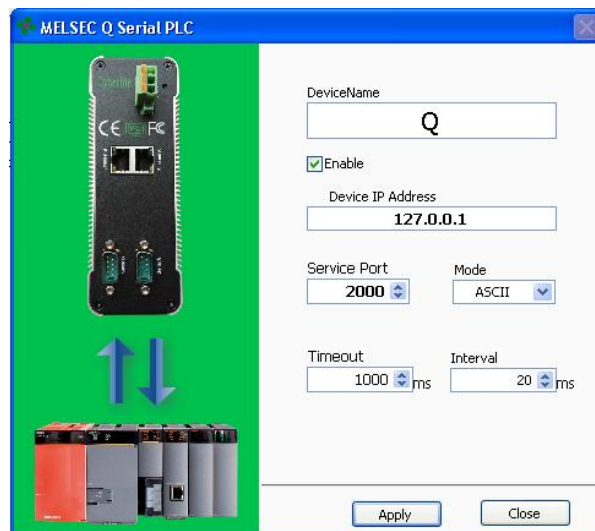
2、 协议设置

通过下面的设置窗口设置 MC 协议的链接。选择【协议】类型为【TCP】，【打开方式】为【MC 协议】，【本站端口号】为【根据实际需求填写，此端口号要与网关中的设置保持一致】



图示：协议设置

7. 4. 4 驱动设置



DeviceName:设备名称，用于识别连接的 PLC 设备，可填写任意字符，不可为空。

Enable: 是否启用设备，不选中则在运行时不会建立与该设备的通讯连接；

Device IP Address: 需要连接的 PLC 设备的 IP 地址，此地址需要与上页图示【基础设置】中的 IP 地址一致

Service Port: PLC 端设置的端口号，此设置需要与上页图示【协议设置】中设置的端口号保持一致。

Mode: 通讯数据格式代码，此处选择 ASCII

Timeout: 通讯超时时间设置，如在此时间内未收到 PLC 反馈 ECS 会自动处理此异常。

Interval: 通讯间隔时间。

7.4.5 数据映射表设置

图示：映射表设置

创建数据映射表时，三菱 Q 系列 PLC 的设置项包含以下内容：

- **数据类型：**DataType 选项。有关 ECS 中的数据类型与 Q-PLC 定义的数据类型的对应关系详见下表

| ECS 数据类型与 Q-PLC 数据类型对应关系 | | |
|--------------------------|------------------|---------|
| ECS | Q-PLC | PLC 符号 |
| BOOL | 位 (bit) | X、Y、B、V |
| I8 | 字节 (Byte) | - |
| U8 | 字节 (Byte) | - |
| I16 | 字 (Word) | DW |
| U16 | 字 (Word) | D W |
| I32 | 双字 (Double Word) | - |
| U32 | 双字 (Double Word) | - |
| Float | Real | - |

- **数据长度：**Quantity 一次传送的数据的个数。
- **系统存储器：**DataArea/TagName 选项。支持标准的 Q-PLC 地址有 X、Y、M、V、B、D、W；
- **起始地址：**Starting 选项。数据的起始地址。.

8 附录:

8.1 子网掩码与 IP 地址及计算方法

IP 地址包含 4 字节的数字, 被分为 4 段, 每段 8 位, 段与段之间用“点”分隔。为了便于表达和识别, IP 地址是以十进制形式表示的 如 210.52.207.2。IP 地址由两部分组成, 即网络号 (Network ID) 和主机号 (Host ID)。网络号标识的是 Internet 上的一个子网, 而主机号标识的是子网中的某台主机。IP 地址根据网络号和主机号的数量而分为 A、B、C 三类:

A 类: 0.0.0.0 到 126.255.255.255。用 8 位 (Bit) 来标识网络号, 24 位标识主机号, 最前面一位为“0”, 即 A 类地址的第一段取值介于 1~126 之间。A 类地址通常为大型网络而提供, 全世界总共只有 126 个 A 类网络, 每个 A 类网络最多可以连接 16777214 台主机。

B 类: 128.0.0.0 到 191.255.255.255。用 16 位来标识网络号, 16 位标识主机号, 前面两位是“10”。b 类地址的第一段取值介于 128~191 之间, 第一段和第二段合在一起表示网络号。B 类地址适用于中等规模的网络, 全世界大约有 16000 个 b 类网络, 每个 B 类网络最多可以连接 65534 台主机。

C 类: 192.0.0.0 到 223.255.255.255。用 24 位来标识网络号, 8 位标识主机号, 前面三位是“110”。C 类地址的第一段取值介于 192~223 之间, 第一段、第二段、第三段合在一起表示网络号。最后一段标识网络上的主机号,C 类地址适用于小型网络, 每个 C 类网络最多可以有 254 台主机。

从上面的介绍我们知道, IP 地址是以网络号和主机号来标示网络上的主机的, 只有在一个网络号下的计算机之间才能“直接”互通, 不同网络号的计算机

要通过网关 (Gateway) 才能互通。但这样的划分在某些情况下显得并不十分不灵活。为此 IP 网络还允许划分成更小的网络, 称为子网 (Subnet), 这样就产生了子网掩码。子网掩码的作用就是用来判断任意两个 IP 地址是否属于同一子网络, 这时只有在同一子网的计算机才能"直接"互通。

关于子网掩码

前面介绍了 IP 地址的构成: 网络号+主机号。可 IP 地址的网络号和主机号各是多少位呢? 如果不指定, 就不知道哪些位是网络号、哪些是主机号, 这就需要通过子网掩码来实现。

子网掩码的设定必须遵循一定的规则。与二进制 IP 地址格式相同, 子网掩码的长度也是 32 位, 左边是网络位, 用二进制 数字 "1" 表示, 1 的数目等于网络位的长度; 右边是主机位, 用二进制数字 "0" 表示, 0 的数目等于主机位的长度。如此, 我们就可以很容易通过 0 的位数确定 子网的主机数 ($2^{\text{主机位数}-2}$, 因为主机号全为 1 时表示该网络广播地址, 全为 0 时表示该网络的网络号, 这是两个特殊地址)。只有通过子网掩码, 才能表明一台主机所在的子网与其他子网的关系, 使网络正常工作。

子网掩码最主要的两个作用: 一是用于屏蔽 IP 地址的一部分以区别网络标识和主机标识, 并说明该 IP 地址是在局域网上, 还是在远程网上。二是用于将一个大的 IP 网络划分为若干小的子网络。IP 默认分配的子网掩码每段只有 255 或 0。

A 类的默认子网掩码 255.0.0.0 一个子网最多可以容纳 1677 万多台电脑

B 类的默认子网掩码 255.255.0.0 一个子网最多可以容纳 6 万台电脑

C 类的默认子网掩码 255.255.255.0 一个子网最多可以容纳 254 台电脑。

要想在同一网段，只要网络标识相同就可以了，那要怎么看网络标识呢？

首先要做的是把每段的 IP 转换为二进制（可通过 Windows 自带计算器），把子网掩码切换至二进制，我们会发现，所有的子网掩码是由一串连续的 1 和一连串的 0 组成的（一共 4 段，每段 8 位，共 32 位）。

A 类: 255.0.0.0: 11111111.00000000.00000000.00000000

B 类: 255.255.0.0: 11111111.11111111.00000000.00000000

C 类: 255.255.255.0: 11111111.11111111.11111111.00000000

这是 A/B/C 三类默认子网掩码的二进制形式，

举例 1：判断 ip 188.188.0.111，188.188.5.222，子网掩码都设为 255.255.254.0，在同一网段吗？

转换 IP(A) 188.188.0.111 为二进制形式

10111100.10111100.00000000.01101111

转换 IP(B) 188.188.5.222 为二进制形式

10111100.10111100.00000101.11011010

转换 Mask 255.255.254.0 为二进制形式

11111111.11111111.11111110.00000000

将 IP(A)、IP(B)分别与 Mask 作逻辑与运算,结果如下:

A=> 10111100.10111100.00000000.00000000

B=> 10111100.10111100.00000100.00000000

很明显:A 与 B 网络标识不一样,IP(A)与 IP(B)不属于同一网段。

举例 2：一个网络有 530 台电脑，组成一个对等网，子网掩码如何设？IP 如何设？

计算:2 的 M 次方=530,求得 M=10

那么子网掩码最后为 10 个 0,如此便是:

11111111.11111111.11111100.00000000

换成 十进制便是: 255.255.252.0

再看 IP, 我们选一个 B 类 IP, 例如: 188.188.x.x前两段按 B 类要随便设就可以, 关键是第三段, 只要网络标识相同就可以在同一网段就可以。

我们先看网络标识: 255.255.252.0:

11111111.11111111.11111100.00000000

188.188.x.x: 10111100.10111100.?????? xx.xxxxxxxxxx

网络标识: 10111100.10111100.?????? 00.00000000

上边x号无论填 0 和 1 结果都是 0, ? 处填 0 和 1 都一样, 我们就全填 0,

结果 IP 便是: 10111100.10111100.000000xx.xxxxxxxxxx,

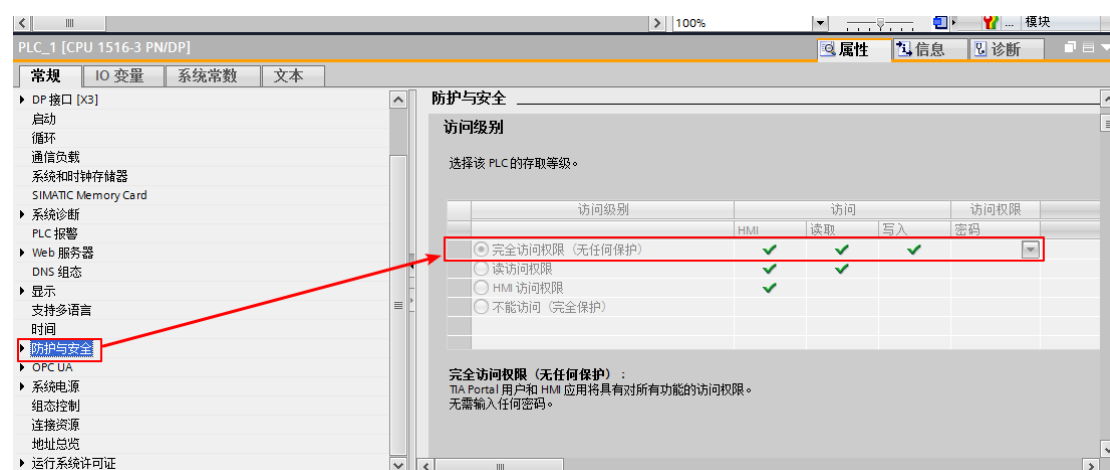
这个 IP 共有 530 台电脑, IP 最后一段分给 254 台, 一共要分

530/254=2.086 段, 进一法则要分成 3 段, 所以 IP 地址 000000xx处分成三个不同的数据即可, 例: 00000001, 00000010, 00000011, 分别是 1, 2, 3, 这样 IP 地址就确定了 188.188.1.x, 188.188.2.x, 188.188.3.x。

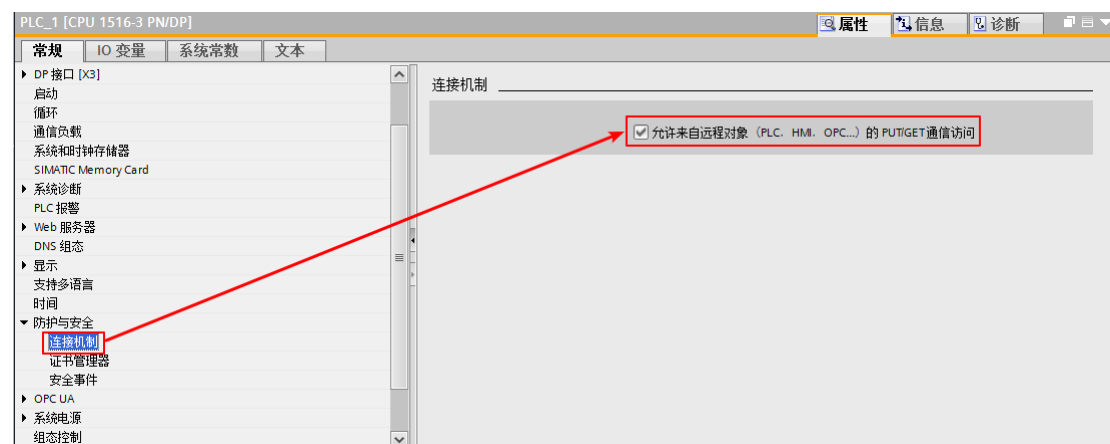
8.2 Siemens S7-1200/1500 通讯特殊设置

西门子为 S7-1200/1500 系列 PLC 加入安全访问机制，PLC CPU 默认的访问级别不允许第三方系统通讯，需要修改设置。请注意【以下三处设置项必须全部设置，缺少任何一项均无法正常通讯】。

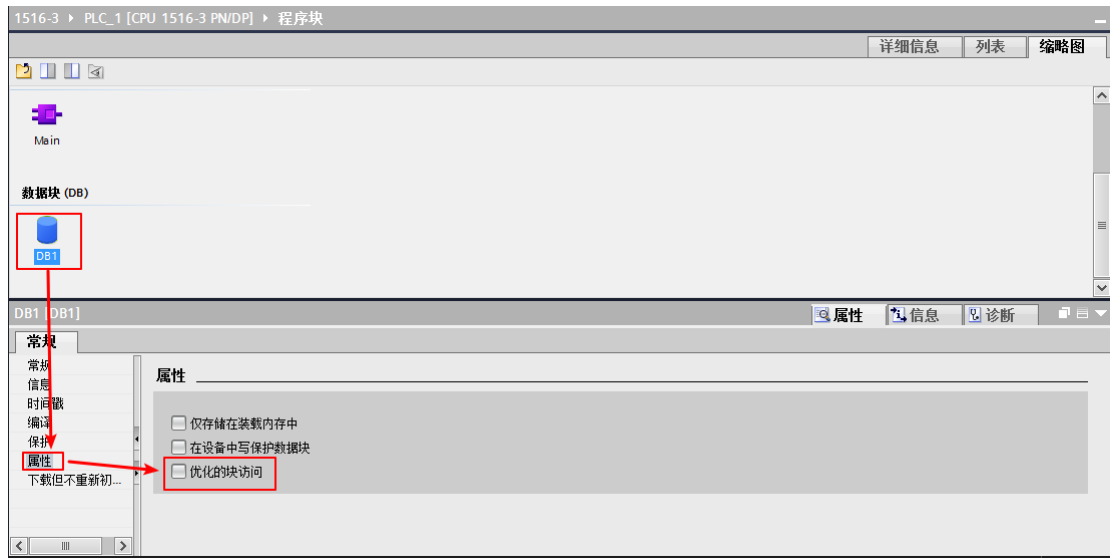
1、 设置访问级别，须设置为完全访问级别



2、 设置连接机制，需要勾选允许远程对象通讯访问



3、 禁用数据块优化，如果涉及到需要网关对数据块进行数据操作，需要将 DB 块的【优化块访问】复选框移除勾选，如下图。

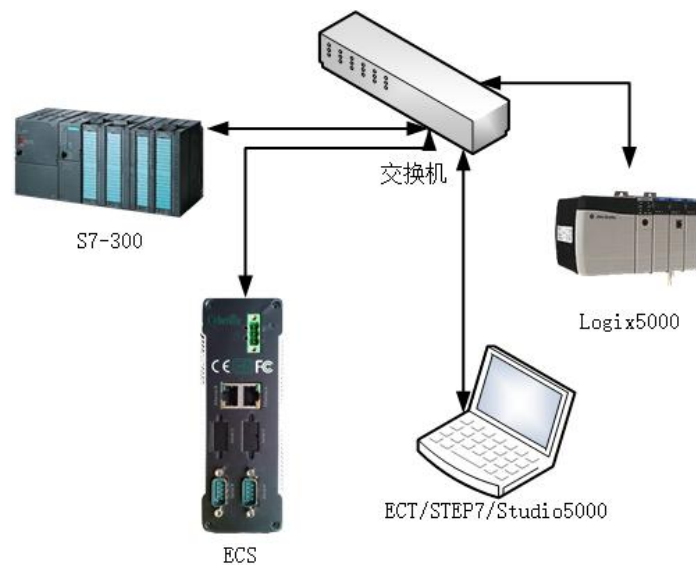


8.3 SIEMENS S7-300 PLC 与 AB Logix 5000 系列 PLC 之间的数据交换

本例中将实现通过 ECS 网关实现 SIEMENS S7-300 PLC 与 AB Logix 5000 系列 PLC (SoftLogix5800 为模拟 PLC) 之间的数据交换,系统网络配置如下:

- 300 PLC IP 地址 10.1.2.115
- SoftLogix5800 IP 地址 10.1.2.116
- Studio 5000 IP 地址 10.1.1.117
- ECS 地址 10.1.2.100

网络结构如下:

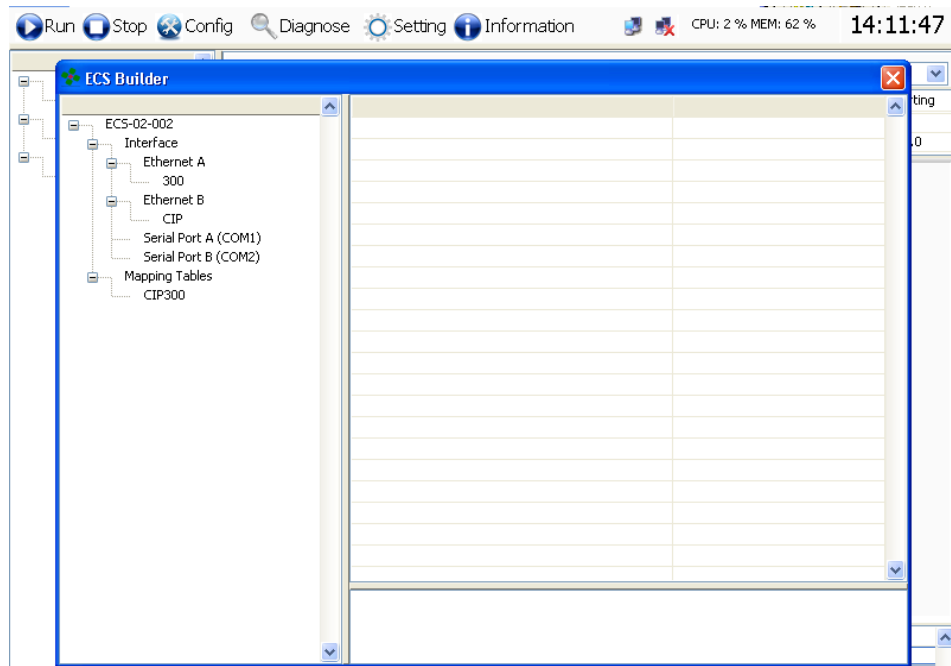


配置流程 (在线模式)

1. 进入组态配置界面

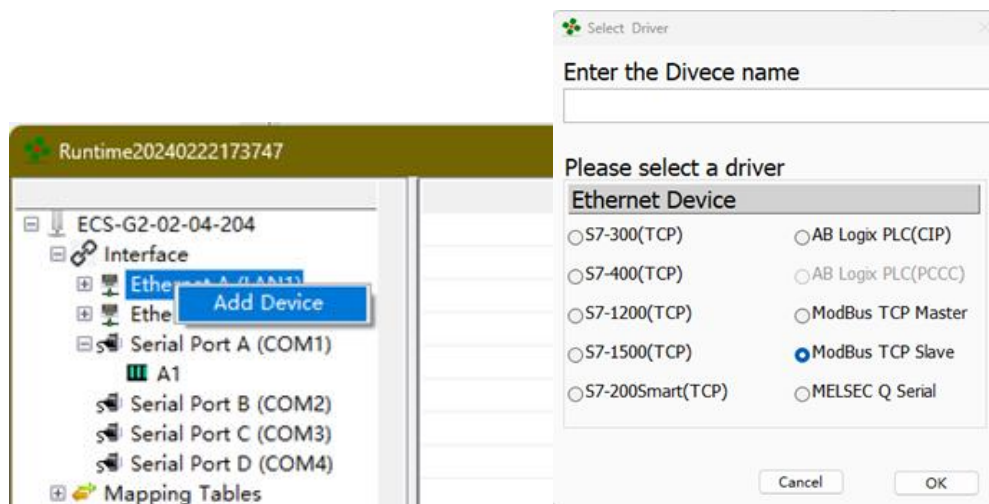
进入在线模式后,通过窗口顶部的 Config 按钮可打开配置工具(ECS Builder)

窗口,如下图所示:

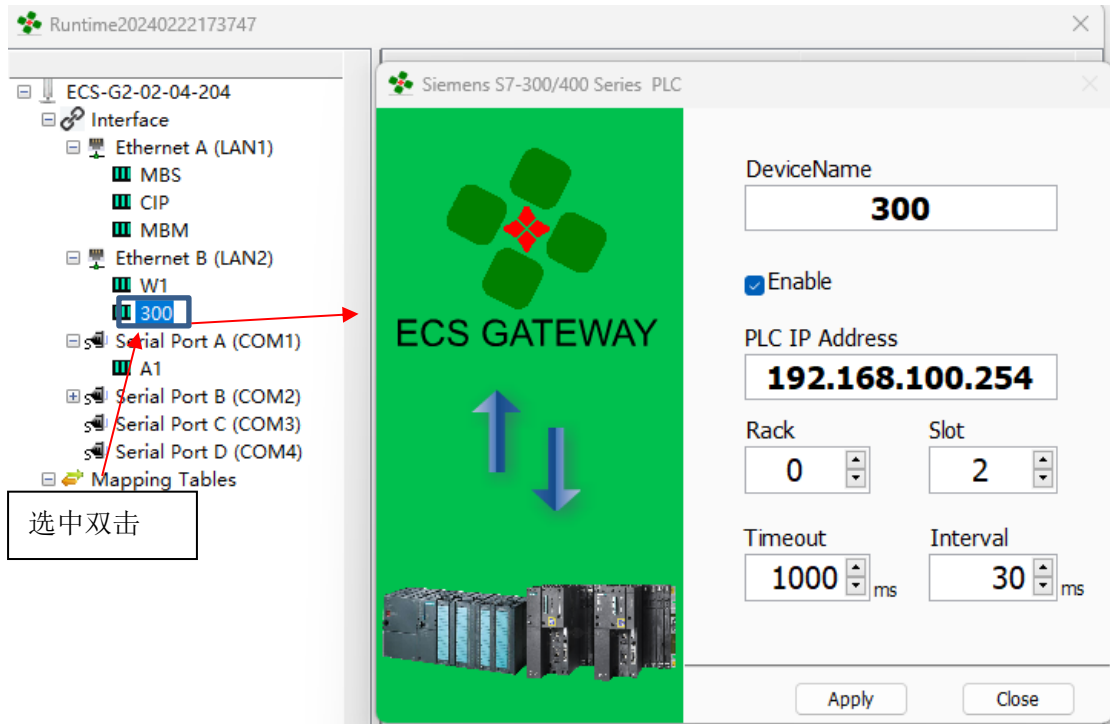


2. 添加 S7-300

依次展开左侧导航 **ECS-02-002** (此为网关型号, 以具体型号为准-) → Interface, 选中 EthernetA → 右键弹出操作快捷菜单, 选择 Driver → Add Driver 添加设备驱动, 设备驱动选择 S7-300(TCP)。



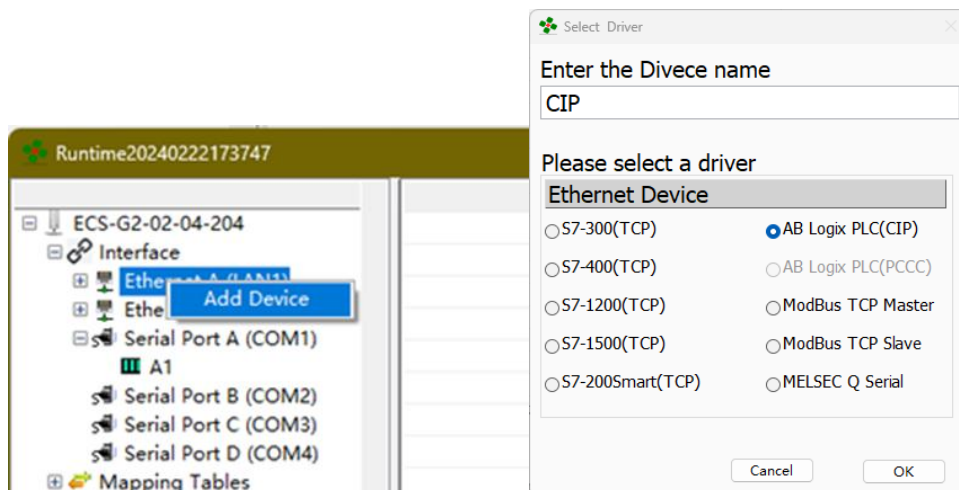
3. 设置 S7-300 参数



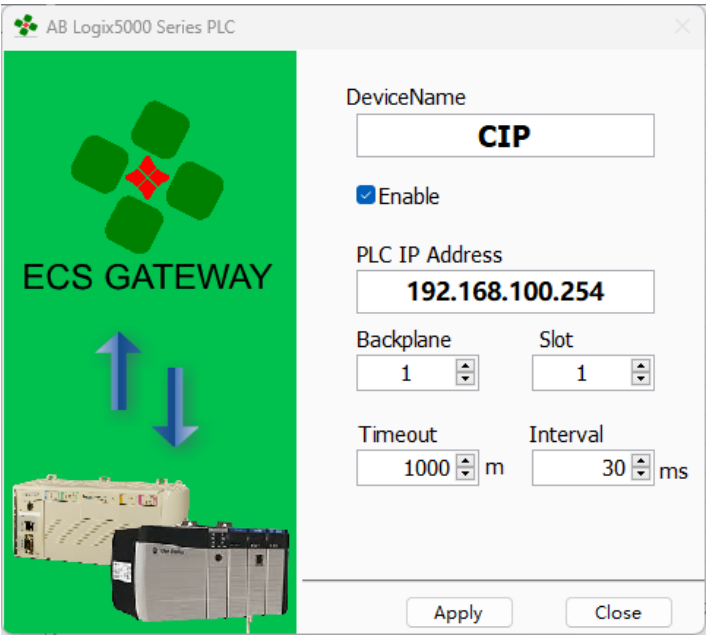
S7-300 添加成功后，新建的设备会出现在左侧的树形导航中，选中，双击即可弹出设备的设置信息，S7-300PLC 需要设置 PLC 的 IP 地址，RACK 为固定值 0，Slot 为固定值 2，其他设置可采用默认值。PLC 测无需任何设置。

4. 添加 Logix5000 设备

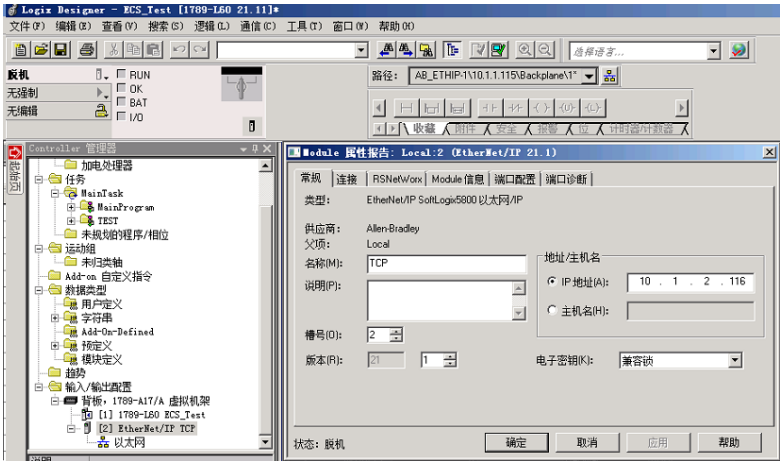
依次展开左侧导航 ECS-02-002（此为网关型号，以具体型号为准-）→ Interface, 选中 EthernetB→右键弹出操作快捷菜单，选择 Driver→Add Driver 添加设备驱动，设备驱动选择 AB Logix(CIP)。

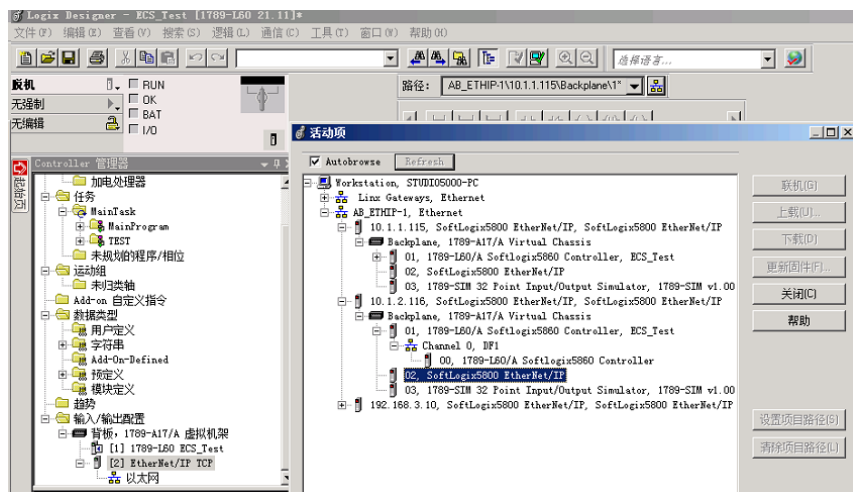


5. 设置 Logix5000 参数



Logix5000 设备添加成功后，新建的设备会出现在左侧的树形导航中，选中，双击即可弹出设备的设置信息，Logix5000 需要设置 PLC 的 IP 地址，Backplane 和 Slot 需要根据实际 PLC 的组态设置，其他设置可采用默认值。PLC 测无需任何设置。在本例中的 Backplane 设为 0，Slot 设为 2.其在 Studio5000 中的配置如下图所示。



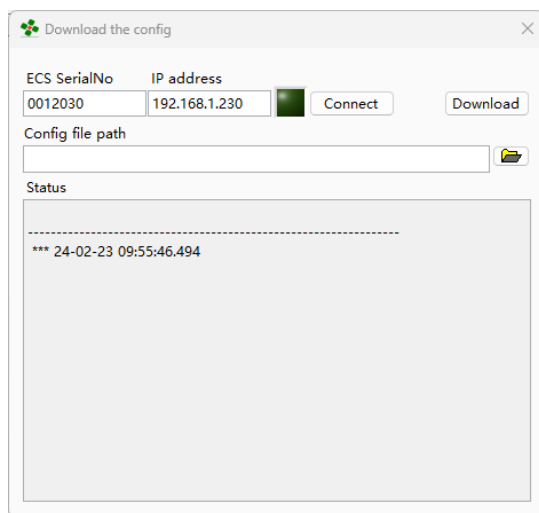


6. 通讯映射表的建立

请根据 ECS 用户手册配置 PLC 间的数据交换映射。

7. 下载组态配置

点击【Download】下载配置文件。



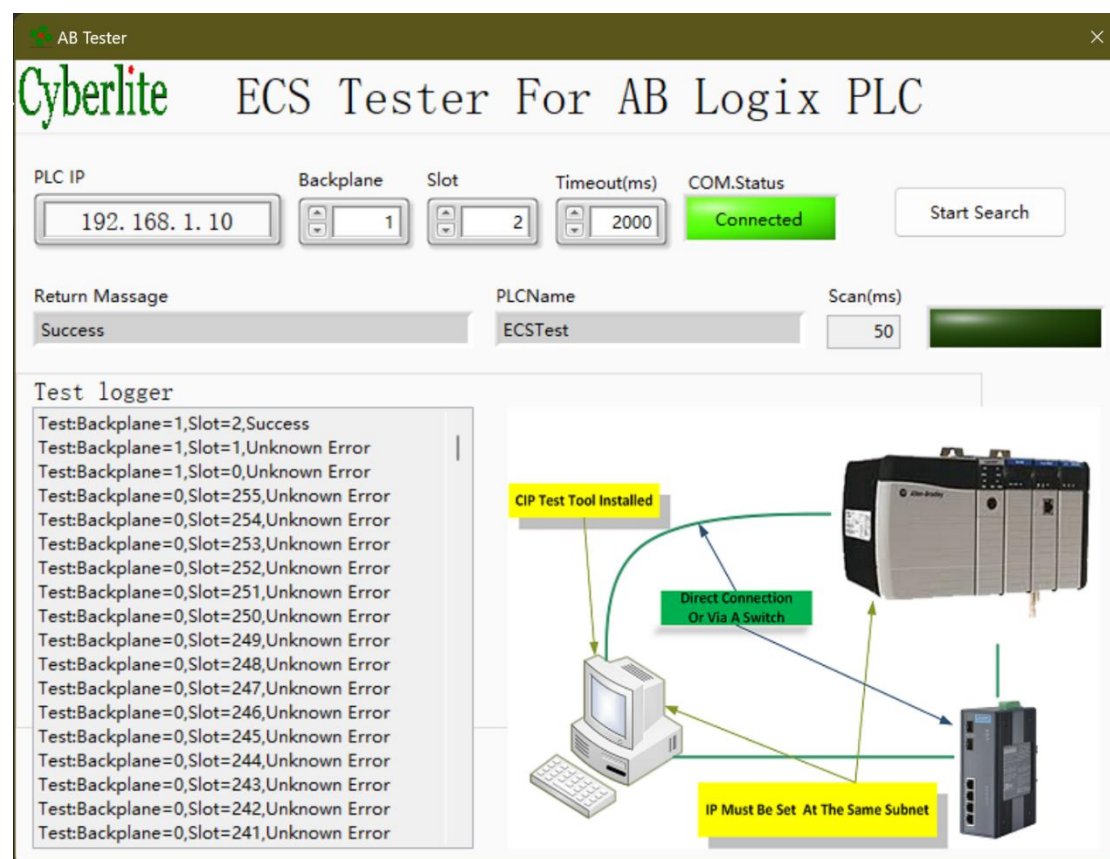
8. 诊断功能的使用

点击【Monitor】快捷按钮即可进入在线监视界面，可看到已设置的设备和数据映射表。

8.4 CIP Test Tool 使用说明

ECT 集成了 CIP 测试工具，用于测试 CIP 的通讯，工具主要功能有：

- a) 验证网关与 AB Logix5000 系列 PLC 的通讯功能
- b) 自动查找 AB Logix5000 系列 PLC 的 Backplane 和 Slot 设置



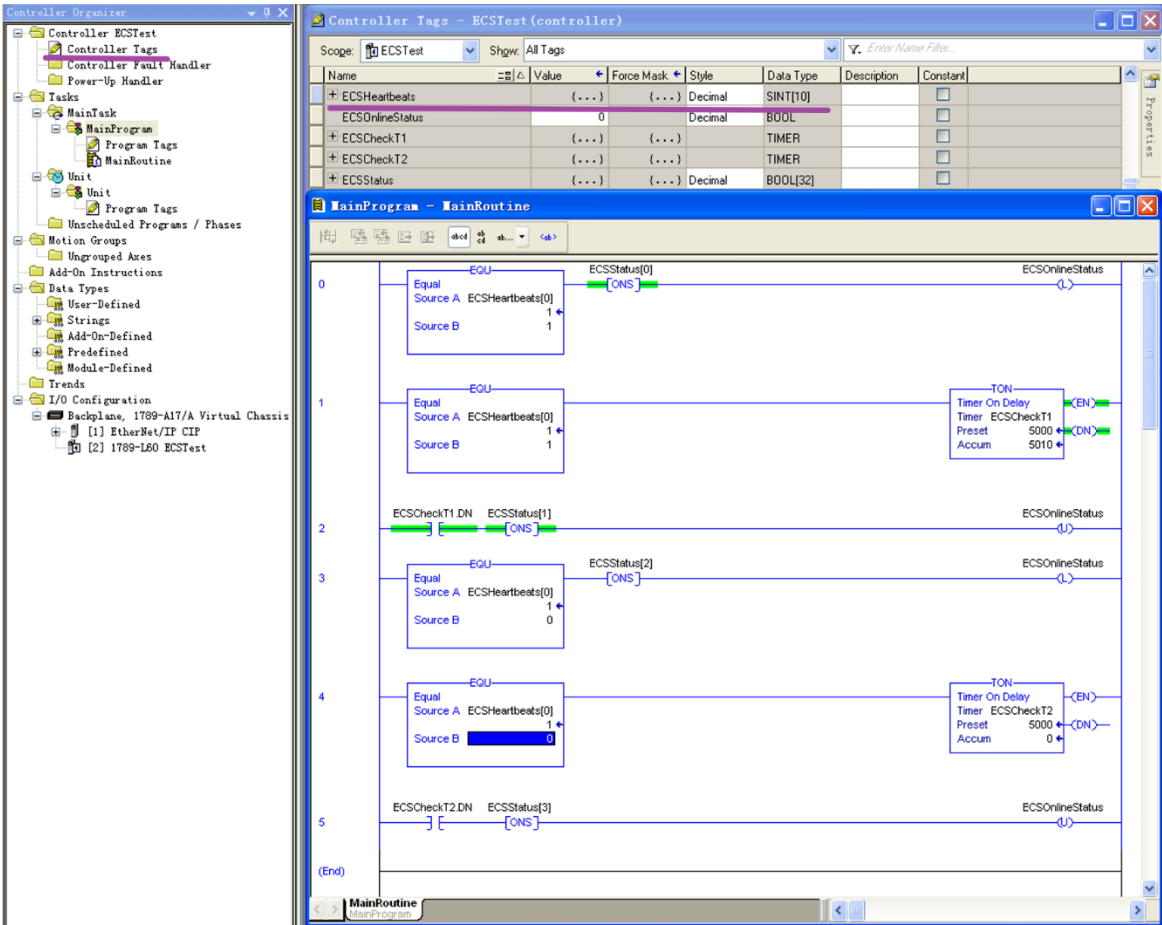
使用步骤：

- 1) 将安装有 CIP Test Tool 的计算机和 PLC 接入同一网络（也可以通过网线直连）
- 2) 请确保计算机的 IP 设置和 PLC 的在同一网段中，可通过 PING 指令验证，能 PING 通即可
- 3) 输入 PLC 的 IP 地址，IP 输入正确后，通讯状态将变为绿色【Connected】
- 4) 点击【Start Search】按钮

- 5) 测试程序将自动搜索 Backplane 和 Slot, 知道 PLC 返回成功信息。最后一次成功信息中包含的 Backplane 和 Slot 即为 PLC 的 Backplane 和 Slot 设置, 在网关中配置 AB PLC 时按照这个配置 Backplane 和 Slot 即可。

8.5 CIP 驱动心跳检测功能实现参考

如需启用心跳检测功能，可参考以下代码实现，其中在控制器标签中添加自定义标签（本例中为 ECSHeartbeats）为必要条件，其他功能实现可根据实际需要自行实现。（程序在安装 ISO 文件里，路径：/Example/ECSTest.ACD）



8.6 心跳信号说明

ECS 网关可以自动发送心跳信号给设备，用于设备诊断功能的实现，心跳信号为一个字节型数组，数组大小为 10。数组中数值的含义如下：

| 数组位次 | 说明 |
|----------|-----------------------------|
| 第 1 个 | 心跳信号为脉冲信号（0/1 周期变化，周期约 2 秒） |
| 第 2 个 | LAN1 口连接的设备通讯状态 |
| 第 3 个 | LAN2 口连接的设备通讯状态 |
| 第 4 个 | COM1 口连接的设备通讯状态 |
| 第 5 个 | COM2 口连接的设备通讯状态 |
| 第 6 个 | COM3 口连接的设备通讯状态 |
| 第 7 个 | COM4 口连接的设备通讯状态 |
| 第 8~10 个 | 预留 |

通讯状态说明

| 状态数值 | 状态说明 |
|------|---------------------------------|
| 1 | 通讯正常 |
| 2 | 正在尝试建立通讯/通讯异常对方设备无响应 |
| 3 | 映射表设置异常 |
| 4 | 等待设备连接（ECS 作为 ModBus Slave 设备时） |
| | |

注意：此为规划功能，目前实现了向 AB 设备发送心跳信号的功能，连接状态功能开发进行中。