

ETHERNET/IP 代理服务器

(EIP-G-MOD2)

V 1.1



北京鼎实创新科技股份有限公司

2020.7

目录

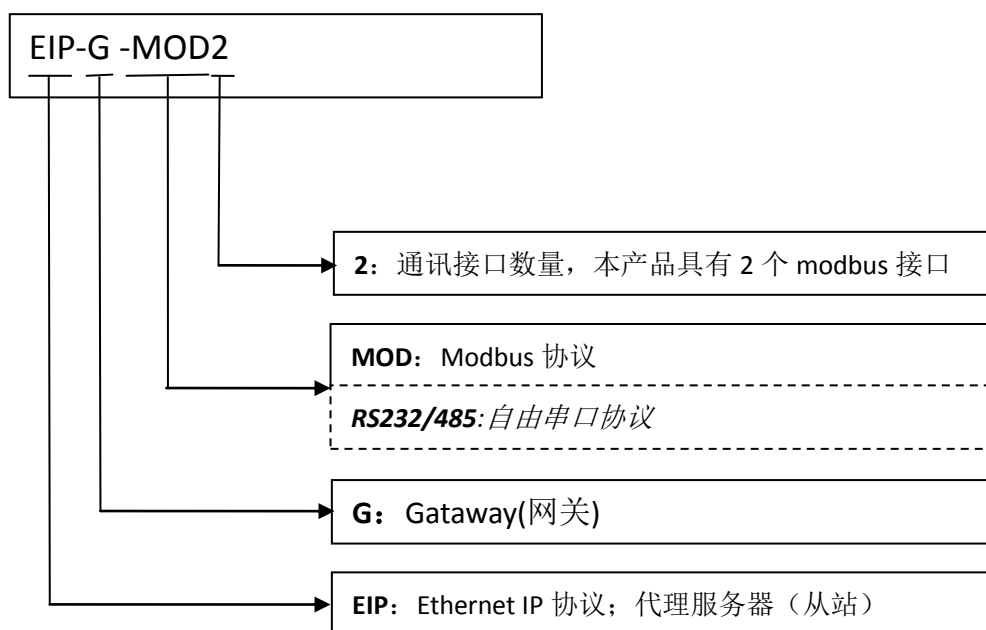
第一章	产品概述.....	1
1.1	产品系列.....	1
1.2	主要用途.....	2
1.3	技术指标.....	2
第二章	产品外观及指示灯.....	4
2.1	产品布局及指示灯.....	4
2.2	网口.....	5
2.3	通讯端子.....	6
2.4	拨码开关.....	6
2.5	电源端子.....	6
第三章	产品外形尺寸与安装.....	7
3.1	产品外形尺寸.....	7
3.2	导轨安装.....	7
3.3	Modbus 接口接插件及安装.....	8
3.4	网线安装.....	8
第四章	配置软件 EipModConfi 的调试.....	9
4.1	配置软件 EipModConfi 安装以及使用说明.....	9
4.1.1	配置软件 EipModConfi 的安装要求.....	9
4.1.2	EipModConfi 安装步骤.....	9
4.1.3	EipModConfi 的使用简介.....	11
第五章	EIP-G-MOD2 的工程配置实例.....	13
5.1	EIPModConfi 软件的配置.....	13
5.1.1	工程的创建.....	13
5.1.2	MODBUS RTU 通讯参数设置.....	14
5.1.3	IO 数据添加与设置.....	15
5.1.4	配置工程的下载.....	17
5.2	产品在 Ethernet/IP 侧（RSLogix 5000 中）的设置.....	18
5.2.1	工程的创建.....	18
5.2.2	EDS 文件的导入.....	18
5.2.3	EIP-G-MOD2 添加及设置.....	22
5.2.4	使用通用网络模块进行配置.....	25
5.2.5	MODBUS 侧状态字和控制字定义.....	27
5.2.6	EIP-G-MOD2 模块在主站模式下的控制字.....	28
5.2.7	RSLogix 工程的下载.....	30
5.2.8	寄存器监视.....	31
5.2.9	MODBUS 从站状态监测.....	34
5.3	/Ethernet/IP 侧 IP 地址设置.....	36
第六章	附录：MODBUS 技术简介.....	40
6.1	MODBUS 通信协议.....	40
6.2	MODBUS 协议要点.....	41
6.3	异常应答.....	42
6.4	MODBUS 存储区.....	43

6.5	MODBUS 功能码.....	43
第七章	有毒有害物质表.....	50

第一章 产品概述

1.1 产品系列

EIP-G-MOD2 代理服务器（以下有时也称为“网关”）是鼎实公司 ETHERNET/IP 代理服务器系列产品中的一种，功能是将 modbus 从站连接到 Ethernet IP 网络的协议转换模块。该产品在 modbus 侧做主站，可以将各种 modbus 从站，如变频器、电机保护器、阀门、仪表、IO 模块等产品接入到 Ethernet IP 主站。



使用该产品时,用户需要在鼎实公司的 EipModConfi 软件中,对 modbus 从站进行组态,内容包括:通讯波特率、站地址、起始地址、数据长度等。然后通过以太网接口下载到 EIP-G-MOD2 模块中。EipModConfi 软件为鼎实公司自主开发产品,用户可以免费使用。在 Ethernet IP 侧,有一个与 EIP-G-MOD2 产品配套使用的 EDS 文件,用户需要将该文件加载到 Ethernet IP 主站组态软件中,并对该产品进行组态。

本产品手册只适用于产品 EIP-G-MOD2。

1.2 主要用途

EIP-G-MOD2 产品用来实现 ETHERNET/IP 协议与 MODBUS 协议的转换。该产品在 ETHERNET/IP 侧作为 Adapter，在 Modbus 侧作为主站，用来将 Modbus 从站设备接入 ETHERNET/IP 网络当中去。产品连接示意如下图 1-1 所示，左侧红框中的产品为 EIP-G-MOD2。

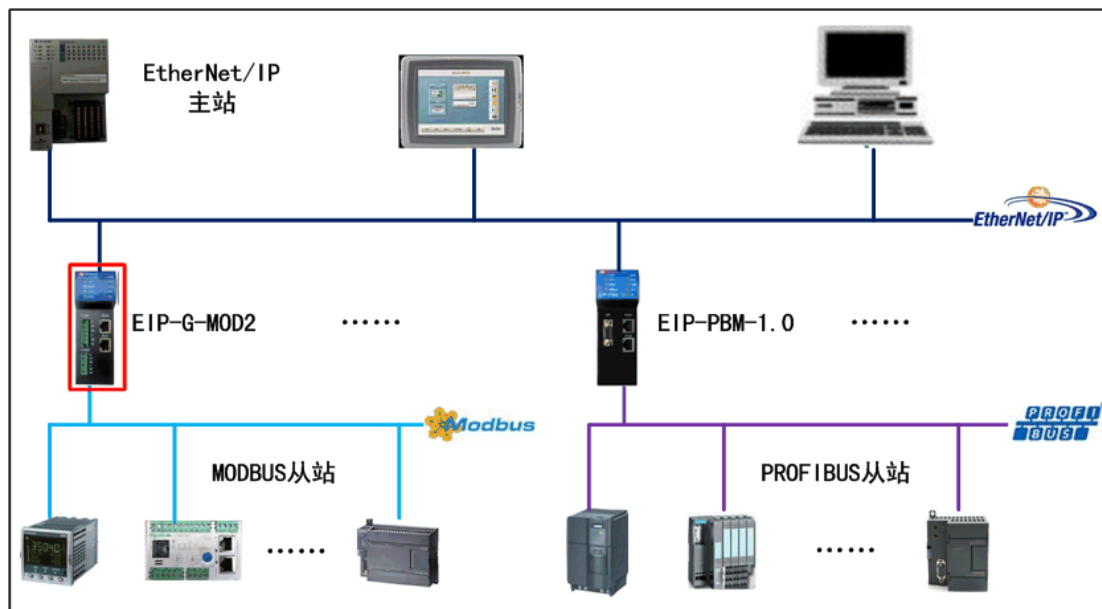


图 1-1 EIP-G-MOD2 应用示意图

1.3 技术指标

(1)、Ethernet/IP 通讯接口

- Ethernet/IP 协议：支持 UCMM 和 GET、SET Attribute，不支持 DLR
- Ethernet/IP 的 RPI：最小 2ms

(2) Modbus RTU 通讯接口

- 标准 Modbus RTU 协议：支持 01H、02H、03H、04H、05H、06H、0FH、10H 功能码；
- 波特率支持：600、1200、2400、4800、9600、19.2K、38.4K、57.6K、115.2Kbps 可选；
- 校验位：(8 位无校验 1 停止位、8 位偶校验 1 停止位、8 位奇校验 1 停止位、8 位无校验 2 停止位) 可选。
- 最大从站数：31
- 状态字与控制字：产品提供控制字节和状态字节，方便 Modbus 从站设备的使用和通讯状态监控。
- 最大 IO 数据总长度：496Bytes 输入+ 496Bytes 输出
- 单从站最大槽数：54

(3)、配置下载

- 配置下载方式：以太网
- 上位软件：EipModConfi;

(4)、EIP-G-MOD2 产品 EDS 文件

EDS 文件将所有数据置于一个 EO 连接中，其中 2 字节状态位占输入的前 2 个字节，用于显示对应 2 条 485 总线状态，总的输入不超过 496Bytes；2 字节控制寄存器占输出的前 2 个字节，用来控制 2 条 485 总线输出，总字节数根据用于配置有所不同，总的输出字节数不超过 496Bytes。

(5)、供电

- 电源电压：DC 24V（±20%）
- 额定电流：24V 下，约为 123mA
- 额定功率：2.9W
- 隔离电压等级：1500V

(6)、防护等级

- 防护等级：IP20

(7)、环境条件

- 运输和存储温度：-40℃ ~ +70℃
- 工作温度：-25℃~ +55℃
- 工作相对湿度：+25℃下，95%（无凝露）

(8)、机械特性

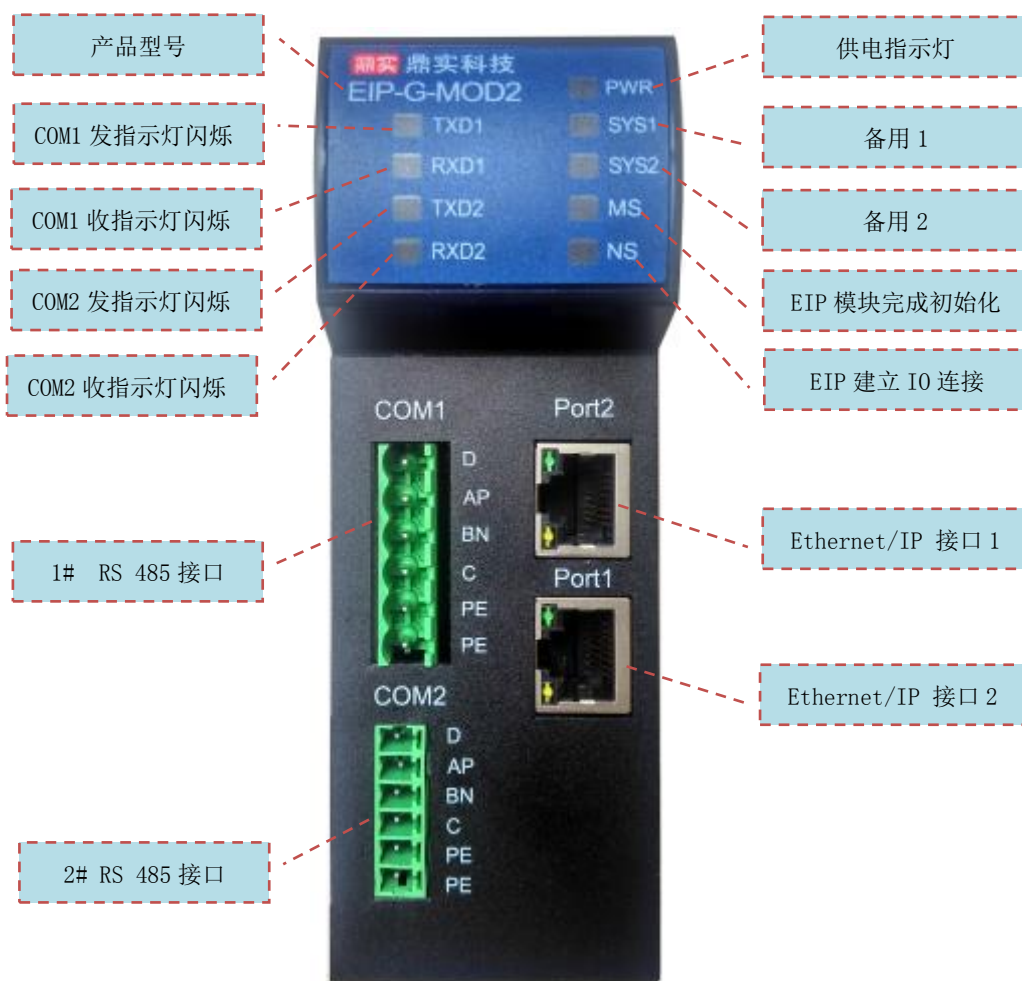
- 外壳主体：ABS+PC
- 尺寸：详见第三章

(9)、EMC 等级

- 静电放电：IEC61000-4-2, 接触放电 4kV, 空气放电 8kV;
- 电快速脉冲群：IEC61000-4-4, 3kV
- 浪涌抗扰度：IEC61000-4-5, 线地 2kV, 线线 1kV

第二章 产品外观及指示灯

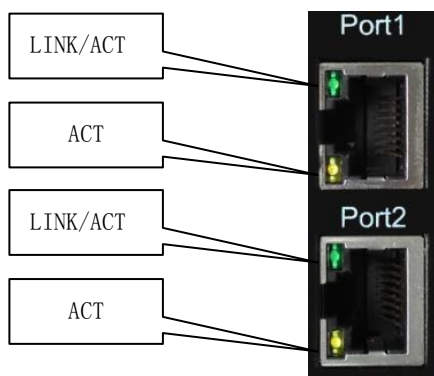
2.1 产品布局及指示灯



模块正面 LED 含义

LED 名称	状态	含义
TXD1	灭	1#RS485 有数据向现场设备发送
	闪烁	1#RS485 设备初始化未完成
RXD1	灭	1#RS485 无数据接收状态
	闪烁	1#RS485 有来自现场设备数据
TXD2	灭	2#RS485 无数据接收状态
	闪烁	2#RS485 有数据向现场设备发送
RXD2	闪烁	2#RS485 有来自现场设备数据
	灭	2#RS485 无数据接收状态
PWR	灭	设备未上电或电源故障
	绿色常亮	设备电源正常
MS	绿色常亮	Ethernet/IP 模块完成初始化
	灭/红色常亮	Ethernet/IP 模块异常
NS	绿色常亮:	Ethernet/IP 建立 IO 连接
	绿色闪烁:	Ethernet/IP 网络参数配置完成 (IP 地址), 等待建立 IO 连接
	灭:	未分配 IP 地址
	红色闪烁:	IO 连接超时

2.2 网口



LED 名称	状态	含义
LINK/ACT	灭	端口无连接, 或连接异常 (Link Down)
	绿灯常亮	端口连接正常 (Link Up)
	绿色闪烁	端口 10/100M 有数据收发
ACT	未使用	

2.3 通讯端子

通讯端子接线定义

端子	PIN	名称	涵义	备注
	1	D	终端电阻 D	将 D 与 AP 短接 将 C 与 BN 短接 可以使总线终端电阻有效
	2	AP	数据线 A-	
	3	BN	数据线 B+	
	4	C	终端电阻 C	
	5	PE	接双绞线屏蔽	
	6	PE	接双绞线屏蔽	

2.4 拨码开关

产品功能码拨码开关 SW1-4



拨码	功能	描述
SW 1	设备默认 IP 地址	ON: 设备使用默认 IP (192.168.0.99) OFF: 设备使用系统分配 IP
SW 2	未定义	保留
SW 3	未定义	保留
SW 4	未定义	保留

2.5 电源端子

电源端子接线定义

端子	PIN	涵义	备注
	1	第一路电源+24V DC	
	2	第一路电源 GND	
	3	第一路电源 PE	
	4	第二路电源+24V DC	
	5	第二路电源 GND	
	6	第二路电源 PE	

第三章 产品外形尺寸与安装

3.1 产品外形尺寸

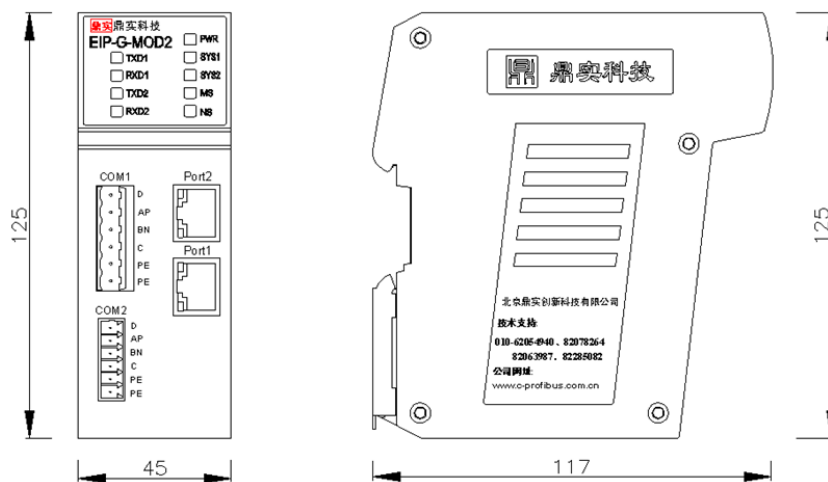


图 1 EIP-G-2MODBUS 外形尺寸图

3.2 导轨安装

安装组件：35mm 宽导轨，安装与拆卸示意图：

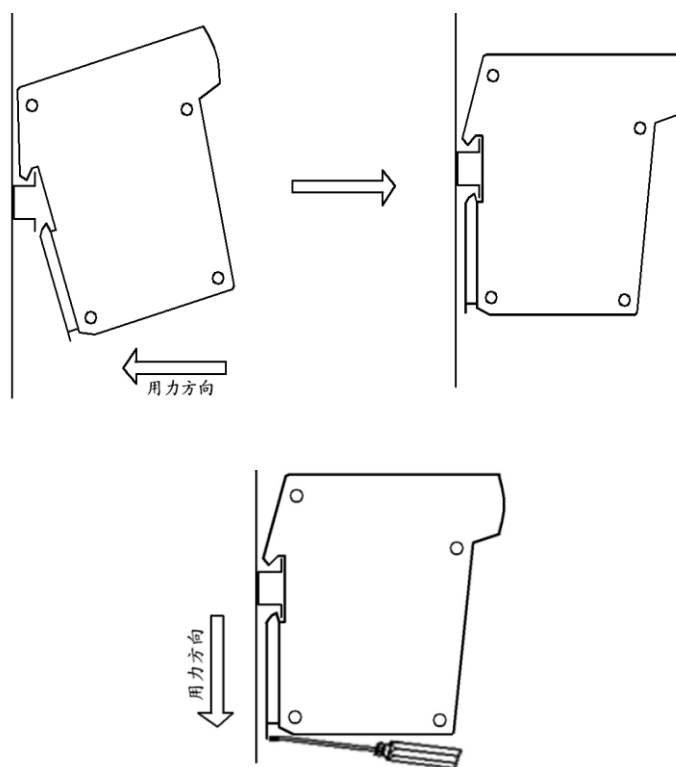


图 2 EIP-G-2MODBUS 安装、拆卸过程示意图

3.3 Modbus 接口接插件及安装

EIP-G-2MODBUS 总线桥的接口，采用标准 RS485 标准，采用端子接线，建议用户使用标准双绞屏蔽电缆，并在总线两端设置终端电阻。

3.4 网线安装

以太网端口：RJ45 接头，平行线、交叉线自适应。如果想得到更加稳定的通讯保障，获得更强的抗干扰能力，建议使用工业以太网网线。工业以太网网线的构造为四芯铜线，带有屏蔽层，具有很强的屏蔽外界信号抗干扰的能力，使用这种网线能够大大提升通讯系统的稳定性。

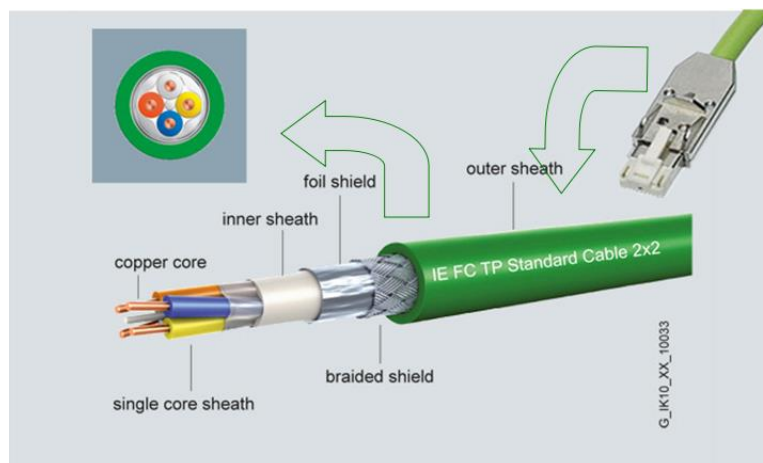


图 3-5 工业以太网网线

第四章 配置软件 EipModConfi 的调试

4.1 配置软件 EipModConfi 安装以及使用说明

4.1.1 配置软件 EipModConfi 的安装要求

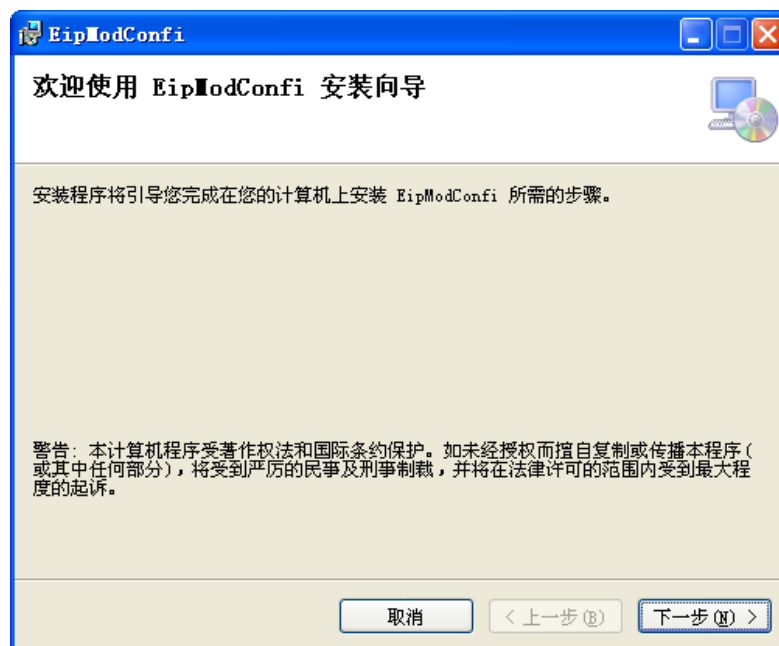
软件安装配置要求	
操作系统	Windows XP(Service Pack 3)以上版本
CPU	Intel Pentium 以上
内存	1GB 以上
显示	1024*768 以上
硬盘	1G 以上硬盘空间

4.1.2 EipModConfi 安装步骤

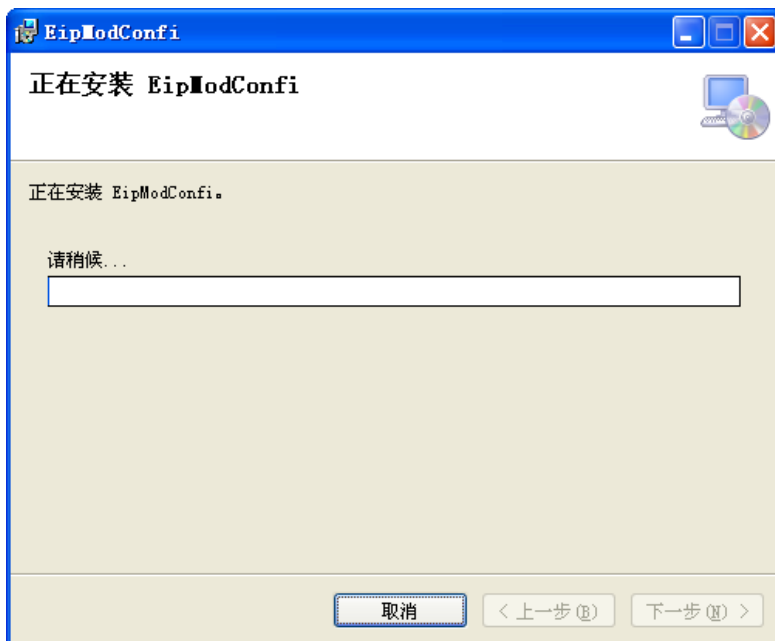
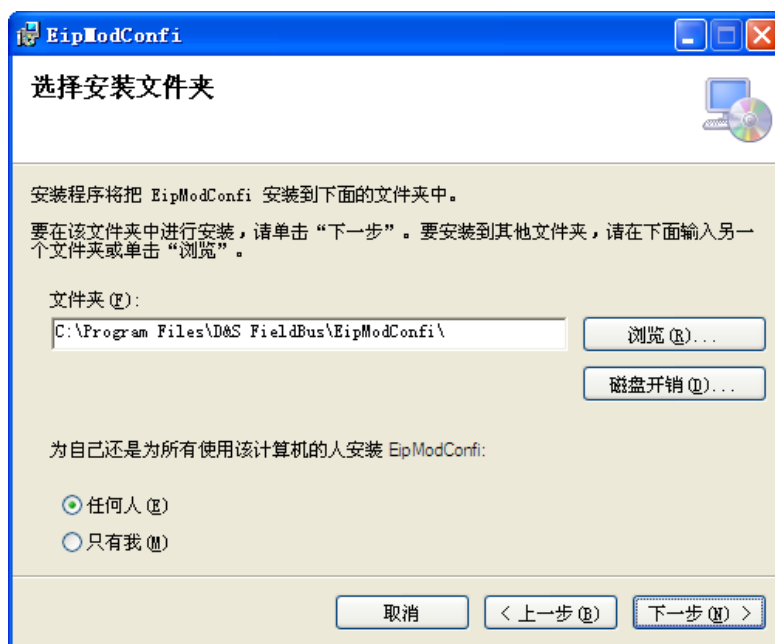


EipModConfi
Setup.msi

安装包双击安装包，弹出选择路径对话框，用户可选择安装路径，保持默认即可



点击下一步

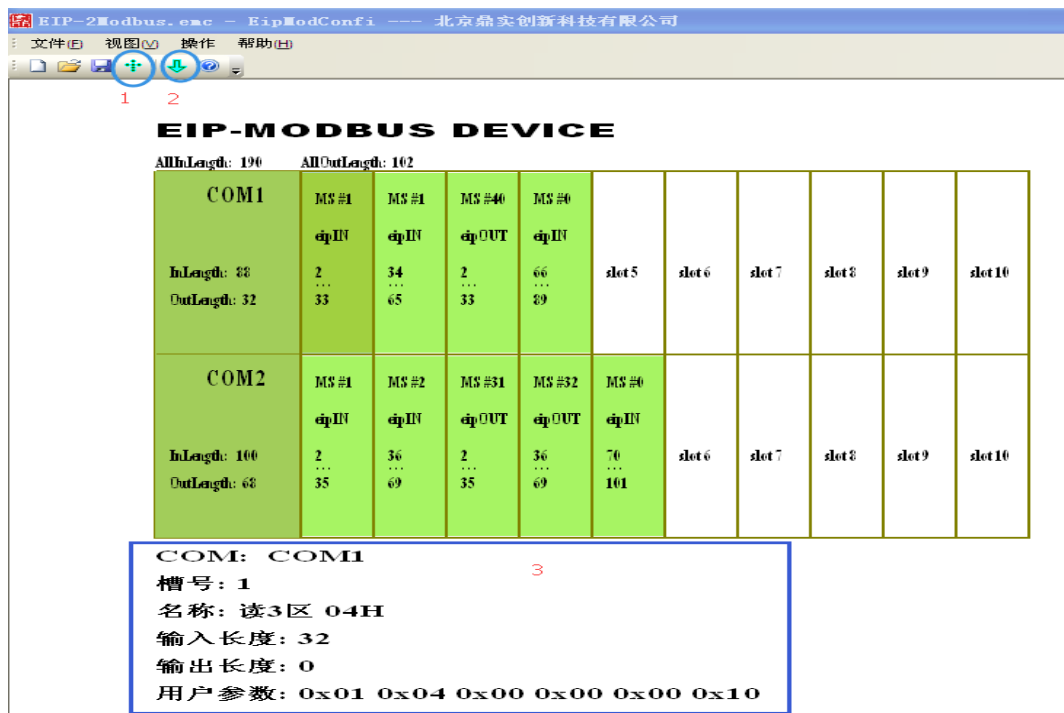


安装完成后, 在程序开始菜单和桌面都会出现快捷方式

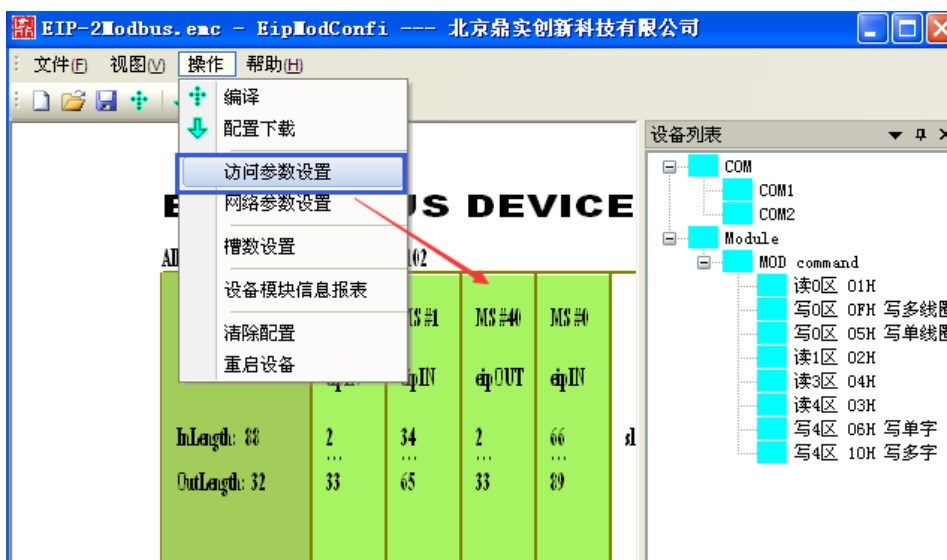


4.1.3 EipModConfi 的使用简介

4.1.3.1 软件主界面



4.1.3.2 编译、下载工程配置、以太网下载接口设置



4.1.3.3 COM 接口参数设置

COM 接口包括

EIP 数据长度：表示此 COM 接口配置 Modbus 设备后，生成的 EIP 输入数据和输出数据长度，
EIP-G-Mod2 设备的 EIP 数据长度：表示此设备生成的 EIP 输入数据和输出数据总长度。



EIP-MODBUS DEVICE

		AllInLength: 22 AllOutLength: 22									
COM1	MS#1										
	eipIN										
InLength: 20	2	slot 2	slot 3	slot 4	slot 5	slot 6	slot 7	slot 8	slot 9	slot 10	
OutLength: 0	...										
	21										
COM2	MS#1										
	eipOUT										
InLength: 0	2	slot 2	slot 3	slot 4	slot 5	slot 6	slot 7	slot 8	slot 9	slot 10	
OutLength: 20	...										
	21										

4.1.3.4 网络参数设置

网络设置可通过 RSLogix 5000 中自带工具 BOOTP-DHCP Server 进行配置也可通过 EIPConfi 配置，具体使用请参照第五章。

第五章 EIP-G-MOD2 的工程配置实例

本产品使用需与 EIPModConfI 配合使用,EIP-G-MOD2 使用的是 EIPModConfI 软件的以太网下载功能,将配置工程参数下载到适配器中,这里以一个应用实例配置为例。具体配置如下:


表 5-1 实例配置表

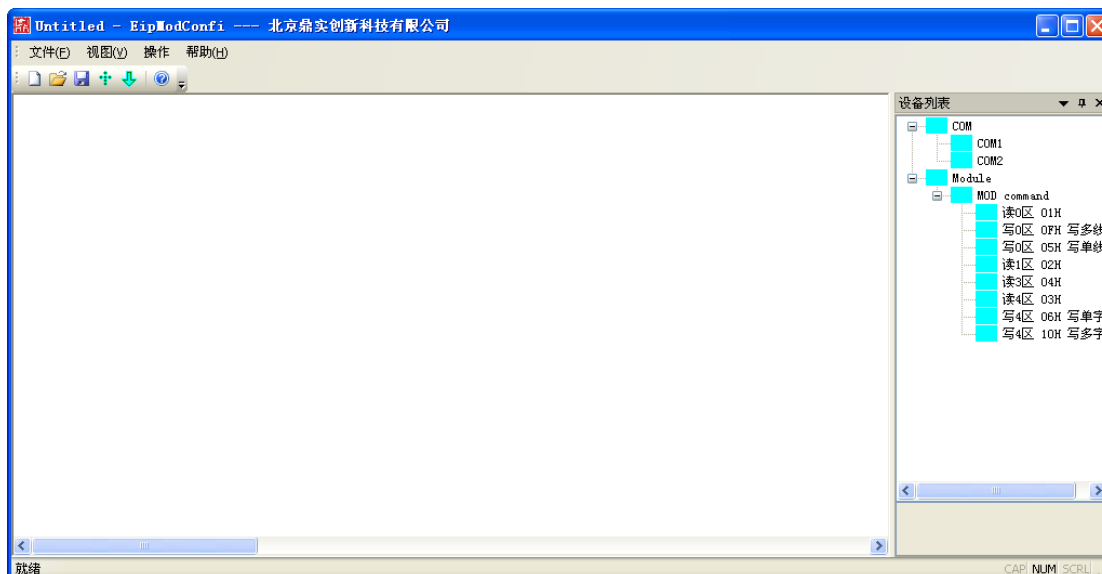
配置实例设备表				
序号	设备名称	型号	数量	备注
1	网关设备	EIP-G-MOD2	1	本产品
2	PC	安装 ModSim 用来模拟 MODBUS RTU 从站	1	
3	CompactLogix L16ER	PC(RSLogix5000 + EIPModConfI1.0)	1	Controller
		1769-L16ER-BB1B	1	
4	485 转 232 模块		1	用来将网关与 PC 相连
5	网线 (带有水晶头)	普通网线	2	建议使用工业以太网线

5.1 EIPModConfI 软件的配置

5.1.1 工程的创建

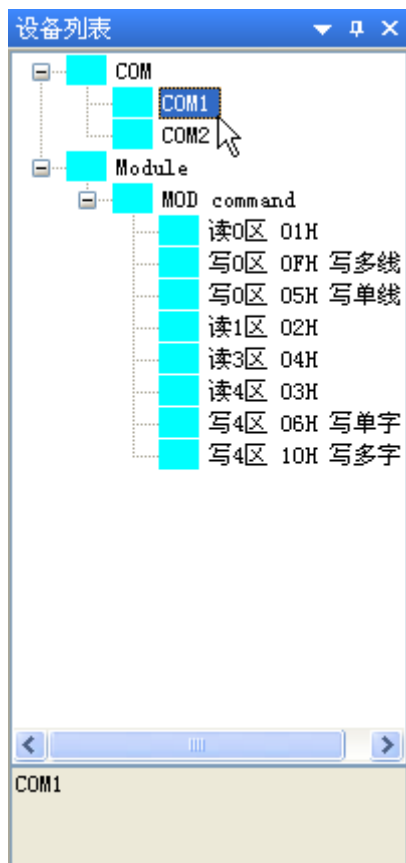


双击桌面快捷方式 ，打开配置软件，如下图：



5.1.2 MODBUS RTU 通讯参数设置

EIP-G-MOD2 自带两路 RS485 总线，COM1 和 COM2，故在配置软件在右侧设备列表中选择对应总线，双击加入到工程，



EIP-MODBUS DEVICE

AllInLength: 2	AllOutLength: 2									
COM1	slot 1	slot 2	slot 3	slot 4	slot 5	slot 6	slot 7	slot 8	slot 9	slot 10
InLength: 0										
OutLength: 0										

双击 EIP-G-MOD2 图标中的最左侧槽位（COM1），弹出总线配置对话框如下图：

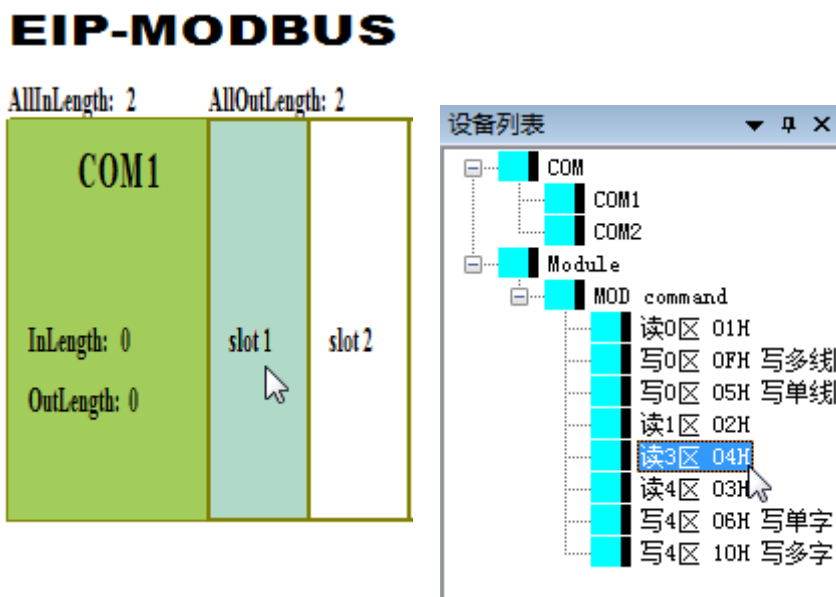


通过此画面可配置 MODBUS 侧通讯参数包括：波特率、奇偶校验、数据位、停止位等，选择默认参数作为样例进行试验。

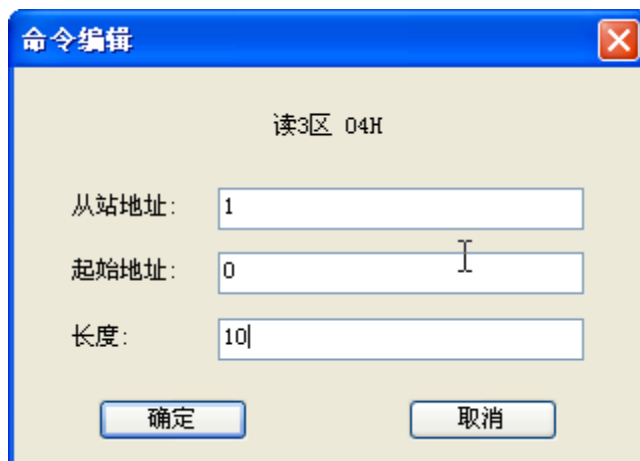
5.1.3 IO 数据添加与设置

在 EIPConfi 工具右侧 Module 中选择对应的操作，以 3 区读 10 个字与 4 区写 10 个字为例进行配置。

选中 slot1 插槽，双击右侧读 3 区 04H，



弹出如下对话框：

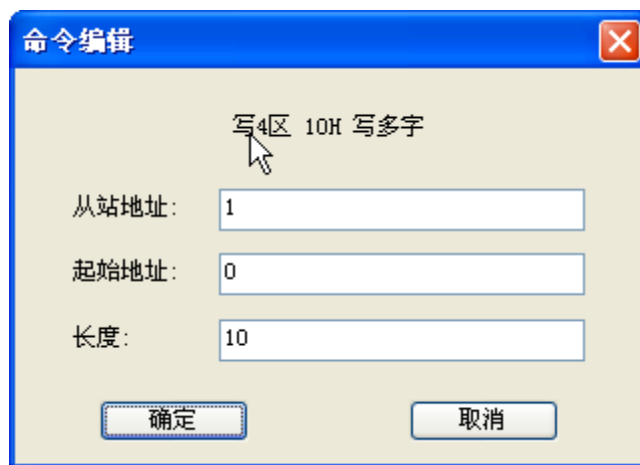


设置从站地址、寄存器起始地址以及数据长度，对应上图进行添加即为：

读取从站地址为：1 数据区：3 区 寄存器起始地址为：0 一次读取数据长度：10 words

同理添加写命令，

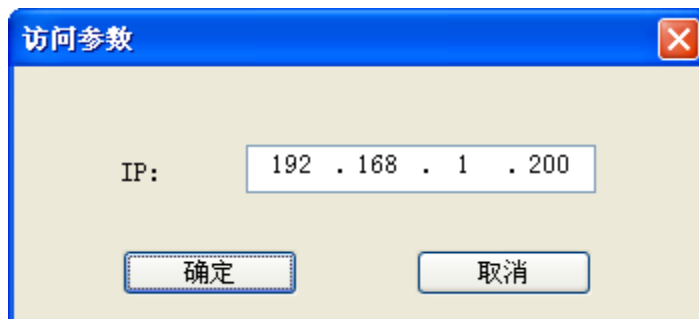
写入从站地址为：1 数据区：4 区 寄存器起始地址为：0 一次写入数据长度：10 words




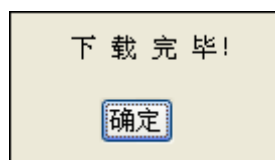
点击编译快捷键  完成工程编译。

5.1.4 配置工程的下载

可将 EIP-G-MOD2 模块下方拨码 1 拨至 ON 使用默认 IP 地址：192.168.0.99，在配置工具菜单中选择 操作-访问参数-设置 IP 地址 192.168.0.99



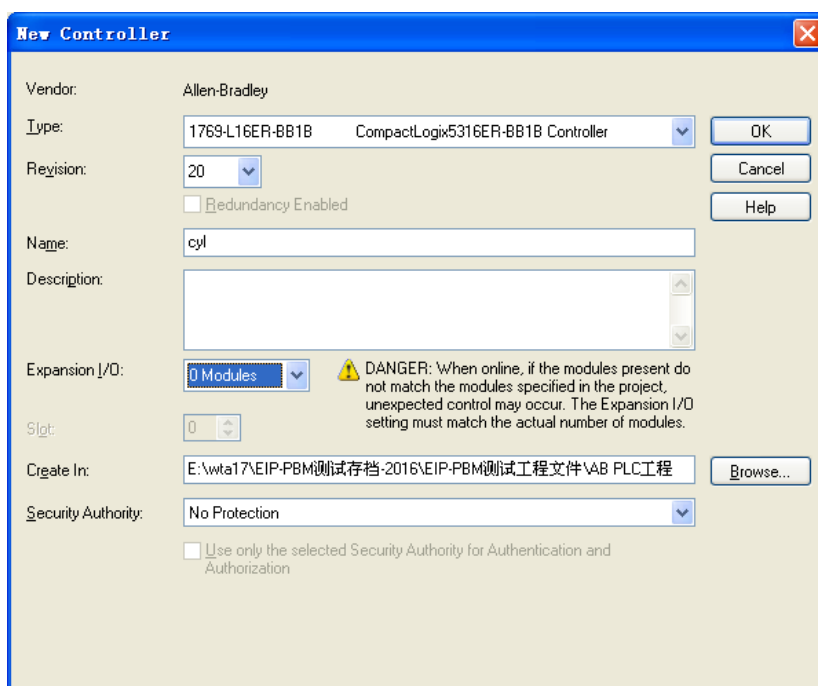
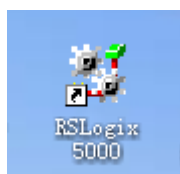
设置好目标 IP 地址以后点击下载配置快捷键, 当 EIPConfi 显示下载完毕时表明配置下载成功，点击确定即可。



5.2 产品在 Ethernet/IP 侧（RSLogix 5000 中）的设置

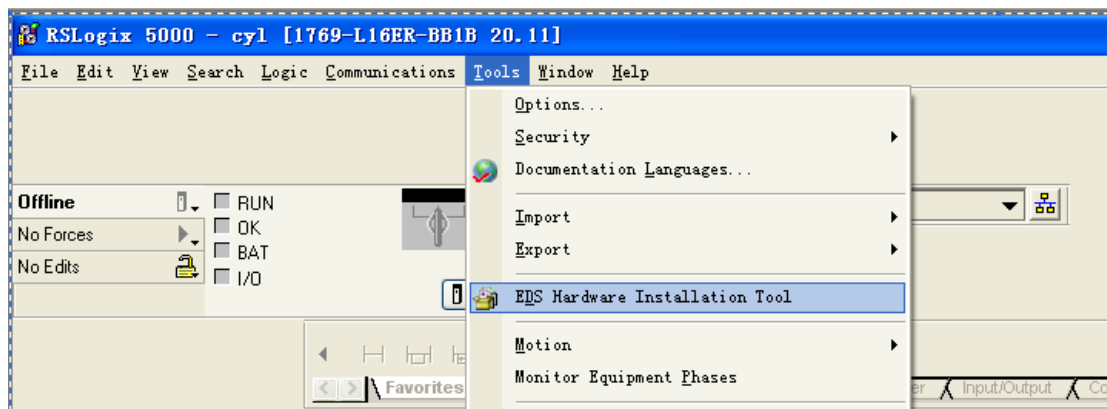
5.2.1 工程的创建

双击已安装好的 AB 编程软件 RSLogix 5000 弹出选择控制器对话框，选择相应的 CPU 如：1769-L16ER-BB1B。

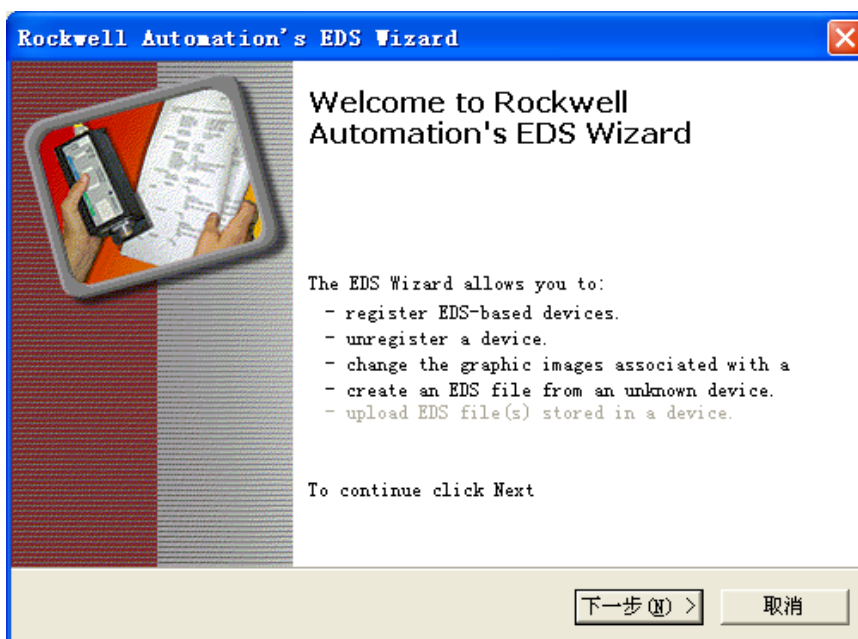


5.2.2 EDS 文件的导入

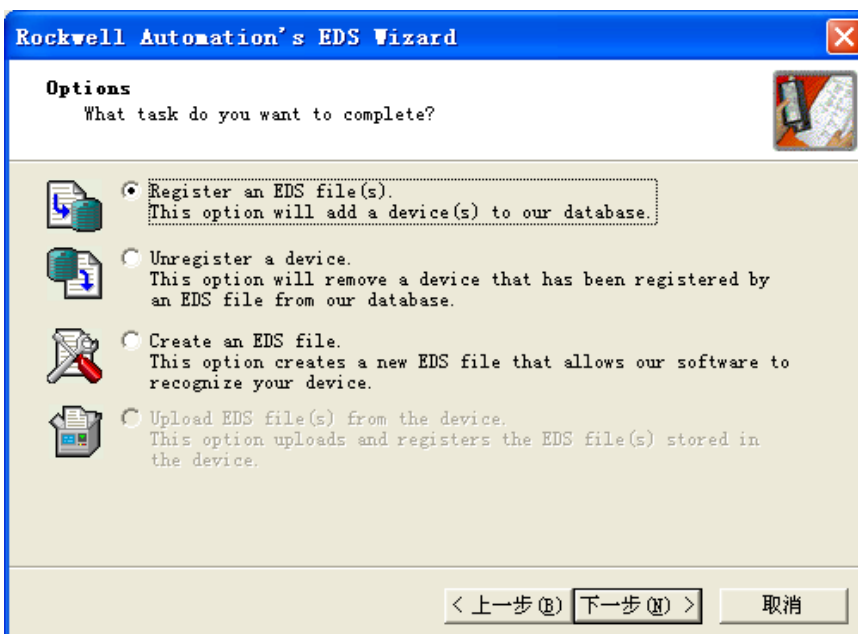
首次使用本适配器需将鼎实公司提供的 EDS 文件导入到 RSLogix 5000 中 EIP-MODBUS.eds, 在软件的菜单 Tools 中选择 EDA Hardware Installation Tool



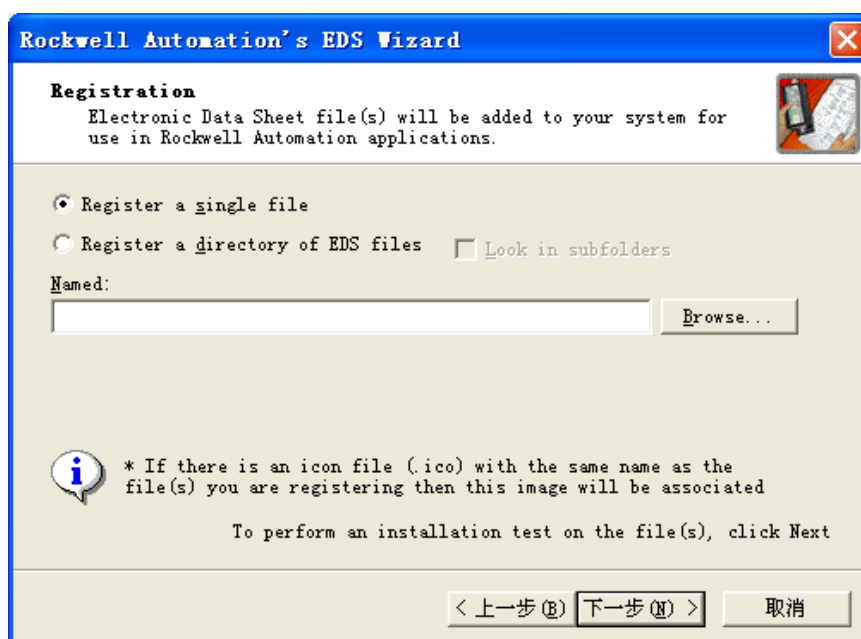
弹出如下菜单点击下一步：



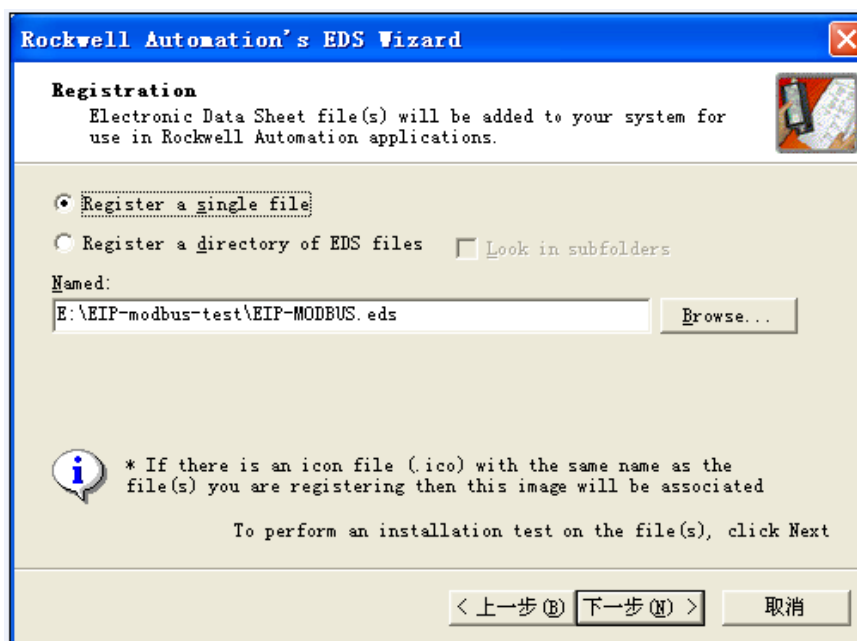
弹出下图菜单，保持默认即可，点击下一步：



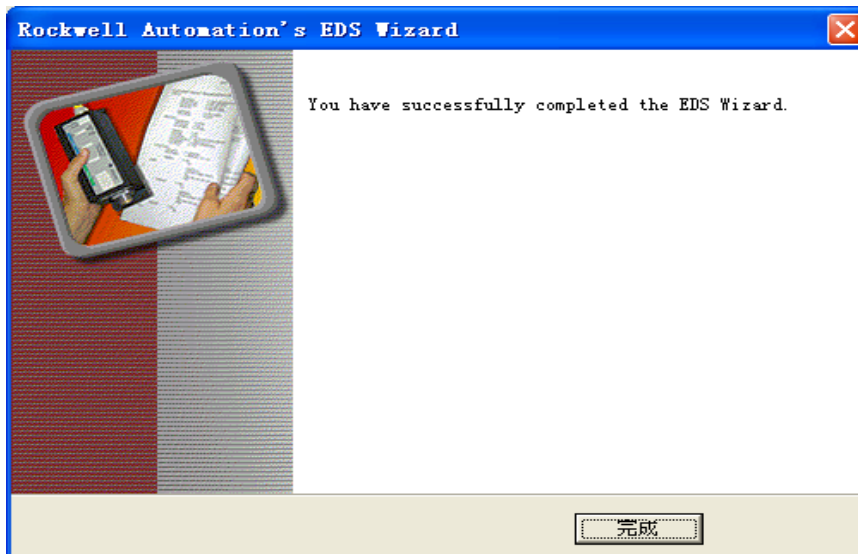
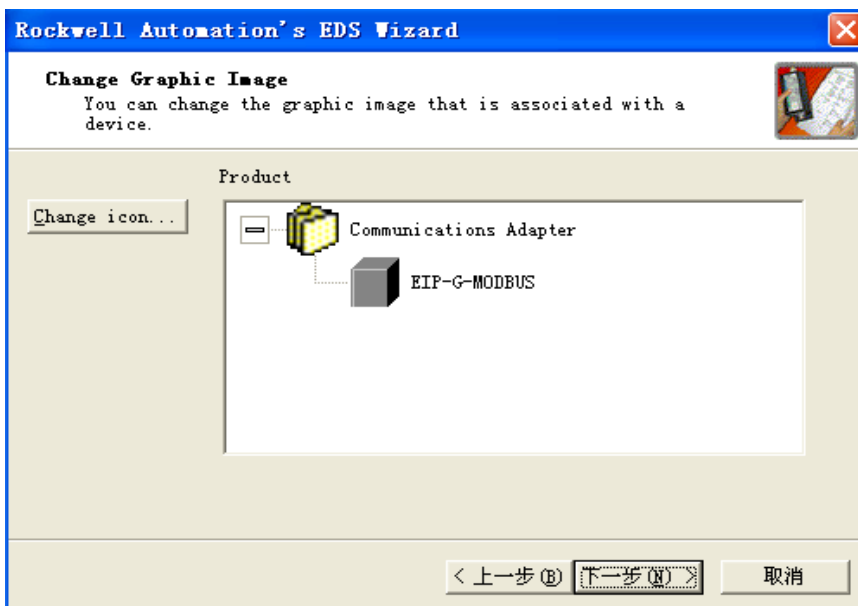
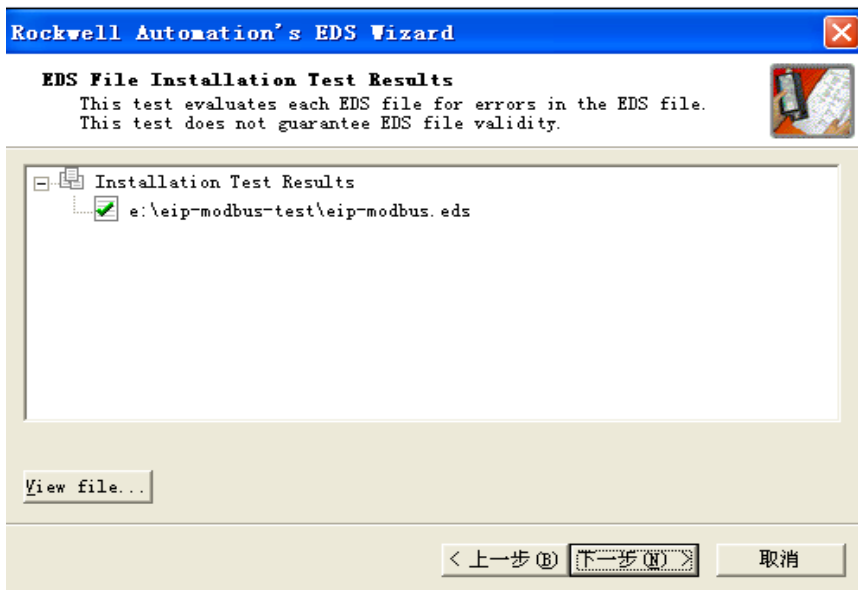
选择点击 Browse 手动选择 EDS 文件所在的目录，



选中 EIP-MODBUS.eds 文件点击打开：

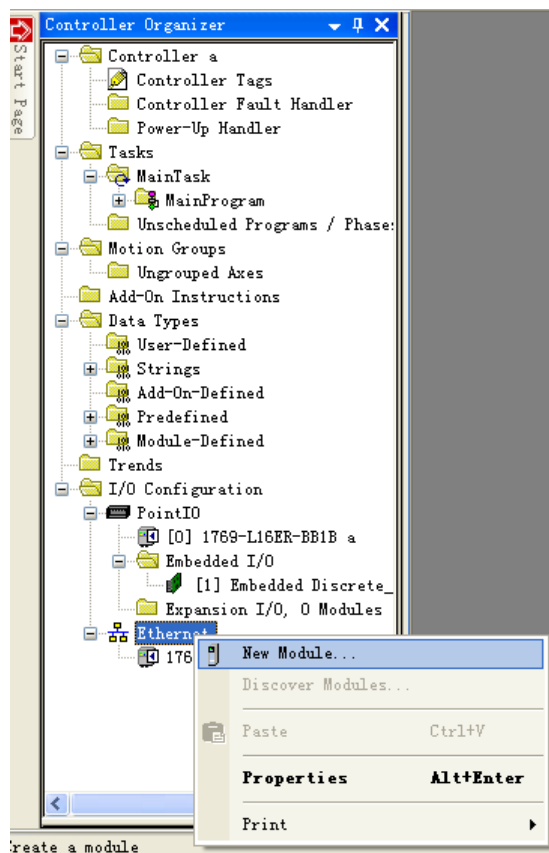


继续点击下一步：

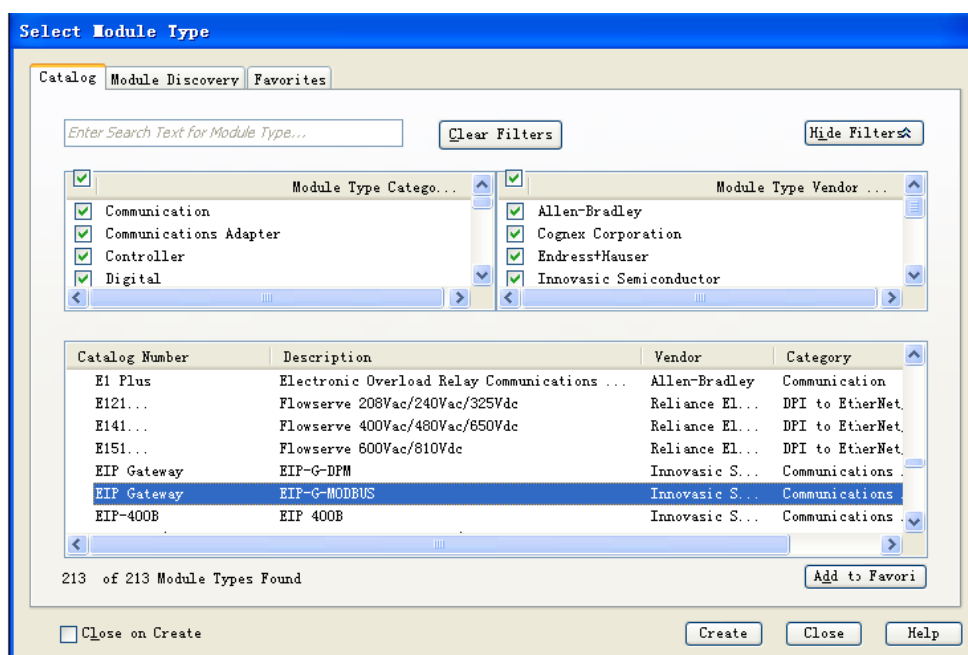


5.2.3 EIP-G-MOD2 添加及设置

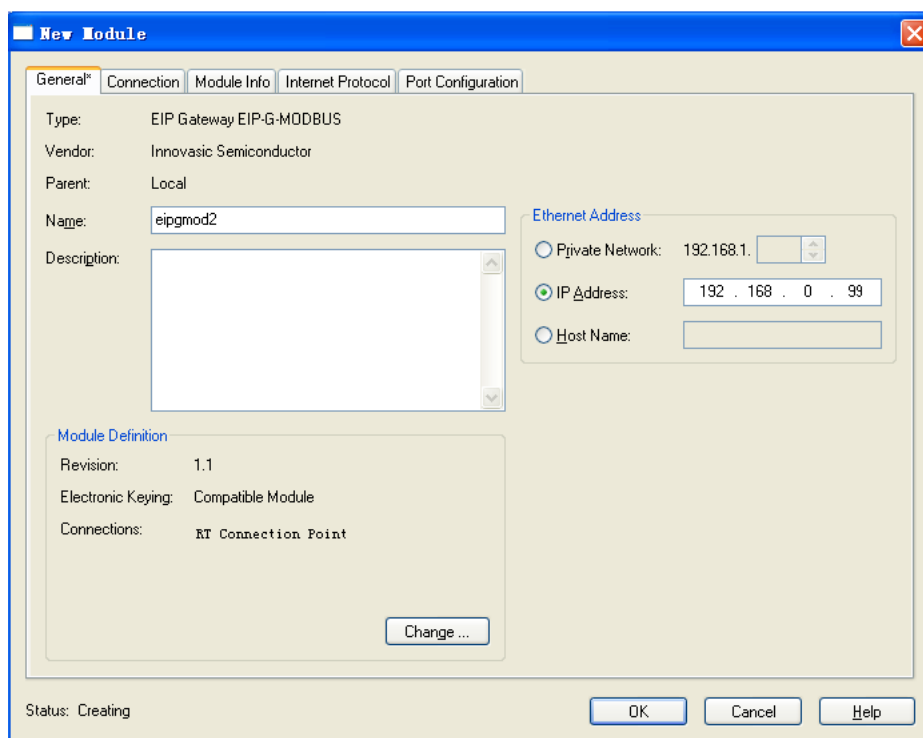
首先在左侧 Controller Organizer 对话框中选中 Ethernet→点右键选择 New Module



在弹出的 Select Module Type 中选中新添加的 EIP-MODBUS.eds 点击 Create，将设备加入到工程。



同时会弹出 New Module 设置对话框如下图：



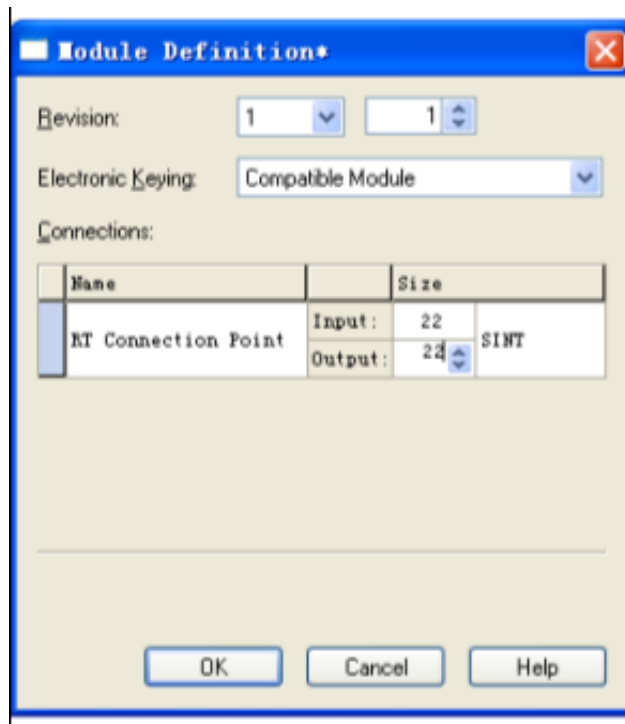
在 Ethernet Address 填入适配器的 IP 地址 (BIT 1 为 ON 时为默认 IP: 192.168.0.99), 点击 Change 按钮弹出 Module Definition 对话框在 Name 列选择 RT Connection Point, 填入对应的 Input、Output 字节数, 输入输出总字节数必须与配置工具总数据量一致, 否则无法通讯。

注: Input 字节长度=MODBUS 侧 Input 数据长度+总线状态字节长度、Output 字节长度=MODBUS 侧 Output 数据长度+总线控制字节长度, 如长度不一致会导致 I/O 无法通讯, 具体适配器状态寄存器定义以及控制寄存器定义见下节。

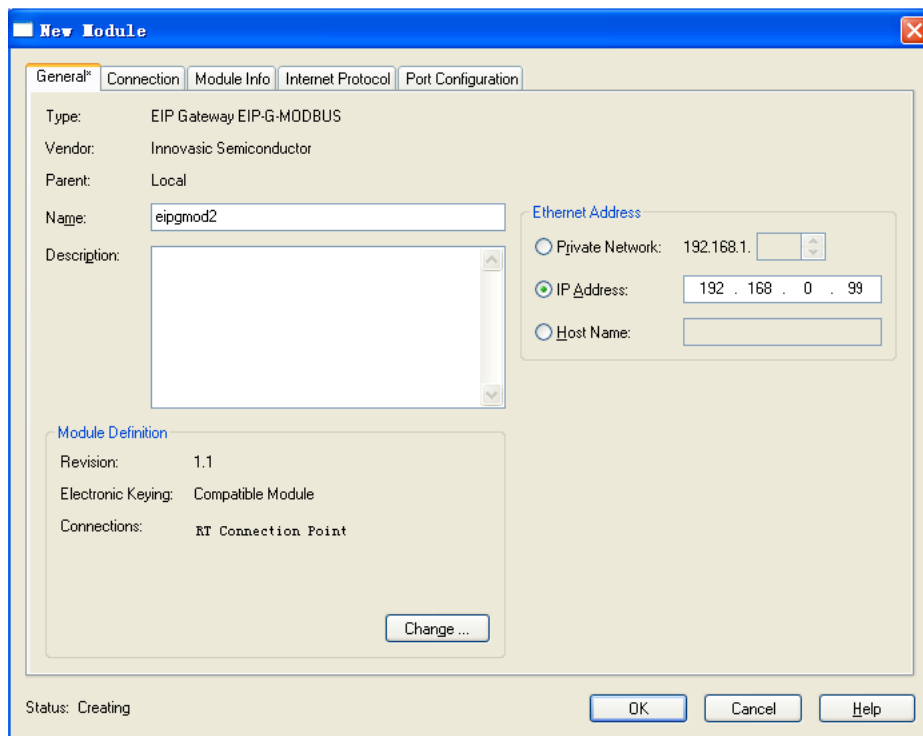
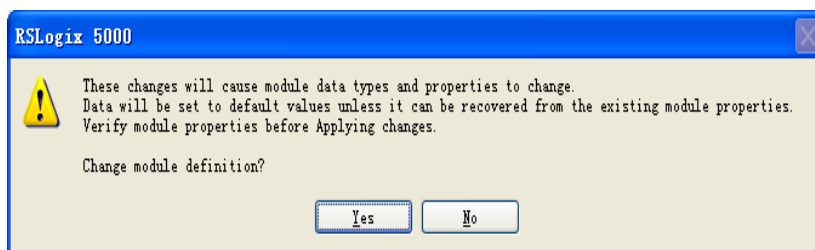
EIP-MODBUS DEVICE

AllInLength: 22 AllOutLength: 22

EIPConfi 配置工具数据量



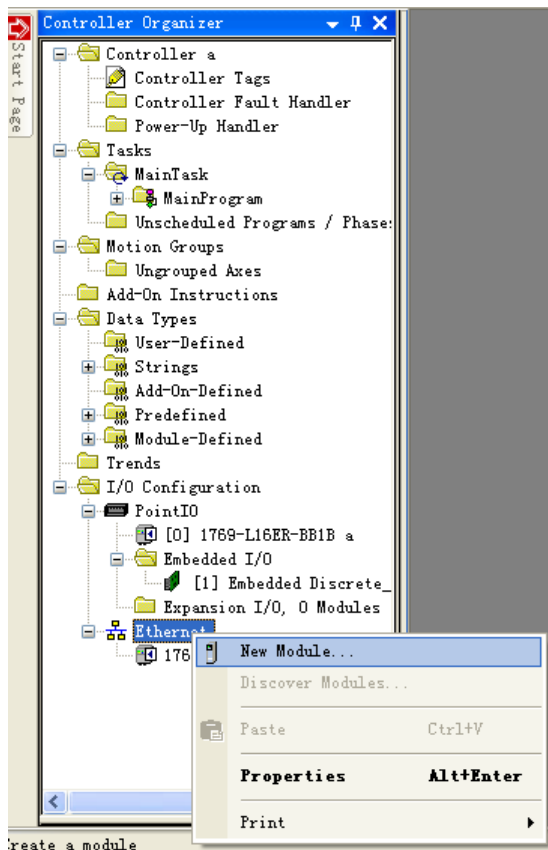
点击 OK 弹出如下提示对话框，选择 YES 即可。



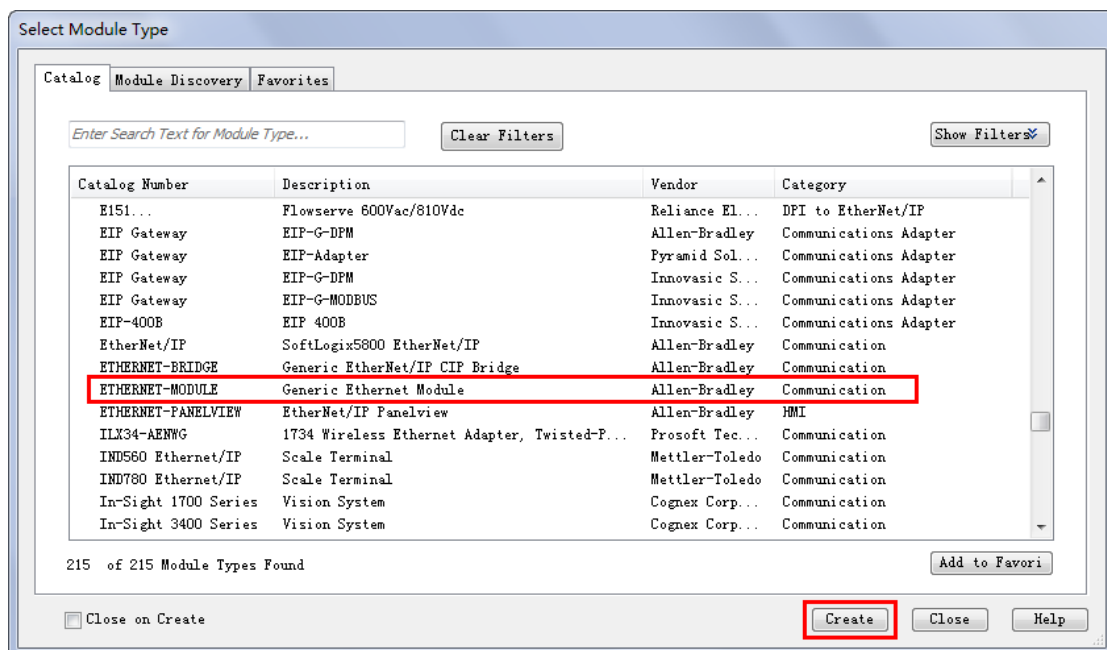
5.2.4 使用通用网络模块进行配置

本公司提供的 EDS 文件在 RSLOGIX5000 组态软件 V20 以上的版本可以正确解析，配置。在 V19 及以下版本，EDS 文件无法正确解析。需要使用通用网络模块（ETHERNET MODULE）进行配置。

(1)、新建 module



(2)、选择“ETHERNET-MODULE (Generic Ethernet Module)”，点击“创建”



(3)、对参数进行修改

Comm Format: 选择数据格式, 本例中选择 SINT

Address/Host Name: 写入网关模块的 IP 地址, 本例中 IP 地址为: 192.168.0.99

Connection Parameters: 设置连接参数

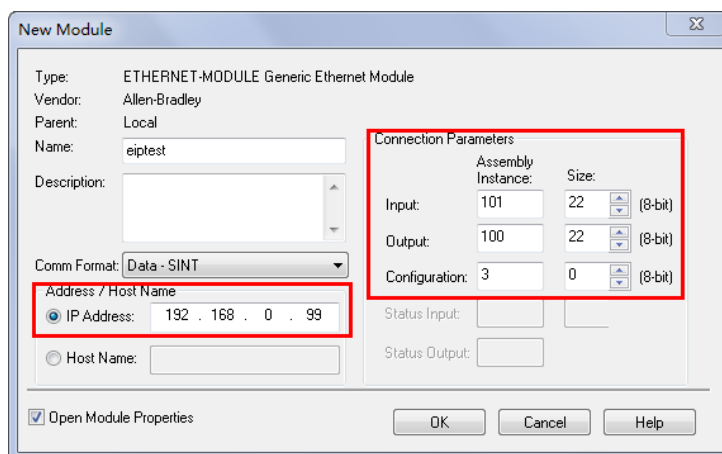
Assembly Instance : 配置实例值

Input: 101

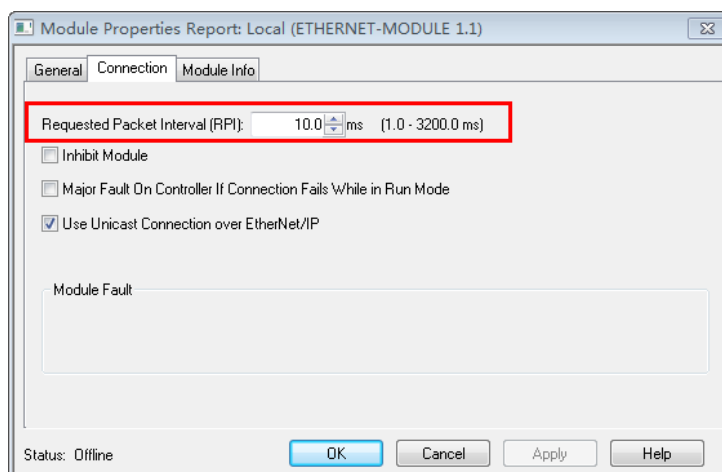
Output: 100

Configuration: 非 0 即可, 本例填写 3

Size: 配置数据长度, 与 5.2.3 一样, 本例配置 22sint 输入, 22sint 输出



点击“确定”后, 进入“Connection”配置界面, 这里可以修改“RP”参数, 改变模块扫描的时间间隔。本例中使用缺省值, 其他参数不做更改。



点击“确定”, 模块添加完成。

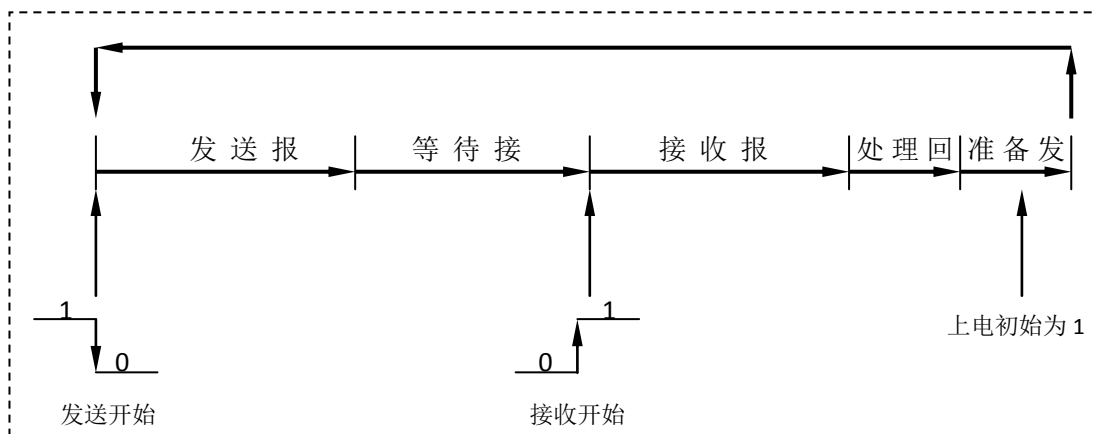
5.2.5 MODBUS 侧状态字和控制字定义

MODBUS RS485 总线状态字跟控制字分别定义在 Ethernet/IP 侧输入与输出前两个字节，具体状态字与控制字定义如下：

(1)、通信状态字格式

D7:oe_er	D6:CRC_er	D5:Tmdr_O	D4~D1:M_ER_CODE	D0:re_tr
奇偶校验错	CRC 校验错	等待 M 回答到时	MODBUS 异常应答码	接收/发送

(2) 接收完毕/发送允许 D0: re_tr



re_tr=1: 接口正在接收或处理接收报文或准备发送的状态。本手册描述 EIP-G-MOD2 产品，只作 MODBUS 设备的主站。因此，接口上电后自动进入“接收/发送 re_tr=1”状态。

re_tr=0: 接口处在发送报文、等待接收状态。

(3)、MODBUS 异常应答码 M_ER_CODE

MODBUS 异常应答码：当接口发送一条 MODBUS 报文后，从机接收到的主机报文，没有传输错误，但从机无法正确执行主机命令或无法作出正确应答时，从机将以“异常应答”回答之。详见“附录 MODBUS 技术简介—3. 异常应答”中的介绍。

注意:整个 MODBUS 报文队列有多条 MODBUS 报文，而只有一个通信状态字。因此，当多条 MODBUS 出现异常应答时，通信状态字中的异常应答码是滚动的。

(4)、等待 M 回答到时 Tmdr_O

总线桥发出 MODBUS 报文后，按配置的“等待回答时间 Time of Replay”等待 MODBUS 设备回答，如果等待时间到时，Tmdr_O=1。MODBUS 扫描器转向发送下一条 MODBUS 报文。

(5)、CRC 校验错 CRC_er

CRC_er=1: 当接口接收到一条 MODBUS 回答报文，CRC 校验出现错误时，本产品认为 MODBUS 回答数据不可靠，废弃不用，不与 PROFINET 对应数据区交换。

(6)、奇偶校验错 oe_er

串口接收字符中发现字符奇偶校验错。此时，本产品认为 MODBUS 回答数据不可靠，废弃不用，不与 Ethernet/IP 对应数据区交换。

5.2.6 EIP-G-MOD2 模块在主站模式下的控制字

(1)、通信控制字格式

D7: reset_M	D6: escape_M	D5: clear_er	D4-D3	D2:M_w_en	D1:M_r_en	D0:start_M
强置 MODBUS 扫描复位	停止等待	清错误标记	不用	MODBUS 写允许	MODBUS 读允许	启动 MODBUS 扫描

(2)、启动 MODBUS 扫描 D0:start_M

启动 MODBUS 扫描，MODBUS 扫描器从当前 MODBUS 扫描器指针开始，发送对应 MODBUS 报文。

(3)、MODBUS 读允许 D1:M_r_en

只发送 MODBUS 报文队列中的读类命令：即 01H、02H、03H、04H 命令。

(4)、MODBUS 写允许 D2:M_w_en

只发送 MODBUS 报文队列中的写类命令：即 05H、06H、0FH、10H 命令。

以上三个控制位 (start_M、M_r_en、M_w_en) 配合使用，主站可以完成“先读（设备状态）→判断→再写（控制设备）等更复杂的功能。

表 3-1 三个控制位 (M_w_en、M_r_en、start_M) 控制功能

D2: M_w_en MODBUS 写允许	D1: M_r_en MODBUS 读允许	D0: start_M 启动 MODBUS 扫描	功能
X	X	0	停止 MODBUS 扫描
0	0	1	启动 MODBUS 扫描，发送所有 MODBUS 读\写命令
1	1	1	
0	1	1	启动 MODBUS 扫描，只发送 MODBUS 读命令
1	0	1	启动 MODBUS 扫描，只发送 MODBUS 写命令

(5)、清错误标记 D5:clear_er

clear_er=1: 总线桥清除通信状态字中错误标记位 D7~D1。

(6)、停止等待 D6:escape_M

escape_M=1: MODBUS 扫描器发出一条 MODBUS 报文后等待 MODBUS 设备回答。在此状态下，如果 escape_M=1，扫描器停止等待，继续扫描下一条 MODBUS 报文。该功能通常配合“等待回答时间 Time of Replay: 无限期等待回答 Waiting.....”的选择使用。

注意 1: 如果 escape_M 保持为 1，那么，下一条 MODBUS 报文发出后，没有等待，立刻转向发送再下一条 MODBUS 报文。因此，escape_M 应配合 start_M 使用。

如下指令系列所示：

↓

↓

MODBUS 扫描器处在无限期待回答中.....

start_M=0;

escape_M=1;

escape_M=0;

start_M=1;

MODBUS 扫描器停止等待，转向发送下一条 MODBUS 报文.....

↓

(7)、强置 MODBUS 扫描复位 D7:reset_M

reset_M=1: 强置 MODBUS 扫描器指针回到第一条 MODBUS 报文位置，MODBUS 扫描器处在复位状态。此时，启动 MODBUS 扫描 start_M 无效。

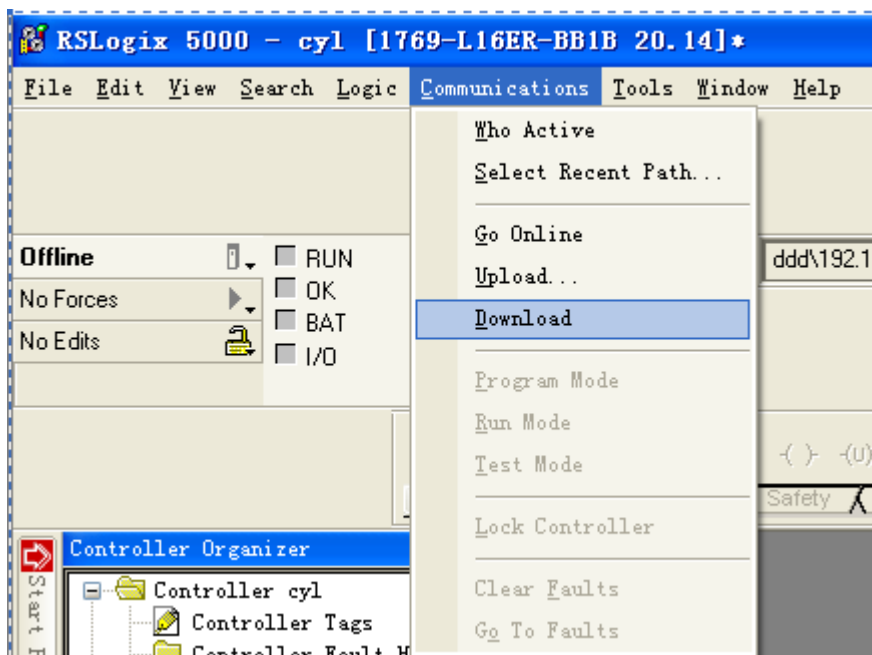
reset_M=0: “强置 MODBUS 扫描器复位” 无效。

注意 2: reset_M 与 escape_M 同时作用无效。

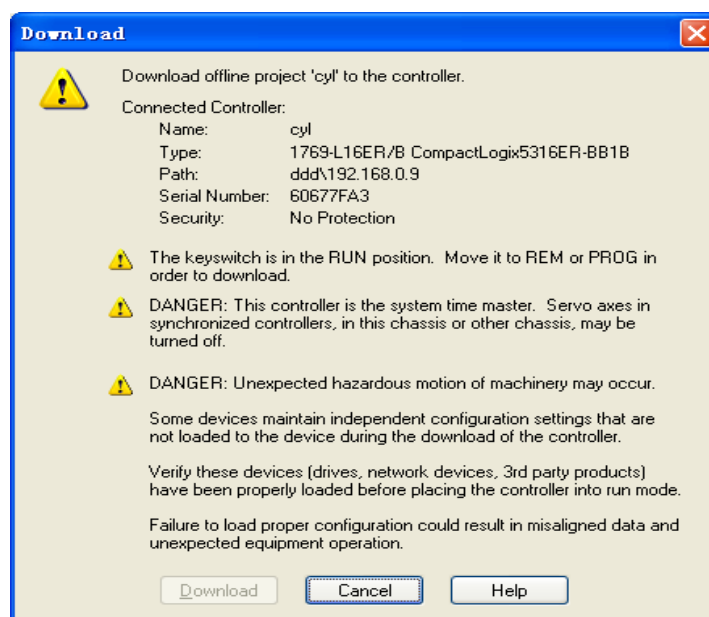
reset_M	escape_M	功能
0	0	无作用
0	1	停止等待
1	0	强置 MODBUS 扫描复位
1	1	无作用

5.2.7 RSLogix 工程的下载

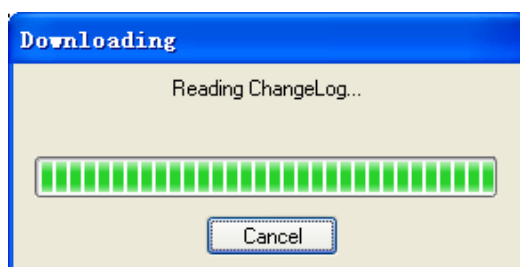
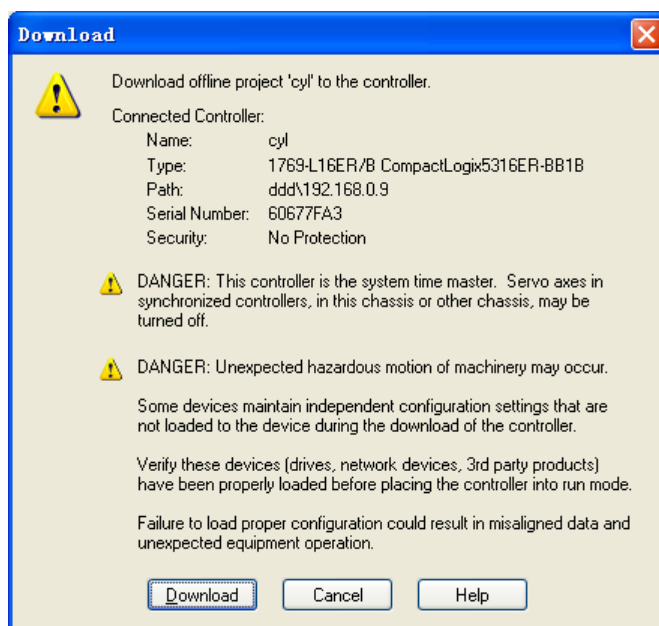
在菜单中选择 Communications→Download



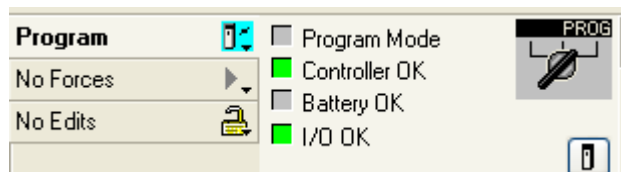
弹出如下对话框，



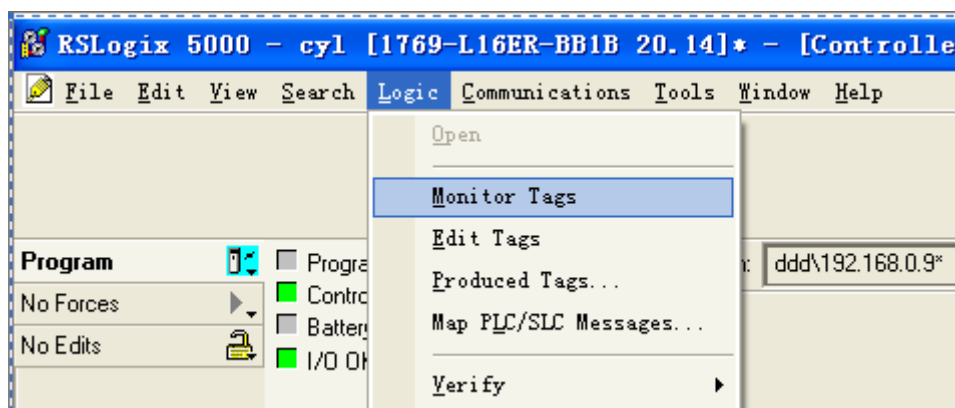
将 CPU 的拨码拨至 PROG 模式，点击 Download 将工程在下载控制器。



当下载成功后 RSLogix 软件自动与控制器在线，并显示 Controller OK, I/O OK，同时适配器的 NS 指示灯由闪烁变为绿色常亮，即表明控制器已于适配器通讯成功。



5.2.8 寄存器监视



启动 COM1 控制字：

Data[0]最低位置 1 启动通讯。

输出数据区监视：

+ Local:1:C	{...}	{...}	
- bb:0	{...}	{...}	
- bb:0.Data	{...}	{...}	Hex
+ bb:0.Data[0]		16#01	Hex
+ bb:0.Data[1]		16#00	Hex
+ bb:0.Data[2]		16#aa	Hex
+ bb:0.Data[3]		16#bb	Hex
+ bb:0.Data[4]		16#cc	Hex
+ bb:0.Data[5]		16#dd	Hex
+ bb:0.Data[6]		16#ee	Hex
+ bb:0.Data[7]		16#ff	Hex
+ bb:0.Data[8]		16#11	Hex
+ bb:0.Data[9]		16#22	Hex
+ bb:0.Data[10]		16#33	Hex
+ bb:0.Data[11]		16#44	Hex
+ bb:0.Data[12]		16#55	Hex
+ bb:0.Data[13]		16#66	Hex
+ bb:0.Data[14]		16#77	Hex
+ bb:0.Data[15]		16#88	Hex
+ bb:0.Data[16]	<input type="text" value="16#99"/>	16#99	Hex
+ bb:0.Data[17]		16#00	Hex
+ bb:0.Data[18]		16#00	Hex
+ bb:0.Data[19]		16#00	Hex

40001: <AABBH>	40011: <0000H>	40021: <0000H>
40002: <CCDDH>	40012: <0000H>	40022: <0000H>
40003: <EEFFH>	40013: <0000H>	40023: <0000H>
40004: <1122H>	40014: <0000H>	40024: <0000H>
40005: <3344H>	40015: <0000H>	40025: <0000H>
40006: <5566H>	40016: <0000H>	40026: <0000H>
40007: <7788H>	40017: <0000H>	40027: <0000H>
40008: <9900H>	40018: <0000H>	40028: <0000H>
40009: <0000H>	40019: <0000H>	40029: <0000H>
40010: <0000H>	40020: <0000H>	40030: <0000H>

输入数据监视区:

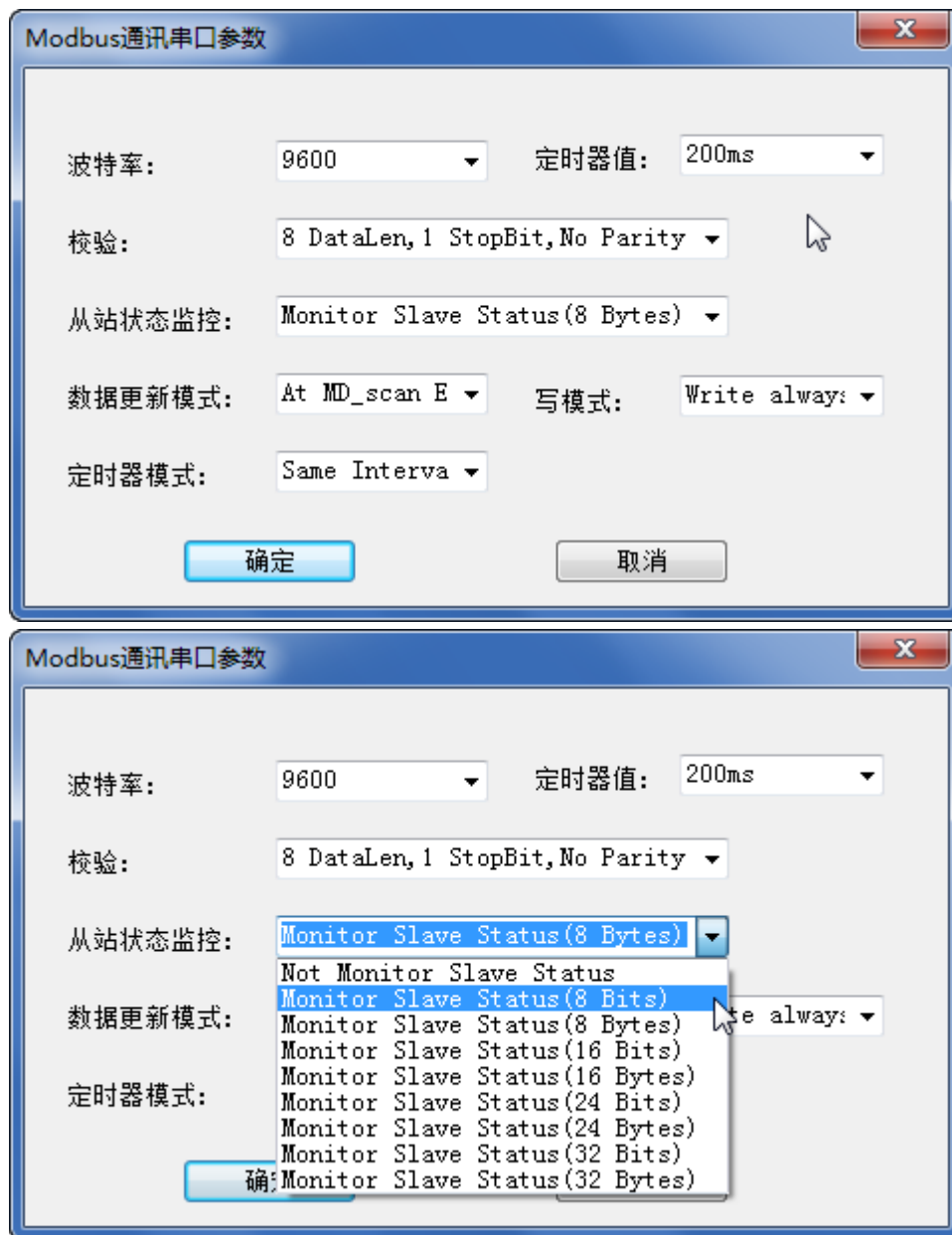
bb:l.Data	(...)	(...)	Hex	SINT[22]
+ bb:l.Data[0]	16#01		Hex	SINT
+ bb:l.Data[1]	16#00		Hex	SINT
+ bb:l.Data[2]	16#55		Hex	SINT
+ bb:l.Data[3]	16#55		Hex	SINT
+ bb:l.Data[4]	16#33		Hex	SINT
+ bb:l.Data[5]	16#33		Hex	SINT
+ bb:l.Data[6]	16#44		Hex	SINT
+ bb:l.Data[7]	16#44		Hex	SINT
+ bb:l.Data[8]	16#aa		Hex	SINT
+ bb:l.Data[9]	16#aa		Hex	SINT
+ bb:l.Data[10]	16#bb		Hex	SINT
+ bb:l.Data[11]	16#bb		Hex	SINT
+ bb:l.Data[12]	16#cc		Hex	SINT
+ bb:l.Data[13]	16#cc		Hex	SINT
+ bb:l.Data[14]	16#dd		Hex	SINT
+ bb:l.Data[15]	16#dd		Hex	SINT
+ bb:l.Data[16]	16#ee		Hex	SINT
+ bb:l.Data[17]	16#ee		Hex	SINT
+ bb:l.Data[18]	16#ff		Hex	SINT
+ bb:l.Data[19]	16#ff		Hex	SINT
+ bb:l.Data[20]	16#77		Hex	SINT
+ bb:l.Data[21]	16#88		Hex	SINT

30001: <5555H>	30011: <0000H>	30021: <0000H>
30002: <3333H>	30012: <0000H>	30022: <0000H>
30003: <4444H>	30013: <0000H>	30023: <0000H>
30004: <AAAAH>	30014: <0000H>	30024: <0000H>
30005: <BBBBH>	30015: <0000H>	30025: <0000H>
30006: <CCCCH>	30016: <0000H>	30026: <0000H>
30007: <DDDDH>	30017: <0000H>	30027: <0000H>
30008: <EEEEH>	30018: <0000H>	30028: <0000H>
30009: <FFFFH>	30019: <0000H>	30029: <0000H>
30010: <7788H>	30020: <0000H>	30030: <0000H>

5.2.9 MODBUS 从站状态监测

启用 MODBUS 从站状态监测功能，需要在软件 EipModConf 中启用配置。

双击 EIP-G-MOD2 图标中的最左侧槽位（COM1），弹出总线配置对话框如下图：



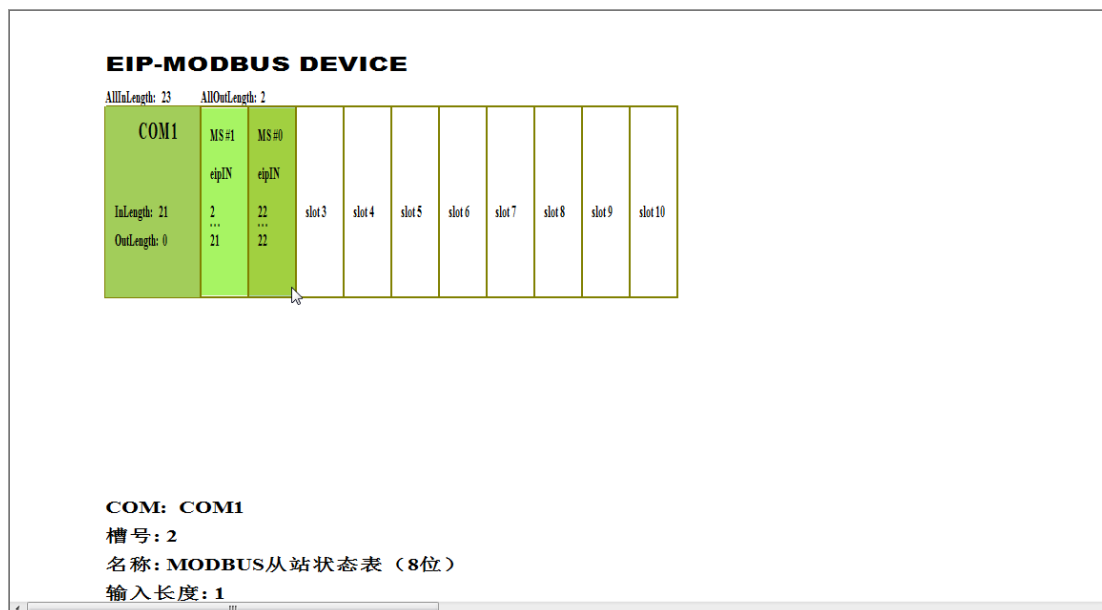
在从站状态监控一栏，点开下拉菜单，根据从站数量及监测需求进行选择，支持从站数量最多为 32 个。

选择 Monitor Slave Status(8 Bits)，最多支持监测 8 个从站，每个从站仅显示通信状态，0 表示未通信，1 表示通信。

选择 Monitor Slave Status(8 Bytes)，最多支持监测 8 个从站，每个从站的通信状态字节：

D7: oe_er	D6: CRC_er	D5	D4~D1: M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	MM 等待回答超时

以选择 Monitor Slave Status(8 Bits)为例，点击确定之后，点击编译 ，后看到



注意：在使用从站状态监测功能时，需要预留出一个卡槽位置
注意：配置完从站状态监测功能后，一定要编译

在 2 号插槽添加进了 MODBUS 从站状态表（8 位）。双击此插槽，



里面是 8 个 MODBUS 从站的站地址，可以手动进行编辑。

配置完成后，按照前述教程，将配置下载到 EIP-G-MOD2 模块，并修改 PLC 中输入输出总字节数，完成 PLC 工程的配置。

完成之后，就可以通过监测相应的输入来查看 MODBUS 从站的状态。

5.3 /Ethernet/IP 侧 IP 地址设置

EIP-G-MOD2 的第一位拨码开关 bit1 拨到 on 位置时，网关的缺省 IP 为 192.168.0.99。本例在此 IP 地址基础上进行修改。

操作步骤如下：

- 1、打开 BOOTP/Server 软件

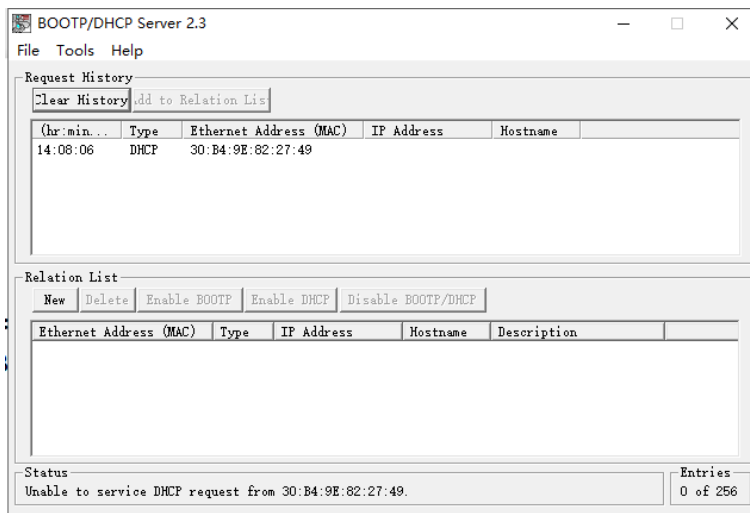


图 1、打开软件

- 2、设置子网掩码(subnet mask)

将子网掩码设置为 255.255.255.0，其他缺省为 0

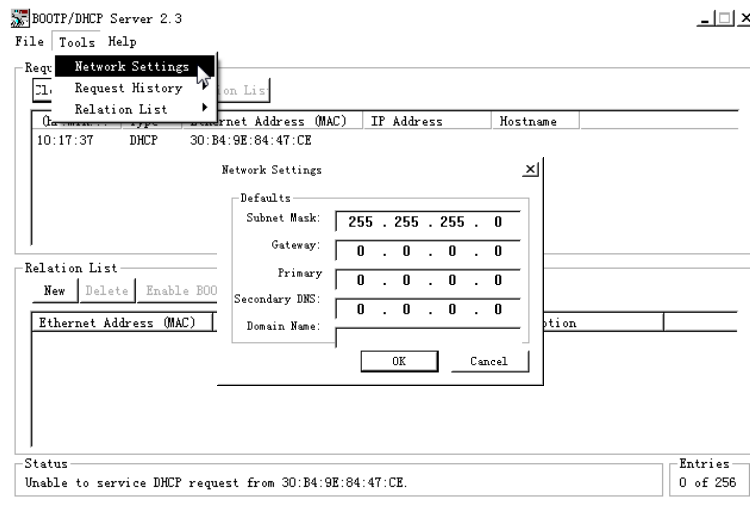


图 2、设置子网掩码

3、新建连接输入网关当前 MAC 地址和 IP 地址

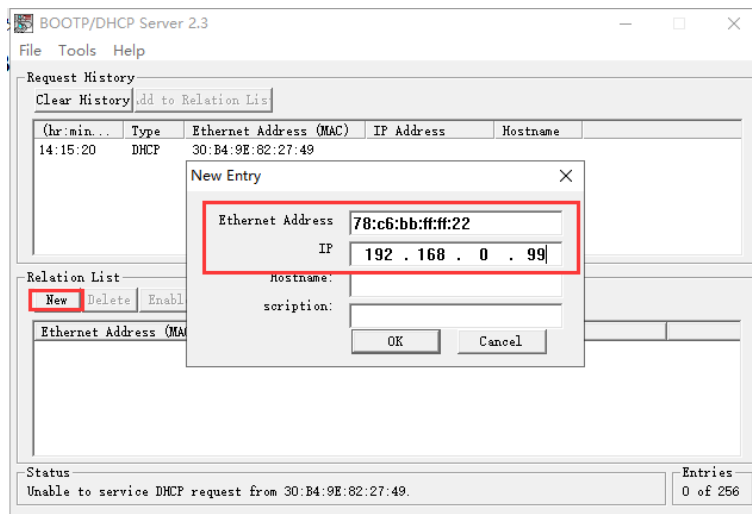


图 3、新建通道输入 mac 地址和 IP 地址

4、使能 DHCP

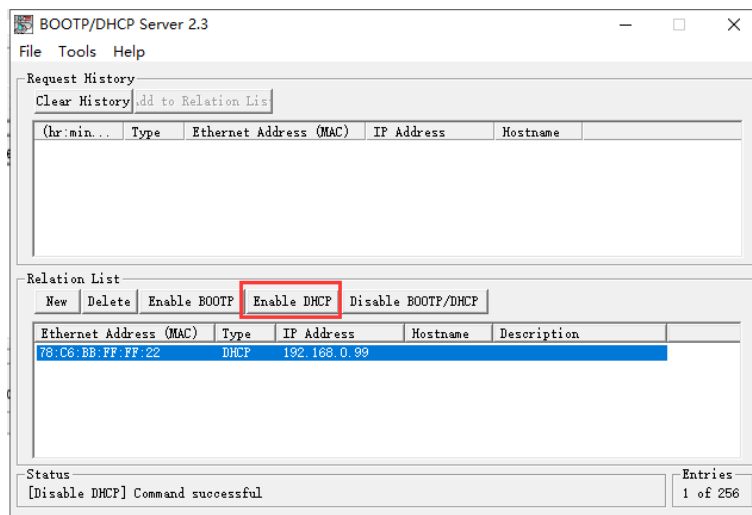


图 4、点击使能 DHCP

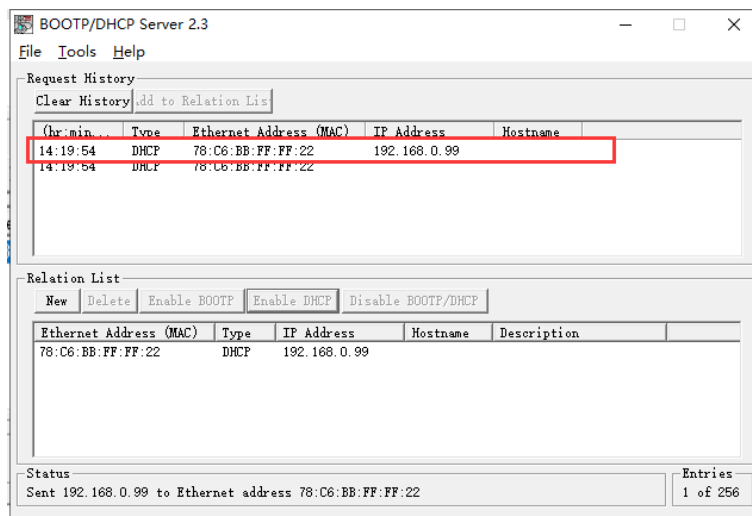


图 5、使能 DHCP

5、删除连接

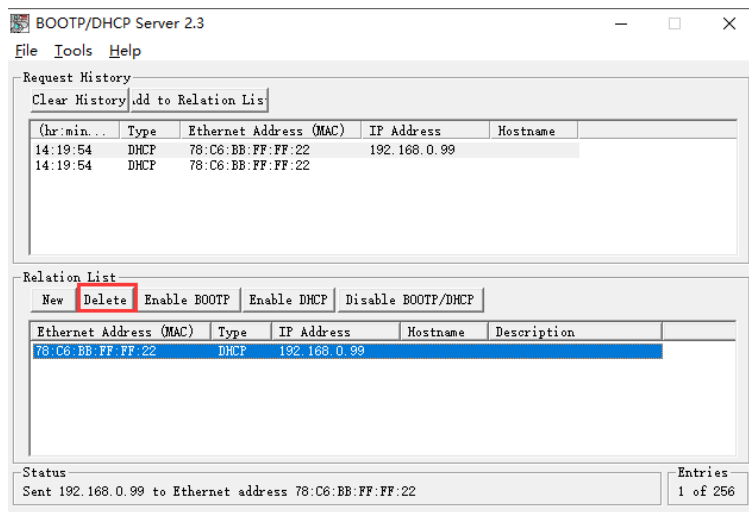


图 6、删除连接

6、修改 IP 地址

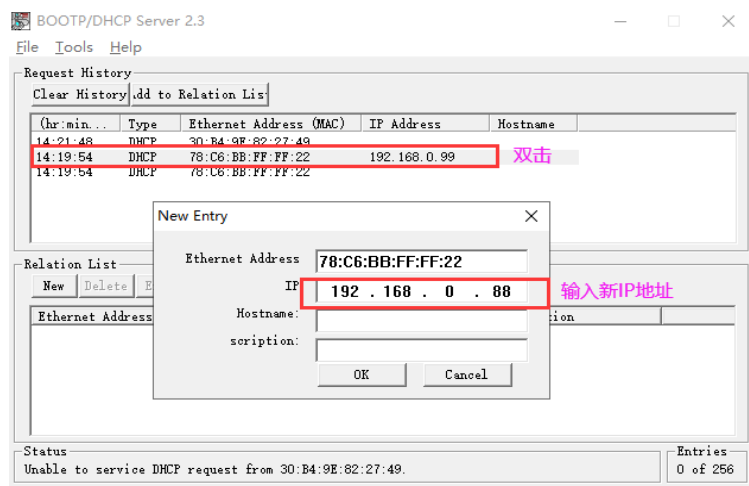


图 7、输入新 IP 地址

7、网关重新上电

将第一位拨码开关 bit1 拨到 off，给网关重新上电后，新 IP 地址生效。

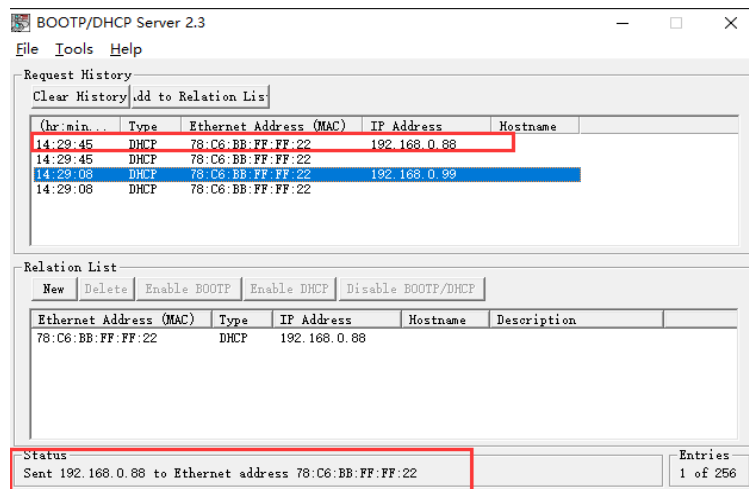


图 8、IP 地址修改成功

8、保存修改后的 IP 地址

点击 Disable BOOTP/DHCP 按钮，关闭 DHCP 功能，IP 地址固定下来。

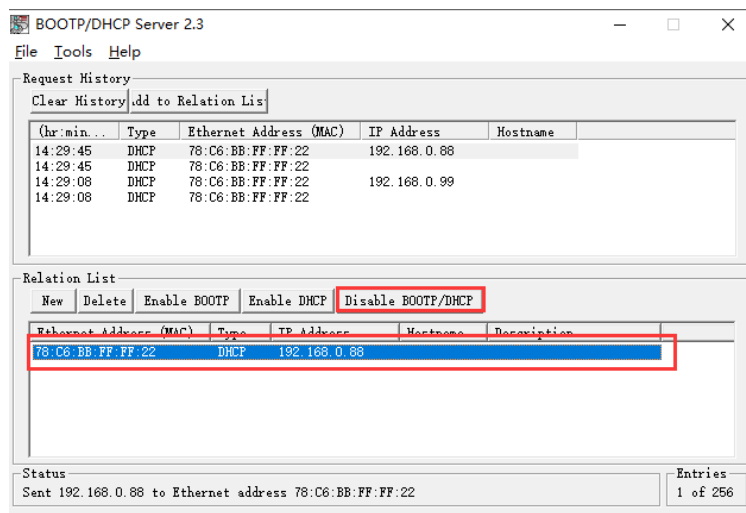


图 9、 Disable BOOTP/DHCP

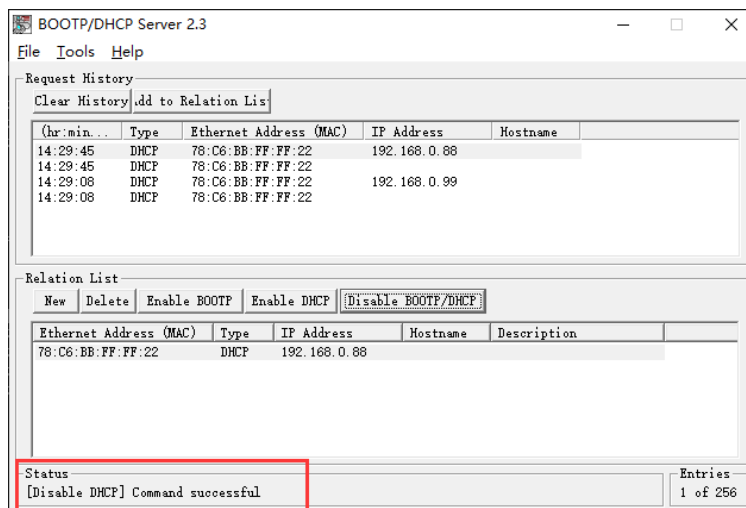


图 10、通过状态栏查看 Disable DHCP 命令成功

6.2 MODBUS 协议要点

(1) MODBUS 是主/从通信协议。主站主动发送报文，只有与主站发送报文中呼叫地址相同的从站才向主站发送回答报文。

(2) 报文以 0 地址发送时为广播模式，无需从站应答，可作为广播报文发送，包括：

- 修改线圈状态；
- 修改寄存器内容；
- 强置多线圈；
- 预置多寄存器；
- 询问诊断；

(3) MODBUS 规定了 2 种字符传输模式：ASCII 模式、RTU（二进制）模式；两种传输模式不能混用；

※ 本产品 PB-B-MODBUS 只能用于 RTU 模式。

特性	RTU 模式	ASCII 模式
编码	二进制	ASCII（打印字符：0-9, a-z, A-Z）
每个字符位数	起始位:1 BIT	起始位:1 BIT
	数据位:8 BITS	数据位:7 BITS
	奇偶校验位(可选):1 位	奇偶校验位(可选):1 位
	停止位:1 或 2	停止位:1 或 2
报文校验	CRC(循环冗余校验)	LRC(纵向冗余校验)

(4) 传输错误校验

→传输错误校验由奇偶校验、冗余校验检验。

→当校验出错时，报文处理停止，从机不再继续通信，不对此报文产生应答；

→通信错误一旦发生，报文便被视为不可靠；MODBUS 主机在一定时间过后仍未收到从站应答，即作出“通信错误已发生”的判断。

(5) 报文级（字符级）采用 CRC-16（循环冗余错误校验）

(6) MODBUS 报文 RTU 格式

小于 3.5 个字符的 报文间隔时间	地址	功能码	数据	CRC 校验	小于 3.5 个字符的 报文间隔时间
	1*byte	1*byte	N*bytes	2*bytes	

6.3 异常应答

(1) 从机接收到的主机报文，没有传输错误，但从机无法正确执行主机命令或无法作出正确应答，从机将以“异常应答”回答之。

(2) 异常应答报文格式

例：主机发请求报文，功能码 01：读 1 个 04A1 线圈值

从机地址	功能码	高位起始地址	低位起始地址	线圈数高位	线圈数低位	CRC
0A	01	04	A1	00	01	XXXX

由于从机最高线圈地址为 0400，则 04A1 超地址上限，从机作出异常应答如下（注意：功能码最高位置 1）：

从机地址	功能码	异常码	CRC
0A	81	02	XXXX

(3) 异常应答码

异常码	名称	说明
01	非法功能	所收到的报文功能对于被编址从机是不允许执行的。若有询问命令发出，则本码表示在此之前无编程功能。
02	非法数据地址	数据字段中的地址对于被编址的从机是禁止的。
03	非法数据	数据字段中的值对于被编址的从机是禁止的。
04	相关设备故障	从机 PC 不能对报文或异常终止错误作出应答（见注 1）。
05	确认	从机 PC 已接受并正在处理长程序任务。应发出“探询”报文。查询该程序何时完成。若尚未完成，PC 会对“探询”报文发出否定应答（见注 2）。
06	忙碌、拒绝执行	收到报文无误，但 PC 已受约执行长程序命令。要求以后等 PC 有空时再传送。
07	否定	刚发送的编程功能无法执行，应发布“探询”报文以取得详细的设备错误信息。本码只对功能 13/14 有效（见注 2）。
08	存储器奇偶校验错误	扩展存储器的读数对正被访问的存储器数位进行检查。应在错误不会重复发生时进行复验。若所有复验均失败，应维修。
注 1：对功能码 1—19，异常码 04 可表示：在应答设备发生不可校正的错误之前，只执行了有关询问报文的一部分。异常功能码 04 要求立即发布管理通告。		
注 2：只是在功能码 18 发生设备错误信息时，884 才支持异常功能码 05 和 06。至于异常码 05、06 和 07 之后发生的应答，可参阅具体设备手册的附录 A		

6.4 MODBUS 存储区

MODBUS 涉及到的控制器（或 MODBUS 设备）存储区以 0XXXX、1XXXX、3XXXX、4XXXX 标识；

存储区标识	名称	类型	读/写	存储单元地址
0XXXX	线圈	位	读/写	00001~0XXXX, XXXX: 与设备有关
1XXXX	输入线圈	位	只读	10001~1XXXX, XXXX: 与设备有关
3XXXX	输入寄存器	字	只读	30001~3XXXX, XXXX: 与设备有关
4XXXX	保持/输出寄存器	字	读/写	40001~4XXXX, XXXX: 与设备有关

6.5 MODBUS 功能码

即 MODBUS 应用层，规定了 MODBUS 报文格式和服务功能。

读取输出状态

功能码：01H

主站询问报文格式：

地址	功能码	起始地址	起始地址	线圈数 高位	线圈数 低位	CRC
11	01	00	13 (19)	00	25	XXXX

功能：读从站输出线圈 0XXXX 状态。

注意：报文中线圈起始地址 00000 对应设备中 00001 地址，其他顺延。

本例：读 11H 号从站输出线圈，起始地址=0013H=19，对应地址 00020；线圈数=0025H=37；
末地址=00020+37-1=00056；

因此，本询问报文功能是：读 17 (11H) 号从站输出线圈 00020—00056，共 37 个线圈状态；

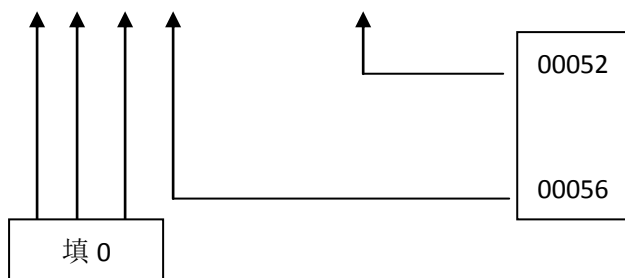
从站应答格式:

地址	功能码	字节计数	线圈状态 20-27	线圈状态 28-35	线圈状态 36-43	线圈状态 44-51	线圈状态 52-56	CRC
11	01	05	CD	6B	B2	0E	1B	XXXX

功能: 从机返回输出线圈 0 XXXX 状态

本例: CD=11001101, 对应 00020-00027;

1B=0 0 0 1 1 0 1 1, 对应 00052-00056;



读取输入状态

功能码: 02H

主站询问报文格式:

地址	功能码	起始地址 高位	起始地址 低位	线圈数 高位	线圈数 低位	CRC
11	02	00	C4	00	16	XXXX

功能: 读从站输入线圈 1XXXX 状态。

注意: 报文中线圈起始地址 00000 对应设备中 10001 地址, 其他顺延。

本例: 读 11H 号从站输入线圈, 起始地址=00C4H=196, 对应地址 10197; 线圈数=0016H=22, 末地址=10197+22-1=10218;

因此, 本询问报文功能是: 读 17 (11H) 号从站输入线圈 10197—10218, 共 22 个输入线圈状态;

从站应答格式:

地址	功能码	字节计数	DI 10197-10204	DI 10205-10212	DI 10213-10218	CRC
11	02	03	AC	DB	35	XXXX

功能: 从机返回 DI=1XXXX 状态

读取保存寄存器

功能码：03H

主站询问报文格式：

地址	功能码	寄存器起始 地址高位	寄存器起始 地址低位	寄存器数 高位	寄存器数 低位	CRC
11	03	00	6B(107)	00	03	XXXX

功能：读从站保持寄存器 4XXXX 值。

注意：报文中寄存器起始地址 00000 对应设备中 40001 地址,其他顺延。

本例：读 11H 号从站保持寄存器值，起始地址=006BH=107，对应地址 40108；寄存器数=0003；

末地址=40108+3-1=40110；

因此，本询问报文功能是：读 17（11H）号从站 3 个保持寄存器 40108—40110 的值；

从站应答格式：

地址	功能码	字节 计数	寄存器 40108 高位	寄存器 40108 低位	寄存器 40109 高位	寄存器 40109 低位	寄存器 40110 高位	寄存器 40110 低位	CRC
11	03	06	02	2B	01	06	2A	64	XXXX

功能：从站返回保持寄存器 40108—40110 的值；(40108)=022BH，(40109)=0106H，

(40110)=2A64H

读取输入寄存器

功能码：04H

主站询问报文格式：

地址	功能码	寄存器起始地址高位	寄存器起始地址低位	寄存器数高位	寄存器数低位	CRC
11	04	00	08	00	01	XXXX

功能：读从站输入寄存器 3XXXX 值。

注意：报文中寄存器起始地址 00000 对应设备中 30001 地址，其他顺延。

本例：读 11H 号从站输入寄存器值，起始地=0008H=0008，对应地址 30009；寄存器数=0001；末地址=30009；因此，本询问报文功能：读 17（11H）号从站 1 个保持寄存器 30009 的值；从站应答格式：

地址	功能码	字节计数	输入寄存器高位	输入寄存器低位	CRC
11	04	02	01	01	XXXX

功能：从站返回输入寄存器 30009 的值；（30009）=0101H

强置单线圈

功能码：05H

询问格式：

地址	功能码	线圈地址	线圈地址	断通标志	断通标志	CRC
11	05	00	AC（172）	FF	00	XXXX

功能：强置 17 号从站线圈 0XXXX 值。报文中线圈起始地址 00000 对应设备中 00001 地址，其它顺延。

断通标志=FF00，置线圈 ON。

断通标志=0000，置线圈 OFF。

例：起始地址=00AC(H)=172，对应设备中的地址为 00173。强置 17 号从站线圈 0173 为 ON 状态。

应答格式：原文返回

地址	功能码	线圈地址	线圈地址	断通标志	断通标志	CRC
11	05	00	AC（172）	FF	00	XXXX

功能：强置 17 号从机线圈 0173 ON 后原文返回

预置单保持寄存器

功能码：06H

询问格式：

地址	功能码	寄存器地址	寄存器地址	数据值 高位	数据值 低位	CRC
11	06	00	87 (135)	03	9E	XXXX

功能：预置单保持寄存器 4XXXX 值。报文中线圈起始地址 00000 对应设备中 40001 地址，其它顺延。

例：预置 17 号从机单保持寄存器 40136 值=0x039E；

应答格式：原文返回

地址	功能码	寄存器地址	寄存器地址	数据值 高位	数据值 低位	CRC
11	06	00	87	03	9E	XXXX

功能：预置 17 号从机单保持寄存器 40136 值=0x039E 后原文返回。

读取异常状态

功能码：07H

本产品 PB-B-MODBUS 暂不支持这一功能。

回送校验

功能码：08H

本产品 EIP-G-MOD2 暂不支持这一功能。

读取通信事件计数器

功能码：0BH

本产品 EIP-G-MOD2 暂不支持这一功能。

读取通信事件计数器

功能码：0CH

本产品 PB-B-MODBUS 暂不支持这一功能。

强置多线圈

功能码：0FH

主站询问报文格式：

地址	功能码	线圈起始 地址高位	线圈起始 地址低位	线圈数 高位	线圈数 低位	字节 计数	线圈状态 20-27	线圈状态 28-29	CRC
11	0F	00	13	00	0A	02	CD	00	XXXX

功能：将多个连续线圈 0XXXX 强置为 ON/OFF 状态。

注意：报文中线圈起始地址 00000 对应设备中 00001 地址，其他顺延。

本例：强置 11H 号从站多个连续线圈，线圈起始地址=0013H=19，对应地址 00020；线圈数=000AH=10；末地址=00020+10-1=00029；

因此，本询问报文功能是：强置 17（11H）号从站 10 个线圈 00020—00029 的值； CDH→00020-00027; 00H→00028-00029；

从站应答格式：

地址	功能码	线圈起始 地址高位	线圈起始 地址低位	线圈数 高位	线圈数 低位	CRC
11	0F	00	13	00	0A	XXXX

预置多寄存器

功能码：10H

主站询问报文格式：

地址	功能码	起始寄存器地址高位	起始寄存器地址低位	寄存器数高位	寄存器数低位	字节计数	数据高位	数据低位	数据高位	数据低位	CRC
11	10	00	87	00	02	04	01	05	0A	10	XXXX

功能：预置从站多个保持寄存器值 4XXXX。

注意：报文中保持寄存器起始地址 40000 对应设备中 40001 地址，其他顺延。

本例：预置 11H 号从站多个保持寄存器值，寄存器起始地址=0087H=135，对应地址 40136，线圈数=0002H=2，末地址=40135+2-1=40137；

因此，本询问报文功能是：预置 17（11H）号从站 2 个保持寄存器值；0105H→40136; 0A10H→40137.

应答格式：

地址	功能码	起始寄存器地址高位	起始寄存器地址低位	寄存器数高位	寄存器数低位	CRC
11	10	00	87	00	02	XXXX

第七章 有毒有害物质表

根据中国《电子信息产品污染控制管理办法》的要求出台

部件名称	有毒有害物质和元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
塑料外壳	0	0	0	0	0	0
电路板	X	0	0	0	0	0
铜螺柱	0	0	0	0	0	0
贴膜	0	0	0	0	0	0
插座/插头	X	0	0	0	0	0
拨码开关	X	0	0	0	0	0

0: 表示在此部件所用的所有同类材料中, 所含的此有毒或有害物质均低于 SJ/T1163-2006 的限制要求;

X: 表示在此部件所用的所有同类材料中, 至少一种所含的此有毒或有害物质高于 SJ/T1163-2006 的限制要求。

注明: 引用的“环保使用期限”是根据在正常温度和湿度条件下操作使用产品而确定的。

现场总线 PROFIBUS (中国) 技术资格中心
北京鼎实创新科技有限公司

电话: 010-82078264、010-62054940

地址: 北京德胜门外教场口 1 号, 5 号楼 A-1 室

Web: www.c-profibus.com.cn

传真: 010-82285084

邮编: 100120

Email: tangjy@c-profibus.com.cn