

BT-EN-SEMB2-S



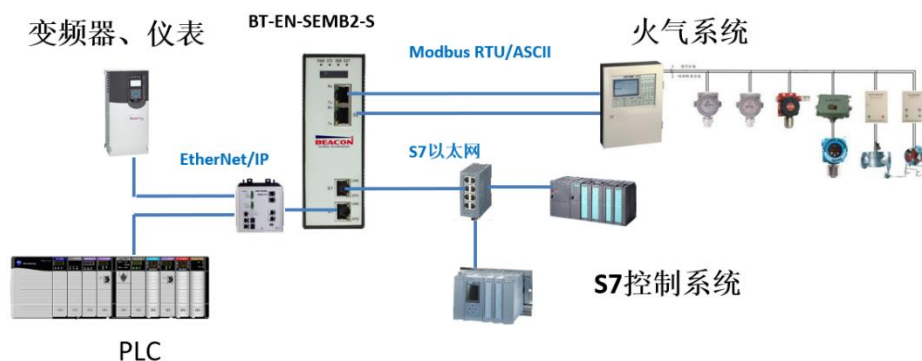
BEACON GLOBAL TECHNOLOGY

目录

BT-EN-SEMB2-S 简介:	2
模块初始配置.....	3
配置模块做 EtherNet/IP Server	5
配置模块做 EtherNet/IP Client	11
配置模块做 Siemens S7 以太网主站.....	17
配置模块做 MODBUS RTU 主站.....	26
Modbus 命令使能控制介绍.....	34
配置模块做 MODBUS RTU 从站.....	36
Modbus RTU 诊断方式.....	40
举例 1. 罗克韦尔 PLC 和西门子 PLC 同时采集 Modbus RUT 从站数据	41
举例 2. 罗克韦尔 PLC 采集 Modbus RUT 从站数据	46
举例 3 罗克韦尔 1756PLC 和西门子 PLC 315-2DP/PN 通讯	47
举例 4. 罗克韦尔 1756PLC 和西门子 PLC 315-2DP/PN 通讯	52
附录 1. 模块支持读写西门子 PLC 的数据类型	54
附录 2. 模块支持读写西门子 PLC 的数据范围	58
联系我们.....	63

BT-EN-SEMB2-S 简介:

- ◆ 模块支持EtherNet/IP协议转换S7以太网协议和Modbus RTU协议通讯。
- ◆ 模块最大支持10000个字数据交换区。
- ◆ EtherNet/IP协议可支持通讯的典型设备主要有罗克韦尔1756系列、1769系列、1746系列、PLC-2系列、PLC-5系列、SLC500系列、Micrologix 系列PLC。以及PowerFlex系列变频器，E300智能马达保护器，PowerMonitor智能电力监控仪，上位机RSView SE软件等。
- ◆ S7以太网协议可支持通讯的典型设备为各类西门子PLC，包括S7-200，S7-300，S7-400，S7-1200，S7-1500，
- ◆ Modbus RTU协议可支持通讯的设备包括各种数显仪表，电动阀门，传感器等。
- ◆ EtherNet/IP与S7以太网协议设备可在相同网段或者不同网段进行通讯。
- ◆ EtherNet/IP与S7以太网协议在同一个网段时，可选择模块上任意一个以太网接口和交换机连接（注意：不能同时把模块E1和E2接口设置成相同的网段），再把同一网段下两种协议的设备同时也接入交换机。
- ◆ EtherNet/IP与S7以太网协议设备如果在不同网段通讯时，需要选用模块的两个以太网口进行通讯，可把模块E1和E2设置成不同的网段，两种协议的设备分别接入E1和E2口即可。
- ◆ 模块有两个以太网口，两个串口，可以任意使用。



E1 端口 == 可选择配置为 EtherNet/IP 主站、从站或者 S7 以太网主站、从站。

E2 端口 == 可选择配置为 EtherNet/IP 主站、从站或者 S7 以太网主站、从站。

S1 端口 == 可选择配置为 Modbus RTU 主站/从站。

S2 端口 == 可选择配置为 Modbus RTU 主站/从站。

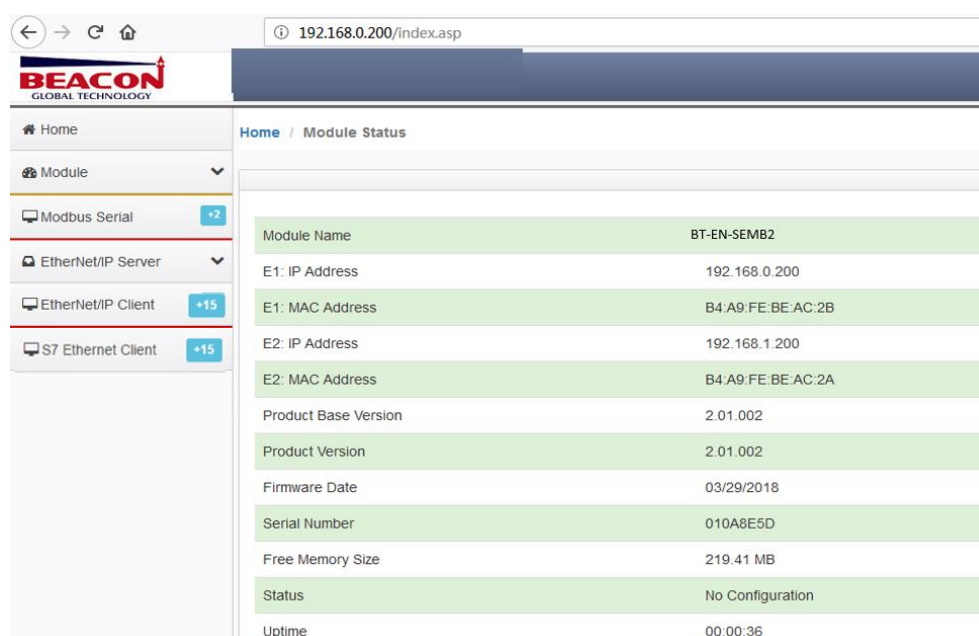
模块初始配置

E1 以太网接口出厂 IP 地址为 192.168.0.200。模块上电后，OLED 显示屏上会滚动显示 IP 地址。

BT系列模块全部采用网页配置形式组态，无需安装其他多余的组态软件，推荐采用如下浏览器及以上版本（更好的支持HTML5的功能）对于模块进行配置：IE10，GOOGLE Chrome 35，FIREFOX 35，Safari 7 及以上的版本。

通过以太网配置模块：

1. 把本地电脑的IP地址与所连接的模块端口配置成相同的IP网段，例如本案例采用E1接口进行配置，本地电脑配置成192.168.0.177，然后在GOOGLE Chrome浏览器的地址框里面输入192.168.0.200，点击回车键后，进入到模块的配置页面如下图。



2. 在配置页面的导航条内，点击Login，将打开如图所示。



3. 按照界面提示，输入用户名和密码进入模块配置。

用户名 (Username): admin

密码 (Password): admin

点击登录 (Sign In)

请注意：如果不登录，只能浏览配置，无法进行配置修改。

The screenshot shows the Beacon web interface. At the top, there is a 'Sign In' box with fields for 'Username' (containing 'admin') and 'Password', and a 'Sign In' button with a 'Remember me' checkbox. Below this, a sidebar menu on the left lists options: Home, Module, General Configuration, Internal Data View, Backup / Restore (highlighted), Change Password, Firmware Upgrade, Set Date & Time, and Reboot Module. The main content area is titled 'Home / Backup And Restore' and contains two sections: 'Upload configuration file to client' with an 'Export Config' button, and 'Download configuration file to Module' with a '选择文件' (Select File) button and the text '未选择任何文件' (No file selected).

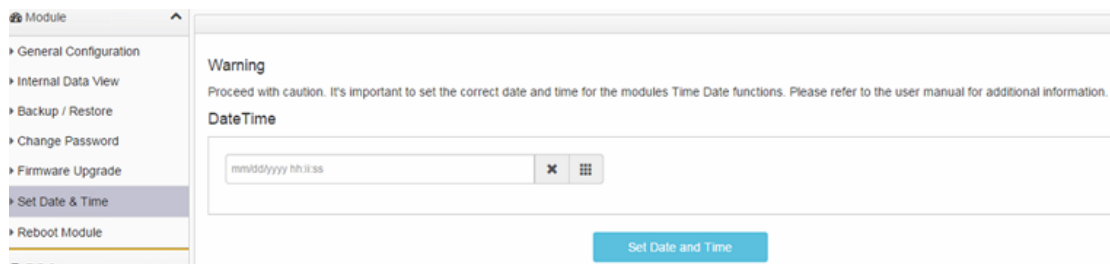
4. 登录后看到导出配置文件 **Export Config** 和恢复配置文件 **选择文件** 未选择任何文件
5. 查看模块 IP 地址，点击 **General Configuration**，修改模块的 IP 地址。

The screenshot shows the 'General Configuration' page for a module. The sidebar menu on the left has 'General Configuration' highlighted. The main content area shows the following fields: 'Module Name' (BT-EN-AC2), 'Comment' (empty), 'Ethernet Port 1' (header), 'IP Address' (192.168.0.200), 'Subnet Mask' (255.255.255.0), and 'Default Gateway' (192.168.0.1).

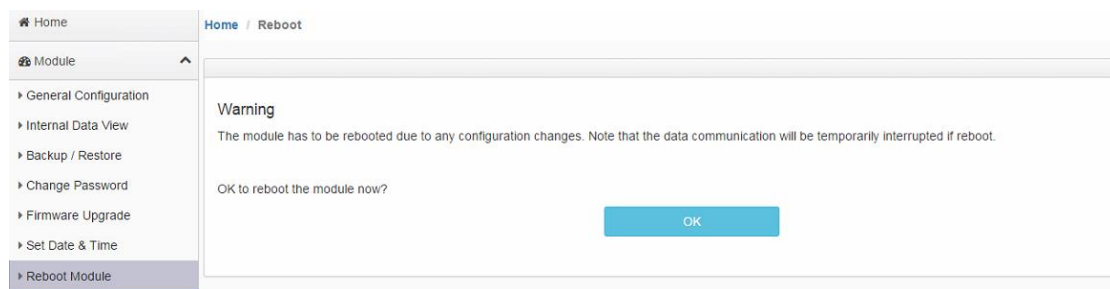
6. 点击修改密码，可以修改模块的登录密码。 **Change Password**

The screenshot shows the 'Change Password' page. The sidebar menu on the left has 'Change Password' highlighted. The main content area shows the following fields: 'User Name: admin', 'Current Password', 'New Password', and 'Confirm Password', followed by a 'Save' button.

7. 点击 **Set Date & Time** 可以设置模块的日期和时间。

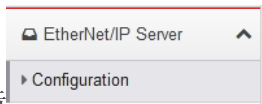


8. 点击 **Reboot Module** 表示重启模块。（不是复位）

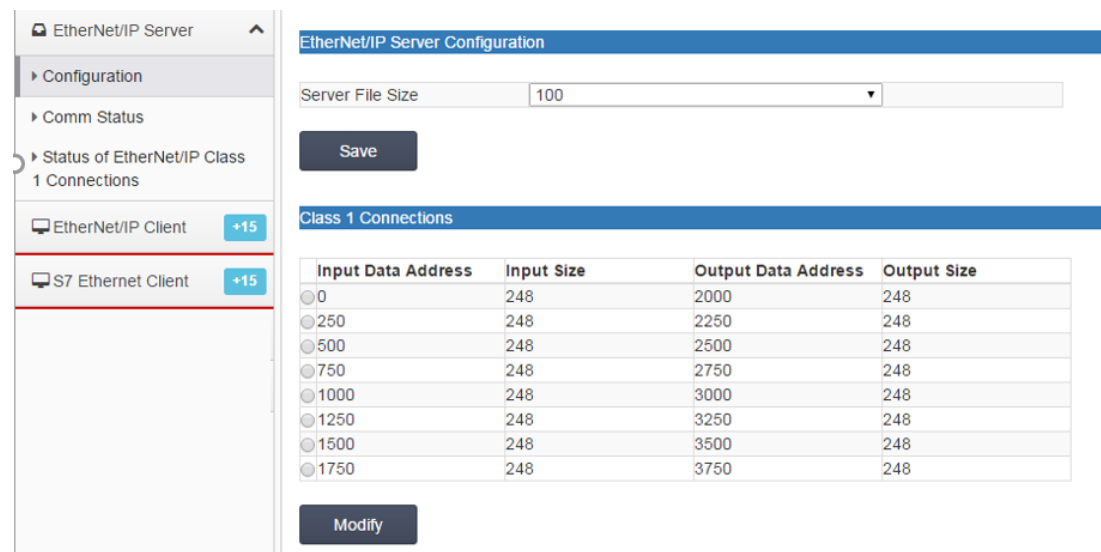


配置模块做 EtherNet/IP Server

这是模块通过以太网和罗克韦尔 PLC 通讯的最主要方式，本章内容关键在于搞清楚内部数据区和 CIP 标签组的对应关系。通过浏览器，进入模块主页面。



在左侧菜单中，点击 **Configuration**，查看 EtherNet/IP Server Configuration 的链接数，不同型号的模块的 EtherNet/IP Server Configuration 链接数不同。可以看到当前模块有多组 Class 1 Connections 的链接，这多组 Class 1 Connections 的链接可以在 Logix5000 软件里进行配置全部采用或者根据需要部分采用，每组 Class 1 Connections 提供 248 个 INT 数据类型的输入和 248 个 INT 数据类型的输出。



模块做为 EtherNet/IP Server时候，可以被多个罗克韦尔PLC 同时访问。**注意，不同型号模块可使用的内部寄存器数量不同，本节内容中举例只使用了 4 组 CIP 链接，在配置模块时请根据实际情况选择模块内部数据区。**

使用了 4 组 CIP 链接时的数据对应关系：

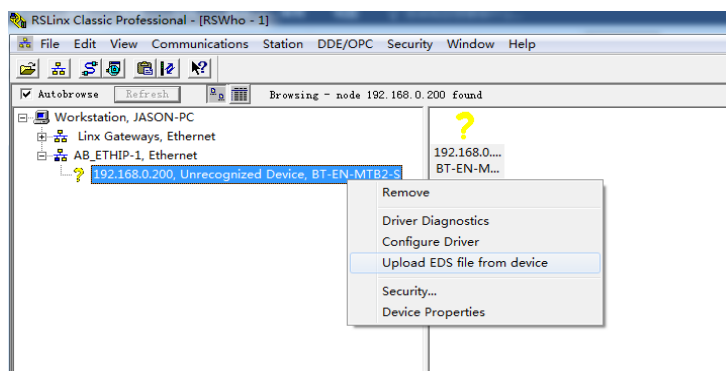
Input Data Address 表示罗克韦尔 PLC 采集模块数据（对 PLC 一侧为输入）的内部寄存器地址范围，0 是指模块内部第 0 个寄存器，输入起始地址为 0，数量 248，表示模块对 PLC 的第一组输入数据，所占用的模块内部寄存器地址范围。

Output Data Address 表示罗克韦尔 PLC 写给模块数据（对 PLC 一侧为输出）的内部寄存器地址范围，1000 是指模块内部第 1000 个寄存器，输出起始地址为 1000，数量 248，表示 PLC 对模块的第一组输出数据，所占用的模块内部寄存器地址范围。

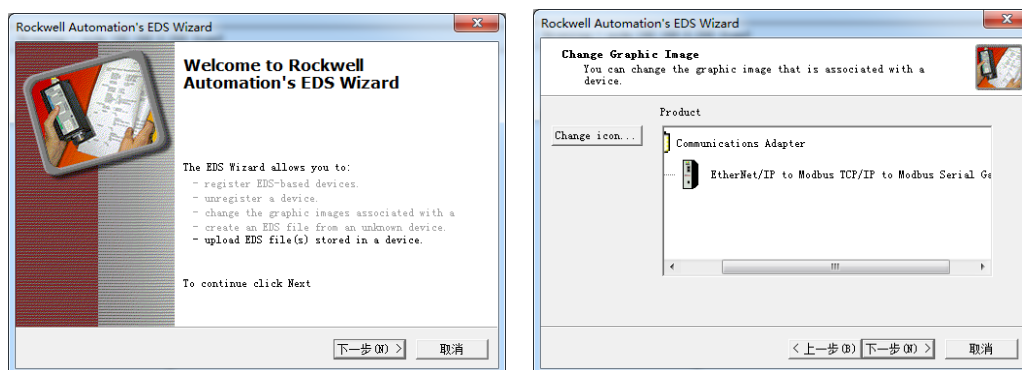
此处 248 个输入寄存器的数量要与 Logix5000 里面的 Class 1 Connections 对应。并且输入输出的起始位置和数量可以任意更改。注：模块默认做 EtherNet/IP 从站，不需要任何设置。

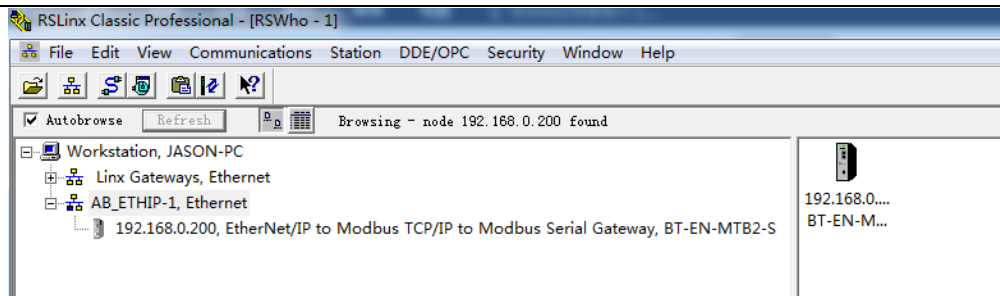
如下步骤为在 Logix5000 配置软件中添加模块：

将网关E1端口和电脑，以及Logix PLC以太网接口相连接。在电脑中使用RSLinx扫描模块，然后在 RSLogix5000中添加该模块的EDS文件，如下图：

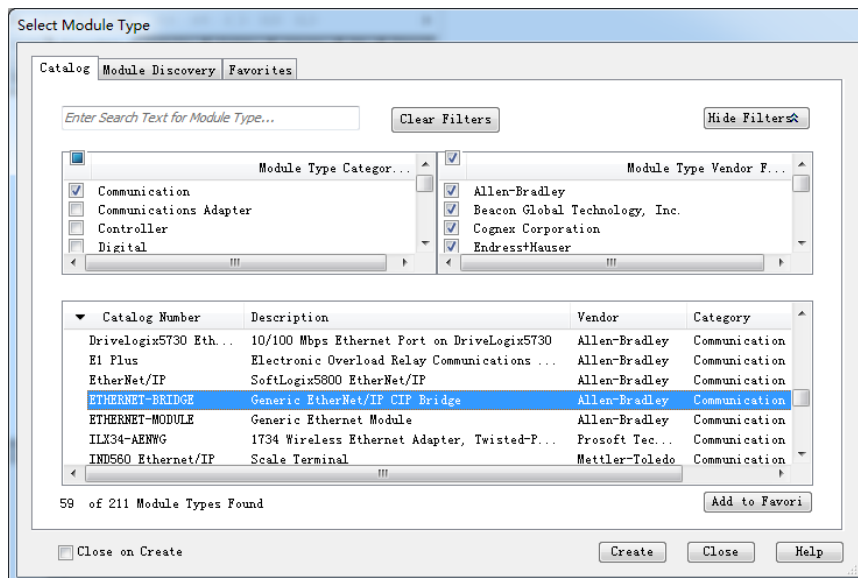
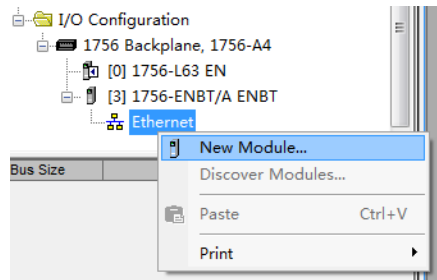


选择从设备上传 EDS 文件，如下图：

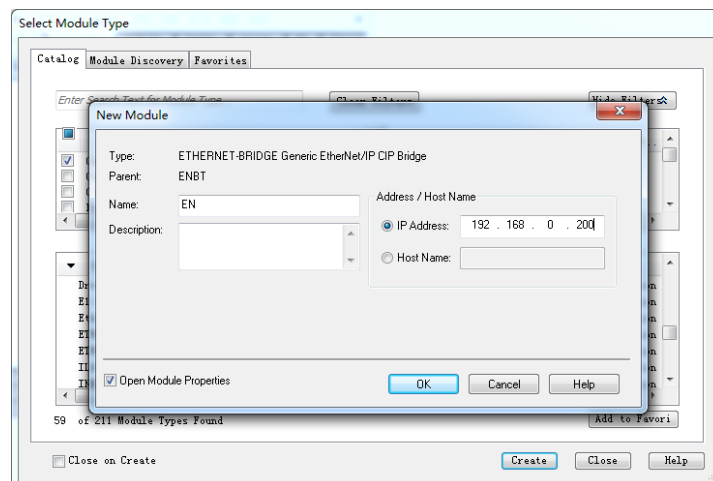




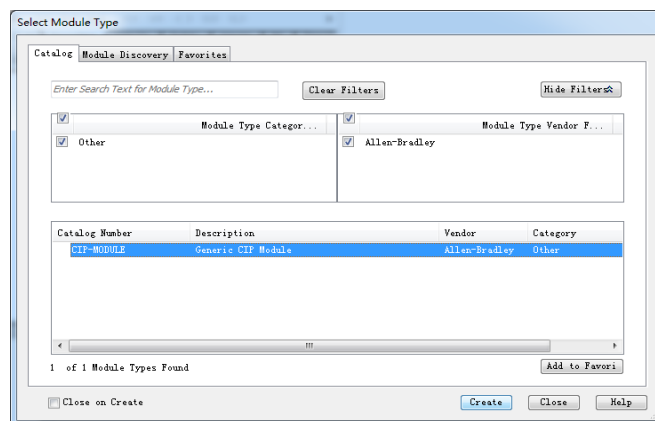
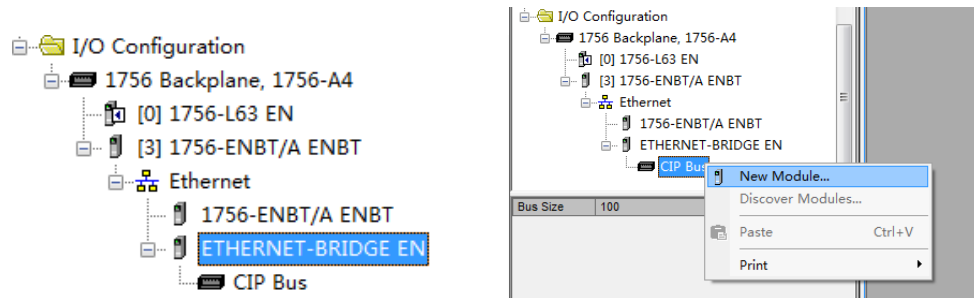
下一步通过添加“Generic EtherNet Bridge”完成 PLC 和模块的通讯，如下图。



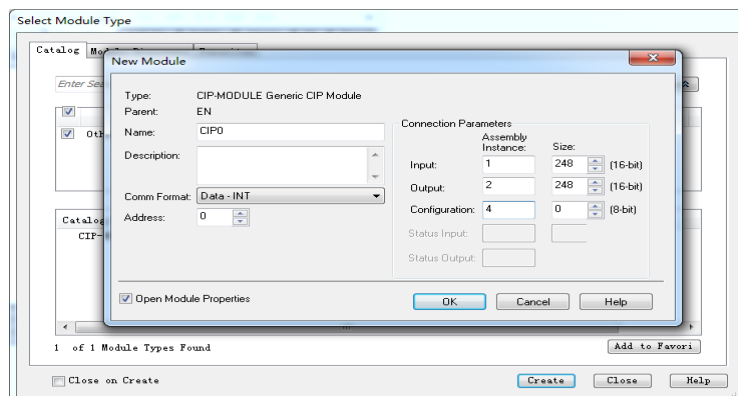
设定模块的 IP 地址，该地址为 E1 端口地址



在 Generic Ethernet Bridge 下添加一个新模块，再添加一个新的 CIP-Connection.



之后开始设定 PLC I/O connection 的参数，如下图：



请使用 Input 和 Output 都为 248 个字，Configuration 为 0。Comm format 需要选择 Data INT。

Assembly instances 设定方式：input 为“1”，output 为“2”，configuration 为“4”。

每一个 I/O connection 都需要进行如上的配置，之后点击 Create，来设定 I/O connection 的 RPI time 时间. 单机 PLC 结构，Use Unicast Connection over EtherNet/IP 要勾选，RPI 时间可以使用 5ms 或者 20ms。冗余 PLC 结构，Use Unicast Connection over EtherNet/IP 不要勾选，RPI 时间可以使用 20ms 或者 40ms。



EN:0:I.Data[0]-EN:0:I.Data[247]对应模块内部寄存器 0-247 的地址 输入

EN:0:0.Data[0]-EN:0:0.Data[247]对应模块内部寄存器 1000-1247 的地址 输出

EN:1:I.Data[0]-EN:1:I.Data[247]对应模块内部寄存器 250-497 的地址 输入

EN:1:0.Data[0]-EN:1:0.Data[247]对应模块内部寄存器 1250-1497 的地址 输出

以此类推。如下图，在 RSLogix5000 第一个 CIP I/O 链接的输出标签的开头写一些数据。



Home / Internal Data View

Decimal Display

Hexadecimal Display

Float Display

ASCII Display

Address	0	1	2	3	4	5	6	7	8	9
1000	8888	8888	8888	8888	8888	8888	8888	8888	8888	8888
1010	8888	0	0	0	0	0	0	0	0	0
1020	0	0	0	0	0	0	0	0	0	0
1030	0	0	0	0	0	0	0	0	0	0
1040	0	0	0	0	0	0	0	0	0	0
1050	0	0	0	0	0	0	0	0	0	0
1060	0	0	0	0	0	0	0	0	0	0
1070	0	0	0	0	0	0	0	0	0	0
1080	0	0	0	0	0	0	0	0	0	0
1090	0	0	0	0	0	0	0	0	0	0

Prev

1

2

...

6

7

8

9

10

11

12

13

14

15

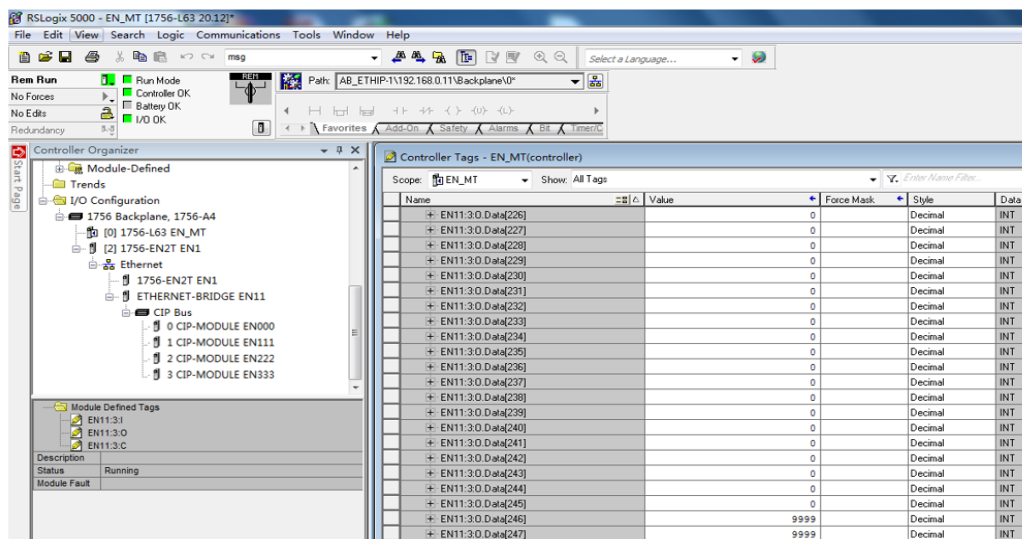
...

19

20

Next

在RSLogix 5000第4个CIP I/O链接的输出标签的结尾写一些数据。



网关Internal Data Base地址1996和1997的数据值的变化。

Home / Internal Data View

Decimal DisplayHexadecimal DisplayFloat DisplayASCII Display

Address	0	1	2	3	4	5	6	7	8	9
1900	0	0	0	0	0	0	0	0	0	0
1910	0	0	0	0	0	0	0	0	0	0
1920	0	0	0	0	0	0	0	0	0	0
1930	0	0	0	0	0	0	0	0	0	0
1940	0	0	0	0	0	0	0	0	0	0
1950	0	0	0	0	0	0	0	0	0	0
1960	0	0	0	0	0	0	0	0	0	0
1970	0	0	0	0	0	0	0	0	0	0
1980	0	0	0	0	0	0	0	0	0	0
1990	0	0	0	0	0	0	9999	9999	0	0

Prev

1

2

...

11

12

13

14

15

16

17

18

19

20

Next

配置模块做 EtherNet/IP Client

模块正常和 Logix 系列 PLC 通讯都是作为 server 从站，不过也可以同时支持作为 Client 和 Server 和 PLC 交换数据。在前一章介绍“模块做 Ethernet/IP server”的时候，很重要的一点是介绍了如何分配模块内部数据区的内容。

如果模块同时作为 EtherNet/IP 的 Client 和 Server 则要特别注意，读写数据区冲突的问题，以免造成数据混乱。

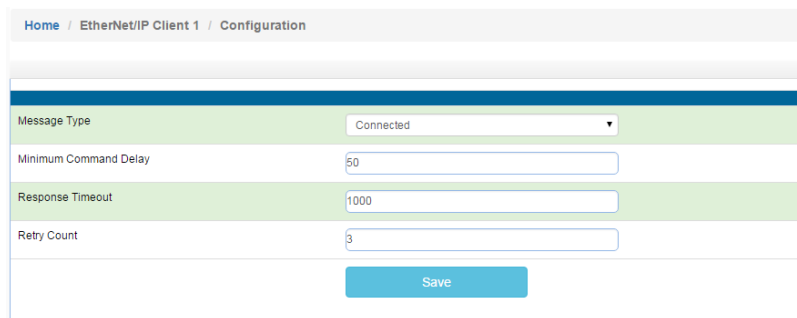


如上图，点击 EtherNet/IP Client ---Client1---Commands。

点开Configuration，查看默认的配置。

Message Type: Unconnected Send
Connected。

连接罗克韦尔 1756 系列，1769 系列，1746 系列，PLC-2 系列，PLC-5 系列，SLC500 系列，Micrologix PLC 系列，PowerFlex 变频器系列，连接 E300 智能马达保护器，PowerMonitor 智能电力监控仪等需要选择 Connected。



此处用于连接 1756 PLC，因此选择 Connected。

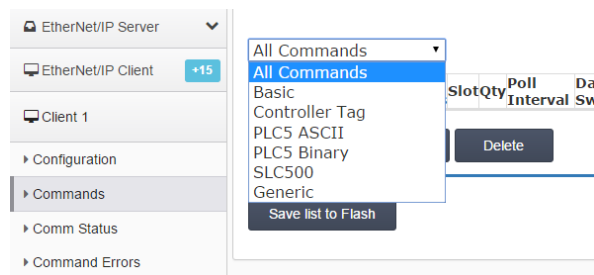
Minimum Command Delay: 每个 Client 执行指令的轮询时间，单位 ms，范围 0-65535

注：该时间越小，发送命令越快，但并非越小越好，需要先查看从站设备的说明书，确定从站响应时间是否能及时接受和反馈，主站发送命令的间隔。

Response Timeout: 所连接设备的响应时间，单位 ms，范围 0-65535

Retry Count: 重新尝试连接次数，范围 0-65535

之后选择指令的类型：



Basic 命令用于罗克韦尔 PLC-5, ControlLogix 数据的读写;

Controller Tag 命令用于罗克韦尔 CompactLogix, ControlLogix 数据标签或标签数组的读写

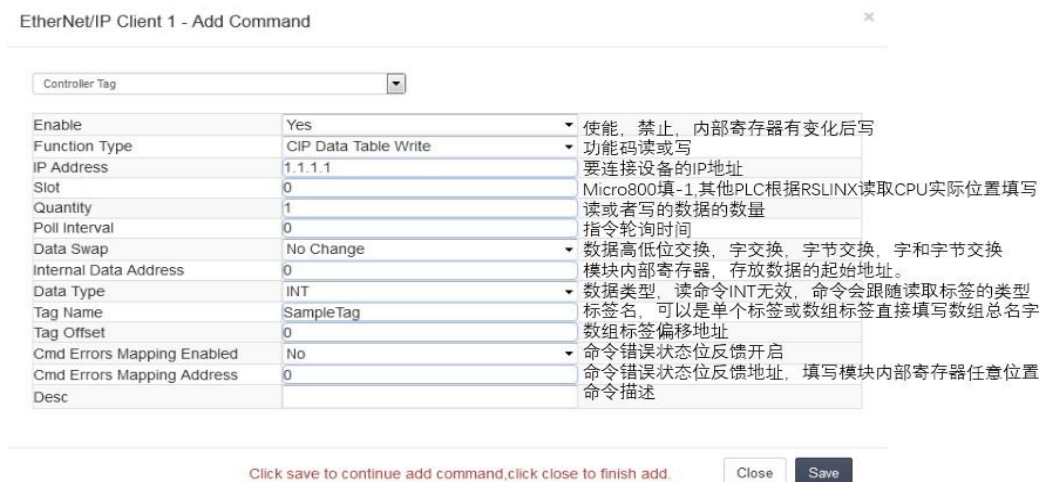
PLC5 ASCII 命令用于罗克韦尔 PLC-5, ControlLogix 数据的读写;

PLC5 Binary 命令用于罗克韦尔 PLC-5, ControlLogix 数据的读写;

SLC500 命令用于罗克韦尔 SLC500, MicroLogix, PowerFlex 变频器数据的读写;

Generic 命令用于罗克韦尔 PowerFlex 变频器, E300 智能马达保护器, PowerMonitor 智能电力监控仪数据的读写。

选择要连接的种类, 选择相应的命令。点击 Add 可以增加命令行。

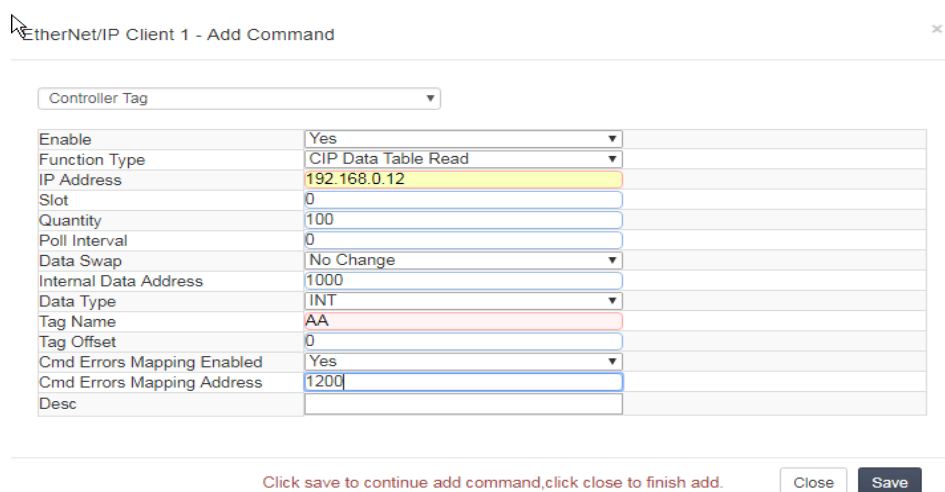


以下按照和 1756 PLC 通讯举例, 和其他罗克韦尔产品的通讯指令详细内容, 可另外参考其他手册或者咨询 BEACON 当地经销商和办事处。

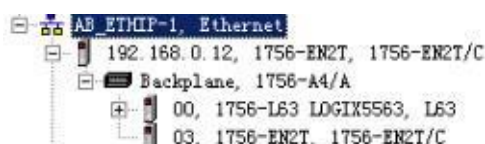
如下举例中, 仅针对 EtherNet/IP Client 指令部分内容进行介绍, 暂不考虑上一章中提到的 PLC CIP 标签和模块内部数据区地址映射的关系, 以及内部数据区大小范围。

在实际操作中, 因为不同产品型号的模块内部数据区大小不同, 请务必注意模块数据区的实际大小, 并根据实际数据寄存器的地址范围来配置指令, 同时还请注意相同地址是否重复被多种协议写入数据。

此选项用于罗克韦尔 PLC 在不能停机的情况下，对 Logix5000 或者 Studio 5000 软件里面标签或者标签数组进行读或写的操作。



举例一：如上图，读取 IP 地址为 192.168.0.12，CPU 位于 0 槽位的 L63 CPU 里面的全局变量标签数组 AA，数组是 INT 格式，数量 100 个 INT(每条命令最大 100 个 INT, 或者 50 个 DINT/REAL), 放到模块内部寄存器 1000-1099 里面，如果命令检测不到 AA 的数组有 100 个 INT 或者没有 AA 数组，或者 IP 地址不对，槽位不对等，就会在模块内部寄存器 1200 的位置报一个非零值，显示这条命令有错误，工程师可以使用 Cmd Errors Mapping 反馈来查看所连接设备的状态。（注：对于读来说 Data: Type 始终是 INT, 不可修改，但是会随着数组的类型自动调整）



⊕ AA			INT[100]		Read/Write	☐	Decimal
------	--	--	----------	--	------------	--------------------------	---------

读取 IP 地址为 92.168.0.12，CPU 位于 0 槽位的 L63 CPU 里面的全局变量标签数组 BB，数组是 REAL 格式，数量 50 个 REAL(每条命令最大 100 个 INT, 或者 50 个 DINT/REAL), 放到模块内部寄存器 1100-1199 里面，如果命令检测不到 BB 的数组有 50 个 REAL 数据，或者 IP 地址不对，槽位不对等，就会在模块内部寄存器 1201 的位置报一个非零值，显示这条命令有错误，工程师可以使用 Cmd Errors Mapping 反馈来查看所连接设备的状态。

Enable	Yes
Function Type	CIP Data Table Read
IP Address	192.168.0.12
Slot	0
Quantity	50
Poll Interval	0
Data Swap	No Change
Internal Data Address	1100
Data Type	REAL
Tag Name	BB
Tag Offset	0
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	1201
Desc	

Close Save

BB	REAL[50]	Read/Write	☐	Float
----	----------	------------	--------------------------	-------

检查命令状态，点击 Comm Status 如下图，可以看发送和接收的次数，最后的错误代码等。

Parameter Name		Value
Command Count		2
TNS		6354
Last Error Code		0
Number of Command Errors		0
Number of Requests Sent		1001
Number of Responses Received		1001
Number of Errors Received		0
Number of Errors Sent		0

Reset Counter

☒ Auto Refresh | 2 Second(s)

在 AA 和 BB 输入些数据：

Controller Tags - L63(controller)							
Scope: L63		Show: All Tags		Y. Enter Name Filter...			
	Name	Value	Force Mask	Style	Data Type	Description	
	[-] AA	{...}	{...}	Decimal	INT[100]		
	[+] AA[0]	11		Decimal	INT		
	[+] AA[1]	11		Decimal	INT		
	[+] AA[2]	123		Decimal	INT		
	[+] AA[3]	123		Decimal	INT		

Controller Tags - L63(controller)					
Scope:  L63		Show: All Tags		 Y. Enter Name /	
	Name	Value	Force Mask	Style	Data Type
	BB	{...}	{...}	Float	REAL[50]
	BB[0]	-888.99		Float	REAL
	BB[1]	0.0		Float	REAL
	BB[2]	0.0		Float	REAL
	BB[3]	77.22		Float	REAL
	BB[4]	0.0		Float	REAL

查看内部寄存器 1000 和 1100 的数据，此处说明 1 个 REAL 的浮点数占 2 个内部寄存器，虽然命令是 50 个浮点数，放到 1100 开始的内部寄存器，实际上是 1100-1199 这 100 个寄存器存放着 50 个浮点数

Home / Internal Data View

Decimal DisplayHexadecimal DisplayFloat DisplayASCII Display

Address	0	1	2	3	4	5	6
1000	11	11	123	123	0	0	0
1010	0	0	0	0	0	0	0
1020	0	0	0	0	0	0	0
1030	0	0	0	0	0	0	0
1040	0	0	0	0	0	0	0
1050	0	0	0	0	0	0	0
1060	0	0	0	0	0	0	0
1070	0	0	0	0	0	0	0
1080	0	0	0	0	0	0	0
1090	0	0	0	0	0	0	0

Prev12...6789101112131415...3233Next

Home / Internal Data View

Decimal DisplayHexadecimal DisplayFloat DisplayASCII Display

Address	0	1	2	3	4	5	6	7	8
1100	16220	-15266	0	0	0	0	28836	17050	0
1110	0	0	0	0	0	0	0	0	0
1120	0	0	0	0	0	0	0	0	0
1130	0	0	0	0	0	0	0	0	0
1140	0	0	0	0	0	0	0	0	0
1150	0	0	0	0	0	0	0	0	0
1160	0	0	0	0	0	0	0	0	0
1170	0	0	0	0	0	0	0	0	0
1180	0	0	0	0	0	0	0	0	0
1190	0	0	0	0	0	0	0	0	0

Prev12...78910111213141516...3233Next

可以看到内部寄存器 1200 和 1201 没有错误反馈：

Home / Internal Data View

Decimal Display Hexadecimal Display Float Display ASCII Display						
Address	0	1	2	3	4	5
1200	0	0	0	0	0	0
1210	0	0	0	0	0	0
1220	0	0	0	0	0	0
1230	0	0	0	0	0	0
1240	0	0	0	0	0	0
1250	0	0	0	0	0	0
1260	0	0	0	0	0	0
1270	0	0	0	0	0	0
1280	0	0	0	0	0	0
1290	0	0	0	0	0	0

Prev

1

2

...

8

9

10

11

12

13

14

15

16

17

...

32

33

Next

如果我们从 Logix5000 里面删除掉 AA 或者 BB 数组标签的时候，命令检测不到有这两个数组，就会在内部寄存器 1200 和 1201 里面报错误，其他协议可以采集存放错误标签寄存器来反馈命令的执行情况。也可以查看命令状态。这里可以看到错误代码 4 产生，这里面错误代码含义很多种，如果命令检测不到 AA 的数组有 100 个或者没有 AA 数组，或者 IP 地址不对，槽位不对等，就会在模块内部寄存器 1200 的位置报一个非 0 值，工程师编程时，此地址不等于 0 就表示命令没有执行下去，因为错误代码组合种类非常多，例如 IP 地址不对，又没有检测不到 AA 数组，这时候就会产生 IP 和检测不到 AA 数组的错误代码组合。这里不再详细介绍。

Home / EtherNet/IP Client 1 / Status

Parameter Name	Value
Command Count	2
TNS	15697
Last Error Code	4
Number of Command Errors	936
Number of Requests Sent	10344
Number of Responses Received	9408
Number of Errors Received	0
Number of Errors Sent	0

Reset Counter

☒ Auto Refresh [2] Second(s)

Home / Internal Data View

	Decimal Display	Hexadecimal Display	Float Display	ASCII Display
Address	0	1	2	3
1200	4	4	0	0
1210	0	0	0	0
1220	0	0	0	0
1230	0	0	0	0
1240	0	0	0	0
1250	0	0	0	0
1260	0	0	0	0
1270	0	0	0	0
1280	0	0	0	0
1290	0	0	0	0

Prev 1 2 ... 8 9 10 11 12 13 14 15 16 17 ... 32 33 Next

举例：连接 E300 马达保护器，请先查看 E300 用户手册，了解关于以太网连接的方法，E300 自带有 3 个输出继电器，如果控制输出继电器 1，继电器 2，继电器 3，就需要使用 CLASS CODE9, 3 个继电器分别对应着 Instance1, Instance2, Instance3。Attribute 选择 3 是对这个继电器写值，0=OFF 1=ON。

Discrete Output Point Object — CLASS CODE 0x0009

The following class attributes are supported for the Discrete Output Point Object:

Instance	Name	Description
1	OutputPt00	Control Module Output 0
2	OutputPt01	Control Module Output 1
3	OutputPt02	Control Module Output 2
4	OutDigMod1Pt00	Digital Expansion Module 1 Output 0
5	OutDigMod1Pt01	Digital Expansion Module 1 Output 1
6	OutDigMod2Pt00	Digital Expansion Module 2 Output 0
7	OutDigMod2Pt01	Digital Expansion Module 2 Output 1
8	OutDigMod3Pt00	Digital Expansion Module 3 Output 0
9	OutDigMod3Pt01	Digital Expansion Module 3 Output 1
10	OutDigMod4Pt00	Digital Expansion Module 4 Output 0
11	OutDigMod4Pt01	Digital Expansion Module 4 Output 1

All instances contains the following attributes.

Table 619 - Discrete Output Point Object Instance Attributes

Attribute ID	Access Rule	Name	Data Type	Value
3	Get/Set	Value	BOOL	0=OFF, 1=ON
5	Get/Set	Fault Action	BOOL	0=Fault Value attribute, 1=Hold Last State
6	Get/Set	Fault Value	BOOL	0=OFF, 1=ON
7	Get/Set	Idle Action	BOOL	0=Fault Value attribute, 1=Hold Last State
8	Get/Set	Idle Value	BOOL	0=OFF, 1=ON
113	Get/Set	Pr Fault Action	BOOL	0=Pr Fault Value attribute, 1=Ignore
114	Get/Set	Pr Fault Value	BOOL	0=OFF, 1=ON
115	Get/Set	Force Enable	BOOL	0=Disable, 1=Enable
116	Get/Set	Force Value	BOOL	0=OFF, 1=ON
117	Get/Set	Input Binding	STRUCT: USINT Array of USINT	Size of appendix I encoded path Appendix I encoded path: NULL path means attribute 3 drives the output. Otherwise, this is a path to a bit in an instance of the DeviceLogix Data Table.

Home / EtherNet/IP Client 1 / Command List

Generic

	Enable	Function Type	IP Address	Slot	Qty	Poll Interval	Data Swap	Internal Data Address	Cls Ins Att	Cmd Errors Mapping Enabled	Cmd Errors Mapping Address	Desc
1	Yes	Write Attribute Single	192.168.0.8	-1	1	0	No Change	1300	9 1 3	Yes	1400	
2	Yes	Write Attribute Single	192.168.0.8	-1	1	0	No Change	1301	9 2 3	Yes	1401	
3	Yes	Write Attribute Single	192.168.0.8	-1	1	0	No Change	1302	9 3 3	Yes	1402	

Add
Modify
Delete

Save list to Flash

如上建立的 3 条指令，表示对 IP 地址为 192.168.0.8 的 E300 马达保护器 3 个输出继电器进行输出操作，如果内部寄存器 1300，1301，1302 值为 1 的时候，3 个输出继电器会进行闭合动作，如果内部寄存器 1300，1301，1302 值为 0 的时候，3 个输出继电器会进行分开动作，如果 3 条命令没有正确执行，内部寄存器 1400，1401，1402 会报一个非零值。注：模块作为 EtherNet/IP Client 可以支持的内容非常多，根据需要连接的设备的不同（Logix 控制器，PowerFlex 变频器，E300 马达保护器，PowerMonitor 电力仪表），可以和我们联系，获取进一步的详细技术支持。联系方式请见手册最后一页。

配置模块做 Siemens S7 以太网主站

1. 点击 S7 Ethernet Client ---Client1 ---Commands

2. 点击 S7 Ethernet Client, 可以看到+15. 表示可以支持作为最多 15 个主站.

点开 Configuration. 查看默认的配置

Minimum Command Delay: 最小通讯延时 0-65535

Response Timeout: 西门子 PLC 响应时间 0-65535

Retry Count: 重新尝试连接次数 0-65535

3. 配置命令参数, **Commands** 用来读或写西门子 PLC 的命令。每个主站支持最大 32 条指令。如果同时连接 5 个西门子 PLC, 建议在 Client1-Client5 配置每一个主站分别对每个西门子 PLC 的读写。可以减少指令执行时间, 以及设备掉线后对于其他设备的影响。

Home / S7 Ethernet Client 1 / Command List

Enable	Function Type	IP Address	PLC Type	RackSlot	TSAP	Data Type	Address Type	DB Number	AddressQuantity	Poll Interval	Data Swap	Internal Data Address	Desc
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0
☐	Yes	Read	1.1.1.1	S7-200		1000INT	Data Block	1	0	1	0	No Change	0

点击 Add , 可以增加新的命令, 如下为针对不同种类西门子 PLC 添加指令的配置界面:

S7 Ethernet Client 1 - Add Command



Enable	Yes	是否启用命令
Function Type	Read	读/写
IP Address	1.1.1.1	西门子S7-200的以太网模块IP地址
PLC Type	S7-200	西门子PLC的种类
TSAP	1000	西门子S7-200的TSAP参数
Data Type	INT	数据类型
Address Type	Data Block (DB)	地址类型
DB Number	1	DB块的号码
Address	0	起始地址
Quantity	1	数量
Data Swap	No Change	数据是否交换高地位
Poll Interval	0	每条命令发送间隔的时间
Internal Data Address	0	网关内部数据库寄存器地址
Desc		命令描述

Click save to continue add command,click close to finish add.

Close

Save

undefined - Add Command



Enable	Yes	是否启用命令
Function Type	Read	读/写
IP Address	1.1.1.1	西门子S7-300, S7-400, S7-1200以太网接口的IP地址
PLC Type	S7-300/S7-400/S7-1200	西门子PLC的种类
Rack	0	西门子CPU所在的机架号
Slot	1	西门子CPU所在的槽位号
Data Type	INT	数据类型
Address Type	Data Block (DB)	地址类型
DB Number	1	DB块的号码
Address	0	起始地址
Quantity	1	数量
Data Swap	No Change	数据是否交换高地位
Poll Interval	0	每条命令发送的间隔时间
Internal Data Address	0	网关内部数据库寄存器地址
Desc		命令描述

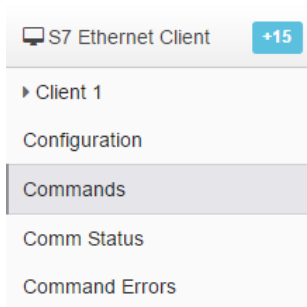
Click save to continue add command,click close to finish add.

Close

Save

举例读写西门子 PLC 整型数据

配置 S7-Ethernet Client 主站指令，点击 S7-Ethernet Client---Commands 建立指令，读或写西门子 DB 数据块的数据。



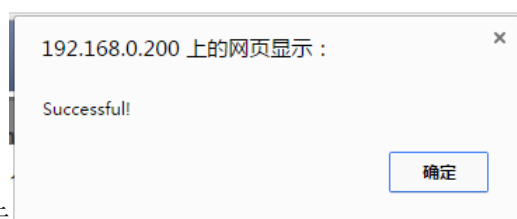
读指令解释如下，读取 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，把其中的 DB1 数据块里面的 3 个 INT 读到模块内部数据寄存器地址 0-2 中。

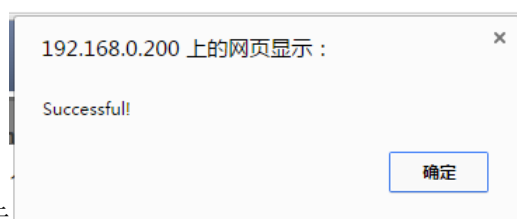
S7 Ethernet Client 1 - Modify Command ✕

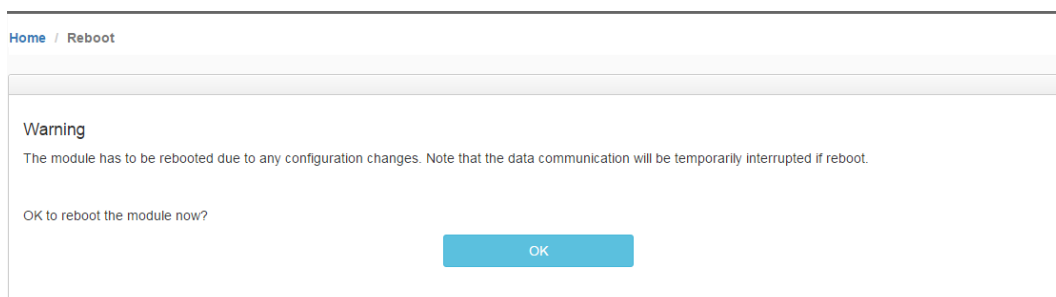
Enable	Yes
Function Type	Read
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	INT
Address Type	Data Block (DB)
DB Number	1
Address	0
Quantity	3
Data Swap	No Change
Poll Interval	0
Internal Data Address	0
Desc	

Close
Save

命令的要注意的地方，Slot 是指西门子 CPU 的槽位，Address 是指 DB 数据的起始地址，Quantity 是指要传输几个数据，Data Swap 是指传输的数据是否进行高低位交换，Internal Data Address 是指模块内部寄存器的起始地址。



点击 Save 保存，提示 ，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。



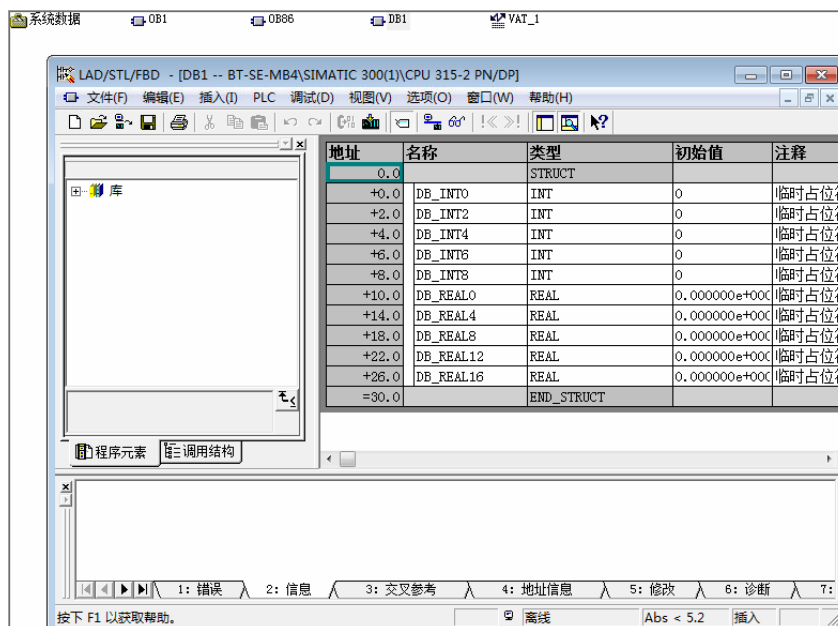
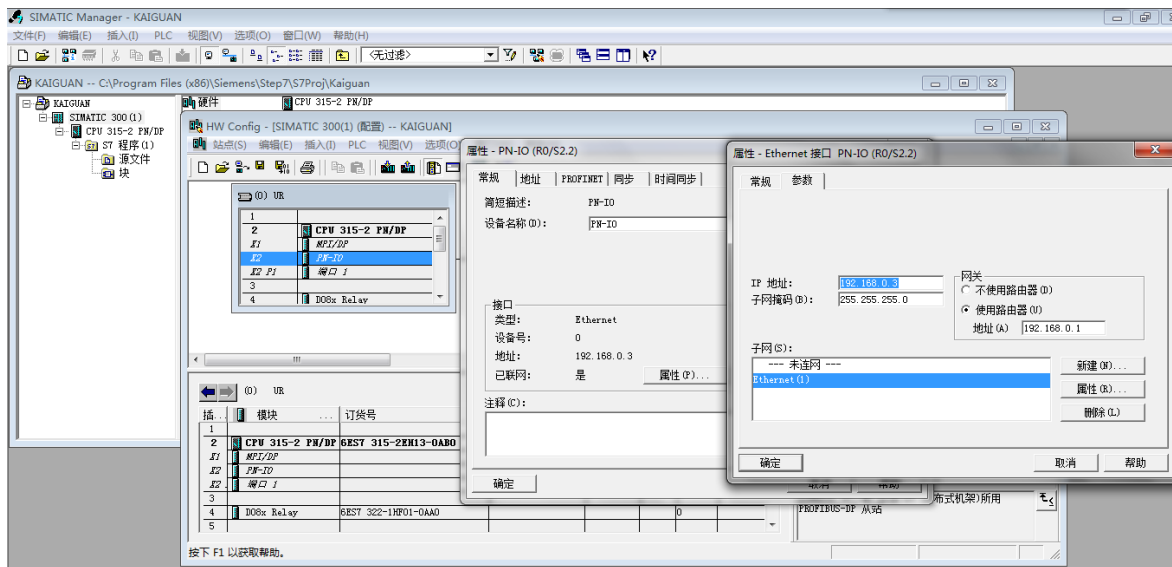
提示重启模块，点击 OK 完成重启。

[Home](#) / [Reboot](#)

Warning

Rebooting will be completed in 16 seconds, please go to [homepage](#) after reboot.

配置西门子 PLC 一侧，建立 DB 块



在 DB1.DBW0, DB1.DBW2, DB1.DBW4 里面写点数据。点击  赋值。



返回模块网页查看内部数据寄存器地址 0-2 中读入了相同的数据。

Module																																			
General Configuration																																			
Internal Data View																																			
Backup / Restore																																			
Change Password																																			
Firmware Upgrade																																			
Reboot Module																																			
Decimal Display Hexadecimal Display Float Display ASCII Display <table> <tr> <th>Address</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th></tr> <tr> <td>0</td><td>1234</td><td>6789</td><td>1357</td><td>0</td><td>0</td></tr> <tr> <td>10</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr> <td>20</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr> <td>30</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> </table>						Address	0	1	2	3	4	0	1234	6789	1357	0	0	10	0	0	0	0	0	20	0	0	0	0	0	30	0	0	0	0	0
Address	0	1	2	3	4																														
0	1234	6789	1357	0	0																														
10	0	0	0	0	0																														
20	0	0	0	0	0																														
30	0	0	0	0	0																														

为模块内部寄存器赋值（不同型号模块，可使用不同的驱动协议为模块数据区赋值），再配置命令写给西门子 DB1.DBW6 和 DB1.DBW8。

模块内部数据寄存器地址 3-4 被赋值数据，地址 0-2 是从西门子读到的数据。

Home																																									
Module																																									
General Configuration																																									
Internal Data View																																									
Backup / Restore																																									
Change Password																																									
Firmware Upgrade																																									
Reboot Module																																									
Decimal Display Hexadecimal Display Float Display ASCII Display <table> <tr> <th>Address</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th></tr> <tr> <td>0</td><td>1234</td><td>6789</td><td>1357</td><td>6688</td><td>7799</td></tr> <tr> <td>10</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr> <td>20</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr> <td>30</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr> <td>40</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> </table>						Address	0	1	2	3	4	0	1234	6789	1357	6688	7799	10	0	0	0	0	0	20	0	0	0	0	0	30	0	0	0	0	0	40	0	0	0	0	0
Address	0	1	2	3	4																																				
0	1234	6789	1357	6688	7799																																				
10	0	0	0	0	0																																				
20	0	0	0	0	0																																				
30	0	0	0	0	0																																				
40	0	0	0	0	0																																				

在模块 S7 以太网一侧配置写出指令如下

S7 Ethernet Client 1 - Modify Command

Enable	Yes
Function Type	Write
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	INT
Address Type	Data Block (DB)
DB Number	1
Address	6
Quantity	2
Data Swap	No Change
Poll Interval	0
Internal Data Address	3
Desc	

Close

Save

以上指令含义为，从模块内部数据区起始地址 3 开始，调用 2 个整型数，写给 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，写入 DB1 数据块里面的 DBW6 和 DBW8. 保存该指令，重启模块。

Enable	Function Type	IP Address	PLC Type	Rack	Slot	TSAP	Data Type	Address Type	DB Number	Address	Quantity	Poll Interval	Data Swap	Internal Data Address	Desc
☐ Yes	Read	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	1	0	3	0	No Change	0	
☐ Yes	Write	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	1	6	2	0	No Change	3	

Add

Modify

Delete

Save list to Flash

查看西门子 PLC 的数据，可以看到 DB1.DBW6 和 DB1.DBW8 的状态值，和模块内部数据区一致。

变量 - VAT_1

表格(T) 编辑(E) 插入(I) PLC 变量(A) 视图(V) 选项(O) 窗口(W) 帮助(H)

VAT_1 -- @BT-SE-MB4\SIMATIC 300(1)\CPU 315-2 PN/DP\S7 程序(3) ...

	地址	符号	显示格式	状态值	修改数值
1	DB1.DBW 0		DEC	1234	1234
2	DB1.DBW 2		DEC	6789	6789
3	DB1.DBW 4		DEC	1357	1357
4	DB1.DBW 6		DEC	6688	0
5	DB1.DBW 8		DEC	7799	0
6	DB1.DBD 10		DEC	L#0	
7	DB1.DBD 14		DEC	L#0	
8	DB1.DBD 18		DEC	L#0	
9	DB1.DBD 22		DEC	L#0	
10	DB1.DBD 26		DEC	L#0	
11					

举例：读写西门子 PLC 浮点数

S7 Ethernet Client 1 - Modify Command

Enable	Yes
Function Type	Read
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	REAL
Address Type	Data Block (DB)
DB Number	1
Address	10
Quantity	3
Data Swap	No Change
Poll Interval	0
Internal Data Address	20
Desc	

Close Save

以上指令解释如下，读取 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，把其中的 DB1 数据块里面，从 DBD10 开始的 3 个 REAL 类型数据，读到模块内部数据寄存器起始地址为 20 的区域中。因为模块内部数据寄存器为 16 位的字，所以 3 个浮点数会占用 6 个寄存器，也就是存放到模块内部地址 20-25 中

如下图，在西门子 PLC 中 DB1.DBD10/14/18 中赋值

地址	符号	显示格式	状态值	修改数值
2	DB1.DBW 2	DEC	6789	6789
3	DB1.DBW 4	DEC	1357	1357
4	DB1.DBW 6	DEC	6688	0
5	DB1.DBW 8	DEC	7799	0
6	DB1.DBD 10	FLOATING_POINT	-58.98	-58.98
7	DB1.DBD 14	FLOATING_POINT	-77.5533	-77.5533
8	DB1.DBD 18	FLOATING_POINT	69.89	69.89
9	DB1.DBD 22	FLOATING_POINT	0.0	
10	DB1.DBD 26	FLOATING_POINT	0.0	
11				
12				

模块内部数据区 20-25 的 6 个寄存器将会读取到了相同的数值。

之后再次为模块内部寄存器 26-29 赋值 2 个浮点数，998.5432 和 -99.1111。（不同型号模块，可使用不同的驱动协议为模块数据区赋值）。

在模块 S7 以太网主站建立一条写指令含义为，从模块内部数据区起始地址 26 开始，调用 2 个 REAL 类型数据，写给 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，写入 DB1 数据块里面的 DBD22 和 DBD26。保存该指令，重启模块。

S7 Ethernet Client 1 - Add Command



Enable	Yes
Function Type	Write
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	REAL
Address Type	Data Block (DB)
DB Number	1
Address	22
Quantity	2
Data Swap	No Change
Poll Interval	0
Internal Data Address	26
Desc	

Click save to continue add command,click close to finish add.

Close

Save

Enable	Function Type	IP Address	PLC Type	Rack	Slot	TSAP	Data Type	Address Type	DB Number	Address	Quantity	Poll Interval	Data Swap	Internal Data Address	Desc
☐ Yes	Read	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	1	0	3	0	No Change	0	
☐ Yes	Write	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	1	6	2	0	No Change	3	
☐ Yes	Read	192.168.0.3	S7-300/S7-400/S7-1200	0	2		REAL	Data Block	1	10	3	0	No Change	20	
☐ Yes	Write	192.168.0.3	S7-300/S7-400/S7-1200	0	2		REAL	Data Block	1	22	2	0	No Change	26	

Add

Modify

Delete

Save list to Flash

点击 Save list to Flash 重启网关，让命令生效。

如下图查看西门子 PLC 的数据，可以看到 DB1.DBW22 和 DB1.DBW26 的数据值，和模块内部数据区一致。

	地址	符号	显示格式	状态值	修改数值
2	DB1.DBW 2		DEC	6789	6789
3	DB1.DBW 4		DEC	1357	1357
4	DB1.DBW 6		DEC	0	0
5	DB1.DBW 8		DEC	0	0
6	DB1.DBD 10		FLOATING_POINT	-58.98	-58.98
7	DB1.DBD 14		FLOATING_POINT	-77.5533	-77.5533
8	DB1.DBD 18		FLOATING_POINT	69.89	69.89
9	DB1.DBD 22		FLOATING_POINT	998.5432	
10	DB1.DBD 26		FLOATING_POINT	-99.1111	
11					
12					

举例. 读写西门子 PLC 的布尔量

Enable	Yes	
Function Type	Read	
IP Address	192.168.1.1	
PLC Type	S7-300/S7-400/S7-1200	
Rack	0	
Slot	1	
Data Type	BOOL	Data Type
Address Type	Data Block (DB)	
DB Number	1	
Address	0	
Quantity	16	Quantity
Data Swap	No Change	
Poll Interval	0	
Internal Data Address	0	
Desc		

This parameter specifies the number of registers or digital points to be associated with the command.

Click save to continue add command,click close to finish add.

Close

Save

以上读指令解释如下，读取 IP 地址为 192.168.1.1 的西门子 1200 系列控制器的位数据，读取 DB1 数据块里面的前两个字节中的 16 个布尔量，放进模块内部数据寄存器起始地址为 0 的区域。
此处需要注意，模块内部寄存器都是 16 位的字，所以 16 个布尔量占用 1 个寄存器地址。

Enable	Yes
Function Type	Write
IP Address	192.168.1.1
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	1
Data Type	BOOL
Address Type	Data Block (DB)
DB Number	1
Address	0
Quantity	16
Data Swap	No Change
Poll Interval	0
Internal Data Address	1600
Desc	

以上指令解释如下，调用模块内部数据寄存器起始地址为 100 的连续 16 个布尔量数据，写入到 IP 地址为 192.168.1.1 的西门子 S7-300 系列控制器中，写入的位置为 DB1 数据块里面的前两个字节中的 16 个位。
此处需要注意，模块内部寄存器都是 16 位的字，所以写出布尔量时，内部寄存器的起始地址的真实位置为 $1600/16=100$ ，写出 16 个布尔量，正好写出一个寄存器内的数据。

以上介绍了 S7 以太网主站指令对 INT 类型，REAL 类型，BOOL 类型数据读写操作指令。
此外 S7 以太网主站指令，还可以对 BYTE，DINT 进行操作，此处不再详细举例。

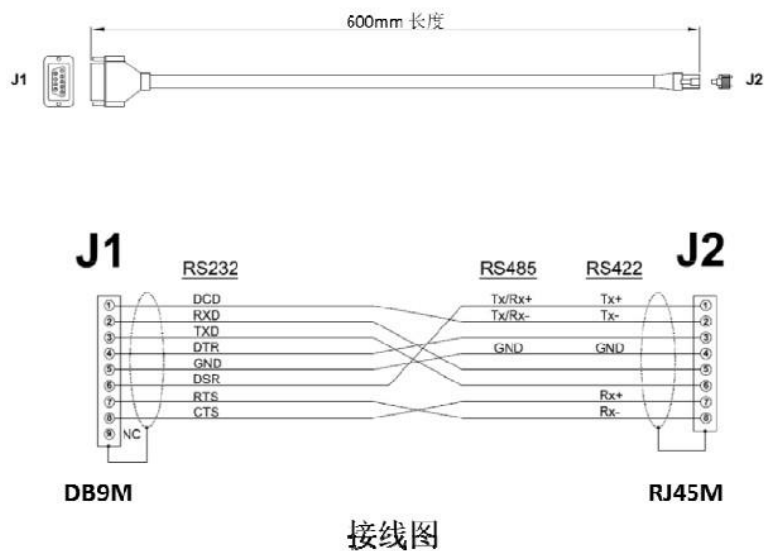
配置模块做 MODBUS RTU 主站

MB指的通讯协议是MODBUS RTU，接线方式提供RS232/422/485三种可以选择。MB2代表2个MODBUS RTU接口，

S1, S2 MODBUS RTU接口可以自由选择做主站或者从站。

Modbus RTU主站可以连接31个从站，两个串口S1和S2可以连接62个从站，RS485接线方式长度在1200米以内。
工程师设计连接每个主站连接从站个数可参考如下原则：

- 1、遵循MODBUS RTU通讯规约。
- 2、主站只读取从站数据，每个RS485串口主站可以接31个从站，MODBUS RTU是令牌轮询方式，连接从站越多，或者距离越长，延时越大。
- 3、主站同时读写从站数据，建议每个RS485串口最多接10-15个从站，避免过长通讯延时，提升通讯响应速度。



上图为S1/S2端口的接线图

举例：S1口引出来RS485接口，端子6+，1-
USB转RS485引出来的RS485接口，端子T/R+，T/R-

6+-----端子T/R+

1-----端子T/R-



或水晶头直插网关串口。



举例：S1口引出来RS232接口，端子2RX，3TX，5GND接线。

如果选用RS232接线方式，每个串口只能连接一个从站，接线长度不能超过15米。串口注意不能热插拔，容易对串口造成不必要的损坏。

打开浏览器，在左侧导航栏点击 Modbus Serial—Port1 里面的 Configuration，显示 S1 端口配置的页面，如下图：

Port	On	端口使能
Mode	RS485	接线方式
Type	Master	端口主站/从站
Protocol	RTU	端口协议
Baud Rate	19200	端口波特率
Parity	None	奇偶效验位
Data Bits	8	数据位
Stop Bits	1	停止位
Response Timeout	1000	从站的响应时间
Retry Count	3	重试次数
Minimum Command Delay	0	最小命令延时
Command Trigger Address	-1	命令触发地址

None
Odd
Even

无效验
奇效验

此处模块作为Modbus主站，请根据需要连接的Modbus从站情况，合理在此页面配置参数。之后，点击Port1里面的Commands显示S1端口命令的配置页面，点击Add。出现如下指令配置页面：

Modbus Port 1 - Modify Command

Enable	Yes	使能，禁止，内部寄存器有变化后写
Modbus Function	FC 3 - Read Holding Registers(4X)	Modbus 功能码FC1,FC2,FC3,FC4,FC5,FC6,FC15,FC16
Slave Address	1	从站地址
Modbus Data Address	0	从站读写数据Modbus起始位
Quantity	10	读或者写的数据的数量
Data Swap	No Change	数据高低位交换，字交换，字节交换，字和字节交换
Poll Interval	0	命令轮询时间
Internal Data Address	2000	模块内部寄存器，存放数据的起始地址
Cmd Errors Mapping Enabled	Yes	命令错误状态位反馈开启
Cmd Errors Mapping Address	2100	命令错误状态位反馈地址，模块内部寄存器任意位置
Desc		命令描述

Modbus 主站命令解释，采用功能码控制读写区域，注意一定要先确定模块内部数据的范围。以下举例中采用的模块最多可以支持 4000 个字数据区地址范围，实际配置模块时，请按照模块真实数据区大小进行指令的使用。

模块内部寄存器是 16 位的 INT 格式，读写布尔量的时需要注意 16 倍关系。

Enable	Yes
Modbus Function	FC 3 - Read Holding Registers(4X)
Slave Address	1
Modbus Data Address	0
Quantity	100
Data Swap	No Change
Poll Interval	0
Internal Data Address	2000
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2501
Desc	

以上指令含义如下：模块使用功能码 FC3，从站数据起始地址是 0 等于 40001，读取数量是 100。模块内部寄存器起始地址 2000。表示读 1 号从站，从站数据地址范围为 40001-40100 的 100 个字，放到模块内部寄存器 2000-2099，命令没有正确返回在内部寄存器 2051 报错。

如果功能码是 FC4 时（只读），从站数据起始地址是 0 等于 30001，读取数量是 100。模块内部寄存器起始地址 2000，表示读 1 号从站，从站数据地址范围为 30001-30100，放到模块内部寄存器 2000-2099，命令没有正确返回，会在内部寄存器 2051 报错。

Enable	Yes
Modbus Function	FC 1 - Read Coil (0X)
Slave Address	1
Modbus Data Address	0
Quantity	16
Data Swap	No Change
Poll Interval	0
Internal Data Address	32000
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2501
Desc	

以上指令含义如下：模块使用功能码 FC1 时，从站数据起始地址是 0 等于 00001，读取数量是 16（此处读取 16 个位等于读取一个字）。模块内部寄存器起始地址 32000（此处为位地址，读取 16 个位等于读取一个字，模块内部寄存器是字，所以实际上模块内部寄存器的起始地址为 $32000/16=2000$ ）。表示读 1 号从站，从站数据地址范围为 00001-00016，放到模块内部寄存器起始地址为 2000（因为读取到 16 个位数据，等于 1 个字数据，所以只占用模块内部寄存器一个地址），命令没有正确返回在内部寄存器 2051 报错。

如果是功能码 FC2 时（只读），从站数据起始地址是 0，读取数量是 16。模块内部寄存器 32000，同上表示读 1 号从站，从站数据地址范围为 00001-00016，放到模块内部寄存器 2000，命令没有正确返回，会在内部寄存器 2051

报错。

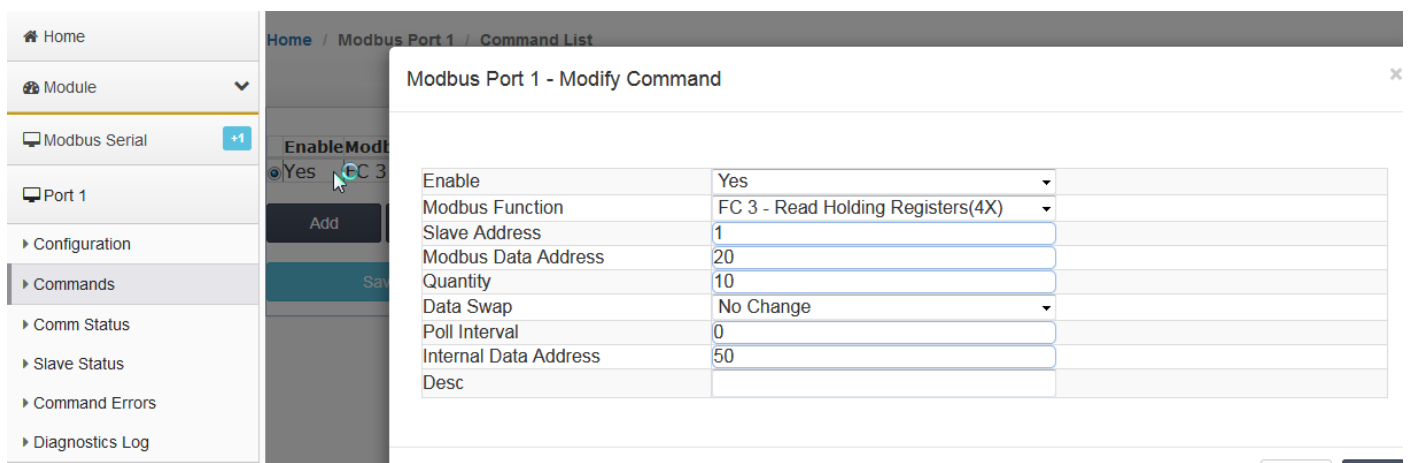
Enable	Yes
Modbus Function	FC 16 - Preset (Write) Multiple Register
Slave Address	1
Modbus Data Address	50
Quantity	20
Data Swap	No Change
Poll Interval	0
Internal Data Address	2000
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2051
Desc	

以上指令含义如下：Conditional 表示有条件情况下，模块使用功能码 FC6 或者 FC16 时，写出数量是 20. 模块内部寄存器起始地址为 2000，表示当模块内部寄存器范围 2000-2019 的任意寄存器发生数据发生变化时候，触发一条写的命令，数据从模块写到 1 号从站，从站接收数据地址范围为 40051-40070，命令没有正确执行，会在内部寄存器 2051 报错。

Enable	Conditional
Modbus Function	FC 16 - Preset (Write) Multiple Register
Slave Address	1
Modbus Data Address	50
Quantity	20
Data Swap	No Change
Poll Interval	0
Internal Data Address	2000
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2501
Desc	

以上指令含义如下：模块功能码 FC6 或者 FC16 时，写出数量是 20. 模块内部寄存器起始地址 2000。表示内部寄存器范围 2000-2019 的数据，一直连续的写出到 1 号从站，从站接收数据的地址范围为 40051-40070，命令没有正确执行，会在内部寄存器 2051 报错。

举例：新建一条命令，

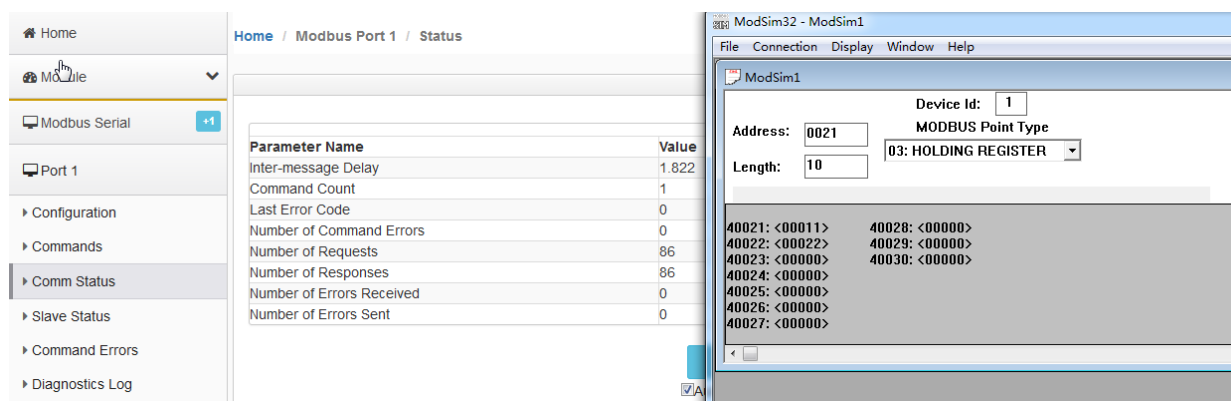
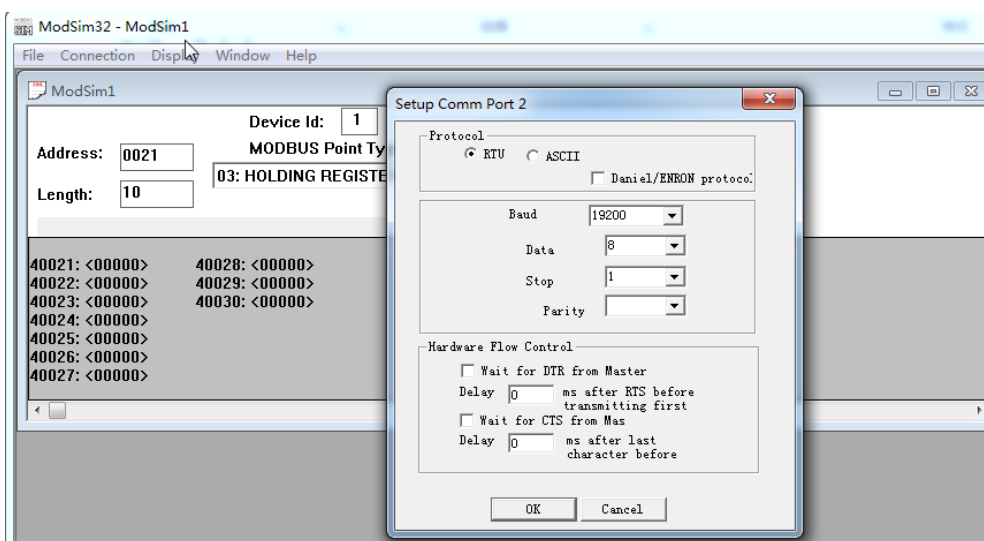


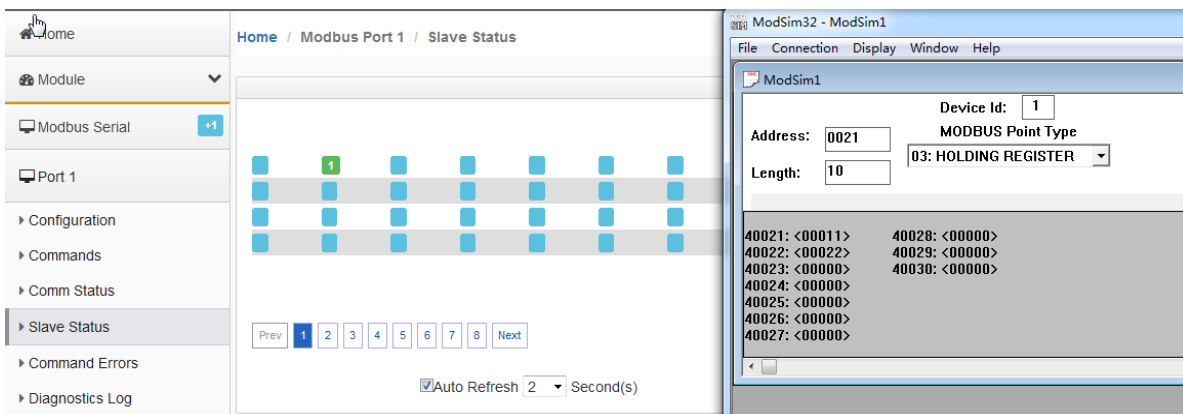
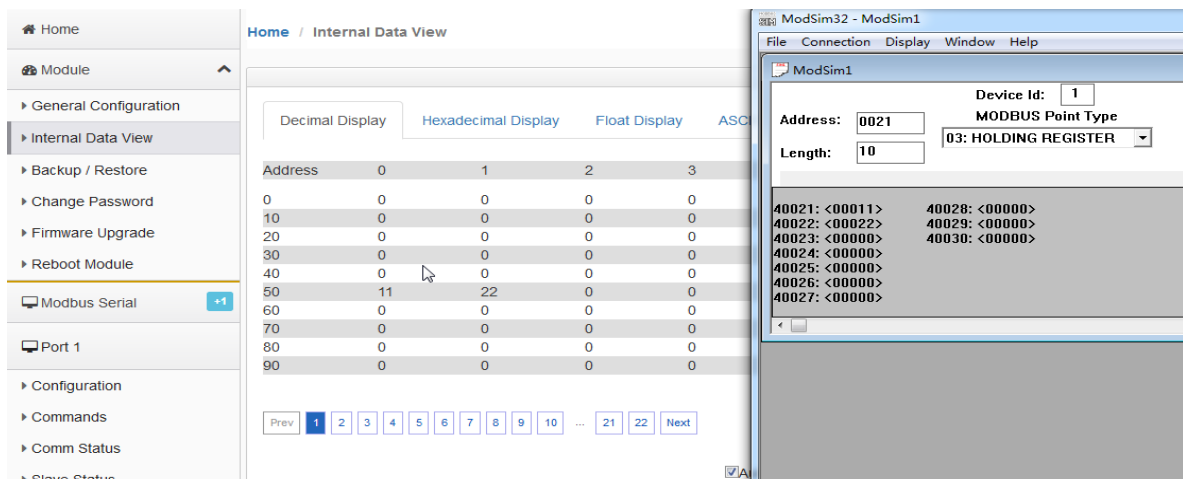
命令含义：把 MODBUS RTU 从站的 40021-40030 这 10 个 16 位的数值读到内部数据库 50-59 里面。

配置完，把这个命令保存到命令列表里面，然后根据提示重启模块。

用户在配置好模块 MODBUS RTU 主站端口后，可以利用 MODBUS RTU 仿真软件 MODSIM32，作为 MODBUS RTU 从站，仿真测试与模块主站端口通讯。

打开 MODSIM 32 软件，配置端口 2 参数，从 40021-40030 写入十个数据。点击 OK。可以看到模块主站对应的内部数据区也相应的显示出从站的数值变化。





Modbus Port 1 - Modify Command

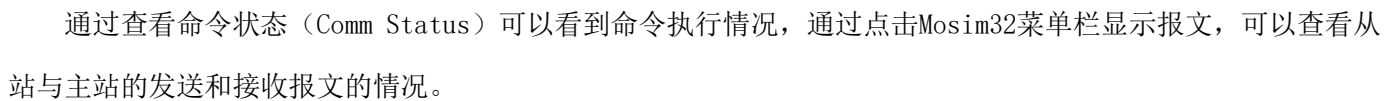
Enable	Yes	使能, 禁止, 内部寄存器有变化后写
Modbus Function	FC 3 - Read Holding Registers(4X)	Modbus 功能码FC1,FC2,FC3,FC4,FC5,FC6,FC15,FC16
Slave Address	1	从站地址
Modbus Data Address	0	从站读写数据Modbus起始位
Quantity	10	读或者写的数据的数量
Data Swap	No Change	数据高低位交换, 字交换, 字节交换, 字和字节交换
Poll Interval	0	命令轮询时间
Internal Data Address	2000	模块内部寄存器, 存放数据的起始地址
Cmd Errors Mapping Enabled	Yes	命令错误状态位反馈开启
Cmd Errors Mapping Address	2100	命令错误状态位反馈地址, 模块内部寄存器任意位置
Desc		命令描述

Cmd Errors Mapping Enabled和Cmd Errors Mapping Address这两个参数;

Cmd Errors Mapping Enabled表示命令错误是否映射, 选择YES表示使用, 选择NO, 表示不使用;

Cmd Errors Mapping Address 表示命令错误映射的地址。

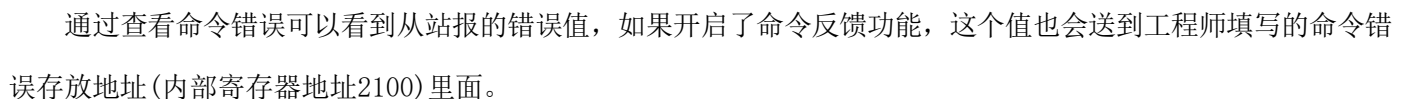
上图命令表示: 读取1号从站, 从站数据地址范围40001-40010, 这10个数放到内部起始地址为2000的连续10个寄存器内 (2000-2009), 如果发送错误, 错误反馈会放到内部寄存器2100里面。指令执行效果如下图显示:

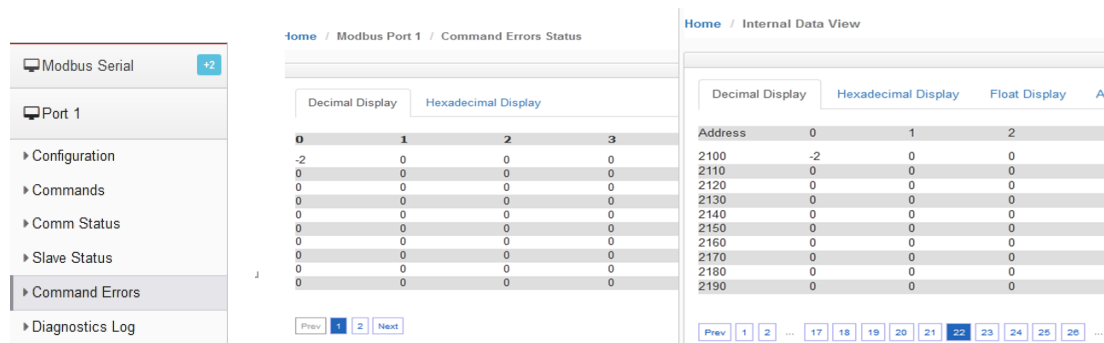


绿色表示线路数据通讯报文都正常;

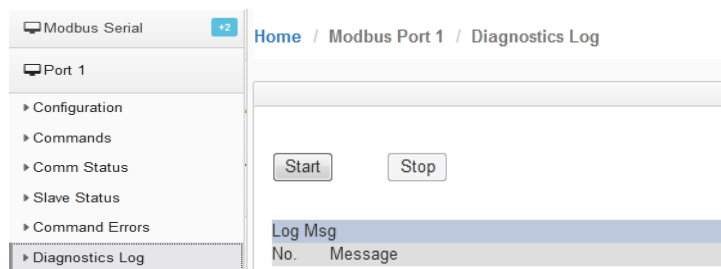
红色表示线路数据通讯报文都不对;

绿色和红色闪烁表示线路正常，数据通讯报文不正常。





通过诊断报文，可以查看主站发送和接收的报文情况。点击Start，就可以看到下面报文发送和接受的情况。

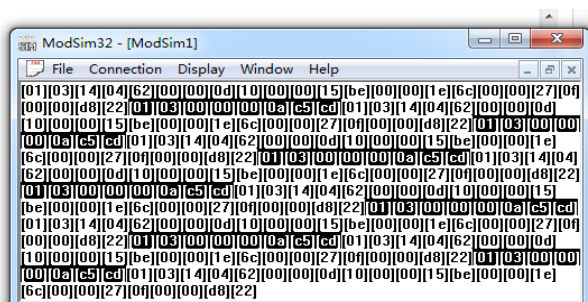


下图为主站发送和接收的报文以十六进制格式显示，Modsim32也可以从十进制报文切换到十六进制报文显示：

```

693 00:02:14.003 >> 01 03 00 00 00 0A C5 CD
694 00:02:14.105 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
695 00:02:14.309 >> 01 03 00 00 00 0A C5 CD
696 00:02:14.432 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
697 00:02:14.637 >> 01 03 00 00 00 0A C5 CD
698 00:02:14.739 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
699 00:02:14.944 >> 01 03 00 00 00 0A C5 CD
700 00:02:15.046 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
701 00:02:15.250 >> 01 03 00 00 00 0A C5 CD
702 00:02:15.353 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
703 00:02:15.557 >> 01 03 00 00 00 0A C5 CD
704 00:02:15.680 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
705 00:02:15.885 >> 01 03 00 00 00 0A C5 CD
706 00:02:16.007 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
707 00:02:16.212 >> 01 03 00 00 00 0A C5 CD
708 00:02:16.315 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22

```



Modbus 命令使能控制介绍

新版本增加了Modbus RTU做主站的命令使能控制，这个作用是表示可以控制发出几个命令，比如模块连接了15个从站，如果有一个从站坏掉了，这时候Modbus RTU网络会变慢，主站每次发送命令会等待这个从站响应，解决的办法是不发送这个从站的命令，具体使用方法如下。

Home / Modbus Port 1 / Command List

	EnableModbus Function	Slave Address	Modbus Data Address	Quantity	Data Swap	Poll Interval	Internal Data Address	Cmd Errors Mapping Enabled	Cmd Errors Mapping Address	Desc
☒	Yes FC 3 - Read Holding Registers(4X)	1	0	10	No Change	0	0	Yes	20	
☒	Yes FC 3 - Read Holding Registers(4X)	2	0	10	No Change	0	10	Yes	21	

上图中建立两条指令：

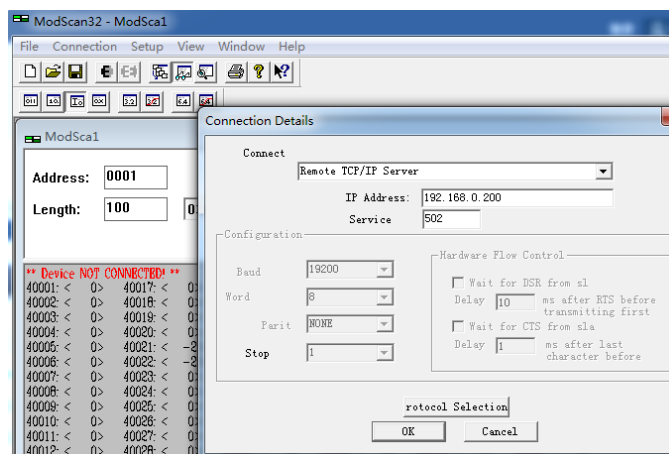
1- 读1号从站的40001-40010到内部寄存器0-9，错误状态放在了内部寄存器20。

2- 读2号从站的40001-40010到内部寄存器10-19，错误状态放在了内部寄存器21

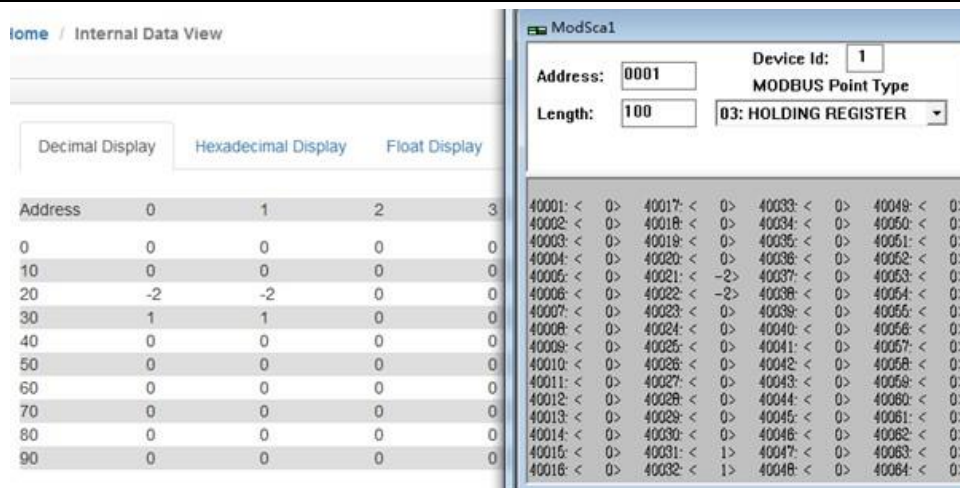
3- 使能命令触发地址，在模块Modbus主站端口配置页面中，Command Trigger Address设置成30，如下图，表示使用模块内部起始地址为30的寄存器作为触发条件。然后保存，重启生效。

Type	Master
Protocol	RTU
Baud Rate	19200
Parity	None
Data Bits	8
Stop Bits	1
Response Timeout	1000
Retry Count	3
Minimum Command Delay	0
Command Trigger Address	30

之后使用ModScan仿真作为Modbus从站，用ModScan的40031和40032可以模拟控制这两条指令的触发状态。



ModScan的40031和40032设置为1，可以看到模块内部寄存器地址30数据是1，内部寄存器地址31也是1，表示以上两条指令处于触发情况。模块内部寄存器地址20-21数据是-2，表示有错误代码，说明以上两条指令都没有正确执行。



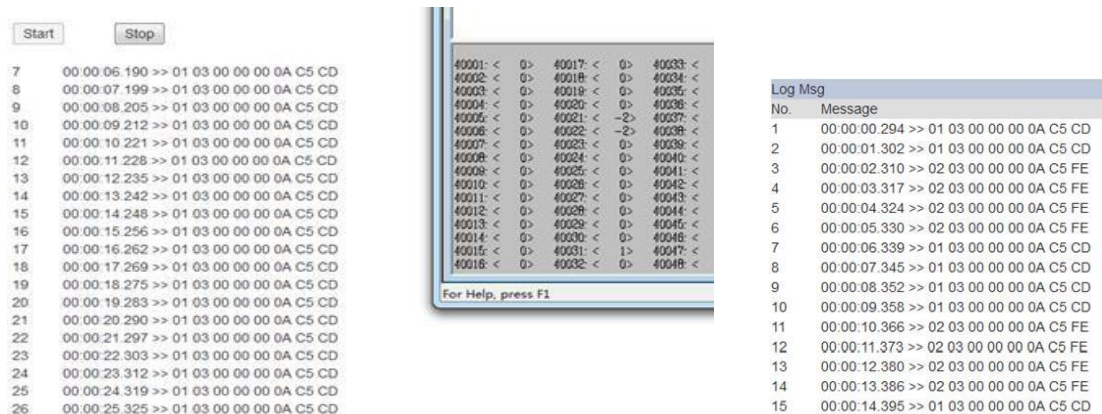
直观表现如下：检查Port1报文发送情况，显示第一条命令发送4次，第二条命令发送4次。因为命令本身发送1次，如果找不到从站设备，该命令会重新发送3次，共计4次。

重发次数，可以在端口配置中进行修改（如下图）：

Retry Count

以上两条指令都没有正确执行，如果是2号从站有问题，我们可以把2号从站的命令停止发送。

需要修改ModScan中40032的数值，从1改成0（如下图），这样相当于停止了触发读取2号从站的指令。

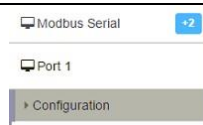


就实现了模块只读取1号从站数值的报文。避免了多个从站中有一个或两个掉线而影响整体Modbus RTU网络变慢的情况。

该功能建议配合前文提到的命令反馈功能一并使用，当其中一个命令反馈回来出现非0值，PLC的程序可以自动关联这个触发值去停止Modbus指令的执行。

配置模块做 MODBUS RTU 从站

点击Port1里面的Configuration显示S1端口配置的页面：

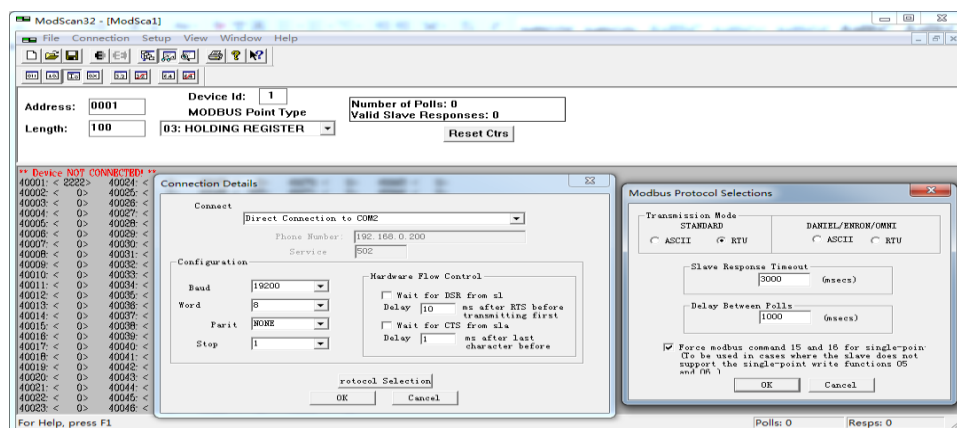


注意事项：S1或者S2作为Modbus从站，只需要配置端口参数，无需配置端口命令。S1和S2共用模块内部数据区。如下图为设置模块的Modbus从站端口参数：

Port	On	端口使能
Mode	RS485	接线方式
Type	Slave	端口主站/从站
Protocol	RTU	端口协议
Baud Rate	19200	端口波特率
Parity	None	奇偶校验位
Data Bits	8	数据位
Stop Bits	1	停止位
Slave ID	1	从站地址
Minimum Response Delay	1	最小响应延时
Holding Register Offset	0	数据偏移
Word Input Offset	0	字输入偏移
Bit Input Offset	0	位输入偏移
Bit Output Offset	0	位输出偏移

Save

使用ModScan32仿真Modbus RTU主站，可以对模块内部寄存器读写。

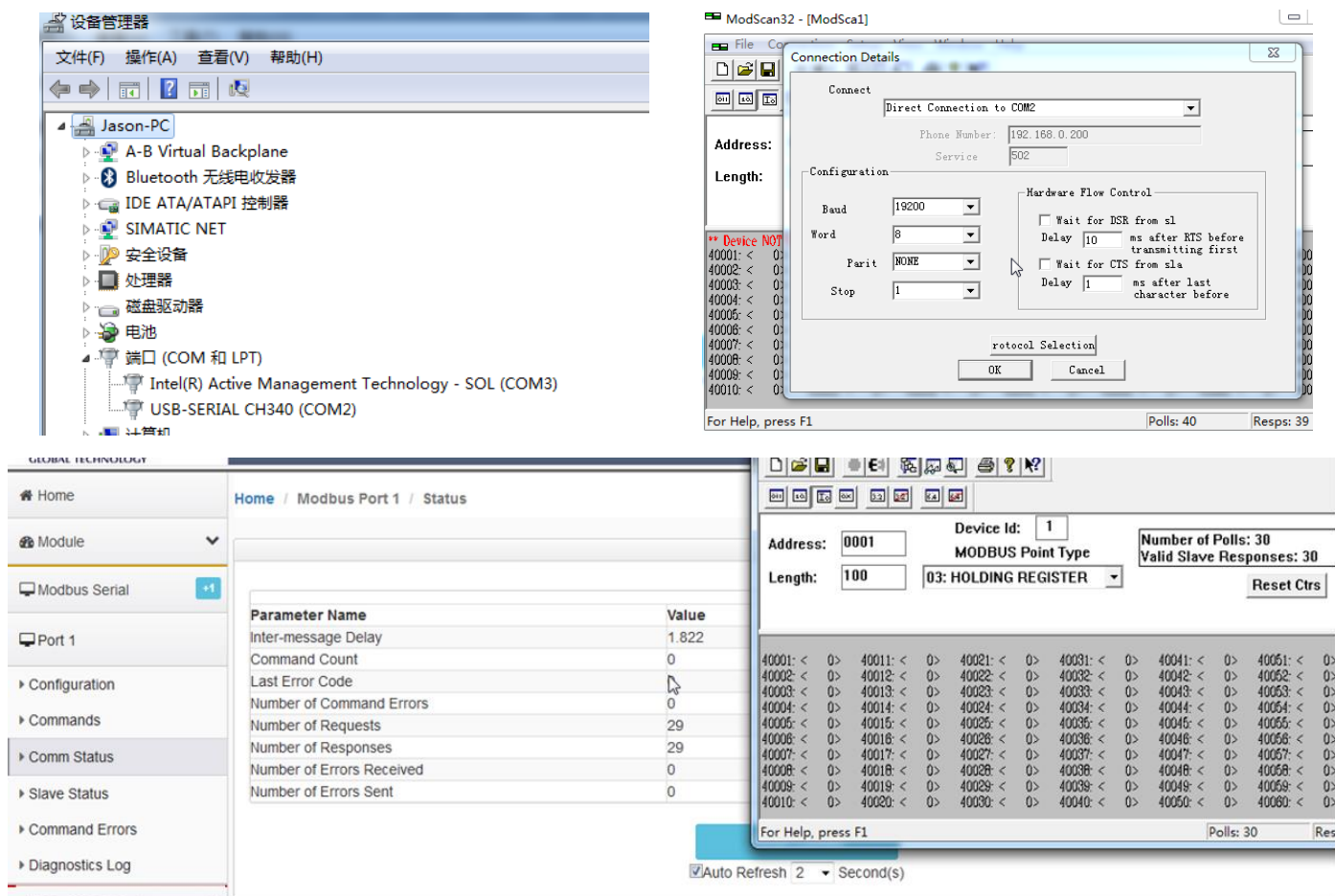


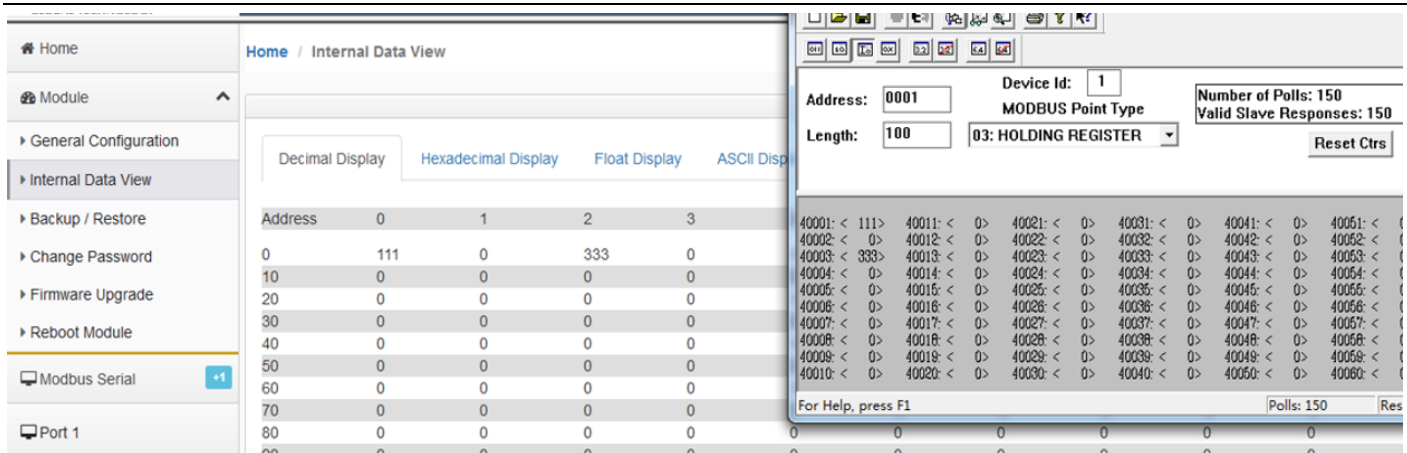
内部寄存器与Modbus数据对应关系：

模块内部寄存器地址	等于	Modbus4区地址	等于	Modbus3区地址	等于	Modbus1区地址	等于	Modbus1区地址	等于	Modbus0区地址	等于	Modbus0区地址
0	=	40001	=	30001	=	10001	至	10016	=	00001	至	00016
1	=	40002	=	30002	=	10017	至	10032	=	00017	至	00032
10	=	40011	=	30011	=	10161	至	10176	=	00161	至	00176
11	=	40012	=	30012	=	10177	至	10192	=	00177	至	00192
20	=	40021	=	30021	=	10321	至	10336	=	00321	至	00336

30	=	40031	=	30031	=	10481	至	10496	=	00481	至	00496
99	=	40100	=	30100	=	11585	至	11600	=	01585	至	01600
100	=	40101	=	30101	=	11601	至	11616	=	01601	至	01616
220	=	40221	=	30221	=	13521	至	13536	=	03521	至	03536
1000	=	41001	=	31001	=	26001	至	26016	=	16001	至	16016
1001	=	41002	=	31002	=	26017	至	26032	=	16017	至	16032
1999	=	42000	=	32000	=	41985	至	42000	=	31985	至	32000
2000	=	42001	=	32001	=	42001	至	42016	=	32001	至	32016
2001	=	42002	=	32002	=	42017	至	42032	=	32017	至	32032
3000	=	43001	=	33001	=	58001	至	58016	=	48001	至	48016

打开 MODBUS RTU 仿真软件 MODSCAN32，其作用是仿真 MODBUS RTU 主站。软件连接作为 MODBUS RTU 从站的模块。选择 Connection，选择电脑的 USB-485 接口 COM2，修改波特率，数据位，奇偶校验位，停止位等参数与模块的端口参数一致。点击 OK，可以看到连接的发送和接收次数。在 40001 等数据区进行写数据，可以看到模块内部对应寄存器同样有数据显示。

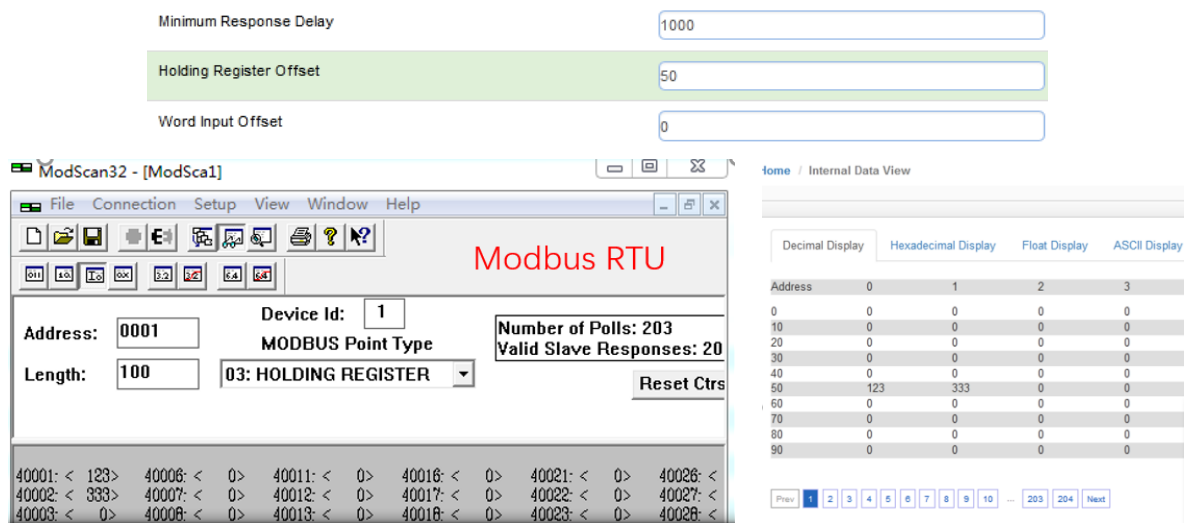




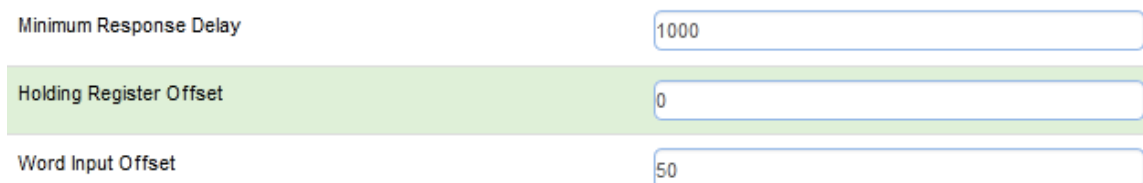
备注：40001 对应着内部寄存器 0，40100 对应着内部寄存器 99，以此类推。

Modbus RTU 配置成从站时，在主页面可以设置接收地址偏移。

Holding Register Offset使用方法：Modbus RTU主站使用FC3功能码，在40001和40002输入两个数据，正常情况下，这两个数据应该会被写入到模块内部寄存器0-1当中去。如果此处偏移量设置成50(如下图)，则数据会直接偏移写入模块内部寄存器50-51里面。4区，3区，1区，0区同样遵循这个原理。

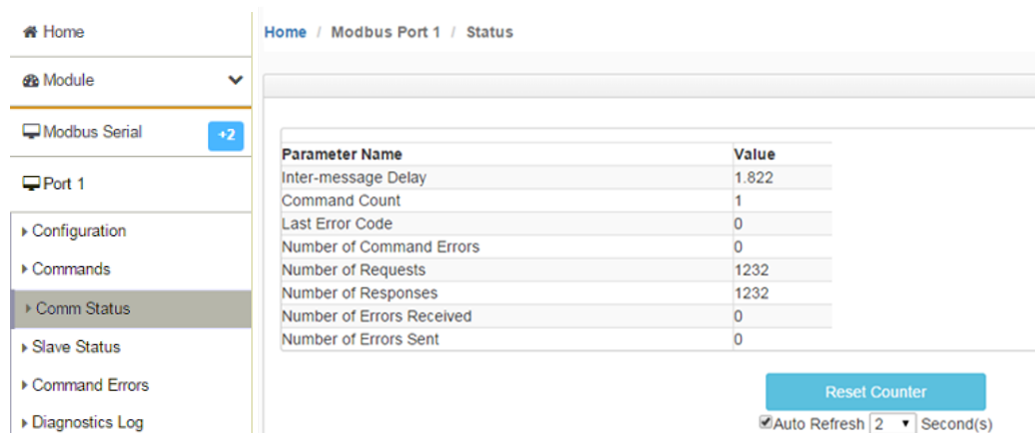


Word Input Offset使用方法：如果此处偏移量设置成50(如下图)，Modbus RTU主站一侧在3区对30001和30002输入两个数据，数据会直接向后偏移放到模块内部寄存器50-51里面，ModScan32仿真软件不能载入3区的数值，请以现场设备实际数据区域来填写。



Modbus RTU 诊断方式

查看主站端口命令是否有错误，发包和收包状态：

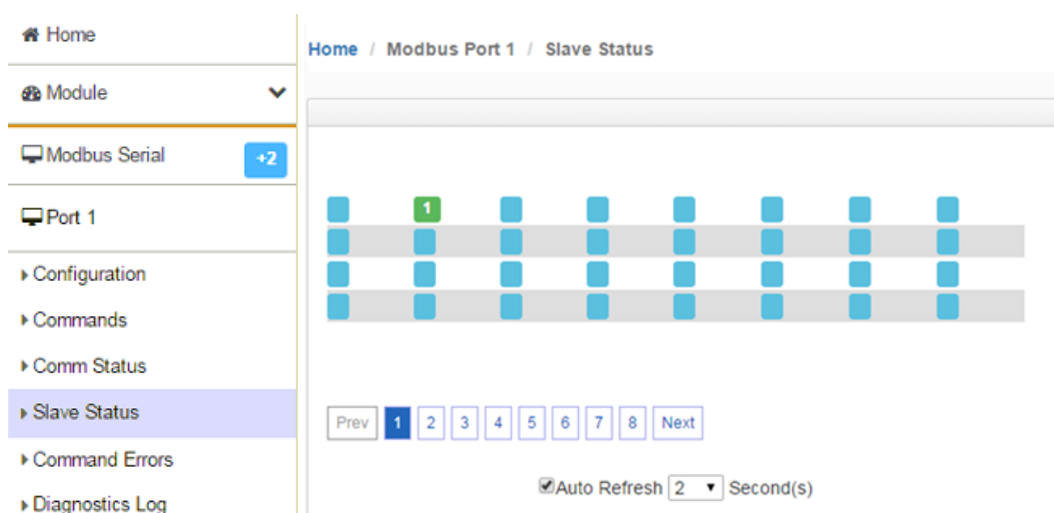


Parameter Name	Value
Inter-message Delay	1.822
Command Count	1
Last Error Code	0
Number of Command Errors	0
Number of Requests	1232
Number of Responses	1232
Number of Errors Received	0
Number of Errors Sent	0

Reset Counter

☒ Auto Refresh 2 Second(s)

可视化查看从站状态 点击Slave Status 可以看到1号从站是绿色的。



Home / Modbus Port 1 / Slave Status

Prev 1 2 3 4 5 6 7 8 Next

☒ Auto Refresh 2 Second(s)

查看命令行是否有错误产生点击：

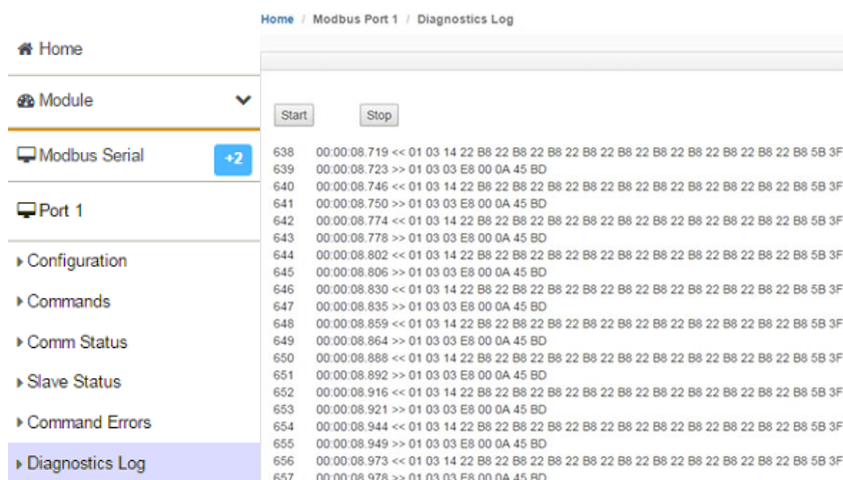
Command Errors

Decimal Display Hexadecimal Display

0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0

报文诊断功能：点击Diagnostics Log，再点击Start端口发送和接收报文的情况。

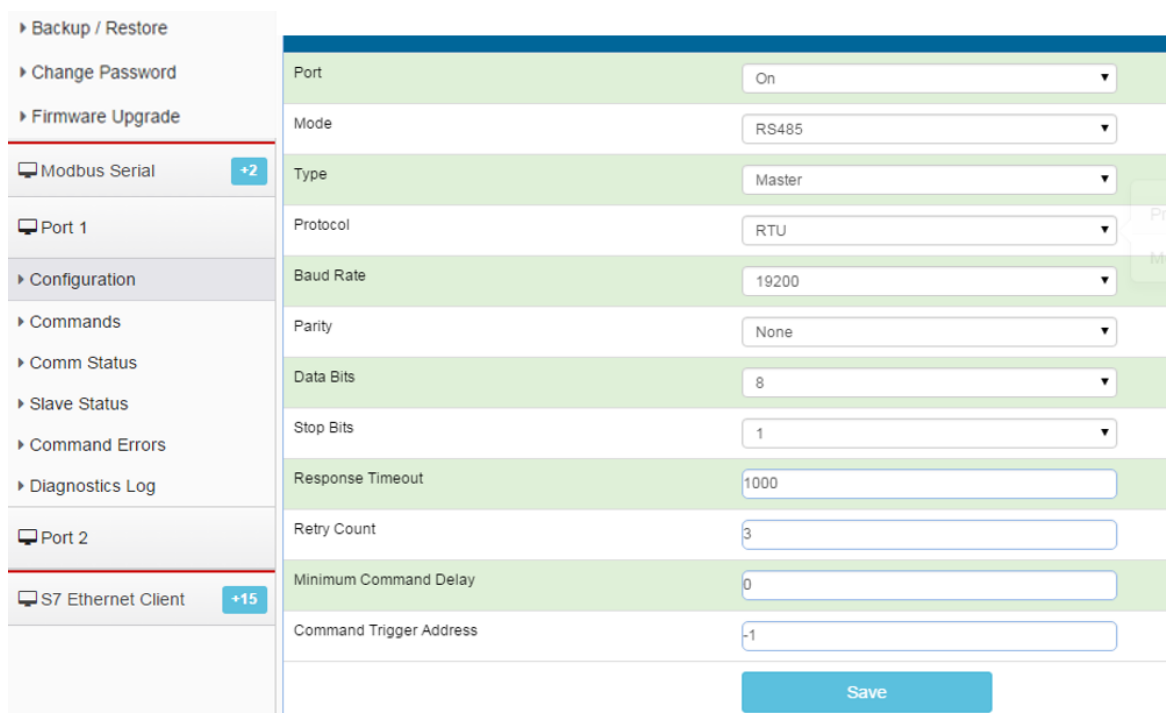
>>符号是S1端口发送的报文，<<符号是S1端口接收的报文。



举例 1. 罗克韦尔 PLC 和西门子 PLC 同时采集 Modbus RTU 从站数据

本案例中，模块EtherNet/IP配置为Client，Modbus RTU串口配置为Master，S7 Ethernet配置成为Client
点击Modbus Serial---Port1---Configuration

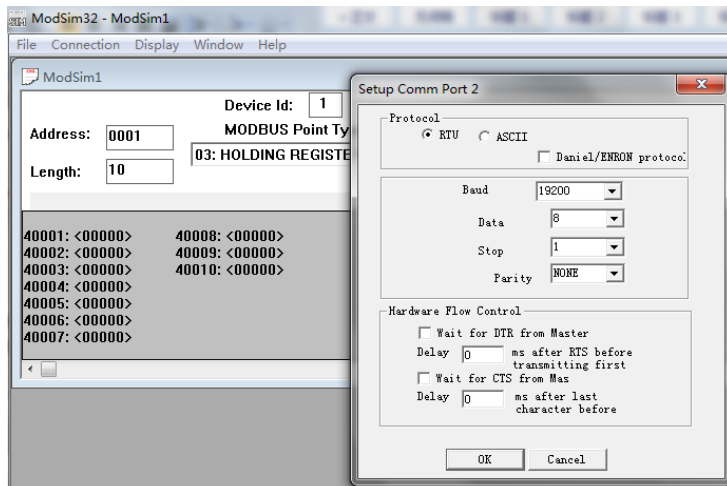
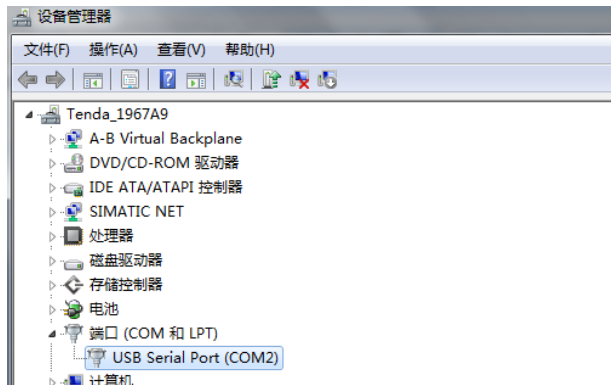
首先配置S1口为MODBUS RTU协议主站，RS485接线方式。注：配置完要保存命令，并重启网关。



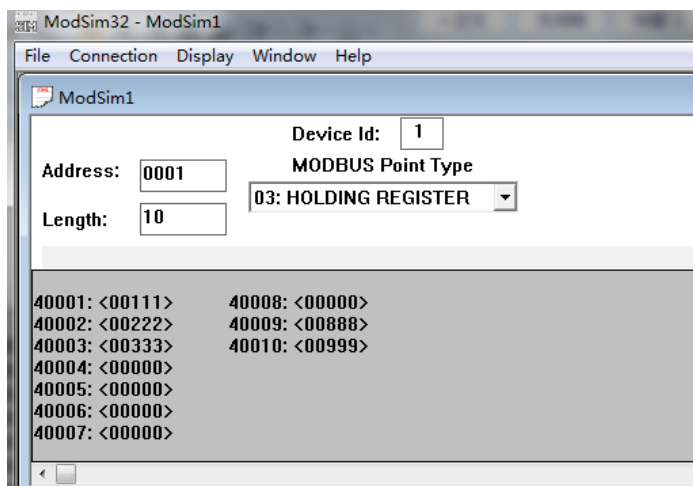
点击Commands, 配置主站命令, 使用功能码FC3读取MODBUS RTU 1号从站地址的设备，读取MODBUS地址40001至40010这10个INT(16位) 数据放到模块0至9里面。

Enable	Modbus Function	Slave Address	Modbus Data Address	Quantity	Data Swap	Poll Interval	Internal Data Address	Desc
☐ Yes	FC 3 - Read Holding Registers(4X)	1	0	10	No Change	0	0	

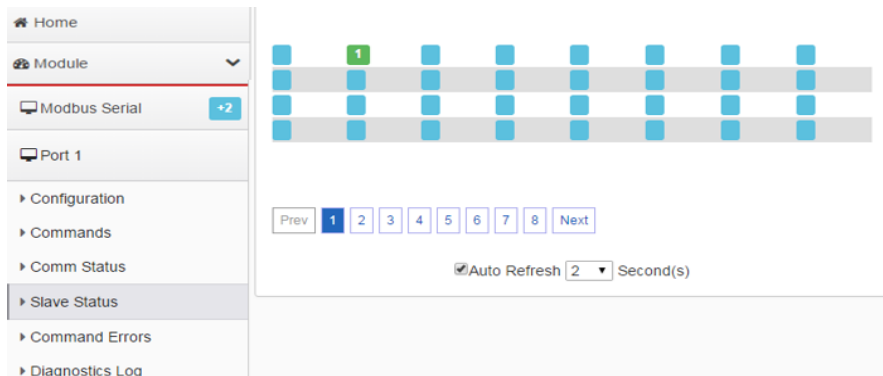
打开MODBUS RTU从站仿真软件 MODSIM 32选择电脑COM2串口。



点击连接，然后在40001至40010里面录入一些数据。



检查从站状态。

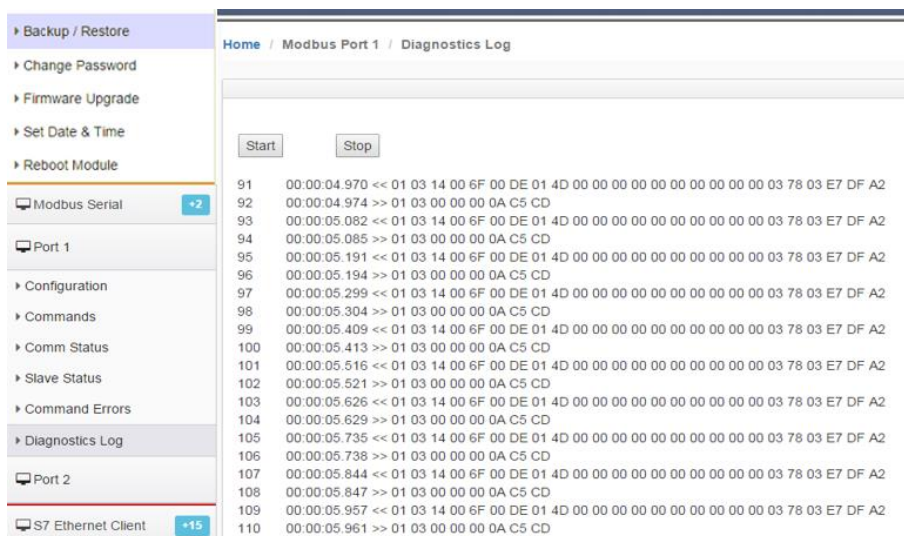


如果是1号从站是绿色，表示命令生效，1号从站连接成功，如果1号从站是红色，表示命令失败，检查 Command Errors的错误信息。

接着检查MODBUS RTU报文，点击Diagnostics Log，点击Start. 会出现发送报文，接收报文。

>>表示发送的报文

<<表示接受的报文

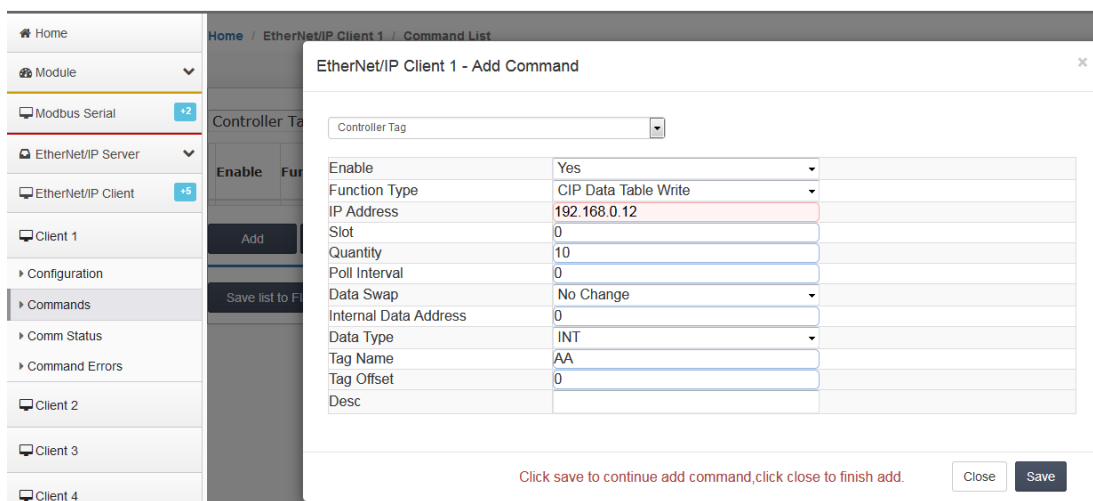


检查网关内部数据库数据情况，可以看到模块作为MODBUS RTU主站读取到了从站的数据

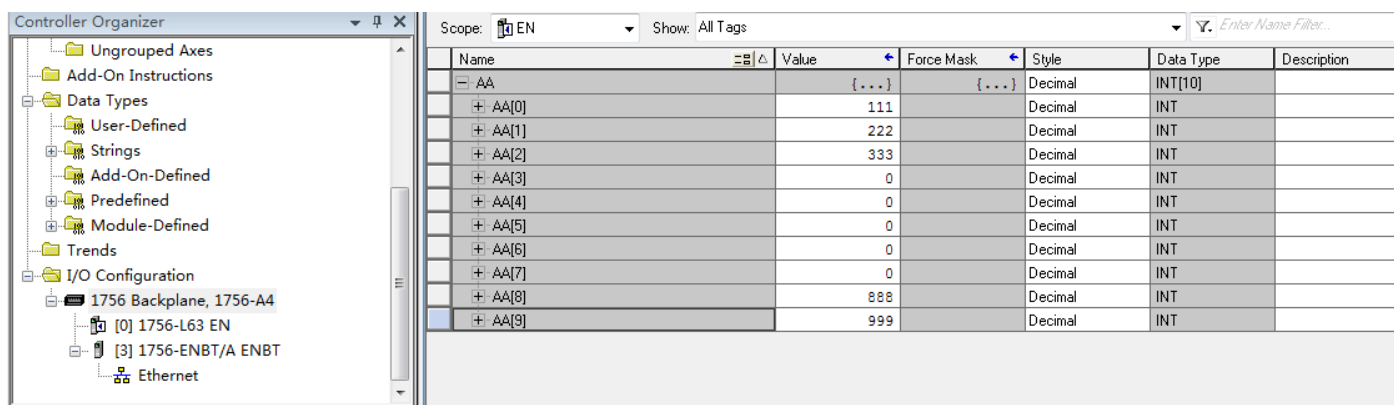
Address	0	1	2	3	4	5	6	7	8	9
0	111	222	333	0	0	0	0	0	888	999
10	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0
50	0	0	0	0	0	0	0	0	0	0
60	0	0	0	0	0	0	0	0	0	0
70	0	0	0	0	0	0	0	0	0	0
80	0	0	0	0	0	0	0	0	0	0
90	0	0	0	0	0	0	0	0	0	0

在模块中配置EtherNet/IP 主站命令

命令含义是把内部数据库0-9这10个INT的整型数, 写到IP地址为192.168.0.12的Logix5000 PLC里面, PLC程序内的标签名为AA的数组。

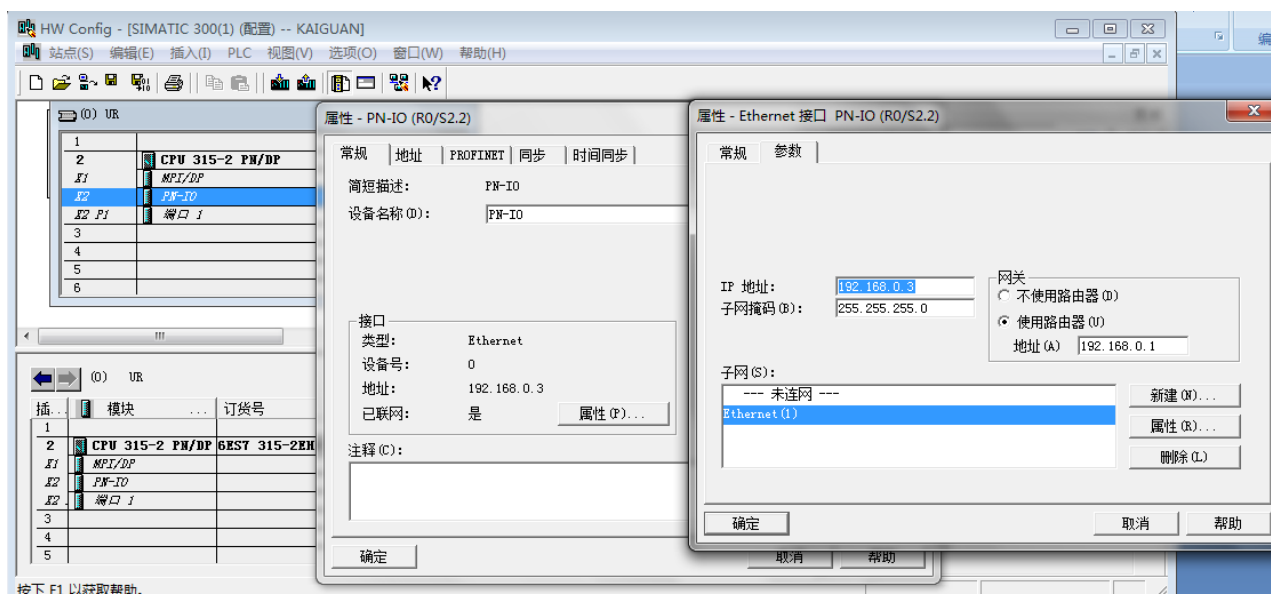


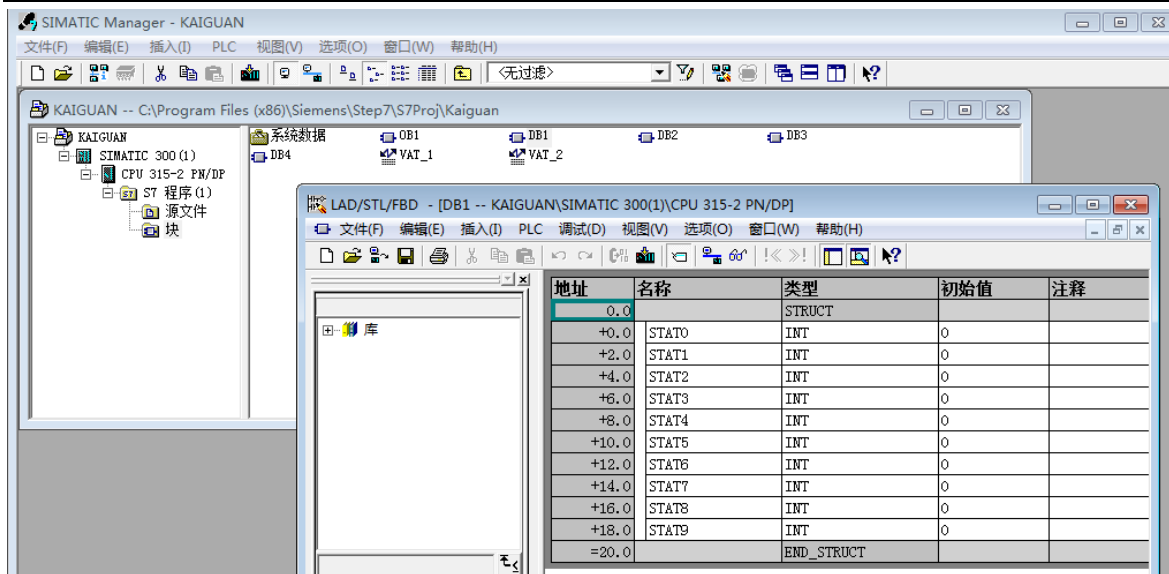
修改完后重启网关。可以在AB PLC中看到数据已经写入。



在模块中配置S7 Ethernet主站命令

首先查看西门子PLC硬件配置和要放到的DB块, 目的是要把MODBUS RTU采集到的数据放到西门子DB1里面。





建立一条 S7 以太网指令，命令的要注意的地方，Slot 是指西门子 CPU 的槽位，Address 是指 DB 数据的起始地址，Quantity 是指要传输几个数据，Data Swap 是指传输的数据是否进行高低位交换，Internal Data Address 是指读到的数据存放在模块内部寄存器起始地址。

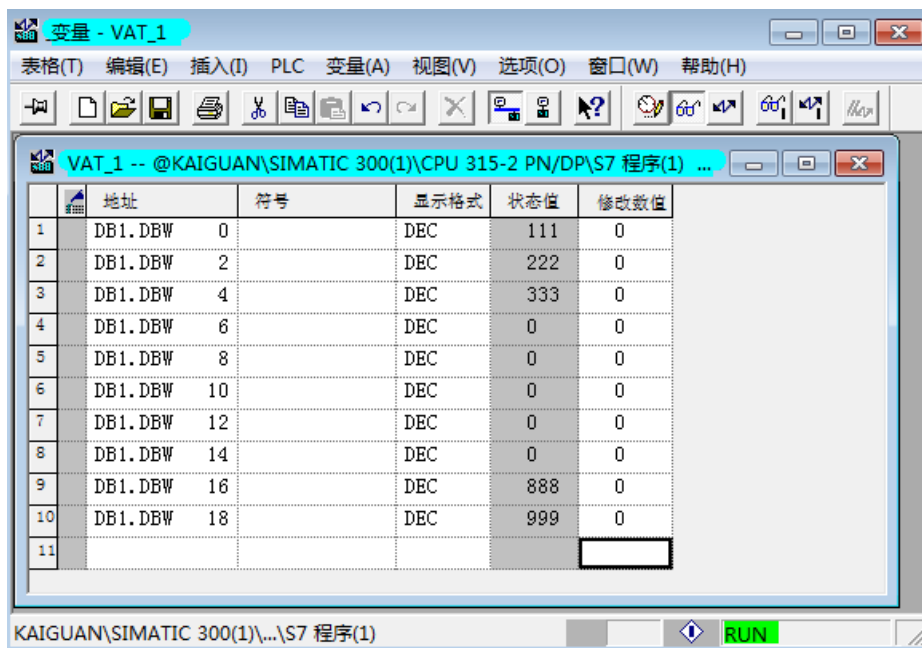
以下指令表示将从模块内部数据区地址0开始的连续10个整型数，写入到IP地址为192.168.0.3的西门子PLC，PLC内部的DB1的最开始的20个字节中，之后点击保存，重启模块。

S7 Ethernet Client 1 - Modify Command ✕

Enable	Yes
Function Type	Write
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	INT
Address Type	Data Block (DB)
DB Number	1
Address	0
Quantity	10
Data Swap	No Change
Poll Interval	0
Internal Data Address	0
Desc	

Close Save

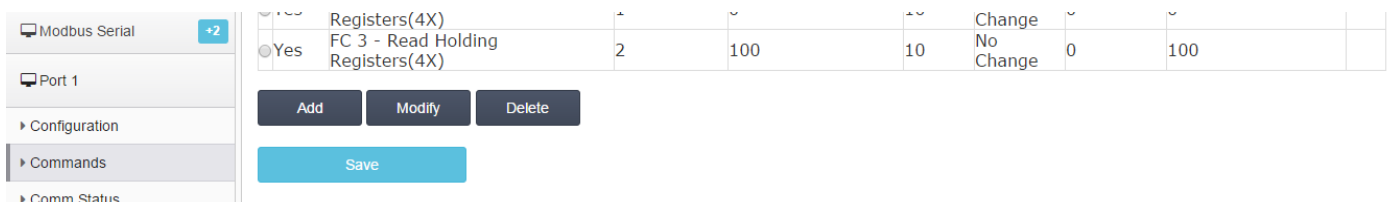
检查西门子DB1标签值



这里可以看到模块作为MODBUS RTU主站采集到的数据，写给了西门子PLC里面的DB1块中。

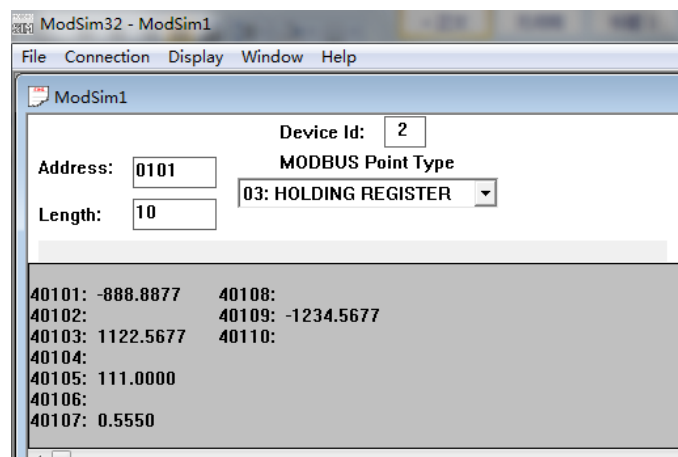
举例 2. 罗克韦尔 PLC 采集 Modbus RTU 从站数据

本案例中，模块EtherNet/IP配置为Client，Modbus RTU串口配置为Master



在模块内配置Modbus主站指令，如上图。命令含义，采集MODBUS RTU 串口2号从站的数据，从40101开始到40110这10个地址的 5个32位浮点数放到模块内部寄存器地址100开始到109里面。

下图截图为仿真软件Modsim作为MODBUS RTU从站，从40101开始到40110这10个地址中有 5个32位浮点数



再为模块配置EtherNet/IP主站一侧的命令

以下截图命令含义把模块内部寄存器100开始的5个32位浮点数数据，写入到Logix PLC标签为BB数组里面

EtherNet/IP Client 1 - Add Command

Controller Tag ▼

Enable	Yes
Function Type	CIP Data Table Write
IP Address	192.168.0.12
Slot	0
Quantity	5
Poll Interval	0
Data Swap	No Change
Internal Data Address	100
Data Type	REAL
Tag Name	BB
Tag Offset	0
Desc	

Click save to continue add command,click close to finish add.

Close Save

保存命令，重启模块。

检查Logix PLC一侧浮点数情况，可以在下图中看到5个浮点数已经写入到PLC的BB数组里面。

1756 Backplane, 1756-A4

[0] 1756-L63 EN

[3] 1756-ENBT/A ENBT

Ethernet

Size	4
------	---

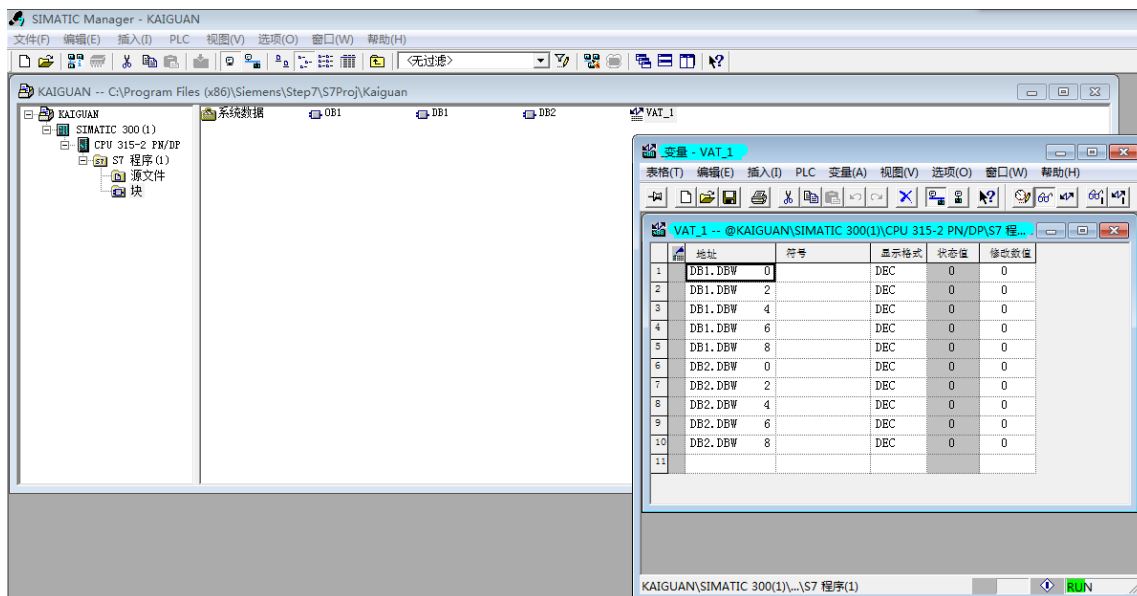
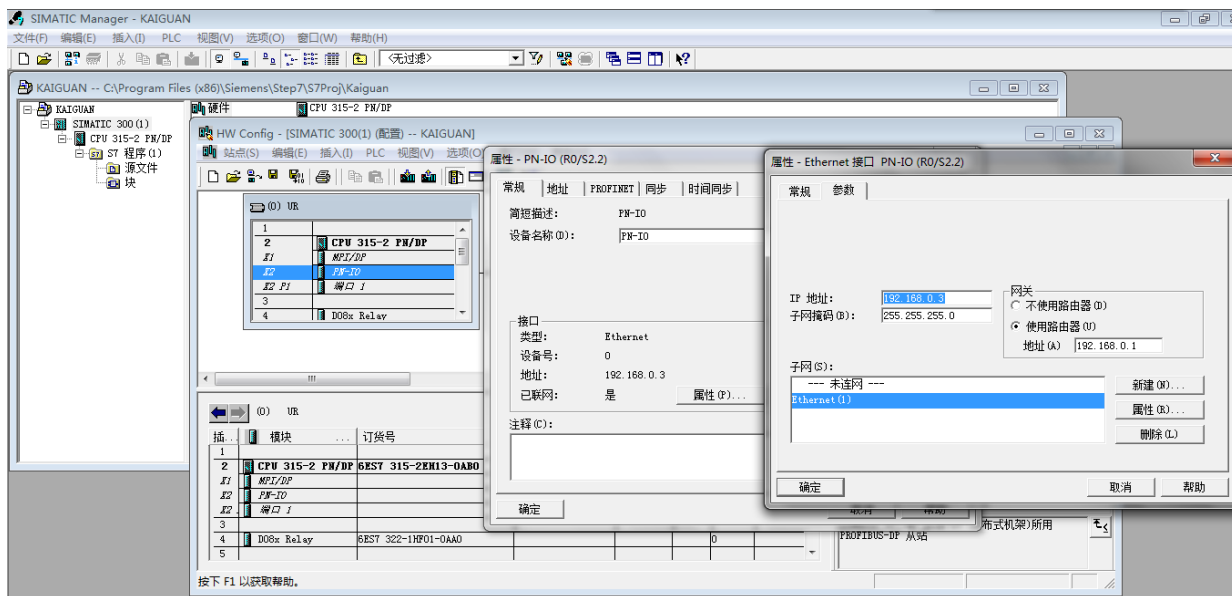
+	AA[8]	888		Decimal	INT
+	AA[9]	999		Decimal	INT
-	BB	{...}	{...}	Float	REAL[5]
-	BB[0]	-888.8877		Float	REAL
-	BB[1]	1122.5677		Float	REAL
-	BB[2]	111.0		Float	REAL
-	BB[3]	0.555		Float	REAL
-	BB[4]	-1234.5677		Float	REAL

举例 3 罗克韦尔 1756PLC 和西门子 PLC 315-2DP/PN 通讯

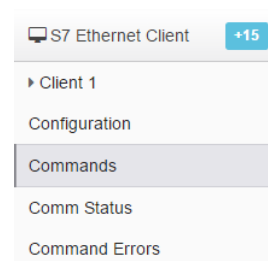
本案例中配置模块做 EtherNet/IP server，做 S7 以太网 client

西门子多个 DB 块的数据可以被读取，本例以 DB1 和 DB2 为例。每个 DB 块包含 5 个数据，由模块进行读取。

西门子 PLC 内部配置如下：



之后在模块中选择S7 Ethernet Client这里做配置,点击S7-Ethernet Client-Commands 建立两条读指令



S7 Ethernet Client 1 - Add Command
✕

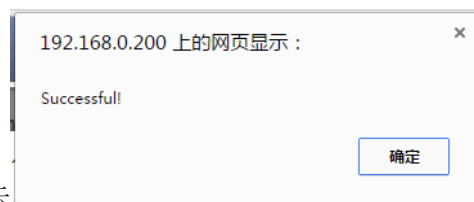
Enable	Yes
Function Type	Read
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	INT
Address Type	Data Block (DB)
DB Number	1
Address	0
Quantity	5
Data Swap	No Change
Poll Interval	0
Internal Data Address	0
Desc	

Click save to continue add command,click close to finish add.

Close
Save

第一条命令的要注意的地方，Slot 是指西门子 CPU 的槽位，Address 是指 DB 数据的起始地址，Quantity 是指要传输几个数据，Data Swap 是指传输的数据是否进行高低位交换，Internal Data Address 是指读到的数据存放在模块内部寄存器起始地址。

第一条命令的含义是模块读取 IP 地址为 192.168.0.3 的西门子 PLC DB1 内的前 5 个 INT 字，存入模块内部寄存器地址 0-4，总共 5 个寄存器里面。



点击 Save 保存，提示

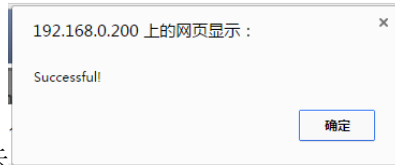
S7 Ethernet Client 1 - Add Command
✕

Enable	Yes
Function Type	Read
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	INT
Address Type	Data Block (DB)
DB Number	2
Address	0
Quantity	5
Data Swap	No Change
Poll Interval	0
Internal Data Address	5
Desc	

Click save to continue add command,click close to finish add.

Close
Save

第二条命令的含义是模块读取 IP 地址为 192.168.0.3 的西门子 PLC DB2 内的前 5 个字，存入模块内部寄存器地址 5-9，总共 5 个寄存器里面。



点击 Save 保存，提示，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。

Home / S7 Ethernet Client 1 / Command List

Enable	Function Type	IP Address	PLC Type	Rack	Slot	TSAP	Data Type	Address Type	DB Number	Address	Quantity	Poll Interval	Data Swap	Internal Data Address	Desc
☒ Yes	Read	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	1	0	5	0	No Change	0	
☒ Yes	Read	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	2	0	5	0	No Change	5	

Add Modify Delete

Save list to Flash

Home / Reboot

Warning

The module has to be rebooted due to any configuration changes. Note that the data communication will be temporarily interrupted if reboot.

OK to reboot the module now?

OK

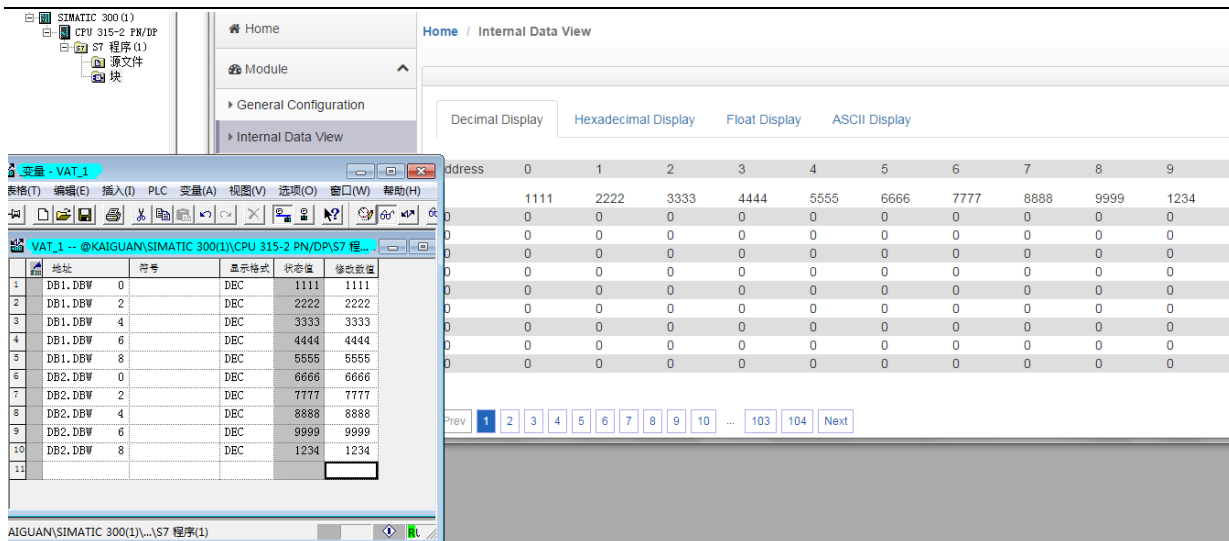
提示重启模块，点击 OK 完成重启。

Home / Reboot

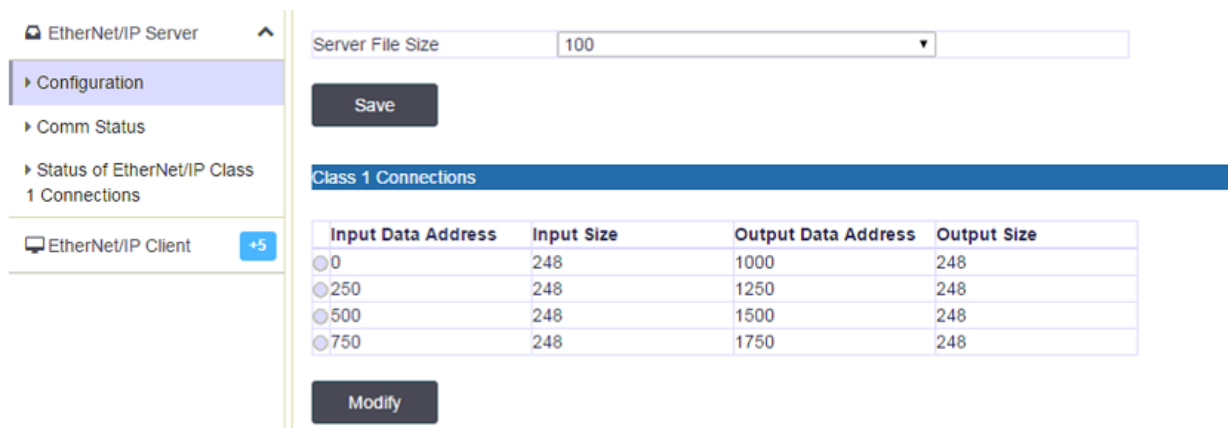
Warning

Rebooting will be completed in 16 seconds, please go to [homepage](#) after reboot.

在西门子 PLC 变量表里面写入一些数据，可以看到模块寄存器 0-9 总共 10 个寄存器显示有数据被读取到。



配置模块做 EtherNet/IP Class 1 Server 从站，根据下图分配输入输出寄存器区域

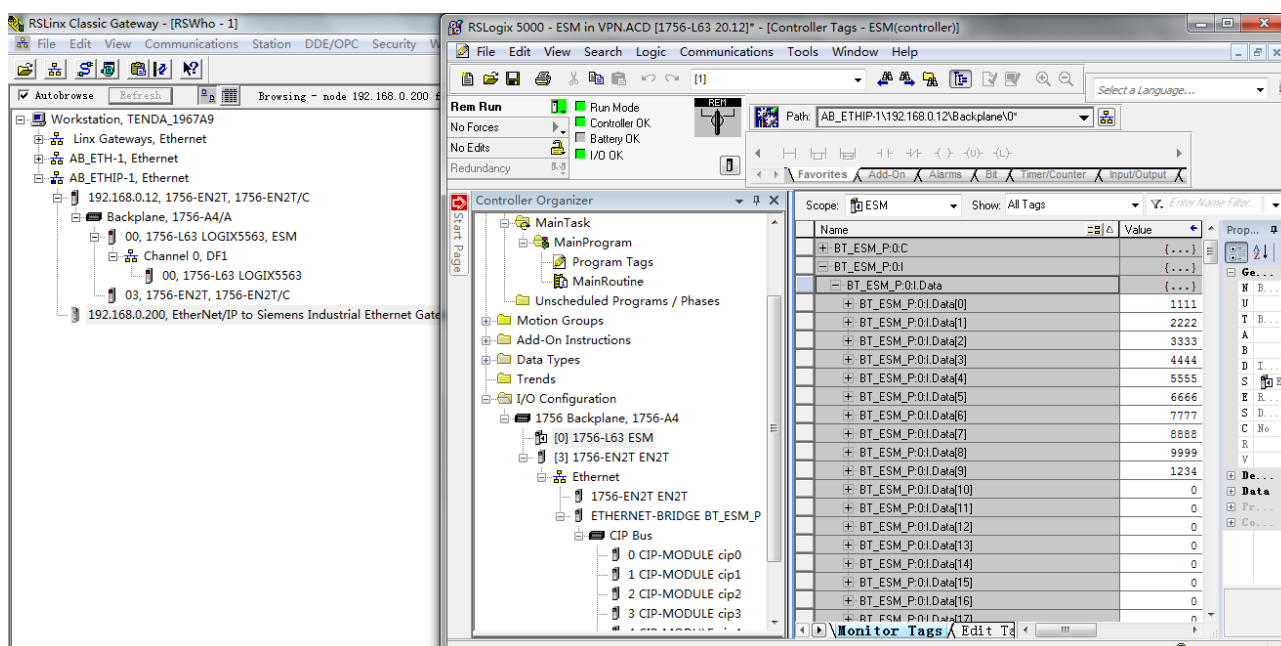


在 Logix50000 内建立 CIP 输入输出数组，具体内容请见前文“配置模块做 EtherNet/IP server”对应关系如下

PLC 输入数据标签组

- BT_ESM_P:0:I.Data[0]– [247]对应模块内部寄存器地址 0–247，
- BT_ESM_P:1:I.Data[0] –[247]对应模块内部寄存器地址 250–497
- BT_ESM_P:0:O.Data[0] –[247]对应模块内部寄存器地址 1000–1247，
- BT_ESM_P:1:O.Data[0] –[247]对应模块内部寄存器地址 1250–1497

配置完成后，可以看到 PLC 内的输入标签组 BT_ESM_P:0:I 有数据从模块传输过来，与之前在西门子 PLC 内部键入的数据一致。



举例 4. 罗克韦尔 1756PLC 和西门子 PLC 315-2DP/PN 通讯

本案例中配置模块做 EtherNet/IP Client，做 S7 以太网 client

模块可以同时做 EtherNet/IP Client 和 server，所以这种方式无需修改 PLC 原有配置，适用于改造项目中不停机传输数据。

首先在罗克韦尔 PLC 程序内建立一个标签“S7_READ”，包含 10 个 INT 数据

S7_READ			INT[10]
+ S7_READ[0]			INT
+ S7_READ[1]			INT
+ S7_READ[2]			INT
+ S7_READ[3]			INT
+ S7_READ[4]			INT
+ S7_READ[5]			INT
+ S7_READ[6]			INT
+ S7_READ[7]			INT
+ S7_READ[8]			INT
+ S7_READ[9]			INT

再配置模块 EtherNet/IP Client---Client 1---Commands，含义为从模块内部数据区 0 开头的 10 个连续数据写给罗克韦尔 PLC 标签“S7_READ”，写入的区域起始地址为“S7_READ[0]”

EtherNet/IP Client 1 - Add Command



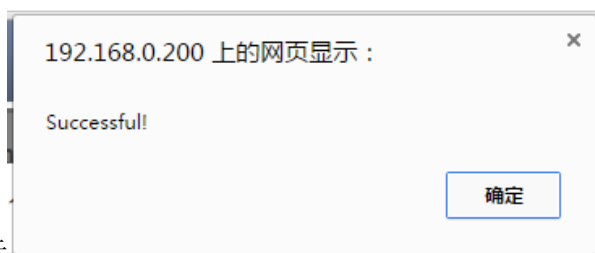
Controller Tag ▼

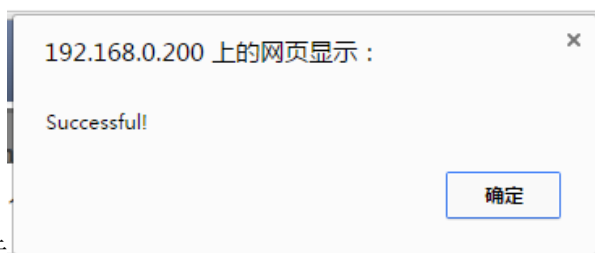
Enable	Yes ▼
Function Type	CIP Data Table Write ▼
IP Address	192.168.0.12
Slot	0
Quantity	10
Poll Interval	0
Data Swap	No Change ▼
Internal Data Address	0
Data Type	INT ▼
Tag Name	S7_READ
Tag Offset	0
Desc	

Click save to continue add command,click close to finish add.

Close

Save



点击 Save，提示 ，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。同时仍然继续使用上一个案例中配置完成的两条 S7 以太网主站的指令，如下图。

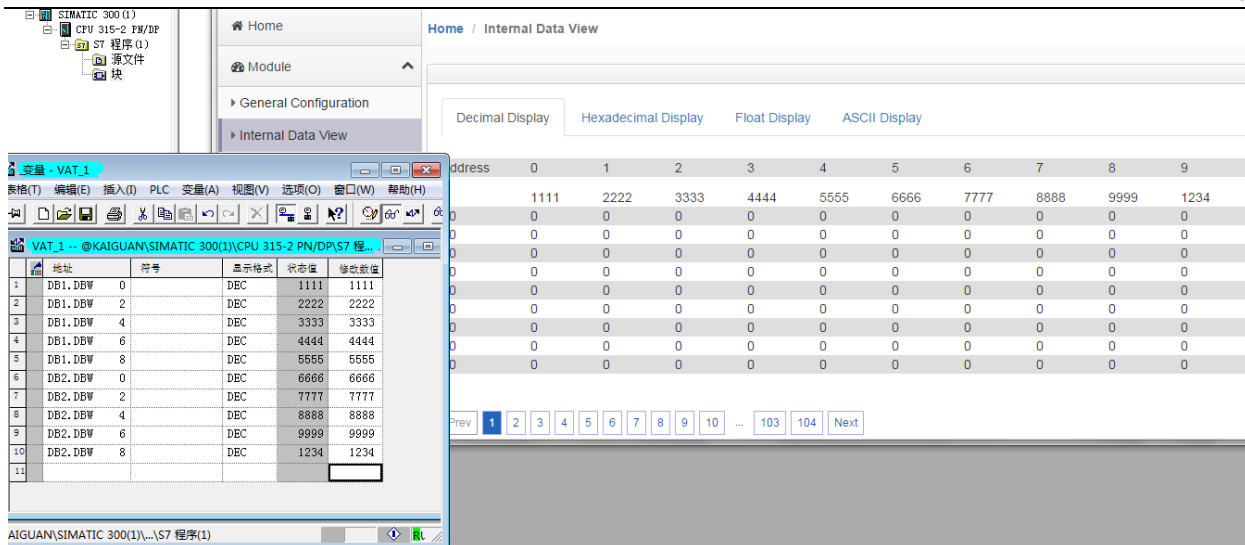
Home / S7 Ethernet Client 1 / Command List

Enable	Function Type	IP Address	PLC Type	Rack	Slot	TSAP	Data Type	Address Type	DB Number	Address	Quantity	Poll Interval	Data Swap	Internal Data Address	Desc
☒ Yes	Read	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	1	0	5	0	No Change	0	
☒ Yes	Read	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	2	0	5	0	No Change	5	

Add
Modify
Delete

Save list to Flash

前文中介绍了，模块配置好的 S7 以太网指令，已经将西门子 PLC 变量已经读取到了模块内部数据 0-9，可以看到模块寄存器地址 0-9 总共 10 个寄存器显示有数据被读入。



再查看罗克韦尔 PLC 建立的标签，可以看到数据从模块写入进来，与之前西门子 PLC 键入数据一致。

S7_READ	{...}	{...}	Decimal	INT[10]
+ S7_READ[0]	1111		Decimal	INT
+ S7_READ[1]	2222		Decimal	INT
+ S7_READ[2]	3333		Decimal	INT
+ S7_READ[3]	4444		Decimal	INT
+ S7_READ[4]	5555		Decimal	INT
+ S7_READ[5]	6666		Decimal	INT
+ S7_READ[6]	7777		Decimal	INT
+ S7_READ[7]	8888		Decimal	INT
+ S7_READ[8]	9999		Decimal	INT
+ S7_READ[9]	1234		Decimal	INT

附录 1. 模块支持读写西门子 PLC 的数据类型

S7-300/S7-400支持的数据类型

地址类型 S7-300/S7-400	功能	数据类型
DB	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT

	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Timer	READ	TIME
Counter	READ	Count
Flag	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Input	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Output	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT

	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT

S7-200支持的数据类型

地址类型 S7-200	功能	数据类型
DB	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
Flag	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
Input	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT

	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
Output	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT

S7-1200 S7-1500支持的数据类型

地址类型 S7-1200	功能	数据类型
DB	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Flag	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL

	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Input	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Output	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT

S7-300/S7-400 最大支持点数

S7-300/S7-400	功能	数据类型	最大数量	最大数量
DB	READ	BOOL	16	
	Write	BOOL		8
	READ	BYTE	164	
	Write	BYTE		164
	READ	DINT	41	
	Write	DINT		41
	READ	REAL	41	
	Write	REAL		41
	READ	INT	82	
	Write	INT		82
	READ	TIME	82	
	Write	TIME		41
	READ	COUNT	82	
	Write	COUNT		82
Timer	READ	TIME	1	
Counter	READ	Count	111	
Flag	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	222	
	Write	BYTE		212
	READ	DINT	55	
	Write	DINT		53
	READ	REAL	55	
	Write	REAL		53
	READ	INT	111	
	Write	INT		106
	READ	TIME	111	
	Write	TIME		53
	READ	Count	111	
	Write	Count		106
Flag	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	222	
	Write	BYTE		212
	READ	DINT	55	
	Write	DINT		53
	READ	REAL	55	
	Write	REAL		53
	READ	INT	111	
	Write	INT		106

	READ	TIME	111	
	Write	TIME		53
	READ	Count	111	
	Write	Count		106
Input	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	128	
	Write	BYTE		128
	READ	DINT	32	
	Write	DINT		32
	READ	REAL	32	
	Write	REAL		32
	READ	INT	64	
	Write	INT		64
	READ	TIME	64	
	Write	TIME		32
	READ	Count	64	
	Write	Count		64

S7-1200 S7-1500 最大支持点数

S7-1200/S7-1500	功能	数据类型	最大数量	最大数量
DB	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	30	
	Write	BYTE		30
	READ	DINT	7	
	Write	DINT		7
	READ	REAL	7	
	Write	REAL		7
	READ	INT	15	
	Write	INT		15
	READ	TIME	15	
	Write	TIME		15
	READ	COUNT	15	
	Write	COUNT		15
Flag	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	212	
	Write	BYTE		212
	READ	DINT	53	
	Write	DINT		53

	READ	REAL	53	
	Write	REAL		53
	READ	INT	106	
	Write	INT		106
	READ	TIME	105	
	Write	TIME		105
	READ	Count	106	
	Write	Count		106
Output	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	212	
	Write	BYTE		212
	READ	DINT	53	
	Write	DINT		53
	READ	REAL	53	
	Write	REAL		53
	READ	INT	106	
	Write	INT		106
	READ	TIME	105	
	Write	TIME		105
	READ	Count	111	
	Write	Count		106
Input	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	222	
	Write	BYTE		212
	READ	DINT	55	
	Write	DINT		53
	READ	REAL	55	
	Write	REAL		53
	READ	INT	111	
	Write	INT		111
	READ	TIME	111	
	Write	TIME		106
	READ	Count	111	
	Write	Count		106

S7-200 最大支持点数

S7-200	功能	数据类型	最大数量	最大数量
DB	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	222	

	Write	BYTE		212
	READ	DINT	55	
	Write	DINT		53
	READ	REAL	55	
	Write	REAL		53
	READ	INT	111	
	Write	INT		106
Flag	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	32	
	Write	BYTE		32
	READ	DINT	8	
	Write	DINT		8
	READ	REAL	8	
	Write	REAL		8
	READ	INT	16	
	Write	INT		16
Output	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	16	
	Write	BYTE		16
	READ	DINT	4	
	Write	DINT		4
	READ	REAL	4	
	Write	REAL		4
	READ	INT	8	
	Write	INT		8
Input	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	16	
	Write	BYTE		16
	READ	DINT	4	
	Write	DINT		4
	READ	REAL	4	
	Write	REAL		4
	READ	INT	8	
	Write	INT		8

联系我们

如果在使用过程中有更多的问题，可以通过以下方式联系我们获得支持。

联系电话 (中国大陆)	13910136425, 15910883727
技术支持	support@beacongt.com
亚太区销售	asia@beacongt.com
北美区销售	usa@beacongt.com
微信公众平台	
网址	http://www.beaconglobaltech.com