

配置西门子S7工业以太网协议 Client（主站）

点击 S7 Ethernet Client,可以看到模块可支持做主站的数量，+15表示可以该模块最多作为15个主站。

点开Configuration.查看默认的配置

S7 Ethernet Client+15

Client 1

Configuration

Commands

Comm Status

Command Errors

Home / S7 Ethernet Client 1 / Configuration

Minimum Command Delay

50

Response Timeout

1000

Retry Count

3

Save

Minimum Command Delay ：每个Client执行发出Client下面建立的指令的轮询时间 单位ms 0-65535

（注：该时间越小,**模块发送命令越快，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，建议根据需要修改成500-1000ms。）**

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

Retry Count：重新尝试连接次数

点击S7 Ethernet Client ---Client1 ---Commands，如果没有出现Add等按钮，应该没有点击右上角登录或者没有使用正确的浏览器导致。

S7 Ethernet Client+15

Client 1

Configuration

Commands

Comm Status

Command Errors

Home / S7 Ethernet Client 1 / Command List

Enable	Function Type	IP Address	PLC Address Type	Rack	Slot	TSAP	Data Type	Address Type	DB Number	Address	Quantity	Poll Interval	Data Swap	Internal Data Address	Cmd Errors Mapping Enabled	Cmd Errors Mapping Address	Cmd Pause on PLC STOP Enabled	PLC STATUS Data Mapping Address	Desc
--------	---------------	------------	------------------	------	------	------	-----------	--------------	-----------	---------	----------	---------------	-----------	-----------------------	----------------------------	----------------------------	-------------------------------	---------------------------------	------

AddModifyDelete

Save list to Flash

配置命令参数，用来读或写西门子PLC的命令。每个主站最大指令数为32个，如果同时连接5个西门子PLC，建议在Client1-Client5配置每个主站分别对应一个西门子PLC的读写。可以减小命令执行延时，以及设备掉线对其他设备的干扰。

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，主要分为两大类：

Enable	Yes	使能，禁止，内部寄存器有变化后写
Function Type	Read	功能码 读或者写
IP Address	1.1.1.1	所连接西门子PLC或者驱动器的以太网地址
PLC Type	S7-300/S7-400/S7-1200/S7-1500/Drive	西门子PLC类型
Rack	0	CPU机架号
Slot	1	CPU槽位
Data Type	BYTE	数据类型
Address Type	Data Block (DB)	地址类型
DB Number	1	DB号，如果地址类型不是DB块,此项失效。
Address	0	数据实际起始地址
Quantity	1	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	0	模块内部寄存器，存放数据的起始地址
Cmd Errors Mapping Enabled	No	命令错误状态位反馈开启
Cmd Errors Mapping Address	0	命令错误状态位反馈地址，模块内部寄存器任意位置
Enable Pause Command when PLC STOP	No	所连接PLC停止状态反馈开启
PLC STOP Status Mapping Address	0	所连接PLC停止状态反馈地址，模块内部寄存器任意位置
Desc		命令描述 英文或中文

西门子S7-300/S7-400/S7-1200/S7-1500/Drive这几种PLC设备采用上图来进行读或写的操作。

Enable	Yes	使能，禁止，内部寄存器有变化后写
Function Type	Read	功能码 读或者写
IP Address	1.1.1.1	所连接西门子PLC或者驱动器的以太网地址
PLC Type	S7-200/S7-200 SMART/LOGO	西门子PLC类型
TSAP	1000	Transport Service Access Point连接资源的地址
Data Type	BYTE	数据类型
Address Type	Data Block (DB)	地址类型
DB Number	1	DB号，如果地址类型不是DB块,此项失效。
Address	0	数据实际起始地址
Quantity	1	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	0	模块内部寄存器，存放数据的起始地址
Cmd Errors Mapping Enabled	No	命令错误状态位反馈开启
Cmd Errors Mapping Address	0	命令错误状态位反馈地址，模块内部寄存器任意位置
Enable Pause Command when PLC STOP	No	所连接PLC停止状态反馈开启
PLC STOP Status Mapping Address	0	所连接PLC停止状态反馈地址，模块内部寄存器任意位置
Desc		命令描述 英文或中文

西门子S7-200/S7-200 SMART/LOGO这几种PLC设备采用上图来进行读或写的操作

点击S7 Ethernet Client ---Client1 ---Comm Status，从这里可以查看整个Client发送和接受命令的状态，命令是否有错误。

S7 Ethernet Client +15

Home / S7 Ethernet Client 1 / Status

Client 1

Configuration

Commands

Comm Status

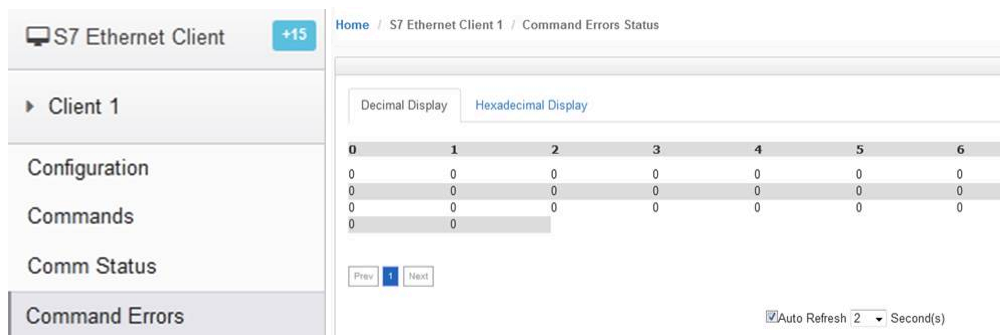
Command Errors

Parameter Name	Value
Command Count	2
Last Error Code	0
Number of Command Errors	0
Number of Requests Sent	279
Number of Responses Received	279
Number of Errors Received	0
Number of Errors Sent	0

Reset Counter

Auto Refresh 2 Second(s)

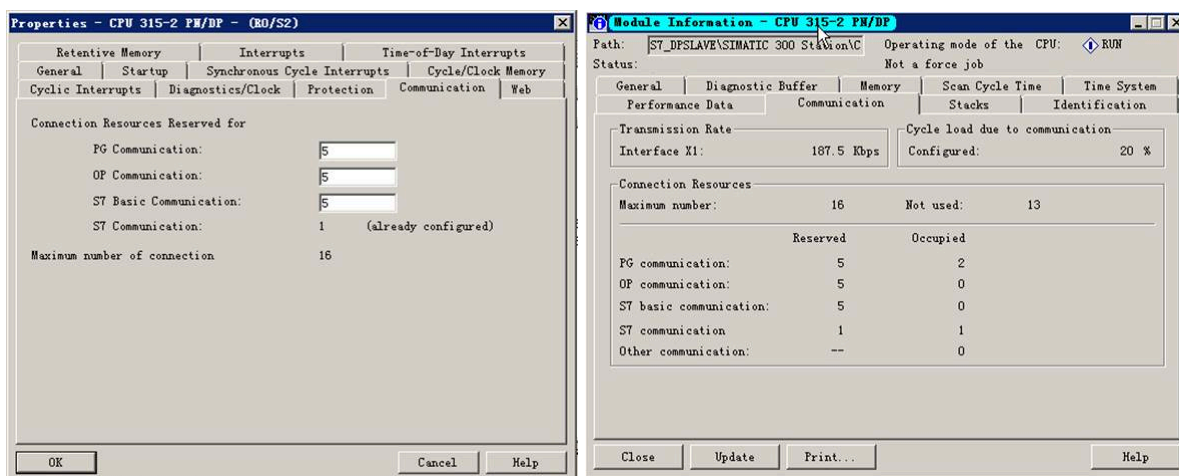
点击S7 Ethernet Client ---Client1 --- Command Errors，从这里可以查看整个Client所建立的第几个命令有错误。



连接西门子PLC注意事项

—特别使用冗余PLC系统和模块进行通讯时

S7-300/400 注意事项： 西门子CPU硬件配置页面里面有最大通讯连接数，以CPU 315-2 PN/DP为例，该CPU模块具有最大16个连接数，我们可以看到S7通讯连接数已经有一个在使用，模块一个Clnet 连接西门子CPU以太网会占用1个S7的连接数。

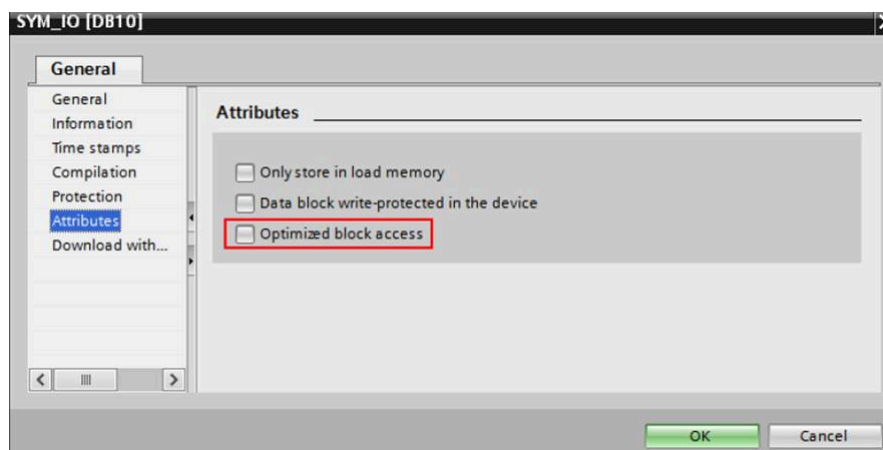


S7-1200/1500 注意事项：

- 1.只能访问全局DB。
- 2.优化的块访问必须关闭。
- 3.访问级别必须为“完全”，并且“连接机制”必须允许GET / PUT。

在“程序块”下的左窗格中选择DB，然后按Alt-Enter（或在上下文菜单中选择“属性...”）

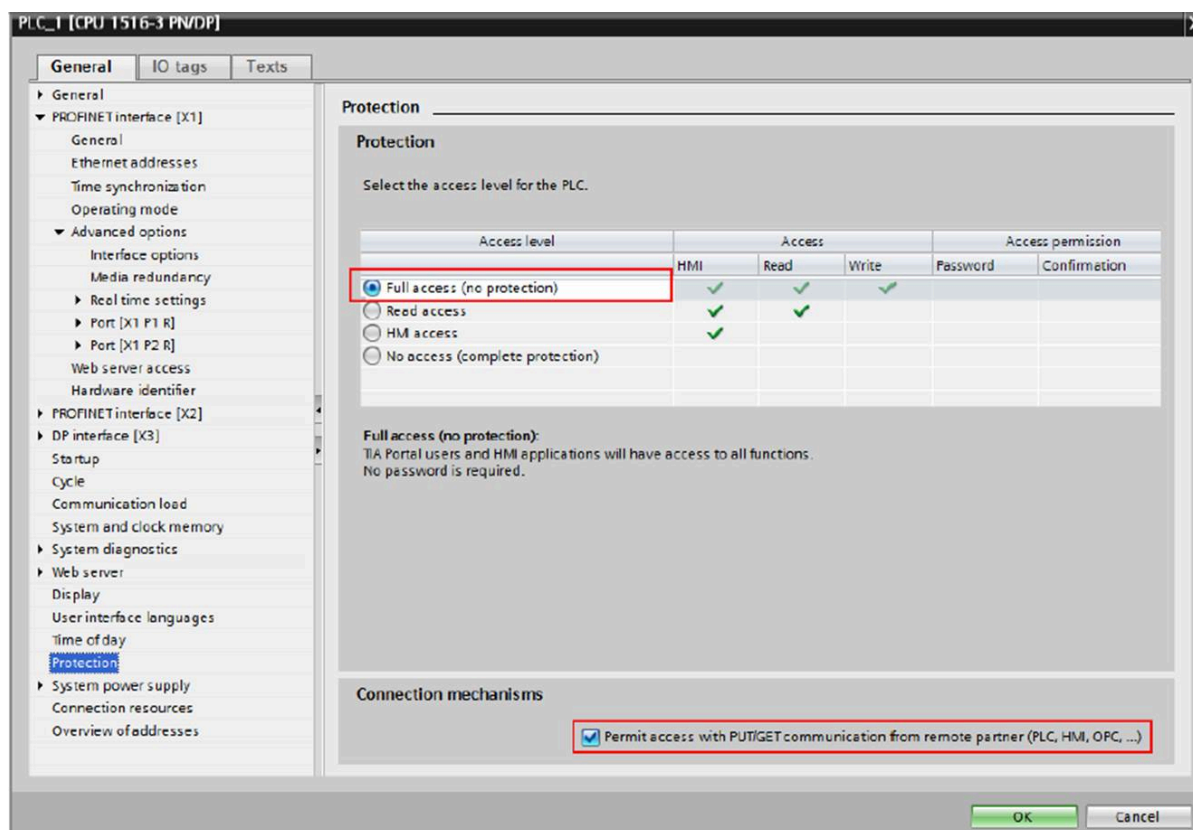
取消选中“优化阻止访问”，默认情况下已选中



Protection 相关内容:

在左窗格中选择CPU项目，然后按Alt-Enter（或在上下文菜单中选择“属性...”）

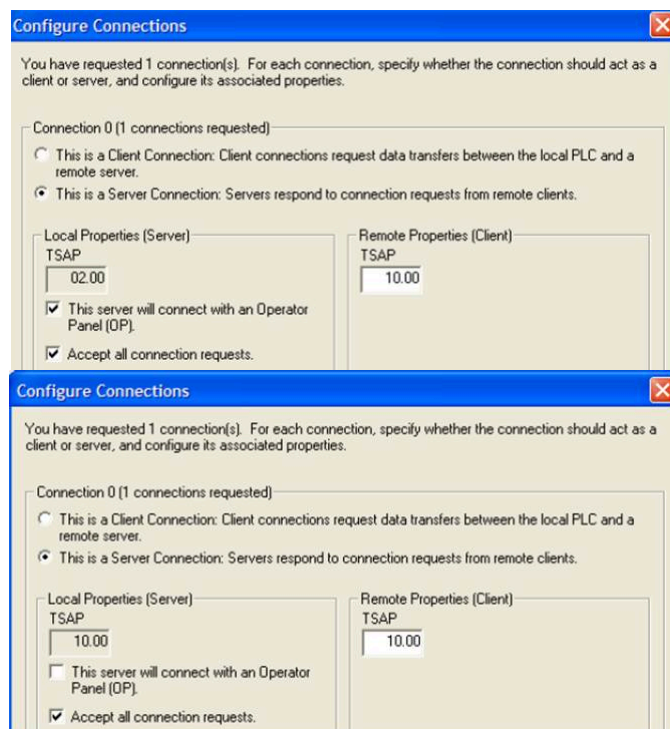
在保护项中，选择“完全访问”，然后选中“使用PUT / GET...允许访问”。如图。



S7-200/S7-200 SMART/LOGO注意事项:

模块建立命令要填写TSAP,这个TSAP是指S7-200/S7-200 SMART/LOGO本地的TSAP。

S7-200 举例，如果本地TSAP是02.00，模块建立命令时候TSAP就填写200，如果本地TSAP是10.00 模块建立命令时候TSAP就填写1000。

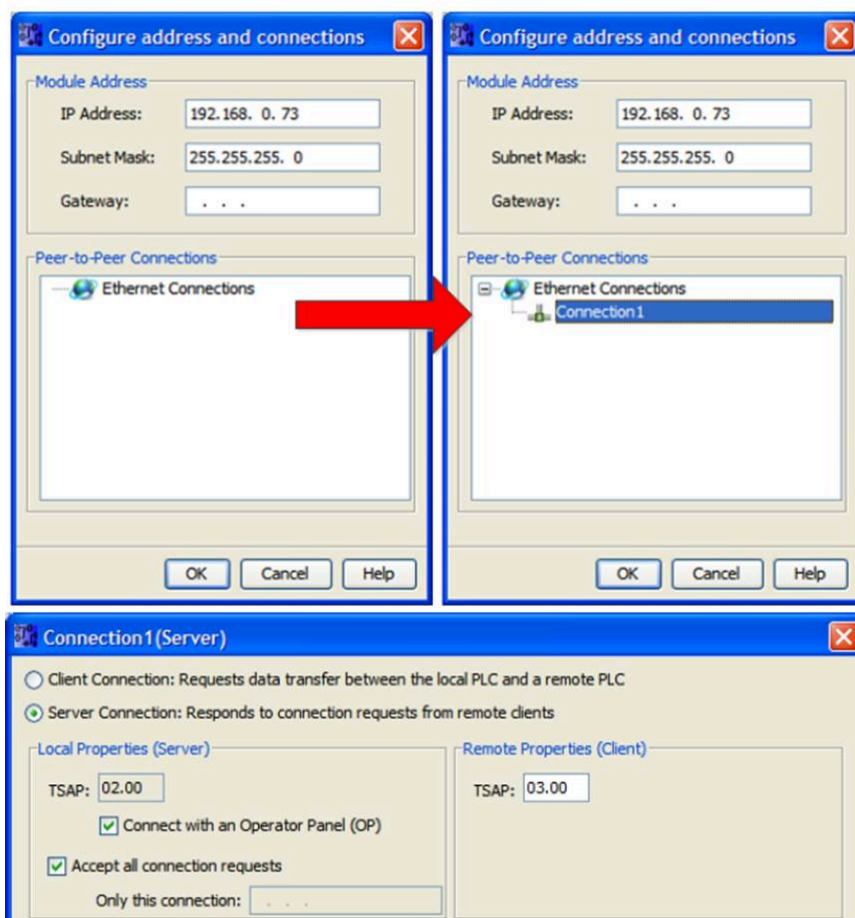


S7-200 SMART 举例，TSAP 端口号 0200，0201,0300,0301.这四个端口号都可以使用，可以任意选择一个端口号填写。

与S7-200 SMART连接有单独介绍模块各种数据类型相连接的方法。

LOGO**举例**

TSAP 端口号 0200，模块建立命令时候TSAP就填写200。



举例1，模块读取西门子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。

(0) UR

1

2

3

4

5

CPU 315-2 PN/DP

MPI/DP

PN-IO

Port 1

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/S7-1500/Drive
Rack	0
Slot	2
Data Type	INT
Address Type	Data Block (DB)
DB Number	1
Address	0
Quantity	5
Data Swap	Byte Swap
Poll Interval	0
Internal Data Address	0
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	50
Enable Pause Command when PLC STOP	Yes
PLC STOP Status Mapping Address	60
Desc	

CloseSave

以上读指令解释如下，

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5个INT读到模块内部数据寄存器地址0-4中，数据高字节和低字节交换

如果第一条命令发生错误后，错误状态存放在模块内部数据寄存器地址50中。

如果第一条命令检测到西门子CPU运行或停止，CPU的运行或停止状态存放在模块内部数据寄存器地址60中。

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。

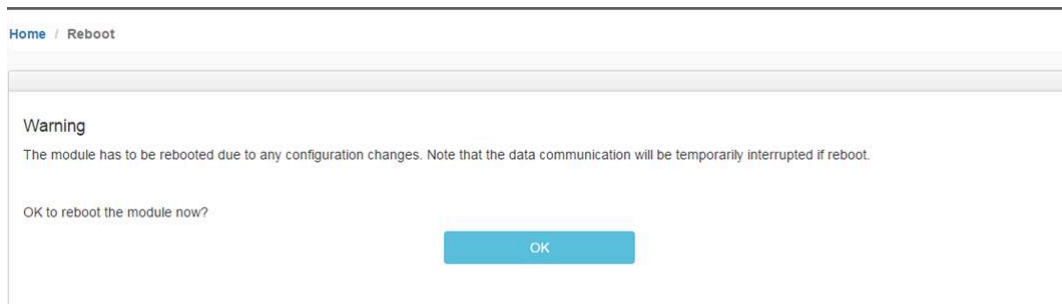
192.168.0.200 上的网页显示 :

Successfull

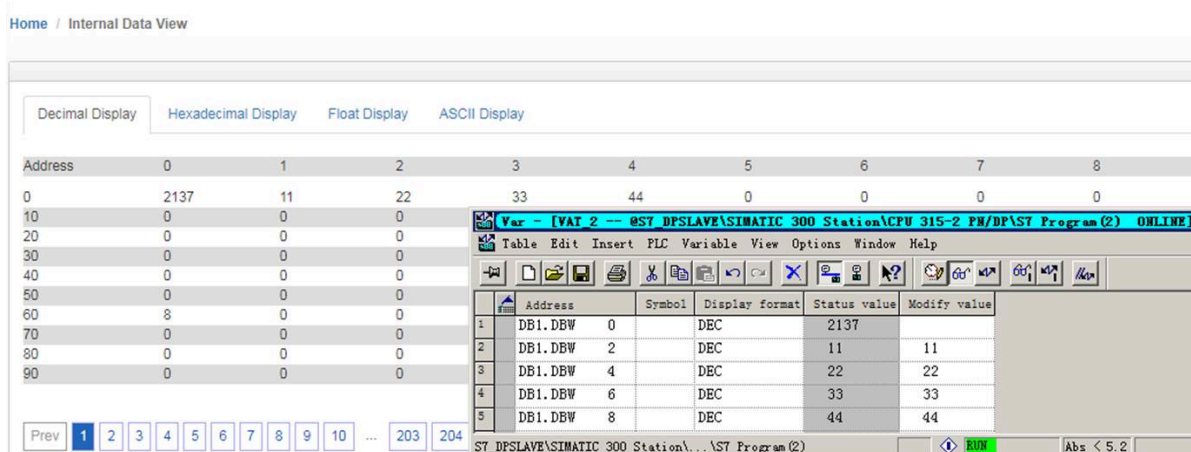
确定

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。

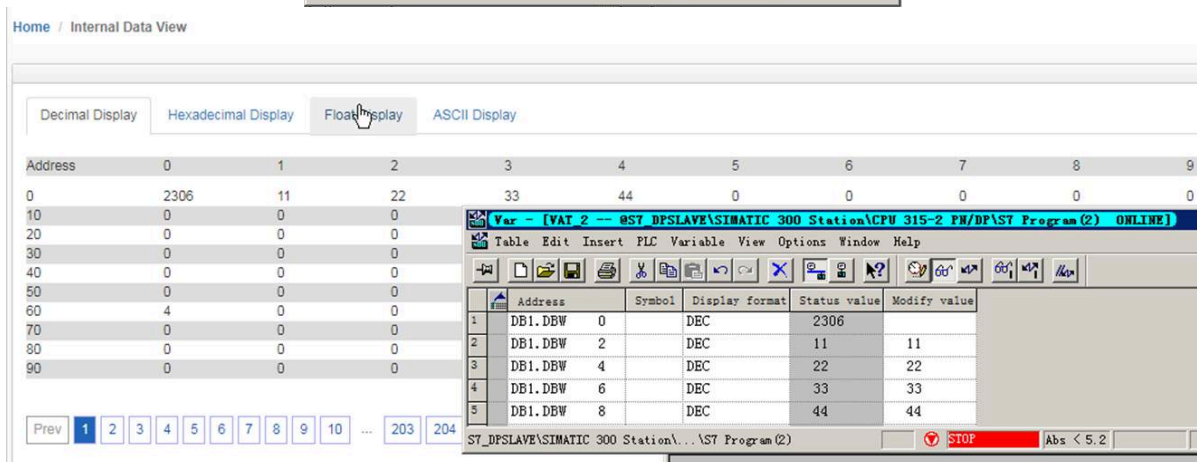
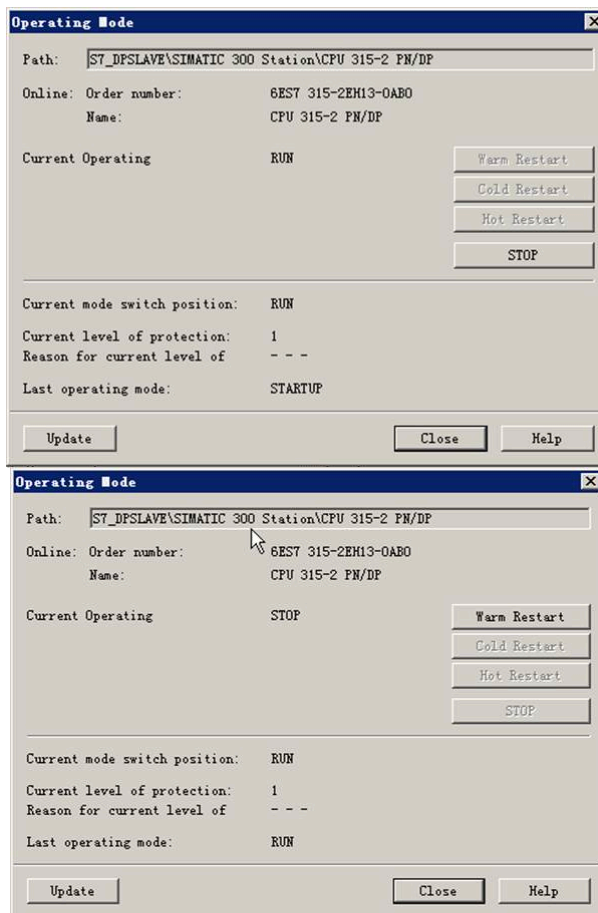


提示重启模块，点击OK 完成重启。



DB1.DBW0是一个加1循环的数值,该数值在一直加1，可以看到模块通过上文中的主站命令把西门子DB1里面5个INT格式的数据存放到了模块内部寄存器0-4里面，内部寄存器50是0 表示没有错误，内部寄存器60是8，（表示运行 注：西门子400冗余系统不使用此功能，请使用S7 Ethernet Server，后面章节会有介绍使用方法），表示西门子CPU在运行状态，错误状态和CPU运行状态可以开启或者关闭。用于设计人员取状态点使用。

把CPU从运行状态转换成停止状态，我们可以看一下这两边的数据关系。



当西门子CPU从运行转换成停止时，内部寄存器60的数值从8变成4，（表示西门子CPU停止状态）

如果内部寄存器50的数值是非零值 表示模块建立的命令没有正确读取到所有的数值，其中可能是IP地址错误，槽位错误，机架号错误，DB块不存在，数据长度没有对应等，这里不再一一讨论，非零值就表示命令错误。

举例2：模块和西门子PLC浮点数的读写

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。

Enable	Yes
Function Type	Read
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200/S7-1500/Drive
Rack	0
Slot	2
Data Type	REAL
Address Type	Data Block (DB)
DB Number	2
Address	0
Quantity	5
Data Swap	No Change
Poll Interval	0
Internal Data Address	20
Cmd Errors Mapping Enabled	No
Cmd Errors Mapping Address	0
Enable Pause Command when PLC STOP	No
PLC STOP Status Mapping Address	0
Desc	

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

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DB2数据块里面，从0地址开始的5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。因为模内部数据寄存器为16位的字，所以5个浮点数会占用10个寄存器，也就是存放到模块内部地址20-29中

本例中未使用指令执行状态查询和CPU运行状态查询的功能。

如下图，在西门子PLC中DB2.DB0-16中赋值

Var - [VAT 2 -- @S7-DPSLAWE\SIMATIC 300 Station\CPU 315-2 PN/DP\ST Program (2) ONLINE]					
	Address	Symbol	Display format	Status value	Modify value
1	DB2.DB0	0	FLOATING_POINT	192.344	192.344
2	DB2.DB0	4	FLOATING_POINT	-7.8	-7.8
3	DB2.DB0	8	FLOATING_POINT	111.0	111.0
4	DB2.DB0	12	FLOATING_POINT	-222.0	-222.0
5	DB2.DB0	16	FLOATING_POINT	1235.0	1235.0

可见模块内部数据区20-29的10个寄存器读取到了相同的数值。

Home / Internal Data View

Decimal Display

Hexadecimal Display

Float Display

ASCII Display

Address	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
20	22544	17216	-26214	-16135	0	17118	0	-15522	24576	17562
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

Prev

12345678910...102103Next

通过Modbus RTU为查看模块内部寄存器数值（注意，本例中使用Modbus作为举例，不同型号模块支持的驱动协议不同，具体配置模块时，可根据实际情况使用不同的驱动协议读写模块数据区）可见ModScan32的40021至40029读取到了相同的数值。

ModScan32 - ModScan

File Connection Setup View Window Help

Address: 0001 Device Id: 1 Number of Polls: 4
Length: 100 MODBUS Point Type Valid Slave Responses: 4
03: HOLDING REGISTER Reset Ctrs

40001: 0.0000	40010: 0.0000	40019: 0.0000	40028: 0.0000	40037: 0.0000	40046: 0.0000	40055: 0.0000	40064: 0.0000	40073: 0.0000
40002: 0.0000	40011: 0.0000	40020: 192.3440	40029: 1235.0000	40038: 0.0000	40047: 0.0000	40056: 0.0000	40065: 0.0000	40074: 0.0000
40003: 0.0000	40012: 0.0000	40021: 0.0000	40030: 0.0000	40039: 0.0000	40048: 0.0000	40057: 0.0000	40066: 0.0000	40075: 0.0000
40004: 0.0000	40013: 0.0000	40022: -7.8000	40031: 0.0000	40040: 0.0000	40049: 0.0000	40058: 0.0000	40067: 0.0000	40076: 0.0000
40005: 0.0000	40014: 0.0000	40023: 0.0000	40032: 0.0000	40041: 0.0000	40050: 0.0000	40059: 0.0000	40068: 0.0000	40077: 0.0000
40006: 0.0000	40015: 0.0000	40024: 0.0000	40033: 0.0000	40042: 0.0000	40051: 0.0000	40060: 0.0000	40069: 0.0000	40078: 0.0000
40007: 0.0000	40016: 0.0000	40025: 111.0000	40034: 0.0000	40043: 0.0000	40052: 0.0000	40061: 0.0000	40070: 0.0000	40079: 0.0000
40008: 0.0000	40017: 0.0000	40026: 0.0000	40035: 0.0000	40044: 0.0000	40053: 0.0000	40062: 0.0000	40071: 0.0000	40080: 0.0000
40009: 0.0000	40018: 0.0000	40027: -222.0000	40036: 0.0000	40045: 0.0000	40054: 0.0000	40063: 0.0000	40072: 0.0000	40081: 0.0000