|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TwinCAT 3 Modbus TCP使用方法**   |  |  | | --- | --- | |  | 作者：张连业  职务：华北区 技术工程师  邮箱：ly.zhang@beckhoff.com.cn  日期：2022-11-11 | | **摘 要：**  本文详细介绍倍福控制器进行ModBusTCP协议通讯的方法步骤，包括控制器作为Server端和Client的不同用法、WinCE系统和Window其他系统使用区别以及ModBusTCP通讯地址偏移修改等内容。 | | | **附 件：**   |  |  |  | | --- | --- | --- | | 序 号 | 文件名 | 备注 | | 1 | ModbusTCP.zip | ModbusTCP测试程序 | | 2 | ModbusTCP.xml | Modbus地址区配置文件 | |  |  |  | | | | **历史版本：**   |  |  |  | | --- | --- | --- | | 2020-10-22 | 徐樱樱 | TwinCAT3 Modbus-TCP Client/Server使用介绍 | |  |  |  | |  |  |  | |  |  |  | | | | **免责声明：**  我们已对本文档描述的内容做测试。但是差错在所难免，无法保证绝对正确并完全满足您的使用需求。本文档的内容可能随时更新，如有改动，恕不事先通知，也欢迎您提出改进建议。 | | | **参考信息：** | | |

**目 录**

[一、 软硬件介绍 3](#_Toc152593046)

[二、 实现功能和概述 3](#_Toc152593047)

[三、 控制器的配置 4](#_Toc152593048)

[1. Modbus TCP 软件安装 4](#_Toc152593049)

[2. Modbus TCP协议防火墙穿透 7](#_Toc152593050)

[1) WinCE系统配置 7](#_Toc152593051)

[2) Windows系统配置 12](#_Toc152593052)

[3. Modbus TCP授权添加 18](#_Toc152593053)

[四、 Modbus TCP通讯测试 19](#_Toc152593054)

[1. TwinCAT做Server端 19](#_Toc152593055)

[1) PLC与Modbus Register的地址对应关系 19](#_Toc152593056)

[2) 通过PLC变量名访问 20](#_Toc152593057)

[3) 通过绝对地址访问 23](#_Toc152593058)

[4) 修改PLC与ModbusTCP的地址对应关系 24](#_Toc152593059)

[5) WinCE系统的地址对应关系配置 28](#_Toc152593060)

[6) 同工程多个PLC项目Modbus地址对应 29](#_Toc152593061)

[2. TwinCAT做Client端 30](#_Toc152593062)

[1) 功能块概览 31](#_Toc152593063)

[2) 功能块说明 31](#_Toc152593064)

[3) Client程序测试 32](#_Toc152593065)

[4) Client程序代码 35](#_Toc152593066)

[5) 功能块错误代码 36](#_Toc152593067)

# 软硬件介绍

|  |  |  |
| --- | --- | --- |
| 编程电脑 |  | TwinCAT版本 |
|  |  | TwinCAT3 V3.1.4024.17 |
|  |  |  |
| 控制器 | 操作系统 | TwinCAT版本 |
| CX9020 | Win CE | TwinCAT3 V3.1.4024.12 |
| C6015 | Windows 10 | TwinCAT3 V3.1.4024.17 |
|  |  |  |
|  |  |  |

# 实现功能和概述

实验对象分别为一台CX9020为WinCE系统以及一台C6015为Windows10系统，以CX嵌入式控制器以及IPC工控机两种类型和WinCE与Windows系统进行Modbus通讯不同的操作方式进行展开讲解。实验最终通过ModSim32和ModScan32完成与控制器的通讯测试。

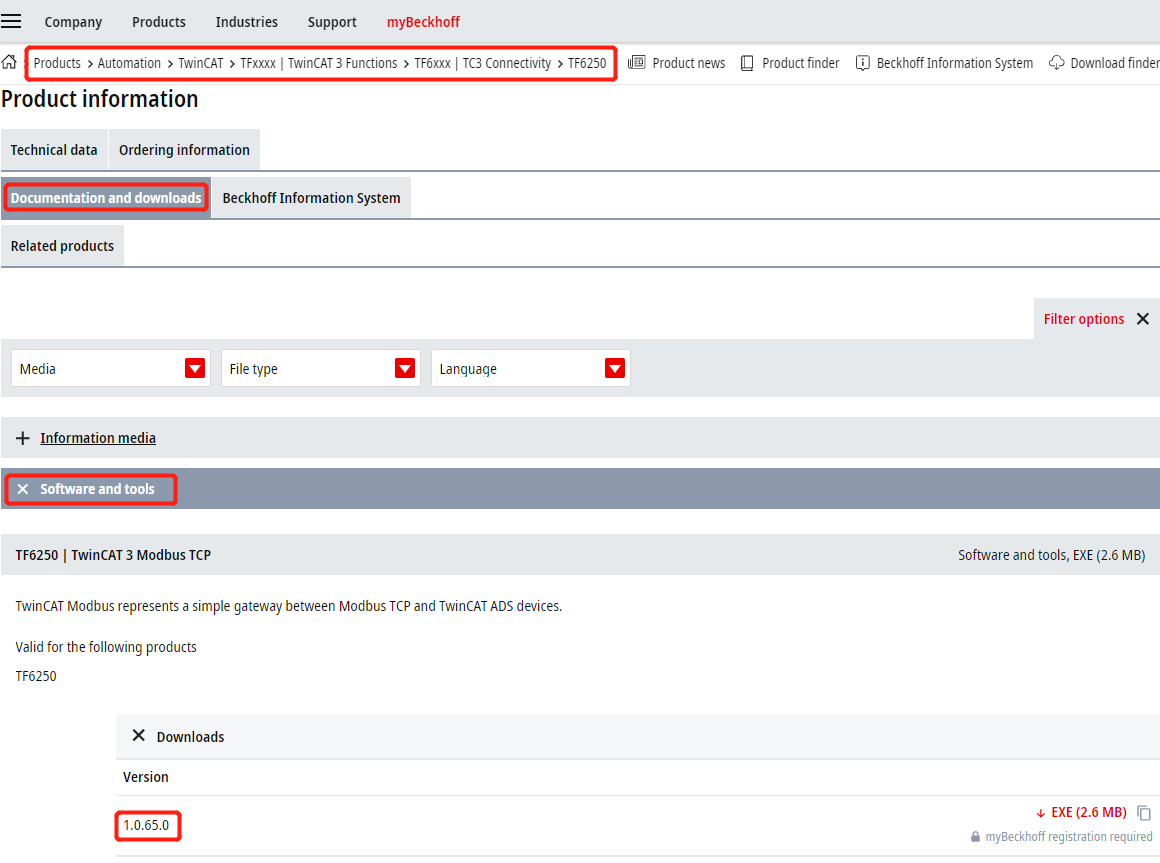
Modbus TCP是基于以太网的Modbus协议。我们知道Modbus RTU是广泛用于工业仪器仪表的串行通讯协议，RTU主从访问中使用的功能码、地址、数据集等规则在Mosbus TCP中同样使用，但以太网的速度比串口的速度提升很大，所以Modbus TCP比Modbus RTU的通讯性能有大大的提高。同时Modbus TCP通讯需要指定一个网卡，对网卡没用特殊需求并且不必独占网卡可以与其他以太网协议并存。

Modbus TCP Server可以理解为以太网的Modbus TCP通讯的驱动程序，Modbus TCP Server就是提供使用RJ45以太网方式实现Modbus通讯的驱动。当然这个Modbus TCP Server有着不同的实现方式，在高级语言里面有开源的代码可以直接使用，在固定产品中厂家也有封装好的服务，在TwinCAT中也是做好的插件直接安装即可。我们知道在TwinCAT中进行Modbus RTU或者串口通讯时，需要将PLC变量与COM口或者EL模块的Process Data之间进行变量绑定，但是在进行Modbus TCP通讯时不需要变量绑定，这是因为PLC对网口通讯使用的不是通过变量映射绑定而是通过上述所说的Modbus TCP Server实现的。一般情况下当TwinCAT PLC与触摸屏或者上位机进行通讯时，通常是作为Server，与智能仪表或者第三方设备进行通讯时作为Client。简单来讲作为Server端时候，只需要启动服务提供对应地址即可不需要编写程序，作为Client时需要编写PLC程序对Server端的地址进行读写操作。

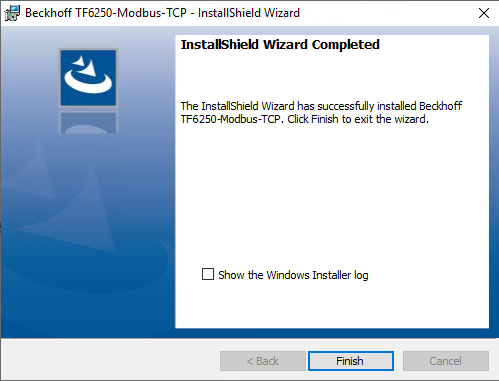
# 控制器的配置

## Modbus TCP 软件安装

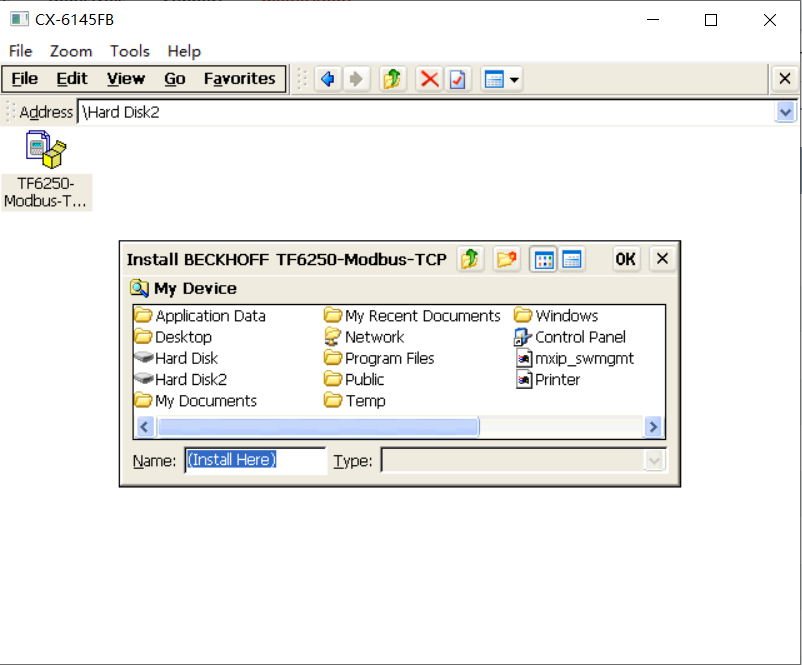
1. 首先到倍福官网（www.beckhoff.com）下载最新的用于MobusTCP通讯的驱动程序TF6250，倍福官网下载软件需要注册账户，用户只需要按照提示进行注册申请邮箱确认即可。



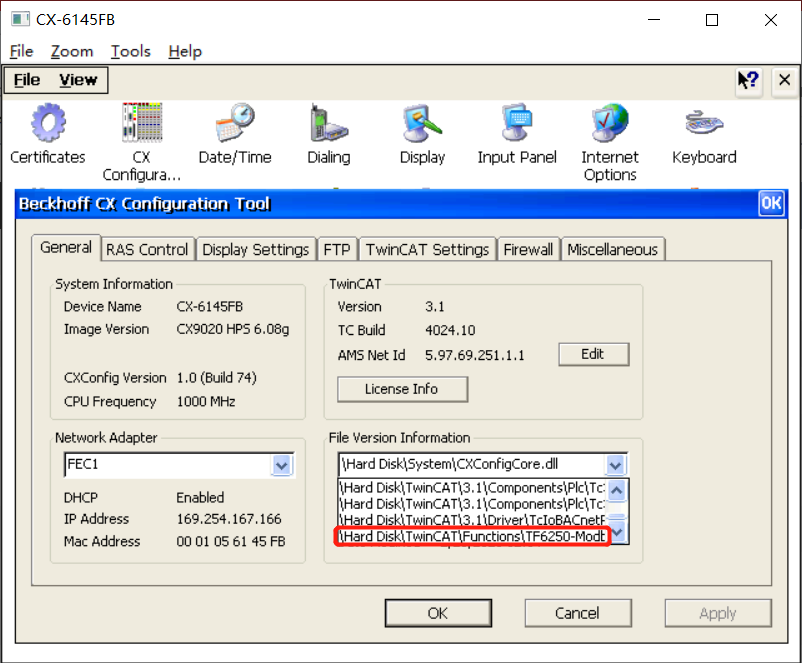
1. 下载完成之后需要将插件安装到控制器中以及自己的编程电脑中，安装到自己电脑上主要是安装ModbusTCP功能程序库。如果控制器是Windows系统那么TF6250的安装就像自己编程笔记本安装一样双击“TF6250-Modbus-TCP .exe”文件进行安装即可。双击exe文件默认安装一直点击Next即可，直到安装完成，此时ModbusTCP服务便安装成功。



1. 但是对于WinCE系统而言.exe文件是不被支持的，我们知道WinCE系统所识别的安装文件是.cab文件。此时我们便可以到上一步所述的控制器或者编程电脑的路径（C:\TwinCAT\Functions\TF6250-Modbus-TCP\CE-ARMV4I，此例中是CX9020控制器为ARM级别）下找到相应的.cab文件。需要注意的是在路径C:\TwinCAT\Functions\TF6250-Modbus-TCP下面关于CE安装文件有两种CE-ARMV4I和CE-x86，此时就需要根据所要安装控制器CPU等级进行选择，是ARM还是x86平台。将选择的安装文件（TF6250-Modbus-TCP.ARMV4I.CAB）转移到WinCE系统的控制器中，转移方式可以通过U盘或者FTP等方式详细方法不做赘述。在控制器中找到转移进去的.cab文件，双击进行安装，选择默认的安装路径点击右上角OK按钮即可。



1. 安装完成后没有任何提示，页面自动关闭，我们可以通过CX Configuration->General->File Version Information当中进行查看，是否已经安装完成。

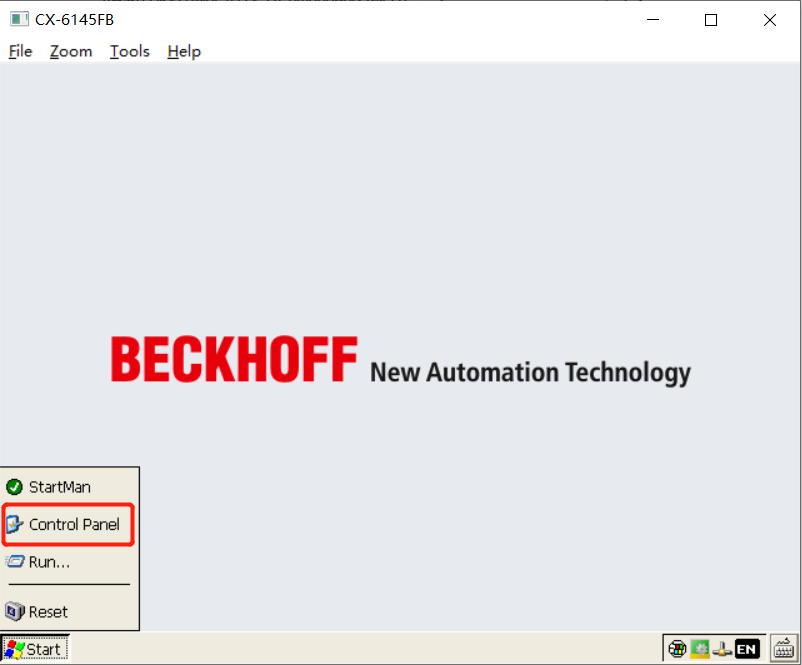


## Modbus TCP协议防火墙穿透

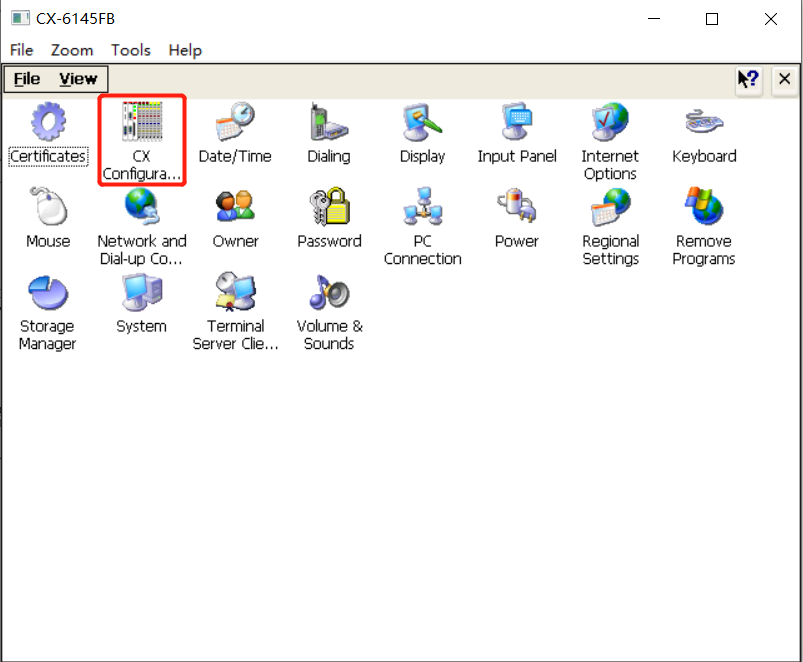
### WinCE系统配置

1. 关闭防火墙

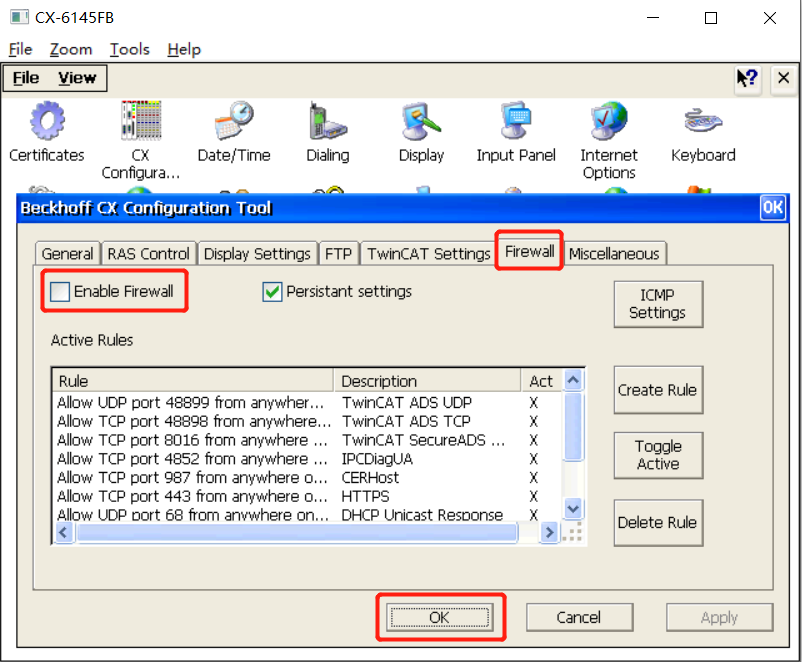
（1）、通过外接显示器或者远程桌面（CerHost）的方式进入控制器的桌面，点击Start选择Control Panel进入控制面板选项。



* 1. 选择CX Configuration选项，进入嵌入式控制器的配置界面。

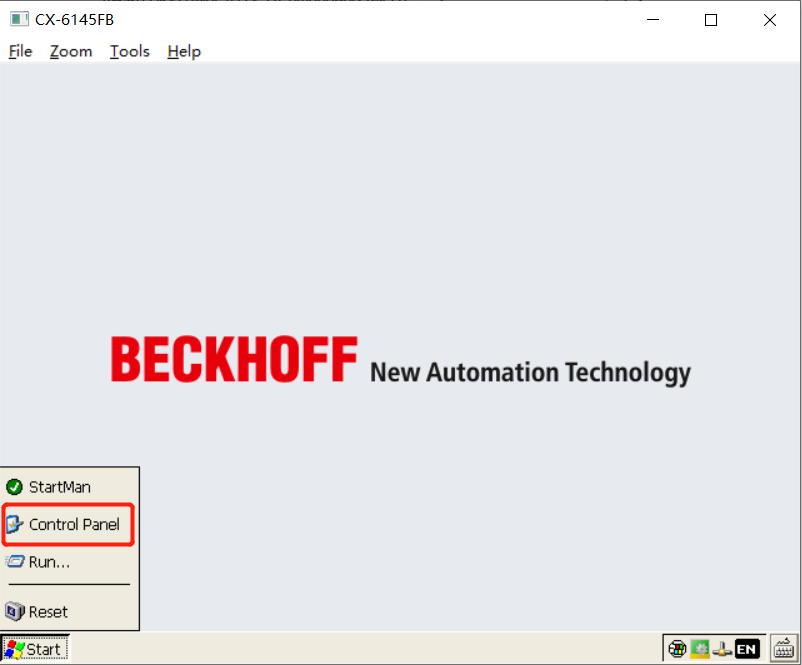


（3）、进入配置界面后找到Firewall选项，就可以通过是否勾选Enable Firewall选项来打开或关闭防火墙。

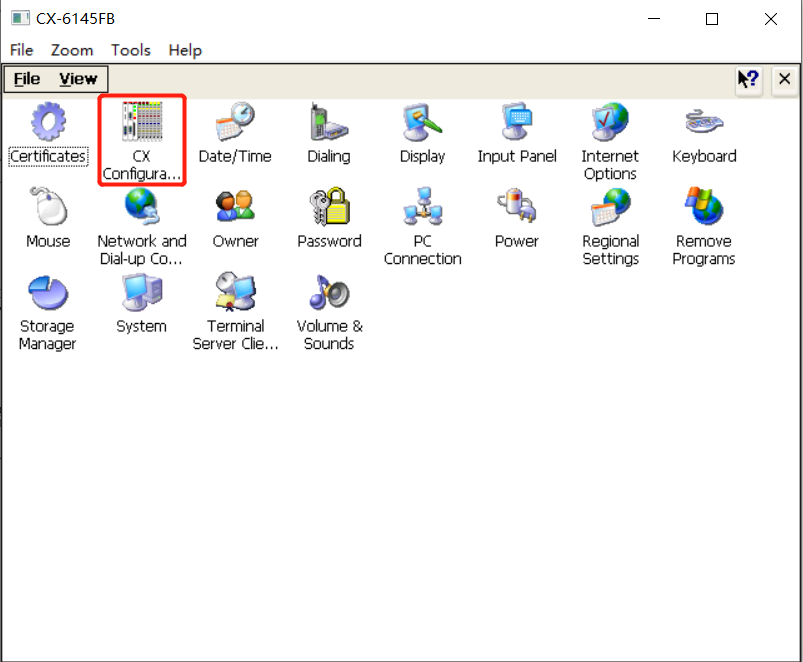


1. 穿透防火墙

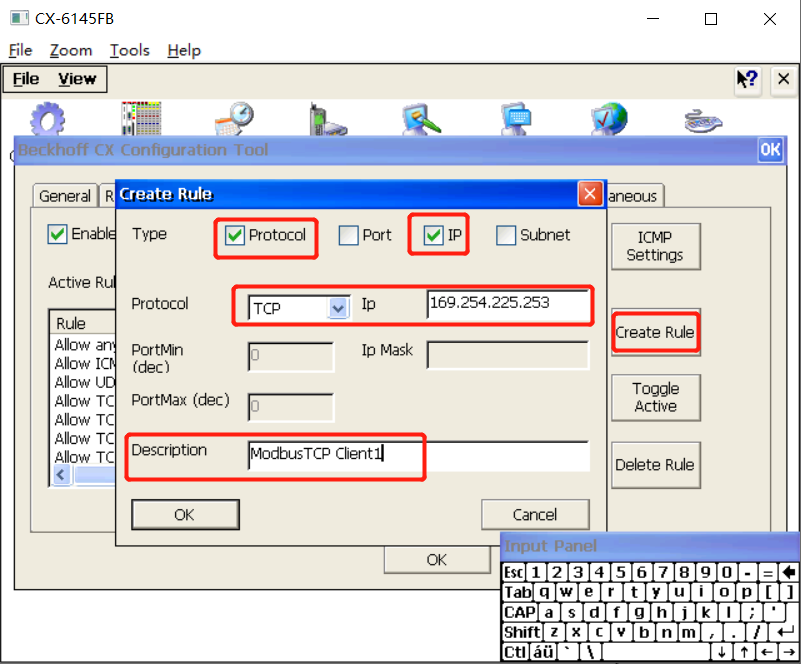
（1）、通过外接显示器或者远程桌面（CerHost）的方式进入控制器的桌面，点击Start选择Control Panel进入控制面板选项。



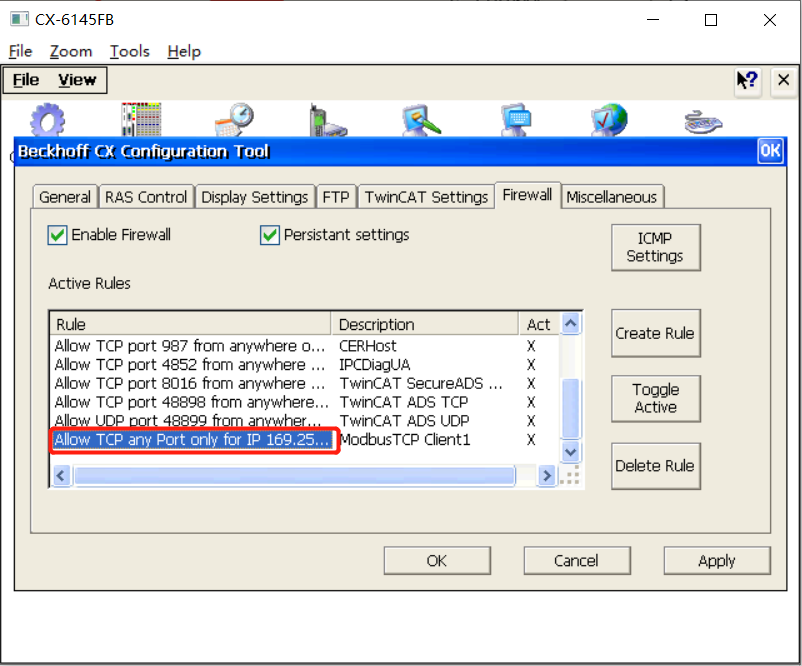
（2）选择CX Configuration选项，进入嵌入式控制器的配置界面。



（3）点击Creat Rule按钮，创建一个新的规则来允许防火墙通过，可以通过Protocol协议、Port端口、IP地址、Subnet子网掩码等条件来限制服务协议通过防火墙。



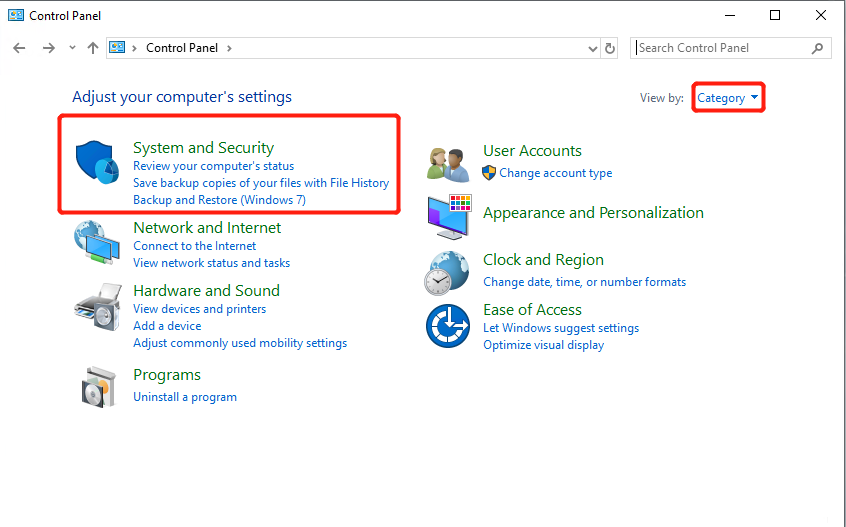
（4）添加之后可以发现，在Active Rules中有了刚刚添加的允许通过的协议类型，这样在打开防火墙的情况下也可以进行Modbus通讯。



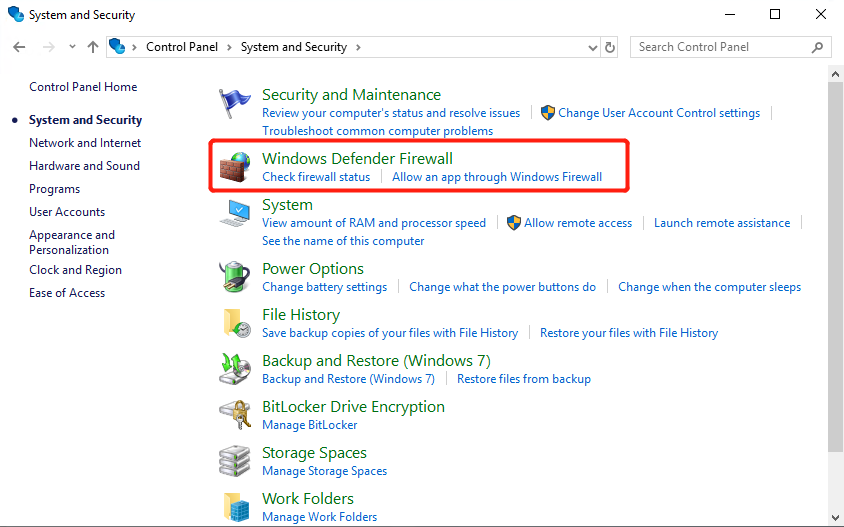
### Windows系统配置

1. 关闭防火墙

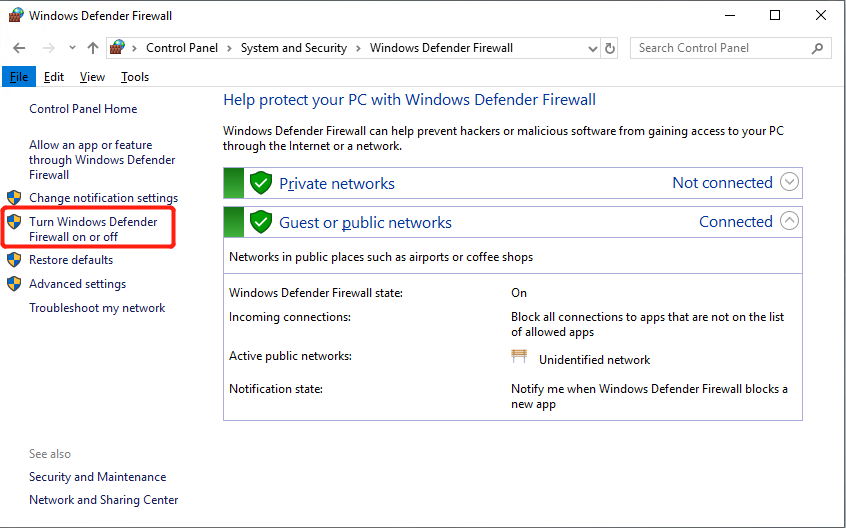
（1）、通过外接显示器或者远程桌面的方式进入控制器的桌面，进入操作系统控制面板界面，选择System and Security选项。



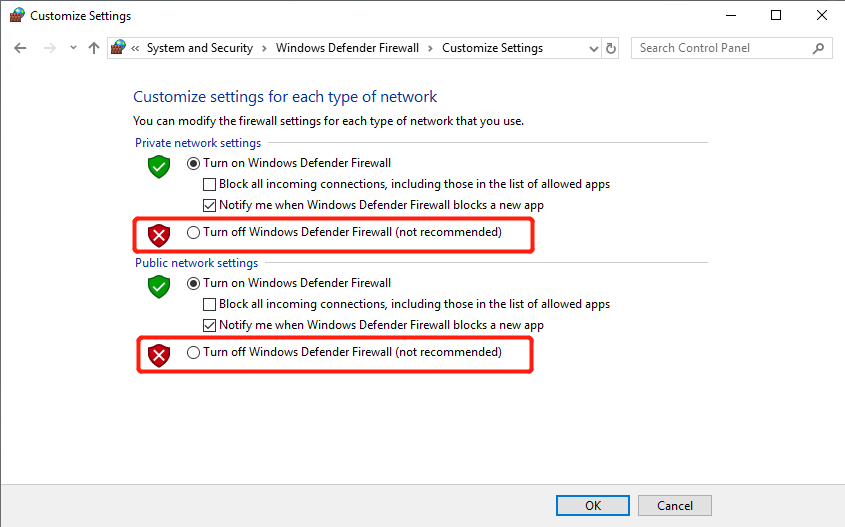
（2）、选择Windows Defender Firewall选项。



（3）、选择Turn Windows Defender Firewall on or off选项。

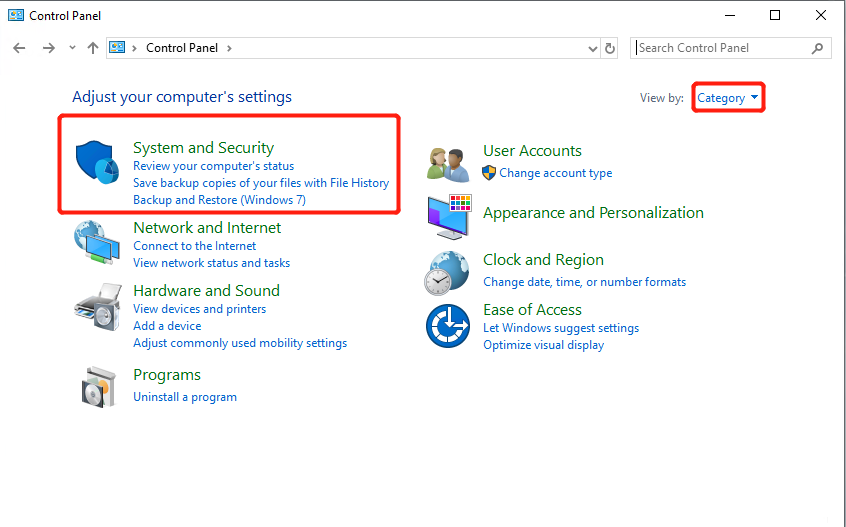


（4）、可以在对应的网络下选择是否关闭防火墙，最后点击确认按钮。简单粗暴的关闭防火墙是可以进行MosbusTCP协议通讯，但是关闭关闭防火墙了也可能会带来其他的未知损坏。要酌情处理，可以通过下一章节介绍的方法设置ModbusTCP服务允许通过防火墙。

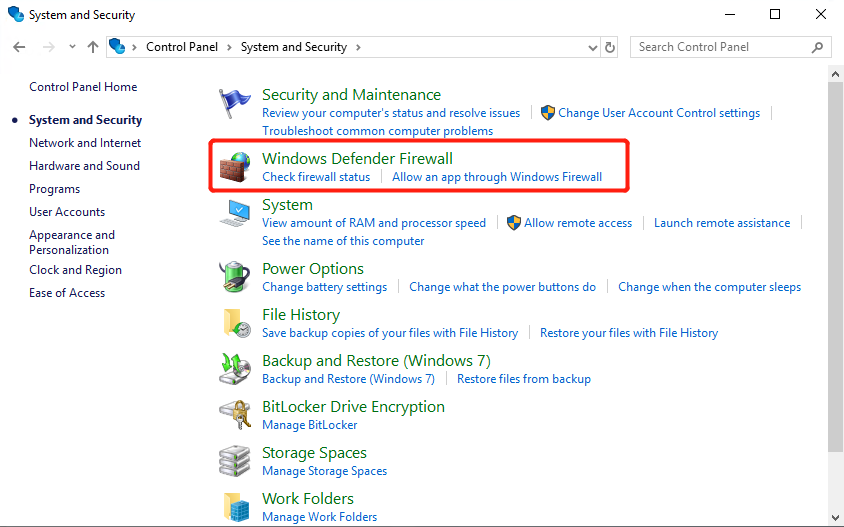


1. 允许ModbusTCP服务通过防火墙

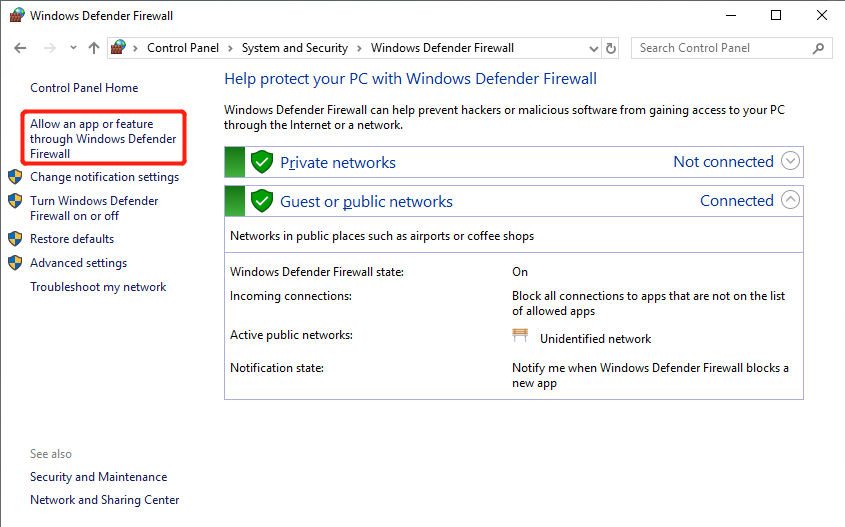
（1）、通过外接显示器或者远程桌面的方式进入控制器的桌面，进入操作系统控制面板界面，选择System and Security选项。



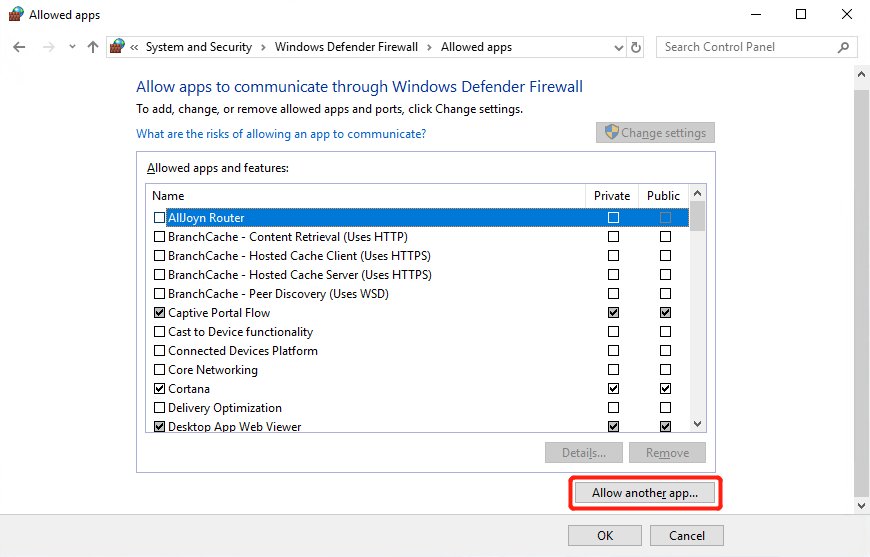
（2）、选择Windows Defender Firewall选项。



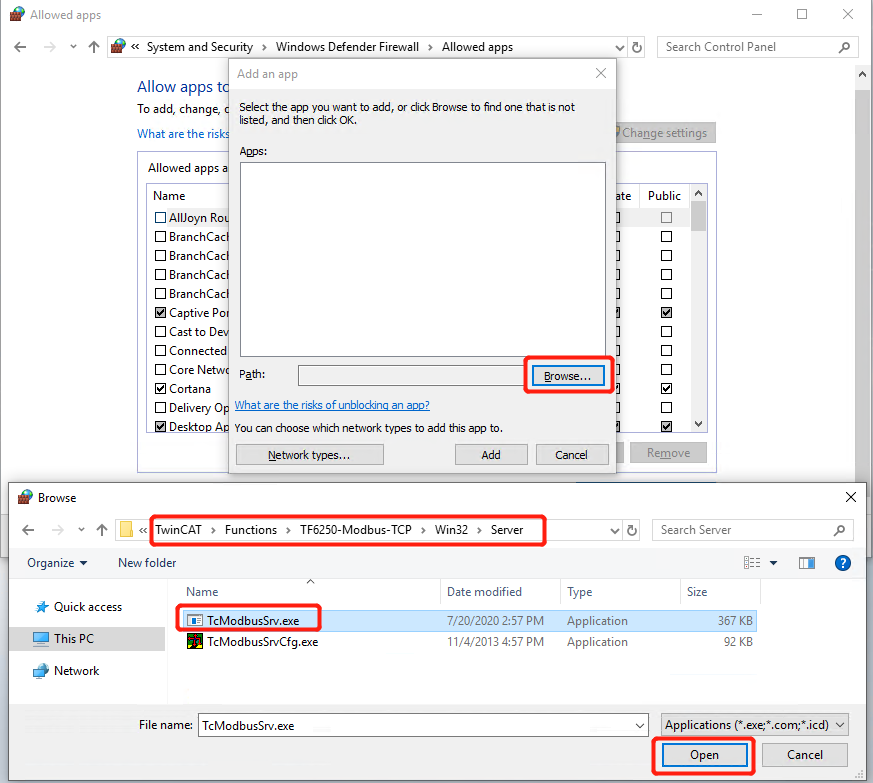
（3）、选择Allow an app or feature though Windows Defender Firewall选项。



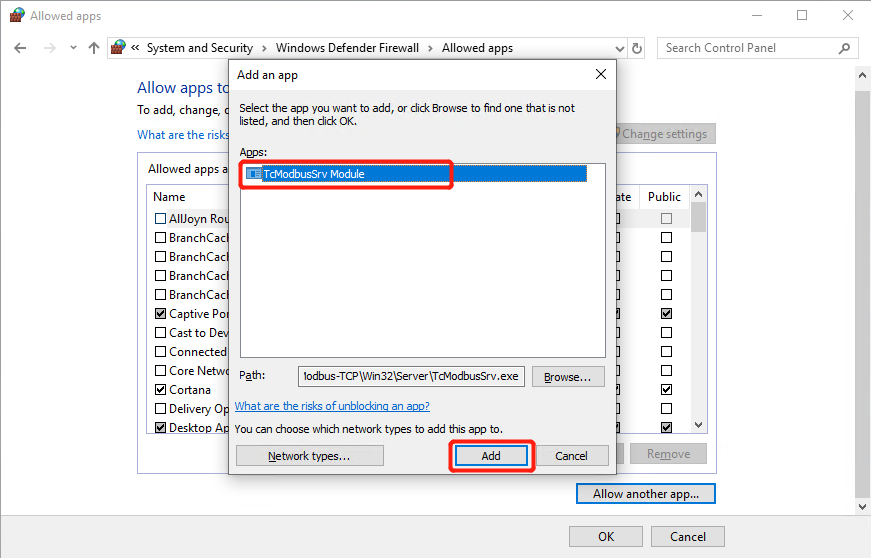
（4）、选择右下角的Allow another app…选项。



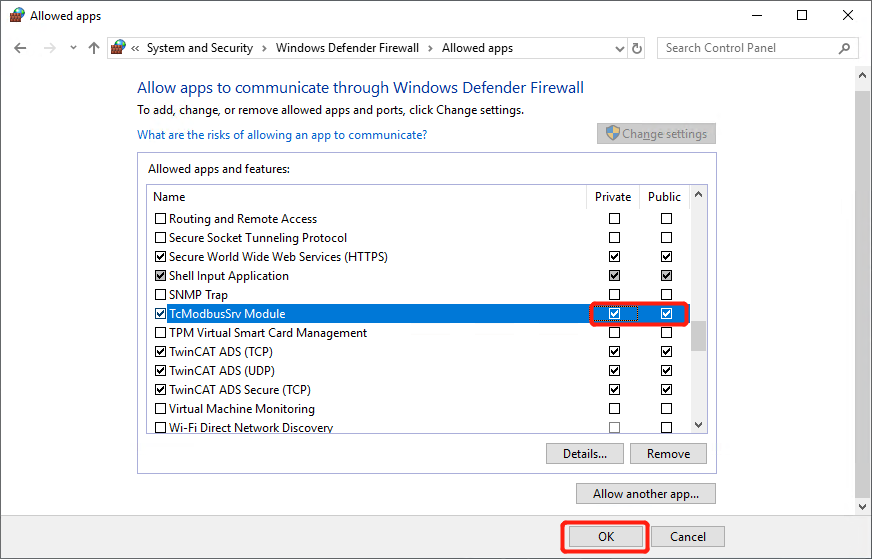
（5）、点击Browse…按钮，手动找到TcModbusSrv.exe文件（Path：C:\TwinCAT\Functions\TF6250-Modbus-TCP\Win32\Server）点击Open按钮确认添加新的服务。



（6）、选择TcModbusSrv Module，点击Add按钮，将服务添加到防火墙列表中。

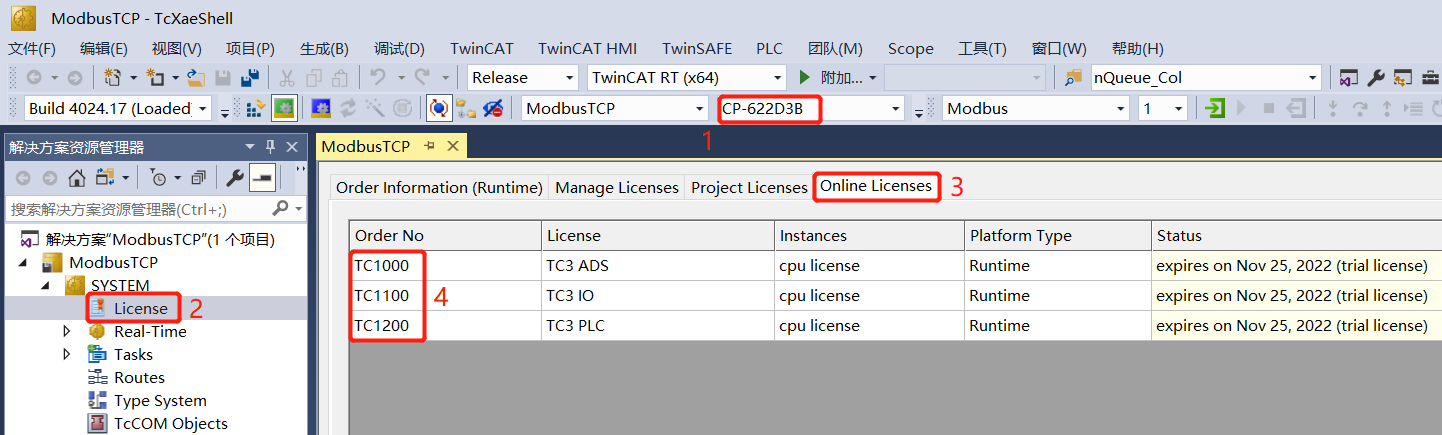


（7）、添加到列表中后，就可以在Allow app and features 中找到TcModbusSrv Module选项，勾选后面的Private和Public选项，这样ModbusTCP服务就可以在公网和私网中通讯使用了。

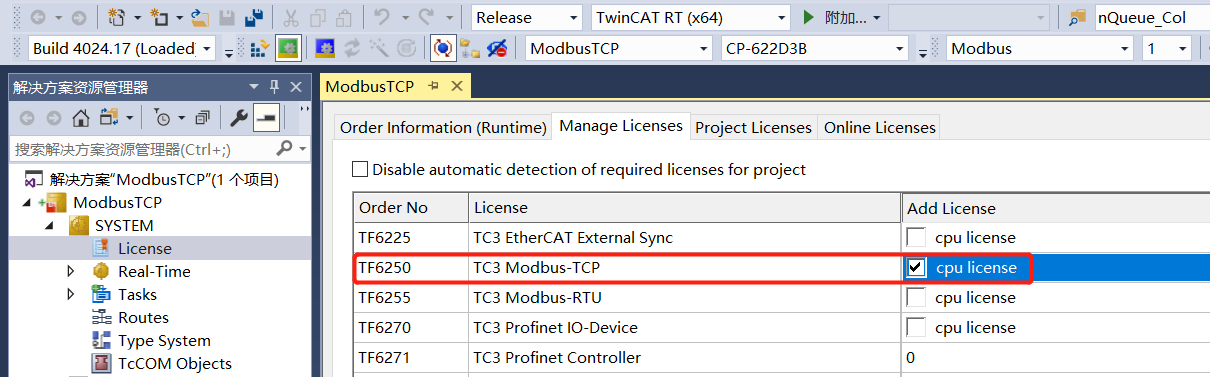


## Modbus TCP授权添加

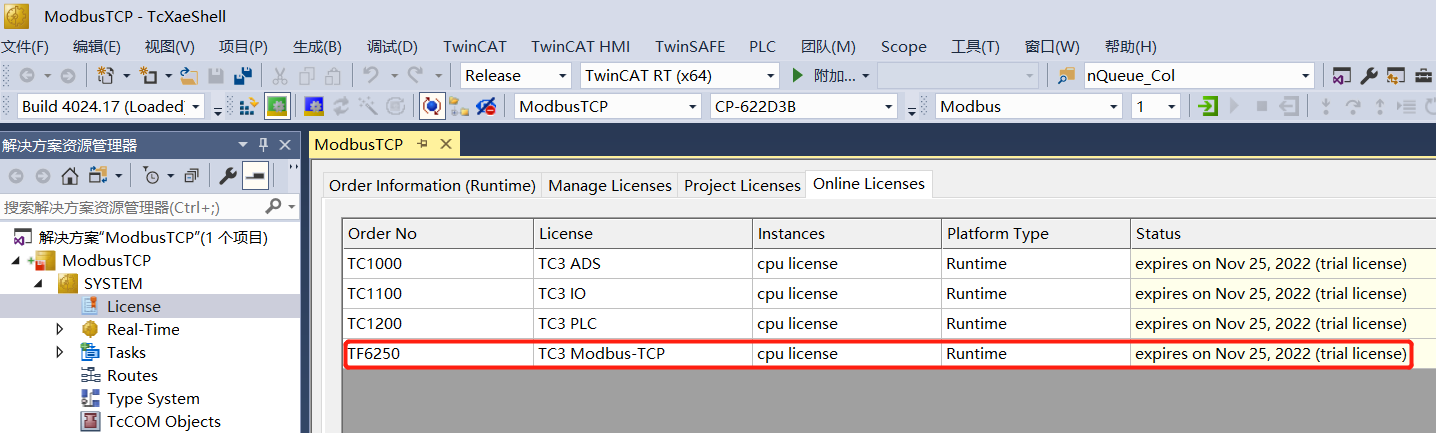
（1）、检查控制器是否存在ModbusTCP的授权，如果没有授权那么需要手动激活一个临时授权以确保ModbusTCP Server的正常运行。



（2）、在此控制器中可以看到没有ModbusTCP的授权，这是需要手动选择ModbusTCP的授权在进行激活配置即可。



（3）、重新激活后再次查看Online License，可以发现TF6250ModbusTCP临时授权已经激活，并且是在7天后到期。



# Modbus TCP通讯测试

## TwinCAT做Server端

当TwinCAT作为ModbusTCP Server工作时，PLC不需要编写任何通讯的程序。在安装了TwinCAT Modbus TCP Server的控制器上，只要TwinCAT PLC启动并运行，该服务就会自动运行，可以随时接受Modbus TCP Client发来的Modbus指令并做出应答响应。此时对于Modbus TCP Client端而言，只要知道PLC地址与Modbus Register的地址映射规则就可以根据这个规则访问到需要的PLC地址信息。

### PLC与Modbus Register的地址对应关系

在倍福官方文档中我们可以查到PLC地址与Modbus Register的地址映射默认关系如下表：

| **Modbus areas** | **Modbus address** | **ADS area** | |
| --- | --- | --- | --- |
| Digital inputs | 0x8000 - 0x80FF | **Name of the variables in the PLC program** | **Data type** |
| GVL.mb\_Input\_Coils | ARRAY [0..255] OF BOOL |
| Digital outputs (coils) | 0x8000 - 0x80FF | **Name of the variables in the PLC program** | **Data type** |
| GVL.mb\_Output\_Coils | ARRAY [0..255] OF BOOL |
| Input registers | 0x8000 - 0x80FF | **Name of the variables in the PLC program** | **Data type** |
| GVL.mb\_Input\_Registers | ARRAY [0..255] OF WORD |
| Output registers | 0x3000 - 0x5FFF | 0x4020 - PLC memory area | 0x0 |
| 0x6000 - 0x7FFF | 0x4040 - PLC data area | 0x0 |
| 0x8000 - 0x80FF | **Name of the variables in the PLC program** | **Data type** |
| GVL.mb\_Output\_Registers | ARRAY [0..255] OF WORD |

通过此表的信息可以看出Modbus TCP地址与PLC的变量的映射关系中M区有两种（可以同时使用）方式可以访问，使用PLC内存中的绝对地址和PLC中的变量名，I区和Q区就只能通过变量名进行访问。需要注意的是我们看表格里划出来的起始地址是0x8000，但当我们用Modscan做测试的时候，实际地址应该是0x8000+1=32769以及他们往后的255个地址。

因此测试得出：

GVL.mb\_Input\_Coils  起始地址对应 02:input status的32769

GVL.mb\_Output\_Coils 起始地址对应 01:coil status的32769

GVL.mb\_Input\_Registers 起始地址对应 04:input register的32769

GVL.mb\_Output\_Registers 起始地址对应 03:holding register的32769

PLC Memory area 为MW0 起始地址对应 03:holding register的12289

Data area 待测试

### 通过PLC变量名访问

（1）、新建ModbusTCP测试程序，添加全局变量表GVL，在全局变量表中添加MoubusTCP通讯变量，用于测试通过变量名进行访问的方式。

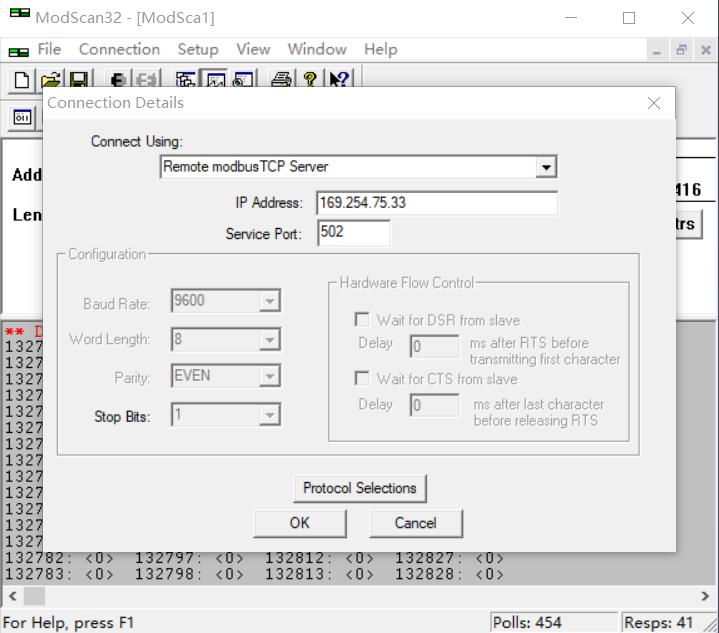
mb\_Input\_Coils : ARRAY [0..255] OF BOOL;

mb\_Output\_Coils : ARRAY [0..255] OF BOOL;

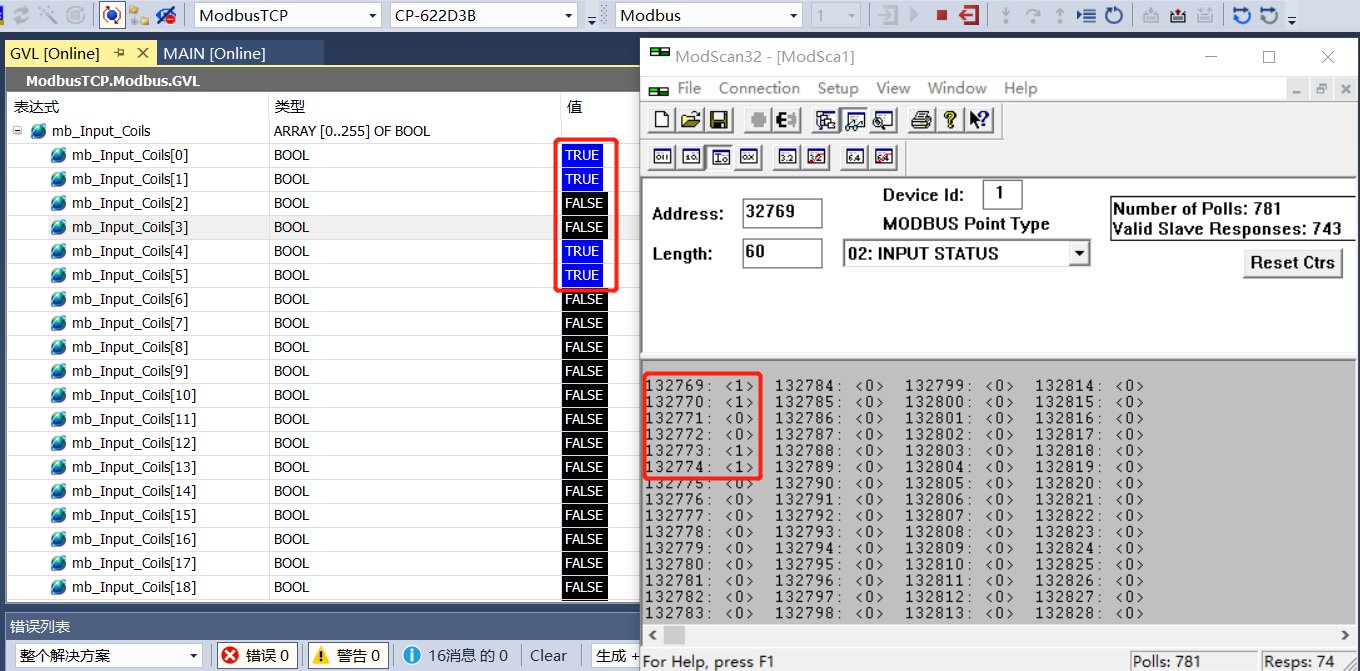
mb\_Input\_Registers : ARRAY [0..255] OF WORD;

mb\_Output\_Registers : ARRAY [0..255] OF WORD;

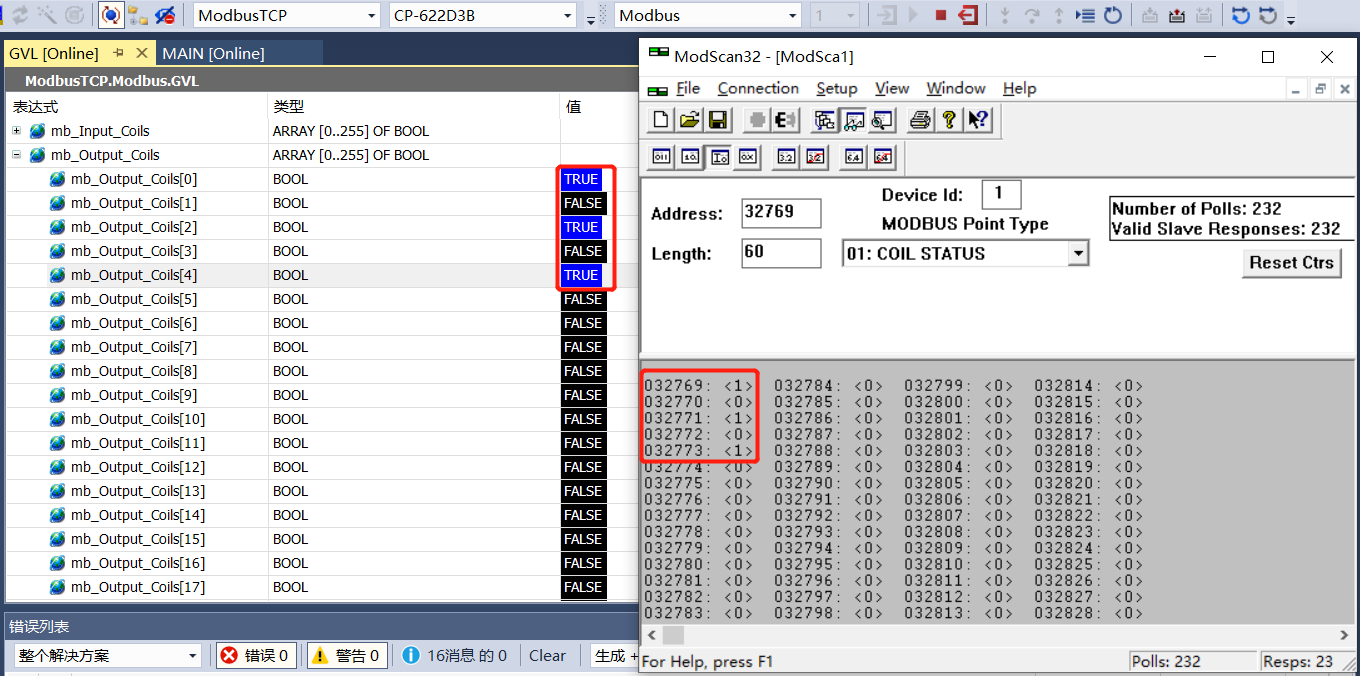
（2）、打开ModScan软件，点击Connection-Connect，弹出对话框中选择Remote modbusTCP Server，输入所要连接的控制器IP Address，Service Port，服务端口默认502即可。



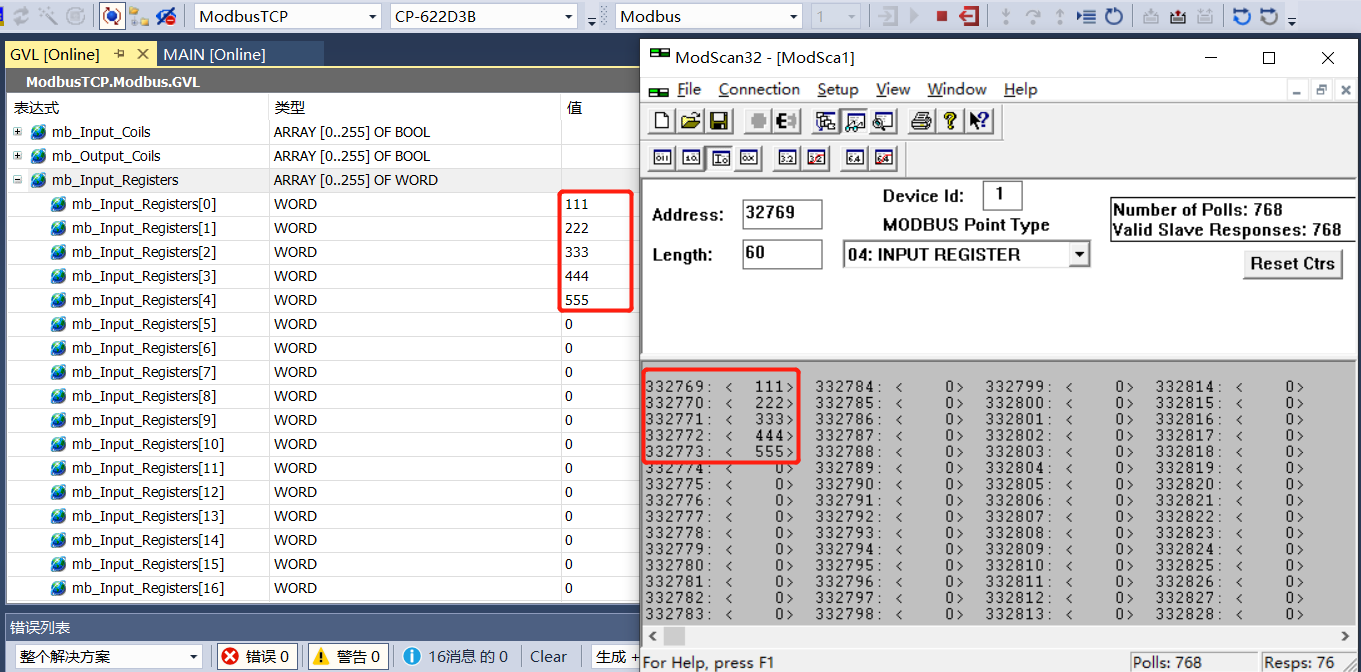
（3）首先测试mb\_Input\_Coils，在ModScan中Modbus Point Type选项选择：02：INPUT STATUS，Adress地址填写32769（上文中已讲述说明）。Lenth长度代表所要监控的数据长度，这个根据需要随意填写。TwinCAT程序中修改变量数值，可以ModScan中对应的地址也在变化，通讯测试成功。



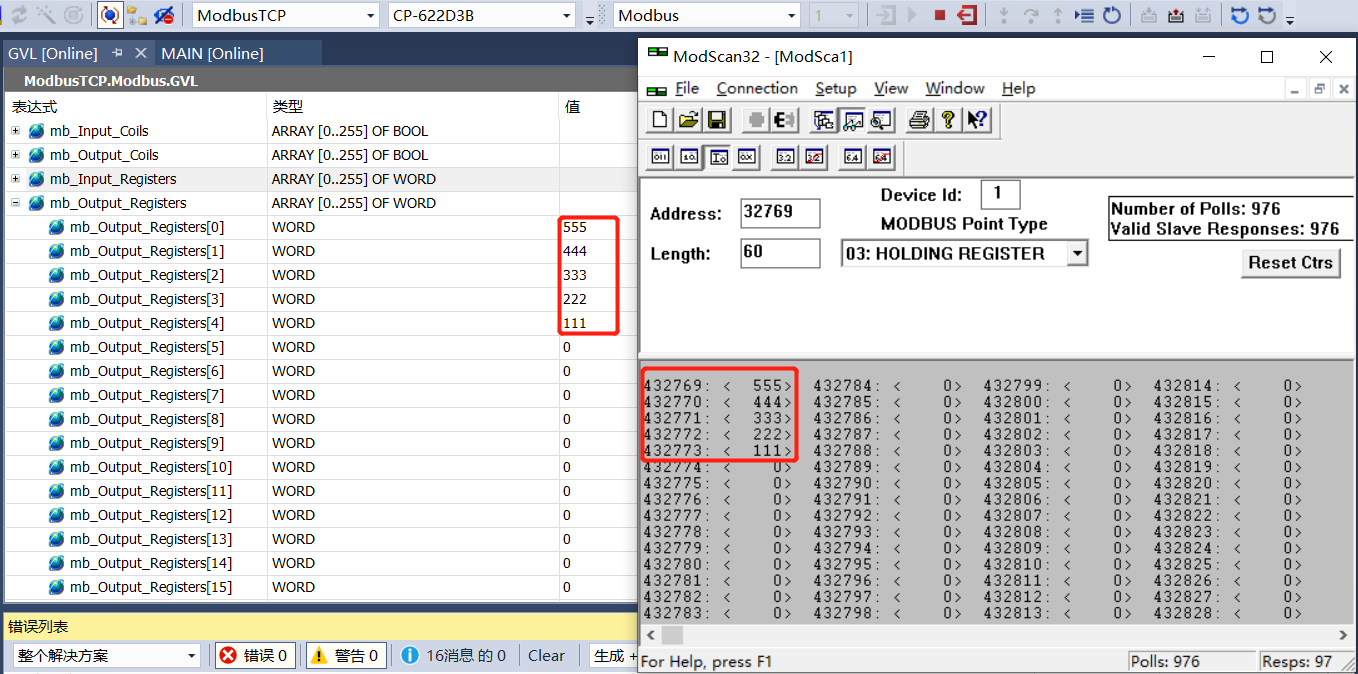
（4）、测试mb\_Output\_Coils，在ModScan中Modbus Point Type选项选择：01：COIL STATUS，Adress地址填写32769。TwinCAT程序中修改变量数值，可以ModScan中对应的地址也在变化，通讯测试成功。



（5）、测试mb\_Input\_Registers，在ModScan中Modbus Point Type选项选择：04：INPUT REGISTER，Adress地址填写32769。TwinCAT程序中修改变量数值，可以ModScan中对应的地址也在变化，通讯测试成功。



（6）测试mb\_Output\_Registers，在ModScan中Modbus Point Type选项选择：03：HOLDING REGISTER，Adress地址填写32769。TwinCAT程序中修改变量数值，可以ModScan中对应的地址也在变化，修改ModScan中的数值，同样PLC中对应的变量也在变化，通讯测试成功。



### 通过绝对地址访问

（1）、在PLC->MAIN程序中添加以下的变量，用于测试通过绝对地址进行ModbusTCP通讯。

MW0 AT%MW0:WORD;

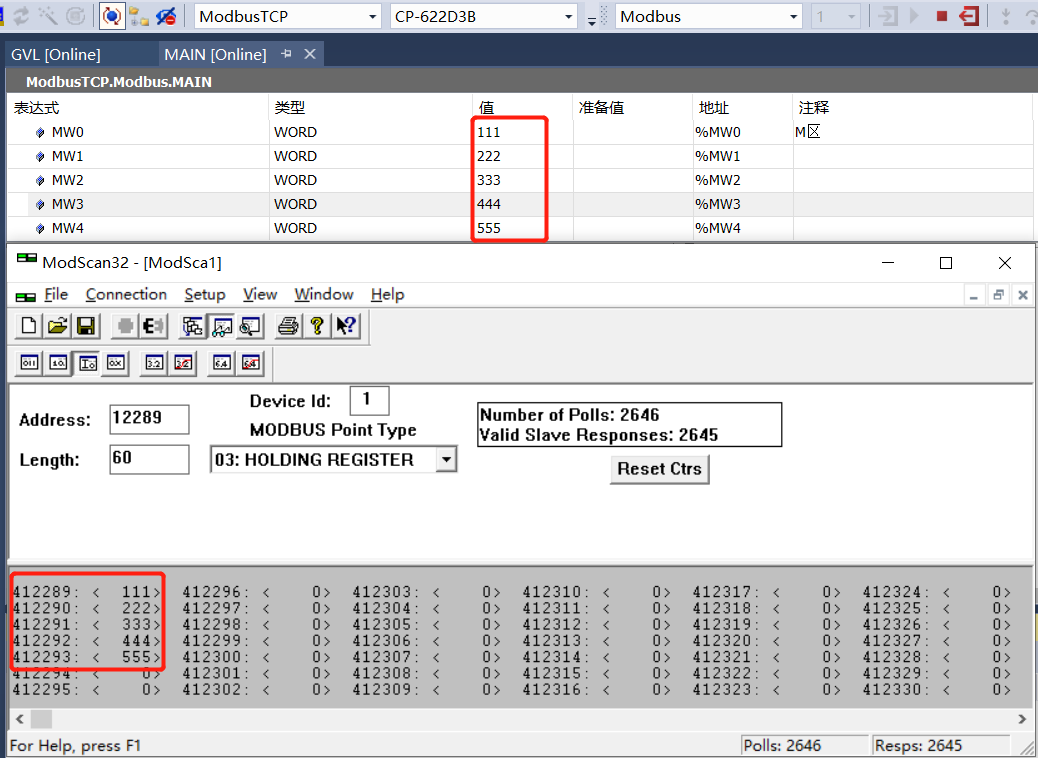
MW1 AT%MW1:WORD;

MW2 AT%MW2:WORD;

MW3 AT%MW3:WORD;

MW4 AT%MW4:WORD;

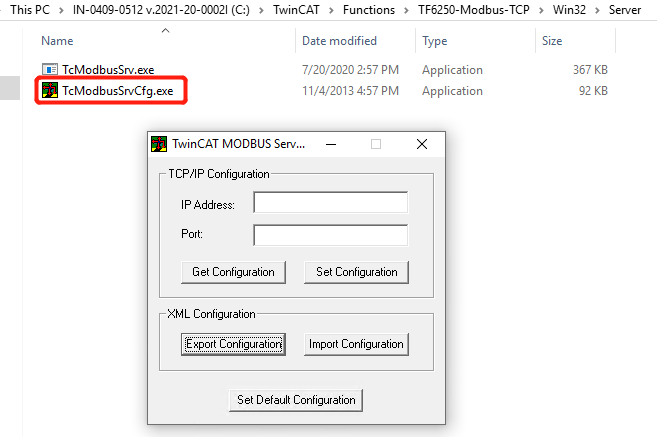
（2）、修改在ModScan中Modbus Point Type选项选择：03：HOLDING REGISTER，Adress地址填写12289。上文中我们知道MW0对应Modbus地址为12289，后面依次进行偏移。TwinCAT程序中修改MW0~MW4数值，可以ModScan中对应的412289~412293地址也在变化，修改ModScan中的数值，同样PLC中对应的变量也在变化，通讯测试成功。



### 修改PLC与ModbusTCP的地址对应关系

在上面的测试中我们可以发现PLC程序中的MW0对应Modbus地址是412289，但是对于实际应用的过程中，有更多的时候我们更希望的是MW0对应400001，这样对应起来使用方便。接下来我们来演示如何进行对应关系的修改。

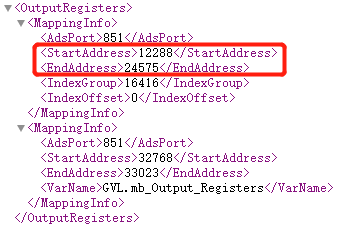
（1）、打开远程桌面进入控制器，在这个路径下C:\TwinCAT\Functions\TF6250-Modbus-TCP\Win32\Server找到TcModbusSrvCfg.exe工具，右键以管理员运行。点击Export Configuration按钮按照提示输入导出的配置文件名，选择一个储存路径导出文件，需要注意的是执行导出文件的时候TwinCAT是需要从运行状态转换到配置状态。导出配置文件如果提示导出文件失败，可以先点击一下Set Default Configuration，进行一下默认配置然后在进行导出操作即可。



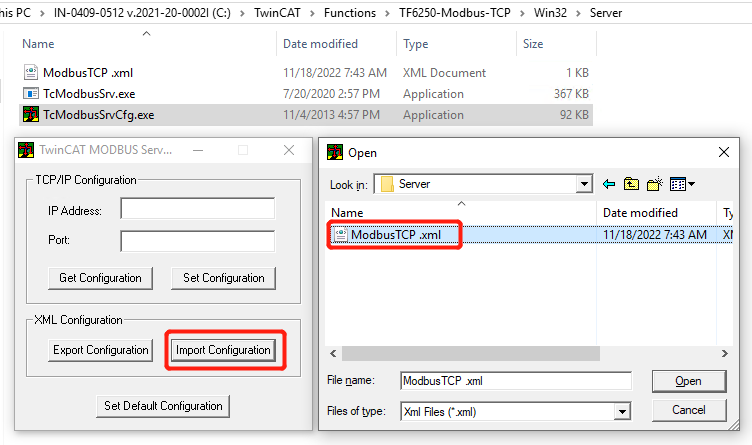
（2）、打开导出的XML配置文件，结构如下所示，结合上面的地址信息可以发现对应的地址关系是一致的。接下来以修改OutputRegisters为例进行测试。



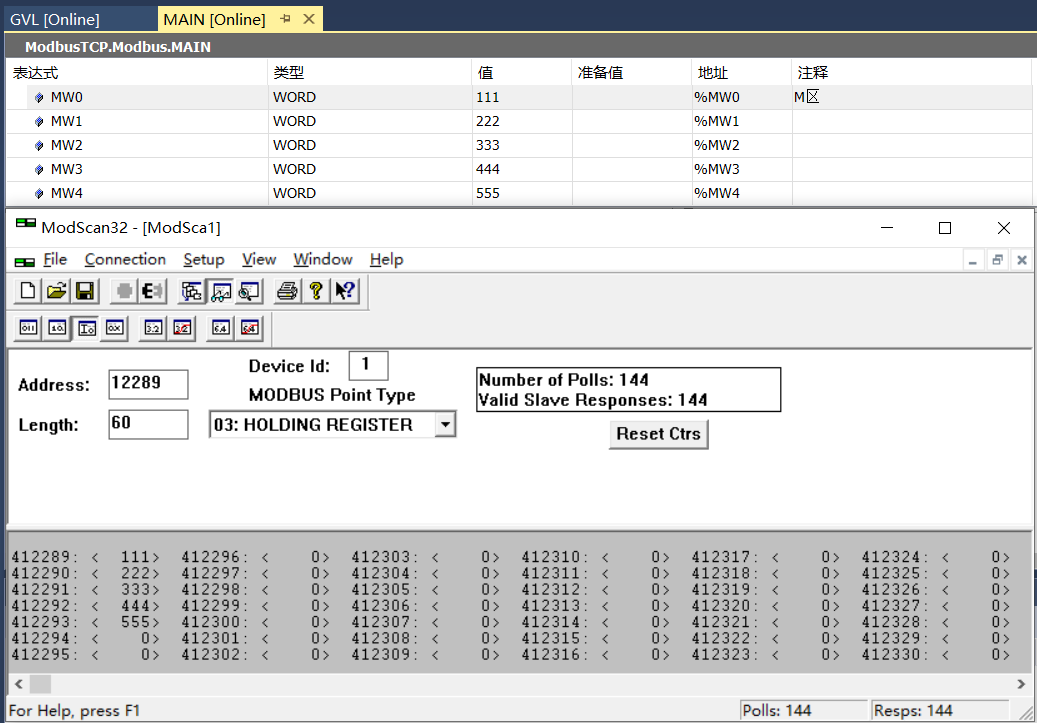
（文本

描述已自动生成3）、修改OutputRegisters中的StartAddress和EndAddress，这里就是修改了M区对应的地址关系。测试修改StartAddress为0，结束地址默认的24575。这就代表开辟了从0到24575的ModbusTCP地址区间。

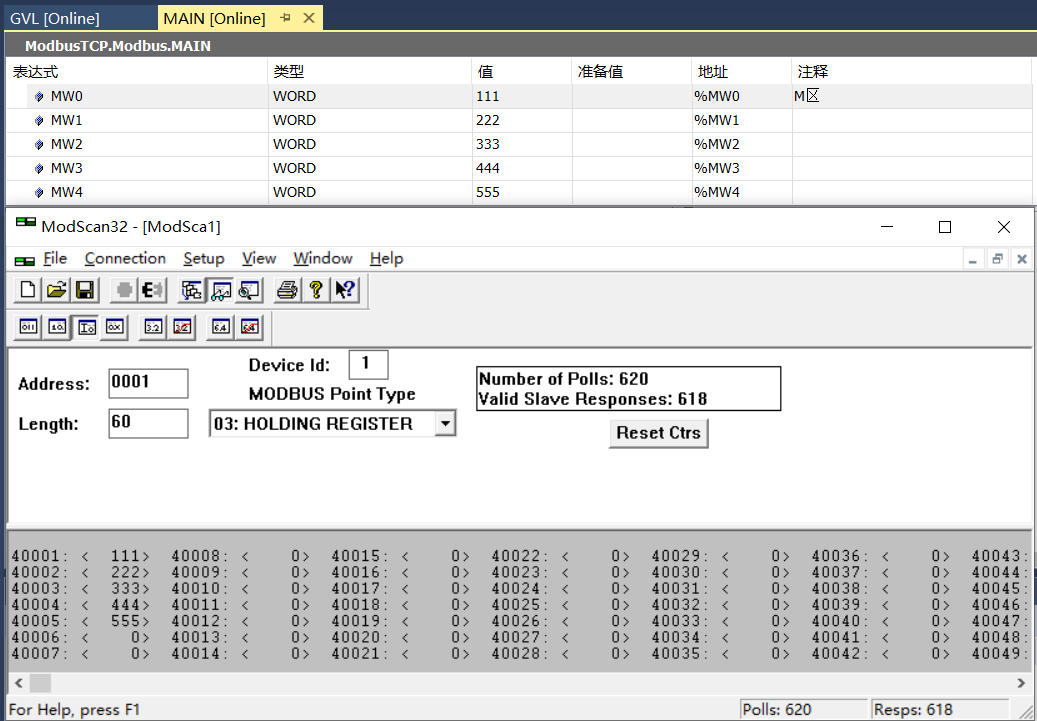
（4）、将修改后的XML文件导入到TwinCAT的配置中去，重启控制器新的配置生效。



修改前默认配置如下所示，MW0对应Modbus地址为412289。



修改后可以发现MW0对应的地址就是Modbus的40001。

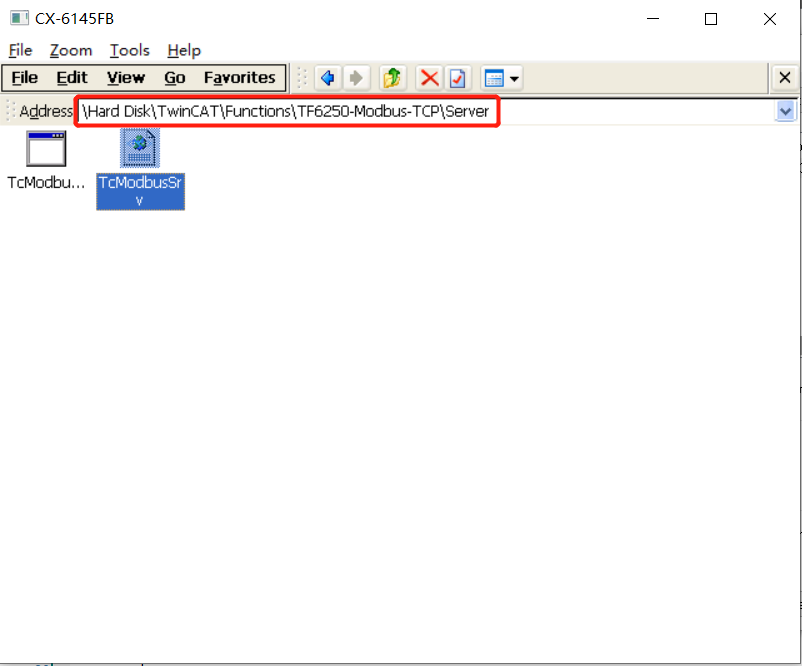


（5）、上文中测试可以看到修改StartAdress即可修改Modbus的起始地址，那么如果想要MW1对应40001怎么办呢？在xml文件中可以看到有一组IndexGroup和IndexOffset参数，在这里IndexGroup中0x4020就是对应PLC memory area也就是M区地址，后面的IndexOffset可以调整M区的起始地址，这个IndexOffset是以Byte为计数单位的，比如想要以MW1对应40001那么修改IndexGroup为2即可。

（6）、需要注意一点，默认情况下变量名和绝对地址可以同时使用。在修改地址时候只要两个地址区域没有重叠那么也是可以同时使用的，但是如果M区的地址放大至变量名的区域，此时变量名访问便不能进行读写操作，数据以M区地址去更新。修改地址时候一定要注意区域重叠问题，如果没有特殊需求不建议去修改这个地址配置文件。

### WinCE系统的地址对应关系配置

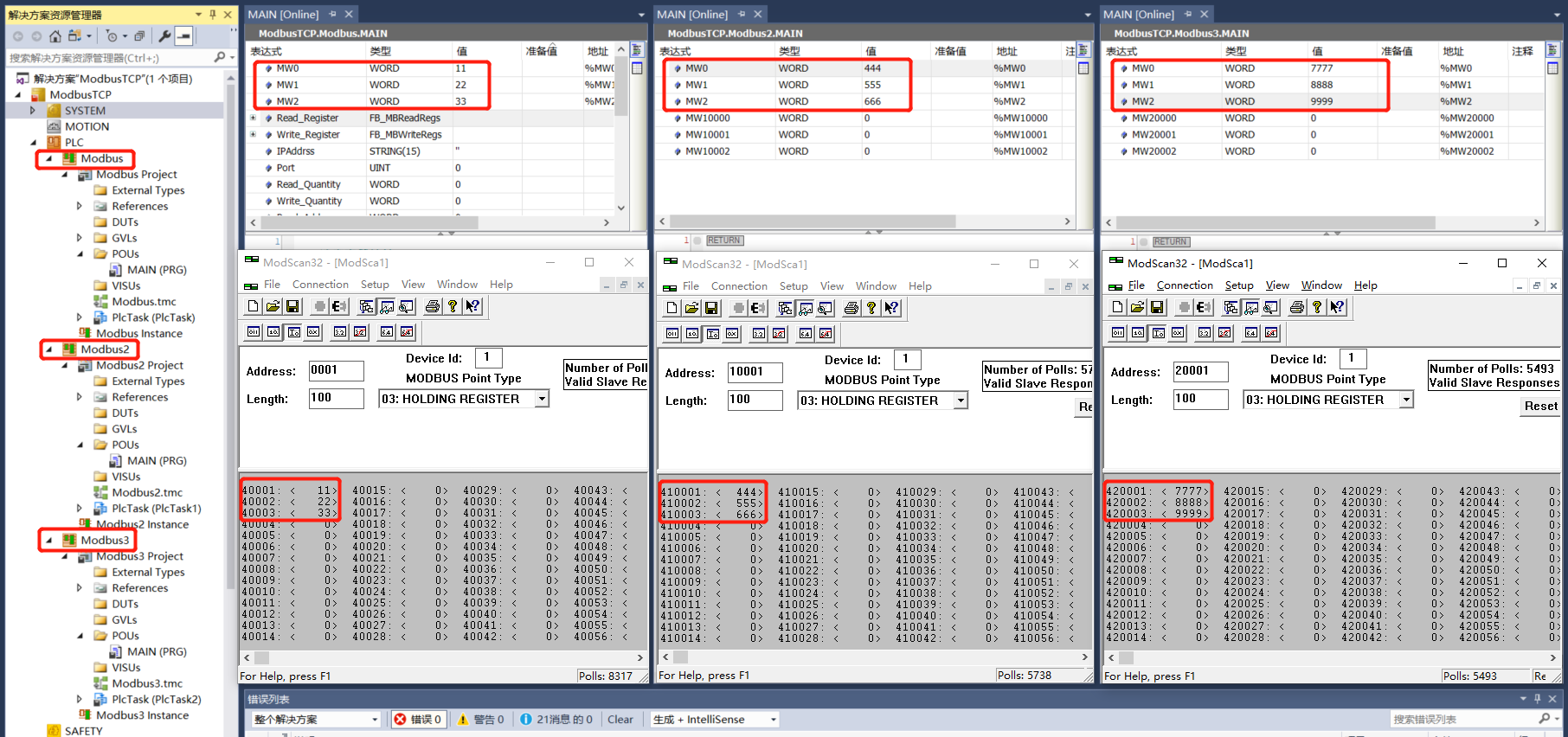
上面所讲的是Windows系统，但对于CE系统并没有配置ModbusTCP的地址的小工具插件，此时对于CE系统找到以下路径(path: \TwinCAT3\Functions\TF6250-Modbus-TCP\Server\ TcModbusSrv.xml)文件进行配置修改。修改完成之后在放到这个路径下覆盖原有的文件即可，复制替代完需要重启控制器才生效。



### 同工程多个PLC项目Modbus地址对应

对于一个项目中建立多个PLC\_Project，那么每个PLC\_Project而言都是创建不同而独立的地址区，每个PLC\_Project都想要使用ModbusTCP通讯，但是此时ModbusTCP Server只有一个，所以此时可以对Modbus地址区进行分区设置如下图配置，将851端口分配0~9999、852端口分配10000~19999、853端口分配20000~29999。这样就将三个不同的PLC\_Project分配了不同的Modbus地址区，上位机可以根据不同地址区与不同的PLC\_Project进行通讯。





## TwinCAT做Client端

当TwinCAT作为ModbusTCP Client工作时，就需要编写ModbusTCP通讯程序，安装完成TF6250插件后TwinCAT就可以引入Tc2\_ModbusSrv程序库，我们就可以通过调用其中的功能块就，就可以实现发送不同的功能码去访问对应的Server端。作为Client端，必须知道Server端的Modbus Register的定义规则，才能通过这个规则访问到特定的变量。

### 功能块概览

不同的程序功能块发送不同的功能码，具体功能块展示如下：

| **Modbus TCP function** | **Function code** | **PLC block** |
| --- | --- | --- |
| Read Coils | 1 | [FB\_MBReadCoils](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192752395.html) |
| Read Inputs | 2 | [FB\_MBReadInputs](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192753931.html) |
| Read Registers | 3 | [FB\_MBReadRegs](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192755467.html) |
| Read Input Registers | 4 | [FB\_MBReadInputRegs](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192757003.html) |
| Write Single Coil | 5 | [FB\_MBWriteSingleCoil](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192758539.html) |
| Write Single Register | 6 | [FB\_MBWriteSingleReg](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192760075.html) |
| Write Multiple Coils | 15 | [FB\_MBWriteCoils](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192761611.html) |
| Write Multiple Registers | 16 | [FB\_MBWriteRegs](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192763147.html) |
| Read/Write Multiple Registers | 23 | [FB\_MBReadWriteRegs](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192764683.html) |
| Diagnostic | 8 | [FB\_MBDiagnose](https://infosys.beckhoff.com/content/1033/tf6250_tc3_modbus_tcp/192766219.html) |

### 功能块说明

Tc2\_ModbusSrv中最常用的两个功能块是FB\_MBReadRegs和FB\_MBWriteRegs，下面以这两个功能块为例说明接口变量的含义。

VAR\_INPUT  
    sIPAddr    : STRING(15);  
    nTCPPort   : UINT:= MODBUS\_TCP\_PORT;  
    nUnitID    : BYTE:=16#FF;  
    nQuantity  : WORD;  
    nMBAddr    : WORD;  
    cbLength   : UDINT;  
    pDestAddr  : POINTER OF BYTE;  
    bExecute   : BOOL;  
    tTimeout   : TIME;  
END\_VAR

sIPAddr：所要访问ModbusTCP Server的IP地址，比如“169.254.225.253”；

nTCPPort：所要访问ModbusTCP Server的端口号；

nUnitID：所要访问ModbusTCP Server的站号，默认为1，如不知道无需更改；

nQuantity：所要访问Register的数量，以Word为单位；

nMBAddr：所要访问Register的首地址，最小值是0，代表第一个Register，根据实际填写；

cbLength：所要读写PLC变量的长度，以Byte为单位，因为要对应一般都写成nQuantity\*2；

pDestAddr：所要读写PLC变量的首地址，一般用ADR(变量名)来引用；

bExcute：读写操作指令，以上升沿触发；

tTimeout：超时时间，超过设定时间没有相应出现报警。

VAR\_OUTPUT  
    bBUSY      : BOOL;  
    bError     : BOOL;  
    nErrId     : UDINT;  
    cbRead     : UDINT;  
END\_VAR

bBusy：功能块被激活正在执行读写操作指令；

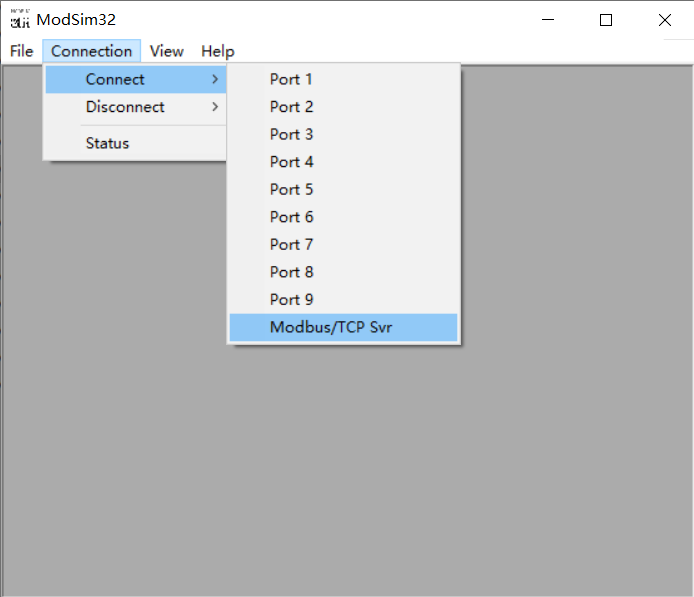
bError：执行功能块出错会被置为1，一般为ADS错误；

nErrorID：错误代码；

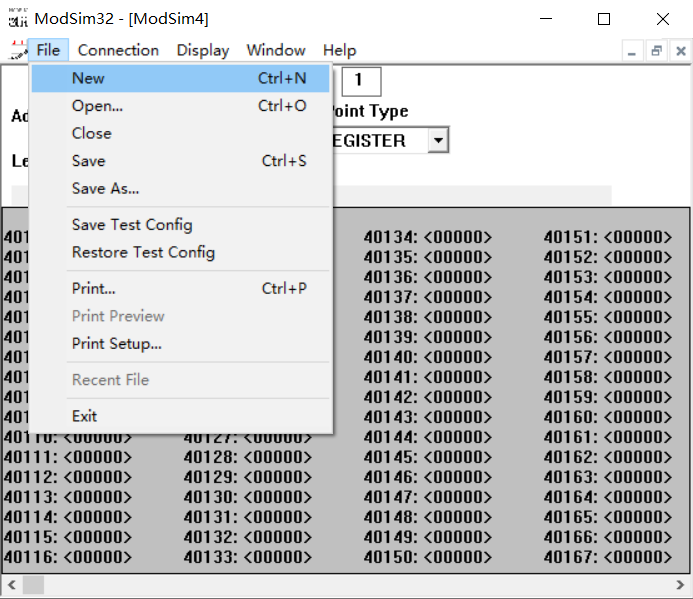
cbRead：反映出读写数据的长度，以Byte为单位。

### Client程序测试

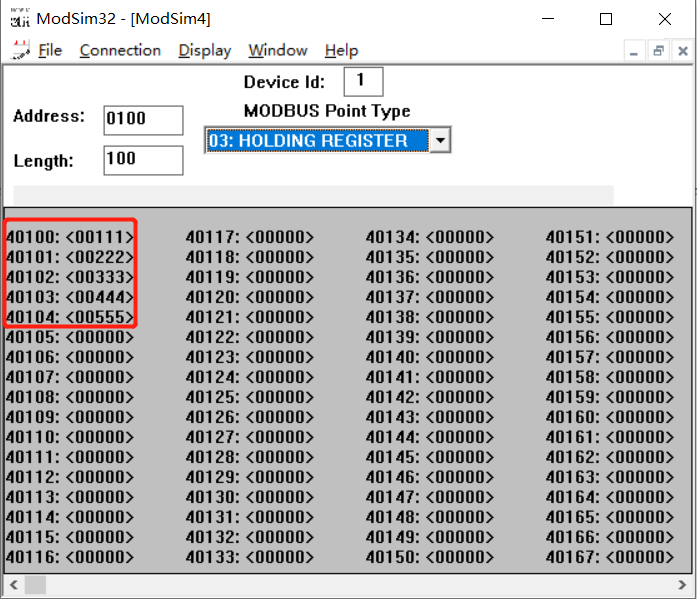
（1）、首先创建ModbusTCP Server端，找到Modsim程序，双击打开Modsim32.exe快捷方式，选择Connection->Connect->Modbus/TCP Server，默认端口502不需要更改。



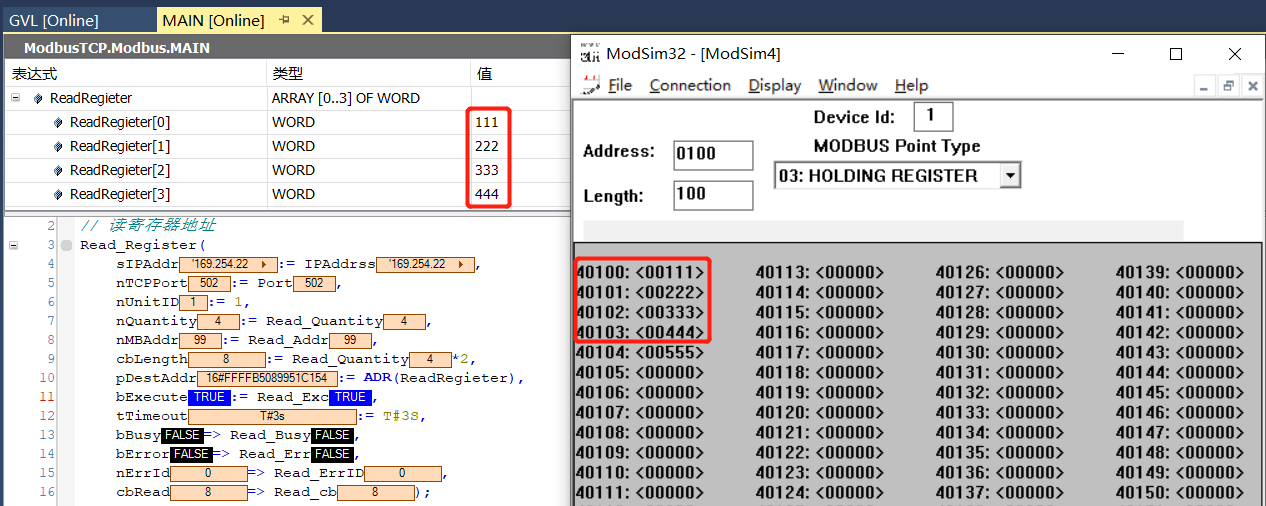
（2）、点击File->New，创建一个监控列表。



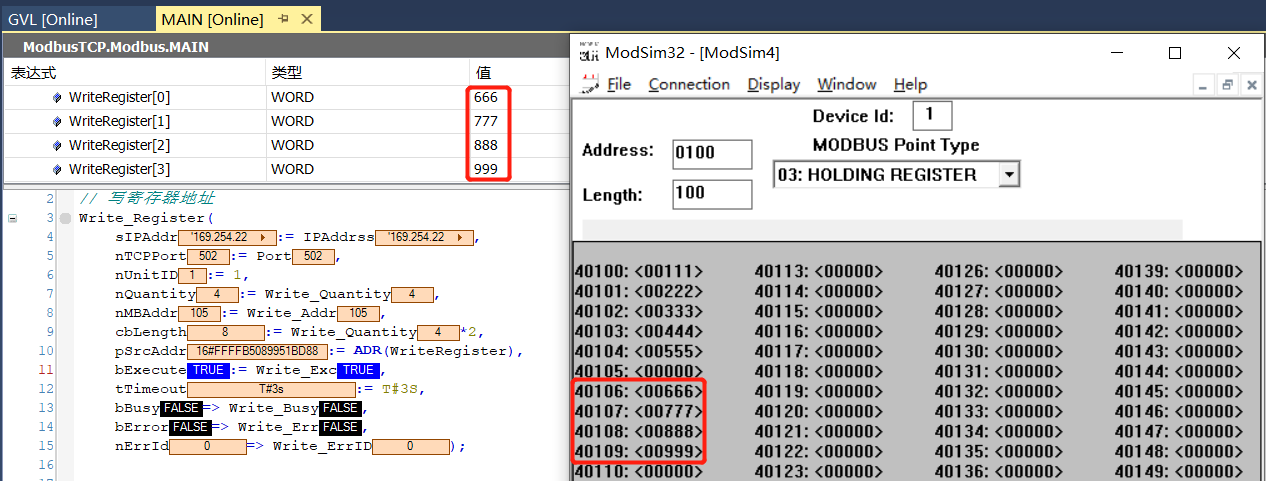
（3）、双击更新40100~40104地址的数值，用以PLC读取这个数据信息。举例程序是Register所以此处MODBUS Point Type选择的是03：HOLDING REGISTER。



（4）编写读取寄存器程序，执行Read\_Exc读取寄存器地址，可以发现PLC程序已经将40100~40104地址内容读取到程序ReadRegieter变量中，程序代码附在最后。



（5）将PLC程序中WriteRegister[0]~ WriteRegister[3]分别赋值666、777、888、999，执行Write\_Exc写寄存器地址，在Modsim中可以发现40106~40109变量已经被赋新值。



### Client程序代码

变量定义区：

PROGRAM MAIN

VAR

Read\_Register :FB\_MBReadRegs;

Write\_Register :FB\_MBWriteRegs;

IPAddrss: STRING(15);

Port: UINT;

Read\_Quantity: WORD;

Write\_Quantity: WORD;

Read\_Addr: WORD;

Write\_Addr: WORD;

ReadRegister: ARRAY[0..3] OF WORD;

WriteRegister: ARRAY[0..3] OF WORD;

Read\_Exc: BOOL;

Write\_Exc: BOOL;

Read\_Busy: BOOL;

Write\_Busy: BOOL;

Read\_Err: BOOL;

Write\_Err: BOOL;

Read\_ErrID: UDINT;

Write\_ErrID: UDINT;

Read\_cb: UDINT;

END\_VAR

程序区：

// 读寄存器地址

Read\_Register(

sIPAddr:= IPAddrss,

nTCPPort:= Port,

nUnitID:= 1,

nQuantity:= Read\_Quantity,

nMBAddr:= Read\_Addr,

cbLength:= Read\_Quantity\*2,

pDestAddr:= ADR(ReadRegister),

bExecute:= Read\_Exc,

tTimeout:= T#3S,

bBusy=> Read\_Busy,

bError=> Read\_Err,

nErrId=> Read\_ErrID,

cbRead=> Read\_cb);

// 写寄存器地址

Write\_Register(

sIPAddr:= IPAddrss,

nTCPPort:= Port,

nUnitID:= 1,

nQuantity:= Write\_Quantity,

nMBAddr:= Write\_Addr,

cbLength:= Write\_Quantity\*2,

pSrcAddr:= ADR(WriteRegister),

bExecute:= Write\_Exc,

tTimeout:= T#3S,

bBusy=> Write\_Busy,

bError=> Write\_Err,

nErrId=> Write\_ErrID);

### 功能块错误代码

（1）、TwinCAT Modbus TCP return code

| **Function specific ADS return code** | **Possible reason** |
| --- | --- |
| 0x8001 | Modbus function not implemented |
| 0x8002 | Invalid address or length |
| 0x8003 | Invalid parameters: - wrong number of registers |
| 0x8004 | Modbus server error |

（2）、TwinCAT ADS return code

| **Hex** | **Dezimal** | **Source** |
| --- | --- | --- |
| 0x00000000-0x00007800 | 0-30720 | [TwinCAT System return codes](https://infosys.beckhoff.com/content/1033/TcDiagnostics/HTML/TcDiagnostics_ErrorOverview.htm) |
| 0x00008000-0x000080FF | 32768-33023 | Internal TwinCAT Modbus TCP |
| 0x80070000-0x8007FFFF | 2147942400-2148007935 | Returncode - 0x80070000 =[Win32 System Returncode](https://infosys.beckhoff.com/content/1033/TcDiagnostics/HTML/TcDiagnostics_WIN32_ErrorCodes.htm) |

（3）、Global error codes

| **Hex** | **Dec** | **HRESULT** | **Name** | **Description** |
| --- | --- | --- | --- | --- |
| 0x0 | 0 | 0x9811 0000 | ERR\_NOERROR | No error. |
| 0x1 | 1 | 0x9811 0001 | ERR\_INTERNAL | Internal error. |
| 0x2 | 2 | 0x9811 0002 | ERR\_NORTIME | No real-time. |
| 0x3 | 3 | 0x9811 0003 | ERR\_ALLOCLOCKEDMEM | Allocation locked – memory error. |
| 0x4 | 4 | 0x9811 0004 | ERR\_INSERTMAILBOX | Mailbox full – the ADS message could not be sent. Reducing the number of ADS messages per cycle will help. |
| 0x5 | 5 | 0x9811 0005 | ERR\_WRONGRECEIVEHMSG | Wrong HMSG. |
| 0x6 | 6 | 0x9811 0006 | ERR\_TARGETPORTNOTFOUND | Target port not found – ADS server is not started or is not reachable. |
| 0x7 | 7 | 0x9811 0007 | ERR\_TARGETMACHINENOTFOUND | Target computer not found – AMS route was not found. |
| 0x8 | 8 | 0x9811 0008 | ERR\_UNKNOWNCMDID | Unknown command ID. |
| 0x9 | 9 | 0x9811 0009 | ERR\_BADTASKID | Invalid task ID. |
| 0xA | 10 | 0x9811 000A | ERR\_NOIO | No IO. |
| 0xB | 11 | 0x9811 000B | ERR\_UNKNOWNAMSCMD | Unknown AMS command. |
| 0xC | 12 | 0x9811 000C | ERR\_WIN32ERROR | Win32 error. |
| 0xD | 13 | 0x9811 000D | ERR\_PORTNOTCONNECTED | Port not connected. |
| 0xE | 14 | 0x9811 000E | ERR\_INVALIDAMSLENGTH | Invalid AMS length. |
| 0xF | 15 | 0x9811 000F | ERR\_INVALIDAMSNETID | Invalid AMS Net ID. |
| 0x10 | 16 | 0x9811 0010 | ERR\_LOWINSTLEVEL | Installation level is too low –TwinCAT 2 license error. |
| 0x11 | 17 | 0x9811 0011 | ERR\_NODEBUGINTAVAILABLE | No debugging available. |
| 0x12 | 18 | 0x9811 0012 | ERR\_PORTDISABLED | Port disabled – TwinCAT system service not started. |
| 0x13 | 19 | 0x9811 0013 | ERR\_PORTALREADYCONNECTED | Port already connected. |
| 0x14 | 20 | 0x9811 0014 | ERR\_AMSSYNC\_W32ERROR | AMS Sync Win32 error. |
| 0x15 | 21 | 0x9811 0015 | ERR\_AMSSYNC\_TIMEOUT | AMS Sync Timeout. |
| 0x16 | 22 | 0x9811 0016 | ERR\_AMSSYNC\_AMSERROR | AMS Sync error. |
| 0x17 | 23 | 0x9811 0017 | ERR\_AMSSYNC\_NOINDEXINMAP | No index map for AMS Sync available. |
| 0x18 | 24 | 0x9811 0018 | ERR\_INVALIDAMSPORT | Invalid AMS port. |
| 0x19 | 25 | 0x9811 0019 | ERR\_NOMEMORY | No memory. |
| 0x1A | 26 | 0x9811 001A | ERR\_TCPSEND | TCP send error. |
| 0x1B | 27 | 0x9811 001B | ERR\_HOSTUNREACHABLE | Host unreachable. |
| 0x1C | 28 | 0x9811 001C | ERR\_INVALIDAMSFRAGMENT | Invalid AMS fragment. |
| 0x1D | 29 | 0x9811 001D | ERR\_TLSSEND | TLS send error – secure ADS connection failed. |
| 0x1E | 30 | 0x9811 001E | ERR\_ACCESSDENIED | Access denied – secure ADS access denied. |

（4）、Router error codes

| **Hex** | **Dec** | **HRESULT** | **Name** | **Description** |
| --- | --- | --- | --- | --- |
| 0x500 | 1280 | 0x9811 0500 | ROUTERERR\_NOLOCKEDMEMORY | Locked memory cannot be allocated. |
| 0x501 | 1281 | 0x9811 0501 | ROUTERERR\_RESIZEMEMORY | The router memory size could not be changed. |
| 0x502 | 1282 | 0x9811 0502 | ROUTERERR\_MAILBOXFULL | The mailbox has reached the maximum number of possible messages. |
| 0x503 | 1283 | 0x9811 0503 | ROUTERERR\_DEBUGBOXFULL | The Debug mailbox has reached the maximum number of possible messages. |
| 0x504 | 1284 | 0x9811 0504 | ROUTERERR\_UNKNOWNPORTTYPE | The port type is unknown. |
| 0x505 | 1285 | 0x9811 0505 | ROUTERERR\_NOTINITIALIZED | The router is not initialized. |
| 0x506 | 1286 | 0x9811 0506 | ROUTERERR\_PORTALREADYINUSE | The port number is already assigned. |
| 0x507 | 1287 | 0x9811 0507 | ROUTERERR\_NOTREGISTERED | The port is not registered. |
| 0x508 | 1288 | 0x9811 0508 | ROUTERERR\_NOMOREQUEUES | The maximum number of ports has been reached. |
| 0x509 | 1289 | 0x9811 0509 | ROUTERERR\_INVALIDPORT | The port is invalid. |
| 0x50A | 1290 | 0x9811 050A | ROUTERERR\_NOTACTIVATED | The router is not active. |
| 0x50B | 1291 | 0x9811 050B | ROUTERERR\_FRAGMENTBOXFULL | The mailbox has reached the maximum number for fragmented messages. |
| 0x50C | 1292 | 0x9811 050C | ROUTERERR\_FRAGMENTTIMEOUT | A fragment timeout has occurred. |
| 0x50D | 1293 | 0x9811 050D | ROUTERERR\_TOBEREMOVED | The port is removed. |

（5）、General ADS error codes

| **Hex** | **Dec** | **HRESULT** | **Name** | **Description** |
| --- | --- | --- | --- | --- |
| 0x700 | 1792 | 0x9811 0700 | ADSERR\_DEVICE\_ERROR | General device error. |
| 0x701 | 1793 | 0x9811 0701 | ADSERR\_DEVICE\_SRVNOTSUPP | Service is not supported by the server. |
| 0x702 | 1794 | 0x9811 0702 | ADSERR\_DEVICE\_INVALIDGRP | Invalid index group. |
| 0x703 | 1795 | 0x9811 0703 | ADSERR\_DEVICE\_INVALIDOFFSET | Invalid index offset. |
| 0x704 | 1796 | 0x9811 0704 | ADSERR\_DEVICE\_INVALIDACCESS | Reading or writing not permitted. |
| 0x705 | 1797 | 0x9811 0705 | ADSERR\_DEVICE\_INVALIDSIZE | Parameter size not correct. |
| 0x706 | 1798 | 0x9811 0706 | ADSERR\_DEVICE\_INVALIDDATA | Invalid data values. |
| 0x707 | 1799 | 0x9811 0707 | ADSERR\_DEVICE\_NOTREADY | Device is not ready to operate. |
| 0x708 | 1800 | 0x9811 0708 | ADSERR\_DEVICE\_BUSY | Device is busy. |
| 0x709 | 1801 | 0x9811 0709 | ADSERR\_DEVICE\_INVALIDCONTEXT | Invalid operating system context. This can result from use of ADS function blocks in different tasks. It may be possible to resolve this through Multi-task data access synchronization in the PLC. |
| 0x70A | 1802 | 0x9811 070A | ADSERR\_DEVICE\_NOMEMORY | Insufficient memory. |
| 0x70B | 1803 | 0x9811 070B | ADSERR\_DEVICE\_INVALIDPARM | Invalid parameter values. |
| 0x70C | 1804 | 0x9811 070C | ADSERR\_DEVICE\_NOTFOUND | Not found (files, ...). |
| 0x70D | 1805 | 0x9811 070D | ADSERR\_DEVICE\_SYNTAX | Syntax error in file or command. |
| 0x70E | 1806 | 0x9811 070E | ADSERR\_DEVICE\_INCOMPATIBLE | Objects do not match. |
| 0x70F | 1807 | 0x9811 070F | ADSERR\_DEVICE\_EXISTS | Object already exists. |
| 0x710 | 1808 | 0x9811 0710 | ADSERR\_DEVICE\_SYMBOLNOTFOUND | Symbol not found. |
| 0x711 | 1809 | 0x9811 0711 | ADSERR\_DEVICE\_SYMBOLVERSIONINVALID | Invalid symbol version. This can occur due to an online change. Create a new handle. |
| 0x712 | 1810 | 0x9811 0712 | ADSERR\_DEVICE\_INVALIDSTATE | Device (server) is in invalid state. |
| 0x713 | 1811 | 0x9811 0713 | ADSERR\_DEVICE\_TRANSMODENOTSUPP | AdsTransMode not supported. |
| 0x714 | 1812 | 0x9811 0714 | ADSERR\_DEVICE\_NOTIFYHNDINVALID | Notification handle is invalid. |
| 0x715 | 1813 | 0x9811 0715 | ADSERR\_DEVICE\_CLIENTUNKNOWN | Notification client not registered. |
| 0x716 | 1814 | 0x9811 0716 | ADSERR\_DEVICE\_NOMOREHDLS | No further handle available. |
| 0x717 | 1815 | 0x9811 0717 | ADSERR\_DEVICE\_INVALIDWATCHSIZE | Notification size too large. |
| 0x718 | 1816 | 0x9811 0718 | ADSERR\_DEVICE\_NOTINIT | Device not initialized. |
| 0x719 | 1817 | 0x9811 0719 | ADSERR\_DEVICE\_TIMEOUT | Device has a timeout. |
| 0x71A | 1818 | 0x9811 071A | ADSERR\_DEVICE\_NOINTERFACE | Interface query failed. |
| 0x71B | 1819 | 0x9811 071B | ADSERR\_DEVICE\_INVALIDINTERFACE | Wrong interface requested. |
| 0x71C | 1820 | 0x9811 071C | ADSERR\_DEVICE\_INVALIDCLSID | Class ID is invalid. |
| 0x71D | 1821 | 0x9811 071D | ADSERR\_DEVICE\_INVALIDOBJID | Object ID is invalid. |
| 0x71E | 1822 | 0x9811 071E | ADSERR\_DEVICE\_PENDING | Request pending. |
| 0x71F | 1823 | 0x9811 071F | ADSERR\_DEVICE\_ABORTED | Request is aborted. |
| 0x720 | 1824 | 0x9811 0720 | ADSERR\_DEVICE\_WARNING | Signal warning. |
| 0x721 | 1825 | 0x9811 0721 | ADSERR\_DEVICE\_INVALIDARRAYIDX | Invalid array index. |
| 0x722 | 1826 | 0x9811 0722 | ADSERR\_DEVICE\_SYMBOLNOTACTIVE | Symbol not active. |
| 0x723 | 1827 | 0x9811 0723 | ADSERR\_DEVICE\_ACCESSDENIED | Access denied. |
| 0x724 | 1828 | 0x9811 0724 | ADSERR\_DEVICE\_LICENSENOTFOUND | Missing license. |
| 0x725 | 1829 | 0x9811 0725 | ADSERR\_DEVICE\_LICENSEEXPIRED | License expired. |
| 0x726 | 1830 | 0x9811 0726 | ADSERR\_DEVICE\_LICENSEEXCEEDED | License exceeded. |
| 0x727 | 1831 | 0x9811 0727 | ADSERR\_DEVICE\_LICENSEINVALID | Invalid license. |
| 0x728 | 1832 | 0x9811 0728 | ADSERR\_DEVICE\_LICENSESYSTEMID | License problem: System ID is invalid. |
| 0x729 | 1833 | 0x9811 0729 | ADSERR\_DEVICE\_LICENSENOTIMELIMIT | License not limited in time. |
| 0x72A | 1834 | 0x9811 072A | ADSERR\_DEVICE\_LICENSEFUTUREISSUE | License problem: Time in the future. |
| 0x72B | 1835 | 0x9811 072B | ADSERR\_DEVICE\_LICENSETIMETOLONG | License period too long. |
| 0x72C | 1836 | 0x9811 072C | ADSERR\_DEVICE\_EXCEPTION | Exception at system startup. |
| 0x72D | 1837 | 0x9811 072D | ADSERR\_DEVICE\_LICENSEDUPLICATED | License file read twice. |
| 0x72E | 1838 | 0x9811 072E | ADSERR\_DEVICE\_SIGNATUREINVALID | Invalid signature. |
| 0x72F | 1839 | 0x9811 072F | ADSERR\_DEVICE\_CERTIFICATEINVALID | Invalid certificate. |
| 0x730 | 1840 | 0x9811 0730 | ADSERR\_DEVICE\_LICENSEOEMNOTFOUND | Public key not known from OEM. |
| 0x731 | 1841 | 0x9811 0731 | ADSERR\_DEVICE\_LICENSERESTRICTED | License not valid for this system ID. |
| 0x732 | 1842 | 0x9811 0732 | ADSERR\_DEVICE\_LICENSEDEMODENIED | Demo license prohibited. |
| 0x733 | 1843 | 0x9811 0733 | ADSERR\_DEVICE\_INVALIDFNCID | Invalid function ID. |
| 0x734 | 1844 | 0x9811 0734 | ADSERR\_DEVICE\_OUTOFRANGE | Outside the valid range. |
| 0x735 | 1845 | 0x9811 0735 | ADSERR\_DEVICE\_INVALIDALIGNMENT | Invalid alignment. |
| 0x736 | 1846 | 0x9811 0736 | ADSERR\_DEVICE\_LICENSEPLATFORM | Invalid platform level. |
| 0x737 | 1847 | 0x9811 0737 | ADSERR\_DEVICE\_FORWARD\_PL | Context – forward to passive level. |
| 0x738 | 1848 | 0x9811 0738 | ADSERR\_DEVICE\_FORWARD\_DL | Context – forward to dispatch level. |
| 0x739 | 1849 | 0x9811 0739 | ADSERR\_DEVICE\_FORWARD\_RT | Context – forward to real-time. |
| 0x740 | 1856 | 0x9811 0740 | ADSERR\_CLIENT\_ERROR | Client error. |
| 0x741 | 1857 | 0x9811 0741 | ADSERR\_CLIENT\_INVALIDPARM | Service contains an invalid parameter. |
| 0x742 | 1858 | 0x9811 0742 | ADSERR\_CLIENT\_LISTEMPTY | Polling list is empty. |
| 0x743 | 1859 | 0x9811 0743 | ADSERR\_CLIENT\_VARUSED | Var connection already in use. |
| 0x744 | 1860 | 0x9811 0744 | ADSERR\_CLIENT\_DUPLINVOKEID | The called ID is already in use. |
| 0x745 | 1861 | 0x9811 0745 | ADSERR\_CLIENT\_SYNCTIMEOUT | Timeout has occurred – the remote terminal is not responding in the specified ADS timeout. The route setting of the remote terminal may be configured incorrectly. |
| 0x746 | 1862 | 0x9811 0746 | ADSERR\_CLIENT\_W32ERROR | Error in Win32 subsystem. |
| 0x747 | 1863 | 0x9811 0747 | ADSERR\_CLIENT\_TIMEOUTINVALID | Invalid client timeout value. |
| 0x748 | 1864 | 0x9811 0748 | ADSERR\_CLIENT\_PORTNOTOPEN | Port not open. |
| 0x749 | 1865 | 0x9811 0749 | ADSERR\_CLIENT\_NOAMSADDR | No AMS address. |
| 0x750 | 1872 | 0x9811 0750 | ADSERR\_CLIENT\_SYNCINTERNAL | Internal error in Ads sync. |
| 0x751 | 1873 | 0x9811 0751 | ADSERR\_CLIENT\_ADDHASH | Hash table overflow. |
| 0x752 | 1874 | 0x9811 0752 | ADSERR\_CLIENT\_REMOVEHASH | Key not found in the table. |
| 0x753 | 1875 | 0x9811 0753 | ADSERR\_CLIENT\_NOMORESYM | No symbols in the cache. |
| 0x754 | 1876 | 0x9811 0754 | ADSERR\_CLIENT\_SYNCRESINVALID | Invalid response received. |
| 0x755 | 1877 | 0x9811 0755 | ADSERR\_CLIENT\_SYNCPORTLOCKED | Sync Port is locked. |

（6）RTime error codes

| **Hex** | **Dec** | **HRESULT** | **Name** | **Description** |
| --- | --- | --- | --- | --- |
| 0x1000 | 4096 | 0x9811 1000 | RTERR\_INTERNAL | Internal error in the real-time system. |
| 0x1001 | 4097 | 0x9811 1001 | RTERR\_BADTIMERPERIODS | Timer value is not valid. |
| 0x1002 | 4098 | 0x9811 1002 | RTERR\_INVALIDTASKPTR | Task pointer has the invalid value 0 (zero). |
| 0x1003 | 4099 | 0x9811 1003 | RTERR\_INVALIDSTACKPTR | Stack pointer has the invalid value 0 (zero). |
| 0x1004 | 4100 | 0x9811 1004 | RTERR\_PRIOEXISTS | The request task priority is already assigned. |
| 0x1005 | 4101 | 0x9811 1005 | RTERR\_NOMORETCB | No free TCB (Task Control Block) available. The maximum number of TCBs is 64. |
| 0x1006 | 4102 | 0x9811 1006 | RTERR\_NOMORESEMAS | No free semaphores available. The maximum number of semaphores is 64. |
| 0x1007 | 4103 | 0x9811 1007 | RTERR\_NOMOREQUEUES | No free space available in the queue. The maximum number of positions in the queue is 64. |
| 0x100D | 4109 | 0x9811 100D | RTERR\_EXTIRQALREADYDEF | An external synchronization interrupt is already applied. |
| 0x100E | 4110 | 0x9811 100E | RTERR\_EXTIRQNOTDEF | No external sync interrupt applied. |
| 0x100F | 4111 | 0x9811 100F | RTERR\_EXTIRQINSTALLFAILED | Application of the external synchronization interrupt has failed. |
| 0x1010 | 4112 | 0x9811 1010 | RTERR\_IRQLNOTLESSOREQUAL | Call of a service function in the wrong context |
| 0x1017 | 4119 | 0x9811 1017 | RTERR\_VMXNOTSUPPORTED | Intel VT-x extension is not supported. |
| 0x1018 | 4120 | 0x9811 1018 | RTERR\_VMXDISABLED | Intel VT-x extension is not enabled in the BIOS. |
| 0x1019 | 4121 | 0x9811 1019 | RTERR\_VMXCONTROLSMISSING | Missing function in Intel VT-x extension. |
| 0x101A | 4122 | 0x9811 101A | RTERR\_VMXENABLEFAILS | Activation of Intel VT-x fails. |

（6）TCP Winsock error codes

| **Hex** | **Dec** | **Name** | **Description** |
| --- | --- | --- | --- |
| 0x274C | 10060 | WSAETIMEDOUT | A connection timeout has occurred - error while establishing the connection, because the remote terminal did not respond properly after a certain period of time, or the established connection could not be maintained because the connected host did not respond. |
| 0x274D | 10061 | WSAECONNREFUSED | Connection refused - no connection could be established because the target computer has explicitly rejected it. This error usually results from an attempt to connect to a service that is inactive on the external host, that is, a service for which no server application is running. |
| 0x2751 | 10065 | WSAEHOSTUNREACH | No route to host - a socket operation referred to an unavailable host. |
| More Winsock error codes: Win32 error codes | | | |

**上海（ 中国区总部）**

中国上海市静安区汶水路 299 弄 9号（市北智汇园）

电话: 021-66312666 传真: 021-66315696 邮编：200072

**北京分公司**

北京市西城区新街口北大街 3 号新街高和大厦 407 室

电话: 010-82200036 传真: 010-82200039 邮编：100035

**广州分公司**

广州市天河区珠江新城珠江东路16号高德置地G2603室

电话: 020-38010300/1/2 传真: 020-38010303 邮编：510623

**成都分公司**

成都市锦江区东御街18号 百扬大厦2305 房

电话: 028-86202581 传真: 028-86202582 邮编：610016

|  |  |
| --- | --- |
| 请用微信扫描二维码  通过公众号与技术支持交流 |  |
| 倍福中文官网：  https://www.beckhoff.com.cn/ |
| 倍福虚拟学院：  https://tr.beckhoff.com.cn/ |
| 招贤纳士：job@beckhoff.com.cn  技术支持：support@beckhoff.com.cn  产品维修：service@beckhoff.com.cn  方案咨询：sales@beckhoff.com.cn |