|  |  |  |  |
| --- | --- | --- | --- |
| 作者： | 关春雨 | | [Logo_Beckhoff_Red](http://www.beckhoff.com.cn/)  北京市海淀区魏公村路6号院丽金智地中心1号楼西塔901室  邮编（100035）  TEL: 010-82200036-634  FAX: 010-82200039 |
| 职务： | 技术工程师 |  |
| 日期： | 2025年6月20日 星期五 | |

|  |
| --- |
| **TF6500 | TwinCAT 3 IEC 60870-5-104 通讯测试** |
| **摘 要**：IEC104规约是一个广泛应用于电力、城市轨道交通等行业的国际标准。IEC104规约由国际电工委员会制定。IEC104规约把IEC101的应用服务数据单元（ASDU）用网络规约TCP/IP进行传输的标准，该标准为远动信息的网络传输提供了通信规约依据。采用104规约组合101规约的ASDU的方式后,可很好的保证规约的标准化和通信的可靠性。  TF6500提供两种方式进行IEC104通讯。‘High level’方式将所有功能封装到一个PLC功能块中，可实现90%的应用，程序员不必完全熟悉协议标准。‘Low level’方式允许自定义ASDU中的所有内容，但需要大量的编程工作，程序员必须熟悉协议标准。 |
| 在杨志伟文档基础上，做了相应的修改和完善，和其它如101通讯等一起归档总结。  **关键字：**IEC60870-5-104，IEC104，TwinCAT3，TF6500 |
| **附 件：**   |  |  |  | | --- | --- | --- | | 序 号 | 文件名 | 备注 | |  |  |  | |  |  |  | |
| **历史版本：**  V1.0 IEC60870-5-104通讯测试 杨志伟测试编写 |
| **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，也欢迎您提出改进建议。 |

**目 录**

[1 软硬件版本 3](#_Toc201655636)

[1.1 倍福Beckhoff 3](#_Toc201655637)

[1.1.1 控制器硬件 3](#_Toc201655638)

[1.1.2 控制软件 3](#_Toc201655639)

[2 准备工作 3](#_Toc201655640)

[2.1 软件安装 3](#_Toc201655641)

[2.2 网络接线 3](#_Toc201655642)

[2.3 下载测试例程 3](#_Toc201655643)

[3 操作步骤 4](#_Toc201655644)

[3.1 打开测试例程 4](#_Toc201655645)

[3.2 扫描并连接控制器 5](#_Toc201655646)

[3.3 ‘High level’Slave程序更改及解析 6](#_Toc201655647)

[3.3.1 总览 6](#_Toc201655648)

[3.3.2 初始化IP地址及端口号 6](#_Toc201655649)

[3.3.3 初始化地址长度参数 7](#_Toc201655650)

[3.3.4 信息体初始化1 7](#_Toc201655651)

[3.3.5 信息体初始化2 8](#_Toc201655652)

[3.3.6 信息体初始化3 9](#_Toc201655653)

[3.3.7 Slave执行的功能块 10](#_Toc201655654)

[3.3.8 遥测、遥信变位测试程序 11](#_Toc201655655)

[3.3.9 信息体定义 13](#_Toc201655656)

[3.4 主站从站通讯测试和变量传输 13](#_Toc201655657)

[3.4.1 主从站连接状态查看 13](#_Toc201655658)

[3.4.2 主从站数据传送查看 14](#_Toc201655659)

[3.5 第三方工具测试 15](#_Toc201655660)

# 软硬件版本

## 倍福Beckhoff

### 控制器硬件

|  |  |  |  |
| --- | --- | --- | --- |
| 型号 | 数量 | TwinCat版本 | 用途 |
| CX2020-0120 | 1 | v3.1.4018.4 /WES7 32-bit | 104 slave端/104 master端 |
| 笔记本电脑 | 1 | v3.1.4024.12/Win10 64-bit | 作为编程笔记本、104 slave端/104 master端 |

### 控制软件

TF6500-IEC-60870-5-10x v3.0.7.0

# 准备工作

## 软件安装

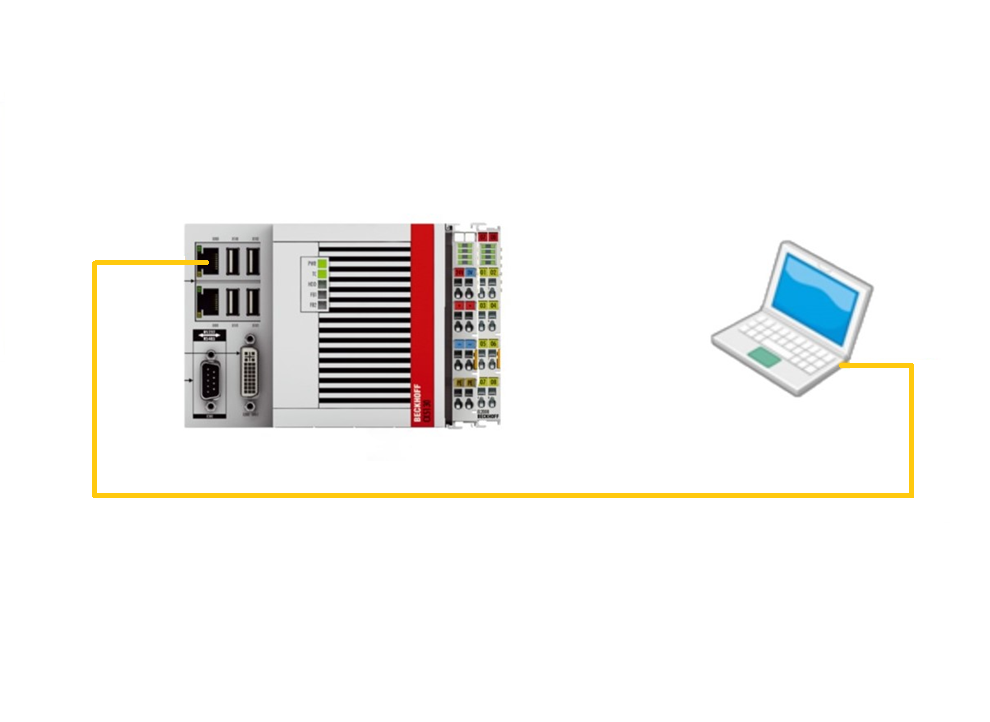
控制器及笔记本电脑上都需安装TF6500软件。

TF6500下载地址：

[TF6500 | TwinCAT 3 IEC 60870-5-10x | Beckhoff Worldwide](https://www.beckhoff.com/en-en/products/automation/twincat/tfxxxx-twincat-3-functions/tf6xxx-tc3-connectivity/tf6500.html)

## 网络接线

倍福控制器上有两个内置交换机的网口，接线如下：



将控制器和笔记本电脑设为同一网段。

控制器IP：

IP：169.254.6.146 子网掩码：255.255.0.0

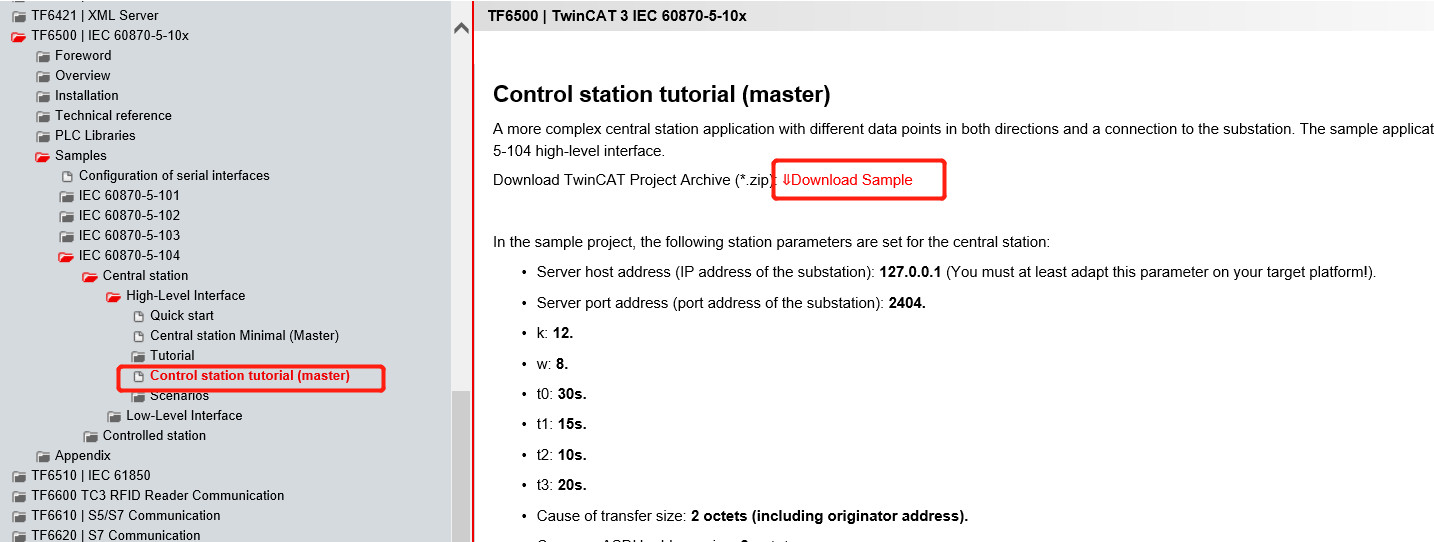
IP：169.254.12.13 子网掩码：255.255.0.0

## 下载测试例程

下载网站：[Beckhoff Information System - German](https://infosys.beckhoff.com/)

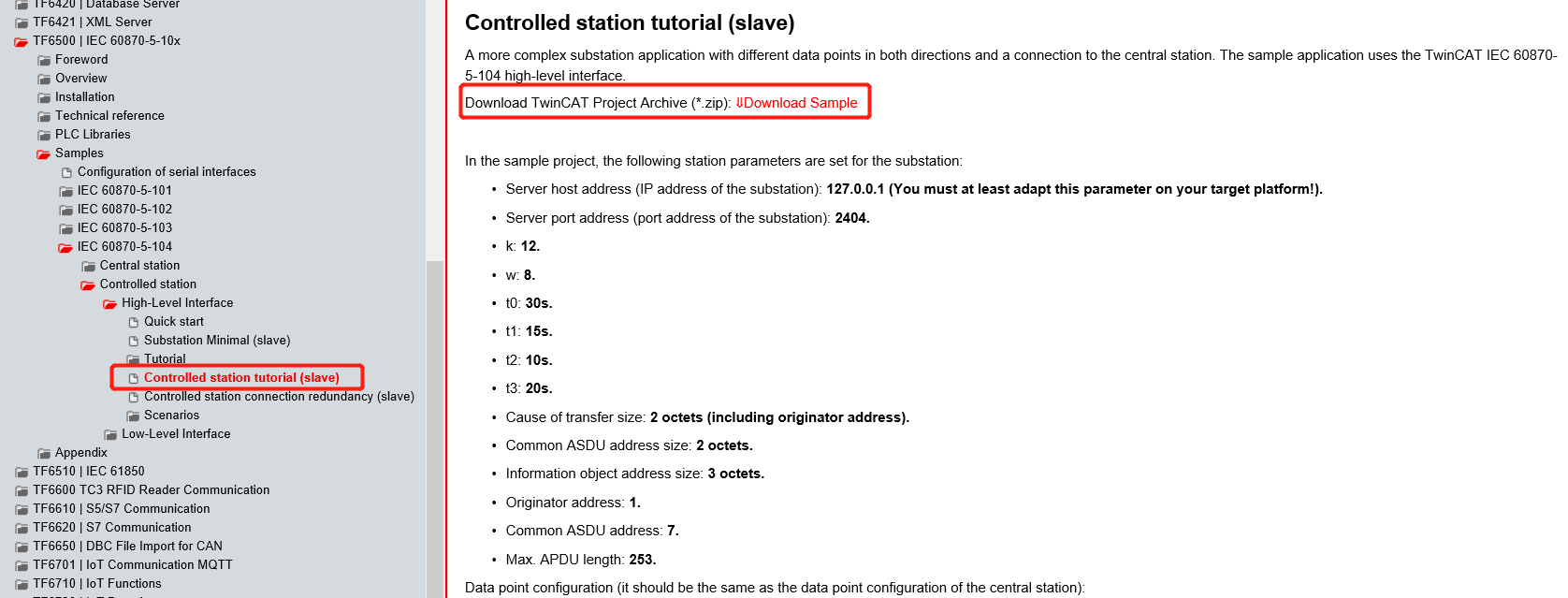
Master:

TwinCAT3 => TFxxxx | Functions => TF6xxx – Connectivity => TF6500 | TwinCAT 3 IEC 60870-5-10x => Samples => IEC 60870-5-104 => Central station => High-Level Interface =>Control station tutorial (master)



Slave:

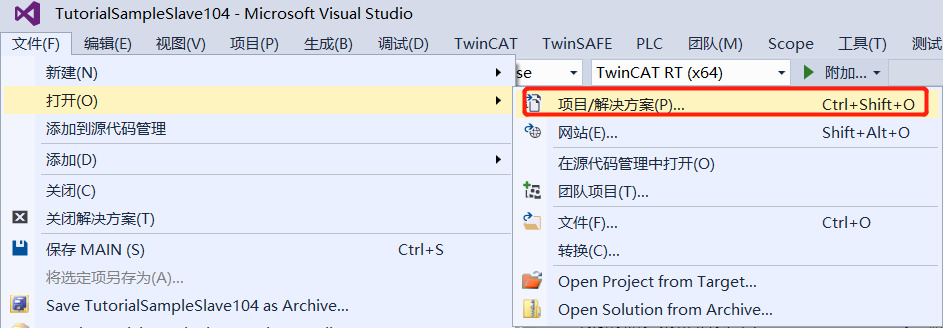
TwinCAT3 => TFxxxx | Functions => TF6xxx – Connectivity => TF6500 | TwinCAT 3 IEC 60870-5-10x => Samples => IEC 60870-5-104 => Controlled station => High-Level Interface => Controlled station tutorial (slave)



# 操作步骤

## 打开测试例程

下载的例程都为.tszip结尾的，按照以下方式打开：



## 扫描并连接控制器

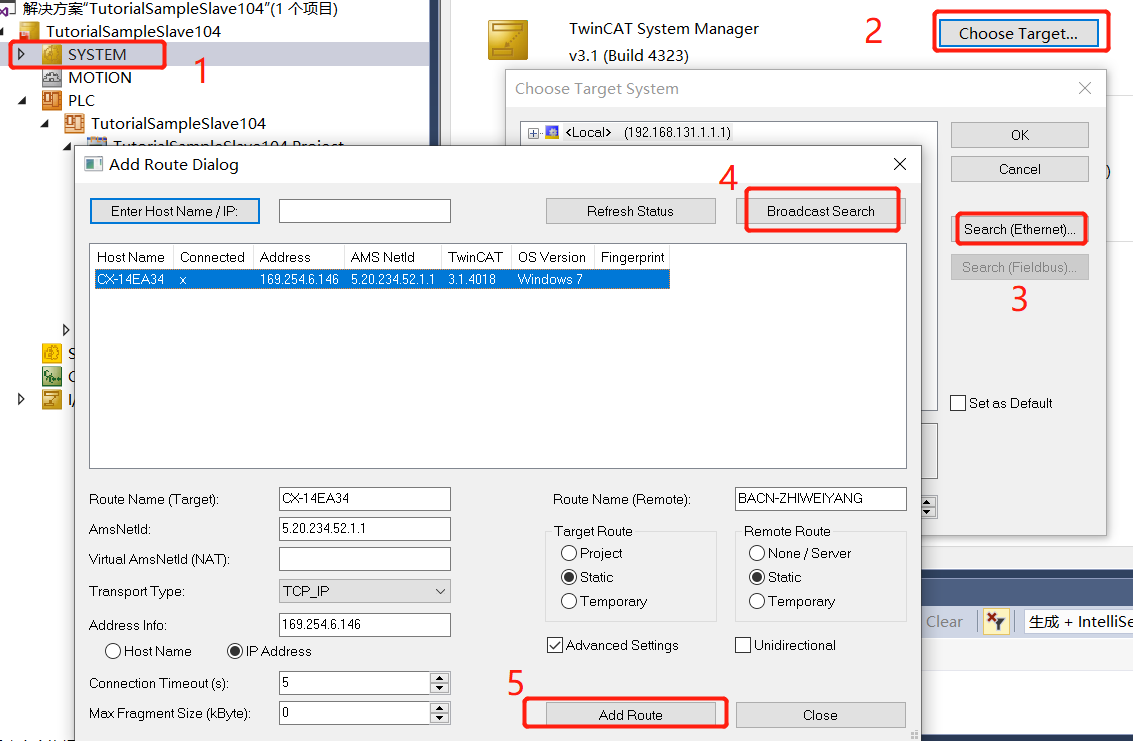
单击SYSYTEM，点击Choose Target..，在弹出的框里点击Search(Ethernet)…，在弹出的框里点击Broadcast Search进行广播搜索。

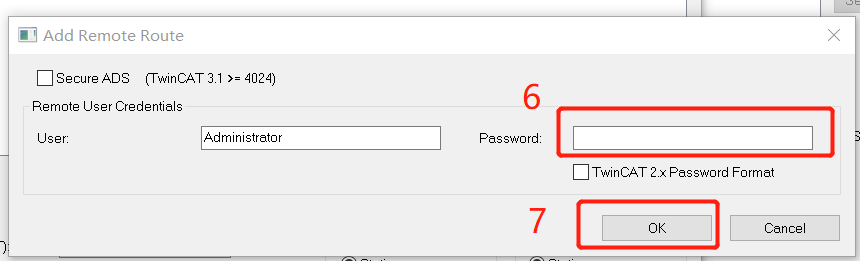
搜索出来控制器后使用IP的方式添加路由，点击Add Route。在弹出框中输入用户名和密码。

用户名：Administrator

密码：1

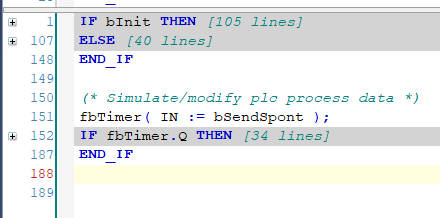
点击OK，如果Connected列表里有x表明已经连接上控制器。





## ‘High level’Slave程序更改及解析

### 总览

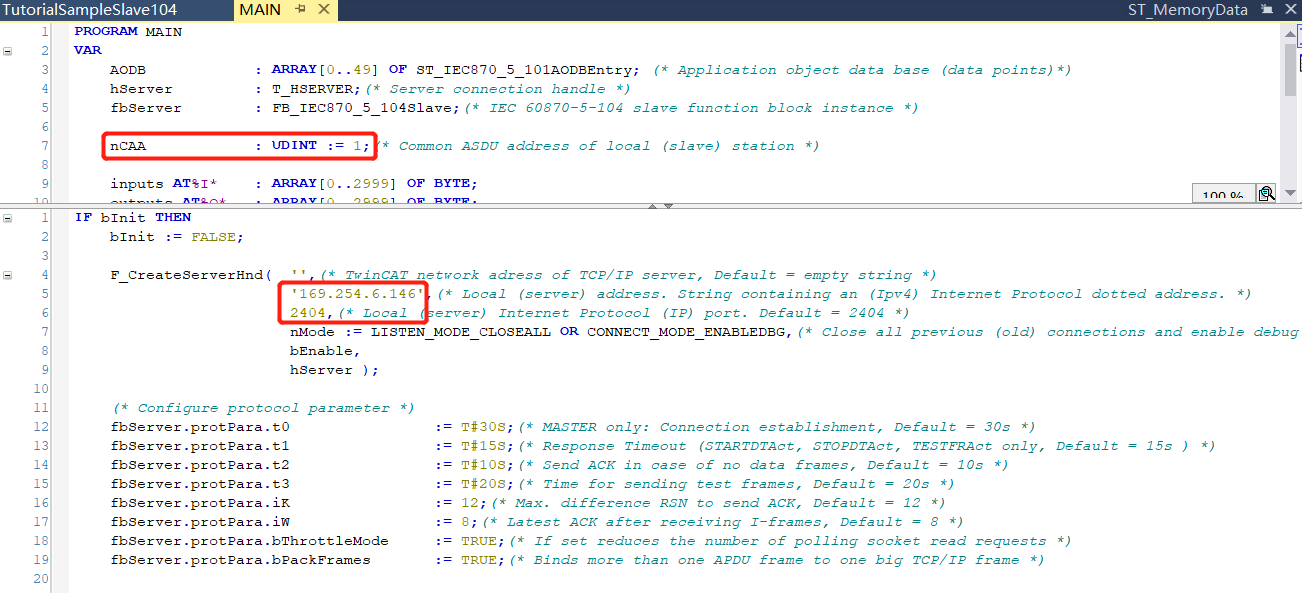


第一个IF …ELSE中为通讯初始化内容，TCPIP通讯IP及端口设置、104通讯参数设置、104通讯类型及信息体地址设置等。

第一个ELSE…END\_IF为Slave执行的功能块。

第二个IF…END\_IF为做遥测、遥信变位测试程序。

### 初始化IP地址及端口号

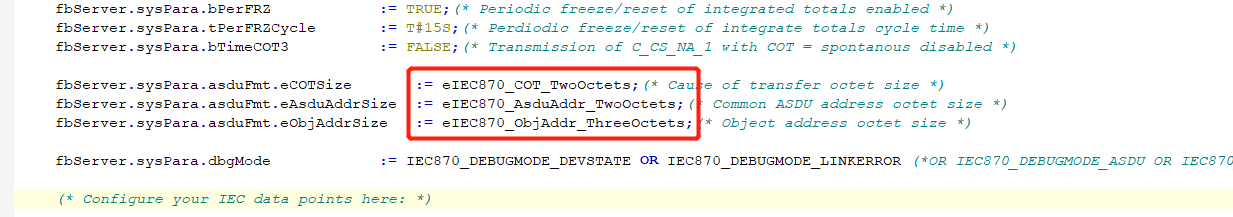


在nCAA更改ASDU公共地址为1。

在F\_CreateServerHnd（）里更改IP地址为Slave端地址，即控制器的IP地址：169.254.6.146。端口号固定为2404。

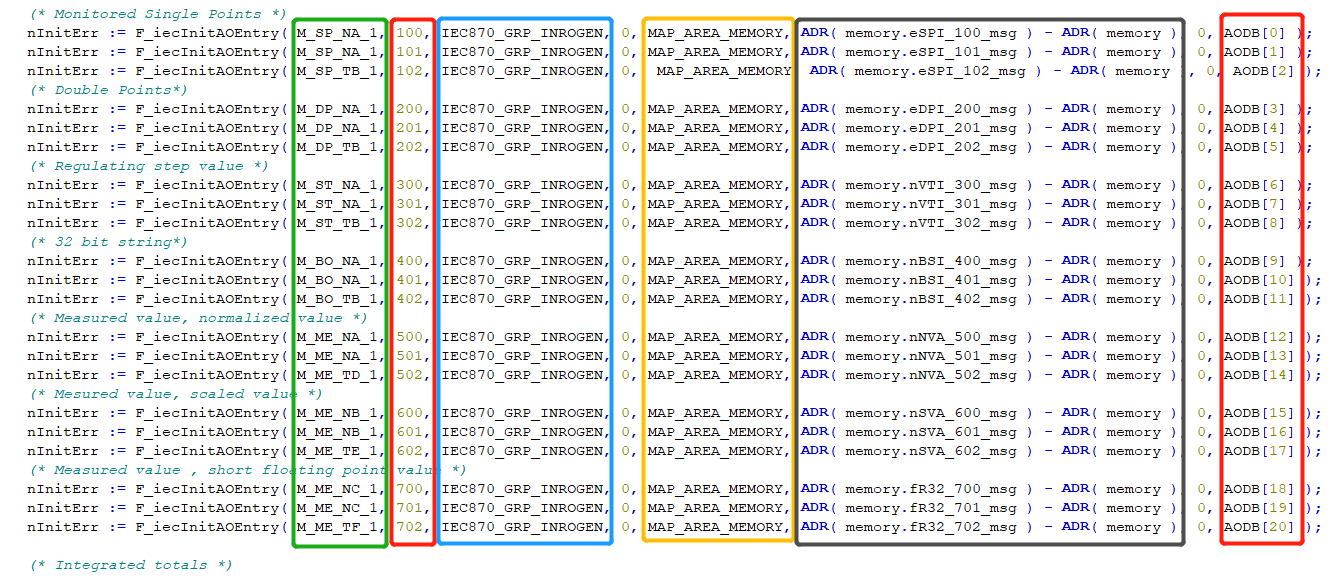
这里IP地址、ASDU公共地址及端口号一定要和master端一致。否则无法建立链路通讯。

### 初始化地址长度参数



上图红框中从上到下依次为传送原因地址长度、ASDU地址长度、信息体地址长度。此处须和master端一致，否则会出现报文传送异常错误。

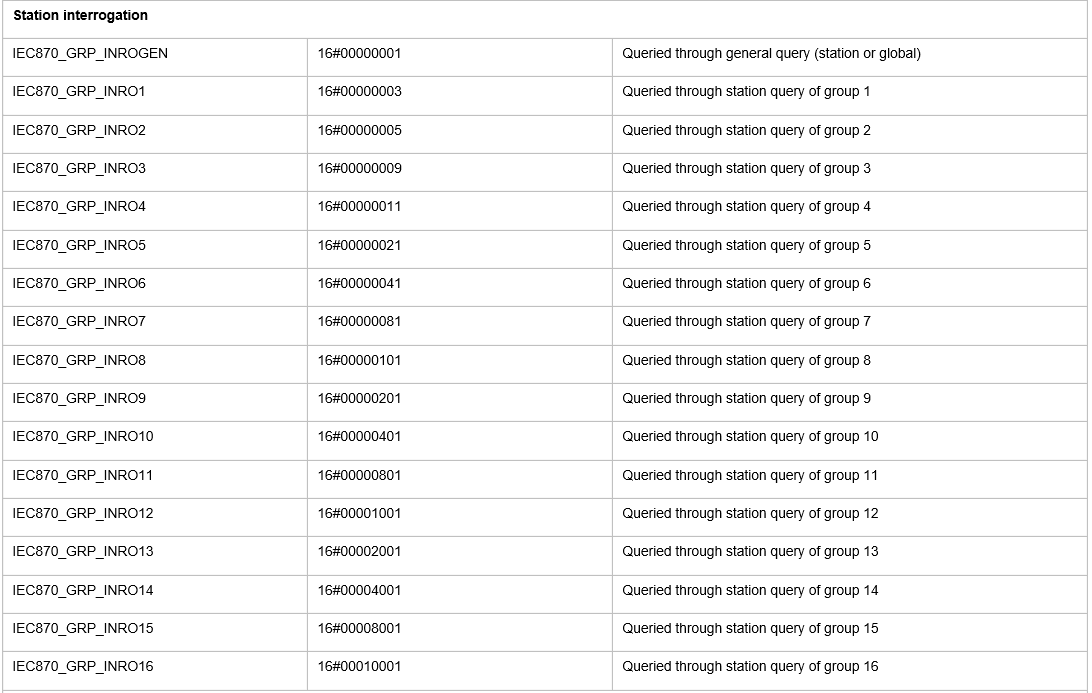
### 信息体初始化1



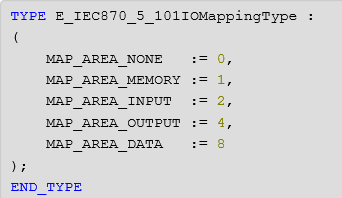
* 纵向看三个一组分别是单点遥信、双点遥信、步位置信息、32位比特串、归一化测量值、标度化测量值、短浮点测量值。
* 横向看绿色框内是类型标识符：

|  |  |  |
| --- | --- | --- |
| 类型标识符号 | 解释 | 类型标识符 |
| M\_SP\_NA\_1 | 单点信息 | 1 |
| M\_SP\_TB\_1 | 带CP56Time2a时标的单点信息 | 30 |
| M\_DP\_NA\_1 | 双点信息 | 3 |
| M\_DP\_TB\_1 | 带CP56Time2a时标的双点信息 | 31 |
| M\_ST\_NA\_1 | 步位置信息 | 5 |
| M\_ST\_TB\_1 | 带CP56Time2a时标的步位置信息 | 32 |
| M\_BO\_NA\_1 | 32比特串 | 7 |
| M\_BO\_TB\_1 | 带CP56Time2a时标的32比特串 | 33 |
| M\_ME\_NA\_1 | 测量值，规一化值 | 9 |
| M\_ME\_TD\_1 | 带CP56Time2a时标的测量值，规一化值 | 34 |
| M\_ME\_NB\_1 | 测量值，标度化值 | 11 |
| M\_ME\_TE\_1 | 带CP56Time2a时标的测量值，标度化值 | 35 |
| M\_ME\_NC\_1 | 测量值，短浮点数 | 13 |
| M\_ME\_TF\_1 | 带CP56Time2a时标的测量值，短浮点数 | 36 |

* 第一个红色框内为信息体地址，这里须和master每个点地址保持一致。建议遍程前建立典表，按照约定好的典表进行遍程。
* 蓝色框内为应用对象组配置标志，例程中都配备到了全局组，也可以根据需要配置到1~16组内，如下图所示。配备到全局组或其他组master可以使用总招全部将数据查询上来，如果只配备到了1~16组内，master也可单独查询某一组内数据。



* 蓝色框右边为用于循环/周期性数据传输的基本周期时间乘法器，0=禁用，基本周期时间可以通过系统参数中的tPerCyclicBase参数进行配置。循环/周期性数据传输周期=乘法器\*基本周期时间。
* 黄色框内为PLC内部地址区域映射，由于要传送的变量（例如memory.eSPI\_100\_msg）定义在了M区（AT%M\*），所以映射标志符为MAP\_AREA\_MEMORY，当然也可映射到I区和Q区。



* 黑色框内为变量的字节偏移量映射，黑色框后面为变量的位偏移量映射。例如单点信息变量memory.eSPI\_100\_msg，它定义在ST\_MemoryData结构体内，在Man程序里实例化为memory，memory定义为AT%M\*，所以memory.eSPI\_100\_msg的字节偏移量映射为“ADR( memory.eSPI\_100\_msg ) - ADR( memory )”，位偏移量为0。



* 最后一个红色框内为数据库元素初始化AODB，这里会存放信息体元素的一些配置信息、通讯原因等信息。此处需要注意所有信息体元素的AODB都不相同，AODB的数组大小最好和信息体元素个数近似相等，总召时会等AODB里面的所有元素上发完后才会收到总召结束报文，合理的AODB长度会减少总召时间。

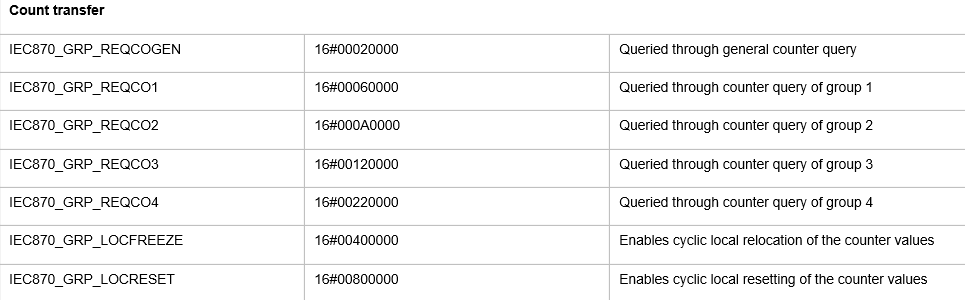
### 信息体初始化2



* 绿色框内为类型标识符：

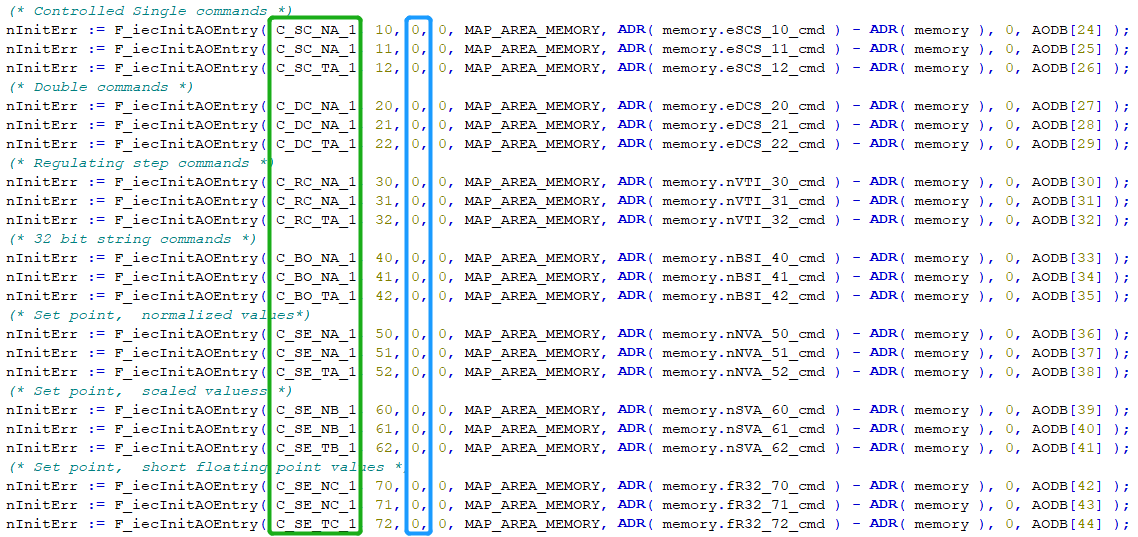
|  |  |  |
| --- | --- | --- |
| 类型标识符号 | 解释 | 类型标识符 |
| M\_IT\_NA\_1 | 累计量 | 15 |
| M\_IT\_TB\_1 | 带CP56Time2a时标的累计量 | 37 |

* 蓝色框为应用对象组配置标志，例程中设置为计数量总召并且启用自发传送的局部冻结。



* 其他信息同信息初始化1描述

### 信息体初始化3

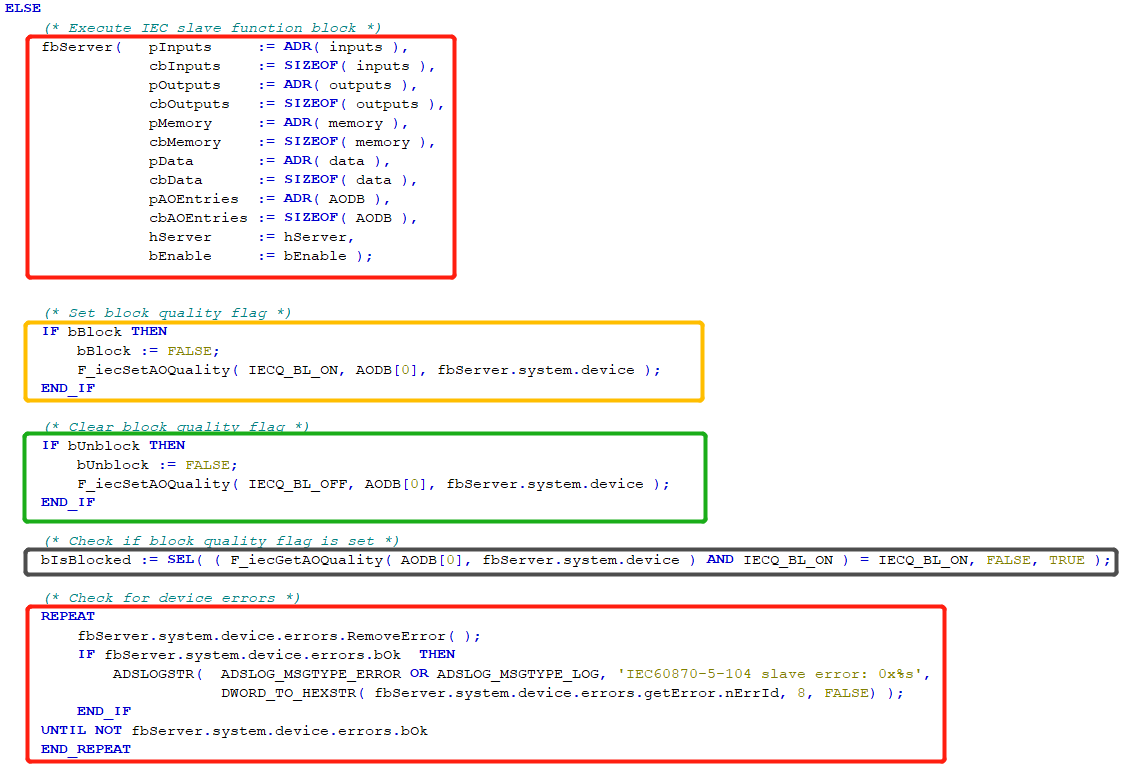


* 绿色框内为类型标识符：

|  |  |  |
| --- | --- | --- |
| 类型标识符号 | 解释 | 类型标识符 |
| C\_SC\_NA\_1 | 单点命令 | 45 |
| C\_SC\_TA\_1 | 带CP56Time2a时标的单点命令 | 58 |
| C\_DC\_NA\_1 | 双点命令 | 46 |
| C\_DC\_TA\_1 | 带CP56Time2a时标的双点命令 | 59 |
| C\_RC\_NA\_1 | 升降命令 | 47 |
| C\_RC\_TA\_1 | 带CP56Time2a时标的升降命令 | 60 |
| C\_BO\_NA\_1 | 32比特串 | 51 |
| C\_BO\_TA\_1 | 带CP56Time2a时标的32比特串 | 64 |
| C\_SE\_NA\_1 | 设定值命令，规一化值 | 48 |
| C\_SE\_TA\_1 | 带CP56Time2a时标的设定值命令，规一化值 | 61 |
| C\_SE\_NB\_1 | 设定值命令，标度化值 | 49 |
| C\_SE\_TB\_1 | 带CP56Time2a时标的设定值命令，标度化值 | 62 |
| C\_SE\_NC\_1 | 设定值命令，短浮点数 | 50 |
| C\_SE\_TC\_1 | 带CP56Time2a时标的设定值命令，短浮点数 | 63 |

* 蓝色框内为对象组配置标志，例程中设置为0。

### Slave执行的功能块



* 第一个红色框内fbServer为Slave执行的功能块，实例化的功能块为FB\_IEC870\_5\_104Slave。

pInputs => PLC处理数据输入区起始地址。cbInputs => PLC处理数据输入区字节大小。

pOutputs => PLC处理数据输出区起始地址。cbOutputs => PLC处理数据输出区字节大小。

pMemory => PLC数据区在缓存区起始地址。cbMemory => PLC处理数据缓存区区字节大小。

pData => PLC数据区域的起始地址。cbData => PLC数据区域字节大小。

pAOEntries => 数据库AODB变量起始地址。cbAOEntries => 数据库AODB变量字节大小。

hServer => TCP/IP服务器句柄。

bEnable => 激活或关闭功能块。从初始化区的F\_CreateServerHnd函数中得到。

Inputs、Outputs、Memory、Data区按照信息体地址的定义得到。如所有信息体定义在M区，可只定义pMemory和cbMemory。如果将多种数据类型定义在M区时，可参照例程建立一个结构体进行管理。

* 黄色框和绿色框内为设置块质量标志例程段，设置AODB[0]的质量标志，即地址为100的单点遥信的质量标志。使用F\_iecSetAOQuality函数进行设置。

IECQ\_BL\_ON => 要设置的质量标志-封锁。

|  |  |  |
| --- | --- | --- |
| IECQ\_BL\_ON | 16#0001 | 封锁 |
| IECQ\_BL\_OFF | 16#0002 | 未被封锁 |
| IECQ\_SB\_ON | 16#0004 | 取代 |
| IECQ\_SB\_OFF | 16#0008 | 未被取代 |
| IECQ\_NT\_ON | 16#0010 | 非当前值 |
| IECQ\_NT\_OFF | 16#0020 | 当前值 |
| IECQ\_IV\_ON | 16#0040 | 不可用 |
| IECQ\_IV\_OFF | 16#0080 | 可用 |
| IECQ\_OV\_ON | 16#0100 | 溢出 |
| IECQ\_OV\_OFF | 16#0200 | 未溢出 |
| IECQ\_EI\_ON | 16#0400 | 时间无效 |
| IECQ\_EI\_OFF | 16#0800 | 时间有效 |
| IECQ\_CY\_ON | 16#1000 | 相应累计时段内计数器溢出carry |
| IECQ\_CY\_OFF | 16#2000 | 相应累计时段内计数器未溢出carry |
| IECQ\_CA\_ON | 16#4000 | 累积量设置/上次读数后被调整 |
| IECQ\_CA\_OFF | 16#8000 | 累积量未设置/上次读数后未调整 |

AODB[0] => 要设置其质量标志状态的应用程序对象。

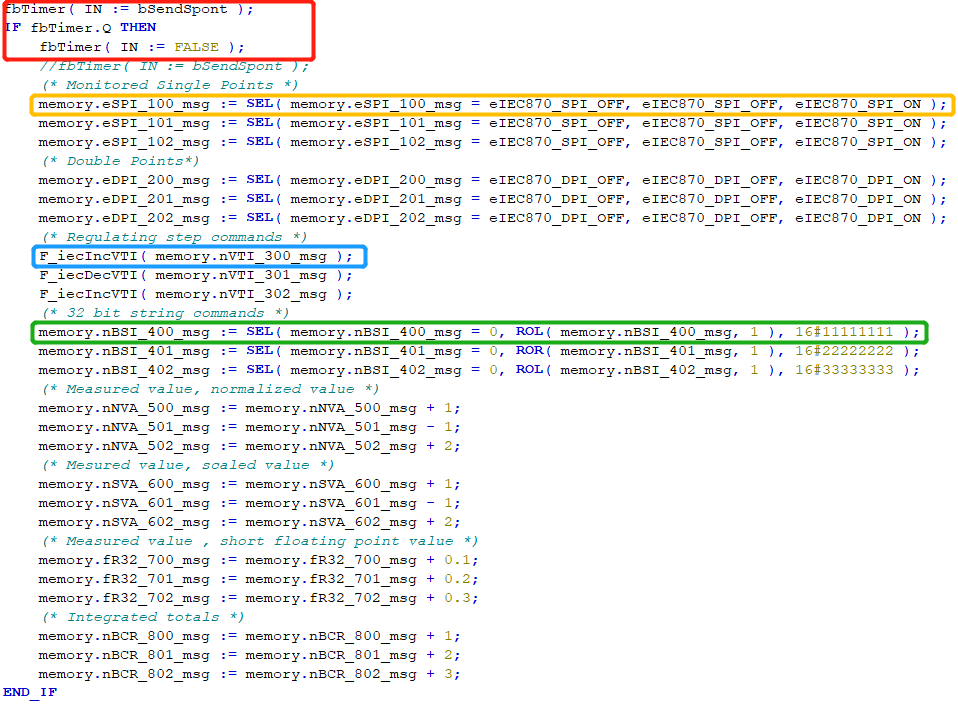
fbServer.system.device => IEC设备通信接口。

* 黑色框内为读取所设质量标志的值，使用F\_iecGetAOQuality函数进行读取。使用F\_iecGetAOQuality读取出来的是整个质量码，需要对质量码进行解析：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bit7 | Bit6 | Bit5 | Bit4 | Bit3 | Bit2 | Bit1 | Bit0 |
| IECQ\_IV\_OFF | IECQ\_IV\_ON | IECQ\_NT\_OFF | IECQ\_NT\_ON | IECQ\_SB\_OFF | IECQ\_SB\_ON | IECQ\_BL\_OFF | IECQ\_BL\_ON |

* 红色框内是将通讯中遇到的错误信息输送到错误列表中。

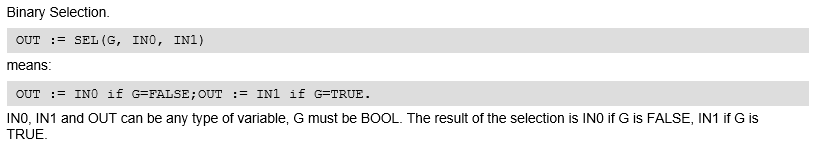
### 遥测、遥信变位测试程序



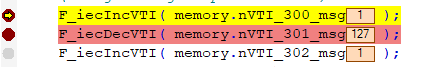
* 红色方框为TON延时程序，延时时间为10s。每十秒刷新一次IF里面的语句，即每十秒进行一次变位，并进行变位上传。



* 黄色方框内为单点遥信变位设置，SEL函数解释如下，如果G为False，则OUT=IN0；如果G为True，则OUT=IN1。针对黄色框内的单点遥信解释，如果memory.eSPI\_100\_msg为OFF，则memory.eSPI\_100\_msg为ON，如此每10s进行一次遥信变位。



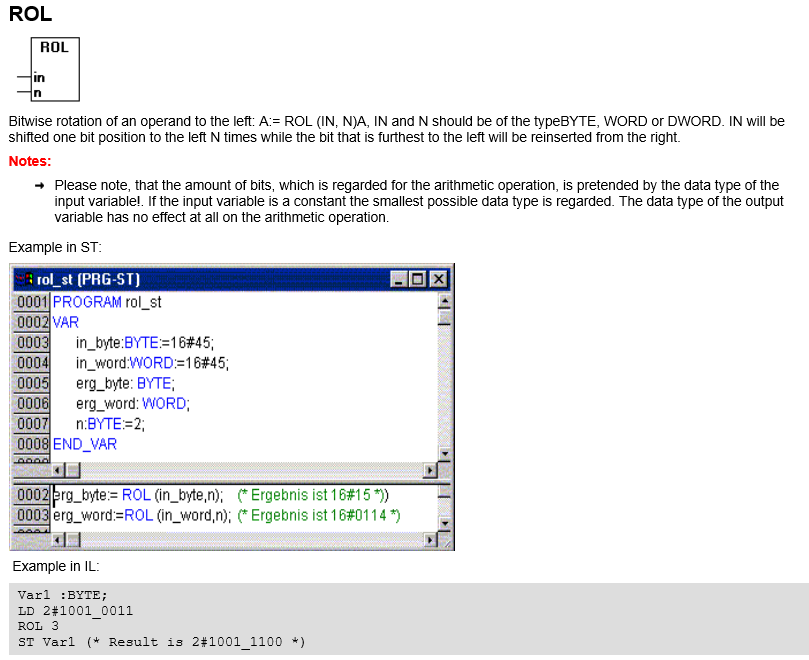
* 蓝色框内为步调节命令，F\_iecIncVTI为步调节增，从0~127递增；F\_iecDecVTI为步调节减，从127~0递减。



* 绿色框内为32为比特串变位命令，ROL为按位向左循环移动，解释如下，对于绿色框内解释为memory.nBSI\_400\_msg每次向左移一位；ROR为按位向右循环移动。SEL解释如上面黄色框内解释。

针对绿色框内解释，开始时memory.nBSI\_400\_msg为0，给它赋初始值16#11111111，之后每10s按位向左移一位，由

16#11111111=>16#22222222=>16#44444444=>16#88888888=>16#11111111循环变化。



### 信息体定义

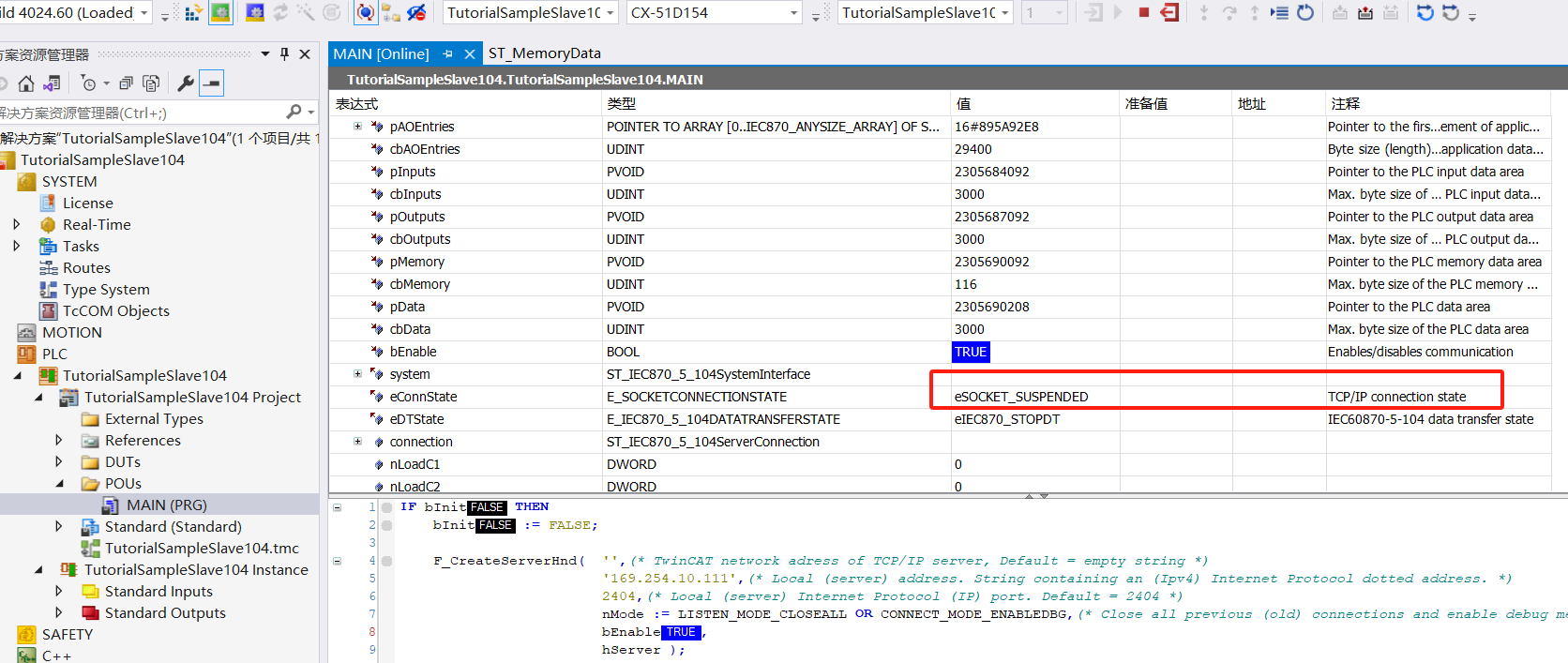
|  |  |
| --- | --- |
| 信息体类型 | 定义 |
| 单点遥信 | E\_IEC870\_5\_101SPI |
| 多点遥信 | E\_IEC870\_5\_101DPI |
| 步调节命令 | BYTE |
| 32位比特串 | DWORD |
| 归一化测量值 | WORD |
| 标度化测量值 | INT |
| 浮点数测量值 | REAL |
| 累计量 | UDINT |
| 单点命令 | E\_IEC870\_5\_101SCS |
| 多点命令 | E\_IEC870\_5\_101DCS |
| 步调节命令 | BYTE |
| 32位比特串命令 | DWORD |
| 归一化设点命令 | WORD |
| 标度化设点命令 | INT |
| 浮点数设点命令 | REAL |

## 主站从站通讯测试和变量传输

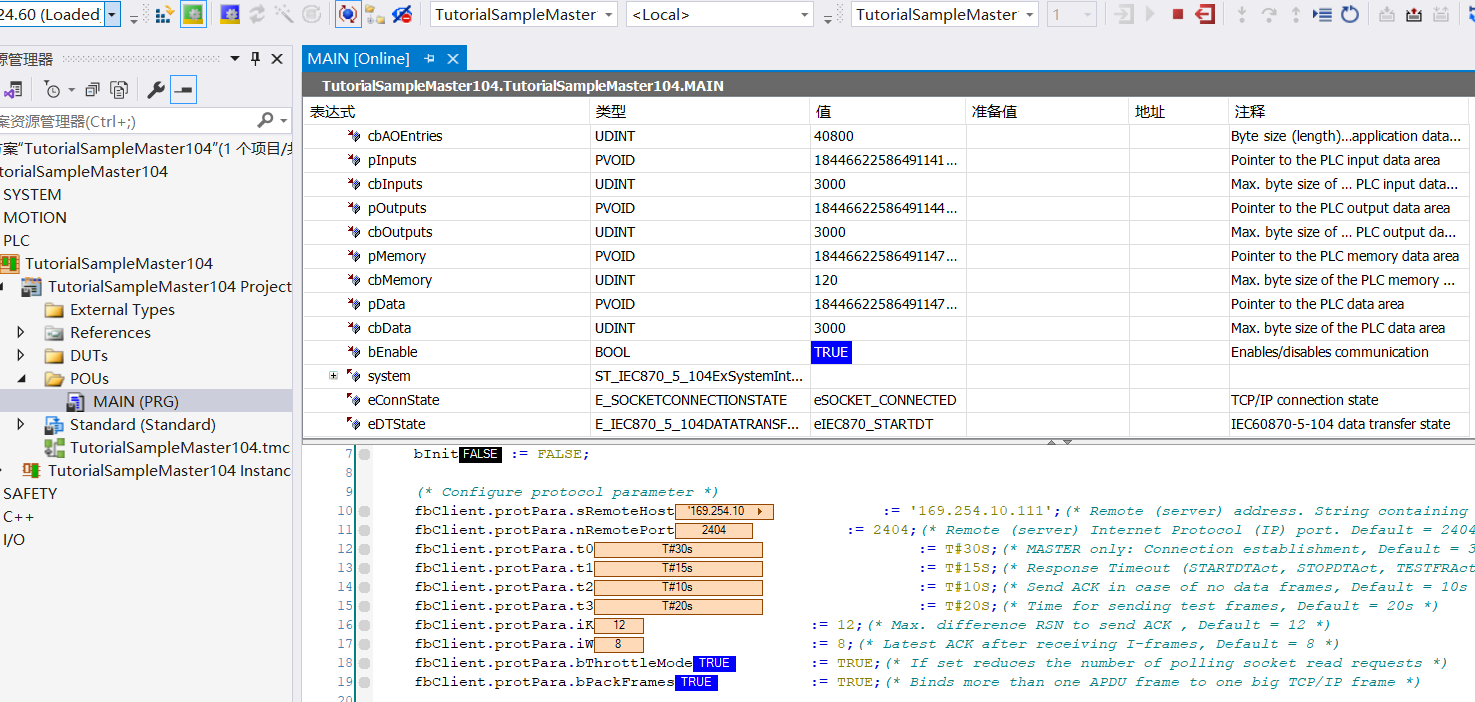
### 主从站连接状态查看

在3.3.1.1中修改完程序后。

点击第一步广播搜索控制器，并添加路由。红色框内显示控制器的名称，表示已经连接上控制器。点击第二步进行程序激活。连接状态suspended。



可以查看连接状态从suspended变为connected,表示通讯已建立成功。

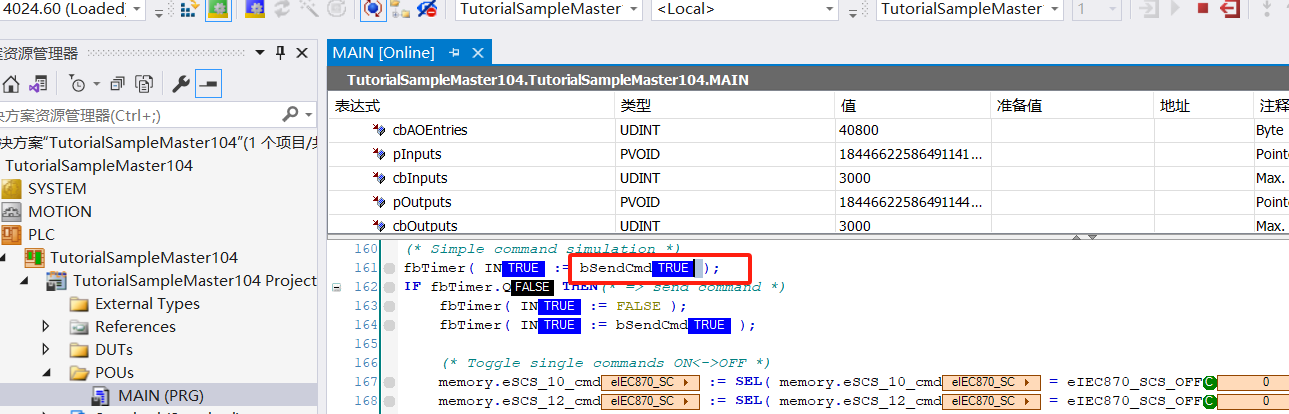


电脑屏幕截图

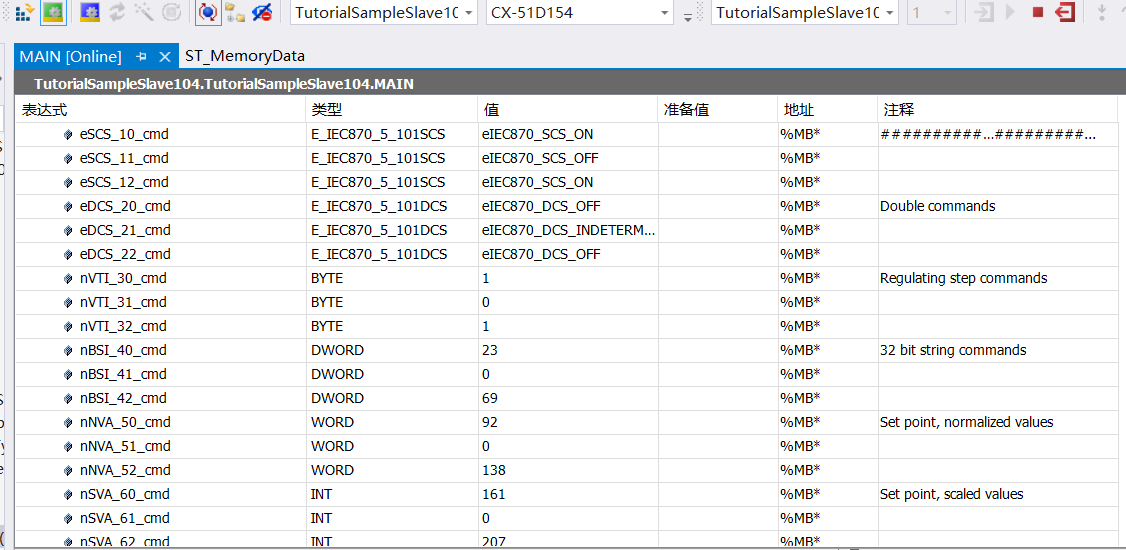
AI 生成的内容可能不正确。

### 主从站数据传送查看

更改主站bSendCmd至true,使memory.eSCS\_10\_cmd等数据变化。

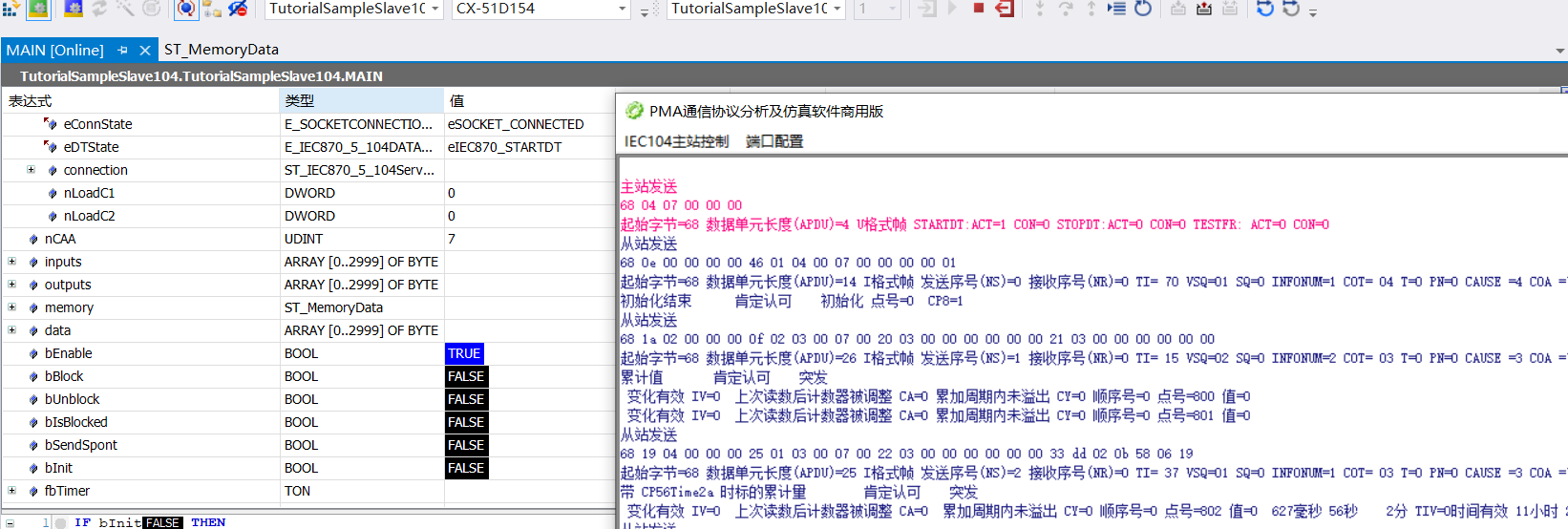


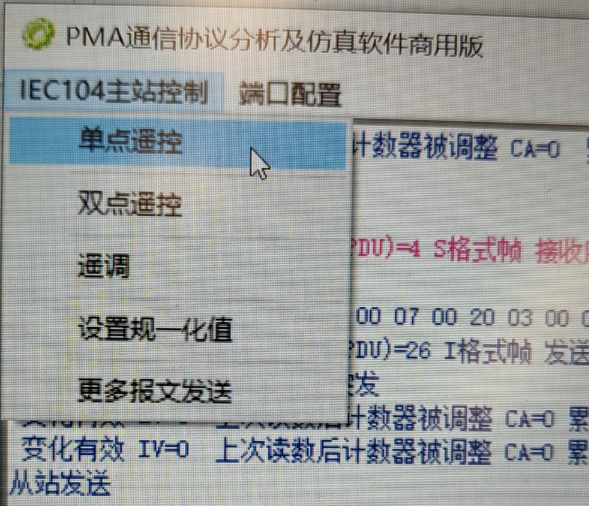
在从站相应的区域可以看到数据变化。



## 第三方工具测试

使用第三方工具可以模拟主站和从站进行连接，并可查看相应的通讯报文，也可以发出相应的测试命令，查看程序动作。





**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 |