**TwinCAT 3基于ADS与PowerShell互相调用**

|  |  |
| --- | --- |
|  | 作者：孙烨  职务：华东区 技术工程师  公司：BECKHOFF中国  邮箱：ye.sun@beckhoff.com.cn  日期：2023-10-17 |
| **摘 要：**  通过Windows平台PowerShell和TwinCAT 3进行ADS通讯。同样可以通过TwinCAT 3的接口，使用NT\_StartProcess调用PowerShellping PING谷歌DNS 8.8.8.8。 | |
| **附 件：**   |  |  |  | | --- | --- | --- | | 序 号 | 文件名 | 备注 | | 1 | TcXaeMgmt | TcXaeMgmt插件包 | |  |  |  | |  |  |  | |  |  |  | | |
| **历史版本：**   |  |  |  | | --- | --- | --- | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | | |
| **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：**  1、TwinCAT\_3\_ADS\_Powershell\_Module\_EN | |

目 录

[1. 软硬件版本 3](#_Toc150431056)

[1.1. 倍福Beckhoff 3](#_Toc150431057)

[1.1.1. 控制器硬件 3](#_Toc150431058)

[1.1.2. 控制软件 3](#_Toc150431059)

[1.2. TcXaeMgmt包及其应用场景 3](#_Toc150431060)

[2. PowerShell安装TcXaeMgmt插件包 3](#_Toc150431061)

[3. TcXaeMgmt介绍 4](#_Toc150431062)

[3.1. TcXaeMgmt之ADS指令使用 4](#_Toc150431063)

[3.2. TcXaeMgmt之实战操作 5](#_Toc150431064)

[3.2.1. 获取TwinCAT 3 路由状态指令：Get-AdsState 10.199.246.131.1.1 5](#_Toc150431065)

[3.2.2. 获取TwinCAT版本指令：Get-TcVersion 10.199.246.131.1.1 6](#_Toc150431066)

[3.2.3. 读取TwinCAT 3 PLC %MW20的值 6](#_Toc150431067)

[3.2.4. 写入TwinCAT 3 PLC %MW20的值 7](#_Toc150431068)

[4. TwinCAT 3 通过NT\_StartProcess指令调用PowerShell 8](#_Toc150431069)

# 软硬件版本

## 倍福Beckhoff

### 控制器硬件

TwinCAT控制制器，PC或者EPC，包括：

嵌入式控制器：CX5020-0125（IMG版本：CX1800-0411-0007 v3.92）

工控机：C6xxx、CP2xxx、CP6xxx等

### 控制软件

笔记本和控制器都是基于TwinCAT 3.1 Build 4024.47版本

TcXaeMgmt是基于3.2.25版本

Win系统PowerShell基于5.1.17134.858版本

## TcXaeMgmt包及其应用场景

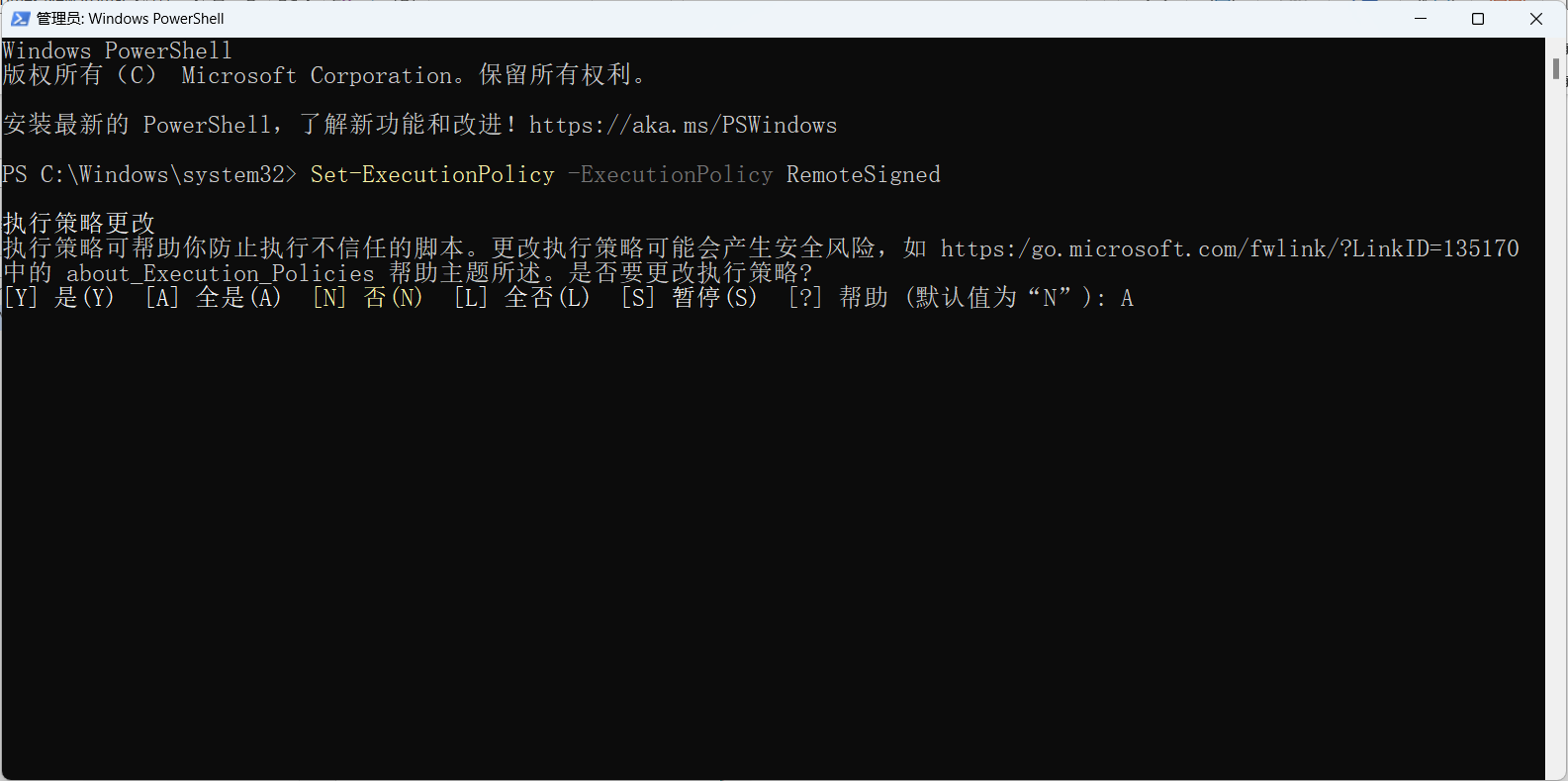
TcXaeMgmt包由倍福公司开发，并提交给PowerShell社区。TcXaeMgmt包含了一组指令，用来管理TwinCAT设备及其通讯。

其应用场景包括：查看网络中PLC设备状态、大量布署AMS路由,大量部署PLC程序，生成设备报表。

由于PowerShell的强大功能，编写PowerShell脚本指令，可以取代人进行简单而繁复工作。

# PowerShell安装TcXaeMgmt插件包

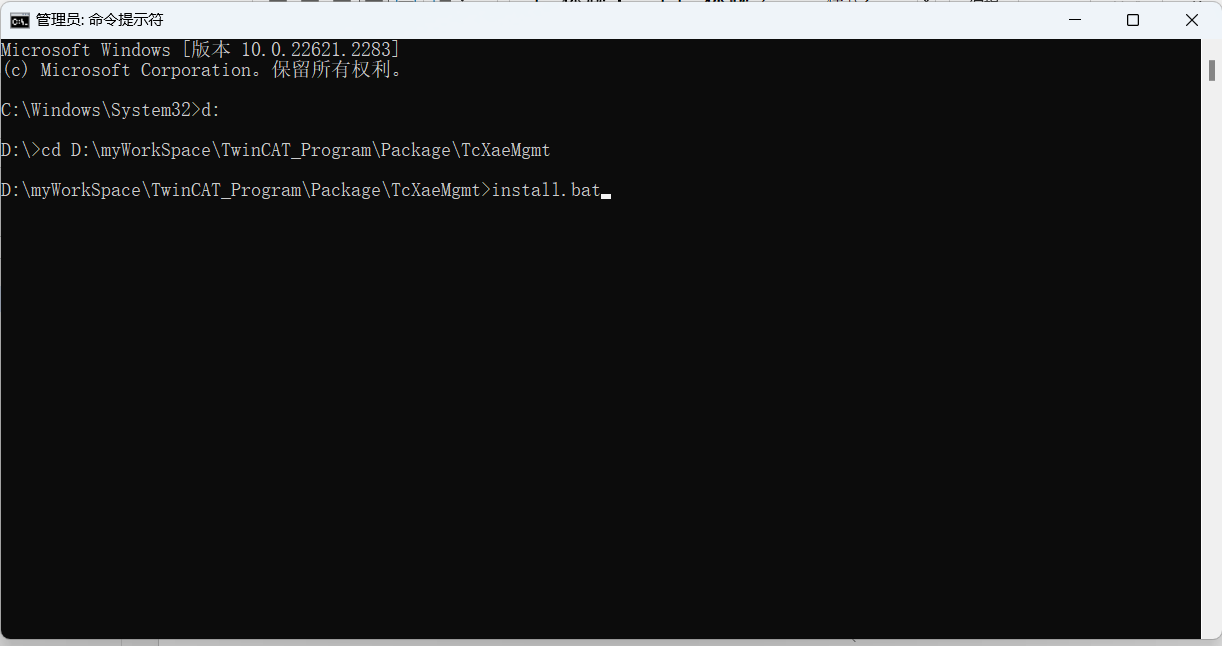
1、以管理员身份打开PoweShell，并执行Set-ExecutionPolicy -ExecutionPolicy RemoteSigned并且回车，如下图:



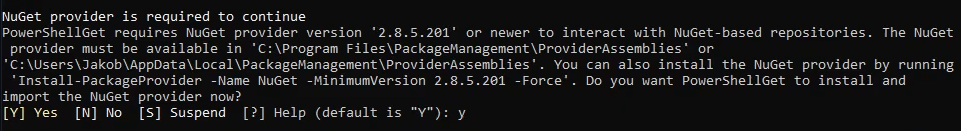
然后键入A，再进行回车。这里主要让PowerShell能安装第三方的库。

2、然后以管理员身份运行CMD命令，安装TcXaeMgmt插件（插件见压缩包，路径因人而异）：

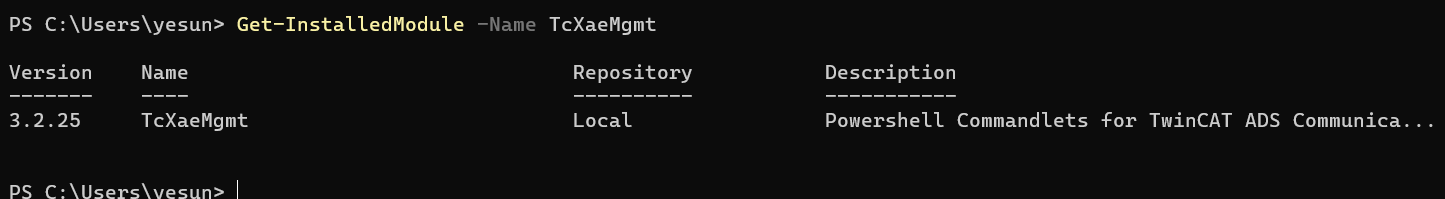
图形用户界面, 文本, 应用程序

描述已自动生成

直接完成后，输入y就完成安装：



安装完成后，通过PowerShell Get-InstalledModule -Name TcXaeMgmt 读一下安装的版本



备注：网上获取的版本是6.0.98。因为笔者这边PowerShell版本问题，不能安装最新版本6.0.98的插件包（使用新版的Powershell从网络安装可以用指令：find-module -name TcXaeMgmt寻找，接Install-Module -Name TcXaeMgmt进行安装）

如果上述两种方法皆无法安装，可以使用Powershell安装，样例指令如下（路径因人而异）：

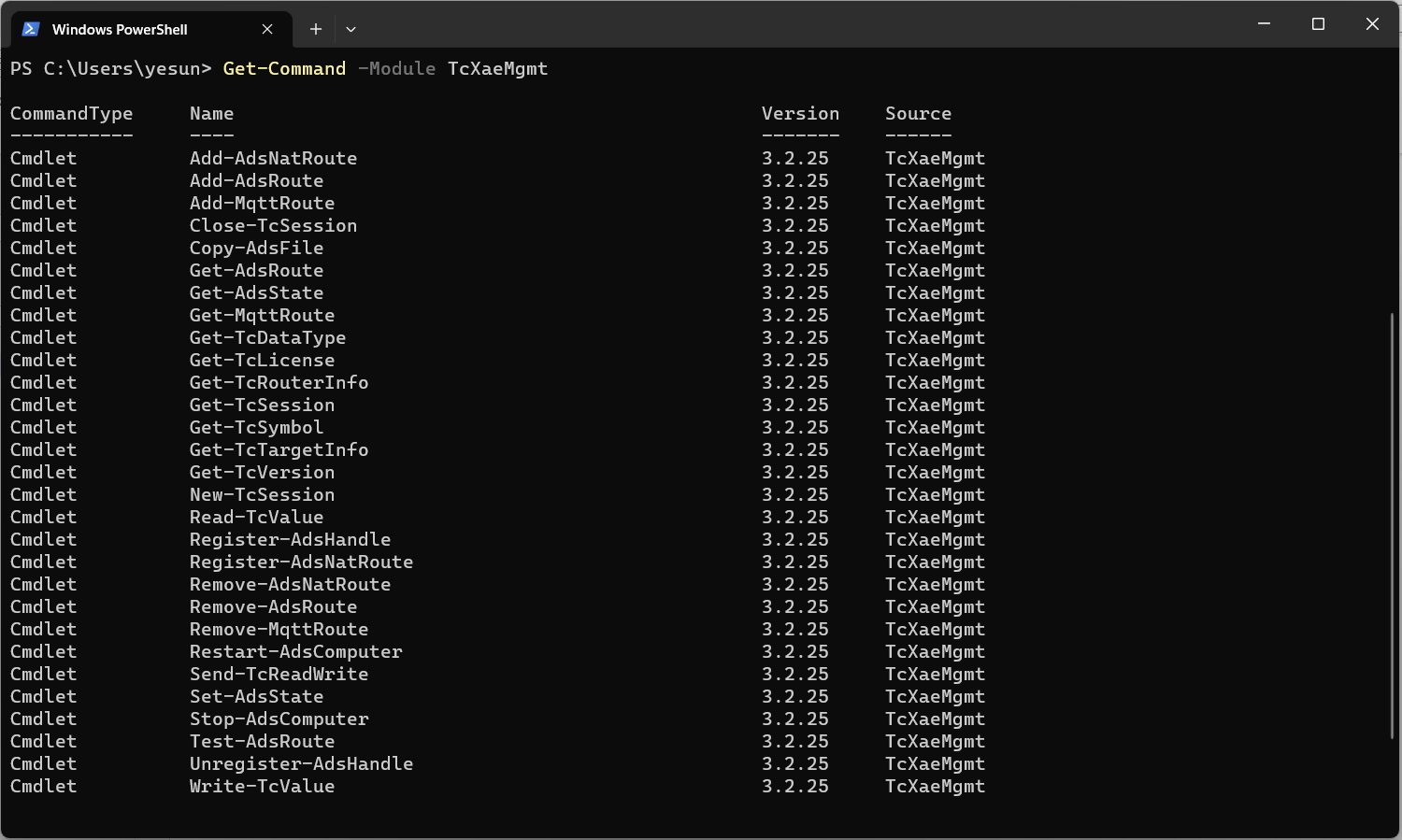
文本

描述已自动生成

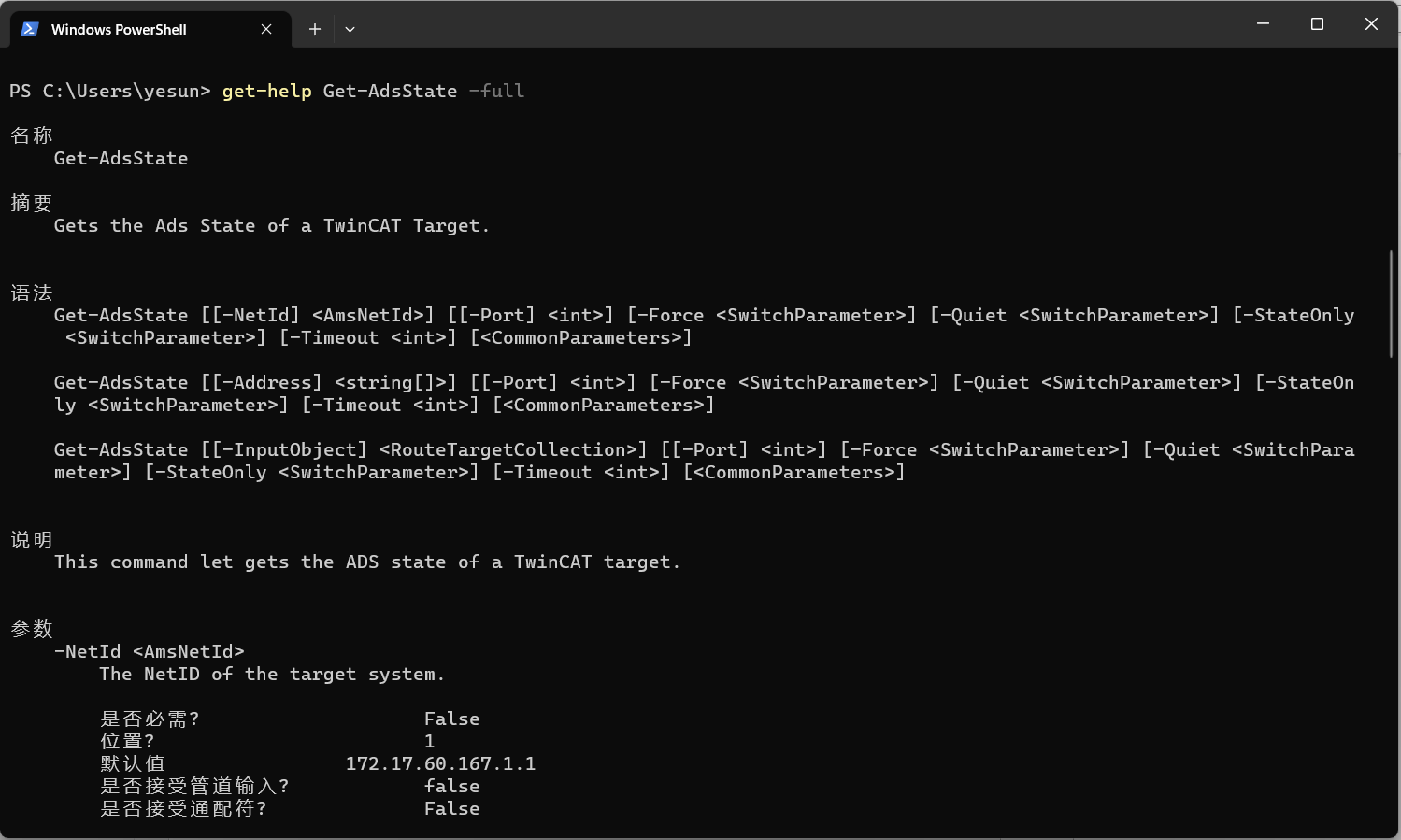
# TcXaeMgmt介绍

## TcXaeMgmt之ADS指令使用

1、列出TcXaeMgmt包中的指令 Get-Command -Module TcXaeMgmt



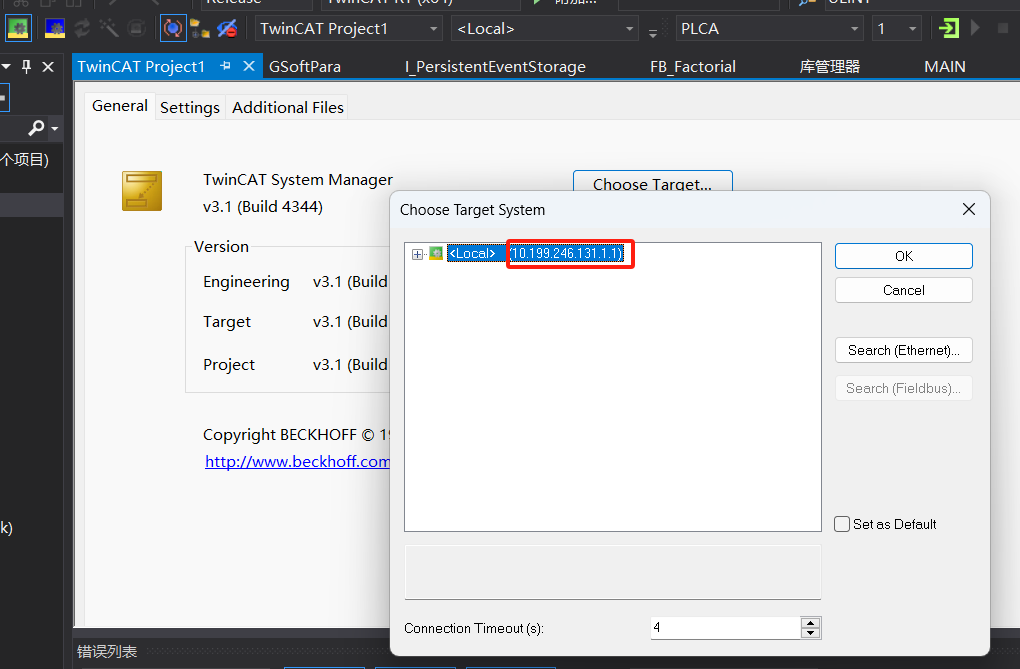
2、获取指令的用法 get-help Get-AdsState -full



## TcXaeMgmt之实战操作

### 获取TwinCAT 3 路由状态指令：Get-AdsState 10.199.246.131.1.1

如下图：(本地TwinCAT 3 AmsNetId 10.199.246.131.1.1)。



执行后获取设备10.199.246.131.1.1时运行状态

文本

描述已自动生成

### 获取TwinCAT版本指令：Get-TcVersion 10.199.246.131.1.1

文本

描述已自动生成

下图是本地安装的TwinCAT 3的版本v3.1.4024.47。

表格

描述已自动生成

### 读取TwinCAT 3 PLC %MW20的值

输入指令：Read-TcValue -IndexGroup 0x4020 -IndexOffset 0x0000 -NetId 10.199.246.131.1.1 -port 851 -size 0xff | format-hex 这个指令是读MW0开始，255个byte的长度。

下面是TwinCAT 3 %MW20的值 100，0x64

图形用户界面, 应用程序, 表格, Excel

描述已自动生成

PoweShell获取的值：64 00 。

图表, 文本

描述已自动生成

### 写入TwinCAT 3 PLC %MW20的值

输入指令：Write-TcValue -IndexGroup 0x4020 -IndexOffset 0x0028 -NetId 10.199.246.131.1.1 -port 851 -size 0x02 -Value 0x10。

文本

描述已自动生成

TwinCAT 3 %MW20的值显示16 （0x10）。

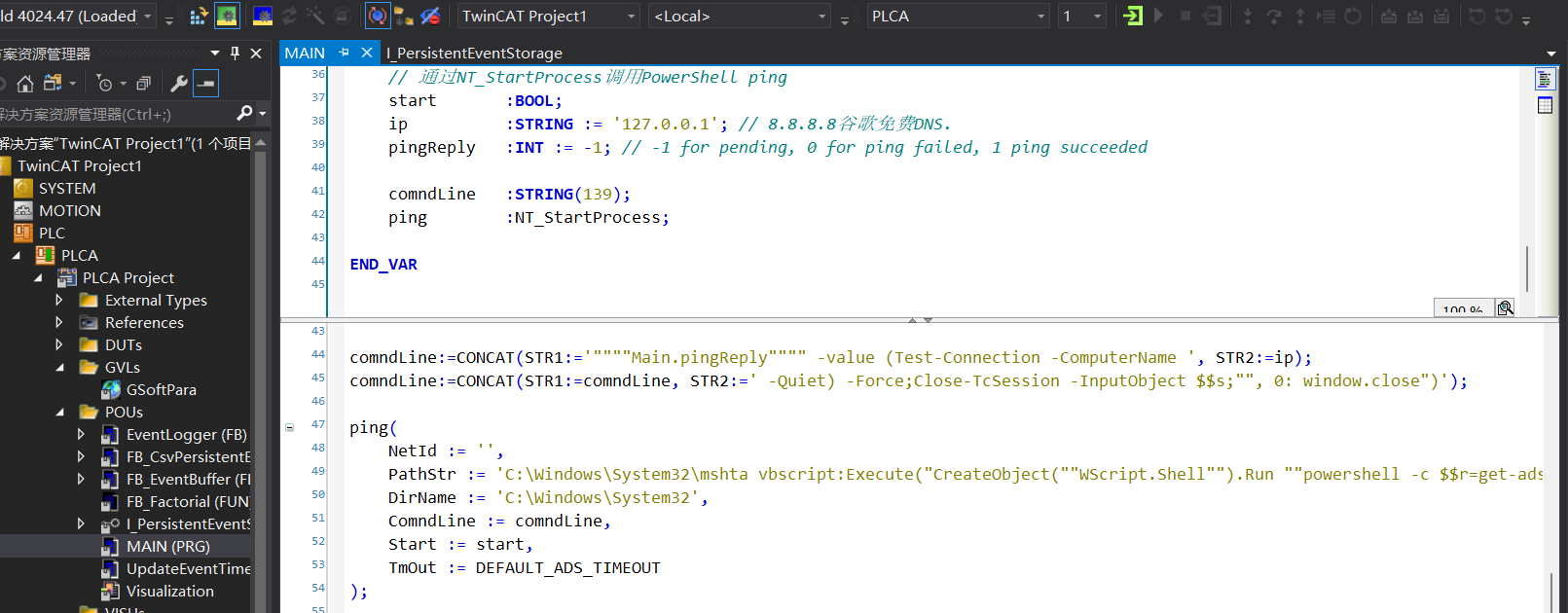
图形用户界面, 应用程序, 表格

描述已自动生成

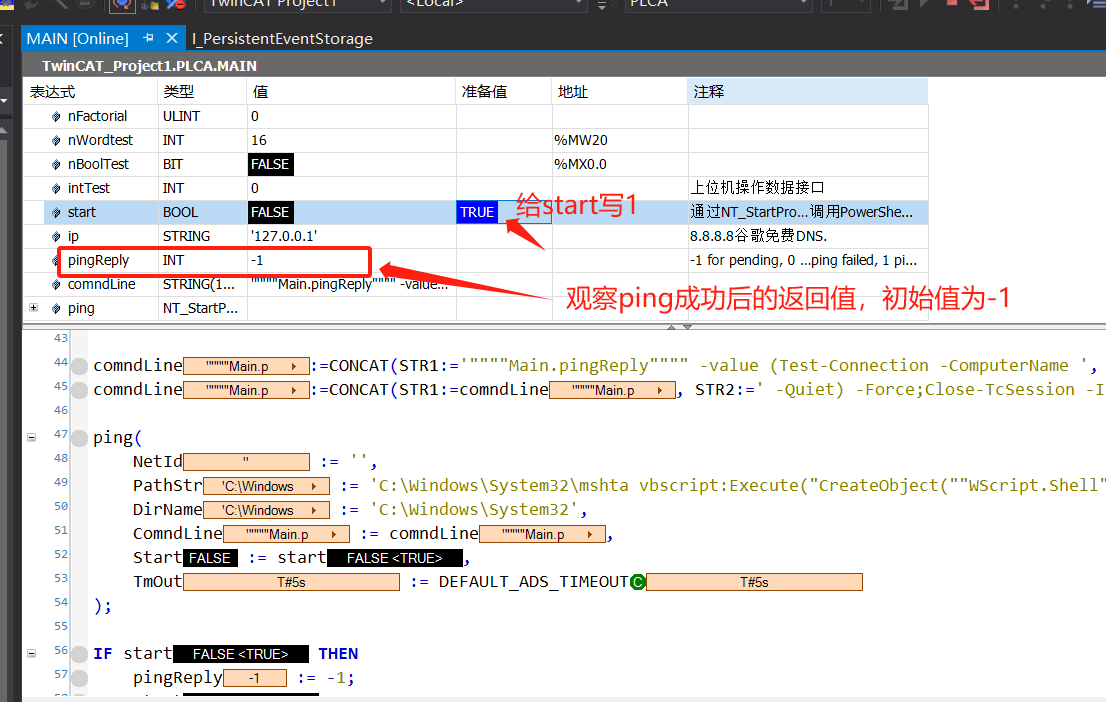
到此PowerShell对TwinCAT 3的基本操作如上述内容。

# TwinCAT 3 通过NT\_StartProcess指令调用PowerShell

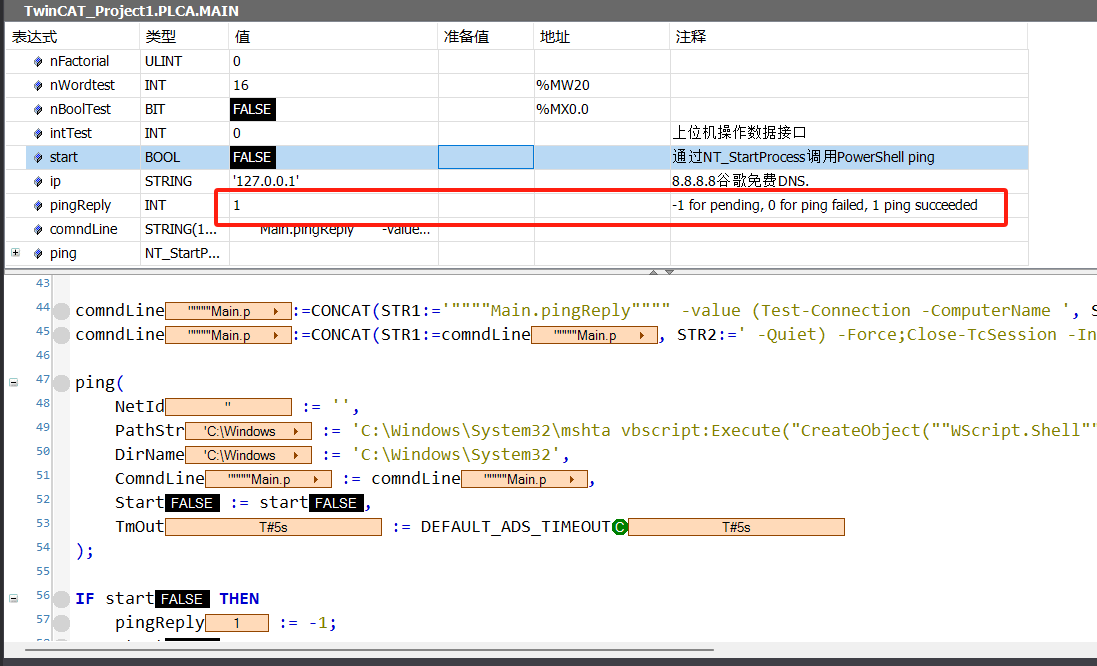
1、使用TwinCAT进行程序编写，如下图：



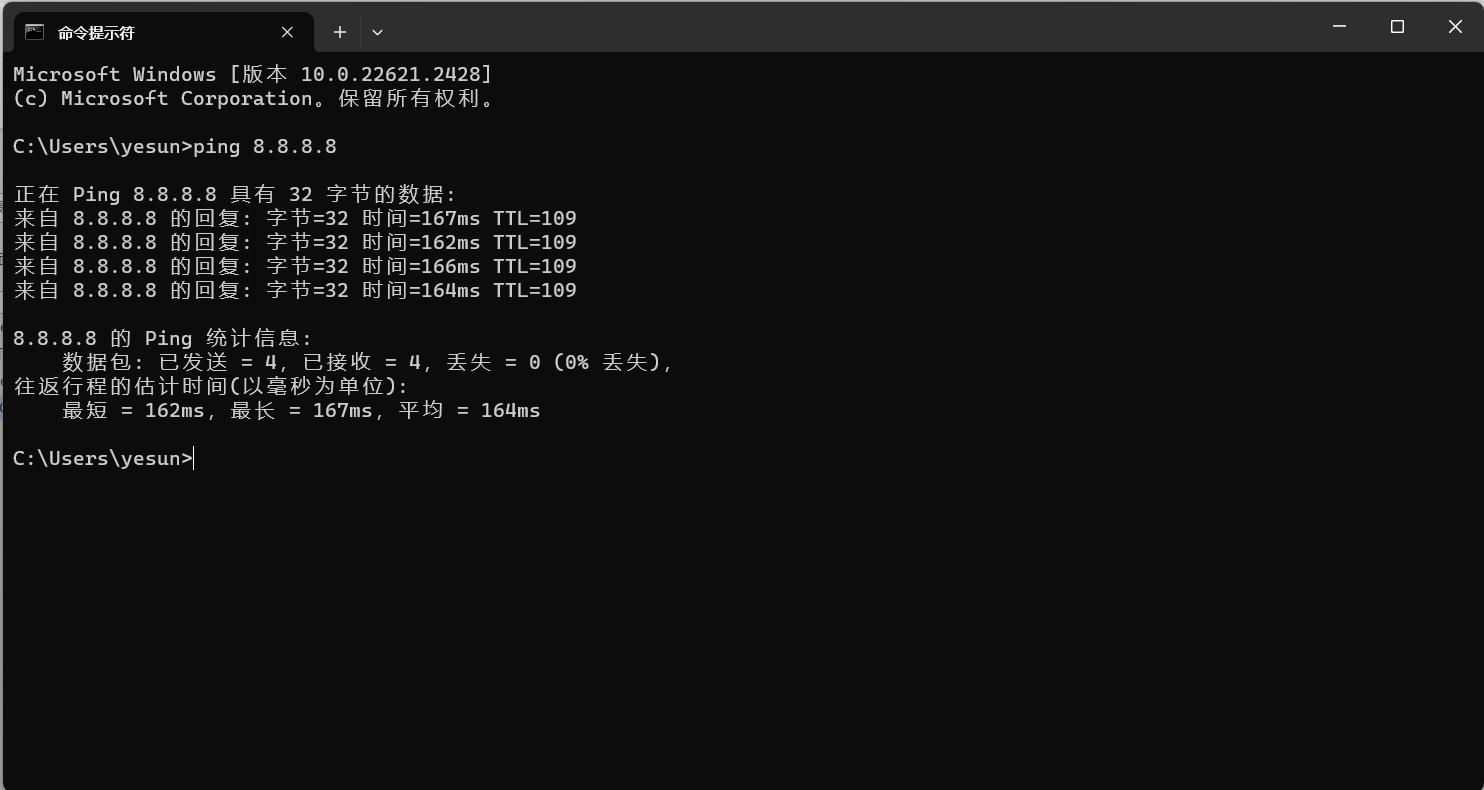
编译并执行，先ping127.0.0.1 回环地址(虚拟网口地址)下图：



等待5-10s才会有返回值，如下图：

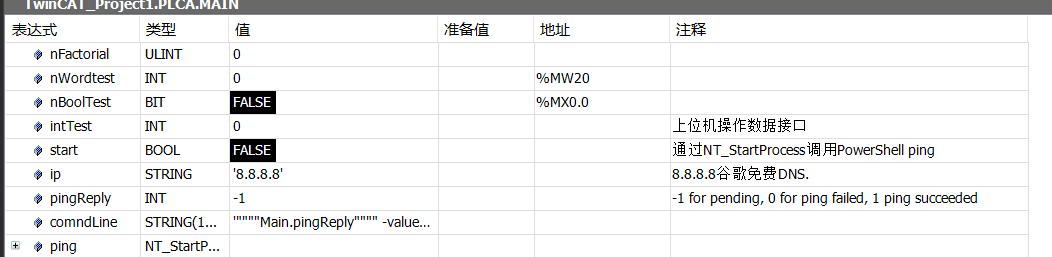


下面现在修改，ping 谷歌DNS8.8.8.8，我先用cmd进行是否能ping成功如下图：

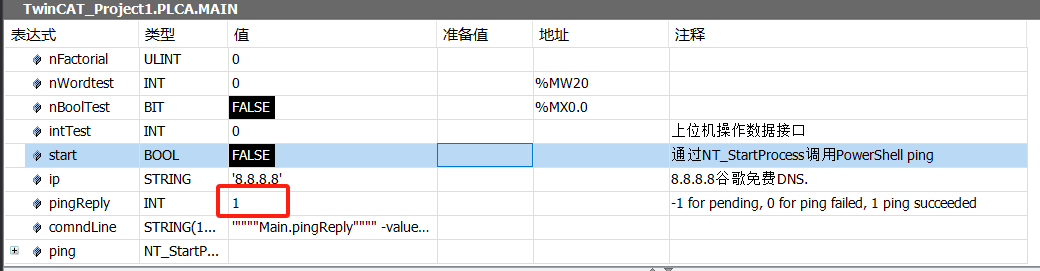


接下来使用TwinCAT 3演示

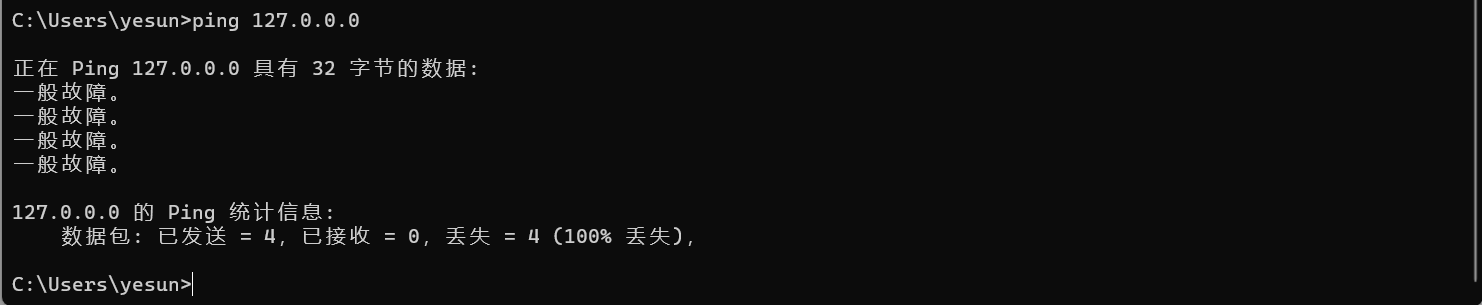
修改了ip8.8.8.8,目前的返回值是-1。然后给start 赋值 TRUE；



执行后效果如图：



继续修改，我ping 127.0.0.0 无效的IP。



接下来使用TwinCAT操作演示：

图形用户界面, 应用程序, Teams

描述已自动生成

执行后观察pingReply的值：0 失败和ping127.0.0.0显示的内容一致。

表格

描述已自动生成

到此，通过TwinCAT调用PowerShell的应用展示如上。

备注：在TwinCAT ping 正常IP（192.168.0.1）且不在同一网络段的设备时，只会重复ping，不是错误只是超时。

**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

**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 邮箱: beijing@beckhoff.com.cn

**广州分公司**

广州市天河区珠江新城珠江东路32号利通广场1303室

电话: 020-38010300/1/2 邮箱: guangzhou@beckhoff.com.cn

**成都分公司**

成都市锦江区东御街18号 百扬大厦2305 室

电话: 028-86202581 邮箱: chengdu@beckhoff.com.cn

|  |  |
| --- | --- |
| 请用微信扫描二维码  通过公众号与技术支持交流 | 倍福官方网站：  https://www.beckhoff.com.cn  在线帮助系统：  https://infosys.beckhoff.com/index\_en.htm |
| 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 |
|  |