TC3 && Windows 7 网络 OPC-DA 的 DCOM 配置

内部版本:

TwinCAT3----- 4018 版本。

由于 OPC (OLE for Process Control) 建立在 Microsoft 的 COM (COmponent Model) 基础 上,并且 OPC 的远程通讯依赖 Microsoft 的 DCOM (Distribute COM),安全 方面则依赖 Microsof 的 Windows 安全设置。

通过网络相互通信,OPC Server (OPC 服务端)和 OPC Client (OPC 客户端)所在的操作系统,需要设置 DCOM 的安全属性,下面使用 Windows 7 系统介绍配置过程。

由于 OPC 通讯需要用到 OPC Foundation 提供的动态库,所以在开始配置前,首先在PLC中安装倍福提供的TF6120-0PC-DA. exe运行包。

OPC Server(服务器)运行在 Windows 7 时的 DCOM 配置

一、 安装 OPC 运行库

OPC 服务器(CX5130做OPC Server)和 OPC 客户端的正常运行需要依赖 OPC 运行库,如果两个组件运行在不同的计算机,那运行计算机上都需要安装运行 库。

- 二、 创建用户并赋予访问权限
- 1. 创建新用户

创建一个新用户,并赋予此用户运行和使用操作系统 DCOM 程序的权限。为了 降低整个系统的安全风险,可以创建一个受限用户,而不是建立管理员级用户。为 操作系统创建新用户需要管理员权限。

注意:

- A、需要在 OPC 服务器所在 OS 系统与 OPC 客户端所在 OS 系统,创建的用户的用 户名和密码相同。
- B、由于 Windows 7 系列的 OS 系统 Guests 用户组的权限非常受限,所以新创建的 用户需要是 Users 用户组级别权限,或比 Users 用户组级别更高的权限。推荐使 用 Users 用户组。



图 2 通过"管理"菜单或"控制面板"创建用户



新用户	?	×
用户名(0):	OPCVser	
全名(@):		
描述(0):	OPC Vser	
		_
密码(P):	*****	
确认密码(C):	*****	
□ 用户下次登录	录时须更改密码(M)	
📝 用户不能更改	收密码 (S)	
📝 密码永不过期	钥(\)	
🔲 帐户已禁用 ((B)	
		-
帮助()	<u> 创建(8)</u> 关闭(0)	

图 4 新用户属性 创建新用户,并设置用

户属性。若是为了安全考量,请保持密码不为空。

2. 赋予用户访问 DCOM 的权限

要想使新创建的用户有使用 DCOM 的权限,需要将用户加入 "Distribute COM Users"用户组。



图 5 用户组

Distributed COM	Users 属性	? ×
常规		
Distri	buted COM Vsers	
描述(2):	成员允许启动、激活和使用此计算机上的 COM 对象。	分布式
成员(M):		
添加 @)	1 直到下一次用户登录时对用 删除 (B) 成员关系的更改才生效。	
- ā	龍 取消 应用 (A)	帮助
	图 6 添加用户到用户组	

.

选择用户	? 💌
选择此对象类型(S): 用户或内置安全主体	对象类型(0)
查找位置():	
ZHAO-PC	位置(L)
输入对象名称来选择(<u>示例</u>)(2):	
	检查名称(C)
高级(A) 确定	取消

图 7 选择要添加的用户

选择用户	? 💌
选择此对象类型(S): 用户或内置安全主体 本线位置 (S):	对象类型(0)
宣孫位立 UD: ZHAO-PC	
一般性查询	-
名称(A): 起始为 ▼	1 (列C)
描述 (0): 起始为 ▼	▲ 立即查找 (अ)
 □ 禁用的帐户 (B) □ 不过期密码 (X) 	停止(T)
自上次登录后的天数 (I):	<i>?</i>
搜索结果 (U):	确定
名称 (RDN) 所在文件夹	~ ×
INTERACTIVE IUSR	
NETWORK 2	
OPCUser ZHAO-PC	Ξ.
A OWNER RIGHTS	
SERVICE	Ŧ



选择用户	? 🔀
选择此对象类型(S): 用户或内置安全主体	对象类型(0)
查找位置 (F): ZHAO-PC	
输入对象名称来选择 (示例) (E):	2 检查名称 (C)
	确定 取消

图 9 选择添加的用户

Distributed CO	M Users 属性	? X
常规		
Dist	tributed COM Vsers	
描述(2):	成员允许启动、激活和使用此计算机上的 COM 对象。	的分布式
成员(M):		
Se OPCVser	1	2
		2
添加᠐)	直到下一次用户登录时对 删除(R) 成员关系的更改才生交。	用户的组
	确定 取消 应用 (以)	帮助

图 10 完成添加

可以添加多个用户到"Distribute COM Users"用户组,也可以添加现有用户到用户组。

三、

修改操作系统 Firewall(防火墙)关于 DCOM 和 OPC 的规则

由于 DCOM 使用操作系统的 135 端口,所以要想不同计算机上面的 OPC 服务器和 OPC 客户端通讯正常,要修改防火墙规则,允许 135 端口的连接。如果 OPC 服务器和 OPC 客户端安装在同一台计算机,不需要修改防火墙规则。下面用 Windows 7 的防火墙 配置过程为示例。

🖅 运行
Windows 将根据您所输入的名称,为您打开相应的程序、 文件夹、文档或 Internet 资源。
打开(O): wf.msc 🔹
确定 取消 浏览(B)

图 11 进入防火墙管理控制台

Windows 7 用户: 要打开防火墙管理控制台,可以从"开始"->"控制面板"->"管理 工具"->"Windows 防火墙"->"高级设置",或在"运行"输入"wf.msc"命令。 Windows Server 2008 R2 用户: 要打开防火墙管理控制台,可以在"服务器管理工具", 或在"运行"输入"wf.msc"命令。

1、 开放 DCOM 访问

在默认状态, Windows 防火墙是阻止另一台计算机连接的。如果要允许 OPC 客户端 与 OPC 服务器正常访问,需要放开这个访问规则。

🔐 高级安全 Windows 防	火墙			
文件(F) 操作(A) 查看	(V) 帮助(H)			
🗢 🄿 🖄 📅 🔒				
🔐 本地计算机 上的高级 3	入站规则			
🔜 入站规则	名称	组 ^		配置文化
出站規则	Media Center Extender - 媒体流(TCP-In)	Media Center	Extender	所有
	Wetlogon 服务(NP-In)	Netlogon 服务		所有
	SNMP Trap Service (UDP In)	SNMP Trap		域
	SNMP Trap Service (UDP In)	SNMP Trap		专用,公
	Windows Management Instrumentation (ASync-In)	Windows Man	agement	域
	Windows Management Instrumentation (ASync-In)	Windows Man	agement	专用,公
	Windows Management Instrumentation (DCOM-In)	Windows Man	agement	域
	Windows Management Instrumentation (DCOM-In)	Windows Man	agement	专用,公
	Windows Management Instrumentation (WMI-In)	启用规则(E)	ment	专用,公
	Windows Management Instrumentation (WMI-In)	剪切(T)	ment	域
	●Windows Media Player (UDP-In) 鼠标右键	复制(C)	ayer	所有
	Windows Media Player 网络共享服务(HTTP-Stream)	删除(D)	ayer	专用,公
	● Windows Media Player 网络共享服务(HTTP-Stream		ayer	域
	● Windows Media Player 网络共享服务(qWave-TCP-I	▶ 唐性(R)	ayer	域
	Windows Media Player 网络共享服务(qWave-TCP-I	帮助(H)	ayer	专用,公
	Windows Media Player 网络共享服务(qWave-UDP-In)	Windows Med	lia Player	专用,公
	II▲Windows Madia Dlayer 网络共享职务(aWayer IDD-In) 图 12 防火墙规则	Windows Mer	lia Dlaver	tat



图 13 允许 DCOM 连接

Windows Management Instrumentation (DCOM-In) 属性
常规 程序和服务 计算机 协议和端口 作用域 高级 用户
本地 IP 地址 7
● 任何 IP 地址 (8)
○ 下列 IP 地址(T):
[編辑 (2)]
远程 IP 地址
■ 任何 IP 地址(Y) < 2
● 下列 IP 地址 00):
了解有关设置范围的详细信息
3
确定 取消 应用(A)

图 14 防火墙 DCOM 规则作用域设置

Windows Management Instrumentation (DCOM-In) 雇性
常规 程序和服务 计算机 协议和端口 作用域 高级 用户
配置文件 指定此规则应用的配置文件。 ☑ 域 (0) ☑ 专用 (2) ☑ 公用 (0)
接口类型 指定应用此规则的接口类型。 自定义(C)
~ 边缘遍历————————————————————————————————————
→ 动缘遍历允许计算机接受未经请求的入站数据包,这 些数据包已通过诸如网络地址转换 (MAT)路由器或防火 墙之类的边缘设备 (B)。
阻止边缘遍历 ▼
阻止应用程序通过 NAT 边缘设备从 Internet 接收主 动提供的流量。
了解这些设置的详细信息 3
确定 取消 <u>应用(A)</u>

图 15 防火墙 DCOM 规则高级属性配置

Windows 7 用户:如果 "COM+ Network access" 或 "DCOM" 规则不在防火墙的预 定义规则列表中,可自己手动添加两个 "PORT" (端口)规则:

- TCP 135
- UDP 135
- 2、创建 OPC 程序规则

需要手动添加 OPC 服务器程序的规则。同样也需要添加 OPCEnum 系统服务程序规则,因为远程的 OPC 客户端计算机就是通过它获得这台计算机上面的 OPC 服务器名称列表的。

下面我们通过创建 OPCEnum 应用的规则,演示如何创建应用的防火墙规则。可用同样步骤创建 OPC 服务器的防火墙规则。



- 图 16 创建应用规则
- *选择"新建规则";
- *选择"程序"类型规则
- *点击"下一步"按钮



图 17 选择应用程序文件

*选择"此程序路径"项目;

*填写程序的完整路径和应用程序名称;

*也可使用"浏览"按钮,在弹出的文件选择对话框里查找磁盘上应用程序的文件 名;

*点击"下一步"按钮;







图 20 规则命名

🔐 高级安全 Windows 防>	火墙					
文件(F) 操作(A) 查看(V) 帮助(H)					
🗢 🔿 🔁 🗔 🗟	? 🗊					
💣 本地计算机 上的高级3	入站规则					
🔜 入站规则	名称	组	配置文件	已启用	操作	替代 🔶
SA 出站规则	OPCEnum		所有	是	允许	否
	Media Center Extender - HTTP 流(TCP	Media Center Extender	所有	否	允许	否 🗉
	BranchCache 对等机发现(WSD-In)	BranchCache - 对等机发	所有	否	允许	否
1	BranchCache 内容检索(HTTP-In)	BranchCache - 内容检索(所有	否	允许	좀 🕒
	● BranchCache 托管缓存服务器(HTTP-In)	BranchCache - 托管缓存	所有	否	允许	否
	iSCSI 服务(TCP-In)	iSCSI 服务	域	否	允许	否
		iSCSI 服务	专用,公用	否	允许	否
	Media Center Extender - qWave (TCP	Media Center Extender	所有	否	允许	否
	Media Center Extender - qWave (UDP	Media Center Extender	所有	否	允许	否
	Media Center Extender - RTSP (TCP-In)	Media Center Extender	所有	否	允许	否
	Media Center Extender - SSDP (UDP-In)	Media Center Extender	所有	否	允许	否
	Media Center Extender - WMDRM-N	Media Center Extender	所有	否	允许	否

图 21 规则处于活跃状态 同

样步骤,创建 OPC 服务器应用程序的防火墙访问规则。

四、 配置 DCOM 安全

为通过网络正常访问 OPC 服务器,需要配置 DCOM 的访问和激活安全属性。

 启动"组件服务" 在菜单"开始\运行",输入: dcomcnfg,点击"确定"按 钮,进入"组件服务 管理器"。 如图:



图 22 运行组件服务

 配置"我的电脑"的安全设置 在"组件服务"管理器的左侧树形菜单,选择 "组件服务\计算机\我的电脑", 在鼠标右键的弹出菜单,选择"属性"项目, 如图:



图 23 属性 在弹出的"我的电脑属性",选择"默认属性"标签 页,如下图:

我的电脑 雇性 ? 王
常规 选项 默认属性 默认协议 COM 安全 MSDTC
☑ 在此计算机上启用分布式 COM (E)
Internet 服务(M)
S默认分布式 COM 通信属性
身份验证级别指定数据包级别上的安全。
默认身份验证级别 (0):
模拟级别指定应用程序是否可以确定其调用者,以及是否可以使
用各户编标识进行操作。
默认模拟级别(I):
标识
如果使用身份验证目默认模拟级别不是匿名,则可以提供引用跟
時安全。
□ 提供附加的引用跟踪安全 (P)
进一步了解如何设置这些属性。
确定 取消 应用 (A)
47

图 24 属性

请确认几个属性的设置内容或状态: 在此计算机上启用分布式 COM,此属性处于"选中"状态;

默认分布式 COM 通信属性栏目下,"默认身份验证级别",选择的项目是:"连接","默认模拟级别",选择的项目是:"标识"。选择"我的电脑属性"属性页面的"默认协议"标签页,如下图:

我的电脑 属性	? <mark>- X-</mark>
常规 选项 默认属性 默认协议 COM 安全 MSDTC	
DCOM 协议(M)	
T 面向连接的 TCP/IP	
添加(D) 移除(R) 上移(U) 下移(D) 属性	(P)
可用于此计算机上 DCOM 的网络协议集。协议顺序反映了 协议的优先级,最上面的协议具有最高优先级。	使用
进一步了解如何设置汉些属性。	
「福宁」「即省」	ு க
	2 million

图 25 属性

确认 DCOM 协议属性内容是:面向连接的 TCP/IP。选择"我的电脑 属性"属性页面的"COM 安全"标签页,如下图:

我的电脑	属性						? 🗙
常规	选项	默认属性	默认协议	COM	安全	MSDTC	
-访问 您 在	权限 可以编辑 应用程序	默认情况下; 上设置限制	允许访问应 以决定其权[用程序 限。	郭的用,	户。您也	可以
	<u>〕</u> 整計	ि: 修改访问 €、执行和/! 	回权限可能会或运行。	景响 2 ·	应用稻 编辑	程序安全』	自动、 1 (2)
一启动 您 户	和激活权 可以编辑 。您也可	限	允许启动应 序上设置限(用程序 制以次	\$或激 史定其 [;]	活对象的 权限。	囲
	▲ ▲ 月3	計 修改启动 功、连接、执	加和激活权陥 〔行和/或运	同能 行。 1 ·	会景河 [编辑	前应用程序 電影认值	序安全 3 (0)
进一步	⇒了解如何	设置这些属	<u>神</u> 。				
			确定		取消		

图 26 COM 安全

选择 "COM 安全"标签页面的"访问权限"栏目的"编辑默认值," 按钮(图 26 中按钮 1),弹出"访问权限"设置对话框,如下图:



图 27 配置访问权限 点击此对话框上的"添加"按钮,添加下边列表的用户, 并设置用户的访问权 限,核实后,点击"确定"按钮保存。

NO.	组或用户名	本地访问	远程访问	属性
1	Distribute COM Users	允许	允许	系统内置用户组
2	Anonymous logon	允许	允许	系统内置帐户
3	everyone	允许	允许	系统内置帐户
4	Interactive	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	系统内置帐户
6	SELF	允许	允许	系统内置帐户
7	NETWORK	允许	允许	系统内置帐户
8	NETWORK	允许	允许	系统内置帐户
9	SERVICE	允许	允许	系统内置帐户
10	Users	允许	允许	系统内置帐户

选择 "COM 安全"标签页面的"访问权限"栏目的"编辑限制,,"按钮(图 26 中按钮 2),弹出"访问权限"设置对话框,如下图:



图 28 配置访问权限 点击此对话框上的"添加"按钮,添加下边列表的用户, 并设置用户的访问权 限,核实后,点击"确定"按钮保存。

NO.	组或用户名	本地访问	远程访问	属性
1	Distribute COM Users	允许	允许	系统内置用户组
2	Anonymous logon	允许	允许	系统内置帐户
3	everyone	允许	允许	系统内置帐户
4	Interactive	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	系统内置帐户
6	NETWORK	允许	允许	系统内置帐户
7	NETWORK SERVICE	允许	允许	系统内置帐户
8	ADMINISTRTORS	允许	允许	系统内置帐户
9	Users	允许	允许	系统内置帐户

选择 "COM 安全"标签页面的 "启动和激活权限"栏目的 "编辑默认值,," 按钮 (图 26 中按钮 3),弹出 "启动和激活权限"设置对话框,如下图:



图 29 配置启动激活权限 点击此对话框上的"添加"按钮,添加下边列表的用 户,并设置用户的访问权 限,核实后,点击"确定"按钮保存。

NO.	用户名	本 地 启动	远程 启动	本 地 激活	远 程 激活	属性
1	Distribute COM Users	允许	允许	允许	允许	系统内置用户 组
2	ANONYMOUS LOGON	允许	允许	允许	允许	系统内置帐户
3	Everyone	允许	允许	允许	允许	系统内置帐户
4	INTERACTIVE	允许	允许	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	允许	允许	系统内置帐户
6	NETWORK	允许	允许	允许	允许	系统内置帐户
7	NETWORK SERVICE	允许	允许	允许	允许	系统内置帐户
8	ADMINISTRTORS	允许	允许	允许	允许	系统内置帐户
9	Users	允许	允许	允许	允许	系统内置帐户

选择 "COM 安全"标签页面的 "启动和激活权限"栏目的 "编辑限制,," 按钮 (图 26 中按钮 4),弹出 "启动和激活权限"设置对话框,如下图:



图 30 配置启动激活权限 点击此对话框上的"添加"按钮,添加下边列表的用 户,并设置用户的访问权 限,核实后,点击"确定"按钮保存。

NO.	用户名	本 地 启动	远程 启动	本 地 激活	远 程 激活	属性
1	Distribute COM Users	允许	允许	允许	允许	系统内置用户 组
2	ANONYMOUS LOGON	允许	允许	允许	允许	系统内置帐户
3	Everyone	允许	允许	允许	允许	系统内置帐户
4	INTERACTIVE	允许	允许	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	允许	允许	系统内置帐户
6	NETWORK	允许	允许	允许	允许	系统内置帐户
7	NETWORK SERVICE	允许	允许	允许	允许	系统内置帐户
8	ADMINISTRTORS	允许	允许	允许	允许	系统内置帐户
9	Users	允许	允许	允许	允许	系统内置帐户

配置完成后,点击"我的电脑属性"属性页面的"确定"按钮,由于涉及到系统安全属性的修改,此时操作系统弹出警告消息,如图:

DCOM 计算机范围设置	23
您将要修改计算机范围的 DCOM 设置,这将影响该计算机上的所有应 用程序,因此某些应用程序可能不能正常工作。是否更新 DCOM 设置? 图 31 警告消息	
是(N)	

由于是我们手动修改的安全设置,并确认修改,点击"是"按钮,保存刚才做出的所有修改,退出"我的电脑属性"属性页面。

3. 配置 OPCENUM 的安全设置 在"组件服务"左侧树形菜单,选择"组件服务\计算 机\我的电脑\DCOM 配置", 在列表中选择 opcenum 项目,在鼠标右键弹出的菜 单,选择"属性"项目,如 下图:



属性,设置项目是:无,如下图:

OpcEnum 雇性 ? 王
常规 位置 安全 终结点 标识
此 DCOM 应用程序的常规属性
应用程序名: OpcEnum
应用程序 ID: {13486D44-4821-11D2-A494-3CB306C10000}
应用程序类型: 本地服务
身份验证级别 (0): 无
服务名称: OpcEnum
讲一步了解如何设置这些属性。
· · · · · · · · · · · · · · · · · · ·

图 33

在"OPCENUM 属性"框,选择"安全"标签页,如下图:

OpcEnum	? <mark>×</mark>
常规 位置 安全 终结点 标识	
启动和激活权限	
◎ 使用默认值 (V)	
● 自定义(S) 1→ 编辑(C)	
访问权限	
◎ 使用默认值 健)	
◎ 自定义 (M) 2 → [编辑 (D)	
電置权限	
	_
进一步了解如何 <u>设置这些属性</u> 。	
确定 取消	应用(A)

图 34

在"安全"标签页,选择"启动和激活权限"栏目,选择"自定义"选项,并 点击"编辑,"按钮,如下图:



图 35 在弹出的"启动和激活权限"属性设置对话框,使用"添加"按钮,添加 下表 的组或用户,核实并确认后,点击"确定"按钮保存。

NO.	用户名	本 地 启动	远程 启动	本 地 激活	远 程 激活	属性
1	Distribute COM Users	允许	允许	允许	允许	系统内置用户 组
2	ANONYMOUS LOGON	允许	允许	允许	允许	系统内置帐户
3	Everyone	允许	允许	允许	允许	系统内置帐户
4	INTERACTIVE	允许	允许	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	允许	允许	系统内置帐户
6	NETWORK	允许	允许	允许	允许	系统内置帐户
7	NETWORK SERVICE	允许	允许	允许	允许	系统内置帐户
8	ADMINISTRTORS	允许	允许	允许	允许	系统内置帐户
9	Users	允许	允许	允许	允许	系统内置帐户

在"安全"标签页,选择"访问权限"栏目,选择"自定义"选项,并点击"编辑,"按钮,如下图:



图 36 在弹出的"访问权限"属性设置对话框,使用"添加"按钮,添加下表的 组或 用户,核实并确认后,点击"确定"按钮保存。

NO.	组或用户名	本地访问	远程访问	属性
1	Distribute COM Users	允许	允许	系统内置用户 组
2	Anonymous logon	允许	允许	系统内置帐户
3	everyone	允许	允许	系统内置帐户
4	Interactive	允许	允许	系统内置帐户
5	SELF	允许	允许	系统内置帐户
6	SYSTEM	允许	允许	系统内置帐户
7	NETWORK	允许	允许	系统内置帐户
8	NETWORK SERVICE	允许	允许	系统内置帐户
9	ADMINISTRTORS	允许	允许	系统内置帐户
10	Users	允许	允许	系统内置帐户

在 "OPCENUM 属性"框,选择"标识"标签页,确认"选择运行此应用程序的用户账户"属性,设置项目是:系统账户(仅用于服务),如下图:

(OpcEnum 雇性 ? 💌
	常规 位置 安全 终结点 标识
	选择运行此应用程序的用户帐户
	● 交互式用户(II)
	○ 启动用户(L)
	◎下列用户(0)
	用户(E): 浏览(B)
	密码 (P):
	确认密码 00):
	◎ 系统帐户(仅用于服务)(S)
	进一步了解如何设置这些属性。
	确定 取消 (A)

图 37

确认后点击"确定"按钮保存所作的修改。

4. OPC 服务器的安全设置

OPC 服务器的安全设置可参照 OPCEnum 的设置过程,只是在"标识"属性页 面有些不同。

OPC服务器(TwinCAT OPC Server)的安全设置在实际的设置 和OPCEnum的设置不同,采用的是"使用默认值"。在组件服务—>DCOM配置中"标识"设置中OPC服务器(TwinCAT OPC Server)和OPCEnum的都是采用的"交互式用户"。

Kepware Communications Server 5.4 属性	? 🔀
常规 位置 安全 终结点 标识	
选择运行此应用程序的用户帐户	
● 交互式用户(1)	
◎ 启动用户 ⑴	
◎ 下列用户 (0)	
用户(2):	浏览(8)
密码 (P):	
确认密码 (M):	
◎ 系统帐户(仅用于服务)(S)	
进一步了解如何设置这些属性。	
确定 取消	

图 38 注册成系统服务的 OPC 服务器

KEPware Enhanced OPC/DDE Server 雇性	? 💌
常规 位置 安全 终结点 标识	
选择运行此应用程序的用户帐户	
◎ 交互式用户(I)	
◎ 启动用户(L)	
◎ 下列用户(0)	
用户(2):	浏览 (8)
密码(P):	
确认密码 (N):	
● 系统帐户(仅用于服务)(S)	
进步中国初期等于	
进一步 」 解如何 这百 这些 腐 性。	
·····································	(A)

图 39 注册成本地应用型 OPC 服务器

- 五、 配置本地安全策略
 - 启动"本地安全策略"管理器 在"开始\运行"输入: secpol.msc, 点击"确 定"按钮, 启动"本地安全策略"管理器, 如下图:

🖅 运行	×
	Windows 将根据您所输入的名称,为您打开相应的程序、 文件夹、文档或 Internet 资源。
打开(O):	secpol.msc 🗸
	确定 取消 浏览(B)
图 40	

2. 修改"网络访问:将 Everyone 权限应用于匿名访问匿名用户"设置

山本地安全策略 文件(F) 操作(A) 查看(V) 帮助(H) 🗢 🄿 🙎 📰 💥 🖻 🔒 🚺 🎞 🔒 安全设置 策略 安全设置 2 🕨 📴 帐户策略 3 网络访问: 不允许 SAM 帐户和共享的匿名枚举 已禁用 🖌 🔀 本地策略 圆 网络访问:不允许存储网络身份验证的密码和凭据 已禁用 🗅 📴 审核策略 📓 网络访问: 将 Everyone 权限应用于匿名用户 已禁用 1 用户权限分配 圆网络访 安全选项 ? × 网络访问: 将 Everyone 权限应用于匿名用户 属性 圆网络访 高级安全 Windows 防火墙 圆 网络访 本地安全设置 说明 网络列表管理器策略 圆 网络访 ▷ 📔 公钥策略 网络访问:将 Everyone 权限应用于匿名用户 圆 网络访 👂 📔 软件限制策略 圆 网络访 ▷ 📔 应用程序控制策略 3 圆系统对 ▷ 🕄 IP 安全策略,在本地计算机 ◎ 已启用 (E) 圆系统对 🗅 🣔 高级审核策略配置 ○ 已禁用 (S) 圆系统加 圆系统加 圆 系统设 圆 系统设 圆 以安全 圆用户帐 圆用户帐 圆用户帐 圆用户帐 圆用户帐 圆用户帐 圆用户帐 圆用户帐 圆用户帐 确定 取消 应用(A)

修改"安全设置\本地策略\安全选项"下的"网络访问:将 Everyone 权限应用于 匿名访问匿名用户"设置,将规则启用,如下图:

图 41

六、 其它

防火墙运行状态下,可能 OPC 客户端会出现拒绝访问,可能是防火墙阻止程序访问网络,可以试着修改防火墙设置。调试或测试时,可先将防火墙禁用,排除干扰;
 其它防火墙软件配置,可参考 Windows 系统防火墙配置。

3. RPC 服务器不可用

这个错误意味着没能建立与 RPC 服务之间的网络连接。

*如果错误发生在尝试读取远程计算机上边的 OPC 服务器列表时,请检查 OPC 服务器 计算机与 OPC 客户端计算机的防火墙配置,看 OPCEnum 应用是否已经加入例外规则 列表。

*DCOM 所使用的 135 端口,是否已加入防火墙规则。

*如果错误发生在连接 OPC 服务器时,请检查 OPC 服务器计算机的防火墙配置,看 OPC 服务器应用程序是否已加入防火墙的例外规则列表。

4. 拒绝访问

请检查 DCOM 的安全配置,包括 OPC 服务器所在计算机与 OPC 客户端所在计算机。

5. "IOPCServerList Interface Not Found"错误

请在安装 OPC 运行库分发包或注册 OPC 运行库后,重新启动计算机系统。

OPC Client(客户端)运行在 Windows 7 时的 DCOM 配置

一、 安装 OPC Client 客户端
 安装倍福OPC Client,需要在本地PC上安装TC3的运行环境及对应的Function。

注: OPC Client. EXE为第三方OPC Client客户端(西门子)。

- 二、 创建用户并赋予访问权限
 - 1. 创建新用户

创建一个新用户,并赋予此用户运行和使用操作系统 DCOM 程序的权限。为了 降低整个系统的安全风险,可以创建一个受限用户,而不是建立管理员级用户。为 操作系统创建新用户需要管理员权限。

注意:

- A、需要在 OPC 服务器所在 OS 系统与 OPC 客户端所在 OS 系统,创建的用户的用 户名和密码相同(不一定)。
- B、由于 Windows 7 系列的 OS 系统 Guests 用户组的权限非常受限,所以新创建的 用户需要是 Users 用户组级别权限,或比 Users 用户组级别更高的权限。推荐使 用 Users 用户组。



图 43 通过"管理"菜单或"控制面板"创建用户



新用户	? 💌
用户名(U):	OPCUser
全名():	
描述(D):	OPC Vser
密码(P):	•••••
确认密码(C):	•••••
□ 用户下次登录	时须更改密码 (M)
📝 用户不能更改	女密码 (S)
🔽 密码永不过期	月(₩)
🔲 帐户已禁用 (B)
帮助(H)	创建(8) 关闭(0)

图 45 新用户属性 创建新用户,并设置用 户属性。若是为了安全考量,请保持密码不为空。

2. 赋予用户访问 DCOM 的权限

要想使新创建的用户有使用 DCOM 的权限,需要将用户加入"Distribute COM Users"用户组。



图 46 用户组

Distributed COM	Users 属性	? <mark>×</mark>	
常规			
Distr	ibuted COM Users		
描述(2):	描述 (E): 成员允许启动、激活和使用此计算机上的分布式 COM 对象。		
成员(M):			
	1		
	■ 古列下 次田 白粱字叶:		
添加 (0)	目到下一次用户受求的 删除(R) 成员关系的更改才生效	° °	
	确定 取消 应用 (A)	帮助	

.

图 47 添加用户到用户组

选择用户	? 🔀
选择此对象类型 (S):	
用户或内置安全主体	对象类型(0)
查找位置 ():	
ZHAO-PC	位置(L)
输入对象名称来选择(示例)(2):	
_1	检查名称(C)
高級 (4) 确定	取消

图 48 选择要添加的用户

选择用户	? 🗙
选择此对象类型(S): 用户或内置安全主体 查找位署(P):	对象类型(0)
ZHAO-PC	位置(L)
一般性查询	
名称(A): 起始为 🚽	列(C)
描述 (0): 起始为 ▼	▲ 立即查找 03)
 ■ 禁用的帐户(B) ■ 不过期密码(X) 	(T)
自上次登录后的天数 (I): 3	<i>?</i>
搜索结果 (U):	定取消
名称 (RDN) 所在文件夹	*
LINTERACTIVE LIUSR LIOCAL SER 2	
RETWORK S	=
CPCUser ZHAO-PC	
REMOTE IN Service	T



选择用户	? 💌
选择此对象类型(S): 用户或内置安全主体	对象类型(0)
查找位置(F): ZHAO-PC	
输入对象名称来选择(<u>示例</u>)(E):	
ZHAO-PC\OPCUser	2 检查名称 (C)
高級(A)	确定 取消

图 50 选择添加的用户

Distributed CO	M Users 属性	8 🛛
常规		
Dist Dist	ributed COM Vsers	
描述(E):	成员允许启动、激活和使用此计算机上 COM 对象。	的分布式
成员(M):		
DPCVser	1	2
添加 (0)	自到下一次用户登录时 删除(B.) 成员关系的更改才生学	加用户的组
	确定 取消 应用 (4)	帮助

图 51 完成添加

可以添加多个用户到"Distribute COM Users"用户组,也可以添加现有用户到用户组。

Ξ,

修改操作系统 Firewall(防火墙)关于 DCOM 和 OPC 的规则

由于 DCOM 使用操作系统的 135 端口,所以要想不同计算机上面的 OPC 服务器和 OPC 客户端通讯正常,要修改防火墙规则,允许 135 端口的连接。如果 OPC 服务器和 OPC 客户端安装在同一台计算机,不需要修改防火墙规则。下面用 Windows 7 的防火墙 配置过程为示例。

🖅 运行
Windows 将根据您所输入的名称,为您打开相应的程序、 文件夹、文档或 Internet 资源。
打开(O): wf.msc 🗸
确定 取消 浏览(B)

图 52 进入防火墙管理控制台

Windows 7 用户: 要打开防火墙管理控制台,可以从"开始"->"控制面板"->"管理 工具"->"Windows 防火墙"->"高级设置",或在"运行"输入"wf.msc"命令。 Windows Server 2008 R2 用户: 要打开防火墙管理控制台,可以在"服务器管理工具", 或在"运行"输入"wf.msc"命令。

3、开放 DCOM 访问

在默认状态, Windows 防火墙是阻止另一台计算机连接的。如果要允许 OPC 客户端 与 OPC 服务器正常访问,需要放开这个访问规则。

🔐 高级安全 Windows 防	火墙			
文件(F) 操作(A) 查看	(V) 帮助(H)			
🗢 🄿 🖄 📅 🛃				
🔐 本地计算机 上的高级3	入站规则			
🔜 入站规则	名称	组		配置文件
1111日1月1日	Media Center Extender - 媒体流(TCP-In)	Media Center	Extender	所有
	Wetlogon 服务(NP-In)	Netlogon 服务		所有
	SNMP Trap Service (UDP In)	SNMP Trap		域
	SNMP Trap Service (UDP In)	SNMP Trap		专用,公
	Windows Management Instrumentation (ASync-In)	Windows Man	agement	域
	Windows Management Instrumentation (ASync-In)	Windows Man	agement	专用,公
	Windows Management Instrumentation (DCOM-In)	Windows Man	agement	域
	Windows Management Instrumentation (DCOM-In)	Windows Man	agement	专用,公
	Windows Management Instrumentation (WMI-In)	启用规则(E)	ment	专用,公
	Windows Management Instrumentation (WMI-In)	剪切(T)	ment	域
	●Windows Media Player (UDP-In) 鼠标右键	复制(C)	ayer	所有
	Windows Media Player 网络共享服务(HTTP-Stream)	删除(D)	ayer	专用,公
	Windows Media Player 网络共享服务(HTTP-Stream)		ayer	域
	● Windows Media Player 网络共享服务(qWave-TCP-I		ayer	域
	Windows Media Player 网络共享服务(qWave-TCP-I	帮助(H)	ayer	专用,公
	● Windows Media Player 网络共享服务(qWave-UDP-In)	Windows Med	ia Player	专用,公
	◎ Windows Madia Dlaver 网络共宣职冬(aWave-LIDD-In) 图 53 防火墙规则	Windows Med	ia Dlaver	+at:



图 54 允许 DCOM 连接

Windows Management Instrumentation (DCOM-In) 雇性 🛛 🛛 🗨		
常规 程序和服务 计算机 协议和端口 作用域 高级 用户		
本地 IP 地址 ● 任何 IP 地址 (M) ● 下列 IP 地址 (T): 1		
[添加 @)]		
远程 IP 地址		
● 任何 IP 地址 (Y) ② 下列 IP 地址 (Y)		
[編辑 (I)]		
3		
确定 取消 应用 (A)		

图 55 防火墙 DCOM 规则作用域设置

Windows Management Instrumentation (DCOM-In) 雇性
常规 程序和服务 计算机 协议和端口 作用域 高级 用户 配置文件
指定此规则应用的配置文件。 ✓ 域 @) ✓ 专用 @) ✓ 公用 @)
接口类型 指定应用此规则的接口类型。 自定义 (C)
→ 近绿遍历允许计算机接受未经请求的人站数据包,这 些数据包已通过诸如网络地址转换(MAT)路由器或防火 墙之类的边缘设备(E)。
阻止边缘遍历 ▼
阻止应用程序通过 NAT 边缘设备从 Internet 接收主 动提供的流里。
<u>了解这些设置的详细信息</u> 3
确定 取消 <u></u>

图 56 防火墙 DCOM 规则高级属性设置

Windows 7 用户:如果 "COM+ Network access" 或 "DCOM" 规则不在防火墙的预 定义规则列表中,可自己手动添加两个 "PORT" (端口)规则:

- TCP 135
- UDP 135
- 4、创建 OPC 程序规则

需要手动添加 OPC 客户端程序的规则。同样也需要添加 OPCEnum 系统服务程 序规则,因为要连接远程的 OPC 服务器计算机就是通过它获得那台台计算机上面的 OPC 服务器名称列表的。

下面我们通过创建 OPCEnum 应用的规则,演示如何创建应用的防火墙规则。可用同样步骤创建 OPC 客户端的防火墙规则。



- 图 57 创建应用规则
- *选择"新建规则";
- *选择"程序"类型规则
- *点击"下一步"按钮



图 58 选择应用程序文件

*选择"此程序路径"项目;

*填写程序的完整路径和应用程序名称;

*也可使用"浏览"按钮,在弹出的文件选择对话框里查找磁盘上应用程序的文件 名;

*点击"下一步"按钮;





图 60 规则适用条件



图 61 规则命名

🔐 高级安全 Windows 防>	火墙					
文件(F) 操作(A) 查看(V) 帮助(H)					
🗢 🄿 🖄 🖬 🗟	? 🗊					
🔐 本地计算机 上的高级3	入站规则					
🗱 入站规则	名称	组	配置文件	已启用	操作	替代 🔶
III 法按由会规则	OPCEnum		所有	是	允许	否
	Media Center Extender - HTTP 流(TCP	Media Center Extender	所有	否	允许	否 🗉
	BranchCache 对等机发现(WSD-In)	BranchCache - 对等机发	所有	否	允许	否
1	BranchCache 内容检索(HTTP-In)	BranchCache - 内容检索(所有	否	允许	否 🗌
	● BranchCache 托管缓存服务器(HTTP-In)	BranchCache - 托管缓存	所有	否	允许	否
	ISCSI 服务(TCP-In)	iSCSI 服务	域	否	允许	否
	● iSCSI 服务(TCP-In)	iSCSI 服务	专用, 公用	否	允许	否
	Media Center Extender - qWave (TCP	Media Center Extender	所有	否	允许	否
	Media Center Extender - qWave (UDP	Media Center Extender	所有	否	允许	否
	Media Center Extender - RTSP (TCP-In)	Media Center Extender	所有	否	允许	否
	Media Center Extender - SSDP (UDP-In)	Media Center Extender	所有	否	允许	否
	Media Center Extender - WMDRM-N	Media Center Extender	所有	否	允许	否

图 62 规则处于活跃状态 同

样步骤,创建 OPC 客户端应用程序的防火墙访问规则。

四、 配置 DCOM 安全

为通过网络正常访问 OPC 服务器,需要配置 DCOM 的访问和激活安全属性。

 启动"组件服务" 在菜单"开始\运行",输入: dcomcnfg,点击"确定"按 钮,进入"组件服务 管理器"。 如图:



图 63 运行组件服务

 配置"我的电脑"的安全设置 在"组件服务"管理器的左侧树形菜单,选择 "组件服务\计算机\我的电脑", 在鼠标右键的弹出菜单,选择"属性"项目, 如图:



图 64 属性 在弹出的"我的电脑属性",选择"默认属性"标签 页,如下图:

我的电脑 属性 ? 王
常规 选项 默认属性 默认协议 COM 安全 MSDTC
☑ 在此计算机上启用分布式 COM (B)
Internet 服务(N)
默认分布式 COM 通信属性
身份验证级别指定数据包级别上的安全。
默认身份验证级别(0):
<u> </u>
用各戶端标识进行操作。
默认模拟级别(I):
标识 ▼
踪安全。
□ 提供附加的引用跟踪安全 (P)
进一步了解如何设置这些属性。
确定 取消 应用 (A)

图 65 属性

请确认几个属性的设置内容或状态: 在此计算机上启用分布式 COM,此属性处于"选中"状态;

默认分布式 COM 通信属性栏目下,"默认身份验证级别",选择的项目是:"连接","默认模拟级别",选择的项目是:"标识"。选择"我的电脑属性"属性页面的"默认协议"标签页,如下图:

我的电脑 属性	? <mark>- × -</mark>
常规 选项 默认属性 默认协议 COM 安全 MSDTC	
DCOM 协议(M)	
▼面向连接的 TCP/IP	
添加 (2) 移除 (8) 上移 (0) 下移 (0) 属 (ŧœ)
┌ 描述	
可用于此计算机上 DCOM 的网络协议集。协议顺序反映了 协议的优先级,最上面的协议具有最高优先级。	了使用
进一步了解如何设置这些事件。	
福完 即消 [「山田徳」
	2 Constant

图 66 属性

确认 DCOM 协议属性内容是:面向连接的 TCP/IP。选择"我的电脑 属性"属性页面的"COM 安全"标签页,如下图:



图 67 COM 安全

选择 "COM 安全"标签页面的"访问权限"栏目的"编辑默认值," 按钮(图 67 中按钮 1),弹出"访问权限"设置对话框,如下图:



图 68 配置访问权限 点击此对话框上的"添加"按钮,添加下边列表的用户, 并设置用户的访问权 限,核实后,点击"确定"按钮保存。

NO.	组或用户名	本地访问	远程访问	属性
1	Distribute COM Users	允许	允许	系统内置用户组
2	Anonymous logon	允许	允许	系统内置帐户
3	everyone	允许	允许	系统内置帐户
4	Interactive	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	系统内置帐户
6	SELF	允许	允许	系统内置帐户
7	NETWORK	允许	允许	系统内置帐户
8	NETWORK SERVICE	允许	允许	系统内置帐户
9	ADMINISTRTORS	允许	允许	系统内置帐户
10	Users	允许	允许	系统内置帐户

选择 "COM 安全"标签页面的"访问权限"栏目的"编辑限制,," 按钮(图 67 中按钮 2),弹出"访问权限"设置对话框,如下图:



图 69 配置访问权限 点击此对话框上的"添加"按钮,添加下边列表的用户, 并设置用户的访问权 限,核实后,点击"确定"按钮保存。

NO.	组或用户名	本地访问	远程访问	属性
1	Distribute COM Users	允许	允许	系统内置用户组
2	Anonymous logon	允许	允许	系统内置帐户
3	everyone	允许	允许	系统内置帐户
4	Interactive	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	系统内置帐户
6	NETWORK	允许	允许	系统内置帐户
7	NETWORK SERVICE	允许	允许	系统内置帐户
8	ADMINISTRTORS	允许	允许	系统内置帐户
9	Users	允许	允许	系统内置帐户

选择 "COM 安全"标签页面的 "启动和激活权限"栏目的 "编辑默认值,," 按钮 (图 67 中按钮 3),弹出 "启动和激活权限"设置对话框,如下图:



图 **70** 配置启动激活权限 点击此对话框上的"添加"按钮,添加下边列表的用 户,并设置用户的访问权 限,核实后,点击"确定"按钮保存。

NO.	用户名	本 地 启动	远程 启动	本 地 激活	远 程 激活	属性
1	Distribute COM Users	允许	允许	允许	允许	系统内置用户 组
2	ANONYMOUS LOGON	允许	允许	允许	允许	系统内置帐户
3	Everyone	允许	允许	允许	允许	系统内置帐户
4	INTERACTIVE	允许	允许	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	允许	允许	系统内置帐户
6	NETWORK	允许	允许	允许	允许	系统内置帐户
7	NETWORK SERVICE	允许	允许	允许	允许	系统内置帐户
8	ADMINISTRTORS	允许	允许	允许	允许	系统内置帐户
9	Users	允许	允许	允许	允许	系统内置帐户

选择 "COM 安全"标签页面的 "启动和激活权限"栏目的 "编辑限制,," 按钮 (图 67 中按钮 4),弹出 "启动和激活权限"设置对话框,如下图:



冬	71 配置启动激活权限	点击	此对话框	上的'	'添加"	按钮,	添加-	下边列表的	用
户,	并设置用户的访问权	限,	核实后,	点击	"确定"	按钮	保存。		

NO.	用户名	本 地 启动	远程 启动	本 地 激活	远 程 激活	属性
1	Distribute COM Users	允许	允许	允许	允许	系统内置用户 组
2	ANONYMOUS LOGON	允许	允许	允许	允许	系统内置帐户
3	Everyone	允许	允许	允许	允许	系统内置帐户
4	INTERACTIVE	允许	允许	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	允许	允许	系统内置帐户
6	NETWORK	允许	允许	允许	允许	系统内置帐户
7	NETWORK SERVICE	允许	允许	允许	允许	系统内置帐户
8	ADMINISTRTORS	允许	允许	允许	允许	系统内置帐户
9	Users	允许	允许	允许	允许	系统内置帐户

配置完成后,点击"我的电脑属性"属性页面的"确定"按钮,由于涉及到系统安全属性的修改,此时操作系统弹出警告消息,如图:

DCOM 计算机范围设置
您将要修改计算机范围的 DCOM 设置,这将影响该计算机上的所有应 用程序,因此某些应用程序可能不能正常工作。是否更新 DCOM 设置?
是(M)、香(N)

图 72 警告消息

_

由于是我们手动修改的安全设置,并确认修改,点击"是"按钮,保存刚才做出的所有修改,退出"我的电脑属性"属性页面。

配置 OPCENUM 的安全设置 在"组件服务"左侧树形菜单,选择"组件服务\计算机\我的电脑\DCOM 配置", 在列表中选择 opcenum 项目,在鼠标右键弹出的菜单,选择"属性"项目,如 下图:





图 74

在"OPCENUM 属性"框,选择"安全"标签页,如下图:

OpcEnum	? <mark>×</mark>
常规 位置 安全 终结点 标识	
启动和激活权限	
◎ 使用默认值 (U)	
● 自定义 (S) 1→ 编辑 0	E)
访问权限	
◎ 使用默认值 健)	
◎ 自定义 (M) 2 → 编辑 0	D)
配置权限 ◎ 使用默认值 (L)	
◎ 自定义 (T) 编辑 C	I)
进一步了解如何设置这些属性。	
确 定 取消	应用(A)

图 75 在"安全"标签页,选择"启动和激活权限"栏目,选择"自定义"选项,并点击"编辑,,"按钮,如下图:



图 **76** 在弹出的"启动和激活权限"属性设置对话框,使用"添加"按钮,添加 下表 的组或用户,核实并确认后,点击"确定"按钮保存。

NO.	用户名	本 地 启动	远程 启动	本 地 激活	远 程 激活	属性
1	Distribute COM Users	允许	允许	允许	允许	系统内置用户 组
2	ANONYMOUS LOGON	允许	允许	允许	允许	系统内置帐户
3	Everyone	允许	允许	允许	允许	系统内置帐户
4	INTERACTIVE	允许	允许	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	允许	允许	系统内置帐户
6	NETWORK	允许	允许	允许	允许	系统内置帐户
7	NETWORK SERVICE	允许	允许	允许	允许	系统内置帐户
8	ADMINISTRTORS	允许	允许	允许	允许	系统内置帐户
9	Users	允许	允许	允许	允许	系统内置帐户

在"安全"标签页,选择"访问权限"栏目,选择"自定义"选项,并点击"编辑,"按钮,如下图:



图 **77** 在弹出的"访问权限"属性设置对话框,使用"添加"按钮,添加下表的 组或 用户,核实并确认后,点击"确定"按钮保存。

NO.	组或用户名	本地访问	远程访问	属性
1	Distribute COM Users	允许	允许	系统内置用户 组
2	Anonymous logon	允许	允许	系统内置帐户
3	everyone	允许	允许	系统内置帐户
4	Interactive	允许	允许	系统内置帐户
5	SELF	允许	允许	系统内置帐户
6	SYSTEM	允许	允许	系统内置帐户
7	NETWORK	允许	允许	系统内置帐户
8	NETWORK SERVICE	允许	允许	系统内置帐户
9	ADMINISTRTORS	允许	允许	系统内置帐户
10	Users	允许	允许	系统内置帐户

在 "OPCENUM 属性" 框,选择 "标识" 标签页,确认 "选择运行此应用程序 的用户账户" 属性,设置项目是:系统账户(仅用于服务),如下图:

OpcEnum 雇性 ? X
常规 位置 安全 终结点 标识
选择运行此应用程序的用户帐户
○ 交互式用户(I)
○ 启动用户(L)
◎ 下列用户(0)
用户(E): 浏览(B)
密码(P):
确认密码 (M):
◎ 系统帐户(仅用于服务)(S)
进一步了解如何设置这些属性。

图 78

确认后点击"确定"按钮保存所作的修改。

- 五、 配置本地安全策略
- 1、启动"本地安全策略"管理器 在"开始\运行"输入: secpol.msc, 点击"确定"按钮, 启动"本地安全策略" 管理器, 如下图:

🥶 运行
Windows 将根据您所输入的名称,为您打开相应的程序、 文件夹、文档或 Internet 资源。
打开(O): secpol.msc 🔹
确定 取消 浏览(B)

图 79

2、修改"网络访问:将 Everyone 权限应用于匿名访问匿名用户"设置 修改"安全设置\本地策略\安全选项"下的"网络访问:将 Everyone 权限应用于匿名访 问匿名用户"设置,将规则启用,如下图:



图 80

3、

六、 其它 Client测试