

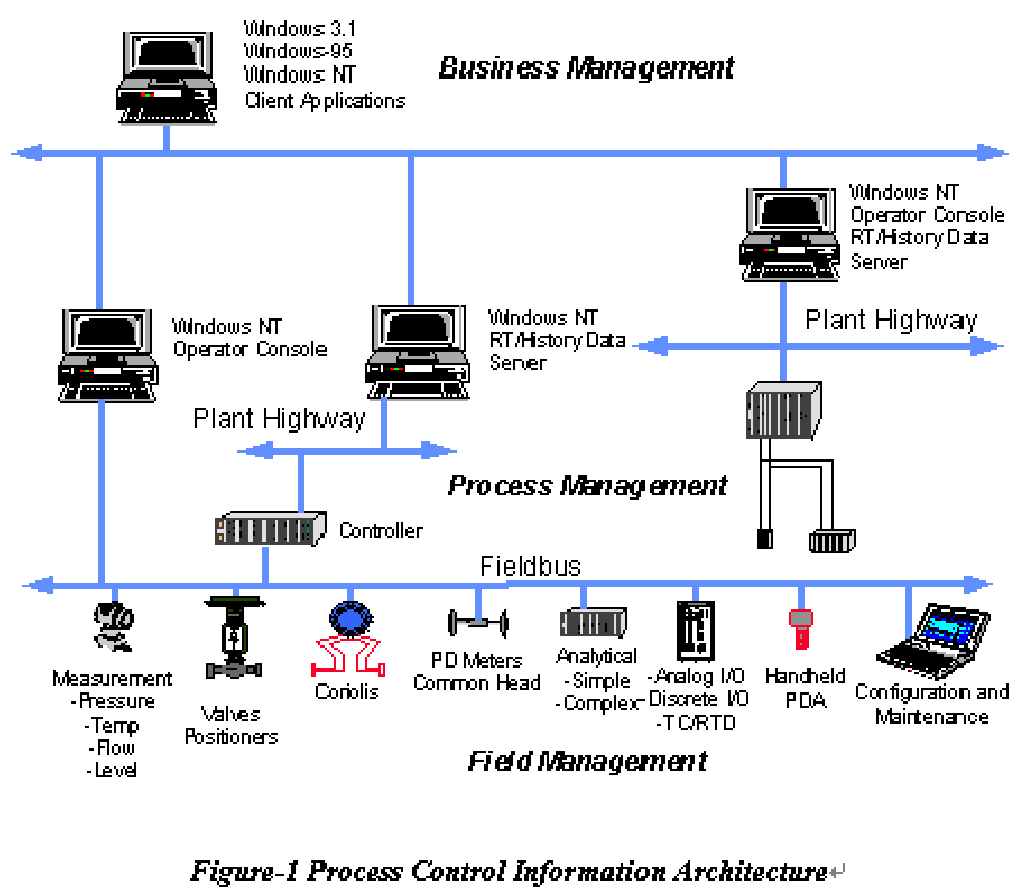
SDK
MEGAsys OPC Server
V1.0
For
OPC Client

2010/7

1.What is OPC?

OPC 是 OLE for Process Control 的縮寫。顧名思義，OPC 是一種利用微軟的 COM/DCOM 技術來達成自動化控制的協定，根據 OPC Specification 的定義，OPC is "a standard mechanism for communicating to numerous data sources, either devices on the factory floor, or a database in a control room."

在現今的工業自動化中，我們需要一套整合的資訊系統，由底層的各项裝置擷取資訊 (Field Management)，中層的控制系統或圖控應用程式進行程序的控制 (Process Management)，再由最上層的整合軟體將這些資訊整合起來以供企業決策或效能提昇，如下圖所示：



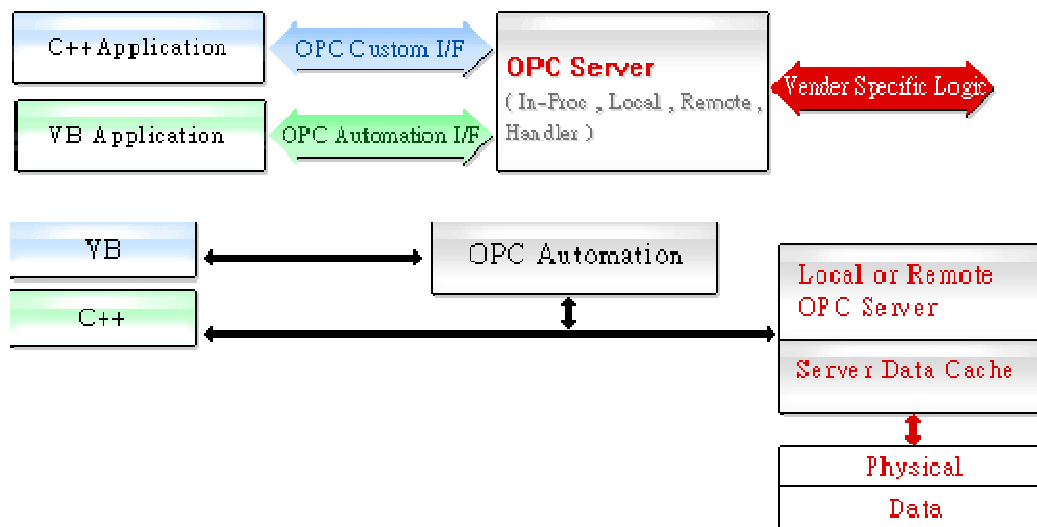
OPC 為硬體製造商與軟體發展商提供了一條橋樑，透過硬體廠商提供的 OPC Server 介面，軟體發展者不必考慮各項不同硬體間的差異，便可自硬體端取得所需的資訊，所以軟體發展者僅需專注於程式本身的控制流程的運作。此外，由於 COM/DCOM 實作並隱藏了網路的細節，透過 OPC 可以很容易地達成遠端控制的理想。

2.How does OPC work?

在說明 OPC Server/Client 運作方式之前，我們先簡單介紹一下 Microsoft 發展的 COM/DCOM 是什麼？

COM 是一種發展軟體元件的方法，所謂的軟體元件，是指一個可以提供應用程式、作業系統、以及其他元件服務的二進位可執行程式。事實上，發展自訂的 COM 物件就好像是在建構一套可以動態執行的物件導向 API 一般。你可以在應用程式執行的時期隨意拼上或移除所需要的元件。依據 COM 這樣的觀念，發展應用程式就像是堆積木一樣，每一個 COM 元件就是一塊積木，你可以利用各式各樣不同的積木，拼湊出你所需要的應用程式。

在實作上，COM 透過一組一組的介面 (Interface) 提供服務，所有 COM 元件的使用者，都必須透過這些 Interface 來使用元件提供的功能。OPC 的規格中便定義了許多 OPC Server 應該提供的 Interface，要撰寫一個 OPC Server 的 COM 元件，你必須在你的元件中加入這些介面，並提供它們的實作，Client 便可以透過這些介面，操作連接到 OPC Server 的硬體裝置，這也就是 OPC Server/Client 運作的方式。以下的圖示可以讓這樣的觀念更清晰：

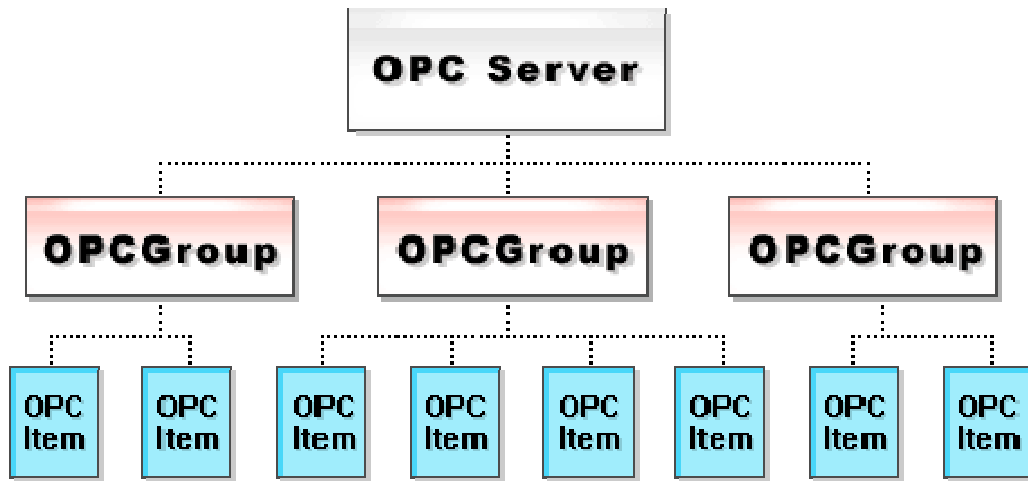


3. OPC Server 架構

如前面所述，OPC Server 透過一組一組的介面提供服務，不過在實作的架構上，OPC Server 共分為三層：分別是 OPCServer, OPCGroup, OPCItem

其中每一個 OPCItem 對應到一個實際的硬體裝置上的某一個 channel 或 port；每一個 OPCGroup 則包含了許多的 OPCItem，同時並定義這些 OPCItem 更新的時間、方式，以及提供讀取 OPCItem 值的介面；而每一個 OPCServer 則包含若干個 OPCGroup，同時提供操作這些 OPCGroup 的介面。

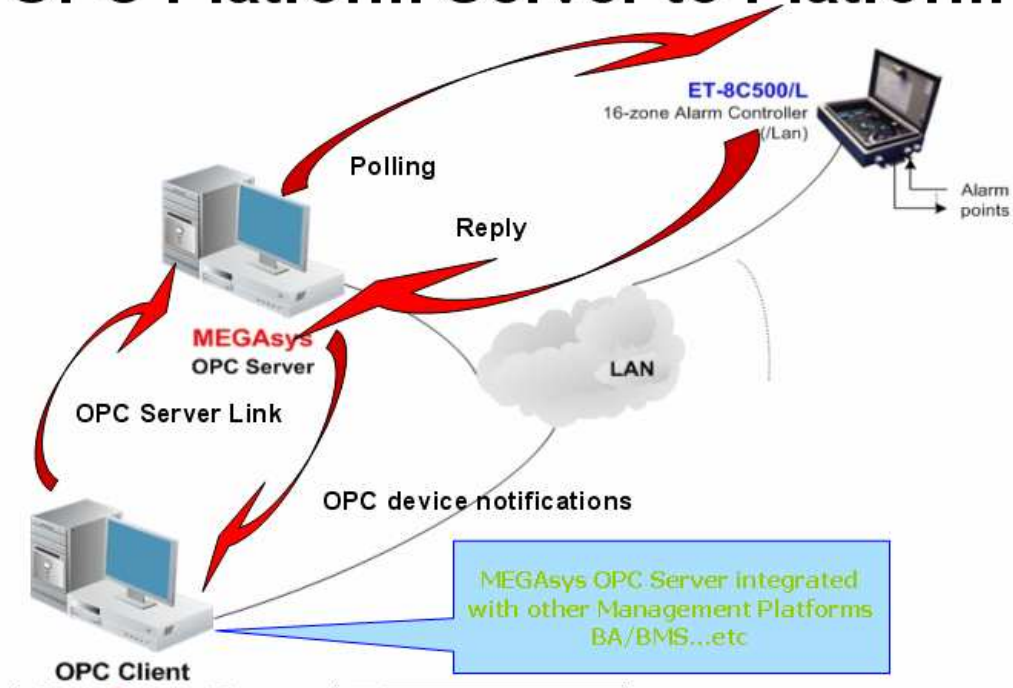
下圖可以較清楚地說明 OPCServer/OPCGroup/OPCItem 間的關係：



OPC Server/Client 是一套利用微軟的 COM/DCOM 技術達成工業自動化資料取得的架構。OPC Server 提供了許多的介面，Client 端透過這些介面，可以取得與 OPC Server 相連的硬體裝置的資訊，而無須瞭解這些硬體裝置的細節資訊。也就是說，程式設計者可以使用相同的程式碼，操作不同的硬體裝置，充分達成 software reuse 的理想。同時，由於 COM/DCOM 已實作了網路部分的細節，也使得 Client 對 OPC Server 進行遠端存取非常容易，使程式設計者很容易地達成遠端控制的目標。

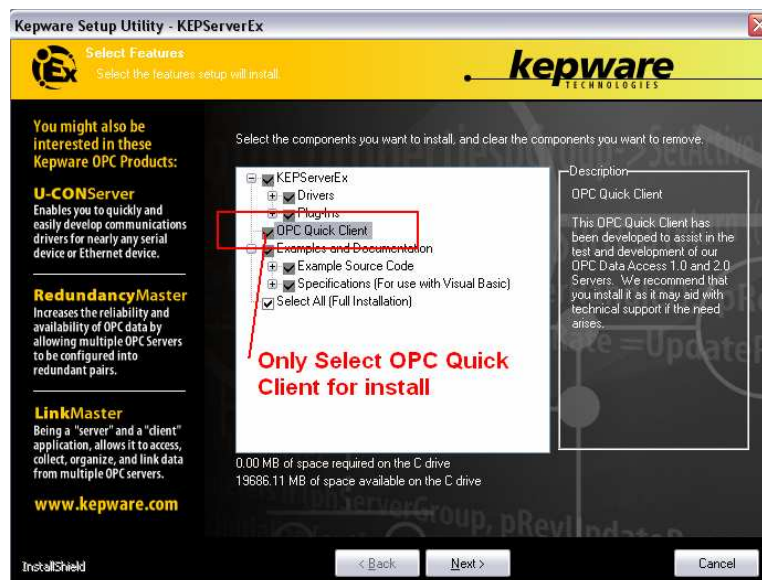
4. MEGAsys OPC Server and OPC Client

OPC Platform Server to Platform

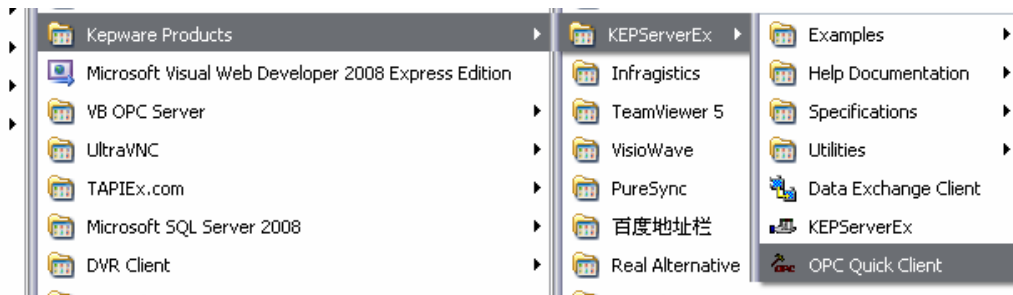


5) Install KEPServerEX as OPC Client and testing

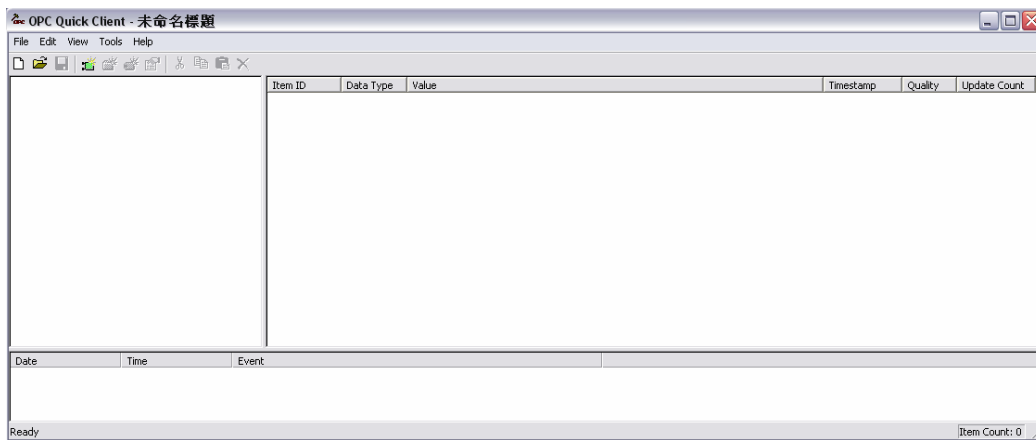
- 1) Install KEPServerEX Client side for Emulation OPC Client use.



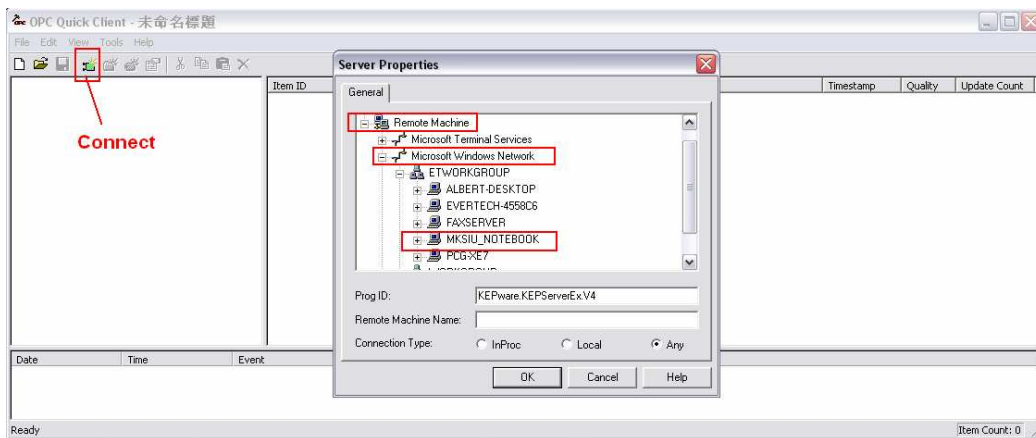
2) After install completed and execute the KEPServerEX OPC Quick Client

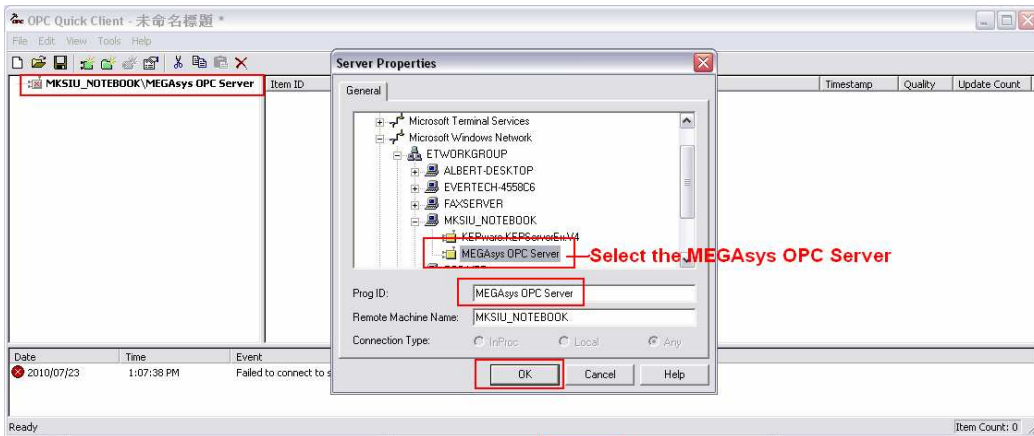


3) Show as follows:

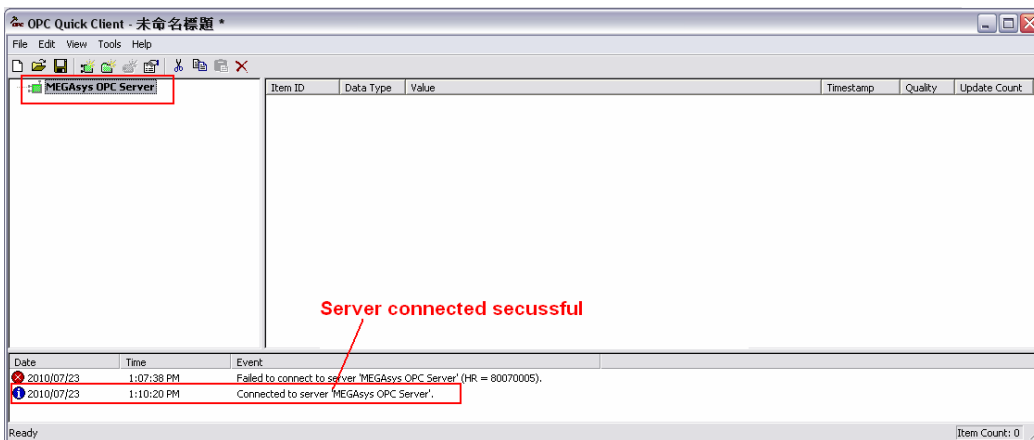


4) Make Connect to MEGAsysOPC server

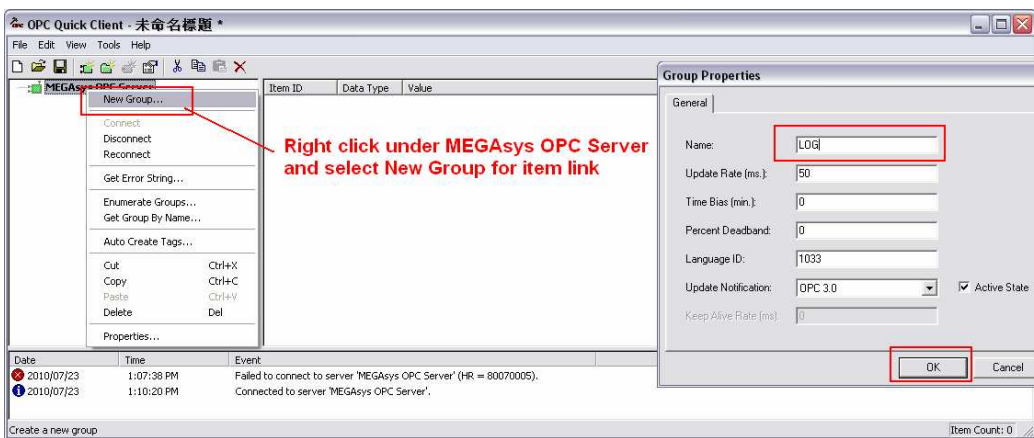




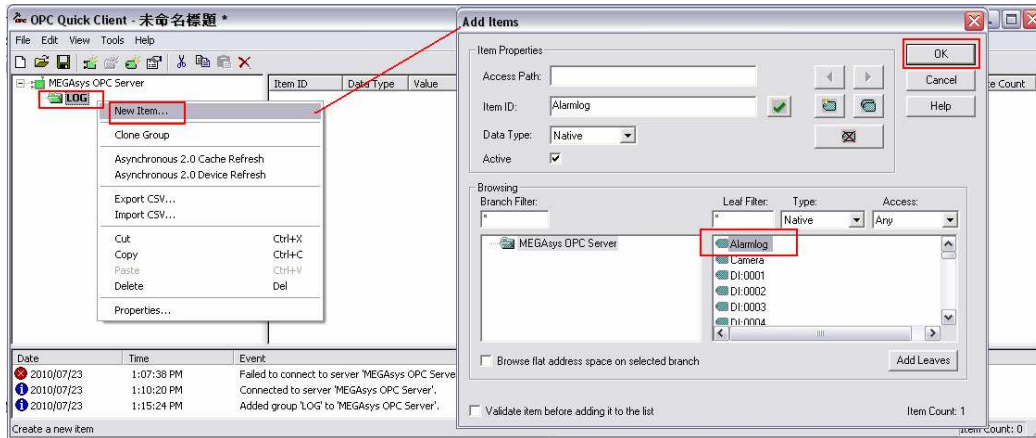
5) Connection is Make



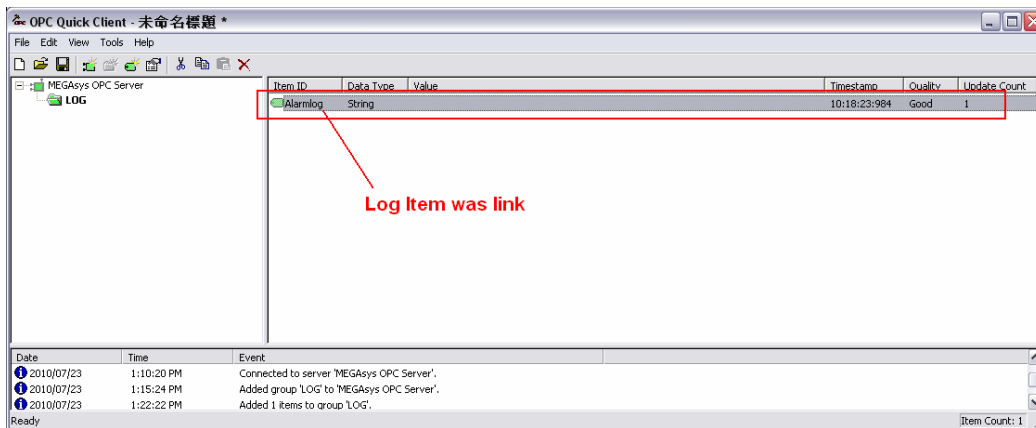
6) Make a OPC Connect **OPC GROUP NAME** for item connection



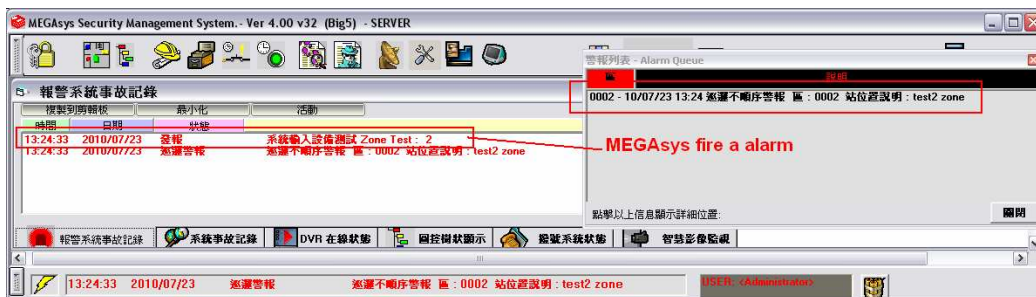
7) Connect with OPC ITEM



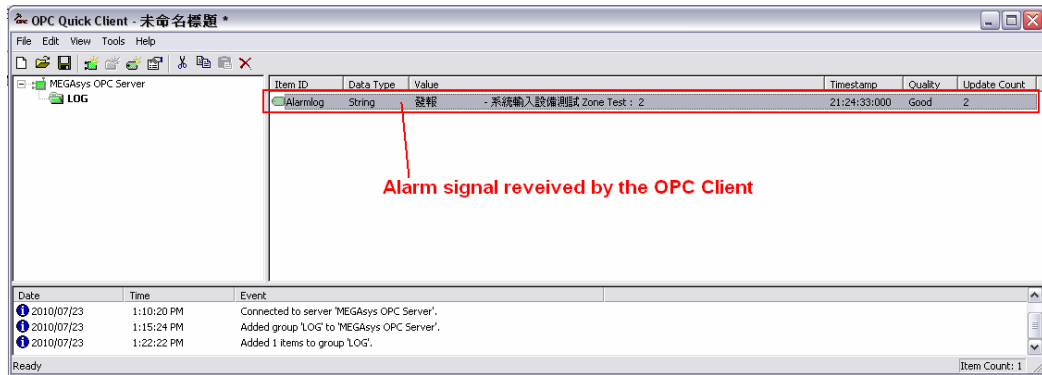
8) Item Link



9) Test it form MEGAsys OPC server



10) OPC Client will received the alarm message from MEGAsys server



6) OPC ITEM name with MEGAsys

1) Alarm Input point

Size: Points start from 0001 to 2048 (Max/Server)

Name: **DI:0001**

DI:0002

-

DI:2048

Direction: From OPC MEGAsys Server and to MEGAsys OPC server

2) Control Output Point

Size: Points start from 0001 to 2048 zones for server

Name: **DO:0001**

DO:0002

-

DO:2048

Direction: Form OPC server and to OPC Server (Input/Output)

3) System Log

Event log: All MEGAsys system event log

Name: **Eventlog**

Alarm log: All MEGAsys system alarm log

Name: **Alarmlog**

Direction: Form OPC Server (Input)

4) System Macro Control

Direct Macro control to MEGAsys Server

Name: **MACRO**

Direction: To MEGAsys OPC Server (Output)

Name: **MacroCtrl**

Direction: To MEGAsys OPC Server

Control: On/Off switch the macro execute

5) CCTV Control

Camera: Switch Camera for Matrix CCTV Control

Name: **Camera**

Size: 1 to 640 (Max/Server)

Direction: To OPC Server (Output)

Monitor: Switch Control for Monitor Matrix CCTV Control

Name: **Monitor**

Size: 1 to 160 (Max/Server)

Direction: To OPC Server (Output)

DVR: DVR status message

Name: **DVR**

Size: 1 – 100 (Max/Server)

Direction: From MEGAsys OPC Server (Input)

6) Access Control System door control

Name: **Door:0001**

Door:0002

-

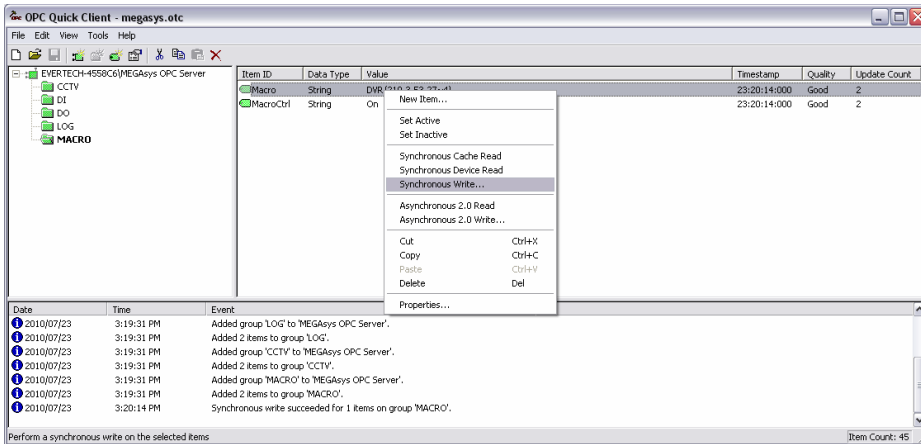
Door:0480 (Max/Server)

Size: 1-480 (Max/Server)

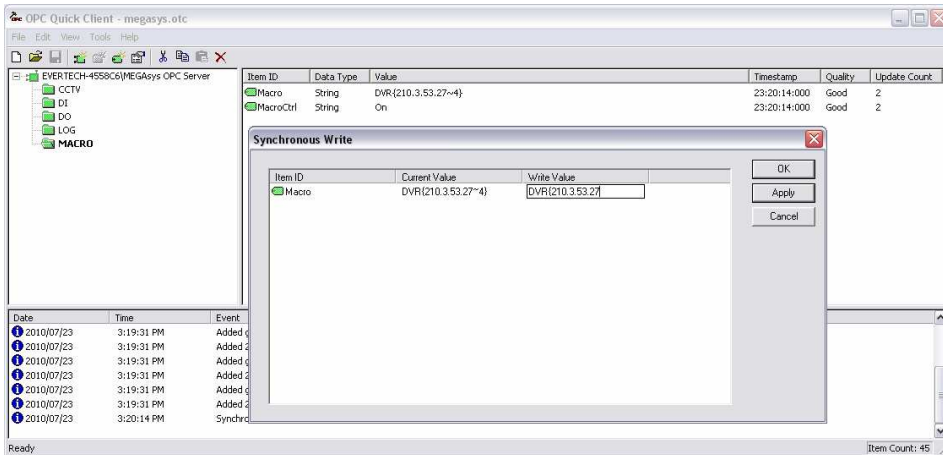
Direction: Form MEGAsys OPC Server and to MEGAsys OPC server

Command:On/Off (Door Open/Door Close)

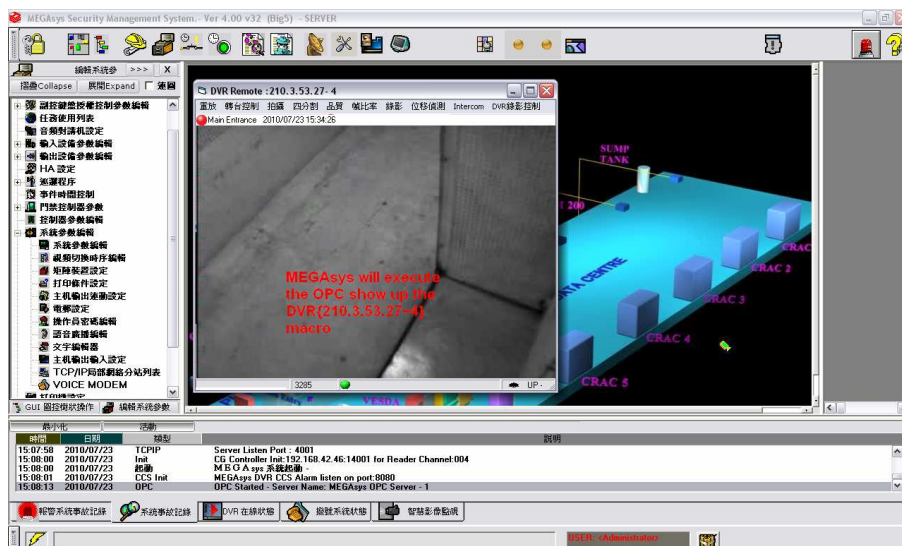
7) MEGAsys OPC Server Control Test



1) Select the MACRO item from OPC client, and right click select sync write.

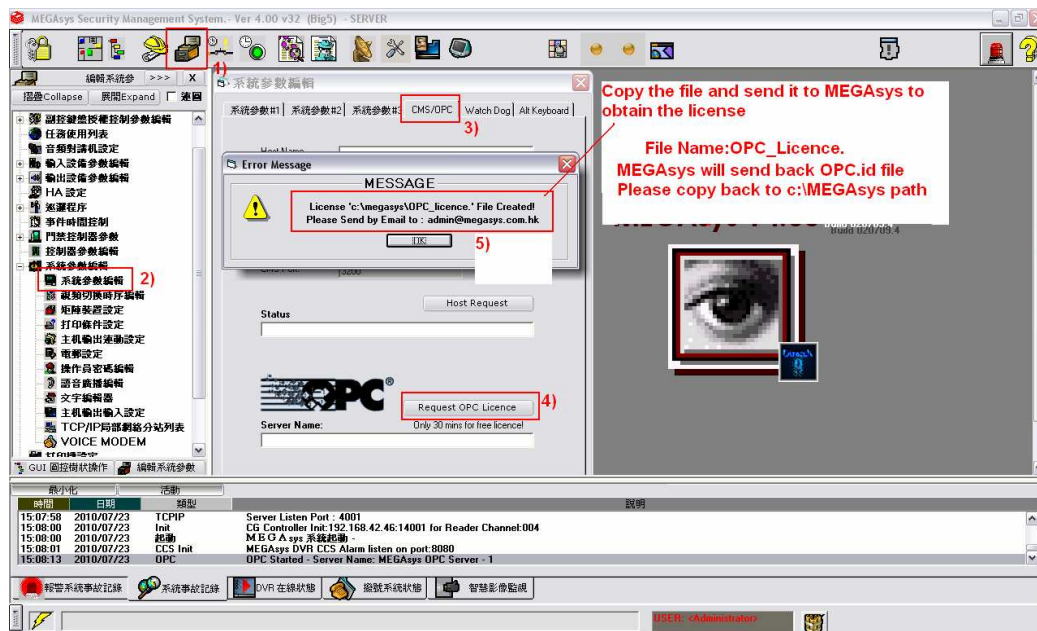


2) Type your Macro command that send to MEGAsys OPC server



Appendix A

Obtain MEGAsys OPC Server License



After obtain the license, copy back "OPC.ID" to c:\MEGAsys path, and restart the MEGAsys.

You will see OPC server enabled message display in event log.

Appendix B

Security Setup for OPC Server/Client

OPC technology relies on Microsoft's COM and DCOM to exchange data between automation hardware and software; however it can be frustrating for new users to configure DCOM properly. If you have ever been unable to establish an OPC connection or transfer OPC data successfully, the underlying issue is likely DCOM-related. This whitepaper discusses the steps necessary to get DCOM working properly and securely.

A simple and effective strategy to establish reliable DCOM communication involves the following steps:

1. Remove Windows Security
2. Setup mutual User Account recognition
3. Configure System-Wide DCOM settings
4. Configure Server Specific DCOM settings
5. Restore Windows Security

In addition, the whitepaper covers troubleshooting tips to identify common OPC and DCOM problems, their symptoms, causes, and how to solve them. This will help integrators set up reliable and secure OPC connections.

1. Remove Windows Security

The first step to establish DCOM communication is to disable the Windows Firewall, which is turned on by default in Windows XP Service Pack 2 and later. The Firewall helps protect computers from unauthorized access (usually from viruses, worms, and people with malicious or negligent intents). If the computer resides on a safe network, there is usually little potential for damage as long as the Firewall is turned off for a short

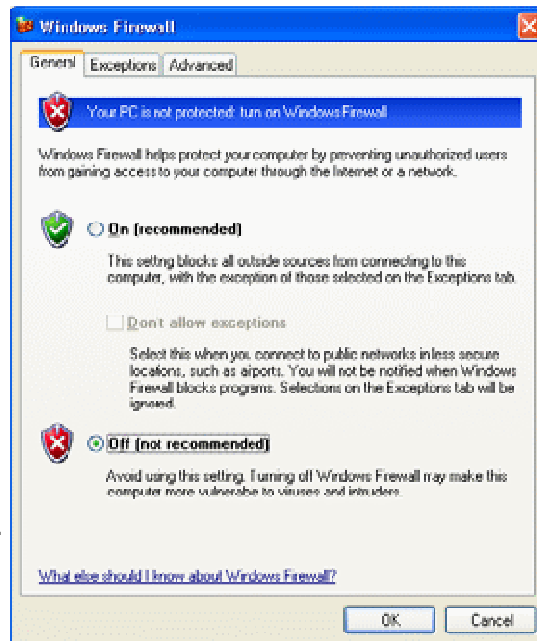


Image 1: Temporarily turn off the Windows Firewall to allow remote access to the OPC Server computer.

period of time. Check with the Network Administrator to ensure it is safe to turn off the Firewall temporarily. You will turn the Firewall back on in section 5, titled “Restore Windows Security,” on page 7.

To turn off the Windows Firewall, follow the steps below:

- a. Click on the Windows Start button, select the Control Panel, and finally click on Windows Firewall.
- b. In the General tab, select the “Off (not recommended)” radio button (refer to Image 1).

2. Setup mutual User Account recognition

To enable both computers to properly recognize User Accounts, it is necessary to ensure that User Accounts are recognized on both the OPC Client and Server computers. This includes all the User Accounts that will require OPC access.

2.1 Adding User Accounts

Ensure that both computers have access to the same User Name and Password combinations. User Names and Passwords must match on all computers that require OPC access. Note:

- A User Account must have a User Name and Password. It is not possible to establish communication if a User Account does not have a Password.
- When using Windows Workgroups, each computer must have a complete list of all User Accounts and Passwords.
- When using a single Windows Domain, User Accounts are properly synchronized by the Domain controller.
- When using multiple Windows Domains, you will either have to establish a Trust between the Domains, or add a Local User Account to the affected computers. (Refer to http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/deploy/dgbe_sec_ztsn.msp?mfr=true about establishing a Domain Trust.)

2.2 Local Users Authenticate as Themselves

In Windows XP and Windows Vista, there is another setting that you should modify. This is not necessary in Windows 2000 or earlier. Simple File Sharing is always turned on in Windows XP Home Edition-based computers. By default, the Simple File Sharing user interface is turned on in Windows XP Professional-based computers that are joined to a workgroup. Windows XP Professional-based computers that are joined to a domain use only the classic file sharing and security interface. Simple File Sharing forces every remote user to Authenticate as the Guest User Account. This will not enable you to establish proper security. There are two ways to turn this option off. Either way will work. I personally prefer the second method because there are more security options that Windows exposes to me.

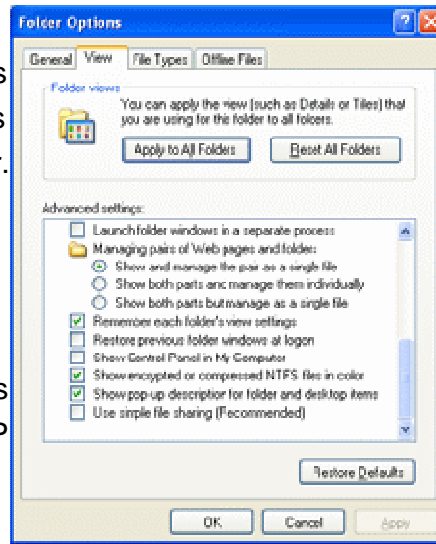


Image 2: Turn off "Simple File Sharing" to enable Windows to Authenticate User Accounts properly.

Method 1: Turning off Simple File Sharing

- a. Double-click "My Computer" on the desktop.
- b. On the Tools menu, click Folder Options.
- c. Click the View tab, and then clear the "Use Simple File Sharing (Recommended)" check box to turn off Simple File Sharing (refer to Image 2).

Method 2: Set Local Security Policies

- Click on the Windows Start button, and then select Control Panel, Administrative Tools, and Local Security Policy. If you can't see Administrative Tools in the Control Panel, simply select Classic View in the Control Panel. As an alternative to all of this, click on the Windows Start button; select the Run menu option, and type "secpol.msc".
- In the tree control, navigate to Security Settings, Local Policies, and finally select the Security Options folder (refer to Image 3).
- Find the "Network access: Sharing and security model for local accounts" option and set it to "Classic – local users authenticate as themselves".

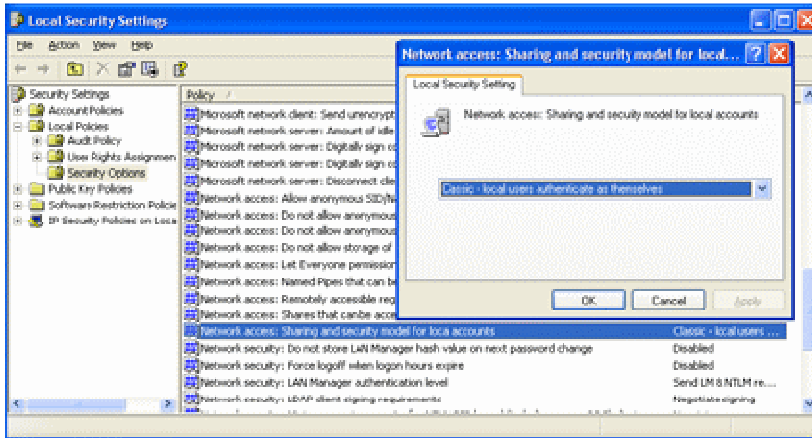


Image 3: Appropriate OPC security for requires Windows to enable local users to authenticate as themselves rather than as Guest.

3. Configure System-Wide DCOM settings

OPC specifications that precede OPC Unified Architecture (OPC UA) depend on Microsoft's DCOM for the data transportation. Consequently, you must configure DCOM settings properly. It is possible to configure the default system-wide DCOM settings, as well for a specific OPC server.

The system-wide changes affect all Windows applications that use DCOM, including OPC application. In addition, since OPC Client applications do not have their own DCOM settings, they are affected by changes to the default DCOM configuration. To make the necessary changes, follow the steps below:

a. Click on the Windows Start button, and select the Run menu option (refer to Image 4).

b. In the Run dialog box, type "DCOMCNFG" to initiate the DCOM configuration process, and click the OK button. The Component Services window will appear (refer to Image 5).

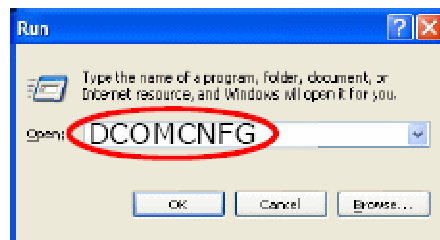


Image 4: Use DCOMCNFG to modify DCOM settings on the computer.

c. Once in the Component Services window (which is initiated by DCOMCNFG as above), navigate inside the Console Root folder to the Component Services folder, then to the Computers folder. Finally, you will see the My Computer tree control inside the Computers folder.

d. Right-click on My Computer. Note that this is not the "My Computer" icon on your desktop; rather it is the "My Computer" tree control in the Console

Services application.

e. Select the Properties option.

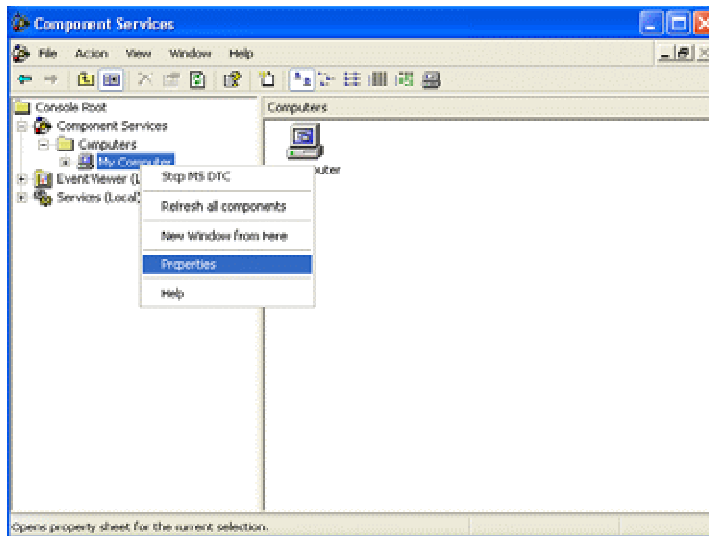


Image 5: Right-click on the My Computer tree control to access the computer's default DCOM settings

3.1 Default Properties

In the Default Properties tab, ensure that three specific options are set as follows (refer to Image 6):

- Check the “Enable Distributed COM on this computer” menu option. Note that you will have to reboot the computer if you make changes to this checkbox.
- Set the “Default Authentication Level” to Connect. It is possible to use other settings in the list, but the “Connect” option is the minimum level of security that you should consider.
- Set the “Default Impersonation Level” to Identify.Default Protocols

In the Default Protocols tab (refer to Image 7), set the DCOM protocols to “Connection- Oriented TCP/IP”. OPC communication only requires “Connection-Oriented TCP/IP”, so it is possible to delete the rest of DCOM protocols. However, if these protocols are indeed required for non-OPC applications, you can leave them there. The only consequence is that timeouts may take a little longer to reach.

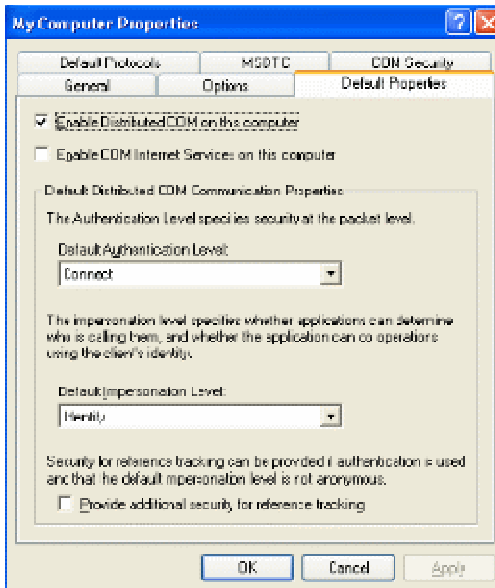


Image 6: The Default Properties tab enables users to turn DCOM on or off, as well as set the Authentication and Impersonation configuration.

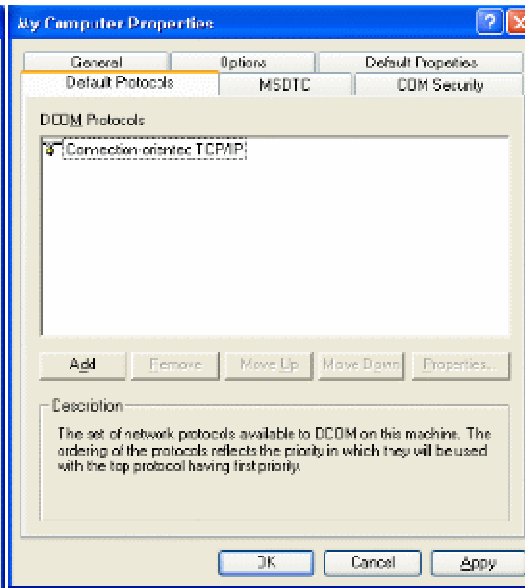


Image 7: In the Default Protocols tab, set the DCOM Protocols to "Connection-Oriented TCP/IP".

3.2 COM Security

Windows uses the COM Security tab (refer to Image 8) to set the system-wide Access Control List (ACL) for all objects. The ACLs are included for Launch/Activation (ability to start an application), and Access (ability to exchange data with an application). Note that on some systems, the "Edit Limits" buttons are not available.

To add the right permissions, follow the steps below:

- a. In the Access Permissions group, click the "Edit Default..." button (refer to Image 9). Add "Everyone" to the list of "Group or user names". Click the OK button.
- b. In the Access Permissions group, click the "Edit Limits..." button (refer to Image 9). Add "Anonymous Logon" (required for OPCenum) and "Everyone" to the list of "Group or user names". Click the OK button.

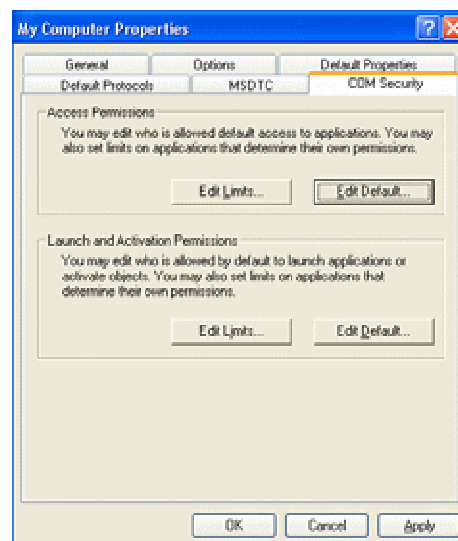


Image 8: Use the COM Security tab to set the default Access Control Lists (ACLs).

- c. In the Launch and Activation Permissions group, click the “Edit Default...” button (refer to Image 9). Add “Everyone” to the list of “Group or user names”. Click the OK button.
- d. In the Launch and Activation Permissions group, click the “Edit Limits...” button (refer to Image 9). Add “Everyone” to the list of “Group or user names”. Click the OK button.

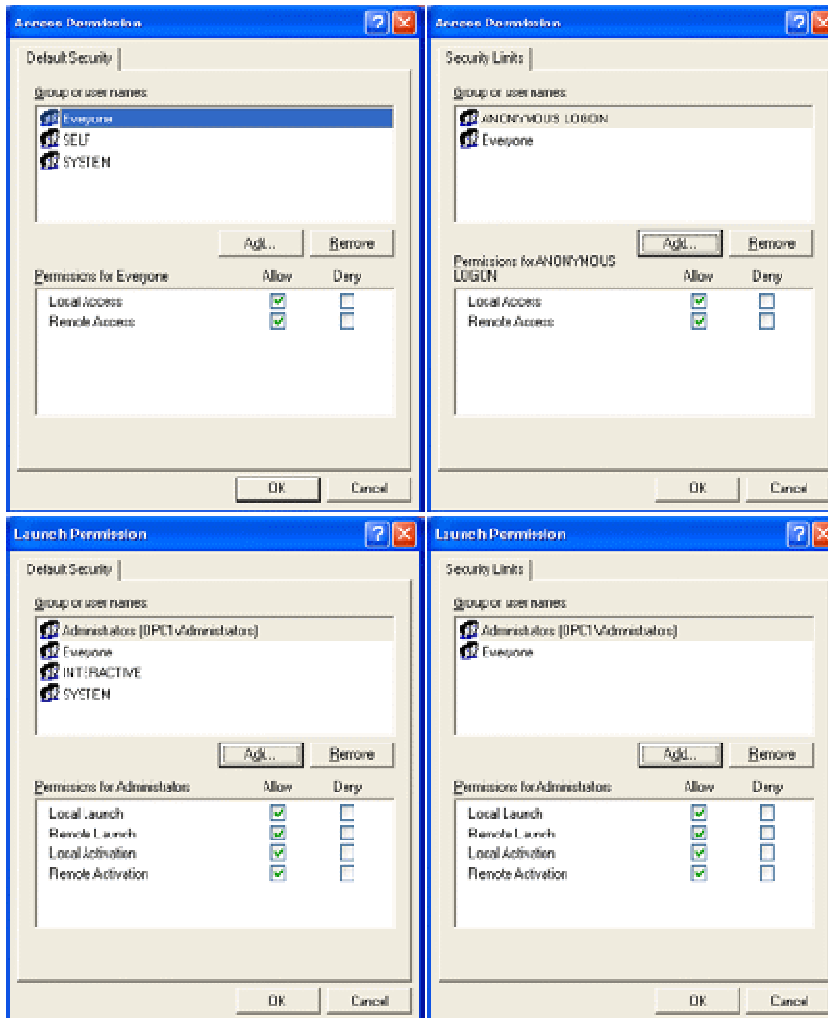


Image 9: Add Everyone and Anonymous Logon to the Launch and Access Permissions. Once communication is working properly, remember to return to this setup to ensure you comply with corporate security policies.

4. Configure Server Specific DCOM settings

Once the system-wide DCOM settings are properly configured, turn attention to the serverspecific DCOM settings. These settings will eventually be different

for every OPC Server. To change these settings, begin by:

- a. Click on the Windows Start button, and select the Run menu option (refer to Image 4).

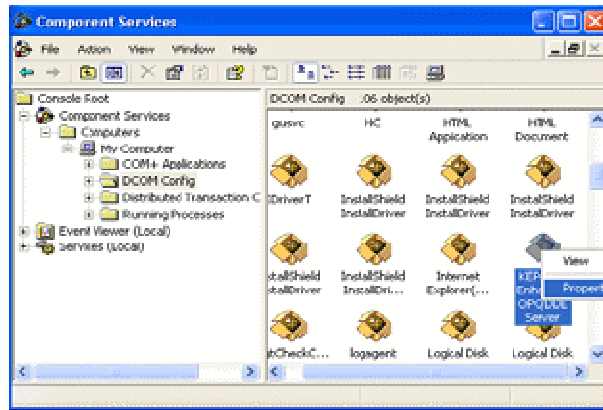


Image 10: Server-specific DCOM settings are located in the DCOM Config folder.

- b. In the Run dialog box, type "DCOMCNFG" to initiate the DCOM configuration process, and click the OK button. The Component Services window will appear (refer to Image 10).

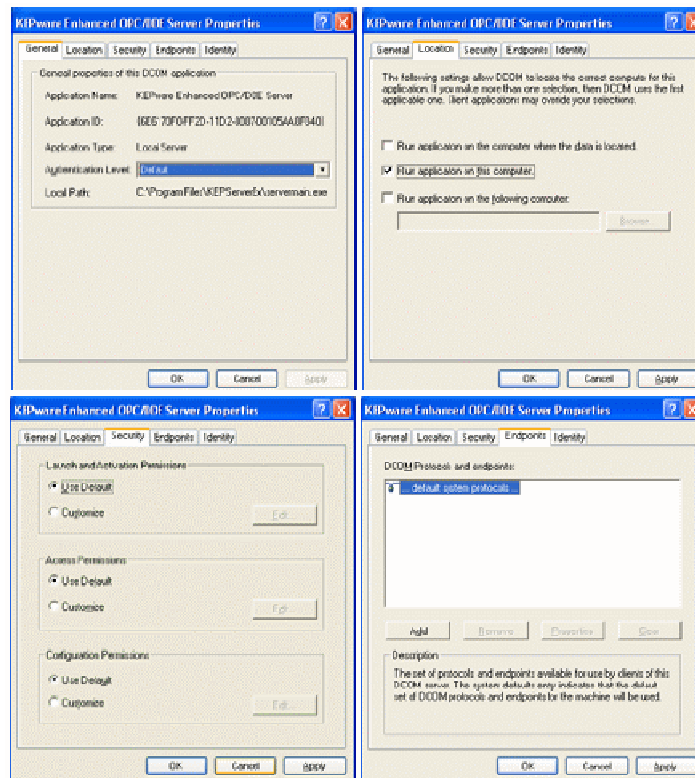


Image 11: The settings in the first four tabs (General, Location, Security, and Endpoints) should remain at their default settings as shown above.

- c. Once in the Component Services window (which is initiated by DCOMCNFG as above), navigate inside the Console Root folder to the Component Services folder, then to the Computers folder, expand My Computer, finally click on the DCOM Config folder.
- d. In the list of objects in the right window pane, find the OPC Server to configure and right-click on it. Select the Properties option.

In the OPC-Server specific settings, only the Identity tab needs to change from the default settings. The rest of the tabs (refer to Image 11) can refer to the default configuration that was set in section 3 (Configure System-Wide DCOM settings).

You must pay special attention to the Identity tab. The Identity tab will look like one of the two screen captions in Image 12 below. The 4 (four) Identity options are:

- **The interactive user:** The OPC Server will assume the identity of the Interactive User. This is the person who is currently logged on and using the computer on which the OPC Server resides. Note that someone must be logged on. If no one is logged on to the computer, the OPC Server will fail to launch. In addition, if someone is currently logged on, the OPC Server will shutdown as soon as the person logs off. Last, in the case of a reboot, the OPC Server will not launch until someone logs on. Consequently, this is typically a poor setting for OPC Servers. OPCTI does not recommend that you use this setting unless the OPC Server vendor specifies this setting explicitly.
- **The launching user:** The OPC Server will take the identity of the User Account that launched it. With this setting, the Operating System will attempt to initiate a new instance for every Launching User. There are three general problems with this setting. The first problem is that some OPC Servers will only allow a single instance to execute. Consequently, the second Launching User will be unable to make the connection because an instance of the OPC Server is already running on the computer. The second problem occurs when the OPC Server vendor allows more than one instance of the OPC Server to execute concurrently. In this case, the computer on which the OPC Server resides will have multiple copies of the OPC Server executing concurrently, which will consume a significant portion of the computer

resources and might have an adverse affect on the computer's performance. In addition, some system resources might be unavailable to any instances of the OPC Server that follow the first. For example, the first Launching User will be able to connect to a serial port, while every other Launching User will simply receive Bad Quality data. OPCTI does not recommend that you use this setting unless the OPC Server vendor specifies this setting explicitly. Last, the Launching User must have Administrative rights on the OPC Server computer. They can not be configured as a "Limited" user.

- **This user:** The OPC Server will take the identity of a specific User Account. This setting might be required when the OPC Server is tightly coupled with the underlying data source. In this case, the OPC Server must assume a specific Identity to exchange data with the data source. However, since the OPC Server uses a specific User Account, it is possible that the computer running the OPC Client does not recognize the OPC Server's User Account. In this case, all callbacks will fail and all OPC data Subscriptions (asynchronous data updates) will fail. If this is indeed the case, you will have to add the OPC Server account on the computer running the OPC Client application. Various DCS vendors require this setting for their OPC Server. OPCTI does not recommend that you use this setting unless the OPC Server vendor specifies this setting explicitly.
- **The system account (services only):** The OPC Server will take the identity of the Operating System (or System for short). This is typically the desired setting for the OPC Server as the System Account is recognized by all computers on the Workgroup or Domain. In addition, no one needs to be logged on the computer, so the OPC Server can execute in an unattended environment. OPCTI recommends configuring the Identity of the OPC Server with this setting, unless the OPC Server vendor specifies a different setting explicitly. Note that Windows disables this option if the OPC Server is not setup to execute as a Windows Service. If this is the case, simply configure the OPC Server to execute as a service before configuring this setting.

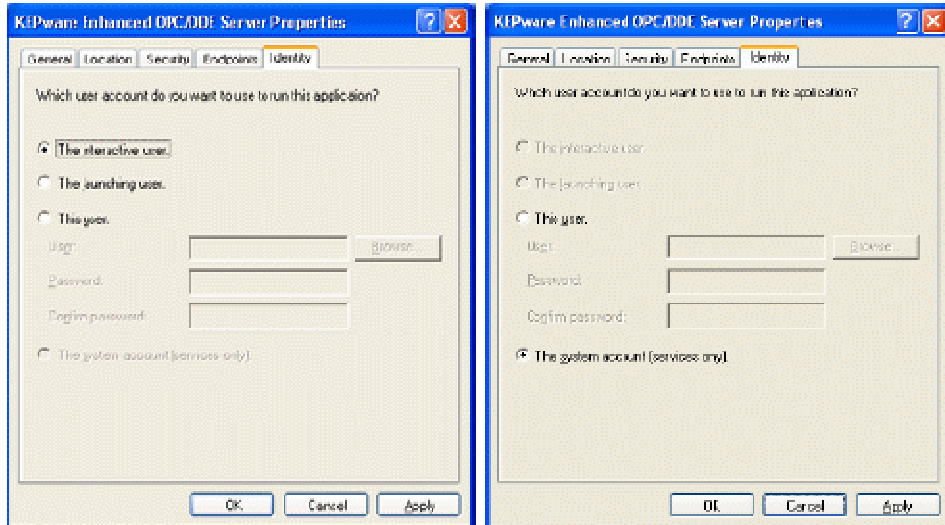


Image 12: Use the Identity Tab to set the OPC Server's identity. Typically, OPC Server Identity should be set to "The system account (services only)".

5. Restore Windows Security

Once you establish the OPC Client/Server communication, it is important to secure the computers again. This includes (but is not limited to):

a. Turn on the Windows Firewall again. This will block all unauthorized network traffic. You will also need to provide exceptions on two main levels:

- Application level: specify which applications are able to respond to unsolicited requests.
- Port-and-protocol level: specify that the firewall should allow or deny traffic on a specific port for either TCP or UDP traffic.

b. Modify the Access Control Lists (ACLs) to allow and deny the required User Accounts. This can be accomplished either through the system-wide settings of DCOMCNFG, or in the server-specific settings. Remember that OPCEnum requires the "Anonymous Logon" access. You may wish to remove this access. The consequence of this action will simply be that OPC Users will be unable to browse for OPC Servers on the specific computer where Anonymous Logon access is not available. However, users will indeed be able to properly connect to and exchange data with the OPC Server.

We encourage you to complete your DCOM setup with this step. Integrators

frequently establish OPC communication and don't spend the necessary time to secure the computers again. This can lead to catastrophic results if network security is compromised due to a virus, worm, malicious intent, or simply unauthorized "experimentation" by well-meaning coworkers. Specific settings are discussed in a separate whitepaper.

6. Conclusion

OPC is powerful industrial communication standard. However, OPC relies on having DCOM work properly. Luckily, DCOM problems can usually be overcome with relatively simple configuration changes as documented in this whitepaper. To get a deeper understanding of OPC, DCOM, and the diagnosis of all common problems OPCTI highly recommends that you take time to get formal OPC training. This will enable you to structure your OPC knowledge to help you reduce your short and long-term project costs. OPCTI also encourages you to provide us with feedback. Let us know about new problems and solutions that you found. We will pass these on to the rest of the OPC community, to help everyone get connected.

