

OPC COMMUNICATIONS

Authors:

Stephen Mueller Senior Project Engineer TÜV Functional Safety Engineer ID TÜV FSEng 0376/06 HIMA Australia Pty Ltd

Dean McNair Managing Director TÜV Functional Safety Engineer ID TÜV FSEng 357/06 HIMA Australia Pty Ltd

ABSTRACT

OPC (OLE for process control) is the modern standard of choice for establishing seamless open communications between the plant and enterprise levels in today's industrial process applications. OPC technology is implemented where end users choose to maintain an open, non-proprietary communication philosophy within their businesses thereby ensuring freedom of choice, the power to negotiate commercially and the ability to choose best-in-class technology.

Since the first release of OPC standards in 1996, this emerging technological development has come of age and interfacing over ethernet via OPC technology today presents a cost effective, reliable and straightforward alternative to aging serial communications protocols or restrictive proprietary communications networks.

INTELLIGENT INTEGRATION

Most process organisations today are well aware of the commercial benefits of making shop floor process data available to the enterprise level. This data was historically locked up in proprietary networks and only available to operations staff and engineers working in those areas.

Today, equipment data is made accessible and available through OPC servers allowing businesses to select and intelligently integrate the most appropriate, fit for purpose technology for their applications.

Shop floor data is integrated at the enterprise level and allows managers to analyse data and make decisions to improve productivity and profitability. This level of integration requires forward planning, and structure and specifications have to be defined. Just as there will be planning and specifications drawn up for those who wish to use the data,



planning is also required at the technology implementation level to ensure seamless integration.

DCOM

OPC Classic technology uses Microsoft's Windows based DCOM (Distributed Component Object Model) technology that enables software components distributed across several networked computers to communicate with each other.

While the OPC Classic based specifications have proven to be highly successful there is a new specification in development called OPC UA (Unified Architecture) that keeps abreast of new technology developments and evolving customer requirements.

One of the drivers of OPC UA is to provide a specification that will allow the implementation of OPC technology on non-Microsoft based platforms from embedded to enterprise systems. In addition to this, OPC UA will also combine OPC DA, A&E and HDA functionality into a single solution as well as the ability to operate as a single client/server in one application.

A major benefit with OPC UA will be in the communication protocol and security model. There will be two choices for the communications layer, TCP or SOAP (XML). The advantage of SOAP is that it uses port 80, which is the same as standard web sites. This means that all firewalls can handle this kind of traffic, which in turn means that there is no major IT involvement required. In Classic OPC, DCOM is used as the security broker, session controller and message router. The OPC UA communications stack essentially removes the need for DCOM.

Until the OPC UA specifications are officially released, OPC Classic continues to provide an outstanding open communications solution. There is however a misunderstood perception that there are issues surrounding OPC configuration and connectivity. As an organisation who has delivered many hundreds of OPC integrated projects, HIMA can state that this simply isn't the case.

The "issues" arise when configuring OPC where people don't realise that without having DCOM configured absolutely correctly the OPC communications will either not work, or appear to work but not be effective. In these cases, OPC is blamed of course rather than DCOM.

Through HIMA's wealth of applied project experience, we can confirm the actual simplicity of setting up DCOM correctly within a protected plant environment. It is even easier to set it up in a single domain, or within two trusted domains.

There are a set of five simple steps as noted by the OPC Training Institute that should be followed to ensure DCOM works correctly. These steps are detailed in the section that follows. It is recommended that the security be increased once DCOM is operating correctly.



OPC AND DCOM: FIVE THINGS YOU NEED TO KNOW

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 unauthorised 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 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 step 5 "Restore Windows Security". To turn off the Windows Firewall, follow the steps below:

a. Click on the Windows Start button, select the Control Panel and 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 recognise User Accounts, it is necessary to ensure that User Accounts are recognised on both the OPC Client and Server computers. This includes all the User Accounts that will require OPC access.

Image 1

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. It is important to 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.

Run	<u>? ×</u>
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	control userpasswords2
	OK Cancel Browse

Image 2



ser Aco	counts
Users	Advanced
Pas: You cha	swords and .NET Passports can manage the passwords you have stored on this computer, or nge your default Passport with the .NET Passport Wizard.
Adv	Local Users and Groups can be used to perform advanced user management tasks.
	 For added security, you can require users to press Chr1+Alt-Delete before logging on. This guarantees that the authentic Windows logon prompt appears, protecting the system from programs that minic a logon to retrieve password information. Require users to press Ctrl+Alt+Delete
	OK Cancel Apply

• 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 synchronised 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/w indows2000serv/reskit/deploy/dgbe_sec_ztsn.ms px?mfr=true about establishing a Domain Trust.)

Image 3

🏇 Local Users and Groups		
Eile Action View Help		
Coal Users and Groups (Local)	Name Administrators Backup Operators Network Configuration Power Users Remote Desktop Users Replicator Users HelpServicesGroup	Description Administrators have complete and U Backup Operators can override secu Guests have the same access as me Members in this group can have som Power Users possess most administr Members in this group are granted t Supports file replication in a domain Users are prevented from making ac Group for the Help and Support Center

Image 4

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. The second method exposes more security options.



Method t. Turning off Simple File Sharing

- Double click "My Computer" on the desktop.
- On the Tools menu, click Folder Options (refer to image 5).

💈 My Computer						_	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	Tools Help						1
🕒 Back 🔻 🅘 👻 🏂 🔎 Se	Map <u>N</u> etwork Drive	ମ । ⊞•					
Address 😼 My Computer	Synchronize						Go
Name 🔺	Folder Options		Total Size	Free Space	Comments		
Local Disk (C:)			48.8 GB	8.00 GB			

Image 5

• Click the View tab, and then clear the "Use Simple File Sharing (Recommended)" check box to turn off Simple File Sharing (**refer to image 6**).

Folder Options
General View File Types Offline Files
Folder views You can apply the view (such as Details or Tiles) that you are using for this folder to all folders. Apply to All Folders <u>R</u> eset All Folders
Advanced settings:
 Launch folder windows in a separate process Managing pairs of Web pages and folders Show and manage the pair as a single file Show both parts and manage them individually Show both parts and manage them individually Show both parts but manage as a single file Remember each folder's view settings Restore previous folder windows at logon Show Control Panel in My Computer Show control Panel in My Computer Show por-up description for folder and desktop items Use simple file sharing (Recommended)
Restore <u>D</u> efaults
OK Cancel Apply

Image 6

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 7).



Storal secondy seconds		Accessive accesses sharing and secondly mean for local accounts (M. 21)	1
Ble Attorn Yew Belp		Local Security Setting Explain This Setting	÷
Control Series Series	Teles Biological Sector S	Renords access: Damp and accurated for tood accounts	

Image 7

correctly. 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 applications. 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: • Find the "Network access: Sharing and security model for local accounts" option and set it to "Classic – local users authenticate as themselves".

3. CONFIGURE SYSTEM-WIDE DCOM SETTINGS

OPC specifications that precede OPC Unified Architecture (OPC UA) depend on Microsoft's DCOM for the data transportation and therefore the DCOM settings must be configured

Run	<u>?×</u>
	いて Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	dcomcnfg
	OK Cancel <u>B</u> rowse

a. Click on the Windows Start button, and select the Run menu option (refer to Image 8).

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 9).

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.

3.1 Default Properties

In the Default Properties tab, ensure that three specific options are set as follows (refer to Image 10):

a. Check the "Enable Distributed COM on this computer" menu option. Note that you will have to

Image 9

Image 8



My Computer Propert	ties	?	×
Default Protocols	S MSDTC	COM Security	l
General	Options	Default Properties	
🔽 Enable Distribute	d COM on this compute		
Enable COM Inte	rnet Services on this co	omputer	
– Default Distributed	COM Communication P	Properties	
The Authentication	Level specifies securiț	ty at the packet level.	
Default A <u>u</u> thentic	ation Level:		
Connect		•	
The impersonation who is calling them using the client's id	level specifies whether , and whether the appli entity.	r applications can determine ication can do operations	
Default Imperson	ation Level:		
Identify		•	
Security for referen and that the defaul <u>P</u> rovide addit	ce tracking can be pro t impersonation level is ional security for referen	wided if authentication is used not anonymous. nce tracking	
	ОК	Cancel Apply	

Image 10

3.2 COM Security

Windows uses the COM Security tab (refer to Image 12) 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

Computer Properti	es	?
General	Options	Default Properties
Default Protocols	MSDTC	COM Security
Access Permissions You may edit who also set limits on a	is allowed default access	to applications. You may their own permissions
	Edit Limits	Edit Default
- Launch and Activati	on Permissions	
You may edit who activate objects. \ determine their ow	is allowed by default to lar You may also set limits on a In permissions.	unch applications or applications that
You may edit who activate objects. Y determine their ow	is allowed by default to la You may also set limits on a In permissions.	unch applications or applications that Edit <u>D</u> efault
You may edit who activate objects. \ determine their ow	is allowed by default to lar /ou may also set limits on a /n permissions.	unch applications or applications that Edit <u>D</u> efault
You may edit who activate objects. determine their ow	is allowed by default to lar Cournay also set limits on a n permissions.	unch applications or applications that <u>Edit D</u> efault
You may edit who activate objects. Y determine their ow	is allowed by default to lar four may also set limits on (n permissions. Edit Limits	unch applications or applications that



reboot the computer if you make changes to this checkbox.

b. 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.

c. Set the "Default Impersonation Level" to Identify. Default Protocols In the Default Protocols tab (refer to Image 11), 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.

My Computer Properties		? ×
General	Options	Default Properties
Default Protocols	MSDTC	COM Security
DCO <u>M</u> Protocols		
Connection-oriented TC	P/IP	
Add Berriove	Move Up Move	e D <u>o</u> wn
The set of network protoc ordering of the protocols with the top protocol havi	cols available to DCOM reflects the priority in w ng first priority.	on this machine. The nich they will be used,
	ОК	Cancel <u>Apply</u>

Image 11

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 13**). 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 13). Add "Anonymous Logon" (required for OPCEnum) and "Everyone" to the list of "Group or user names". Click the OK button.

c. In the Launch and Activation Permissions group, click the "Edit Default..." button (refer to Image 13). Add "Everyone" to the list of "Group or user names". Click the OK button.

Access Permission	? ×	Access Permission	<u>?×</u>	Launch Permission	Launch Permission	<u>? ×</u>
Default Security		Security Limits	~	Default Security	Security Limits	
Group or user names:)	Broup of Unit Parties"		Stoop or user names:	Stoup or user name: Administrators IATLAS\Administrators1 E Veryone	
Permissions for Everyone Local Access Remote Access	Add <u>Bemove</u> Allow Deny 2 2 2 1	Permissions for ANDNYMOUS LOGIN Local Access Remote Access	AddBemove	Add Eenove Permitisions for Everyone Alow Deny Local Launch Image: Color and Color	Add. Permissions for Everyone Allow Local Laurch Remote Laurch Local Activation	V Deny U Deny U Deny U Deny
	OK Cancel		OK Cancel	OK Cancel	OK	. Cancel

Image 13

4. Configure Server Specific DCOM settings

Once the system-wide DCOM settings are properly configured, turn attention to the

Component Services			_0>
Elle Action Yew Window Help	_		_ @ ×
· → 🗈 🖬 × 🕾 🖻 🔮 🖻	• * * • • • • • •		
Console Root	DEOM Config 273 object(s)		
Component Services	Name	Application TD	
E Computers	A EpictCore	(4657%) c.b165.4051.a045.6a501072aarf)	
B- B My Computer	C EPIOCOPE	(405/2010/010/49/1404/005/19/2000/) (72012EE2.EED0.402E.0200.406.04040EDEE)	
	Chotcator Deplate dear Tools	(15913E) 5-3E00-10E3-RE03-1R0R101RE03E) (0E97D39E EE07 4/E7 P249 B79E9E3E9E49)	
Distributed Transaction (EPidEditori II	(05745D61_D66C_db38_B076_F36F50BBE357)	
Running Processes	DED DECISION	(889E0017.84E8.4r6r.8314.C3C6C6303E06)	
Event Viewer () ocal)	D EDiatModel	(2a212909.azb1.da2b.b251.d159.d21.d079)	
Services (Local)	DEDiot Deciderer	(db247020.5ac0.41 xE.0a4 x.b.722EE4:d9EF)	
Gr	Chorden Del tel	(01557/0201800-1185-9618-070307(0003) (01555209.0557.4051.9555.750950049020)	
	Event Object Channe	(D0565000.9DE4.11D1.4281.00C04EC40447)	
	Event Object Change	(880786/D_CD56_4F63_68EE_CBE0355E80E4)	
	Even coject change 2	(F7Dr 29D7-1577-45D2-RE99-RED61842/E99)	
	FyprestliewerDI	(55523467-4054-4064-8880-0070305(19695)	
	FlachBroker	(D43048/FE/B8E9.4835/BE40.0/58522670/2)	
	GenReferencing	(05AE4ABE-3ACE-41AC-943B-28226BR0EB10)	
	GeoReft his	{AC7E0675-04E8-4318-8D81-0EC340345484}	
	GoodeFarth	(46A9989C-4ACR-4FF9-AF70-002816CFC314)	
	CPSMapEdR	(9375C706-2947-4574-9964-184120F3CC04)	
	OH-	(EC7D9E01-3E9E-11D3-93C0-00C04E72D4E7)	
	Health Key and Certificate Management Service	(46298694,0F/3,47F3,04h3,65650,65h364)	
	HIMA Alarm/Event OPC Server	(53688a18-2009-4461-8102-8a63E4EC77DD)	
	August the operation	(44042000 (0000 4402 0000 00000000000)	
(HIMA OPC-Server	(A1245725-E64D-11d2-8A28-006094511A9D)	
	HP Port Resolver	(55E3E296,4775,4AE9,80AA,52393842EE3C)	
	HP Status Server Pyoperties	(3B05E114-4087-4557-8952-AAE023709EB0)	
	Children trusin	(11PED0E7 0EP0 4P06 0E02 6270EE2(E270)	
	HTM Application	(404FE486-8ED4-41+3-945E-8350D4(FC491)	
	(SicrdCl	(53046386-0125-41A2-8881-0CC16C688E96)	
	DriverT	(E58088EA-D080-421E-A1EE-3CE5898051D6)	
	3 IdSystem	(87D3F975-1964-4F39-8CEE-2FB4A5B6889D)	
	Mage Document	(02B01C80-E03D-101A-B294-00DD010F28F9)	
	A InstallShield InstalDriver	(018A3896-2FE0-48E0-8965-83ED78E1884E)	
	A InstallShield InstalDriver	(18B3D82F-9803-4d29-8232-1F2F14E52A2E)	
	Tostal/Shield Instal/Driver	(C2B96968-8E30-4BA4-A3E9-E40D09D1EA7E)	

server specific 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 8).

b. In the Run dialog box, type "DCOMCNFG" to initiate the DCOM configuration process, and click

Image 14

the OK button. The Component Services window will appear (refer to Image 14).

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 15)** can refer to the default configuration that was set in section 3 (Configure System-Wide DCOM settings).

HIMA OPC-Server Properties	HIMA OPC-Server Properties	HIMA OPC-Server Properties	HIMA OPC-Server Properties
General Location Security Endpoints Identity	General Location Security Endpoints Identity	General Location Security Endpoints Identity	General Location Security Endpoints Identity
General properties of this DCOM application	The following settings allow DCDM to locate the correct computer for this	Launch and Activation Permissions	DCOM Protocols and endpoints:
Application Name: HIMA OPC-Server	application. If you make more than one selection, then DCDM uses the first applicable one. Client applications may overide your selections.		an default system protocols
Application ID: (A1245725-F64D-11d2-8A28-006094511A9D)		C Customize	
Application Type: Local Server	Run application on the computer where the data is located.		
Authentication Level Detaut	Run application on this computer.	Access Permissions	
Local Path: C:\PROGRA~1\HIMA\OPCSER~1.X\bin\hima	Run application on the following computer:	Use Default	
	Browse	C Customize Edit	
			Add Remove Properties Dear
		Configuration Permissions	Description
		 Use Default 	The set of protocols and endpoints available for use by clients of this DCOM server. The system defaults entry indicates that the default
		C Customize Edit	set of DCOM protocols and endpoints for the machine will be used.
OK Cancel Apply	OK Cancel Apply	OK Cancel Apply	OK Cancel Apply

Image 15

You must pay special attention to the Identity tab. The Identity tab will look like the two screen caption in **Image 16** 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

HIMA OPC-Server Properties	×			
General Location Security Endpoints Identity				
Which user account do you want to use to run this application?				
The interactive user.				
C The launching user.				
C This <u>u</u> ser.				
User: Browse				
Password:				
Confirm password:				
C The system account (services only).				
OK Cancel Apply				

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.

Image 16

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 cannot 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.

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 unauthorised 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 unless it is has modified DCOM properties. 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 unauthorised "experimentation" by well-meaning co-workers.

CONCLUSION

OPC is a robust modern communication option for end users looking for an open and reliable communications network free of the technical and commercial restrictions of closed proprietary networks.

OPC Classic devices require the correct set up of Microsoft's DCOM and access control lists and the failure to consider this in the past has lead to incorrect assumptions about the reliability and ease of use of OPC technology.

This paper has demonstrated how simple it is to configure DCOM correctly and ensure seamless and easy to use OPC communications are available on each and every application.

REFERENCES

Kondor, R. 2007, OPC and DCOM: 5 Things You Need to Know, OPC Training Institute.