SINUMERIK OPC ACCESS

To be able to access the Siemens Sinumerik 840D built in OPC Servers OPC.SINUMERIK.Machineswitch and OPC.SinumerikEvents (Alarm Server) from a remote PC that is member of a workgroup or a domain some configuration tasks are necessary.

Note: If you want to avoid wasting your time do NOT use any of the solutions that can be found on the internet about configuring DCOM or OPC security. None of them works in this case.

The Sinumerik OPC servers heavily rely on DCOM. Successful communication between client and server requires proper authentication, nothing more.

CONTROLLER SETUP

At the controller there's almost nothing to do.

Start up the controller in service mode without HMI.

It is recommended that you turn off simple sharing.
Click Start->Run type in eplorer.exe click on Tools->Folder Options. In tab View uncheck 'Use simple file sharing (Recommended)'. Click OK.

Just in case you have the firewall enabled proceed as follows: The most simple way to avoid communication problems is to turn off the firewall. Click on Start->Settings->Control Panel->Windows Firewall. Click on Off (not recommended) followed by OK. You're done.

If you want to keep the firewall switched on you have to adjust some settings.

1. Add Port 135 to exceptions.
2. Check 'File and Printer Sharing'.
3. Add program 'Simatic OPC Server' (..\mmc2\opc\dataaccess\SOPC_MachineSwitch.exe)*
4. Add program 'OPCSinumerikAlarm.exe' (..\opc\alarmevent\OPCSinumerikAlarm.exe)*
5. Click OK.

* Depending on the setup of your controller these files may be stored at a different location.

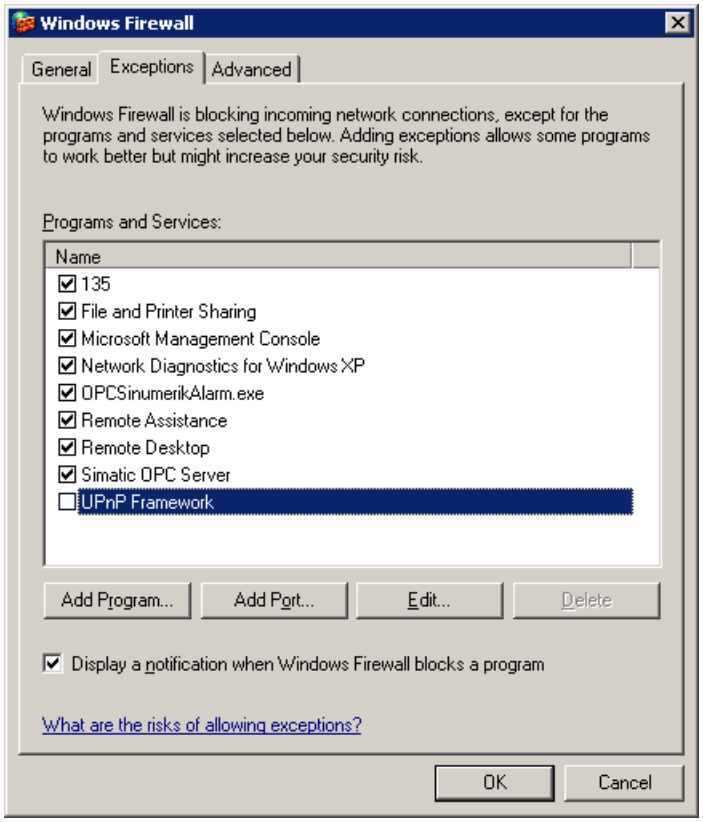

FIG 1: Firewall settings on Sinumerik 840D

Restart the controller in normal mode to enable HMI again.

PC SETUP

DCOM GENERAL

Either click on Start->Programs->Administrative Tools->Component Services or Start->Run and type in dcomcnfg and click OK.
Expand Component Services->Computers->My Computer
Right click My Computer select Properties
Open tab Default Properties
Make sure that Enable Distributed COM on this computer is checked.

NETWORK ACCESS TO CONTROLLER

For successful communication between PC and controller it is necessary that the querying computer is able to access the controller and its Operating System via the network with proper credentials.

Typically the account you're using on your PC does not have the rights to access the controller. To resolve this you need to setup an additional account:

1. Right click 'This PC' on your desktop and select Manage.
2. Expand Local Users and Groups
3. Right click on 'Users' and select 'New User'
4. In 'User name' enter 'auduser' (without quotes)
5. In 'Password' enter the password for user 'auduser' used at the controller, (typically 'sunrise')
6. Confirm the password, uncheck 'User must change password at next logon', click button Create followed by Close.
7. Right click on username 'auduser', select Properties.
8. In tab 'Member Of' click button Add and type in Administrators, click button Check Names followed by OK.
9. Close the Properties dialog by clicking on OK.

Test access to your controller:

1. Create a shortcut to explorer.exe (%SYSTEMROOT%\explorer.exe) on your desktop.
2. Next, right click the shortcut with the shift key pressed and select 'Run as different user'.
3. Type in the name of your PC followed by a backslash and auduser (e.g. MYPC\auduser) followed by its password.
4. In the address field input two backslash characters followed by the IP Address or DNS Hostname of your controller e.g. \\192.168.1.100 and press enter. You should get access to your controller.

OPC TEST

To test access to your controller's OPC servers extract TestDCOM.exe and Config.ini to a folder of your choice at the server.

CONFIGURE INI FILE

With a text editor such as notepad edit Config.ini and change the IP Address right to ipaddr = to the IP Address of your controller. Save and close Config.ini.

Right click on TestDCOM with the shift key pressed, select 'Run as different user' and enter your PC's name followed by a backslash and auduser (e.g. MYPC\auduser) followed by its password.

A dialog window opens.

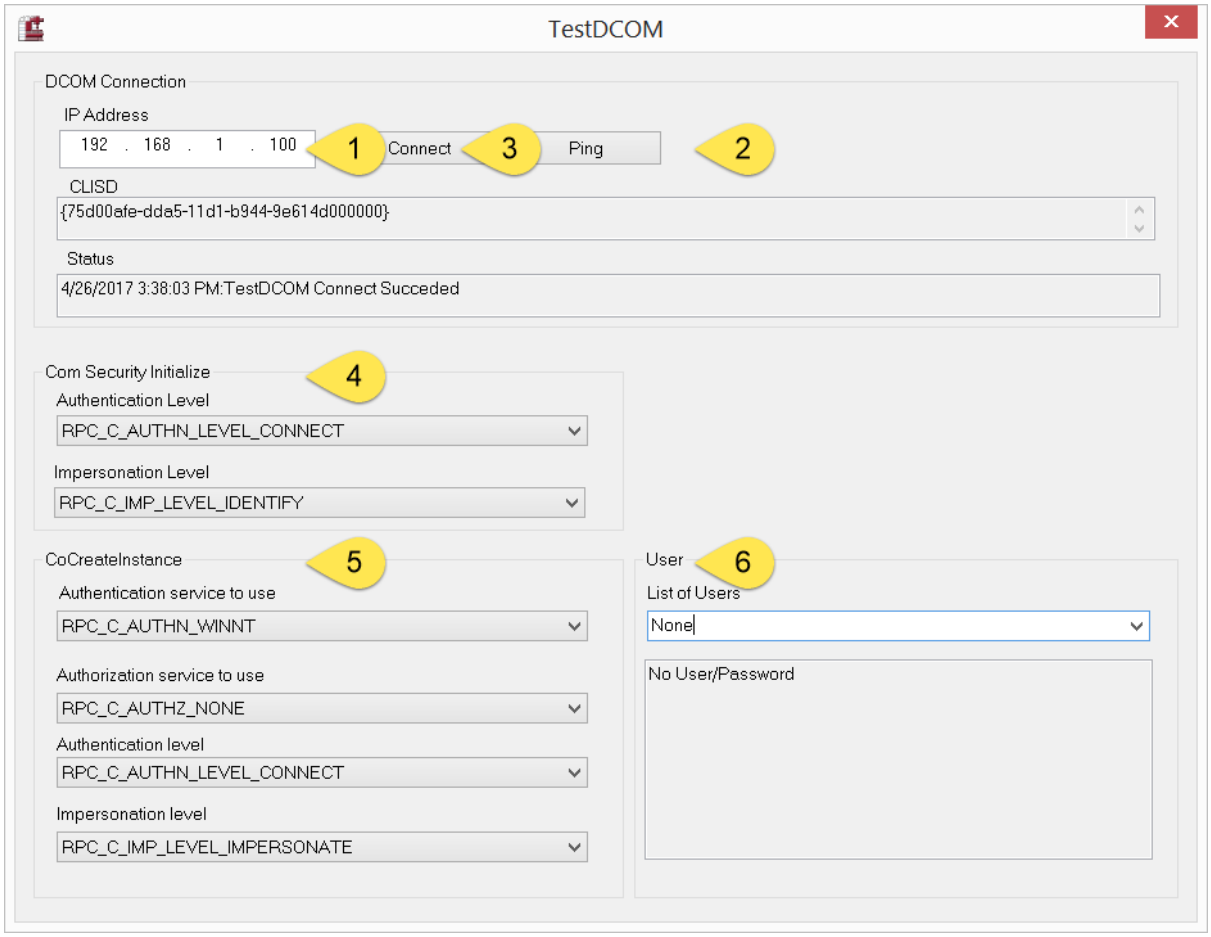

FIG 2: TestDCOM dialog window

RUN TEST

On top you see the IP Address (1) of your controller, click on button Ping (2) right to it.

Under Status you should see something like '… Reply from 192.168.1.100: bytes=14 time=<1ms TTL=128'.

Next click on button Connect (3). If it works you should see '…DCOM Connect Succeeded'.

All fields in sections 'Com Security Initialize' (4) and 'CoCreateInstance' (5) are preset with values that should work. So usually no changes have to be made here. Of course you can run tests with different parameters.

DCOM DEFAULT PARAMETERS

Section Com Security Initialize

Authentication level default: RPC_C_AUTHN_LEVEL_CONNECT
Impersonation level default: RPC_C_IMP_LEVEL_IDENTIFY

Section CoCreateInstance

Authentication service to use default: RPC_C_AUTHN_WINNT (RPC_C_AUTHN_GSS_NEGOTIATE and RPC_C_AUTHN_DEFAULT work also)
Authorization service to use default: RPC_C_AUTHZ_NONE
Authentication level default: RPC_C_AUTHN_LEVEL_CONNECT (only RPC_C_AUTHN_LEVEL_NONE, does not work!)

Impersonation level default: RPC_C_IMP_LEVEL_IMPERSONATE

DCOM USERS

In section User (6) you can optionally set specific domain, and usernames and passwords for access to your controller in the form of DOMAINNAME,USERNAME,PASSWORD separated by commas. If your controller is member of a workgroup use a dot instead of domain name.