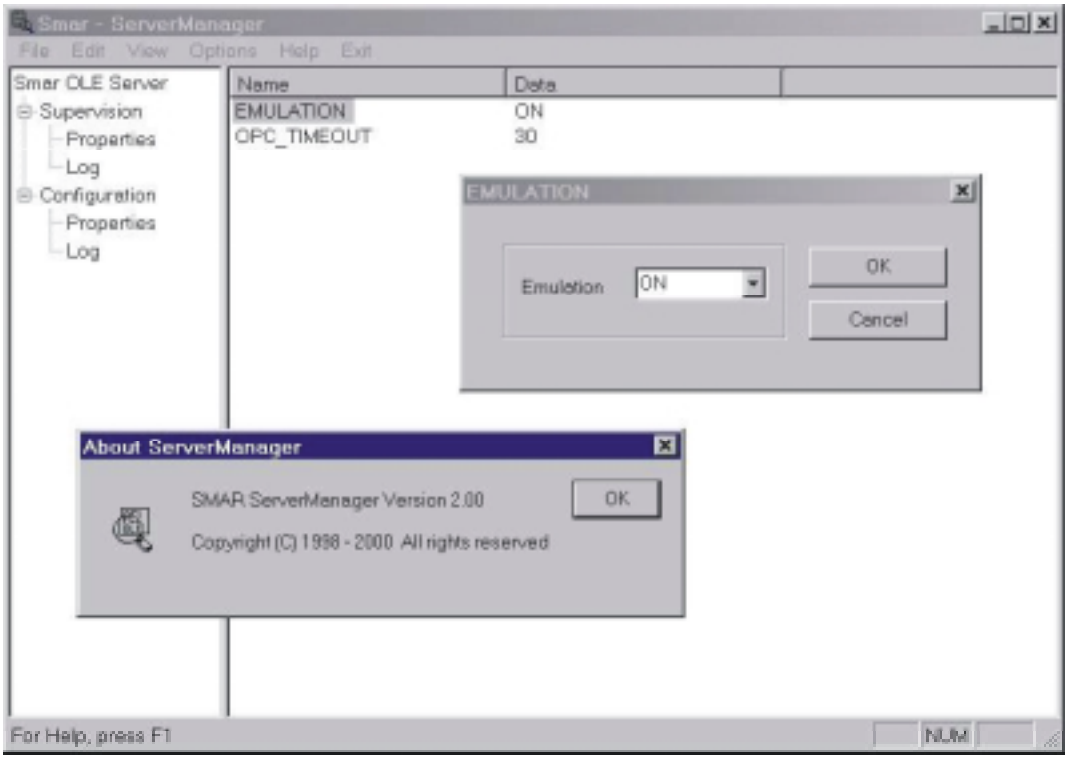
Smar Ole Server - Smar Ole Server

smar FIRST IN FIELDBUS

USER'S MANUAL

Smar Ole Server



JULY / 02

Smar Ole Server

VERSION 2.0

FOUNDATION

PCI OPCME

www.smar.com

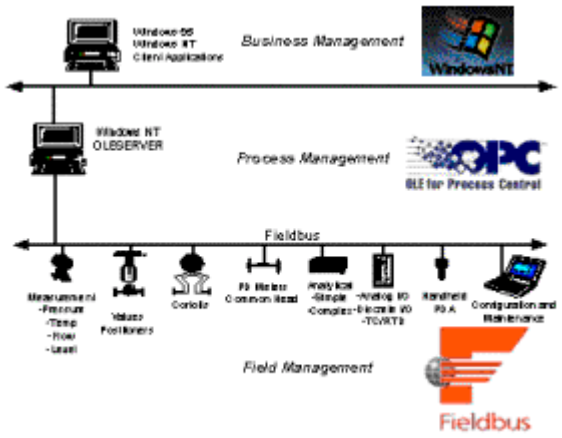
Specifications and information are subject to change without notice.
Up-to-date address information is available on our website.

web: www.smar.com/contactus.asp

Index

Introduction

Using all the benefits of OLE (Object linked and embedded) and OPC (OLE for Process Control), you can write Fieldbus client applications for Client / Server based systems at a higher level of programming, without having to deal with the details of specific Fieldbus protocol. OLESERVER for Smar Fieldbus Interfaces provides a consistent set of functions for Supervision and Configuration. This consistency minimizes code changes you need to make if the underlying protocol changes.



Typical application using OLE Server.

Highlights

Client/Server Architecture via OLE
Distributed computing to provide a single system image to users and applications and to permit use of services in a networked environment regardless of location, machine architecture, or implementation environment.

Win32-based platform
The Server was designed for 32 bits systems. The server must be running in a Windows NT machine while a Client can also be running in a Windows 95 machine.

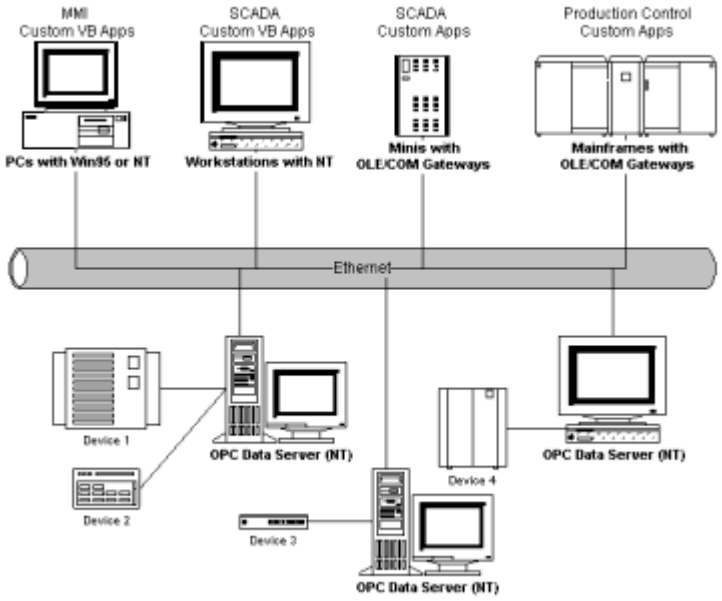
OPC compliant
Providing the server with an OPC interface allows any supervision client to access devices in a standard way. OLE for Process Control (OPC™) draws a line between hardware providers and software developers.

OLE for Fieldbus Configuration
Going further on OPC benefits Smar has developed a set of functions for plant configuration via OLE. This provides a way to both Supervision and Configuration clients work at the same time, remotely or not.

OPC

OLE for Process Control (OPC™) is a method to allow business and supervision applications access to plant floor data in a consistent manner. With wide industry acceptance and open architecture, OPC provides many benefits like *OPC Server* where Hardware manufacturers only have to make one set of software components for customers to utilize in their applications. Another benefit is OPC Client where Software developers won't have to rewrite drivers because of feature changes or additions in a new hardware release. Customers will have more choices with which to develop World Class

integrated manufacturing systems. With OPC, system integration in a heterogeneous computing environment will become simple. Leveraging OLE/COM the environment shown below becomes possible.



System integration in a heterogeneous computing environment

Overview

OPC is based on Microsoft's OLE/COM technology.

An OPC Client can connect to OPC Servers provided by one or more vendors. Different vendors provide OPC Servers. The code written by the vendor determines the devices and data to which each server has access, the way in which data items are named and the details about how the server physically accesses that data.

Within each server the client can define one or more OPC Groups. The OPC Groups provide a way for clients to organize the data in which they are interested. For example, the group might represent items in a particular operator display or report. Data can be read and written. Exception based connections can also be created between the client and the items in the group and can be enabled and disabled as needed. The 'freshness' (time resolution) of the data in the group can be specified. Within each Group the client can define one or more OPC Items.

The OPC Items represent connections to data sources within the server. Associated with each item is a value, a Quality Mask and a Time Stamp. The value is in the form of a VARIANT and the Quality Mask is similar to that specified by Fieldbus. Note that the items are not the data sources - they are just connections to them. For example the tags in a DCS system exist regardless of whether an OPC client is currently accessing them.

Local vs. Remote Servers

It is expected that OPC Server vendors will generally take one of two approaches to networking. They can indicate that the client should always connect to a local server which makes use of an existing proprietary network scheme. In this case the 'node' of the data might be specified as part of the OPC ItemDefinition. It is expected that this approach will commonly be used by vendors who are adding OPC capability to an existing distributed product. They can indicate the client should connect to the desired server on the target node and thus make use of DCOM™ to provide networking. For this reason all of the RPC_E_ error codes should also be considered as possible returns.

Minimum DCOM Settings

1. Please certify that your hardware is installed according its specific user manual.
2. Log with Administrative rights on the local machine.
3. Certify that you have TCP/IP and RPC protocols is installed in your computer.
4. Proceed with the installation using System302 setup.

Note: All sets concerning to PCI OLE Server will only be successfully done if the account being used under setup has administrative rights.

Client and Server running in the same machine

The default setup use to be enough to get local access and extra configuration is necessary only if you intend to have security points.

Anyway, just to make sure your computer will work properly, check ahead the minimum DCOM settings necessary for that.

1. Run the DCOMCNFG program:
   1.1. Press the **Start** button on NT Taskbar and choose the option Run.
   1.2. Fill the edit field with *dcomcnfg* and press the button OK.

2. Select the Default Properties folder and set the following fields:
   2.1. ☑ Enable Distributed COM on this computer.
   2.2. Default Authentication Level: **Connect**.
   2.3. Default Impersonation Level: **Identify**.

3. Select the Default Security folder:
   3.1. Press Edit Default button under Default Launch Permissions.
      3.1.1. Make sure Administrators, INTERACTIVE and SYSTEM are added with Allow Access.

4. Select the Applications folder and double click on Smar OPC & Conf Server for ????

5. Select the Location folder and check the Run application on this computer: option.

6. Select now the Security folder:
   6.1. Check the option Use default access permissions.
   6.2. Check the option Use default launch permissions.
   6.3. Select the Identity folder and check The interactive user.

Client and Server running in different machines

You must perform two different configurations to be able to connect through DCOM: the client-side one and the server-side one. In the client-side you may have an end-user program like Syscon and some components of Smar OLE Server software (CONFPrx.dll, IProxy.dll and OPCProxy.dll files, and the required information to NT registry). In the server-side you must have the whole Smar OLE Server software in order to establish communication between software client(s) and Hardware plugged in the computer.

Creating Client/Server connection with security

Step 1. Configuring your Network Hosts
You may have two possibilities when configuring your machines to be involved in DCOM communication. You can use only Workstations (standalone) or Workstations in a Domain with a NT Server. Note that any NT Server may be or not a server-side machine for the PCI OLE service.

The advantages of one over another may depend on your local network architecture. Both processes require help of your network administrator. To choose which one to use remember that Domain based architecture has a single security database and thus is the simplest way.

Option 1 - Network Based on standalone Workstations

1. Run the User Manager program on each machine and create a new group to your Fieldbus based system (suggestion: call it *FFGroup*).

2. Remains in the User Manager program and create on each machine a new user to your Fieldbus based system (suggestion: call it *FFUser*).

3. Still in the User Manager program, insert every user (including the one created before) which must have access to the Fieldbus services (configuration, supervision, etc…) in the group created in item 1.

Option 2 - Network Based on a NT Domain

1. Run the User Manager program on the domain server machine and create a new group to your Fieldbus based system (suggestion: call it *FFGroup*).

2. Remains in the User Manager program and create a new user to your Fieldbus based system (suggestion: call it *FFUser*).

3. Still in the User Manager program, insert every user (including the one created before) which must have access to the Fieldbus services (configuration, supervision, etc…) in the group created in item 1.

4. Be sure that every workstation is a member of NT domain (Folder Identification in Network from Control Panel).

Step 2. Client-Side

1. Run the DCOMCNFG program:
   1.1. Press the **Start** button on NT Taskbar and choose the option Run.
   1.2. Fill the edit field with *dcomcnfg* and press the button OK.

2. Select the Default Properties folder and set the following fields:
   2.1. ☑ Enable Distributed COM on this computer.
   2.2. Default Authentication Level: **Connect**.
   2.3. Default Impersonation Level: **Identify**.

3. Select the Default Security folder and press the Edit button.
   3.1. If you don't have *Everyone* with Allow Access, you must at least have *FFGroup* and *SYSTEM* with Allow Access in the Name list.

4. Select the Applications folder and double click on Smar OPC & Conf Server for ????.

5. Select the Location folder and check Run application on this computer option.

6. If your client application does not have the remote connection option check Run application on the following computer: option, filling down with the computer name or IP that will be the server-side for this client-side.

7. Select now the Security folder:
   7.1. Check the option Use custom access permissions and press the Edit button.
      7.1.1. You must have only the group *FFGroup* with Allow Access as Type of Access.

Step 3. Server-Side

1. Run the DCOMCNFG program:
   1.1. Press the **Start** button on NT Taskbar and choose the option Run.
   1.2. Fill the edit field with *dcomcnfg* and press the button OK.

2. Select the Default Properties folder and set the following fields:
   2.1. ☑ Enable Distributed COM on this computer.
   2.2. Default Authentication Level: **Connect**.
   2.3. Default Impersonation Level: **Identify**.

3. Select the Applications folder and double click on Smar OPC & Conf Server for ????.

4. Select the Location folder and check the Run application on this computer: option.

5. Select now the Security folder:
   5.1. Check the option Use custom access permissions and press the Edit button.
      5.1.1. You must have only the groups *SYSTEM* and *FFGroup* with Allow Access as Type of Access.

   5.2. Check the option Use custom launch permissions and press the Edit button.
      5.2.1. You must have only the group *FFGroup* with Allow Launch as Type of Launch.

   5.3. Select the Identity folder and check This user: option, filling down with the username *FFUser* in the User: field.

   5.4. Using the NT User Manager, select Policies/User Rights…
      5.4.1. Click on the ☑ Show Advanced User Rights box.
      5.4.2. Select Log on as a batch job on the Right: field.
      5.4.3. Add *FFUser* account.

Creating Client/Server connection without security

Step 1. Configuring your Users

1. Run the User Manager program on each machine and create the users involved on the process. Example: Machine1, Machine2, etc…

Step 2. Client-Side

1. Run the DCOMCNFG program:
   1.1. Press the **Start** button on NT Taskbar and choose the option Run.
   1.2. Fill the edit field with *dcomcnfg* and press the button OK.

2. Select the Default Properties folder and set the following fields:
   2.1. ☑ Enable Distributed COM on this computer.
   2.2. Default Authentication Level: **Connect**.
   2.3. Default Impersonation Level: **Identify**.

3. Select the Default Security folder and press the Edit button for Default Access Permissions.
   3.1. Add *Interactive*, *Everyone* and *SYSTEM* with Allow Access.

4. Select now the Security folder:
   4.1.1. Check the option Use default access permissions

Step 3. Server-Side

1. Run the DCOMCNFG program:
   1.1. Press the **Start** button on NT Taskbar and choose the option Run.
   1.2. Fill the edit field with *dcomcnfg* and press the button OK.

2. Select the Default Properties folder and set the following fields:
   2.1. ☑ Enable Distributed COM on this computer.
   2.2. Default Authentication Level: **Connect**.
   2.3. Default Impersonation Level: **Identify**.

3. Select the Default Security folder and press the Edit button for Default Access Permissions.
   3.1. Add *Interactive*, *Everyone* and *SYSTEM* with Allow Access.

4. Select the Default Security folder and press the Edit button for Default Launch Permissions.
   4.1. Add *Interactive*, *Everyone* and *SYSTEM* with Allow Launch.

5. Select the Applications folder and double click on Smar OPC & Conf Server for ????.

6. Select the Location folder and check Run application on this computer option.

7. Select now the Security folder:
   7.1.1. Check the option Use default access permissions and Use default launch permissions

PCI OLE Server details

PCI OLE Server for Windows NT® is server-side software used to carry out connection between client-side software and PCI cards plugged in the local computer. The access may be done locally or through a network.

- Please certify that all PCI cards were correctly installed with the same I/O port and IRQ number, avoiding conflict with other local devices.
- After installation and after restarting machine, make sure your PCI-NT device driver is started and working properly, using the NT *Event Viewer*.
- File: PCISvr.exe
- ProgID: Smar.IServer.0
- Name: Smar OPC & Conf Server for PCI Card.

DFI OLE Server details

DFI OLE Server for Windows NT® is server-side software used to carry out connection between client-side software and DFI302 plugged in the Network.

- Please certify that DFI302 were correctly installed under Network.
- File: DfiSvr.exe
- ProgID: Smar.DFIOLEServer.0
- Name: Smar OPC & Conf Server for DFI302

HSE OLE Server details

HSE OLE Server for Windows NT® is server-side software used to carry out connection between client-side software (e.g. OPC Client) and any HSE Device plugged in the Network.

HSE Device Definition: Any Fieldbus Foundation device type connected directly to HSE Media. All HSE devices contain an FDA Agent, an HSE SMK, and an HSE NMA VFD. Examples include Linking Devices, I/O Gateways, and HSE Field Devices. DFI302 is a Linking Device.

- Please certify that DFI302 or any HSE Device was correctly installed under Network.
- File: HseSvr.exe
- ProgID: Smar.HSEOLEServer.0
- Name: Smar OPC & Conf Server for HSE

SmarOleServer.ini configuration

SmarOleServer.ini file, located under OleServers folder provides some SECTION and KEYS which are permited enable and disable logs, set timeouts, configure network details, etc. Let's to describe these sections:

- In Log and LogForOPC Sections, it is possible to enable some log features and see the results in Events.log and EventOPC.log files respectively. Both files have its (.log#) file used for swap.

```
[Log]
GENERAL=0
DEBUG=0
MEMORY=0
INIT=1
DRIVER=0
TRANSFER=0
TRANSACTION=0
CONF=0
OPC=0
OPCDEBUG=0
IDSHELL=0
;=0        (Default) Log disabled
;=1        Enable log and see the results in Events.log and Events.log#

[LogForOPC]
GENERAL=0
;=0        (Default) Log disabled
;=1        Enable log and see the results in EventOPC.log and EventOPC.log#
```

- In NIC Adapter Section, in the case of more than one NIC adapter are installed in the machine, choose the desired NIC adapter to be connected with the local DFI OLE Server.

```
[NIC Adapter]
; More than one NIC (Network Interface Card) are installed in the local machine
; Set the NIC which is connected to the network where is the desired DFI302
; In the NIC key (next line), set the IP and remove ';' to activate the key
;NIC=xxx.yyy.www.zz
```

- In DFI Time Settings Section, tune the better startup time which the DFI OLE Server takes to look for DFI302 spread to the network. The default time use to be enough if not using routers.

```
[DFI Time Settings]
; Define a delay which the server will wait till complete DFI connection
;=3   (Default) 3 seconds before concluding server connection with DFIs
NETWORK_STARTUP=3
```

- In Remote DFI Section, when using Routers in the Network topology, insert the other IPs located out of the local subnet. Do not forget to tune in DFI Time Settings Section, the better time necessary to DFI OLE Server.

```
[Remote DFI]
; Specify on this section IPs to be reached in remote networks.
; Remember to set Default Gateway under DFI settings using FBTools.
; Format: xxx.yyy.zzz.sss=1 enable IP polling.
;       xxx.yyy.zzz.sss=0 disable IP polling.
;192.168.164.100=0
```

- In Supervision Section, it is possible to switch the Server (PCI and DFI) to emulation. This mode is only used for debug purposes.

```
[Supervision]
; This section is used for Supervision purposes.
; OPC_TIMEOUT is the maximum time which the Server waits for data refresh.
; EMULATION turns the Emulation on.
; EMULATION_RATE specify the rate for refreshing of emulation.
OPC_TIMEOUT=30
;=30         (Default) 30 seconds

EMULATION=OFF
;=ON         Activate Emulation Mode for Supervision
;=OFF        (Default) Normal Mode

EMULATION_RATE=1000
;=1000       (Default) 1000 seconds, valid when EMULATION=ON
```

- In Configuration Section, it is possible to configure timeouts for each Syscon Configuration procedure. DO NOT CHANGE ANY VALUE IN THIS SECTION WITHOUT SMAR R&D RECOMMENDATION.

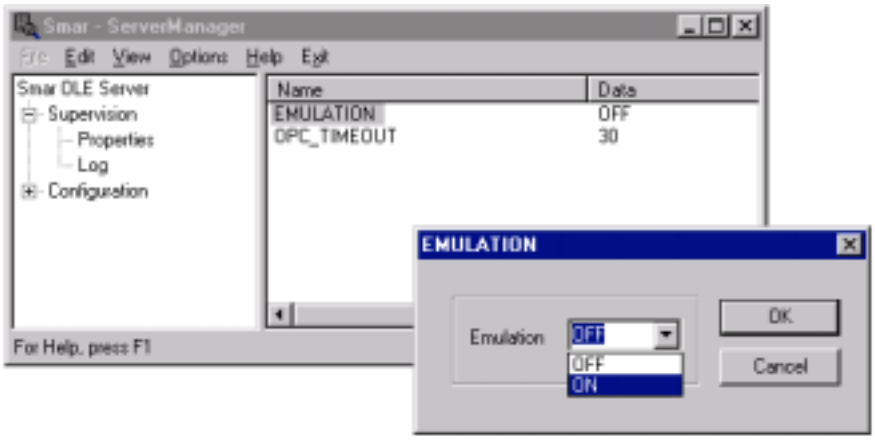
```
[Configuration]
;Default Timeout 10 seconds
Timeout.Default=30
Timeout.MULTILINKTOPOLOGYREQ=60
…
```

Smar ServerManager Application

Smar ServerManager Application had been designed to handle all the configurable features available in Smar OLE Servers like that described in SmarOleServer.ini configuration section.

Many of them are available now and many others are being developed.

- A good example for that is change the Server to Emulation mode using ServerManager application instead of using SmarOleServer.ini configuration file.



- Another feature implemented by ServerManager is load the servers at startup when configured and located in Windows Startup. Just go to Options, click the Servers desired to load at startup and move the ServerManager shortcut to Windows Startup Folder.