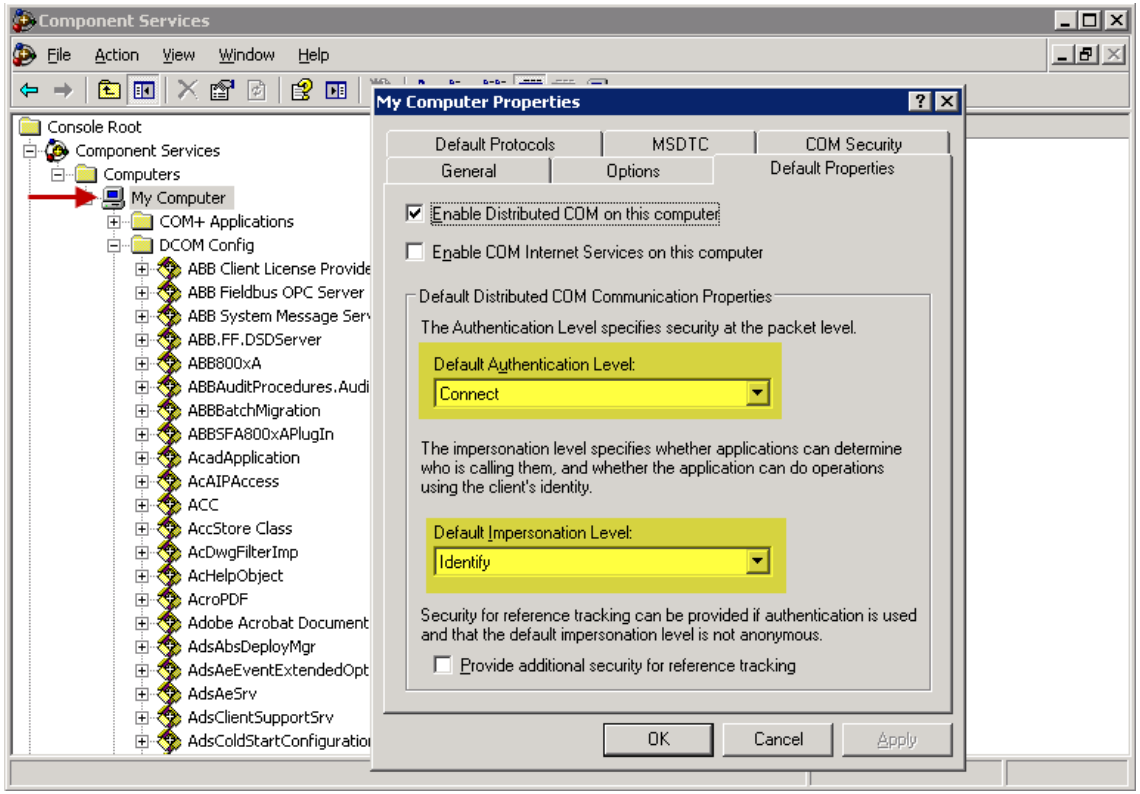
E143 – OPC Data Access
Third Party OPC DA Connection via DCOM

- The Configuration User's Guide (3BDS011222) is correct, but…
  - May be very complex to fully understand
  - Does not put system hardening in focus

- It is easy to make mistakes!
  - Mix up ***local*** vs ***domain*** vs ***800xA*** user accounts
    - Two separate accounts are often required
    1. Connect account (to enable DCOM calls between two computers)
    2. 800xA User Account (to enable entry to 800xA)
  - Firewall settings
  - Bi-directional DCOM settings is required to enable asynch. calls
    1. Server computer must allow client to login and launch OPC server
    2. Client computer must allow OPC server to call back to OPC client

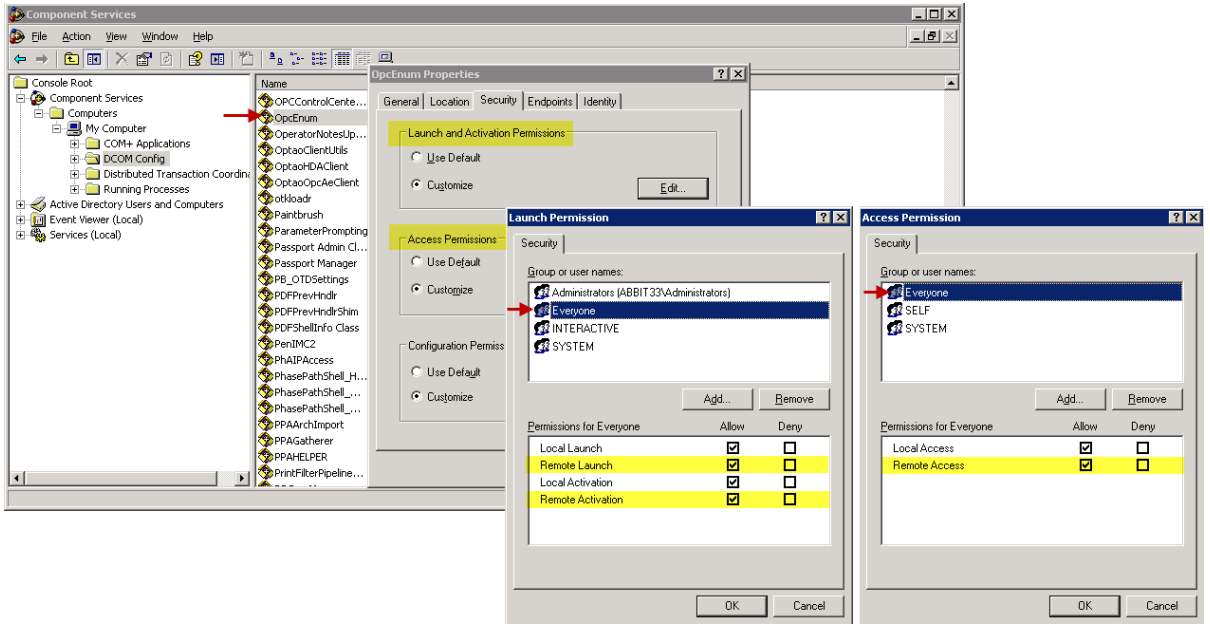
E143 – OPC Data Access
Third Party OPC DA Connection via DCOM

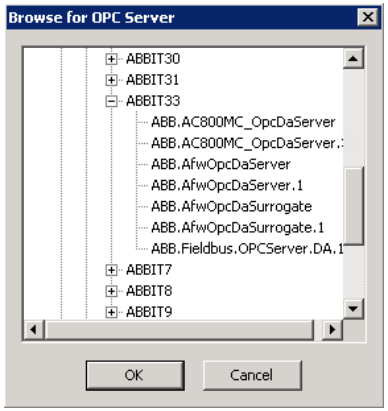
- Required settings in both server and client computer



E143 – OPC Data Access
Third Party OPC DA Connection via DCOM

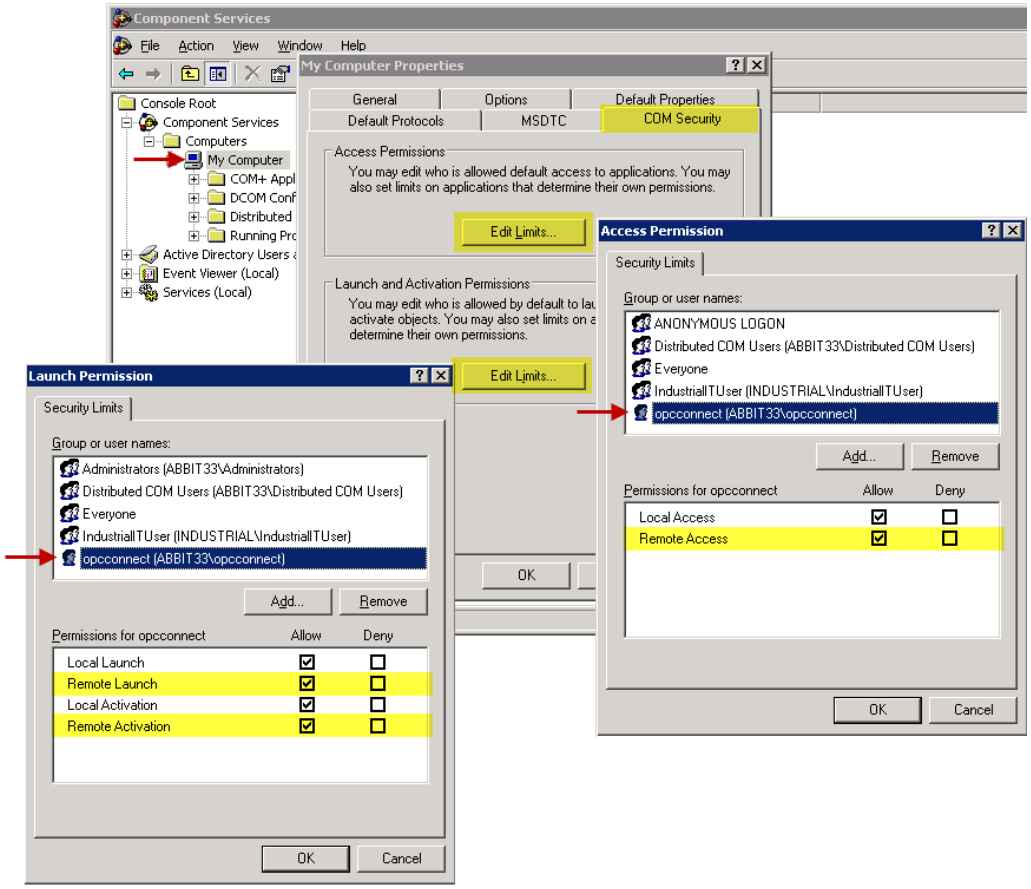
- Browsing for remote OPC servers require OPCEnum.exe in server
- OPCEnum.exe require DCOM Remote Access + Launch + Activation
- Defining a dedicated connect account is more secure than **Everyone**





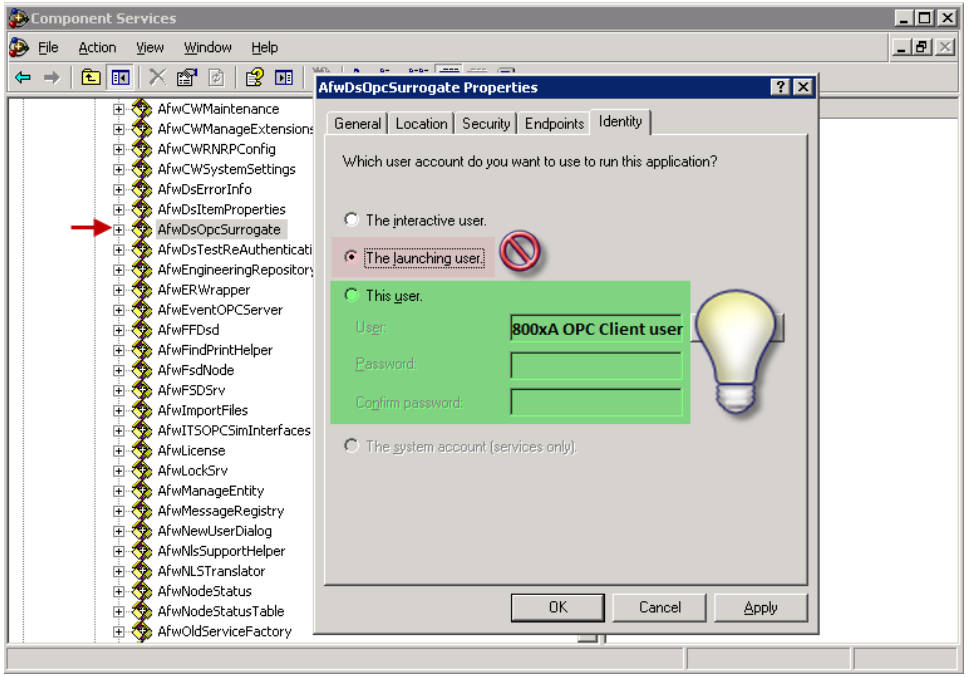
E143 – OPC Data Access
Third Party OPC DA Connection via DCOM

- The connect account must be granted access with DCOMCNFG.EXE



E143 – OPC Data Access
Third Party OPC DA Connection via DCOM

- Default DCOM settings on AfwDsOpcSurrogate.1 does no longer work from 5.0 SP2 RevE and 5.1 RevB due to system hardening
- A dedicated (preferably non-admin) 800xA user is required as launching identity for the AfwDsOpcSurrogate.1 server



E143 – OPC Data Access
Third Party OPC DA client connection via DCOM

Client

Domain A

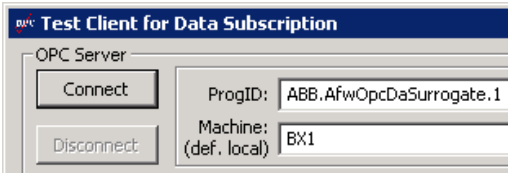
Domain account:
OPC Connect Account A_D\opcconnect
Member of Domain Users

Computer A1

Local account:
OPC Transfer Account $A1_L$\opctransfer

OPC DA Client

(Launched from the A_D\opcconnect account)
DCOM permission for Access:
Remote Access allow $A1_L$\opctransfer



The account's passwords must match:
$A1_L$\opctransfer = B_D\opctransfer
A_D\opcconnect = $BX1_L$\opcconnect

Server

Domain B

Domain account:
800xA OPC Transfer Account B_D\opctransfer
Member of Domain Users and IndustrialITUser

800xA System X

System 800xA account:
800xA OPC Transfer Account B_D\opctransfer
Member of 800xA Everyone (to read) and possibly more (to write)

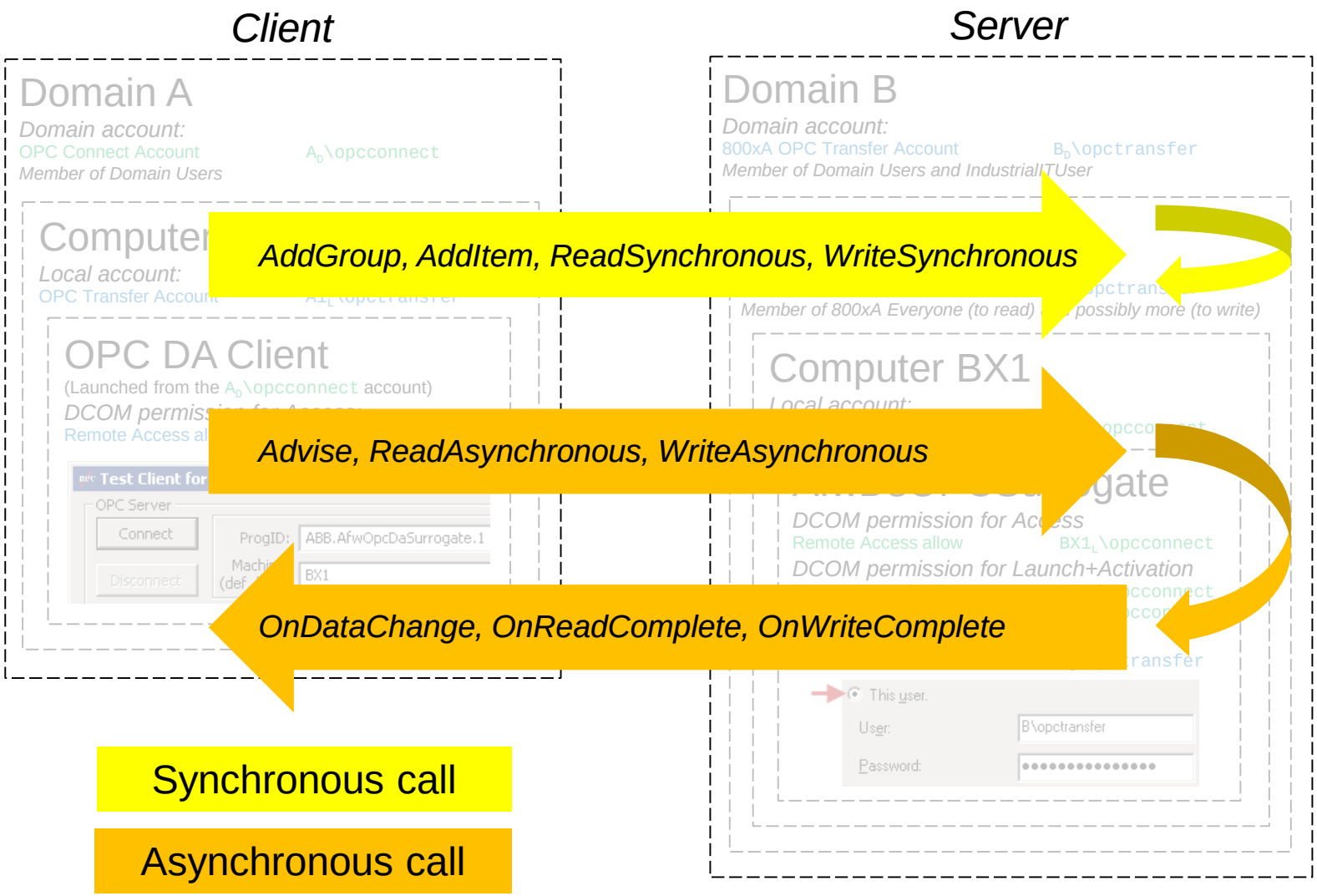
Computer BX1

Local account:
OPC Connect Account $BX1_L$\opcconnect

AfwDsOPCSurrogate

DCOM permission for Access
Remote Access allow $BX1_L$\opcconnect
DCOM permission for Launch+Activation
Remote Launch allow $BX1_L$\opcconnect
Remote Activation allow $BX1_L$\opcconnect
DCOM Identity
This user B_D\opctransfer

E143 – OPC Data Access
Third Party OPC DA Connection via DCOM



E143 – Asynchronous OPC Data Access
Client and server on <u>different</u> domain or workgroup

OPC Client *(some 3rd party)*		***OPC Server*** *(AfwDsOPCSurrogate.exe)*	
Account A	The account used to launch the OPC client	Account C	The account used to run the OPC server
Account B	The account matching the user used by the OPC server	Account D	The account matching the user used by the OPC client

1. Client (running as A) attempts to perform remote launch of the server via DCOM

Account X will match even if workgroup and domain name are different:
WORKGROUP Y\USER X = DOMAIN Z\USER X

Account D must have the following DCOM permission on AfwDsOPCSurrogate.exe:
- Remote Access
- Remote Launch
- Remote Activation

2. If A's name + password matches D, DCOM will launch the AfwDsOPCSurrogate.exe
   (The AfwDsOPCSurrogate <u>must</u> have DCOM Identity set to *This user* = C. Account C must also be a known System 800xA user and have appropriate object access)

3. Client (A) adds groups and items

4. Server (running as C) is sending data to the client

5. If C matches B, DCOM allow delivery of data to client.

Account B must have the following DCOM permission on 3rd party server's xxx.exe:
- Remote Access