### Firewall and DCOM Settings on PC and PCU Required to Operate MCIS Products

#### Contents:

1.	General DCOM settings on the controller (PCU) and master computer	
2.	Settings for MCIS DNC Cell/Plant/IFC	5
3.	Settings for MCIS TPM Cell/Plant/IFC	
4.	Settings for MCIS TDI Cell/Plant/IFC	
5.	Settings for MCIS MDA Cell/Plant/IFC	
6.	Settings for ADDM Client/Agent	
7.	Settings for MCIS RPC SINUMERIK	

# 1. General DCOM settings on the controller (PCU) and master computer

The general settings made on the controller with Win XP SP2 and a master computer with Win XP SP 2 are identical.

#### Limitations:

This description is valid as from MCIS version numbers V2.0. Further supplementary conditions may apply (please refer to Prodis Updates under http://support.automation.siemens.com resp. the Installation / Upgrade Instructions supplied with the relevant software products).

DCOM settings are not required for MCIS RPC, MCIS TDI and MCIS TPM software. Regarding the MCIS MDA software, the user "auduser" must be replaced by the user "PDA".

(The screenshots have been created with the German Windows XP  $\rightarrow$  for English screens see controller)

Please ensure that DCOM has been activated: Start the DCOM configuration via: start... execute... "dcomcnfg"





Navigate to: Component Services  $\rightarrow$  Computer  $\rightarrow$  Workstation: Right mouse button  $\rightarrow$  Call up "Properties"



In this screen, "Activate DCOM ..." must be checkmarked.

Default Protoc	ols MSDTC	COM Security
General	Options	Default Properties
<ul> <li>Enable Distribu</li> <li>Enable COM Ir</li> </ul>	ted COM on this computer Iternet Services on this con	iputer
Default Distribute	d CUM Communication Pro	perties
The Authenticati	on Level specifies security	at the packet level.
Default Auther	itication Level:	
Default Auther Connect The impersonatio	ntication Level:	pplications can determine
Default Auther Connect The impersonation who is calling the using the client's Default Impers	ntication Level: In level specifies whether a Im, and whether the application identity.	pplications can determine ation can do operations
Default Auther Connect The impersonatic who is calling the using the client's Default Impers Identify	ntication Level: In level specifies whether a Im, and whether the application identity.	pplications can determine ation can do operations

Confirm screen with OK.

Subject to change without prior notice.



Set DCOM Limits (this description is based on the assumption that the DCOM connection is authentified via a local user "auduser" located on master computer and controller who has the same password).

### Set up DCOM limits on master computer and controller (release auduser and anonymous for DCOM):

(Screens have been created using the German Windows XP  $\rightarrow$  English screens accordingly)

For this, change to the COM security tab in Workstation - Properties. In the column "Access Permission", press "Edit Limits..." and enter auduser with full rights:

Component Services	My Computer Properties	? ×	Access Permission	? 🗙
<ul> <li>File Action View Will</li> <li>File Action View Will</li> <li>Console Root</li> <li>Component Services</li> <li>Computers</li> <li>My Computer</li> <li>COM+ Appli</li> <li>DCOM COM+ Appli</li> <li>DCOM COM+ Appli</li> <li>DCOM COM+ Appli</li> <li>DCOM COM+ Appli</li> <li>COM+ Appli</li> <li>DCOM COM+ A</li></ul>	General       Options       Default Properties         Default Protocols       MSDTC       COM Security         Access Permissions       You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.       Edit Limits       Edit Default         Launch and Activation Permissions       You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.       Edit Limits       Edit Default	Ч	Security Limits Group or user names: ANONYMOUS-ANMELDUNG Suduser (MCIS_SERVER\auduser) Jeder Add Remo Permissions for auduser Allow Deny Local Access Remote Access	ve
j <b>&lt;</b> j	DK Cancel App	oly	ОКС	ancel

Confirm with OK and configure anonymous user:



Component Services	My Computer Propertie	25	? 🗙	Access Permission		? 🛛
File Action View Wir      Console Root      Console Root      Component Services      Computers      Computers      COM+ Appli      DCOM Confi      Distributed      Distributed      Component Viewer (Local)      Event Viewer (Local)	General Default Protocols Access Permissions You may edit who is a also set limits on appli	Options MSDTC allowed default access cations that determine Edit Limits	Default Properties         COM Security         to applications. You may their own permissions.         Edit Default	Security Limits Group or user names: ANONYMOUS-ANMELDUN auduser (MCIS_SERVER\au Jeder	<u>R</u> emove	
⊡ 🏠 Services (Local)	activate objects a activate objects of determine their own p	nowed by derault to la may also set limits on ermissions. Edit Limits	Edit Default	Permissions for ANDNYMOUS-ANMELDUNG Local Access Remote Access		
<		ОК	Cancel Apply			

Confirm with OK and change to the "Launch and Activation Permissions". Press "Edit Limits..." and enter auduser together with relevant rights as displayed in the screen on the next page:

Ay Computer Properties	? 🔀	Launch Permission		? 🔀
General Options Default Protocols MSDTC Access Permissions You may edit who is allowed default access also set limits on applications that determine Edit Limits	Default Properties COM Security to applications. You may their own permissions.	Security Limits Group or user names: Administrators (MCIS_SER auduser (MCIS_SERVER) Jeder	VER\Administrators) auduser)	
Launch and Activation Permissions You may edit who is allowed by default to la activate objects. You may also set limits on determine their own permissions. Edit Limits	unch applications or applications that Edit Default	Permissions for auduser Local Launch Remote Launch Local Activation Remote Activation	Add Allow V V	Remove Deny
ок (	Cancel Apply		OK	Cancel

Confirm with OK.



### 2. Settings for MCIS DNC Cell/Plant/IFC

### DCOM configuration on the controller

Start the DCOM configuration as follows: start... run... "dcomcnfg"

Navigate to: Component Services  $\rightarrow$  Computers  $\rightarrow$  My Computer  $\rightarrow$  dhs.DHS\_SRV -- $\rightarrow$  click with the right mouse button  $\rightarrow$  call up "Properties"

The DHS process has been designed for external access to the communication server used by another computer to access the controller. For this reason, this "Server" must be configured as follows for network access.

🐌 Component Services				
🚱 File Action View Window Help				_18
	**	# <b>0</b>	dhs.DHS_SR¥ Properties	? >
Console Root	DCOM Config		General Location Secu	urity   Endpoints   Identity
Component Services	Name	Application ID	General properties of th	is DCOM application
Computers	ACCLoader32, Cfi	{53CF8A72-ED12-4D3 {DE5DBCDC-104A-4cb	Application Name:	dhs.DHS_SRV
E-COM+ Applications	AccVar. Md	{67BADD85-0EF3-11D {CC54E651-95D4-11D	Application ID:	{42AC1CE4-CE69-11D3-8D9E-00105A55E146}
	Automatic Updates	{653C5148-4DCE-4905	Application Type:	Local Server
E AccVar.Md	Background Intelli	{69AD4AEE-51BE-439t {783C030F-E948-487E	Authentication Level:	None
	COM+ Event Syst	{4E14FBA2-2E22-11D1 {ECABB0C3-7F19-11D3	Local Path:	f:\ADD_ON\Dhs.exe
Blocked Drivers     GOM+ Event Syst	ComEvents. Com	{ECABB0C6-7F19-11D: {797EF3B3-127B-4283		
ComEvents.ComS		{84D586C4-A423-11D:		
Command line Tric	Defrag FAT engine	{80EE4902-33A8-11d1		
DBServerTask	Defrag NTFS engine	{80EE4901-33A8-11d1		
	DG. COM_Alarm	{43E5B57A-AC8B-4649		
🕀 🧒 Defrag NTFS engi	dhs. DHS_SRV	{42AC1CE4-CE69-11D		
🕀 🧒 DG.COM_Alarm	DNC_IFC. CDNC	{4DF3DF34-5517-4E11		
🕀 🧒 dhs.DHS_SRV	DNC_IFCDB	{65192292-8064-11D7		
	Event Object Cha	{D0565000-9DF4-11D:		
E 🧑 DNC_IFCDB	Event Object Cha	{BB07BACD-CD56-4E6		OK Cancel Apply
In the "general" tab	ROT DUC 211	reczngeni-sege-ling	n lovol to "n	020"

ths.DHS_SRV Properties	? X Launch Permission ? >
General Location Security Endpoints Identity	Security
Launch and Activation Permissions C Use Default C Customize Edit	Group or user names: Administrators (840D1\Administrators) I 2 auduser (840D1\auduser) I 3 INTERACTIVE
Access Permissions © Use Default © Customize Edit	E Add Remove
Configuration Permissions © Use Default © Customize Edit	71     Local Launch     Image: Comparison of the
OK Cancel A	pply IC OK Cancel

In the "Security" tab, set the Launch Permissions for auduser as described above.

eneral Location Security Endpoints Identity Launch and Activation Permissions C Use Default C Customize Edit	Security Group or user names: EC Grauduser (840DI\auduser) 11 Grauduser (840DI\auduser) 12 SELF DE Graves SYSTEM
Access Permissions C Use Default Configuration Permissions C Use Default	C 51 99 Add Removing 7F Permissions for auduser 7F Local Access 2 Remote Access 44 5F
© Customize Edit	

In the "Security" tab, set the Access Permissions for auduser as described above.



hs.DHS_SRV Properties	? ×	Change Configuration Permission	?
General Location Security Endpoints Identity Launch and Activation Permissions  Use Default  Customize Edit.		Security Group or user names: Administrators (840D1\Administrators) CREATOR OWNER CREATOR OWNER CREATOR OWNER CREATOR OWNER	×
Access Permissions © Use Default © Customize Edit.		E Add  Permissions for auduser Allow  Full Control  Read	Remove
Configuration Permissions Cuse Default Customize	271 A42 5F3 3A 3A	Special Permissions	Ë
		For special permissions or for advanced settings, A click Advanced.	dvanced Cancel

In the "Security" tab, set the Configuration Permissions for auduser as described above.

Component Services			
File Action View Window Help ← ⇒ € II × 21	10 <b>-</b> 1- 1- 1- 1- 1- 1- 1- 1- 1- 1- 1- 1- 1-	T	dhs.DHS_SR¥ Properties
Console Root	DCOM Config 108 obj	ect(s)	General Location Security Endpoints Identity
E 🚱 Component Services	Name	Application ID	Which user account do you want to use to run this application?
Computers  My Computer  COM+ Applications  COM+ Applications  COM+ Applications  COM+ Config  C	ACCLoader32.Cfi AccStore Class AccVar.Md AccVar.Md Automatic Updates Background Intelli Blocked Drivers COM+ Event Syst ComEvents.ComS Comevent	453CF8A72-ED12-4D3 453CF8A72-ED12-4D3 40E5DBCDC-104A-4cb 467BADDB5-0EF3-11D 40C54E651-95D4-11D 4653C5148-4DCE-4905 469AD4AEE-51BE-4398 4783C030F-E948-487C 4E14FBA2-2E22-11D1 4ECABB0C3-7F19-11D 4ECABB0C6-7F19-11D 4CABB0C6-7F19-11D 4B0EE4902-33A8-11d1 40EE4901-33A8-11d1 4325B57A-AC88-4645 442AC1CE4-CE69-11D 40D53DF34-5517-4E11 40D565000-9DF4-11D 4B07BACD-CD56-4E6	
Change to the "Identi	ty" tab and	set to "Th	e interactive user".

Confirm your selection with OK.



### DCOM configuration on the master computer

Start the DCOM configuration: start... execute... "dcomcnfg"

Navigate to: Component Services  $\rightarrow$  Computer  $\rightarrow$  Workstation  $\rightarrow$  DCOM Configuration  $\rightarrow$  DBServerTask  $\rightarrow$  Click with the right mouse button  $\rightarrow$  Call up "Properties"

The DBServerTask process is a Windows service for external master computer access by the communication server DNC. For this, this "Server" must be configured as follows for network access:





In the "General" tab, set the "Authentication Level" to "None"



Decomponent Services							
S File Action View Window Help							
← → È III × E DBServerTask Properties ? 🛛	Launch Permission 🛛 ? 🔀						
Console Root       General Location Security Endpoints Identity         Computers       My Computer         My Computers       Launch and Activation Permissions         CoM+ A       Customize         Access Permissions       Edit         Access Permissions       Edit         Compose Complete       Customize         Complete       Customize         Complete       Customize         Complete       Customize         Customize       Ed	Security Group or user names:  auduser (MCIS_SERVER\auduser)  interRAKTIV  System  Add Remove  Add Remove  Permissions for auduser  Allow Deny  Local Launch  Remote Launch  Local Activation  Remote Activation  Permote Activation  Add Permissions  Add Remove  Add						
	OK Cancel						

In the "Security" tab, adapt the Launch Permission for the auduser as displayed above (if necessary, enter auduser via "Add...").

Somponent Services		×
File Action View Window Help	_ 8	X
← → 🖻 🖬 🗙 🛛 DBServerTask Properties 🛛 🔹 🛛	Access Permission	
Console Root       General Location Security Endpoints Identity         Component Services       Computers         My Compute       Launch and Activation Permissions         DCOM C       Customize         Auto       Access Permissions         Auto       Access Permissions         Back       Access Permissions         Com       Com         Com       Configuration Permissions         Configuration Permissions       Edit         Defr       Use Default         Configuration Permissions       Edit         Defr       Use Default         Configuration Permissions       Edit         Defr       Customize       Edit	Security Group or user names:  Group or user names:  SetLBST SetLBST SetLBST Add Remove Permissions for auduser Local Access Remote Access	
Ever Ever Monore Apply	OK Cancel	

In the "Access Permission" tab, adapt the Access Permission for the auduser as displayed above (if necessary, enter auduser via "Add...").



Component Services	
File Action View Window Help	
← → 🗈 🖬 🗙 🛛 DBServerTask Properties	Change Configuration Permission ? 🛛
Console Root       General Location       Security       Endpoints       Identity         Component Services       My Compute       Launch and Activation Permissions       Launch and Activation Permissions         My Compute       COM+A       Launch and Activation Permissions       Edit         DCOM C       Access Permissions       Edit         Auto       Back       Access Permissions       Edit         Bock       Com       Use Default       Edit         Com       Customize       Edit       Edit	Security Group or user names: Security Group or user names: Security ERSTELLER-BESITZER horst (ITDOMAIN\horst) Power Users (MCIS_SERVER\Power Users) Add Remove Permissions for auduser Allow Deny Full Control
Configuration Permissions Configuration Permiss	Read     Image: Constraint of the second setting second second setting second setting second setting

In the "Configuration Permission" tab, adapt the permissions for the auduser as displayed above (if necessary, enter auduser via "Add...").



Difference Services	
➢ File Action View Window Help ← → € III × P 2 2 2	DBServerTask Properties
Console Root Component Services Computers My Computer COM+ Applications COM+ Applications COM+ Config AccStore Class Ant Automatic Update Background Intelli Blocked Drivers COM+ Event Syst ComEvents.ComS ComEvents.ComS ComEvents.ComS ComEvents.ComS ComEvents.ComS ComEvents.ComS DBServerTask Defrag RAT engin Defrag NTFS engi Conconv.CodeCc Covent Object Cha Covent Object Cha	General Location Security Endpoints Identity         Which user account do you want to use to run this application?         The interactive user.         The Jaunching user.         This user.         User:         Browse         Password:         Copfirm password:         The system account (services only);
	OK Cancel Apply

In the "Identity" tab, set the DBServerTask to "System account". Confirm DCOM settings with OK.



Restart the service to activate the settings on the master computer. For this, open a command shell via start  $\rightarrow$  run... "cmd" and enter the following:

 C:WINDOWS\system32\cmd.exe
 Microsoft Windows XP [Uersion 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.
 C:\Documents and Settings\auduser>net The syntax of this command is:
 NET [ ACCOUNTS : COMPUTER : CONFIG : CONTINUE : FILE : GROUP : HELP : HELPMSG : LOCALGROUP : NAME : PAUSE ! PRINT ! SEND : SESSION : SHARE : START : STATISTICS : STOP : TIME : USE : USER : VIEW ]
 C:\Documents and Settings\auduser>net stop dbservertask The DBServerTask service is stopping. The DBServerTask service is stopped successfully.
 C:\Documents and Settings\auduser>net start dbservertask The DBServerTask service is starting. The DBServerTask service is starting.
 C:\Documents and Settings\auduser>net start dbservertask
 C:\Documents and Settings\auduser>net start dbservertask

Net Stop dbservertask  $\rightarrow$  stops the service Net Start dbservertask  $\rightarrow$  restarts the service

#### Microsoft - Personal - Firewall - Configuration on the controller

To start the firewall configuration on the controller, proceed as follows: Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall  $\rightarrow$  Exceptions

Windo	ws Firewall	1
ieneral	Exceptions	Advanced
Windov progran to work Progran	ws Firewall is b ns and service better but mig ns and Servic	locking incoming network connections, except for the is selected below. Adding exceptions allows some programs jht increase your security risk. es:
Name	,	
<b>1</b> 3	35 tep	
I ⊂ p	_840di	
	ns.exe	
<b>⊻</b> Fil	e and Printer S	Sharing
	emote Assistar Secola Declara	
	emote Deskto PoP Framewo	
Add	Program	Add Port <u>E</u> dit <u>D</u> elete
	elev e vetificat	ian ultan Viliadawa Firawali biraka a arawara
	рау а <u>п</u> олиса	ion when windows Filewall blocks a program
<u>What a</u>	ire the risks of	allowing exceptions?
		OK Cancel



Allow the following ports resp. applications in the personal firewall:

Port number 135 TCP Application DHS.EXE File and Printer Sharing

#### Microsoft - Personal - Firewall - Configuration on the master computer

To start the firewall configuration on the master computer, proceed as follows: Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall  $\rightarrow$  Exceptions

Windo	ows Firewa	ill	
ieneral	Exceptions	Advanced	
Windov program to work Program	vs Firewall is b ns and service better but mig ns and Servic	llocking incoming net is selected below. Ad jht increase your sec es:	work connections, except for the Iding exceptions allows some programs urity risk.
Name	9		
<b>☑</b> 13	5 top		
☑ 14	33 top sqlserv	/er	
🗹 DE	ServerTask.e	exe	
🗹 DN	IC HMI		
File	e and Printer S	Sharing	
🗹 Mi	crosoft Manag	gement Console	
🗹 Re	emote Assistar	nce	
Re	emote Desktoj	P	
	PnP Framewo	'k	
Add	Program	Add Port	Edit Delete
🗹 Disp	olay a notificat	ion when Windows F	irewall blocks a program
<u>What a</u>	re the risks of	allowing exceptions?	
			OK Cancel

Port number 135 TCP Application DBServerTask.EXE Application DNC HMI File and Printer Sharing

If necessary, share the port or application for MSSQLServer with DNC Plant!

Adapt file sharing mode in the network on the master computer:

	IC Taola Hala	
Back - 🔊 - 🏂	D Search Polders 2 Search	
Address 🛅 C:\Siemens\MCIS\Dat	a\DNC	So So
Folders	ONC Properties	Permissions for DNCS
<ul> <li>Desktop</li> <li>My Documents</li> <li>My Computer</li> <li>3% Floppy (A:)</li> <li>3% Floppy (A:)</li> <li>System (C:)</li> <li>Documents and Se</li> <li>Program Files</li> <li>Siemens</li> <li>MCIS</li> <li>Common</li> <li>Data</li> <li>Data</li> <li>DAta</li> <li>DC</li> <li>Cc</li> <li>DC</li> <li>Cc</li> <li>DAta</li> <li>DKC</li> <li>Ex</li> <li>Im</li> <li>Tn</li> <li>Gerno</li> <li>MDA</li> <li>MSQI</li> <li>TDI</li> <li>VL</li> <li>DNC</li> <li>Errors</li> <li>etc</li> <li>MDA</li> </ul>	General       Sharing       Security       Customize         Image: Sharing       You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.         Image: Do not share this folder       Image: Do not share this folder         Image: Do not share this folder       Image: Do not share this folder         Image: Do not share this folder       Image: Do not share this folder         Image: Do not share this folder       Image: Do not share this folder         Image: Do not share this folder       Image: Do not share this folder         Image: Do not share this folder       Image: Do not share this folder         Image: Do not share this folder       Image: Do not share this folder         Image: Do not share this folder       Image: Do not share this folder         Image: Do not share this folder on the network, click Permissions.       Image: Do not share this folder the share this folder on the network, click Permissions.         Image: Do configure settings for offline access, click       Caching         Image: Do configure settings for offline access, click       Caching         Image: Do configure to allow this folder to be shared with other computers on the network.       New Share         Undows Firewall is configured to allow this folder to be shared with other computers on the network.       Mane         DK       Cancel       Annly <td>Share Permissions         Group or user names:         auduser (MCIS_SERVER\auduser)         Add         Remove         Permissions for auduser         Allow         Deny         Full Control         Change         Read         OK       Cancel</td>	Share Permissions         Group or user names:         auduser (MCIS_SERVER\auduser)         Add         Remove         Permissions for auduser         Allow         Deny         Full Control         Change         Read         OK       Cancel

In the Windows Explorer, navigate to the DNC directory (for example, c:\Siemens\MCIS\DATA\DNC). Select DNC, click with the right mouse button and navigate to "Properties".

Click on "Sharing".

Share the folder as hidden share (in the example, via "DNC\$") in the network. Set auduser rights as displayed above and confirm with OK.



In the Windows Explorer, via "Tools" - "Folder Options" change to the "View" tab:



Untick "Use simple file sharing". As a result, the system performs a real user authentification for shared network drives and does not use the "guest login".  $\rightarrow$  Confirm with OK.



Check registry parameterization on the master computer ------Open registry under HKLM \ Software \ Siemens

The following entry must be made (provided with MCIS DNC V2.1 Setup): Key name: DBServerTask Dword Name: initsec Value of initsec: 1

### 3. Settings for MCIS TPM Cell/Plant/IFC

DCOM configuration on the controller

No configuration required

Microsoft - Personal - Firewall - Configuration on the controller No configuration required

#### Microsoft - Personal - Firewall - Configuration on the master computer

-----

To start the firewall configuration on the master computer, proceed as follows: Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall  $\rightarrow$  Exceptions

Windows Firew	all
ieneral Exceptions	Advanced
Windows Firewall is programs and servic to work better but m	blocking incoming network connections, except for the es selected below. Adding exceptions allows some programs ight increase your security risk.
Programs and Servi Name	ces.
✓ 135 tcp	
✓ 1433 tcp sqlse	rver
DBServerTask	exe
DNC HMI	
File and Printer	Sharing
Microsoft Man	agement Console
Remote Assist	ance
🗌 Remote Deskt	op
UPnP Framew	ork
Add Program	Add P <u>o</u> rt <u>E</u> dit <u>D</u> elete
Add Program	Add Port       Edit       Delete         ation when Windows Firewall blocks a program         of allowing exceptions?
Add Program	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel
Add Program	Add P <u>o</u> rt <u>E</u> dit <u>D</u> elete ation when Windows Firewall blocks a program of allowing exceptions? OK Cancel
Add P <u>r</u> ogram Display a <u>n</u> otificat What are the risks of Edit a Port	Add P <u>o</u> rt <u>E</u> dit <u>D</u> elete ation when Windows Firewall blocks a program of allowing exceptions? OK Cancel
Add Program  Display a notificat What are the risks of Edit a Port Use these settings pumber and protocome	Add Port Edit Delete ation when Windows Firewall blocks a program of allowing exceptions? OK Cancel Cancel to open a port through Windows Firewall. To find the port all compute the program or service upper
Add Program Display a notificat What are the risks of Edit a Port Use these settings number and protoc want to use.	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         Image: Consult the documentation for the program or service you
Add Program Display a notificat What are the risks of Edit a Port Use these settings number and protoc want to use.	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         OK       Cancel         Image: Comparison of the port of the program of service you       of open a port through Windows Firewall. To find the port of, consult the documentation for the program or service you
Add Program Display a notificat What are the risks of Edit a Port Use these settings number and protoc want to use.	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         Ok       Cancel         it open a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you
Add Program  Display a notificat What are the risks of Edit a Port Use these settings number and protoc want to use. Name:	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         Open a port through Windows Firewall. To find the port of, consult the documentation for the program or service you         1433 top sqlserver
Add Program  Display a notification  What are the risks of  Edit a Port  Use these settings number and protoc want to use.  Name:	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         OK       Cancel         it open a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you         1433 tcp sqlserver
Add Program  Display a notificat What are the risks of Edit a Port Use these settings number and protoc want to use. Name: Port number:	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         Object       OK         It allowing exceptions?       It is a set of the port of the program or service you         1433 tcp sqlserver       It is a set of the port of the program of the port of the port of the program of the port of the port of the program of the port of the
Add Program  Display a notificat What are the risks of Edit a Port Use these settings number and protoc want to use. Name: Port number:	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         Object       OK         Image: Comparison of the port of the port of the program or service you         1433 top sqlserver         1433
Add Program  Display a notification  Mhat are the risks of  Edit a Port Use these settings number and protoc want to use.  Name: Port number:	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         OK       Cancel         It allow a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you         1433 tcp sqlserver         1433         It CP       UDP
Add Program  Display a notificat What are the risks of Edit a Port Use these settings number and protoc want to use. <u>Name: Port number:</u>	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?       OK       Cancel         of allowing exceptions?       OK       Cancel       Cancel         to open a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you       1433 tcp sqlserver       1433         o ICP       UDP       OLP       OLP
Add Program  Display a notificat What are the risks of Edit a Port Use these settings number and protoc want to use. <u>Name:</u> Port number: What are the risks	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         OK       Cancel         Image: Consult the documentation for the program or service you       Image: Consult the documentation for the program or service you         1433       Image: Consult the documentation for the program or service you         Image: OF       Image: OF         Image: OF       Image: OF
Add Program  Display a notificat What are the risks of Edit a Port Use these settings number and protoc want to use.  Name: Port number: What are the risks	Add Port       Edit       Delete         ation when Windows Firewall blocks a program       of allowing exceptions?         OK       Cancel         OK       Cancel         Image: Consult the documentation for the program or service you       of allowing exceptions?         1433       to open a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you         1433       Image: Consult the documentation for the program or service you         1433       Image: Opening a port?

Port number 1433 TCP SQLServer

Subject to change without prior notice.



File and Printer Sharing

### 4. Settings for MCIS TDI Cell/Plant/IFC

#### DCOM configuration on the controller

No configuration required

#### DCOM configuration on the master computer

-----

No configuration required

#### Microsoft - Personal - Firewall - Configuration on the controller

To start the firewall configuration on the controller, proceed as follows: Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall

	Add a Program 🛛 🔀
In the control panel, call up the "Windows Firewall" and change to the "Exceptions" tab. Press the "Program" button, "Browse" in the following screen, select the application "TDI.exe" in the TDI installation directory (F:\Add_on\TDI) via "Open". Confirm the selected application with "OK" and press OK again to exit the "Windows Firewall". The settings become immediately active.	To allow communications with a program by adding it to the Exceptions list, select the program, or click Browse to search for one that is not listed. Programs: HMI Startup Install-Deinstall MCIS RCS Host TDI TDI TDI TouchWare Monitor
	Path: F:\Add_on\TDI\TDI.exe Browse
	Change scope OK Cancel

#### Microsoft - Personal - Firewall - Configuration on the master computer

To start the firewall configuration on the master computer, proceed as follows: Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall  $\rightarrow$  Exceptions

Windows Firev	vall					
General Exception	s Advanced					
Windows Firewall is programs and servi to work better but r Programs and Serv	s blocking incor ces selected br night increase y ices:	ming network elow, Adding vour security	connectior exceptions risk.	is, except allows so	t for the me progra	ms
Name						
✓ 135 tcp						
✓ 1433 tcp sqls/	erver					í
DBServerTas	k.exe					
DNC HMI						
File and Printe	er Sharing					
Microsoft Mar	agement Cons	ole				
Remote Assis	tance					
	top					
	iork					
	NOIN					
Add Program	Add Port		Edit		Delete	
Add Program  Display a notific What are the risks	Add Port	ndows Firew	Edit all blocks a j	orogram	Delete	
Add Program	Add Port	ndows Firew	Edit all blocks a j	orogram OK	Delete	
Add Program  Display a notific  What are the risks  Edit a Port	Add Port	ndows Firew	Edit all blocks a j	orogram OK	Delete Can	
Add Program  Add Program  Mhat are the risks  Edit a Port Use these settings number and protoc want to use.	Add Port	ndows Firew eptions? through Win	Edit all blocks a j dows Firewa	Drogram	Delete Can the port service yo	cel
Add Program  Add Program  Display a notific  What are the risks  Edit a Port  Use these settings number and protoc want to use.  Name:	Add Port ation when Wir of allowing exc to open a port ol, consult the o	through Win documentatio	Edit all blocks a p dows Firewa	orogram OK II. To find	Delete Can the port service yo	cel
Add Program  Add Program  Display a notific  What are the risks  Edit a Port Use these settings number and protoc want to use.  Name: Port number:	Add Port ation when Wir of allowing exc to open a port ol, consult the [1433 top sqlst 1433	through Win	Edit all blocks a p dows Firewa	orogram OK II. To find ogram or s	Delete Can the port service yo	cel
Add Program  Add Program  Display a notific  What are the risks  Edit a Port  Use these settings number and protoc want to use.  Name: Port number:	Add Port ation when Wir of allowing exc to open a port ol, consult the [1433 () TCP	through Windocumentatio	Edit all blocks a p dows Firewa	OK	Delete Can the port service yo	u
Add Program  Add Program  Mater are the risks  Edit a Port Use these settings number and protoc want to use.  Name: Port number:  What are the risks	Add Port ation when Wir of allowing exc to open a port ol, consult the o [1433 top sqlsr 1433 TCP of opening a port	through Win documentation	Edit all blocks a p dows Firewa	DK	Delete Can	u u
Add Program  Add Program  Display a notific  What are the risks  Edit a Port  Use these settings number and protoc want to use.  Name: Port number:  What are the risks  Change scope	Add Port ation when Wir of allowing exc to open a port ol, consult the [1433 () TCP of opening a port ()	through Win documentation	Edit all blocks a p dows Firewa on for the pro	Drogram	Delete Can the port service yo	u u

Port number 1433 TCP SQLServer File and Printer Sharing

Subject to change without prior notice.

© Siemens AG 2007 Page 21 / 35 1-6A03EP\_MCIS-SW-DCOM-plus-Firewall-bei-WinXPSP2\_eng.doc



Application MCIS-TDI PC

### 5. Settings for MCIS MDA Cell/Plant/IFC

### DCOM configuration on the controller No configuration required

#### DCOM configuration on the master computer

Before configuring DCOM, you have to create the MDA-specific user "PDA" (required when performing the MDA setup):





This user must have administrator rights.

(The following setting is only required up to/including MDA Version 02.01.x.x) Start the DCOM configuration: start... execute... "dcomcnfg"

Navigate to: Component Services  $\rightarrow$  Computer  $\rightarrow$  Workstation  $\rightarrow$  DCOM configuration  $\rightarrow$  ErrorHandler.ErrorObject  $\rightarrow$  Click with the right mouse button  $\rightarrow$  Call up "Properties"

The ErrorHandler process must be configured as follows:



Domponent Services			
n File Action View Window Help			
	# # # 9		
Console Root  Component Services  Computers  My Computer  Adobe Acrobat-Dokument  Ant  Adobe Acrobat-Dokument  Ant  Cluster Configuration Server  Cluster Node Eviction Asynchronous  Cluster Node Eviction Processor  Cluster Service Node Evict Notificatic  Cluster Service Startup Notifications  COM+ Event System  ComEvents, ComServiceEvents  Command line Trigger Consumer  ConnectLogdatenMaschine Objekt  CustReg Class  DoBServerTask  CustReg Class  DoBServerTask  Component Service  CustReg Class  Component Service  CustReg Class  CustReg Class	ErrorHandler.ErrorObject General   Location   Sec Which user account do The interactive user The launching user. User: Password: Confirm password: The system account	t Properties surity Endpoints Identity you want to use to run this ap PDA. ••••••• ••••••••	? × oplication? Browse
Event Object Change      Field Strengt Change      Field Strengt Change 2			ncel Apply

In the Identity tab, enter the user "PDA"



Component Services					
😰 File Action View Wind	ow Help				
⇔ → € 🛛 × 🗗	8   😢 🖬   🎦   🏊 🔚 🏥 🏢 🌐				
Console Root	rrorHandler.ErrorObject Properties	?×	Access Permission		<u>?</u> ×
Computer Services     Computers     Computers     COM+ App     COM+ App     COM+ App     COM+ CON     CO	General Location Security Endpoints Iden Launch and Activation Permissions C Use Default C Customize Access Permissions	Edit	Security Group or user names: Distributed COM Users (M SI-15-21-2308103852-370 SI-5-21-230810 SI-5-21-230810	CIS-W2003S\Distributed )6444998-3854934179-1( ers)	COM U 007
E 🛠 Cluster E 🛧 Cluster E 🛧 Cluster E 🛧 COM+ E 🛧 ComEvi	<ul> <li>C Use Default</li> <li>I Customize</li> </ul>	Edit	Permissions for Users Local Access Remote Access	Allow [	Deny
E - S ComEvi E - S Comma B - S Connec E - S CustRe E - S DBServ B - S DCOMS E - S DCOMS E - S Defrag E - S Defrag	Configuration Permissions C Use Default C Customize	Edit			
dfrgifc     dfs.DH     DNCCom		Cancel Apply		ОК	Cancel
	iert Change				

In the "Security" tab, adapt the "Access Permission" for the local users as described above.

Make DCOM settings for errorhandler **analogously** to **Tracehandler, Eventhandler and MDEServer** !

Microsoft - Personal - Firewall - Configuration on the controller No configuration required

#### Microsoft - Personal - Firewall - Configuration on the master computer

\_\_\_\_\_

To start the firewall configuration on the master computer, proceed as follows: Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall  $\rightarrow$  Exceptions

👹 Windows Firewall	×	Edit a Port 🛛 🔀
General Exceptions Advanced Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk. Programs and Services:	8	Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use. Name: 3501 TCP for ISM (Message Manager)
Name		Port number: 3501
I 133 top         I 1433 top sqlserver         I 3501 TCP for ISM (Message Manager)         I DBServerTask.exe         I DNC HMI         I File and Printer Sharing         I Microsoft Management Console         Remote Assistance         Remote Desktop         I TDLPC         I IPnP Framework         Add Program         Add Port         Edit         Delete         What are the risks of allowing exceptions?         OK		TCP UDP  What are the risks of opening a port? Change scope     OK Cancel



Windows Firewall	Edit a Port	
General Exceptions Advanced Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.	Use these settings number and protoc want to use.	to open a port through Windows Firewall. To find the port col, consult the documentation for the program or service you
Programs and Services:	Name:	B409 TCP for MMPing
Name	Port number:	3409
<ul> <li>I 135 tcp</li> <li>I 1433 tcp sqlserver</li> <li>3409 TCP for MMPing</li> <li>3501 TCP for ISM (Message Manager)</li> <li>DBServerTask.exe</li> <li>DNC HMI</li> <li>File and Printer Sharing</li> <li>Microsoft Management Console</li> <li>Remote Assistance</li> <li>Remote Desktop</li> <li>Tn1 Pr</li> <li>Add Program Add Port Edit Delete</li> <li>Display a notification when Windows Firewall blocks a program</li> <li>What are the risks of allowing exceptions?</li> </ul>	What are the risks Change scope	TCP UDP of opening a pot? OK Cancel

Allow the following exceptions in the firewall (configure manually): Port number 3409 TCP for MMPing Port number 3501 TCP for ISM (Message Manager) File and Printer Sharing

### 6. Settings for ADDM Client/Agent

### DCOM configuration on the controller

Start the DCOM configuration: start... run... "dcomcnfg"

Navigate to: Component Services  $\rightarrow$  Computer  $\rightarrow$  My Computer  $\rightarrow$  DCOM Config  $\rightarrow$  P7tldagn  $\rightarrow$  Click with the right mouse button  $\rightarrow$  Call up "Properties"

The P7tldagn process (ADDM Agent) must be configured as follows:

Services					
🌮 File Action View Window Help					
	0 🖭 🗄 🔠 🗰 🖷	ļ			-15
Console Root	DCOM Config 162 object(s)				
Component Services	Name Application ID				
	p7SerIntSvr.Mac {7A3F8E80-39F6-11D3-9E86-00105AB0427D}				
E OM+ Applications	P7tldagn {A248	C040-0F2C-4AF4-	805A-898DAA476C0A}		
DCOM Config	P7tldjmx {1A9F	9B3B-6AC5-11D5-	B9AA-00105AC43D70}		
P7tIdago Properties	TOPP/TLDM5X {/BBA	813F-6A09-11D5-	BAF-00105AB04241}		at will
General Location Security Endpoints	Identity	-A6DF-48C 9D75-101/	Security		<u> Y</u> X
- Launch and Activation Permissions -		0991-11d3	Group or user names:		
C. Use Default		105B-11D4	Administrators (840DI\Ad	dministrators)	_
		714B-11D6	🛒 auduser (840DI\auduser	)	
<ul> <li>Customize</li> </ul>	Edit	-4138-4AC	<b>MINTERACTIVE</b>		
		F99E-461C	SYSTEM		
Assess Demissions		-D644-11d			
ACCESS F Emissions		A296-4F2[	197		
C Use Default		-8F53-11D		Add Remov	
Customize	Edit	85ED-4751	Permissions for auduser	Allow Deny	
		DF5E-40C0	Local Launch		_
		-FE3E-11CE	Remote Launch		
Configuration Permissions		7B8F-11D1	Local Activation		
Use Default		-761E-11D	Remote Activation		
	· · · · · ·	A109-11D0			
C Lustomize	E dit	A109-11DL			
In the Security tab, auduser with above-me	adapt the Launc ntioned rights	h Permis	sions as descr	ibed above: Add	
Component Services					
File Action View Window Help		1121.7			
		3			
Console Root	DCOM Config 162 object(s)	2	1.00		
Component Services	Computers Application ID				
Computers     My Computer     My Computer					
COM+ Applications     COM+ Applications					
	P7TLDMSX {7BB/	A813F-6A09-11D5	-BBAF-00105AB04241}		
P7tldagn Properties		-6B8E-11D5	-BBB		21 2
Consul Landian Security J. F. L	[ Internation ]	-A6DF-48C3	-8D7		<u>م</u> ب
General Location Security Endpoints	General Location Security Endpoints Identity   9D75-101A-8C3( Security				
- Launch and Activation Permissions -		0991-11d3- -4B81-4AAA	-8E3I Group or user names:		

General     Location     Security     Endpoints     Identity       Launch and Activation Permissions       Use Default       Customize     Edit	-9075-101A-8C3( 0991-11d3-b822- -4B81-4AAA-8E3) -105B-11D4-87AE -714B-11D6-8A19 -4138-4AC4-A49; F99E-461C-86C3 -61FF-11D4-8725 -D6AA-11d0-9ED	Security Group or user names: auduser (840DI\auduser) SELF SYSTEM		
C Use Default C Customize Edit	-A296-4F2D-A2F{ -8F53-11D0-BFA( 85ED-4751-A3C7	Permissions for auduser	Add	Remove Deny
Configuration Permissions   Cuse Default Customize Edit	DF5E-40C0-94A2 -350D-11D2-8014 -FE3F-11CE-A58/ -788F-11D1-8F67 -761E-11D1-9586 A109-11D0-AA8; A109-11D0-AA8;	Local Access Remote Access	N N	

Subject to change without prior notice. © Siemens AG 2007

© Siemens AG 2007 Page 28 / 35 1-6A03EP\_MCIS-SW-DCOM-plus-Firewall-bei-WinXPSP2\_eng.doc



In the Security tab, adapt the Access Permissions as described above: Add auduser with above-mentioned rights

DCOM configuration on the master computer

-----

No configuration required

#### Microsoft - Personal - Firewall - Configuration on the controller

To start the firewall configuration on the controller, proceed as follows:

Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall  $\rightarrow$  Exceptions

Ø Windows Firewall	x protect my computer?
General Exceptions Advanced	can monitor. Click Recommendations to find out
Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.	Recommendations
Programs and Services:	er is more vulnerable to viruses and other
Name	A lates to have Windows automatically keep your w does Automatic Updates help protect my
☑ 3011 tcp	
	Turn on Automatic Updates
Also TCP	
Adaptive Server Anywhere Network Server	
☑ cp_840di Edit a Program	<u>×</u>
☑ Dhs.exe       You can allow communication of the second s	unication with this program from any computer, Internet or just from computers on your network. &&D DataManagement Agent
Path: E:\Pro	ogram Files\Siemens\ADDM Agent\p7tldagn.exe
Add Program Add Port Edit	
Display a notification when Windows Firewall blocks Change scope	OK Cancel

General Exceptions Advanced	can monitor. Click Recommendations to find out
Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some progra to work better but might increase your security risk.	ams
Programs and Services:	er is more vulnerable to viruses and other
Name	A lates to have Windows automatically keep your
3011 tcp	
Edit	t a Port 🔀
<ul> <li>□ A&amp;&amp;D DataManagement Agent</li> <li>□ Adaptive Server Anywhere Network Server</li> <li>□ Cp_840di</li> <li>□ Dhs.exe</li> <li>□ File and Printer Sharing</li> <li>□ Microsoft Management Console</li> <li>□ P7TLDSOK Module</li> <li>□ Remote Assistance</li> </ul>	e these settings to open a port through Windows Firewall. To find the port mber and protocol, consult the documentation for the program or service you ant to use. Name: 4135 TCP Port number: 4135
Add Program Add Port Edit Dek	
I ■ Display a notification when windows niewali blocks a program	hat are the risks of opening a port?
What are the risks of allowing exceptions?	Change scope OK Cancel

Windows Firewall	wall helps protect your computer against viruses and
General Exceptions Advanced Windows Firewall is blocking incoming network connections, except programs and services selected below. Adding exceptions allows sor to work better but might increase your security risk.	for the me programs Recommendations to find out <u>R</u> ecommendations
Programs and Services:	OFF (®
Name  ✓ 3011 tcp  ✓ 135 tcp  ✓ A&&D DataManagement Agent	computer is more vulnerable to viruses and other tic Updates to have Windows automatically keep your tes, <u>How does Automatic Updates help protect my</u>
<ul> <li>✓ cp_840di</li> <li>✓ Dhs.exe</li> <li>✓ File and Printer Sharing</li> <li>✓ Microsoft Management Console</li> <li>✓ P7TLDSOK Module</li> <li>□ Remote Assistance</li> <li>✓ Remote Desktop</li> </ul>	Edit a Port Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Add Program Add Port Edit	Port number: 135 • TCP C UDP
	What are the risks of opening a port?     Change scope     OK Cancel



Allow the following exceptions in the firewall (configure some of them manually): Application A&D Datamanagement Agent Port number 4135 TCP Port number 135 TCP File and Printer Sharing

#### Microsoft - Personal - Firewall - Configuration on the master computer

\_\_\_\_\_

To start the firewall configuration on the master computer, proceed as follows: Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall  $\rightarrow$  Exceptions

Windows Firewall	×	Edit a Service	
General Exceptions Advanced Windows Firewall is blocking incoming network connections, except for the		You can individually configues service. To open a port, sel	ure the port(s) that are associated with t lect the check box next to it.
programs and services selected below. Adding exceptions allows some program to work better but might increase your security risk. Programs and Services:	S	Name ✓ TCP 139 ✓ TCP 445	Scope Subnet Subnet
Name	~	UDP 137	Subnet
<ul> <li>✓ 135 top</li> <li>✓ 1433 top sqlserver</li> <li>✓ 3409 TCP for MMPing</li> <li>✓ 3501 TCP for ISM (Message Manager)</li> <li>✓ DBServerTask.exe</li> <li>✓ DNC HMI</li> </ul>		Change scope	OK Cancel
✓ File and Printer Sharing			
Microsoft Management Console			
Remote Desktop	-		
Add Program Add Port Edit Delete  Display a notification when Windows Firewall blocks a program  What are the risks of allowing exceptions?			
OK Cance			

Allow the following exceptions in the firewall: File and Printer Sharing



### 7. Settings for MCIS RPC SINUMERIK

DCOM configuration on the controller

-----

No configuration required

DCOM configuration on the master computer

No configuration required

#### Microsoft - Personal - Firewall - Configuration on the controller

To start the firewall configuration on the controller, proceed as follows: Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall  $\rightarrow$  Exceptions

Windows Firewal		X		😈 security cer	iter
General Exceptions	Advanced			Help protect ye	our PC
Windows Firewall is programs and service	blocking incoming network connections, except for the sesselected below. Adding exceptions allows some prog	rams	le your V entials ar he Securi	Vindows security settings. To help protect your computer, re marked ON. If the settings are not ON, follow the ity Center later, open Control Panel.	-
to work better but n	light increase your security risk.	MCI5 RP	E SINUM	1ERIK (SinCOM) Configuration	>
Programs and Servi	ces:	Machin	e Host	Tools RPC Logging GUD	
Name		Name		840DI	
I 3011 tcp		Endpo	oint:	3011	
Full a Port				[]	
Use these settings number and protoc	to open a port through Windows Firewall. To find the por ol, consult the documentation for the program or service.	Put-D	rectory:	F:\TMP\PUT	
want to use.		Get-D	irectory:	F:\TMP\GET	
Name:	3011 tcp				
Port number:	3011	Test NCSTATE			
	C 100				
		1		ОК	Cancel
What are the risks	of opening a port?				
			ivirus sol	ftware that you will monitor yourself. To help protect you	r,
Lhange scope	UK Cancel		ow does	antivirus software help protect my computer?	

Depending on the port number configured, share this port in the firewall. Port **3011 TCP** is the default port on the controller.

#### Microsoft - Personal - Firewall - Configuration on the master computer

\_\_\_\_\_

To start the firewall configuration on the master computer, proceed as follows: Start  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  Windows Firewall  $\rightarrow$  Exceptions

🗑 Windows Firewall 🛛	×	Edit a Port 🛛 🔀
General Exceptions Advanced Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk. Programs and Services:		Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name         ▲           ☑ 135 tcp         ☑		Port number: 3010
I 1433 top sqiserver 3010 TCP 3409 TCP for MMPing 3501 TCP for ISM (Message Manager) DBServerTask.exe DNC HMI File and Printer Sharing Microsoft Management Console Remote Assistance Remote Deskton Add Program Add Port Edit Delete Value Display a notification when Windows Firewall blocks a program What are the risks of allowing exceptions? OK Cancel		What are the risks of opening a port? Change scope OK Cancel

Depending on the port number configured, share this port in the firewall. Port **3010 TCP** is the default port on the controller.

Siemens AG. A&D MC CS 2