SIEMENS

Grundeinstellungen	1
Konfiguration der Firewall	2
DCOM-Konfiguration	3
DCOM-Konfiguration als "Machine Default"	4

SIMATIC HMI

Einsatz von OPC über DCOM mit Windows XP SP3

Readme

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

GEFAHR

bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

NORSICHT

mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

VORSICHT

ohne Warndreieck bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG

bedeutet, dass ein unerwünschtes Ergebnis oder Zustand eintreten kann, wenn der entsprechende Hinweis nicht beachtet wird.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG Industry Sector Postfach 48 48 90026 NÜRNBERG DEUTSCHLAND

@ 01/2010

Inhaltsverzeichnis

1	Grundeinstellungen	. 3
2	Konfiguration der Firewall	. 3
3	DCOM-Konfiguration	. 3
4	DCOM-Konfiguration als "Machine Default"	. 3

1 Grundeinstellungen

Kurzbeschreibung

Das Windows XP Service Pack 3 dient hauptsächlich dazu, die gängigsten Versuche böswilliger Zugriffe auf Windows XP abzuwehren. Das Service Pack verringert damit die Auswirkungen der häufigsten Angriffe.

Nach Ansicht der Autoren werden in diesem Beitrag die besten Verfahrensweisen beschrieben; dennoch übernehmen die OPC Foundation und die Autoren keine Verantwortung für die Richtigkeit oder Anwendungstauglichkeit dieses Dokuments für die jeweiligen Leser.

Benutzerverwaltung

Auf allen (DCOM-) Rechnern müssen die gleichen Benutzer mit ihren jeweiligen Administratorrechten eingerichtet sein. Für die Erstellung der Benutzerprofile müssen sich die betreffenden User einloggen.

Windows Firewall

Die Firewall-Ausnahmen können auf zwei Hauptebenen festgelegt werden, auf Anwendungsebene und auf Port- und Protokollebene. Um eine OPC Client/Server-Anwendung über DCOM einzurichten, müssen die Änderungen auf beiden Ebenen erfolgen.

2 Konfiguration der Firewall

Konfiguration der Firewall

1. Mit der Voreinstellung "On" ist die Windows-Firewall aktiviert.

Falls die Maschine durch eine unternehmenseigene Firewall geschützt ist, kann es zweckmäßig sein, die Windows-Firewall dauerhaft abzuschalten.



2. Wählen Sie den Reiter "Exceptions" und tragen Sie sämtliche OPC Clients und Server in die Ausnahmenliste ein. Fügen Sie aus dem Verzeichnis Windows\System32 auch die Microsoft Management Console (wird vom DCOM Konfigurationsprogramm im nächsten Abschnitt verwendet) hinzu sowie das OPC-Programm OPCEnum.exe. Über die Schaltfläche "Browse' können Sie nach weiteren ausführbaren Dateien auf ihrem Rechner suchen.

Eventions	Adversed
ieneral Exceptions	Advanced
Windows Firewall is t programs and service to work better but mig	blocking incoming network connections, except for the es selected below. Adding exceptions allows some programs ght increase your security risk.
Programs and Servic	es:
File and Drinter	Charing
GenAgentique	onainy
	ruar ava :
GraphWorX32	a vel.exe (
I ASEngine exe	
License Monitor	
Microsoft Mana	gement Console
☑ OPC DataSpy	→ A 2015 A 2015 A 2015 A 2017 A 2
OPC Simulator	
🗹 Remote Assista	nce
	n 🔛
Add Program	Add Port <u>E</u> dit <u>D</u> elete
Display a <u>n</u> otifical	ion when Windows Firewall blocks a program
What are the risks of	allowing exceptions?

Hinweis

In die Ausnahmenliste können nur EXE-Dateien aufgenommen werden. Bei momentan im Einsatz befindlichen OPC-Servern und -Clients (DLLs und OCXs) müssen Sie die aufrufenden EXE-Anwendungen extra hinzufügen.

Add a Program	×
To allow communications with a program by adding it to the Exceptions lis	t
select the program, or click Browse to search for one that is not listed.	
Programs:	_
Alarm Logger Configurator	^
Kara Alarm Server Configurator	-
AlarmWorX32	
tai DataWorX32	
DBOPCServerConfigurator	
3 DIDCOM	
GenDUS3 to GFW16	
CarChelinia Visual	
	~
Path: C:\Program Files\ICONICS\GENESIS-32\Bin\ Browse.	
	_
Change scope OK Cancel	

3. Fügen Sie den TCP-Port 135 hinzu, da dieser für den Start der DCOM-Kommunikation benötigt wird und erlauben Sie eingehende Echo Requests (Echo-Anforderungen).

4. Klicken Sie im Reiter "Exceptions" auf die Schaltfläche "Add Port...".

🞾 Windows F	irewa	Ш				
General Excep	otions	Advanced				
Windows Firev programs and : to work better <u>P</u> rograms and	vall is bl service: but migl Service	ocking inco s selected b ht increase y s:	ming netwo elow. Addir your securit	rk connect g exceptio y risk.	tions, excep ns allows s	ot for the ome programs
Name						~
File and F	Printer S	haring				
🗹 GenAgen	it.exe					
🗹 Gen Regis	strarSer	ver.exe				-
🗹 GraphWo	orX32					
☑ LASEngir	ne.exe					
License N	1onitor		29.23			
	Manag -Cou	ement Lons	ole			
	ulator					
I Bemote A	alotoi Seeistan	ce				
	leskton					×
Add Program	n 🕻	Add P <u>o</u> r		<u>E</u> dit		Delete
Display a <u>n</u>	otificatio	on when Wi	ndows Fire	wall blocks	a program	
What are the r	isks of a	allowing exc	eptions?			
					OK	Cancel

5. Tragen Sie im "Add a Port"-Dialogfenster Folgendes ein:

Name: DCOM

Port number: 135

6. Aktivieren Sie das Optionsfeld TCP

Add a Port	
Use these settings number and protoc want to use.	to open a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you
<u>N</u> ame:	ОСОМ
<u>P</u> ort number:	135
<u>What are the risks</u>	of opening a port?
Change scope	OK Cancel

3 DCOM-Konfiguration

DCOM-Konfiguration

In DCOM können Sie zwischen "machine default" (Maschinenvoreinstellung) und "each server" (jeder Server) wählen.

Bei Verwendung von OPC über DCOM erfolgt die Konfiguration am einfachsten über die "machine default".

Die im Folgenden aufgeführten Einstellungen müssen sowohl client-, als auch serverseitig erfolgen.

4

4 DCOM-Konfiguration als "Machine Default"

DCOM-Konfiguration als "Machine Default" (Maschinen-Standardeinstellungen)

Um die Maschinen-Standardeinstellungen in DCOM für die OPC-Kommunikation in Windows XP SP3 zu konfigurieren, gehen Sie wie folgt vor:

1. Wählen Sie Start -> Run, geben Sie "DCOMCnfg" ein und klicken Sie dann auf OK.

Run	? 🔀
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	DCOMCnfg
	OK Cancel Browse
🐮 sta	art 🛛 😂 🕲 😒

- 2. Klicken Sie unter "Console Root" auf "Component Services", um die Unterverzeichnisse anzuzeigen.
- 3. Klicken Sie im Verzeichnis "Component Services" auf "Computers".
- 4. Klicken Sie im rechten Fenster mit der rechten Maustaste auf "My Computer" und wählen Sie das Menü "Properties".



5. Wählen Sie den Reiter "COM Security" und achten Sie auf die vier zu bearbeitenden Zugriffsberechtigungen:

General	Options	Default Properties
Default Protocols	MSDTC	COM Security
Access Permissions You may edit who is also set limits on ap	s allowed default acces plications that determin	s to applications. You may e their own permissions.
	Edit <u>L</u> imits	<u>E</u> dit Default
You may edit who is activate objects. Yo determine their own	s allowed by default to l ou may also set limits or i permissions.	aunch applications or applications that
You may edit who is activate objects. Yo determine their own	s allowed by default to I ou may also set limits or opermissions. Edit Limits	aunch applications or applications that Edit <u>D</u> efault
You may edit who is activate objects. Yo determine their own	s allowed by default to l ou may also set limits or permissions. Edit Limits	aunch applications or applications that Edit <u>D</u> efault

Bearbeiten der Zugriffs- und Startbeschränkungen :

• Access Permissions (Zugriffsberechtigungen)

Falls noch nicht vorhanden, tragen Sie die Benutzer "Administrators" und "Everyone" ein. "Remote access" und "Local access" muss für alle Benutzer aktiviert sein.

curity Limits		
roup or user names:		
ANONYMOUS LOGON		
ermissions for ANDNYMOUS	Add	<u>R</u> emove
Local Access		
Remote Access		

Launch and Activation Permissions (Start- und Aktivierungsberechtigungen)
 Falls noch nicht vorhanden, fügen Sie die Benutzer "Administrators" und "Everyone" ein.
 "Remote access" und "Local access" muss für alle Benutzer aktiviert sein.

Hinweis Beim Einsatz von Windows 7 muss der Benutzer explizit in die Sicherheitseinstellungen des "OPC.Simatic.HMI.HmiRTm" eingetragen werden.

Die Konfiguration der DCOM-Einstellungen muss für jeden beteiligten PC vorgenommen werden.

nch Permission		?
ecurity Limits		
àroup or user names:		
🕵 Administrators (WINXP-2	VAdministrators)	
Everyone		
	Add	Remove
ermissions for Everyone	Allow	 Deny
Local Launch		
Remote Launch		
Local Activation	×	
Bemote Activation		
Remote Activation		

Bearbeiten der standardmäßigen Zugriffs- und Startberechtigungen:

• Access Permissions (Zugriffsberechtigungen)

Falls noch nicht vorhanden, fügen Sie die Benutzer "Administrators" und "Everyone" ein.

Stellen Sie sicher, dass die Kontrollkästchen "Local Allow" und "Remote Allow" für jeden Teilnehmer (oder Teilnehmergruppe) der OPC-Kommunikation (z.B. .OPC-User) aktiviert sind.

Zugriffsberechtigungen für jeden Benutzer:

Permissions for Everyone	Allow	Deny
Local Access	 Image: A start of the start of	
Remote Access	✓	

Start- und Aktivierungsberechtigungen

Falls noch nicht vorhanden, fügen Sie die Benutzer "Administrators" und "Everyone" ein.

Stellen Sie sicher, dass die Kontrollkästchen "Local Allow" und "Remote Allow" für jeden Teilnehmer (oder Teilnehmergruppe) der OPC-Kommunikation (z.B. .OPC-User) aktiviert sind.

Permissions for Everyone	Allow	Deny
Local Launch	\checkmark	
Remote Launch	\checkmark	
Local Activation	~	
Remote Activation	~	

Start- und Aktivierungsberechtigungen für alle Benutzer: