SIEMENS

SIGUARD PDP
Phasor Data Processing

V2.10

Administrator-Handbuch

E50417-H1000-C496-A1

HINWEIS

Bitte beachten Sie zu Ihrer eigenen Sicherheit die Warn- und Sicherheitshinweise in diesem Handbuch.

Dokumentversion: V1.00

Ausgabestand: 11.2011

Version des beschriebenen Produkts: V2.10

Vorwort

Zweck des Handbuchs

Dieses Handbuch ist eine Anleitung zur Software SIGUARD PDP. Sie erhalten einen Überblick über die Einsatz- und Konfigurationsmöglichkeiten.

Zielgruppe

Dieses Handbuch wendet sich vorzugsweise an das Betriebspersonal, Inbetriebnehmer und Qualitätsmanager, die für die Konfiguration, Parametrierung und Überwachung von Energienetzen und deren Komponenten zuständig sind.

Gültigkeitsbereich des Handbuchs

Dieses Handbuch ist gültig für SIGUARD PDP V2.10.

Normen

Die Entwicklung von SIGUARD PDP wurde nach den Richtlinien der DIN EN ISO 9001:2008 durchgeführt.

Weitere Unterstützung

Bei Fragen zum System wenden Sie sich an Ihren Siemens-Vertriebspartner.

Support

Unser Customer Support Center unterstützt Sie rund um die Uhr.

Tel.: +49 (1805) 24-7000

Fax: +49 (1805) 24-2471

E-Mail: support.energy@siemens.com

Schulung

Sie können das individuelle Kursangebot bei unserem Training Center erfragen:

Siemens AG

Siemens Power Academy

Humboldtstraße 59

90459 Nürnberg

Tel.: +49 (911) 433-7415

Fax: +49 (911) 433-7929

E-Mail: power-academy.energy@siemens.com

Internet: http://www.siemens.com/energy/power-academy

Hinweise zu Ihrer Sicherheit

Dieses Handbuch ist kein vollständiges Verzeichnis aller für einen Betrieb des Betriebsmittels (Baugruppe, Gerät) erforderlichen Sicherheitsmaßnahmen. Es enthält aber Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise sind je nach Gefährdungsgrad wie folgt dargestellt:

GEFAHR

GEFAHR bedeutet, dass Tod oder schwere Verletzungen eintreten **werden**, wenn die angegebenen Maßnahmen nicht getroffen werden.

✧ Beachten Sie alle Hinweise, um Tod oder schwere Verletzungen zu vermeiden.

WARNUNG

WARNUNG bedeutet, dass Tod oder schwere Verletzungen eintreten **können**, wenn die angegebenen Maßnahmen nicht getroffen werden.

✧ Beachten Sie alle Hinweise, um Tod oder schwere Verletzungen zu vermeiden.

VORSICHT

VORSICHT bedeutet, dass mittelschwere oder leichte Verletzungen eintreten **können**, wenn die angegebenen Maßnahmen nicht getroffen werden.

✧ Beachten Sie alle Hinweise, um mittelschwere oder leichte Verletzungen zu vermeiden.

ACHTUNG

ACHTUNG bedeutet, dass Sachschäden entstehen **können**, wenn die angegebenen Maßnahmen nicht getroffen werden.

✧ Beachten Sie alle Hinweise, um Sachschäden zu vermeiden.

HINWEIS

ist eine wichtige Information über das Produkt, die Handhabung des Produktes oder den jeweiligen Teil der Dokumentation, auf den besonders aufmerksam gemacht werden soll.

Inhaltsverzeichnis

1 Übersicht

1.1 Allgemeines

Dieses Handbuch richtet sich an den Systemadministrator beim Betreiber des SIGUARD PDP-Systems. Es beschreibt den Netzwerkaufbau und gibt Hinweise zur Verbesserung der Sicherheit im Netzwerk.

Das Handbuch besteht aus folgenden Hauptteilen:

- Allgemeine Regeln für Systemsicherheit
- Hinweise für Netztopologie
- Installation der SIGUARD PDP-Komponenten
- Zeitsynchronisation
- Details zur Sicherheitseinstellung

1.2 Empfohlene Maßnahmen, die Ihr System sicherer machen

Um Ihr SIGUARD-System sicherer zu machen, beachten Sie folgende Punkte:

- Legen Sie eine Liste der Dienste (Ports und Protokolle) an, die im IT-System verwendet werden. Diese Liste können Sie dazu verwenden, die Firewall in Ihrem System zu konfigurieren.
- Folgen Sie der Empfehlung, die Windows-Desktop Firewall zu aktivieren und richten Sie sich nach der Beschreibung, welche Ports für eingehenden Datenverkehr geöffnet werden müssen.
- Deaktivieren Sie alle nicht benötigten Dienste, z.B. **File and Printer sharing for Microsoft networks**.
- Legen Sie eine spezielle Windows-Benutzergruppe **Users** für Ihr installiertes Programm an. Nur diese Benutzergruppe darf die Berechtigung zum Starten des entsprechenden Programms und zum Navigieren zu den Ordner besitzen. Dieser Benutzergruppe darf nur Lesezugriff für die gemeinsamen Ordner des SIGUARD PDP Servers eingeräumt werden.
- Legen Sie Benutzer an, die Mitglieder der Windows-Benutzergruppe **Users** und der definierten Benutzergruppe, z.B. **SIGUARD PDP Engineer** sind.

  Verwenden Sie kein Administrator-Benutzerkonto für das normale Arbeiten mit dem Rechner.

  Nur die definierten Benutzer dürfen berechtigt sein, das installierte Programm zu benutzen, nicht aber normale Windows-Benutzer. Diese Vorgehensweise gewährleistet einen hohen Grad an Sicherheit und vermeidet das Eindringen von Schad-Software, wie fremden DLL- oder EXE-Dateien.
- Wenn ein direkter Zugang zum Internet besteht, aktivieren Sie immer die automatische Update-Funktion von Windows und aktualisieren Sie alle Software-Produkte von Fremdherstellern, wie z.B. Adobe Acrobat Reader oder die Oracle-Java Runtime-Umgebung. Viele andere Programme bieten einen automatischen Update-Service an. Wenn kein direkter Zugang zum Internet besteht, können Sie die Software per Hand aktualisieren oder Sie führen WSUS (Windows Server Update Service) ein.
- Um das Eindringen von Schad-Software über Speichermedien (CD-ROM, USB-Stick u.a.) oder über gemeinsame Datennutzung zu vermeiden, installieren Sie auf Ihrem System einen freigegebenen Viren-Scanner mit der Einstellung **on access**.

  Wenn ein direkter Zugang zum Internet besteht, dann beachten Sie, dass nur eine Viren-Software mit täglich aktualisierten Virensignaturen einen hohen Grad an Sicherheit gewährleistet. Für alle Systeme müssen die Virensignaturen automatisch oder manuell zur Verfügung gestellt werden.
- Um die Vollständigkeit und die Diskretion der übertragenen Daten zwischen der Benutzeroberfläche und dem SIGUARD PDP Server zu gewährleisten, können die Daten verschlüsselt werden. Hierfür wird die in Windows implementierte IPSec-Funktion verwendet, um die Datenübertragung sicherer zu gestalten.

  Weitere Informationen hierzu erhalten Sie in den Kapiteln *7.5.2.1 Allgemeines* und *7.5.1.1 Allgemeines*.
- Um mit anderen Partnern zu kommunizieren, verwenden Sie die in Windows integrierte IPSec-Lösung für eine sichere und authentisierte Datenverbindung bei Verwendung von einfachen Textprotokollen. Wenn Sie eine Firewall verwenden, geben Sie das IPSec-Protokoll frei (ESP/UDP-Port 500 oder UDP-Port 4500/UDP-Port 500).

  Weitere Informationen hierzu erhalten Sie in den Kapiteln*7.5.1.1 Allgemeines* und *7.5.2.1 Allgemeines*.
- Sichern Sie die Engineering-Daten mit dem **Windows-Task Scheduler** regelmäßig auf einem externen Laufwerk oder in einem gemeinsam genutzten Ordner. Somit ist sichergestellt, dass bei einem Systemausfall die Engineering-Daten ohne oder nur mit geringfügigem Datenverlust wiederhergestellt werden können.
- Sammeln und speichern Sie Protokolldateien innerhalb eines bestimmten Zeitraumes. Mit dem von Windows zur Verfügung gestellten **Remote Registry Service** erfolgt der Fernzugriff auf die Protokolldateien des SIGUARD PDP Servers. Zum Einsatz kommt der **Event Viewer**, ein Standard-Programm von Microsoft.

1.3 Empfohlene Regeln zur Verbesserung des Sicherheitsprozesses

Um den Sicherheitsprozess für Ihr SIGUARD-System zu verbessern, beachten Sie folgende Regeln:

- Benutzen Sie niemals das Windows-Benutzerkonto **Gast**. Deaktivieren Sie immer dieses Benutzerkonto!
- Erlauben Sie Zugriff nur wenn unbedingt notwendig und auch nur für die entsprechenden Benutzergruppen. Löschen Sie die Gruppe für diese Zugriffsrechte und fügen Sie die richtige Benutzergruppe hinzu. Stellen Sie die Lese-/Schreibrechte mit der **Security-Funktion** ein.
- Benutzen Sie für das normale Arbeiten an Ihrem Rechner kein Benutzerkonto, das zur Administrator-Gruppe gehört.
- Verwenden Sie keine einfachen Passwörter für das Benutzerkonto. Beachten Sie die in Ihrem Unternehmen gültigen Regeln für Passwörter.
- Ändern Sie, wenn möglich, Ihr Passwort in regelmäßigen Abständen.
- Arbeiten Sie nicht mit Windows ohne die Desktop-Firewall zu aktivieren, außer Sie haben Ihr System in einer zuverlässigen, begrenzten Sicherheitszone installiert.
- Arbeiten Sie nur dann mit einem mit Patches aktualisierten Windows, wenn Ihr System nicht in einer zuverlässigen, begrenzten Sicherheitszone installiert ist.
- Arbeiten Sie nicht mit Windows, auf dem kein aktueller Viren-Scanner installiert ist, außer Sie haben Ihr System in einer zuverlässigen, begrenzten Sicherheitszone installiert.
- Benutzen Sie, wenn immer möglich, keine Software aus dritter Hand mit bekannten Sicherheitslücken. Falls erforderlich, richten Sie eine zuverlässige, begrenzte Sicherheitszone ein.
- Installieren Sie keine unzuverlässige Software auf dem System, mit dem Sie arbeiten.

■

2 Netzwerktopologie

2.1 Übersicht

In diesem Kapitel erhalten Sie eine Übersicht über die Konfiguration bezüglich Sicherheit im SIGUARD-Netzwerk. Das SIGUARD-Netzwerk ist kein eigenständiges Netzwerk, sondern ein verteiltes System. Das System ist mit unterschiedlichen Netzwerkzonen verbunden, die unterschiedliche Sicherheitsvoraussetzungen erfüllen müssen.

Aus diesem Grund empfiehlt Siemens, das hier beschriebene Konzept für Sicherheitsnetzwerke umzusetzen. Wenn Sie eigene, begrenzte Sicherheitszonen mit strengen Sicherheitsbedingungen definiert haben, können gegebenenfalls ein oder 2 Sicherheitstunnel oder -mechanismen weggelassen werden.

2.2 Netzwerkkonfiguration

Das folgende Bild zeigt ein Beispiel einer Netzwerkkonfiguration des SIGUARD-Systems. Im Normalfall sind die PMUs auf Stationsebene landesweit verteilt. Eine Trennung zwischen dem SIGUARD PDP Server, dem SIGUARD PDP UI-Rechner und dem SIGUARD PDP Engineer-Rechner ist möglich. Alternativ kann die Konfiguration aus einem System auf Büroebene mit einer gemeinsamen UI- und Engineer-Umgebung bestehen.

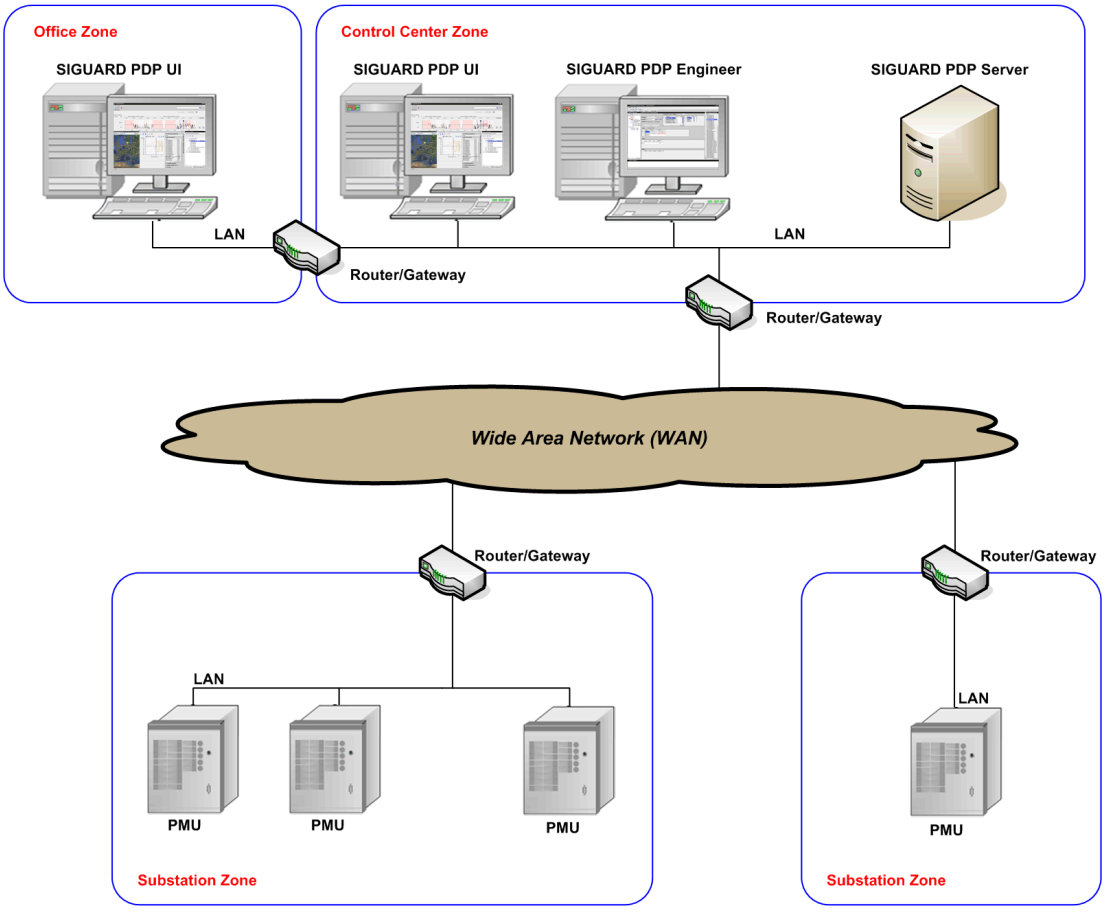

Bild 2-1 Netzwerkkonfiguration (Beispiel)

2.3 Netzwerkkonfiguration mit IPSec

Durch diese Konfiguration erreichen Sie einen komplett verschlüsselten Datenverkehr:

- Zwischen den Programmen SIGUARD PDP UI, SIGUARD PDP Engineer und dem SIGUARD PDP Server
- Zwischen der PMU und dem SIGUARD PDP Server

Bei vielen PMUs wird IPSec nicht direkt in der Gerätekommunikation unterstützt. Deshalb wird eine zusätzliche Hardware, das **Siemens Scalance S Security Module**, benötigt. Sie können die Scalance S Security Module einfach konfigurieren und bedienen. Die anderen Sicherheits-Tunnel sind über eine Windows-eigene Anwendung konfigurierbar.

Weitere Informationen zur Konfiguration erhalten Sie im Kapitel *7.5.1.2 IPSec-Konfiguration*.

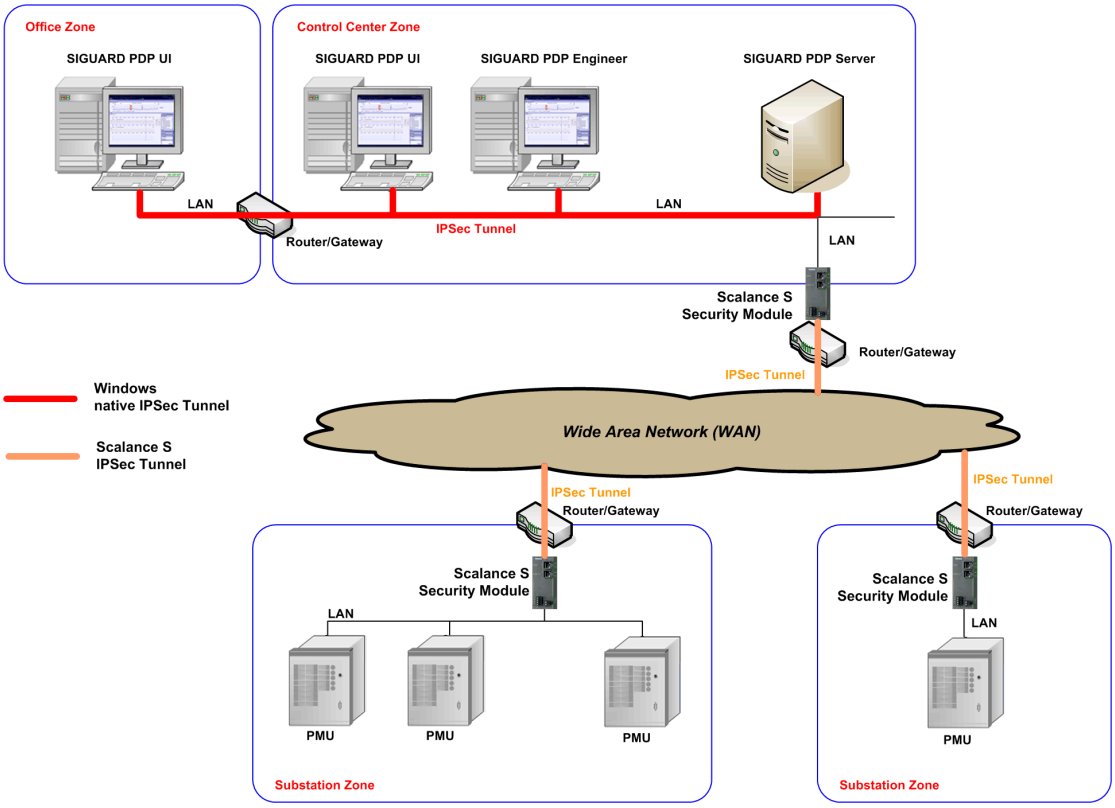

Bild 2-2 Netzwerk mit Windows-native IPSec-Tunnel und Security Module Scalance S

2.4 Kommunikationsprotokolle für den Einsatz einer Firewall

Nachfolgend sind die Dienste aufgelistet, die bei einem externen Zugriff vom SIGUARD PDP Engineer/UI-Rechner auf den SIGUARD PDP Server verwendet werden. Beachten Sie, dass der Microsoft-Network Discovery Service optional ist. Wenn Sie keinen Browser benötigen, deaktivieren Sie diesen Dienst über die Funktion **Services** und/oder über **Microsoft Desktop Firewall**.

HINWEIS

Beachten Sie, dass die TCP-Kommunikation zwischen SIGUARD PDP Server und PMU über SIGUARD PDP Engineer frei definierbar ist. Die TCP-Kommunikation ist nur eine ausgehende Verbindung vom SIGUARD PDP Server.

Tabelle 2-1 Kommunikationsmatrix

Service	Layer 4-Protokoll	Layer 7-Protokoll	Vom Host (Client)	Vom Port (Client)	Zum Host (Server)	Zum Port (Server)
Microsoft-Network Discovery	TCP	Microsoft-Network Browsing (http) Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	SIGUARD PDP Engineer/UI-Rechner		SIGUARD PDP Server	5357
SIGUARD Service-Schnittstelle	TCP	SIGUARD Service-Schnittstelle	SIGUARD PDP Engineer/UI-Rechner	> 1024	SIGUARD PDP Server	59152
File Sharing	TCP	netbios-ssn	SIGUARD PDP Engineer/UI-Rechner	> 1024	SIGUARD PDP Server	139
File Sharing	TCP	netbios-ssn	SIGUARD PDP Engineer/UI-Rechner	> 1024	SIGUARD PDP Server	445
PMU-Protokoll (C37.118)	TCP	PMU-Protokoll (C37.118)	SIGUARD PDP Server	> 1024	PMU	frei definierbar

■

3 SIGUARD PDP Systeminstallation

3.1 Installationsvoraussetzungen

3.1.1 Hardware

Bei einem SIGUARD-System werden folgende Anforderungen bezüglich der Hardware gestellt:

Tabelle 3-1 Anforderungen an die SIGUARD-Hardware

Hardware		**Mindestanforderungen**	**Empfohlene Anforderungen**
SIGUARD PDP Server	Prozessor	Dual Core	Quad Core
	Taktfrequenz	2,0 GHz	≥ 2,5 GHz
	Arbeitsspeicher (32-Bit-Betriebssystem)	2 GB	4 GB
	Freie Festplattenkapazität	4 GB (Betriebssystem) Archiv siehe unten	
	Grafikkarte	Standardgrafikkarte	DirectX V9.0c-kompatibel
	USB-Port	USB 2.0	
	Netzwerkschnittstelle	100 MBit/s	1 GBit/s
SIGUARD UI-Rechner	Prozessor	Dual Core	Quad Core
	Taktfrequenz	2,0 GHz	≥ 2,5 GHz
	Arbeitsspeicher (32-Bit-Betriebssystem)	2 GB	4 GB
	Arbeitsspeicher (64-Bit-Betriebssystem)	4 GB	8 GB
	Freie Festplattenkapazität	10 GB (UI, Google Earth)	
	Grafikkarte	DirectX V9.0c-kompatibel	
SIGUARD PDP Engineer-Rechner	siehe SIGUARD UI-Rechner		

Speicherplatz für das Archiv

Für die schnellere Bearbeitung des Archivs (speichern, öffnen) sollten das Permanentarchiv und das Ringarchiv auf 2 getrennten physikalischen Festplatten abgelegt werden.

Der Speicherplatzbedarf muss entsprechend den folgenden Bedingungen zur Verfügung gestellt werden:

Tabelle 3-2 Anforderungen an die SIGUARD-Hardware

Hardware		**Mindestanforderungen**	**Empfohlene Anforderungen**
Ringarchiv		bei folgenden Randbedingungen	
	PMUs/mit je 8 Kanäle	8	14
	Kanäle	64	112
	Wiederholrate (Werte/Sekunde)	10	10
	Speicherzeitraum	7 Tage	7 Tage
	Freie Festplattenkapazität	**ca. 14 GB**	**ca. 25 GB**

Für die Speicherung von Ereignissen, Warnmeldungen und Zeitbereichen ist eine zusätzliche Festplattenkapazität erforderlich.

3.1.2 Software

Betriebssystem

Nachfolgende Betriebssysteme werden unterstützt:

Tabelle 3-3 Unterstützte Betriebssysteme

Betriebssystem	**SIGUARD-Rechner**		
	SIGUARD PDP Server	**SIGUARD PDP UI-Rechner**	**SIGUARD PDP Engineer-Rechner**
Windows XP Professional SP3 (32-Bit)	X	X	X
Windows 7 Professional (32-Bit)	X	X	X
Windows 7 Professional (64-Bit)		X	X
Windows Server 2008 Standard Edition (32-Bit)	X		

Sonstige Software-Voraussetzungen

Installieren Sie **Google Earth** Version 6.0 (getestet wurde die Version V 6.0.3.21790).

HINWEIS

Beachten Sie die Lizenzbedingungen der Open Source Software, die bei SIGUARD PDP verwendet wird.

Im Wurzelverzeichnis der SIGUARD PDP Installations-DVD finden Sie dazu das PDF-Dokument **ReadMe_OSS.pdf.**

3.2 Installation der Software

3.2.1 Übersicht

Über ein Installationsprogramm richten Sie SIGUARD PDP auf Ihrem Rechner ein. Beim Installieren übertragen Sie alle erforderlichen Daten auf Ihren Rechner:

- SIGUARD PDP
- Automation License Manager
- Service Controller Tool

Um SIGUARD PDP nutzen zu können, lizenzieren Sie SIGUARD PDP nach der Installation über den Automation License Manager (siehe Handbuch *Automation License Manager*).

Die Installation der Software-Komponenten **OPC** und **ICCP** erfolgt mit dem Setup von SIGUARD PDP und für ICCP mit einem zusätzlichen Software-Add-on. Die Lizenzierung erfolgt für jede Softwarekomponente separat.

Hinweise zur Installation der Software-Komponenten finden Sie in den entsprechenden Kapiteln im *Administrator-Handbuch*.

HINWEIS

Sie können SIGUARD PDP und ICCP Add-on in beliebiger Reihenfolge installieren.

3.2.2 Installation

Installation starten

So installieren Sie SIGUARD PDP:

✧ Legen Sie die DVD **SIGUARD PDP** in das DVD-Laufwerk ein.

Der Installationsvorgang wird automatisch gestartet.

Wenn der Installationsvorgang nicht automatisch startet, doppelklicken Sie auf die Datei **Setup.exe** im Wurzelverzeichnis der DVD.

✧ Folgen Sie den Anweisungen der Installationsroutine.

Installationstyp

Während der Installation müssen Sie den **Installationstyp** festlegen.

HINWEIS

In einem SIGUARD PDP-System muss immer 1 Server vorhanden sein. An diesem Server können bis zu 8 SIGUARD PDP UI betrieben werden.

HINWEIS

Der SIGUARD PDP Engineer wird bei SIGUARD PDP UI mitinstalliert. Für den SIGUARD PDP Engineer besteht keine separate Installationsmöglichkeit.

- ✧ Installieren Sie bei einem SIGUARD PDP-System, das aus mehreren Rechnern besteht, zuerst den SIGUARD PDP Server.
- ✧ Wählen Sie zwischen den Installationstypen **Server** und **UI Client**.

Wenn Sie ein SIGUARD PDP UI installieren, geben Sie während der Installation den Rechnernamen ein, auf dem der SIGUARD PDP Server installiert ist.

- ✧ Wenn Sie einen SIGUARD PDP Server installieren, markieren Sie die Softwarekomponenten **OCP** und/oder **ICCP**, wenn Sie diese mitinstallieren wollen.

HINWEIS

Wenn Sie ein verteiltes System (1 Server, mehrere UI-Rechner) betreiben wollen, müssen Sie auf dem Server die Shares **\\<Rechnername>\SIGUARD_Config** und **\\>Rechnername>\SIGUARD_Export** einrichten. Vergeben Sie die Rechte gemäß Ihren Unternehmensrichtlinien.

- ✧ Legen Sie während der Installation den Pfad und das Verzeichnis für die SIGUARD PDP fest.
- ✧ Legen Sie den Pfad für das Programm fest.
- ✧ Legen Sie den Pfad für die Konfigurationsdatei fest.
- ✧ Legen Sie die CSV-Datei fest.

HINWEIS

Siemens empfiehlt, das Ring- und das Permanentarchiv auf separaten Festplatten zu speichern.

- ✧ Legen Sie den Pfad für das Ringarchiv fest.
- ✧ Legen Sie den Pfad für das Permanentarchiv fest.

Rechner neu starten

- ✧ Starten Sie den Rechner nach der Installation neu.

3.2.3 SIGUARD PDP lizenzieren

3.2.3.1 Lizenzierung vorbereiten

Durch die Übertragung der Lizenz von einem oder mehreren Lizenz-USB-Stick(s) auf Ihren Rechner mit dem Automation License Manager (ALM) lizenzieren Sie das Produkt SIGUARD PDP (siehe Handbuch *Automation License Manager*).

Individuelle Lizenzen sind für alle SIGUARD PDP-Komponenten oder -Applikationen erforderlich. Die Lizenz-Schlüssel (License Keys) werden ausschließlich auf dem SIGUARD PDP Server verwaltet, d.h. dort muss der ALM installiert sein, und dort werden die Lizenzen vom SIGUARD PDP Server abgefragt.

Während der Laufzeit fragt der SIGUARD PDP Server die Lizenzen ab und stellt nur dann eine Verbindung zum SIGUARD PDP UI-Rechner her, wenn die entsprechende Lizenzierung vorhanden ist. Zusätzlich wird über die Lizenzierung geprüft, wie viele SIGUARD PDP UI-Rechner am SIGUARD PDP Server betrieben werden dürfen.

HINWEIS

Auf einem Rechner mit Lizenzverwaltung (SIGUARD PDP Server) dürfen Sie keine Programme ausführen, die die Aufteilung oder Struktur der Festplatten verändern.

Dazu zählen Programme zur Festplattenwartung, wie z.B. Reparatur, Defragmentierung, Partitionierung.

Wenn Sie derartige Programme verwenden, riskieren Sie den Verlust Ihrer Lizenz-Schlüssel!

Um dies zu verhindern, müssen Sie die Lizenz-Schlüssel vorübergehend wieder auf den Lizenz-USB-Stick übertragen (siehe auch *3.3.2 SIGUARD PDP-Lizenzierung entfernen*).

HINWEIS

Wenn kein Zugriff auf eine USB-Schnittstelle des SIGUARD PDP Servers, auf den die Lizenzen kopiert werden müssen, möglich ist, dann müssen die Lizenzen zunächst auf dem SIGUARD PDP UI-Rechner installiert werden. Dazu installieren Sie den Automation License Manager (ALM) auf dem SIGUARD PDP UI-Rechner. Im Wurzelverzeichnis der DVD liegt ein Link auf das Setup des ALM.

Wenn die Lizenzen auf dem SIGUARD PDP UI-Rechner installiert sind und eine Netzwerkverbindung zum SIGUARD PDP Server besteht, können sie mit dem ALM vom SIGUARD PDP UI-Rechner zum SIGUARD PDP Server übertragen werden.

Ein Zugriff vom ALM, der auf einem SIGUARD PDP Server installiert ist, auf einen USB-Stick eines über eine Terminal-Sitzung verbundenen Rechner ist nicht möglich.

ACHTUNG

Im Ordner **C:\AX NF ZZ** sind verborgene Dateien enthalten. Sie dürfen diese Dateien und Ordner nicht löschen, verschieben oder kopieren. Sie beinhalten Daten, die zur Lizenzierung Ihrer Software benötigt werden!

Bei Nichtbeachtung besteht die Gefahr, dass die Lizenzierung unwiderruflich verloren geht. Um die Lizenzierung nicht unwiederbringlich zu verlieren, beachten Sie die folgenden Punkte:

- Wenn Sie ein Optimierungsprogramm (z.B. Scandisk/Defrag) verwenden, das die Möglichkeit anbietet, feste Blöcke zu verschieben, so dürfen Sie diese Option nur verwenden, wenn Sie vorher die Lizenzen von der Festplatte auf den Lizenz-USB-Stick zurückübertragen.
- Mit der Lizenzierung entsteht auf dem Ziellaufwerk ein als defekt gekennzeichneter Cluster. Versuchen Sie nicht, diesen wiederherzustellen.
- Beim Überschreiben eines Systems mit hinterlegten Lizenzen (das ist in der Regel der SIGUARD PDP Server, kann aber auch ein anderer Rechner mit dort abgelegen Lizenzen sein) mit einem Backup besteht die Gefahr eines Lizenzverlustes. Daher empfiehlt Siemens, vor dem Anlegen einer Sicherungskopie alle Lizenzen zu entfernen oder den Ordner **C:\AX NF ZZ** aus der Sicherung auszuschließen.

HINWEIS

Es besteht die Gefahr, dass ein Virenaustausch von Festplatten zum Lizenz-USB-Stick stattfindet. Überprüfen Sie deshalb vor jeder Installation/Deinstallation einer Lizenz Ihren Rechner auf Virenfreiheit.

3.2.3.2 Lizenzierung ausführen

So lizenzieren Sie SIGUARD PDP:

- ✧ Stecken Sie den mitgelieferten Lizenz-USB-Stick in die USB-Schnittstelle des SIGUARD PDP Servers.
- ✧ Klicken Sie auf **Start > Programme > Siemens Automation > Automation License Manager**.
- ✧ Übertragen Sie die Lizenz vom Lizenz-USB-Stick auf die Festplatte des SIGUARD PDP Servers.

HINWEIS

Wenn Sie mehrere Lizenz-USB-Sticks erhalten haben, dann wiederholen Sie diese Schritte.

3.2.4 SIGUARD PDP parametrieren

Nach der Installation und Lizenzierung legen Sie mit dem Tool **SIGUARD PDP Engineer** ein neues Projekt an, parametrieren und aktivieren es.

Sie können auch ein bestehendes Projekt um Funktionalitäten erweitern.

Hinweise siehe Handbuch *SIGUARD PDP - SIGUARD PDP Engineer - Leistungsmerkmale*.

3.2.5 SIGUARD PDP starten

3.2.5.1 Übersicht

Nach der Parametrierung und Aktivierung eines neuen Projektes muss vom Administrator auf dem SIGUARD PDP Server das **Service Controller Tool** geöffnet und die von **SIGUARD PDP** benötigten Dienste installiert und gestartet werden.

Das **Service Controller Tool** muss nach der Neuinstallation des SIGUARD PDP Servers ausgeführt werden. Für die Ausführung des Tools sind Administratorrechte auf dem SIGUARD PDP Server erforderlich.

Hierfür siehe auch *Administrator-Handbuch - Service Controller Tool*.

Anschließend kann im Diagnose-Tool **Communication UI** geprüft werden, ob alle Verbindungen zwischen SIGUARD PDP Server und PMUs korrekt aufgebaut wurden und ob Fehler aufgetreten sind.

Hierfür siehe auch *Administrator-Handbuch - Diagnose-Tool Communication UI*.

3.2.5.2 Konfigurationsdatei bearbeiten

Wenn die SIGUARD PDP-Software auf einem verteilten System installiert ist (SIGUARD PDP Server und UI-/Engineer-Rechner getrennt), dann müssen Sie die IP-Adresse des Servers in die Konfigurationsdatei eintragen. Dazu gehen Sie wie folgt vor:

- ✧ Öffnen Sie die Konfigurationsdatei **RT/PDP_config.xml** mit einem entsprechenden Text-Editor.
- ✧ Geben Sie anstelle der vorhandenen IP-Adresse die IP-Adresse des SIGUARD PDP Servers ein.

```
<Common>
  <PDP ipAddress="127.0.0.1" port="59152" retentionPeriod="15"
  <Protocol noOfThreads="2" recoveryDelay="5" chatterBlockingD
  <Archive pathToRingBuffer="D:\Siemens Energy\SIGUARD PDP\Arc
    <CacheParameterTable>
      <Cache repRate="-60" duration="60" />
      <Cache repRate="1" duration="19" />
      <Cache repRate="5" duration="18" />
      <Cache repRate="10" duration="17" />
      <Cache repRate="25" duration="16" />
      <Cache repRate="50" duration="15" />
    </CacheParameterTable>
  </Archive>
  <UIApplication instantChartsCycleTimeInMs="200" minLineChart
</Common>
```

Bild 3-1 IP-Adresse ändern

✧ Speichern Sie die geänderte Datei.

3.2.5.3 Service Controller Tool

Das Diagnose-Tool **SIGUARD PDP Service Controller** kann unabhängig von SIGUARD PDP geöffnet werden. Das Starten der Dienste ist aber Voraussetzung für das Starten von SIGUARD PDP.

So starten Sie das **Service Controller Tool**:

✧ Wählen Sie **Start > Siemens Energy > SIGUARD PDP > Service Controller Tool**.

Das Fenster **SIGUARD PDP Service Controller** wird geöffnet.

Bild 3-2 SIGUARD PDP Service Controller, Dienste installieren

✧ Klicken Sie auf die Schaltfläche **Install**, um einen Dienst zu installieren.

-- oder --

✧ Klicken Sie auf die Schaltfläche **Uninstall**, um einen Dienst zu deinstallieren.

Für die Dienste kann ein automatischer Start eingestellt werden.

✧ Klicken Sie auf die Schaltfläche **Start**, um einen Dienst zu starten.

-- oder --

✧ Klicken Sie auf die Schaltfläche **Stop**, um einen Dienst zu beenden.

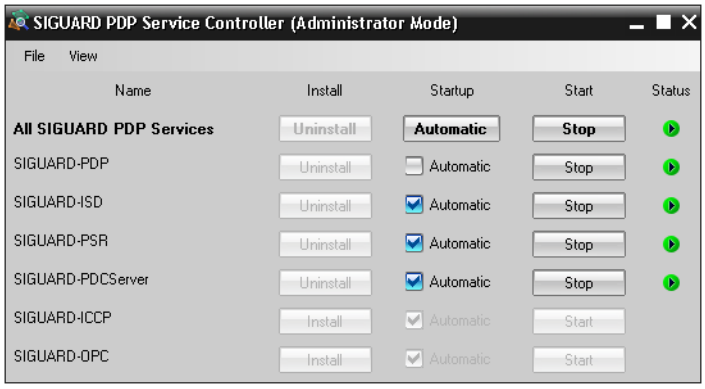

Bild 3-3 Service Controller, Dienste installiert und gestartet

In der letzten Spalte wird der **Status** der Dienste angezeigt:

Tabelle 3-4 Statusanzeigen des Service Controller Tools

Status	Erklärung
	Dieser Status zeigt an, dass dieser Dienst installiert und gestartet wurde.
	Dieser Status zeigt an, dass dieser Dienst gestartet oder gestoppt wurde und die Verarbeitung noch läuft.
	Dieser Status zeigt an, dass dieser Dienst installiert oder gestoppt wurde und eine Aktion (Dienst deinstallieren oder Dienst starten) erwartet wird.

Im nachfolgenden Beispiel einige Dienste gestoppt.

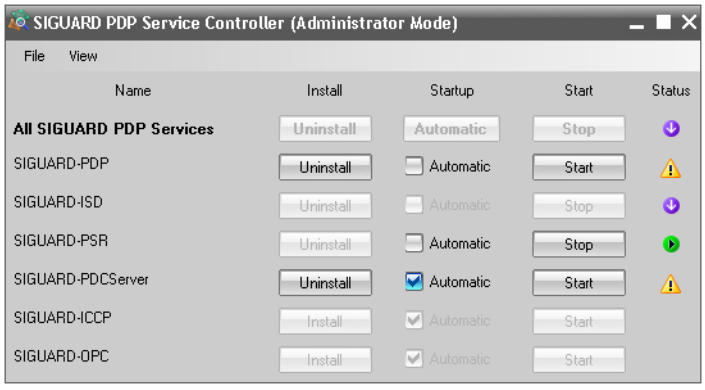

Bild 3-4 Beispiel: Service Controller mit gestoppten Diensten

3.2.5.4 Diagnose-Tool Communication UI

Das **SIGUARD PDP Communication UI** ist ein Diagnosefenster, das nach dem Start von SIGUARD PDP geöffnet werden kann.

Wenn das **SIGUARD PDP Communication UI** vor oder während des SIGUARD PDP Server-Anlaufs gestartet wird, dann wird folgendes Diagnosefenster geöffnet:

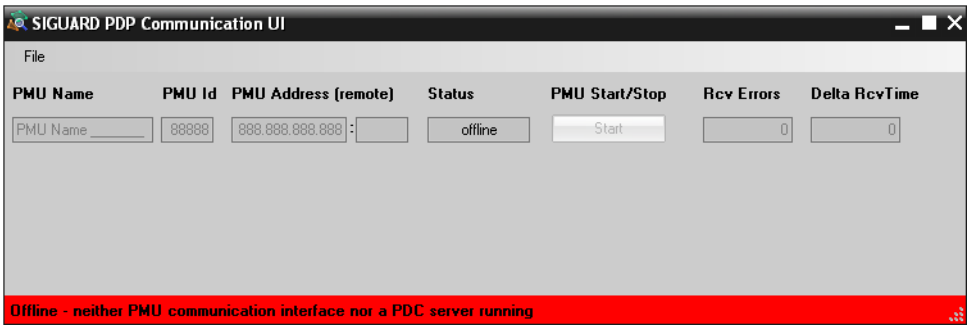

Bild 3-5 Diagnosefenster ohne gestarteten SIGUARD PDP Server

Da noch keine Verbindung zwischen PMU und SIGUARD PDP Server besteht, können keine Diagnosedaten angezeigt werden (Status: **offline**).

Bei gestartetem SIGUARD PDP Server wird das Diagnosefenster mit allen konfigurierten PMU-Verbindungen angezeigt:

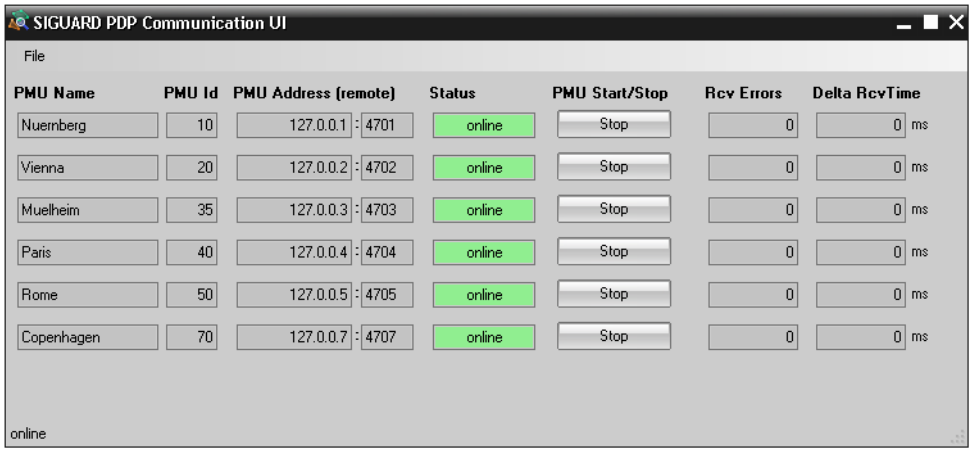

Bild 3-6 Diagnosefenster mit gestartetem SIGUARD PDP Server

Alle konfigurierte PMU-Verbindungen zum SIGUARD PDP Server sind hergestellt (Status: **online**).

Das Diagnosefenster

Im Diagnosefenster wird für jedes PMU-Gerät, das in der Konfiguration angelegt wurde, eine Zeile angelegt. In jeder Zeile werden folgende Parameter aus der Konfiguration übernommen:

- PMU Name
- PMU Id
- PMU Address (remote)

  Die PMU-Adresse besteht aus der IP-Adresse und der Port-Nummer.

Das nächste Feld zeigt den Status der Verbindung zwischen PMU und SIGUARD PDP Server.

Tabelle 3-5 Statusanzeigen des Communication UI

Status	Erklärung
offline	Der Status **offline** zeigt an, dass das Diagnosefenster geöffnet wurde, ohne dass der SIGUARD PDP Server gestartet wurde.
online	Der Status **online** zeigt an, dass eine korrekte Verbindung zwischen PMU und SIGUARD PDP Server besteht, über die Daten ausgetauscht werden.
stopped	Der Status **stopped** zeigt an, dass jegliche Informationsauswertung von dieser physikalischen PMU im SIGUARD-System vom Benutzer, z.B. über die Schaltfläche **Stop** angehalten wurde, da sie z.B. nicht optimal läuft. Nur eine gestoppte PMU kann auch wieder über die Schaltfläche **Start** aktiviert werden.
failure	Der Status **failure** zeigt an, dass die Verbindung zwischen PMU und SIGUARD PDP Server ausgefallen ist oder nicht aufgebaut werden kann.
timestamp err	Der Status **timstamp err** zeigt an, dass die Zeitstempel der empfangenen Telegramme dieser PMU ungültig sind (zu alt, in der Zukunft oder im falschen Raster).
config fail	Der Status **config fail** zeigt an, dass die PMU-eigene Konfiguration mit der Konfiguration aus SIGUARD PDP Engineer nicht übereinstimmt.

Im Feld **Rcv Errors** werden die seit dem Start des SIGUARD PDP Servers aufgetretenen Telegrammfehler (z.B. CRC-Fehler) gezählt. Damit ist eine grobe Aussage über die Qualität der Verbindung möglich.

Im Feld **Delta RcvTime** wird die Differenz der aktuell empfangenen Zeitstempel gegenüber dem jüngsten Zeitstempel ($\Delta = 0$) angezeigt.

Im nachfolgenden Beispiel wird ein **timestamp err** für die PMU Nürnberg angezeigt, da die Differenz des Zeitstempels zur PMU Rom außerhalb der Toleranz liegt (oranger Hintergrund im Feld **Delta RcvTime**). Die Differenz des Zeitstempels zur PMU Mühlheim ist unkritisch (weißer Hintergrund im Feld **Delta RcvTime**).

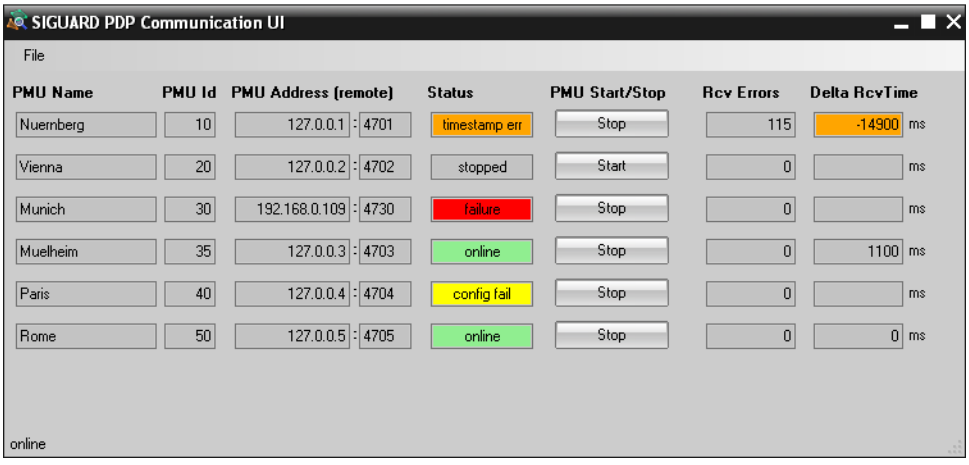

Bild 3-7 Beispiel: Diagnosefenster mit verschiedenen Statusanzeigen

3.3 Deinstallation der Software

3.3.1 SIGUARD PDP deinstallieren

Über das Deinstallationsprogramm des Betriebssystems entfernen Sie SIGUARD PDP von Ihrem Rechner. Dabei löschen Sie alle durch das Installationsprogramm von SIGUARD PDP installierten Daten. Ob das Archiv und die Konfigurationsdateien ebenfalls entfernt werden sollen, können Sie während der Deinstallation entscheiden.

Der **Automation License Manager** und die Diagnose-Software **BMC AppSight Black Box** werden bei der Deinstallation von SIGUARD PDP nicht entfernt. Diese Programme müssen Sie gesondert deinstallieren. Deinstallieren Sie diese Programme nicht, wenn Sie noch von anderer Software benötigt werden.

Deinstallation der Dienste

So deinstallieren Sie die Dienste für SIGUARD PDP:

- ✧ Öffnen Sie das Service Controller Tool mit **Start > Siemens Energy > SIGUARD PDP > Service Controller Tool**
- ✧ Stoppen Sie die Dienste.
- ✧ Deinstallieren Sie die Dienste.
- ✧ Schließen Sie das Service Controller Tool.

Deinstallation von SIGUARD PDP

So deinstallieren Sie SIGUARD PDP:

- ✧ Klicken Sie **Start > Einstellungen > Systemsteuerung**.
- ✧ Öffnen Sie die Liste der installierten Software-Programme.
- ✧ Markieren Sie das Programm **Siemens SIGUARD PDP V2.10** und klicken Sie die Schaltfläche **Entfernen**. Die Deinstallation wird gestartet.
- ✧ Folgen Sie den Anweisungen der Deinstallationsroutine.

HINWEIS

Sollte die Deinstallation bei Windows 7 fehlschlagen, beenden Sie den Dienst **Network Time Protocol** per Hand und wiederholen Sie den Deinstallationsvorgang.

Nach der Deinstallation ist ein Neustart des Rechners erforderlich.

3.3.2 SIGUARD PDP-Lizenzierung entfernen

HINWEIS

Wenn dieselbe Softwareversion von SIGUARD PDP mit einer neuen Softwarekomponente installiert wird, muss die Lizenzierung von SIGUARD PDP nicht entfernt werden.

Durch die Übertragung der Lizenz von Ihrem Rechner auf den Lizenz-USB-Stick entfernen Sie die Lizenzierung.

HINWEIS

Die Lizenz kann auch auf einen anderen Wechseldatenträger, z.B. Fremd-USB-Stick, übertragen werden.

So entfernen Sie die Lizenzierung von SIGUARD PDP:

- ✧ Stecken Sie den mitgelieferten Lizenz-USB-Stick in die USB-Schnittstelle.
- ✧ Klicken Sie **Start > Programme > Siemens Automation > Automation License Manager**.
- ✧ Übertragen Sie die Lizenz oder die Lizenzen von der Festplatte auf den Lizenz-USB-Stick.

■

4 OPC

4.1 Übersicht

OPC ist ein offener Schnittstellenstandard basierend auf der COM- und DCOM-Technologie (Distributed Component Object Model). Dieser Standard ermöglicht einen einfachen, standardisierten Datenaustausch zwischen Automatisierungs-/Steuerungsapplikationen, Feldgeräten und Büroanwendungen.

So können Sie beispielsweise Messwerte von SIGUARD PDP an ein Stationsleitsystem SICAM PAS senden und dort Automatikfunktionen ablaufen lassen, die von den Phasormesswerten gesteuert werden.

Installieren Sie zuerst den **OPC-Server** und konfigurieren Sie den Server anschließend nach Ihren Bedürfnissen.

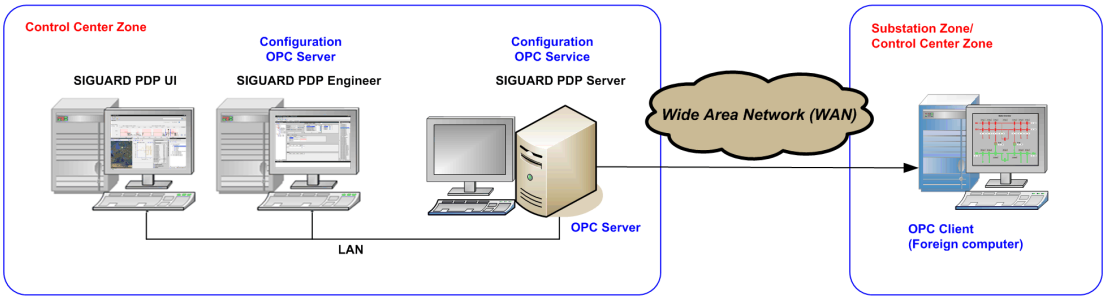

Bild 4-1 Systemübersicht mit OPC-Server

4.2 OPC-Server installieren

So installieren Sie den **OPC-Server**:

- ✧ Deinstallieren Sie SIGUARD PDP, falls schon auf dem Rechner vorhanden.
- ✧ Installieren Sie SIGUARD PDP neu mit der Option **OPC**.

Lizenzierung des OPC-Servers

Die Option **OPC** muss lizenziert werden.

- ✧ Übertragen Sie die Lizenzen vom Lizenz-USB-Stick über den ALM.

4.3 OPC-Server konfigurieren

Bei Verwendung der Funktion **OPC-Server** müssen Sie **SSR** (Service und System Renewal) als Windows-Dienst einrichten und Einstellungen für **DCOM** (Distributed Component Object Model) vornehmen.

Nach der Installation von SIGUARD PDP mit der **OPC**-Option ist der Dienst **SSR** vorhanden. Sie können diesen Dienst wie in den folgenden Abschnitten beschrieben konfigurieren.

Windows-Dienst SSR einrichten

So konfigurieren Sie den Dienst **SSR**:

✧ Öffnen Sie **Services** über **Start > Settings > Control Panel > Administrative Tools > Services**.

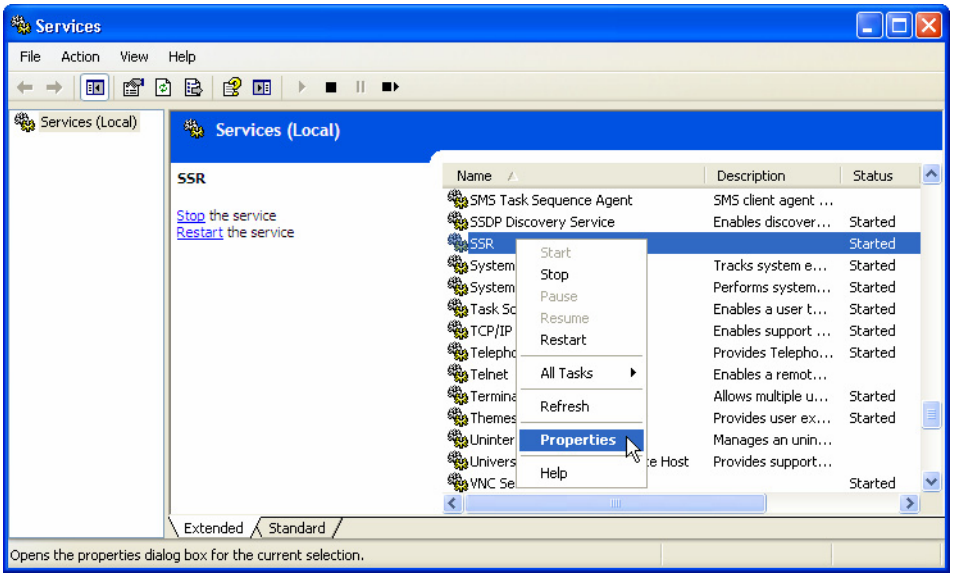

Bild 4-2 Services

✧ Klicken Sie mit der rechten Maustaste auf **SSR** und wählen Sie das Kontextmenü **Properties**.

Der Dialog **SSR Properties** wird geöffnet.

✧ Wählen Sie die Registerkarte **Log On**.

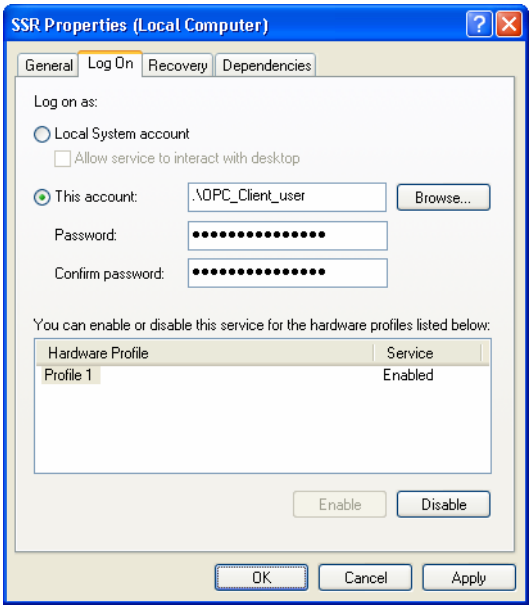

Bild 4-3 Log On

- ✧ Aktivieren Sie **This account**.
- ✧ Tragen Sie hier den Benutzer ein, der beim **OPC-Server** Zugriffsrechte besitzt.
- ✧ Geben Sie ein **Password** und die Bestätigung des Passworts ein.
- ✧ Schließen Sie den Dialog mit **OK**.
- ✧ Schließen Sie das Fenster **Services**.

DCOM konfigurieren

Die Konfiguration von DCOM führen Sie mit dem Microsoft-Werkzeug **dcomcnfg.exe** durch.

So konfigurieren Sie DCOM:

- ✧ Öffnen Sie über **Start > Run** das Fenster **Run**.
- ✧ Geben Sie **dcomcnfg** ein und bestätigen Sie mit **OK**.

Das Fenster **Component Services** wird geöffnet.

- ✧ Klicken Sie mit der rechten Maustaste auf **My Computer** und wählen Sie das Kontextmenü **Properties**.

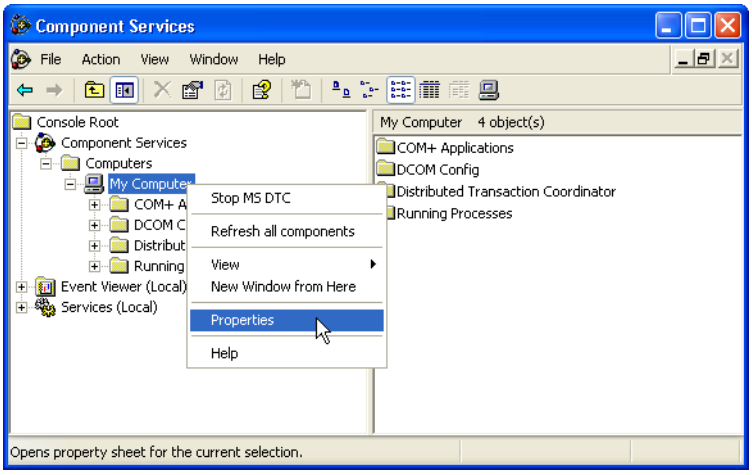

Bild 4-4 Component Services

Das Fenster **My Computer Properties** wird geöffnet.

✧ Wählen Sie die Registerkarte **Default Properties**

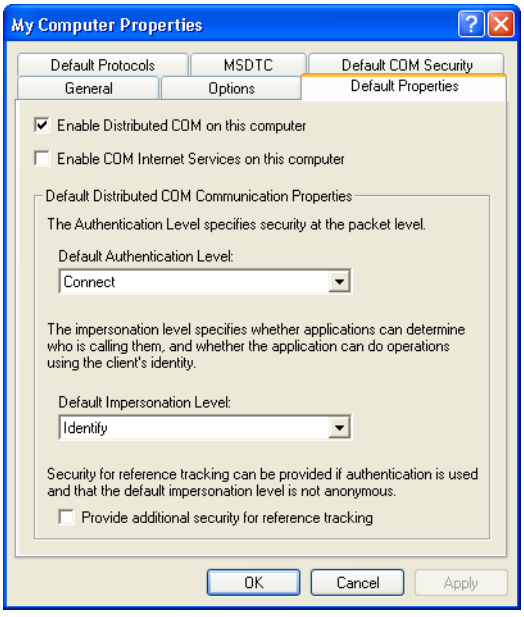

Bild 4-5 Default Properties

✧ Aktivieren Sie **Enable Distributed COM on this computer**.

✧ Wählen Sie unter **Default Authentication Level** die Einstellung **Connect**.

✧ Wählen Sie unter **Default Impersonation Level** die Einstellung **Identify**.

In den übrigen Registerkarten müssen Sie keine Einstellungen vornehmen.

✧ Schließen Sie den Dialog mit **OK**.

✧ Markieren Sie im Fenster **Component Services** unter **My Computer** den Eintrag **DCOM Config**.

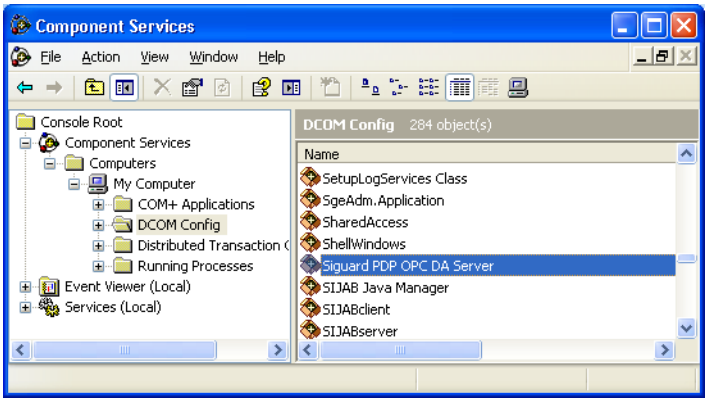

Bild 4-6 Eigenschaften von SIEMENS SIGUARD PDP OPC DA Server öffnen

✧ Klicken Sie mit der rechten Maustaste auf **SIEMENS SIGUARD PDP OPC DA Server** und wählen Sie das Kontextmenü **Properties**.

Der Dialog **SIEMENS SIGUARD PDP OPC DA Server Properties** wird geöffnet.

✧ Wählen Sie die Registerkarte **General**.

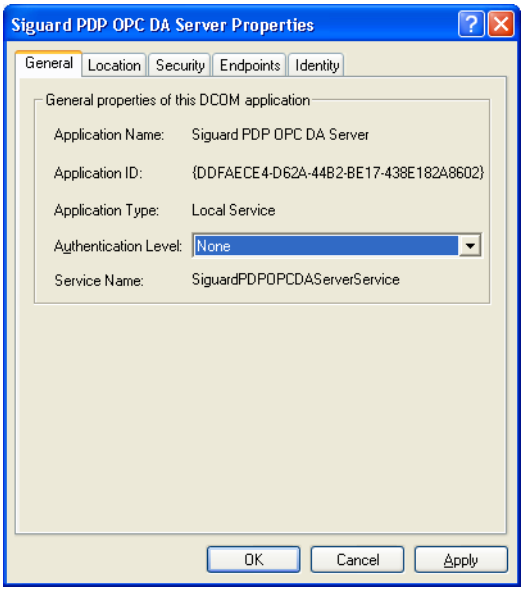

Bild 4-7 General

✧ Wählen Sie bei **Authentication Level** die Einstellung **None**.

✧ Wählen Sie die Registerkarte **Location**.

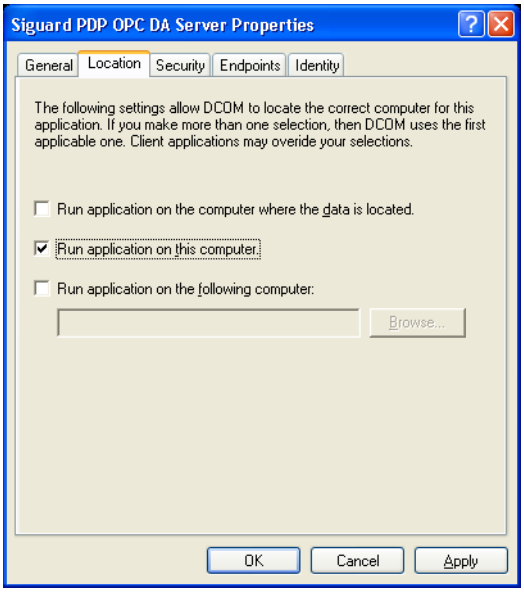

Bild 4-8 Location

✧ Wählen Sie **Run application on this computer**.

Zusätzlich müssen Sie für DCOM dem Benutzer, der sich beim OPC-Client anmeldet und über ein Netzwerk auf den OPC-Server zugreifen will, Start-, Zugriffs- und Konfigurationsrechte geben.

✧ Wählen Sie die Registerkarte **Security**.

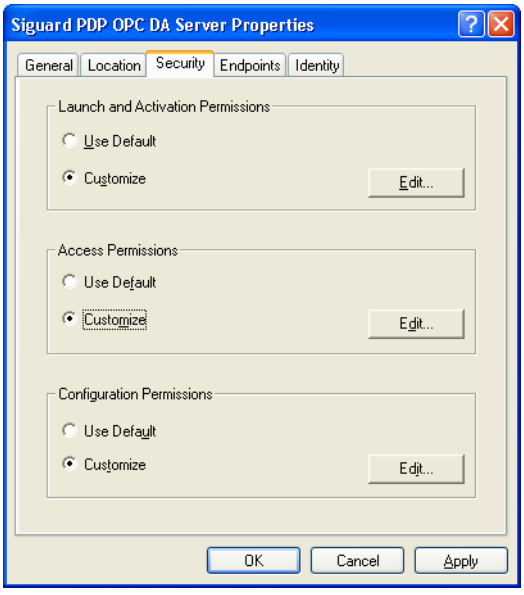

Bild 4-9 Security

✧ Aktivieren Sie unter **Launch Permissions** die Option **Customize**.

✧ Klicken Sie auf **Edit...**.

Der Dialog **Launch Permission** wird geöffnet.

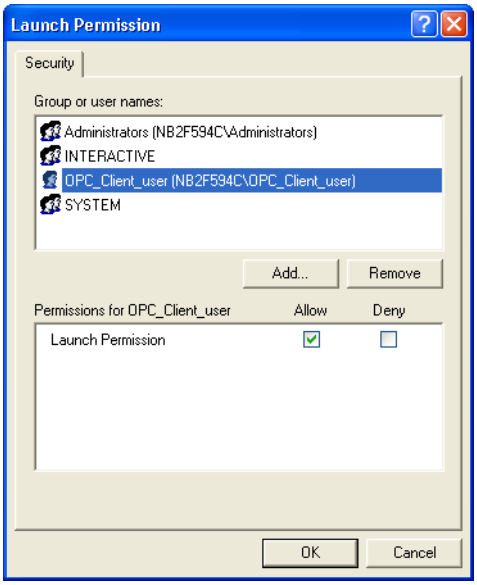

Bild 4-10 Startberechtigung festlegen

- ✧ Fügen Sie mit **Add...** den Benutzer ein, der mit dem OPC-Server/Client arbeiten soll. Sie können zu diesem Zweck auch einen neuen Benutzer anlegen.
- ✧ Aktivieren Sie für den Benutzer für **Launch Permission** die Option **Allow**.
- ✧ Schließen Sie den Dialog mit **OK**.

- ✧ Aktivieren Sie unter **Access Permissions** die Option **Customize**.
- ✧ Klicken Sie auf **Edit...**.

Der Dialog **Access Permission** wird geöffnet.

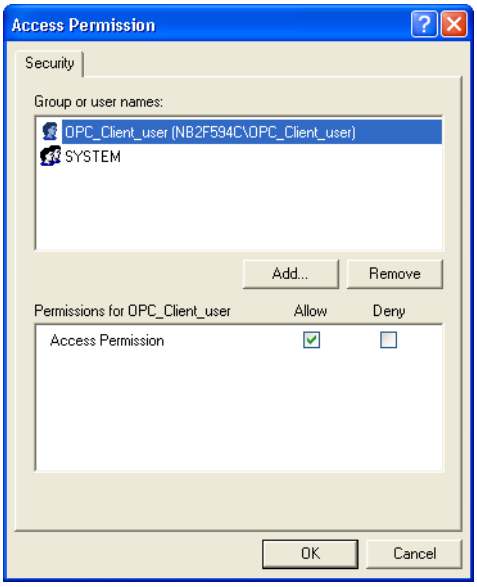

Bild 4-11 Zugriffsrecht festlegen

- ✧ Fügen Sie mit **Add...** den Benutzer ein, mit dem OPC-Server/OPC-Client arbeiten soll.
- ✧ Aktivieren Sie für den Benutzer die Option **Allow**.
- ✧ Schließen Sie den Dialog mit **OK**.
- ✧ Aktivieren Sie unter **Configuration Permissions** die Option **Customize**.
- ✧ Klicken Sie auf **Edit...**.

Der Dialog **Change Configuration Permission** wird geöffnet.

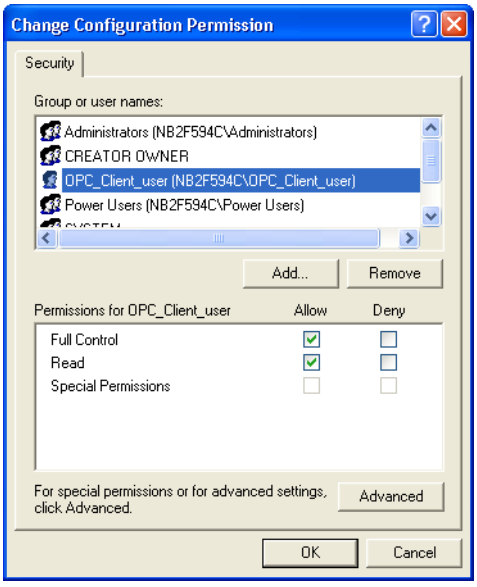

Bild 4-12 Konfigurationsberechtigung festlegen

- ✧ Fügen Sie mit **Add...** den Benutzer ein, mit dem OPC-Server/OPC-Client arbeiten soll.
- ✧ Aktivieren Sie für den Benutzer die Option **Allow** für **Full Control** und **Read**.
- ✧ Schließen Sie den Dialog mit **OK**.
- ✧ Wählen Sie die Registerkarte **End Points**.

  Auf dieser Registerkarte sind die Protokolle und Endpunkte aufgelistet, die der OPC-Client benutzen kann. Sie müssen nichts einstellen.

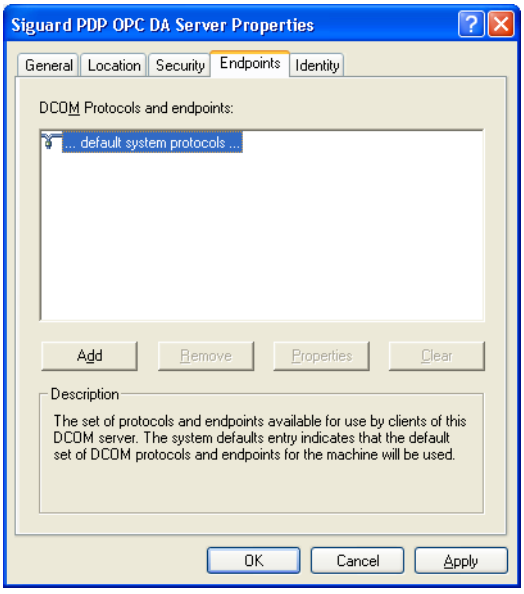

Bild 4-13 Endpunkte festlegen

✧ Wählen Sie die Registerkarte **Identity**.

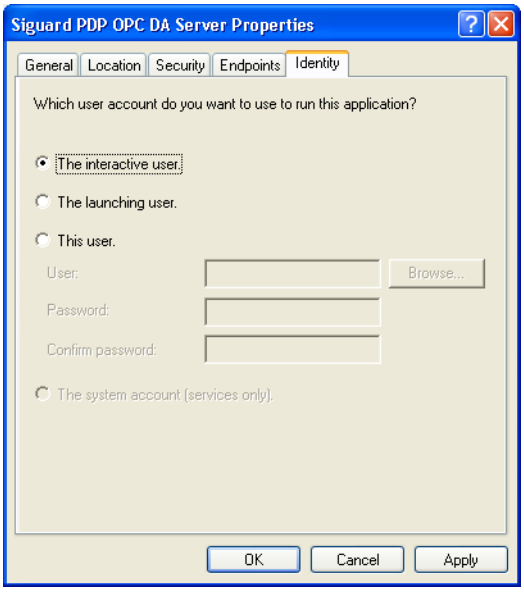

Bild 4-14 Identity

✧ Aktivieren Sie **The interactive user**.

✧ Schließen Sie den Dialog mit **OK**.

✧ Schließen Sie das Fenster **Component Services**.

HINWEIS

Wenn die Microsoft Firewall aktiviert ist, müssen Sie für den OPC-Server zusätzliche Einstellungen vornehmen (siehe *2.4 Kommunikationsprotokolle für den Einsatz einer Firewall*).

■

5 ICCP

5.1 Allgemeines

Das ICCP-Protokoll

Das ICCP-Protokoll unterstützt den Austausch von Netzdaten über ein Netzwerk (WAN oder LAN) zwischen einer lokalen EVU-Leitstelle und

- Anderen Elektrizitätsversorgungsunternehmen (EVUs)
- Power Pools
- Regionalen Leitstellen
- Nicht-EVU-Erzeugungseinheiten

Das Protokoll wurde gemäß IEC 61870-6 (TASE.2) standardisiert.

ICCP unterstützt:

- Funktionen für die Vorverarbeitung von Daten
- Eine Benutzeroberfläche zur Anzeige von Fehlerstatistiken mit leistungsstarken Test- und Diagnosefunktionen

SIGUARD PDP nutzt das ICCP-Protokoll, um Messwerte und Ereignisse an eine Netzleitstelle zu übertragen.

Einleitung

Mit dem SIGUARD PDP Engineer wird eine Konfigurationsdatei **PDP_config.xml** erstellt, die alle Daten für die ICCP-Kanäle enthält, um die entsprechenden Komponenten zu steuern und zu parametrisieren. Jede Komponente des Netzwerks liest diese xml-Datei während des Starts.

Vorgehensweise

Um mit dem ICCP arbeiten zu können, gehen Sie vor wie folgt:

- Installieren Sie den ICCP-Treiber.
- Lizenzieren Sie den ICCP-Treiber.
- Bearbeiten Sie die Konfigurationsdatei **osill2.cfg** des ICCP-Treibers.

5.2 Installation des ICCP-Treibers

5.2.1 Installationsvorbereitung

Gehen Sie bei der Installation für den ICCP-Treiber folgendermaßen vor:

- ✧ Deinstallieren Sie SIGUARD PDP, falls schon auf Ihrem Rechner vorhanden.
- ✧ Installieren Sie SIGUARD PDP mit der Option **ICCP**.

  Weitere Informationen hier erhalten Sie im Kapitel *3.2.2 Installation*.

5.2.2 Installation

Installation starten

So installieren Sie SIGUARD PDP ICCP Add-on:

- ✧ Legen Sie die DVD **ICCP Add-on** in das DVD-Laufwerk ein.

HINWEIS

Der Installationsvorgang startet nicht automatisch.

- ✧ Um den Installationsvorgang zu starten, doppelklicken Sie auf die **setup.exe**-Datei aus dem Wurzelverzeichnis der Add-on-DVD.
- ✧ Folgen Sie den Anweisungen der Installationsroutine.

Rechner neu starten

- ✧ Starten Sie den Rechner nach der Installation neu.

HINWEIS

Nachdem der ICCP-Treiber installiert wurde, finden Sie eine Beispiel-Konfigurationsdatei **osill2.cfg** im Verzeichnis **C:\Program Files\SISCO\osill2**. Informationen zur Bearbeitung der Konfigurationsdatei erhalten Sie im entsprechenden Kapitel im *Administrator-Handbuch*.

5.3 Lizenzierung des ICCP-Treibers

Aktivierung des ICCP-Treibers

✧ Öffnen Sie das Fenster **SISCO MMS-EASE Activation** über das Menü **Start > Programme > SISCO > MMS-EASE > Activate MMS-EASE**.

Bild 5-1 Lizenzierung des ICCP-Treibers

✧ Um den ICCP-Treiber zu aktivieren, klicken Sie auf **Activate**.

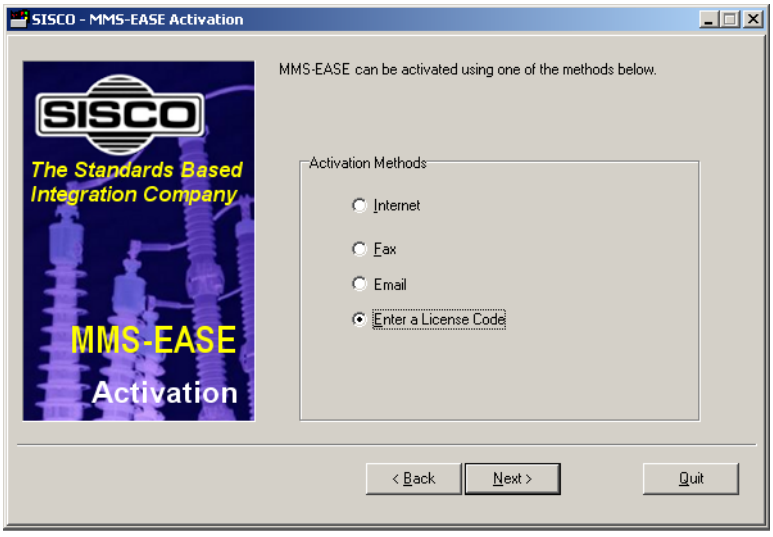

Bild 5-2 Lizenzierung des ICCP-Treibers

Um den ICCP-Treiber zu registrieren, haben Sie verschiedene Möglichkeiten:

✧ Wählen Sie die Aktivierungsmethode **Enter a License Code**.

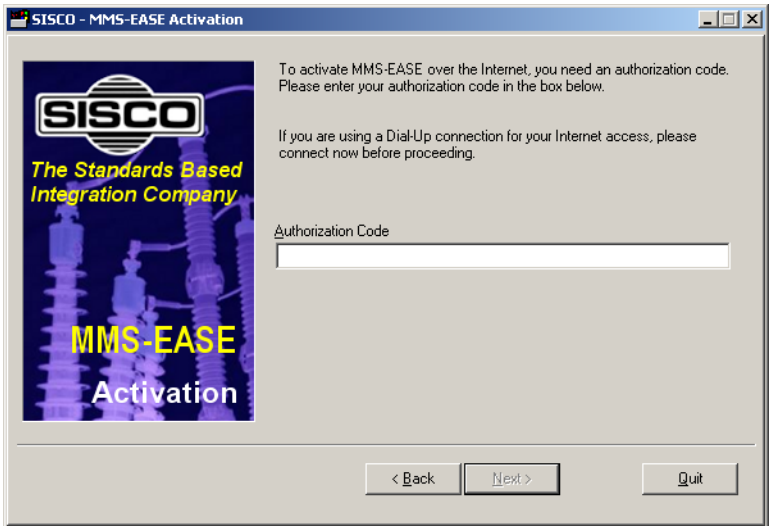

Bild 5-3 Eingabe des Lizenzschlüssels

✧ Geben Sie den Lizenzschlüssel ein, den Sie mit dem Produkt erhalten haben.

HINWEIS

Geben Sie nicht den Authorization-Code ein, der auf der CD-Hülle steht!

5.4 Bearbeitung der Konfigurationsdatei

Die Felder **Local AR Name**, **Primary Remote AR Name**, **Alternate Remote AR Name**, **Third Remote AR Name** und **Fourth Remote AR Name** sind die Aliasnamen der IP-Adressen für eine Verbindung von einer lokalen und einer Remote-Leitstelle. Diese Aliasnamen sind in einer Konfigurationsdatei **osill2.cfg** im Pfad **C:\ProgramFiles\SISCO\osill2** definiert. Um eine lokale mit einer Remote-Leitstelle zu verbinden zu können, müssen innerhalb der Konfigurationsdatei für jede Verbindung mindestens 4 Felder definiert werden:

- IP-Adresse (für TCP-Verbindungen)
- P-Selector (Local Presentation Selector)
- S-Selector (Local Session Selector)
- T-Selector (Local Transport Selector)

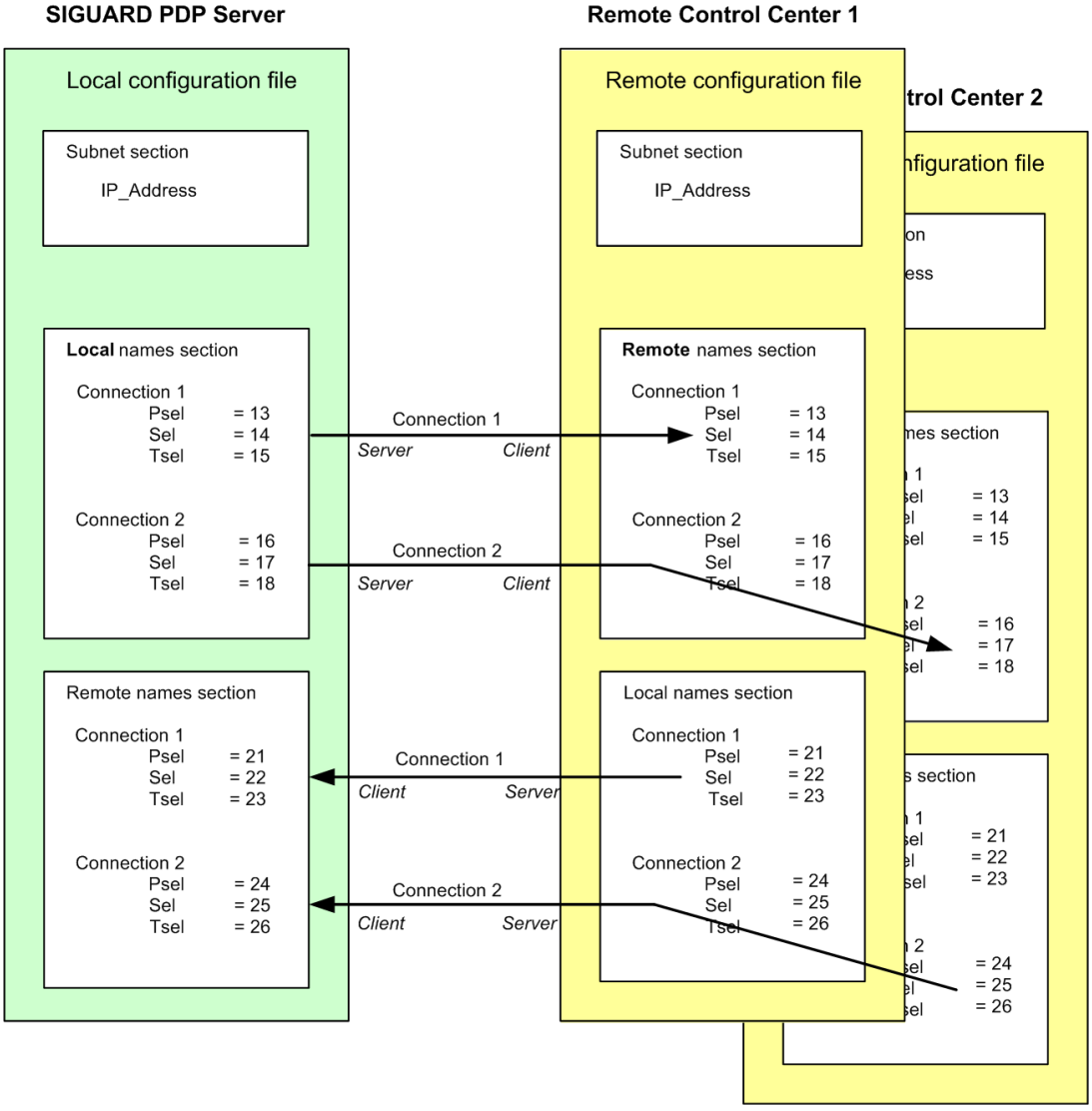

Bild 5-4 Übersicht der Konfigurationsdateien

Bereich Subnet anpassen

✧ Öffnen Sie die Konfigurationsdatei **osill2.cfg**.

✧ Geben Sie im Bereich **Subnet** die IP-Adresse des lokalen Rechners ein.

```
##############################################################################
# COMPONENT_NAME: OSILL2 configuration file for Windows 2000/XP
#
# \Program Files\SISCO\osill2\osill2.cfg
#
# This file is the source for Directory Information Base and
# stack configuration parameters.
#
##############################################################################

Begin_Subnet
  Type                          = 0
  NSAP                          = 49 00 02 11 22 33 44 01
  IP_Address                    = 128.0.0.1
  ES_CT                         = 60
  ES_HT                         = 60
  Error_Bit_On                  = N
  Internet_Type                 = 2
  Checksum                      = Y
  Driver                              = osillc1
End_Subnet
```

Bild 5-5 Einstellung der IP-Adresse des lokalen Rechners

✧ Speichern Sie die Konfigurationsdatei.

Bereich Local Names Section anpassen

✧ Passen Sie im Bereich **Local Names Section** für jede Verbindung den Parameter **AR_Name** an.

Der Name kann frei vergeben werden, z.B. **LocalToICCPREM** (Local > ICCP-Remote).

HINWEIS

Der Parameter muss identisch sein mit dem Namen, der in SIGUARD PDP Engineer vergeben wird.

✧ Vergeben Sie für die Parameter **Psel**, **Ssel** und **Tsel** Werte, die eindeutig im SIGUARD-System sind, z.B. *13 / 14 / 15* für Verbindung 1 oder *16 / 17 / 18* für Verbindung 2.

Diese Werte müssen identisch sein mit den Werten für die entsprechenden Parameter der Konfigurationsdatei des Remote Control Centers in Abstimmung mit dessen Administrator. Die Abstimmung der identischen Werte ist für alle Verbindungen erforderlich.

Weiterführende Informationen finden Sie unter *SISCO's Installation Guide for MMS-EASE for Windows*.

```
#########################################################################
#
# Local Names Section.
#
#
#   AR_Name:      Is an alias for the P-Address; it may be up to 32
#                 characters
#   Transport:    Is the Transport Provider TP4 (OSI) vs. TCP (RFC1006)
#                    Default is TP4
#   AP_Title:  Is an OPTIONAL array of up to 16-bit decimal integers
#   AP_InvokeID:  Is an OPTIONAL 32-bit decimal integer
#   AE_Qualifier: Is an OPTIONAL 32-bit decimal integer
#   AE_InvokeID:  Is an OPTIONAL 32-bit decimal integer
#   Psel:            Up to 32 characters (16 octets) of ASCII encoded hex
#   Ssel:            Up to 32 characters (16 octets) of ASCII encoded hex
#   Tsel:            Up to 64 characters (32 octets) of ASCII encoded hex
#   Shared:       Shared the local name with other application (Y/N)
#                 Default is N.
#   QOS:             Is an Optional decimal integer representing Quality
#                 Of Serv.
#
#########################################################################
```

```
Begin_Local
  AR_Name                 = LocalToICCPREM
  AP_Title                = 1 2 32 2
  AP_InvokeID             = 100
  AE_Qualifier            = 1
  Psel                    = 13
  Ssel                    = 14
  Tsel                    = 15
  Subnet                  = 0
  Shared                  = N
  QOS                     = 0
Transport                 = TCP
End_Local
```

1. Verbindung

```
Begin_Local
  AR_Name                 = LocalToICCPBKUP
  AP_Title                = 1 2 32 2
  AP_InvokeID             = 100
  AE_Qualifier            = 1
  Psel                    = 16
  Ssel                    = 17
  Tsel                    = 18
  Subnet                  = 0
  Shared                  = N
  QOS                     = 0
Transport                 = TCP
End_Local
```

2. Verbindung

Bild 5-6 Local Names Section

Bereich Remote Names Section anpassen

✧ Passen Sie im Bereich **Remote Names Section** für jede Verbindung den Parameter **AR_Name** an.

Der Name kann frei vergeben werden, z.B. **ICCPBKUPAddress1**.

✧ Vergeben Sie für die Parameter **Psel** , **Ssel** und **Tsel** Werte, die eindeutig im SIGUARD-System sind, z.B. *21 / 22 / 23* für Verbindung 1 oder *24 / 25 / 26* für Verbindung 2.

Diese Werte müssen identisch sein mit den Werten für die entsprechenden Parameter der Konfigurationsdatei des Remote Control Centers in Abstimmung mit dessen Administrator. Die Abstimmung der identischen Werte ist für alle Verbindungen erforderlich.

Weiterführende Informationen finden Sie unter *SISCO's Installation Guide for MMS-EASE for Windows*.

```
#########################################################################
#
# Remote Names Section.
#
#   AR_Name:   Is an alias for the P-Address; it may be up to 32
#              characters
#   Transport:    Is the Transport Provider: TP4(OSI) vs. TCP(RFC1006)
#                 Default is TP4
#   AP_Title:  Is an OPTIONAL array of up to 16-bit decimal integers
#   AP_InvokeID:  Is an OPTIONAL 32-bit decimal integer
#   AE-Qualifier: Is an OPTIONAL 32-bit decimal integer
#   AE-InvokeID:  Is an OPTIONAL 32-bit decimal integer
#   Psel:            Up to 32 characters (16 octets) of ASCII encoded hex
#   Ssel:            Up to 32 characters (16 octets) of ASCII encoded hex
#   Tsel:            Up to 64 characters (32 octets) of ASCII encoded hex
#   Nsap:            Up to 40 characters (20 octets) of ASCII encoded hex
#   IP_Address:   dotted decimal IP Address or host name
#   QOS:             Is an Optional decimal integer representing Quality
#                 Of Serv.
#   Static_Route: Is an OPTIONAL flag (default = 'N')
#                 'Y' creates a static routing record for this entry
#                 'N' does not
#   SNPA:        Is AR Name's SNPA (MAC Address)
#                Ignored if Static_Route is 'N'
#                Mandatory if Static_Route_Flag is 'Y'
#########################################################################
```

```
Begin_Remote
  AR_Name                 = ICCPBKUPAddress1
  Psel                    = 21
  Ssel                    = 22
  Tsel                    = 23
  Subnet                  = 0
  Transport               = TCP
  IP_Address              = 192.168.1.22
End_Remote
```

1. Verbindung

```
Begin_Remote
  AR_Name                 = ICCPBKUPAddress4
  Psel                    = 24
  Ssel                    = 25
  Tsel                    = 26
  Subnet                  = 0
  Transport               = TCP
  IP_Address              = 192.168.1.22
End_Remote
```

2. Verbindung

Bild 5-7 Remote Names Section

■

6 Zeitsynchronisation

6.1 Übersicht

Siemens empfiehlt, den SIGUARD PDP Server wie die PMus zeitsynchronisiert zu betreiben. Wenn der SIGUARD PDP Server nicht zeitsynchronisiert betrieben wird, kann nicht zuverlässig erkannt werden, ob die Zeitstempel der empfangenen Telegramme in einem zulässigen Zeitfenster liegen. Es kann also nicht erkannt werden, ob die empfangenen Telegramme zu alt sind oder quasi in der Zukunft liegen. Bei unsynchronisierter Server-Zeit könnten sowohl Telegramme mit an sich gültigem Zeitstempel verworfen, als auch solche mit fehlerhaftem Zeitstempel als gültig erkannt und verarbeitet werden.

Die Zeitsynchronisation innerhalb des SIGUARD PDP-Systems kann realisiert werden durch:

- **GPS-Empfänger** Hopf6039-Karte der Firma Hopf

  Die Hopf6039-Karte ist eine PCI-Karte für den SIGUARD PDP Server.
- **NTP-Zeit-Server** (z.B. SICLOCK, Hopf Zeit-Server, Meinberg Zeit-Server)

Die Zeitsynchronisation von SIGUARD PDP beruht auf dem **NTP** (Network Time Protocol) und dem zugehörigen Dienst **NTPD** (Network Time Protocol Daemon). Dieser Dienst läuft unter Windows im Hintergrund.

Bei der Installation von SIGUARD PDP wird dieser Dienst als **Network Time Protocol Service** bezeichnet. Konfiguriert wird dieser Dienst mit Hilfe der ASCII-Datei **ntp.conf**.

Weitere Informationen hierzu erhalten Sie im Kapitel *6.5 Konfigurationsdatei für den NTPD*.

Bei der Installation von **SIGUARD PDP** wird der NTPD mitinstalliert. Nach einem Neustart des Rechners wird er aktiviert.

In einem SIGUARD PDP-System können mehrere NTPDs aktiv sein, z.B. auf der externen Funkuhr und dem SIGUARD PDP Server. Ein NTPD kann als Server oder als Client konfiguriert sein. Der Server teilt einem Client auf dessen Anfrage seine Zeit mit.

Mit dem NTP kann bei einem Windows-Betriebssystem eine Genauigkeit von ca. 0,1 Millisekunden erreicht werden. Um zu dieser Genauigkeit zu kommen, müssen die NTPDs des Systems umfangreiche Berechnungen durchführen. Dies kann nach dem Systemstart bis zu einigen Stunden dauern. Wenn der aktuelle Timing-Master ausfällt, versuchen die NTPDs, die Zeit mit Hilfe der ermittelten Daten solange wie möglich genau zu halten.

Weitere Informationen zum NTP finden Sie im Internet unter der Adresse *http://www.ntp.org*.

6.2 Hopf-Zeit-Server installieren

Nach dem Einbau der Hopf6039-Karte müssen Sie zuerst die zugehörige Software installieren. Anschließend können Sie die Hopf6039-Karte initialisieren.

Bei der Installation von SIGUARD PDP wird ebenfalls ein NTPD (Network Time Protocol Daemon) mitinstalliert. Dieser NTPD erlaubt eine genauere Zeitsynchronisation als der von Hopf mitgelieferte NTPD.

Gehen Sie deshalb bei der Verwendung einer Hopf6039-Karte so vor:

- ✧ Bauen Sie die Hopf6039-Karte in den Rechner ein.
- ✧ Installieren Sie die Software zur Hopf6039-Karte. Dies ist zur Initialisierung der Hopf6039-Karte notwendig.
- ✧ Deinstallieren Sie den NTPD der Hopf6039-Karte (siehe *6.3 NTPD der Hopf-Karte deinstallieren*).
- ✧ Installieren Sie SIGUARD PDP. Der von SIGUARD PDP mitgelieferte NTPD wird automatisch mitinstalliert.

6.3 NTPD der Hopf-Karte deinstallieren

So deinstallieren Sie den NTPD der Hopf6039-Karte:

- ✧ Wählen Sie **Start > Einstellungen > Systemsteuerung**.
- ✧ Doppelklicken Sie auf **Verwaltung**. Das Fenster **Verwaltung** wird geöffnet.
- ✧ Doppelklicken Sie auf **Dienste**. Das Fenster **Services** wird geöffnet.
- ✧ Um den Dienst zu beenden, klicken Sie mit der rechten Maustaste auf **Network Time Protocol** und wählen Sie im Kontextmenü **Beenden**.
- ✧ Wählen Sie **Start > Ausführen**.
- ✧ Um den Dienst zu deinstallieren, geben Sie **<Hopf-Installationspfad>\instsrv remove** ein und klicken Sie auf **OK**.

6.4 NTP-Daemon

Für die Konfiguration des NTPDs ist ein Verständnis der wesentlichen Funktionen notwendig. Einige NTPD-Funktionen und Begriffe werden nachfolgend erläutert.

Server, Client und Peer

Der NTPD kann als **Server** oder als **Client** konfiguriert sein. Der Server führt die aktuelle Zeit, die er von einer Uhr bekommt. Die Clients holen sich die Zeit vom Server.

Außerdem kann ein NTPD als **Peer** konfiguriert sein. Dies ist der Fall, wenn in einem verteilten System mehrere gleichberechtigte Uhren vorhanden sind. Die Rollen (Server/Client) der einzelnen NTPDs sind nicht fest vergeben. Die Peers verständigen sich untereinander über die Qualität ihrer Zeit. Der NTPD des Peers mit der besseren Zeit übernimmt dann die Rolle des Servers.

Stratum, Offset und Dispersion

Die Zeitverteilung ist beim NTP hierarchisch strukturiert. Die Zeit wird von der obersten Ebene an die Ebenen darunter verteilt. Eine Ebene wird als **Stratum** bezeichnet. Die Uhr ist die oberste Ebene und hat das Stratum 0. Der Zeit-Server, der seine Zeit direkt von der Uhr bekommt, hat das Stratum 1. Der Server, der ein Client zu diesem Server ist, hat das Stratum 2. Die Nummerierung wird nach diesem Muster fortgesetzt.

Der **Offset** ist die Abweichung der Zeit der Client-Uhr von der Server-Uhr. Der NTPD versucht, den Offset klein zu halten. Er ist bei der Beurteilung der Zeitqualität das wichtigste Kriterium.

Ein weiteres Kriterium zur Beurteilung der Qualität ist die **Dispersion**. Die Dispersion definiert die Obergrenze für die Abweichung der Systemzeit von der echten Uhrzeit. Je kleiner die Dispersion ist, desto höher ist die Qualität der Zeit.

Qualität der Zeit

Innerhalb der SIGUARD-Laufzeit wird bei der Ermittlung der Systemzeit dem gelieferten Zeitstempel eine **Qualität** zugeordnet. Diese umfasst 4 Stufen:

- **Hoch** bedeutet, dass das System eine Abweichung von weniger als 10 Millisekunden zur echten Uhrzeit besitzt und die Qualität der Zeitquellen ausreichend für diese Aussage ist. Eine Dispersion von unter 10 ms ist für die Standardanforderungen in der automatisierten Energieversorgung ausreichend.
- **Mittel** bedeutet, dass das System eine Abweichung von weniger als 2 Sekunden zur echten Uhrzeit besitzt und die Qualität der Zeitquellen ausreichend für diese Aussage ist. Damit ist sichergestellt, dass keine Zeitstempel mit einer niedrigen Qualität erzeugt werden, wenn eine Schaltsekunde eingefügt wird und damit die Uhr vorübergehend eine Abweichung von ~1 Sekunde aufweist.
- **Niedrig** bedeutet, dass zwar eine Uhrzeit zur Verfügung steht, diese aber so ungenau ist, dass das System als nicht synchronisiert betrachtet werden muss.
- **Unbekannt** wird zugeordnet, wenn erkannt wird, dass entweder kein NTP-Dienst läuft oder dieser keine Uhrzeitquelle ermitteln konnte.

Außerdem enthält ein SIGUARD-interner Zeitstempel aus Kompatibilitätsgründen die Statusbits **ClockSync** und **ClockValid**. Diese werden entsprechend der Qualität des Zeitstempels gesetzt:

- **hoch**

  Die Status-Bits **ClockSync** und **ClockValid** werden gesetzt.
- **mittel**

  Die Status-Bit **ClockValid** wird gesetzt.
- **niedrig**

  Ein Status-Bit wird nicht gesetzt.
- **unbekannt**

  Ein Status-Bit wird nicht gesetzt.

6.5 Konfigurationsdatei für den NTPD

Bei der Installation von **SIGUARD PDP** wird eine Konfigurationsdatei **ntp.conf** in das Verzeichnis **...\windows\system32\drivers\etc** kopiert. Mit Hilfe dieser Datei konfigurieren Sie den **NTPD**.

In den Konfigurationsdateien der Clients sind die Zeit-Server angegeben. Im Gegensatz dazu sind in den Konfigurationsdateien der Server die Clients nicht angegeben. Dadurch ist es sehr einfach, einem System einen Zeit-Client hinzuzufügen. Nur die Konfigurationsdatei des neuen Clients muss bearbeitet werden.

Die Konfigurationsdatei enthält einige Kommentare zu ihrem Inhalt. In diesem Abschnitt sind wichtige Einträge ausführlicher erklärt.

Weitere Informationen finden Sie im Internet unter der Adresse *http://www.ntp.org*.

General settings

```
#--------------------------------------------------------------------------
# general settings
#--------------------------------------------------------------------------

# -- panic threshold --
# if system clock is more than that distance from the best external source,
# stop the service because something is really weird. Setting this to zero
# (0.0) disables all sanity checks, which is quite useful if the BIOS clock
# of the system is unreliable or some(one/thing/entity) tends to shoot the
# clock miles off...
tinker panic 0.0

# -- stepout threshold --
# If a clock step is required to sync the system, this condistion must be
# stable for a given amount of time (default: 900 seconds, or 15 minutes).
# The default is too long for a SICAM PAS system, so we set it to 1.5 minutes.
# (setting this to 0.0 will no longer suppress popcorn spikes and is not
# recommended; only do this if you do not mind occasional unnecessary steps
# of the system clock!)
tinker stepout 90.0

# -- driftfile storage --
# NTPD will store the clock drift here, so after restart the service will
# lock the FLL/PLL faster. On embedded systems, make sure that file is
# writeable and on a non-write-protected file system!
driftfile %windir%\ntp.drift

# -- logfile storage --
# make sure this is a writeable file on a non-write protected file system!
#logfile D:\tmp\ntpd.log

# -- Statistic file storage --
# make sure this is a directory on a non-write protected file system!
#statsdir D:\tmp\ntpstats\

#--------------------------------------------------------------------------
# make sure we operate well enough with windows and a limited number
# of clock sources
#--------------------------------------------------------------------------
tos orphan 10                    # stratum 10 if no clock source avail
tos mindist 0.020            # allow 20ms distance in sync group
tos minclock 1 minsane 1     # require only one clock source for grouping
```

Bild 6-1 ntp.conf - general settings

- **tinker panic**

  Die Zeit wird nicht synchronisiert, wenn die eigene Uhr mehr als 7200 Sekunden von der besten externen Uhr abweicht. Der NTPD beendet sich oder läuft nicht an.

  Im **Services-Manager** sehen Sie, ob der NTPD gestartet ist. Aktualisieren Sie den Services-Manager mit der Taste **F5**. Stellen Sie die lokale Systemzeit manuell ein. Starten Sie anschließend den NTPD.

- **driftfile, logfile, statsdir**

  Mit diesen Zeilen legen Sie den Speicherort der **Drift-** und **Protokolldateien** fest. Für die angegebenen Verzeichnisse muss eine Schreibberechtigung bestehen.

  Aktivieren Sie die Zeilen **logfile, statsdir** nur zur Fehlersuche.

  In der Datei **ntp.drift** wird die ermittelte Quarzkorrektur gespeichert. Dies ermöglicht nach einem Systemstart eine schnellere Synchronisierung, da Sie die Uhr mithilfe des Korrekturwertes auf annähernd die richtige Geschwindigkeit einstellen können. Wenn kein beschreibbares (und reset-festes!) Dateiensystem zur Verfügung steht, dann kann die Drift-Datei deaktiviert werden. Bei deaktivierter Drift-Datei dauert es nach einem Systemstart einige Zeit bis die optimale Synchronisierung erreicht wird. Das kann einige Stunden dauern.

Reference clocks

```
#--------------------------------------------------------------------------
# reference clocks
#--------------------------------------------------------------------------
# -- local system clock
# the local system clock is used as level 10 fallback if everything fails and
# the server must continue to operate because of (S)NTP clients like
# IEC61850 devices et al.
server 127.127.1.0
fudge 127.127.1.0 stratum 10

# -- HOPF6039 receiver
# mode 53-->bail out if no radio operation possible.
#server 127.127.39.0 mode 53 minpoll 2 maxpoll 6 prefer iburst
# Windows 7 recommendation: minpoll 4 maxpoll 4
```

Bild 6-2 ntp.conf - reference clocks

Mit den Zeilen unter **local system clock** können Sie die lokale Uhr als Zeitgeber definieren. Parametrieren Sie für das Stratum einen hohen Wert. Die lokale Zeit wird dann genommen, wenn keine andere, bessere Zeit zur Verfügung steht.

Mit den Zeilen unter **Hopf6039 receiver** parametrieren Sie den Einsatz einer **Hopf6039**-Karte.

- **mode**

  Mit mode 53 (siehe *Tabelle 6-2*) wird von der Karte keine Zeit abgefragt, wenn diese keinen Empfang hat.

- **minpoll, maxpoll**

  Die Zeit soll in einem Abstand zwischen 4 und 64 Sekunden abgefragt werden. Die Werte von minpoll und maxpoll sind die Exponenten bei einer Basis von 2 ($2^2 = 4$, $2^6 = 64$).

- **iburst**

  Der Parameter **iburst** sorgt dafür, dass beim 1. Mal 5 Werte im Abstand einer Sekunde gelesen werden. Damit werden die internen Filter schneller in einen eingeschwungenen Zustand gebracht, sodass der synchronisierte Zustand schneller erreicht wird.

Servers

```
#--------------------------------------------------------------------------
# servers
#--------------------------------------------------------------------------
# If the local system has no reference clock access, mention all systems that
# have reference clock access here. If there is a network path to an external
# clock source (NTP server in the control center, for example) list them
# here, too. And furthermore mention all fallback servers that can be used!

# minpoll 2 -> 4s / maxpoll 6 -> 64s, iburst -> initial burst poll
# Windows 7 recommendation: minpoll 4 maxpoll 4
#server yyy.yyy.yyy.yyy minpoll 2 maxpoll 6 iburst
```

Bild 6-3 ntp.conf - servers

In den folgenden Zeilen sehen Sie Beispiele zur Definition von Zeit-Servern. Sie dienen nur der Demonstration. In der Praxis müssen Sie Parameter für reale Zeit-Server eingeben.

server 139.25.31.13 minpoll 2 maxpoll 6 iburst

server 139.25.208.27 minpoll 2 maxpoll 6 iburst server ntp.lpz.siemens.de minpoll 2 maxpoll 6 iburst

6.6 Treiber für Hopf6039-Karte

Die Hopf6039-Karte ist eine PCI-Karte mit einem DCF77- oder GPS-Empfänger mit Uhr-Funktion. Während die Uhr eine Genauigkeit von einer Mikrosekunde hat, kann das Betriebssystem nur eine Auflösung von maximal einer Millisekunde verarbeiten. Mit dem modifizierten Treiber für die Hopf6039-Karte kann im Modus zum Polling der Flanke die Auflösung verbessert werden.

Die Hopf6039-Karte hat einen Quarzoszillator, der stabiler ist als der Oszillator eines Standard-Rechners. Eine Kombination aus Hopf6039-Karte und NTPD kann, nach einer Stabilisierungsphase von einigen Stunden, die Zeit auch ohne Zeitsignale noch 2 Stunden genauer als eine Millisekunde halten.

Beim modifizierten Treiber können verschiedene Modi eingestellt werden. Dadurch ist es möglich, das Verhalten des Treibers im Fehlerfall (kein Zeitzeichenempfang der Uhr) zu bestimmen. Der Treiber kann den Wert des Stratums erhöhen und die Uhr als fehlerhaft kennzeichnen.

Eine typische Zeile in der Konfigurationsdatei für eine Hopf6039-Karte sieht so aus:

server 127.127.39.0 mode 53 minpoll 2 maxpoll 6 prefer iburst

Der Parameter **mode 53** ist als Bit-Muster (Dezimalwert) zu interpretieren. Die Bedeutung der Bits ist in den folgenden Tabellen erläutert.

Tabelle 6-1 Bit-Muster zu mode 53

Bit	7	6	5	4	3	2	1	0
Bit-Muster	0	0	1	1	0	1	0	1
Wert	1			1	5			

Tabelle 6-2 Parameter mode 53

Bit-Position	Bedeutung
Bit 0 bis 3	Stratum drop Wert, der im Fehlerfall zum Stratum addiert wird (siehe *Tabelle 6-3*).
Bit 4	Modus zum Polling der Flanke Die Hopf6039-Karte unterstützt keine Interrupts. Die Karte hat eine Auflösung von 1 Millisekunde, führt die Uhrzeit aber mit einer wesentlich höheren Präzision. Bei einmaligem Lesen des Zeitstempels ergibt sich ein statistischer Fehler von +/- 0,5 Millisekunden; durch wiederholtes Lesen bis zu einer Änderung des gelesenen Wertes kann dieser Fehler auf 1/10 des ursprünglichen Wertes gesenkt werden. Damit ergibt sich eine schnellere Synchronisierung. Wenn Bit 4 gesetzt ist, dann wird wiederholtes Lesen bis zur Wertänderung aktiviert.
Bit 5 bis 7	Dropout mode Mit diesen Bits wird das Verhalten im Fehlerfall festgelegt (siehe *Tabelle 6-3*).

Tabelle 6-3 Parameter mode

dropout mode	stratum drop	Bedeutung
0	0	Die Verbindung zum Satelliten wird nicht überprüft, jedoch der Status der internen Uhr. Wenn die Uhr anzeigt, dass sie nur vom internen Quarz synchronisiert wird, markiert der Treiber die Uhr als fehlerhaft. Die Zeit wird nicht mehr abgefragt. Dieses Verhalten ist identisch mit dem Verhalten des nicht modifizierten Uhrtreibers.
0	1 bis 15	Die Zeit wird weiterhin abgefragt, auch wenn die Uhr nur vom internen Quarz synchronisiert wird. Der Treiber addiert aber den Wert **stratum drop** zum Stratum der Uhr. Der Wert des Stratums wird dabei auf ein Maximum von 15 begrenzt.

dropout mode	stratum drop	Bedeutung
1	1 bis 15	Der Treiber stellt fest, von wie vielen Satelliten die Uhr Zeitsignale empfängt. Wenn sie von keinem Satelliten ein Zeitsignal empfängt, wird der Wert **stratum drop** zum Stratum der Uhr addiert. Die Zeit wird nicht mehr abgefragt, wenn die Uhr nur vom internen Quarz synchronisiert wird.
2	0	Die Zeit wird weiterhin abgefragt, auch wenn die Uhr nur vom internen Quarz synchronisiert wird. Dieses Verhalten ist identisch mit dem Verhalten des nicht modifizierten Uhrtreibers, wenn bei diesem der Statusindikator **fudge1** auf **1** gesetzt ist.
2	1 bis 15	Der Treiber stellt fest, von wie vielen Satelliten die Uhr Zeitsignale empfängt. Empfängt sie von keinem Satelliten ein Zeitsignal, wird der Wert **stratum drop** zum Stratum der Uhr addiert. Die Zeit wird weiterhin abgefragt, auch wenn die Uhr nur vom internen Quarz synchronisiert wird.

6.7 Beispielkonfigurationen

6.7.1 Übersicht

In diesem Abschnitt sind typische Systemkonfigurationen dargestellt. Die Verteilung der Systemzeit und die Konfigurationsdateien der NTPDs sind beschrieben.

- Im 1. Beispiel kommt eine PCI-Karte der Firma Hopf zu Einsatz. Sie ist im SIGUARD PDP Server eingebaut.
- Im 2. Beispiel wird die Zeit von einer externen Funkuhr oder einem NTP-Zeitgeber vorgegeben. Die Funkuhr oder ein NTP-Zeitgeber ist direkt mit dem Ethernet verbunden.

6.7.2 PCI-Karte als Zeitgeber

Die PCI-Karte **FG6039GPS** der Firma Hopf ist in diesem Beispiel im SIGUARD PDP Server eingebaut und ist der Timing-Master des Systems. Andere Uhren werden nur dann zum Timing-Master, wenn die PCI-Karte ausfällt oder ihre Zeit eine schlechte Qualität hat.

Sowohl auf dem SIGUARD PDP UI-Rechner als auch auf dem SIGUARD PDP Engineer-Rechner ist der NTPD aktiv:

- Auf dem SIGUARD PDP Server als Server
- Auf dem SIGUARD PDP UI-Rechner und dem SIGUARD PDP Engineer-Rechner als Client

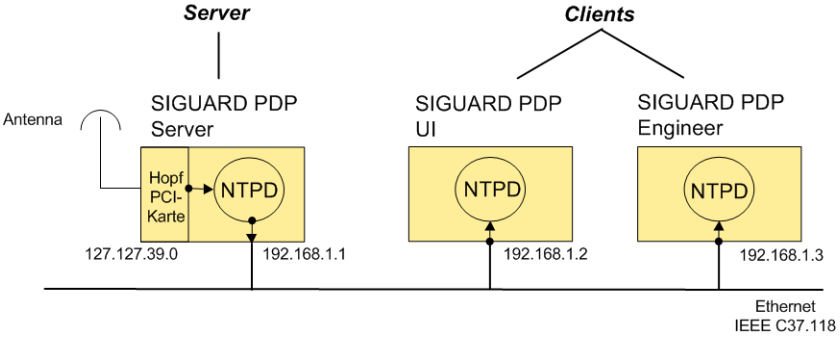

Bild 6-4 Zeitsynchronisation durch Hopf6039-Karte im SIGUARD PDP Server (Beispiel)

HINWEIS

Die Zeit der PMUs wird über GPS vor Ort (auf Feldebene) synchronisiert.

Konfigurationsdateien

In den folgenden Abschnitten sind die Konfigurationsdateien **ntp.conf** für den SIGUARD PDP Server und die Clients (SIGUARD PDP UI-Rechner und SIGUARD PDP Engineer-Rechner) aufgelistet. Die Einträge sind passend zu dem dargestellten Beispiel ausgeführt. In der Praxis müssen Sie sich an der realen Systemkonfiguration (z.B. IP-Adressen) orientieren.

Änderungen an den vorgegebenen Konfigurationsdateien sind hervorgehoben.

6.7.3 Konfigurationsdateien PCI-Karte

6.7.3.1 Konfigurationsdatei - Server

Konfigurationsdatei für den **SGUARD PDP Server**:

```
#--------------------------------------------------------------------------
# reference clocks
#--------------------------------------------------------------------------

# -- If this machine must be always the master of the island,
#    make sure it is capable of doing so:
tos cohort 1 orphan 5


# -- HOPF6039 receiver
# mode 53 --> bail out if no radio operation possible.
# At least for testing purposes, make sure the clock from the card is used
# even if no GPS antenna is connected or the receiver fails to track
# satellites. The card's clock is much more stable than ordibary PC clocks.

server 127.127.39.0 mode 64 minpoll 2 maxpoll 6 prefer iburst
# Windows 7 recommendation: minpoll 4 maxpoll 4
```

Bild 6-5 ntp.conf - reference clocks

In der blau markierten Zeile müssen Sie die IP-Adresse der Hopfkarte (z.B. 127.127.39.0) eintragen.

6.7.3.2 Konfigurationsdatei - Clients

Konfigurationsdatei für die Clients (**SIGUARD PDP UI-Rechner** und **SIGUARD PDP Engineer-Rechner**):

```
#--------------------------------------------------------------------------
# servers
#--------------------------------------------------------------------------
# If the local system has no reference clock access, mention all systems that
# have reference clock access here. If there is a network path to an external
# clock source (NTP server in the control center, for example) list them
# here, too. And furthermore mention all fallback servers that can be used!

# minpoll 2 -> 4s / maxpoll 6 -> 64s, iburst -> initial burst poll
# Windows 7 recommendation: minpoll 4 maxpoll 4
server 192.168.1.1 minpoll 2 maxpoll 6 iburst
```

Bild 6-6 ntp.conf - servers

In der blau markierten Zeile müssen Sie die IP-Adresse des SIGUARD PDP Servers (z.B. 192.168.1.1) als Verweis vom Client auf den Server eintragen.

6.7.4 Externe Funkuhr oder NTP-Zeit-Server als Zeitgeber

Bei dieser Systemkonfiguration wird eine **externe Funkuhr** (z.B. SICLOCK, Meinberg, Hopf) oder ein NTP-Zeit-Server als Timing-Master am Ethernet eingesetzt. Wenn z.B. die Uhr ausfällt oder die Qualität ihrer Zeit schlecht ist, wird eine andere Uhr des Systems der Timing-Master. Welche Uhr der neue Timing-Master wird, können Sie in den Konfigurationsdateien der NTPDs definieren.

Sowohl auf dem SIGUARD PDP Server als auch auf dem SIGUARD PDP UI-Rechner und dem SIGUARD PDP Engineer-Rechner ist der NTPD aktiv. Der NTPD der Funkuhr oder des NTP-Zeit-Servers ist der Zeit-Server, die NTPDs der SIGUARD-Rechner sind Clients.

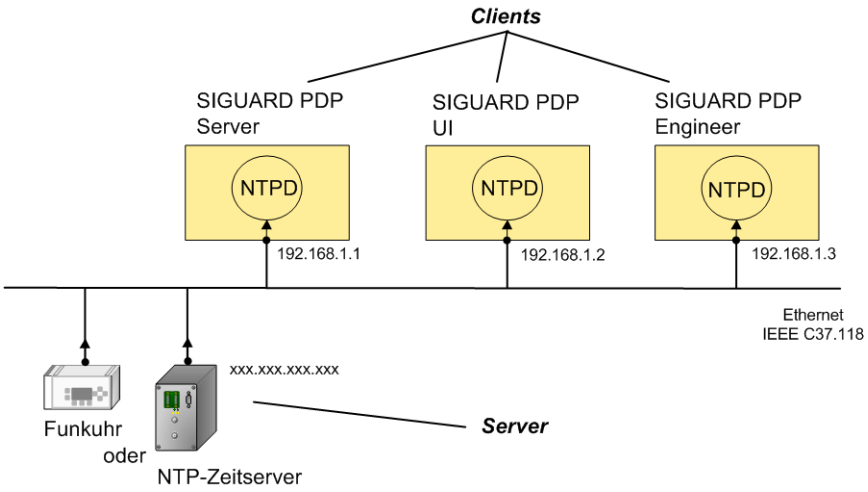

Bild 6-7 Zeitsynchronisation durch externe Funkuhr oder NTP-Zeit-Server

HINWEIS

Die Zeit der PMUs wird über GPS vor Ort (auf Feldebene) synchronisiert.

Konfigurationsdateien

In den folgenden Abschnitten sind die Konfigurationsdateien **ntp.conf** für die NTP-Clients aufgelistet. Die Einträge sind passend zu dem dargestellten Beispiel ausgeführt. In der Praxis müssen Sie sich an der realen Systemkonfiguration (z.B. IP-Adressen) orientieren.

Änderungen an den vorgegebenen Konfigurationsdateien sind hervorgehoben.

6.7.5 NTP-Konfigurationsdatei

6.7.5.1 Konfigurationsdatei - Clients

Konfigurationsdatei für die Clients (**SIGUARD PDP Server**, **SIGUARD PDP UI-Rechner** und **SIGUARD PDP Engineer-Rechner**):

```
#--------------------------------------------------------------------------
# servers
#--------------------------------------------------------------------------
# If the local system has no reference clock access, mention all systems that
# have reference clock access here. If there is a network path to an external
# clock source (NTP server in the control center, for example) list them
# here, too. And furthermore mention all fallback servers that can be used!

# minpoll 2 -> 4s / maxpoll 6 -> 64s, iburst -> initial burst poll
# Windows 7 recommendation: minpoll 4 maxpoll 4
server AAA.AAA.AAA.AAA minpoll 2 maxpoll 6 iburst
server BBB.BBB.BBB.BBB minpoll 2 maxpoll 6 iburst
server XXX.XXX.XXX.XXX minpoll 2 maxpoll 6 iburst
server YYY.YYY.YYY.YYY minpoll 2 maxpoll 6 iburst
```

Bild 6-8 ntp.conf - servers

In den blau markierten Zeilen müssen Sie die IP-Adressen der zur Verfügung stehenden Zeit-Server eingetragen. Nur die eingetragenen Zeit-Server werden abgefragt.

HINWEIS

Wenn eine Funkuhr als Zeitgeber verwendet wird, dann müssen die Einstellungen des entsprechenden Herstellers berücksichtigt werden.

6.7.6 Konfiguration abschließen

- ✧ Speichern Sie die Konfigurationsdateien für Server und Clients im entsprechenden Pfad des Rechners.
- ✧ Starten Sie den Dienst **Network Time Protocol** neu.

  Die Vorgehensweise zum Starten des **Network Time Protocols** ist dieselbe wie in Kapitel *4.3 OPC-Server konfigurieren* beschrieben.

6.8 NTP-Treiber abfragen

Mit dem nachfolgenden Befehl können Sie den NTP-Treiber abfragen, um zu sehen, ob er ordnungsgemäß arbeitet:

- ✧ Öffnen Sie ein Eingabefenster.
- ✧ Geben Sie den Befehl **ntpq-seq -pn** ein.

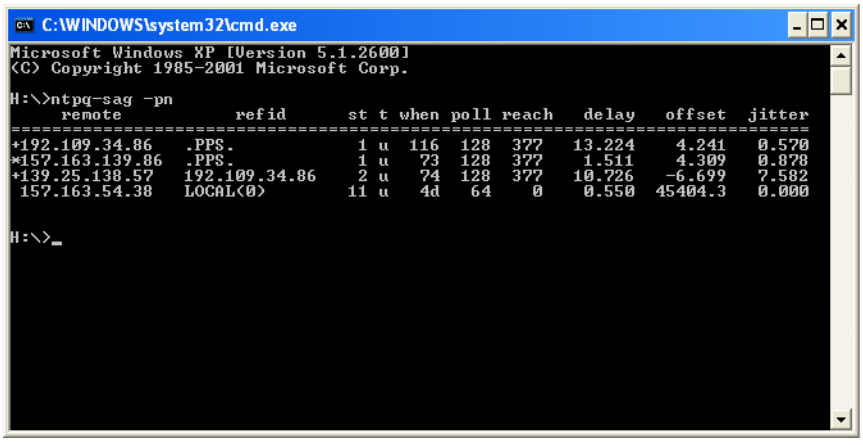

Bild 6-9 Ergebnis der Abfrage des NTP-Treibers

Für jeden eingetragenen NTP-Zeit-Server wird eine Zeile als Abfrageergebnis angezeigt. Das *** -Symbol** zeigt an, dass dieser Zeit-Server aktuell verwendet wird. Das **+ -Symbol** zeigt an, dass auch zu diesen Zeit-Servern eine Verbindung besteht und eine Auswertung deren Zeit stattfindet.

Der Parameter **reach** zeigt an, wie viele erfolgreiche Abfragen mit dem Zeit-Server erfolgt sind. Der Wert **377** sollte erreicht werden.

Weitere Informationen siehe *http://www.ntp.org/documentation.html*

■

7 Sicherheitseinstellungen

7.1 Übersicht

Damit Sie ein komplexes System wie das SIGUARD PDP-Netzwerk schützen können, gibt es mehrere Punkte zu beachten. In diesem Kapitel erfahren Sie einige wichtige Punkte zum zusätzlichen Schutz des Netzwerks.

7.2 Die Desktop-Firewall

Allgemeines

Siemens empfiehlt, die Windows Firewall auf dem SIGUARD PDP Server zu aktivieren. Bei einer reinen SIGUARD PDP Server-Anwendung sind nur einige Ports und Services erforderlich.

Firewall einrichten

✧ Öffnen Sie am SIGUARD PDP Server das Fenster **Windows Firewall** über **Start > Settings > Control Panel > Windows Firewall**.

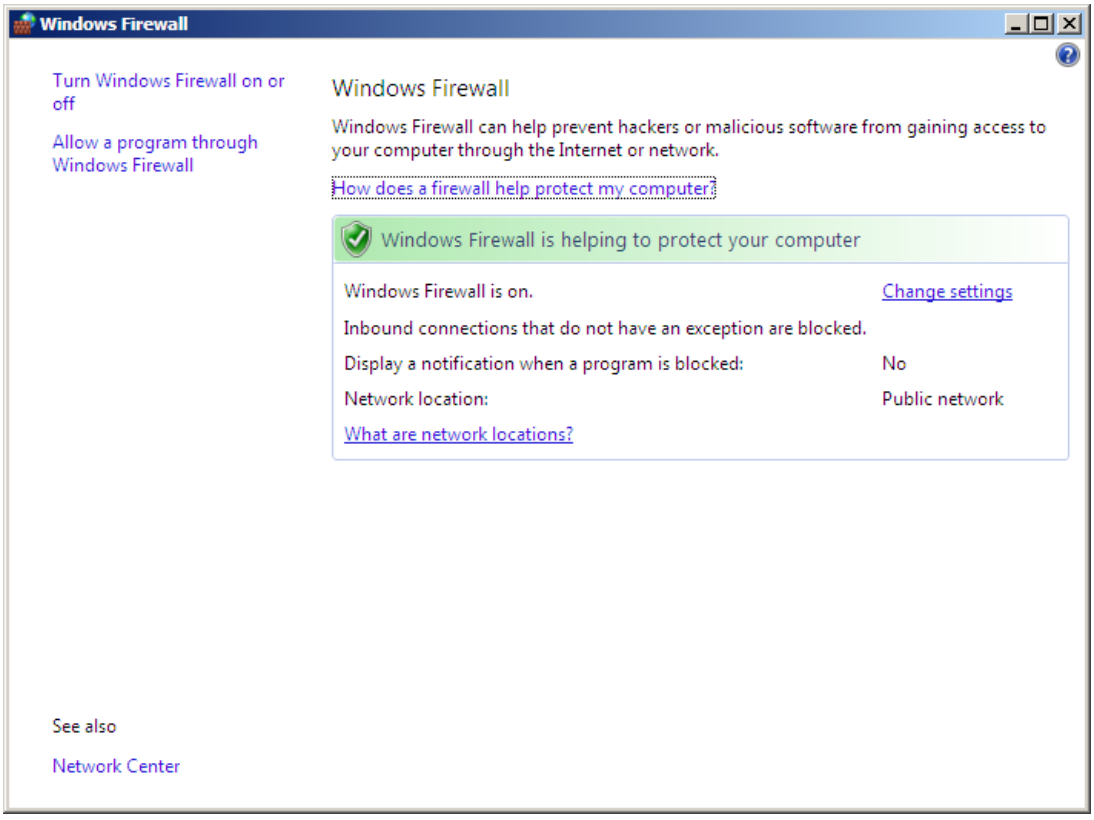

Bild 7-1 Windows Firewall

✧ Wählen Sie **Change settings**.

✧ Aktivieren Sie die Firewall.

Fügen Sie einen Port für den SIGUARD PDP Server hinzu, der ankommende Verbindungen entgegen nimmt.

✧ Öffnen Sie das Fenster **Add a Port**.

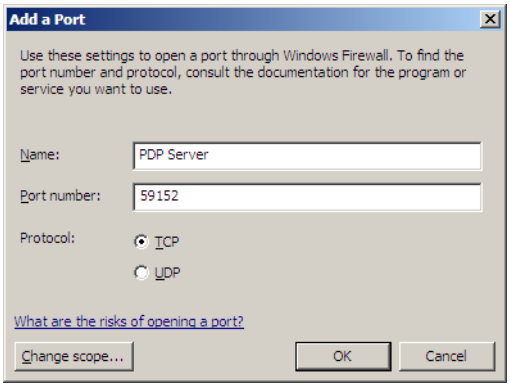

Bild 7-2 TCP-Port am SIGUARD PDP Server hinzufügen

- ✧ Geben Sie als Namen für den Port *PDP Server* ein.
- ✧ Vergeben Sie die **Port number**, z.B. *59152*.
- ✧ Stellen Sie das Protokoll auf **TCP** ein.
- ✧ Schließen Sie den Dialog mit **OK**.

Wenn der SIGUARD PDP Server wahlweise als **NTP Server** eingesetzt wird, müssen eingehende Verbindungen auch am UDP-Port 123 angenommen werden.

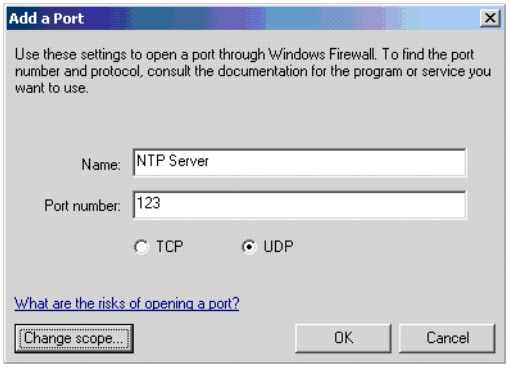

Bild 7-3 UDP-Port am NTP Server hinzufügen

- ✧ Geben Sie als Namen für den Port *NTP Server* ein.
- ✧ Vergeben Sie die **Portnumber**, z.B. *123*.
- ✧ Stellen Sie das Protokoll auf **UDP** ein.
- ✧ Schließen Sie den Dialog mit **OK**.

Neben den Grunddiensten des Netzwerkes müssen Ausnahmebedingungen für die Firewall definiert werden:

- File and Printer Sharing
  Datei und Druckdienst (Port 139/445) für einen gemeinsamen Ordner auf dem SIGUARD PDP Server
- Network Discovery
  Anzeige des Netzwerks, falls gewünscht

- PDP Server
  Der definierte Port für den SIGUARD PDP Server
- Remote Event Log Management
  Für den Remote-Zugriff auf die Protokolldatei von Ereignissen

✧ Öffnen Sie das Fenster **Windows Firewall Settings**.

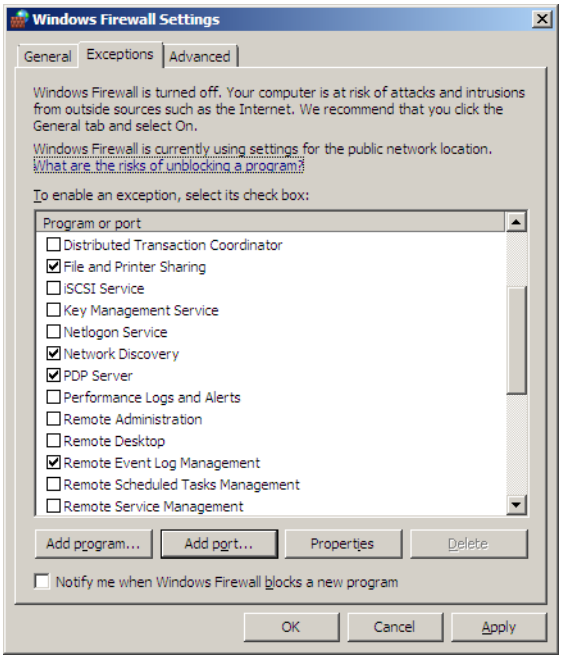

Bild 7-4 Exceptions

✧ Markieren Sie die entsprechenden Ausnahmebedingungen.

✧ Fügen Sie die Ports mit **Add port...** hinzu.

✧ Schließen Sie den Dialog mit **OK**.

7.3 Logging

7.3.1 Allgemeines

Vorschriften, wie NERC-CIP oder das BDEW Whitepaper Security, fordern die Aufzeichnungen von Änderungen und sicherheitsrelevanten Aktivitäten. Zu den sicherheitsrelevanten Aktivitäten zählen das Ändern des Benutzer-Passwortes oder eine Konfigurationsänderung für die Rückverfolgung im Fehlerfall oder bei Fremdeingriffen. Darüber hinaus sind die zentralen Aufzeichnungen eine Voraussetzung für eine gute Übersicht und für eine vereinfachte Fehlersuche durch Siemens.

Das zentrale Logging (Erfassen von Ereignissen in einer Protokolldatei) von Microsoft, das auch systemeigene Programme beinhaltet, ist nicht so einfach. Es ist nicht möglich, alle relevanten Log-Daten auf einem zentralen Syslog-Server aufzuzeichnen. Aus diesem Grund muss eine Software einer Drittfirma verwendet werden, z.B. **Datagram Syslog Agent**, die von Datagram Consulting als Free Software vertrieben wird, siehe *Webseite von Datagram Consulting*.

Microsoft Windows unterstützt auch den Remote-Zugriff auf aufgezeichnete Ereignisse über den darin enthaltenen **Event Viewer**.

Beachten Sie, dass einige Bedingungen eingehalten werden müssen, um die Protokolldateien über Remote-Zugriff einsehen zu können. Bei Problemen, siehe *Webseite Event Viewer Troubleshooting von Microsoft*.

- Als Erstes benötigen Sie Administratorrechte auf dem Remote-Rechner, um die Protokolldateien lesen zu können. Dieser Benutzer muss auch mit dem gleichen Passwort auf dem lokalen Rechner angelegt sein. Um den besten Sicherheitsnutzen zu erzielen, verwenden Sie **Run as**, um den Vorgang abzuschließen. Es wird empfohlen, einen Audit-Administrator, der Administratorrechte besitzt, auf dem Remote-Rechner und dem Lokalen Rechner anzulegen.
- Um die Bezeichnungs- und Kategoriefelder im Eigenschaftenfenster einer Ereignisaufzeichnung einsehen zu können, muss auf einigen Windows-Betriebssystemen der **Remote Registry Service** gestartet werden.
- Wenn die Firewall wie vorgeschlagen aktiviert ist, geben Sie den eingehenden Datenverkehr für Remote-Ereignisaufzeichnungen frei.

✧ Öffnen Sie das Fenster **Windows Firewall Settings**.

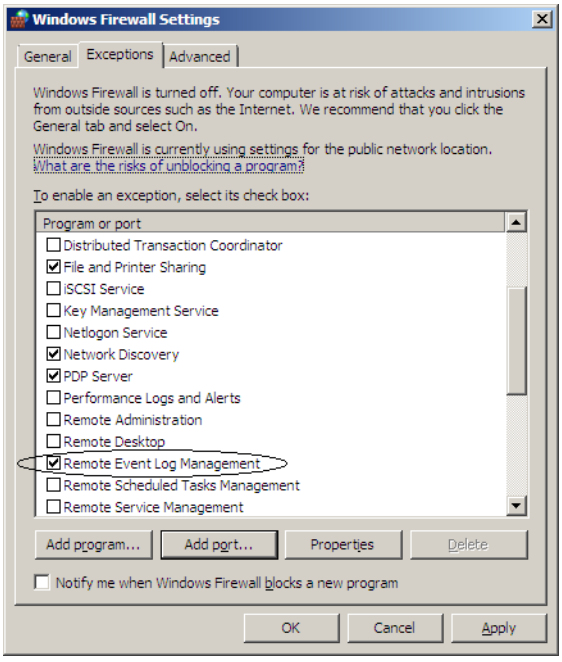

Bild 7-5 Datenverkehr für Remote-Ereignisaufzeichnungen freigegeben

- ✧ Markieren Sie **Remote Event Log Management**.
- ✧ Schließen Sie den Dialog mit **OK**.

7.3.2 Logging mit dem Event Viewer für Windows XP

Benutzer anlegen

- ✧ Legen Sie einen Benutzer mit Administratorrechten auf dem Lokalen Rechner und dem Remote-Rechner an.
- ✧ Öffnen Sie das Fenster **Computer Management** über die Systemsteuerung.
- ✧ Markieren Sie den Benutzer **Auditor**.

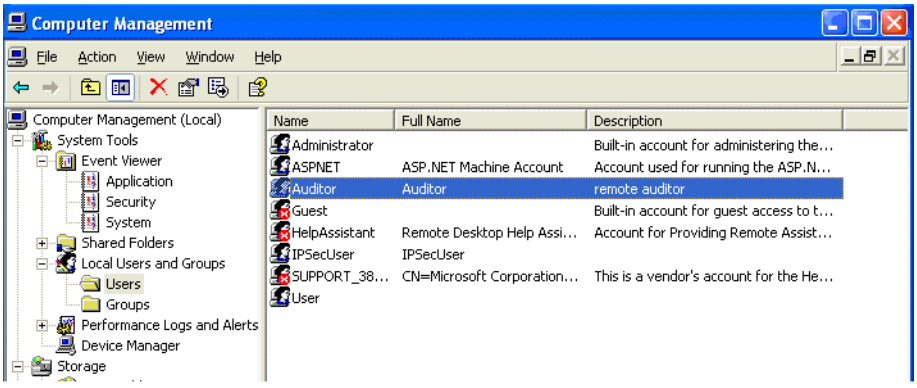

Bild 7-6 Computer Management mit markiertem Benutzer Auditor

✧ Öffnen Sie mit Doppelklicken das Eigenschaftenfenster für diesen Benutzer.

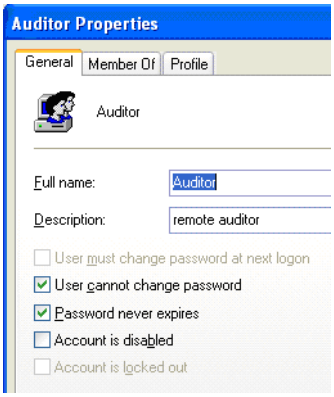

Bild 7-7 Auditor Properties

✧ Legen Sie auf der Registerkarte **General** die Rechte für diesen Benutzer fest.

✧ Ordnen Sie auf der Registerkarte **Member Of** den neuen Benutzer der Benutzergruppe **Administrators** zu.

✧ Bestätigen Sie Ihre Eingaben mit **OK**

Remote Registry Service auf dem Remote-Rechner aktivieren

✧ Öffnen Sie das Fenster **Computer Management** über die Systemsteuerung.

✧ Markieren Sie den Service **Remote Registry**.

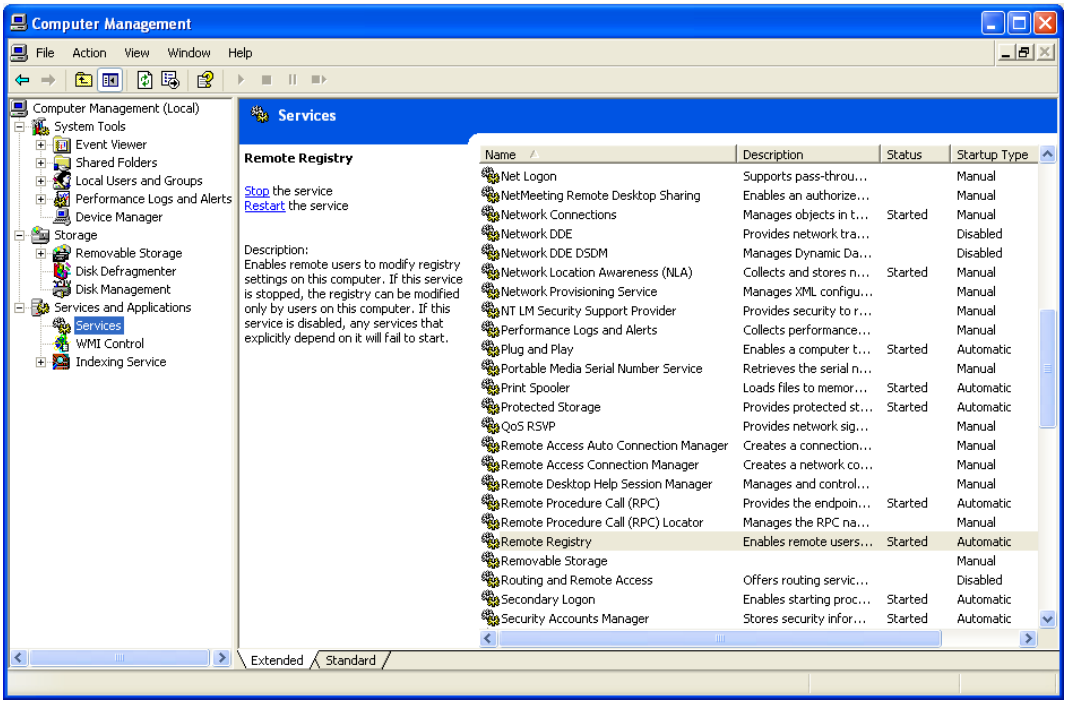

Bild 7-8 Remote Registry Service

- ✧ Stoppen Sie den Service mit **Stop** oder starten Sie den Service wieder mit **Restart**.
- ✧ Schließen Sie das Fenster **Computer Management**.

Event Viewer starten

- ✧ Da der Windows-Parameter **/auxsource** hier nicht funktioniert, müssen Sie den **Event Viewer** das 1. Mal per Hand starten. Öffnen Sie ein Eingabefenster mit dem Befehl **Start > Run > cmd** und geben Sie den Befehl **runas /netonly /user:auditor "mmc.exe /a eventvwr.exe"** ein.
- ✧ Starten Sie den **Event Viewer** in Zukunft als Benutzer **Auditor**. Klicken Sie hierzu mit der rechten Maustaste auf das Programmsymbol Event Viewer und wählen Sie im Kontextmenü **Auditor**.

Bild 7-9 Anmeldung als Auditor

- ✧ Wählen Sie als Benutzername *Auditor*.
- ✧ Geben Sie das korrekte Passwort ein.
- ✧ Schließen Sie den Dialog mit **OK**.

Verbindung zu einem anderen Rechner herstellen

- ✧ Markieren Sie im Fenster **Event Viewer** das Hauptverzeichnis **Event Viewer**
- ✧ Öffnen Sie mit der rechten Maustaste das Kontextmenü **Connect to another computer...**

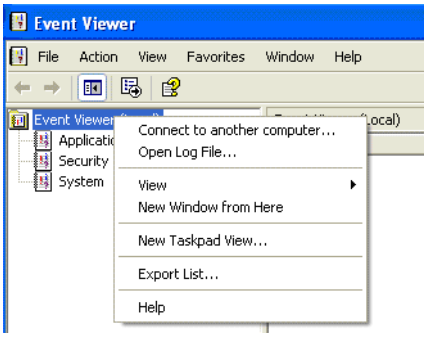

Bild 7-10 Kontextmenü Connect to another computer...

- ✧ Geben Sie die **IP-Adresse** oder den **Domain-Namen** des Remote-Rechners ein.

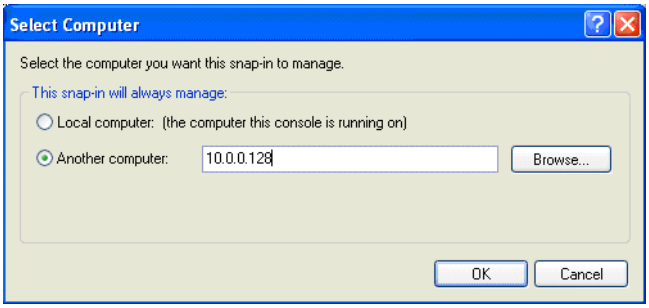

Bild 7-11 Event Viewer, Remote-Verbindung einrichten

✧ Schließen Sie den Dialog mit **OK**.

Protokolldateien einsehen

✧ Markieren Sie im Fenster **Event Viewer** das Verzeichnis **Application**

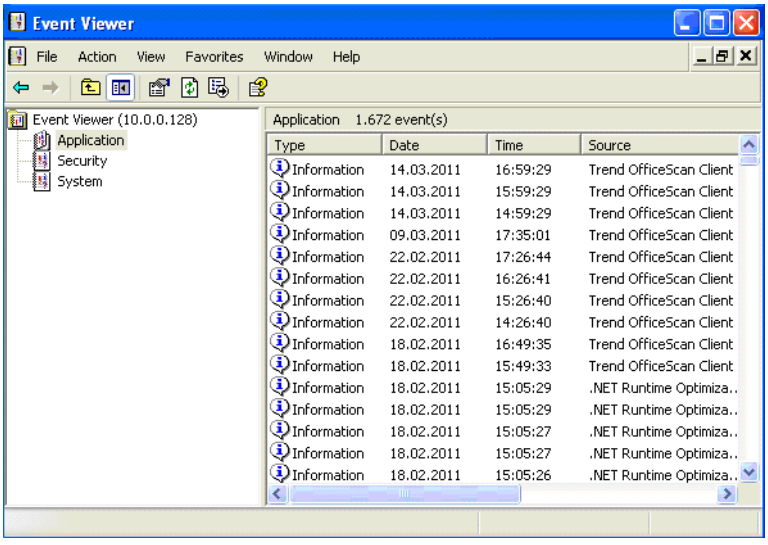

Bild 7-12 Event Viewer des Remote-Rechners

Im rechten Fensterbereich sind alle Ereignisse aufgelistet.

Konfiguration für den Remote-Zugriff speichern

Um zukünftig einen schnellen Zugriff auf Ihre Konfigurationsdaten zu bekommen, speichern Sie diese ab.

✧ Wählen Sie im Event Viewer das Menü **File > Save As...**

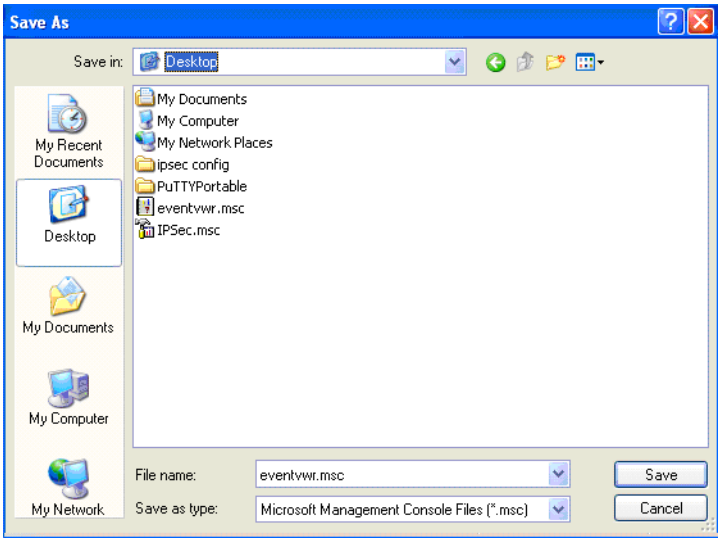

Bild 7-13 Konfiguration des Remote-Zugriffs speichern

- ✧ Wählen Sie einen beliebigen Pfad.
- ✧ Speichern Sie mit **Save**.
- ✧ Schließen Sie den Dialog mit **OK**.

Protokolldateien speichern

So können Sie Protokolldateien über den **Event Viewer** im Format **.txt** oder **.csv** speichern.

- ✧ Markieren Sie im **Event Viewer** das Verzeichnis **Application** und öffnen Sie das Kontextmenü **Save Log File As...**

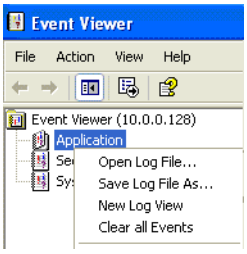

Bild 7-14 Kontextmenü Save Log File As...

- ✧ Geben Sie einen beliebigen Dateinamen ein.
- ✧ Wählen Sie einen beliebigen Pfad.
- ✧ Speichern Sie mit **Save**.

HINWEIS

Während des Remote-Zugriffs ist das Speichern einer Protokolldatei im Format **.evt** nicht möglich.

7.3.3 Logging mit dem Event Viewer für Windows 7 (Lokaler Rechner) und Windows Server 2008 (Remote-Rechner)

Benutzer anlegen

✧ Legen Sie einen Benutzer **Auditor** mit Administratorrechten auf dem lokalen Rechner und dem Remote-Rechner an.

HINWEIS

Achten Sie aus Konsistenzgründen darauf, dass auf dem lokalen Rechner und auf dem Remote-Rechner immer der gleiche Benutzername und das gleiche Passwort vergeben werden.

✧ Öffnen Sie das Fenster **Computer Management** über die Systemsteuerung.

✧ Markieren Sie den Benutzer **Auditor**.

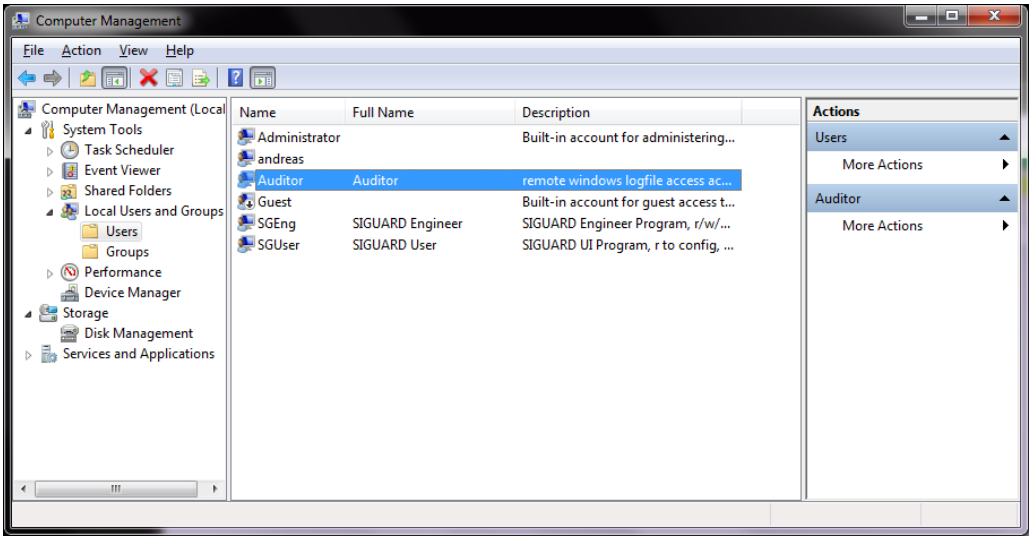

Bild 7-15 Computer Management

✧ Öffnen Sie mit Doppelklicken das Eigenschaftenfenster für diesen Benutzer.

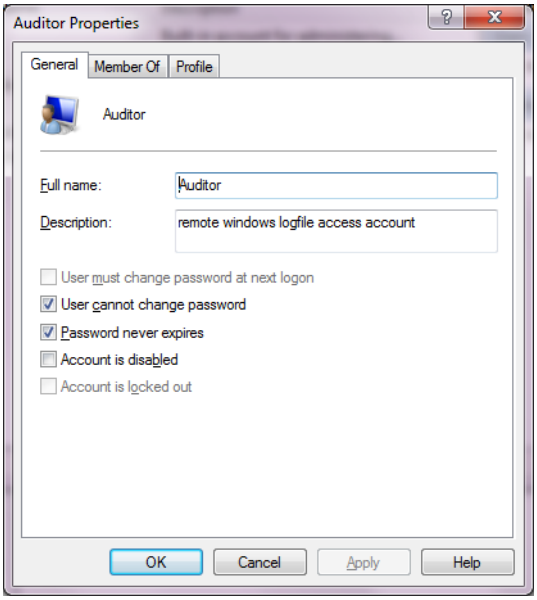

Bild 7-16 Auditor Properties - General

- ✧ Legen Sie auf der Registerkarte **General** die Rechte für diesen Benutzer fest.
- ✧ Um den neuen Benutzer der Benutzergruppe **Administrators** zuzuordnen, wählen Sie die Registerkarte **Member Of**.

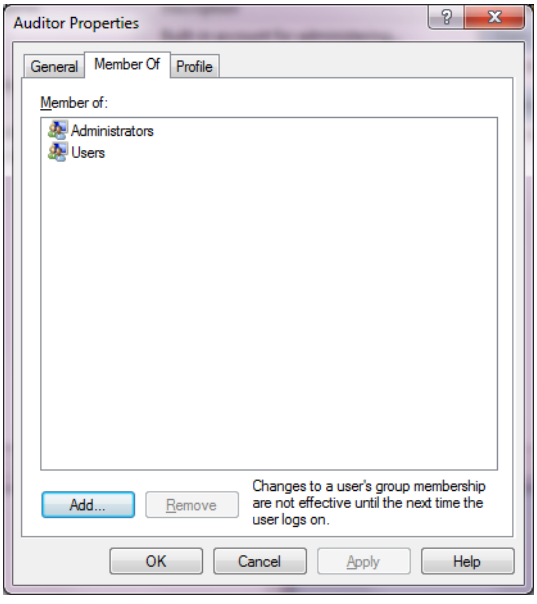

Bild 7-17 Auditor Properties - Member Of

Der Benutzer **Auditor** ist den Benutzergruppen **Administrators** und **Users** zugeordnet.

- ✧ Bestätigen Sie Ihre Eingaben mit **OK**.

Freigabe der Remote-Ereignisaufzeichnungen

✧ Aktivieren Sie im Fenster **Windows Firewall Settings** auf der Registerkarte **Exceptions** die Funktion **Remote Event Log Management**.

Nähere Informationen siehe *7.1 Übersicht*.

Event Viewer starten

Unter Windows 7 / Server 2008 können Sie den **Event Viewer** über folgende Elemente starten:

- die Benutzeroberfläche oder
- das Eingabefenster.

✧ Starten Sie den **Event Viewer** über die Benutzeroberfläche mit dem Menü **All Programs > Administrative Tools > Event Viewer**

-- oder --

✧ Starten Sie den **Event Viewer** über das Eingabefenster.

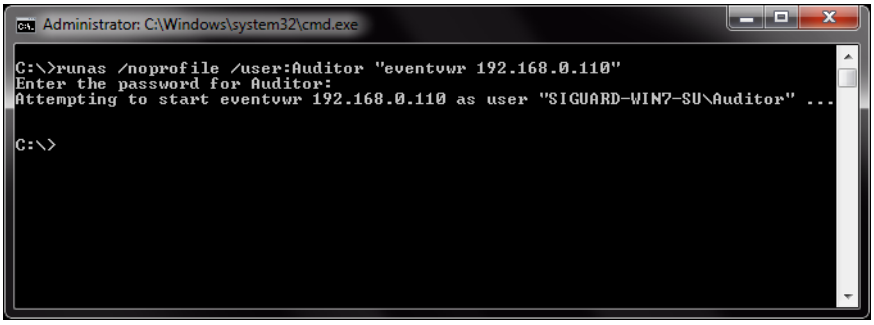

Bild 7-18 Starten des Event Viewers über das Eingabefenster

Das Fenster **Event Viewer** wird geöffnet.

Verbindung zu einem anderen Rechner herstellen

✧ Öffnen Sie im **Event Viewer** das Menü **Action > Connect to another Computer...**

✧ Markieren Sie **Another Computer** und geben Sie die IP-Adresse oder den Domain-Namen des Remote-Rechners ein.

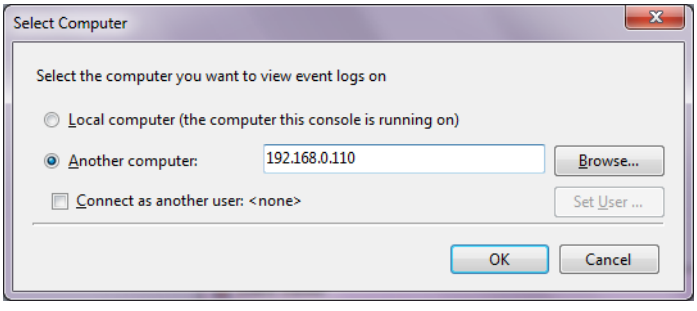

Bild 7-19 Event Viewer, Remote-Verbindung einrichten

✧ Schließen Sie den Dialog mit **OK**.

Protokolldateien einsehen

Der SIGUARD PDP Server besitzt einen eigenen Bereich, wo Fehlermeldungen angezeigt werden können.

✧ Markieren Sie unter **Applications and Services Logs** das Unterverzeichnis **SIGUARD_PDP**.

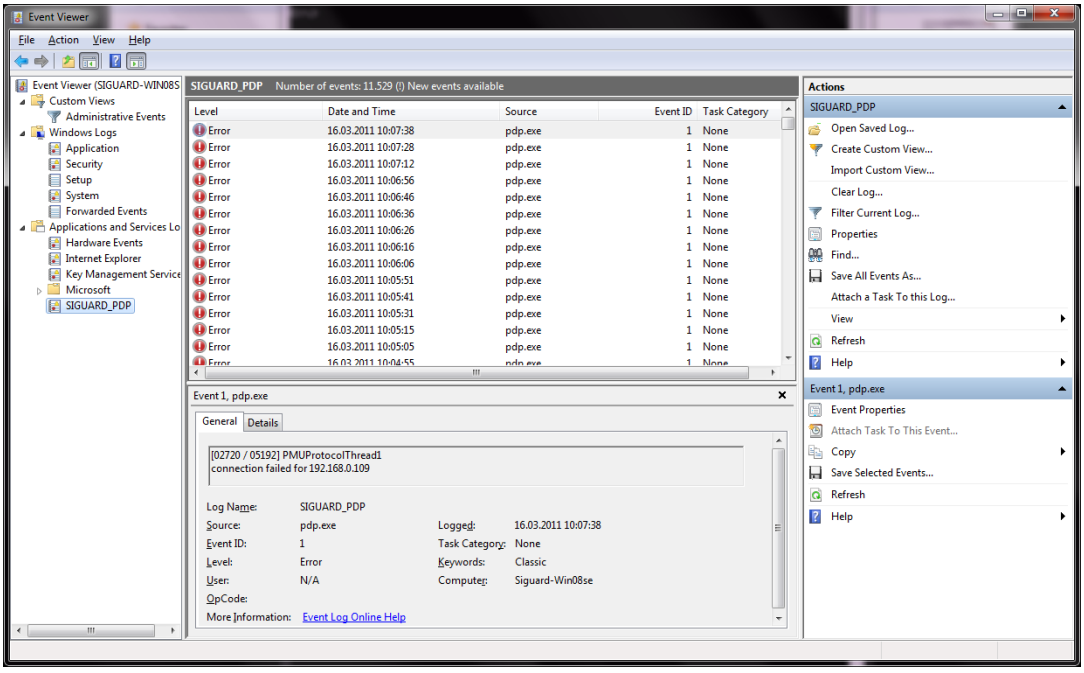

Bild 7-20 Event Viewer im Remote-Zugriff

Hier werden alle Ereignisse des SIGUARD PDP Servers angezeigt.

Protokolldateien speichern

✧ Markieren Sie im **Event Viewer** Fehlermeldungen (Zeilen), die Sie speichern möchten.

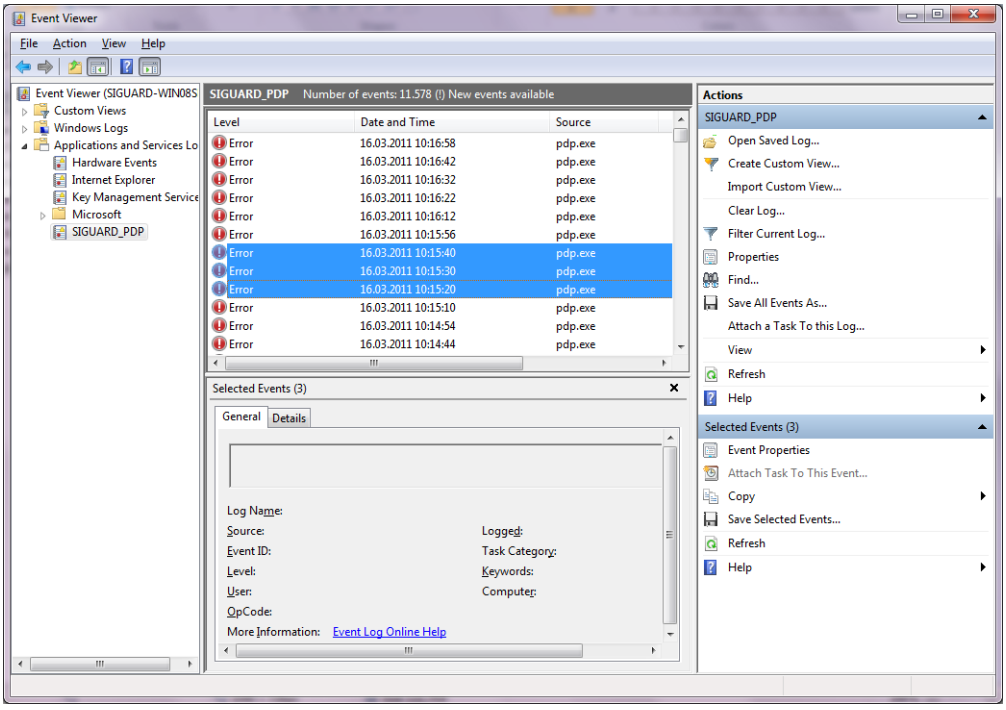

Bild 7-21 Markierte Fehlermeldungen

✧ Wählen Sie im Fenster **Actions** den Menüeintrag **Save Selected Events...**

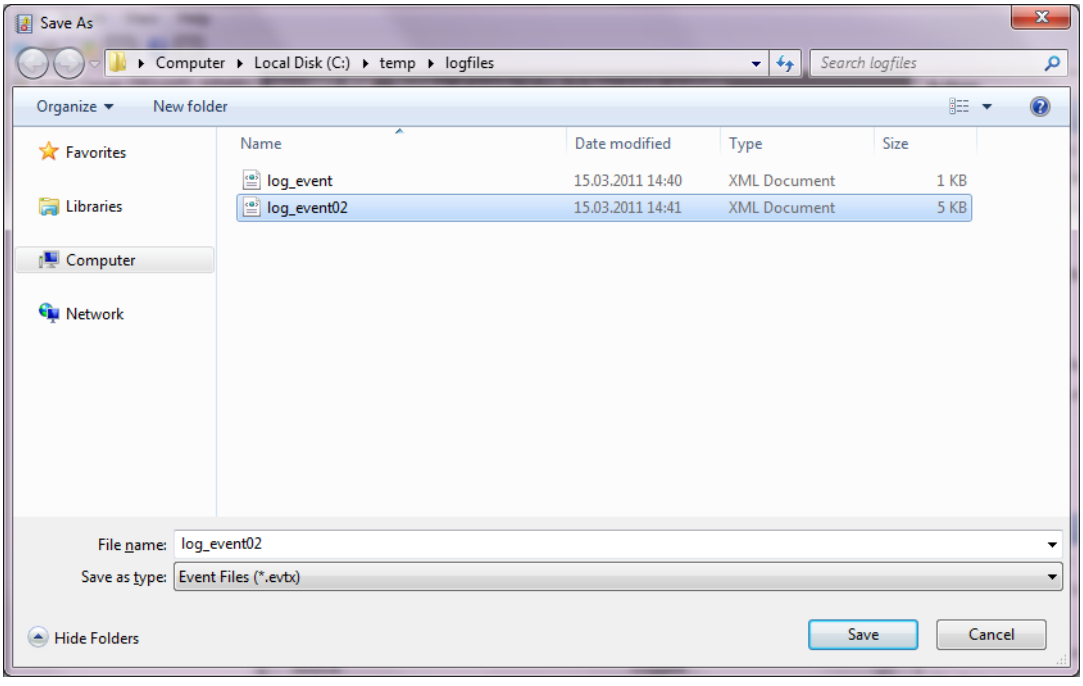

Bild 7-22 Save As...

✧ Geben Sie einen Dateinamen ein.

✧ Wählen Sie das Dateiformat.

✧ Schließen Sie den Dialog mit **Save**.

Protokolldateien im Text- oder XML-Format speichern

Protokolldateien können in folgenden Formaten gespeichert werden

- Textformat
- XML-Format

✧ Wählen Sie im Fenster **Actions** den Menüeintrag **Save All Events As...**

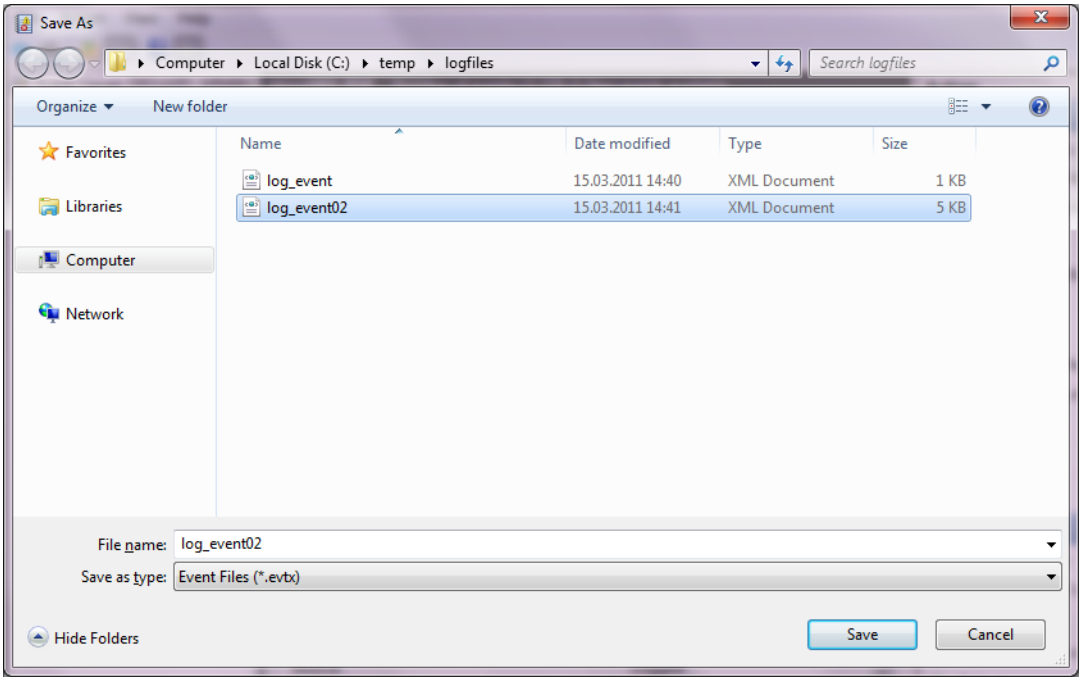

Bild 7-23 Save As...

✧ Geben Sie einen Dateinamen ein.

✧ Wählen Sie das Dateiformat.

✧ Schließen Sie den Dialog mit **Save**.

XML-Datei einsehen

Für spätere Auswertungen können XML-Dokumente geöffnet werden.

✧ Öffnen Sie ein XML-Dokument mit Doppelklick auf den Dateinamen.

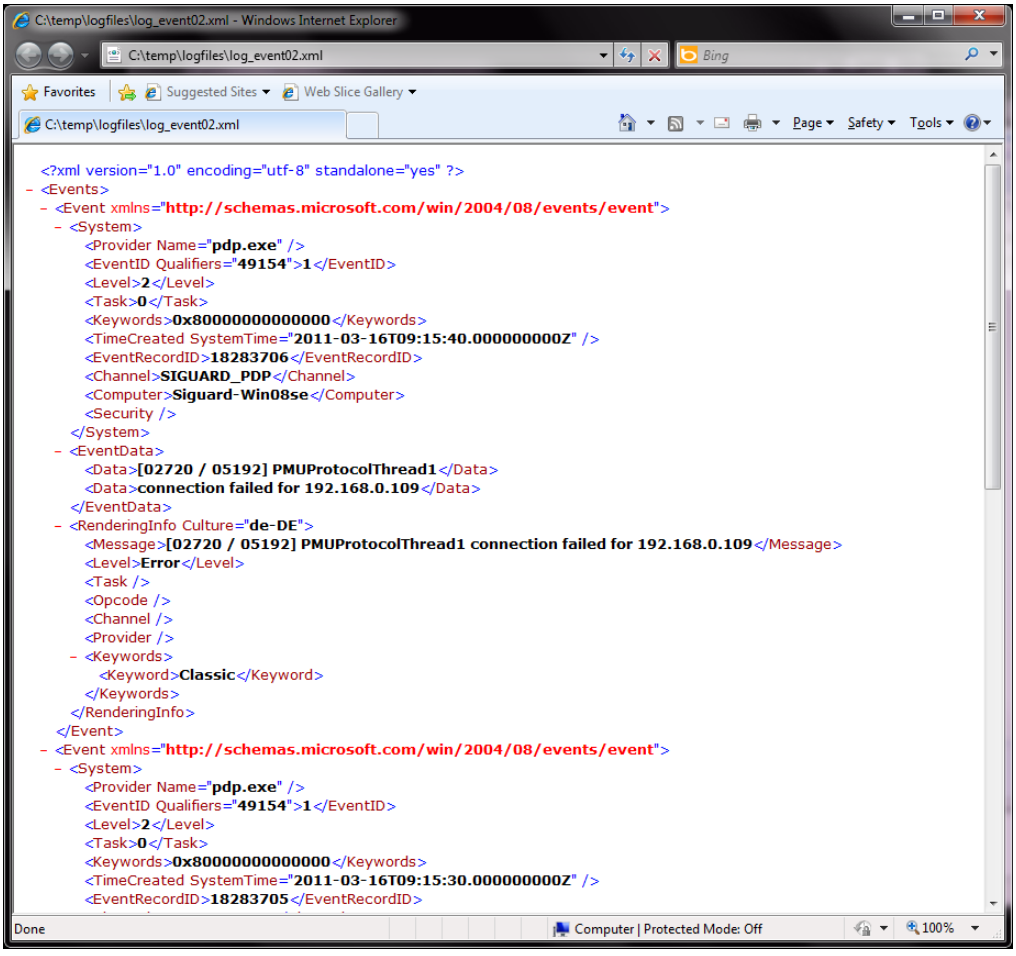

Bild 7-24 Protokolldatei im XML-Format geöffnet

7.4 Benutzerverwaltung

7.4.1 Allgemeines

Ein SIGUARD PDP-System besteht aus einem SIGUARD PDP Server, dem SIGUARD PDP Engineer und der Benutzeroberfläche, dem SIGUARD PDP UI. Falls gewünscht, können alle Komponenten auf ein eigenes System aufgeteilt werden. Um dies umzusetzen, benötigen Sie auf dem SIGUARD PDP Server eine Freigabe für den Remote-Zugriff auf SIGUARD PDP Engineering und SIGUARD PDP UI.

✧ Schalten Sie die Funktion **File and Printer Sharing** für Microsoft-Netzwerke in der Konfiguration Ihrer Netzwerkkarte Ihres SIGUARD PDP-Systems ein.

-- oder --

✧ Lassen Sie eingehenden Datenverkehr über die Desktop-Firewall von Microsoft zu, indem Sie die Funktion **File and Printer Sharing**. markieren.

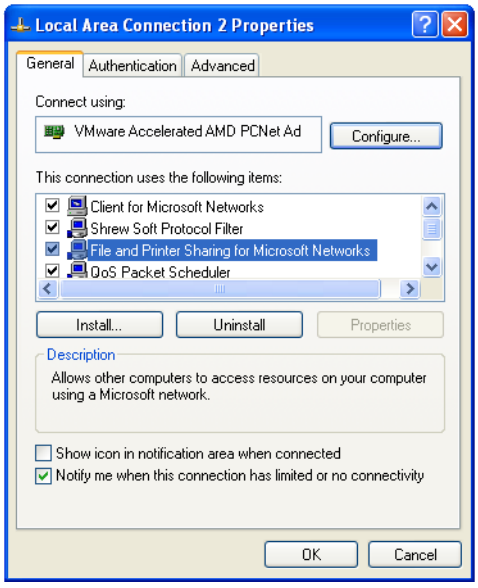

Bild 7-25 Konfiguration der Netzwerkkarte

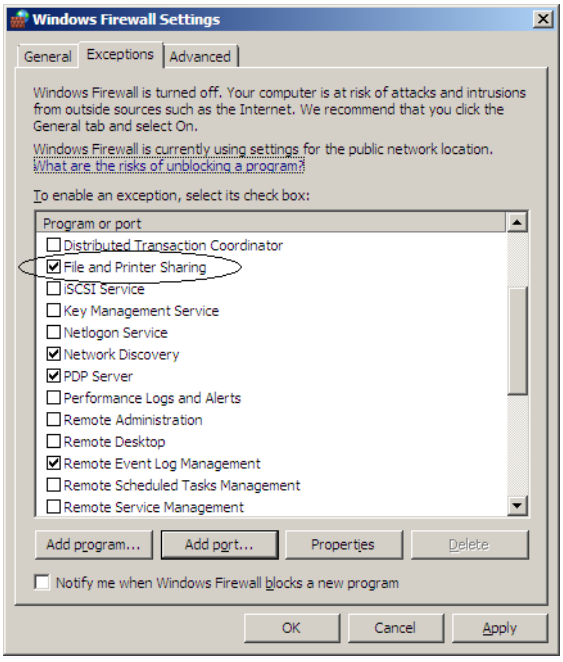

Bild 7-26 Konfiguration über Windows Firewall Settings

Wenn alle Systeme auf einem Rechner installiert sind, ist kein **File and Printer Sharing** erforderlich.

Dann müssen Sie die Funktion **File and Printer Sharing** in der Konfiguration Ihres Netzwerkes Ihres SIGUARD PDP-Systems oder im Fenster **Windows Firewall Settings** auf der Registerkarte **Exceptions** deaktivieren.

In jedem Fall müssen Sie Benutzergruppen für SIGUARD PDP Engineer und SIGUARD PDP UI anlegen und Benutzer den entsprechenden Gruppen zuordnen. Auf dem SIGUARD PDP Server wird bei der Installation automatisch ein Benutzer **SiguardRuntime** angelegt.

In der nachfolgend beschriebenen Konfiguration sind SIGUARD PDP Engineer und SIGUARD PDP UI auf dem gleichen Rechner installiert. Sie sind aber mit entsprechenden Rechten ausgestattet, die es ermöglichen SIGUARD PDP Engineer und SIGUARD PDP UI von verschiedenen Benutzern zu verwenden.

HINWEIS

Für eine leichtere Verwaltung und eine sichere Passwort-Strategie empfiehlt Siemens, das Microsoft Domain Controller-Konzept zu verwenden.

Für die Installation von **Active Directory Domain Services (ADDS)** auf Windows Server 2008 oder Windows 2008 R2, siehe *Webseite AD DS Installation and Removal Step-by-Step Guide von Microsoft*.

Für die Installation von **Active Directory Domain Services (ADDS)** auf Windows Server 2003, Windows Server 2003 mit SP1 oder Windows Server 2003 mit SP2, siehe *Webseite Installing a domain controller von Microsoft*.

7.4.2 Benutzer und Benutzergruppen anlegen

Um mit dem SIGUARD PDP Server arbeiten zu können, erstellen Sie ein SIGUARD PDP-Projekt. Sie erstellen und aktualisieren die Konfigurationsdatei und speichern diese auf dem SIGUARD PDP Server. Wenn Sie die Konfiguration auf einem Remote-Rechner bearbeiten, wird auf dem SIGUARD PDP Server eine Freigabe für

den Remote-Zugriff benötigt. Gemeinsame Ordner sind sehr kritisch in Bezug auf die Sicherheit. Deshalb sollte der Zugriff auf diese gemeinsamen Ordner durch entsprechende Rechte eingegrenzt werden.

Ein SIGUARD PDP-Benutzer darf die Konfigurationsdateien auf dem SIGUARD PDP Server nur lesen und Export-Dateien für das SIGUARD PDP-Logging erstellen. Darüber hinaus benötigt ein SIGUARD PDP-Benutzer Lese- und Schreibzugriff für einen gemeinsamen Export-Ordner auf dem SIGUARD PDP Server.

HINWEIS

Alle Benutzer und Benutzergruppen müssen auf dem SIGUARD PDP Server und dem lokalen Rechner mit gleichem Passwort angelegt werden. Die Zuordnungen von Benutzern zu den Benutzergruppen muss auf allen Rechnern gleich sein.

Benutzergruppen anlegen

- ✧ Öffnen Sie das Fenster **Computer Management** auf dem SIGUARD PDP Server und dem lokalen Rechner, auf dem SIGUARD PDP Engineer und SIGUARD PDP UI installiert sind.
- ✧ Öffnen Sie den Ordner **Local Users and Groups**.
- ✧ Legen Sie die Benutzergruppen **SIGUARD PDP Engineer** und **SIGUARD PDP Users** an.

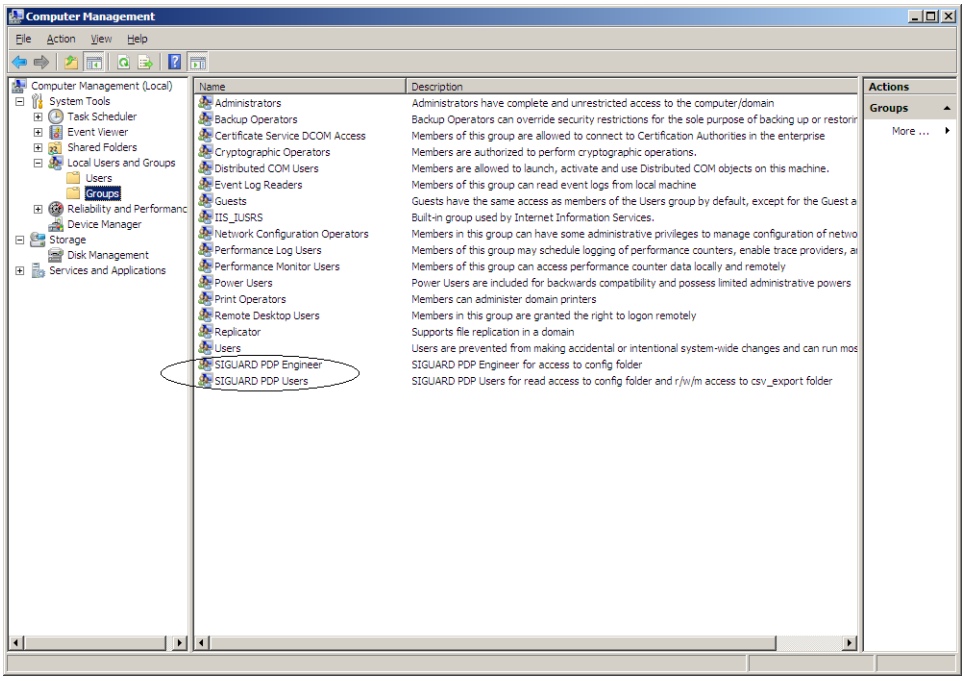

Bild 7-27 Benutzergruppen auf dem SIGUARD PDP Server

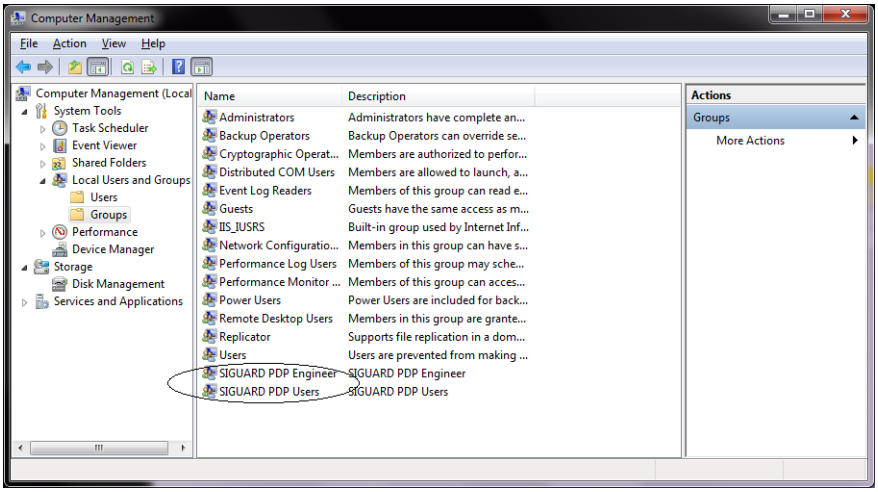

Bild 7-28 Benutzergruppen auf dem SIGUARD PDP Engineer/UI-Rechner

Benutzer SGEng auf dem SIGUARD PDP Server anlegen

In der beschriebenen Konfiguration legen Sie einen Benutzer **SGUser** auf dem SIGUARD PDP Server an, der Mitglied der Benutzergruppe **SIGUARD PDP Users** ist. Danach legen Sie einen Benutzer **SGEng** an, der Mitglied der Benutzergruppe **SIGUARD PDP Engineer** ist.

- ✧ Legen Sie den SIGUARD PDP Engineer-Benutzer **SGEng** an.
- ✧ Legen Sie die Eigenschaften für diesen Benutzer fest.

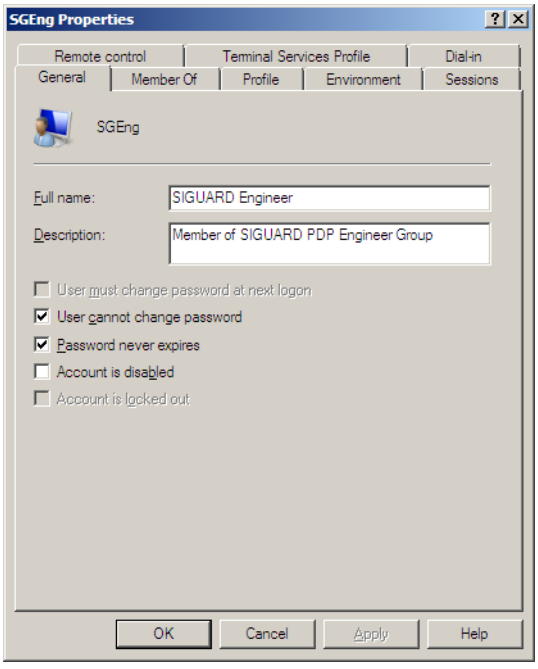

Bild 7-29 General des Benutzers SGEng

- ✧ Geben Sie den Namen und die Beschreibung für den neuen Benutzer ein.
- ✧ Legen Sie die Kriterien für das Passwort fest.

Benutzer SGEng der Benutzergruppe SIGUARD PDP Engineer zuordnen

- ✧ Wählen Sie die Registerkarte **Member Of**, um den Benutzer **SGEng** der Benutzergruppe **SIGUARD PDP Engineer** zuzuordnen.
- ✧ Klicken Sie auf **Add...**

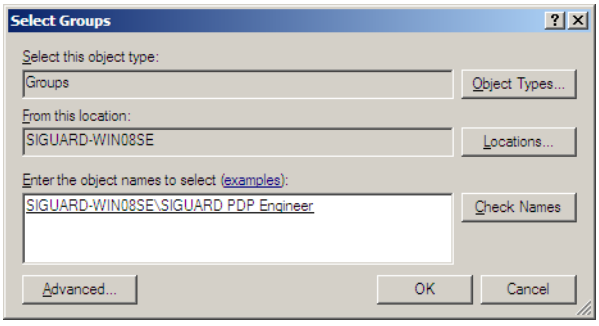

Bild 7-30 Select Groups

- ✧ Markieren Sie die Benutzergruppe **SIGUARD PDP Engineer**.
- ✧ Bestätigen Sie Ihre Auswahl mit **OK**.

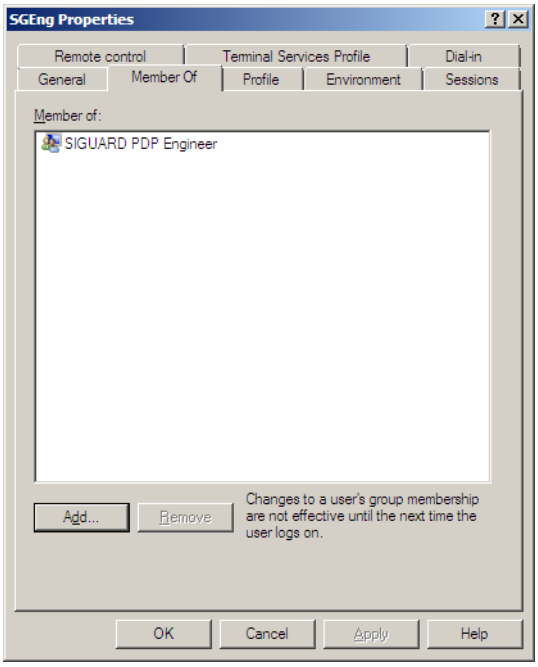

Bild 7-31 Member Of des Benutzers SGEng

Benutzer SGUser auf dem SIGUARD PDP Server anlegen

- ✧ Legen Sie den SIGUARD PDP Engineer-Benutzer **SGUser** an.
- ✧ Legen Sie die Eigenschaften für diesen Benutzer fest.

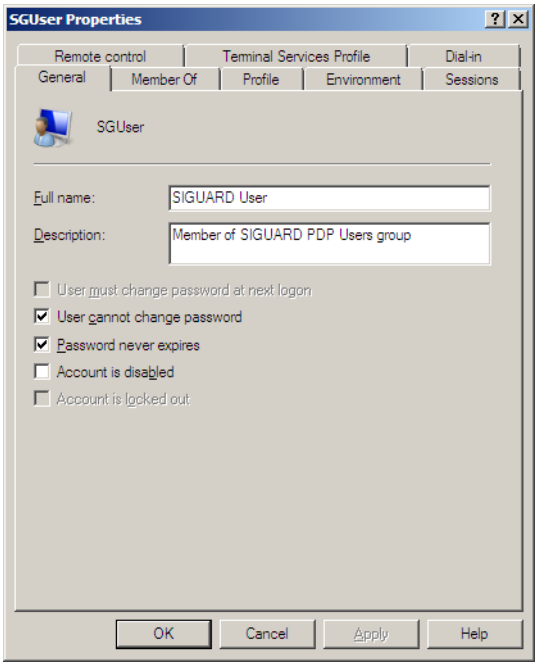

Bild 7-32 General des Benutzers SGUser

- ✧ Geben Sie den Namen und die Beschreibung für den neuen Benutzer ein.
- ✧ Legen Sie die Kriterien für das Passwort fest.

Benutzer SGUser der Benutzergruppe SIGUARD PDP User zuordnen

- ✧ Wählen Sie die Registerkarte **Member Of**, um den Benutzer **SGUser** der Benutzergruppe **SIGUARD PDP Users** zuzuordnen.
- ✧ Klicken Sie auf **Add...**

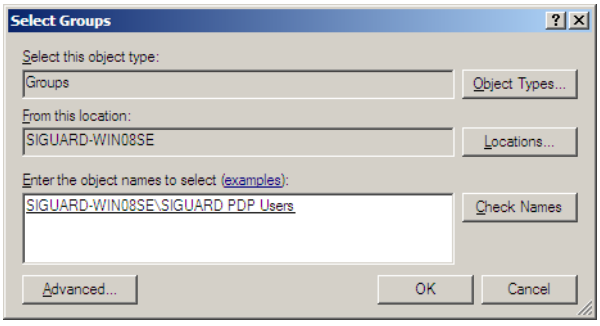

Bild 7-33 Select Groups

- ✧ Markieren Sie die Benutzergruppe **SIGUARD PDP Users**.
- ✧ Bestätigen Sie Ihre Auswahl mit **OK**.

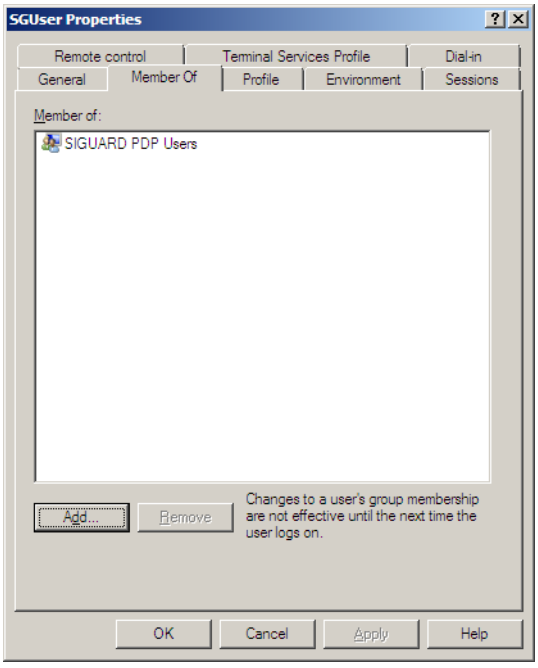

Bild 7-34 Member Of des Benutzers SGUser

✧ Schließen Sie den Dialog mit **OK**.

Die neuen Benutzer werden in die Liste **Users** aufgenommen.

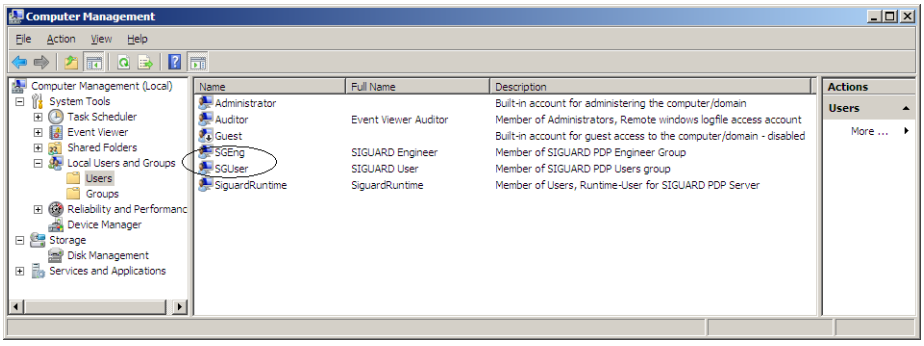

Bild 7-35 Benutzer auf dem SIGUARD PDP Server

Benutzer anlegen auf dem SIGUARD PDP Engineer-/UI-Rechner

Auf dem SIGUARD PDP Engineer-/UI-Rechner legen Sie die gleichen Benutzer an, wie auf dem SIGUARD PDP Server, die zusätzlich Mitglieder der Windows-Benutzergruppe **Users** sind.

✧ Legen Sie den SIGUARD PDP Engineer-Benutzer **SGEng** an.

✧ Legen Sie die Eigenschaften für diesen Benutzer fest.

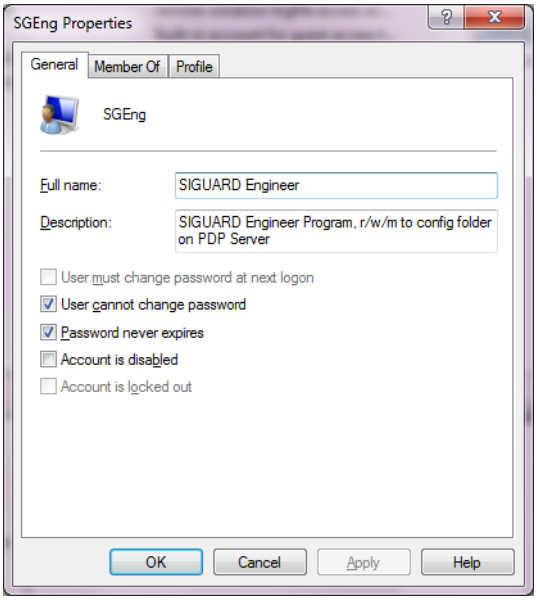

Bild 7-36 General des Benutzers SGEng

- ✧ Geben Sie den Namen und die Beschreibung für den neuen Benutzer ein.
- ✧ Legen Sie die Kriterien für das Passwort fest.

Benutzergruppe zuordnen

- ✧ Wählen Sie die Registerkarte **Member Of**, um den Benutzer **SGEng** der Benutzergruppe **SIGUARD PDP Engineer** und der Benutzergruppe **Users** zuzuordnen.

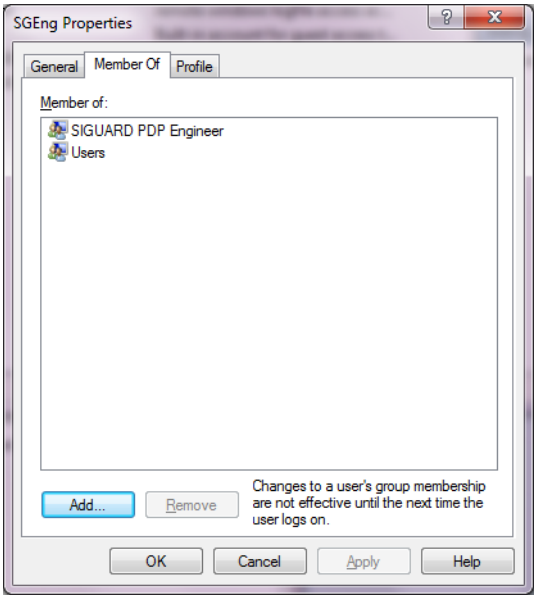

Bild 7-37 Zugeordnete Benutzergruppen des Benutzers SGEng

- ✧ Schließen Sie den Dialog mit **OK**.

✧ Wiederholen Sie die Zuordnung des Benutzers **SGUser** zur Benutzergruppe **SIGUARD PDP Users** und zur Benutzergruppe **Users**.

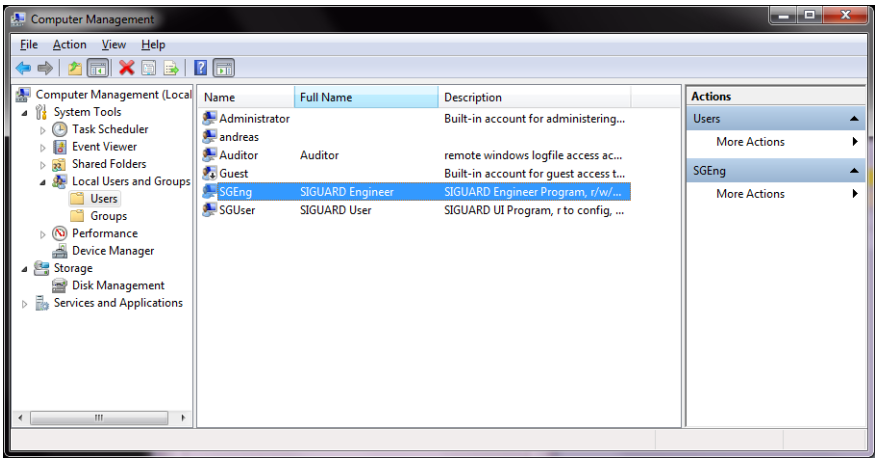

Bild 7-38 Zuordnung des Benutzers SGUser

7.4.3 Zugriffsrechte auf den gemeinsamen Ordner des SIGUARD PDP Servers anlegen

Allgemeines

Auf dem SIGUARD PDP Server gibt es 2 gemeinsame Ordner, **Config** und **CSV-Export**, auf die vom SIGUARD PDP Engineering/UI-Rechner Zugriff bestehen muss.

✧ Geben Sie der Benutzergruppe **SIGUARD PDP Engineer** Lese-/Schreib- und Änderungsrechte für den gemeinsamen Ordner **Config** und Lesezugriff für den gemeinsamen Ordner **CSV-Export**.

✧ Geben Sie der Benutzergruppe **SIGUARD PDP Users** Lese-/Schreib- und Änderungsrechte für den gemeinsamen Ordner **CSV-Export** und Lesezugriff für den gemeinsamen Ordner **Config**.

✧ Geben Sie zusätzlich diesen gemeinsamen Ordner **nur** für diese 2 Benutzergruppen für den Remote-Zugriff frei, falls der SIGUARD PDP Server auf einem anderen Rechner installiert ist als SIGUARD PDP Engineering/UI.

Die Zugriffsrechte für die 2 Benutzergruppen auf die gemeinsamen Ordner müssen nicht über Sicherheitseinstellungen eingeschränkt werden.

Gemeinsame Ordner fehlen

✧ Wenn die beiden Ordner auf Ihrem System noch nicht vorhanden sind, legen Sie diese in folgenden Pfaden an:

..\ProgramData\Siemens Energy\SIGUARD PDP\Config und

..\ProgramData\Siemens Energy\SIGUARD PDP\CSV-Export

✧ Vergeben Sie für beide Benutzergruppen getrennt die vollen Zugriffsrechte wie nachfolgend beschrieben.

Zugriffsrechte für den Ordner Config einrichten

✧ Zeigen Sie die gemeinsamen Ordner des SIGUARD PDP Servers an.

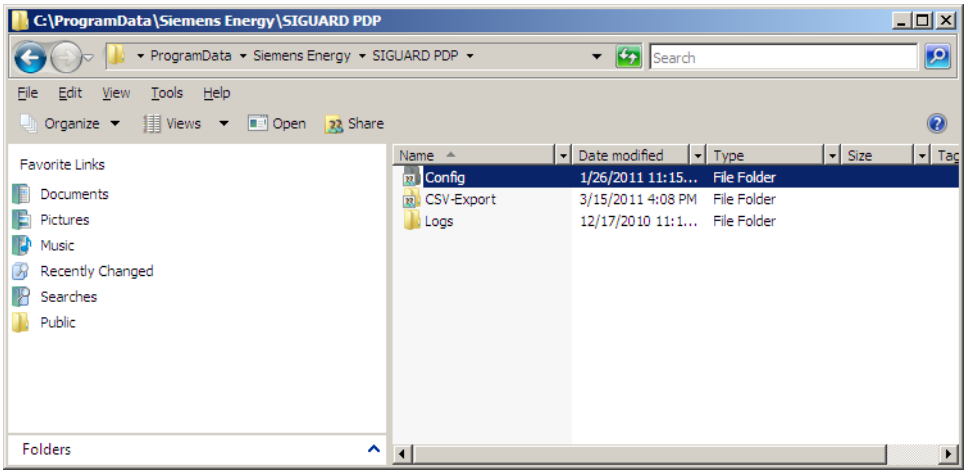

Bild 7-39 Gemeinsamer Ordner Config auf dem SIGUARD PDP Server

✧ Klicken Sie mit der rechten Maustaste auf den Ordner **Config** und wählen Sie den Menüeintrag **Advanced**, um dessen Sicherheitseinstellungen zu bearbeiten.

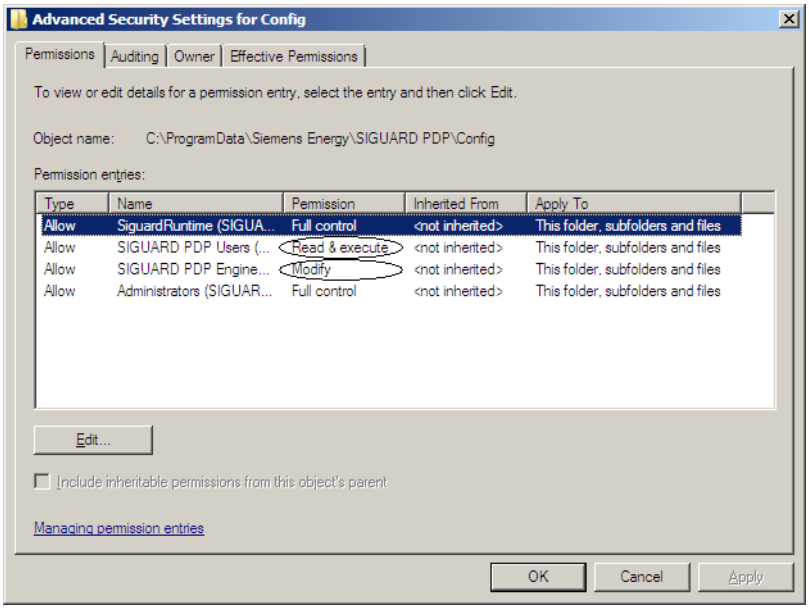

Bild 7-40 Zugriffsrechte für den Ordner Config

✧ Um einen Sicherheitseintrag zu bearbeiten, markieren Sie auf der Registerkarte **Permissions** den entsprechenden Eintrag und klicken Sie auf **Edit...**

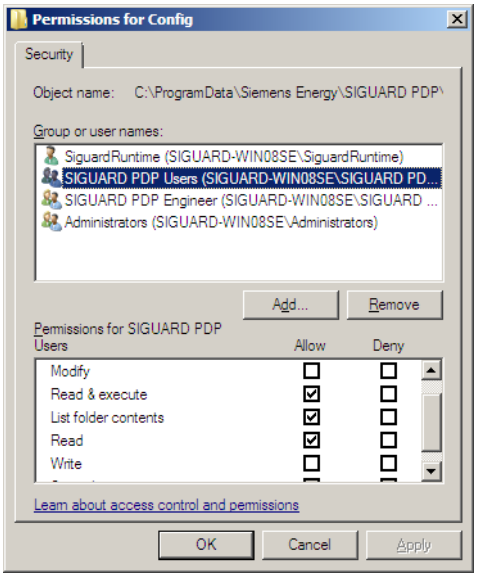

Bild 7-41 Zugriffsrechte für die Benutzergruppe SIGUARD PDP Users

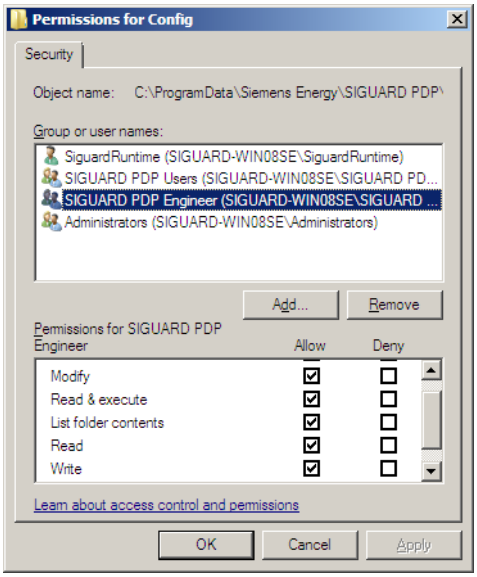

Bild 7-42 Zugriffsrechte für die Benutzergruppe SIGUARD PDP Engineer

✧ Schließen Sie den Dialog mit **OK**.

Zugriffsrechte für den Ordner CSV-Export einrichten

✧ Zeigen Sie die gemeinsamen Ordner des SIGUARD PDP Servers an.

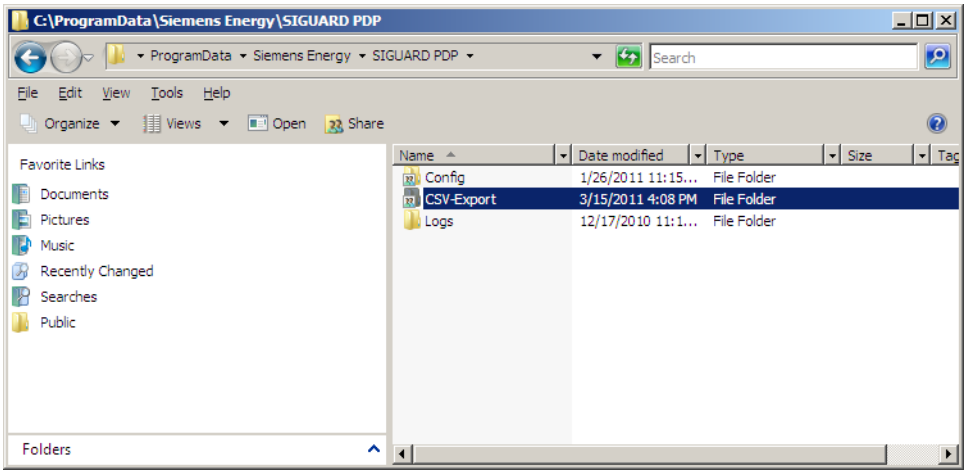

Bild 7-43 Gemeinsamer Ordner CSV-Export auf dem SIGUARD PDP Server

✧ Klicken Sie mit der rechten Maustaste auf den Ordner **CSV-Export** und wählen Sie den Menüeintrag **Advanced**, um dessen Sicherheitseinstellungen zu bearbeiten.

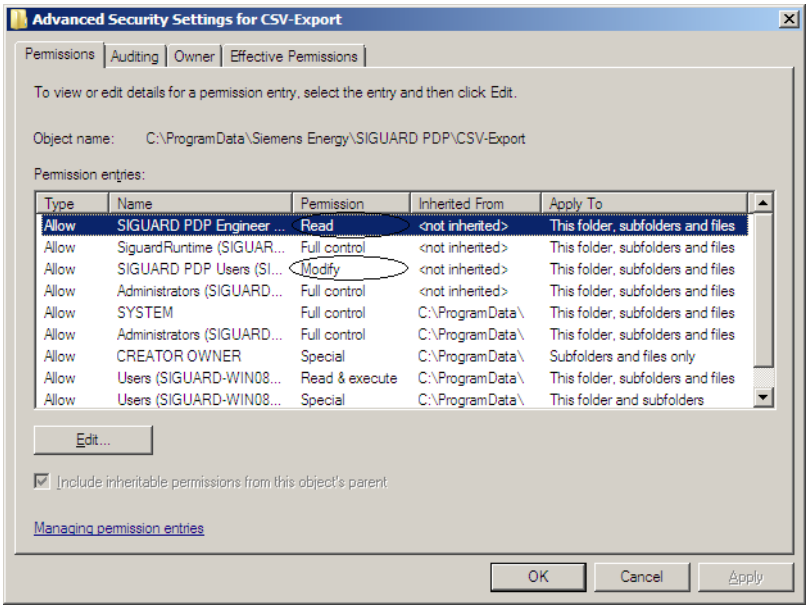

Bild 7-44 Zugriffsrechte für den Ordner CSV-Export

✧ Um einen Sicherheitseintrag zu bearbeiten, markieren Sie auf der Registerkarte **Permissions** den entsprechenden Eintrag und klicken Sie auf **Edit...**

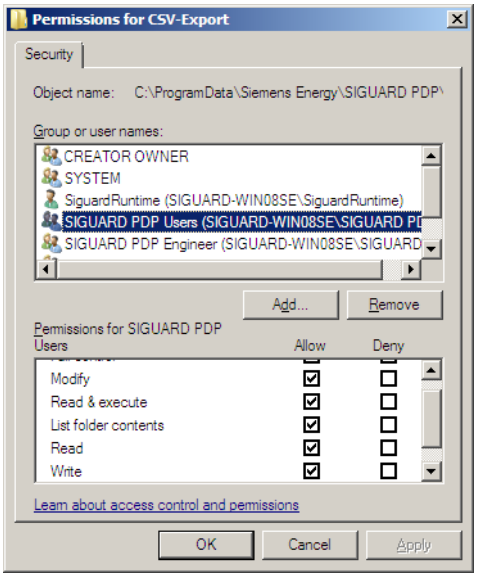

Bild 7-45 Zugriffsrechte für die Benutzergruppe SIGUARD PDP Users

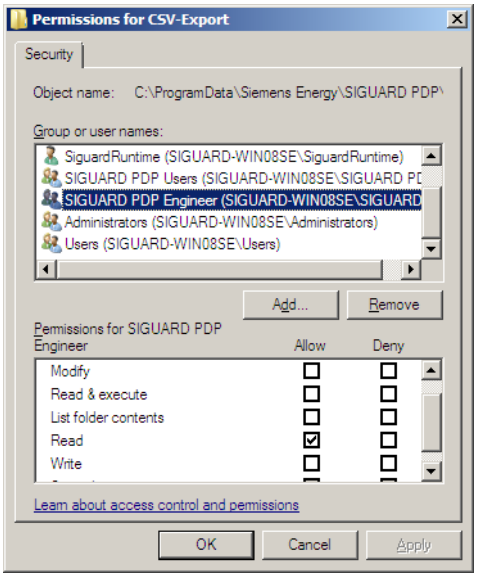

Bild 7-46 Zugriffsrechte für die Benutzergruppe SIGUARD PDP Engineer

✧ Schließen Sie den Dialog mit **OK**.

7.4.4 Lokale Zugriffsrechte einstellen

Allgemeines

Falls **SIGUARD PDP Engineer** und **SIGUARD PDP UI** auf dem gleichen Rechner installiert sind, müssen Sie die Zugriffsrechte gesondert einstellen.

✧ Geben Sie der Benutzergruppe **SIGUARD PDP Engineer** nur Zugriffsrechte für das Programm **SIGUARD PDP Engineer**.

✧ Geben Sie der Benutzergruppe **SIGUARD PDP Users** nur Zugriffsrechte für das Programm **SIGUARD PDP UI**.

Wenn ein Benutzer beide Aufgaben übernimmt, werden ihm beide Benutzergruppen zugeordnet. Diese Benutzergruppen benötigen Rechte zum Lesen und Ausführen für das Hauptverzeichnis **SIGUARD PDP** auf dem lokalen Rechner (SIGUARD PDP Engineer-/UI-Rechner).

HINWEIS

Wenn ein SIGUARD PDP-Ingenieur Zugriffsrechte auf den SIGUARD PDP UI-Rechner benötigt, fügen Sie Ihn als Mitglied der Benutzergruppe **SIGUARD PDP Users** hinzu.

Zugriffsrechte für den SIGUARD PDP-Ordner

Für den Ordner **SIGUARD PDP** im Pfad **\Program Files\Siemens Energy** auf dem lokalen Rechner müssen Sie für beide SIGUARD-Benutzergruppen Rechte zum Lesen, Ausführen und zum Anzeigen des Ordnerinhaltes vergeben.

✧ Öffnen Sie den Pfad **\Program Files\Siemens Energy**.

✧ Öffnen Sie für den Ordner **SIGUARD PDP** das Fenster **Advanced Security Settings for SIGUARD PDP**

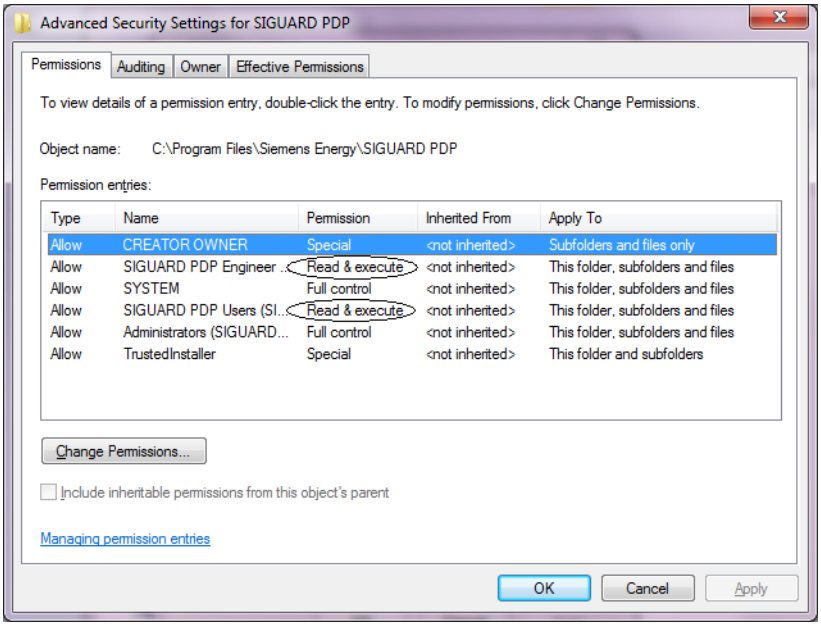

Bild 7-47 Sicherheitseinstellungen für den lokalen Ordner SIGUARD PDP

✧ Markieren Sie den entsprechenden Eintrag und klicken Sie auf **Change Permissions...**, um dessen Zugriffsrechte zu bearbeiten.

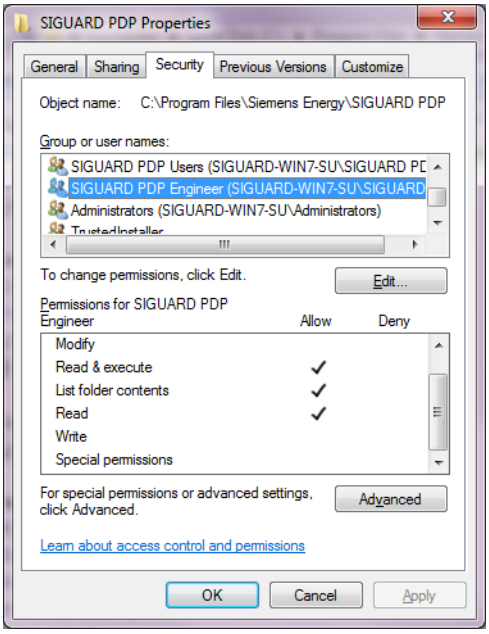

Bild 7-48 Zugriffsrechte der Benutzergruppe SIGUARD PDP Engineer auf den SIGUARD PDP-Ordner

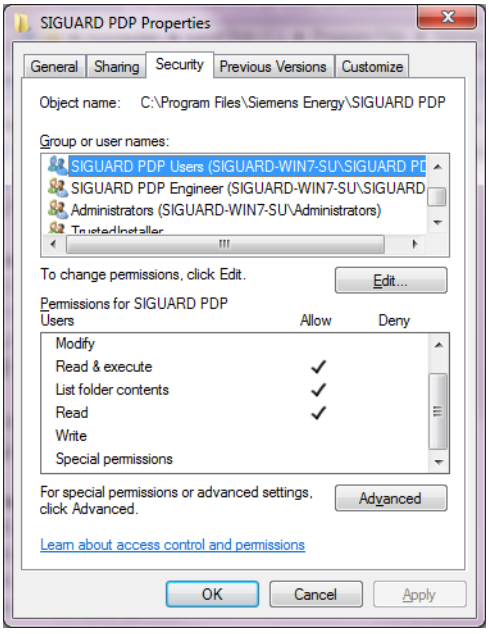

Bild 7-49 Zugriffsrechte der Benutzergruppe SIGUARD PDP Users auf den SIGUARD PDP-Ordner

✧ Schließen Sie den Dialog mit **OK**.

Bearbeiten der Zugriffsrechte auf das Programm SIGUARD PDP UI

✧ Öffnen Sie das Eigenschaftenfenster von **SiguardUI.exe**.

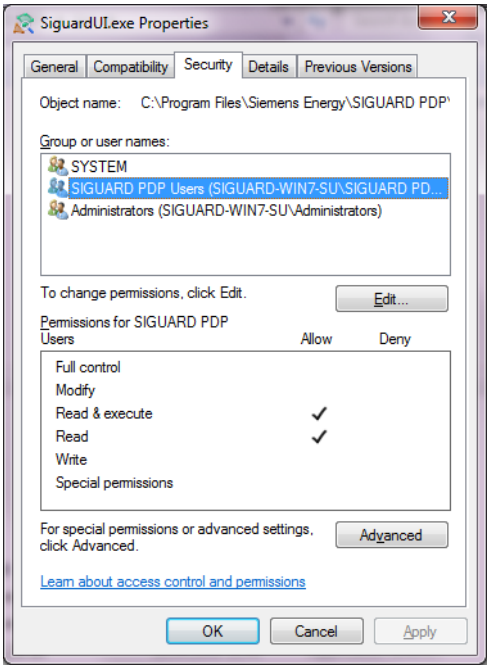

Bild 7-50 Zugriffsrechte für SIGUARD PDP UI

- ✧ Markieren Sie die Benutzergruppe und klicken Sie auf **Edit...**, um deren Rechte zu ändern.
- ✧ Markieren Sie die Benutzergruppe und klicken Sie auf **Advanced...**, um deren erweiterte Einstellungen zu ändern.
- ✧ Schließen Sie den Dialog mit **OK**.

Bearbeiten der Zugriffsrechte auf das Programm SIGUARD PDP Engineer

- ✧ Öffnen Sie das Eigenschaftenfenster von **Engineer.exe** und verfahren Sie wie bei SIGUARD PDP UI, um die Programmeinstellungen zu ändern.

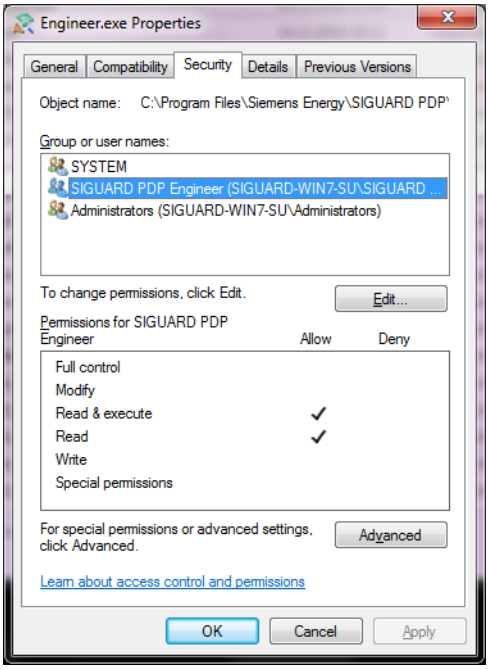

Bild 7-51 Zugriffsrechte für SIGUARD PDP Engineer

Bearbeiten der Zugriffsrechte für das Programm SIGUARD PDP Communication UI

Diese Einstellungen sind nur auf dem SIGUARD PDP Server erforderlich.

✧ Öffnen Sie das Eigenschaftenfenster von **Comm_UI.exe** und verfahren Sie wie bei SIGUARD PDP UI, um die Programmeinstellungen zu ändern.

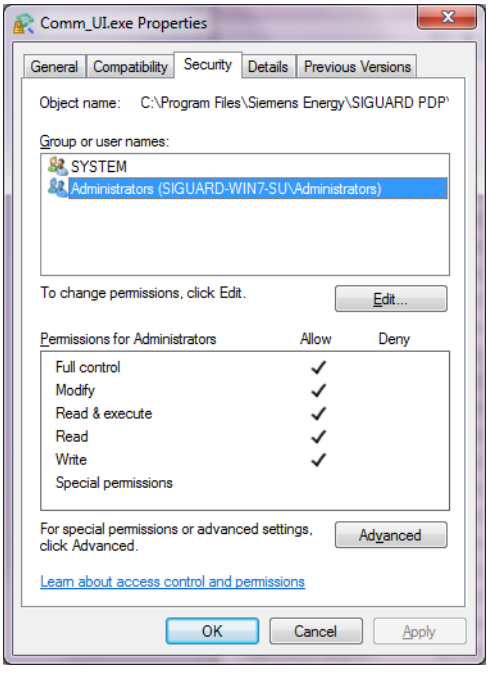

Bild 7-52 Zugriffsrechte für SIGUARD PDP Communication UI

7.5 IPSec Tunneling

7.5.1 IPSec-Tunnel zwischen SIGUARD PDP Server und lokalem Rechner

7.5.1.1 Allgemeines

Wegen des Datenaustausches von reinem Text zwischen dem SIGUARD PDP Server und dem SIGUARD PDP Engineer-/UI-Rechner empfiehlt Siemens, einen beglaubigten und vertrauenswürdigen VPN-Verbindungstunnel (Virtual Private Network) eines Fremdherstellers zu verwenden, der den entsprechenden Richtlinien entspricht.

IPSec (Internet Protocol Security) ist ein Sicherheitsprotokoll, das für die Kommunikation über IP-Netze die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleistet. Es wird zum Aufbau virtueller, privater Netzwerke verwendet.

Es ist sehr einfach, dieses in Windows implementierte IPSec zu verwenden. IPSec ist unter anderem in Windows XP, Windows 7 und Windows Server 2008 enthalten.

In der folgenden Konfiguration wird die PSK-Authentifikation und die ESP-Verschlüsselung verwendet.

Preshared Key (vorher vereinbarter Schlüssel) oder kurz PSK bezeichnet ein Verschlüsselungsverfahren, bei denen die Schlüssel vor der Kommunikation beiden Teilnehmern bekannt sein müssen. Encapsulating Security Payload (ESP) stellt die Authentisierung, Integrität und Vertraulichkeit von IP-Paketen sicher. ESP basiert direkt auf IP und verwendet die IP-Protokoll Nummer 50.

Am einfachsten ist es, IPSec mit PSK-Authentifikation für ein Administrator-Benutzerkonto auf einem SIGUARD PDP Server und einem SIGUARD PDP Engineer/UI-Rechner einzurichten, da bei SIGUARD nur wenige Systeme eingebunden sind. Installieren Sie keine weitere Software für die IPSec-Authentifikation/-Verschlüsselung. Somit sind die Vollständigkeit und die Vertraulichkeit der Daten gewährleistet.

Gehen Sie vor wie folgt:

- ✧ Konfigurieren Sie den IPSec-Tunnel auf dem SIGUARD PDP Server.
- ✧ Exportieren Sie die Konfigurationsdaten.
- ✧ Importieren Sie die Konfigurationsdaten auf dem lokalen Rechner.

7.5.1.2 IPSec-Konfiguration

Einfügen des IPSec Snap-in

- ✧ Starten Sie die **Configuration Management Console**.
- ✧ Wählen Sie das Menü **Add/Remove Snap-in...** .

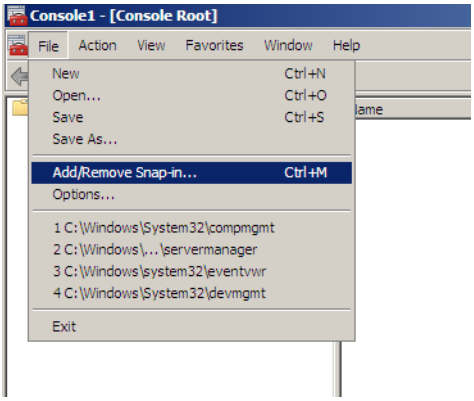

Bild 7-53 Configuration Management Console

✧ Markieren Sie das Snap-in **IP Security Monitor** und **IP Security Policy Manager** und fügen Sie diese mit **Add >** zu den ausgewählten Snap-ins hinzu.

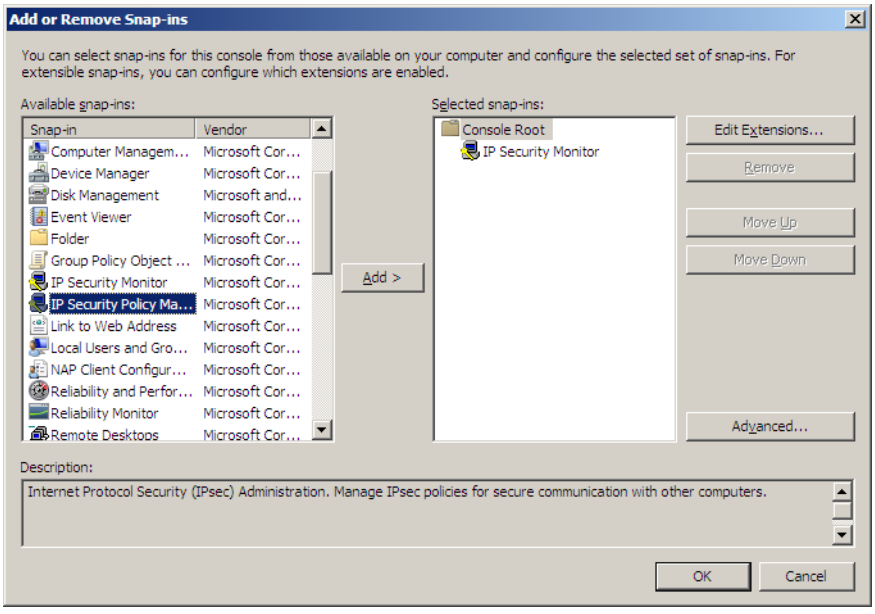

Bild 7-54 IP Security Policy Snap-in hinzufügen

✧ Bestätigen Sie die Auswahl mit **OK**.

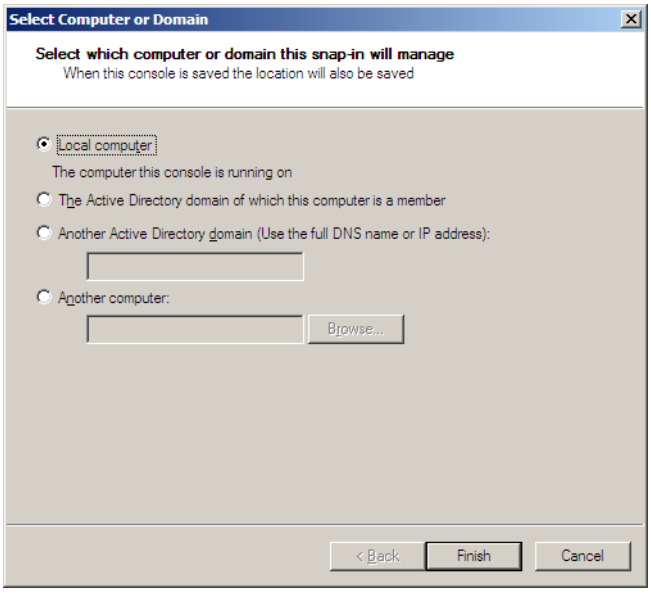

Bild 7-55 Auswahl des lokalen Rechners

✧ Markieren Sie mit **Local Computer** den Rechner, auf dem diese Konfiguration laufen soll.

✧ Schließen Sie den Dialog mit **Finish**.

Festlegen einer Sicherheitsstrategie und Filtereinstellungen

Mit dem Assistenten in der **Configuration Management Console** stellen Sie folgende Funktionen ein:

- Erstellen einer IPSec-Richtlinie mit **Create IP Security Policy...**
- Filtereinstellungen für den Export mit **Manage IP filter lists and filter actions...**

HINWEIS

Beachten Sie, dass immer beide Übertragungsrichtungen für die Richtlinien und Filtereinstellungen benötigt werden.

✧ Klicken Sie mit der rechten Maustaste auf das Snap-in **IP Security Policies on Local Computer**.

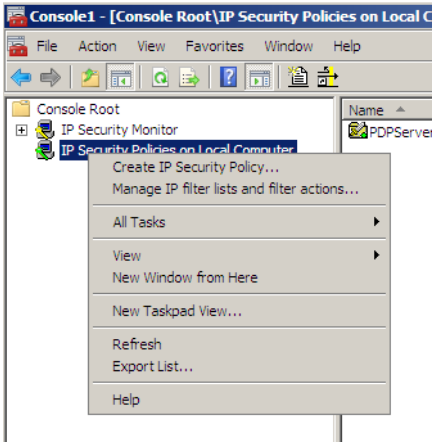

Bild 7-56 Aufruf der Snap-ins

Filterbearbeitung

- ✧ Wählen Sie den Menüeintrag **Manage IP filter lists and filter actions...**
- ✧ Wählen Sie die Registerkarte **Filter Action**

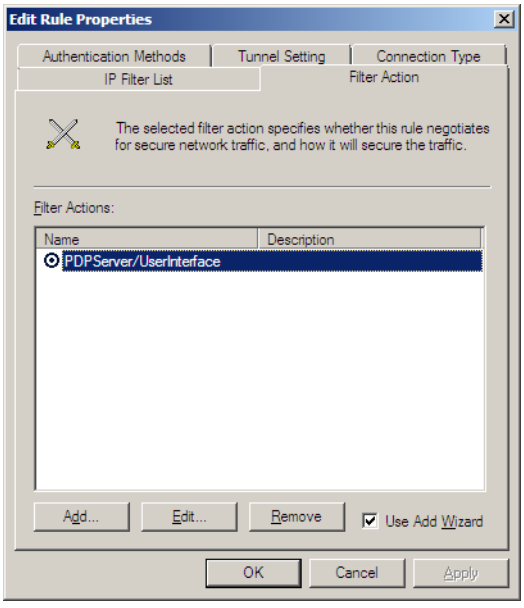

Bild 7-57 Filter hinzufügen und Einstellungen bearbeiten

- ✧ Wählen Sie **Add...**, um ein neues Filter zu erstellen.
- ✧ Markieren Sie ein Filter und wählen Sie **Edit...**, um dessen Eigenschaften zu bearbeiten.

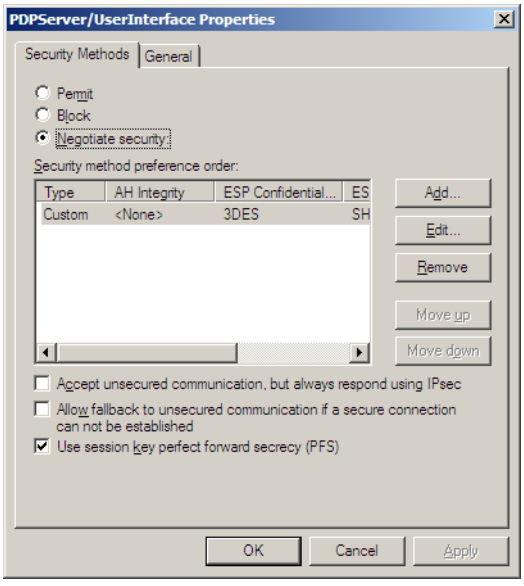

Bild 7-58 Filtereinstellungen bearbeiten

- ✧ Markieren Sie **Negotiate security**. Die Sicherheitsregeln für die Übertragung werden vom System ausgehandelt, z.B. welche Regeln und welche Algorithmen verwendet werden.
- ✧ Markieren Sie **PFS (Perfect Forward Security)**. Der Filter verwendet einen Schlüssel mit perfekt fortgesetzter Geheimhaltung, ein Verschlüsselungsverfahren, bei dem aus einem aufgedeckten Schlüssel nicht auf vorhergehende oder nachfolgende Schlüssel eines Kommunikationskanals geschlossen werden kann.
- ✧ Um die Sicherheitsmethode festzulegen, wählen Sie **Edit...**.

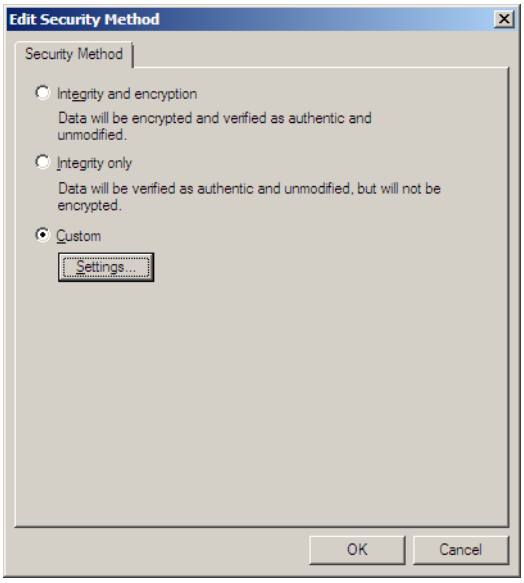

Bild 7-59 Sicherheitsmethode festlegen

- ✧ Um diese Sicherheitsmethode zu konfigurieren, wählen Sie **Settings...**.

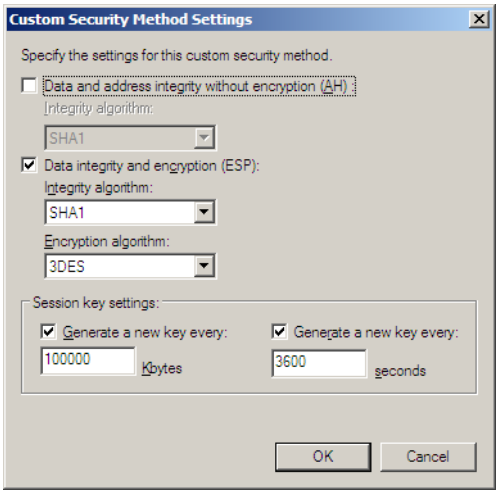

Bild 7-60 Sicherheitsmethode konfigurieren

- ✧ Wählen Sie **ESP** als Methode für die Datenverschlüsselung und die Datensicherheit.

- ✧ Wählen Sie aus der Ausklappliste **SHA-1** als Sicherheitsalgorithmus und **3DES** als Verschlüsselungsalgorithmus.
- ✧ Behalten Sie die Einstellungen für **Session key** bei.
- ✧ Bestätigen Sie Ihre Einstellungen in den Fenstern **Security Method Settings**, **Edit Security Method** und **PDPServer/UserInterface Properties** mit **OK**.

Definition der IPSec-Sicherheitsregeln

- ✧ Wählen Sie das Menü **Create IP Security Policy...**
- ✧ Wählen Sie die Registerkarte **Rules**

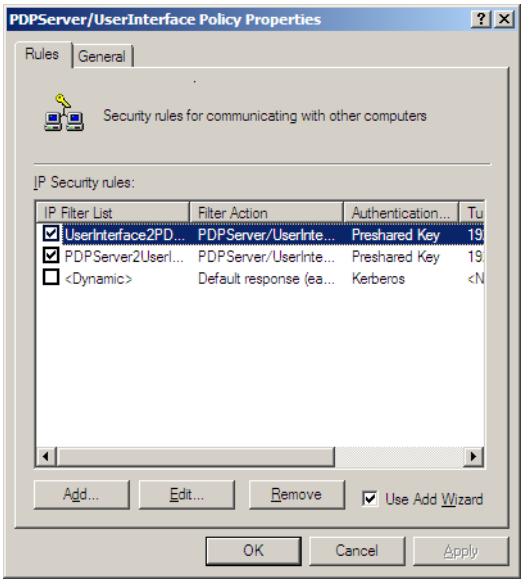

Bild 7-61 IPSec-Sicherheitsregel UserInterface2PDPServer

- ✧ Um 2 neue Sicherheitsregeln **Filter PDP Engineer/UI system (UserInterface) > PDPServer** und **PDPServer > UserInterface** hinzuzufügen, wählen Sie **Add...**.
- ✧ Setzen Sie einen Haken in das Kontrollkästchen, damit beide Regeln nach dem PSK-Verschlüsselungsverfahren arbeiten.
- ✧ Markieren Sie eine Sicherheitsregel und wählen Sie **Edit...**, um deren Eigenschaften zu bearbeiten.
- ✧ Wählen Sie die Registerkarte **IP Filter List**.

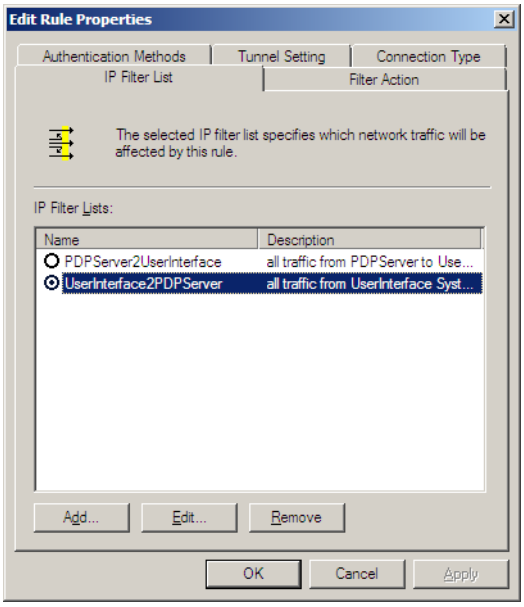

Bild 7-62 Bearbeiten der Sicherheitsregel UserInterface2PDPServer

✧ Markieren Sie das Filter **UserInterface2PDPServer**, um dessen Eigenschaften zu bearbeiten.

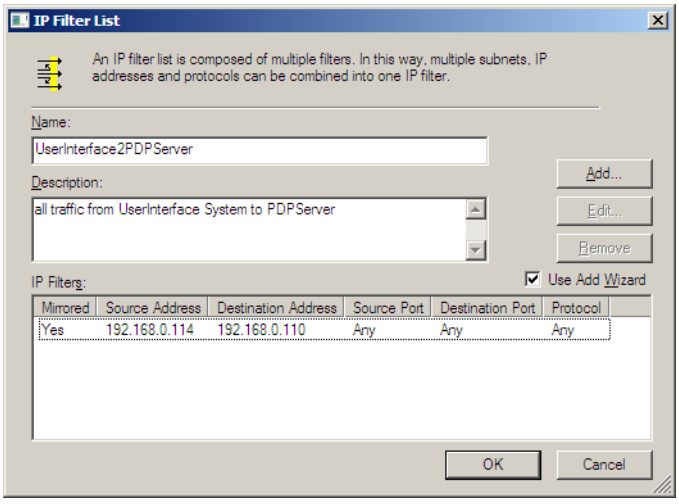

Bild 7-63 IP Filter List

✧ Geben Sie die IP-Adresse des SIGUARD PDP Engineering/UI-Rechners oder dessen Domain-Namen als **Source Address** ein.

✧ Geben Sie die IP-Adresse des SIGUARD PDP Servers oder dessen Domain-Namen als **Destination Address** ein.

✧ Damit alle Protokolle, z.B. UDP, TCP und Port 445 und 139 durch den IPSec-Tunnel gelangen können, geben Sie in der Spalte **Protocol Any** ein.

✧ Schließen Sie den Dialog mit **OK**.

✧ Wählen Sie die Registerkarte **Tunnel Setting**.

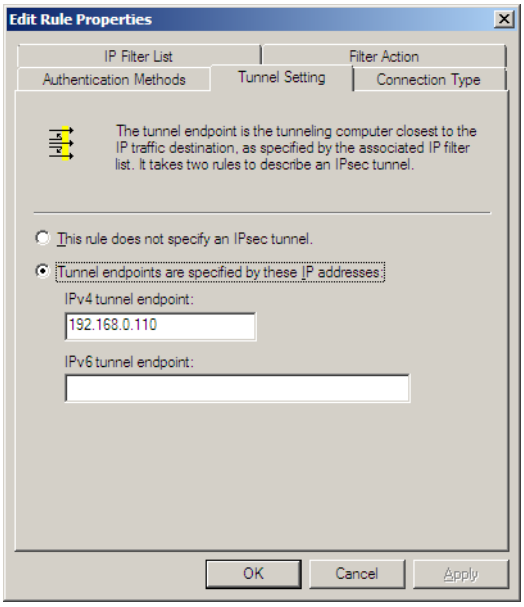

Bild 7-64 Einstellungen für den IPSec-Tunnel

✧ Markieren Sie **Tunnel endpoints are specified by these IP addresses**.

Bei diesem Eintrag in der IP-Filterliste ist die **Destination Address** der Tunnelendpunkt des SIGUARD PDP Servers.

✧ Schließen Sie den Dialog mit **OK**.

✧ Wählen Sie die Registerkarte **Connection Type**, um den Verbindungstyp einzustellen.

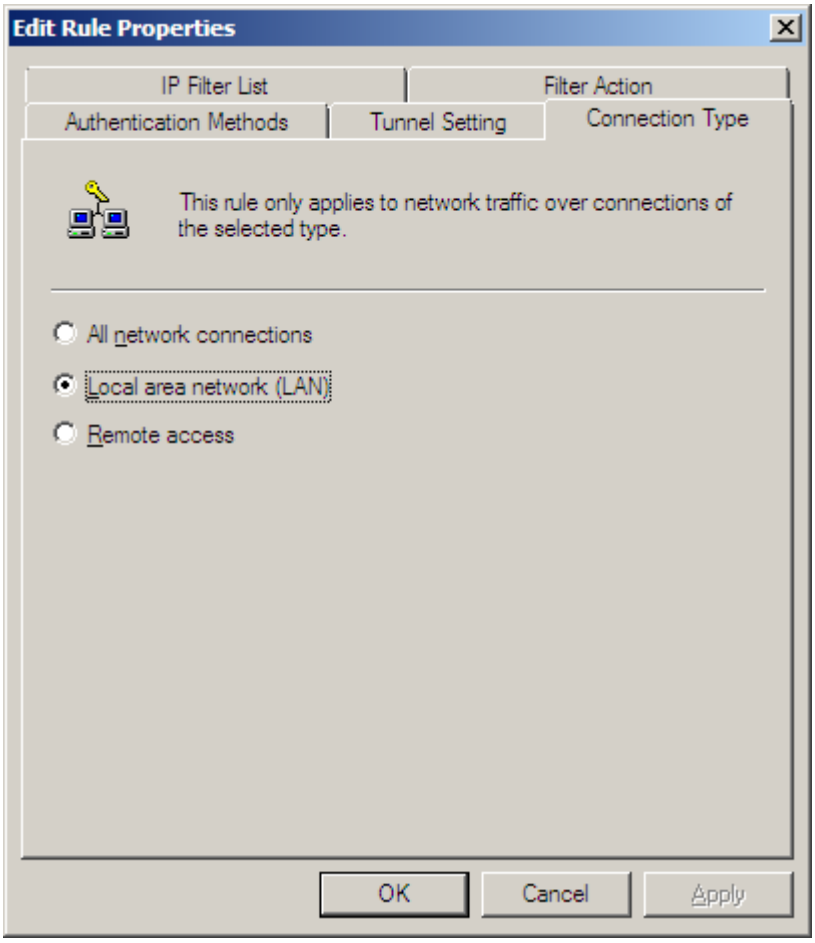

Bild 7-65 IPSec-Verbindungstyp

- ✧ Wählen Sie **Local Area Network (LAN)**.
- ✧ Schließen Sie den Dialog mit **OK**.
- ✧ Wählen Sie die Registerkarte **Authentication Methods**.

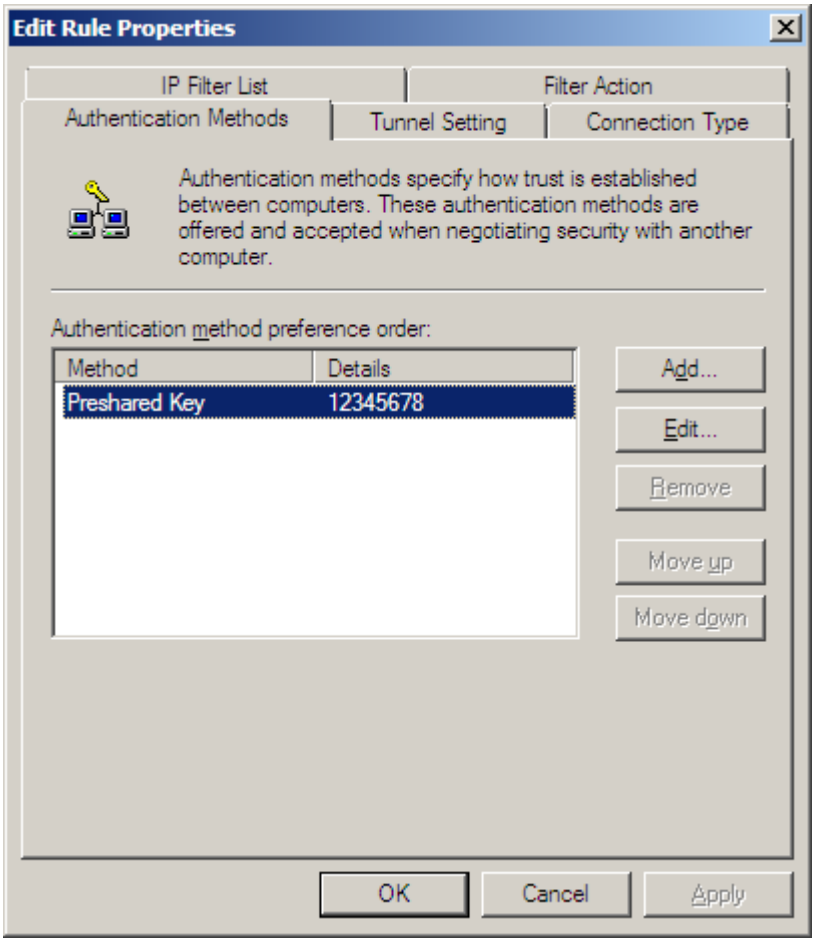

Bild 7-66 IPSec-Authentifizierung

- ✧ Wählen Sie **Add..**, um eine neue IPSec-Authentifizierung hinzuzufügen.
- ✧ Markieren Sie eine Authentifizierungsmethode und wählen Sie **Edit...**, um deren Eigenschaften zu bearbeiten.
- ✧ Geben Sie als Methode **Preshared Key** ein.
- ✧ Geben Sie unter **Details** Ihren persönlichen Sicherheitsschlüssel ein.

  Ändern Sie die vorgegebene Zahlenfolge ab. Wählen Sie einen Sicherheitsschlüssel, der mindestens 10 Zeichen lang ist und alphanumerische Zeichen und Sonderzeichen enthält.

HINWEIS

Der Sicherheitsschlüssel muss nicht an die Benutzer weitergegeben werden. Wenn die exportierte Konfigurationsdatei zur Installation auf dem lokalen Rechner über einen sicheren Kommunikationsweg übertragen wird, muss kein Sicherheitsschlüssel eingegeben werden. Verwenden Sie deshalb einen langen, komplexen Sicherheitsschlüssel.

- ✧ Schließen Sie den Dialog mit **OK**.

Konfiguration für die andere Übertragungsrichtung

- ✧ Wählen Sie die **IP Filter List** für die andere Übertragungsrichtung.

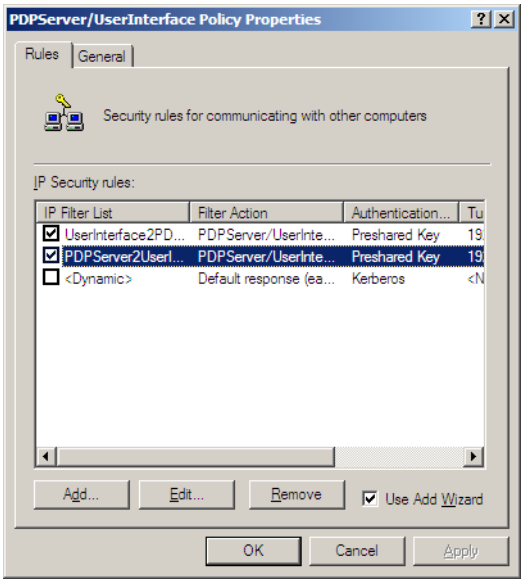

Bild 7-67 IPSec-Sicherheitsregel PDPServer2UserInterface

✧ Wählen Sie die Registerkarte **IP Filter List**.

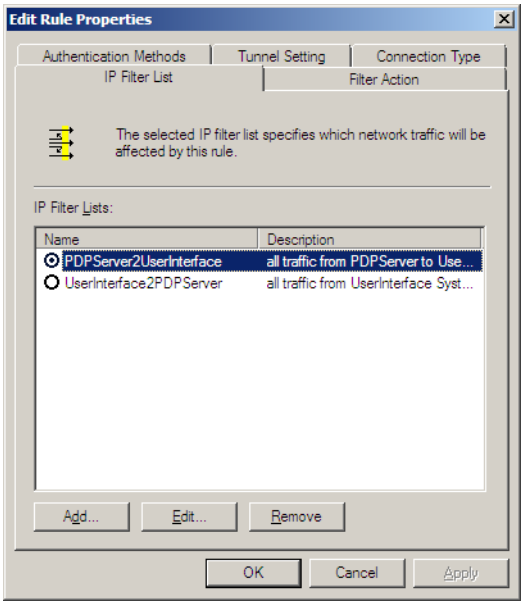

Bild 7-68 Bearbeiten der Sicherheitsregel PDPServer2UserInterface

✧ Markieren Sie das Filter **PDPServer2UserInterface**, um dessen Eigenschaften zu bearbeiten.

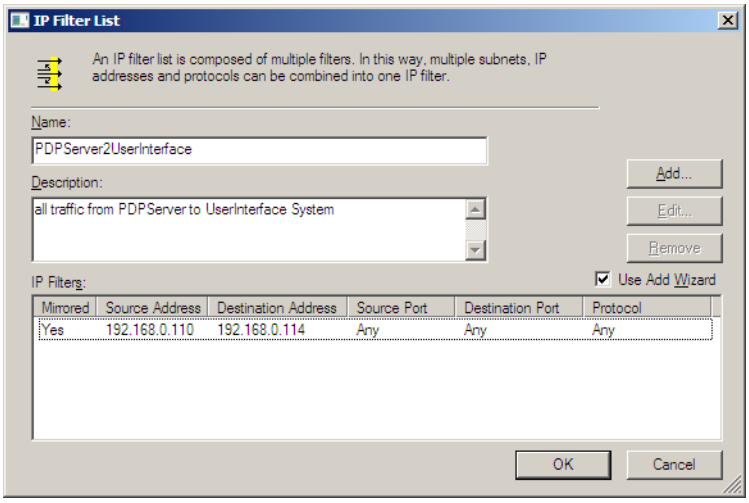

Bild 7-69 IP Filter List

- ✧ Geben Sie die IP-Adresse des SIGUARD PDP Servers oder dessen Domain-Namen als **Source Address** ein.
- ✧ Geben Sie die IP-Adresse des SIGUARD PDP Engineer/UI-Rechners oder dessen Domain-Namen als **Destination Address** ein.
- ✧ Geben Sie in der Spalte **Protocol Any** ein, damit alle Protokolle, z.B UDP, TCP und Port 445 und 139 durch den IPSec-Tunnel gelangen können.
- ✧ Wählen Sie die Registerkarte **Tunnel Setting**.

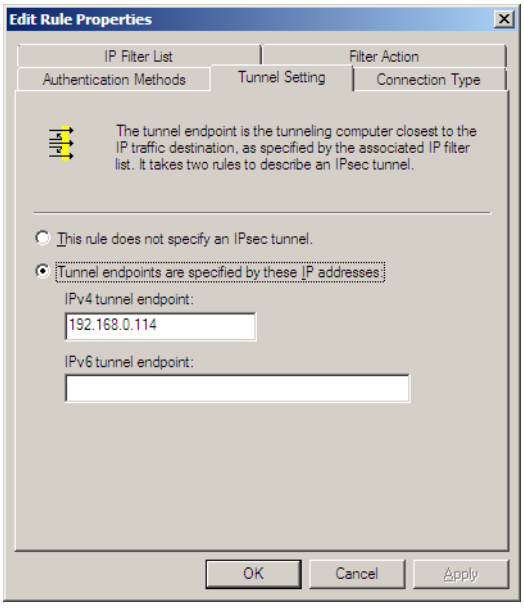

Bild 7-70 Einstellungen für den IPSec-Tunnel

- ✧ Markieren Sie **Tunnel endpoints are selected by these IP addresses**.

Bei diesem Eintrag in der IP-Filterliste ist die **Destination Address** der Tunnelendpunkt des SIGUARD PDP Engineering/UI-Rechners.

✧ Wählen Sie die Registerkarte **Connection Type**, um den Verbindungstyp einzustellen.

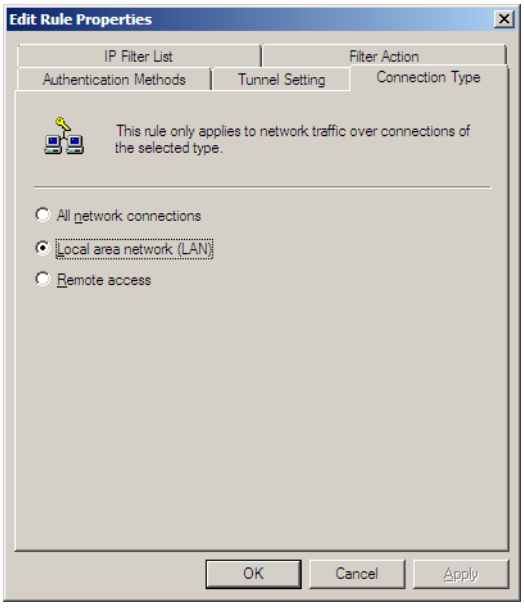

Bild 7-71 IPSec-Verbindungstyp

✧ Wählen Sie **Local Area Network (LAN)**.

✧ Wählen Sie die Registerkarte **Authentication Methods**.

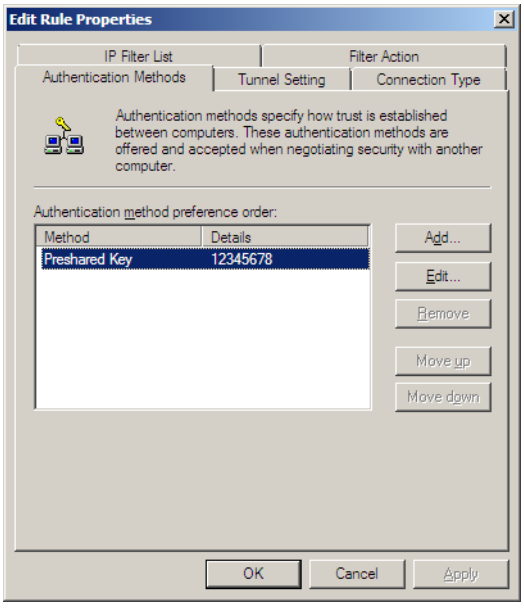

Bild 7-72 IPSec-Authentifizierung

✧ Geben Sie die Methode und den Sicherheitsschlüssel wie für die andere Übertragungsrichtung ein.

✧ Schließen Sie den Dialog mit **OK**.

Export der Konfigurationsdatei

Die Konfigurationsdatei, die auf dem SIGUARD PDP Server erstellt wurde, wird hier im Format **Ipsec** exportiert. Diese Datei wird auf einem **sicheren Weg** auf den lokalen Rechner überspielt und dort importiert. Anschließend aktivieren Sie die Sicherheitseinstellungen auf **beiden** Systemen, auf dem SIGUARD PDP Server und auf dem lokalen Rechner.

- ✧ Öffnen Sie die **Configuration Management Console**.
- ✧ Klicken Sie mit der rechten Maustaste auf das Snap-in **IP Security Policies on Local Computer** und wählen Sie den Menüeintrag **All Tasks > Export Policies...**.

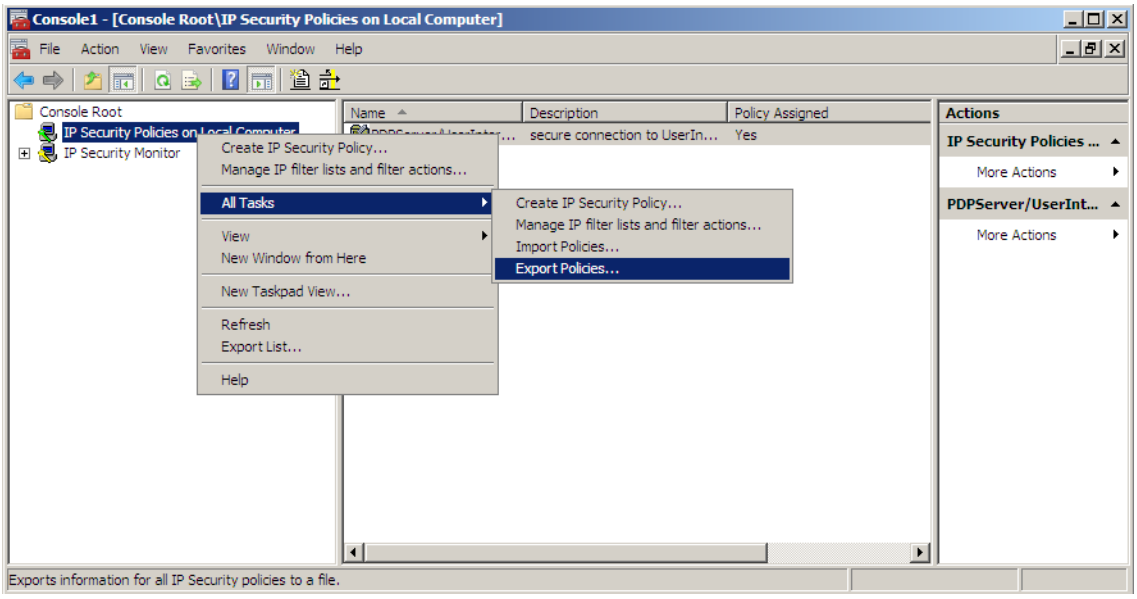

Bild 7-73 Aufruf für den Export der Konfigurationsdatei

- ✧ Vergeben Sie einen Namen für die Konfigurationsdatei.
- ✧ Schließen Sie den Dialog mit **Save As...**.
- ✧ Übertragen Sie die Konfigurationsdatei auf einem **sicheren Weg** auf den lokalen Rechner.

Import der Konfigurationsdatei

Der Import der Konfigurationsdatei wird auf dem lokalen Rechner ausgeführt.

- ✧ Fügen Sie die Snap-ins in der **Configuration Management Console** des lokalen Rechners hinzu.
- ✧ Klicken Sie mit der rechten Maustaste auf das Snap-in **IP Security Policies on Local Computer** und wählen Sie das Menü **All Tasks > Import Policies...**.

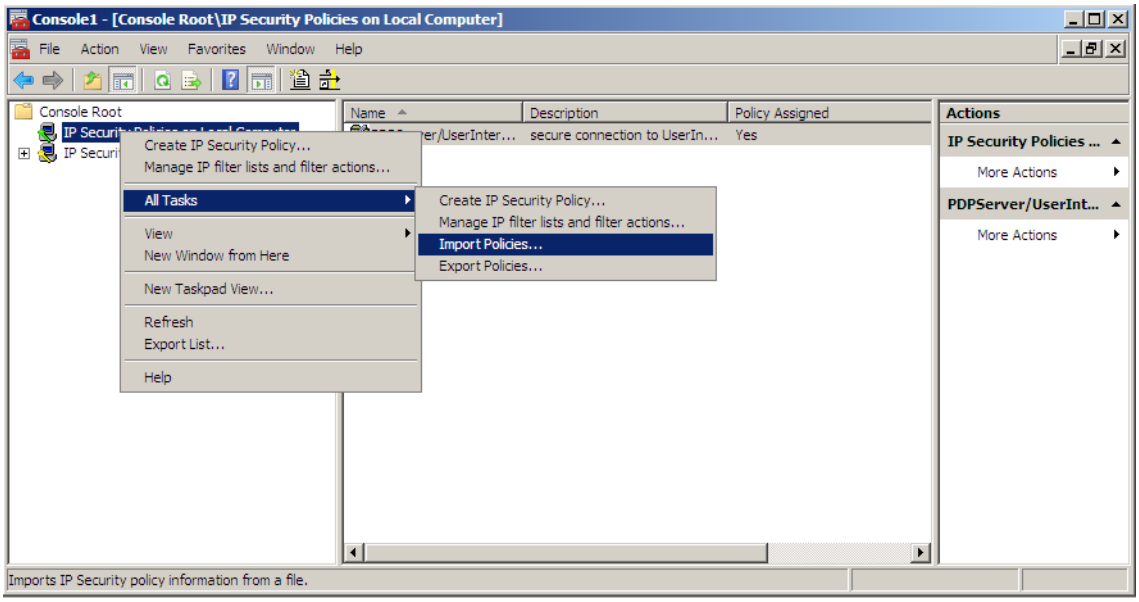

Bild 7-74 Aufruf für den Import der Konfigurationsdatei

- ✧ Markieren Sie die Konfigurationsdatei.
- ✧ Schließen Sie den Import mit **Open...** ab.

Aktivierung der Sicherheitseinstellungen

Aktivieren Sie die Sicherheitseinstellungen auf beiden Systemen.

- ✧ Klicken Sie unter **IP Security Policies on Local Computer** mit der rechten Maustaste auf den Eintrag **PDPServer/UserInterface Policy** und wählen Sie den Menüeintrag **Assign**.

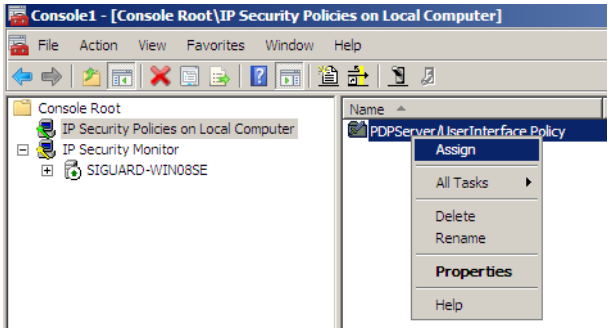

Bild 7-75 Aktivierung der IPSec-Sicherheitseinstellungen

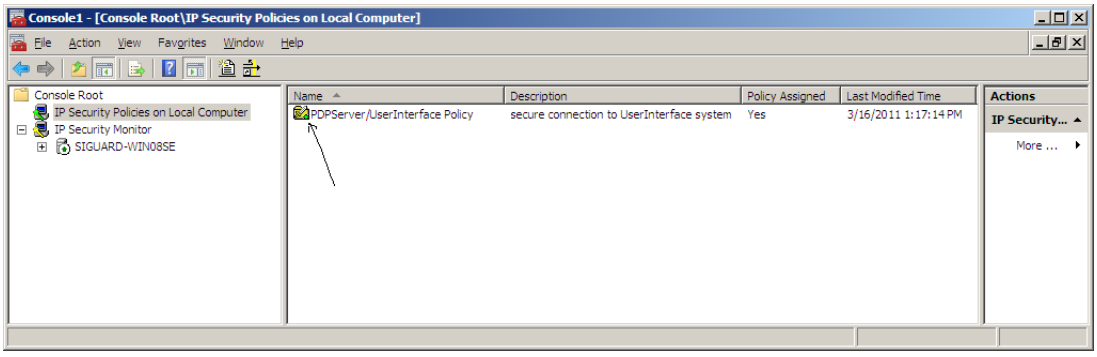

Bild 7-76 IPSec-Sicherheitseinstellungen sind aktiviert

Sobald die Sicherheitseinstellungen geladen sind, erscheint ein grüner Pfeil im Symbol der Konfigurationsdatei.

Nun ist der komplette IP-Datenverkehr zwischen SIGUARD PDP Server und dem SIGUARD PDP Engineer/UI-Rechner verschlüsselt. Diese Einstellung bleibt auch erhalten, falls das System neu gestartet wird und sich ein normaler Benutzer auf dem SIGUARD PDP Engineer/UI-Rechner anmeldet.

HINWEIS

Beachten Sie, dass zusätzliche Sicherheitsstrategien auf beiden Systemen hinzugefügt werden können, entweder für den Zugriff auf weitere SIGUARD PDP Server oder für den Zugriff über den SIGUARD PDP Engineer-/UI-Rechner auf einen Server. Das Prinzip ist dasselbe.

✧ Wenn Sie unsicher sind, ob das System gut konfiguriert ist, verwenden Sie das Überwachungs-Snap-in.

IPSec-Überwachung

Auf dem SIGUARD PDP Server kann die aktuelle Konfiguration überwacht werden.

✧ Wählen Sie im Fenster **Configuration Management Console** den Pfad **Console Root > IP Security Monitor > SIGUARD-WIN08SE > Quick Mode > Statistics**.

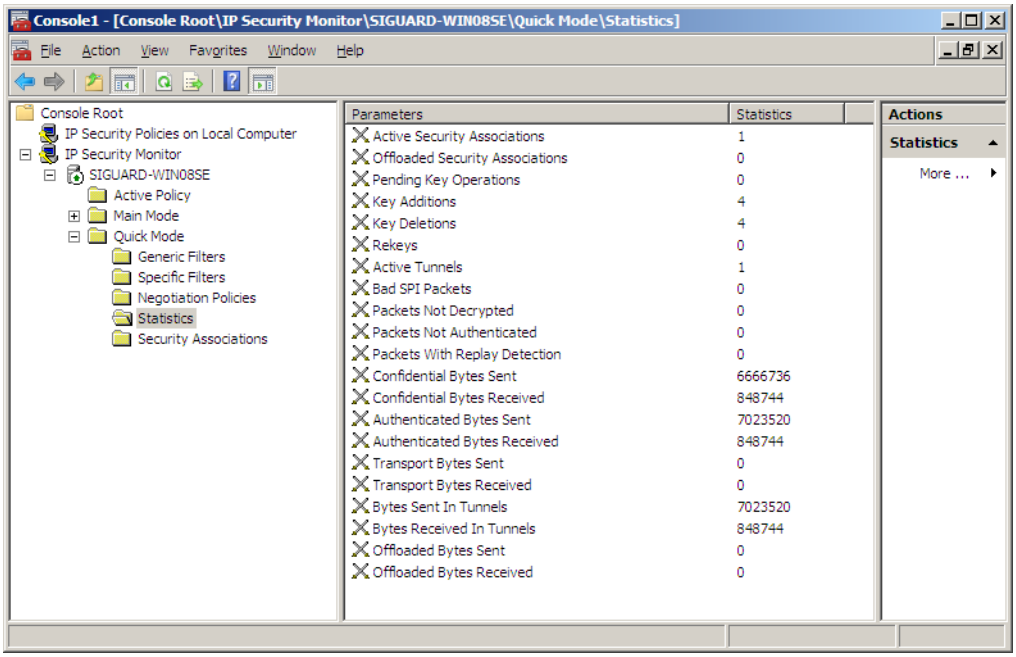

Bild 7-77 IPSec-Überwachung

Die wichtigsten Parameter sind **Bytes Sent In Tunnels** und **Bytes Received In Tunnels**. Dabei sind mit Tunnels die IPSec-Tunnel gemeint.

7.5.2 IPSec-Tunnel zwischen PMU und SIGUARD PDP Server

7.5.2.1 Allgemeines

Wenn Sie unsichere firmenfremde Kommunikationsnetzwerke benutzen, empfiehlt Siemens, einen IPSec-Tunnel zwischen den PMUs und dem SIGUARD PDP Server einzusetzen. Um diesen IPSec-Tunnel nutzen zu können, muss eine weitere Sicherheitskomponente, z.B. SIEMENS **Scalance S**, eingesetzt werden.

Gehen Sie vor wie folgt:

- ✧ Bauen Sie das Security Modul **Scalance S** ein.

  Siehe hierzu auch *Bild 2-2*.
- ✧ Installieren Sie die Software **Security Configuration Tool**.
- ✧ Konfigurieren Sie das Security Modul **Scalance S**.

7.5.2.2 IPSec-Konfiguration

Wenn Firewalls und/oder Router zwischen dem SIGUARD PDP Server und den PMUs eingesetzt werden, können die Scalance S-Module hinter den entsprechenden Eingängen eingebaut werden. Da das IPSec-Protokoll über die Firewalls geleitet wird, muss ESP-Datenverkehr zugelassen und der UDP-Port 500 freigeschaltet werden. Wenn NAT-T (Network Address Translation Traversal) verwendet wird, muss der UDP-Port 4500 freigeschaltet werden und statt **ESP** das **encapsulated ESP** zugelassen werden.

Da Handlungsfreiheit bei der Definition des PMU-Protokolls besteht, empfiehlt Siemens, den kompletten Datenverkehr zwischen dem SIGUARD PDP Server und den PMUs zuzugelassen. Definieren Sie eine VPN-Gruppe für das Scalance S-Netzwerk zwischen dem SIGUARD PDP Server und den PMUs.

HINWEIS

Alle Scalance S-Module müssen nach einer globalen **IP- Default-Drop-Firewall**-Richtlinie eingerichtet werden. Diese Richtlinie muss als letzte bei der Firewall-Konfiguration eines Scalance S-Moduls eingerichtet werden. Ohne diese Richtlinie ist der komplette Datenverkehr durch den IPSec-Tunnel zugelassen.

Für die Konfiguration der Scalance S-Module steht eine grafische Benutzeroberfläche (Security Configuration Tool) zur Verfügung. Für die Bedienung und die Konfiguration der Scalance S Security Module siehe SIEMENS Industry Handbuch, das Sie unter folgender Adresse herunterladen können: *Download des Handbuches*.

7.6 Schutz gegen Schadsoftware

7.6.1 Allgemeines

Der SIGUARD PDP Server und SIGUARD PDP Engineer/UI-Rechner arbeiten mit dem Windows-Betriebssystem. Deshalb empfiehlt Siemens als Schutz gegen die Infektion von Schads-Software, eine Antiviren-Software zu installieren, deren Virensignaturen ständig aktualisiert werden. Als Antiviren-Software empfiehlt Siemens **Trend Micro OfficeScan**.

HINWEIS

Achten Sie darauf, dass die Antiviren-Software in der von Siemens empfohlenen Weise konfiguriert wird.

Um eine Infektion über USB-Geräte, wie USB-Sticks oder USB-Festplatten, zu vermeiden, muss die Autostart-Funktion deaktiviert werden. Dies verhindert das automatische Ausführen der Software. Zusätzlich wird empfohlen, alle USB-Geräte mit einer aktualisierten Antiviren-Software auf Schad-Software zu scannen, bevor sie an das System angeschlossen werden. Die Antiviren-Software muss in der Betriebsart **on-access** konfiguriert werden. Die gleiche Vorgehensweise gilt für CDs oder DVDs.

Neben der Infektion durch Schad-Software über USB-Geräte kann die Infektion durch Schad-Software auch durch E-Mails oder das Durchsuchen im Internet erfolgen. Deshalb empfiehlt Siemens, eine Antiviren-Software zu installieren, die folgende Möglichkeiten bietet:

- Überprüfen von E-Mails
- Verhindern des Zugriffs auf unsichere Internet-Auftritte
- Verbieten der Verwendung von unsicheren E-Mail-Servern

Der Rechner muss so konfiguriert werden, dass die Infektion durch Schad-Software sicher vermieden wird. Eine sichere Konfiguration beinhaltet auch die ständige Aktualisierung aller installierter Fremdkomponenten.

Systemadministratoren müssen so geschult werden, dass die Systeme (z.B. Domain Controller, File Server etc.), die sie verwalten, ausschließlich zu administrativen Zwecken verwendet werden.

Besonders SIGUARD PDP Server, die für Verwaltungszwecke benutzt werden, dürfen nicht für folgende Aufgaben verwendet werden:

- Durchsuchen des Internets oder Abspielen jeglicher multimedialen Inhalte
- Testen oder Installieren nicht vertrauenswürdiger Software von zweifelhaften Quellen (z.B Internet, CD-ROM mit Shareware)
- Experimentieren mit SIGUARD PDP-Systemen

7.6.2 Virenscanner-System

Virenscanner stehen in verschiedenen Ausführungen zur Verfügung:

- Eigenständiges Produkt
- Client-Server-Konfiguration

  Ein Beispiel hierfür finden Sie im folgenden Bild.

Über einen Virus-Scan-Server werden die Setup-Daten, die Konfiguration und die aktualisierten Virensignaturen verteilt. Mit den Mechanismen **push & pull** werden die Informationen oder die Software an die Systeme weitergegeben.

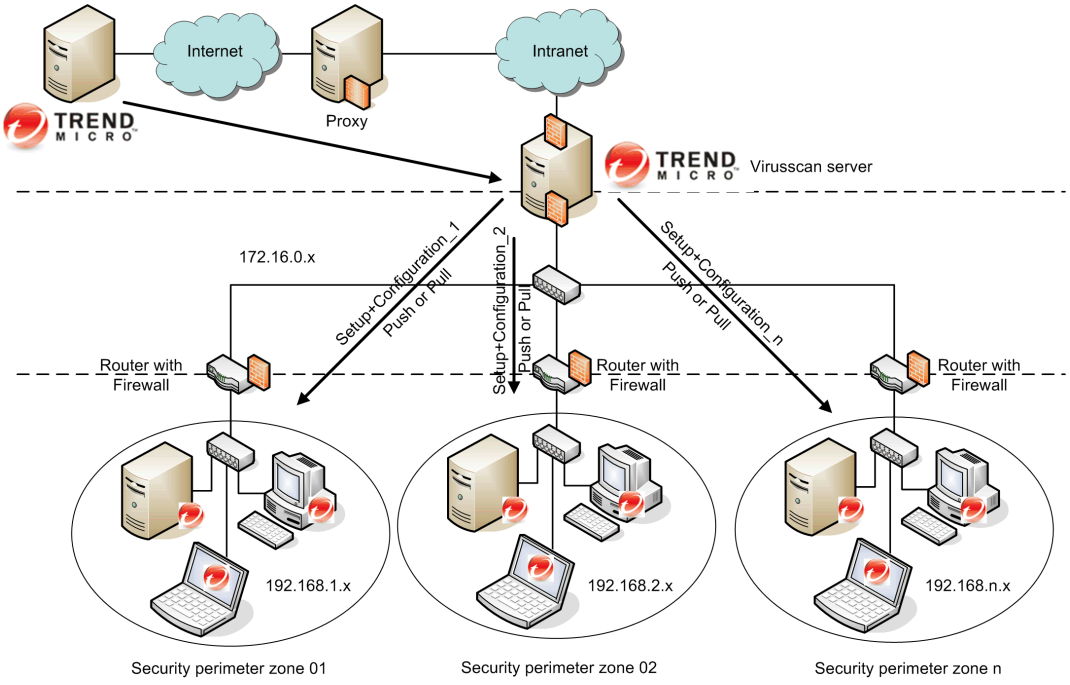

Bild 7-78 Das Virenscanner-System von TrendMicro

Das Virenscanner-System von TrendMicro ist getestet und wird von Siemens empfohlen.

7.7 Patch- und Update-Informationen

Die Sicherheit bei Patch- und Update-Informationen ist wichtig während des ganzen Lebenszyklus eines Produktes. Die Verwaltung von Patches für eine Software ist ein wesentlicher Teil dieses Prozesses. Falls möglich, aktivieren Sie immer die automatische Update-Funktion der installierten Software, z.B. für Microsoft Windows, Adobe Acrobat oder Oracle Java. Falls ein Internet-Zugang nicht zugelassen ist oder nicht zur Verfügung steht, installieren Sie die Sicherheitspatches für die installierte Software per Hand.

Falls Sie keinen direkten Zugriff oder einen Proxy-Zugriff auf das Internet besitzen, richten Sie sich Ihren eigenen WSUS-Server ein (Windows Server Update Services). Mit WSUS können Sie alle Microsoft-Patches in Ihrem Windows-System verteilen. Der Mechanismus ist vergleichbar mit dem Client-Server von Virus Scan. Das ganze System erhält die Patches über den in Windows automatisierten Update-Mechanismus. Der bedeutende Unterschied ist der Server, der die Patches zur Verfügung stellt.

Nicht alle Software-Hersteller stellen solch ein Update-System wie Microsoft zur Verfügung, mit dem im Fernzugriff gearbeitet werden kann. Falls Sie keinen direkten Zugriff oder einen Proxy-Zugriff auf das Internet besitzen, installieren Sie die Sicherheitspatches für die installierte Software per Hand. Informieren Sie sich hierzu regelmäßig auf der Homepage des entsprechenden Herstellers.

■

Stichwortverzeichnis

T

U

V

Z