MANUAL

INTUS COM OPC-Server

Installation und Wartung

D3000-432.00

www.pcs.com

INTUS COM OPC-Server

Installation und Wartung

Stand 02/2023

Bestell-Nr. D3000-432.00

PCS Systemtechnik GmbH

Pfälzer-Wald-Str. 36
81539 München

Tel. +49 89 68004 - 0

https://www.pcs.com

PCS Technischer Support

Tel.: +49 89 68004 - 666
Fax: +49 89 68004 - 562

E-Mail: support@pcs.com

Inhaltsverzeichnis

1 Über dieses Handbuch

1.1 Verwendete Symbole

Dieses Symbol warnt vor Gefahren für Gesundheit und Leben sowie vor Gefahren, die zu Schäden des Geräts oder des Systems führen können. Den Text neben diesem Zeichen sollten Sie in jedem Fall lesen und beachten!

Dieses Symbol weist auf Informationen hin, die für den Umgang mit dem Gerät wichtig sind und beachtet werden müssen.

Dieses Symbol weist auf eine Handlungsanweisung hin.

1.2 PCS Service-Tools und -Handbücher

Auf folgender Seite stehen Ihnen PCS Service-Tools für Inbetriebnahme und Wartung der INTUS Terminals und die dazugehörigen Handbücher kostenlos zum Download zur Verfügung:

https://download.pcs.com/service-tools/

1.3 Weitere Handbücher

Außer dem vorliegenden Handbuch ist noch folgendes weiteres Handbuch erhältlich:

INTUS COM Anwenderhandbuch (Bestellnummer D3000-430)

Dieses Handbuch beschreibt Installation, Betrieb und Schnittstellen der Kommunikations- und Administrationskomponenten des INTUS COM Terminal Management Systems.

Das INTUS COM Terminal Management System ist Voraussetzung für den Einsatz des OPC-Servers.

2 Einleitung

Der INTUS COM OPC-Server, im Weiteren nur OPC-Server genannt, stellt eine OPC Data Access Schnittstelle für OPC-Clients zur Verfügung. Über diese Schnittstelle können Statusinformationen von INTUS Terminals, INTUS Subterminals und Türen abgerufen und Steuerbefehle (z. B.: Türfreigabe) abgesetzt werden. Der OPC-Server steht als 32Bit Programm nur für Windows zur Verfügung und wird als Windows-Dienst gestartet.

Dieses Handbuch beschreibt die Installation und Konfiguration des OPC-Servers.

2.1 Notwendige Vorkenntnisse

Dieses Handbuch wendet sich an die Betreiber eines OPC-Clients z. B. Gebäudemanagement- und Überwachungssysteme. Daher werden Kenntnisse über den Aufbau und Funktionsweise der OPC Data Access Schnittstelle und in der Konfiguration des jeweiligen OPC-Clients vorausgesetzt.

Der OPC-Server verbindet sich zum INTUS COM Admin-Server. Daher werden Kenntnisse von INTUS COM, des jeweils eingesetzten Betriebssystems und dessen Bedieneroberfläche und Grundlagen von TCP/IP-Netzwerken vorausgesetzt.

3 Architektur

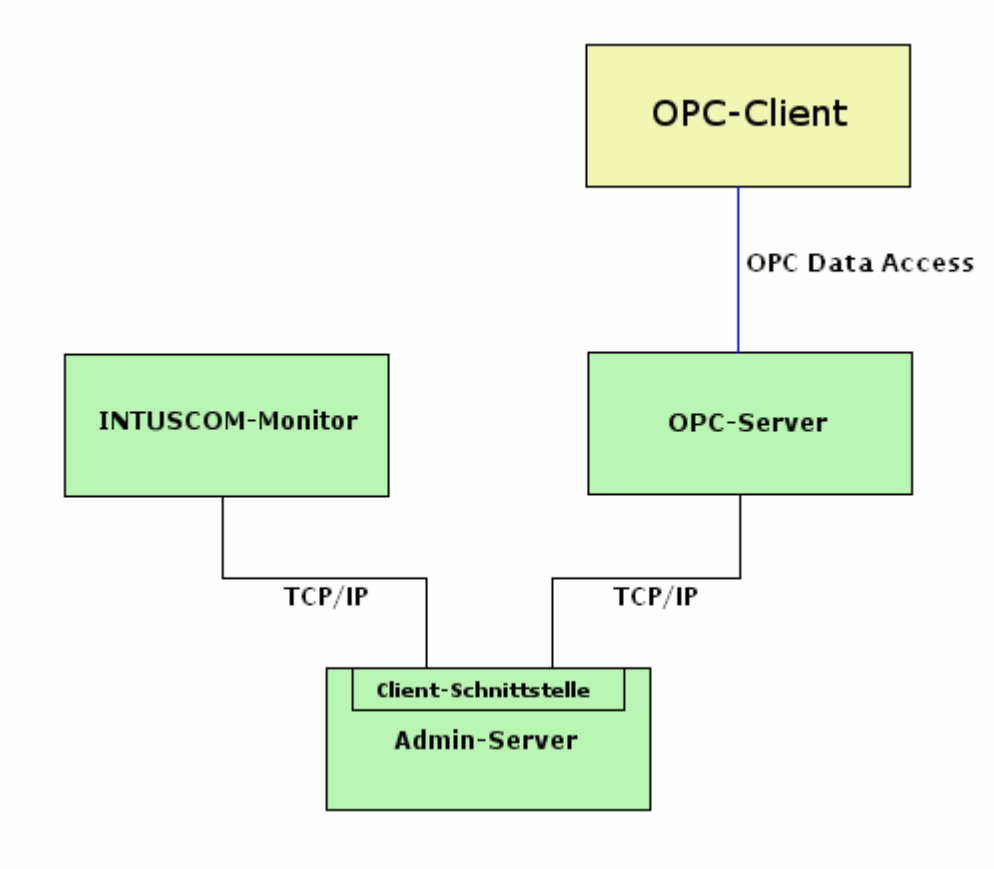

Abbildung 3.1 – Architektur

Der OPC-Server meldet sich als Client am INTUS COM Admin-Server an und stellt Statusinformationen der angeschlossenen INTUS Terminals, INTUS Subterminals und Türen über die OPC Data Access Schnittstelle den OPC-Clients zur Verfügung.

4 Installation und Konfiguration

4.1 Installationsvoraussetzungen

Um den OPC-Server zu betreiben, sind die folgenden Voraussetzungen zu beachten:

- INTUS COM Installation (lokal installiert oder über das Netzwerk erreichbar)
- INTUS COM Benutzer für die Anmeldung an INTUS COM
- Der OPC-Server muss in der INTUS COM Lizenz enthalten sein.
- Microsoft Visual C++ 2008 Laufzeitumgebung
- OPC Core Components

4.2 Installationsprogramm

Das Installationsprogramm OPC_Server_Setup1.1.0.exe kopiert die für den OPC-Server benötigten Programmdateien auf einen Zielrechner.

Zusätzlich können die folgenden Aufgaben mit dem Installationsprogramm durchgeführt werden:

- Installation der Microsoft Visual C++ 2008 Laufzeitumgebung,
- Installation der OPC Core Components und
- Erzeugung der Konfigurationsdatei opc_server.ini für den OPC-Server.

4.2.1 Installation

Starten Sie das Installationsprogramm. Nach der Auswahl des Installationspfads werden Sie aufgefordert, die Zugangsdaten für den INTUS COM Benutzer, den der OPC-Server verwenden soll, einzugeben.

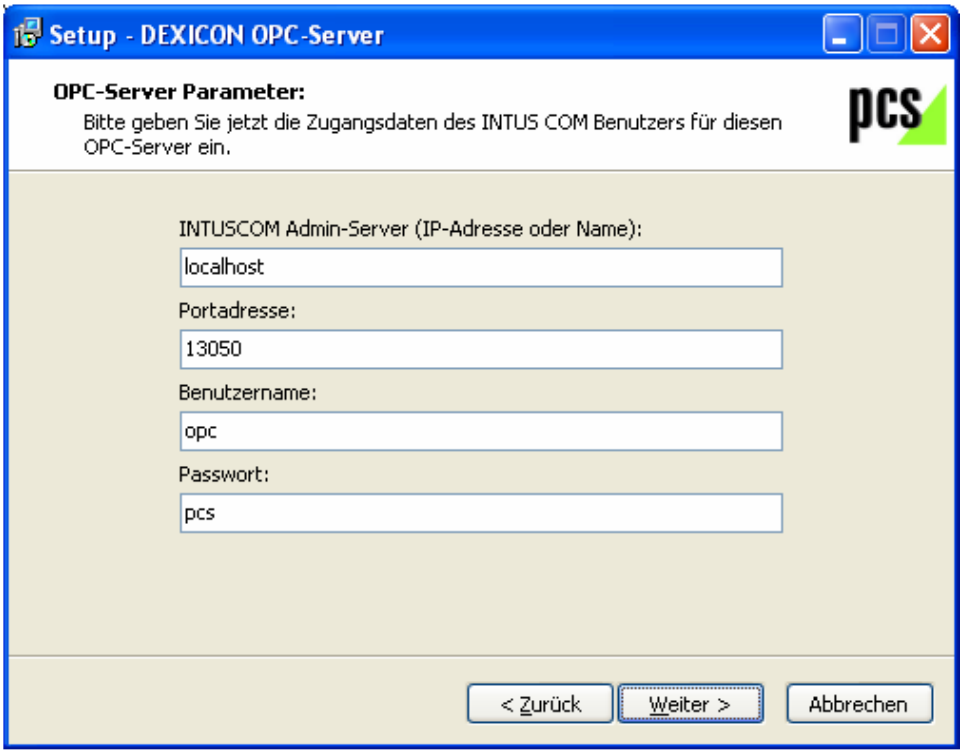

Abbildung 4.1 – Installation, INTUS COM Benutzer

Tragen Sie hier

- Rechnernamen bzw. die IP-Adresse,
- TCP-Port,
- Benutzernamen und
- Passwort

für die Verbindung zum INTUS COM Admin-Server ein.

Die hier eingestellten Werte werden verwendet, um die Konfigurationsdatei opc_server.ini (siehe Kapitel 3.5) zu erzeugen.

Nach Festlegung der Startmenügruppe folgt eine Auswahl zusätzlicher Aufgaben, die durch das Installationsprogramm durchgeführt werden können.

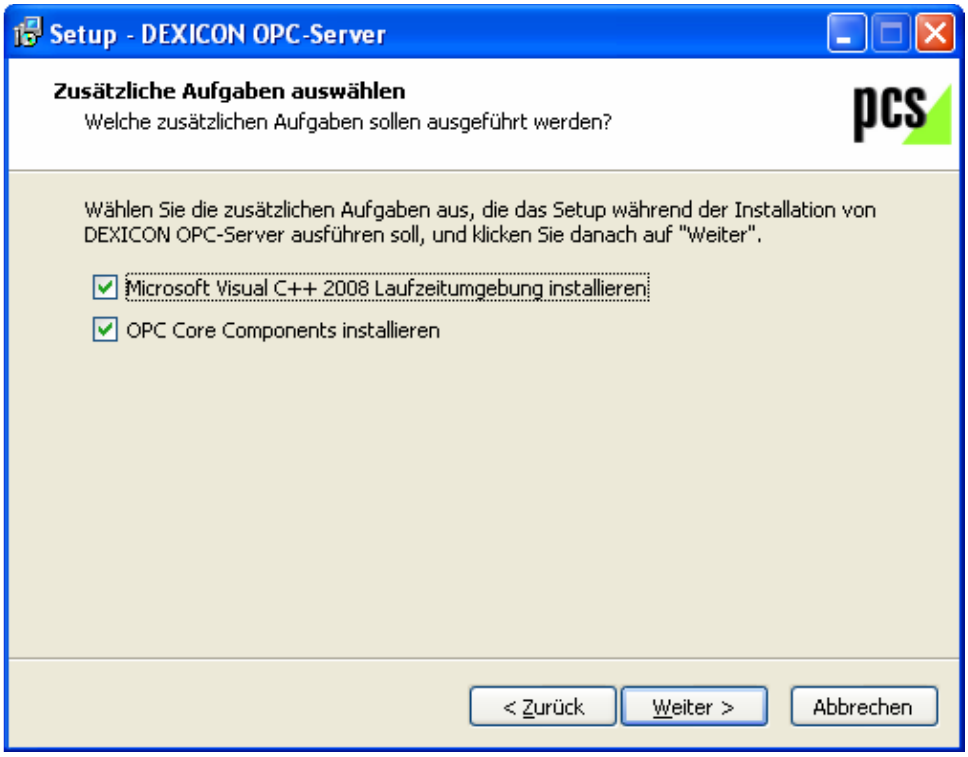

Abbildung 4.2 – Installation, Zusätzliche Aufgaben

Sowohl die Microsoft Visual C++ 2008 Laufzeitumgebung als auch die OPC Core Components werden für den Betrieb des OPC-Servers benötigt.

3 Wenn Sie sich nicht sicher sind, ob eine dieser Komponenten bereits auf dem Zielsystem installiert ist, wählen Sie bitte die Komponente zur Installation aus.

Nach Abschluss der Installation finden Sie im Startmenü unter dem Namen der gewählten Startmenügruppe (Standard: INTUSCOM) die zwei Verknüpfungen Start INTUS COM OPC-Server und Stopp Dexicon OPC-Server. Über diese beiden Verknüpfungen kann der OPC-Server gestartet bzw. beendet werden.

4.3 Kommandozeilenparameter des OPC-Servers

Der OPC-Server kann auch über die Kommandozeile gestartet werden. Der OPC-Server ist ein Windows-Dienst ohne grafische Oberfläche und befindet sich im Unterverzeichnis bin des Installationsverzeichnisses.

Die folgenden Kommandozeilenoptionen stehen zur Verfügung:

Kommandozeilenoption	Beschreibung
-?	Anzeige der Kommandozeilenoptionen des OPC-Servers
-b	OPC-Server Dienst starten
-k	OPC-Server Dienst beenden

4.4 INTUS COM Benutzer anlegen

Um einen Benutzer für den OPC-Server anzulegen, starten Sie zunächst den INTUSCOM-Monitor und melden sich mit einem Benutzer an, der das Recht hat, Benutzer anzulegen (z. B.: „admin“). Wählen Sie dann im Menü Neu->Benutzer aus.

1

Abbildung 4.3 – INTUS COM Benutzer anlegen

Auf der Karteikarte Benutzer, im K&S-Fenster des neuen Benutzers, legen Sie den Loginnamen und ein Passwort für den neuen Benutzer fest.

2

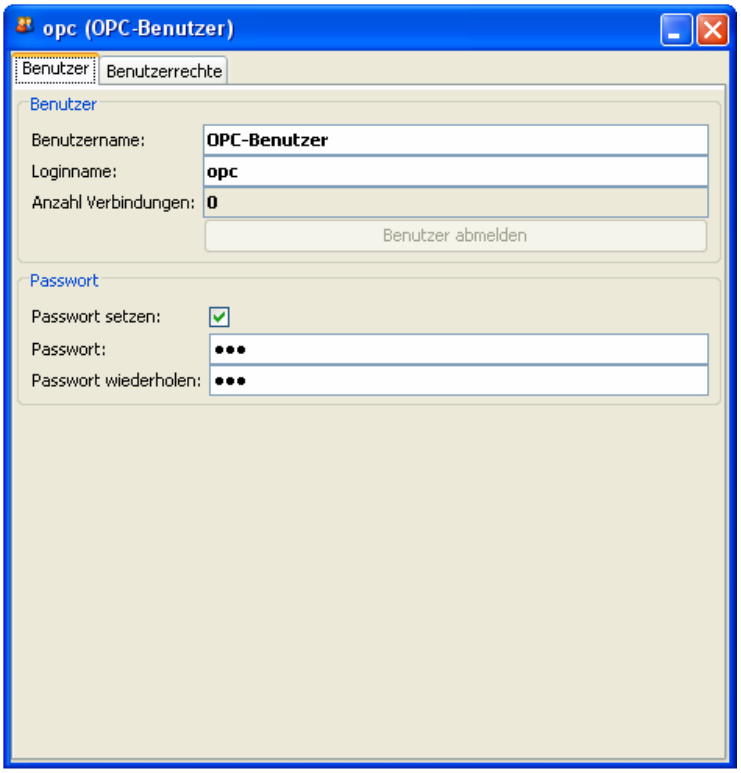

Abbildung 4.4 – INTUS COM Benutzer, Name und Passwort

3

Auf der Karteikarte Benutzerrechte werden die Berechtigungen für den neuen INTUS COM Benutzer eingestellt.

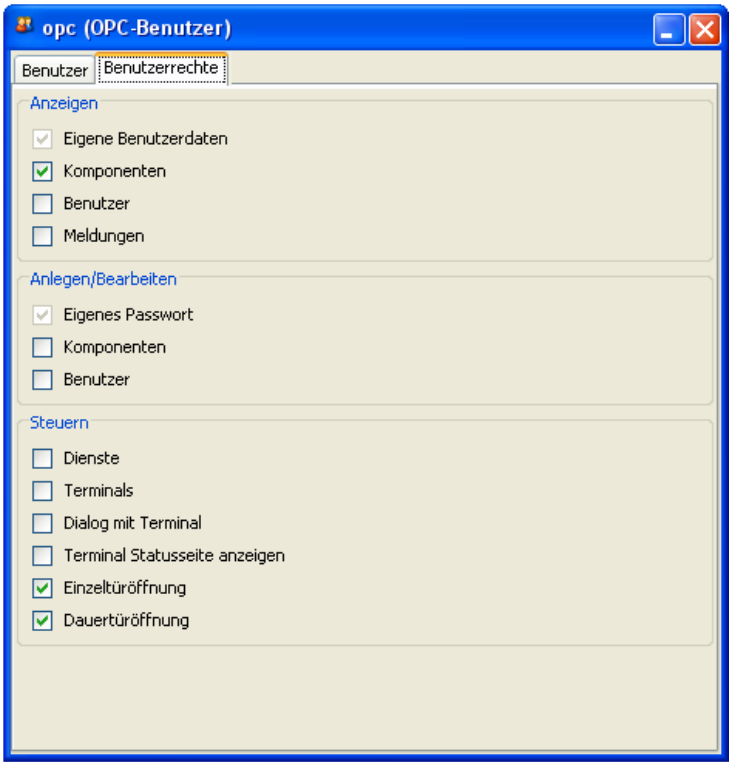

Abbildung 4.5 – INTUS COM Benutzer, Benutzerrechte

Der INTUS COM Benutzer für den OPC-Server benötigt zumindest das Anzeigerecht für Komponenten, um Statusinformationen der INTUS Komponenten zu erhalten.

Soll die Einzeltüröffnung oder Dauertüröffnung durch einen OPC-Client gesteuert werden können, aktivieren Sie diese Rechte ebenfalls.

4.5 Konfigurationsdatei

Der OPC-Server verbindet sich beim Start mit dem INTUS COM Admin-Server.

4

Der OPC-Server liest die für die Verbindung benötigten Informationen aus der Datei opc_server.ini im Verzeichnis conf des Installationsverzeichnis des OPC-Servers. Fehlt die Konfigurationsdatei opc_server.ini oder ist ein Schlüssel in der Konfigurationsdatei nicht vorhanden, so verwendet der OPC-Server Standardwerte.

Die Konfigurationsdatei opc_server.ini enthält genau eine Sektion [login]. Die Einstellungen in dieser Sektion werden vom OPC-Server verwendet, um die Verbindung zum INTUS COM Admin-Server herzustellen.

In der Sektion [login] können die folgenden Einstellungen vorhanden sein:

Schlüssel	Standardwert	Beschreibung
host	127.0.0.1	Rechnername bzw. IP-Adresse des Rechners, auf dem der INTUS COM Admin-Server läuft
port	13050	Port, auf dem der INTUS COM Admin-Server auf eingehende Verbindungen wartet
user	opc	INTUS COM Benutzer für die Anmeldung am INTUS COM Admin-Server
pass	pcs	Passwort des INTUS COM Benutzers

Der in der Konfigurationsdatei eingetragene INTUS COM Benutzer muss in INTUS COM angelegt sein, damit der OPC-Server sich am INTUS COM Admin-Server anmelden kann.

Beispiel:

```
[login]
host=127.0.0.1
port=13050
user=opc
pass=pcs
```

4.6 DCOM Konfiguration

4.6.1 Lokaler Zugriff auf den OPC-Server

Als Benutzer

Als lokaler Benutzer müssen keine Änderungen an den Windows-Standardeinstellungen vorgenommen werden, um Zugriff auf den OPC-Server zu erhalten.

Als Dienst

Damit ein Dienst auf den OPC-Server zugreifen kann, muss entweder:

- der Dienst als ein Benutzer gestartet werden, der auf dem System bekannt ist
- der Benutzer „SYSTEM“ für DCOM berechtigt werden.

4.6.2 Remotezugriff auf den OPC-Server

DCOM erlaubt keinen entfernten, anonymen Zugriff ohne Passwort. Deshalb muss jeder Benutzer, der auf den OPC-Server von einem anderen Rechner zugreifen soll, für diesen Zugriff berechtigt werden.

4.7 Arbeitsgruppe

Jeder Benutzer, der auf den OPC-Server zugreifen soll, muss sowohl auf dem OPC-Server-Rechner als auch auf dem OPC-Client-Rechner bekannt sein. Dabei ist zu beachten, dass sowohl der Benutzername als auch das Passwort gleich sein muss.

Das folgende Beispiel zeigt die notwendigen Konfigurationsschritte, um auf einen OPC-Server remote zuzugreifen.

Serverrechner:

- Betriebssystem: Windows 2012 Server R2 (64Bit).
- Name: W2012-SVR-X64-R2
- OPC-Core Components
- INTUS COM 3.2.0 und OPC-Server. Der OPC-Server ist so konfiguriert, dass er sich beim Start mit dem INTUS COM Admin-Server verbindet.
- Firewall deaktiviert.

Clientrechner:

- Betriebssystem: Windows 8.1 64Bit.
- Name: WIN_8_1_X64
- OPC-Core Components
- Matricon OPC Explorer (Freeware) zum Testen der Verbindung.
- Firewall deaktiviert.

Benutzergruppe anlegen

Damit nicht jeder Benutzer einzeln für den Remote-Zugriff auf den OPC-Server berechtigt werden muss, empfiehlt es sich, diese Berechtigungen über eine Benutzergruppe zu verwalten.

Legen Sie über „Computerverwaltung / Lokale Benutzer und Gruppen / Gruppen“ eine neue Benutzergruppe „OPC-Gruppe“ auf dem Serverrechner an. Der Name dieser Gruppe ist frei wählbar, sollte aber deren Zweck verdeutlichen.

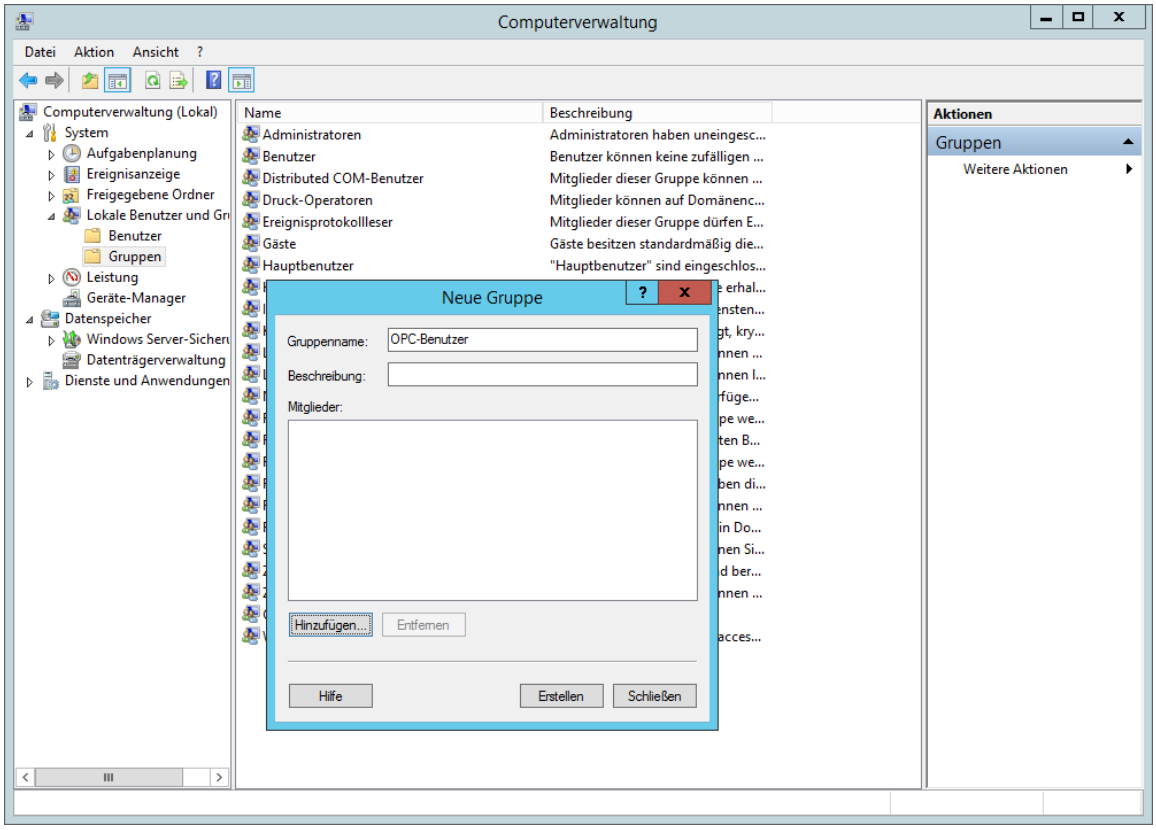

Abbildung 4.6 – OPC-Benutzergruppe anlegen

Benutzer/Gruppe für Remote DCOM-Zugriff berechtigen

Starten Sie über Start->Ausführen das Programm c:\windows\syswow64\dcomcnfg.exe.

Öffnen Sie für Konsolenstamm->Computer->Arbeitsplatz das Kontextmenü (rechte Maustaste) und wählen Sie Eigenschaften.

5

6

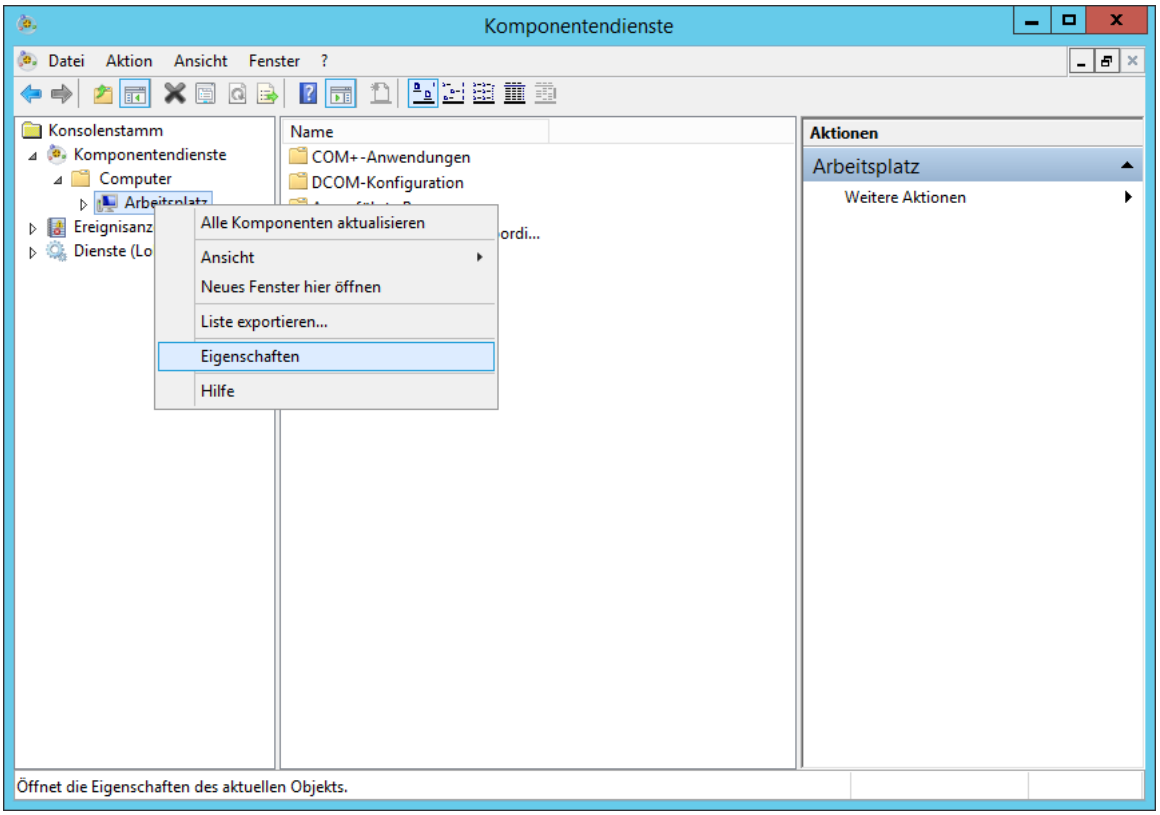

Abbildung 4.7 – dcomcnfg

Im Eigenschaftsfenster wählen Sie den Reiter COM-Sicherheit aus.

7

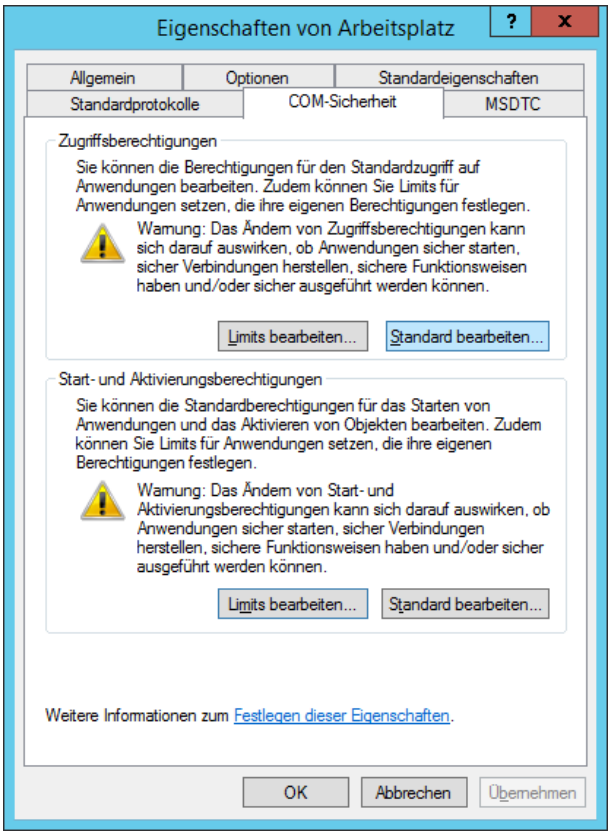

Abbildung 4.8 – dcomcnfg – COM-Sicherheit

Betätigen Sie die Schaltfläche Limits bearbeiten… im Rahmen Zugriffsberechtigungen.

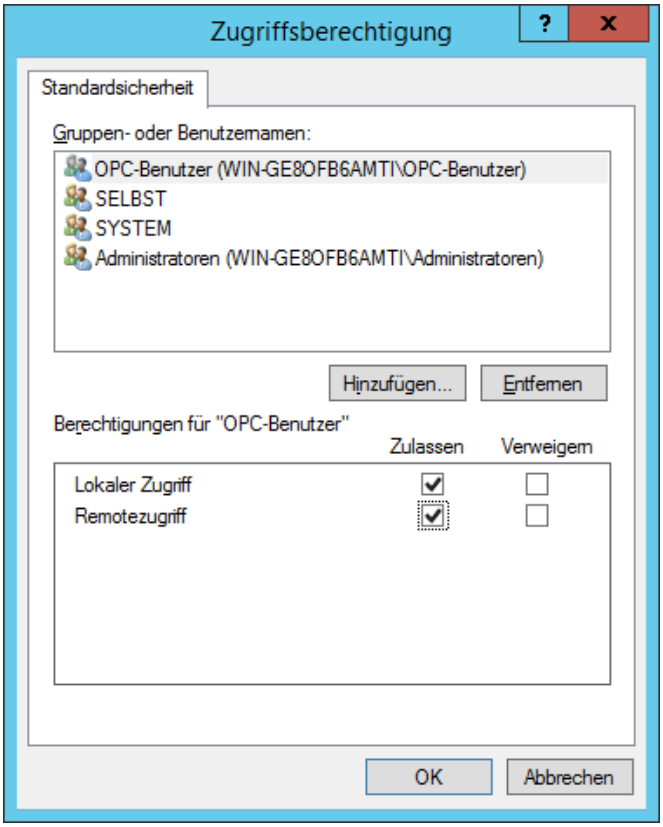

Abbildung 4.9 – dcomcnfg – Benutzer/Gruppe berechtigen

Fügen Sie über die Schaltfläche Hinzufügen die Benutzergruppe OPC-Gruppe hinzu und berechtigen Sie die Gruppe für den Lokalen und den Remotezugriff.

Fügen Sie über die Schaltfläche Hinzufügen den Benutzer ANONYMOUS-ANMELDUNG hinzu und berechtigen Sie diesen Benutzer ebenfalls für den Lokalen und den Remotezugriff. Die ANONYMOUS-ANMELDUNG wird für den Dienst OPCEnum benötigt, der für das „browsen“ der OPC-Objekte benötigt wird. Bestätigen Sie den Dialog mit OK.

Betätigen Sie die Schaltfläche Standard bearbeiten… im Rahmen Zugriffsberechtigung und fügen Sie auch hier die Benutzergruppe OPC-Gruppe mit denselben Berechtigungen hinzu.

Betätigen Sie die Schaltfläche Limits bearbeiten… im Rahmen Start und Aktivierungsberechtigungen.

12

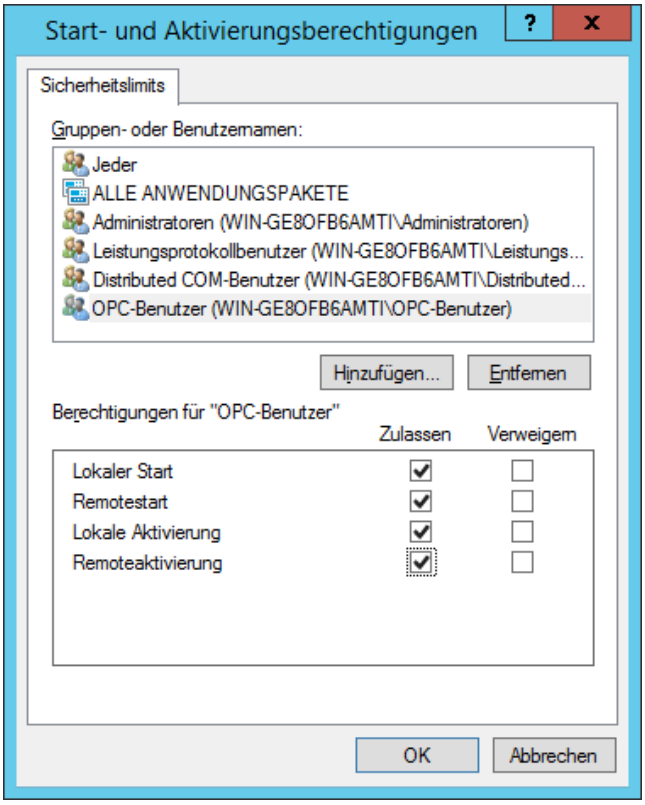

Abbildung 4.10 – dcomcnfg – Benutzer/Gruppe berechtigen

13

Fügen Sie über die Schaltfläche Hinzufügen die Benutzergruppe OPC-Gruppe hinzu und berechtigen Sie die Gruppe für den Lokaler Start, Remotestart,

14 Lokale Aktivierung und Remoteaktivierung. Sie den Dialog mit OK.

Betätigen Sie die Schaltfläche Standard bearbeiten… im Rahmen Start und Aktivierungsberechtigungen und fügen Sie auch hier die Benutzergruppe OPC-Gruppe mit denselben Berechtigungen hinzu.

DCOM auf dem Client-Rechner konfigurieren

Damit die DCOM-Kommunikation in beiden Richtungen funktioniert, muss der

1 Benutzer ANONYLOUS-ANMELDUNG auch auf dem Client-Rechner für den Lokalen und den Remotezugriff berechtigt werden.

2

OPC-Benutzer anlegen

Legen Sie auf dem Serverrechner einen Benutzer OPC-Benutzer mit dem Passwort 1234 an und fügen Sie ihn der Benutzergruppe OPC-Gruppe hinzu.

Legen Sie auf dem Clientrechner einen Benutzer OPC-Benutzer mit dem Passwort 1234 an.

Es kann natürlich jeder Benutzer, der auf dem Clientrechner bereits vorhanden ist, verwendet werden. Wichtig ist nur, dass ein Benutzer mit demselben Namen und Passwort auch auf dem Serverrechner angelegt und der Gruppe OPC-Gruppe hinzugefügt wird. Es ist aus Sicherheitsgründen jedoch nicht ratsam, den Benutzer Administrator zu verwenden.

Damit ein Dienst auf dem Clientrechner den OPC-Server remote verwenden kann, muss entweder der Benutzer SYSTEM der OPC-Gruppe auf dem Serverrechner hinzugefügt werden oder der Dienst wird so konfiguriert, dass er ein Benutzerkonto verwendet, das auf dem Serverrechner der OPC-Gruppe zugeordnet ist.

Verbindungstest mit Matricon OPC-Explorer

Installieren Sie den Matricon OPC-Explorer auf dem Clientrechner und starten Sie den Matricon OPC-Explorer als Benutzer OPC-Benutzer.

1

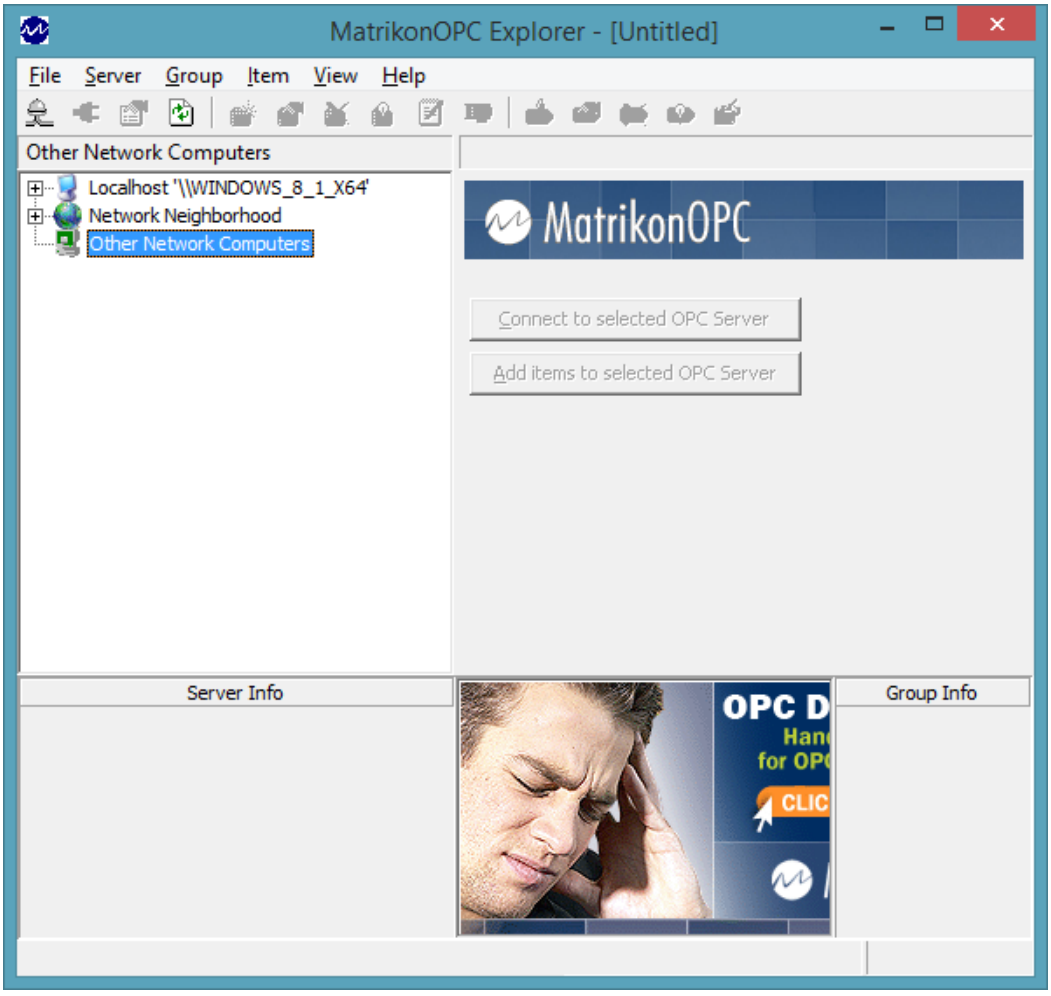

Abbildung 4.11 – Matricon OPC-Explorer

Markieren Sie den Knoten Other Network Computers und wählen Sie im Kontextmenü den Punkt Add/Connect Server.

2

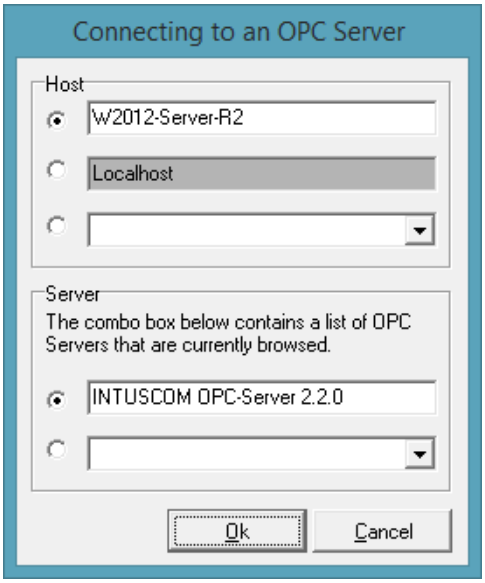

Abbildung 4.12 – OPC-Explorer – Server hinzufügen

3 Geben Sie im Rahmen Host die IP-Adresse oder den Rechnernamen ein und geben Sie im Rahmen Server INTUS COM OPC-Server ein. Bestätigen Sie den Dialog mit Ok.

4 Im folgenden Dialog geben Sie einen Namen für die Gruppe ein, dem die Objekte des OPC-Servers zugeordnet werden.

Fügen Sie der Gruppe die Datenpunkte des OPC-Servers hinzu.

5

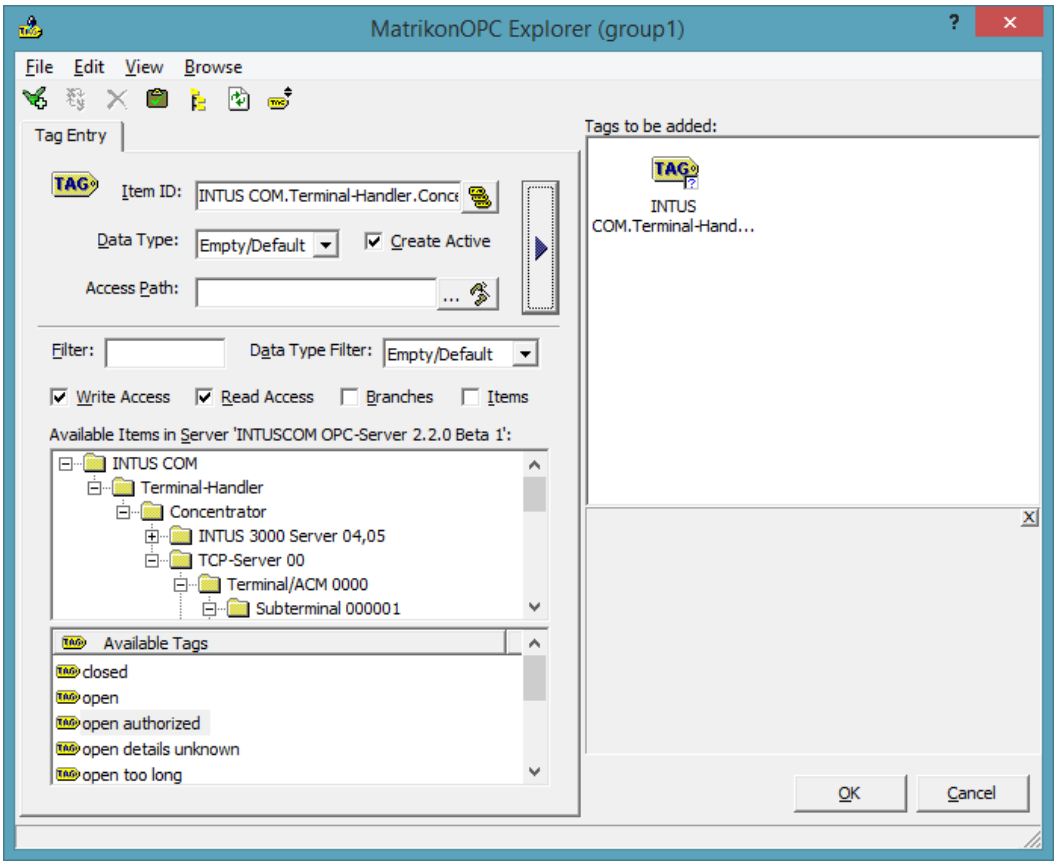

Abbildung 4.13 – OPC-Explorer – Datenpunkt hinzufügen

4.8 Domäne

Innerhalb einer Domäne werden die Benutzer zentral verwaltet. Deshalb ist es nicht notwendig, die Benutzer auf den beteiligten Rechnern anzulegen.

Das Vorgehen entspricht dem oben besprochenen Beispiel. Die Benutzer müssen jedoch nicht auf dem Serverrechner angelegt werden, sondern können direkt der Benutzergruppe OPC-Gruppe hinzugefügt werden.

4.9 Firewall

Im oben besprochenen Beispiel wurden die Windows Firewall auf dem Server- und Clientrechner deaktiviert. In einer Produktivumgebung ist dieses Vorgehen jedoch nicht ratsam. Damit die Remoteverbindung mit dem OPC-Server auch bei aktivierter Firewall funktioniert, müssen die folgenden Einstellungen sowohl auf dem Server- als auch auf dem Clientrechner vorgenommen werden.

Legen Sie die folgenden Firewall-Regeln für aus- und eingehende Verbindungen an:

Serverrechner:

Programm <Installationspfad>\Intuscom\bin\opc_server.exe zulassen.

Programm %SystemRoot%\SysWOW64\OpcEnum.exe zulassen.

Programm: %SystemRoot%\SysWOW64\mmc.exe zulassen.

Port 135 TCP zulassen.

Clientrechner:

Programm <Installationspfad>\Matricon\OPC\Explorer.exe zulassen.

Programm %SystemRoot%\SysWOW64\OpcEnum.exe zulassen.

Programm: %SystemRoot%\SysWOW64\mmc.exe zulassen.

Port 135 TCP zulassen.

5 OPC-Baum

Der Aufbau des OPC-Baumes ist an die Struktur des Komponentenbaums des INTUSCOM-Monitors angelehnt.

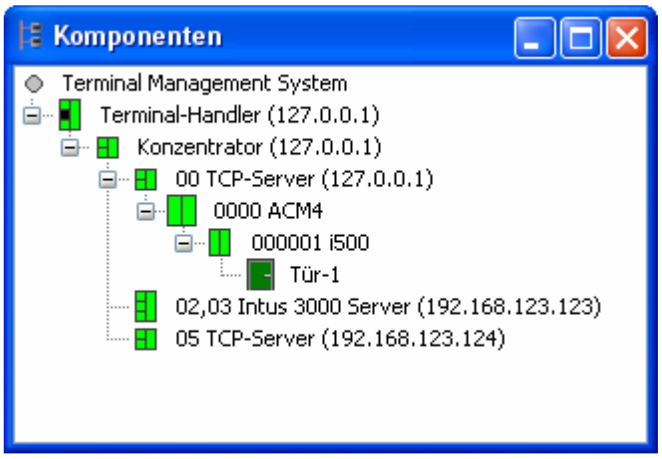

Abbildung 5.1 – INTUS COM, Komponentenbaum

Die folgende Abbildung zeigt die OPC-Baum-Version der INTUS COM Komponenten aus der vorhergehenden Abbildung:

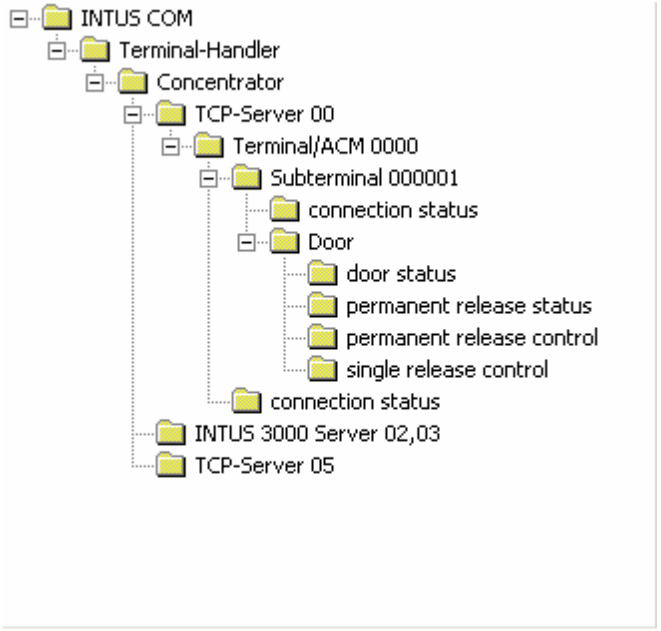

Abbildung 5.2 – OPC-Baum

Die hier gewählte Darstellung verzichtet zunächst auf die enthaltenen Datenpunkte, um die Übersichtlichkeit zu erhöhen.

Die Wurzel des OPC-Baumes enthält genau ein Element INTUS COM. Unterhalb dieses „Wurzel“-Elementes sind alle weiteren Elemente eingeordnet.

Das Element INTUS COM enthält genau ein Element Terminal-Handler. Dieser wiederum enthält genau ein Element Concentrator. Unterhalb des Concentrator-Elements sind die konfigurierten INTUS COM Server angeordnet.

5.1.1 Server

Die INTUS COM Server enthalten selbst keine Datenpunkte. Der Name der Serverkomponenten setzt sich aus dem Servertyp und der zweistelligen Server-ID zusammen.

```
<Servertyp> <Server-ID>
```

In Abbildung 4.2 sind das:

- TCP-Server 00
- INTUS 3000 Server 02,03
- TCP-Server 05

Ein INTUS 3450 Server kann zwei Server-IDs besitzen. Die zweite Server-ID ist aber nur vorhanden, wenn die zweite Line des INTUS 3450 Server aktiviert ist.

5.1.2 Terminals <Terminal/ACM>

Die Server-Komponenten enthalten für jedes INTUS Terminal/ACM, das an diesem Server konfiguriert ist, ein Element. Der Name dieses Elements ist aus der festen Bezeichnung Terminal/ACM, der zweistelligen Server-ID und der zweistelligen Terminal-ID zusammengesetzt.

```
Terminal/ACM <Server-ID><Terminal-ID>
```

Die Beispielkonfiguration aus Abbildung 4.2 enthält ein Terminal-Element Terminal/ACM 0000.

Ein Terminal-Element kann die folgenden Elemente enthalten:

Elementtyp	Beschreibung	Anzahl
Subterminal	Enthält die Elemente und Datenpunkte eines Subterminals	0 – 16
Door	Enthält die Elemente und Datenpunkte für eine Tür	0-1
tamper contact status	Enthält die Elemente und Datenpunkte für den Sabotagekontaktstatus des Terminals	1
connection status	Enthält die Datenpunkte für den Verbindungsstatus des Terminals	1

Ein Terminal-Element enthält immer ein Element connection status, das die Datenpunkte für den Verbindungsstatus des Terminals enthält. Auf die Elemente connection status und tamper contact status wird an im weiteren Verlauf eingegangen.

5.1.3 Subterminals <Subterminal>

Unter einem Terminal-Element können bis zu 16 Subterminal-Elemente vorhanden sein. Der Name eines Subterminal-Elements ist aus der festen Bezeichnung Subterminal, der zweistelligen Server-IF, der zweistelligen Terminal-ID und der zweistelligen Subterminal-ID zusammengesetzt.

`Subterminal <Server-ID<Terminal-ID><Subterminal-ID>`

Die Beispielkonfiguration aus Abbildung 4.2 enthält ein Subterminal-Element Subterminal 000001.

Ein Subterminal-Element kann die folgenden Elemente enthalten:

Elementtyp	Beschreibung	Anzahl
Door	Enthält die Elemente und Datenpunkte für eine Tür.	0 – 1
tamper contact status	Enthält die Elemente und Datenpunkte für den Sabotagekontaktstatus des Subterminals	1
connection status	Enthält die Datenpunkte für den Verbindungsstatus des Subterminals	1

5.1.4 Türen <Door>

Das Tür-Element kann unter einem Terminal- und/oder einem Subterminal-Element vorhanden sein. Der Name des Tür-Elements lautet Door.

Die Beispielkonfiguration aus Abbildung 4.2 enthält ein Tür-Element unterhalb des Subterminal-Element Subterminal 000001.

Ein Tür-Element kann nur genau einmal pro Terminal- oder Subterminal-Element vorhanden sein.

Ein Tür-Element enthält die folgenden Elemente:

Elementtyp	Beschreibung	Anzahl
door status	Enthält die Datenpunkte für den Türstatus	1
permanent release status	Enthält die Datenpunkte für den Daueroffenstatus der Tür	1
permanent release control	Enthält die Datenpunkte zur Steuerung der Dauertüröffnung	1
single release control	Enthält die Datenpunkte zur Steuerung der Einzeltüröffnung	1

5.1.5 Verbindungsstatus <connection status>

Für ein Terminal oder Subterminal gibt es immer genau ein Element <connection status>, das die Datenpunkte für den Verbindungsstatus enthält.

Terminal

Das Verbindungsstatus-Element für ein Terminal enthält die folgenden Datenpunkte:

Datenpunkt	Beschreibung	Datentyp	Zugriff
connected	Verbindung zum Terminal besteht in INTUS COM	Boolean	Lesend
deactivated	Das Terminal ist in INTUS COM deaktiviert	Boolean	Lesend
disconnected	Das Terminal ist absichtlich nicht verbunden (kein Fehler)	Boolean	Lesend
offline	Das Terminal ist aufgrund eines Fehlers nicht verbunden.	Boolean	Lesend
online	Verbindung zum Terminal besteht und das Terminal ist bereit.	Boolean	Lesend
unknown	Der Verbindungsstatus des Terminals ist unbekannt.	Boolean	Lesend

Subterminal

Das Verbindungsstatus-Element für ein Subterminal enthält die folgenden Datenpunkte:

Datenpunkt	**Beschreibung**	**Datentyp**	**Zugriff**
deactivated	Das Subterminal ist deaktiviert.	Boolean	Lesend
offline	Das Subterminal ist offline.	Boolean	Lesend
online	Das Subterminal ist online.	Boolean	Lesend
unknown	Der Verbindungsstatus des Subterminals ist unbekannt.	Boolean	Lesend

5.1.6 Sabotagekontaktstatus <tamper contact status>

Für ein Terminal oder Subterminal gibt es immer genau ein Element <tamper contact status>, das die Datenpunkte für den Sabotagekontaktstatus enthält.

Das Sabotagekontaktstatus-Element für ein Terminal oder Subterminal enthält die folgenden Datenpunkte:

Datenpunkt	Beschreibung	Datentyp	Zugriff
housing closed	Das Gehäuse des Sub/Terminal ist geschlossen.	Boolean	Lesend
housing open	Das Gehäuse des Sub/Terminal ist offen.	Boolean	Lesend
unknown	Der Status des Sabotagekontakt ist unbekannt.	Boolean	Lesend

5.1.7 Türstatus <Door status>

Für eine Tür gibt es immer genau ein Türstatus-Element <door status>, in dem die Datenpunkte für den Türstatus enthalten sind.

Das Türstatus-Element enthält die folgenden Datenpunkte:

Datenpunkt	Beschreibung	Datentyp	Zugriff
closed	Die Tür ist geschlossen	Boolean	Lesend
open	Die Tür ist geöffnet	Boolean	Lesend
open authorized	Die Tür ist berechtigt geöffnet	Boolean	Lesend
open details unknown	Die Tür ist geöffnet. Informationen ob berechtigt oder unberechtigt liegen nicht vor.	Boolean	Lesend
open too long	Tür ist zu lange auf	Boolean	Lesend
open too long repeat	Wiederholung, Tür zu lange auf	Boolean	Lesend
open unauthorized	Die Tür ist unberechtigt geöffnet	Boolean	Lesend
Open unauthorized repeat	Wiederholung, Tür unberechtigt geöffnet	Boolean	Lesend
unknown	Der Türstatus ist unbekannt	Boolean	Lesend

5.1.8 Daueroffenstatus <permanent release status>

Für eine Tür gibt es immer genau ein Daueroffenstatus-Element <permanent release status>, in dem die Datenpunkte für den Daueroffenstatus enthalten sind.

Das Daueroffenstatus-Element enthält die folgenden Datenpunkte:

Datenpunkt	Beschreibung	Datentyp	Zugriff
not released	Die Daueröffnung ist nicht aktiviert	Boolean	Lesend
released	die Daueröffnung ist aktiviert	Boolean	Lesend
release by control record	Die Daueröffnung für diese Tür wurde durch einen Steuersatz aktiviert	Boolean	Lesend
released by fire alarm	Die Daueröffnung für diese Tür wurde durch die Brandmeldeanlage aktiviert	Boolean	Lesend
released by profile	Die Daueröffnung für diese Tür wurde durch ein Steuerprofil aktiviert	Boolean	Lesend
Released by toggle function	Die Tauertüröffnung für diese Tür wurde durch eine Toggle-Buchung aktiviert	Boolean	Lesend
unknown	Der Daueroffenstatus für diese Tür ist unbekannt	Boolean	Lesend

5.1.9 Dauertüröffnung <permanent release control>

Für eine Tür gibt es immer genau ein Element <permanent release control>, in dem die Datenpunkte zur Steuerung des Daueroffenstatus enthalten sind.

Um die Dauertüröffnung zu steuern, benötigt der INTU COM Benutzer zusätzlich das Recht zur Steuerung der Dauertüröffnung.

Das Element zur Steuerung des Daueroffenstatus enthält die folgenden Datenpunkte:

Datenpunkt	Beschreibung	Datentyp	Zugriff
start permanent release	Aktiviert die Dauertüröffnung für eine Tür durch einen Steuersatz	Boolean	Lesend, Schreibend
stop permanent release	Deaktiviert die Dauertüröffnung für eine Tür durch einen Steuersatz	Boolean	Lesend, Schreibend

Bei der Türsteuerung durch Steuersätze sind die folgenden Punkte zu beachten:

- Bei Einsatz einer Einbruchmeldeanlage kann die Dauertüröffnung nicht durch den Datenpunkt <start permanent release> gestartet werden, solange die Einbruchmeldeanlage „scharf“-geschalten ist.
- Bei Einsatz einer Brandmeldeanlage kann eine Dauertüröffnung, die durch die Brandmeldeanlage geschaltet wurde, nicht durch den Datenpunkt <stop permanent release> beendet werden.
- Bei Einsatz von Steuerprofilen wird die „Profil“-Steuerung durch <start permanent release> übersteuert. Durch <stop permanent release> wird die „Profil“-Steuerung wiederhergestellt.

5.1.10 Einzeltüröffnung <single release control>

Für eine Tür gibt es immer genau ein Element <single release control>, in dem der Datenpunkt zur Steuerung der Einzeltüröffnung enthalten ist.

Um die Einzeltüröffnung zu steuern, benötigt der INTUS COM Benutzer zusätzlich das Recht zur Steuerung der Einzeltüröffnung.

Das Element zur Steuerung der Einzeltüröffnung enthält die folgenden Datenpunkte:

Datenpunkt	Beschreibung	Datentyp	Zugriff
release	Führt eine Einzeltüröffnung für eine Tür durch einen Steuersatz aus. Die Dauer der Türöffnung wird durch die Terminalparametrierung bestimmt.	Boolean	Lesend, Schreibend

Bei der Türsteuerung durch Steuersätze sind die folgenden Punkte zu beachten:

- Bei Einsatz einer Brandmeldeanlage kann eine Dauertüröffnung, die durch die Brandmeldeanlage geschaltet wurde, nicht durch den Datenpunkt <stop permanent release> beendet werden.
- Bei Einsatz von Steuerprofilen wird die „Profil“-Steuerung durch <start permanent release> übersteuert. Durch <stop permanent release> wird die „Profil“-Steuerung wiederhergestellt.

6 Änderungsindex

Datum	Version	
10.02.23	2.4.2	Version 2.4.2
17.06.10	1.0.0 gku	Version 1.0.0
21.10.14	1.1.0 gku	Version 1.1.0

7 Abbildungsverzeichnis

Haben Sie noch Fragen?

Rufen Sie uns an.

PCS-Hotline: +49 89 68004 – 666

E-Mail: support@pcs.com

Dieses Handbuch soll so hilfreich wie möglich sein. Wenn Sie Anregungen zur Optimierung haben, lassen Sie es uns bitte wissen. Wir bedanken uns schon jetzt für Ihre Mühe.

Ihre PCS Systemtechnik GmbH

Zeit für Sicherheit.

made in germany

PCS Systemtechnik GmbH
Pfälzer-Wald-Str. 36
81539 München
Tel. +49 89 68004 – 0
intus@pcs.com
www.pcs.com

Ruhrallee 311
45136 Essen
Tel. +49 201 89416 – 0

pcs