Kommunikation von Automatisierungsgeräten über Ethernet und TCP/IP

Ingenieurmäßiges Arbeiten im SS 03, Betreuer Prof. Walter
von Nils Eckardt, Matr.Nr. 7040343, überarbeitete Version Prof. Walter vom 21.4.04

Kommunikation mit Ethernet /TCP/IP

Kommunikation mit CP343-IT

Fernwartung von Automatisierungsgeräten

OPC-Kommunikation

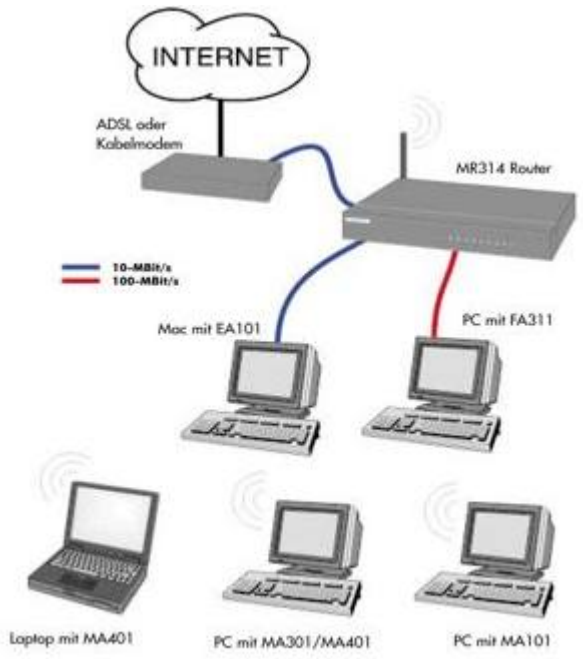
Kommunikation mit Ethernet /TCP/IP

Entwicklung von Ethernet

Jahr	Standard	Bitrate
1983	10 Base5 (Thick Ethernet) mit Koaxleitung	10 MBit /s
1985	10 Base2 (Thin Ethernet) mit Koaxleitung	10 MBit /s
1990	10 BaseT (Twisted Pair Ethernet) mit UTP Kabel	10 MBit /s
1992	Switches für Full Duplex	10 MBit /s
1993	10 BaseF (Fiber Optic)	10 MBit /s
1994	100 BaseT (Twisted Pair Fast –Ethernet)	100 MBit /s
1996	Autosensing (automatische Umschaltung 10 -100 MBit /s)	100 MBit /s
1998	1000 BaseX	1000 MBit /s
2001	10 000 Gigabit Ethernet wird erarbeitet	10000 MBit /s
2003	Wireless Ethernet (WLAN) Der Standard für drahtlose Netze ist der IEEE 802.11-Standard und ermöglicht mobilen Benutzern den kabellosen Zugriff auf unternehmenseigene Netzwerke, E-Mails und das Internet. Der Standard 802.11a benützt den 5GHz-Bereich und erreicht Datentransferraten bis zu 54Mbit/s. Der Standard 802.11b arbeitet im 2,4GHz-Bereich mit einer Geschwindigkeit von 11-MBit/s. Der Standard 802.11g arbeitet ebenfalls im 2,4GHz-Bereich mit einer Geschwindigkeit von 54-MBit/s bzw. 108 MBit/s und ist kompatibel zum 802.11b Standard.	11-MBit/s-108 MBit/s

Netzwertopologie

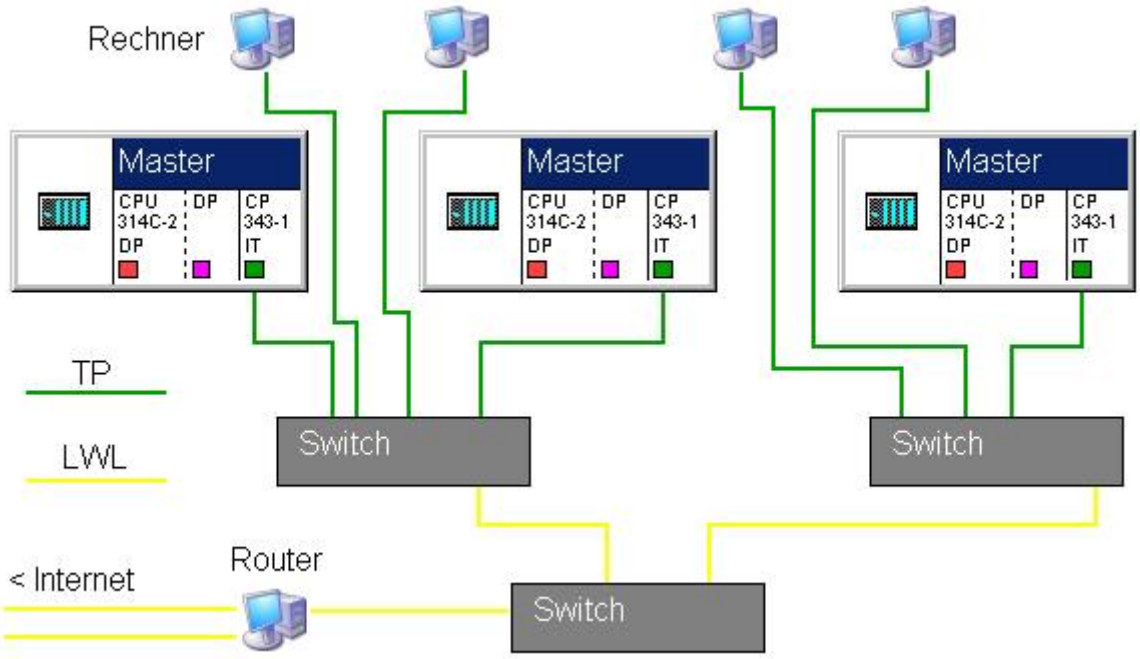
Beispiel zu Wireless Ethernet (WLAN)	Beispiel zu Twisted Pair



Im Labor Raum 4.1.06 kommt die heute übliche strukturierte Twisted Pair Verkabelung zum Einsatz.

Die strukturierte TP Verkabelung basiert auf Sternpunkten, in denen die einzelnen Netzwerkteilnehmer zusammengeführt werden. Diese Sternkoppler sind Hubs oder Switches, die eine direkte Verbindung zwischen den Netzwerkteilnehmern über die physikalischen Netzwerkadressen ermöglichen. Im Labor 4.1.06 kommen Switches zum Einsatz, die die einzelnen miteinander kommunizierenden Teilnehmer direkt miteinander über 10 MB verbinden, ohne das andere Teilnehmer des gleichen Sternpunktes etwas von deren Kommunikation mitbekommen, dadurch also auch nicht bei der eigenen Kommunikation beeinflusst werden.

Mehrere Sternpunkte können wieder in Sterntopologie zusammengeführt werden, wobei hier der eventuell gestiegene Bandbreitenbedarf berücksichtigt werden muss. Im Labor 4.1.06 wird dieses durch die Verwendung von Lichtwellenleitern mit höherer Übertragungskapazität von 100 MB berücksichtigt, wie die nachfolgende Grafik veranschaulicht. Der unterste Switch ist im Verteilerraum 4.E.14.



Aufbau einer Ethernet Nachricht

Jede Ethernet Karte hat eine weltweit eindeutige 6 Byte MAC (Medi Access Control) Adresse. Unter der Adresse FF FF FF FF FF FF HEX= 255.255.255.255 werden alle Karten im Netz angesprochen (MAC Broadcast Adresse)

Die Ethernet Nachricht wird seriell (von links nach rechts) über den Bus übertragen.

7 Bytes	1 Bytes	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes		4 Bytes
Preamble	Start kennung	Zieladresse	Quelladresse	Länge	LLC	Verpackte Daten	FCS Prüfen
		Destination MAC Adresse des Empfängers	Source MAC Adresse des Absenders	Anzahl folgenden Bytes	Logical Link Control Typinformation	Ethernet Data	Frame Check Sequenze

Bei Verwendung von TCP/IP werden die Nutzdaten in Ethernet Data eingebettet.

Ethernet Data			
IP Header für IP Empfänger + Absender	IP Data		
	TCP Header für Empfangs + Absender PORT	TCP Data	
		Header	Nutzdaten

IP Adressen

Die IP Adresse besteht aus 4 Bytes, die meist als vierstellige Dezimalzahl dargestellt wird. Sie besteht aus dem Subnet Adresse und der Hostadresse. Die IP Adresse muss weltweit eindeutig sein, wenn man sich im Internet bewegt. Diese Adressen werden statisch vom Provider vergeben oder dynamisch (DHCP= Dynamic Host Control Protocol) bei Bedarf vergeben. Lokale Netzwerke, die nicht mit dem Internet verbunden sind, können beliebige IP Adressen haben.

IP Adresse (4 Byte)	
Subnet Adresse	Hostadresse

Alle Rechner, die an einem gemeinsamen Ethernet Segment angeschlossen sind, müssen eine IP Adresse mit gleicher Subnet Adresse haben.
Anhand der ersten Dezimalzahl kann man erkennen welcher Klasse die IP Adresse entspricht.

Klasse	1. Dezimalzahl	Anzahl Bytes für Subnet Adresse	Anzahl Bytes für Hostadresse	Anzahl Subnet Adressen	Anzahl Hostadressen in einem Netz	Anwender
A	1-126	1	3	126	16.387.064	Grosse Firmennetze
B	128-191	2	2	16.384	64.534	Mittlere Firmennetze
C	192-223	3	1	2.097.152	254	Firmennetze

Es gibt reservierte IP Adressen, z.B. MAC Broadcast Adresse und private IP Adressen, z.B. für Klasse C der Bereich 192.168.0.0 bis 192.168.255.255, die nicht im Internet verwendet werden dürfen. Diese werden für private Netze verwendet, die nicht im Internet erreichbar sind. Falls diese Netze im Internet erreichbar sein sollen, müssen die private IP Adressen vom Router in offizielle IP Adressen umgesetzt werden.

Subnet Mask

Wird die IP Adressen mit der Subnet Mask bitweise logisch und verknüpft, so erhält man die Subnet Adresse
Jede Klasse hat folgende Standard- Subnet Mask.

Klasse	Standard- Subnet Mask	Binär
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

Dies erlaubt in Klasse C maximal 254 Hostadressen in einem Netz. Falls die IP Adressen knapp sind, kann man von den Standard- Subnet Mask abweichen und mehrere Subnet bilden, die weniger Host enthalten, z.B. 4 Subnet mit maximal 254/4 Host.

Beispiel:

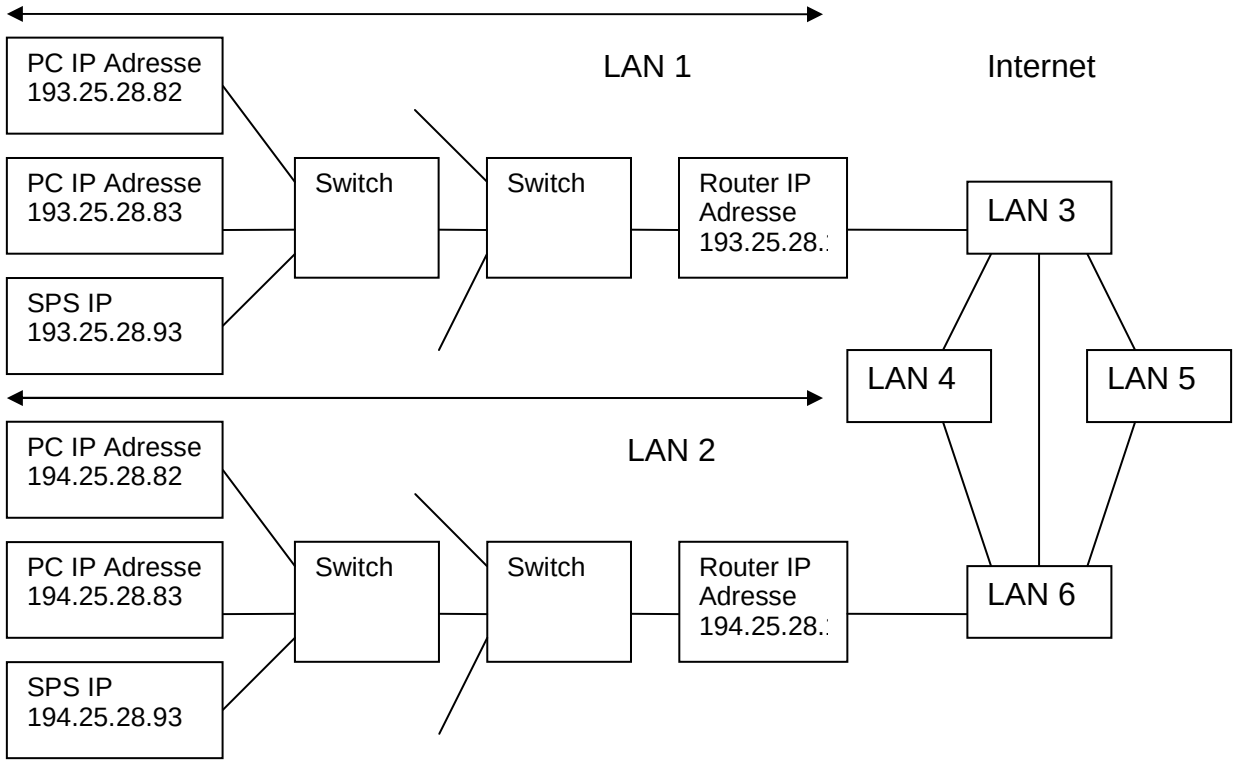
IP Adresse	193.25.28.55	11000001.00011001.00011100.00110111
Subnet Mask	255.255.255.0	11111111.11111111.11111111.00000000
Subnet Adresse	**193.25.28**.0	11000001.00011001.00011100.00000000

Netzwerk Protokolle

ISO /OSI Ebenen und S7 Systeme mit OPC

ISO /OSI Ebenen	**Bezeichnung**	**Funktion**	**Merkmale**	**S7 Systeme**
				Herstelleruna Client Zugriff
				Herstelleruna Server oder Programm St
7	Application layer (Anwendungsschicht)	Bereitstellung anwendungsspezifischer Kommunikationsdienste	Kommunikationsdienste z.B. Read/Write Start/Stop	Herstellerabh Protocol S7 F
6	Presentation layer (Darstellunsschicht)	Datendarstellung Umsetzung der normierten Darstellungsart des Kommunikationssystems in eine gerätespezifische Form	Gemeinsame Sprache	
5	Session layer (Sitzungsschicht)	Synchronisation Auf , Abbau und Überwachung einer Sitzung	Koordination der Sitzung	
4	Transport layer (Transportschicht)	Verbindungsauf / abbau, Paketwiederholung, Paketsortierung, Paketierung	Gesicherte Übertragung von Paketen	Transport Co TCP (Fehlerf Softwarekana
3	Network layer (Vermittlungsschicht)	Adressierung anderer Netze/ Wegewahl (Routing), Fluß kontrolle	Kommunikation zwischen zwei Subnetzen	Internet Proto Adress Resol ARP
2	Data link layer (Sicherungsschicht)	Zugriffsverfahren, Begrenzung der Datenblöcke, gesicherte Datenübertragung, Fehlererkennung, Fehlerbehandlung	CRC Check, CSMA/CD Token	Ethernet
1	Physical layer (Bitübertragungsschicht)	Physik der Datenübertragung, Übertragungsmedium, Baudrate, Festlegung der elektrischen, mechanischen, funktionellen Parameter der Leitung/Bus	Koax/Triaxkabel, LWL Kabel, 2 Draht Leitung	

Beispiel Topologie



Zentrales Protokoll, welches in dem Anwendungsfeld der Internetkommunikation die wichtigste Rolle spielt, ist das Internet-Protokoll abgekürzt IP, welches häufig auch mit der wichtigsten Ergänzung, dem Transport Control Protokoll abgekürzt TCP als Kombination TCP/IP bekannt ist.

IP Standard
Das IP ist die Basis für die Kommunikation im Internet, durch die Netzwerkteilnehmer in der ganzen Welt angesprochen werden können. Die Verbindung wird unter Umständen über mehrere Rechner (Router) im Internet geknüpft. Diese Route wird dynamisch für jedes versandte Datenpaket erstellt und kann zwischen zwei gleichbleibenden Kommunikationspartnern verschiedene Wege nehmen. Dieses Verhalten macht im Zusammenhang mit redundanten Netzwerkverbindungen im Fehler- oder Auslastungsfall Sinn. Ermöglicht wird dieses dynamische Routing durch die strukturierte IP-Adressierung, welche beim noch aktuellen Stand aus insgesamt vier Bytes besteht. (Eine Erweiterung dieser Adressierung von bisher 32 Bit auf 128 Bit steht unmittelbar durch die Einführung des renovierten IPv6 bevor, da der Adressraum im explosionsartig wachsenden Internet mittlerweile knapp geworden ist.)

Will ein Netzwerkteilnehmer einen anderen Teilnehmer über IP ansprechen, muss er auf der Basis der Subnet Mask feststellen, ob der Kommunikationspartner im eigenen Subnetz erreichbar ist, denn dann kann er den Partner direkt physikalisch adressieren und ohne einen Router mit einzubeziehen. Ist der Partner außerhalb des eigenen Subnetzes zu erreichen, werden die Daten an einen im eigenen Subnetz erreichbaren Router übergeben. Dieser weiß, wie das Subnetz des Partners zu erreichen ist und vermittelt die Daten dorthin über das Internet weiter.

Hierzu ein Beispiel:

Ein Rechner mit der IP-Adresse 193.25.28.55 und der Subnetmask 255.255.255.0 möchte an den Kommunikationsprozessor mit der IP-Adresse 193.25.28.142 ein Datenpaket versenden. Die UND-Verknüpfung der Subnetmask mit der eigenen und der Ziel-Adresse ergibt, dass die beiden Teilnehmer in dem gleichen Subnet kommunizieren und das Datenpaket somit direkt an den CP gesandt werden kann.

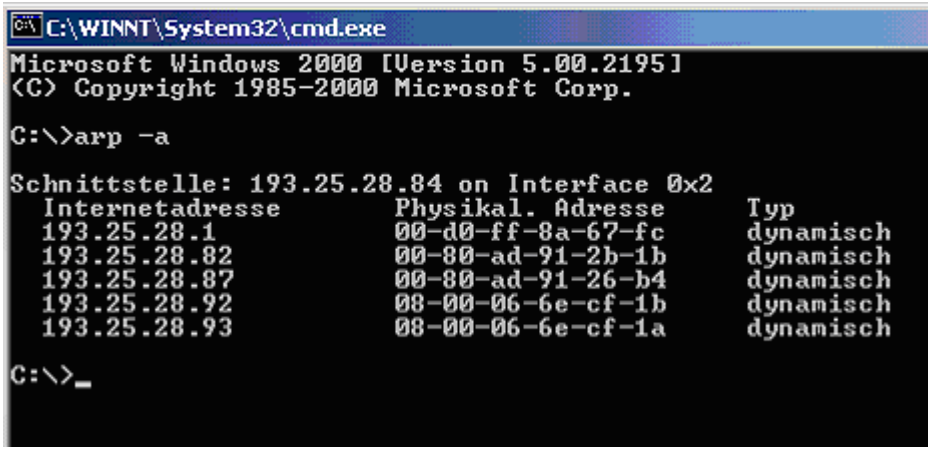
	Rechner	CP
IP-Adresse	193.25.28.55	193.25.28.142
Subnetmask	**255.255.255**.0	**255.255.255**.0
Subnet Adresse	**193.25.28**.0	**193.25.28**.0

Dies entspricht den Verhältnissen im Labor 4.1.06, jeder Rechner kann jeden anderen Rechner oder CP im Labor direkt im gleichen Subnetz erreichen, sodass hier kein Router an der Kommunikation beteiligt ist. Rechner wie z.B. der Mailserver der FH oder ein CP in einem anderen Gebäude lägen außerhalb des eigenen Subnetzes und könnten nur über einen Router erreicht werden. Das gesamte Netzwerk hat die Adresse 193.25.28.0 und diesem Netzwerk ist der Router unter 193.25.28.1 erreichbar.

Damit also die Kommunikationsprozessoren am IP- Datenverkehr teilnehmen können muss Ihnen bei der Projektierung eine eigene eindeutige IP- Adresse und die Subnetmask sowie bei erweiterter Kommunikation auch die IP- Adresse des Routers im eigenen Subnetz mitgeteilt werden. Letzteres ist nicht notwendig solange man keine Kommunikation mit Teilnehmern außerhalb des Labors aufnehmen will.

Die eigentliche Datenkommunikation läuft immer auf der Ebene der physikalischen MAC- Adressen ab. Jede Ethernet-Komponente ist mit einer weltweit einmaligen MAC-Adresse vom Hersteller versehen, über die sich die Netzwerkkomponenten innerhalb eines Netzwerksegmentes direkt ansprechen können. TCP/IP ist ein überlagertes Protokoll, was die Verbindung über mehrere Rechner in andere LAN über einen Router ermöglicht.

Läuft die Kommunikation über TCP/IP ab, dann wird mit Hilfe des Adress Resolution Protokolls (ARP) die IP- Adresse in eine MAC- Adresse aufgelöst indem alle Teilnehmer des Subnetzes gefragt werden, wer denn die gefragte IP- Adresse hat. Danach wird die Verbindung direkt unter Verwendung der MAC-Adressen hergestellt. Die Auflösung der IP- in MAC- Adressen erfolgt nicht bei jeder Datenübertragung, sondern die Teilnehmer halten sich die Ergebnisse bereits aufgelöster Anfragen in einer Tabelle für die nächste Übertragung an diese IP- Adresse vor, um Netzwerkverkehr und Zeitaufwand zu reduzieren. Die Tabelle läst sich auf Windows NT Systemen in der Befehlseingabe (DOS Box) mit arp –a` anzeigen.



Ist der Partner außerhalb des eigenen Subnetzes zu erreichen, werden die Daten an einen im eigenen Subnetz erreichbaren Router übergeben. Dieser weiß, wie das Subnetz des Partners zu erreichen ist und vermittelt die Daten dorthin über das Internet weiter. Jeder Router kennt die beiden Subnet Adressen der benachbarten LAN und sucht den günstigsten Weg.

Die Übertragung der Daten erfolgt in Datenpaketen, die unterschiedliche Wege nehmen können.

IP Standard
Der IP Standard garantiert nicht, dass die Datenpakete auch ankommen. Der TCP Standard stellt dies sicher. Fehler werden korrigiert. Weiter wird ein bidirektionaler Kommunikationskanal zwischen 2 Programmen auf Basis der Port Nr. zur Verfügung gestellt.

Port Nr	Dienst
1-1024	well known portnumbers (bekannte Dienste)
20 21	FTP = File Transfer Protocol, Zugriff auf Daten eines FTP Servers
23	TELNET = Interactive Terminal Login, um auf einem fernen Rechner Programme oder Dienste zu nutzen
25	SMTN =Simple Mail Transfer Protocol, e-mail
80	http = Hyper Text Transfer Protocol, um HTML Seiten (Web Seiten) zu übertragen, HTML = Hyper Text Markup Language
102	Prozesswerte lesen und schreiben
Ab 1024	Not well known portnumbers (nicht bekannte Dienste)

Die Dienste beruhen auf dem Client Server Prinzip. Der Server stellt den Dienst an einer TCP- Port-Nummer bereit. Der Client öffnet einen Softwarekanal durch Angabe einer Socket- Nummer, die aus IP Adresse und Port Nummer besteht.

Beispiel: Es soll vom Client (PC) mit der IP Adresse 193.25.28.82 auf eine HTML Seite auf eines Servers (SPS) mit IP 193.25.28.93 zugegriffen werden.
Ziel Socket : 193.25.28.93: 80
Bei diesem Zugriff des Clients reserviert der Client eine zufällige Port- Nummer, z.B. 2000 und teilt dies dem Server mit. Damit ist dem Server bekannt, an wen er die Daten der Webseite schicken kann.
Absender Socket: 193.25.28.82: 2000

Kommunikation nur innerhalb eines Subnet
Solange die Kommunikation nur innerhalb eines eigenen Subnetzes erfolgt, also die Teilnehmer sich direkt über die physikalische Adresse erreichen können, kann eine Kommunikation auch ohne das TCP/IP Protokoll auskommen, z.B. können die CP´ s und PG´ s von Siemens auch über eine sogenannte ISO-Verbindung miteinander kommunizieren, über eine Protokoll, welches von der Firma Siemens speziell für die eigenen Automatisierungsgeräte im Ethernet entwickelt wurde, bevor sich IP als Standard bewährt hatte. Diese Kommunikation funktioniert dann nur zwischen Teilnehmern im gleichen Netzwerksegment kann also nicht geroutet werden.

IP Adressen Raum 4.1.06, 4.1.08

Allgemein	Raum 4.1.06: PC IP Adresse	Raum 4.1.06: CP 343-1IT IP Adresse	Raum 4.1.08: PC IP Adresse
Subnetzmaske 255.255.255.0 Standardgateway 193.25.28.1 Bevorzugter DNS Server 193.25.16.3 Alternativer DNS Server 129.217.131.35	Fb3-rt2 193.25.28.82 Fb3-rt3 193.25.28.83 Fb3-rt4 193.25.28.84 Fb3-rt5 193.25.28.85 Fb3-rt6 193.25.28.86 Fb3-rt7 193.25.28.87	193.25.28.93 193.25.28.92 193.25.28.94	fb3-sps01 193.25.28.50 fb3-sps02 193.25.28.51 fb3-sps03 193.25.28.52 fb3-sps04 193.25.28.53 fb3-sps05 193.25.28.54 fb3-sps06 193.25.28.55 fb3-sps07 193.25.28.56 fb3-sps08 193.25.28.57 fb3-sps09 193.25.28.58 fb3-sps10 193.25.28.59

Kommunikation mit CP343-IT

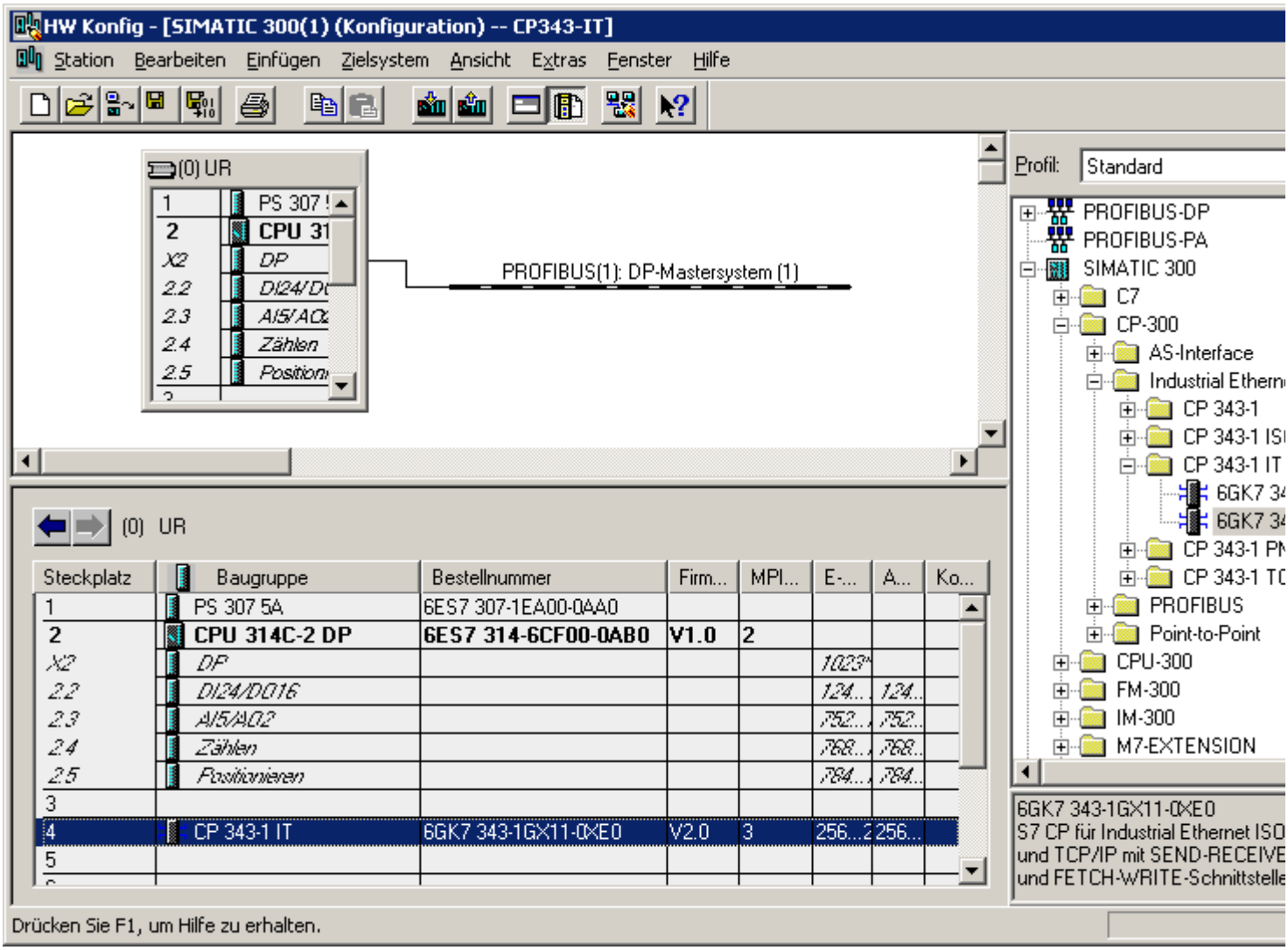
Kommunikations Hardware

Um Ethernet in der SPS-Kommunikation einsetzen zu können, bedarf es eines Kommunikationsprozessors (CP) für SPS, der die Kommunikation über Ethernet zur Verfügung stellt. Der CP selbst führt alle notwendigen Operationen für Ethernet-Kommunikation in seiner eigenen Hardware aus, ohne die CPU mit Kommunikationsaufgaben zu belasten. Der CP kann neben der reinen Ethernet-Kommunikation zwischen verschiedenen SPS oder anderen Automatisierungsgeräten und PCs auch für Visualisierungsaufgaben eingesetzt werden. Außerdem ist es möglich die SPS-Anlage mit einem solchen CP auch aus der Ferne mit einem Programmiergerät über das Internet Protokoll (IP) anzusprechen, sodass eine umfassende Fernwartung möglich ist. Der hier verwendete CP verfügt über einen integrierten Webserver, der im Zusammenhang mit Java-Programmierung Visualisierungen von Prozessen für jeden internetfähigen PC zur Verfügung stellen kann. Der CP kann auch Alarm- und Zustandsmeldungen per Mail übers Internet versenden.

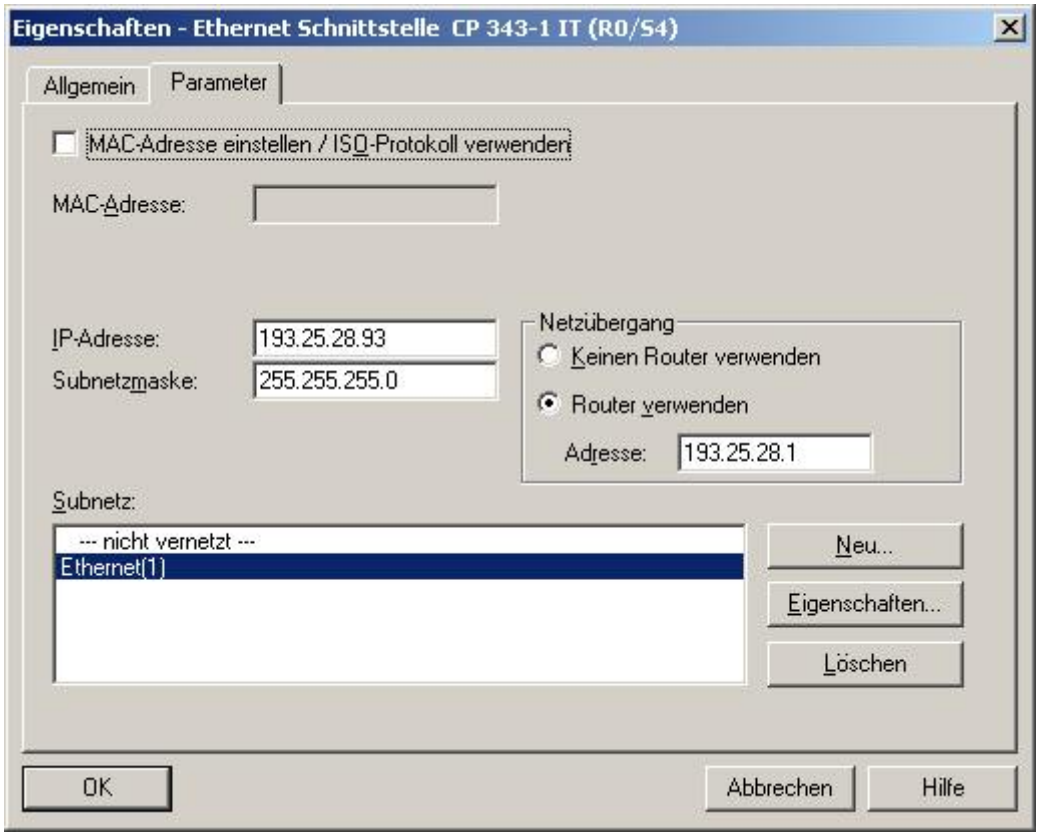
Im SPS-Labor sind drei SPS-Systeme mit einem Ethernet CP ausgerüstet. Dabei handelt es sich um drei CPU 314C-2 DP zusammen mit jeweils einem CP 343-1 IT, der die oben beschriebenen Fähigkeiten besitzt. Der CP wird wie andere Ergänzungsmodule der SPS auf der Profilschiene montiert und über den Rückwandbus mit der SPS verbunden, benötigt aber noch zur Energieversorgung eine zusätzliche Verbindung zum Netzteil der SPS. Netzwerktechnisch kann der CP über zwei verschiedene Anschlüsse an das Ethernet angeschlossen werden. Der AUI-Anschluss ermöglicht den Anschluss an eine nur noch selten eingesetzte Bustopologie, der RJ45-Anschluss ermöglicht die Verbindung über die heute weit verbreitete strukturierte Twisted Pair Verkabelung, die in der Rechnerwelt Standard geworden ist. Im Labor werden die CPs über die letzte Möglichkeit in das Rechnernetz des Labors integriert.

Einbinden des CP in die Hardwarekonfiguration

Öffnen der Hardwarekonfiguration im Simatic Manager, Auswahl des CP 343-1 IT aus dem Katalog (Simatic 300 – CP-300 – Industrial Ethernet), Ziehen der CP auf Steckplatz 4 (der CP erhält eine eigene MPI-Adresse)

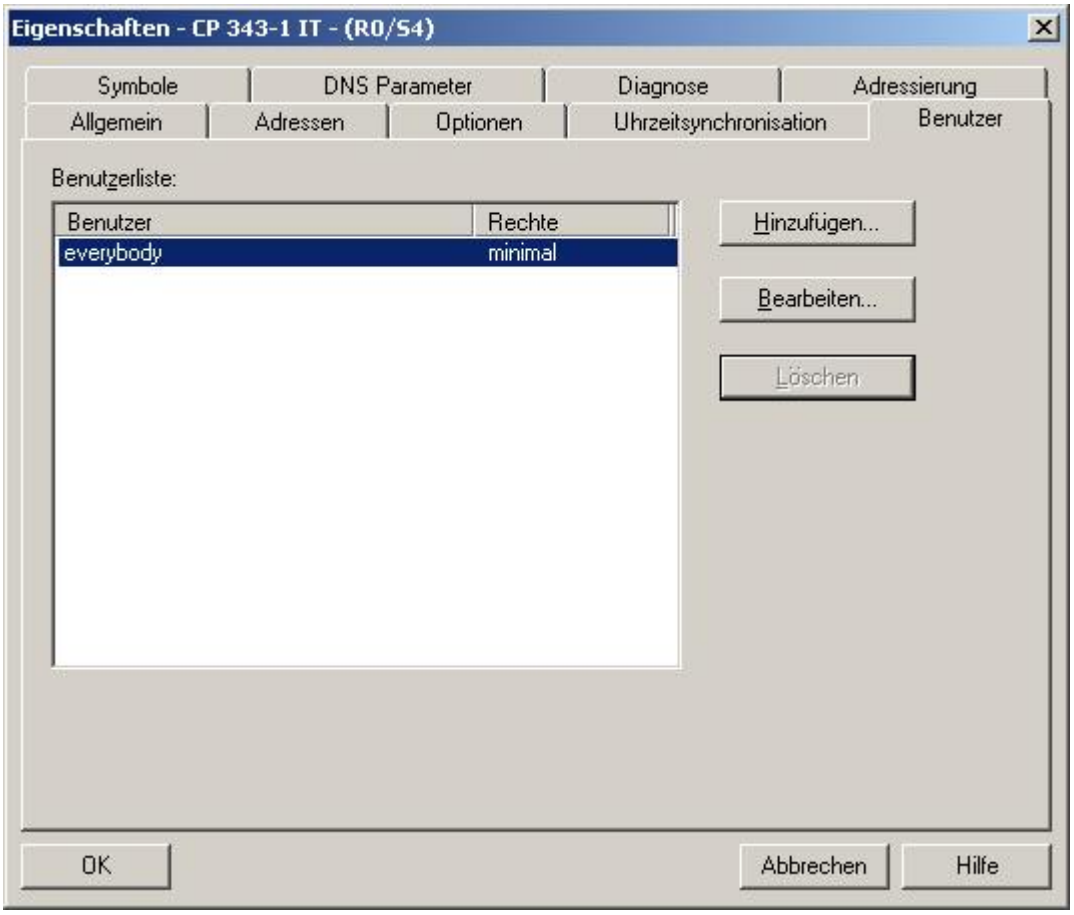


Einstellen der Netzwerkparameter, also IP-Adresse und Subnetzmaske (auch später durch Doppelklick auf den CP möglich), Auswahl des logischen Netzes, in dem die Kommunikation mit anderen Automatisierungsgeräten stattfindet. Bei *Siemens* auch Subnetz genannt, ohne das es direkt mit dem physikalischen Subnetz zusammenhängt, sondern einfach eine logische Verbindungsebene zwischen den Kommunikationspartnern benennt. Eventuell zuerst dieses „Ethernet-Subnetz“ über Button -Neu-erzeugen. Wenn nötig Router-Adresse eintragen

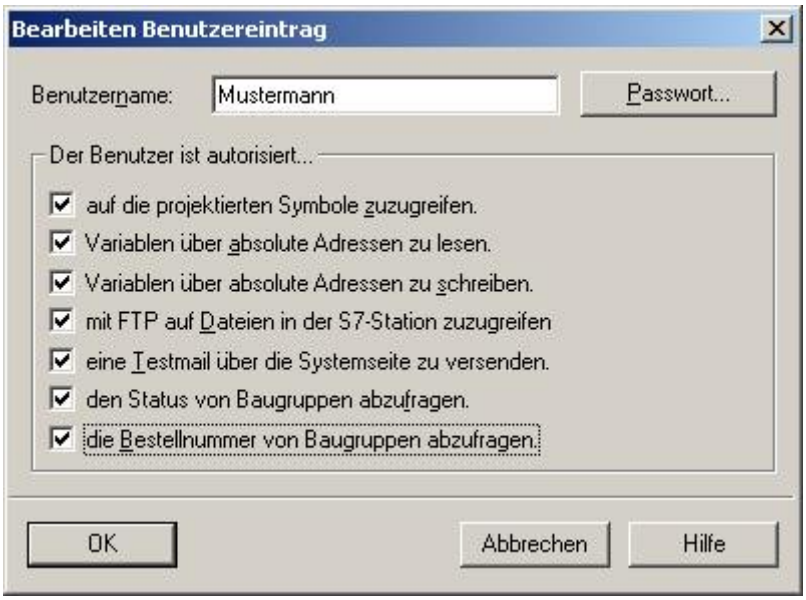


Einrichten der Benutzerrechte

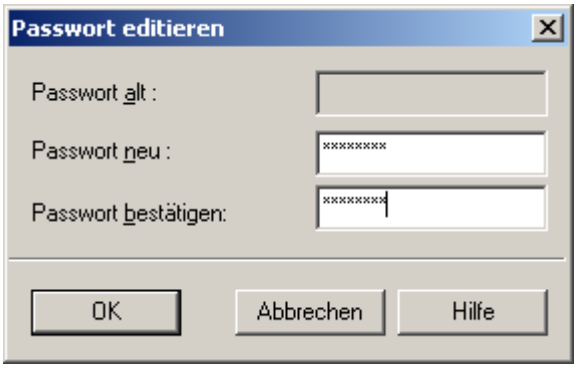
Der CP kann für verschiedene Aufgaben der Fernwartung und Visualisierung eingesetzt werden. Damit diese Möglichkeiten des Fernzugriffs auf eine Automatisierungsanlage nicht missbraucht werden kann, muss sich der Benutzer, der über das Netzwerk auf den CP zugreifen will, in vielen Fällen eine Authentifizierung durchführen. Da sich die Webserver-Visualisierung gut für einen Funktionstest nach der ersten Konfiguration eignet, werden auch hier Benutzerrechte vergeben. Für die Kommunikationslösungen, die im weiteren Verlauf näher erläutert werden, ist die Authentifizierung nicht notwendig. Hier werden die Berechtigungen konfiguriert, um die Netzwerkanbindung des CP´ s zu überprüfen.
Durch Doppelklick auf den CP das Eigenschaften- Fenster öffnen und in die Registerkarte „Benutzer“ wechseln



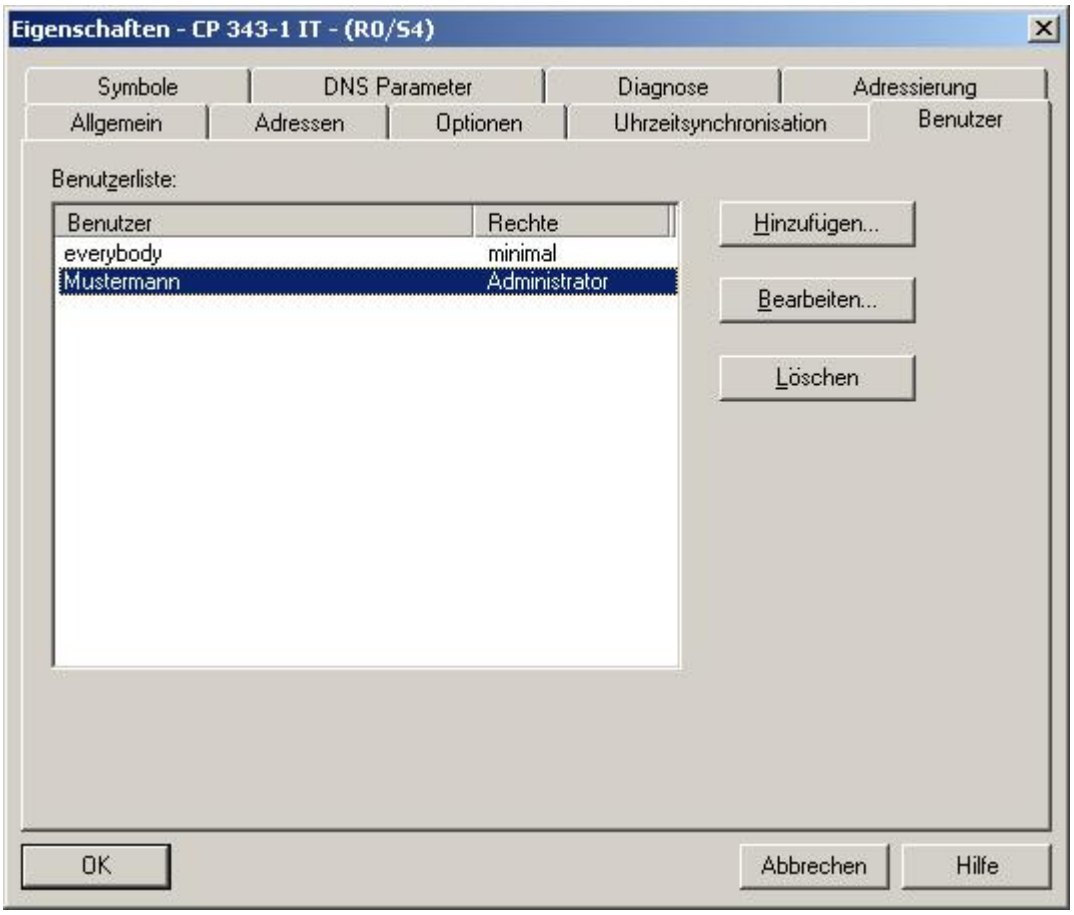
Standardbenutzer hat nur eingeschränkte Zugriffsrechte, daher über Button „Hinzufügen“ einen neuen Benutzer mit allen Zugriffsrechten anlagen



Eventuell ein Passwort für den angegebenen Benutzernamen anlegen



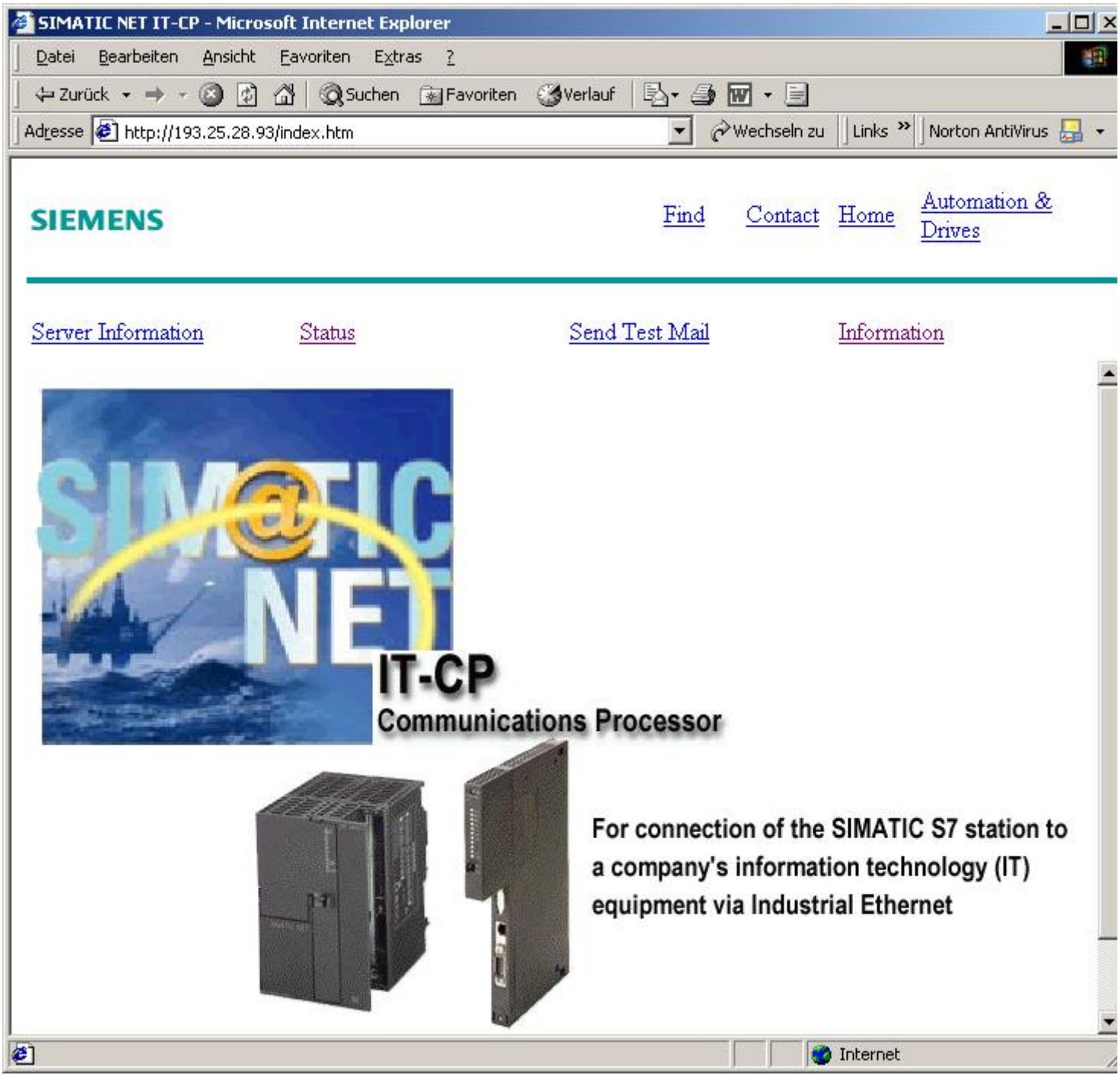
Der neu angelegte Benutzer gilt nun als „Administrator“



Laden der Hardwarekonfiguration in die CPU

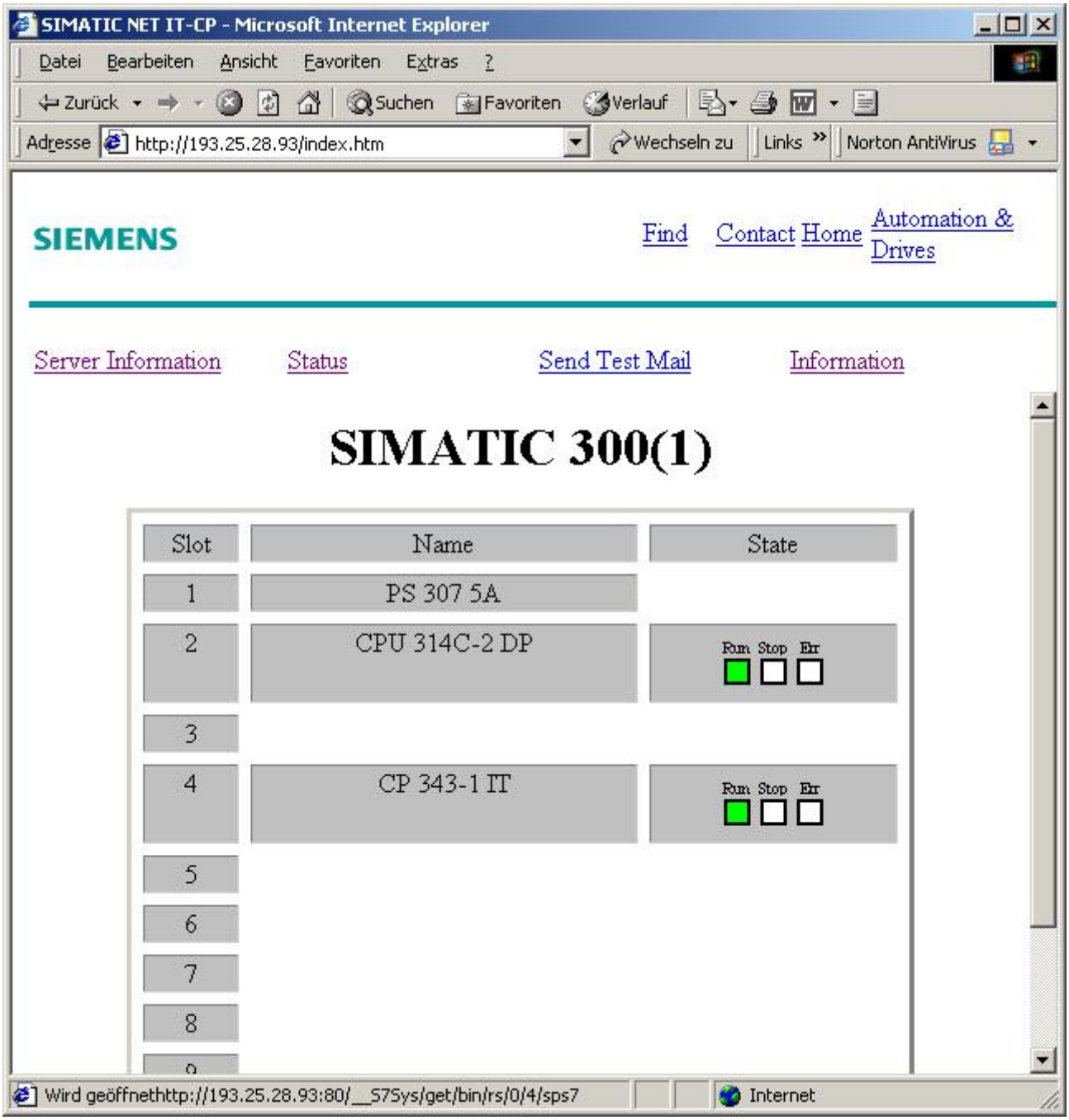
Testen der Verbindung zum CP über einen Webbrowser

Starten des Webbrowsers und Eingabe der vorher konfigurierten IP-Adresse des CP



Auswahl des Menüpunktes „Status“ und bei Passwortabfrage Benutzername und Passwort angeben

Muster-Webseite zur Statusabfrage der CPU- und CP-Zustände wird angezeigt.



Konfiguration und Programmierung einer Datenverbindung zwischen Automatisierungsgeräten über *Ethernet /TCP/IP*

Voraussetzungen:

- Step7 V5.1 + ServicePack 4
- SIMATIK NET PC Software V6.0
- Zwei S7 300 *CPU314C-2 DP* mit CP 343-1 IT, über *Ethernet* vernetzt.

Inbetriebnahme und Konfiguration einer ISO-on-TCP Verbindung

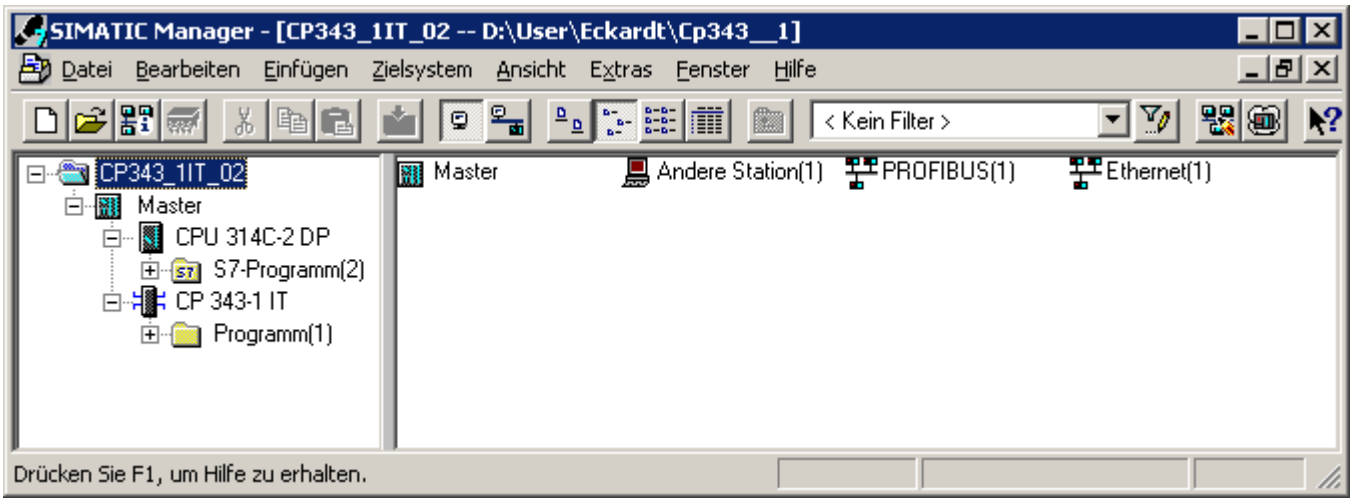
Für jede Station wird ein eigenes Projekt angelegt, bei dem wie oben beschrieben die Hardware und Netzwerkparameter konfiguriert werden. Wichtig ist nun, dass natürlich die beiden CPs unterschiedliche eindeutige IP- Adressen bekommen und das unter den Eigenschaften des CPs ein „Subnetz“ (*Ethernet* (1)) existiert und ausgewählt ist. Da die IP- Adressen nicht frei gewählt werden können, sondern durch die Netzwerkadministration vorgegeben werden, sind die CP s im Labor hinter der Frontklappe mit ihrer IP-Adresse beschriftet. Die Subnetmask ist innerhalb eines Netzwerkes immer gleich.

Die drei IP- Adressen die hier für die CP s zur Verfügung stehen sind

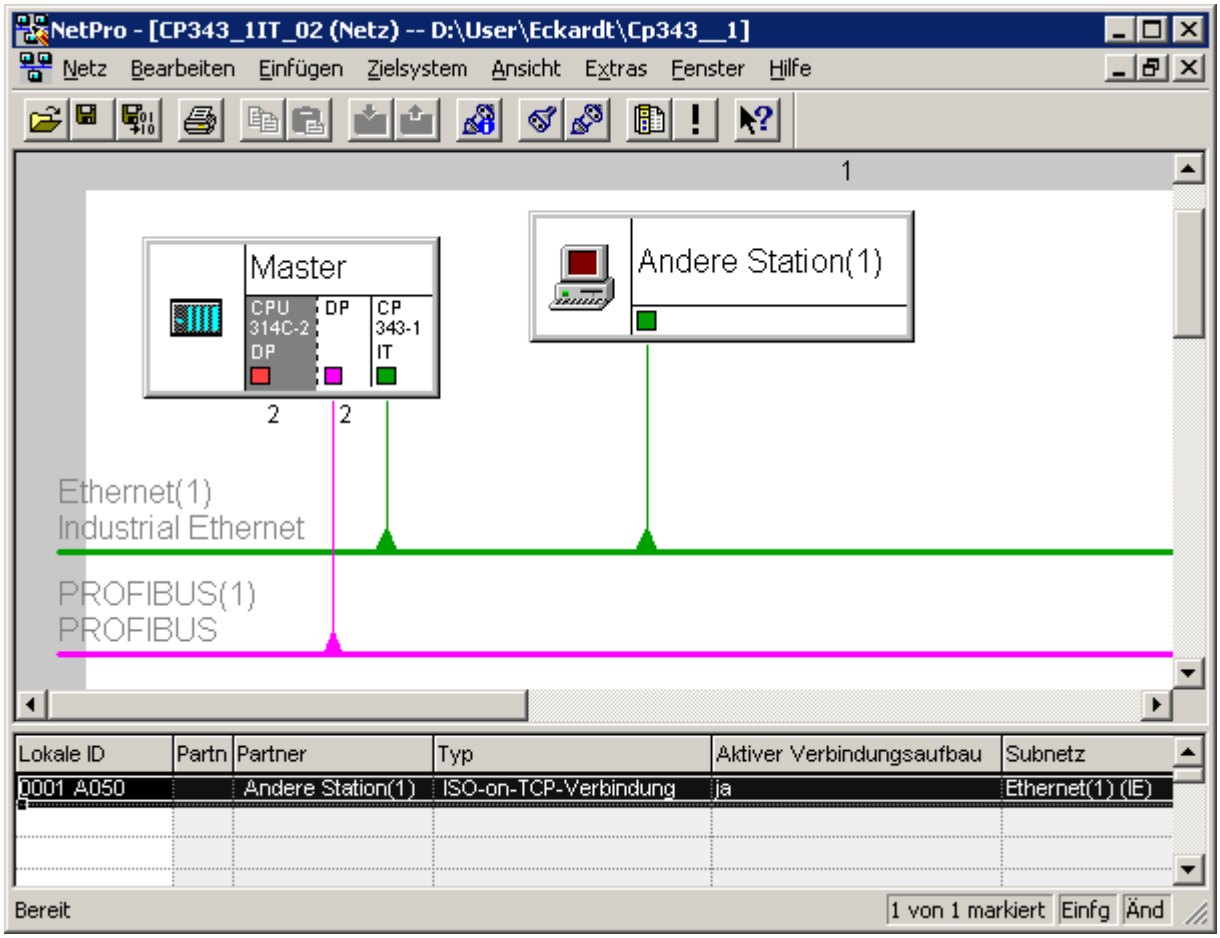
1. 193.25.28.92 Subnetmask 255.255.255.0
2. 193.25.28.93
3. 193.25.28.94

Eine Angabe der Router IP-Adresse ist nicht notwendig, da sich die CP s im Labor in einem Netzwerk befinden.

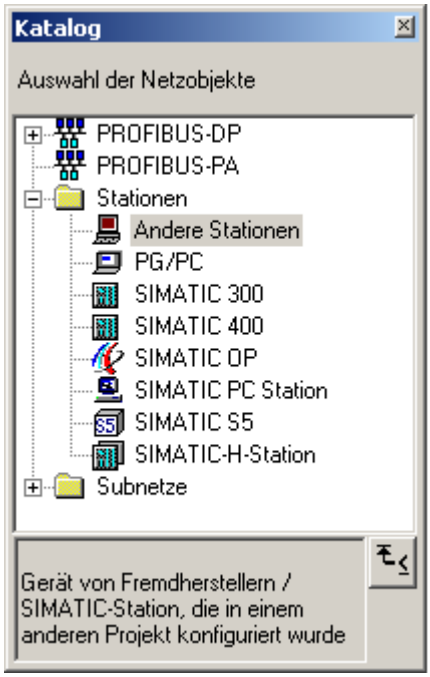
Das bei den Eigenschaften der Ethernetschnittstelle angelegte „Subnetz“ (*Ethernet*(1)) findet sich nun in dem Projektcontainer unter Step7 wieder:



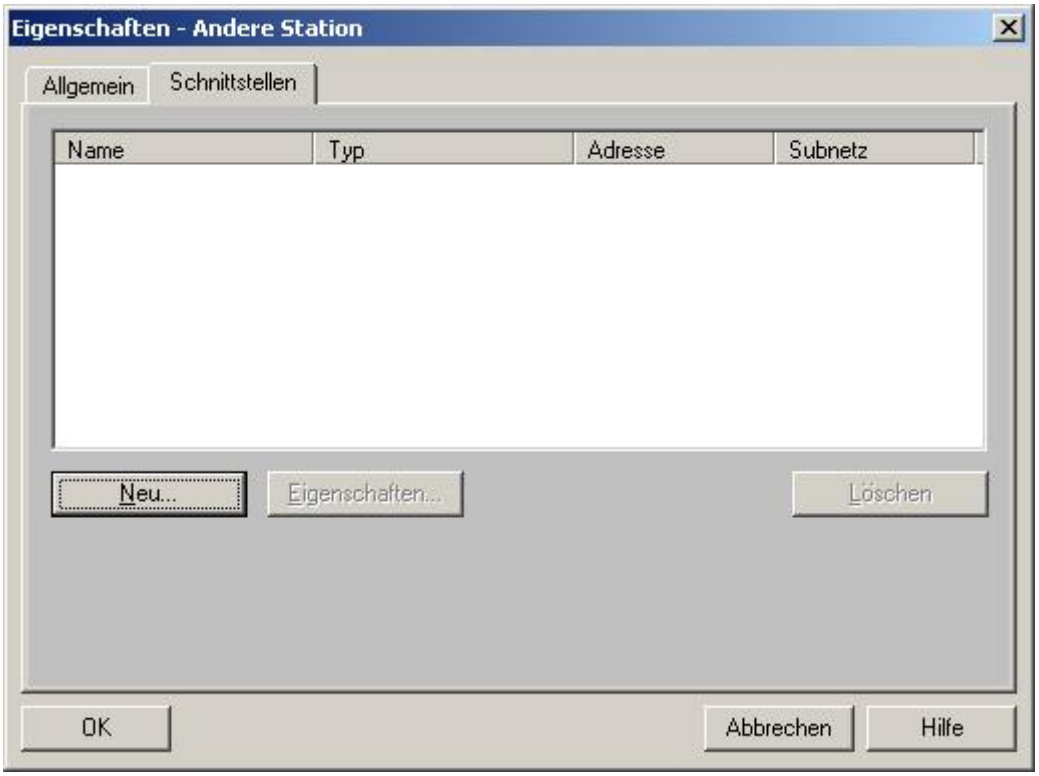
Durch Doppelklick auf dieses öffnet sich NetPro. Dort wird nun die andere Station mit den entsprechenden Netzwerkparametern eingefügt, sodass eine Verbindung zwischen den Stationen projektiert werden kann.



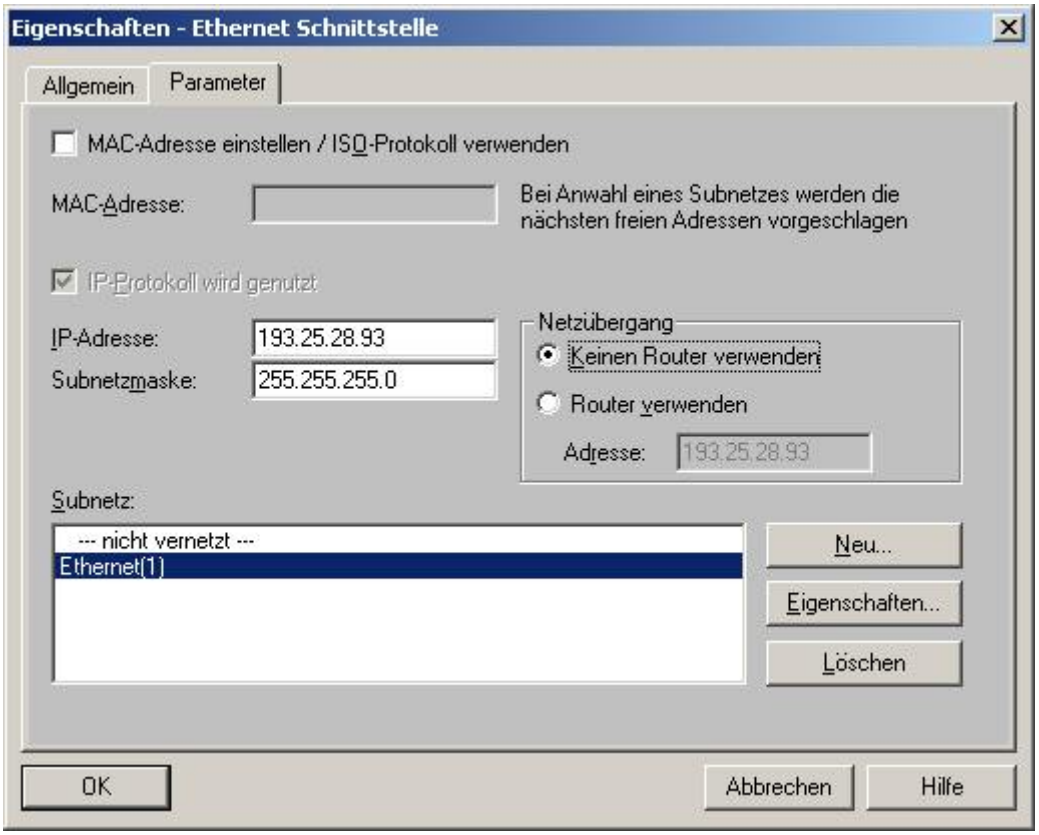
Mit Einfügen - Netzobjekte öffnet sich ein Katalog aus dem man unter Stationen „Andere Station“ auswählt.



Durch Doppelklick auf diese gelangt man in die Konfiguration derselben und fügt unter Schnittstellen eine neue Schnittstelle vom Typ Ind.Ethernet ein.



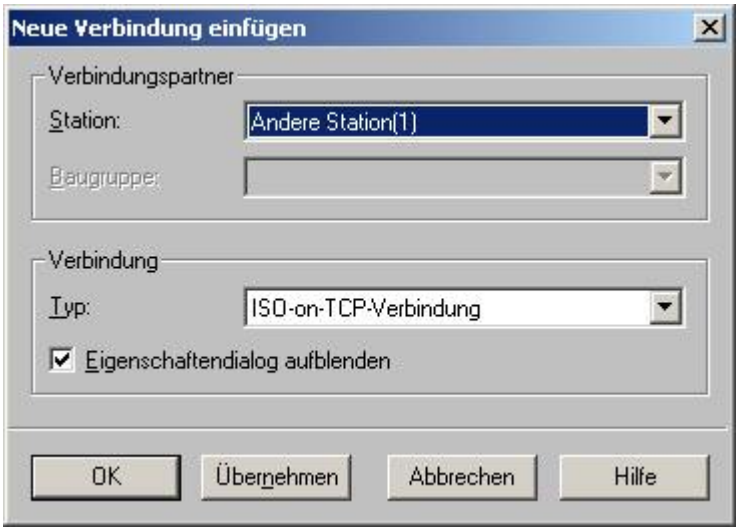
Worauf sich automatisch der Dialog für die Netzwerkweinstellungen der Partnerstation öffnen.



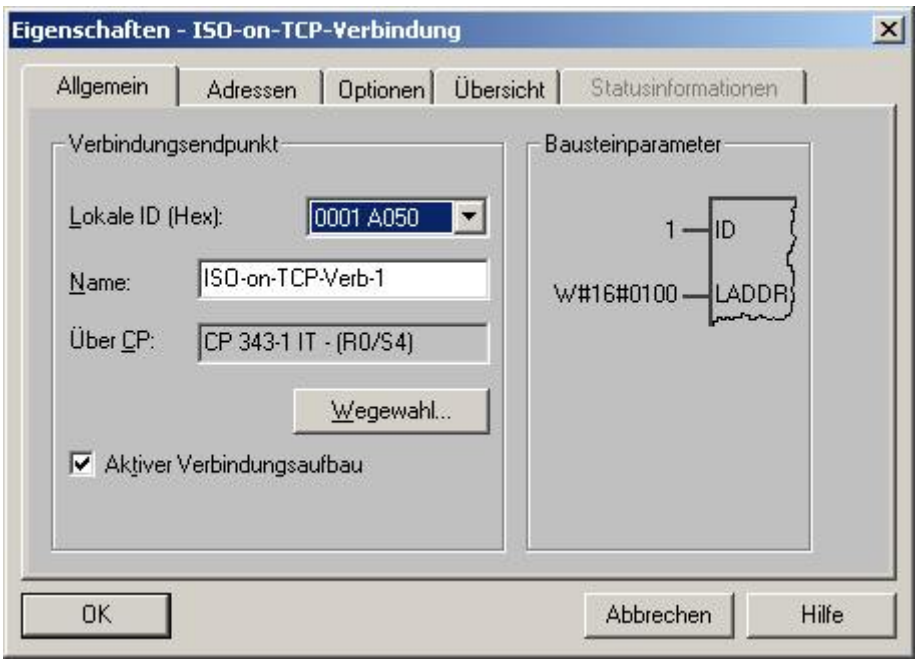
Dort ist darauf zu achten, dass die IP-Adresse der anderen Station angegeben wird und nicht die der Station in die das Projekt geladen wird. Wichtig ist auch, dass das Häkchen bei MAC-Adresse einstellen nicht gesetzt ist.

Nun kann eine ISO-on-TCP Verbindung eingerichtet werden, indem unter NetPro die *CPU* der eigenen Station ausgewählt wird und dann über Einfügen - Neue Verbindung die Maske entsprechend

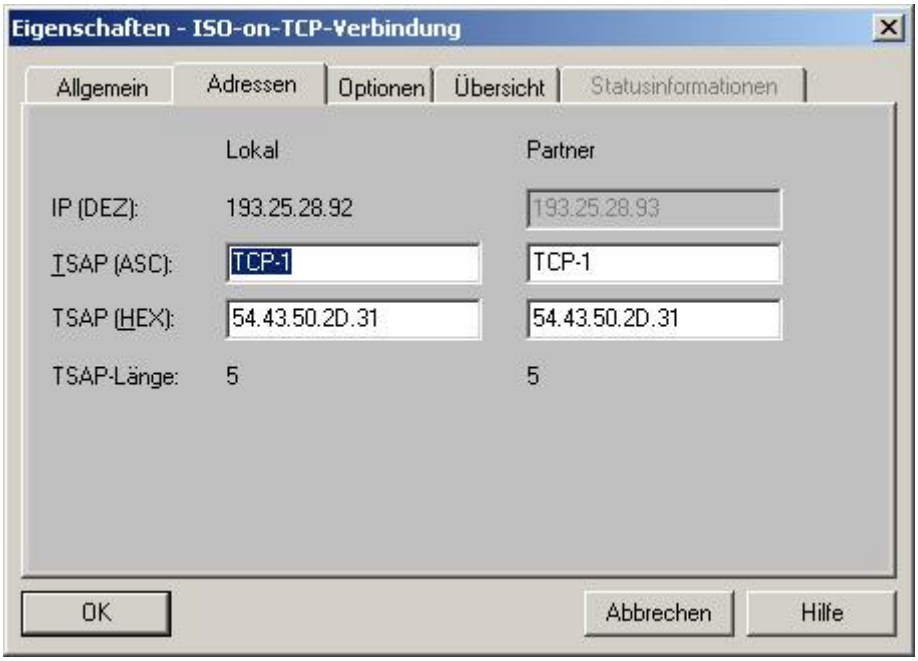
ausgefüllt wird:



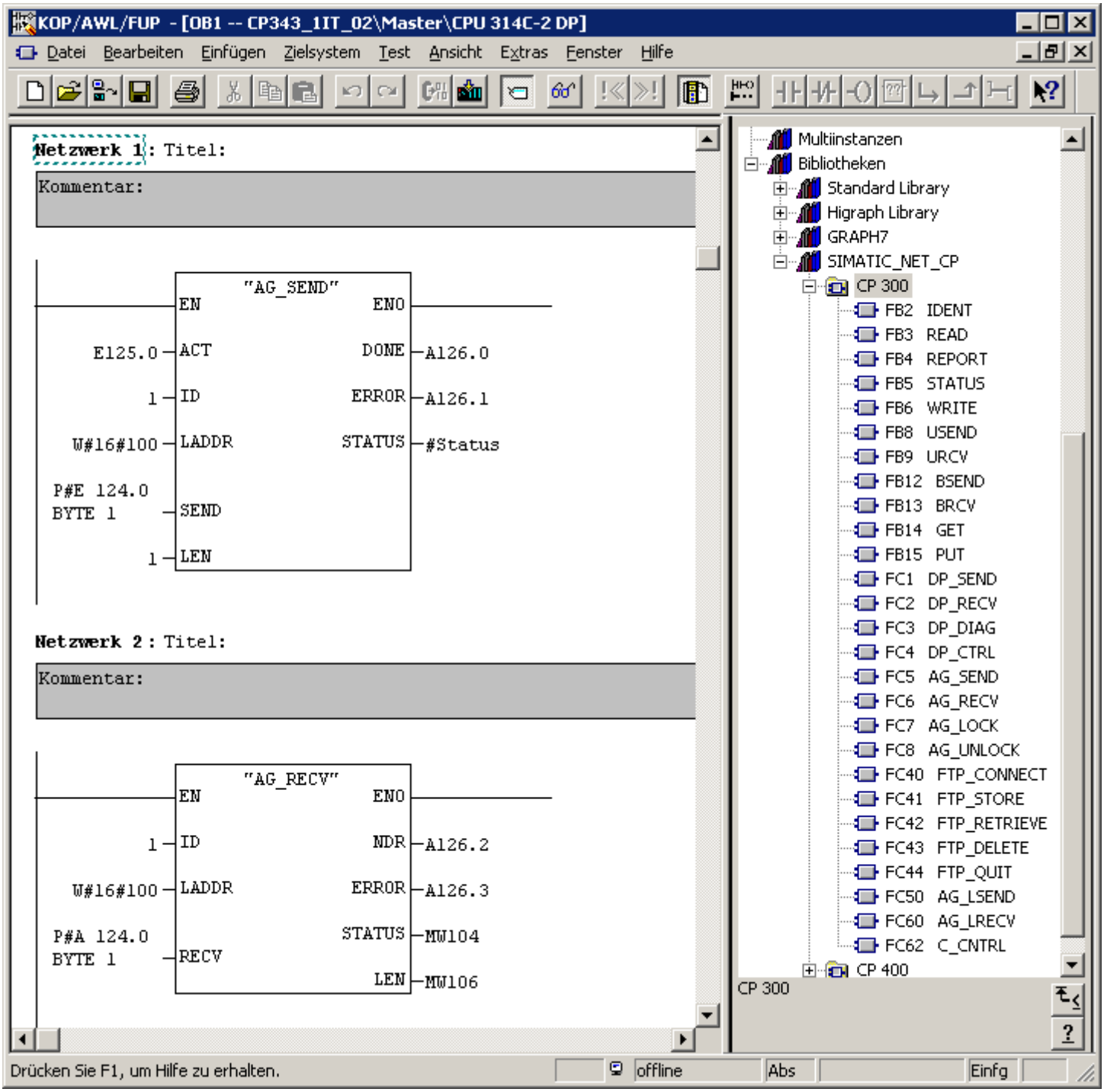
Nach der Auswahl der Verbindung öffnet sich auch hier automatisch die Konfiguration für die Verbindung, wobei die erste Maske „Allgemein“ für spätere Schritte zwei wichtige Angaben enthält, die bei der Programmierung der Verbindung gebraucht werden. Diese beiden Bausteinparameter sind zum einen die ID (in diesem Fall 1) und die LADDR (W#16#0100). Diese spezifizieren die Kommunikationsschnittstelle zwischen der *CPU* und dem CP für diese Verbindung.



Unter „Adressen“ wird der Verbindung noch eine Art Erkennungsname mit auf den Weg gegeben (hier TSAP). Diese Kennung ist frei wählbar, muss aber für beide Partner gleich lauten. Unter dem Feld TSAP (ASC) werden die eingegebenen Buchstaben noch einmal in Hexadezimal Darstellung angezeigt haben aber keine weitere Bedeutung.



Um nun Daten über diese eingerichtete Verbindung von einer Station zu einer anderen zu Übertragen, muss die Übertragung noch programmiert werden. Zu diesem Zweck gibt es zwei Funktionen AG_SEND (FC 5) und AG_RECV (FC 6), die in den Funktionsbibliotheken „SIMATIC_NET_CP“ zu finden sind.



Beide Funktionen benötigen nun die vorher schon erwähnten Verbindungsparameter ID und LADDR, die die Verbindung spezifizieren über die Daten gesendet oder empfangen werden sollen. Mit dem Pointer bei SEND bzw. RECV wird der Adressbereich angegeben, aus dem die Daten gesendet werden, bzw. wohin die Daten geschrieben werden, die empfangen wurden. Der Pointer benennt die Anfangsadresse und die Menge der Daten. In diesem Fall werden also alle 8 Bit des Eingangsbyte 124 gesendet und empfangene Daten auf das Ausgangsbyte 124 ausgegeben.

AG_RECV empfängt alle Daten, die über diese Verbindung gesendet wurden, AG_SEND wird durch ACT zustandsgesteuert aktiviert.
Die weiteren Parameter geben Status- und Fehlermeldungen aus und können im Detail in der Hilfe nachgeschaut werden.

Diese Konfiguration und Programmierung wird nun auf beiden Seiten weitgehend gleich projektiert, lediglich die eigene IP Adresse und die des Partners ist die jeweils andere. Dann werden in diesem Beispiel auch schon die Eingangsbits der einen Station auf die Ausgangsbits der anderen Station in beiden Richtungen übertragen, sobald der ACT Eingang von AG_SEND aktiviert wurde.

Fernwartung von Automatisierungsgeräten

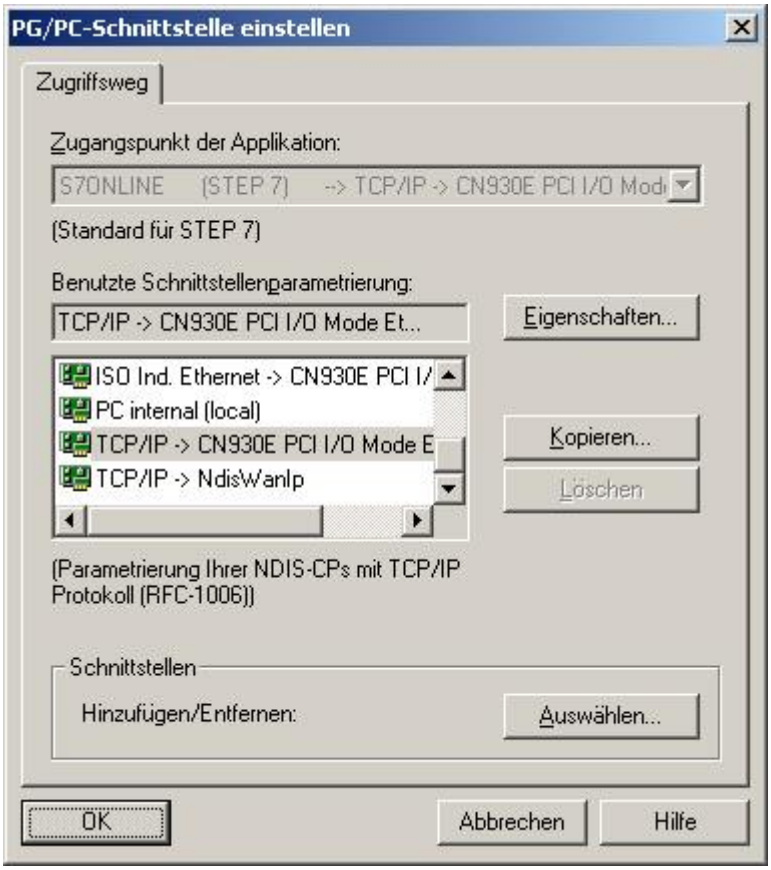
Voraussetzungen:

- Step7 V5.1 ServicePack4
- SIMATIC NET PC Software V6.0

Als Basisprojekt wurde hier zur Einbeziehung des Profibusses das archivierte Beispielprojekt (PB_NETZ.ARJ) benutzt, welches im Internet zur Verfügung steht. Dort muss nur noch wie oben beschrieben der Kommunikationsprozessor in der Hardwarekonfiguration hinzugefügt werden.

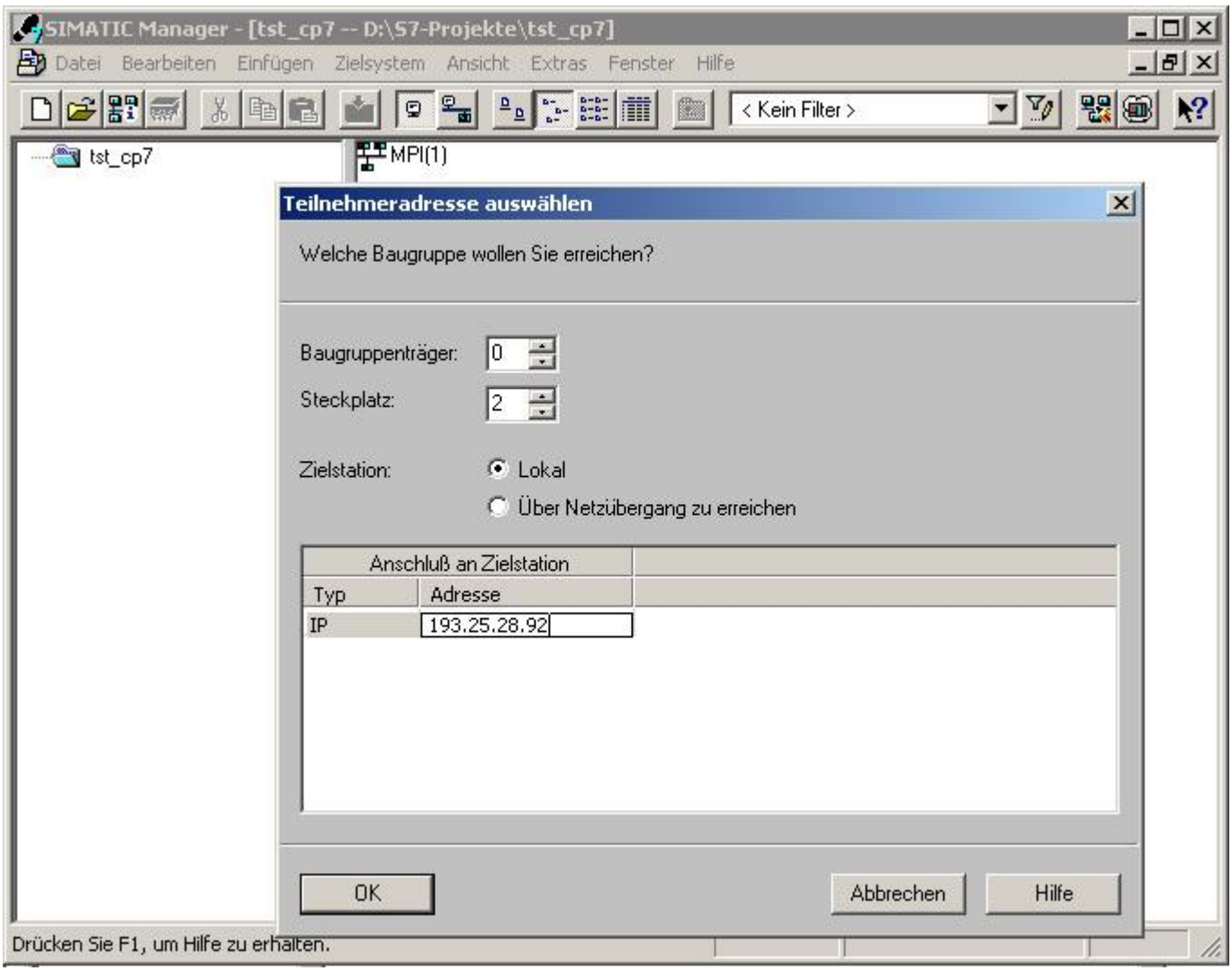
Ist der CP in einem Projekt eingebunden und bereits korrekt konfiguriert und in Betrieb genommen, kann man die Station auch über *Ethernet* mit einem Programmiergerät oder dem PC erreichen und über TCP/IP die Station theoretisch von jedem PC der Welt mit Internetanschluss erreichen.

Unter Step7 kann über „Extras“ – „PG/PC-Schnittstelle einstellen“ die Schnittstelle zur Kommunikation mit der *SPS* auf TCP/IP -> „Name der Lokale Netzwerkkarte“ umgestellt werden. Nun erreicht Step7 die *SPS* über *Ethernet-TCP/IP* genauso wie zuvor über *MPI* oder *Profibus* und die Anlage kann somit über große Entfernungen über das Internet beobachtet und Programmiert werden.



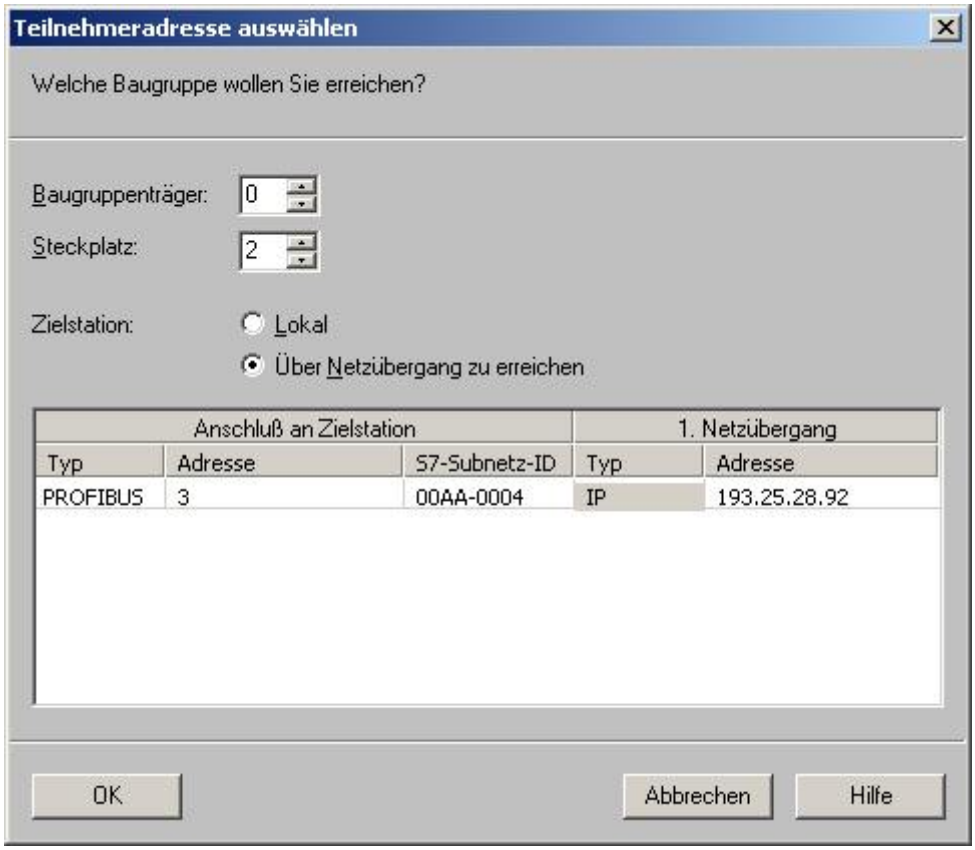
Soll eine *Automatisierungsanlage* ohne vorhandenes Projekt ferngewartet werden, dann muss die

Programmierung in ein neues Projekt aus der Anlage ausgelesen werden. Dazu legt man ein neues Projekt an „Datei – Neu“ und öffnet über „Zielsystem – Station laden in PG“ den Dialog, in dem die fernzuwartende Station adressiert wird.

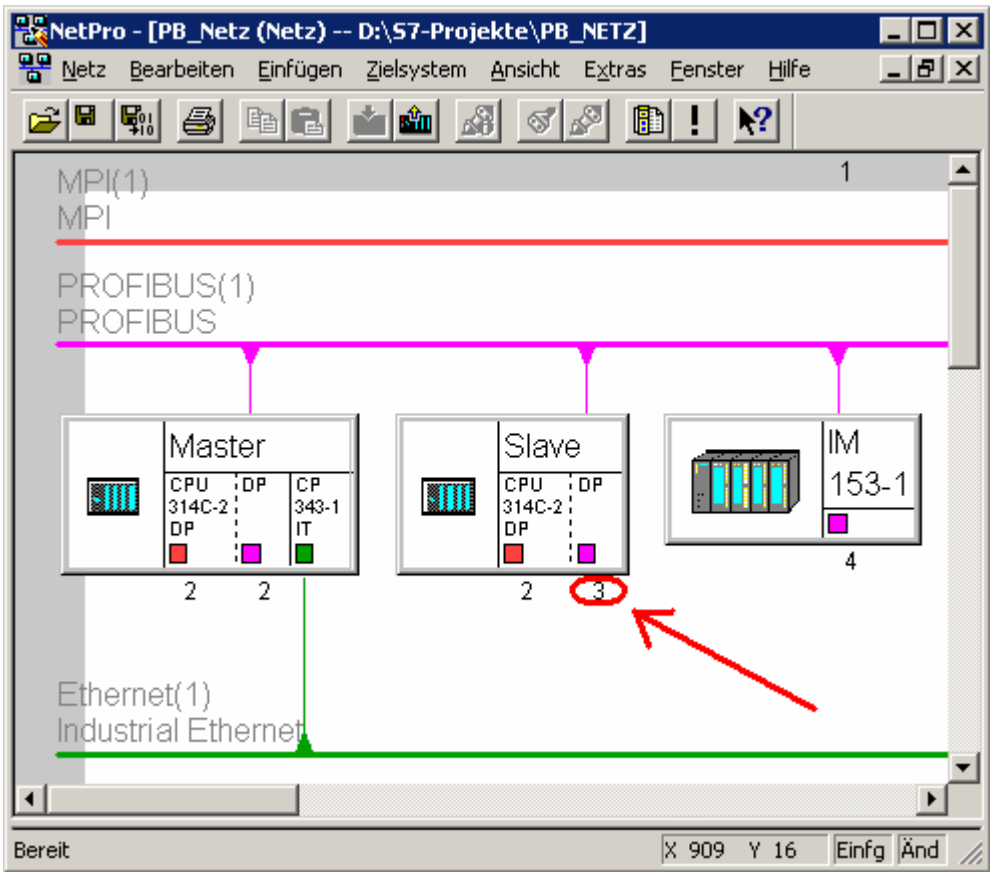


Um auf die *CPU* zuzugreifen, an der der Kommunikationsprozessor angeschlossen ist, muss die Maske analog zur obigen Abbildung ausgefüllt werden. Sobald nun die Station in das Projekt geladen wurde, kann man wie gewohnt darauf zugreifen.

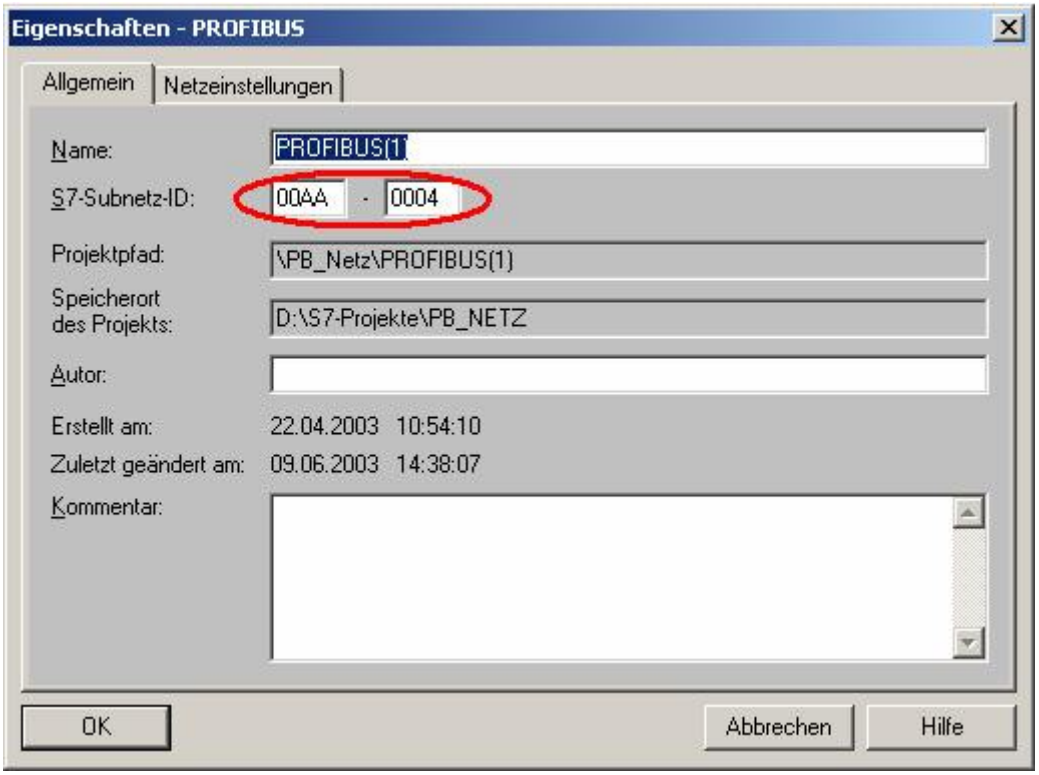
Wenn eine Slave -Station angesprochen werden soll, die über *Profibus* an die *CPU* mit dem CP angeschlossen ist, dann ruft man wieder den obigen Dialog über (Zielsystem – Station laden in PG) auf und stellt Zielstation von „Lokal“ auf „Über Netzübergang zu erreichen“.
Nun muss zusätzlich zu der IP Adressierung natürlich noch die Busadressierung berücksichtigt werden.



Zunächst durch Klick auf die Busbezeichnung (unter Typ) den Bustyp (*Profibus*) auswählen. Die *Profibus* –Adresse und S7-Subnetz-ID erfährt man aus der Netzprojektierung des ursprünglichen Projektes.



Durch Doppelklick auf die Profibuslinie erreicht man die folgende Maske aus der man die S7-Subnetz-ID ablesen kann.



Sind diese Angaben alle gefunden und eingetragen, wird nun die Station über TCP/IP und *Profibus* in den fernen PC geladen. Nun kann auch diese Slave –Station über TCP/IP bedient, gewartet und beobachtet werden, als wenn der PC direkt am Bus der Anlage angeschlossen wäre.

Es werden nur die ausführbaren Bausteine aus der CPU hochgeladen. Die Symboltabelle steht z.B. nicht zur Verfügung. Es empfiehlt sich daher das Projekt direkt an der Anlage zu archivieren und dem Betreiber der Fernwartung per Mail zuzustellen. Die Archivierung kann auch bei CPU s mit FLASH ROM direkt in der CPU erfolgen, wenn die FLASH ROM Kapazität ausreicht. Dann kann das Projekt mit dem Menübefehl „Projekt auf Memory Card speichern“ archiviert und mit dem Menübefehl „Projekt aus Memory Card holen“ dearchiviert werden. Dies funktioniert auch bei Fernwartung.

OPC-Kommunikation

Herstellerübergreifende Kommunikation in der Automatisierungstechnik

Voraussetzungen in Raum 4.1.06 oder 4.1.08:

- SIMATIK ProTool/Pro CS V6.0 + ServicePack 1a
- SIMATIK ProTool/Pro RT V6.0 + ServicePack 1a
- Steuerung z.B. S7 300 *CPU314C-2 DP*
- Programmierung Anwendung für OPC Server Step 7 V5.1 + ServicePack 4
- Booten des PC mit Administratorrechten
- DCOM Einstellungen lt. ProTool Handbuch vornehmen
- DCOM Einstellungen über Windows Aufruf „Ausführen / Öffnen : DCOMCNFG.EXE“ einstellbar.

OPC - Technik Einleitung

OPC ist die Abkürzung für „OLE for Process Control“ und ist eine Technik zur Hersteller unabhängigen Kommunikation zwischen Automatisierungsgeräten. Die eigentliche OPC Kommunikation basiert auf Windows NT Systemen und DCOM und kann mit TCP/IP auch über ein Netzwerk stattfinden. Die OPC - Technik benutzt eine Server – Client Struktur, wobei mehrere Clients sich mit einem Server verbinden können. Der Server wird normalerweise vom Hersteller des Automatisierungsgerätes zur Verfügung gestellt und spricht das Gerät über die Herstellerabhängige Kommunikation an. Der Server stellt dann Messwerte, Ein- und Ausgänge des Gerätes in der standardisierten OPC Schnittstelle zur Verfügung, welche dann von jedem OPC - Client aus angesprochen werden kann.

Diese Clients können alles Mögliche im Bereich der Automatisierung sein, z.B. SCADA - Systeme (Supervisory Control and Data Acquisition) oder andere Automatisierungsgeräte.

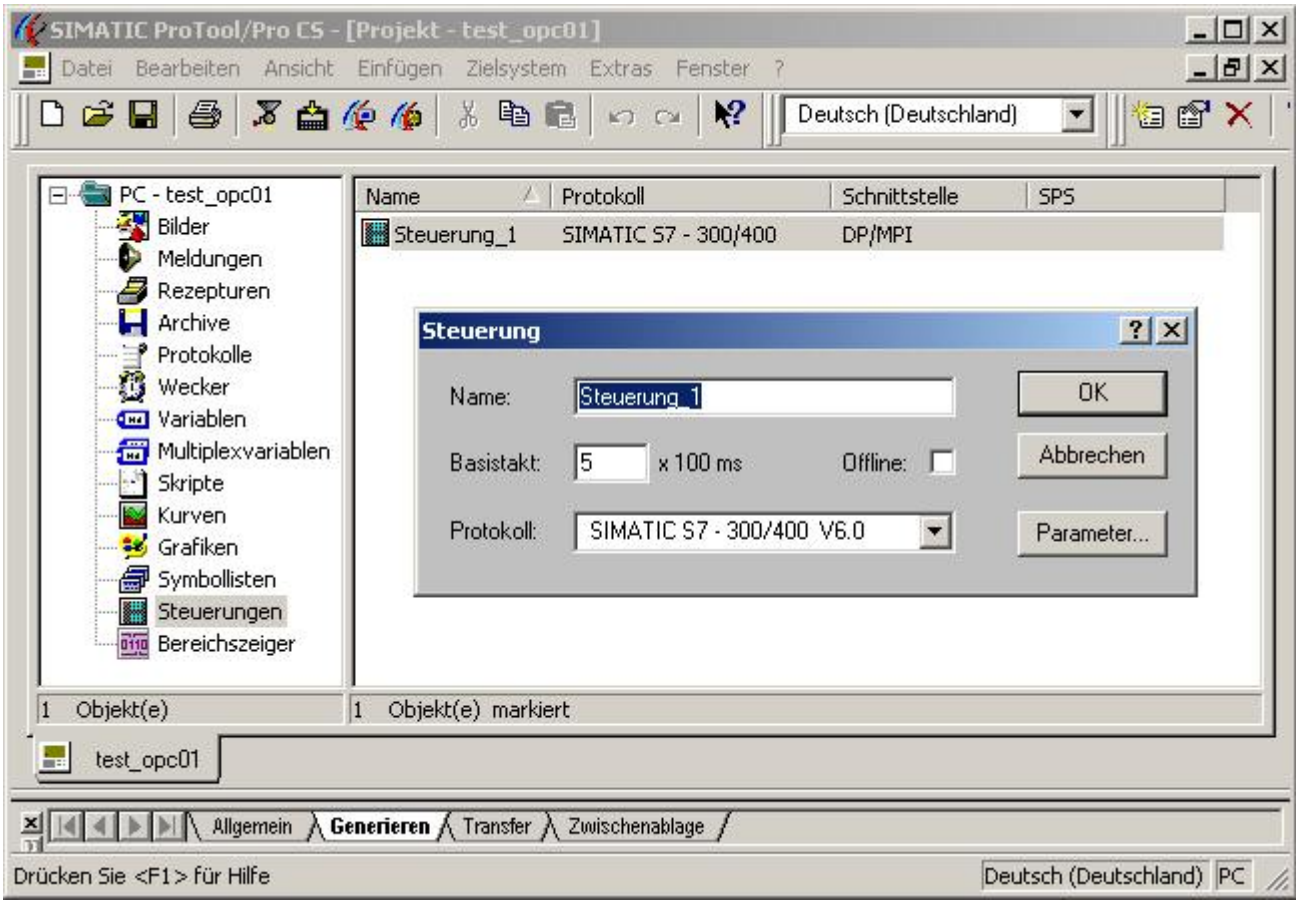
OPC - Server für S7 *SPS*

Es gibt mehrere OPC - Server für S7 300 *SPS*. Im Labor 4.1.06 stehen meistens vier zur Verfügung:

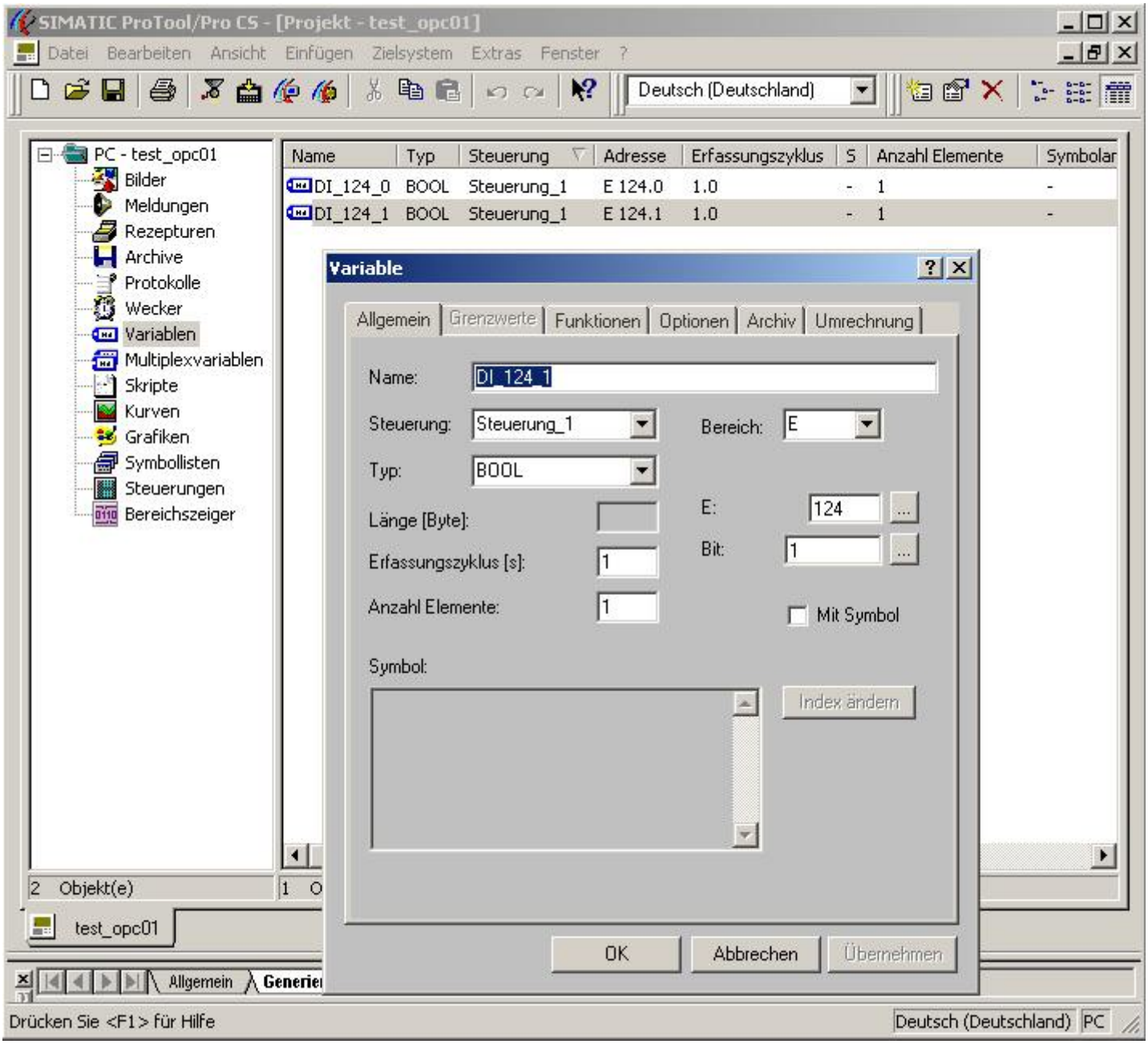
OPC.SimaticHMI.PTPro	ist der OPC – Server von ProTool
OPC.SimaticNET	ist der OPC – Server von SimaticNet
OPC.SimaticNET.DP	ist der OPC – Server von SimaticNet *Profibus*
OPCServer.WinCC	ist der OPC – Server von WinCC

Eine Möglichkeit einen OPC - Server für S7 *SPS* in Betrieb zu nehmen ist die Verwendung der Software ProTool von *Siemens*. ProTool stellt nicht nur die Visualisierung und Bedienung zur Verfügung, sondern kann die unter ProTool definierten und mit der *SPS* verbundenen Variablen auch als OPC - Server für Clients zur Verfügung stellen.

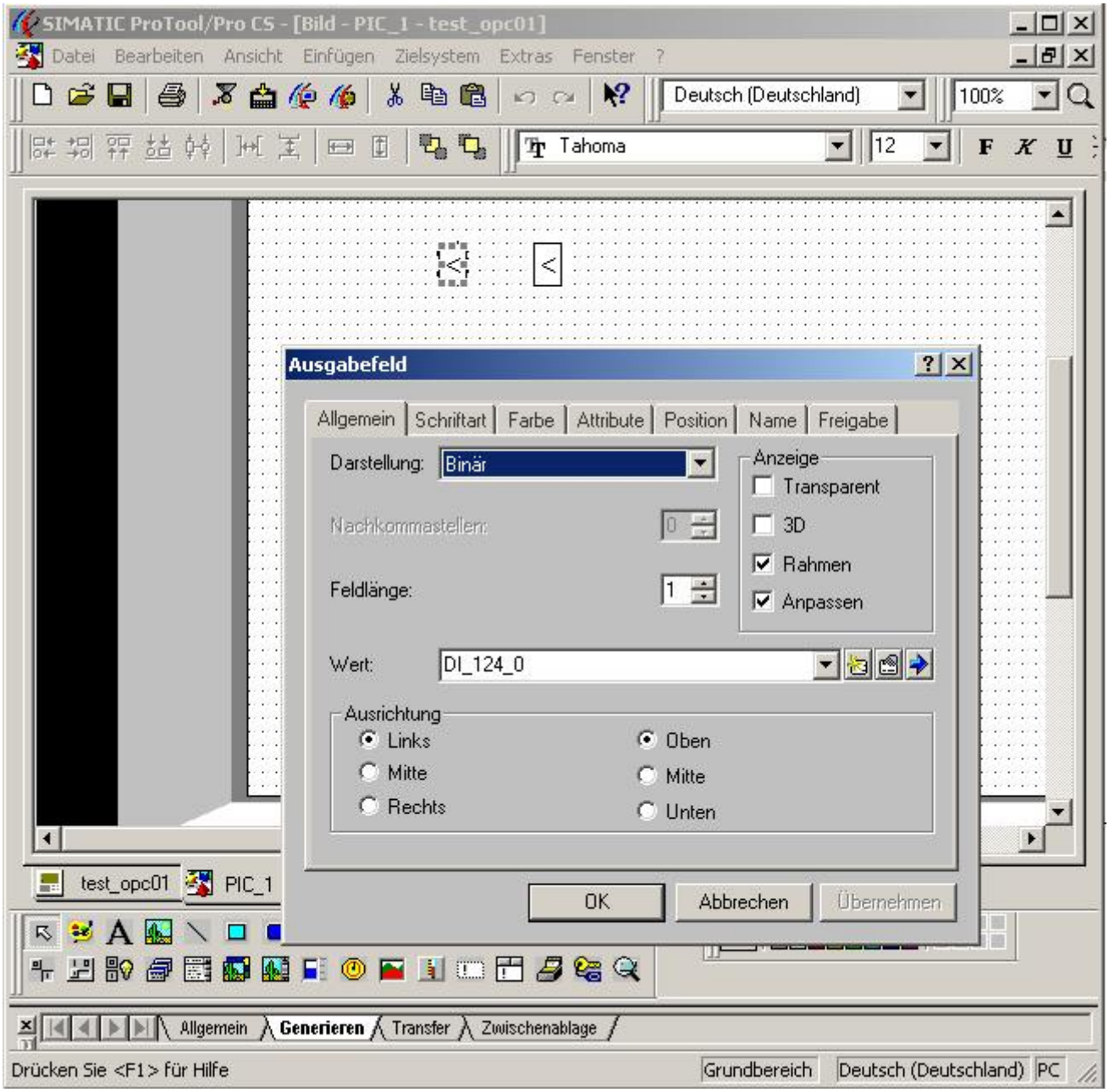
Zunächst muss eine Verbindung zwischen ProTool und der *SPS* hergestellt werden, dazu wird in einem neuen ProTool - Projekt eine Steuerung eingefügt. Und über das Protokoll *Simatic S7* – 300/400 V6.0 mit der *SPS* verbunden.



Nun müssen die Variablen in ProTool definiert werden, die später über OPC beobachtet werden sollen. In diesem Beispiel einfach die beiden ersten Bits des Eingangsbyts 124.

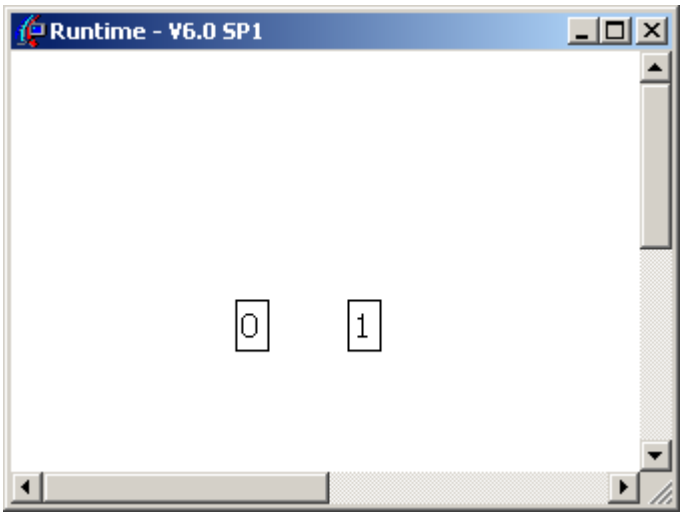


Da ProTool eine Visualisierungssoftware ist, ist für den Start der Runtime und damit des OPC-Serves noch ein Bild notwendig, in dem man die Variablen auch noch einmal visualisieren kann.



Damit ProTool neben seiner normalen Funktion auch als OPC - Server arbeitet, muss lediglich unter Zielsystem – Einstellungen das Häkchen für OPC - Server aktiviert werden.

Nun muss nur noch die Runtime über „Datei – Testen –Runtime starten“ gestartet werden und wenn die Visualisierung der beiden Eingangsbits funktioniert, dann werden die Variablen auch über OPC zu erreichen sein.



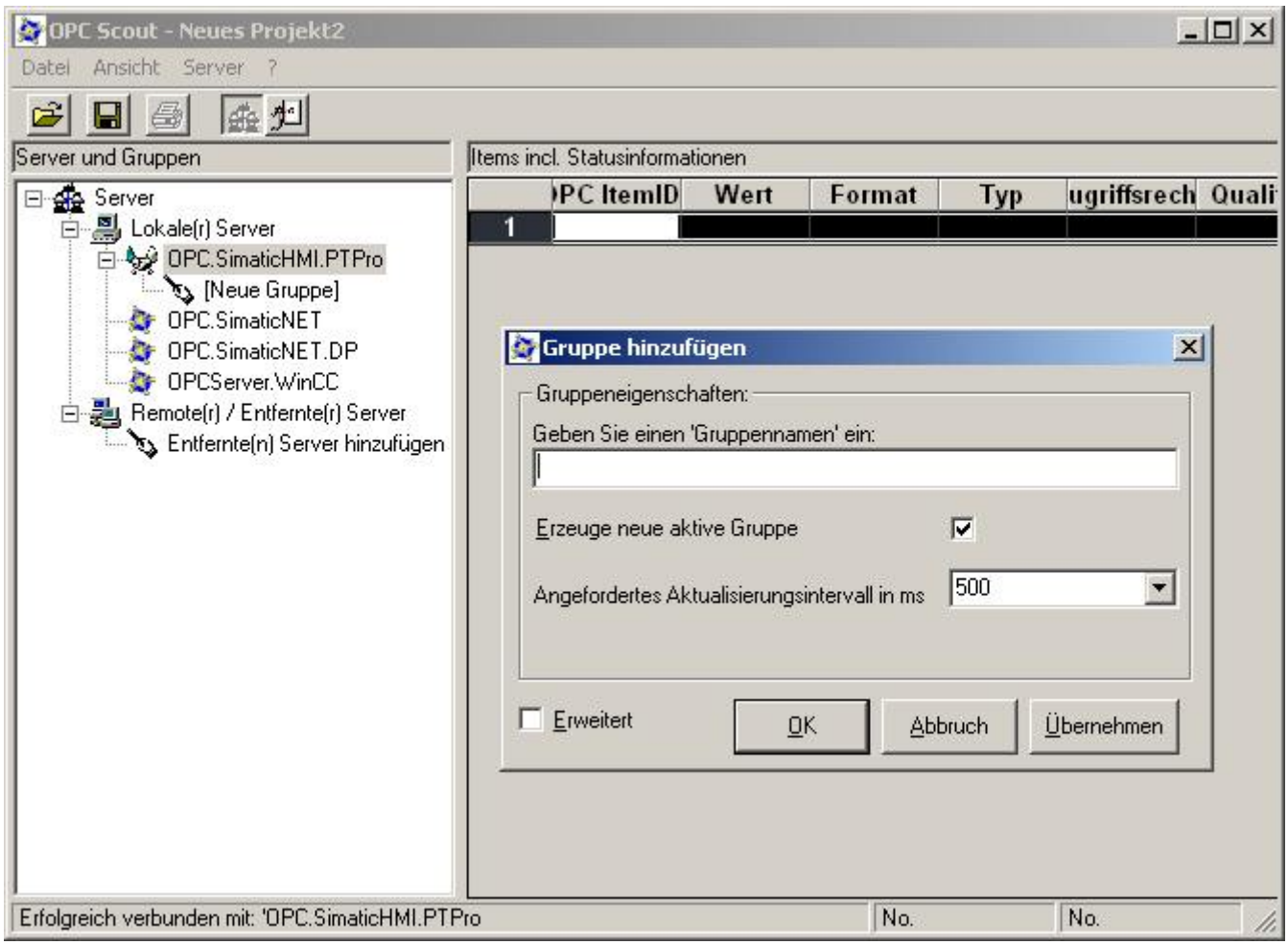
OPC Scout als lokaler OPC Client

Voraussetzungen in Raum 4.1.06 oder 4.1.08:

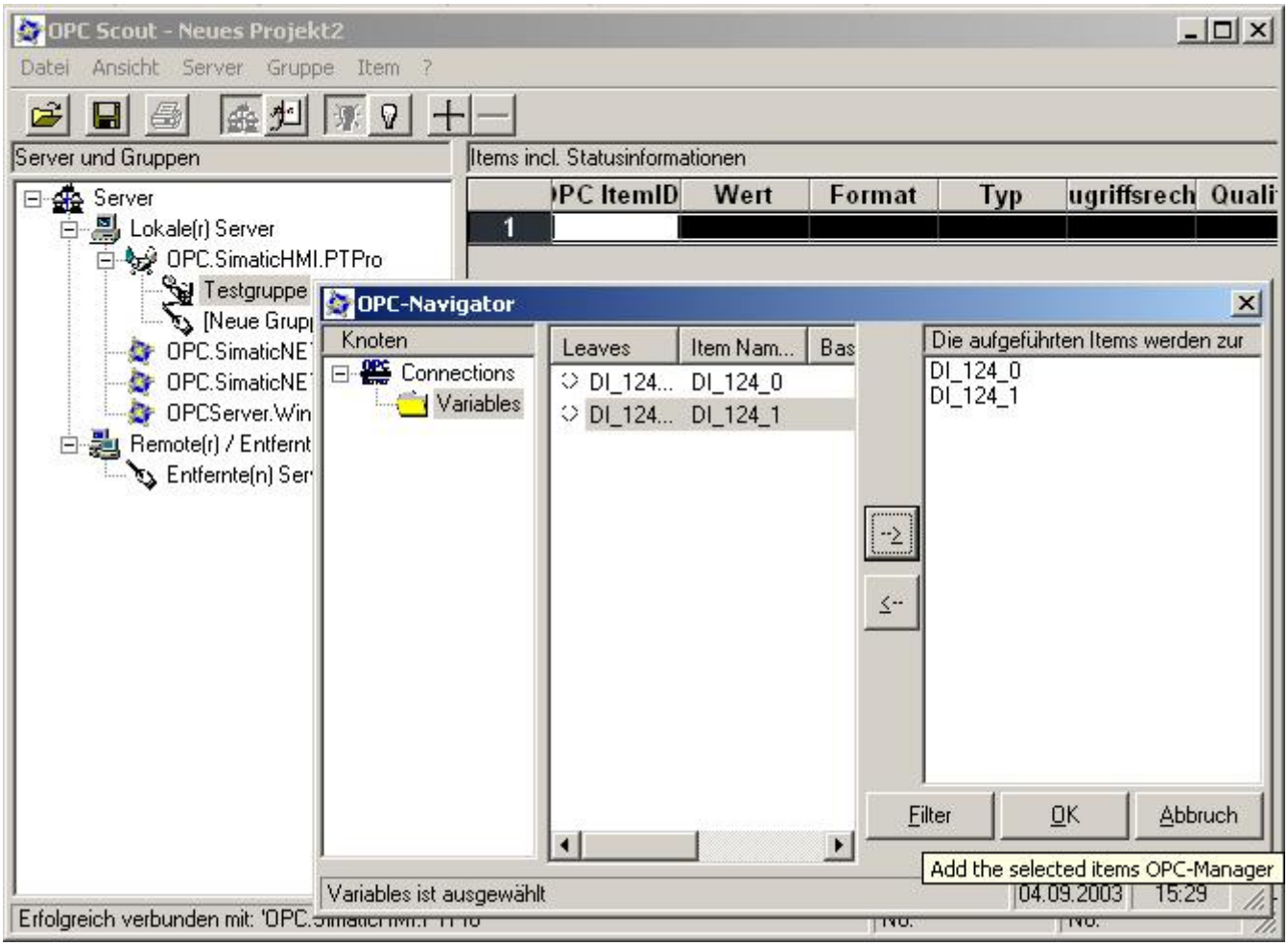
SimaticNET PC Software V6.0 für den OPC Scout

Als OPC - Client kommt das *Siemens* OPC – Analyse -Tool „OPC Scout“ zum Einsatz (Start – Simatic - SIMATIC NET - Industrial *Ethernet* - PROFInet OPC Server – OPC Scout).
Zunächst kann man die Funktion des OPC - Servers lokal überprüfen, bevor man versucht den Server über TCP/IP von einem anderen Rechner aus zu erreichen. Wenn der OPC Scout gestartet ist, dann zeigt er links auch schon die lokal zur Verfügung stehenden OPC - Server an. Der OPC - Server von

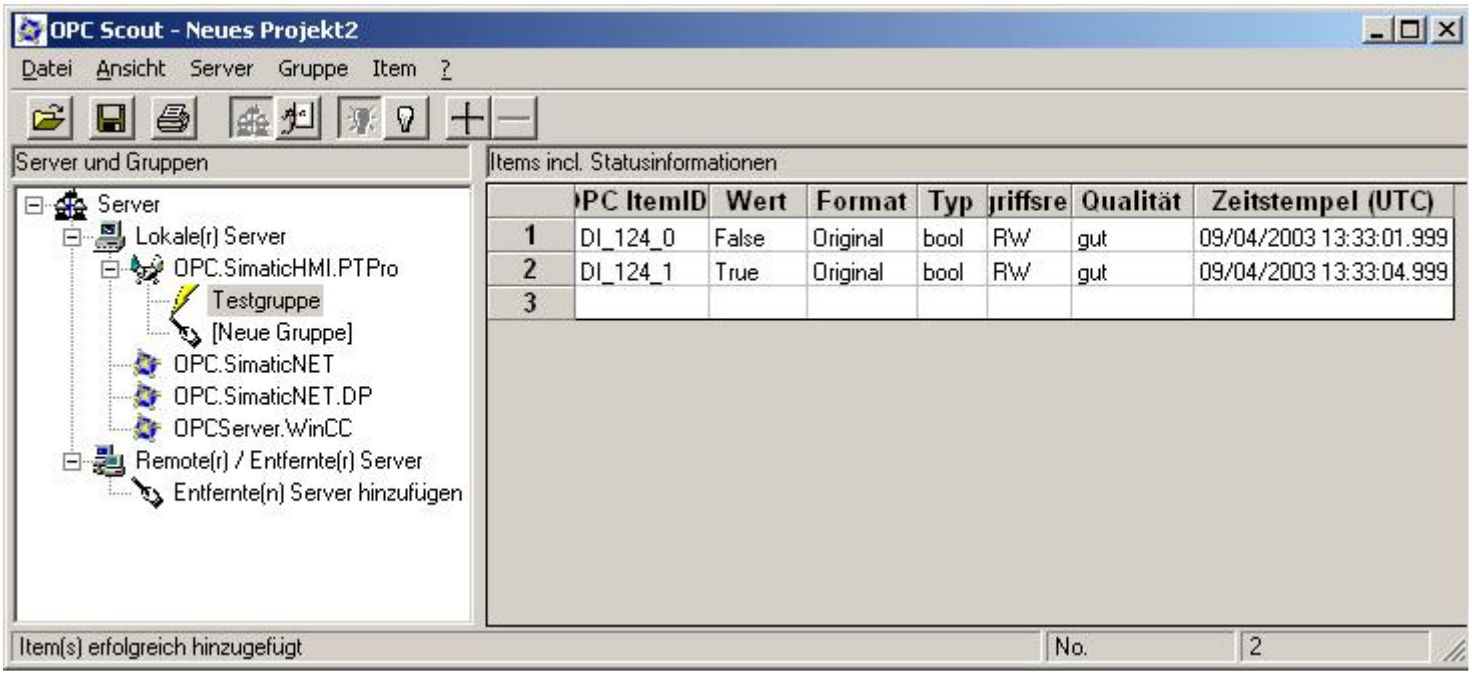
ProTool heißt „OPC.SimaticHMI.PTPro“. Durch Doppelklick kann OPC Scout sich mit diesem Server Verbinden, worauf bei erfolgreicher Verbindungsaufnahme die Aufforderung erscheint einen Gruppennamen anzugeben. Hier kann zu Testzwecken jeder beliebige Name eingegeben werden, z.B. „Testgruppe“.



Durch Doppelklick auf diese Testgruppe öffnet sich nun der OPC - Navigator mit dem die Variablen, die von ProTool zur Verfügung gestellt werden, als sogenannte Items in die Testgruppe eingefügt werden.



Als dann zeigt OPC Scout die beiden Items, die ja die mit der *SPS* verbundenen Variablen unter ProTool abbilden, mit den OPC - typischen Zusatzparametern an.



Hinweis zu Benutzerrechten im Netzwerk

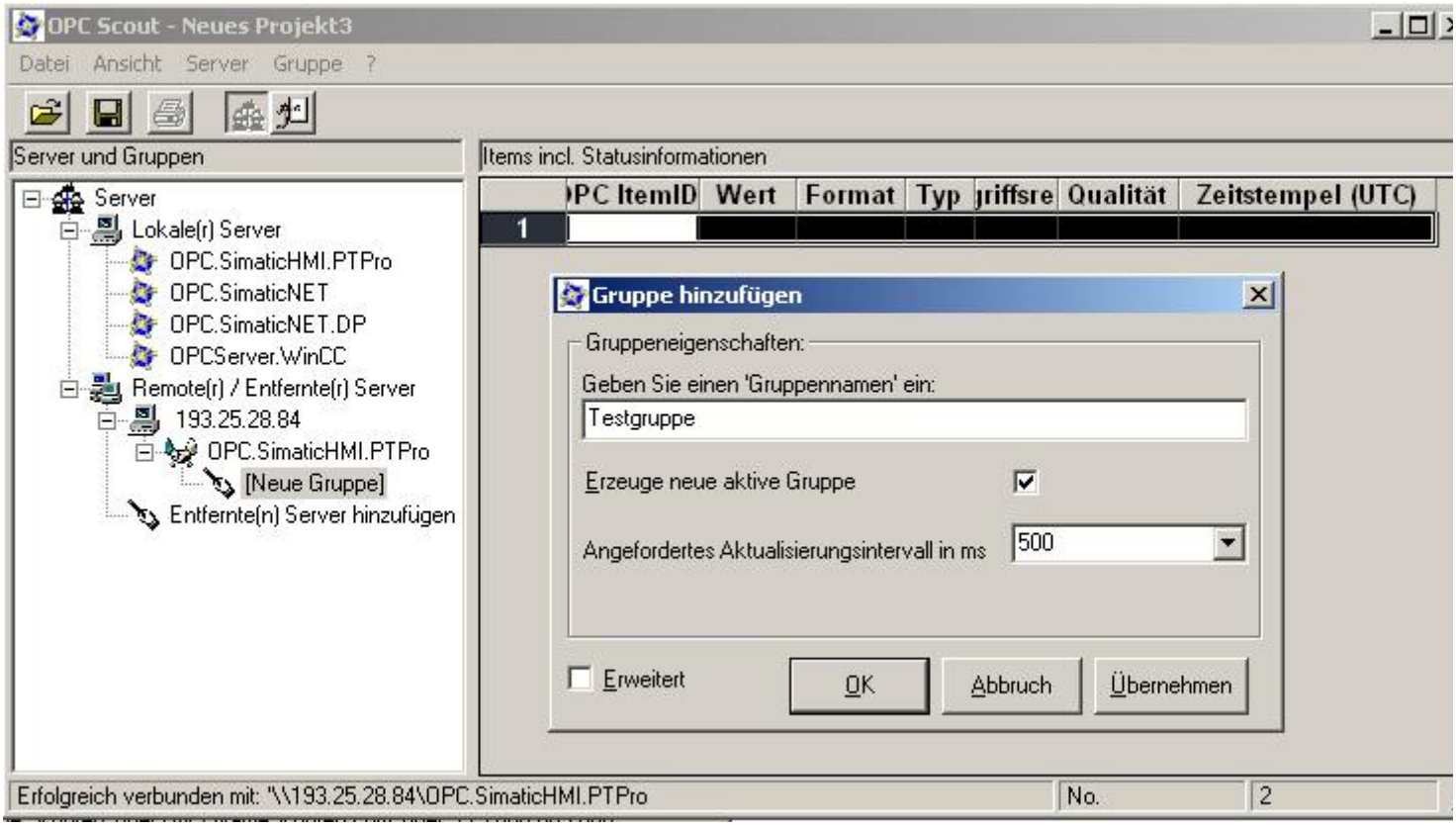
Die Nachstehende Vorgehensweise funktioniert unter Umständen nur, wenn man als Administrator an die Windows-Systeme angemeldet ist, die an dem OPC - Test beteiligt sind.

OPC Scout als remote OPC Client der über Netzwerk auf den Server zugreift

Die Vorgehensweise unterscheidet sich lediglich in dem Verbindungsaufbau mit dem Server, da dieser jetzt über „Remote / Entfernte Server“ verbunden wird. Dazu benötigt man die IP-Adresse oder den Netzwerkname des Windows Systems, auf dem der Server läuft, in diesem Beispiel 193.25.28.84.

Durch Doppelklick auf „Entfernte Server hinzufügen“ öffnet sich der Dialog in dem man den Knotennamen (also den Rechner auf dem der Server Läuft) und den OPC - Server benennen kann.

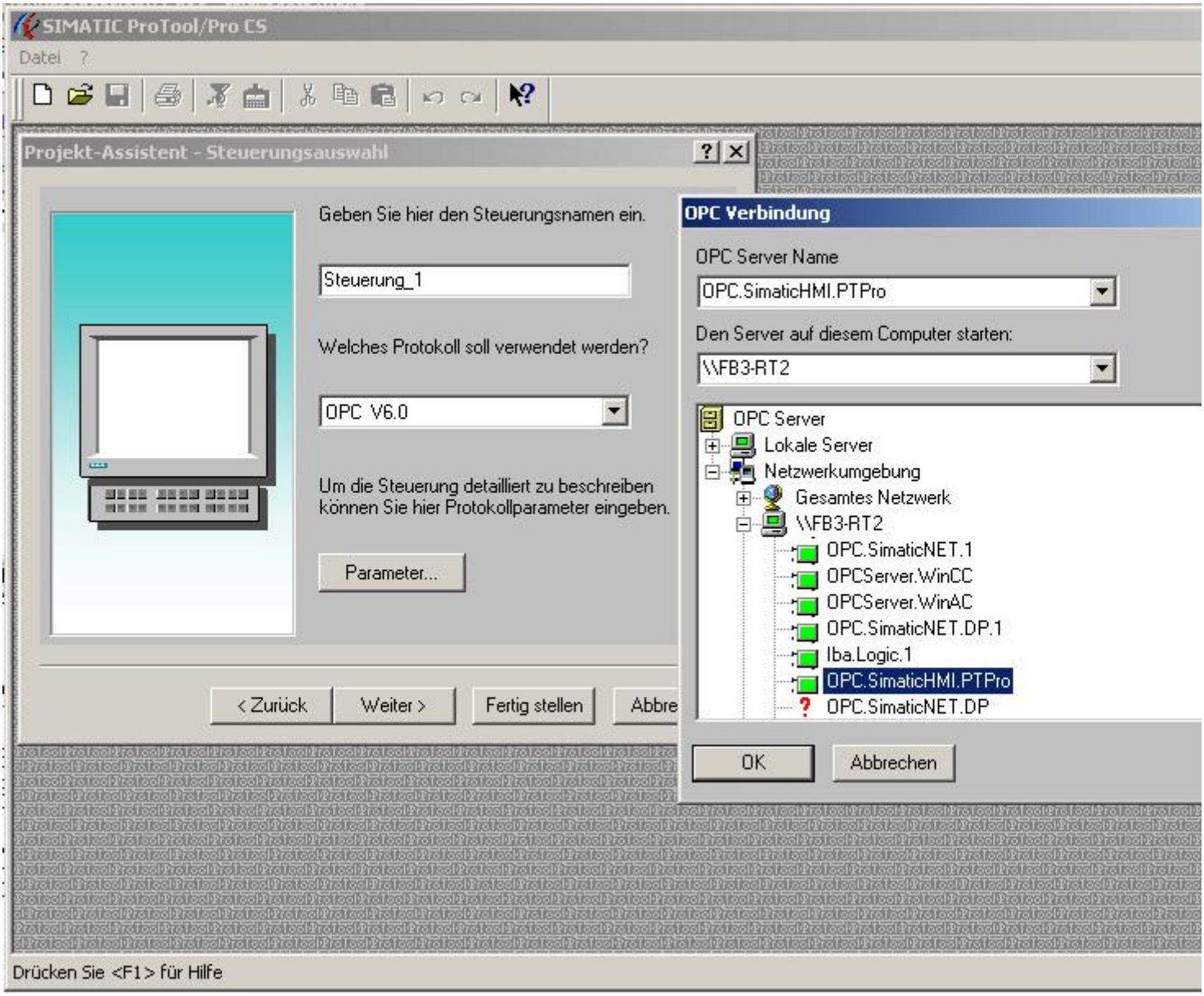
Nun kann man sich wie zuvor beschrieben mit dem OPC - Server durch Doppelklick verbinden und die Gruppe und Items einfügen und beobachten.



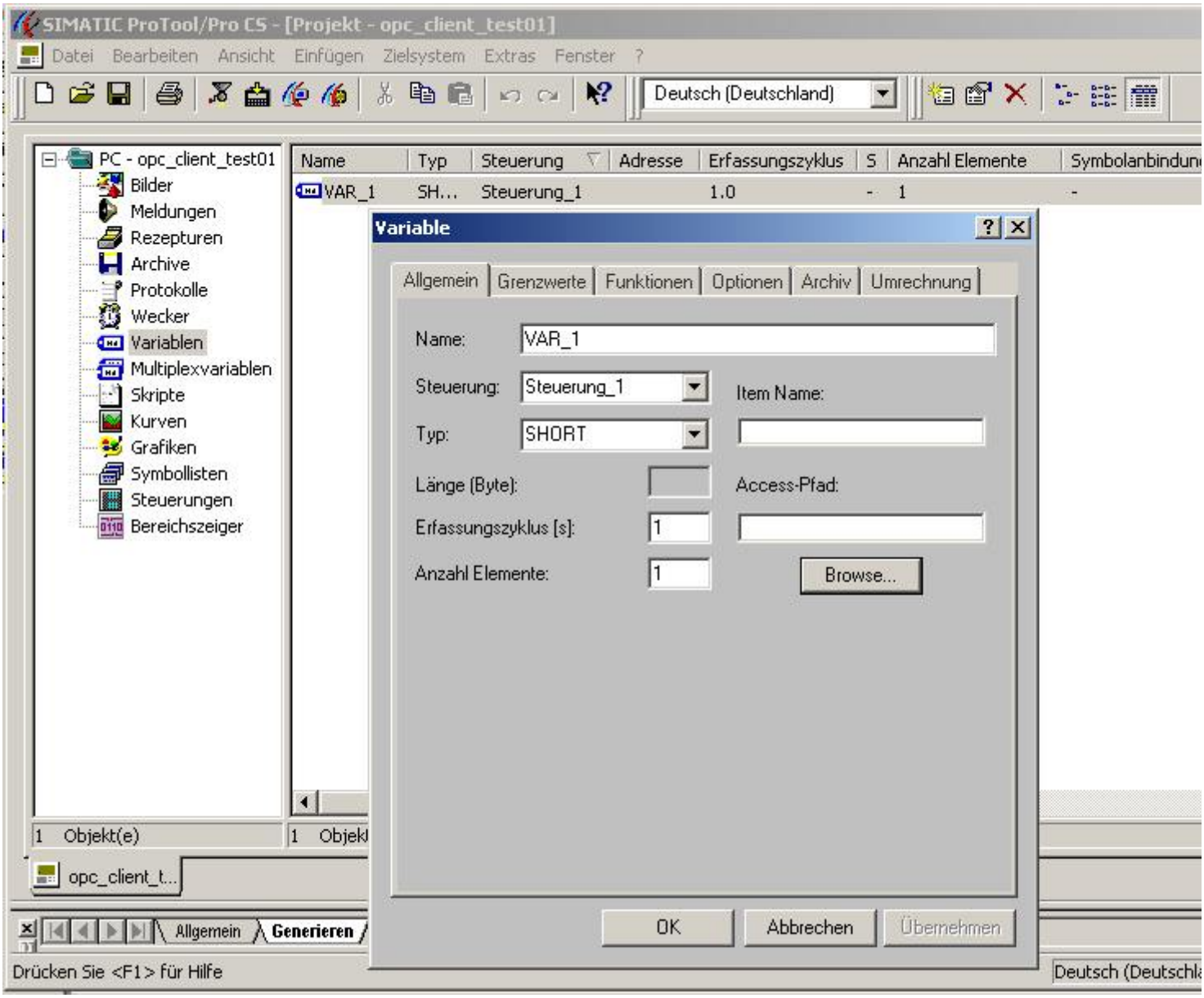
ProTool als OPC – Client

Eine etwas leistungsfähigere und komfortablere Variante eines OPC – Client stellt wiederum ProTool selbst dar. D.h. ProTool kann nicht nur Server sein, sondern auch auf OPC - Server zugreifen, wie hier wird nun in einem kleinen Beispiel gezeigt wird.

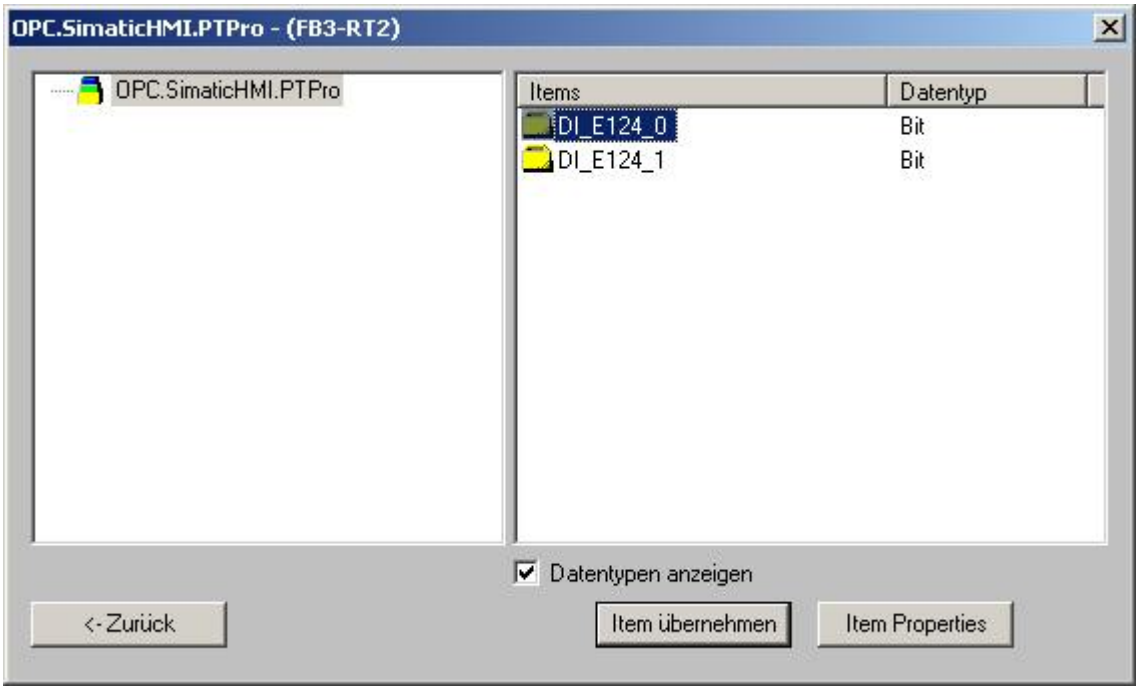
Anlegen eines neuen ProTool Projektes und einfügen einer neuen Steuerung. Wichtig ist nun die Auswahl des Steuerungsprotokolls OPC V6.0. Durch klick auf Parameter kann man nun den gewünschten OPC – Server auswählen.



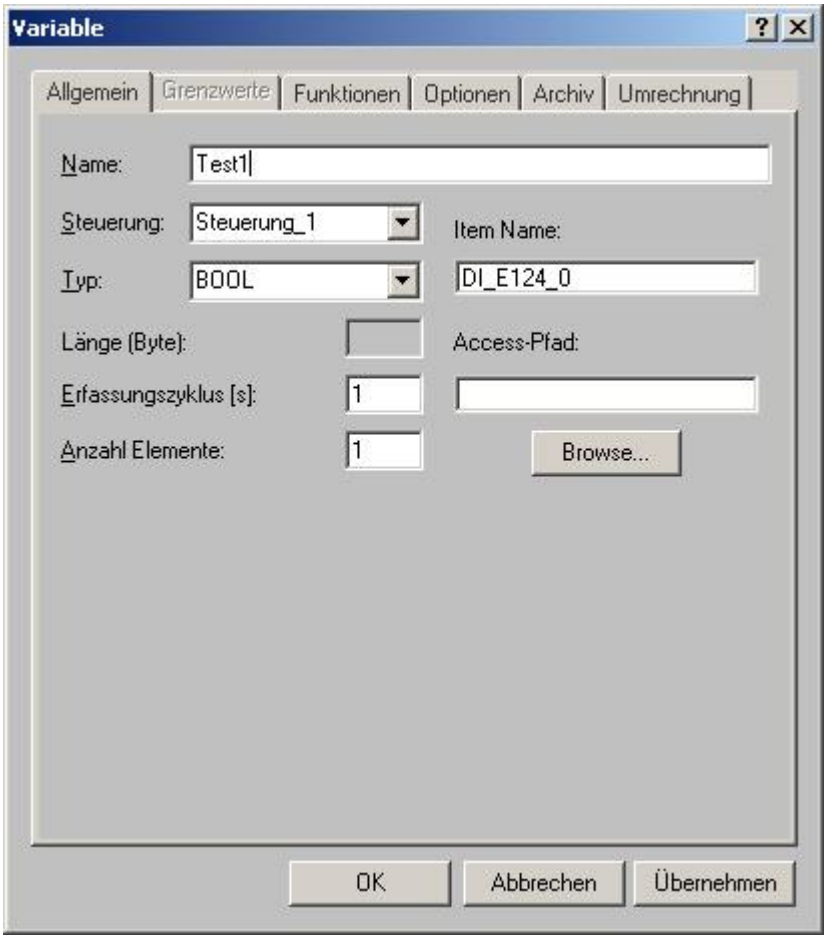
Nach der Auswahl des OPC – Servers (Klick auf OK und Fertigstellen) können nun die Variablen eingerichtet werden, welche auf die Items des OPC – Servers zugreifen.



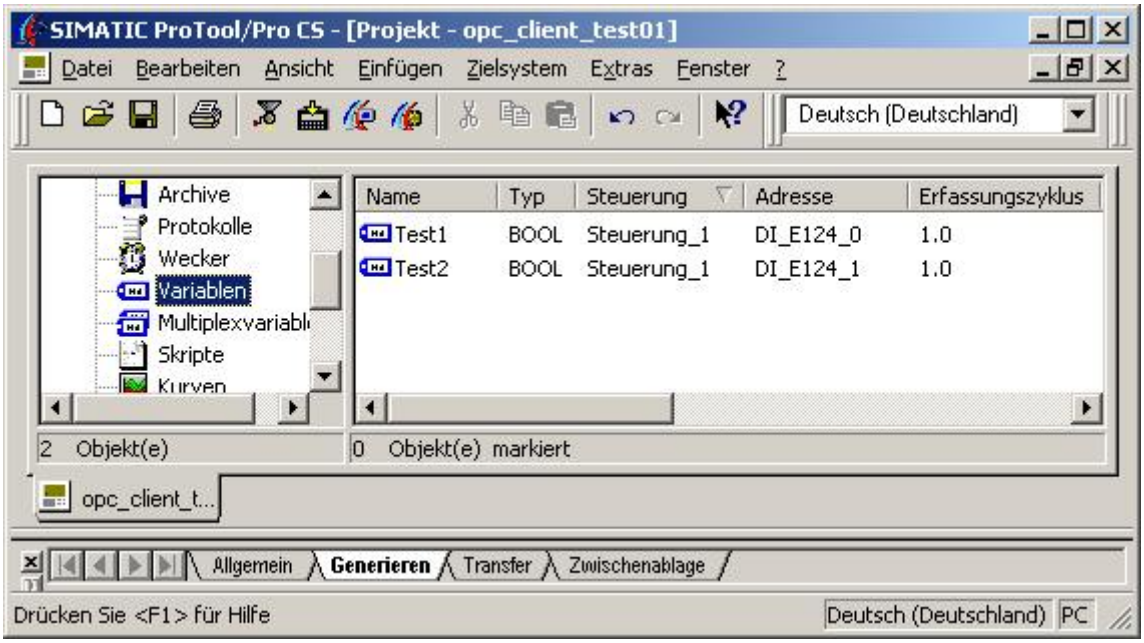
Durch Klick auf Browse kann man ein Item für die Variable auswählen, und somit die Maske automatisch verfollständigen.

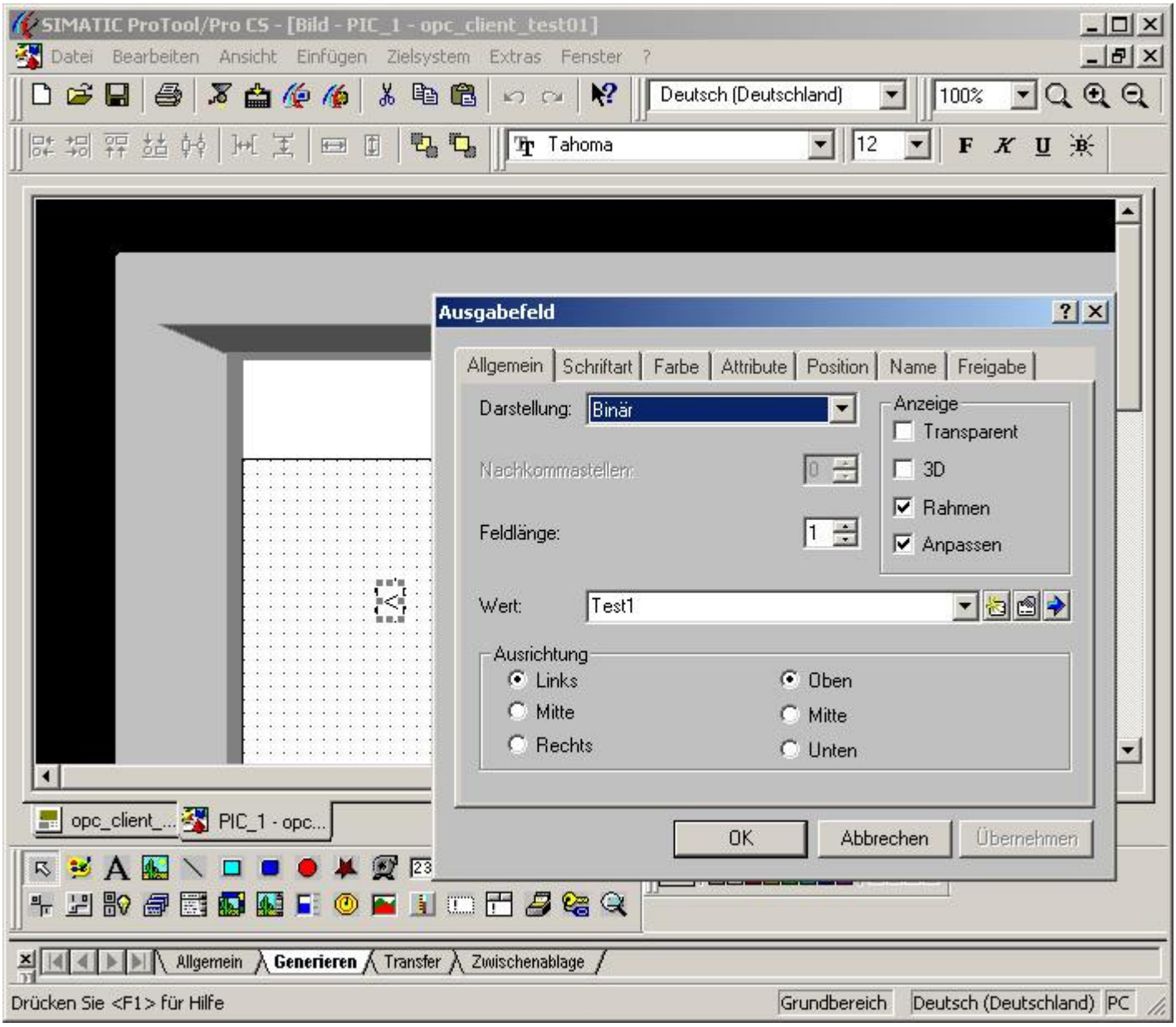


Nach Item übernehmen sieht die Variablen Maske so aus:



Der Name ist natürlich frei zu vergeben.
Diese Variablen sind nun wieder wie gewohnt unter ProTool in einem Bild zu Visualisieren.


SIMATIC ProTool/Pro CS - [Projekt - opc_client_test01]
Datei Bearbeiten Ansicht Einfügen Zielsystem Extras Fenster ?
Deutsch (Deutschland)
Archive
Protokolle
Wecker
Variablen
Multiplexvariabl
Skripte
Kurven
Name Typ Steuerung Adresse Erfassungszyklus
Test1 BOOL Steuerung_1 DI_E124_0 1.0
Test2 BOOL Steuerung_1 DI_E124_1 1.0
2 Objekt(e)
0 Objekt(e) markiert
opc_client_t...
Allgemein Generieren Transfer Zwischenablage
Drücken Sie <F1> für Hilfe
Deutsch (Deutschland) PC


SIMATIC ProTool/Pro CS - [Bild - PIC_1 - opc_client_test01]
Datei Bearbeiten Ansicht Einfügen Zielsystem Extras Fenster ?
Deutsch (Deutschland)
100%
Tahoma
12
Ausgabefeld
Allgemein Schriftart Farbe Attribute Position Name Freigabe
Darstellung: Binär
Nachkommastellen: 0
Feldlänge: 1
Anzeige
Transparent
3D
Rahmen
Anpassen
Wert: Test1
Ausrichtung
Links
Mitte
Rechts
Oben
Mitte
Unten
OK
Abbrechen
Übernehmen
opc_client_...
PIC_1 - opc...
Allgemein Generieren Transfer Zwischenablage
Drücken Sie <F1> für Hilfe
Grundbereich
Deutsch (Deutschland) PC

Nun muss nur noch die Runtime über „Datei – Testen –Runtime starten“ gestartet werden.