NetToPLCsim - Netzwerkerweiterung für Plcsim

Thomas Wiens

18. April 2017

NetToPLCsim - Netzwerkerweiterung für Plcsim
von Thomas Wiens

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Was kann NetToPLCsim?

NetToPLCsim ermöglicht es, die Funktionen der SPS-Simulation S7-Plcsim über die Netzwerkschnittstelle des PCs auf dem die Simulation läuft zu nutzen. Dadurch lässt sich beispielsweise eine Visualisierungsanwendung im Büro zusammen mit Plcsim vollständig testen, ohne dazu die echte SPS verfügbar haben zu müssen.

NetToPLCsim unterstützt dabei weitestgehend die Funktionen die auch durch S7-Plcsim unterstützt werden, wie:

- Variablendienste: D.h. Lesen und Schreiben von SPS-Speicherbereichen
- Bausteindienste: Programme hochladen, Bausteine beobachten
- Bausteinbezogene Meldungen mit Alarm_S, Alarm_D, Alarm_8
- Unterstützung von mehreren Plcsim Instanzen

1.2 Was kann NetToPLCsim nicht?

Folgende Funktionen sind bekannterweise mit NetToPLCsim nicht möglich:

- Alle Netzwerkfunktionen die aus dem Programm aufgerufen werden (über sog. T-Bausteine wie TCON, TSEND, usw.) oder über NetPro projektierte Verbindungen stehen auch über NetToPLCsim nicht zur Verfügung
- Es werden andere System-Zustandslisten (SZL) als bei einer realen S7 unterstützt, die enthaltenen Werte unterscheiden sich von denen einer echten CPU
- Programmierfunktionen über das TIA-Portal zu einer S7-300/400 Simulation sind mit NetToPLCsim nicht möglich, da das TIA-Portal beim Verbindungsaufbau die Kompatibilität der Partnerstation prüft. Meldet diese nicht kompatible Daten (in diesem Fall eine S7-Simulation) so verweigert das TIA-Portal den Verbindungsaufbau. Step7 V5.x ist in dieser Hinsicht toleranter.
- Über die Funktion "Erreichbare Teilnehmer" in Step 7 ist die Plcsim/NetToPLCsim CPU nicht sichtbar. Diese Funktion läuft über das sog. LLDP-Protokoll auf MAC-Ebene. Auf einem PC mit installierter Simatic-Software wird sich der PC immer als "PC-Station" melden.
- Des Weiteren existieren geringfügige Unterschiede im Kommunikationsverhalten zwischen einer echten S7-CPU und S7-Plcsim/NetToPLCsim.

WICHTIG

Ein Test mit NetToPLCsim ersetzt nicht den Test des Systems an der realen CPU.

1.3 Wie funktioniert NetToPLCsim?

Die ersten Versionen von NetToPLCsim (bis einschließlich V0.7.2) verwendeten die offizielle Schnittstelle zu Plcsim, welche in Form des S7ProSim-COM-Objekt für andere Anwendungen zur Verfügung gestellt wurde. Bei diesen Versionen wurden Teile des S7-Protokolls in NetToPLCsim verarbeitet, und die Daten über die S7ProSim-Schnittstelle aus Plcsim gelesen, bzw. geschrieben. Dadurch waren ausschließlich Variablendienste möglich. Ein weiterer Nachteil der S7ProSim-Schnittstelle ist der äußerst bescheidene Datendurchsatz.

Bei Plcsim für die 1200/1500 ist die S7ProSim-Schnittstelle komplett entfallen. Darum verwenden alle folgenden Versionen die sogenannte S7online-Schnittstelle.

1.4 S7online-Schnittstelle

Die S7online-Schnittstelle stellt im OSI-Modell die Schichten 1 bis 4 für alle Anwendungen im Simatic-Universum zur Verfügung. Kommuniziert eine Simatic-Anwendung mit einer SPS, so geschieht dies immer über die S7online-Schnittstelle. Die Funktionen der S7online-Schnittstelle sind über die Programmbibliothek s7onlinx.dll im Windows-Systemverzeichnis ansprechbar.

Die S7online-Schnittstelle reicht die Daten an die unterlagerten Transportprotokolle wie TCP/IP, MPI oder Profibus weiter. Die Einstellung des von der S7online-Schnittstelle verwendeten Transportprotokolls, wird über die Funktion "PG/PC-Schnittstelle einstellen" vorgenommen. Auch die Kommunikation zu Plcsim läuft über diese Schnittstelle. Auf dieser Schnittstelle wird zur SPS rein im S7-Protokoll "gesprochen". Die Aufgabe von NetToPLCsim besteht darin, dem S7-Protokoll die Transportebenen IP/IsoOnTCP beim Senden hinzuzufügen, bzw. beim Empfang von Daten zu entfernen und in die S7online-Schnittstelle zu übertragen. Die S7online-Schnittstelle ist offiziell nicht dokumentiert, was das Hauptproblem bei der Verwendung dieser Schnittstelle darstellt.

2 Bedienung

2.1 Schnelleinstieg

2.1.1 Plcsim für S7-300/S7-400 (Step 7 V5.5, TIA-Portal)

Im Folgenden eine Kurzfassung um eine einzelne Plcsim Simulation mittels NetToPLCsim erreichbar zu machen. Die Anleitung gilt für Plcsim unter Step7 V5.5, als auch wenn Sie eine S7-300/S7-400 mit dem TIA-Portal verwenden.

1. Starten Sie den Simatic Manager
2. Öffnen Sie ihr zu testendes Projekt
3. Starten Sie Plcsim, und laden Sie ihr Projekt inkl. Hardwarekonfiguration in Plcsim. Vorraussetzung für die Anbindung an NetToPLCsim ist eine in der Hardwarekonfiguration vorhandene Ethernet-Baugruppe (PN-CPU oder Ethernet-CP).
4. Starten Sie NetToPLCsim mit Administratorrechten (diese sind notwendig um einen Siemens-Dienst zu beendigen)
5. Lassen Sie NetToPLCsim den Siemens-Dienst beenden
6. Klicken sie auf die Schaltfläche "Add"
7. Im Stationsdialog klicken Sie neben dem Feld "Network IP Address" auf die Schaltfläche "...". Es werden ihnen die IP-Adressen ihrer Netzwerkkarte(n) angezeigt. Wählen Sie die Adresse aus, unter der Ihre Plcsim später erreichbar sein soll.
8. Klicken Sie neben dem Feld "Plcsim IP Address" auf die Schaltfläche "...". Ihre Simulations-Baugruppe sollte dort erreichbar sein. Übernehmen Sie die Baugruppe die sie über NetToPLCsim erreichbar machen möchten
9. Stellen Sie Rack/Slot 0/2 ein (oder bei S7-400 je nach Hardwarekonfiguration)
10. Schließen Sie den Dialog mit OK
11. Klicken Sie im Hauptfenster auf "Start Server"
12. Ihre Plcsim Simulation ist nun unter der bei "Network IP Address" angezeigten IP-Adresse erreichbar

2.1.2 Plcsim für S7-1200/S7-1500 (TIA-Portal)

Als Vorraussetzung für den Betrieb mit TIA-Plcsim für die S7-1200/S7-1500 muss die PG/PC-Schnittstelle korrekt eingestellt sein. Starten Sie dazu in der Windows Systemsteuerung das Programm "PG/PC-Schnittstelle einstellen". Im Dialog stellen Sie den Zugangspunkt S7ONLINE auf die Schnittstellenparametrierung "PLCSIM S7-1200/S7-1500(TCP/IP)" ein.

Bei TIA Portal Version V14 ist die Schnittstellenparametrierung "PLCSIM.TCPIP.1" einzustellen.

2.2 Bedienung allgemein

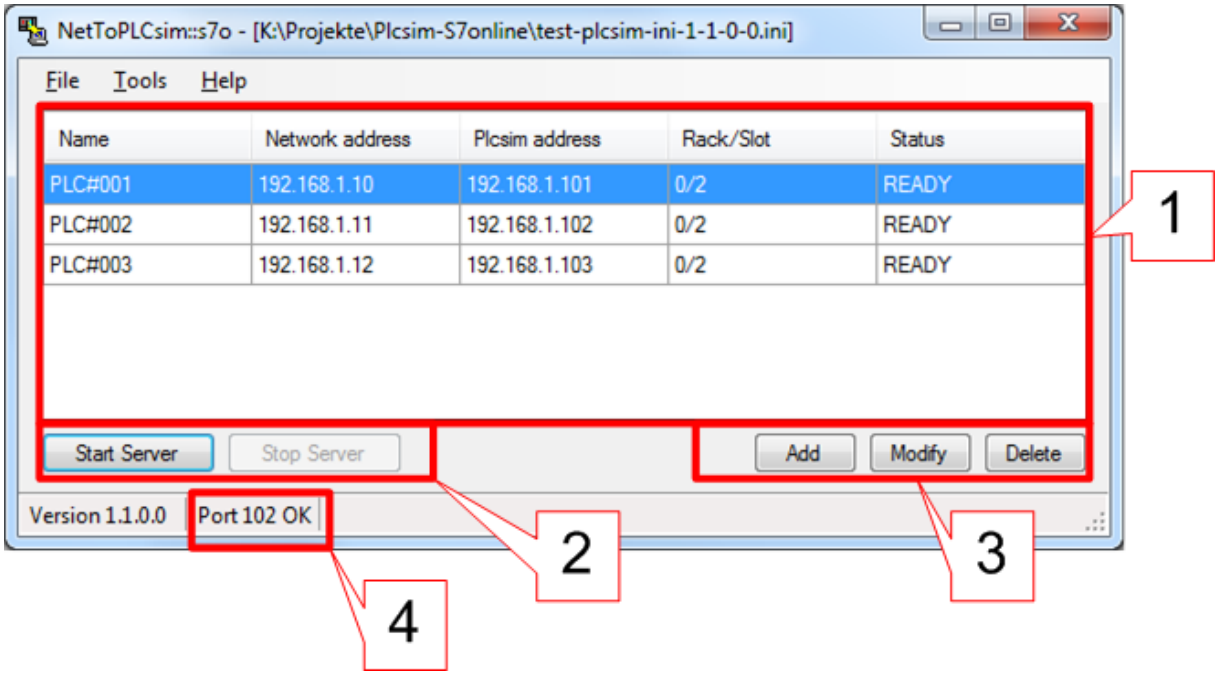
2.2.1 Vorraussetzungen

Sie benötigen Step 7 Plcsim mit mindestens Version V5.4, oder Plcsim für TIA-Portal.

Um diese Version von NetToPLCsim zu verwenden, muss in der Plcsim-Simulation zwingend eine Ethernet-Schnittstelle (CP oder PN-CPU) in der Hardware-Konfiguration vorhanden sein.

2.2.2 Hauptfenster

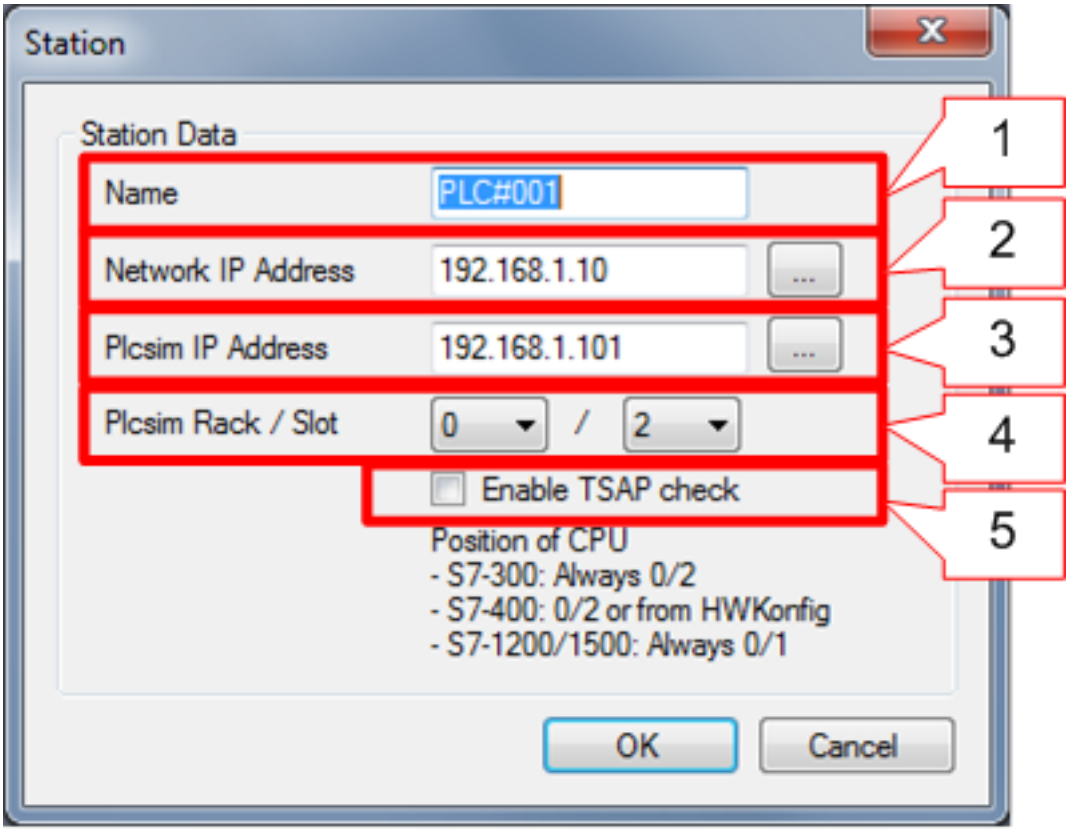
Abbildung 1 NetToPLCsim Hauptfenster



1. Anzeigebereich mit den konfigurierten Stationen
2. Schaltflächen um die Server für die konfigurierten Stationen zu starten und zu stoppen
3. Schaltflächen um eine neue Station hinzuzufügen, zu bearbeiten oder zu löschen
4. Status der Port-Überprüfung bei Programmstart. Funktion von NetToPLCsim ist nur bei OK gegeben.

2.2.3 Stationsdialog

Abbildung 2 NetToPLCsim Stationsdialog



1. Eindeutiger Name
2. IP-Adresse der Netzwerkschnittstelle unter der dieser Server erreichbar sein soll
3. IP-Adresse der Plcsim-CPU
4. Rack/Slot Position der CPU. Die Einstellung ist nur für den optionalen TSAP-Check relevant. Ist diese Option gesetzt, so muss auf Clientseite als TSAP die korrekte Rack/Slot Kombination eingestellt sein damit auf ISO-On-TCP-Ebene eine Verbindung zustandekommt (für Experten: es wird dann eine Verbindung über die eingestellte Rack/Slot Kombination und auf den Verbindungsressourcen 1=PG, 2=OP, und 3=Step7Basic angenommen)

2.2.4 Protokollmonitor

Bei gestarteten Servern ist im Kontextmenü (klick mit rechter Maustaste auf eine Station) der Stationsliste der Eintrag "Start monitoring" verfügbar. Es kann für jede Station ein eigenes Monitoring-Fenster geöffnet werden.

Zur Zeit wird nur die S7-Kommunikation für die S7-300/400 unterstützt. Es werden nur ausgewählte Telegramme des S7-Protokolls angezeigt. Aufgeschlüsselt werden nur eingehende Telegramme für Variablendienste (Speicherbereiche lesen und schreiben) sowie SZL-Anfragen.

Über ein Mausklick auf die Statusleiste kann die Ausgabe pausiert und fortgesetzt werden. Die Kommunikation läuft auch bei pausierter Ausgabe weiter.

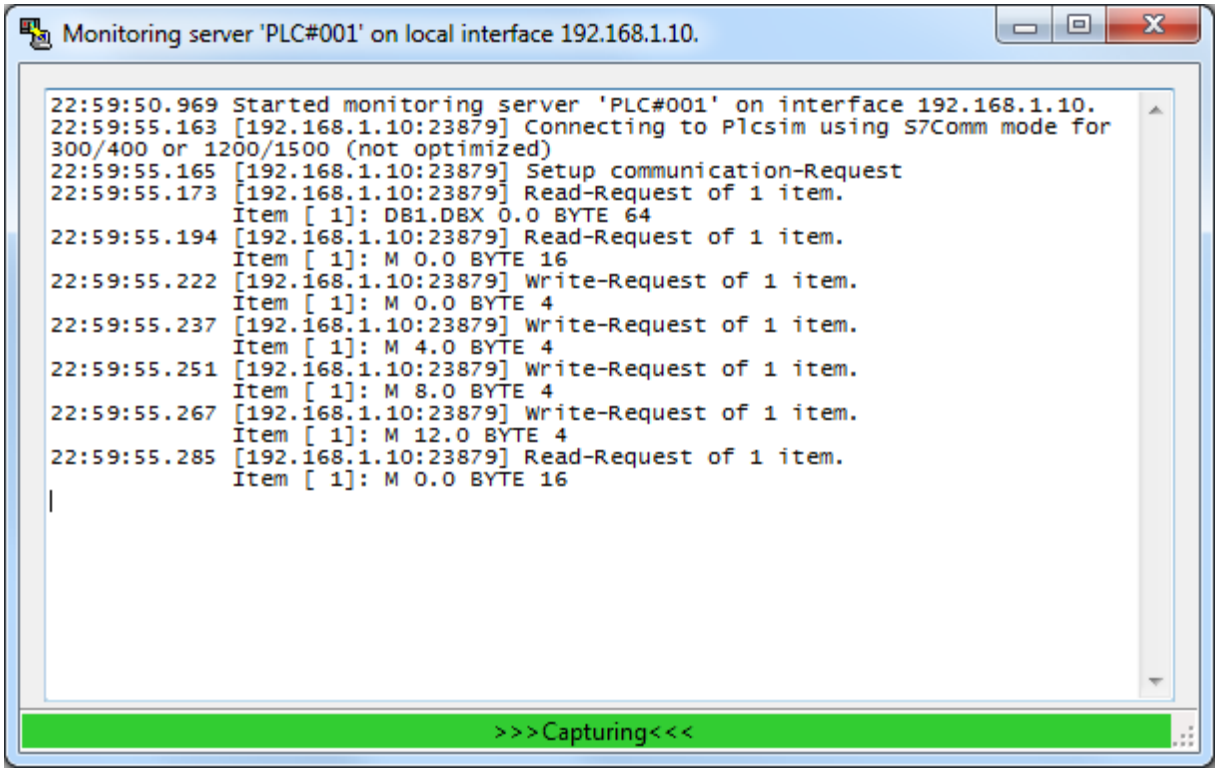
Um sich weitere Details des Datenaustausches anzusehen, bietet sich die Verwendung von Wireshark in Verbindung mit meiner Plugin-dll für die S7-Kommunikation an (ab Wireshark Version 2.0 ist das S7-Protokoll direkt integriert).

http://sourceforge.net/projects/s7commwireshark

ANMERKUNG

Durch das aktivierte Monitoring wird der Datenaustausch erheblich verlangsamt.

Abbildung 3 NetToPLCsim Protokollmonitor



2.2.5 Kommandozeilenparameter

Folgende Kommandozeilenparameter sind verfügbar:

Tabelle 1 Kommandozeilenparameter

Option	Beschreibung
-f=config.ini	Lädt automatisch die angegebene Datei
-s=Option	Verhalten zur Überprüfung und Autostop des S7DOS Help Service. Optionen: YES=Automatisch stoppen, NO=Nicht stoppen, ASK=abfragen
-autostart	Ist eine Konfigurationsdatei angegeben, werden automatisch die Server für die aktivierten Stationen gestartet

Beispiel:

```
NetToPLCSim.exe -f=testconfig.ini -s=NO -autostart
```

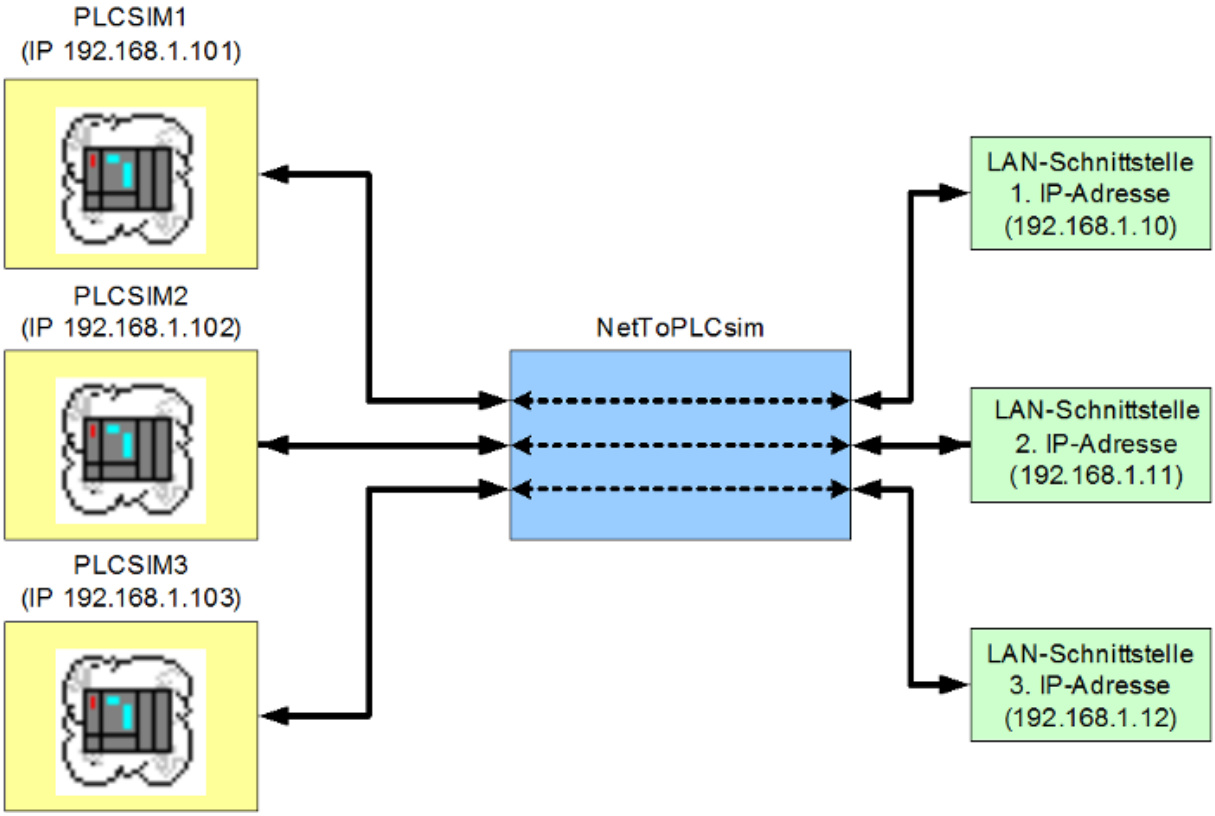
Des Weiteren ist es möglich, eine ini-Datei per Drag&Drop auf die NetToPLCsim.exe zu ziehen. Dann wird NetToPLCsim automatisch mit dieser Konfigurationsdatei gestartet.

2.3 Weitere Informationen

2.3.1 Mehrere Plcsim-Instanzen

Am folgenden Beispiel wird gezeigt, wie Sie drei Plcsim-Instanzen über NetToPLCsim erreichbar machen können. Das Prinzip lässt sich auf eine beliebige weitere Anzahl an Instanzen erweitern (bisher mit 6 Instanzen getestet).

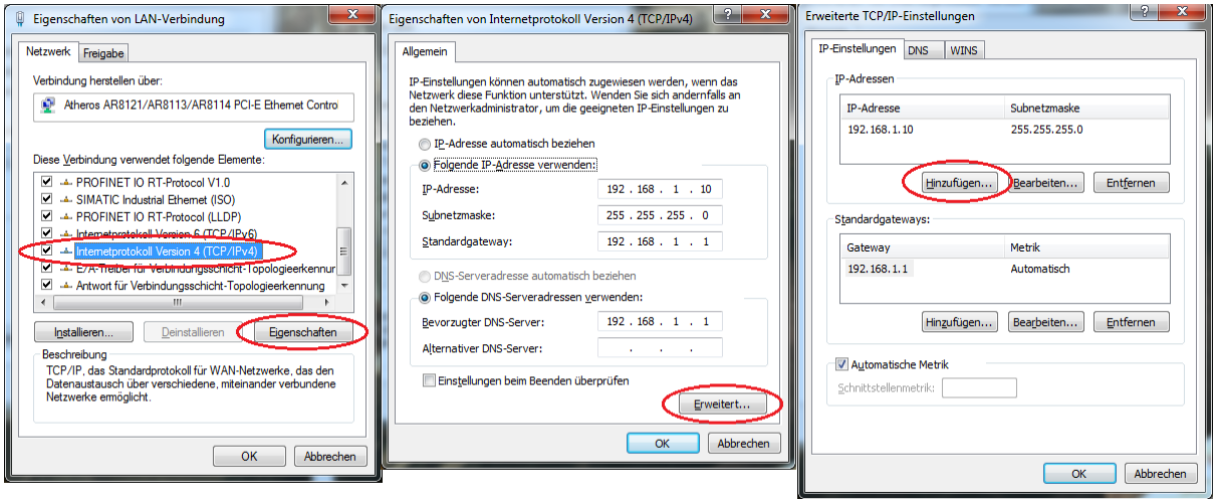
Abbildung 4 Schema Simulation mit drei Plcsim CPUs



Um gleichzeitig mehrere PLCSIM-Simulationen über das Netzwerk erreichbar zu machen, werden für jede Simulation eine eigene IP-Adresse benötigt. Entweder man hat in dem PC entsprechend viele Netzwerkkarten, oder man fügt der verfügbaren Netzwerkkarte die benötigte Anzahl an weiteren IP-Adressen hinzu.

In den folgenden Bildern ist das Hinzufügen von weiteren IP-Adressen unter Windows 7 gezeigt.

Abbildung 5 Hinzufügen einer weiteren IP-Adresse (Windows 7)



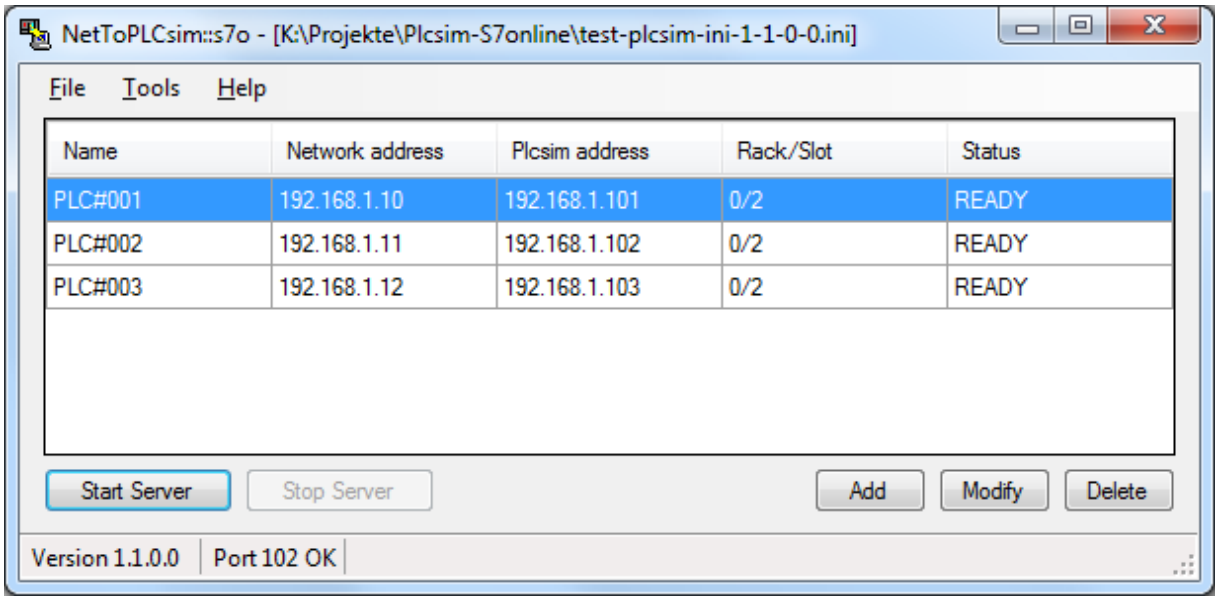
ANMERKUNG

Um spätere Netzwerkprobleme zu vermeiden, sollten nach dem Test die zusätzlichen IP-Adressen wieder entfernt werden.

Die weiteren Plcsim Instanzen können nach dem Start der ersten Plcsim Instanz aus dem SIMATIC-Manager aus Plcsim heraus gestartet werden (Menüpunkt Simulation → Zielsystem Neu). In die neue Simulation sollte dann direkt danach das SPS-Programm inkl. Systemdaten geladen werden, da erst danach die Simulation die korrekte *virtuelle* IP-Adresse erhält.

Das grundsätzliche Anlegen der Stationsdaten in NetToPLCsim erfolgt genauso wie oben für eine Station beschrieben. Es werden dann entsprechend zusätzliche Stationen mit den zugehörigen IP-Adressen für Plcsim und die Netzwerkkarte angelegt. Für das oben gezeigte Schema wäre dann folgende Konfiguration notwendig:

Abbildung 6 Konfiguration in NetToPLCsim für drei SPS



2.3.2 Simatic S7DOS Dienst

Die S7-Kommunikation wird über den TPC-Port 102 abgewickelt.

Eine Step7-Installation bringt einen Dienst "SIMATIC S7DOS Help Service" (ehemals "SIMATIC IEPG Helper") mit, welcher den beschriebenen Port belegt. Der Siemens-Dienst lauscht dabei auf allen verfügbaren Netzwerkadressen, was bedeutet, dass solange dieser Dienst läuft kein eigener Server auf diesem Port gestartet werden kann.

Seit Step 7 V5.5 SP2 unter 64-Bit Windows reicht es nicht mehr aus diesen Dienst nur zu beenden, da dadurch diverse Funktionen von Siemens Programmen eingeschränkt sind.

Aus diesem Grunde wird über die Funktion "Get Port 102" oder über die Dienst-Funktion beim Start von NetToPLCsim (seit Version 1.1.0) folgende Sequenz ausgeführt:

1. Stoppen des Dienstes "SIMATIC S7DOS Help Service"
2. Starten eines eigenen TCP-Servers auf Port 102 und allen verfügbaren IP-Adressen
3. Starten des Dienstes "SIMATIC S7DOS Help Service". Da der Server-Port 102 nun reserviert ist, kann der Siemens-Dienst sich diese Ports nicht in Beschlag nehmen
4. Stoppen des eigenen TCP-Servers
5. Prüfung ob der TCP-Port 102 frei ist

Im Anschluss daran ist der Port 102 für die Verwendung mit NetToPLCsim frei.

Wurde der Dienst beim Start von NetToPLCsim beendet, wird bei Beendigung des Programms abgefragt ob dieser Dienst neu gestartet werden soll, um die Funktionalität wieder herzustellen.

ANMERKUNG

Soll nach Beendigung der Tests mit NetToPLCsim an einer realen SPS programmiert werden, so sollte auf jeden Fall ein Neustart des Rechners durchgeführt werden!

3 Versionshistorie

3.1 Version 0.9.0

- Erste Version welche die S7online-Schnittstelle verwendet

3.2 Version 0.9.1

- Optionales Monitoring des Datenaustausches (Anzeige von Lese- und Schreibbefehlen mit den entsprechenden Datenbereichen) hinzugefügt

3.3 Version 0.9.2

- Fehlerbehebung: Gelegentliches hängenbleiben der S7online-Schnittstelle bei Daten mit bestimmten PDU-Größen behoben
- Abfrage des auf dem System vorhandenen IEPG-Helper Dienstnamens, damit dieser auch unter Windows 32 oder 64 Bit gestartet / gestoppt werden kann
- Kommandozeilenparameter hinzugefügt, Drag&Drop einer Konfigurationsdatei auf die NettoPLCsim.exe möglich

3.4 Version 0.9.3

- Funktionserweiterung / temporäre Fehlerbehebung: Eine Client Anfrage mit SZL-ID 0x0131 Index 3 wird nicht an Plcsim durchgeleitet sondern von NetToPLCsim selber beantwortet. In der Antwort wird dem Client mitgeteilt dass NetToPLCsim keine zyklischen Lesedienste beherrscht. Dieser sollte dann auf die "normalen" Variablendienste zurückschalten. Die Verwendung von zyklischen Lesediensten führte in vorigen Versionen dazu, dass die Client Verbindung öfters abgebrochen wurde, bzw. die S7online-Schnittstelle gelegentlich nicht mehr benutzbar blieb. Der eigentliche Fehler liegt in einer zur Zeit noch nicht korrekten Anwendung der S7online-Schnittstelle von NetToPLCsim, da Plcsim an sich diese Funktion unterstützt.
- Vereinfachung der Bedienbarkeit: Wird eine neue Station hinzugefügt, wird jetzt ein automatischer Name vergeben der bei Bedarf angepasst werden kann.

3.5 Version 0.9.4

- Antwort beim Verbindungsaufbau dass nur ein Telegramm zur Zeit bearbeitet werden kann (MaxAmQCalling/MaxAmQCalled)
- Einstellmöglichkeit für Rack/Slot Kombination, dadurch sollte evtl. mit der Kombination 0/1 mit TIA-Portal funktionsfähig sein (ab TIA V13)
- Optional aktivierbarer TSAP check: Bei aktivierter Option werden nur Verbindungen der Rack/Slot Kombination zugehörigen TSAPs angenommen, mit den Verbindungsressourcen 1, 2 oder 3 (PG, OP, S7basic)
- Protokoll-Monitor: SZL Anfragen (Index und ID) werden aufgeschlüsselt

3.6 Version 0.9.5

- Hinzufügen der Tool-Funktion "Get Port 102" damit ein Betrieb auch unter Step 7 V5.5 SP2 64 Bit möglich ist

3.7 Version 1.0.0

- Umstellung der Handhabung der S7online-Schnittstelle. NetToPLCsim stellt die volle Funktionalität von Plcsim über Netzwerk zur Verfügung. D.h. Es sind jetzt auch Programmierfunktionen (Programme laden, beobachten etc.) möglich. Auch Bausteinbezogene Meldungen über Alarm_S oder Alarm_8, und zyklische Variablendienste sind jetzt möglich.
- Eine Antwort auf SZL-ID 16#0x74 für den Zustand der Baugruppen-LEDs wird selber generiert, da von Plcsim nicht unterstützt. Unabhängig vom Betriebszustand der Plcsim-Simulation, wird immer der Zustand RUN-LED ein, und alle anderen LEDs aus gemeldet.

3.8 Version 1.1.0

- Fehlerbehebung: mehrere ISO-Pakete zusammen in einem TCP Telegramm führten zu einem Programmfehler mit nachfolgendem Verbindungsabbruch (für V1.0.0)
- Unterstützung von S7-Plcsim für TIA-Portal S7-1200/1500
- Ehemalige Funktion "Get Port 102" aus dem Tools-Menü wird jetzt standardmäßig bei Programmstart ausgeführt
- Telegrammmonitor: Mit Mausklick auf die Statusleiste lässt sich die Aufzeichnung pausieren und fortsetzen
- Neue Dokumentation in Form von Windows-Help Dateien
- Lizenzänderung von der GPL zur LGPL

3.9 Version 1.2.0

- Fehlerbehebung: Korrektur der Verarbeitung des Stationsnamens in der Funktion zum Anzeigen der erreichbaren Plcsim-Teilnehmer. Führte gelegentlich dazu, dass überhaupt keine Teilnehmer gefunden wurden, oder ein Ausnahmefehler auftrat.
- Timeout-Zeit beim Stoppen des S7DOS-Dienstes erhöht, optionaler weiterer Versuch. Auf langsamen Maschinen reichte die bisherige Zeit zum Stoppen nicht aus.

3.10 Version 1.2.1

- Fehlerbehebung: Mehrere TPDUs wurden nicht immer korrekt aus dem TCP-Stream gelesen. Bei Client-Anwendungen die mehr als eine unquittierte PDU gesendet haben führte das zu Verbindungsproblemen.
- Protokoll-Monitor: Aufschlüsselung von angefragten Bereichen bei zyklischen Variablendiensten

4 Lizenz