

NetToPLCsim S7online Version

Introduction

The old NetToPLCsim-Version used the S7ProSim-COM-Object to exchange data with Plcsim. The version described in this document uses the so called S7online interface. The old version had to dissect the S7-protocol and read/write data through the S7ProSim interface. The new version starts a IsoOnTCP server and forwards the payload into the S7online-interface.

The main differences between 'old' and 'new' version:

- Support of multiple clients (max. 100)
- No limits in supported data areas, it's possible to read and write timer (T) and counter (C), read digital-inputs (I) and write digital-outputs (O)
- Support of multiple Plcsim instances
- Improved data throughput
- Support of other PLC functions, like Run/Stop, timesystem, reading of SZL (maybe different to a 'real' PLC)

To use this new version, you have to configure a PLC with a network interface, like a PN-CPU or a classis CPU with additional Ethernet CP.

NetToPLCsim acts as intermediary between Plcsim and your real network interface.

The service „SIMATIC IEPG Helper“

As you have Step7 installed on your PC, then there is a Windows service called „SIMATIC IEPG Helper“ running in the background. This service holds TCP port 102 in use. But this port is used for S7-communication, so this service must be stopped before starting NetToPLCsim.

At program start, NetToPLCsim checks if port 102 is free. If it's not, then it asks to stop the „SIMATIC IEPG Helper“ service.

When you ended with testing with NetToPLCsim, it's recommended to restart the service before doing other work with SIMATIC software.

Alternitavely you can stop the service with the following two little batch files:

32-Bit Step7:

Stop IEPGhelper.bat:

```
net stop s7oiehsx
```

Start IEPGhelper.bat:

```
net start s7oiehsx
```

64-Bit Step7:

Stop IEPGhelper.bat:

```
net stop s7oiehsx64
```

Start IEPGhelper.bat:

```
net start s7oiehsx64
```

Hint

You need administrative rights to make changes on the windows service control. On Windows XP your actual user account needs admin-rights, on Windows 7 you need to start NetToPLCsim with administrative rights

Simulation with one single Plcsim instance

Example configuration:

S7-300 PN-CPU with IP-address: 192.168.1.101

LAN interface IP-address: 192.168.1.10

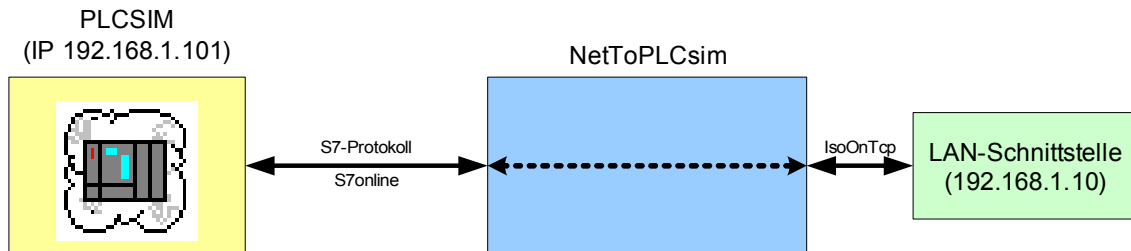
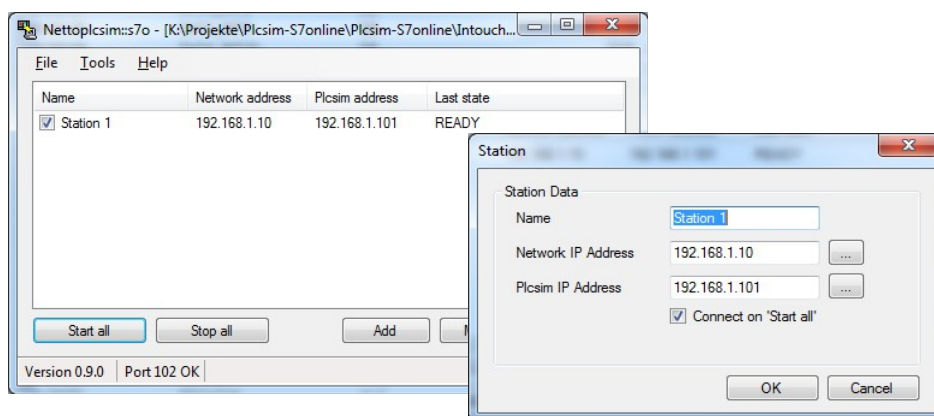


Figure 1: Simulation with one single Plcsim-PLC

- 1) Start PLCSIM out of the SIMATIC-Manager
- 2) Set PG/PC interface in PLCSIM to 'PLCSIM(TCP/IP)'
- 3) Load your PLC program including system data into PLCSIM
- 4) Start NetToPLCsim
- 5) In NetToPLCsim add a new station
- 6) Insert unique name in „Name“ field for this station
- 7) In „Network IP Address“ field, insert the IP-address of your LAN interface, on which Plcsim should be reachable (e.g. 192.168.1.10). Clicking on (...) shows a new windows where all interface IP-addresses are listed.
- 8) In „Plcsim IP Address“ field, insert the IP-address of your PLC (IP-address which is shown in Plcsim status bar). Clicking on (...) shows a new windows where all PLCSIM reachable PLCs are listed.
- 9) Apply station configuration with OK
- 10) A click on „Start all“ will start the servers



When state changes to 'RUNNING', a client like SCADA/visualisation-systems can reach the Plcsim PLC on IP-address 192.168.1.10

To stop the simulation, at the first step stop NetToPLCsim. At the second step stop PLCSIM.

Simulation of multiple Plcsim-Instances

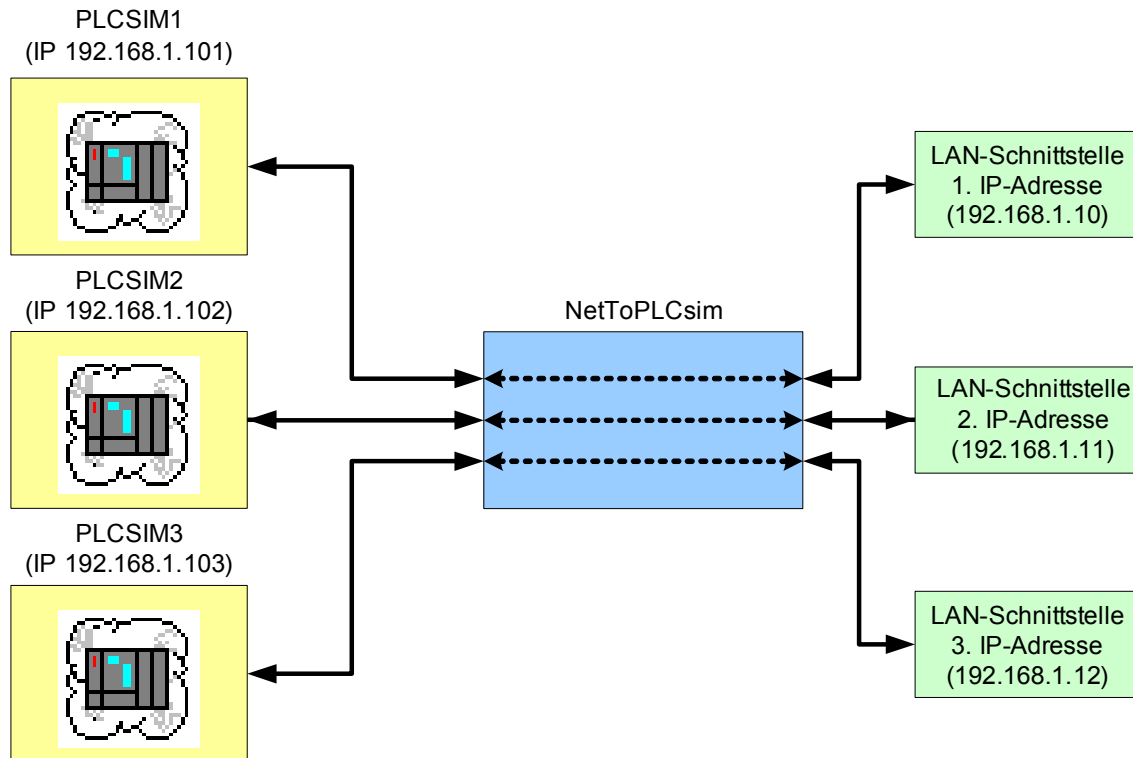
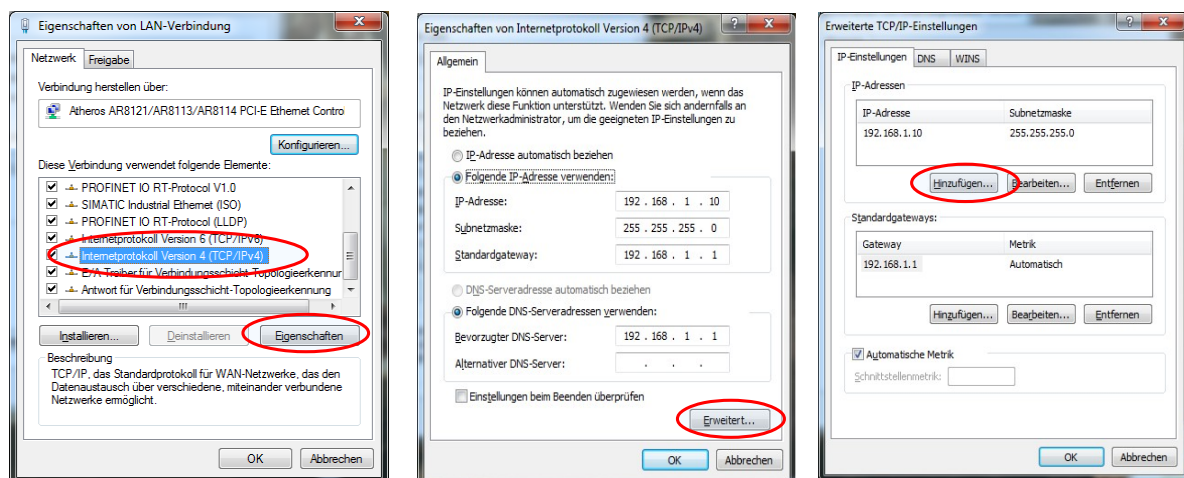


Figure 2: Simulation with three Plcsim-PLCs

To connect to multiple PLCSIM-simulations at the same time, NetToPLCsim needs a separate IP-address for each server to start on. It's possible to realize this with inserting more than one network interface card, or by simply adding additional IP-addresses to the existent interface.



The image sequence above shows how to add additional IP-addresses to you LAN interface. (german Windows 7 version)

Hint

To avoid later network problems, you should delete the additional IP-addresses when finished with testing (my experience)

A new PLCSIM instance can be started out of the first PLCSIM instance by menu File → „New Plc“ (or something like that, I've got only the german version).

The following steps are equal to simulation with on PLCSIM instance.

For the constellation shown in fig.2, the configuration shown in this image is needed:

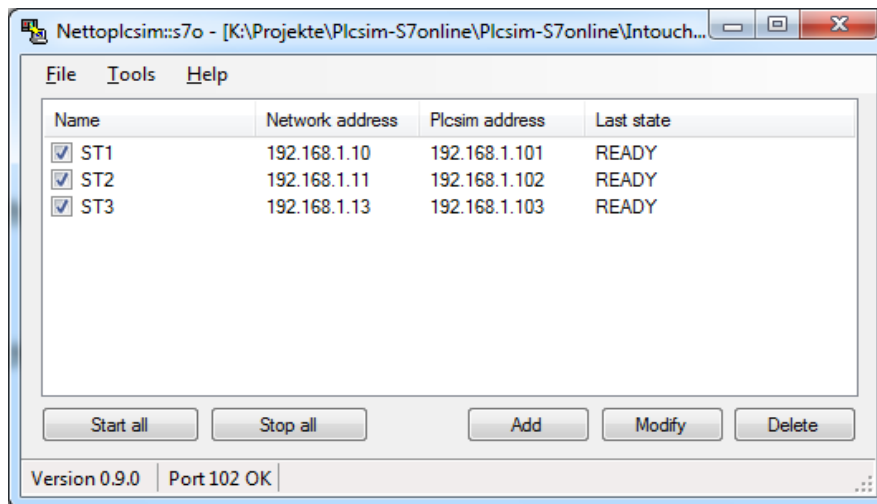


Figure 1: Nettoplcsim configuration with three PLCs

Monitoring of the data-exchange

When the nettoplcsim servers are started, the „Start monitoring“ entry in the context-menu of the station list is enabled. For each station a separate monitoring-windows can be started. In the monitoring-windows only the usually telegrams for data-exchange (Read/Write-Requests) between a PLC and a SCADA-system are shown.

To debug more details of the protocol, you can use Wireshark with my s7comm plugin-dll.

<http://sourceforge.net/projects/s7commwireshark>

Notice

The activated monitoring reduces the data exchange rate significant.

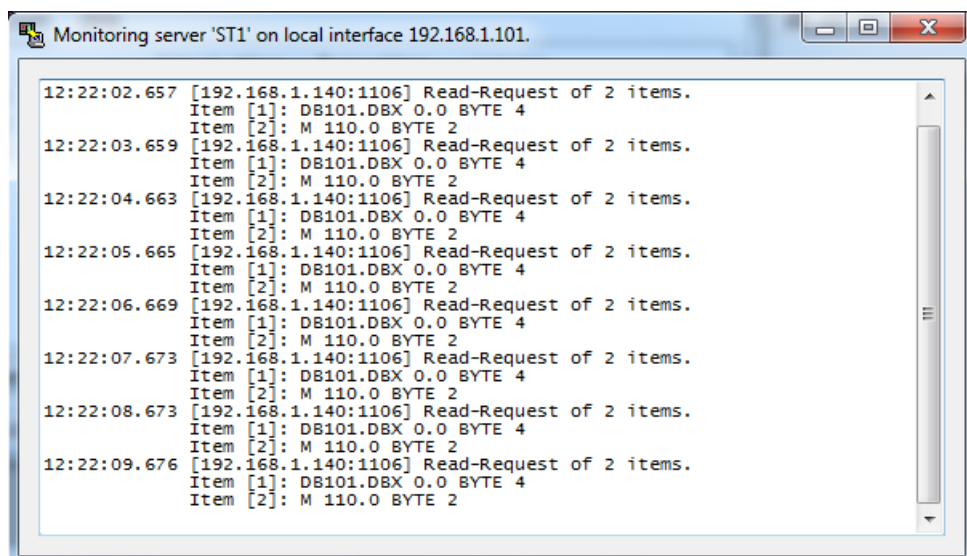
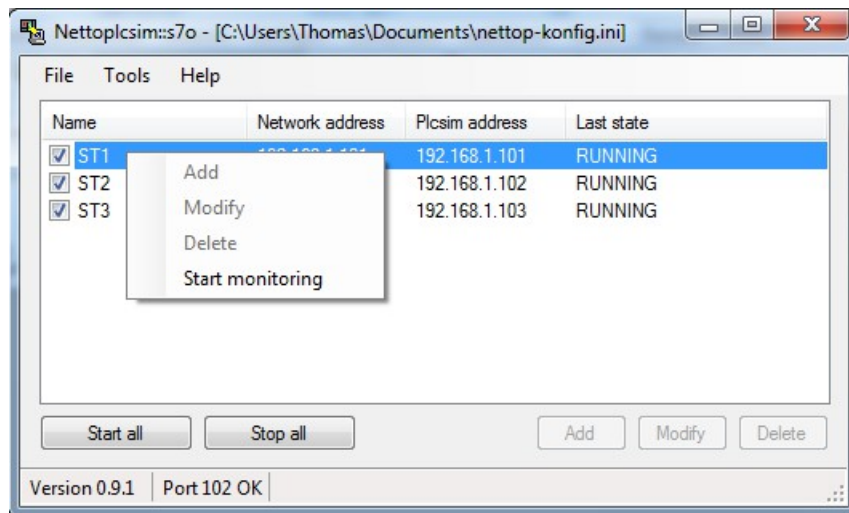


Figure 2: Nettoplcsim protocolmonitor

Command-Line Arguments

The following command-line arguments are possible:

- f=configurationfile.ini Loads this station configuration file
- s=Option Autostop control of IEPG-Helper service.
Options:
YES=Automatically stop the service, NO=Don't stop, ASK=ask
- autostart Is a valid configuration file given, the servers for activated station are automatically started

Example:

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

Further it is possible to Drag&Drop a configuration file on the NetToPLCSim.exe file. Then this

NetToPLCsim starts with this configuration.

Version history

0.9.0

- First version using the S7online interface

0.9.1

- added optional monitoring of the data exchange

0.9.2

- Fixed: Data exchange with plcsim doesn't hang up any more, when packets of some PDU sizes occur
- Check of the running IEPG-Helper servicename to stop/start service in Windows 32 or 64 Bit OS
- Added Command-Line Arguments, and the possibility to Drag&Drop a configuration file on the NetToPLCsim.exe

0.9.3

- Temporary fix: Implemented own response for SZL-ID 0x0131 index 3 request, to force clients not to use the cyclic data exchange mechanism, which causes sometimes communication failures
- Usability: Automatic name generation when a new station is added