NetToPLCsim - Network extension for Plcsim

Thomas Wiens

April 18, 2017

NetToPLCsim - Network extension for Plcsim
by Thomas Wiens

Contents

List of Figures

List of Tables

1 Introduction

1.1 What you can do with NetToPLCsim

NetToPLCsim allows you to use network communication together with the PLC-Simulation S7-Plcsim, using the network interface of the PC on which the simulation is running. For example, you can test your client application (SCADA system, etc.) together with S7-Plcsim, without a real PLC.

NetToPLCsim supports most of the functions which are supported by S7-Plcsim, like:

- Tag services: reading and writing data areas
- Block services: Program upload, program block online view, ...
- Block specific messages with Alarm_S, Alarm_D
- Support of multiple Plcsim instances on a single computer

1.2 What you cannot do with NetToPLCsim

The following functions are not supported by NetToPLCsim:

- All communication functions which are programmed via the T-Blocks (TCON, TSEND, etc.) or configured via NetPro are not supported
- NetToPLCsim supports other system state lists (SSL/SZL) as a real CPU, and they contain different values
- You can't use programming functions using TIA-Portal with a S7-300/400 simulation, because TIA-Portal checks the compatibility of the CPU you want to upload the program to. With Step7 V5.x this is no problem, as it's more tolerant uploading the program into a different type of CPU
- The Plcsim/NetToPLCsim CPU will not be visible if you are using "Display Accessible Nodes" in Step 7. This method uses the LLDP protocol on MAC layer. On a PC with installed Simatic software, your PC will always be listed as "PC-Station". Furthermore the communication behaviour of S7-Plcsim/NetToPLCsim is slightly different to a real CPU.

IMPORTANT

A test with NetToPLCsim does not substitute the test on the real hardware.

1.3 How does NetToPLCsim work?

The first versions of NetToPLCsim (including V0.7.2) were using the official interface to Plcsim, which is a library implemented in the so called S7ProSim-COM-object. In this versions the S7 protocol was processed inside NetToPLCsim, and the requested data were read or written to Plcsim through this interface. Due to the limitation in this interface, to get only access to data areas, is was only possible to realize tag services with NetToPLCsim. Another disadvantage of the S7ProSim interface is, that it's rather slow.

Plcsim for 1200/1500 has no interface like S7ProSim. Due to this limitations, all following versions are using the so called S7online-interface.

1.4 S7online-interface

The S7online-interface represents the OSI layers 1 to 4 for all applications inside the Simatic universe. If a Simatic application communicates to a PLC, the data goes always through the S7online-interface. The functions of the S7online-interface are accessible through the program library s7onlinx.dll inside the windows system directory.

The S7online-interface passes the data from the application to the underlying transport layer, like TCP/IP, MPI or Profibus. The transport layer which S7online is using, is configured in the dialog "Set PG/PC interface" from the Simatic application or the Windows control panel. Also the communication to Plcsim runs through this interface. The data running through this interface are already S7-communication. Thus the job of NetToPLCsim is to represent the IP/IsoOnTcp transport layer, and pass the payload into the S7online-interface and back. The main problem with the S7online-interface is that it's not official documented, which was the main problem using this interface with NetToPLCsim.

2 Manual

2.1 Quickstart

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

Use the following steps to setup a network accessible Plcsim simulation using NetToPLCsim. The description is valid for Plcsim with Step 7 V5.5.

1. Start the Simatic manager
2. Open your S7 project you want to test
3. Start Plcsim, upload the program including system data into Plcsim. You need a CPU with a ethernet network device (PN-CPU or CPU plus Ethernet CP)
4. Start NetToPLCsim with administrative rights (these are neccessary to stop a Siemens service)
5. If NetToPLCsim asks to stop the Siemens service, click yes
6. In NetToPLCsim click on "Add"
7. In the station configuration dialog, click on "..." next to the text field "Network IP Address". You get a list with all IP addresses of the existing network devices of your computer. Choose the address on which Plcsim should be accessible
8. Next to the text field "Plcsim IP Address" click on "...". You should see the Plcsim CPU you have uploaded. Select the device and click "OK"
9. Set a rack/slot combination of 0/2 (for S7-400 dependant of your hardwareconfiguration
10. Close the dialog with "OK"
11. In the main window click on "Start server"
12. Your Plcsim simulation is now reachable at the IP address shown under "Network IP address"

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

To use NetToPLCsim with TIA-Plcsim, it's required to set the correct PG/PC interface settings. In the Windows Control Panel you open the "Set PG/PC interface" program, and set the access point for S7ONLINE to "PLCSIM S7-1200/S7-1500(TCP/IP)".

Since TIA Portal Version V14 you have to set the access point to "PLCSIM.TCPIP.1"

2.2 General operation

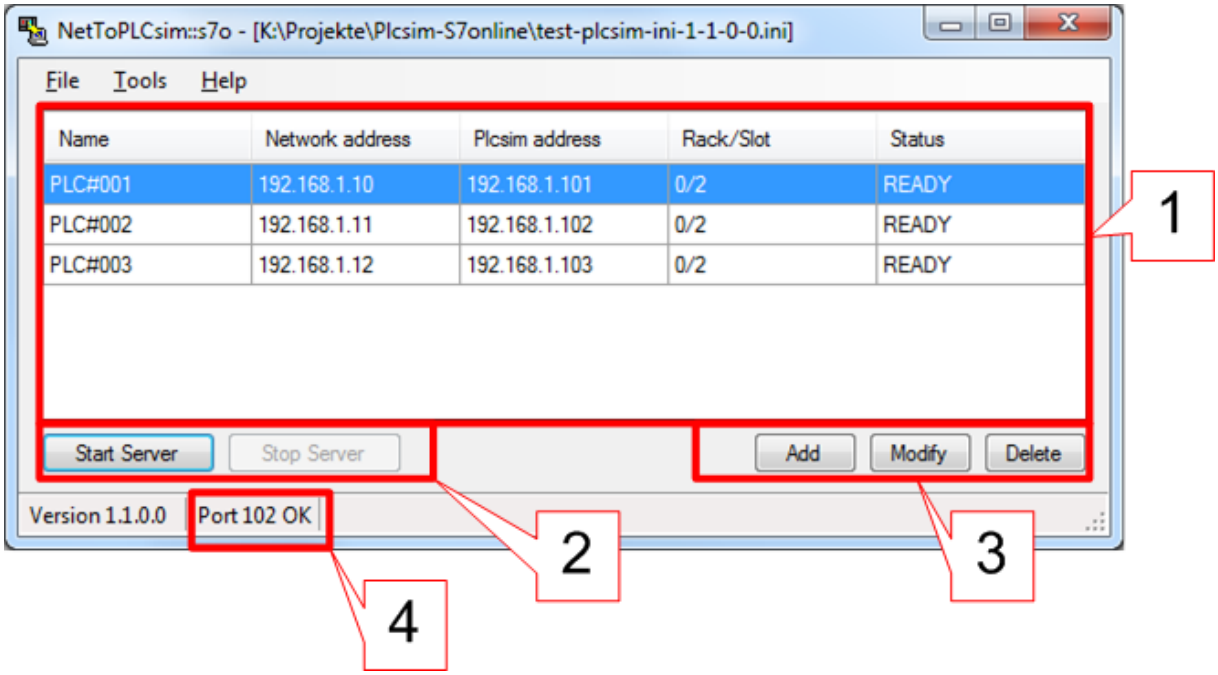
2.2.1 Neccessary requirement

You need Step 7 Plcsim with V5.4 or later, or Plcsim for TIA-Portal.

In your Step 7 hardware configuration you must have an Ethernet device (PN-CPU or CPU plus Ethernet CP).

2.2.2 Main window

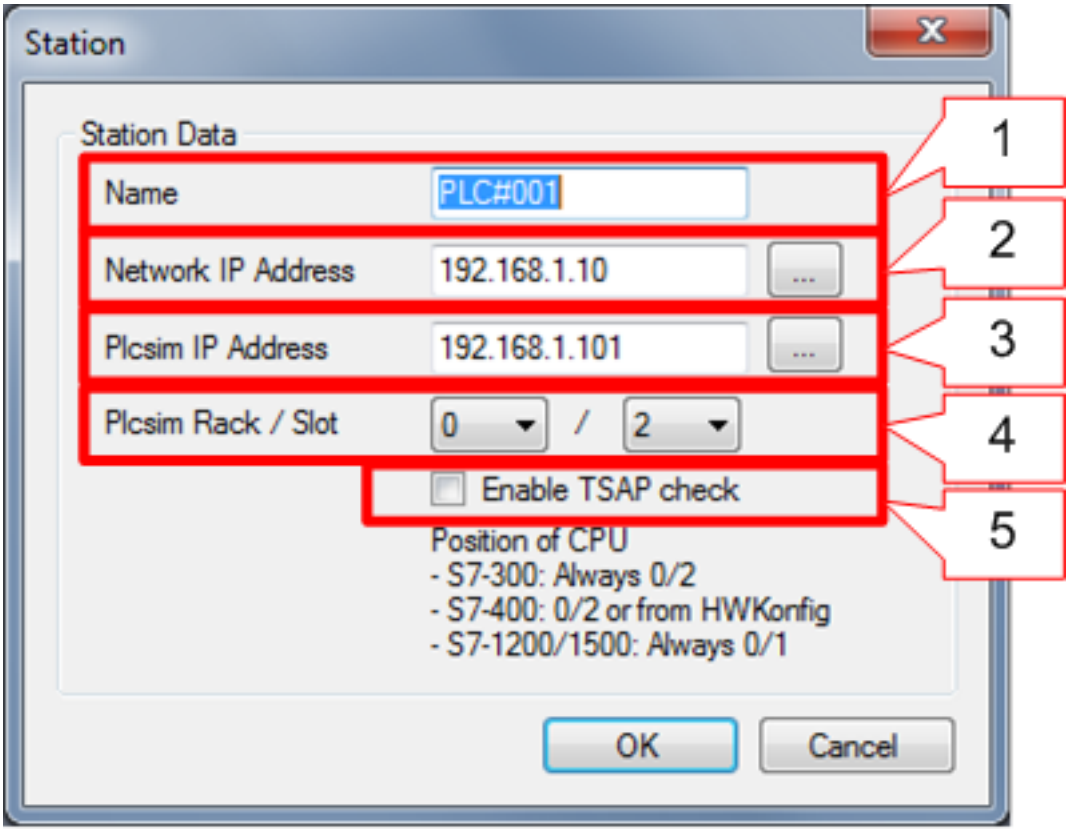
Figure 1 NetToPLCsim Main window



1. Area showing your configured stations
2. Buttons to start and stop the server for the configured stations
3. Buttons to add, modify or delete a station
4. Result of the port-check which is done on start of NetToPLCsim. You can use NetToPLCsim only with status OK.

2.2.3 Station dialog

Figure 2 NetToPLCsim Station dialog



1. Unique Name
2. IP address of the network interface at which this server should be reachable
3. IP address of the Plcsim-CPU
4. Rack/Slot position of the CPU. This setting is only relevant if you set the option TSAP-check. If you enable this option, your client application needs to use the correct TSAP corresponding to the rack/slot combination. NetToPLCsim accepts as connection ressource 1=PG, 2=OP and 3=Step7Basic.

2.2.4 Protocolmonitor

If you have started the NetToPLCsim server, you can start the protocolmonitor via context menu (right mouse-click) of the station you want to monitor. If you select "Start monitoring", a new window with the protocolmomitor opens.

At this time only S7 communication for S7-300/400 is shown, and only some parts of the S7 protocol are dissected. Only incoming telegrams using variable services (reading and writingdata areas in the S7) and SSL-(SZL)-Requests are decoded.

With mouseclick on the statusbar, you can pause and resume the capture output. The communication is not stopped when you pause the output.

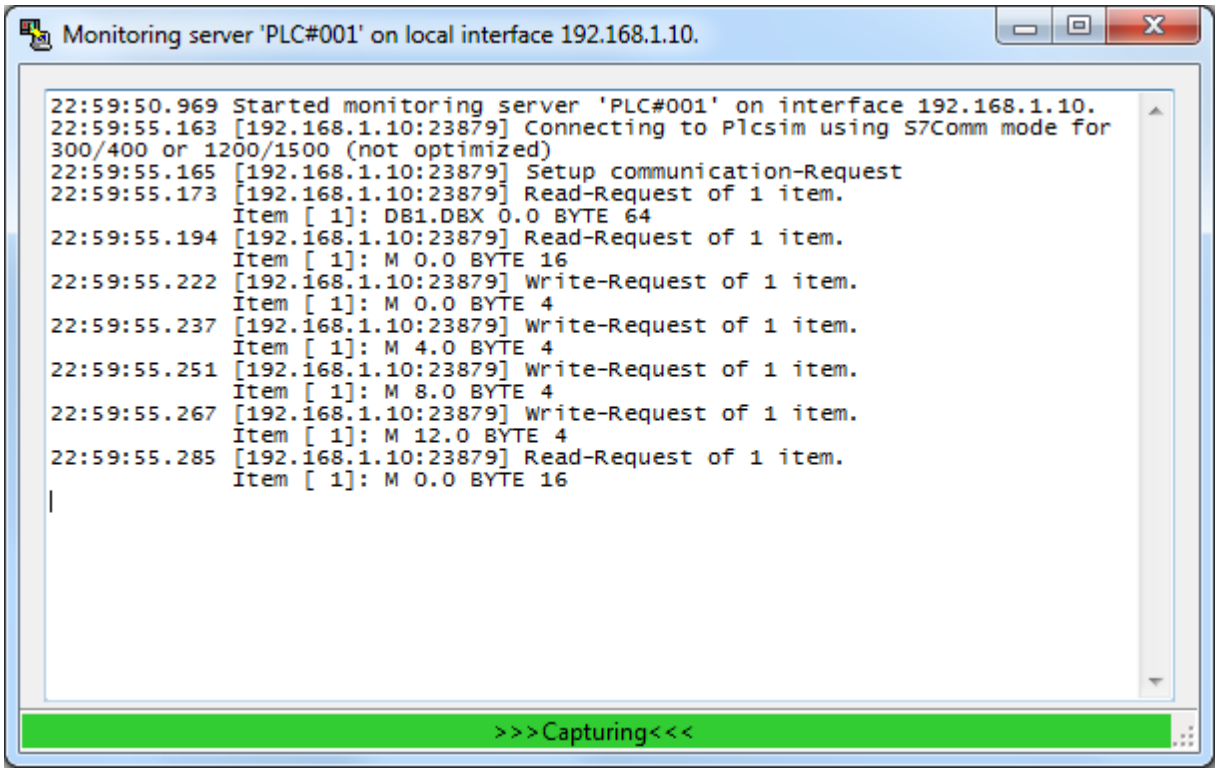
If you want to see all details of the S7 protocol, you can use the network protocol analyzer Wireshark. Since Wireshark version 2.0 the S7 protocol is integrated. On older versions you need a plugin-dll for the S7 communication, you can download from the link below.

http://sourceforge.net/projects/s7commwireshark

NOTE

The activated monitoring reduces the data exchange rate significant.

Figure 3 NetToPLCsim Protocolmonitor



2.2.5 Command-line arguments

You can use the following command-line arguments with NetToPLCsim:

Table 1 Command-line arguments

Option	Description
-f=config.ini	Loads this station configuration file
-s=Option	Autostop control of the S7DOS Help Service. Options: YES=Stop the service, NO=Don't stop the service, ASK=ask
-autostart	If a valid configuration-file is loaded, the servers for the stations in the file are automatically started

Example:

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

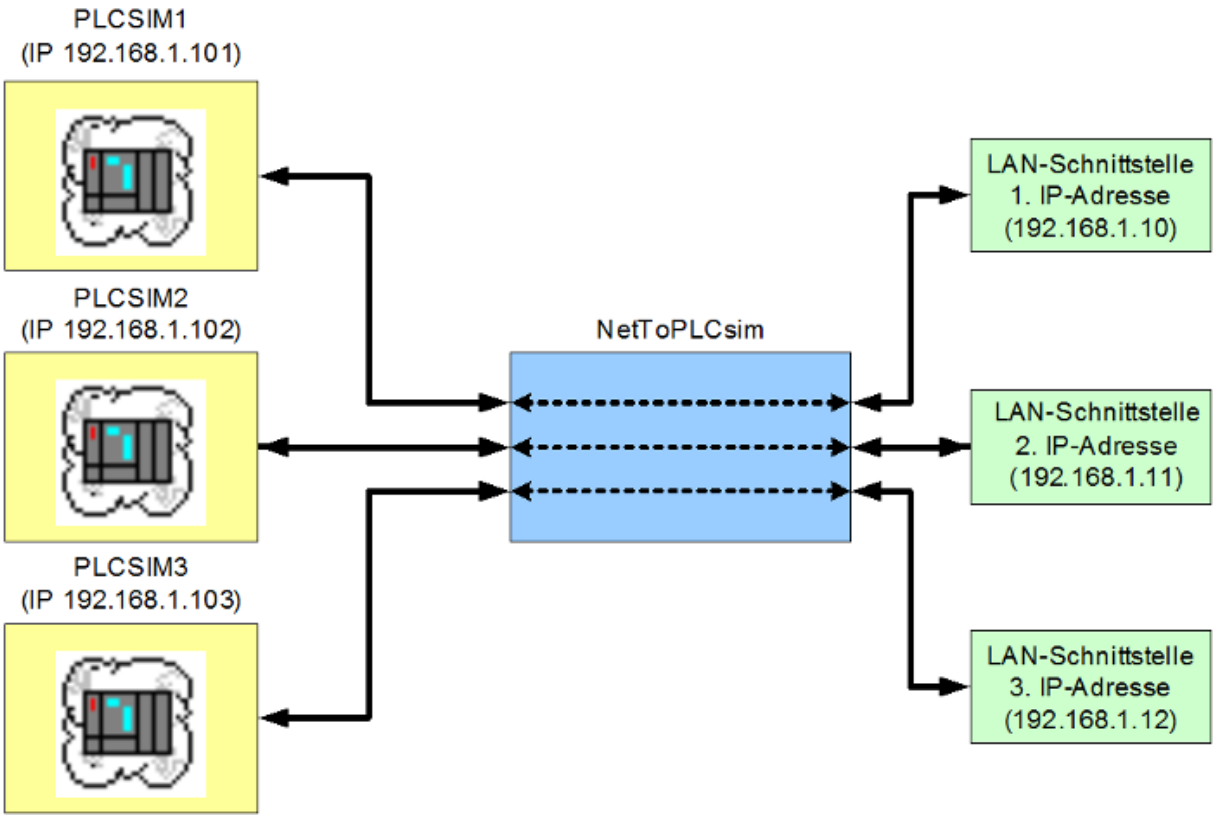
Further it's possible to Drag&Drop a configuration file on the NetToPLCsim.exe file. Then NetToPLCsim starts and loads this configuration.

2.3 Further informations

2.3.1 Multiple Plcsim-Instances

The following example demonstrates how to realize three network reachable Plcsim instances with NetToPLCsim. The main principle could be extended to a arbitrary number of additional instances (tested with 6 Plcsim instances).

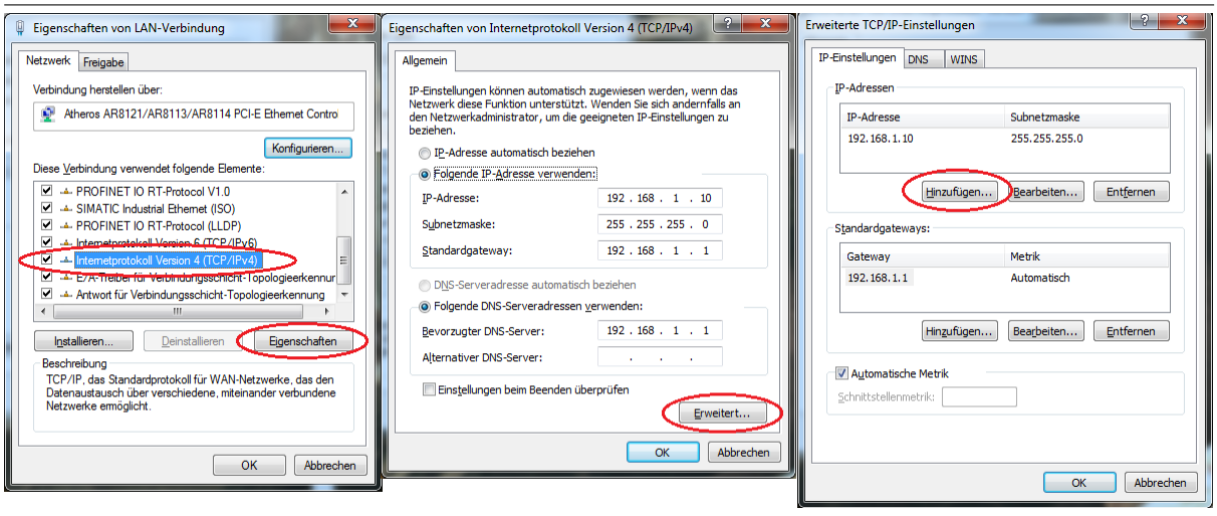
Figure 4 Simulation of three Plcsim instances



Each Plcsim instance needs it's own IP address, under which it's later reachable from your network. One option is that you've got more than one network interface in your computer. The other option is to add one or more IP addresses to the existing network interface.

In the following screenshot, it is shown how to add an additional IP address to your network interface under Windows 7 (german).

Figure 5 Adding an IP address to a network interface (Windows 7)



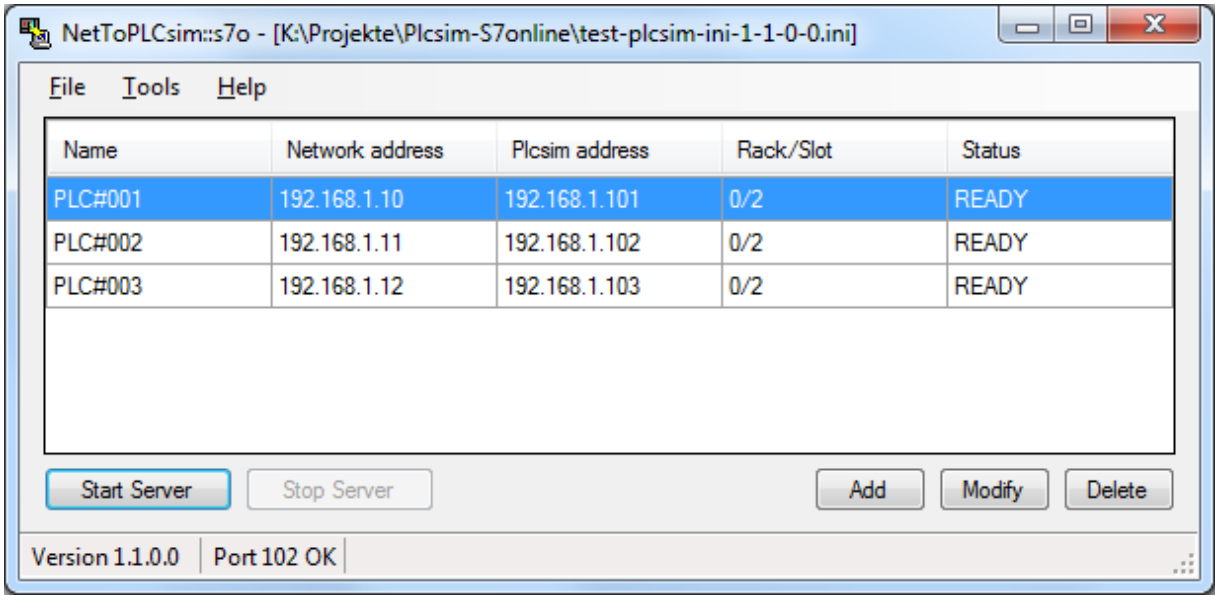
NOTE

To avoid later network problems, you should delete the additional IP-addresses when finished with testing.

You can start a new Plcsim instance after you started the first instance, using the menu "File" → "New Plc" in Plcsim. When the new Plcsim instance has started, upload the PLC program including system data into Plcsim. Only with uploaded system data the simulation has the configured "virtual" IP address.

The setup of the stations in NetToPLCsim is done in the same way as described for a single station. For the simulation overview shown above the following setup in NetToPLCsim is needed:

Figure 6 Example configuration in NetToPLCsim for three Plcsim instances



2.3.2 Simatic S7DOS service

The S7-communication uses TCP port 102.

If you have Step 7 installed on your system, you've got a service called "SIMATIC S7DOS Help Service" (old name was "SIMATIC IEPG Helper"). This service listens on all available network interfaces for incoming connections on TCP port 102. Thus as long this service is running, it's not possible to start an server from another application like NetToPLCsim using this port.

Since Step 7 V5.5 SP2 unter 64 bit Windows, it's no longer possible to simply stop the service, as this affects other Siemens program functions.

For that reason the function "Get Port 102" from Tools-Menu, and the automatic service-stop function when you start NetToPLCsim (since version 1.1.0) starts the following sequence:

1. Stop the service "SIMATIC S7DOS Help Service"
2. Start own TCP server on port 102 on all available interfaces
3. Start the service "SIMATIC S7DOS Help Service". As TCP port is now not available for the service, it cannot reserve it
4. Stop own TCP server
5. Check if TCP port 102 is now available If the last check succeeded, port 102 is now available for using with NetToPLCsim.

NetToPLCsim remembers when you have stopped the Siemens service on program start. If you close NetToPLCsim, you can optional restart the Siemens service (recommended).

NOTE

If you want to program a real S7-PLC after testing with NetToPLCsim, it's recommended to restart the computer!

3 Version history

3.1 Version 0.9.0

- First version using the S7online interface

3.2 Version 0.9.1

- added optional monitoring of the data-exchange

3.3 Version 0.9.2

- Fixed: Data exchange with Plcsim doesn't hang up any more, when packets of some special PDU sized 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

3.4 Version 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

3.5 Version 0.9.4

- NetToPLCsim answers a client that only one single request at time can be handled (MaxAmQCalling/MaxAmQCalled)
- Added optional setting for rack/slot combination of CPU (maybe possible to connect to TIAPortal Plcsim)
- Added option for TSAP check corresponding to entered rack/slot. Connection ressources 1, 2 or 3 are valid (1=PG, 2=OP, 3=S7basic)
- Protocol monitor: requested index and ID of SZL requests are shown

3.6 Version 0.9.5

- Adding Tool "Get Port 102" in Menu Tools, which helps to get NetToPLCsim working under Step 7 V5.5 SP2 and Windows 64 Bit

3.7 Version 1.0.0

- Redesign of handling the S7online interface. NetToPLCsim supports now the full functionality of Plcsim. Programming functions like up- and downloading of program blocks and online diagnostics are possible. Also block-specific messages like ALARM_S, ALARM_8 and cyclic variable services are supported.
- Added own response telegram to SZL-ID 16#0x74, used to get the LED state of the CPU. Independent of the operating mode, the response is always RUN-LED on, and all other LEDs off.

3.8 Version 1.1.0

- Fixed: if many ISO packets were sent in a single TCP telegram, this may have caused an exception and disconnect (for V.1.0.0)
- Added support to S7-Plcsim for TIA-Portal S7-1200/1500
- Function "Get Port 102" from tools-menu is now executed on program start to stop the Siemens service
- Monitor window: With mouseclick on statusbar the capturing can be paused and resumed
- New documentation using Windows-Help files
- Changed license from GPL to LPGL

3.9 Version 1.2.0

- Fixed: Handling of the station-name used in the function to browse the reachable Plcsim partners. Fixes the problem that sometimes no Plc was found, or an exception occured.
- Increased the timeout to stop the S7DOS service and added an optional second try, to prevent that a timeout occurs on slow machines.

3.10 Version 1.2.1

- Fixed: Reading multiple TPDUs from TCP-stream corrected. Data from client applications which used to send more than one unacked PDU are now processed without problems.
- Protocol monitor: show requested variables in cyclic variable services

4 License