PLC-ANALYZER pro 6

PLC-Logic analysis in no time

Driver Addendum

PLC-driver

Siemens SIMATIC S7

MPI / PPI / PROFIBUS - cycle precise

Industrial Ethernet TCP/IP / PROFINET - cycle precise

AUTEM

www.autem.de

PLC-ANALYZER pro **6 - Driver Addendum**

Siemens SIMATIC S7 - MPI / PPI / PROFIBUS - cycle precise
Siemens SIMATIC S7 - Industrial Ethernet TCP/IP / PROFINET - cycle precise

AUTEM GmbH
Dithmarscher Straße 29
26723 Emden
Germany

+49 4921 9610 0
info@autem.de
www.autem.de

For references, suggestions and improvement suggestions we are always grateful. Please send these to AUTEM.

1st Edition 2022

Table of Contents

Signal source

Siemens SIMATIC S7 / TIA

This driver addendum describes the particularities of the following PLC drivers and gives you hints on using them.

- Siemens SIMATIC S7 / TIA - Industrial Ethernet TCP/IP / PROFINET - cycle-precise
- Siemens SIMATIC S7 / TIA - MPI / PPI / PROFIBUS - cycle-precise

With the PLC driver Siemens SIMATIC S7 / TIA - Industrial Ethernet TCP/IP / PROFINET PLC signals can be acquired via Industrial Ethernet (TCP/IP) or PROFINET. The PLC driver Siemens SIMATIC S7 / TIA - MPI / PPI / PROFIBUS enables the acquisition of PLC signals via PROFIBUS or via the multi-point MPI interface of the SIMATIC S7.

Both S7 drivers can load STEP 7 and TIA projects directly. The contained symbols are available for convenient address selection.

In addition to normal acquisition, cycle exact data acquisition is possible for many controllers. Chapter Cycle-precise acquisition explains special characteristics of this recording method.

It is important that you read through the driver addendum before using a PLC driver. Please pay attention to the WARNINGS that advise you on possible dangers when using PLC-ANALYZER pro.

> **!** **WARNING**
>
> Errors that may occur in the automated facility, endangering humans or causing large-scale material damage, must be prevented by additional precautions. These precautions (e.g. independent limit monitors, mechanical interlocks) must guarantee safe operation, even in case of dangerous errors.

Installation

The PLC driver can be added to the project as a new signal source. If the driver you want is not yet in the list of available signal sources, you must first activate the license for the PLC-driver with the AUTEM LicenseManager on your computer.

Installing additional hardware

If you have already connected your PG/PC to the PLC via MPI, PROFIBUS or Ethernet (LAN) for programming under STEP7 / TIA, you normally do not need to do anything else. Practically all common interfaces connections are supported.

Installing additional software

For new CPUs of types S7-1200 and S7-1500 no additional software is required .

For older controllers of the S7 series (S7-200/S7-300/S7-400) STEP7 or the TIA Portal must be installed on your computer.

Configuration

Open driver settings to set important parameters for data recording. If you have added the driver to the project several times, you can set the properties individually for each individual driver.

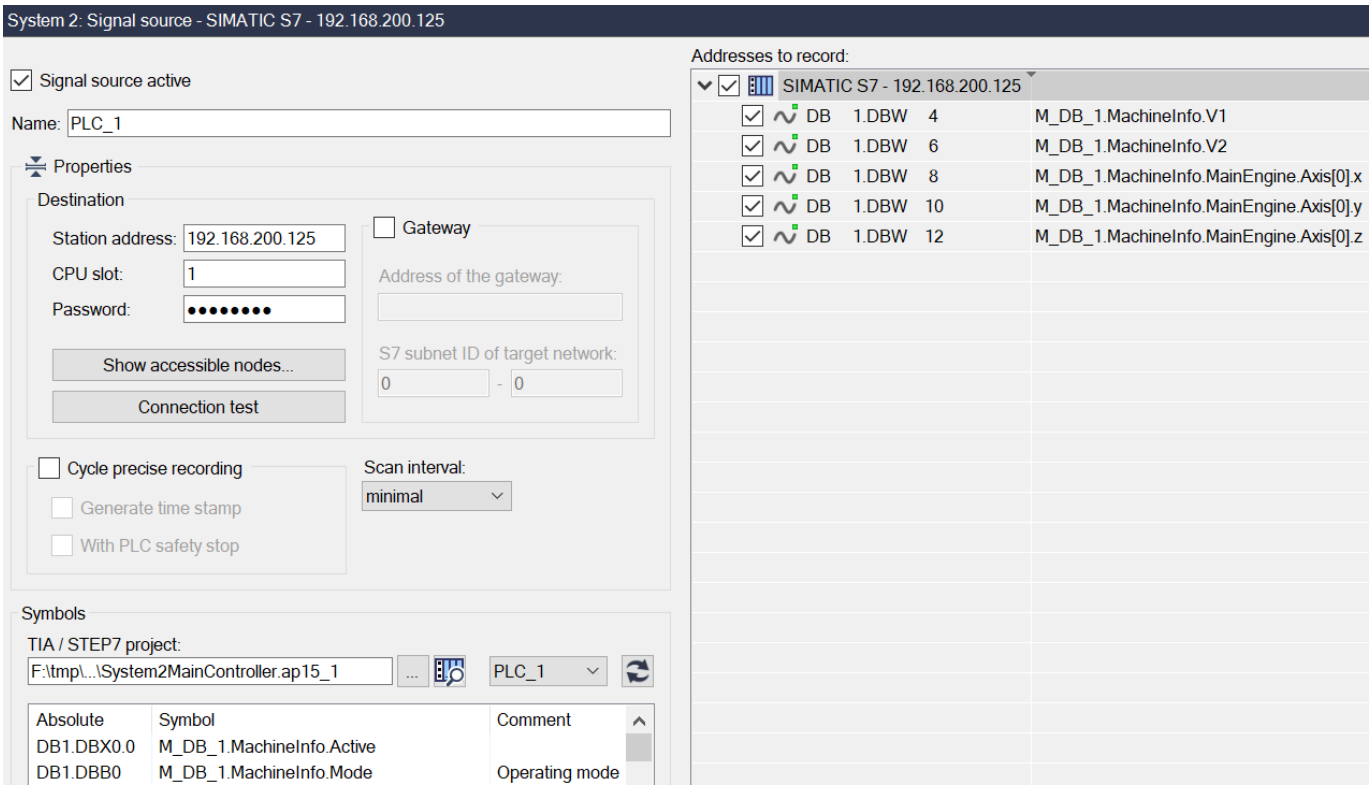

Fig. 1-1 Settings Siemens SIMATIC S7

Load an existing TIA project under *TIA / Step 7 project*, apply the communication settings and select the desired variables conveniently by drag & drop for recording.

The settings can also be entered manually. First give the driver a meaningful *Name*. Set the *Station address* and the *slot number* of the desired CPU. Depending on the PLC driver, the *Station address* can be an MPI/PPI/PROFIBUS- or an Ethernet address. Under *Symbols* load an existing TIA project to load the contained settings of the target station directly. Enter a *password* if the CPU is password-protected.

NOTE

If the CPU is protected with a password, make sure that at least the "HMI access" is allowed in the settings. If the access level "No access (complete protection)" is active, the PLC-ANALYZER pro 6 cannot acquire any data.

Show accessible nodes provides you with an overview of reachable nodes. Use *Connection test* to check whether a connection to the controller can be established successfully.

NOTE

For SIMATIC S7 Ethernet-driver you can enter either the TCP/IP-address or the MAC-address of the CP. Pay attention to enter under slot the slot of the CPU and not the slot of the CP.

If the station can only be reached via a gateway, activate Gateway. Specify the *station address* of *the network transfer* and *the S7 subnet ID of the target network*. Activate Gateway only if there indeed a cross over occurs, e.g. from Ethernet to PROFIBUS. Refer to the hardware configuration of your STEP7 project for these settings:

If the target controller can only be reached via a network gateway, activate *Gateway*. Enter the *Address of the gateway* and the *S7 subnet ID of target network*. The gateway may only be activated if a transition actually takes place, e.g. from Ethernet to PROFIBUS. The settings for the gateway transition can be found in the hardware configuration of your STEP7/TIA project:

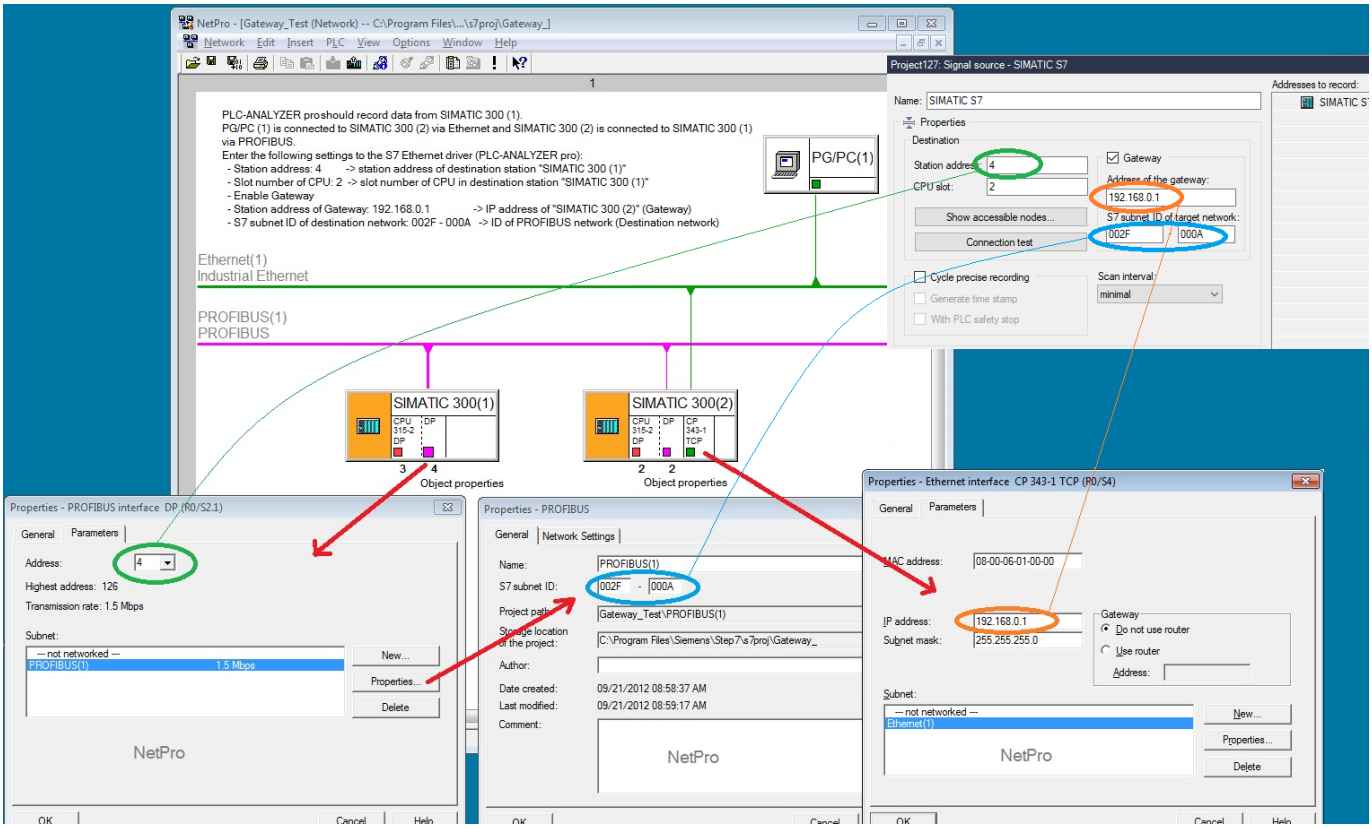

Fig. 1-2 Settings Gateway

Under *Scan interval* you specify the time interval at which measured values are read out from the PLC. A longer sampling interval can be selected for signal paths that are not time-critical, e. g. temperature. As a result, the generated signal files become smaller.

To ensure that even very short signal changes are reliably detected, activate *Cycle-precise recording*.

Under *Symbols,* select a STEP 7- or TIA project to make the symbols of this project available for address selection. Alternatively you may import the symbols directly from a S7-1500/S7-1200 CPU. For this click on the button . With the imported symbol list you can use symbolic identifiers when entering addresses. In addition to the absolute address, the symbolic identifier and comment are also displayed and stored in a signal- or project file.

After setting the communication properties, add the PLC signals to be recorded. When a STEP7 or TIA project is loaded, the signals to be recorded can be conveniently selected from the symbol list by double-click or drag and drop.

Data acquisition

Supported PLC models and CPUs

The SIMATIC S7-Driver supports the CPUs of SIMATIC S7-200, S7-300, S7-400, S7-1200, S7-1500, M7, C7, SINUMERIK ONE / S7, SAIA xx7, VIPA S7 and S7-PLCSIM.

Recordable PLC addresses

The following table shows the recordable addresses and the corresponding address syntax:

Syntax	Type of address	Example
Qx.z	Output byte x, bit z	Q32.4
QBx	Output byte x	QB9
QWx	Output word x	QW14
QDx	Output double word x	QD98
Ix.z	Input byte x, bit z	I17.0
IBx	Input byte x	IB127
IWx	Input word x	IW12
IDx	Input double word x	ID124
Fx.z	Flag byte x, bit z	F3.7
FBx	Flag byte x	FB250
FWx	Flag word x	FW24
FDx	Flag double word x	FD134
FBx	Flag byte x	FB250
Tx	Timer x	T2
Cx	Counter x	C5
DByDBXx.z	Data byte x, bit z from data block y	DB23DBX2.5
DByDBBx	Data byte x from data block y	DB2DBB5
DByDBWx	Data word x from data block y	DB12DBW5
DByDBDx	Data double word x from data block y	DB27DBD0
PIB x	Peripheral input byte x	PEB 231
PID x	Peripheral input double word x	PED 304

Table 1-1: SIMATIC S7 address syntax

Number of recordable addresses

A maximum of 16 million addresses can be acquired from up to 250 signal sources.

Time behaviour and particularities

NOTE

Acquiring data with PLC-ANALYZER pro 6 results in a small increase in cycle time in the automation device to the same extent as with STEP7/TIA in the monitor operating mode.

In the TIA Portal, the value for the CPU property "*Communication load - Cycle load due to communication*" should not be set too high. To keep the cycle time extension as low as possible, the value 20% is recommended here.

The intervals between scan transfers from the SIMATIC PLC to the computer depend on the PLC-CPU, the number of acquired signals and kind of connection. In addition, the scanning distance is influenced by the size of the network and the selected transmission speed.

With an S7-300, the scan distance for acquisition via MPI/PROFIBUS for one byte is approx. 25-30 ms, i.e. from a cycle time > 30 ms, one scan is received for each cycle. With each additional byte acquired, the scan distance increases by about 2 ms.

A scan interval of at least 1 ms can be achieved for the detection of an S7-1500 via PROFINET/Industrial Ethernet (TCP/IP).

Cycle-precise recording

> **WARNING**
>
> The PLC ANALYZER pro 6 programs a small addition to the PLC program in the controller for cycle-precise acquisition. We would like to point out that an influence of this modification on the mode of operation of the PLC or the PLC program cannot be completely excluded.

The cycle-precise signal acquisition enables the continuous measurement of selected signals in each PLC cycle without gaps.

With cycle-accurate signal acquisition, a limited number of signals are pre-measured within the PLC. The selected signals are stored in the memory of the PLC in each PLC cycle and transferred to the PC by means of intelligent procedures in such a way that continuous cycle-accurate acquisition is possible.

As a user, you do not see any visible difference from the normal recording. Even live display is possible as usual.

Cycle-precise signal acquisition is available for many controllers of the S7 family.

Configuration of PLC-driver for cycle-precise acquisition

In the *Settings* window of the S7 driver, activate the *cycle-precise acquisition.*

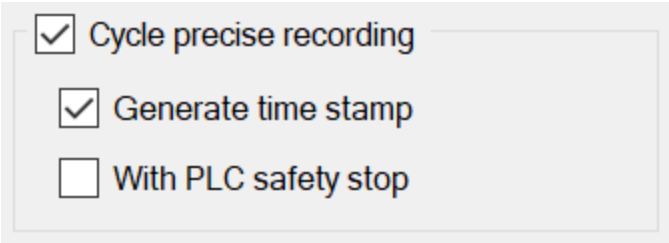

Fig. 1-3 Cycle-precise acquisition (SIMATIC S7)

For recording of very brief signal changes, activate *Cycle-precise recording*.

Generate time stamps is used to provide the data with time stamps during cycle-precise recording. Deactivate this option if you have so much data to record that data loss cannot be prevented. In this case no time information is available during the signal analysis.

You also specify here whether the PLC is to be stopped for safety reasons before and after the transfer of the data blocks.

> **NOTE**
>
> If more addresses are stored to the memory than can be read from the PLC at one time, an overflow of the circular memory will occur and data will be lost. This can be avoided by reducing the number of addresses to be recorded.

Input of addresses

Up to 200 addresses (byte-, word- or double word-values) can be acquired simultaneously in the cycle-precise acquisition mode. This restriction is the result of the restricted memory capacity of the PLC and the transmission speed of the MPI-, PROFIBUS- or Ethernet-Interface. If the number of signals to be recorded is too large, a recording of the data without gaps is not guaranteed in every case. The number of addresses that can be recorded without gaps depends on the following factors:

- Cycle time of the PLC program
- Transmission speed of the Interface
- Recording with/without time stamp

With an S7-300 (CPU315-2 DP), for example, with a cycle time of 10 ms, about 50 bytes can be recorded without gaps.

Start acquisition

> **!** **WARNING**
>
> It is essential to ensure that the system is brought into a safe condition before the modification for cycle precise recording is carried out. If " *With PLC safety stop*" is set, the PLC-ANALYZER pro 6 switches the controller to the STOP state for a short time to transfer or modify the blocks. The process after the end of the recording is analogous.

Now start the Acquisition. Depending on the default settings you have selected in the *Settings* window of the PLC driver, the blocks are transferred either during operation or after the controller has been stopped. One of the following message windows appears:

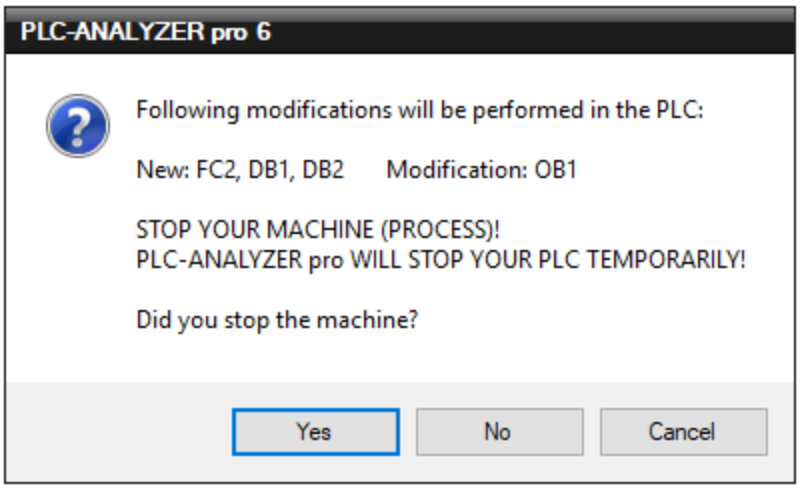

Fig. 1-4 Message before modifications in the PLC for pre-setting „With PLC safety stop“

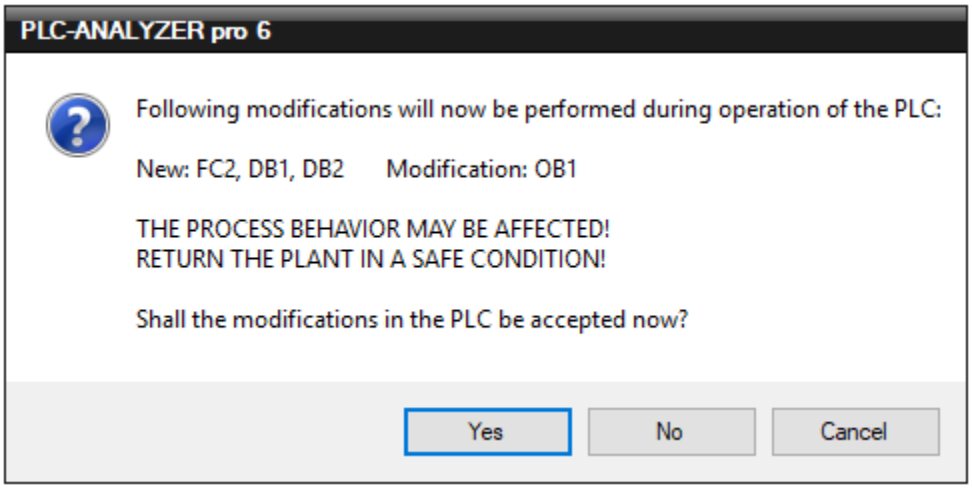

Fig. 1-5 Message before modifications in the PLC for pre-setting „No PLC safety stop“

Confirm with *Yes* only after you have stopped the process or if it is in a safe state. Make sure that damages to person or property by impairment of the function of the control is impossible!

The PLC-ANALYZER pro 6 searches for free block numbers in the PLC and generates one function block and two data blocks for data recording. In addition, a call to the new function block is added to the end of OB1.

The controller is in the RUN state or is now switched back to the RUN state. The cycle-precise acquisition begins. The signal changes are now displayed live on the screen.

Recording is stopped with *Stop acquisition*. You should now stop your system (process) or bring the system into a safe condition. Removal of the modifications is now done analogously in the STOP state or online. One of the following message windows will appear:

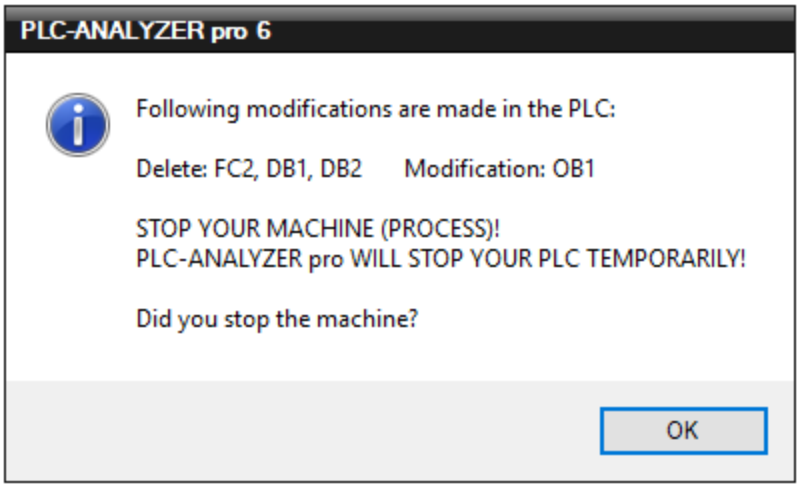

Fig. 1-6 Message before modifications in the PLC for pre-setting „With PLC safety stop“

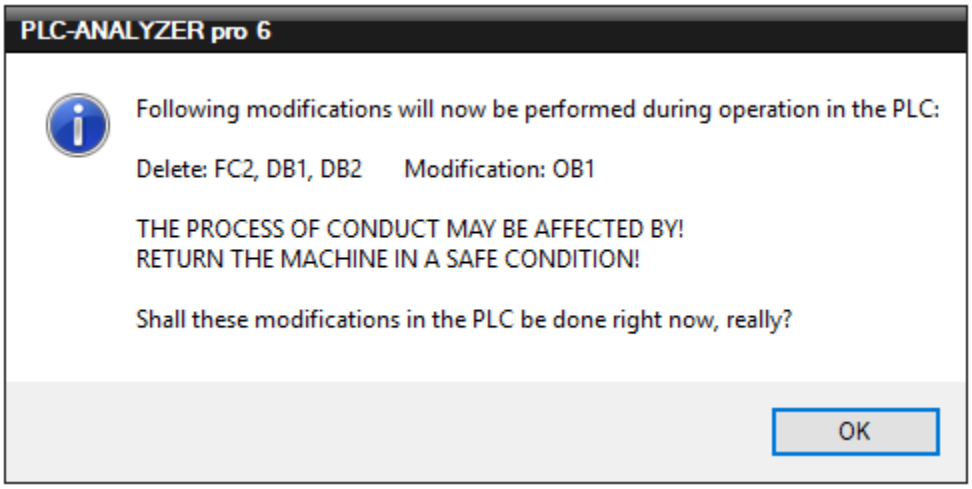

Fig. 1-7 Message before modifications in the PLC for pre-setting „No PLC safety stop“

Confirm the message after you have stopped your system or bring it into a safe condition. The original state in the PLC is restored now.

After the end of acquisition, the last signal file created is automatically opened for display.

Particularities in signal display and analysis

The evaluation of signal files acquired with cycle accuracy is practically identical to that of normal signal files. However, if no time stamp is generated during recording (see configuration of the S7 driver), no time is assigned to the data. In this case, the time is specified in cycles. The time base here is "ZP" (cycles per pixel).

Example: With a set time base of 0.1 ZP, a PLC cycle is displayed over 10 screen pixels.

If more addresses are recorded than can be continuously read from the PLC, the PLC ring buffer overflows. This causes data to be lost. These recording gaps during acquisition are displayed as a grey line.