SH ARCALYZER
Tutorial (english)

SOHARD
EMBEDDED SYSTEMS

Examples for using SH ARCALYZER

SH ARCALYZER is a multifunctional and powerful tool for analyzing and debugging ARCNET networks as well as networks related to or based on ARCNET (e.g. EC-Net, PDnet, BACnet etc.).

This tutorial describes several use cases where SH ARCALYZER will come in handy.

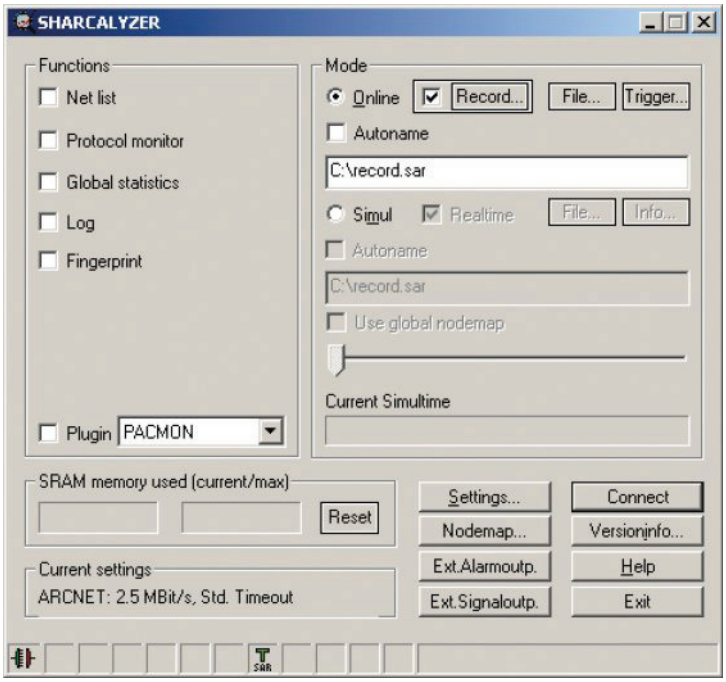
Selecting Function Windows:

SH ARCALYZER offers plenty of functions to examine and troubleshoot ARCNET networks. It may also be used to document the structure of a network.

The following general approach is recommended for debugging:

1. Start the SH ARCALYZER software
2. Adjust in *"Settings…"* in the main window the bit rate and the extended timeout settings..
3. Connect the ARCNET interface of SH ARCALYZER to the network. Take care if a termination resistor is needed.
4. Click on *"Connect"*.
5. The status line should now show basic information on the network.
6. When there is no activity indicated, the network may be inactive or SH ARCALYZER may not be correctly connected to the network.

The following use cases are intended to help you with doing service, maintenance and troubleshooting.



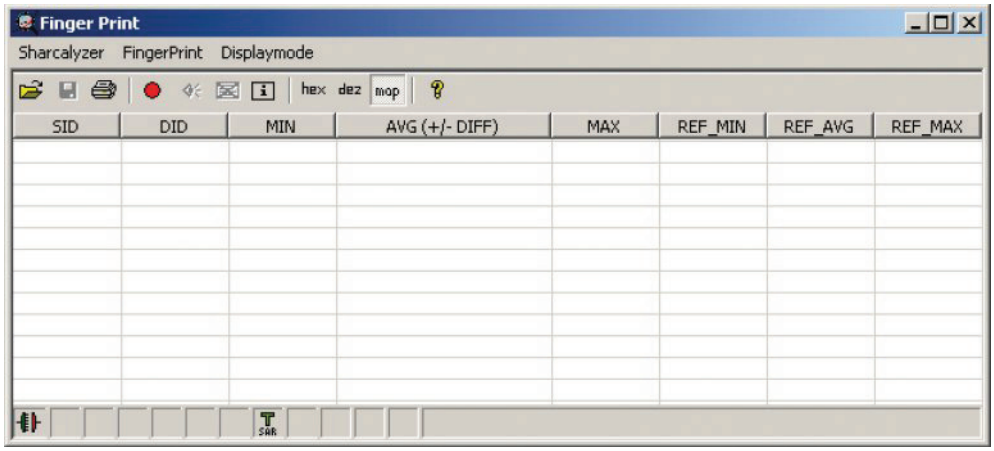
Use case:
How to take the fingerprint of a network

Background:

The characteristic of the network may be captured and documented by means of a so-called fingerprint. This allows you to detect manipulations of the network later in time. Note that fingerprint comparison only works when fingerprints are recorded at the same point in a network. An appropriate point is e.g. an unused plug of a hub as there is a lower risk of disturbing the data traffic.

Procedure:

1. Start the SH ARCALYZER software and activate in *"Settings…"/"More…"* in the main window the checkboxes *"ITT always on"* and *"ITT FIRST NODE always on"*.
2. Establish a link to the network clicking on *"Connect"* and activate the checkbox *"Fingerprint"*. The function window *"Fingerprint"* will open.
3. Start the fingerprint recording by clicking on the red button. The button will return to start position when the recording is complete.
4. Save the fingerprint. The application will demand you to describe the network and the point in the network where the fingerprint was recorded.
5. Add the storage medium containing the fingerprint to the network documentation for the costumer as well as for your own usage. A hardcopy of the fingerprint may also be filed.



Tip:

Note down the point in the network where the fingerprint was recorded in the network diagram for later references.

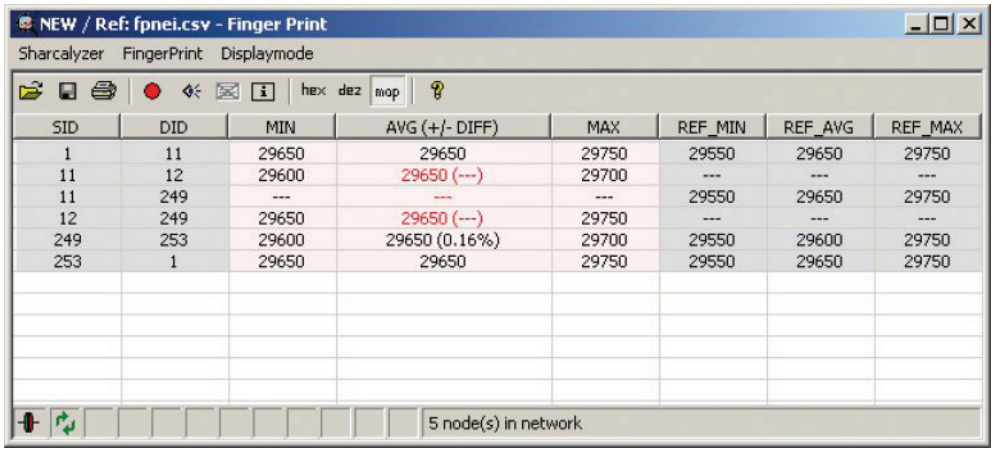
Use case:
How to check a network's fingerprint

Precondition:

A reference fingerprint of the network was recorded and filed at a earlier point in time (e.g. before delivery to the costumer).

Procedure:

1. Insert the storage medium containing the reference fingerprint into the PC SH ARCALYZER is connected to. Connect the analyzer's ARCNET interface to same point where the reference fingerprint was recorderd, otherwise the new fingerprint will differ from reference one.
2. Start the SH ARCALYZER software and activate in *"Settings…"/"More…"* in the main window the checkboxes *"ITT always on"* und *"ITT FIRST NODE always on"*.
3. Activate the checkbox *"Fingerprint"*. The function window *"Fingerprint"* will open.
4. Load the reference fingerprint using *"Load…"* in the menu *"Fingerprint"*. By clicking on *"Fingerprint"/"Fingerprint Info"* you may look in the field *"Meas. Location"* for the point in the network where the footprint was recorded. Even if you know this point you are encouraged to look it up.
5. Unless you already did so, connect the analyzer's ARCNET interface to this reference point in the network.
6. Establish a link to the network by clicking on *"Connect"* in the main window or on the connector symbol in the down left corner of any window and start the recording of the network's current fingerprint by clicking on the red button. The button will return to its start position when the recording is complete.
7. By calling *Fingerprint/Compare…* the comparison of the two fingerprints is started. If the fingerprints are matching the message *"No differences found!"* is displayed and the columns *MIN*, *AVG* and *MAX* will be pastel green, otherwise the message will run *"The Fingerprints are different"*, the columns being pastel red.



SID	DID	MIN	AVG (+/- DIFF)	MAX	REF_MIN	REF_AVG	REF_MAX
1	11	29650	29650	29750	29550	29650	29750
11	12	29600	29650 (---)	29700	---	---	---
11	249	---	---	---	29550	29650	29750
12	249	29650	29650 (---)	29750	---	---	---
249	253	29600	29650 (0.16%)	29700	29550	29600	29750
253	1	29650	29650	29750	29550	29650	29750

Use case:
How to find changes in a network

Background:

The fingerprint of a network documents its characteristics and consists of the list of token runtimes between logically neighboring nodes. These times result from the lengths and specific signal speeds of the transmission lines and the signal through put times of hubs and repeaters.

Procedure:

1. Proceed as described in the use case “How to check a network’s fingerprint”.

The reference fingerprint and the current fingerprint will be displayed in a spreadsheet:

The first two columns list the sender and the destination node of the token.

The next three columns list the minimum, average and maximum runtime of the tokens for the current network.

The AVG column will also show runtime differences between the fingerprints or “---” when the nodes differ in ID or number.

The last three columns list the minimum, average and maximum runtimes of the tokens as recorded in the reference fingerprint.

2. In case the two fingerprints differ this may be owed to the following causes:

a. Different runtimes may occur when the lengths of transmission lines are changed or hubs or repeaters are replaced by devices featuring different signal through-put times. The percentage of the runtime differences is displayed in the AVG column. If they are considerably high the information will be displayed in red.

b. If nodes differ in ID or number because nodes have been removed, added or given different IDs, the SID/DID combinations will not match. Three dots in the runtime cells indicate that a SID/DID pair is not listed either in the current or the reference fingerprint. In the example shown the node 12 has been added to the network:

Old sequence (from reference fingerprint): 1 > 11 > 249 > 253 > 1

New sequence (from current fingerprint): 1 > 11 > 12 > 249 > 253 > 1

If the number of nodes match in both fingerprints one or more nodes may have changed their IDs.

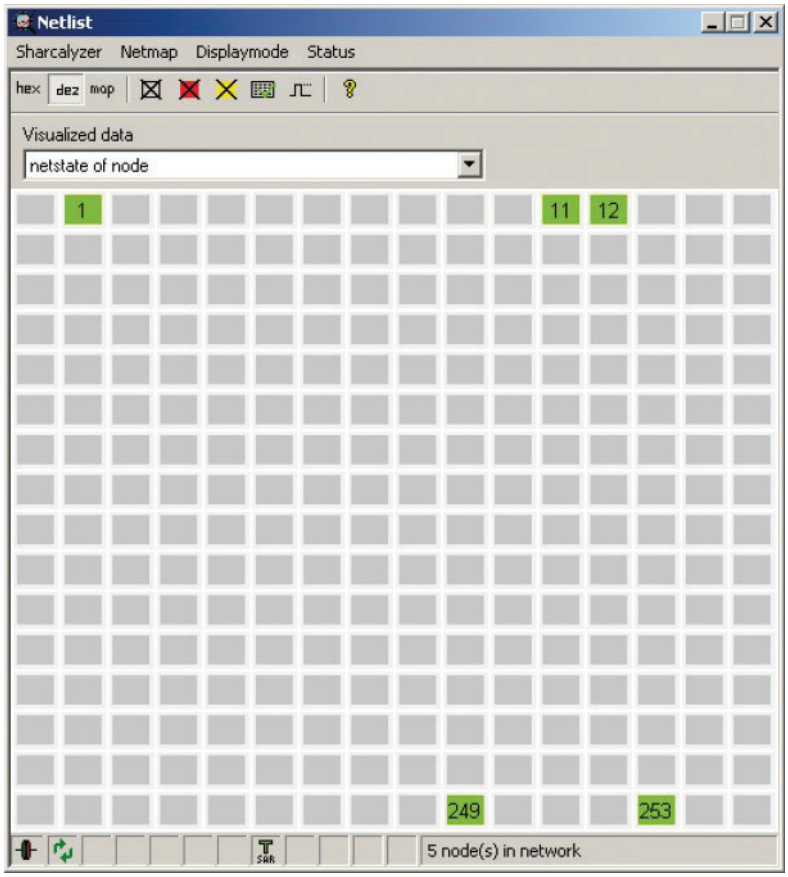
Use case:
Instable network

Background:

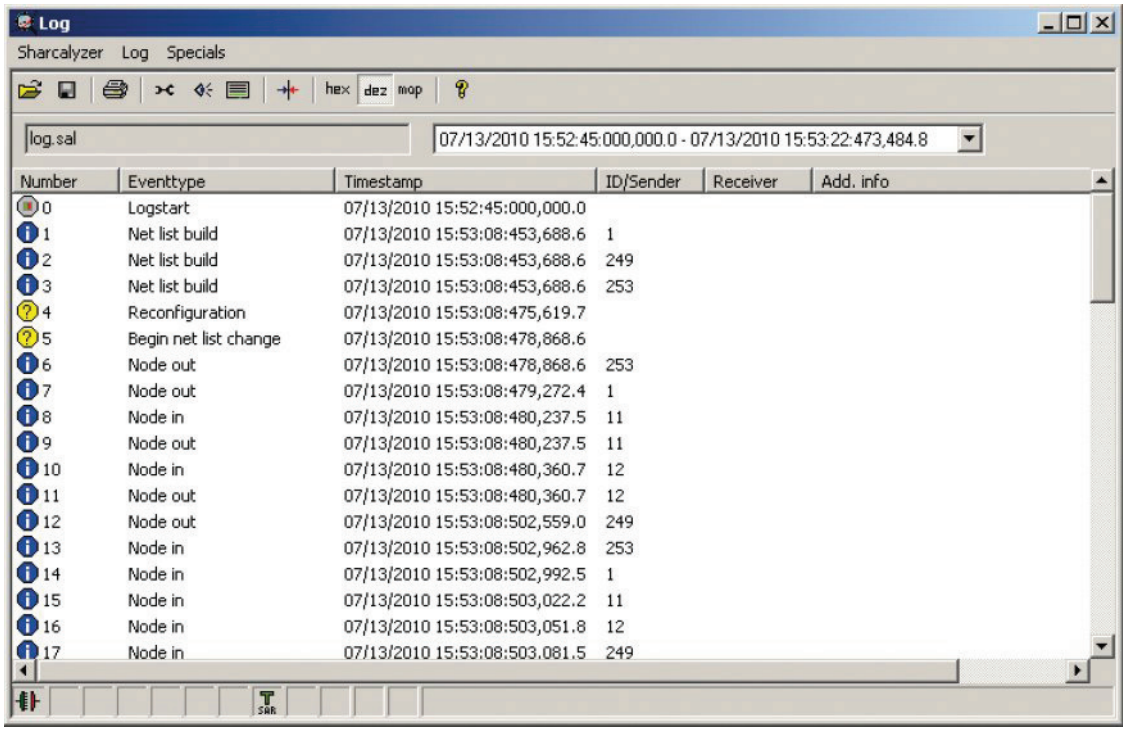
Data transmission in a network is delayed and the LEDs of ARCNET nodes and hubs indicate irregularities.

Procedure:

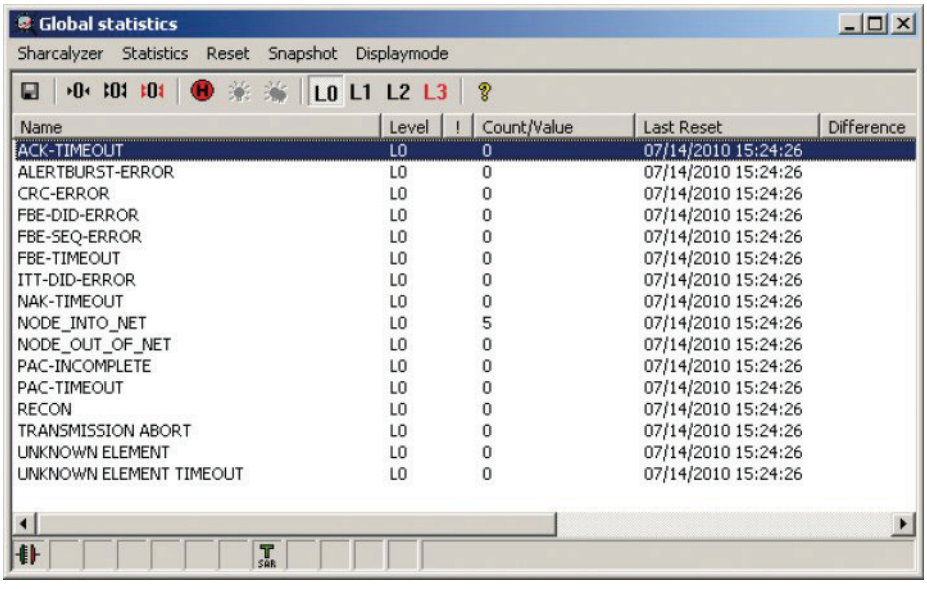
1. Activate the function *Keep changes* in the function window *"Net List"*. If a node ID is displayed yellow the respective node has left or entered the network.



2. Watch the entries in the function window *"Log"*. Do nodes enter and leave the network without reason? How often does this occur?



3. Watch the level L0 counter in the function window *"Global Statistics"*. In stable networks the counters remain at zero with exception of NODE_INTO_NET which should remain at its starting value.



Use case:
Sporadic network failures

Background:

If there are sporadic failures in a network, it is recommended to run a long-term surveillance with SH ARCALYZER. Owing to the resulting amount of data it is advised not to record the complete data traffic during this time, but to pick out short periods which the failures occur in.

Procedure:

1. Initiate a triggerd recording of a limited number of ARCNET elements in *"Trigger…"* in the *SH ARCALYZER* main window.

   Activating Multitrigger you can force a recording every time the trigger event occurs.

   Recommend events are RECON, UNKNOWN, alertburst error, PAC with CRC error. It may be convenient to record 1000 elements before (Pretrigger) and after (Posttrigger) the event.

2. After adequate time (depending on the watch the entries in the function window *Log*:

a. Do nodes leave or enter the network unexpectedly? By means of the network diagram you may locate segments causing the failures. Causes for such dysfunctions may be disruption of supply power or loose connections in cables or connectors.

b. When do RECONs, UNKNOWNs or alertburst errors occur? Is there an obvious cycle of occurrence? Are there events in the proximity of the network like shock or vibration or electromagnetic disturbances caused by big relays or starting engines or service personnel?

Use case:
Data loss

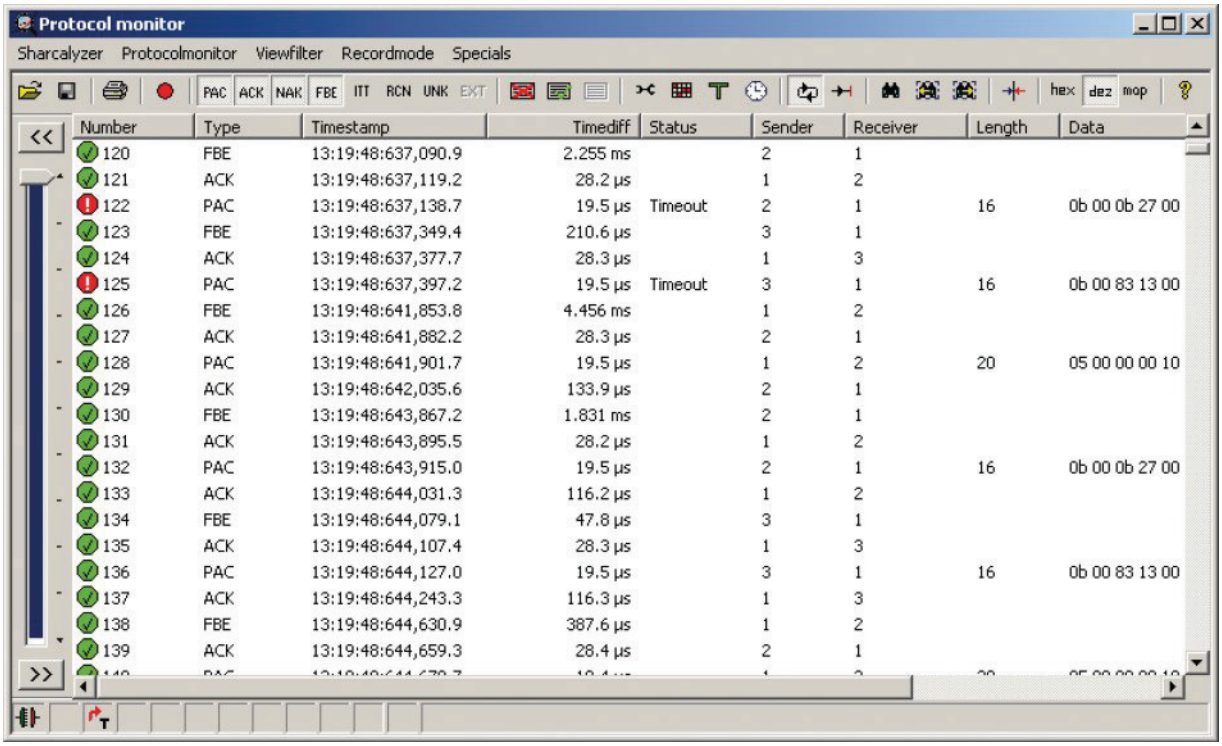
Background:

Data is lost in a network.

Procedure:

1. Start a (multi)triggered recording as described in the use case ”Sporadic network failures”. Recommendable trigger events are timeouts, PACs with CRC error and UNKNOWNs. Activate the elements FBE, PAC, NAK and ACK in Specials/Recording filter in the function window *”Protocol Monitor”*.
2. Is the data expected transmitted and acknowledged by ACK?

The sending nodes end their attempts to transmit after a defined number of tries which can be adjusted. Check in the *”Net List”* whether the addressed nodes do exist. It may be possible that nodes have been given other IDs.



Number	Type	Timestamp	Timediff	Status	Sender	Receiver	Length	Data
120	FBE	13:19:48:637,090.9	2.255 ms		2	1		
121	ACK	13:19:48:637,119.2	28.2 µs		1	2		
122	PAC	13:19:48:637,138.7	19.5 µs	Timeout	2	1	16	0b 00 0b 27 00
123	FBE	13:19:48:637,349.4	210.6 µs		3	1		
124	ACK	13:19:48:637,377.7	28.3 µs		1	3		
125	PAC	13:19:48:637,397.2	19.5 µs	Timeout	3	1	16	0b 00 83 13 00
126	FBE	13:19:48:641,853.8	4.456 ms		1	2		
127	ACK	13:19:48:641,882.2	28.3 µs		2	1		
128	PAC	13:19:48:641,901.7	19.5 µs		1	2	20	05 00 00 00 10
129	ACK	13:19:48:642,035.6	133.9 µs		2	1		
130	FBE	13:19:48:643,867.2	1.831 ms		2	1		
131	ACK	13:19:48:643,895.5	28.2 µs		1	2		
132	PAC	13:19:48:643,915.0	19.5 µs		2	1	16	0b 00 0b 27 00
133	ACK	13:19:48:644,031.3	116.2 µs		1	2		
134	FBE	13:19:48:644,079.1	47.8 µs		3	1		
135	ACK	13:19:48:644,107.4	28.3 µs		1	3		
136	PAC	13:19:48:644,127.0	19.5 µs		3	1	16	0b 00 83 13 00
137	ACK	13:19:48:644,243.3	116.3 µs		1	3		
138	FBE	13:19:48:644,630.9	387.6 µs		1	2		
139	ACK	13:19:48:644,659.3	28.4 µs		2	1		

Use case:
Data inspection

Background:

You want to inspect the content of transmitted data packets (PACs).

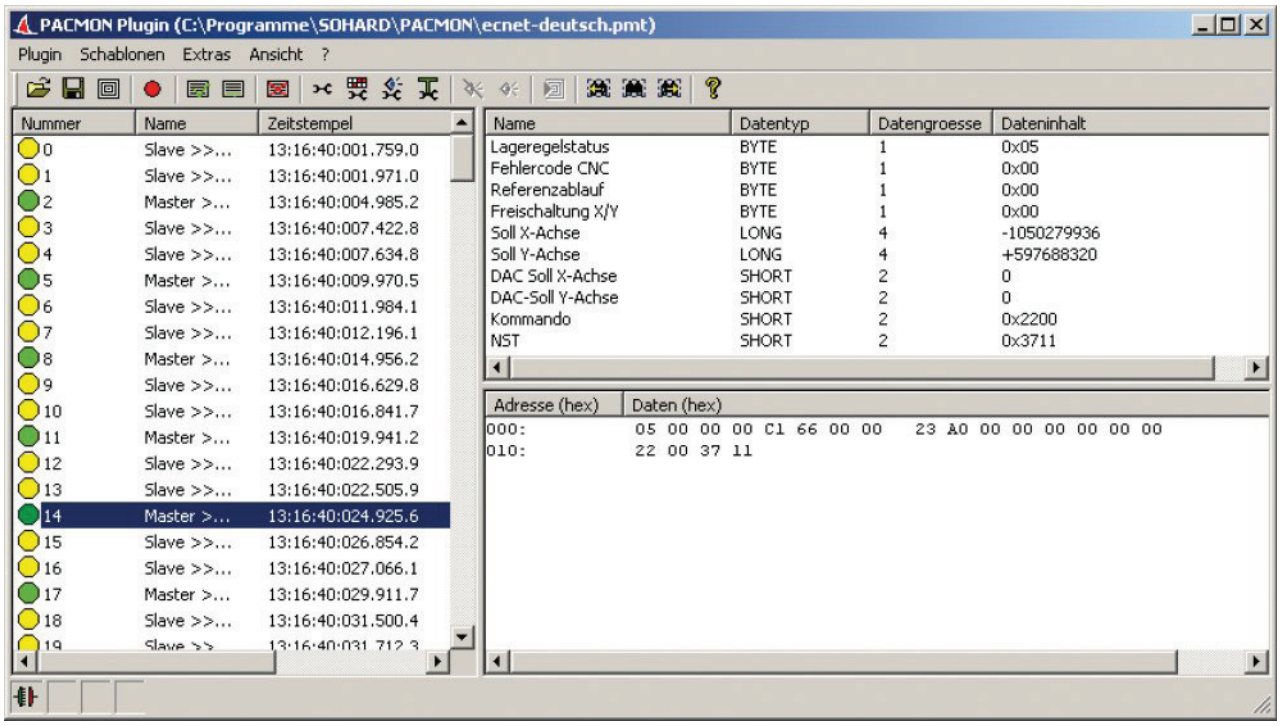
Procedure:

1st case: You want to have a general look on the content of transmitted data packets:

1. Open the function window *"Protocol Monitor"*.
2. Select the element PAC in the recording filter and the view filter. If necessary initiate a triggered or time controlled recording.
3. Start the protocol monitor recording using the red button. Depending on your settings the recording will stop automatically or has to be manually stopped.
4. Double-clicking on a PAC element will display its content as hexdump or decimal-dump and in ASCII.

2nd case: You want to inspect special data packets having a given structure or containing given data:

1. Open the *Plug-in PACMON*. Select a suitable template set (if necessary create a template yourself), which describes the structure or the content of the desired packets.
2. If necessary select recording options, view options and trigger.
3. Start the recording by clicking on the red button in the plug-in window and establish a link to the network by clicking on *Connect* in the main window.
4. Clicking on a PAC element in the PACMON listing will display its content structured according to the selected templates and as hexdump or decimal-dump in right PACMON windows.



Subject to technical changes and printing errors excepted.
Release: August 2010