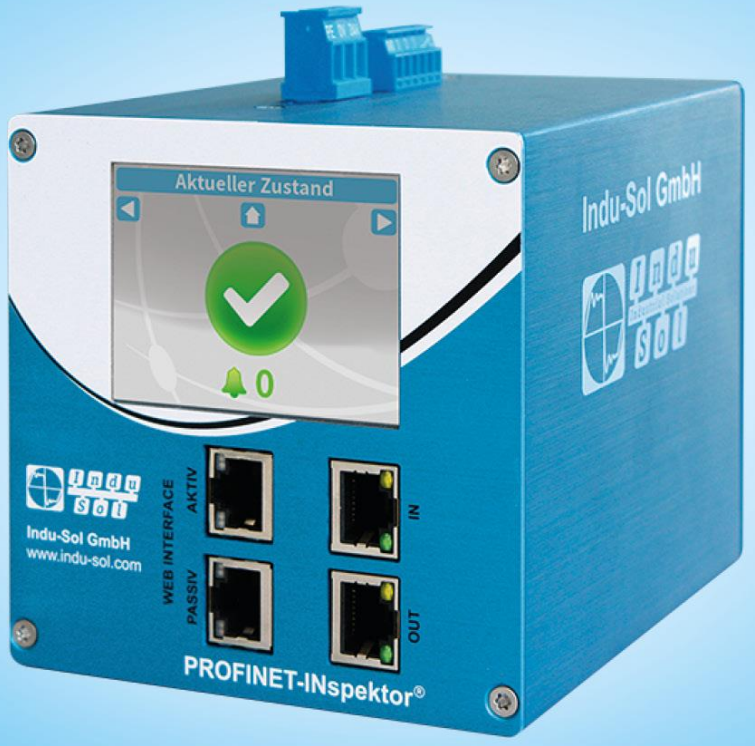
Indu-Sol GmbH – Specialist in Industrial Networks

PROFINET-INspektor® NT

User Manual



Diagnostic and service tools for PROFINET

PROFIBUS PROFINET INDUSTRIAL ETHERNET CAN DeviceNet SafetyBUS p ASi INTERBUS EMC WIRELESS

Indu-Sol GmbH

Blumenstraße 3

D-042626 Schmölln

Phone: +49 (0)34491 / 580-0

Fax: +49 (0)34491 / 5818-99

Email: info@indu-sol.com

Web: https://www.indu-sol.com

Our **technical support** team is available at +49 (0)34491 / 580 321, weekdays between 7:30 – 16:30 (CET). You can also email us at: support@indu-sol.com

Is your plant standing still? You can reach our emergency service around the clock at: +49 (0)34491 / 580 0.

Revision overview

Date	Revision	Change(s)
10/09/2015	0	First version
04/07/2016	1	Firmware Update 1.4
22/12/2016	2	Firmware Update 1.5
10/05/2019	3	Firmware Update 2.0
15/05/2020	4	Firmware Update 2.1
27/10/2021	5	Firmware Update 2.2
10/08/2022	6	Firmware Update 2.3
03/11/2023	7	Firmware Update 2.4
27/06/2024	8	Firmware Update 2.5

W A R N I N G

Commissioning and operation of this device must only be performed by qualified personnel. Qualified personnel within the meaning of the safety notices in this manual are persons authorised to commission, ground, and mark devices, systems, and circuits in accordance with safety engineering standards.

Improper use or configuration of the ***PROFINET-INspektor®*** in the network may cause severe physical injury as well as property and material damage, also due to uncontrolled machine movements.

Contents

1 General information

Please read this document thoroughly from start to finish before you begin installing the device and putting it into operation.

1.1 Purpose of use

The PROFINET-INspektor® NT permanently monitors all data traffic in a PROFINET (PN) master system. You will receive a maintenance requirement notification when critical changes that could lead to unplanned system downtimes are detected.

Based on the report analysis (purely passive behaviour), the following quality parameters are monitored:

- Update rate
- Error telegrams (sent/received)
- Alarms (low and high priority)
- Telegram gaps
- Telegram overtakes
- Bus node failure
- Bus node restart
- Jitter
- Netload (sent/received)

One PN-INspektor® NT is required per PROFINET master system. This PN-INspektor is looped into the connection between the IO controller (PLC) and the first device (switch) for analysis or integrated within the network through a feedback-free measurement point (e.g. PNMA II; art. no. 114090100).

No additional IP addresses or adjustments to the PLC program are required for using the PN-INspektor® NT. It works in an entirely manufacturer-independent way, i.e. the analysis works completely independently of the type of control system and IO devices.

For long-term analysis, the PN-INspektor® NT can remain in the bus system without any time restrictions. The relevant telegram traffic is continuously analysed and evaluated to detect deviations from normal conditions and trigger alarms.

1.2 Use of Open-Source Licenses

Indu-Sol offers to provide source code of software licensed under the GPL or LGPL or other open-source licenses requiring source code distribution. The individual licenses used in Indu-Sol products can be found in the product front ends.

1.3 Scope of supply

The scope of supply comprises the following individual parts:

- PROFINET-INspektor® NT
- 3-pole plug-in terminal block (power supply)
- 6-pole plug-in terminal block (alarm contacts)
- User Quick Start Guide

Please check the contents are complete before putting into operation.

1.4 General safety instructions

1.4.1 Operating personal

This device may only be put into operation and operated by qualified personnel. Qualified personnel, as referred to in the safety-related information of this manual, are persons who are authorised to put into operation, to earth and to label devices, systems and electrical circuits in accordance with the standards of safety engineering.

1.4.2 Power supply

The devices are designed for the operation with SELV-voltages (Safety Extra Low Voltage) via LPS (Limited Power Source). Only SELV/LPS conformal extra-low voltages according to IEC 60950-1 / EN60950-1 / VDE0805-1 as well as power packs for voltage supplies according to NEC Class 2 (National Electrical Code) may be used.

The shield of the RJ45-socket is connected to the device housing for dissipating interferring currents. Note possible short circuits when using shielded cables.

1.4.3 Utilization of PROFINET-INspektor® NT

Do not open the housing of the device. The warranty expires when the housing is opened. The device should be sent back to the supplier in case of any defects. There are no components in the devices, which could be maintained by the user.

1.4.4 Intended use

The devices are designed for use in the industrial sector in the protection class IP20. These must therefore not be connected directly to the public low-voltage network. The installation must be carried out in an industrial control cabinet. The industrial control cabinet may be located at a maximum height of 3000 meters.

1.4.5 Batteries

Caution: Risk of Explosion if Battery is replaced by an Incorrect Type. Dispose of Used Batteries According to the Instructions

2 Installation

2.1 Device interfaces

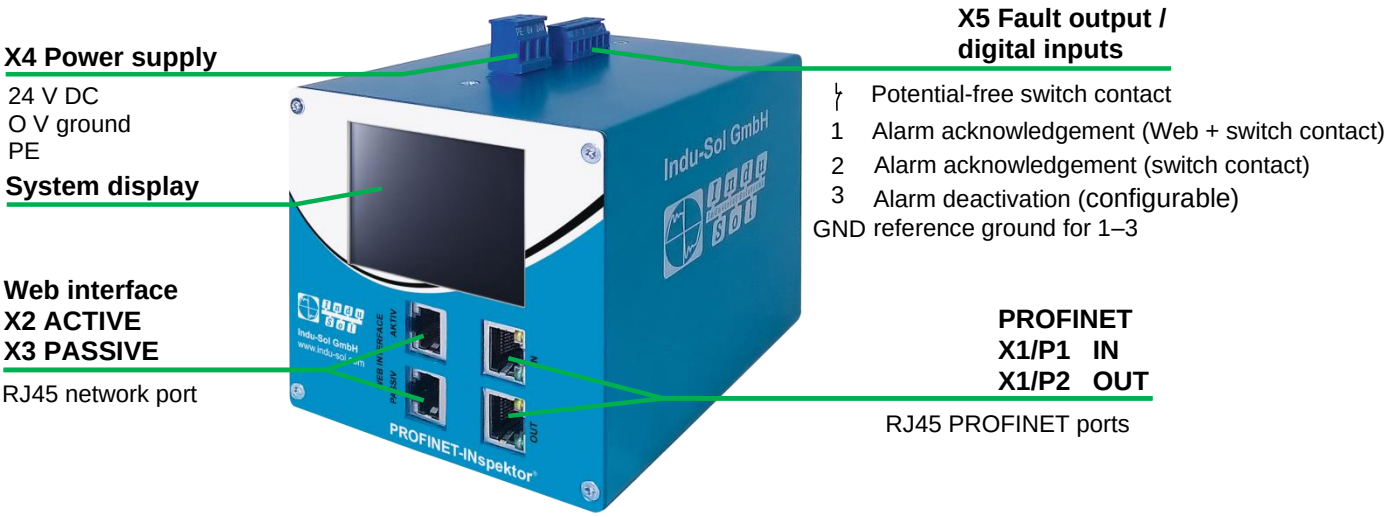


Figure 1: Device ports

2.2 Installation instructions

PROFINET-INspektor® NT is installed horizontally inside the cabinet on a 35 mm top-hat rail in accordance with DIN EN 60715.

Figure 2: Device installation on top-hat rail

Caution: The following distances must be maintained from other modules for correct installation:

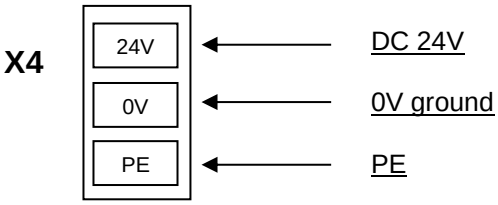
- From left and right: 20 mm
- From top and bottom: 50 mm

Removal for alternate use of the PN-INspektor® NT in different master systems is illustrated in Figure 3.

Figure 3: Removal

2.3 Voltage supply

Operation requires 24 V of external direct current, which is to be connected to the device via the 3-pole plug-in terminal block (X4) supplied in the package. The PE contact should be connected to the local PE system.



Caution: When connecting, make sure that the polarity is correct.

2.4 Measurement location

Wherever possible, the PN-INspektor® NT should always be installed in the network connection between the PLC and the first I/O device or switch, since the majority of communication typically takes place via this connection.

2.5 Connection to the PROFINET network

You can connect to the PROFINET network in different ways. The various options are described below.

2.5.1 Fixed installation within the master system

The PN-INspektor® NT is firmly integrated into the network for continuous, permanent network analysis. To do this the device is integrated into the system via the IN and OUT sockets.

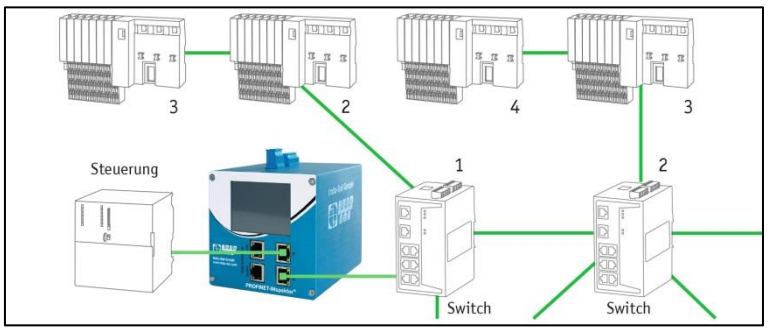


Figure 4: PROFINET-INspektor® NT fixed installation

Caution: Installing the device with this connection option causes a PROFINET network fault and should be performed during system standstill.

2.5.2 Connection via feedback-free measurement point

In conjunction with a feedback-free measurement point (e.g. PNMA II; art. no. 114090100), PN-INspektor® NT can be connected to the PROFINET-system at any time without compromising ongoing system operation. This can also be performed on a temporary basis if required. To do this, the PN-INspektor® NT is hooked up to the M1 and M2 monitor sockets of the measurement point by means of two patch cables.

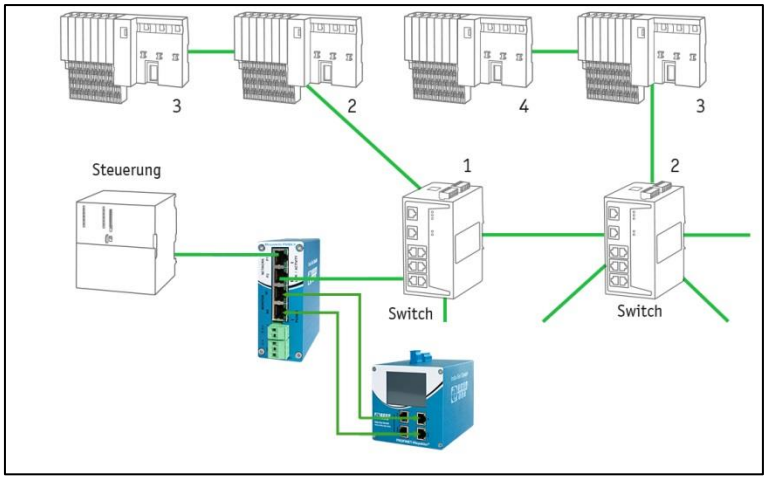


Figure 5: PN-INspektor® NT connection via PNMA II

2.6 Web interface

The LAN connections X2 and X3 of the web interface constitute the link to the PN-INspektor® NT. This involves 10Base-T/1000Base-T RJ45 interfaces. A standard Ethernet cable is used as a connection cable to a PC/ laptop (not included in the scope of supply).

A Web-server function is integrated for access to the device and can be opened with an appropriate standard browser (e.g. Microsoft Internet Explorer from version 11 or Mozilla Firefox from version 45; JavaScript must be activated). You can reach the device's user interface by entering the IP address of the PN-INspektor® NT in the browser's command line.

Caution: To display the website correctly, the following ports must be enabled in firewalls, gateways and routers: TCP/80 (http) and TCP/443 (https).

The PROFINET-INspektor® NT is supplied with the following factory-set network configuration:

	PASSIVE – X2	ACTIVE – X3
IP address:	192.168.212.212	192.168.213.212
Subnet mask:	255.255.255.0	255.255.255.0

Both the evaluation of internally recorded data and the parametrisation of the device are possible through the **PASSIVE** and **ACTIVE** connection sockets. These are two independent network access. Additional to the web access the active web interface can send requests to the PROFINET Network. For this it is necessary to start a "Device scan" in the Device overview. This is used to retrieve and store information such as the name, IP address and network topology for the respective device.

The active port must be configured to a free IP address from the PROFINET system to be scanned (see section 3.5.1.6 Network) and integrated into the network (e.g., via a free switch port).

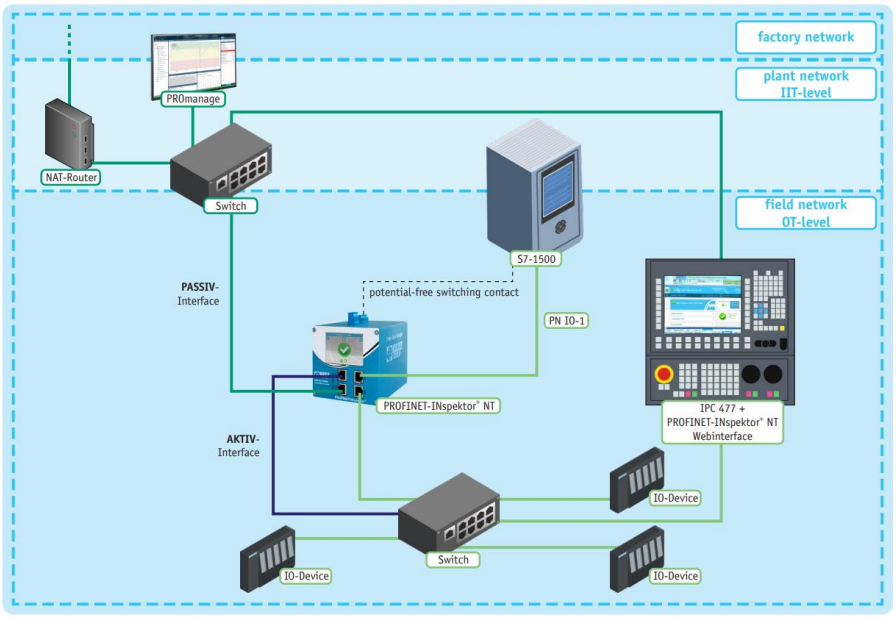
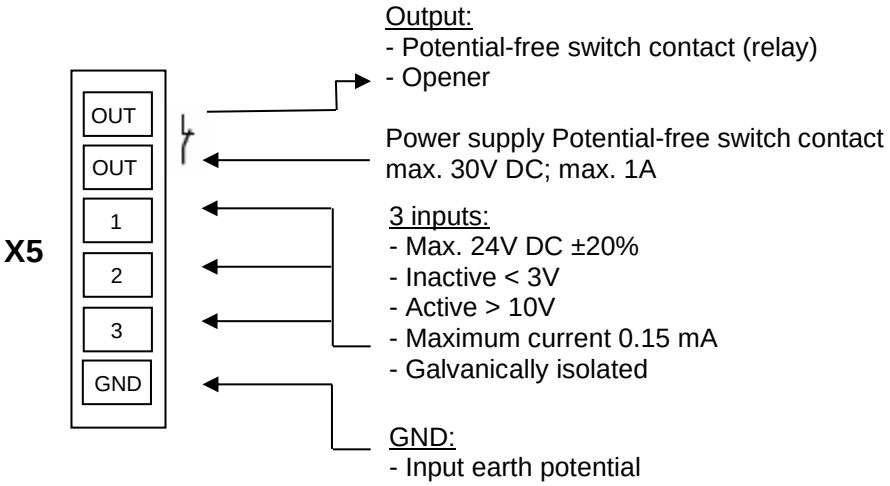


Figure 6: Active / Passive web interface

2.7 Signal inputs and outputs

The 6-pole connector terminal block (X5) at the top of the device is assigned as follows:



Input 1: Alarm acknowledgement (Web interface + switch contact)

Input 2: Alarm acknowledgement (switch contact)

Input 3: Alarm deactivation

Additional functions can be configured via the Web interface (see point 3.5.1.7 Digital Input)

2.8 Display screen

After connecting the power supply, the display conveys the system start-up of the PN-INspektor® NT. After successful system start-up, the current state of the PROFINET network is always displayed on the home screen. You can scroll between the menu items with the arrow keys on both sides. The Home key takes you directly to the home screen.

The pending alarms are acknowledged by longer pressing (> 5 s) on the status symbol.

Figure 7: Touch-Screen menu

3 Web interface and selection functions

To access the Web interface, and thus the recorded data of the PN-INspektor® NT, use an Internet browser and enter the IP address (PASSIVE: 192.168.212.212; ACTIVE: 192.168.213.212) of the device to open the web interface.

The following icons were used in the Web interface for a simple overview of the individual statuses of the network and devices:

No faults: PROFINET communication is working without any problems.

Warning: A communication fault or a diagnostic message has appeared in the network, or originated from a device, and this fault or message has not yet led to system failure. The sources of these events should be localised and resolved.

Fault: A critical fault has appeared in the network, or originated from a device, and this fault leads to system failure. It is urgently necessary to resolve the fault.

The bus communication in the network has failed or cannot be detected by the PN-INspektor® NT (serious fault in the network) or the device is no longer communicating or is not in the network.

3.1 Homepage

The homepage provides a complete overview of the status of the connected PROFINET system since the start since the start of the current measurement.

If there are no entries here, the system is working stably and there are no urgent actions required.

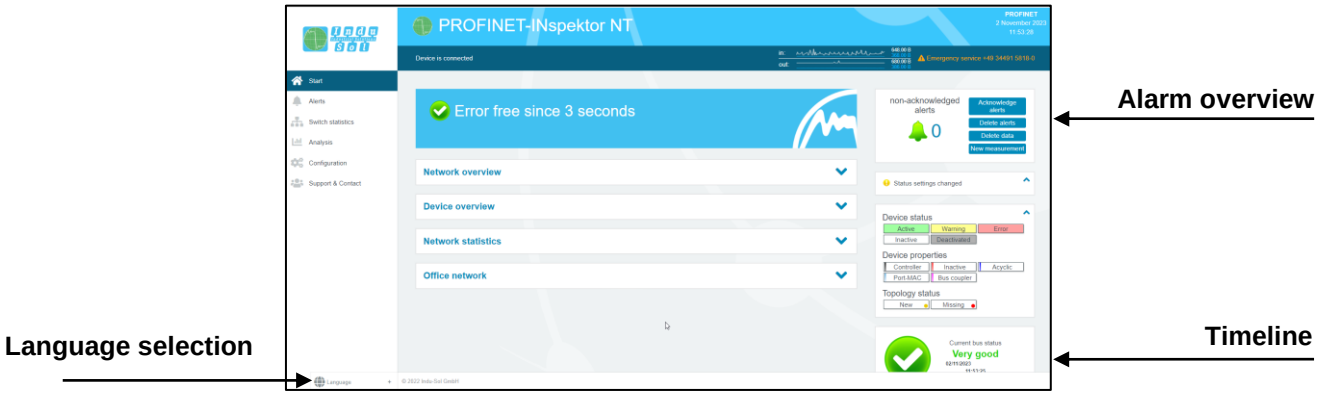


Figure 8: Complete overview

There are additional helpful functions for obtaining more detailed information on the state of the network. These can be accessed via drop-down menus or the Alarm Overview.

Specifying the time period, with a corresponding display of device information, is possible in the sub-menus of the homepage. The relevant period of evaluation can be selected by switching the time window between “current”, “last minute” and “history”. The “current” setting always displays the node condition (live list) at that particular moment, and the “last minute” option shows the device information over the course of the previous minute. With the “history” pre-selection, all data is displayed since the beginning of the recording or the last time the “Delete data” or “New measurement” function was commanded. You can use these different time references to determine whether PROFINET faults are occurring occasionally or permanently.

To adapt the user language of the web interface, it is possible to select the language by means of a mouse over function on the "Language" item.

Language switching only affects the user interface. The settings for the display and the log text are made by changing the system language (see section 3.5.1.5 Time and language settings).

If errors occur during the overrun period, the relevant error trigger is triggered. This leads to entries in the alarm overview, the timeline and the alarm list.

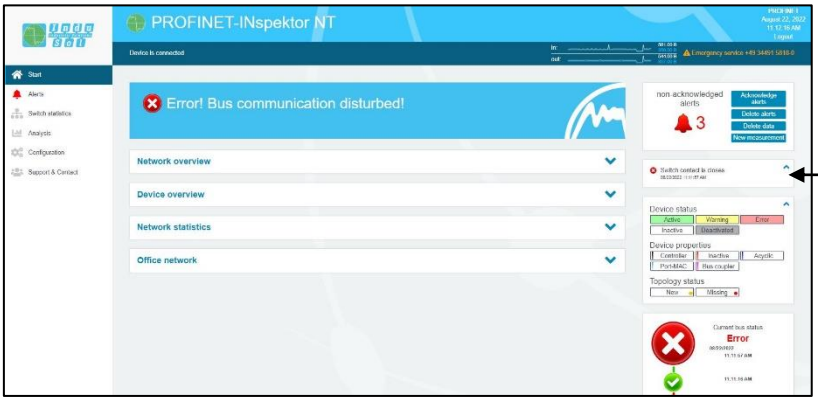


Figure 9: General overview in case of error

If the switching contact is activated at this time (see section 3.5.2.4 Triggers & alarms, factory setting: On), the alarm signalling contact is switched on at the same time (contact opens) and the entry "Switching contact is open" with the corresponding time stamp is displayed in the hint field.

In addition, changes made to the basic settings in the "Device status" menu (see section 3.5.2.3. Device status) are indicated by the message "Status Settings have been changed" and in the "Triggers & Alarms" menu (see section 3.5.2.4 Triggers & Alerts) by the display "Alarm Settings have been changed".

3.1.1 Alarm overview

In the alarm overview the number of unacknowledged alarms is indicated to you. The entries in the alarm list are opened automatically with a mouse click on the alarm bell.

You can also perform the following functions in this window:

Acknowledge alarms: Unacknowledged alarms are acknowledged, but the entries stay in the alarm list. The switch contact for the alarm is reset.

Delete alarms: All entries in the alarm list, including snapshots, are deleted.

Delete data: All previously recorded data is reset, and the network analysis is restarted. The device information (IP address, PN name) and configured settings are retained.

New measurement: This item is to be applied in the event of alternating use in different PROFINET systems. By selecting this function, all previous entries including the node list are deleted, and the network analysis is restarted. Any configuration settings made are retained.

Hint:

By regenerating the participant list, it is necessary to select the automatic deactivation of new participants again, if desired. Settings for the configuration of monitored connections can also be reset by pressing an optional selection field with the start of a new measurement. Otherwise, the previously selected connections will continue to be monitored.

3.1.2 Timeline

The timeline offers you a compact visual overview of the state of the network over the course of time. If different network statuses are analysed within the course of the monitoring period, the point in time when the respective status change started is presented as a new node (maximum 50 entries). Detailed information accumulated within this time frame can be accessed by selecting one such node. The minimum time for a status change (new nodes) is one minute.

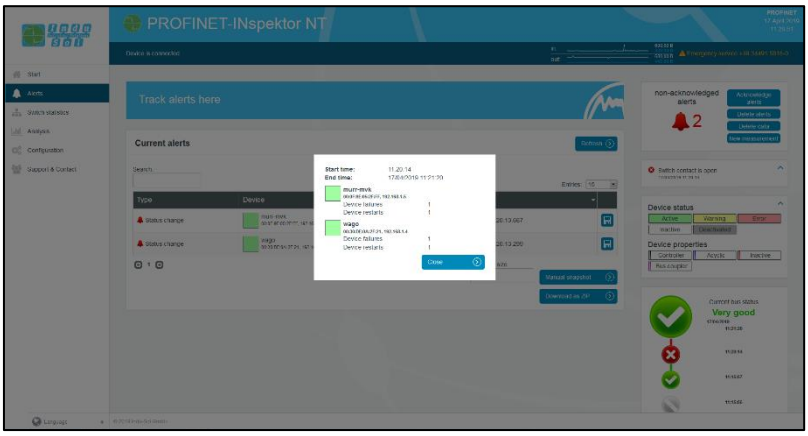


Figure 10: Timeline entry

The individual status changes can be adjusted for each node separately (See point 3.5.2.3 Device status) in order to adapt the display to the plant conditions.

3.1.3 Network overview

By activating the "Network overview" selection window, the status variables determined for all important quality parameters of the connected PROFINET network are displayed. These form the basis for stable, error-free communication. The individual parameters are explained in more detail under point 4. Explanation of terms. For a simple evaluation of the quality criteria, these can be highlighted in color using predefined limit values by selecting the "Colorize status" function (see section 3.5.2.2 Network state).

The display of the network load per second indicates the maximum value of the received and transmitted communication direction. In addition, both directions can be viewed separately.

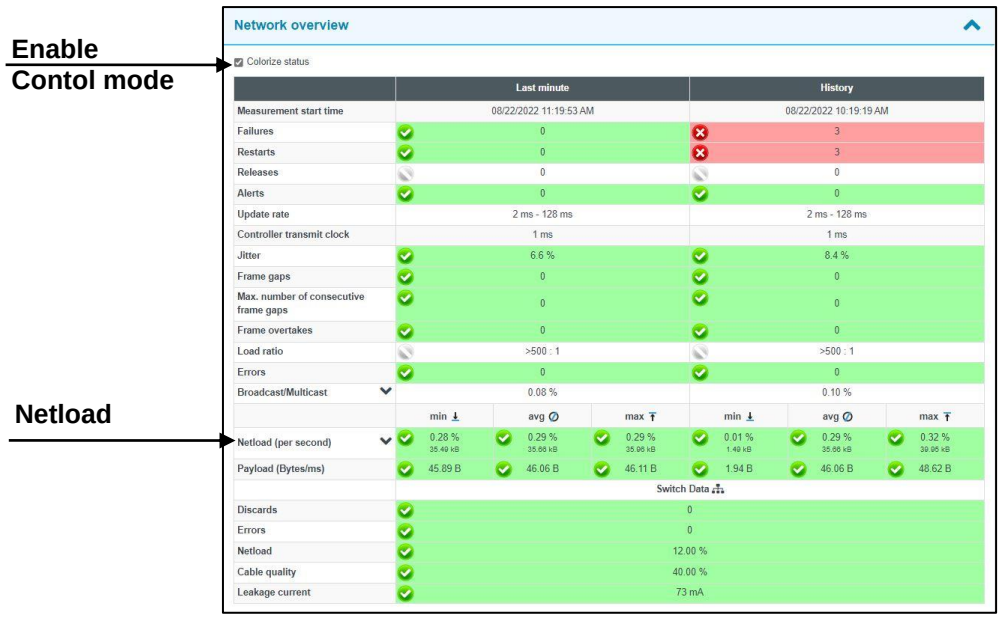


Figure 11: “Network overview” selection window

3.1.4 Node overview

This overview provides you with a complete outline of all devices communicating within the PROFINET network. The individual devices are marked in different colours based on node condition and communication protocol (PROFINET or acyclical communication). The meaning of the respective statuses is explained in the legend at the top.

To increase the clarity, you can select the display for the different protocol types and the individual evaluation criteria. In order that all projected device information (PN name, IP address) can be determined and displayed for the respective participant, it is possible to carry out a participant scan to query the data when the **ACTIVE** port is connected. (see section 2.6 Web interface).

Participant-specific information can be assigned to the associated participants in the participant overview via the "Display" selection field. The sorting of all detected participants can be adjusted according to selectable criteria such as IP address, PROFINET name, etc. via the "Sort" selection list.

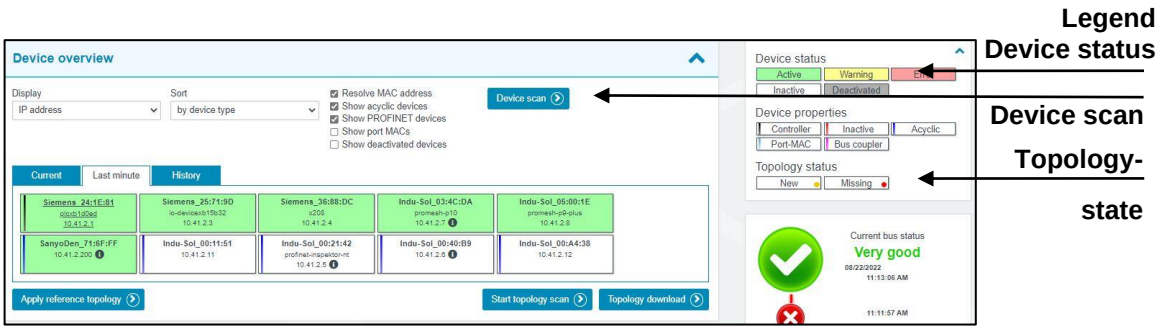


Figure 126: “Node overview” selection window

Via the participant overview, changes in comparison to a previously defined reference topology can be visualised directly. To do this, the current topology must first be adopted as the standard reference via the "Adopt reference topology" button. Occurring changes such as new or missing participants compared to the reference topology are symbolised by yellow and red dots in the lower right corner of each participant. The button "Start Topology Scan" can be used to initiate a new topology scan after the settings for the scan area and the scan configuration have been made in the dialogue box that opens (see 3.5.2.6 Network Scan and Topology Determination).

The last recorded topology can be downloaded to the PC via the "Download topology" button and opened and edited there using the PROscan Active software.

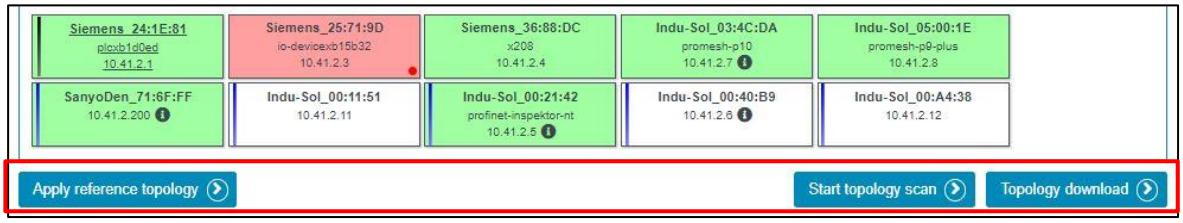


Figure 137: Determination of the reference topology

For a detailed view of the device-related information, select the corresponding device by mouse click. All relevant data for the evaluation of the communication quality of this participant are then displayed.

Figure 148: Detailed information window

As a sub-item to the detailed information, additional, more detailed device-related data is listed through the “Network statistic” page.

	Last minute	History
Load ratio	>500 : 1	>500 : 1
Broadcasts (of these PROFINET)	0 (0 | -)	8 (0 | 0.00 %)
Multicasts (of these PROFINET)	0 (0 | -)	0 (0 | -)
Frames (sent) (of these PROFINET)	30,000 (30,000 | 100.00 %)	2,841,946 (2,841,918 | 100.00 %)
Frames (received) (of these PROFINET)	30,000 (30,000 | 100.00 %)	2,841,918 (2,841,902 | 100.00 %)
Bytes (sent) (of these PROFINET)	2.04 MB (2.04 MB | 100.00 %)	193.26 MB (193.25 MB | 100.00 %)
Bytes (received) (of these PROFINET)	2.04 MB (2.04 MB | 100.00 %)	193.26 MB (193.25 MB | 100.00 %)
Errors (sent) (of these PROFINET)	0 (0 | -)	0 (0 | -)
Errors (received) (of these PROFINET)	0 (0 | -)	0 (0 | -)
Payload (sent)	1.32 MB	125.04 MB
Payload (received)	1.32 MB	125.04 MB

Figure 15: Device-related network statistics

3.1.5 Network statistics

Further detailed information on the **whole** PROFINET network is displayed below the “Network statistics” selection window.

Network statistics

	Last minute	History
Broadcasts (of these PROFINET)	0 (0 | 0%)	1 (0 | 0.00%)
Multicasts (of these PROFINET)	98 (0 | 0.00%)	5.023 (0 | 0.00%)
Frames (sent) (of these PROFINET)	1.506.054 (1.506.044 | 100.00%)	77.201.967 (77.201.349 | 100.00%)
Frames (received) (of these PROFINET)	1.506.056 (1.506.045 | 100.00%)	77.201.969 (77.201.349 | 100.00%)
Bytes (sent) (of these PROFINET)	102,01 MB (101,99 MB | 99,99%)	5,23 GB (5,23 GB | 99,99%)
Bytes (received) (of these PROFINET)	102,00 MB (101,99 MB | 100,00%)	5,23 GB (5,23 GB | 100,00%)
Payload (sent)	65,85 MB	3,38 GB
Payload (received)	65,85 MB	3,38 GB

Figure 16: Whole system network statistics

3.1.6 Office network

In addition to scanning a PROFINET topology via the ACTIVE port of the PN inspector, it is also possible to display the participants of the connected (higher-level) office network. This scan is carried out via the PASSIVE port of the inspector, so that all participants in the IP address range of the passive interface are recorded.

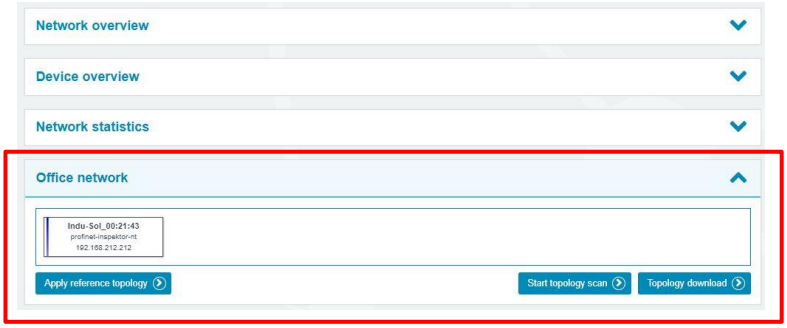


Figure 17: Office network

Via the participant overview, changes in comparison to a previously defined reference topology can be visualised directly. To do this, the current topology must first be adopted as the standard reference via the "Adopt reference topology" button. Occurring changes such as new or missing participants compared to the reference topology are symbolised by yellow and red dots in the lower right corner of each participant. The button "Start Topology Scan" can be used to initiate a new topology scan after the settings for the scan area and the scan configuration have been made in the dialogue box that opens (see 3.5.2.6 Network Scan and Topology Determination).

3.2 Alarms

This overview represents a list of all alarm entries since the restart or the resetting of alarms through the “Delete alarms”, “Delete data” or “New measurement” commands. All unacknowledged entries are indicated with the icon. The maximum quantity of saved alarms is 2,048. Any additional entries over that overwrite the oldest entries.

An entry is automatically made in the alarm list, including a telegram record (snapshot), when a triggering event occurs. Such an entry will contain all important information, such as the device address, fault event and time. In addition to an entry in the alarm overview, the value for unacknowledged alarms increases by one. The saved snapshots can be downloaded by pressing the disc icon and opened with the “Wireshark” software (this software is included in the scope of supply).

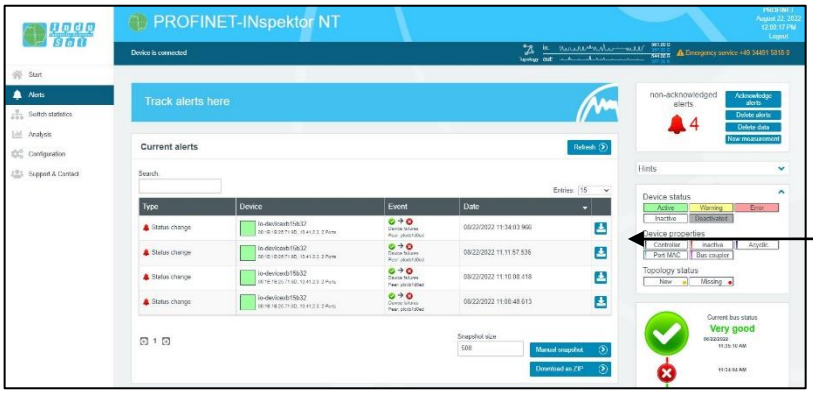


Figure 189: Alarms

The following functions are also available to you in this menu:

Update: Updates the entries in the alarm list

Manual snapshot: Records the current telegram traffic, which is also stored as an entry in the alarm list. The snapshot size can be set manually and is a maximum of 50,000 telegrams.

Download as ZIP: You can download all snapshots and a currently created log as a ZIP archive through this option.

3.3 Switch statistics

This overview serves as a central display of all switch statistics of managed switches in the network. All relevant data for the proof of stable communication (network load, discards, errors, port status) are queried and listed for each device. If switches of the PROmesh family are used in the network, additional diagnostic parameters such as port-related line quality values or device-related leakage currents can be evaluated. The listed information is updated every minute. An ongoing scan process is symbolically indicated in the upper status bar by the appearance of a "switch scan" icon. The switch name is automatically entered after a device scan (see point 3.1.4 Node overview) has been performed.

This process is an active query in the network. The prerequisite for this is the integration of the AKTIV port into the network (see point 2.6 Web interface) as well as the activation and definition of the address range to be scanned in the menu item: 3.5.2.6 Network scan and topology determination

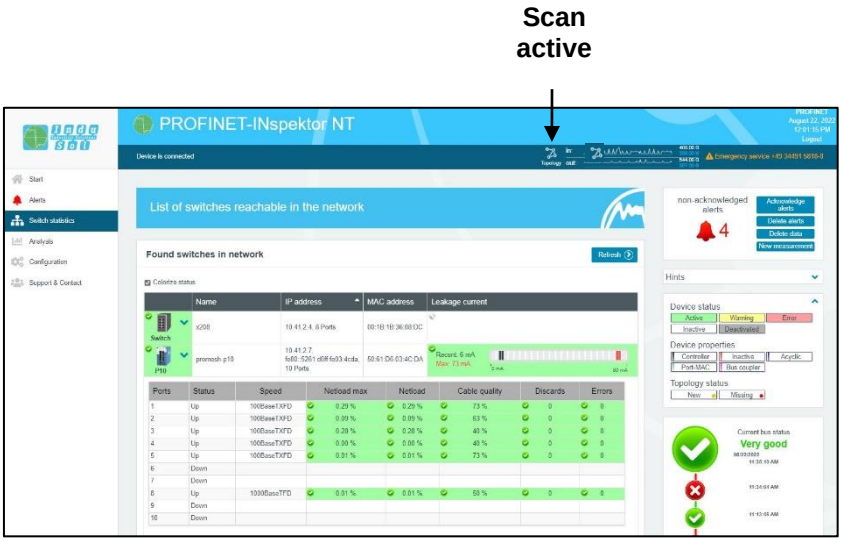


Figure 109: Switch statistics

3.4 Analysis

The analysis menu contains different statistics overviews as well as the report and topology function.

3.4.1 Netload chart

In the chart function, this sub-menu provides a quick visual overview of the netload performance of the communication route. Here data is distinguished between incoming and outgoing netloads and presented in second and minute-cycles.

Figure 20: Netload charts

3.4.2 Reports

The report function allows for all information gathered since the beginning of the recording to be documented in a report in summary form. These reports are stored in the report directory and can be opened, printed or deleted from here.

The report function can be used both as a one-time action by pressing the "Create Report" button and can also be configured by automatic protocol generation (see section 3.5.2.5 Automated Report).

The reports can be used for one's own documentation or as an acceptance report.

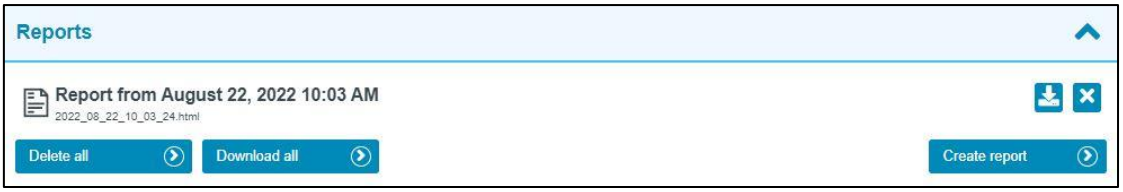


Figure 21: Reports

For the complete representation of the symbols in the printout, the "Print Background" function must be activated in printer settings.

3.4.3 Topologies

PROFINET Scan

By triggering a scan process with the "Start PROFINET Scan" button, the current device information and the real wiring sequence (topology) of all participants of the PROFINET network present in the set address range are queried and combined in a file (.topo). The topology scan is carried out via the ACTIVE port of the PN Inspector. The resulting files are marked with the addition "Profinet topology of ..." and can be evaluated using the PROscan® Active software.

Office scan

By triggering a scan process with the "Start Office Scan" button, the current device information as well as the real wiring sequence (topology) of all participants of the office network present in the set address range are queried and combined in a file (.topo). The topology scan is carried out via the PASSIVE port of the PN Inspector. The resulting files are marked with the addition "Office topology of ..." and can be evaluated with the help of the PROscan® Active software.

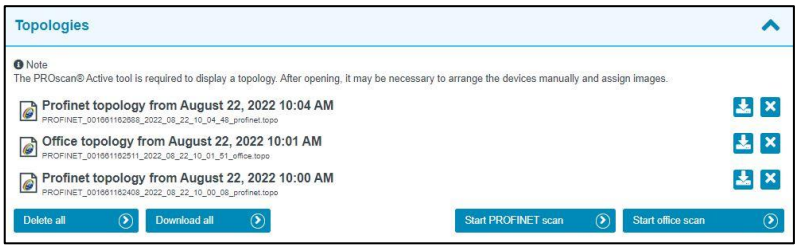


Figure 22: Topologies

The overview shows the last three scan results. The files can be downloaded or deleted from here either individually or in total.

The topology scan is also an active function. Therefore, the same conditions apply as for the participant scan (see point 2.6 Web interface).

3.4.4 Jitter overview

For each update rate that was set in the PROFINET network, the jitter overview displays the corresponding jitter values that were detected, including global values and device-specific values. At a glance, you can see the update rates and devices that have increased jitter values.

The jitter overview provides a tabular overview of all update rates determined in the PROFINET network as well as the corresponding percentage jitter values. With this information, you can see at a glance at which update rates and devices there are increased deviations in clock behavior.

To display the results, you can choose between a table, diagram or list view.

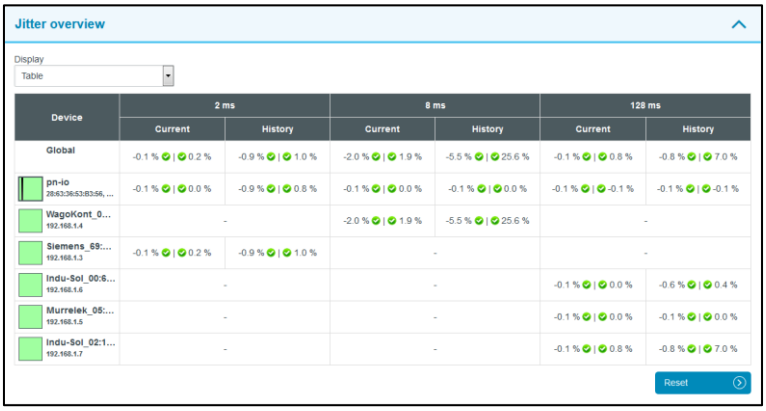


Figure 23: Jitter overview

3.4.5 Node statistic

This sub-menu offers a statistics function for individual PROFINET quality parameters through all analysed network devices. Through this option you can see the device-related accumulation for the selected parameter immediately.

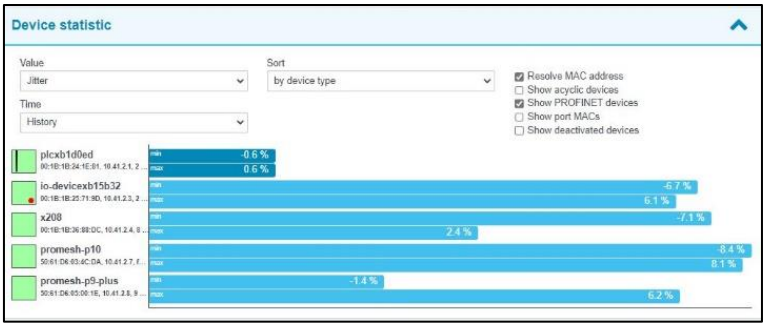


Figure 24: device statistic

3.4.6 Frame statistic

Under the point Telegram Statistics, the number of telegrams is grouped according to the different protocol types and is displayed graphically. With this graphic you can easily see which log type has a negative influence on the load ratio.

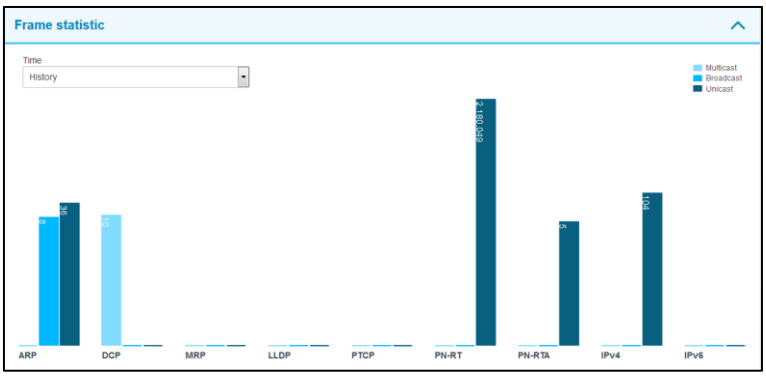


Figure 25: Frame statistic

3.4.7 Tools

Under Tools, you can perform a ping and a traceroute to a specific IP address.

- Ping: Check for entered IP address
- Traceroute: Determination of quantity and IP address of network transitions between the inspector and the specified IP address

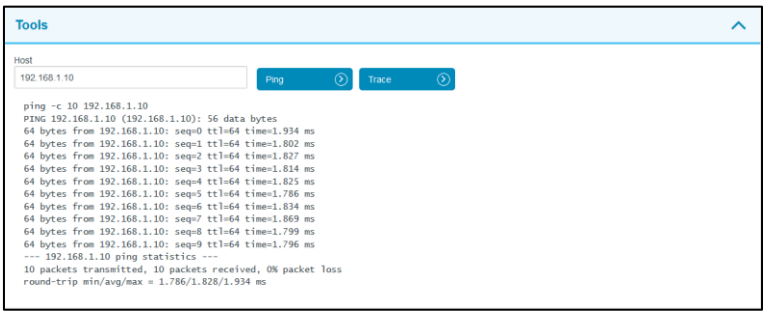


Figure 2611: Tools

3.5 Configuration

Within the configuration menu, you can make changes to the general device settings of the PN-INspektor® NT and adapt the monitoring function specifically to your PROFINET network.

All entries are saved in the device by pressing the **“Apply”** button or reset to the default setting through **“Reset” + “Apply”**.

The functions are described individually below.

3.5.1 System

Basic device settings, such as date / time, device name, IP address, etc., are displayed in the system settings and can be changed here. The entries are kept in the event of power failure or device modification.

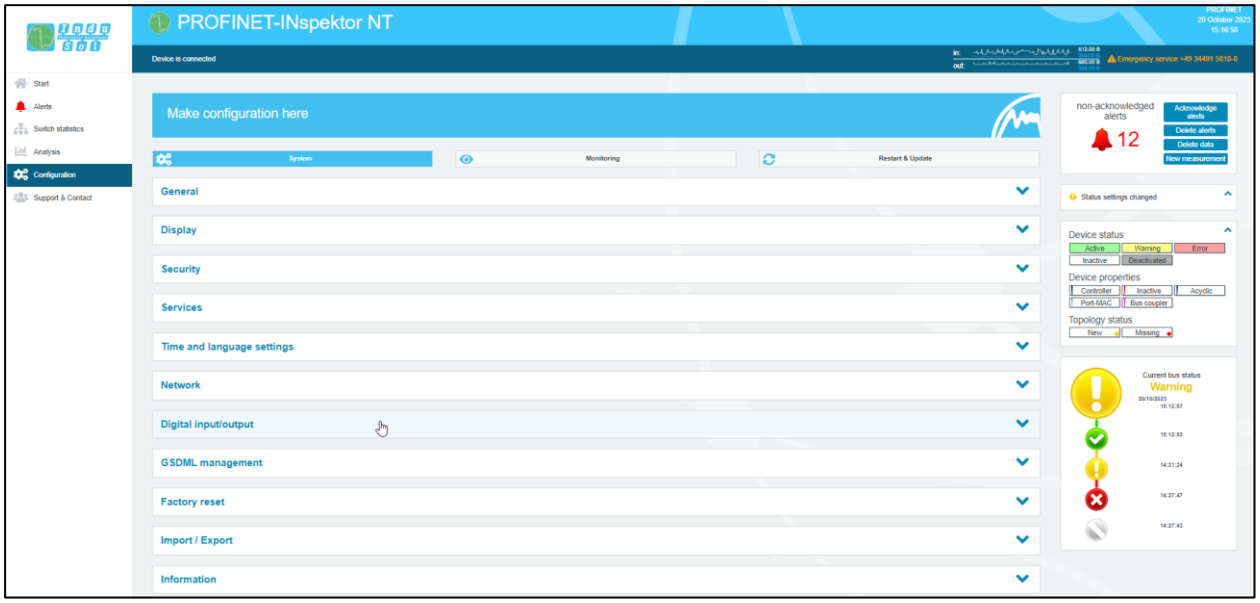


Figure 27: System settings – complete overview

3.5.1.1 General

In this submenu, the details of the unit's name, installation location, network name and notes are entered, which serve to describe the unit and the network to be monitored in more detail. Furthermore, a password for the PN-INspektor® NT can be set up in this menu. This password is then required for all changes to the unit and monitoring settings. Optionally, access restriction to the web interface can be used by activating a login page using the same password.

In addition, it is possible to deactivate the touch screen display in this window. In the factory setting, this is always activated. The calibration process can also be started from here.

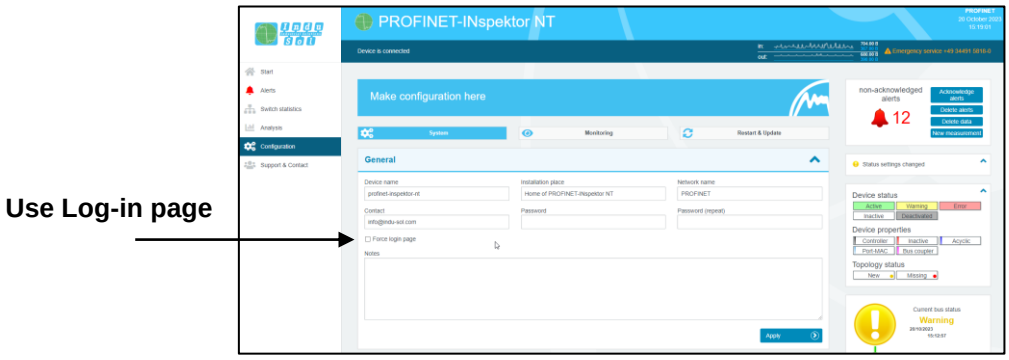


Figure 28: System settings – general

3.5.1.2 Display

The "Display" menu item is used to activate and configure the touch display on the front of the PN-Inspektor NT.
If required, the display can be deactivated via the "Activate display" checkbox. In the factory setting, this is always switched on. Optionally, a text identifier with an individual free text can be stored in the lower left display area of the PN inspector display. If the checkbox "Activate display identifier" is selected, the free text stored in the field display identifier appears there. Furthermore, an optional image, e.g. in the form of a customer logo, can be displayed if desired. For this purpose, the appropriate image file in .png format is selected after activating the "Activate logo" checkbox. Via the button "Reset" the default Indu-Sol logo is restored.

Furthermore, the calibration process of the display can be started via the menu item "Display". All changes made to the display settings must be confirmed by clicking the "Apply" button.

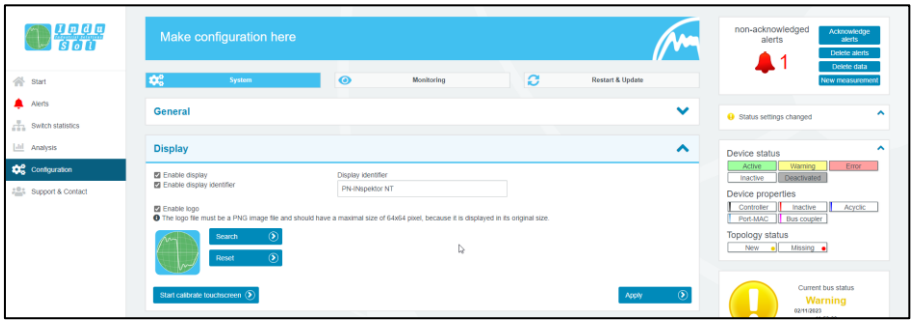


Figure 29:System settings Display

3.5.1.3 Security

In this area, secure web access via HTTPS can be activated and automatic redirection can be set up. To use your own certificate, this function must be activated and the certificate imported via the "Browse" button.

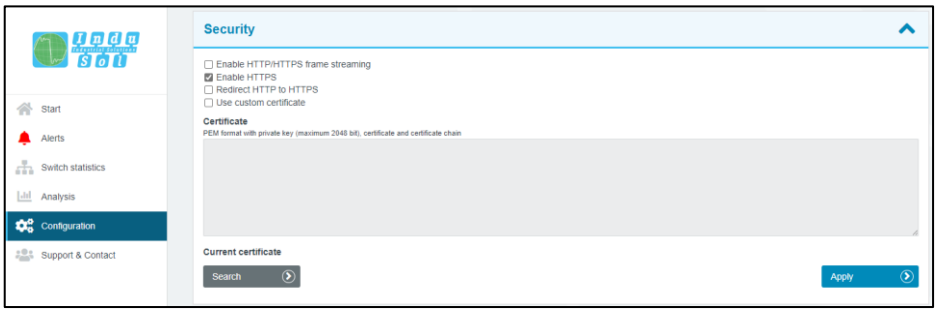


Figure 30: Security

Telegram Streaming

Via the selection field "Activate telegram streaming via http/HTTPS" it is possible to activate telegram recordings directly via the web browser. Neither the installation of a mirror port nor other configurations are necessary for this.

In order to trigger a telegram recording, the following entries must be made via the address line of the web browser and supplemented with the parameters of the following table:

Web URL for starting the telegram stream:

http:// (IP address of the PN-Inspektor NT) /capture, e.g., http://192.168.212.212/capture

To adapt the telegram stream, the address line listed above must be extended by at least one of the parameters listed below. The added parameters are introduced by means of a "?" directly after the "capture" command. The linking of several parameters can be done by a "&" between the parameters (see example below). Completed telegram streams are stored in the download path stored in the web browser by default. A telegram stream is always considered completed when the first of the linked fulfilment criteria "frame", "time" or "size" has been met.

Parameter	Possible values	Standard	Description
format	raw / gedt / pcap / pcapng	pcapng	Data format of streamed telegrams
skipheader	0 / 1 / true / false / yes / no	false	Writing the file header of the streamed data
frames	Integer number	/	Stop recording after x telegrams
time	Integer number	/	Stop recording after x seconds
size	Integer number	/	Stop recording after x bytes

Example:

A telegram stream is to be started via the PN-INspektor NT with IP address 10.41.2.148. In the process, 10,000 telegrams are to be saved in .pcap format. To do this, enter the following command in the address line of the web browser:

https://10.41.2.148/capture?format=pcap&frames=10000

3.5.1.4 Services

The SNMP or OPC UA services can be used to query device and diagnostic/monitoring information. These two interfaces can be activated and configured as required. To use the SNMP interface, the manufacturer-specific MIB file is stored on the unit in the download area in the Support and Contact menu. In the case of OPC UA, no further data is required to capture the information, as the PROFINET-INspektor® NT provides the information to be captured after the communication setup. To get an overview, the OPC UA Information Model is shown under point 6. OPC UA Information Model.

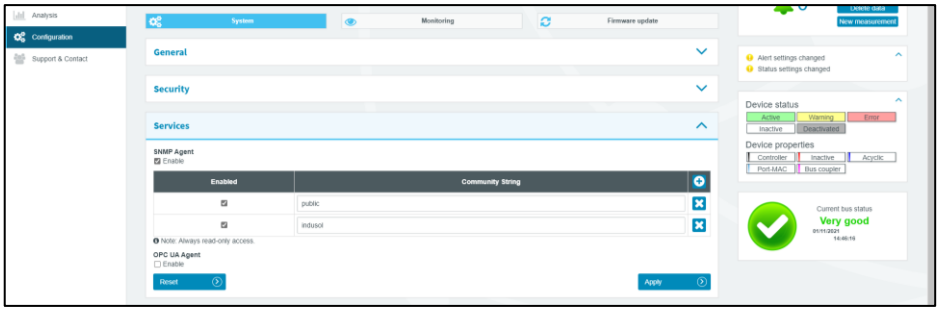


Figure 3112: Services

3.5.1.5 Time and language settings

The configuration of the system time and the standard language for display and protocol text is done in this menu. The system time can either be entered manually, be adopted automatically from local PC system time, or be retrieved from a time server.

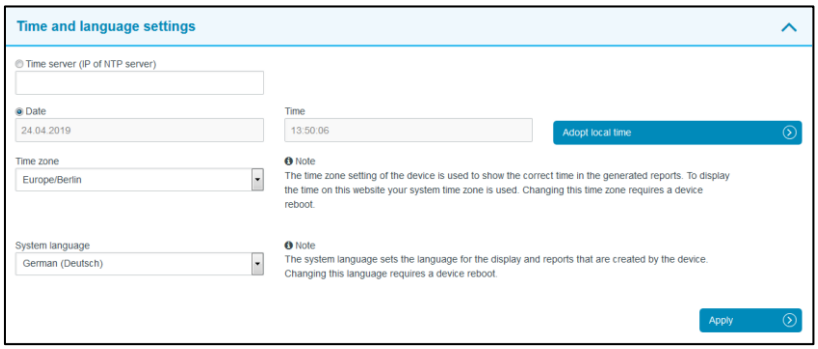


Figure 32: Time and language settings

In order for the time to be displayed correctly in the log, you must always specify the time zone, both if the time is entered manually and if it is retrieved automatically.

The selection of the system language includes: German, English, Spanish and Chinese.
The changes made here have no effect on the display of the web interface (see section 3.1 Homepage).

Changing the language setting requires a device restart.

3.5.1.6 Network

Under this item the network address settings are defined for both the “ACTIVE” and “PASSIVE” network connections of the PN-INspektor® NT (e.g. address, subnet mask, gateway). In this process, you can decide whether you want to use a fixed address or if the IP address should be obtained automatically (DHCP).

In addition, the status of the interfaces (connected / not connected) is displayed.

To ensure error-free access to the Web interface, addresses from different address ranges or subnets must be assigned to both network connections

The configuration of a mirror port is also possible in this menu. The function allows telegrams that are recorded to the diagnostic ports (IN / OUT) to be forwarded to the ACTIVE or PASSIVE web interface. This function is deactivated by default after each boot of the device. The mirror port configuration can optionally be permanently retained via the "Save settings after restart" selection field.

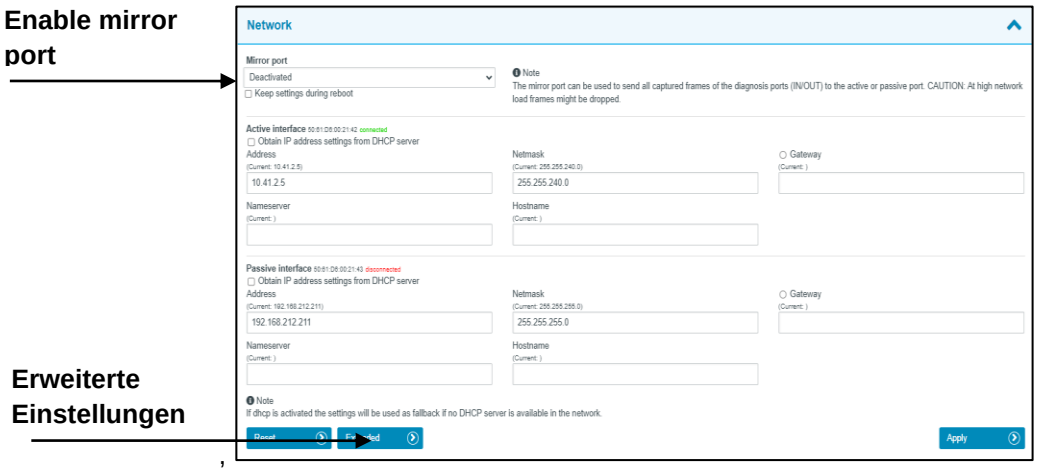


Figure 133: Network settings

After selecting the extended display, additional routing and DNS server settings can be configured for both interfaces.

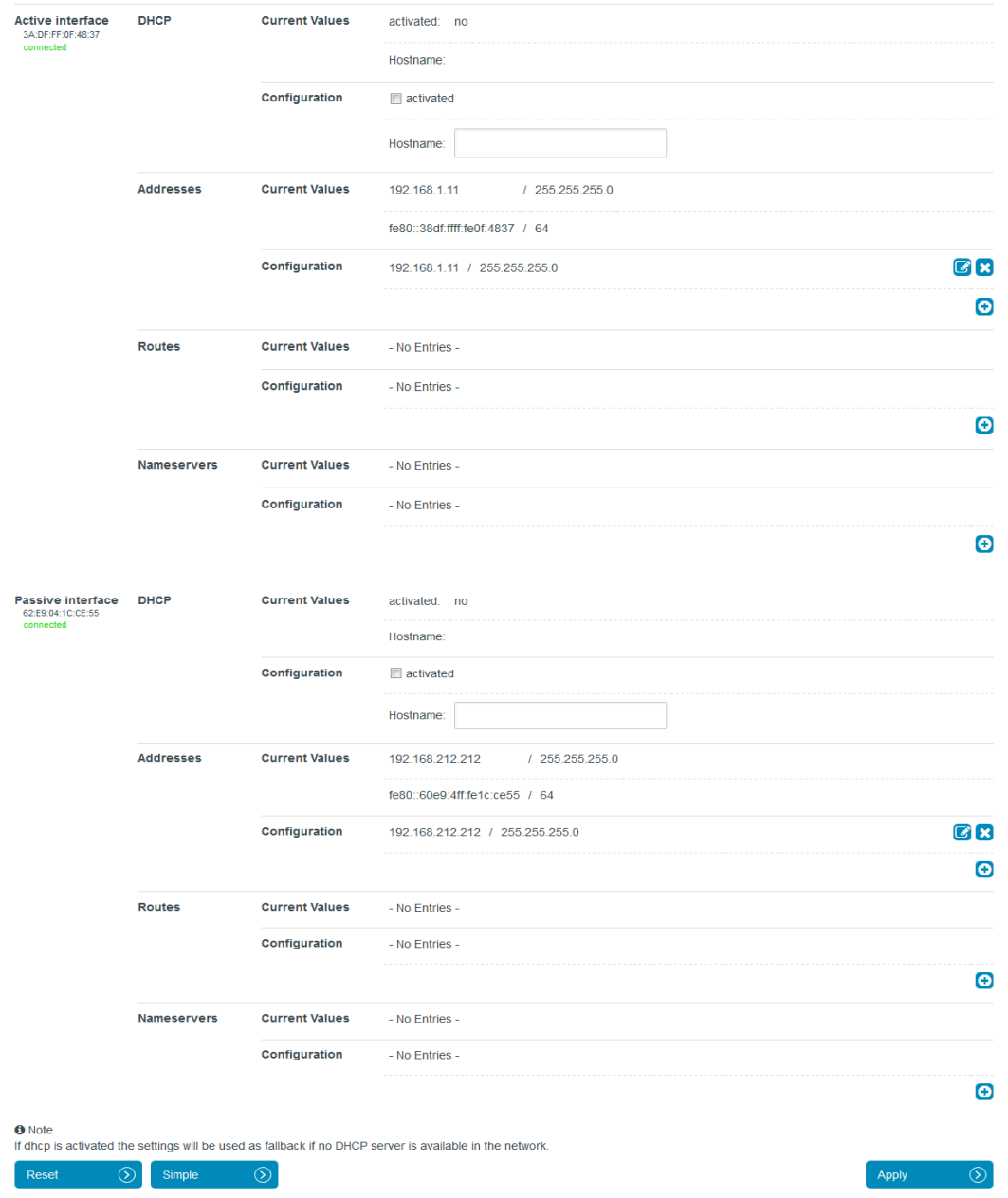


Figure 144: Network settings – extended view

3.5.1.7 Digital Input

The PN-INspektor® NT has three digital inputs, the function of which can be adapted as required. These can thus be used in conjunction with the real system for targeted control measures of the device and the interaction of the PN-INspektor® NT with the production process can be optimised. This ensures that the monitoring function is only documented for the normal operating status and that system start-ups and maintenance failures are suppressed.

The following function selection is available for parameterising the digital inputs:

- Disable alerts (level) → no alarm display and evaluation any more
- Delete data (edge) → Delete the old data and start a new recording, device information of the participants is retained
- New measurement (edge) → Start a new measurement, old data are completely deleted
- Create report (edge) → Documentation of the data acquired since the start time
- Acknowledge alerts (edge) → Alarm display and switching contact are reset; entries in the alarm list are retained
- Reset digital output (edge) → Switch contact is reset; alarm display and alarm list in PN-INspektor® NT remain unchanged
- Disable diagnosis (level) → no evaluation of data traffic
- Start topology scan (edge) → a new topology scan is initiated

The activation of the corresponding events is triggered either by an edge change (edge) or by a permanently present signal (level).

The inputs are configured with the following functions when delivered:

- Input 1: Acknowledge alerts (edge)
- Input 2: Reset digital output (edge)
- Input 3: Disable alerts (level)

To further specify the system, it is also possible to define a specific (rising, falling) or any edge change as the active switching pulse. The selection can be extended or adapted by adding (+) or deleting (x) inputs. This allows multiple assignment of different functions to the individual digital inputs. An example of this is shown under point 7. Example program for controlling the PN-INspektor® NT.

A time delay (max. 15 min) for the start of recording can also be set by selecting " Measurement start delay". This makes it possible to hide the start-up process from the monitoring function when the system starts slowly.

The function of the switching output can be stored either as a normally closed or normally open contact.

The basic setting is restored by pressing the "Reset" button.

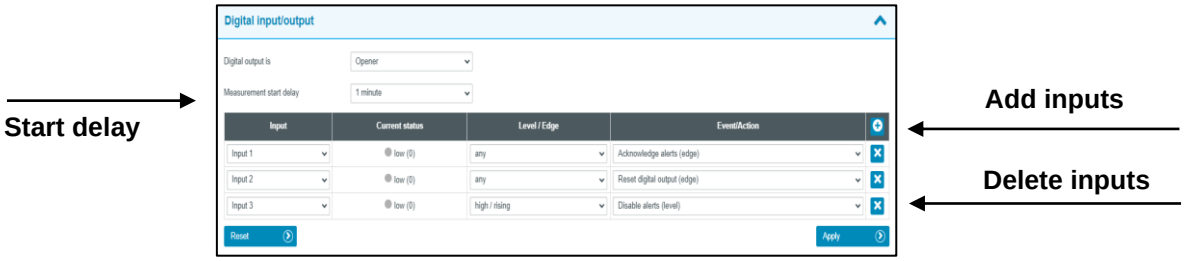


Figure 35: Digital Input

The status of the three switching inputs and the switching output can be tracked in real time at any time via the touchscreen of the PN Inspector. Switching between the screen views is done by using the arrow keys in the upper screen area.

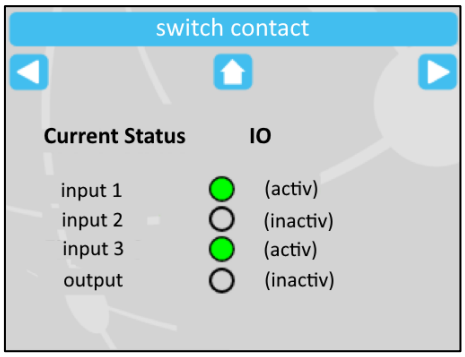


Figure 36: Display visualization of the switching inputs / outputs

3.5.1.8 GSDML Administration

With the help of GSDML files, PROFINET INspektor® NT can display device-specific alarms, which are usually only readable as error codes, in a clear text.

Figure 37: Plain text diagnosis

In general, the PROFINET Inspector already has the GSDML files of the most frequently used switches. If some GSDML files are not available, they can be loaded into the inspector in this menu.

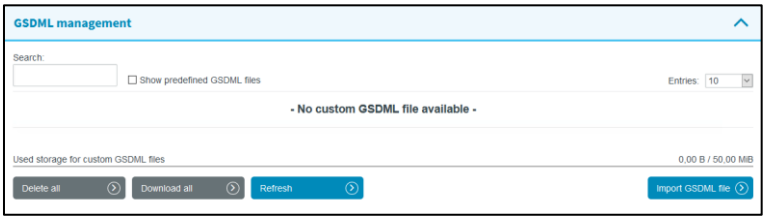


Abbildung 158: GSDML administration

The following functions are available:

- Delete All: Delete all GSDML files
- Download all: Export all GSDML files and load them into another inspector.
- Refresh: Refresh the displayed list
- Show included GSDML file: Standard GSDML files can be displayed by selecting them in the list or they can be neglected by deselecting them in the list.
- Import GSDML file: Not yet existing GSDML files can be imported

3.5.1.9 Factory reset

Here you can reset the PN-INspektor® NT to default settings. You have the option to retain the network settings, or to reset them as well. After the reset, the device is available again immediately.

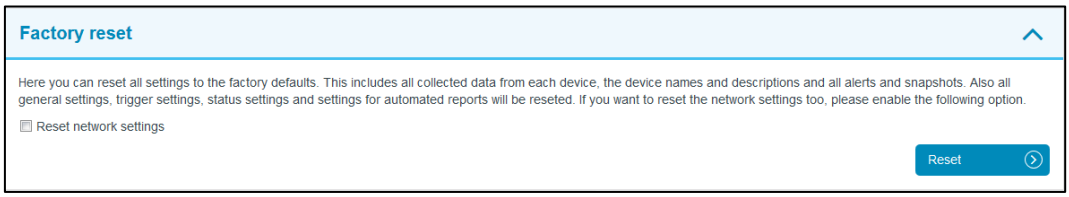


Figure 39: Factory reset

In a reset to default settings, all previously made settings and records are lost.

3.5.1.10 Import/Export

By means of the Import/Export function, all settings that have been made, e.g. general device settings and changes to PROFINET monitoring, can be saved, and loaded again into a PN-INspektor® NT whenever required.

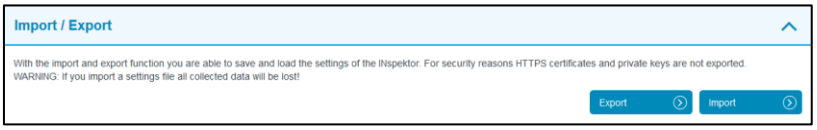


Figure 40: Import/Export

After selecting the "Import" button, the .pnex file to be imported must be selected. Then you can determine which of the values to be imported are to be taken over with the following options. You can choose between:

- No changes
- Create default values
- Import values (current values as fallback)
- Import values (default values as fallback)

The listed options can be selected for the following settings:

- Settings: includes all basic unit settings and configurations, unless listed separately below.
- System language: language setting of the web interface
- Network settings: Configuration of the active and passive interface
- Station list: Configuration of captured subscriber names and monitoring options
- Time zone: time settings
- GSD files: stored GSD library, incl. individual additions

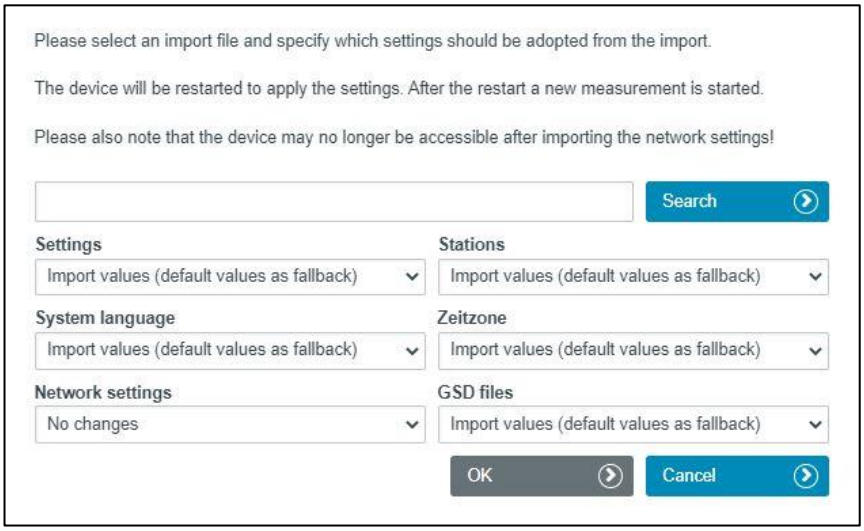


Figure 41: Import parameters

3.5.1.11 Information

Current resource usage and the firmware and hardware versions of the PN-INspektor® NT are displayed in the information overview.

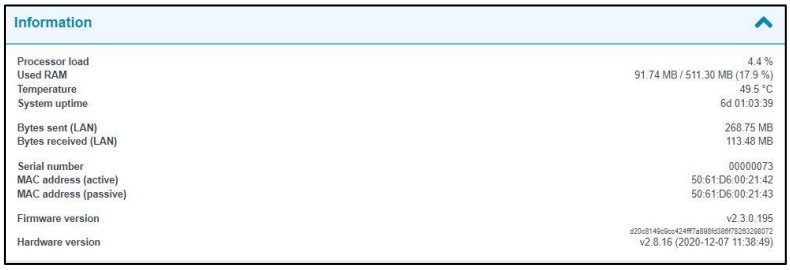


Figure 42: PN-INspektor® NT device information

3.5.2 Monitoring

You can specifically adjust the monitoring function of the PN-INspektor® NT to your network, define customised trigger and alarm thresholds and set up automated reporting with the specifications in these fields.

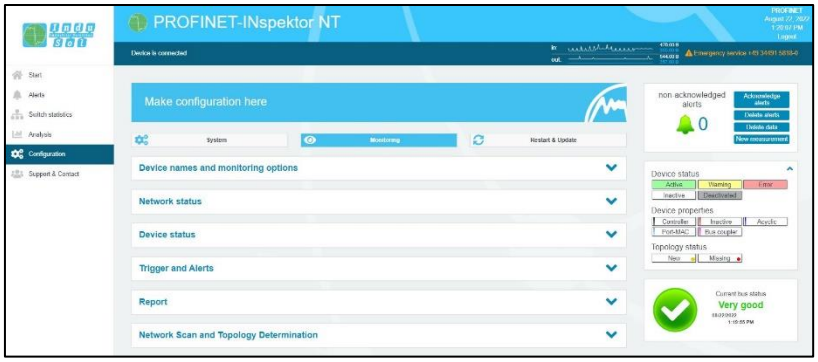


Figure 43: Monitoring – complete overview

3.5.2.1 Node names and monitoring

The point "Node names and monitoring" allows to assign an alias name to each device. It is therefore possible, for example, to adopt and to save the device model, equipment identifier or installation location from the electrical diagrams. All entries will be visible throughout the entire system.

In addition, in this menu the monitoring can be deactivated for individual or for newly detected devices and the analysis can be limited to the participants that communicate exclusively with the selected station.

To increase clarity, it is possible to select according to the different protocol types and to sort the order according to predefined criteria. The filter line with free text search can be used to quickly find individual participants.

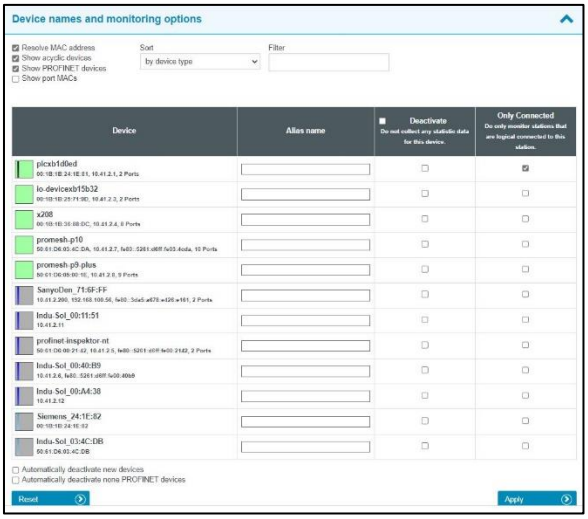


Figure 44: overview node names

3.5.2.2 Network state

For a quick visual assessment of the PROFINET network, the individual quality parameters can be colour-coded by defining special acceptance threshold values. Once these values have been reached, the subscriber is displayed in yellow in the event of a warning or in red in the event of an error, depending on the objective. If no error has occurred, the display remains green. The basic settings can be adapted according to customer-specific requirements.

This colour coding becomes effective both in the network overview (see point 3.1.3 Network overview) and in the protocol display after the activation of the status colouring.

Resetting to the preset default values is possible at any time via the "Reset" button.

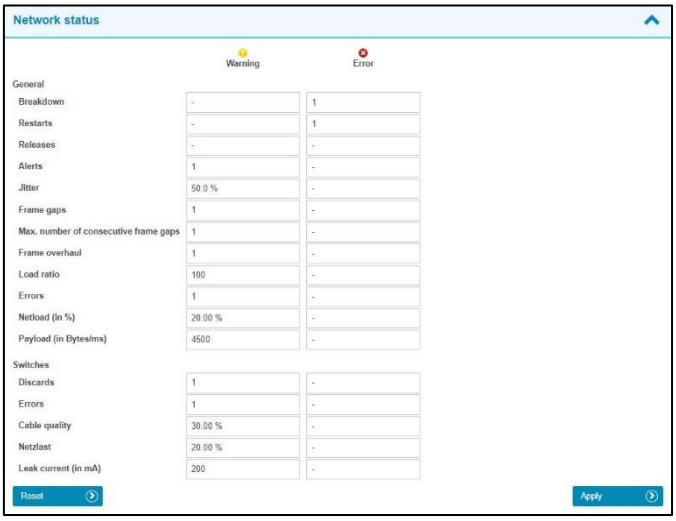


Figure 165: Network state

3.5.2.3 Device status

The settings in this submenu allow the display of devices in PROFINET-INspektor® NT to be adapted to the conditions of the system. These settings can be carried out for all devices of the entire system (Global), as well as for each device. In this process, a device may adopt the following conditions, depending on the fault event and setting:

- No fault
- Warning
- Fault

In the default setting, the PN-INspektor® NT is programmed so that alarms, error telegrams, increased jitter, telegram gaps, telegram overtakes and an increased netload of any node lead to “Warning” status; and failures lead to “Fault” status.

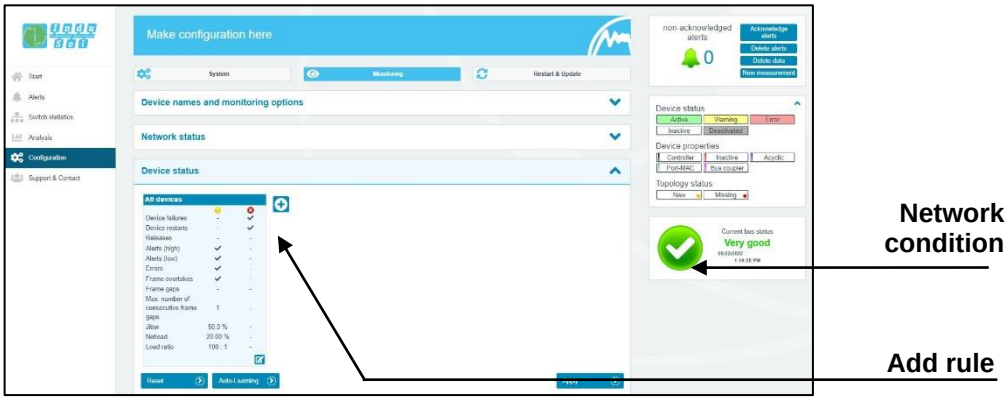


Figure 46: Node condition – default setting

By adding and editing additional rules, the display of the device states can be individually adapted, e.g. due to special production conditions: In this process, node-specific settings overwrite global values. This means it is possible to create node-specific settings to hide fault events which are justified in normal system operation. With the "auto-learning" function, these values can be automatically adapted to the state of the device to be monitored, both participant-related and globally.

Example: The system operator must enter a light barrier for a part change. This results in a device alarm (low) which is irrelevant to bus status evaluation. By deselecting the alarm (low) function of the nodes concerned in the PN-INspektor® NT, these stay “green” in the display.

As can be seen in the following illustration, in this example the “Telegram gap” event was deselected for the controller and the status change for the IO-Device was fully deactivated.

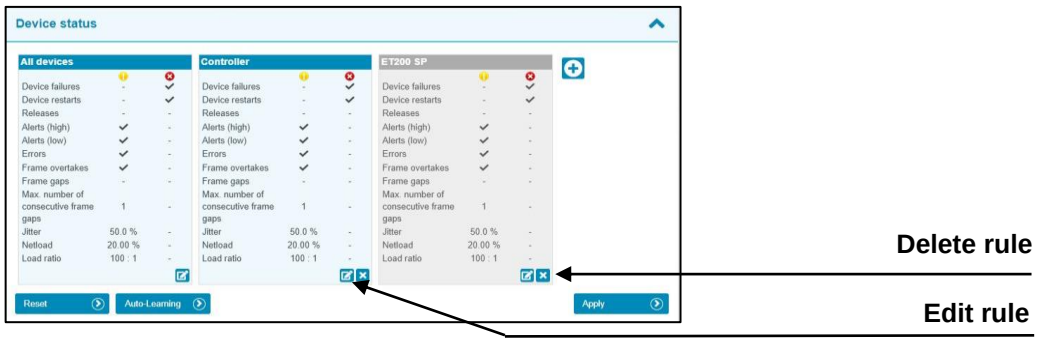


Figure 47: Applying filters

The setting options in the editing window for the selected group become clear in the following image. Participants whose monitoring options are to be configured via this group can be added to the group via the (+) button.

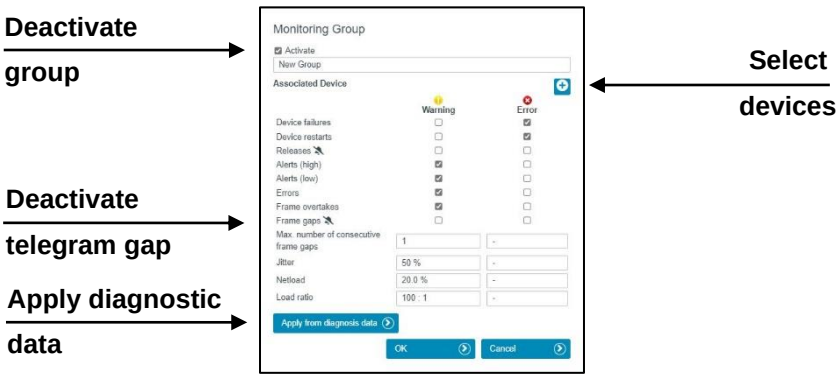


Figure 48: Controller telegram gap deactivated

Via the function " Apply from diagnostic data" an automatic limit value adjustment is carried out according to the currently determined network parameters.

Pressing the "Reset" button returns all changes made to the initial state (factory setting).

After selecting the (+) button to add new participants, all accessible participants are listed in the selection window that opens. By selecting the corresponding participant, it can be selected and included in the monitoring. Alternatively, the buttons "Select all" and "Deselect all" can be used to select all associated participants at the same time.

For better clarity, various sorting and free text filter functions are available.

Use the "OK" button to confirm the selected participants and add them to the monitoring group.

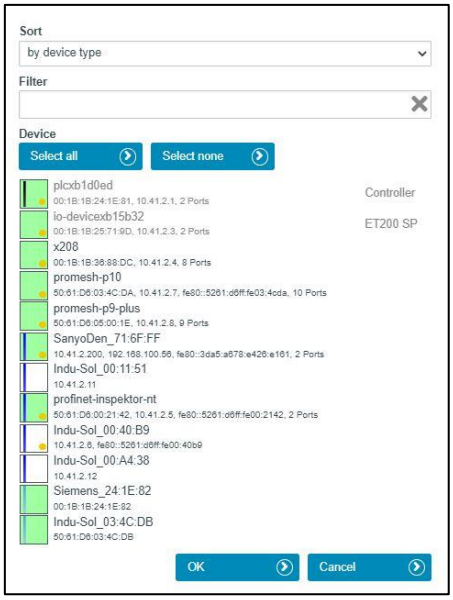


Figure 49: Adding new participants to the monitoring group

3.5.2.4 Triggers & alarms

For the customer-specific adaptation of the alarming and evaluation via switching contact, snapshot, e-mail, SNMP trap, MQTT message or topology scan, the corresponding parameterisation is carried out under the item "Triggers and alarms".

In the basic setting of the unit, all faulty events of any PROFINET participant automatically led to an entry in the alarm list.

Figure 5017: Triggers & alarms - basic setting

By variably parameterising the error triggers to different predefined trigger types as well as special subscriber addresses, it is possible to make the corresponding settings here for a targeted error search or subscriber monitoring.

A selection of predefined trigger events is already set up in the basic setting. The various options for editing the individual triggers and the associated actions are described in more detail below.

Hint:

Each of the triggers set up is always linked to at least one action. As described below, when editing a trigger, the linked action can be edited. Conversely, when editing actions, the triggering trigger events can also be selected.

The entire scope of all configuration options for triggers and actions can be usefully employed to indicate the first signs of a communication deterioration by means of an early warning before a unit failure occurs.

Via the item "Reset", all changes made are restored to the initial state.

3.5.2.4.1 Configuration of triggers:

Selecting the edit mode via the edit symbol opens the selection menu for adjusting the trigger settings. New triggers can be added by selecting the (+) button.

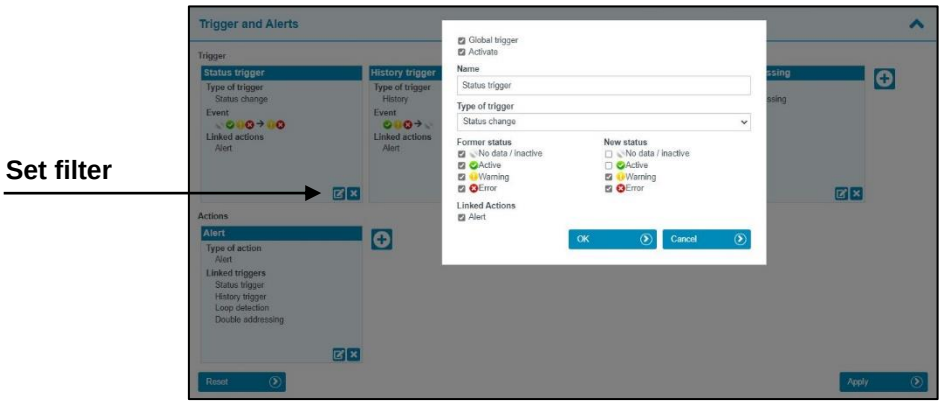


Figure 5118: Selection menu for trigger type "Change of state

The following selection items are available for defining the trigger type:

- Alarms (low priority)
- Alarms (high priority)
- Failures
- Restarts
- Logouts
- Errors
- Telegram gaps
- Max. Number of consecutive telegram gaps
- Telegram overtakes
- Jitter
- Load ratio
- Network load
- Change of state
- Chronicle
- Global network load
- Telegram surge
- New subscriber
- Double addressing
- S7 communication
- Loop detection
- Topology
- Interval
- SNMP trap

A more detailed explanation of the individual functions can be found under point 4. Explanation of terms.

For threshold-related alarms, the number of events that should lead to the triggering of a trigger is specified in the corresponding submenu.

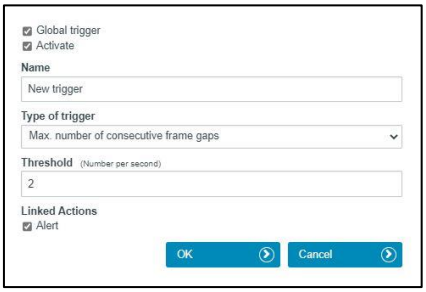


Figure 52: Threshold setting for telegram gap

By assigning individual actions to the corresponding trigger type, the measures to be carried out in the event of an error are determined.

In addition, an address-related selection of triggers is provided. In the default setting, the monitoring of all participants is active (global). By deselecting the item "global trigger", the button "Select stations" appears. Via this button, one or more devices can be activated / deactivated from the station list that then appears. The addresses displayed are automatically recognised by the PN-INspektor® NT depending on the system. By deselecting the "activate" item, the entire trigger can be deactivated if required.

Activate participant list

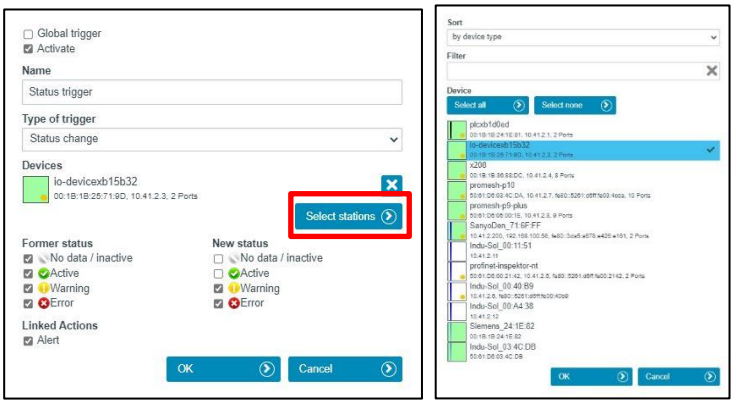


Figure 5319: Example Activate address list

3.5.2.4.2 Configuration of actions:

In addition to the configuration of trigger events, various actions for alerting and notification can be configured in the lower section of the menu item "Triggers and alarms", which are to be executed when the linked trigger event is triggered.

Selecting the edit mode via the edit symbol opens the selection menu for adjusting the settings.

The following selection items are available for defining actions:

- Alarm
- E-Mail
- SNMP Trap
- TCP Event
- Switch contact
- Topology Scan
- MQTT message

Under the selection of the action type, you will find a list of all available triggers. By selecting the respective trigger, the selected action can be linked to the respective trigger event.

Figure 54: Activation of new actions

Some of the actions require further configurations, which are displayed in the configuration window after selecting the respective action type:

Action type Alarm:

In the basic setting of the device, all faulty events of any PROFINET participant automatically lead to an entry in the alarm list and chronicle. The snapshot size can be freely defined by specifying the number of telegrams between 0 and 50,000 before and after an event as required. The higher the snapshot size is selected, the fewer snapshots can be stored (e.g. a maximum of 4 snapshots at 50,000 before and 50,000 after trigger events).

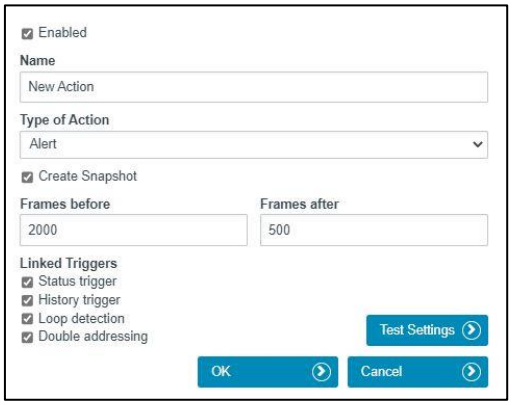


Figure 5520: Action type Alarm

Action type E-mail:

This action type allows to initiate the sending of an email by the PROFINET-INspektor® NT in case of an alarm. The prerequisites for this are a valid recipient address, the IP address of the email server, an existing Ethernet connection between the device and the server and a correct configuration of the email connection. Optionally, the email can be encrypted via SSL/TLS.

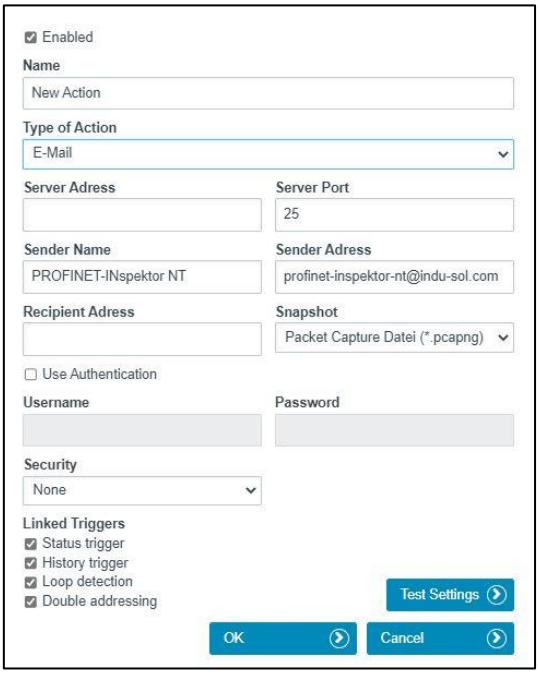


Figure 5621: Action type e-mail

Action Type SNMP Trap Event / TCP Event

This alarm type allows the PROFINET-INspektor® NT to send an SNMP trap or a TCP event in the event of an alarm. The prerequisites for this are a valid address of the trap receiver and an Ethernet connection between the device and the server.

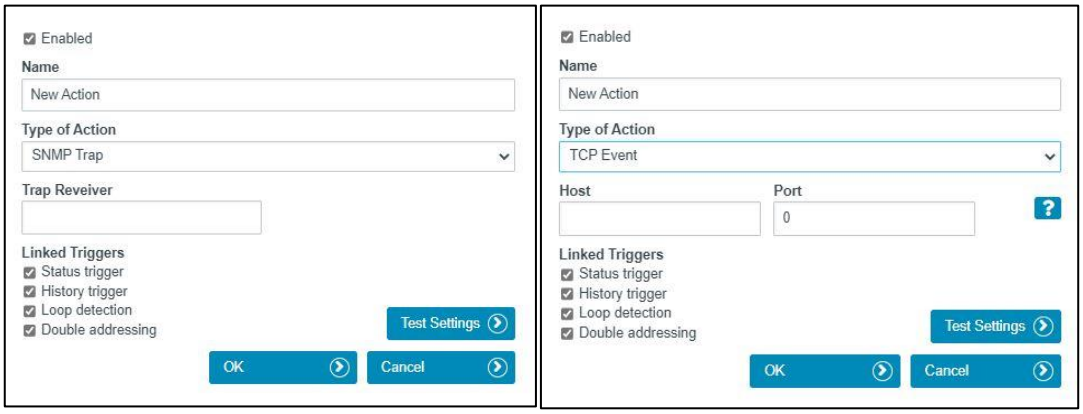


Figure 57: Action Type SNMP Trap / TCP Event

Action type Switching contact

By triggering this action, the external switching contact of the PN Inspector NT can be activated, for example, to display a visualisation of the system status via traffic lights.

Topology scan action type

By using the Topology scan action type, an event-related topology scan of the network is started via the PN-INspektor NT when a trigger condition is triggered. This means that a current topology plan is stored in the PN-INspektor NT at all times, which can be used for topology comparisons, e.g. in the PROmanage NT monitoring software.

Action type MQTT message

This alarm type enables the sending of an MQTT message from the PN-INspektor NT (MQTT client) to a pre-configured MQTT broker when the linked trigger condition is triggered.

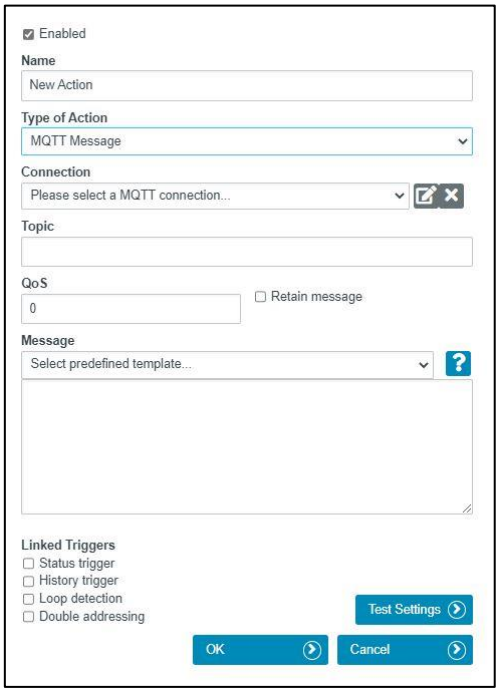


Figure 228: Action type MQTT message

To set up the MQTT client in the PROFINET-INspektor® NT, or to configure the MQTT notification, the following settings must be made in the dialogue view:

1. Action name

The MQTT notification action must be assigned a unique action name for subsequent linking with trigger conditions.

2. Selection of a connection

In order to establish an MQTT communication between a client and a broker, the corresponding connection between both components must first be configured. Any connections can be added, edited and removed.
For each of the connections, information on the IP address of the broker including the corresponding port must be stored (unencrypted connection: port 1883 / encrypted connection: port 8883).
The keep alive interval is a numerical value that specifies the seconds a client can be inactive and still be considered to be functioning correctly. If the value is set to 0, the keep alive functionality is disabled.

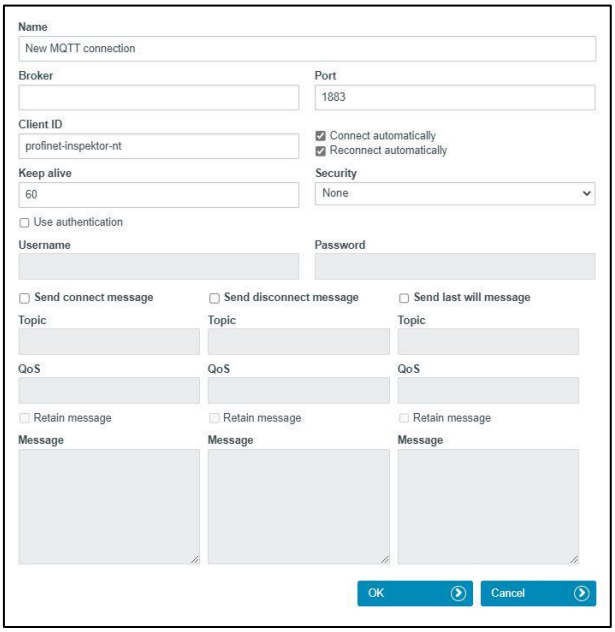


Figure 239: New MQTT connection

Optionally, the following additional messages can be configured:

- Connection establishment: Message when a new Broker-Client connection is established
- Disconnect: Message when an existing Broker-Client connection is terminated.
- Lastwill: The lastwill message is used to inform other clients about an improperly disconnected client. The broker stores the message until it determines that the client has involuntarily disconnected. The broker then sends the Last Will message to all subscribed clients of the Last Will message topic.

3. Specifying the topic

With each MQTT message, the client (PN-INspektor® NT) sends messages with a topic to the MQTT server ("broker") after establishing a connection. Other clients in turn can subscribe to these topics, whereby the server forwards the received messages to the corresponding subscribers. The topic thus serves to uniquely identify a message, comparable to the subject of an e-mail.

4. Selecting the Quality of Service Level

Quality of Service is an agreement between client and broker about the guarantee of delivery of a message. The QoS level can be defined separately for each message.

QoS Level	Description
0: at most once	The client sends the message once, there is no confirmation by the broker.
1: at least once	The broker acknowledges receipt of the message with a confirmation to the sender. The client repeats its message until it receives a valid confirmation from the broker.
2: exactly once	A handshake sequence of 4 messages is used between the sender and receiver to confirm that the main message has been sent and that the confirmation has been received for it.

5. Message content

In this section, the actual message content for each MQTT message can be specified. This can be designed either from any free text or using dynamic data, so-called tokens. Dynamic data consists of the parameter name and the name of the token in the syntax shown in the example below.
If required, predefined templates can be used as standardised message content, but all tokens can also be combined individually in any combination in a message. In the following message, the time stamp in two different formats as well as the event data of a PN-INspektor® NT event are sent as an example.

Example:

```
{       „timestamp“; <% data; general.timestamp %>,
        „timestampIso8601“; <% data; general.timestampIso8601 %>,
        “eventData”: <% data; diagnosis.jsonTriggerValues %>                    }
```

A list of all available tokens, incl. description texts and examples, can be found via the help symbol in the menu item or in the appendix of this manual in point 9. "MQTT tokens - dynamic data".

6. Linking triggers

Finally, any triggers are to be linked, when they are triggered the MQTT message is to be send

Example: Trigger & alert configuration drive 0815

In PROFINET controllers the maximum number of concurrent frame gaps permitted in the default settings without a system malfunction occurring is 3. In order to receive an early warning promptly at this point and prior to failure, the threshold value is set to 2 concurrent frame gaps in the PN-INspektor® NT. If there are then occasional single gaps in normal operation for process-related reasons, that can be considered perfectly normal. If these frame gaps accumulate to 2 due to ageing, an alarm is triggered by the PN-INspektor® NT; even though the bus system continues to function without device failure. Thanks to this timely warning, you now have time to react before system failure to get to the bottom of the issue.

With the settings in the following example (Figure 45), only the failure of “Drive 0815” causes a trigger. This results in an alert including a snapshot record in PROFINET-INspektor® NT, as well as the activation of the switch contact and the sending of an email notification.

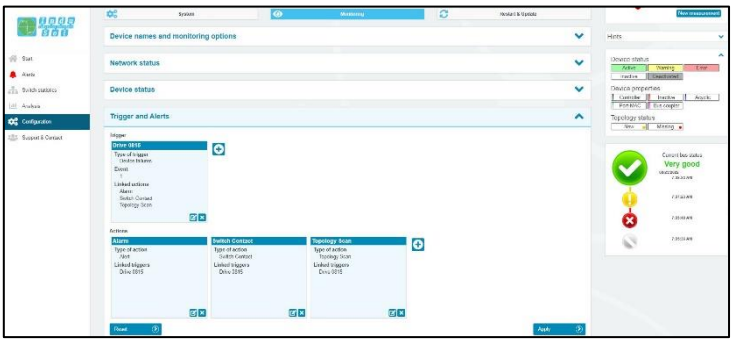


Figure 6024: Trigger setting failure "Drive 0815”

3.5.2.5 Automated report

The function “Automated report” provides you with the option of documenting the current system status at pre-set time intervals. These reports are then saved in the device regularly and are thus available to you for opening at any time (see item 3.4.2 Reports).

For the completion of the documentation, both the customer data and that of the system inspector can be added. Furthermore, the different sections for report creation can be selected or deselected, and an individual company logo can be used.

After creation, you can optionally select whether the data collected so far should be retained or deleted, or whether a new measurement should be started.

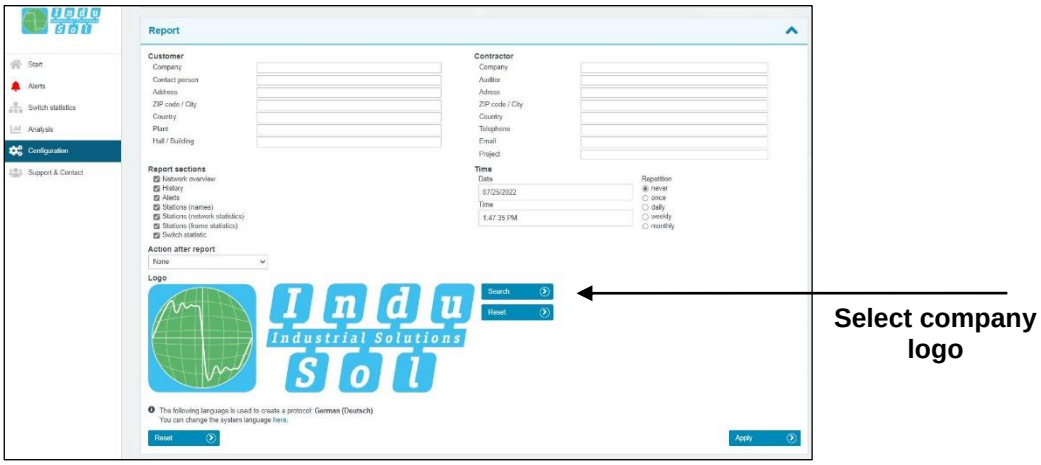


Figure 61: Selection window for automatic report creation

3.5.2.6 Network scan and Topology determination

The PROFINET-INspektor® NT offers a configuration option for up to 4 different network scan types, each of which can be activated and configured separately. The scans can then be carried out either manually or at cyclical intervals.

The following scan types are available for selection

- PROFINET scan (topology)
- Office scan (topology)
- Switch scan (query of switch statistics)
- OID scan (query of user-defined object identifiers)

The prerequisite for the PROFINET scan, the switch scan and the OID scan is the integration of the ACTIVE port into the network, whereas the scan of the office network is carried out via the PASSIVE port.

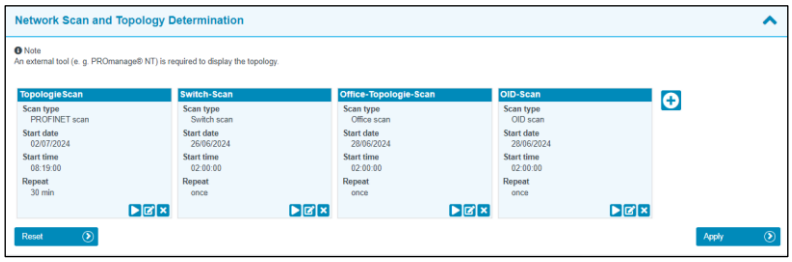


Figure 62: Settings for topology acquisition

A separate tile is created in the scan menu for each added scan, which describes the basic functions and properties of the scan. The scan can be configured using the three buttons at the bottom right of each tile. After selecting the two configuration buttons on the left, a new dialog window appears in which scan-specific settings and selection options such as start time, scan interval, SNMP community and scan range can be entered. The entries must be confirmed with OK so that the scan can be carried out correctly.

	Configuration and start of a one-off manual scan.
	Configuration and activation of a permanent, interval-controlled scan.
	Remove the current scan. Scan options can be added again at any time using the (+) button.

3.5.2.6.1 PROFINET Topologie Scan

By activating the Scan types "Activate PROFINET Topology Scan", the network structure of the PROFINET network is determined by the PROFINET-INspektor® NT via the AKTIV interface and then transferred to the PROmanage® NT monitoring software via Web API transmission for further evaluation and display. PROmanage® NT is a software installed on a central server for analysing, managing and storing device data to assess the communication quality of industrial networks. With the help of the topology information, a structure-related evaluation of the results and thus an efficient early detection of weak points as well as a targeted allocation of the device-related measured values in the event of a fault is possible.

Depending on the selection, the topology scan can be repeated at predefined time intervals or triggered once by selecting the "Start Scan" button. For this purpose, a start date and time for the first scan as well as the time span between two scans are specified. Furthermore, various address ranges can be edited, added or deleted based on the IP addresses. If no IP addresses are stored here, the address range of the configured AKTIV interface is automatically used for the topology scan and scanned for network participants within this range. The request interval (very high, normal, low) is set under Network Settings.

In addition to the default community "Public", further individual communities can be added to the community council list.

3.5.2.6.2 Switch Scan

By activating the Scan types "Switch Scan", the query of all values of the managed switches in the network is activated (see section 3.3. Switch statistics). The prerequisite for this is the integration of the AKTIV interface of the PROFINET-INspektor® NT into the network to be monitored (see section 2.6 Web interface).

The switch scan, like the topology scans, can be repeated at predefined time intervals or triggered once by selecting the "Start scan" button, depending on the selection. For this purpose, a start date and time for the first scan as well as the time span between two scans are specified.

The switches to be scanned must be selected once via the arrow button when configuring the switch scan for the first time and added to the switch scan. Alternatively, new devices can be added via the (+) button by entering the IP address.

In addition to the default community "Public", further individual communities can be added to the community council list.

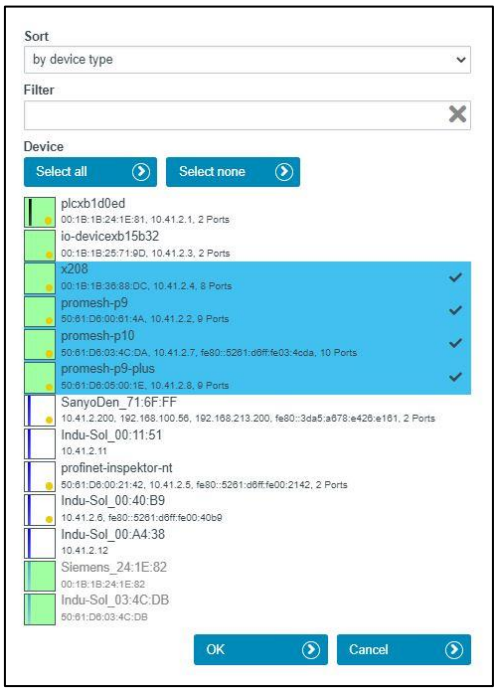


Figure 63: Adding switches to the switch scan

3.5.2.6.3 Office Topologie Scan

By activating the subitem "Activate Office Topology Scan", the network structure of the office network is determined via the PASSIVE interface by the PROFINET-INspektor® NT and then transferred to the monitoring software PROmanage® NT for further evaluation and display by means of Web API transfer. PROmanage® NT is a software installed on a central server for analysing, managing and storing device data to assess the communication quality of industrial networks. With the help of the topology information of the office network, device-related information and the associated structures of the higher-level networks can be summarised and visualised centrally.

Depending on the selection, the topology scan can be repeated at predefined time intervals or triggered once by selecting the "Start Scan" button. For this purpose, a start date and time for the first scan as well as the time span between two runs are specified. Furthermore, various address ranges can be edited, added or deleted based on the IP addresses. If no IP addresses are stored here, the address range of the configured PASSIVE interface is automatically used for the topology scan and scanned for participants within this range. The request interval (very high, normal, low) is set under Network Settings.

In addition to the default community "Public", other individual communities can be added to the community council list.

3.5.2.6.4 OID-Scan

By activating the scan type "OID Scan", the query of user-defined parameters (object identifiers) from the IP devices in the network is activated. The prerequisite for this is the integration of the PROFINET-INspektor® NT's ACTIVE interface into the network to be monitored.

An object identifier (OID) is a unique sequence of numbers that is assigned to a specific parameter of a device. For example, the parameter "sysDescr" has the OID ".1.3.6.1.2.1.1.1.0", which can be used to uniquely query the value of the content of the parameter at any time.

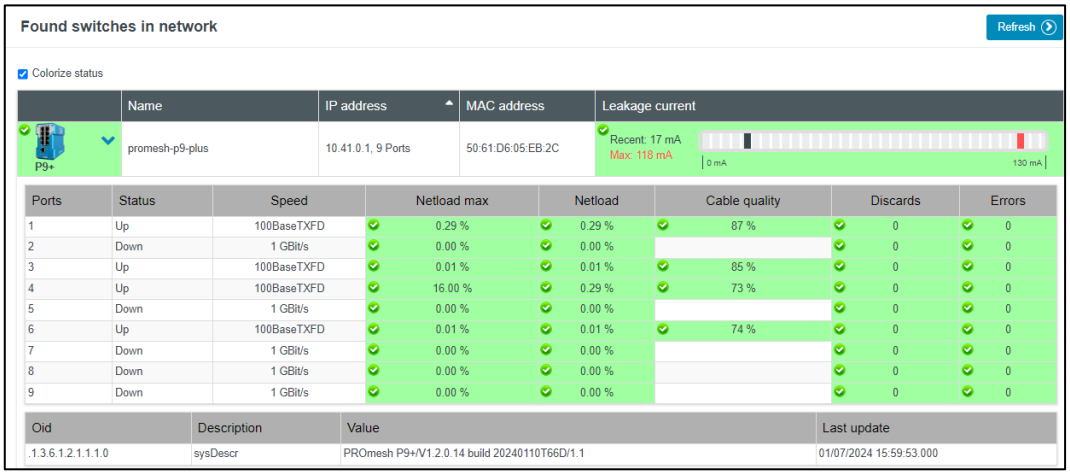
The OID scan can either be triggered once using the "Start scan" button or repeatedly at set intervals. A start date and time for the first scan and the interval between subsequent scans must be specified.

The request interval (very high, normal, low) can be adjusted in the network settings. In addition to the default community "Public", other individual communities can also be added to the community rate list.

Before the actual OID can be added, the first step is to select the device to be monitored by selecting an IP address. This can either be done using the arrow button by selecting the device from the device list or manually by adding the specific IP address.

In the second step, any number of object identifiers to be queried are added and configured for the selected IP address(es) using the (+) button. The entries can be subsequently adjusted using the "Edit" button and the "Remove" button.

All monitored object identifiers of an IP device are assigned to the monitored device in the menu item Switch statistics after a successful scan and can be found in tabular form below the switch statistics.



3.5.3 Firmware update

During the continuous further development of the PROFINET-INspektor® NT, new firmware versions are occasionally released. These can be installed via a firmware update from this menu item. To do this, the new firmware file is selected and uploaded via the "Browse" button. After successful installation, it is necessary to trigger a restart in the unit via the "Restart" button.

Figure 64: Firmware update

If you would like to be informed automatically about current firmware changes, you can register via our download area (https://www.indu-sol.com/en/support/downloads/update-service) by selecting the appropriate software.

4 Explanation of terms

4.1 PROFINET quality parameters

4.1.1 Bus node failures

In PROFINET node failures are diagnosed by means of the watchdog time of the controller or the node itself. This is determined by the set update time between the controller and node, as well as the number of accepted update cycles with missing I/O data.

If the watchdog time is exceeded, the PN-INspektor® NT reports a failure.

4.1.2 Bus node restart

The parameter 'Bus device restart' counts all device restarts that occur. A restart of a bus device occurs after a failure or a system start when a bus device has its parameters set by the control system without any faults and then begins the cyclical data exchange.

4.1.3 Releases

If it is necessary for the control of the process that additional PROFINET devices are required or are no longer required, then these can be logged out by the control so that no further cyclical PROFINET communication takes place. The logouts are evaluated with this counter “Releases”. After a successful release, the PROFINET device is not evaluated as failed if no PROFINET communication is detected.

Example: Robot that uses different tools with different PROFINET devices.

4.1.4 Alarm (high priority / low priority)

Diagnostics messages that appear are sent to the PLC as high-priority or low-priority alarms in PROFINET. The event-based division of these alerts (e.g. the shorting of an ET200S module) is defined by each manufacturer themselves for their devices. Unfortunately, a more precise definition is therefore not possible, since the alarms are classified system and node-specifically.

4.1.5 Update rate

The update rate is a fixed value (specific to each device) set in the controller (e.g. 1 ms) indicating the time between data updates in the controller and the I/O device. The decisive criterion for the actual update rate is the netload on the one hand, and the line depth, i.e. the installed network structure and the number of passing devices.

The increasing number of passing devices causes fluctuations in the transit time of telegrams, referred to as “jitter” (see point 4.1.7 Jitter).

4.1.6 Controller Transmit clock

This is the period between two consecutive intervals for IRT or RT communication. The transmit clock is the smallest possible transmission interval for data exchange. The calculated update times are a multiple of the transmission rate. We recommend to set the transmission clock to 1 ms.

4.1.7 Jitter

PROFINET communication is based on maintaining the set update rate of each device with the controller. Positive and negative deviations from this configured update time are referred to as “jitter” in PROFINET.

Jitter of up to 50% of the configured update time is in an acceptable range. Jitter values greater than 50% suggest network performance problems, device issues or an unfavourable layout of the network structure.

4.1.8 Telegram gaps

A telegram gap in PROFINET means the absence of an update time. Equally, a jitter of 100% may suggest a telegram gap. Telegram gaps are frequently caused by incorrect firmware versions of devices. In such cases the devices do not pass on a telegram or “forget” to send off their own telegram.
The threshold setting under the "Telegram Gap" selection item in the Triggers and Alarms menu (3.5.2.4 Triggers and Alarms) refers to the number per second.

4.1.9 Consecutive telegram gaps

The threshold value specification for the trigger type " Consecutive telegram gaps" determines the maximum permissible number of telegram gaps directly following each other.

4.1.10 Telegram overtakes

A telegram overtake may arise in PROFINET if peak loads occur in the switch or I/O device. When circumstances are particularly bad, a new telegram may be sent before an old one in the buffer of the switch. Telegram overtakes indicate excessive utilisation or device malfunctions.

4.1.11 Load ratio

The load ratio indicates the relation of the number of PROFINET telegrams to other telegram types in the same network (e.g. TCP/IP, Modbus TCP, etc.).

4.1.12 Error telegrams

This entry indicates the number of faulty telegrams detected in the PROFINET-INspektor® NT connection (checksum errors and packet fragments).

4.1.13 Netload

This includes the netload produced by all reports. This is given as a percentage based on the maximum possible load of a cable at 100 MBit/s. For stable system operation the netload should not exceed 20% in new systems.

4.1.14 Data throughput

The term data throughput in PROFINET refers to the amount of data per time unit that can be processed by the respective control (related to the process image).

4.2 Trigger types

4.2.1 Threshold-dependent trigger parameters

Often triggers are to be triggered and associated actions initiated as soon as certain quality criteria of the network have been exceeded or fallen short of. These "quality triggers" are summarised in the following list and can be configured separately for each of the parameters. To do this, simply define the corresponding trigger threshold values for the respective trigger type and link the actions to be carried out.

- Alarms (low priority)
- Alarms (high priority)
- Failures
- Restarts
- Abandonments
- Errors
- Telegram gaps
- Max. Number of consecutive telegram gaps
- Telegram overtakes
- Jitter
- Load ratio
- Network load
- S7 – communication
- Topology change

4.2.2 Status change

The "Status change" trigger becomes effective when an activated state from the "old state" selection list changes to an activated state from the "new state" selection for at least one device of the system to be monitored. The status functions are freely selectable.

4.2.3 History

The trigger type "History" causes after activation an alarm, as well as in the history overview the change of an activated state from the selection list " old state " to an activated state of the selection " new state " takes place. The status options are free selectable.

4.2.4 Global netload

By activating this trigger, the maximum value of the global network load is monitored and informed if it is exceeded. The selection windows can be used to define the limit value for incoming or outgoing data traffic within the specified observation period with a freely selectable load threshold.

4.2.5 Frame flood

Within the defined update times, there is usually no continuous data exchange within this time window, but peak loads often occur, which can also lead to disruptions of the telegram traffic. Such transients can be detected by selecting this trigger type. Settings for this are made by the direction selection of the data traffic, the maximum time between the packets and the maximum time of the packet flood.

4.2.6 New device detection

Starting from the currently available device list, an alarm is issued after activation of this trigger, just as another device is added. This indicates a change in the starting configuration.

4.2.7 Double addressing

For an error-free telegram flow a clear address assignment is a basic requirement. In order to receive an early indication of a double addressing, an alarm is issued via this trigger type. The trigger is always activated in the factory setting.

4.2.8 S7 Communication

Communication for parameterizing or querying a Siemens controller beyond the normal PROFINET telegram traffic is carried out via special telegram formats. An alarm can be triggered by setting this trigger to recognize whether accesses to the CPU have been executed (possibly for program changes).

4.2.9 Loop Detection

An increased number of broadcast telegrams can be an indication of an unwanted ring structure. As an early indication of this, the activated trigger function "Loop Detection" triggers a corresponding alarm. In the factory setting, this function is preset with a threshold value of 5000 broadcast telegrams/sec.

4.2.10 Interval

The "Interval" trigger can cyclically execute any linked actions at freely defined time intervals. For example, a topology scan could be triggered every hour via this trigger.

4.2.11 SNMP Trap

The trigger "SNMP Trap" can trigger linked actions as soon as SNMP traps are received from freely definable OIDs or IP ranges. Both the OID's and the IP ranges can be extended by any number of entries, IP ranges can optionally be automatically taken over from the set scan ranges of the active or passive interface, or the defined topology scan range.

4.2.12 Topology

In many applications, an automatically created topology can provide valuable information about current changes in the network structure. The trigger type "Topology" is used to report messages about newly added or deleted participants in comparison to the defined reference topology (see 3.1.4 Node overview).

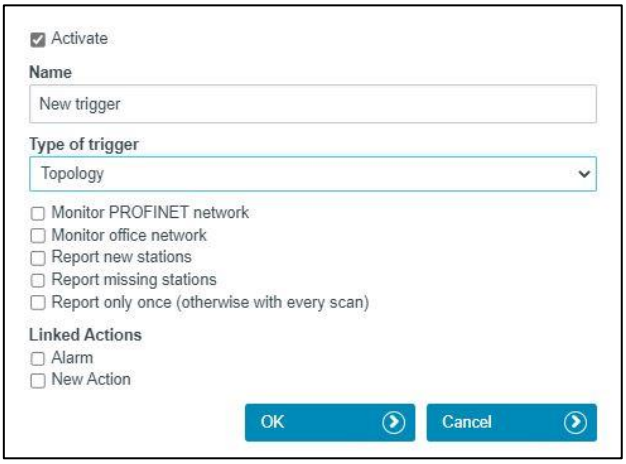


Figure 65: Trigger topology

To configure the trigger, first select whether only the PROFINET network, only the office network or both networks are to be monitored. Then select whether only new stations, only missing stations or both options should trigger the trigger event. Optionally, the alarm frequency (once / with every topology scan) is selected in the last selection item.

4.3 Other

4.3.1 IPv4

The Internet Protocol Version 4 (IPv4) is used in Ethernet networks for the logical addressing of devices. The IP address of a device can be freely selected and assigned. Devices that communicate with each other require an IP address from the identical range (determined by the subnet mask).

Example: 192.168.0.1

4.3.2 IPv6

The Internet Protocol Version 6 (IPv6) is used in Ethernet networks for the logical addressing of the devices and represents the extension to IPv4, whereby the maximum possible number of addresses to be used has been extended.

example: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344

4.3.3 Broadcast telegrams

A broadcast telegram is a message in which data packets are transmitted to all nodes of a communication network from one point. The term “broadcast telegrams” refers to the number of telegrams that have to be received by all nodes.

4.3.4 Multicast telegrams

Multicast describes a message transmission from one point to a group and is therefore a form of multipoint connection. There should not be too many of these types of telegram, because they burden the entire network.

4.3.5 Unicast telegrams

Unicast telegrams represent the communication between a sender and a single receiver.

4.3.6 ARP

The Address Resolution Protocol (ARP) is a network protocol that is used almost exclusively in connection with IPv4 addressing in Ethernet networks, i.e. to determine MAC addresses (hardware address of the devices) for assigned IP addresses. The result of this determination is stored in corresponding address tables.

4.3.7 DCP

The Dynamic Configuration Protocol (DCP) is used in PROFINET systems, for example, to address devices (IP configuration and PROFINET name) via the network or to find devices in the network.
Example: Each time a new PROFINET connection is established, the PROFINET device is searched for in the network using the PROFINET name.

4.3.8 MRP

The Media Redundancy Protocol (MRP) is used in PROFINET systems as a simple media redundancy solution. It allows a ring topology to be set up and prevents communication disruption in the event of a connection interruption within the ring with a guaranteed switchover time of no more than 200 ms.

4.3.9 LLDP

The LLDP (Link Layer Discovery Protocol) is a manufacturer-independent layer 2 protocol that offers the possibility of exchanging information between neighbouring devices.

4.3.10 PTCP

The prerequisite for synchronous real-time communication, such as for PROFINET IRT (Conformance Class C), is that all devices work with the same system time. For this time synchronisation, the Precision Time Control Protocol (PTCP) is used in PROFINET systems.

4.3.11 PN-RT

PN-RT (PROFINET real-time) telegrams are all telegrams that are used for cyclical real-time communication.

Example: Transmission of process data

4.3.12 PN-RTA

PN-RTA (PROFINET real-time acyclic) telegrams are all telegrams that are used for acyclic real-time communication.

Example: Transmission of alarms

5 Support and contact

Should you wish to contact us for any reason, further information can be accessed from this page.

You can find the manual stored in the download area as a quick aid as well as the Management Information Base (MIB) and Support data, which you can send to our service personnel if you need further help.

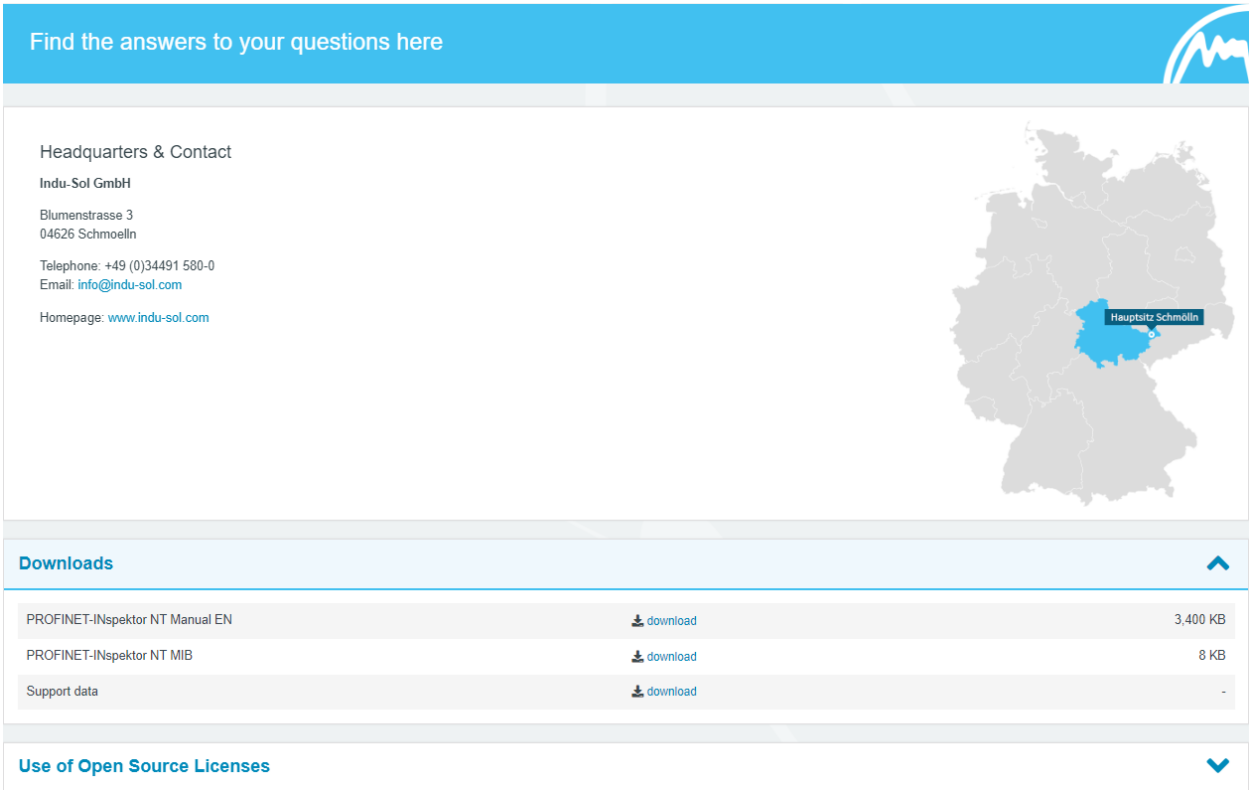
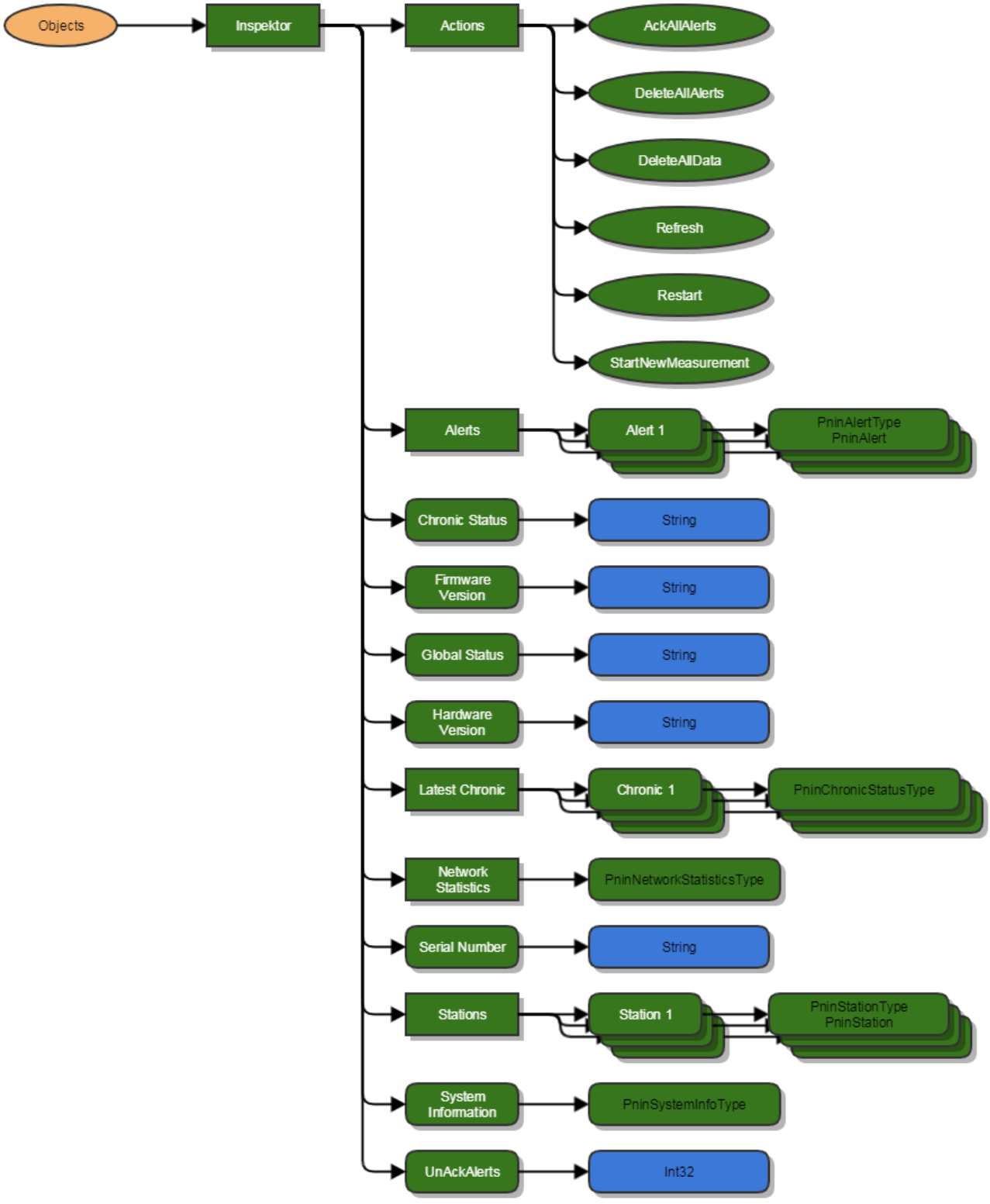
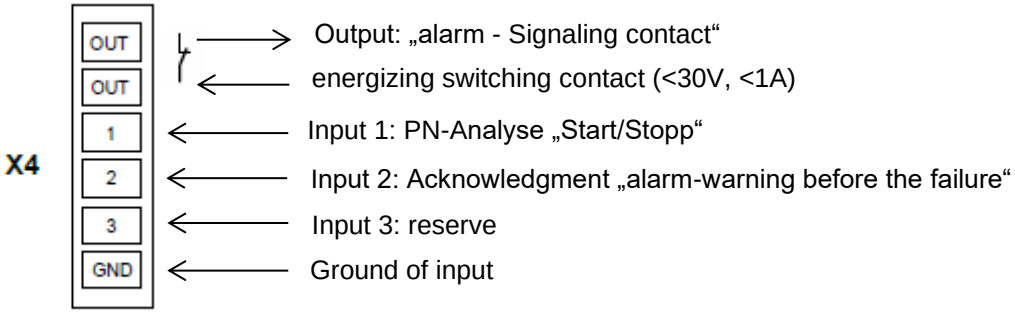


Figure 66: Support and contact

6 OPC UA Information Model



7 Example program for controlling the PN-INspektor® NT



Input 1: PN-Analyse „START / STOPP“

The input 1 is connected to an output of the PLC which outputs a signal from 0 to 1 (> 10V) as a continuous signal when the machine is enabled (**„**All media are switched on and the complete protection zone is active**“**). In the case of "**automatic operating stop**", wanted or unwanted, this enable (continuous signal) must be switched off and is thus set from 1 to 0.

Input 2: Acknowledgment „alarm-warning before the failure“

The input 2 is connected to an output of the PLC and serves to acknowledge the alarm message. This is to be executed as a switching pulse from 0 to 1 (> 10V).

Input 3: Reserve

Output: „alarm – Signaling contact“

The signaling contact is designed as a potential-free break contact. The confirmation is carried out as a function of the thresholds internally set in the PN-INspektor® NT. Alarms are signaled from 1 to 0.

Explanation of the target function:

- Scenario 1: Avoiding the alarm when the machine is booted:
  The PN-INspektor® NT data are deleted when the signal change at input 1 (START / STOP) of the PN-INspektor® NT continuous signal from 0 to 1.
  If a LOW level is present at input 1, the measurement/monitoring in PN-INspektor® NT is deactivated, no alarms are generated and it is shown accordingly in the display and on the website.
- Scenario 2: PROFINET alarm/warning:
  For a PROFINET alarm / warning, the NC (Normally Close) contact "OUT" The input on the PLC is switched from 1 to 0 and thus an alarm / warning for the visualization is output.

If the PROFINET alarm is acknowledged at the visualization, the output at the PLC, which is connected to input 2 (acknowledgment) of the PN-INspektor® NT, is to be provided with a switching pulse from 0 to 1. The alarm is acknowledged and the alarm contact is reset to the PN-INspektor® NT.

- Scenario 3: Automatic logging of the PN-INspektor® NT:
  In order to obtain a trace of the network state, a protocol is automatically created each time the machine is switched off in the PN-INspektor® NT. This is achieved by the use of the signal **AUTOMATIC START / STOP** during the signal change of the permanent signal 1 to 0 at input 1 (START / STOP) of the PN-INspektor® NT.

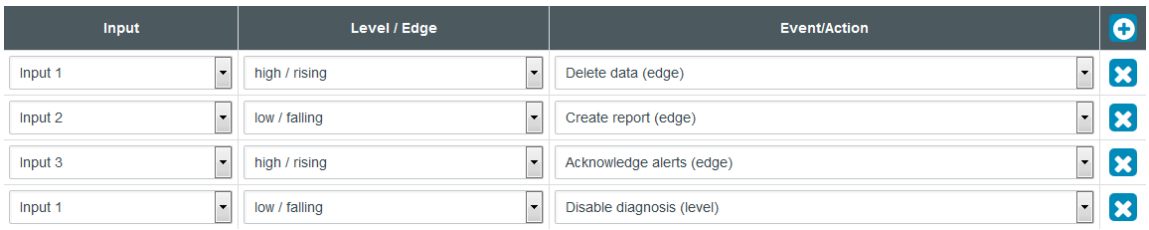
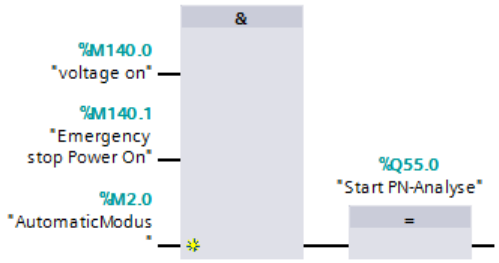


Figure 67: Configuration of the digital switching input

7.1 TiA-Portal Program example

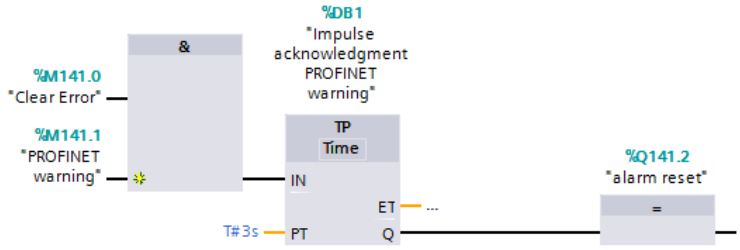
Netzwerk 1: Start PROFINET Analyse, High-Pegel on Output A.55

This message is started when voltage is present, no emergency stop is confirmed, eg automatic mode is active. If all conditions are fulfilled, a high level is present at the output,which goes to the first input of the INspektor.



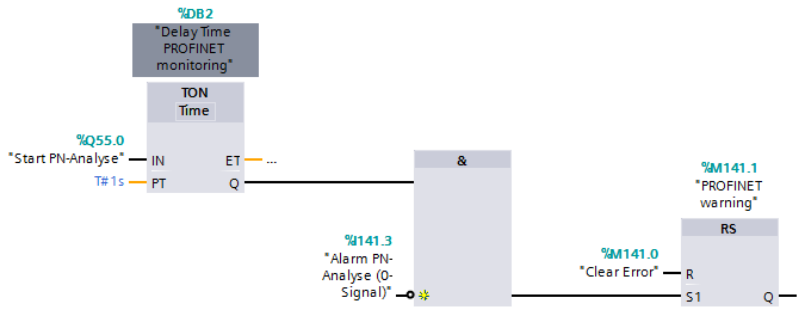
Netzwerk 2: Acknowledgment PROFINET Alarm/Warning

An alarm can be acknowledged by means of a pushbutton M142, but a high level is applied to input 2 of the INspector for 3s.



Netzwerk 3: PROFINET Alarm/Warning

If the PROFINET measurement (network 1) is running and an alarm is present at the output of the INspector, a PROFINET warning is output on the control panel.



8 Block diagram

The following image is a schematic diagram of the PN-INspektor® NT.

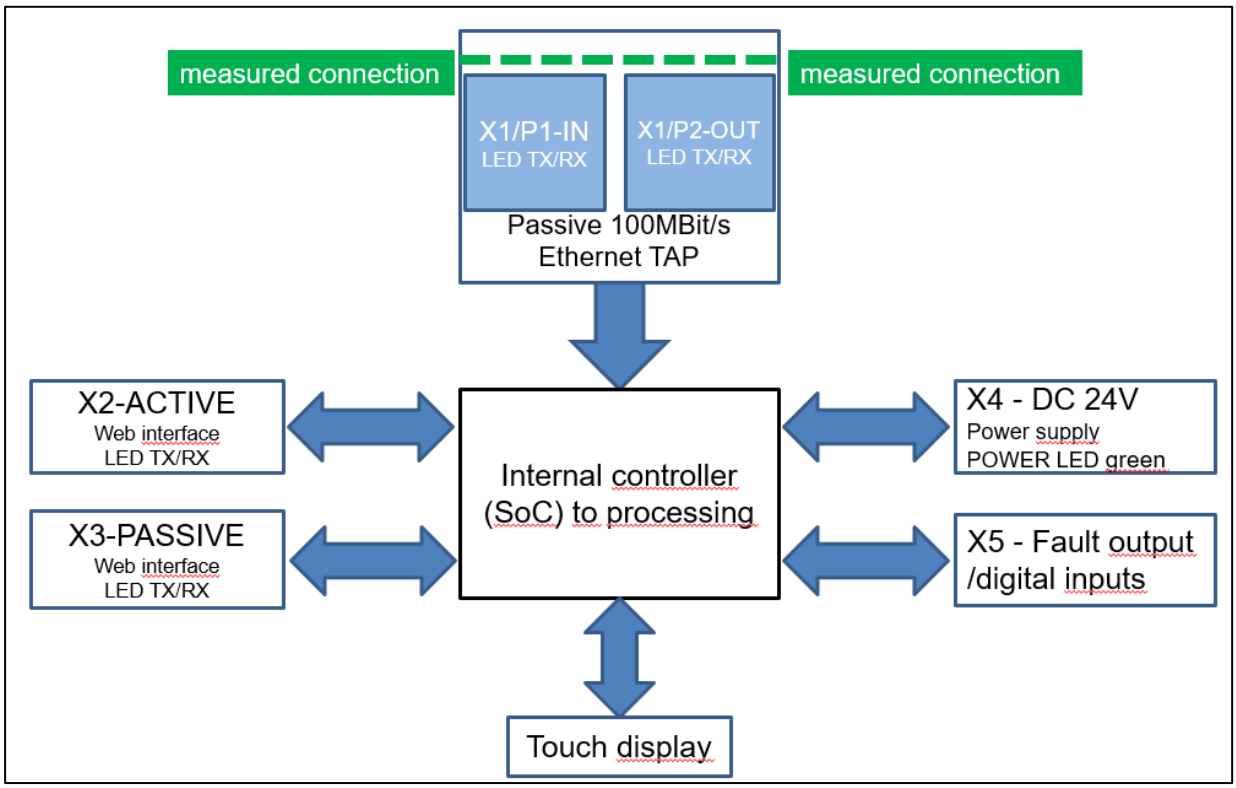


Figure 68: Block diagram

9 MQTT-Token – dynamic dates

It is possible to use dynamic data (tokens) in all MQTT messages. The tokens are replaced by the INspector with the real value before the messages are sent. With <% data; general.hostname %>, for example, the current hostname of the INspector can be inserted into the MQTT message. The following tokens can be used:

token name	description	example
connection.name	custom name of MOTT connection	My Custom Name
connecsion.clientEd	given client ID of MOTT connection	profinet-inspektor
connection.broker	address of MOTT broker	test.mosgvitto.org
connection.port	TCP/IP port of MOTT broker	1883
connection. keepAlive	keep alive of MOTT connection	60
connection. security	indecicates if MOTT connection should secured with TLS or not	0
connection. username	username used for authentication	userName
general. hostname	gives the hostname of the INspektor	profinet-inspektor-nt
general. location	gives the installed location	Home of INsepktor
general.complex	gives the network name of the INspektor	PROFINET
general.concact	gives the contact person of the INspektor	info@indu-sol.com
general.serialnumber	gives the serial number of the INspektor	00000001
general.version	firmware version of INspektor	2.3.0.0
general.timestamp	unix time-stamp	1135167516
general.timestampIso8601	ISO 8601 time-stamp	2021-10-28E13:11:56+0000
network.macActive	MAC address of active userface	60:61:D6:00:00:01
network.macPassive	MAC address of passive interface	80:61:D6:00:00:02
network.ip4Passive	first IPv4 of passive Interface	192.168.212.212
network.ip4Active	first IPv4 of active interface	192.168.213.212
diagnosis.jsonTriggerValues	all relevant information of an event raised by the Inspektor formatted as JSON	<JSON data>

10 Technical data

- Voltage supply: +24V DC
- Tolerance: ±10%
- Power consumption: Max. 350 mA
- Starting current: Max. 350 mA
- Dimensions (W x H x D): 105,2 x 123,2 x 128,8 (in mm)
- Assembly: TS35 DIN top-hat rail (EN 50022)
- Weight: 0.840 kg
- Protection class: IP20
- Operating temperature: +5 °C to +55 °C
- Storage temperature: -20 °C to +70 °C
- Relative air humidity: 10%…90%

10.1 Technical drawing

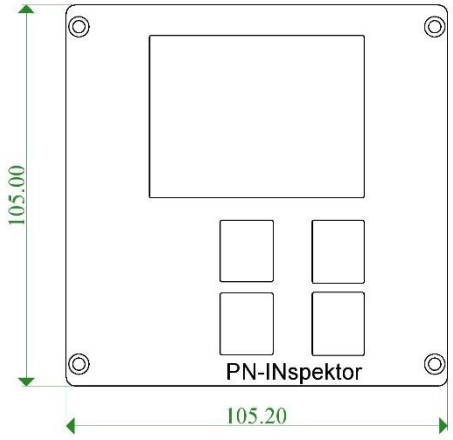


Figure 69: Front view

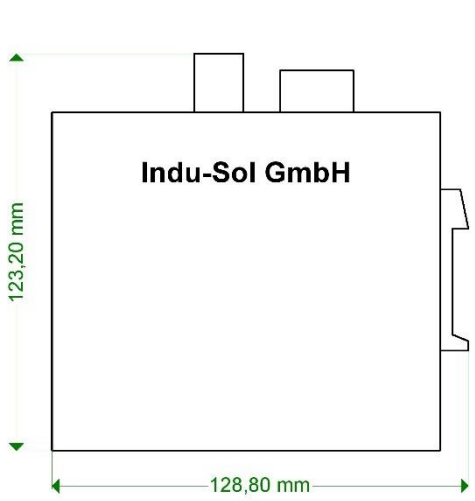


Figure 70: Side view with plugs and top-hat rail mounting

Indu-Sol GmbH
Blumenstrasse 3
04626 Schmoelln

Telephone: +49 (0) 34491 580-0
Telefax: +49 (0) 34491 580-499

info@indu-sol.com
www.indu-sol.com

We are certified according to DIN EN ISO 9001:2015