Indu-Sol GmbH – Specialist in fieldbus technologies

PROFINET-INspektor® NT

User Manual

Diagnostic and service tools for PROFINET / Ethernet

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

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

Caution!

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.

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 in order 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)
- CD with software for the report analysis and device manual

Please check the contents are complete before putting into operation.

1.4 General safety instructions

1.4.1 Operating personnel

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

Die Geräte sind für den Betrieb mit SELV-Spannungen (Safety Extra Low Voltage) über eine LPS (Limited Power Source) konstruiert. Es dürfen nur SELV/LPS konforme Sicherheitskleinspannungen nach IEC 60950-1 / EN60950-1 / VDE0805-1 zur Anwendung kommen bzw. Netzteile zur Spannungsversorgung nach NEC Class 2 (National Electrical Code).

Der Schirm der RJ45-Buchsen ist zur Ableitung von Störströmen mit dem Gerätegehäuse verbunden. Beachten Sie mögliche Kurzschlüsse bei Verwendung geschirmter Kabel.

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 Bestimmungsgemäße Verwendung

Die Geräte sind für den Einsatz im Industriebereich in der Schutzart IP20 konzipiert. Diese dürfen somit nicht direkt an das öffentliche Niederspannungsnetz angeschlossen werden, die Montage ist in einem industriellen Schaltschrank durchzuführen.

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 Device ports and status indicators

2.1 Device ports

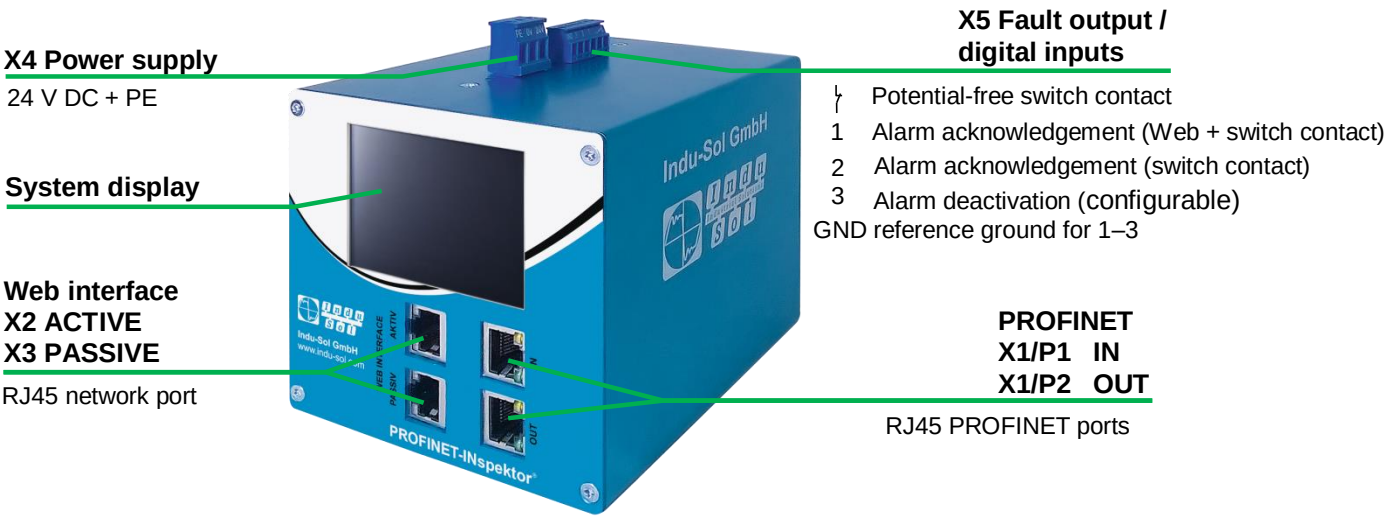


Figure 1: Device ports

3 Installation

3.1 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:

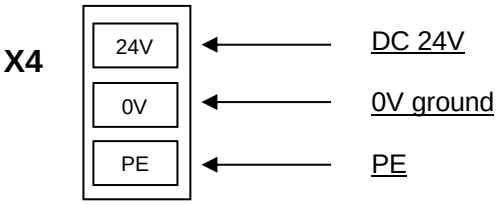
- From left and right: 20 mm
- From top and bottom: 50 mm

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

Figure 3: Removal

3.2 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.

3.3 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.

3.4 Connection to the PROFINET network

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

3.4.1 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.

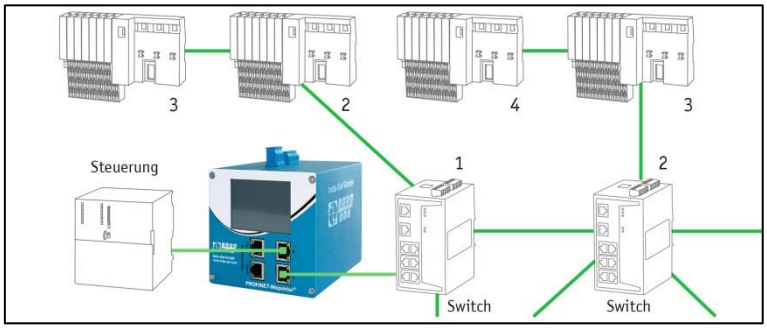


Figure 4: PROFINET-INspektor® NT fixed installation

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

3.4.2 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.

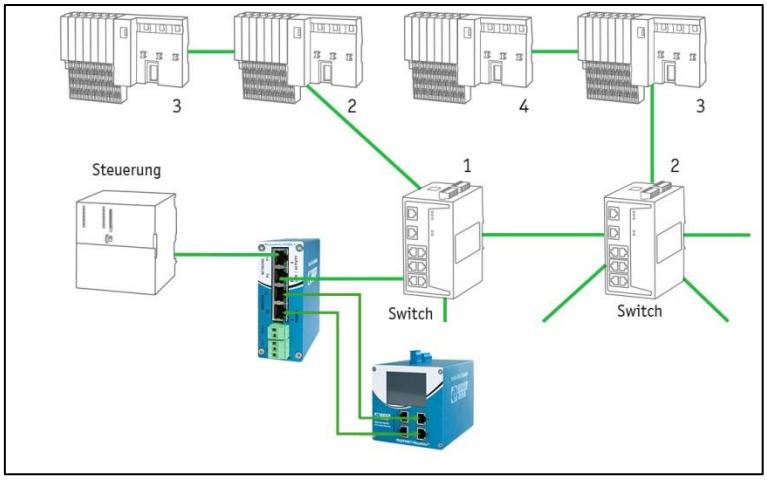


Figure 5: PN-INspektor® NT connection via PNMA II

3.5 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 10 or Mozilla Firefox from version 11; 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:

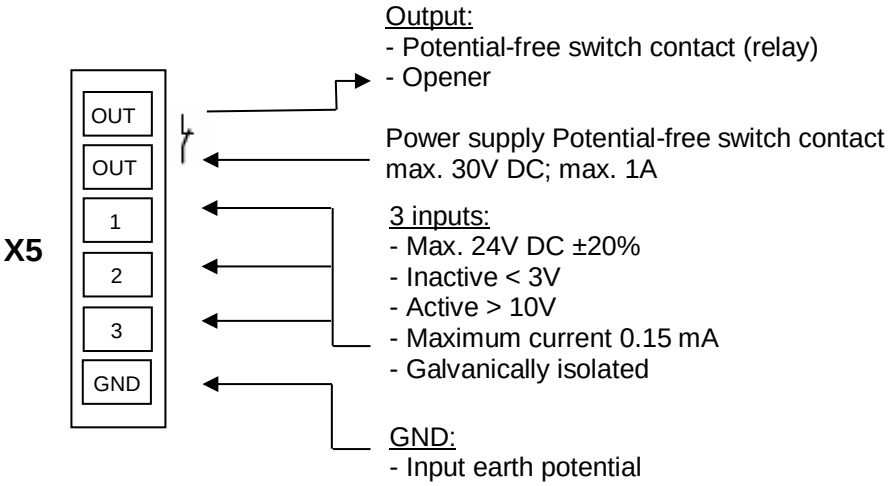
	PASSIVE – X2	**ACTIVE – X3**
IP address:	192.168.212.212	192.168.213.212
Subnet mask:	255.255.255.0	255.255.255.0

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 4.5.1.4 Network) and integrated into the network (e.g. via a free switch port).

3.6 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 4.5.1.6. Digital Input)

3.7 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 6: Touch-Screen menu

4 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 are 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.

4.1 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.

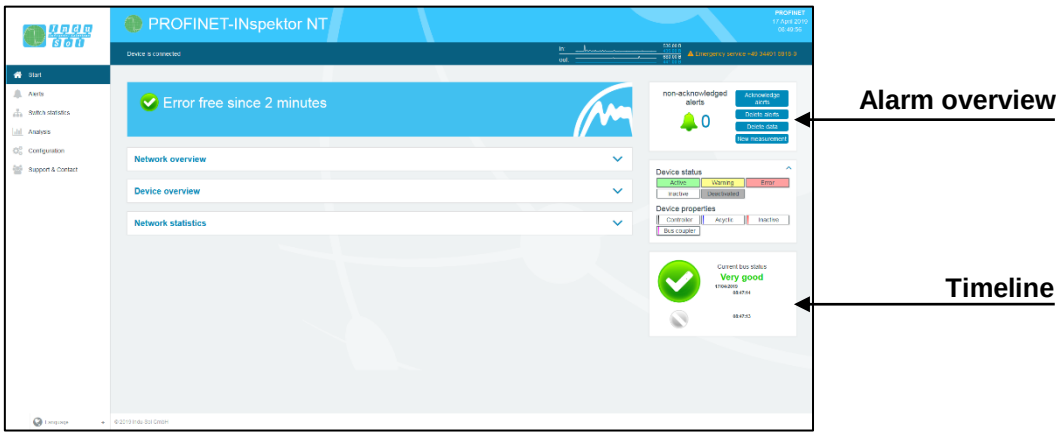


Figure 7: Complete overview

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 4.5.1.3 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.

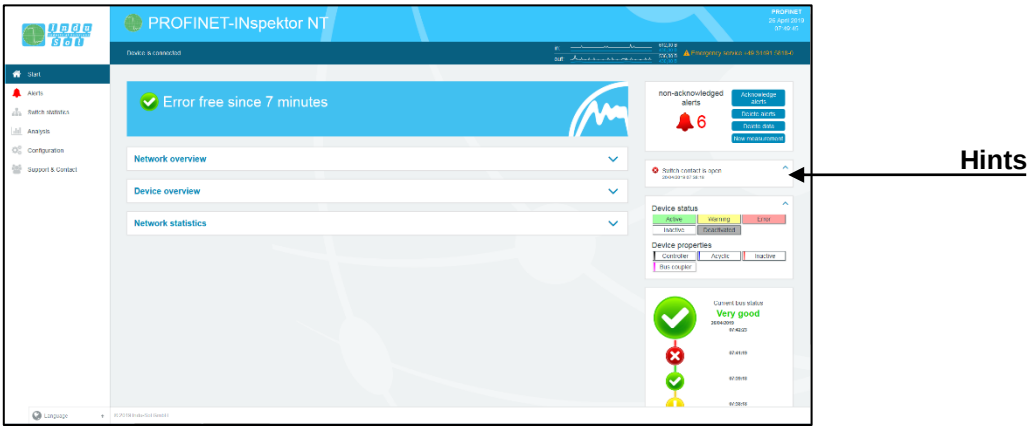


Figure 8: General overview in case of error

If the switching contact is activated at this time (see section 4.5.2.3 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 4.5.2.2. Device status) are indicated by the message "Status Settings have been changed" and in the "Triggers & Alarms" menu (see section 4.5.2.3 Triggers & Alerts) by the display "Alarm Settings have been changed".

4.1.1 Alarm overview

In the alarm overview the number of unacknowledged alarms are 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.

4.1.2 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 period for a status change (new nodes) is one minute.

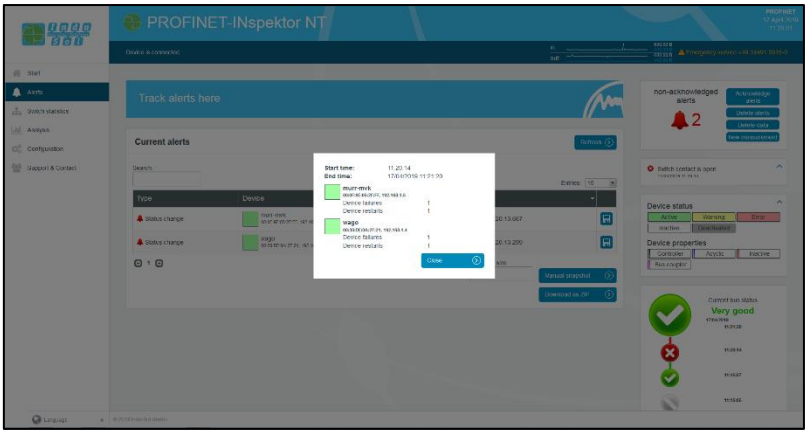


Figure 9: Timeline entry

The individual status changes can be adjusted for each node separately (See point 4.5.2.2 Device status) in order to adapt the display to the plant conditions.

4.1.3 Network overview

You obtain a complete overview of all the important quality parameters of the PROFINET master system through the “Network overview” selection window. These form the basis for evaluating a network’s stability. The individual parameters are explained in more detail in point 5. Device parameters. To make it easier to evaluate the quality parameters, they can be coloured according to predefined acceptance values. (see point 4.5.2.6 Control mode)

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 5. Device parameters. For a simple evaluation of the quality criteria, these can be highlighted in color using predefined limit values by selecting the "Activate acceptance mode" function (see section 4.5.2.6 Control mode).

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.

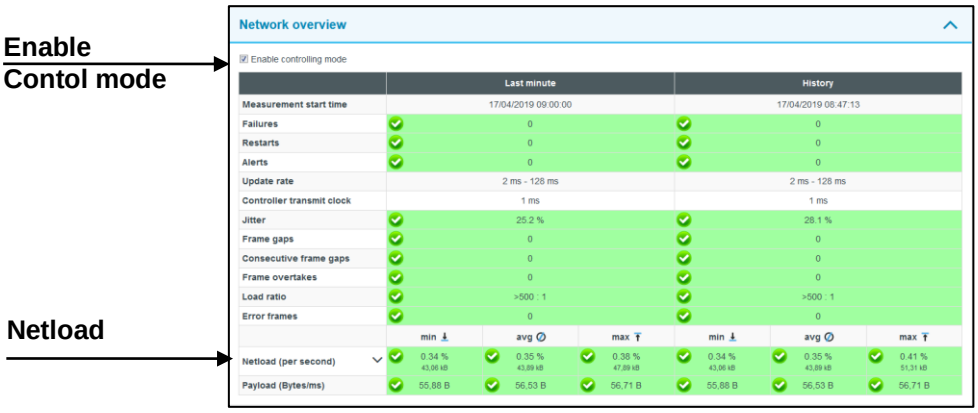


Figure 10: “Network overview” selection window

4.1.4 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.

For greater clarity, you can select the displaying of different types of protocol and individual evaluation criteria. To display all configured device Information (PN-Name, IP-Adresse), it is possible to start a device scan to retrieve the information (see section 3.5 Web interface).

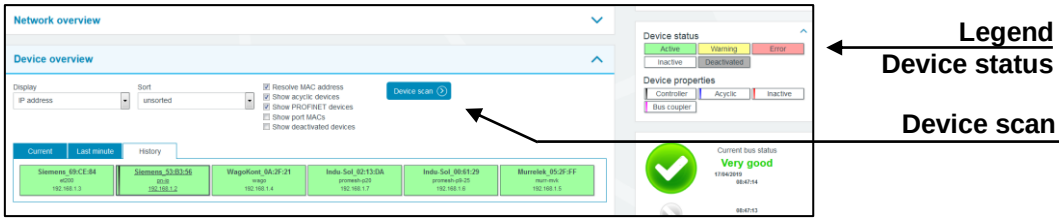


Figure 11: “Node overview” selection window

For a detailed view of device information, select the relevant device with a mouse click. The essential data for evaluating the communication quality of this node is then displayed.

Enable controlling mode

	General					
MAC address	Siemens_53:B3:56					
IP address	192.168.1.2					
Name	pn-io					
Alias						
Device Type Name	S7-300					
Vendor ID	SIEMENS AG (42)					
Device ID	257					
Device role	Controller					
	Last minute			History		
Alert (low priority)	0			0		
Alert (high priority)	0			0		
Failures	0			0		
Restarts	0			0		
Frame gaps	0			0		
Consecutive frame gaps	0			0		
Frame overtakes	0			0		
Error frames	0			0		
Jitter	0.1 %			0.1 %		
	min	avg	max	min	avg	max
Update rate	2 ms	-	128 ms	2 ms	-	128 ms
Transmit clock	1 ms	-	1 ms	1 ms	-	1 ms
Measured update rate	2.00 ms	78.80 ms	128.00 ms	2.00 ms	78.80 ms	128.00 ms
Payload (sent)	28,34 B	28,54 B	28,60 B	28,20 B	28,54 B	28,64 B
Payload (received)	27,72 B	28,00 B	28,07 B	27,68 B	28,00 B	28,11 B
Netload (sent per sec)	0.35 % 43,79 kB	0.35 % 44,11 kB	0.36 % 44,41 kB	0.35 % 43,59 kB	0.35 % 44,11 kB	0.36 % 44,54 kB
Netload (received per sec)	0.35 % 43,20 kB	0.35 % 43,57 kB	0.35 % 43,73 kB	0.34 % 43,06 kB	0.35 % 43,57 kB	0.35 % 43,80 kB

Figure 12: 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 | 0%)	0 (0 | 0%)
Multicasts (of these PROFINET)	24 (0 | 0.00%)	798 (0 | 0.00%)
Frames (sent) (of these PROFINET)	752.345 (752.343 | 100.00%)	25.023.838 (25.023.836 | 100.00%)
Frames (received) (of these PROFINET)	753.696 (753.696 | 100.00%)	25.068.810 (25.068.810 | 100.00%)
Bytes (sent) (of these PROFINET)	51,16 MB (51,16 MB | 100.00%)	1,70 GB (1,70 GB | 100.00%)
Bytes (received) (of these PROFINET)	50,84 MB (50,84 MB | 100.00%)	1,69 GB (1,69 GB | 100.00%)
Error frames (sent) (of these PROFINET)	0 (0 | 0%)	0 (0 | 0%)
Error frames (received) (of these PROFINET)	0 (0 | 0%)	0 (0 | 0%)
Payload (sent)	33,10 MB	1,10 GB
Payload (received)	32,75 MB	1,09 GB

Figure 13: Device-related network statistics

4.1.5 Network statistics

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

Figure 14: Whole system network statistics

4.2 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).

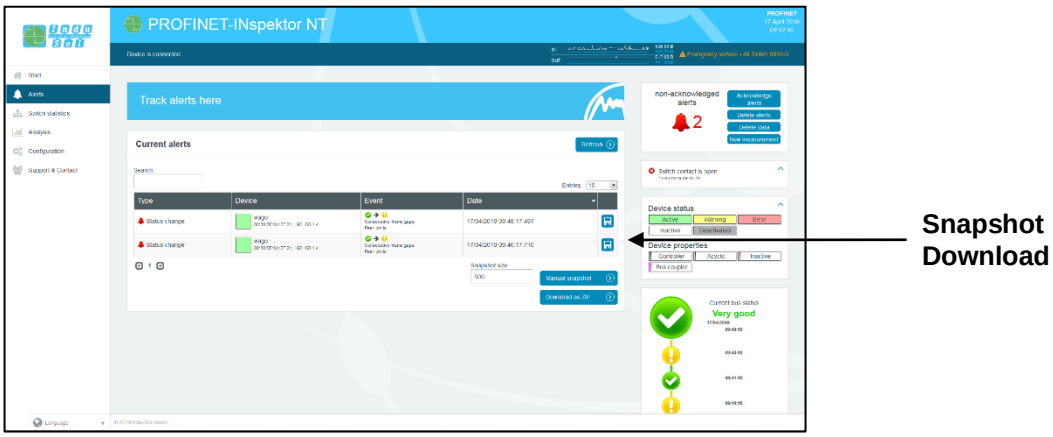


Figure 15: Alarms

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.

4.3 Switch statistics

This overview serves the central representation of all switch statistics of the PROmesh series from Indu-Sol available in the network. All relevant data for the proof of a stable communication (network load, discards, errors, leakage current) are queried and listed device related. The listed information is updated every minute. An active scan process is symbolically displayed in the status bar at the top. The switch name is automatically entered after a device scan 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 3.5 Web interface) as well as the activation and definition of the address range to be scanned in the menu item: 4.5.2.5 Network scan and topology determination

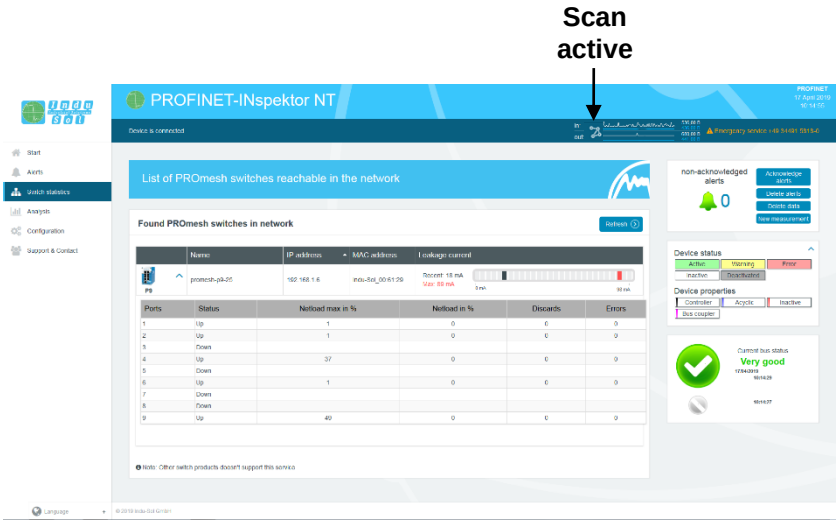


Figure 16: Switch statistics

4.4 Analysis

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

4.4.1 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 17: Netload charts

4.4.2 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 4.5.2.4 Report).

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

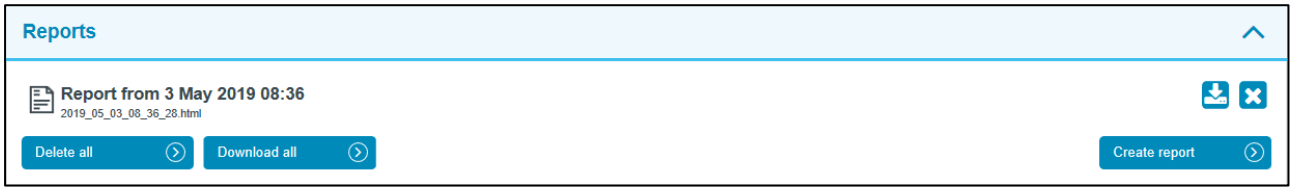


Figure 18: Reports

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

4.4.3 Topologies

By starting a scan process, the current device information as well as the real wiring structure (topology) of all participants of the PROFINET network present in the set address range are queried and merged in a file (.topo). The resulting files can be evaluated using the PROscan® Active software (chargeable; not included in the scope of delivery).

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 3.5 Web interface).

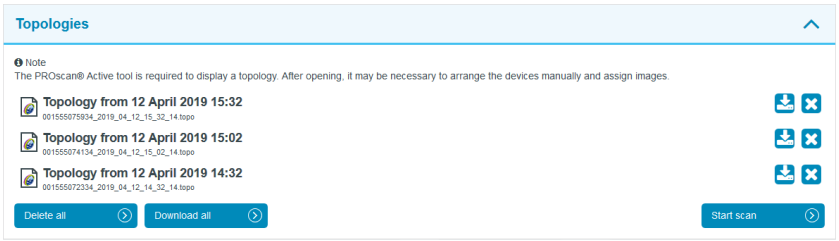


Figure 19: Topologies

4.4.4 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.

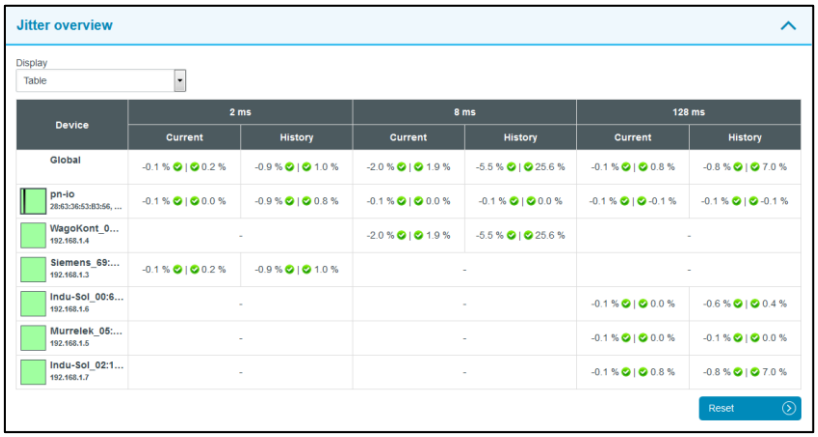


Figure 20: Jitter overview

4.4.5 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 at a glance.

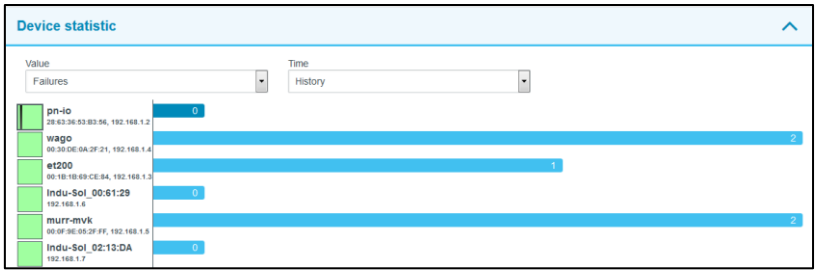


Figure 21: Node statistic

4.4.6 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.

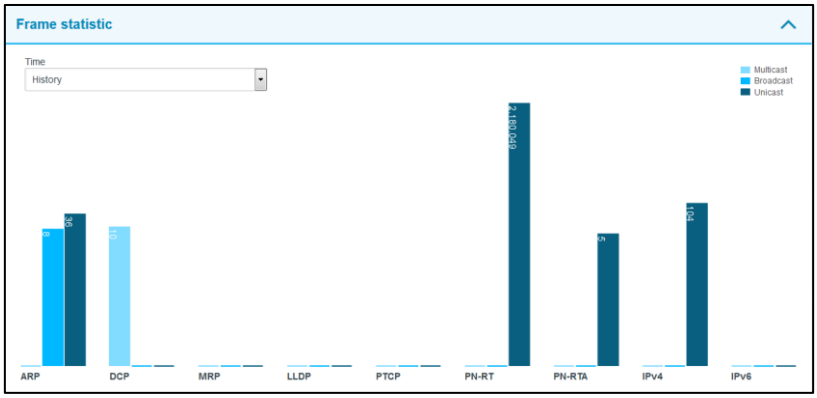


Figure 22: Frame statistic

4.4.7 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

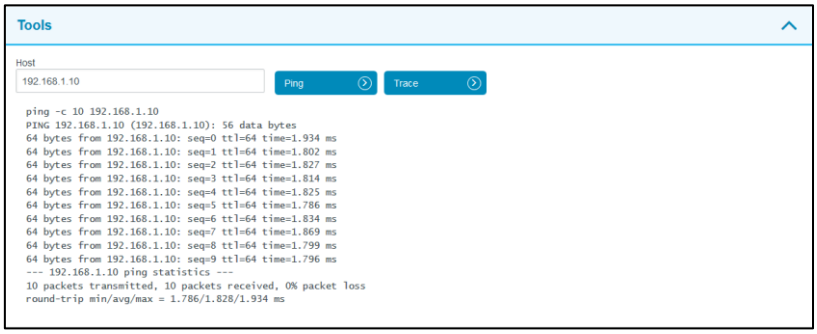


Figure 23: Tools

4.5 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.

4.5.1 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.

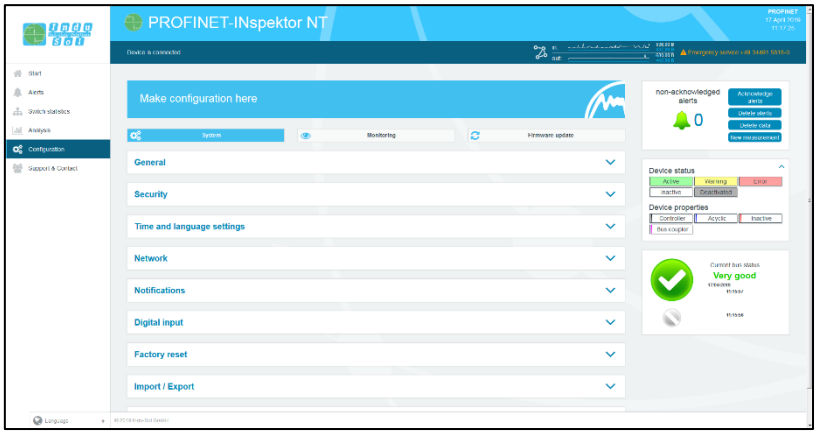


Figure 24: System settings – complete overview

4.5.1.1 General

In this sub-menu, entries can be made for device name, installation location, network name and notes that provide a more detailed description of the device and the network to be monitored. In addition to these entries, this menu allows setting up a password for the PN-INspektor® NT. This password will then be required for all changes made to device and monitoring settings. A general access restriction is not provided.

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.

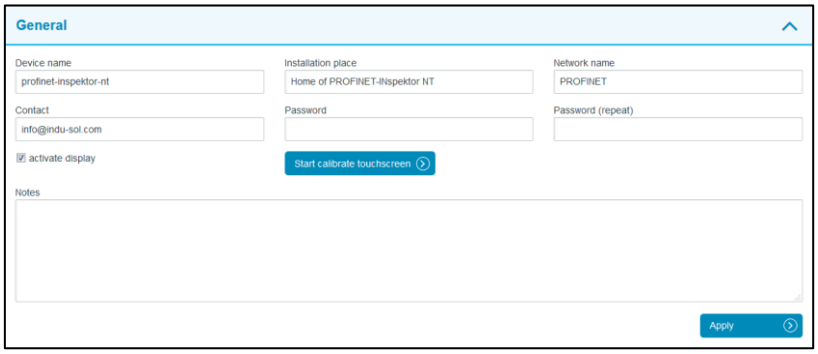


Figure 25: System settings – general

4.5.1.2 Security

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

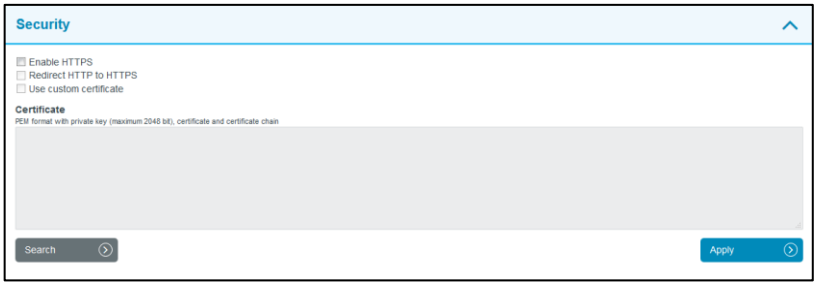


Figure 26: Security

4.5.1.3 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.

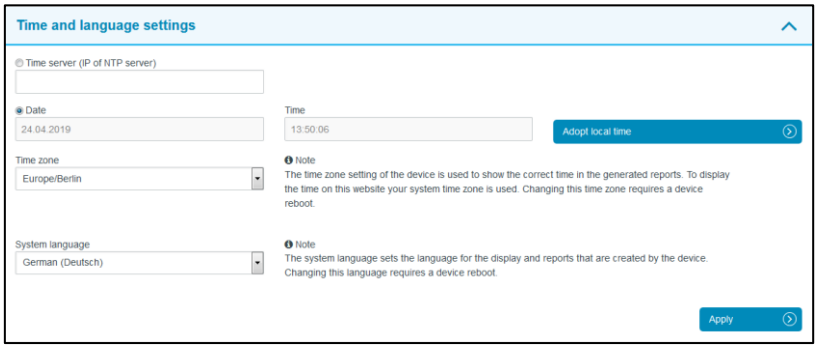


Figure 27: Time and language settings

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 4.1 Homepage).

Changing the language setting requires a device restart.

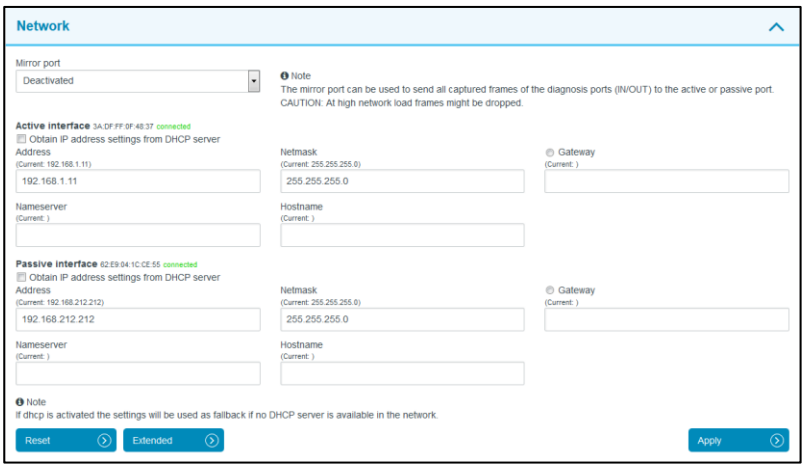
4.5.1.4 Network

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 current 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.



,

Figure 28: Network settings

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

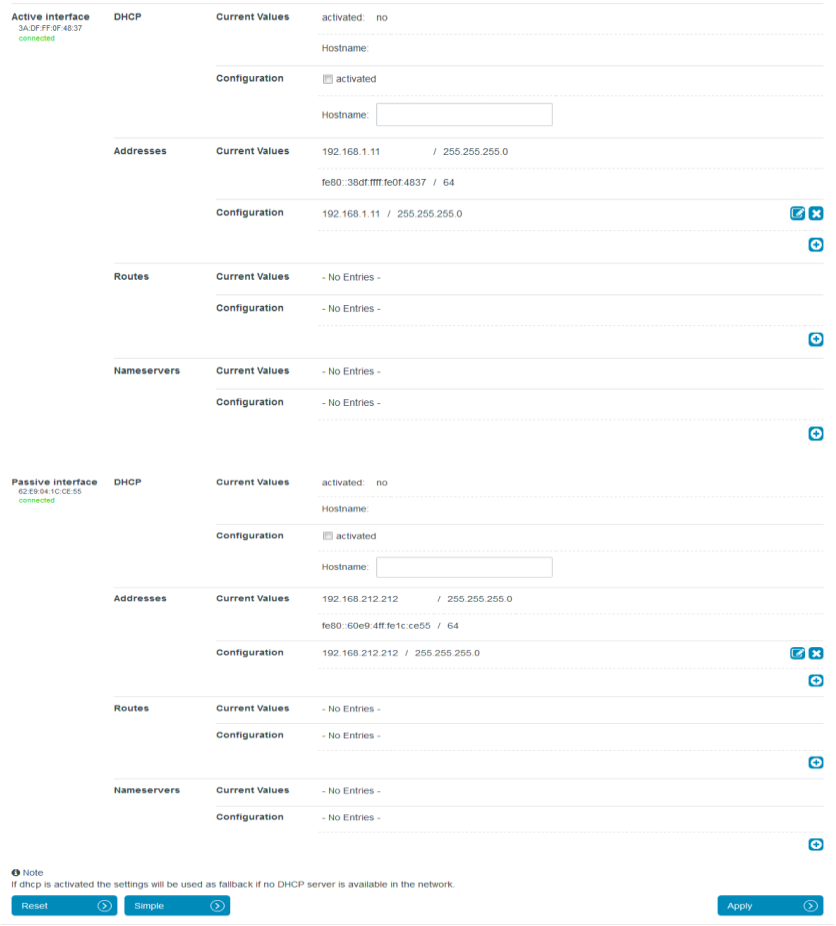


Figure 29: Network settings – extended view

4.5.1.5 Messages

With the message function, it is possible to arrange the sending of an email through the PN-INspektor® NT in the event of an alarm. To do this you require a valid recipient address, the IP address of the email server resp. SNMP trap host and an Ethernet connection between the device and the server.

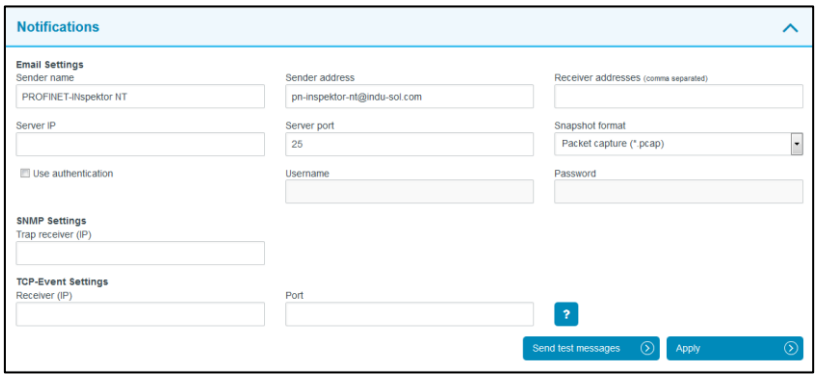


Figure 30: “Messages” selection window

For email alerts, it is imperative that the “Email” action has been activated for the desired trigger condition (see section 4.5.2.3 Triggers & Alarms).

Only unencrypted mails can be sent.

4.5.1.6 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

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

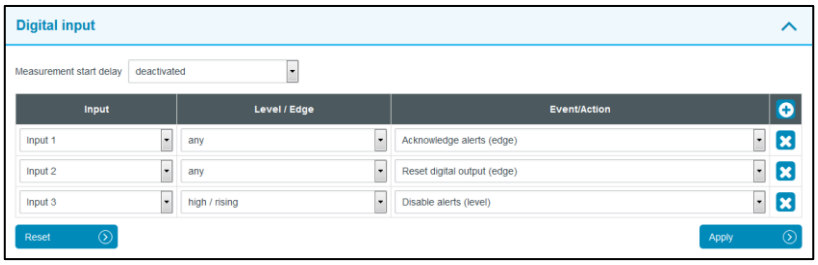


Figure 31: Digital Input

4.5.1.7 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.

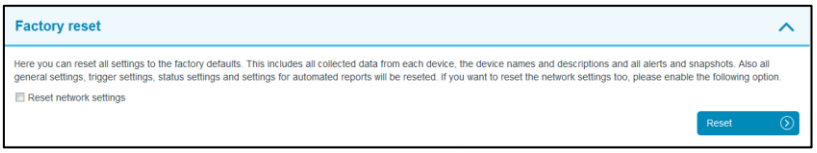


Figure 32: Factory reset

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

4.5.1.8 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.

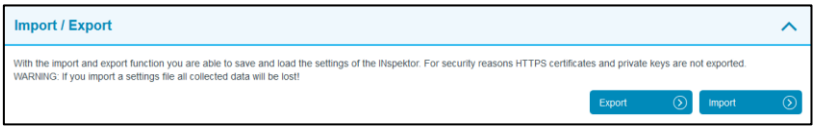


Figure 33: Import/Export

4.5.1.9 Information

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

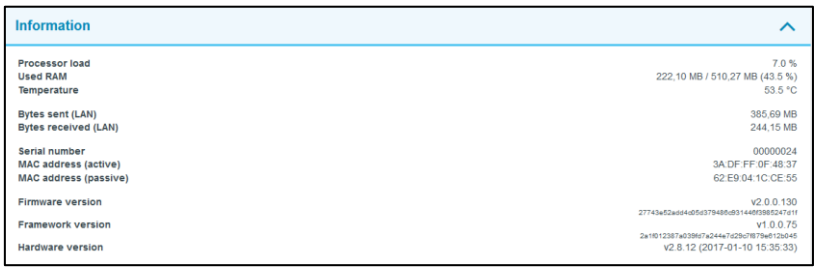


Figure 34: PN-INspektor® NT device information

4.5.2 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.

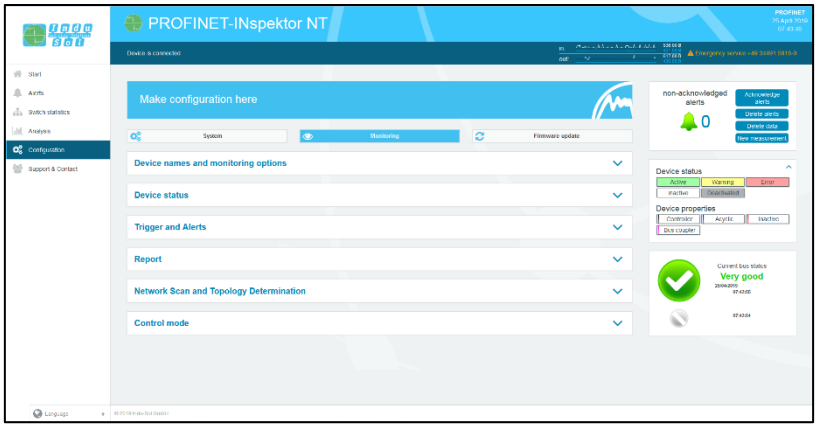


Figure 35: Monitoring – complete overview

4.5.2.1 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, this menu allows to deactivate monitoring for individual or newly detected devices or limited the analysis to the device, which communicate exclusively with the corresponding station.

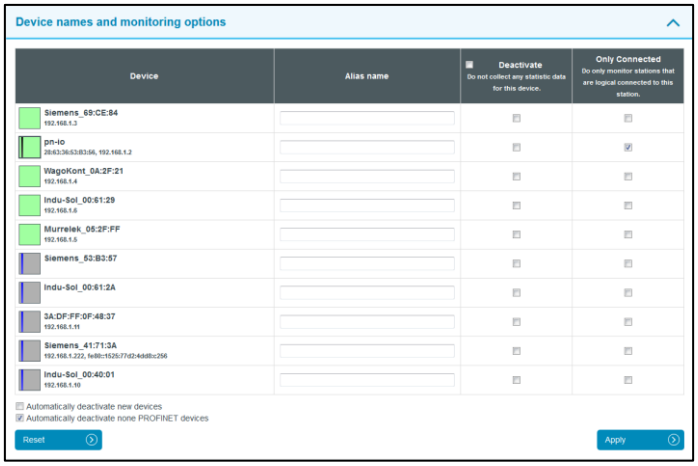


Figure 36: overview node names

4.5.2.2 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.

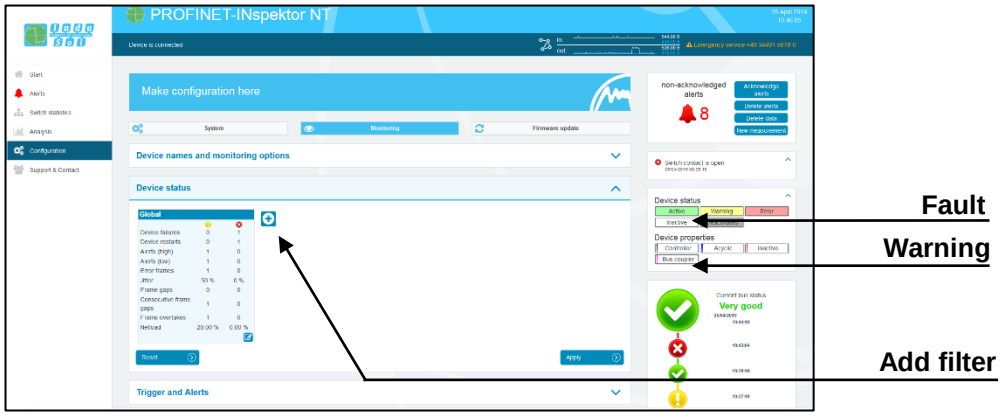


Figure 37: Node condition – default setting

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.

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 ET200SP was fully deactivated.

Figure 38: Applying filters

The setting options in the editing window for the selected controller become clear in the following picture. By setting the event to "0" (telegram gap → 0) it is deactivated for the analysis.

Figure 39: 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).

4.5.2.3 Triggers & alarms

For the configuration of alarms and evaluation through switch contact, snapshot, email and SNMP Trap, the relevant parameters can be set under the item “Triggers & alarms”.

In the device’s default settings, all fault events of any PROFINET node automatically lead to an alarm entry in the status display and timeline, the creation of a fault record (snapshot), the connection of the switch contact and notification via email and SNMP-trap (if configured). The number of telegrams before and after an event can be set between 0 and 50,000 to define the snapshot size as required. If the snapshot size is set higher, less snapshots can be saved (e.g. maximum 4 snapshots at 50,000 before and 50,000 after trigger event).

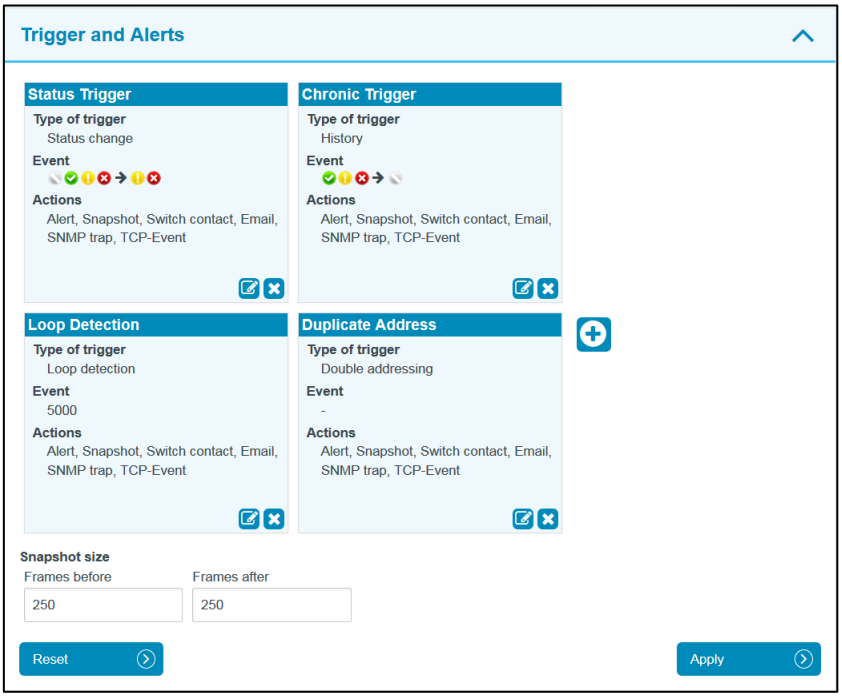


Figure 40: Triggers & alarms – default setting

Through a variable configuration of fault triggers in the form of different trigger types and special node addresses, it is possible to make the relevant adjustments here for a targeted fault search or targeted node monitoring.

The various options for editing individual filters are described in greater detail below.

By selecting the editing mode via the edit icon, the selection menu opens for adjusting the settings.

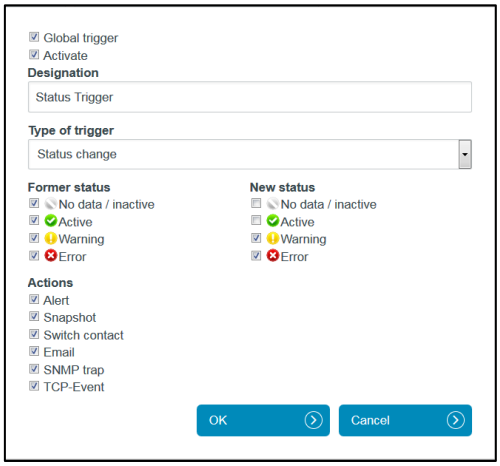


Figure 41: Selection menu for trigger type “status change”

The menu presented in Figure 42 is available for specifying the trigger type.

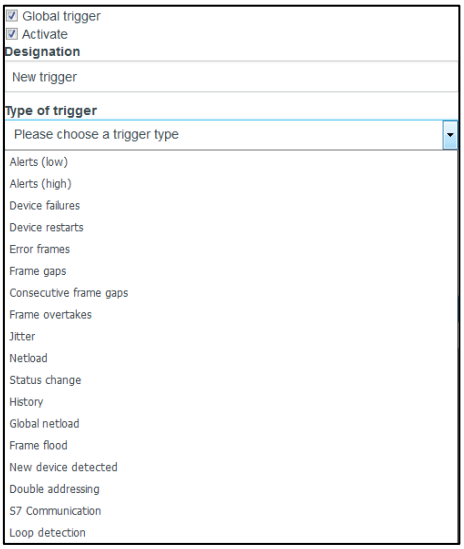


Figure 42: Trigger types

A more detailed explanation of the individual functions can be found under point 5. Device parameters / Trigger types.

In the case of threshold-related alarms, the number of events that are to trigger a trigger is specified in the corresponding submenu.

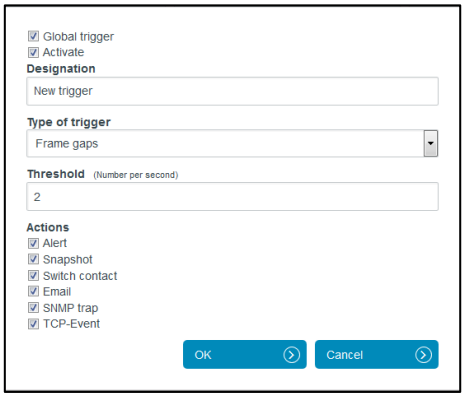


Figure 43: Threshold value setting for telegram gap

The assignment of individual actions to the corresponding trigger type determines the actions to be executed in the event of an alert.

In addition, an address-related selection of triggers is provided. By default, the monitoring of all participants is active (global). By deselecting the "global trigger" item, one or more devices from the address list can be activated via the participant overview that appears.

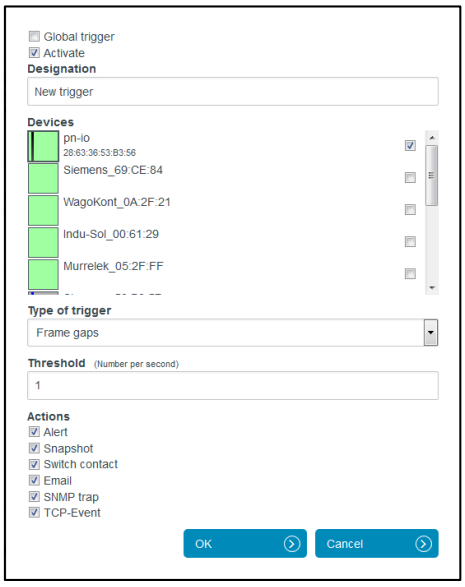


Figure 44: Address list example

The entire range of setting options can be used to provide an early warning to indicate the first signs of a deterioration in communication before a device failure occurs.

The item "Reset" returns all changes to the initial state (factory setting).

Example: 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.

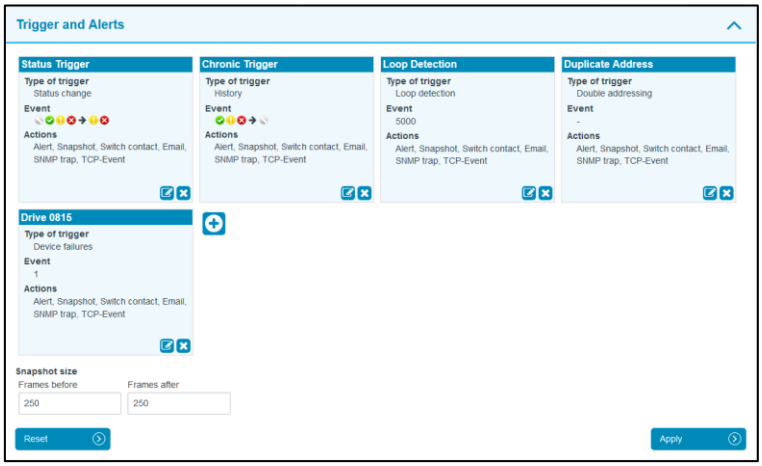


Figure 45: “Drive 0815” failure trigger setting

4.5.2.4 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 4.4.2 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.

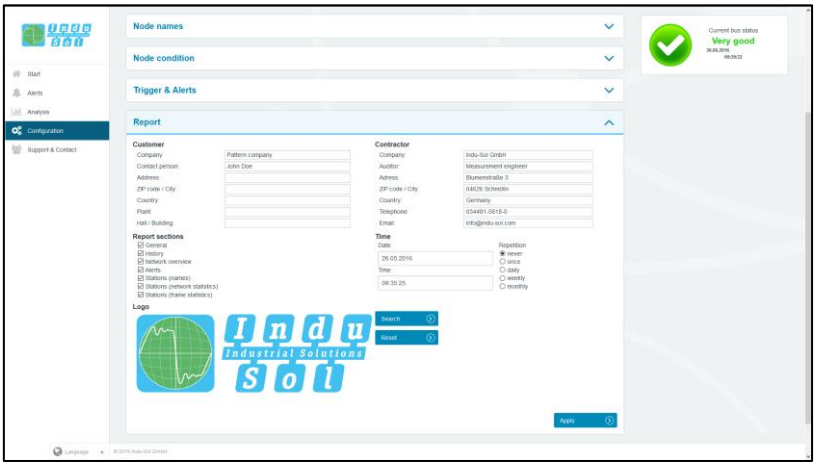


Figure 46: Selection window for automatic report creation

4.5.2.5 Network scan and Topology determination

After activating the corresponding settings on this page, the PROFINET-INspektor® NT executes a network scan at cyclic intervals to query the switch statistics (see section 4.3 Switch Statistics) and/or a topology scan (see section 4.4.3 Topologies). The prerequisite for this is the integration of the AKTIV port into the network (see section 3.5 Web interface).

By activating the option "Topology", the network structure is determined by the PROFINET-INspektor® NT and afterwards the network structure is given to the monitoring software PROmanage® NT via Web API transmission for further evaluation and display. PROmanage® NT is a software installed on a central server for the analysis, management and storage of device data for the assessment of 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 purposeful allocation of the device-related measured values in case of failure is possible.

Depending on the selection, the scan function can be repeated at specified time intervals. A start date and time for the first scan as well as the time interval between two scans are defined. Furthermore, different address ranges can be edited, added or deleted by using the IP addresses. The request interval (very high, normal, low) is set under Network settings.

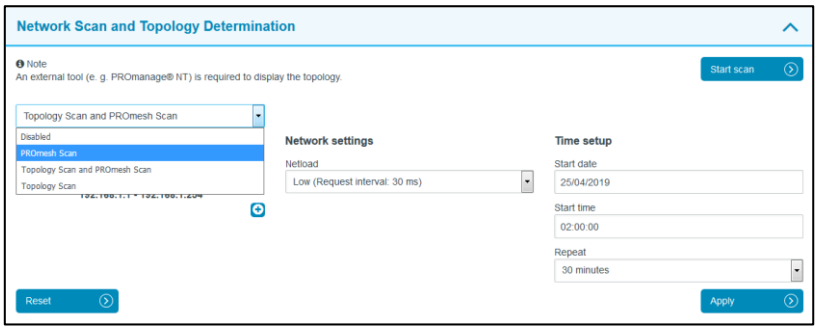


Figure 47: Settings for Topology scan

4.5.2.6 Control mode

To allow rapid visual evaluation of the PROFINET network, individual quality parameters can be coloured by entering specific acceptance values. This setting is used both for the website (see point 4.1.3 Network overview) and for the report.

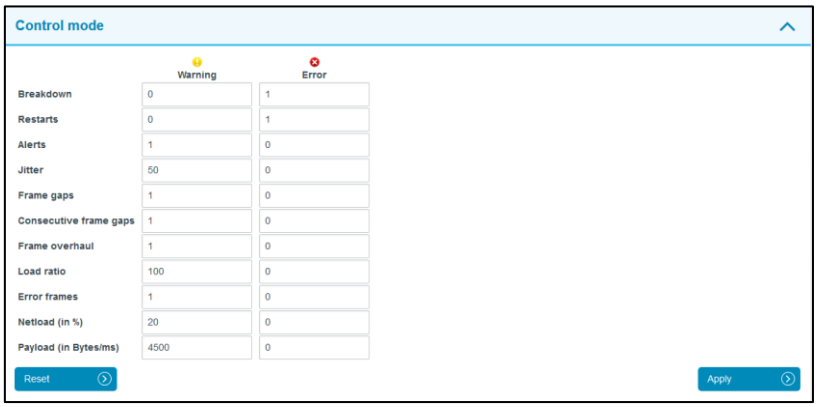


Figure 48: Control mode

4.5.3 Firmware update

You can perform a firmware update for the PN-INspektor® NT using this function, if required. To do this, the new firmware file is selected and uploaded via the “Search” button. Following successful installation, triggering a restart is required in the device with the “Restart” button.

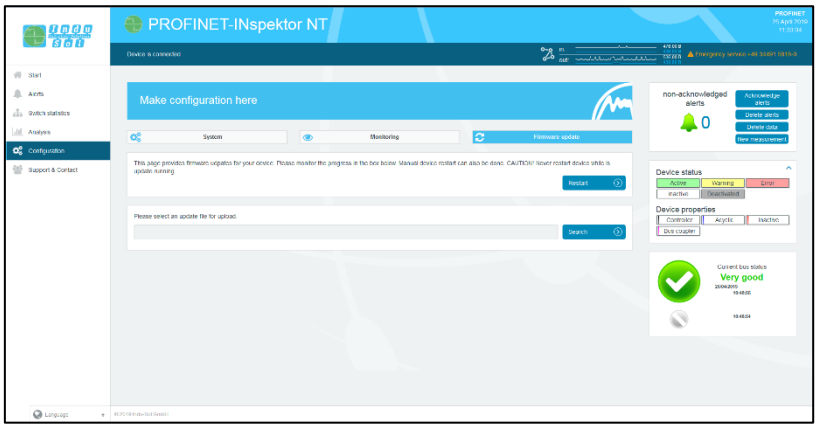


Figure 49: Firmware update

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.

5 Device parameters / Trigger types

5.1 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 5.5 Jitter).

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 Error telegrams

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

5.7 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.

5.8 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.

5.9 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.

5.10 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.

5.11 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.

5.12 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.

5.13 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.

5.14 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 in order to recognize whether accesses to the CPU have been executed (possibly for program changes).

5.15 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.

5.16 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.

5.17 Unicast telegrams

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

5.18 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.

5.19 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.

5.20 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.

5.21 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.

5.22 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.

6 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.

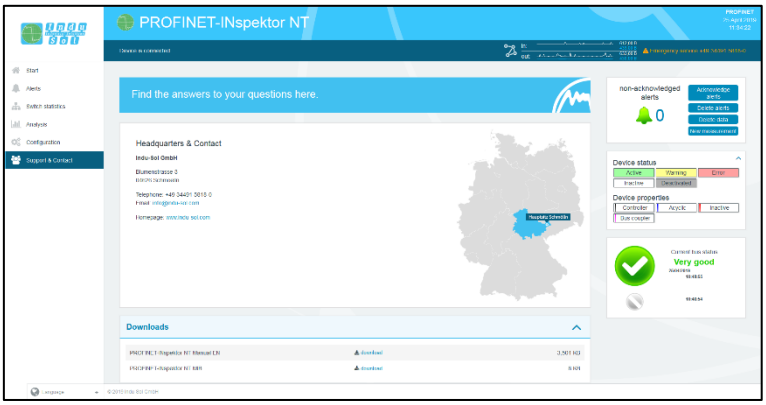
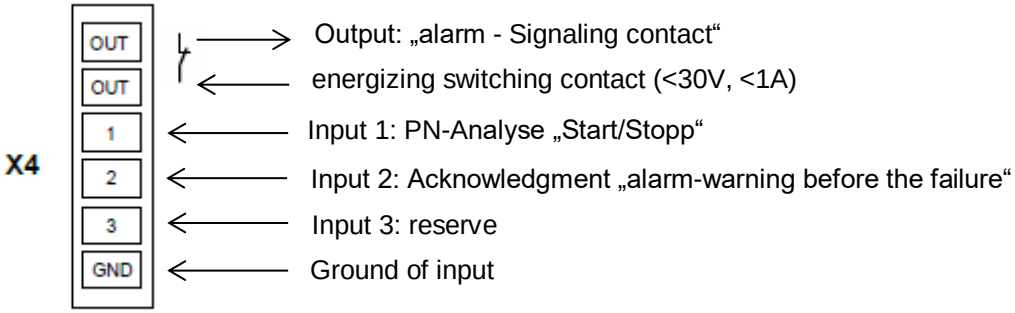


Figure 50: Support and contact

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.

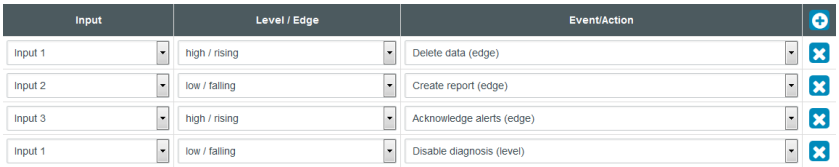
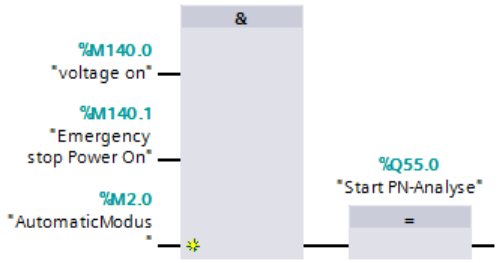


Figure 51: Configuration of the digital switching input

7.1 TiA-Portal Program example

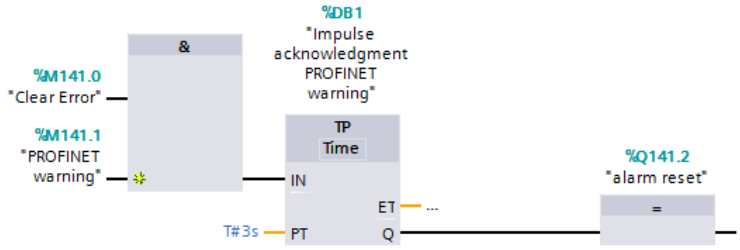
Netzwerk 1: Start PROFINET Analyse, High-Pegel on Output A.55

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.



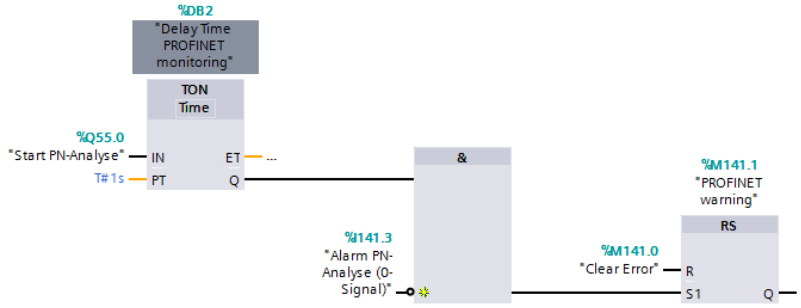
Netzwerk 2: Acknowledgment PROFINET Alarm/Warning

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.

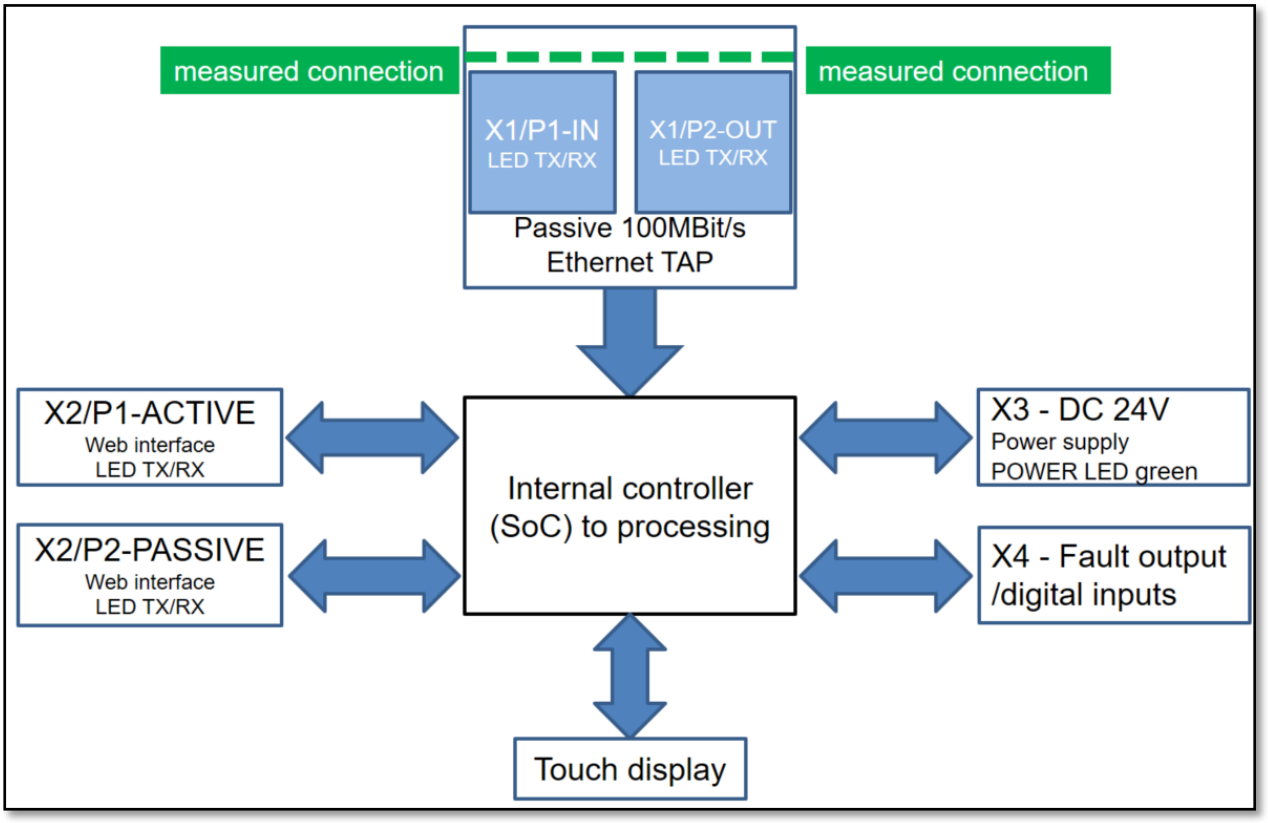


Figure 52: Block diagram

9 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%

9.1 Technical drawing

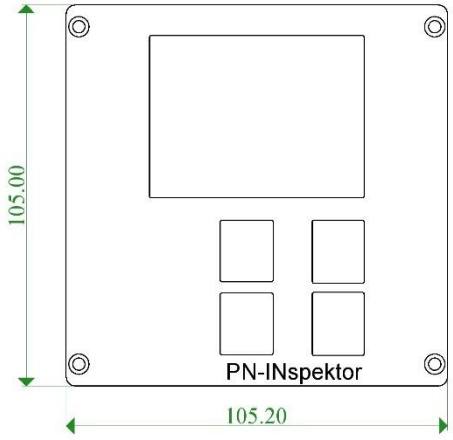


Figure 53: Front view

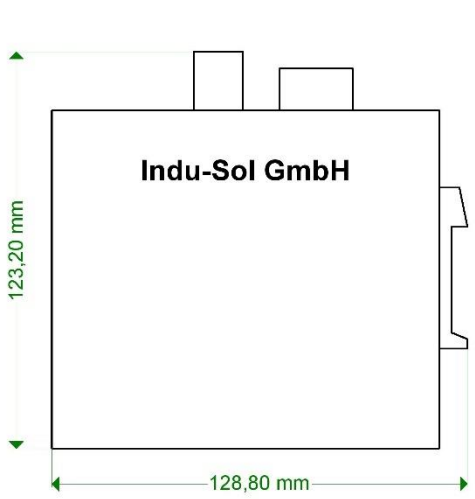


Figure 54: Side view with plugs and top-hat rail mounting

Indu-Sol GmbH
Blumenstrasse 3
04626 Schmoelln

Telephone: +49 (0) 34491 5818-0
Telefax: +49 (0) 34491 5818-99

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

We are certified according to DIN EN ISO 9001:2008

InduSol America, LLC
980 Birmingham Rd. Ste 721
Alpharetta, GA 30004 USA

+1 (678) 880-6910
info@indusolamerica.com

Guadalajara, Jal., MEX

+52 (55) 8526-6442
ventas@indusolamerica.com

www.indusolamerica.com