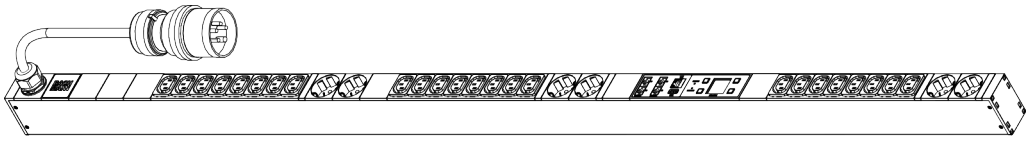
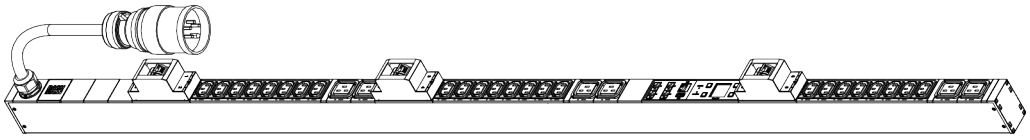
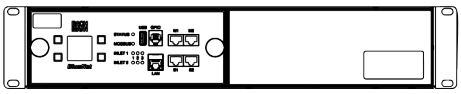
Operating manual

BlueNet PDU BN3000/3500/5000/7000/7500 and BlueNet Power Unit 2







BluNet

BACHMANN

Software version V2.01.XX

Read the instructions prior to performing any task!

Bachmann GmbH
Ernsthaldenstrasse 33
70565 Stuttgart
Germany
Telephone: +49 711 86602-0
Fax: +49 711 86602-34
Email: bluenet@bachmann.com
Internet: www.bachmann.com

Bach-41472-DE, 1, en_GB

About these instructions

These instructions facilitate safe and efficient operation of the BlueNet power distribution unit (hereinafter called “PDU”) and the Power Unit 2 (hereinafter called “PU2”).

The PDU and PU2 are operated and function in essentially the same way. For this reason, the term PDU is used in the following to refer to both devices. Sections that apply only to the PU2 are indicated accordingly.

These instructions constitute an integral part of the PDU and must be retained. If the PDU is transferred to a third party, these instructions must also be transferred with the PDU.

Persons who are entrusted to work on the PDU must have carefully read and understood these instructions prior to starting any work. Compliance with all the safety information and instructions set out in these instructions is an essential prerequisite for safe operation.

The illustrations in these instructions are provided for the purpose of a basic understanding and may deviate from the actual version.

Copyright

Software licenses

This product contains components that are protected by copyright and are licensed under various license models. A copy of the terms of the licences is included with the PDU and can be accessed using the web interface for the PDU.

Other applicable documents

In addition to these instructions, the following documents apply:

- Data sheet
- Mounting and installation instructions
- Safety information

Customer service

Telephone: +49 711 86602-888

Email: service@bachmann.com

Table of contents

1 Overview **7**
1.1 Overview of the PDU 7
1.2 Overview of the PU2 10
1.3 Short description 11
1.4 Displays and controls 12
1.5 Communication 15
1.6 Scope of delivery 16
1.7 Attaching the non-heating appliance locking device (PDU only) 17
1.8 Optional accessories 18

2 Explanation of symbols **19**

3 Personnel requirements and responsibilities **20**

4 Functions **21**
4.1 Cascading master and slave PDUs 21
4.2 Residual current monitoring (RCM) 21
4.3 GPIO port 24

5 Operating the PDU and PU2 using the buttons next to the display **25**
5.1 Operating the PU2 at the display 25
5.2 Setting up a network with DHCP protocol 26
5.3 Setting up a network without DHCP protocol 28
5.4 Acknowledging alarms on the display 31
5.5 Displaying the measured data 33
5.6 Carrying out an RCM self-test 34
5.7 Resetting the effective energy 37
5.8 Displaying the system information 40
5.9 Setting the illumination time 40
5.10 Setting the display orientation 41
5.11 Setting the Modbus address on the slave PDU 43
5.12 Resetting the PDU or PU2 to the factory settings via the menu 44
5.13 Restarting the PDU 46
5.14 Resetting the PDU to factory settings using the buttons (Master PDU only) 47
5.15 Resetting the PU2 to factory settings using the buttons 47

6 Overview and operation of the web interface **49**
6.1 Menu structure of the web interface 49
6.2 Login to the web interface 50
6.3 Setting the user language 50
6.4 Explanation of the web interface 51
6.5 “Status” menu 54
6.5.1 “Status” tab 54

6.5.1.1 Overview ... 54
6.5.1.2 Modifying the grouping of the measured data ... 59
6.5.1.3 Modifying the names of individual elements ... 60
6.5.1.4 Resetting and removing slave PDUs ... 60
6.5.1.5 Switching and identifying sockets ... 61
6.5.1.6 Carrying out an RCM self-test ... 64
6.5.2 “Groups” tab ... 66
6.5.2.1 Overview ... 66
6.5.2.2 Managing socket groups (BN3500/5000/7000/7500 only) ... 67
6.5.2.3 Switching and identifying socket groups ... 68
6.5.3 “Sensors” tab ... 69
6.5.3.1 “Sensors” menu view ... 69
6.5.3.2 “GPIO Module” menu view ... 70
6.6 “Log” menu ... 73
6.6.1 “Event Log” tab ... 73
6.6.1.1 Overview of the tab ... 73
6.6.1.2 Filtering the event log ... 74
6.6.1.3 Removing filters on the event log ... 75
6.6.2 “RCM Log” tab (only for PDUs with RCM) ... 76
6.6.2.1 Overview of the tab ... 76
6.6.2.2 Displaying the RCM log (only for PDUs with RCM) ... 76
6.7 “Signal Sequences” menu ... 77
6.7.1 Overview of the menu ... 77
6.7.2 Configuring signal sequences ... 78
6.7.3 Setting up signal sequences and threshold values for individual elements ... 80
6.7.4 Setting up signal sequences and threshold values for a differential current analyser ... 81
6.7.5 Setting up signal sequences for a GPIO module ... 84
6.8 “Users” menu ... 87
6.8.1 Overview ... 87
6.8.2 Managing a local user ... 88
6.9 “Configuration” menu ... 91
6.9.1 Overview of the menu items ... 91
6.9.2 Configuring network configuration ... 93
6.9.3 Configuring SNMP settings ... 95
6.9.4 Configuring the trap receiver ... 95
6.9.5 Calling up system information ... 98
6.9.6 Executing system commands ... 99
7 Operation using the SSH console ... 103
7.1 Description of executable commands ... 103
7.2 Restarting the PDU using the SSH console ... 108
7.3 Resetting the PDU to factory settings using the SSH console ... 108

7.4 Creating cronjobs at the PDU 108
8 Operation using the serial console 111
9 Carrying out a software update from USB stick or via SCP 112
10 Miscellaneous 114
10.1 IT security 114
10.2 SNMP MIB 115
10.3 Modbus TCP 119
10.4 LDAP 120
10.4.1 Managing users in the directory service 120
10.4.2 Configuring LDAP settings 121
11 Troubleshooting 123
12 Technical data 124
13 Abbreviations 125
14 Index 127

1 Overview

Scope of functions

Functions Product name	Measurement per phase	Measurement per socket	Identification	Switching
BN3000	x	–	–	–
BN3500	x	x	x	–
BN5000	–	–	x	x
BN7000	x	–	x	x
BN7500	x	x	x	x
Power Unit 2	x	–	–	–

1.1 Overview of the PDU

Example of a 16-amp version

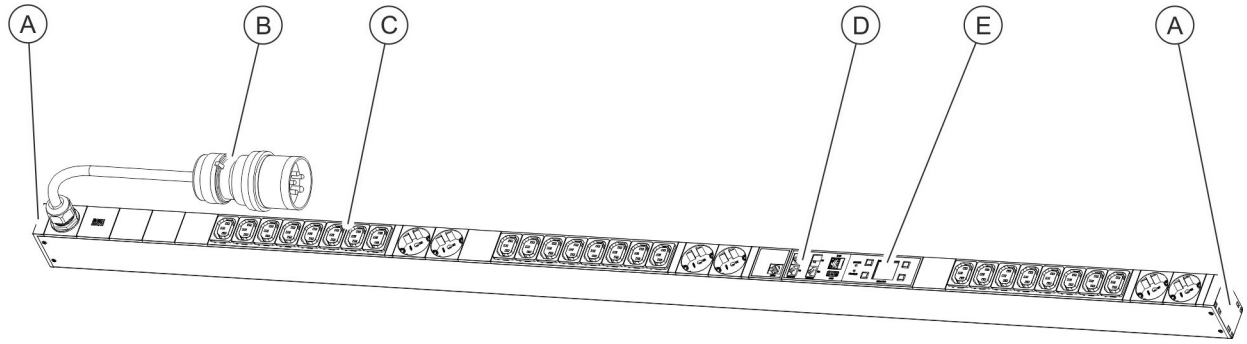


Fig. 1: Product overview (16 amp version)

Ⓐ Fitting slots for plug-in bracket
Ⓑ CEE connector plug
Ⓒ Sockets
Ⓓ Connector panel
Ⓔ Control panel

Example of a 32-amp version

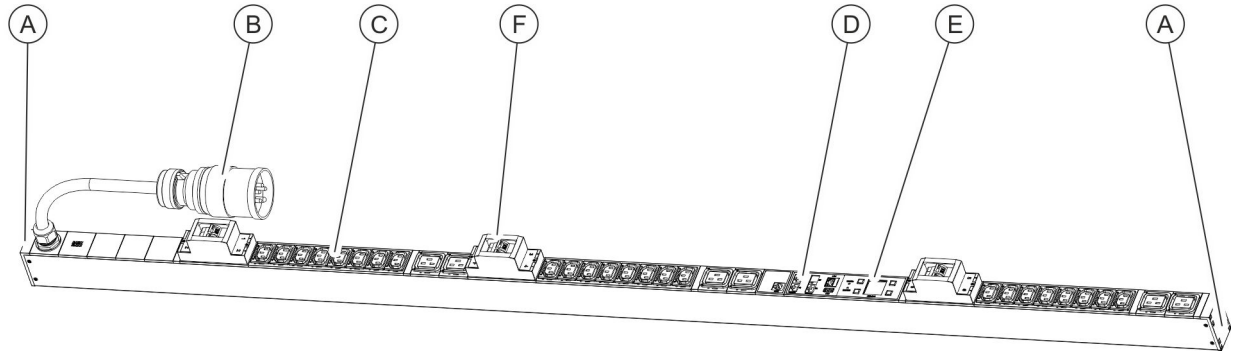
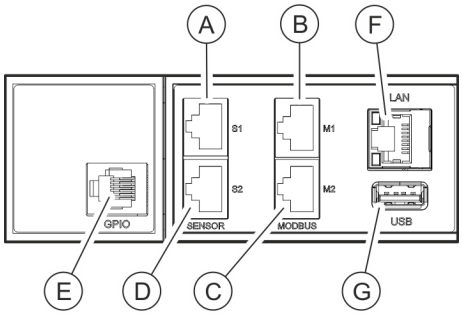


Fig. 2: Product overview (32 amp version)

Ⓐ Fitting slots for plug-in bracket
Ⓑ CEE connector plug
Ⓒ Sockets
Ⓓ Connector panel
Ⓔ Control panel
Ⓕ Circuit breakers

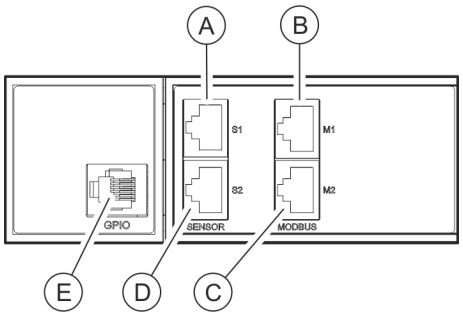
Connector panel for a master PDU



Ⓐ Sensor port S1 (RJ-45, to connect a sensor via a Cat 5e cable or to connect to a serial console)
Ⓑ Modbus port M1 (RJ-45, to connect a slave PDU via a Cat 5e cable)
Ⓒ Modbus port M2 (RJ-45, port for future applications)
Ⓓ Sensor port S2 (RJ-45, to connect a sensor via a Cat 5e cable)
Ⓔ GPIO port (RJ-12)
Ⓕ LAN port (RJ-45)
Ⓖ USB port

Fig. 3: Connector panel (master PDU)

Connector panel for a slave PDU



Ⓐ Sensor port S1 (RJ-45, to connect a sensor via a Cat 5e cable)
Ⓑ Modbus port M1 (RJ-45, to connect a master PDU and upstream slave PDUs via a Cat 5e cable)
Ⓒ Modbus port M2 (RJ-45, to connect a slave PDU via a Cat 5e cable)
Ⓓ Sensor port S2 (RJ-45, to connect a sensor via a Cat 5e cable)
Ⓔ GPIO port (RJ-12)

Fig. 4: Connector panel (slave PDU)

Control panel

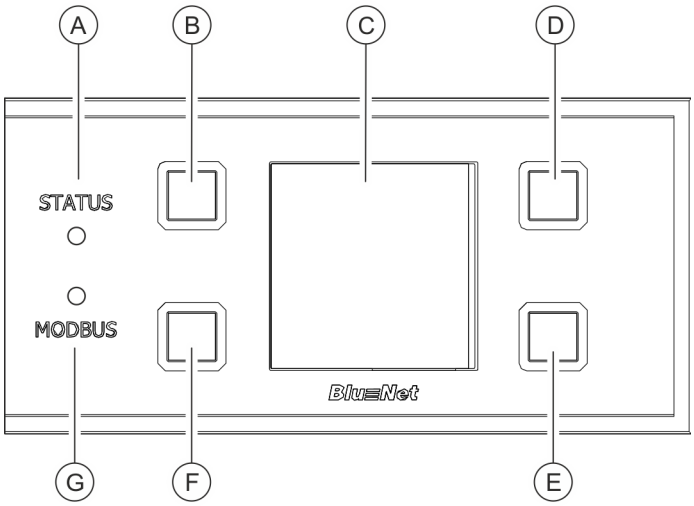


Fig. 5: Control panel

Ⓐ Status LED
Ⓑ Operating button 1
Ⓒ Display
Ⓓ Operating button 2
Ⓔ Operating button 3
Ⓕ Operating button 4
Ⓖ Modbus LED

Mounting options

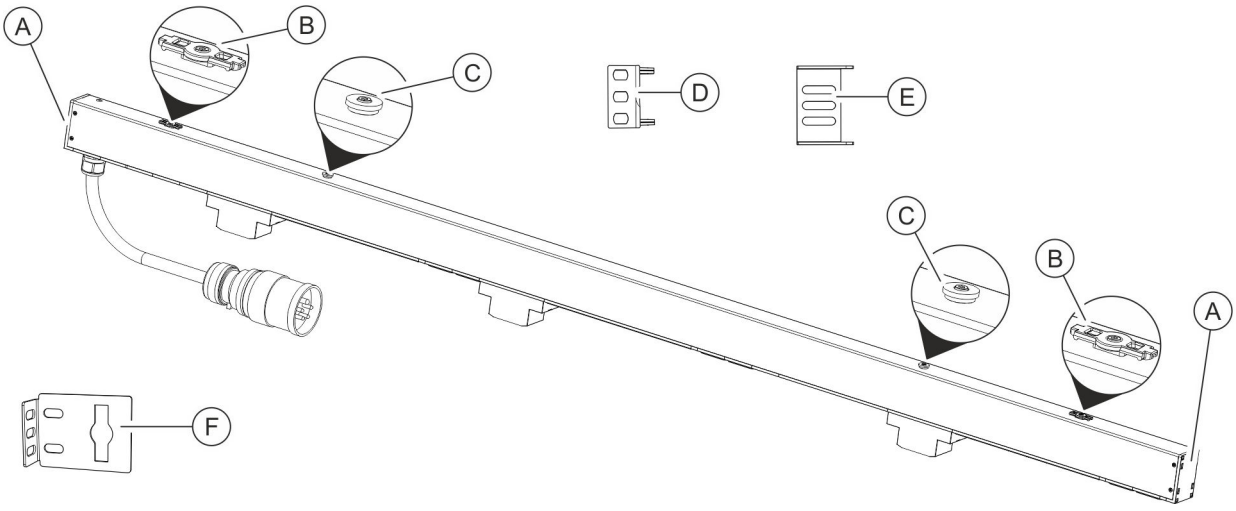


Fig. 6: Overview of the fitting options for the PDU

Ⓐ Fitting slots for plug-in bracket
Ⓑ Attachment for the mounting bracket
Ⓒ Attachment for the mounting solution in the rack
Ⓓ Plug-in bracket for mounting the PDU via the back (2 each)
Ⓔ Plug-in bracket for mounting the PDU via the sides (2 each)
Ⓕ Mounting bracket (x 2)

1.2 Overview of the PU2

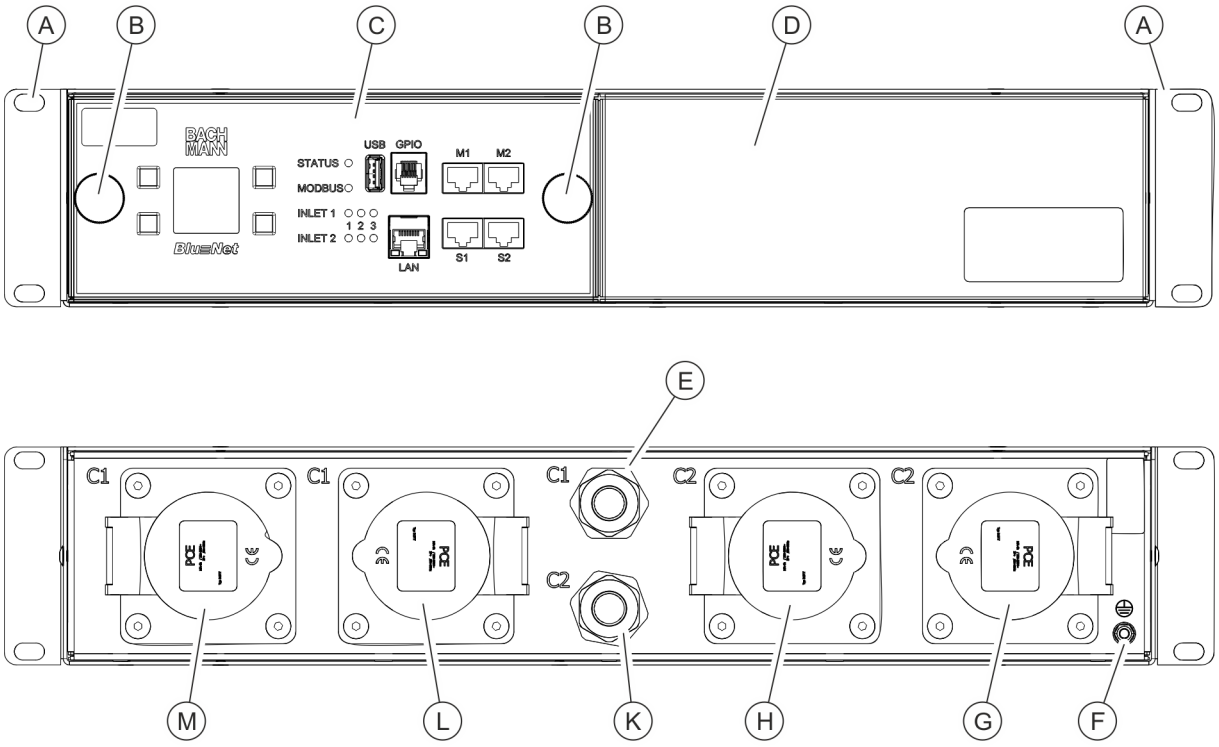


Fig. 7: Overview

Ⓐ Holder for fastening in the rack
Ⓑ Knurled screws for fastening the measuring unit* in the housing of the base unit
Ⓒ Measuring unit*
Ⓓ Base unit
Ⓔ Power supply C1 (inlet 1)
Ⓕ Protective earth
Ⓖ Socket output C2.2
Ⓗ Socket output C2.1
Ⓚ Power supply C2 (inlet 2)
Ⓛ Socket output C1.2
Ⓜ Socket output C1.1

*) The measuring unit is an optional extra. If no measuring unit is installed, this part is covered. The base unit also functions without a measuring unit, but no measured data can be retrieved from the measuring unit.

Measuring unit

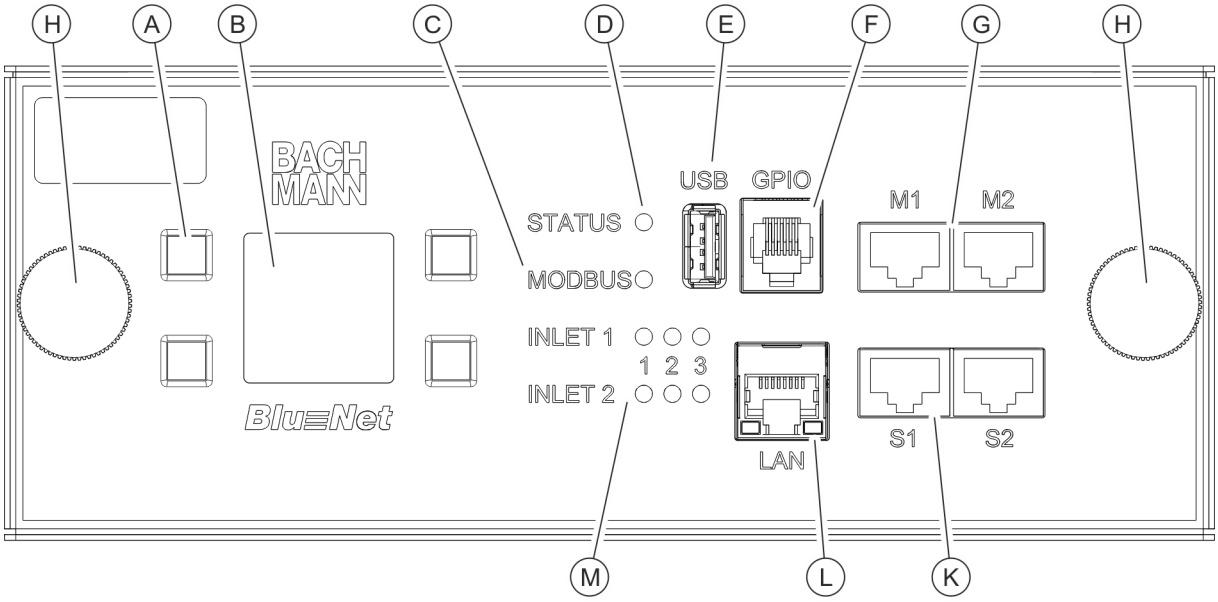


Fig. 8: Measuring unit

Ⓐ Control buttons for the display
Ⓑ Display
Ⓒ Modbus LED (not currently used)
Ⓓ Status LED
Ⓔ USB port
Ⓕ GPIO port (RJ-12)
Ⓖ Modbus port M1/M2 (RJ-45)
Ⓗ Knurled screw for fastening the measuring unit in the base unit
Ⓚ Sensor port S1/S2 (RJ-45, to connect a sensor via a Cat 5e cable)
Ⓛ LAN port (RJ-45)
Ⓜ Inlet LEDs for displaying the status of the power supply (single-phase or three-phase)

1.3 Short description

The power supply of a data centre can be monitored and controlled remotely using the PDU. The PDU can be set up for single-phase or three-phase systems. The individual phases can be distinguished by their colours. The PDU is supplied with electricity via a CEE plug.

The PU2 consists of two parts: a base unit and an optional measuring unit. The base unit distributes the current in the rack. The measuring unit can be used to monitor the connected loads. If needed, the measuring unit can be retrofitted or replaced during live operation, without interrupting the power supply.

The PU2 can be set up as single-phase or three-phase and has one or two electrically isolated feeds (16 – 32 A/230 – 400 V).

The current, power (effective, apparent and reactive power), power consumption, voltage and frequency of all phases are monitored using the PDU or PU2. This enables the efficient planning of resources and the issuing of an alarm in the event of a fault. The PDU is designed for a power range of 3.6 to 22 kW.

The PDU is integrated into the company network via the LAN port (only available on the Master PDU or PU2). Up to 11 Slave PDUs can be cascaded with a Master PDU via the Modbus port.

The PDU or PU2 can be operated locally using the display, SNMP access or with a web browser via a network, and the HTTP, HTTPS, SSH and SNMP protocols are used.

The PDU is made of a sturdy aluminium profile and is installed directly into the rack. The PU2 is made of a 19” steel plate housing and is also installed directly into the rack.

Depending on the type, the PDU has a range of equipment features such as safety sockets or sockets for IEC320 C14 and C20 non-heating appliances and for connecting external sensors (temperature/air humidity).

Depending on the type, the PU2 has a range of equipment features such as sockets for IEC60320 C20 non-heating appliances or CEE plugs (single-phase or three-phase) on the back.

A connector inserted into the PDU can be secured via the non-heating appliance locking device (C13/C19).

1.4 Displays and controls

Display with control buttons

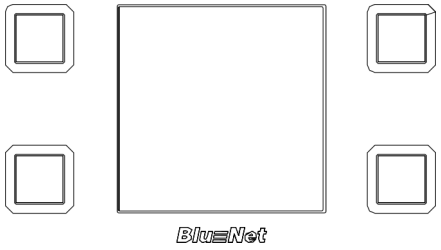


Fig. 9: Display with control buttons

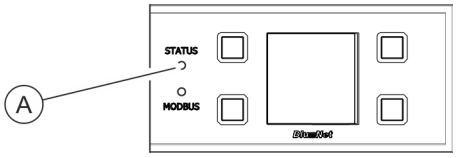
The PDU can be operated locally using the display with the control buttons:

- Display of system data (hardware and software version, serial number, MAC address (only for master PDUs and the optional measuring unit for the PU2) and item number)
- Display of the measured data
- Set the duration and orientation of the display
- Display and adjustment of the network configuration as well as enabling or disabling the DHCP protocol (only for master PDUs and PU2)
- Setting for Modbus (only for slave PDUs)

Inlet LEDs (PU2 only)

The Inlet LEDs on the optional measuring unit display the status of the feeds (Inlet 1 and Inlet 2). The feeds can be single-phase or three-phase. In normal operation, the LEDs light up green (LED 1 – 3 for three-phase, LED 1 for single-phase feed). In the event of a fault, the LED in question does not light up.

Master PDU and PU2 status LED

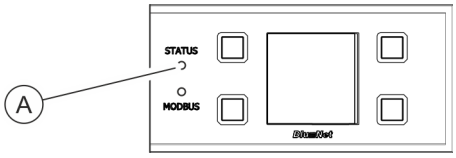


The status LED (Fig. 10/Ⓐ) indicates the status of the PDU or PU2. Possible statuses are:

Fig. 10: Master PDU status LED

Colour	Light	State
Green	Continuously green	All measured data is OK and the status of the individual connected loads and sensors are OK
Orange	Continuously orange	The measurement monitor issues a warning (based on all the measured data of the PDU and sensors)
Red	Continuously red	The measurement monitor issues an alarm (based on all the measured data of the PDU and sensors) or the connection to a sensor is interrupted
Orange	Continuously orange	PDU starting up
White	Continuously white	Performing factory reset (after releasing the pressed buttons)
Purple	500 ms off, 500 ms purple	An update of a PDU is in progress
Purple, red	500 ms off, 500 ms purple, 500 ms off, 500 ms red	An error occurred during the update of a PDU

Slave PDU status LED



The status LED (Fig. 11/Ⓐ) indicates the status of the PDU. Possible statuses are:

Fig. 11: Slave PDU status LED

Tab. 1: Starting process

Colour	Light	Status
Blue, orange	900 ms blue, 100 ms orange	Connection to Master PDU not yet established or lost
Green	Continuously green	Connection to Master PDU present
Blue, purple	500 ms blue, 500 ms purple	An update of a PDU is in progress
Blue, purple, red	500 ms blue, 500 ms purple, 500 ms blue, 500 ms red	Error during the update of a PDU

Tab. 2: In operation

Colour	Light	Status
Orange	900 ms off, 100 ms orange	Connection to Master PDU not yet established or lost
Green, red	500 ms off, 100 ms green, 500 ms off, 100 ms red	Connection to Master PDU present, internal communication problems have occurred
Green	Continuously green	Connection to Master PDU present, internal communication functioning
Purple	500 ms off, 500 ms purple	An update of the internal modules of a PDU is being carried out
Purple, red	500 ms off, 500 ms purple, 500 ms off, 500 ms red	Error during update of the internal modules of a PDU
Red	Continuously red	The measurement monitor is issuing an alarm
Orange	Continuously orange	The measurement monitor is issuing a warning

Slave PDU Modbus LED

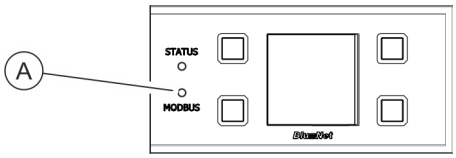


Fig. 12: Slave PDU Modbus LED

The Modbus LED (Fig. 12/Ⓐ) indicates the activity of the PDUs connected to the Modbus.

The Modbus LED lights up continuously green. If there is communication between the Master and a Slave PDU, the Modbus LED lights up yellow.

Status LED on (BN3500/5000/7000/7500 only)

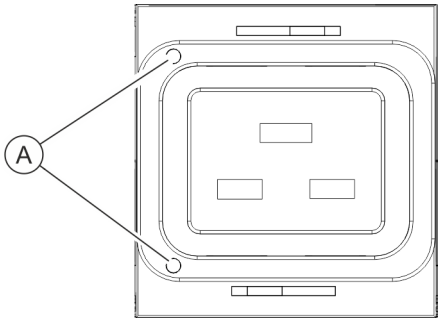


Fig. 13: Socket LEDs

The socket LEDs (Fig. 13/Ⓐ) (only available on BN3500/5000/7000/7500) indicate the socket monitoring status. Possible statuses are:

Colour	Light	State
Green	Continuously green	Measured data OK
Red	Continuously red	HighAlarm measured data
Red	Continuously red	LowAlarm measured data

Colour	Light	State
Orange	Continuously orange	HighWarning measured data
Orange	Continuously orange	LowWarning measured data
Red, off	800 ms red, 200 ms off	For sockets, indicates that the relay is switched on, an alarm is present and identification has been set
Red, off	200 ms red, 800 ms off	For sockets, indicates that the relay is switched off, an alarm is present and identification has been set
Red, off	100 ms red, 400 ms off	For sockets, indicates that the relay is switched off and an alarm is present
Orange, off	800 ms orange, 200 ms off	For sockets, indicates that the relay is switched on, a warning is present and identification has been set
Orange, off	200 ms orange, 800 ms off	For sockets, indicates that the relay is switched off, a warning is present and identification has been set
Orange, off	100 ms orange, 400 ms off	For sockets, indicates that the relay is switched off and a warning is present
Green, off	800 ms green, 200 ms off	For sockets, indicates that the identification has been set and the relay is switched on
Green, off	200 ms green, 800 ms off	For sockets, indicates that the identification has been set and the relay is switched off
Off	Continuously off	For sockets, indicates that the relay has been switched off permanently

Automatic deactivation of all relays of the master PDU

The automatic deactivation of all relays of the master PDU in the event of a power loss can only be ensured if the master PDU is operated in PoE mode and if at the same time the power supply works via Ethernet and is not affected by the power failure.

1.5 Communication

Connection for sensors S1/S2

Temperature sensors, combination sensors (temperature, air humidity and dew point) and GPIO modules can be connected to the PDU via the ports for sensors. The values can be called up on the web interface under *“Status ➔ Sensors”* or via the display.

Connection for Modbus M1/M2

Individual PDUs can be connected to each other with the Modbus port. This way, up to 11 slave PDUs can be cascaded with one master PDU and managed using the web interface. The first slave PDU is connected to Modbus port M1 of the master PDU via Modbus port M1. Further slave PDUs are connected from their Modbus port M1 with the Modbus port M2 of the slave PDU connected upstream.

LAN port (10/100 Mbit/s)

The PDU can be integrated into the network via the LAN port. The data transfer rate is controlled using the network.

USB port for software updates (only on the master PDU and PU2)

There is a USB port on the PDU next to the display and control panel. It is for updating the software.

On the PU2, the USB port is on the measuring unit.

GPIO port

For details of the GPIO port, see *Chapter 4.3 “GPIO port” on page 24*.

1.6 Scope of delivery

PDU

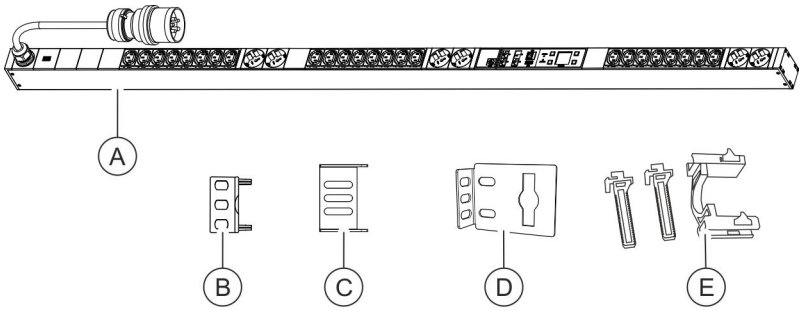


Fig. 14: Scope of delivery

The scope of delivery includes:

- PDU (Fig. 14/Ⓐ)
- Two plug-in brackets for mounting the PDU via the back (Fig. 14/Ⓑ)
- Two plug-in brackets for mounting the PDU via the sides (Fig. 14/Ⓒ)
- Two mounting brackets (Fig. 14/Ⓓ)
- Two sets of non-heating appliance locking devices (C13/C19) (Fig. 14/Ⓔ)
- Mounting and installation instructions
- Safety information

PU2

The scope of delivery includes:

- Power Unit 2 base unit
- Power Unit 2 measuring unit (optional)
- Earthing kit (only for base unit)
- Mounting and installation instructions
- Safety information

1.7 Attaching the non-heating appliance locking device (PDU only)

Overview

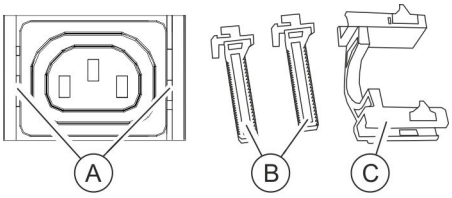


Fig. 15: Non-heating appliance locking device

Ⓐ Holder for the non-heating appliance locking device
Ⓑ Posts
Ⓒ Locking clip

The holder for the non-heating appliance locking device is beside the individual sockets (Fig. 15/Ⓐ). The posts (Fig. 15/Ⓑ) must be inserted into the holder (Fig. 15/Ⓐ) and engaged in position with the recess pointing inwards. The locking clip (Fig. 15/Ⓒ) must be pushed onto the posts from above to secure the posts in position.

Attaching the non-heating appliance locking device

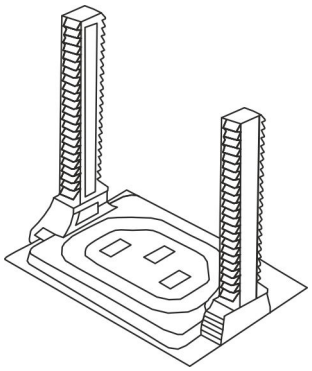


Fig. 16: Attaching the posts

1. Insert the posts into the holder with the recess pointing inwards (Fig. 16).
2. Insert the plug into the socket.

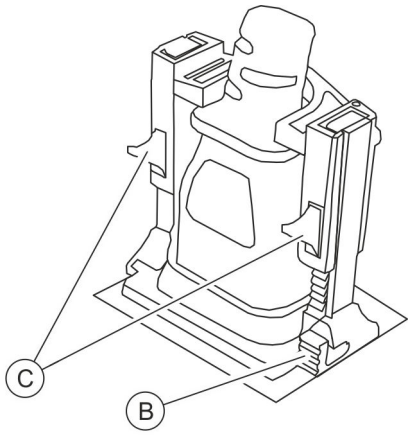


Fig. 17: Attaching the locking clip

3. Secure the plug in position by pushing the locking clip onto the posts from above (Fig. 17).

To release, the locking clip and/or the posts have to be released using the unlocking lever (Fig. 17/Ⓐ and Ⓑ).

1.8 Optional accessories

Temperature and combination sensor

The temperature, air humidity and dew point at the installation location of the PDU can be measured via a temperature sensor or a combination sensor for temperature and humidity. The values can be displayed on the display and on the web interface. The CAT5e cable required to connect the sensors is included.

GPIO module

The GPIO module can be used to connect the PDU to external devices in order to read out input statuses and to switch outputs.

2 Explanation of symbols

Safety information

Safety information is indicated by symbols in these instructions. The safety information is introduced by signal words that express the nature of the danger.

DANGER!
This combination of symbol and signal word indicates that there is an imminent danger that will result in death or serious injury if it is not avoided.

WARNING!
This combination of symbol and signal word indicates that there is a potential danger that can result in death or serious injury if it is not avoided.

NOTICE!
This combination of symbol and signal word indicates that there is a potential danger that can result in damage to property if it is not avoided.

Tips and recommendations

This symbol highlights useful tips and recommendations as well as information for efficient and trouble-free operation.

The following markings are used to highlight specific instructions, results, lists, references and other elements in these instructions:

Marking	Explanation
	Step-by-step instructions
⇨	Results of the steps of an instruction
	References to sections in these instructions and to other applicable documents
■	Items in a list without a specified sequence
[Key]	Controls (e.g. keys, switches), display elements (e.g. signal lamps)
“Display”	Screen elements (e.g. buttons, assignment of function keys)

3 Personnel requirements and responsibilities

WARNING!

Risk of injury if the personnel is insufficiently qualified!

If unqualified personnel carry out the installation work on the PDU, serious injuries or substantial damage to property can be caused.

– The installation and the connection of the PDU must be carried out by an IT specialist.
– Defective components on the PDU must be repaired by a qualified electrician.

Only permit persons to work on the PDU who can be expected to carry out their work reliably. Persons whose capacity to react is impaired, e.g. through drugs, alcohol, or medication, cannot be permitted to perform such work.

In these instructions, the following personnel qualifications are required for the various tasks listed below:

IT specialist

IT specialists have obtained specialist training or the appropriate experience in dealing with IT systems and have a basic knowledge of electrical engineering.

Due to their specialist training, IT specialists are in a position to assess the consequences of their actions in dealing with the system as well as its components and the potential dangers in respect thereof and are able to avoid these.

The duties of an IT specialist include the following tasks:

- Setting up hardware and software systems
- Installing updates
- Maintenance work on the PDU
- Administration of the PDU via the web interface
- System diagnostics

Qualified electrician

Due to their professional training, knowledge and experience, as well as their knowledge of the relevant standards and regulations, qualified electricians are capable of working on electrical installations and independently identify and avoid potential dangers.

Qualified electricians are specifically trained for the working environment in which they work and know the relevant standards and regulations.

4 Functions

4.1 Cascading master and slave PDUs

When cascading master and slave PDUs, note the following:

- Update the master PDU to the latest firmware version as regularly as possible. Otherwise it will be unable to detect slave PDUs with a newer firmware version. These slave PDUs are then marked as “too new” (blue LED in the web interface).
- The “Modbus RTU” function must be activated to use this function. You can deactivate it if no slave PDUs are to be connected. This function is activated by default.

  If the “Modbus RTU” function is deactivated, any detected slave PDUs are removed from the system. The slave PDUs retain their configuration here. When you deactivate the function, a security prompt appears if one or more slave PDUs are connected.
- The Modbus address must be set uniquely for each slave PDU if more than one slave PDU is to be connected to the master PDU.
- The element name of the slave PDU is not dependent on the Modbus address, it is assigned after detection. If multiple slave PDUs are connected simultaneously, they are detected independently of the Modbus address.
- A slave PDU can only be removed if it has the status “Lost”.
- If a slave PDU is moved from one master PDU to another master PDU, it takes its configuration with it. If you do not want this to happen, you have to perform a factory reset on the slave PDU. If a slave PDU is moved, the Modbus address has to be checked for uniqueness.
- During an update, the slave firmware is automatically updated by the master PDU, if necessary. There is no specific firmware update on the slave PDU from the user’s perspective.

If a slave PDU is not connected to its master (status “Lost”):

- Switching commands are discarded.
- No measured data are displayed (“n/a” is displayed instead).
- Modified settings are saved and sent to the slave PDU as soon as it is available again.
- Firmware updates are carried out as soon as the slave PDU is available again.

4.2 Residual current monitoring (RCM)

Introduction

For today’s companies, the security, maximum availability and cost-effectiveness of computer centres and server parks are very important. An uninterrupted supply of power to the server racks is crucial here.

Even when designed in accordance with standards, modern consumers increasingly cause malfunctions in the electrical systems used, thereby representing a growing challenge to secure operation. Possible dangers include service interruptions, inexplicable malfunctions, unexpected triggering of protective equipment, fire or even personal injury.

The use of residual current monitoring solutions (RCM) aids the prevention and early detection of problems, helping ensure smooth operation of data centres. If this monitoring is sufficiently finely structured, it can also significantly reduce the time needed to localise and rectify the error and even, in the best case, allow action before serious problems occur.

Residual current monitoring (RCM) operates on the principle of measuring the residual current, also known as the differential current. Here, the conductors for the outgoing line to be protected (except for the protective earth conductor) are routed through a measuring current transformer with a secondary winding and their residual current is evaluated by a set of electronics. In an electricity supply and distribution system without any errors, the vectorial sum of all the currents is equal to zero, so that no voltage is induced in the secondary winding of the measuring current transformer. If, however, current flows out via the protective earth, the current differential in the measuring current transformer causes a current that is recorded by the electronics, is evaluated and, if necessary, results in an alarm via a signal sequence.

To monitor residual currents, one or more AC/DC-sensitive RCM modules (type B) can be installed in a PDU:

- This can be used at the supply, phase or fuse level.
- RCM measured data are propagated/added up at higher levels, where alarms can be issued.
- In addition to the measured data (AC and DC), resettable peak values are also determined.
- The AC measured data include the DC measured value.
- Setpoints for measurement monitoring and measurement alarms can be defined according to load.

  This is only possible at levels on which a current value is present (i.e. not at the fuse level for a BN3000/7000 and not for a BN5000).
- A prescribed RCM self-test can be executed via the web interface or CLI for all RCMs or individually for each RCM.

  A self-test for the RCM modules of the PDU in question can be executed via the display.

  During an RCM self-test, no peak values can be determined and the measured data cannot be forwarded to the higher levels.

  The result is recorded in the RCM log.

RCM types

	Form of residual current	RCM type		
		AC	A	B
AC, sinusoidal	occurring suddenly	x	x	x
	slowly ascending			
DC, pulsating	occurring suddenly		x	x
	slowly ascending			
DC, smooth				x
Screen icon				

Dynamic RCM

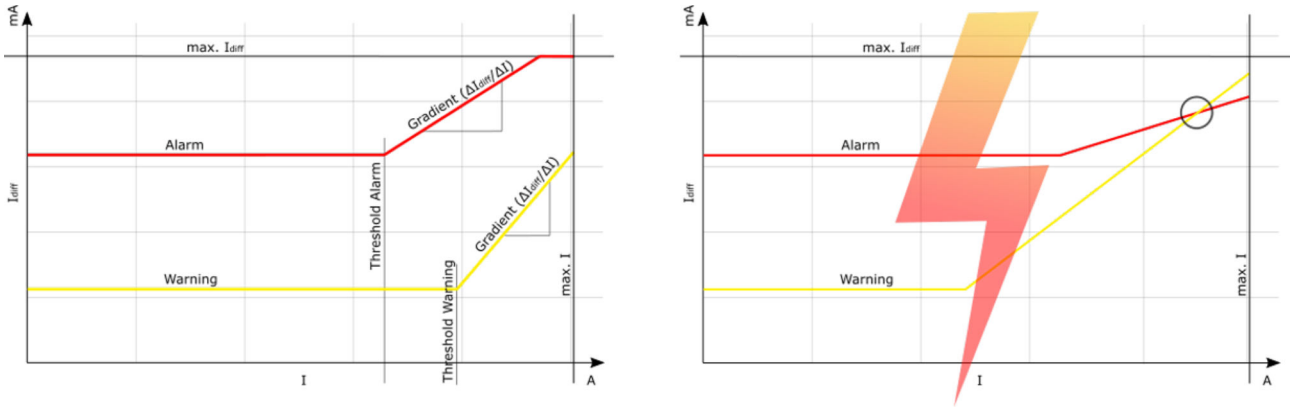


Fig. 18: Dynamic RCM

As the residual current increases with the connected load, it is useful to be able to configure the RCM threshold value (AC only, warning and alarm) dynamically according to the current. The ratio between residual current and current is proportional. At lower loads, constant RCM limits can be used. For each threshold value (AC only, warning and alarm), it is possible to configure a current threshold value at which dynamic calculation begins.

The maximum configurable threshold value (in A) corresponds to the maximum permissible current at this level. The granularity of the configurable threshold is 0.1 A. In addition, gradients “RC (in mA) per current (in A)” have to be defined in order to calculate the dynamic warning or alarm. The user must ensure that the warning threshold is always smaller than or equal to the alarm threshold. Otherwise, the configuration cannot be saved. The maximum value for the gradients is 100 mA/A, the granularity is 0.1 mA/A. If the calculated threshold values exceed the limits, the threshold values are limited to the limit value for the level in question.

4.3 GPIO port

Types of GPIO port

There are two types of GPIO port:

- PDUs with a new controller board (master PDUs with hardware version 2.00 or higher, or slave PDUs with hardware version 5.02 or higher) have an internal GPIO port with one input and output.
- An external GPIO module with four inputs and outputs for connecting to a master PDU or slave PDU.

External GPIO module

The GPIO module is compatible with the BlueNet master and slave PDUs BN3000 – BN7500 and Power Unit 2. It is connected to these devices using a Cat 5e cable via sensor port S1 or S2.

The GPIO module has four relay outputs as changeover contacts, which can be switched manually or by means of a signal sequence.

Furthermore, there are four digital inputs that can be operated with an auxiliary voltage of 7 V and a maximum current of 5 mA.

If there is a firmware update of the external GPIO module, the states that were set previously are retained.

When a GPIO module is put into operation for the first time, all the inputs/outputs are set to “disabled” and the outputs are switched off.

If a GPIO module is already known in a PDU, the PDU configures the GPIO module when they are connected.

This also applies if a GPIO module is replaced by another.

5 Operating the PDU and PU2 using the buttons next to the display

5.1 Operating the PU2 at the display

The PDU and PU2 are essentially operated the same way at the display. For the PU2, there is an upstream dialogue that needs to be selected before the measured data are displayed.

Press the ⓘ button to open the “System” menu from the start screen, as on the PDU.

For the PU2, there is one page for the base unit and one for the measuring unit.

Personnel: ■ IT specialist

1. Press any button on the PU2 to activate the display.

2. Press the ⇩ button to select the desired outlet and confirm by pressing the ⇨ button.

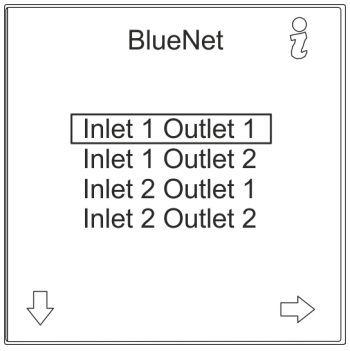


Fig. 19: “BlueNet” menu

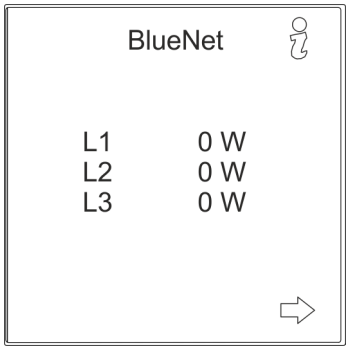


Fig. 20: “BlueNet” menu

⇨ The measured data for the selected outlet are displayed.

From this dialogue on, the PDU and PU2 are essentially operated the same way at the display.

5.2 Setting up a network with DHCP protocol

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.
2. Use the button to open the “System” menu.

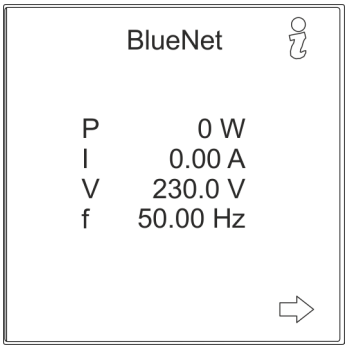


Fig. 21: “BlueNet” menu

3. Use the button to open the “Settings” menu.

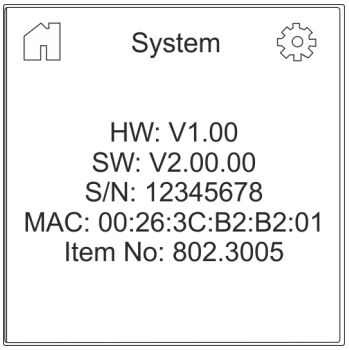


Fig. 22: “System” menu

4. Use the button to select the “Network” menu and confirm by pressing the button.

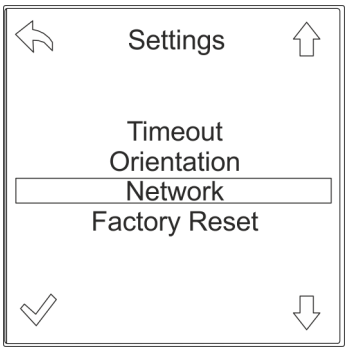


Fig. 23: “Settings” menu

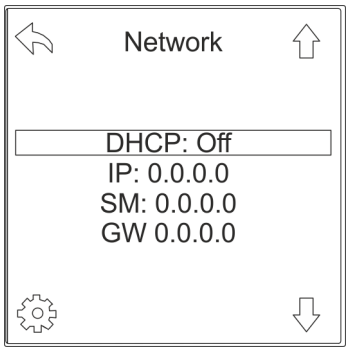


Fig. 24: “Network” menu

5. Use the ⚙ button to open the option menu for the DHCP setting.

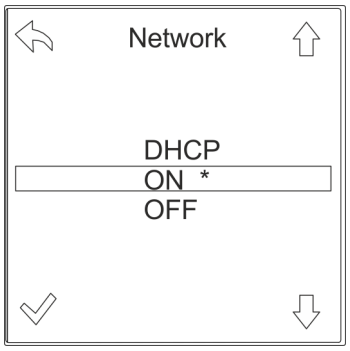


Fig. 25: “Network” menu

6. Use the ⇧ button to select the “ON” parameter and confirm by pressing the ✓ button.

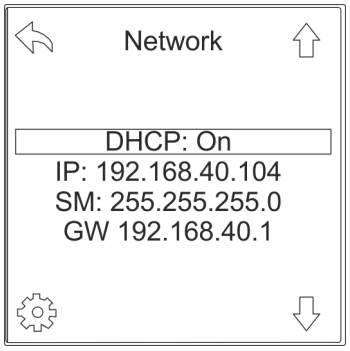


Fig. 26: “Network” menu

⇨ The PDU automatically obtains an IP address from one of the DHCP servers on the network.

7. Make a note of the IP address for subsequent entry in the web browser.

5.3 Setting up a network without DHCP protocol

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.
2. Use the button to open the “System” menu.

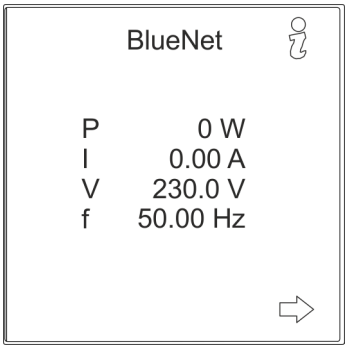


Fig. 27: “BlueNet” menu

3. Use the button to open the “Settings” menu.

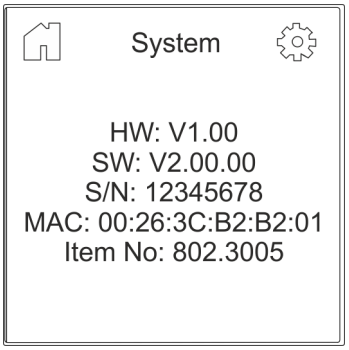


Fig. 28: “System” menu

4. Use the button to select the “Network” menu and confirm by pressing the button.

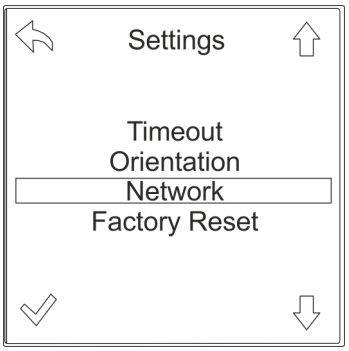


Fig. 29: “Settings” menu

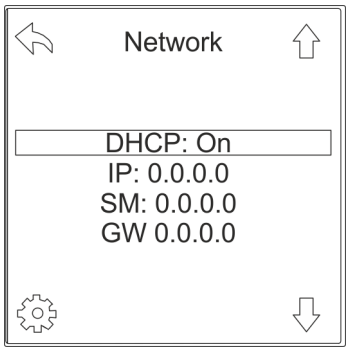


Fig. 30: “Network” menu

5. Use the ⚙ button to open the option menu for the DHCP setting.

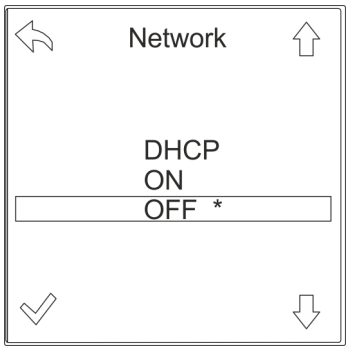


Fig. 31: “Network” menu

6. Use the ⇩ button to select the “OFF” parameter and confirm by pressing the ✓ button.

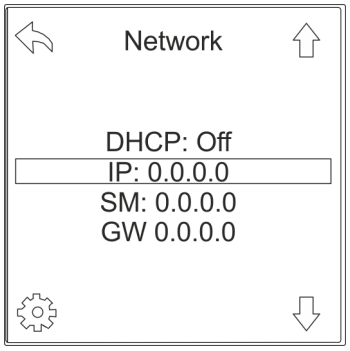


Fig. 32: “Network” menu

7. Use the ⇩ button to select the “IP” parameter and confirm by pressing the ⚙ button.

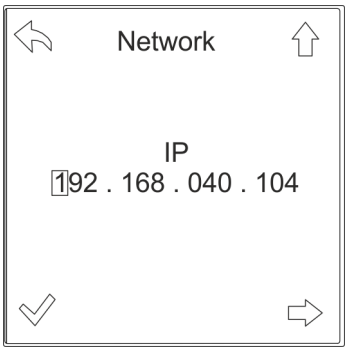


Fig. 33: “Network” menu

8. Enter the IP address and confirm by pressing the ✓ button.

You can select individual digits with the ⇨ button and change them with the ⇧ button.

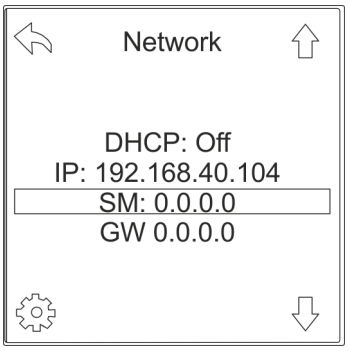


Fig. 34: “Network” menu

9. Use the ⇩ button to select the “SM” parameter and confirm by pressing the ⚙ button.

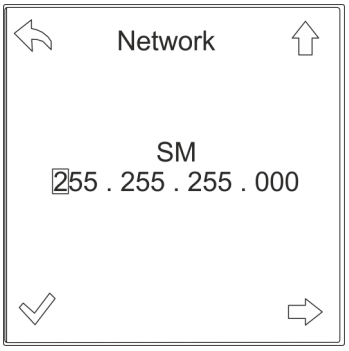


Fig. 35: “Network” menu

10. Enter the subnet mask and confirm by pressing the ✓ button.

You can select individual digits with the ⇨ button and change them with the ⇧ button.

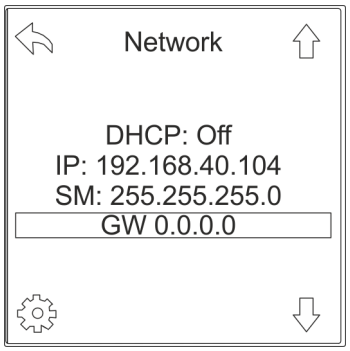


Fig. 36: “Network” menu

11. Use the ⇩ button to select the “GW” parameter and confirm by pressing the ⚙ button.

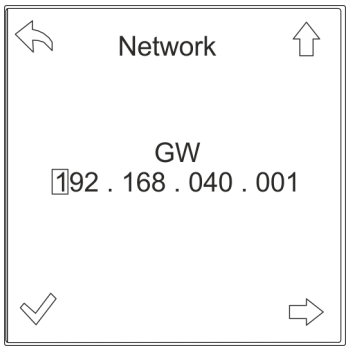


Fig. 37: “Network” menu

12. Enter the gateway and confirm the selection by clicking the ✓ button.

You can select individual digits with the ⇨ button and change them with the ⇧ button.

⇨ The PDU is set to an IP address and the web interface can be called up in a web browser.

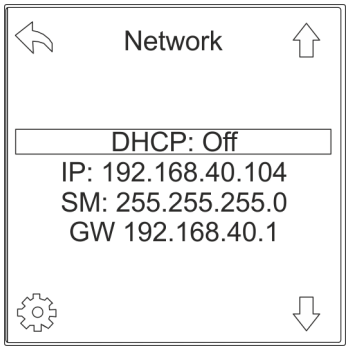


Fig. 38: “Network” menu

13. Make a note of the IP address for subsequent entry in the web browser.

5.4 Acknowledging alarms on the display

Alarm on the display

If a signal sequence has been set up with a display alarm (↬ *Chapter 6.7.3 “Setting up signal sequences and threshold values for individual elements” on page 80*) and an alarm is pending, a corresponding alarm message is shown on the display. If the display is inactive, it switches on automatically for the duration of the set timeout. If the display was already switched on, the alarm message covers the page that is currently displayed.

The alarm message remains in place until it is either acknowledged or the alarm is no longer pending. An individual alarm is acknowledged with the “OK” button and all further alarm messages can be acknowledged with the “CLR” button. Acknowledged alarm messages do not reappear unless the corresponding alarm occurs

again. If the system returns to the normal state, the alarm message disappears from the display, provided a signal sequence has also been set up for the “OK” alarm state. If, however, the alarm message was already acknowledged before this, an “alarm state OK” alarm message appears on the display and this also has to be confirmed.

The “warning” alarm state is shown in orange, an “alarm” is shown in red and the “OK” alarm state is green.

Special case: RCM

RCM alarms do not require a signal sequence. They are always shown on the display. RCM alarms have a higher priority than other alarms. Other alarm messages are not lost, but they are only displayed once all the RCM alarm messages have been acknowledged or the RCM alarms are no longer pending. For safety reasons, RCM alarm messages flash continuously on the display.

Acknowledging an alarm state

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.

⇨ If an alarm status exists, the current alarm message is shown on the display.

2. Press the “OK” button to acknowledge the current alarm message.

Alternatively: Press the “CLR” button to acknowledge all pending alarm messages.

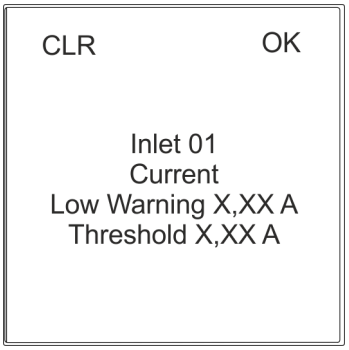


Fig. 39: Alarm message on the display

5.5 Displaying the measured data

Displaying the measured data on a single-phase PDU

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.
2. Scroll within the menus using the ⇦ / ⇨ buttons.

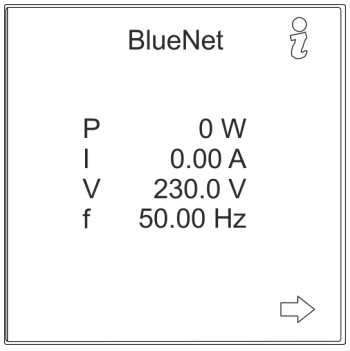


Fig. 40: “BlueNet” menu

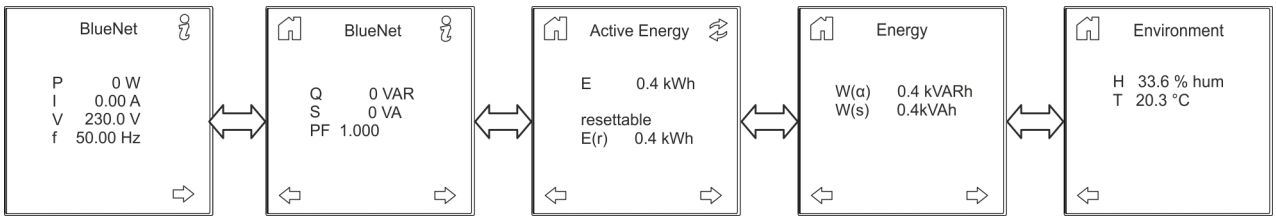


Fig. 41: Display of the measured data

⇨ The individual measured data elements are displayed.

Displaying the measured data on a three-phase PDU

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.
2. Scroll within the menus using the ⇦ / ⇨ buttons.

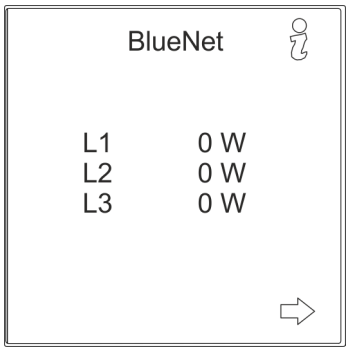


Fig. 42: “BlueNet” menu

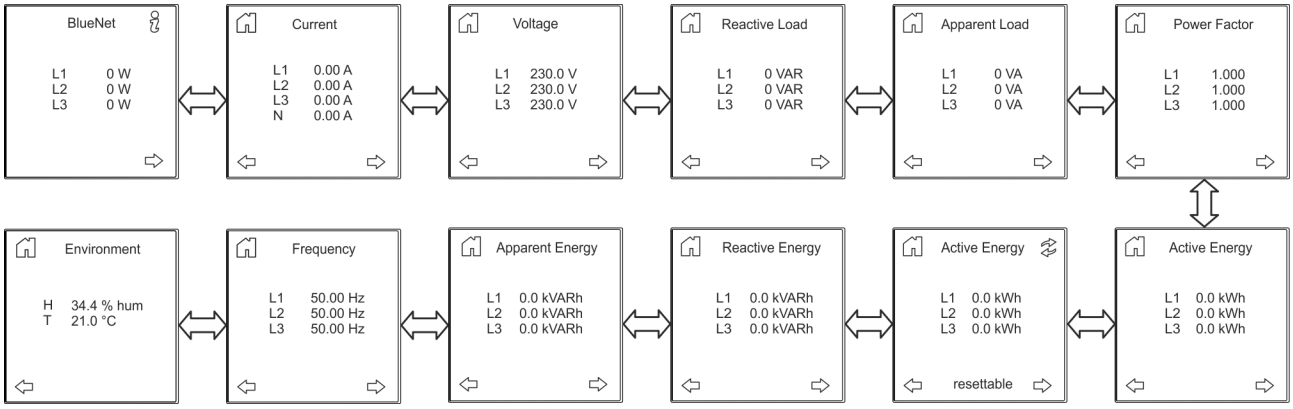


Fig. 43: Display of the measured data

⇨ The individual measured data elements are displayed.

5.6 Carrying out an RCM self-test

RCM self-tests at a slave PDU are only displayed in the RCM log if they were triggered via the web interface (↯ Chapter 6.5.1.6 “Carrying out an RCM self-test” on page 64).

If more than one RCM module is installed in a PDU, the RCM self-test can be executed for an individual RCM or for all the RCMS at once (example: ↯ “Carrying out an RCM self-test with RCM module at the phase level (three-phase PDU)” on page 36).

The RCM self-test for RCMs on different levels (Inlet, Phase, Fuse) works in the same way.

Performing an RCM self-test with RCM module at the inlet level (single-phase PDU)

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.

2. Use the button to open the “RCM” menu.

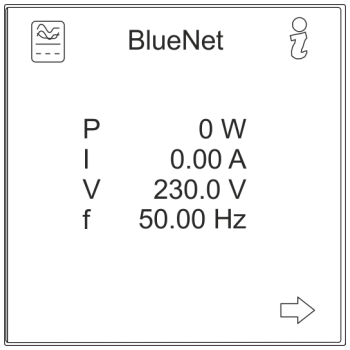


Fig. 44: “BlueNet” menu

3. Use the button to open the “RCM Selftest” menu.

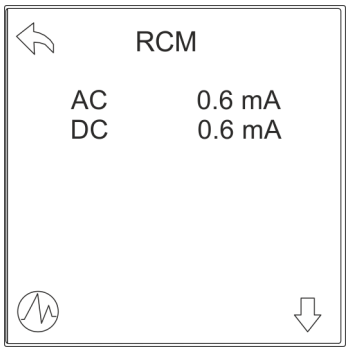


Fig. 45: “RCM” menu

4. Use the button for confirmation.

⇨ The RCM self-test is carried out.

The result of the RCM self-test is logged in the RCM log.

The result of the RCM self-test is indicated by colour coding on the display.

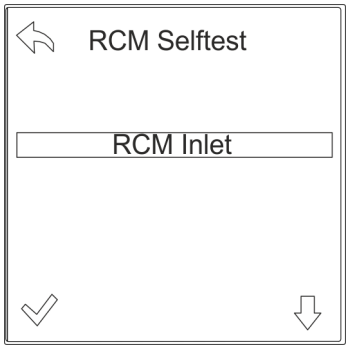


Fig. 46: “RCM Selftest” menu

The result of the RCM self-test is displayed with the following colour coding:

- *Green = the RCM self-test was successful.*
- *Red = the RCM self-test was not successful.*
- *Blue = the RCM self-test could not be carried out.*

Carrying out an RCM self-test with RCM module at the phase level (three-phase PDU)

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.
2. Use the button to open the “RCM” menu.

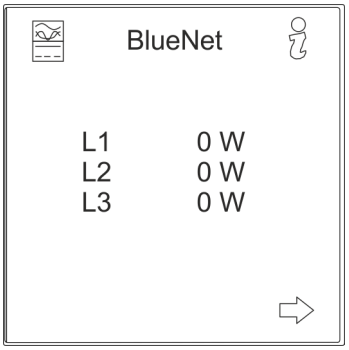


Fig. 47: “BlueNet” menu

3. Use the button to open the “RCM Selftest” menu.

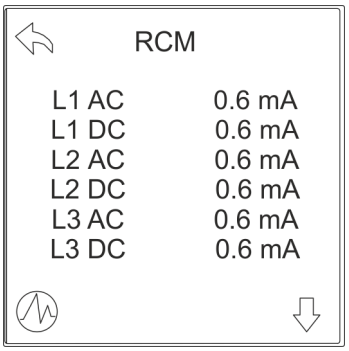


Fig. 48: “RCM” menu

4. Use the ⇩/⇧ buttons to select the desired phase and confirm by pressing the ✓ button.

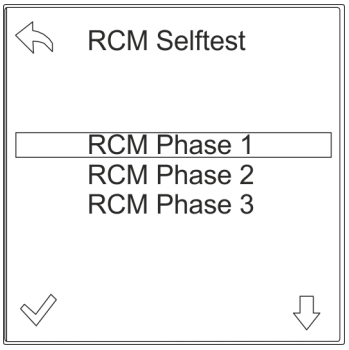


Fig. 49: “RCM Selftest” menu

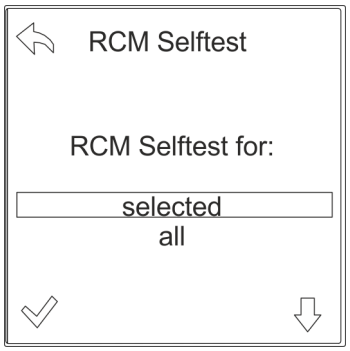


Fig. 50: “RCM Selftest” menu

5. Use the ⇩/⇧ buttons to select if the RCM self-test is only to be carried out for the selected phase or for all phases. Use the ✓ button for confirmation.

⇨ The RCM self-test is carried out.

The result of the RCM self-test is logged in the RCM log.

The result of the RCM self-test for the corresponding phase is displayed marked in colour at the display.

The result of the RCM self-test is displayed with the following colour coding:

- *Green = the RCM self-test was successful.*
- *Red = the RCM self-test was not successful.*
- *Blue = the RCM self-test could not be carried out.*

5.7 Resetting the effective energy

Resetting the effective energy on a single-phase PDU

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.

2. Scroll within the menus to the *“Active Energy”* menu using the ⇨ button.

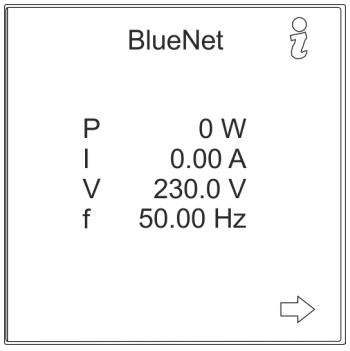


Fig. 51: “BlueNet” menu

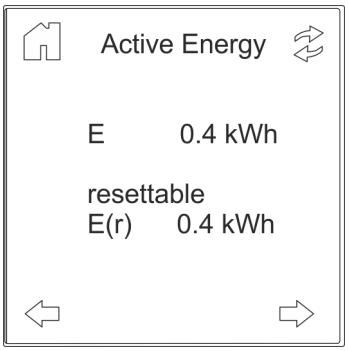


Fig. 52: “Active energy” menu

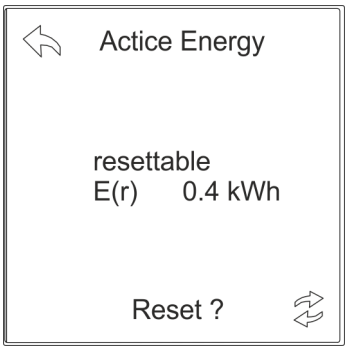


Fig. 53: “Active energy” menu

Resetting the effective energy on a three-phase PDU

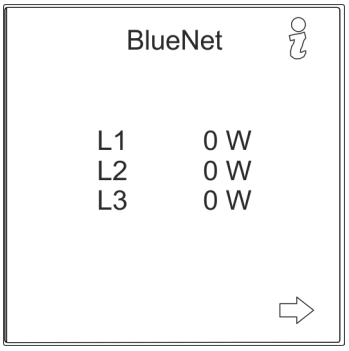


Fig. 54: “BlueNet” menu

3. *In the “Effective energy” menu, the display of the effective energy E(r) can be reset.*

Press the ⇄ button in the “Active energy” menu.

4. Use the ⇄ button to reset the display.

⇨ The display is reset and you return to the previous screen.

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.

2. Scroll within the menus to the *“Active Energy resettable”* menu using the ⇨ button.

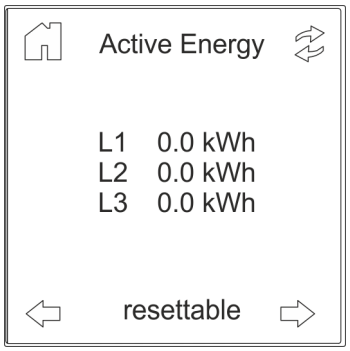


Fig. 55: "Active Energy resettable" menu

3. *In the "Effective energy resettable" menu, the display of the effective energy E(r) can be reset.*

Press the ⇄ button in the "Active energy resettable" menu.

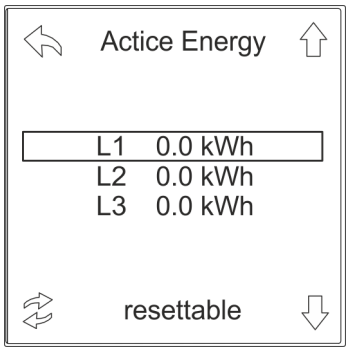


Fig. 56: "Active Energy resettable" menu

4. Use the ⇩/⇧ buttons to select the desired phase and press the ⇄ button.

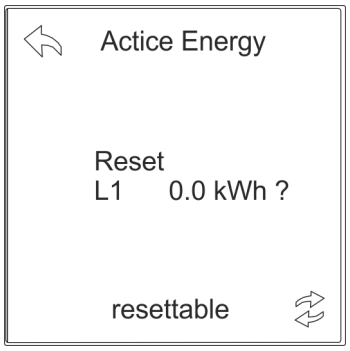


Fig. 57: "Active Energy resettable" menu

5. Use the ⇄ button to reset the display.

⇨ The display is reset and you return to the previous screen.

5.8 Displaying the system information

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.
2. Use the button to open the “System” menu.

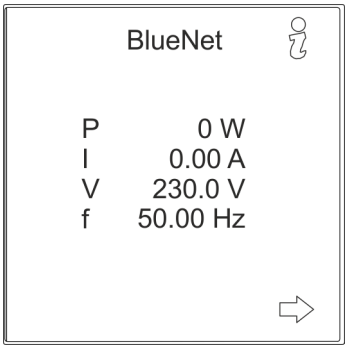


Fig. 58: “BlueNet” menu

⇨ The system settings are displayed.

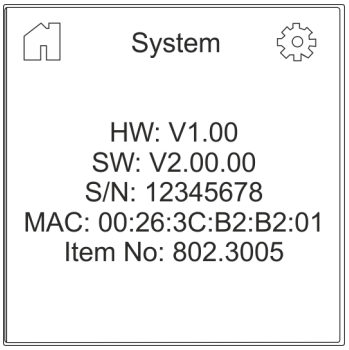


Fig. 59: “System” menu

5.9 Setting the illumination time

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.
2. Use the button to open the “System” menu.

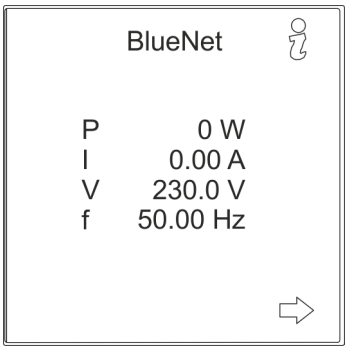


Fig. 60: “BlueNet” menu

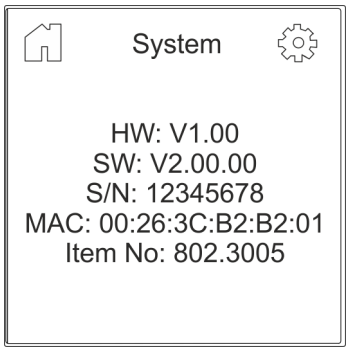


Fig. 61: “System” menu

3. Use the ⚙ button to open the “Settings” menu.

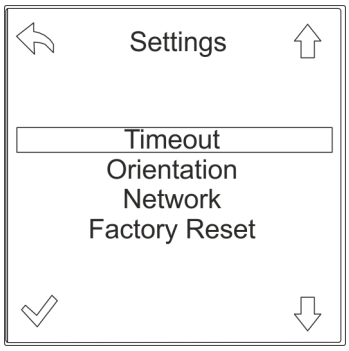


Fig. 62: “Settings” menu

4. Select the “Timeout” menu and confirm by pressing the ✓ button.

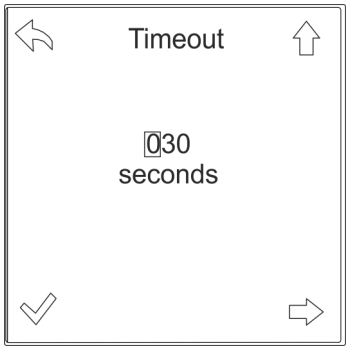


Fig. 63: “Timeout” menu

5. Select the desired time for the display illumination and confirm by pressing the ✓ button.

Individual digits can be selected using the ⇨ button and incremented using the ⇧ button.

⇨ The set illumination time is accepted.

5.10 Setting the display orientation

Depending on the installation position, the display may be difficult to read. For this purpose, the display orientation can be adjusted manually.

Personnel: ■ IT specialist

1. Press any button on the PDU to activate the display.
2. Use the button to open the “System” menu.

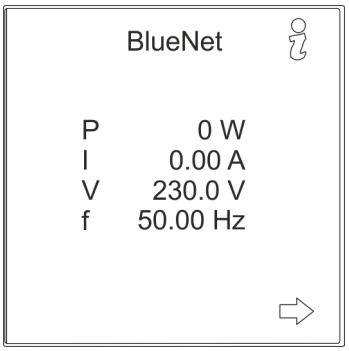


Fig. 64: “BlueNet” menu

3. Use the button to open the “Settings” menu.

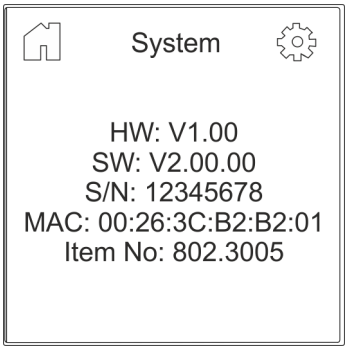


Fig. 65: “System” menu

4. Use the button to select the “Orientation” menu and confirm by pressing the button.

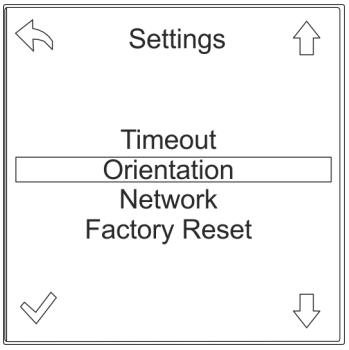


Fig. 66: “Settings” menu

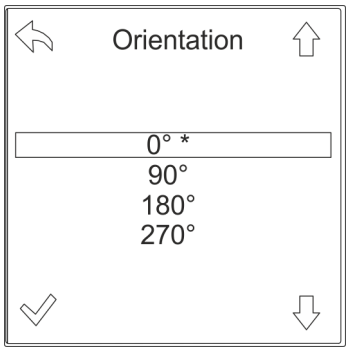


Fig. 67: “Orientation” menu

5. Use the ⇩/⇧ buttons to select the desired display orientation and confirm by pressing the ✓ button.

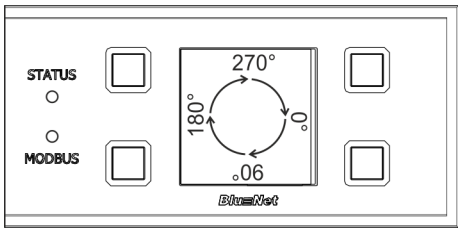


Fig. 68: Display orientation

⇨ The orientation of the display changes and the function of the individual buttons changes accordingly.

5.11 Setting the Modbus address on the slave PDU

1. Press any button on the slave PDU to activate the display.
2. Use the ⓘ button to open the “System” menu.

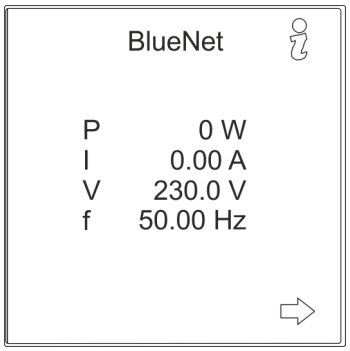


Fig. 69: “BlueNet” menu

3. Use the ⚙ button to open the “Settings” menu.

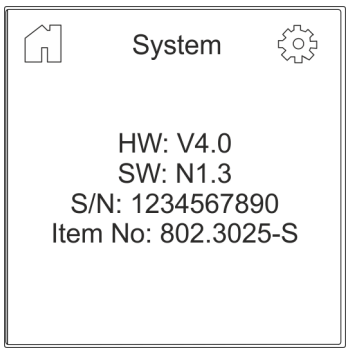


Fig. 70: “System” menu

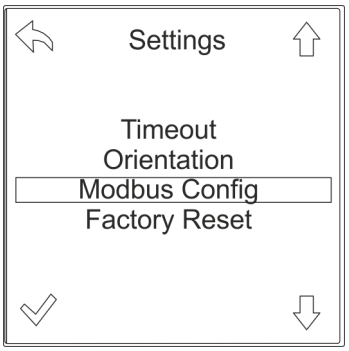


Fig. 71: “Settings” menu

4. Use the ⇩ button to select the “Modbus Config” menu and confirm by pressing the ✓ button.

The baud rate must not be changed!

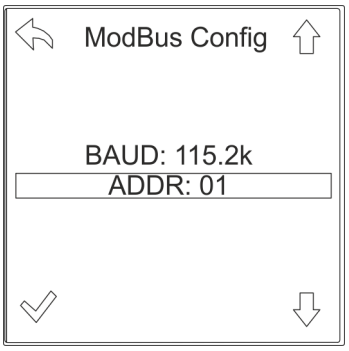


Fig. 72: "Modbus Config” menu

5. Use the ⇩ button to select the “ADDR” menu and confirm by pressing the ✓ button.

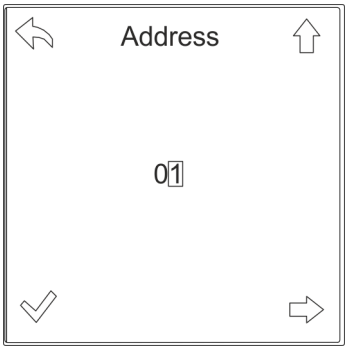


Fig. 73: Setting the Modbus address

6.

Valid Modbus addresses can be assigned from 1 to 16. The Modbus address must be unique.

If necessary, use the ⇨ button to switch between digits. Use the ⇧ button to set the address for the slave PDU and confirm by pressing the ✓ button.

5.12 Resetting the PDU or PU2 to the factory settings via the menu

If the PDU or PU2 is reset to the factory settings, any settings made on the device are lost.

Personnel: ■ IT specialist

1. Press any button on the PDU or PU2 to activate the display.
2. Use the button to open the “System” menu.

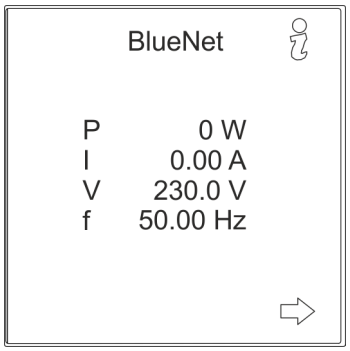


Fig. 74: “BlueNet” menu

3. Use the button to open the “Settings” menu.

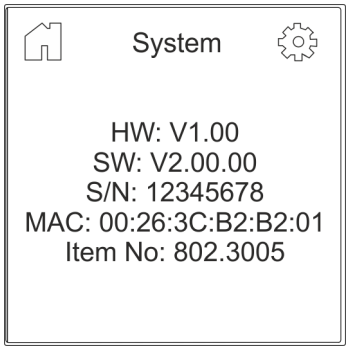


Fig. 75: “System” menu

4. Press the button to select the “Factory Reset” menu and confirm by pressing the button.

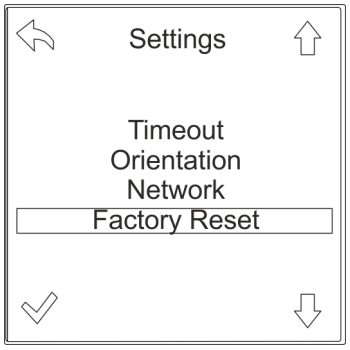


Fig. 76: “Settings” menu

Fig. 77: Query on the display

5. Confirm the query *"Do you really want to reset the device to factory default settings?"* by pressing the ✓ button.

Fig. 78: Message on the display

⇨ The message *"Factory reset will be performed after rebooting device"* appears. The PDU or PU2 is restarted and reset to the factory settings.

5.13 Restarting the PDU

Personnel: ■ IT specialist

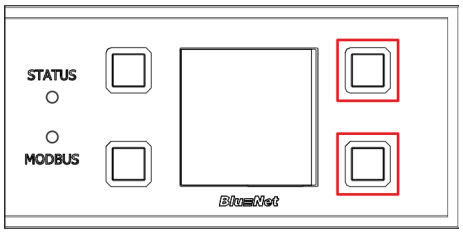


Fig. 79: Display with control buttons

1. Press and hold the two buttons to the right of the display (Fig. 79/red marking).

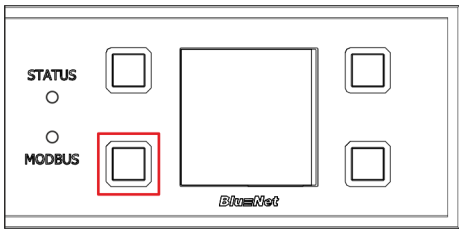


Fig. 80: Display with control buttons

2. Press the button next to the Modbus LED for two seconds and release it again (Fig. 80/red marking).

3. Wait until the display goes off.

4. Release the two buttons next to the display (Fig. 79/red marking).

⇨ The PDU restarts.

5.14 Resetting the PDU to factory settings using the buttons (Master PDU only)

Personnel: ■ IT specialist

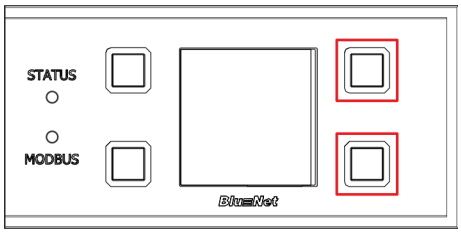


Fig. 81: Display with control buttons

1. Press and hold the two buttons to the right of the display (Fig. 81/red marking).

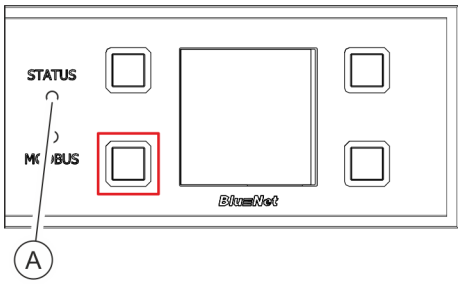


Fig. 82: Display with control buttons

2. Press the button next to the Modbus LED for two seconds and release it again (Fig. 82/red marking).
3. Wait until the status LED lights up white (Fig. 82/Ⓐ).
4. Release the two buttons next to the display (Fig. 81/red marking).

   ⇨ The PDU is reset to the factory settings.

5.15 Resetting the PU2 to factory settings using the buttons

Personnel: ■ IT specialist

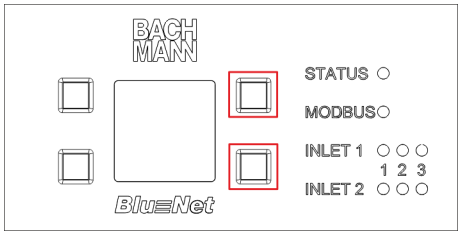


Fig. 83: Display with control buttons

1. Press and hold the two buttons to the right of the display (Fig. 83/red marking).

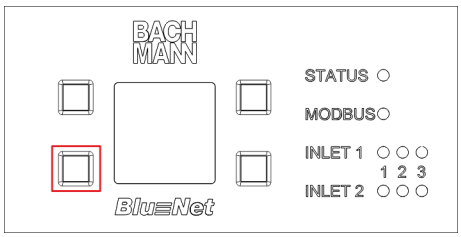


Fig. 84: Display with control buttons

2. Press the button at the bottom left for two seconds and release it again (Fig. 84/red marking).
3. Wait until the display goes off.
4. Release the two buttons to the right of the display (Fig. 83/red marking).

   ⇨ The PU2 restarts.

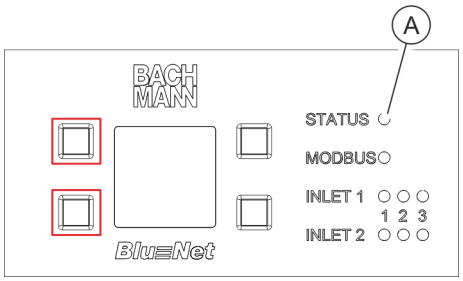


Fig. 85: Display with control buttons

5. Press the buttons to the left of the display during the restart (Fig. 85/red marking).

6. Wait until the status LED lights up white (Fig. 85/Ⓐ).

7. Release the two buttons to the left of the display (Fig. 85/red marking).

⇨ The PU2 is reset to the factory settings.

6 Overview and operation of the web interface

Initial login

Initial login to the web interface takes place via HTTP. The IP address of the PDU is entered in the format “http://<IP address>" in the address line of the web browser. To use HTTPS, it has to be activated in the web server settings. If HTTPS is activated, the IP address of the PDU is entered in the format “https://<IP address> in the address line of the web browser.

Changes to the system

Changes to the system, such as changing the network configuration or creating a user, can only be made by a user with the “admin” user role.

6.1 Menu structure of the web interface

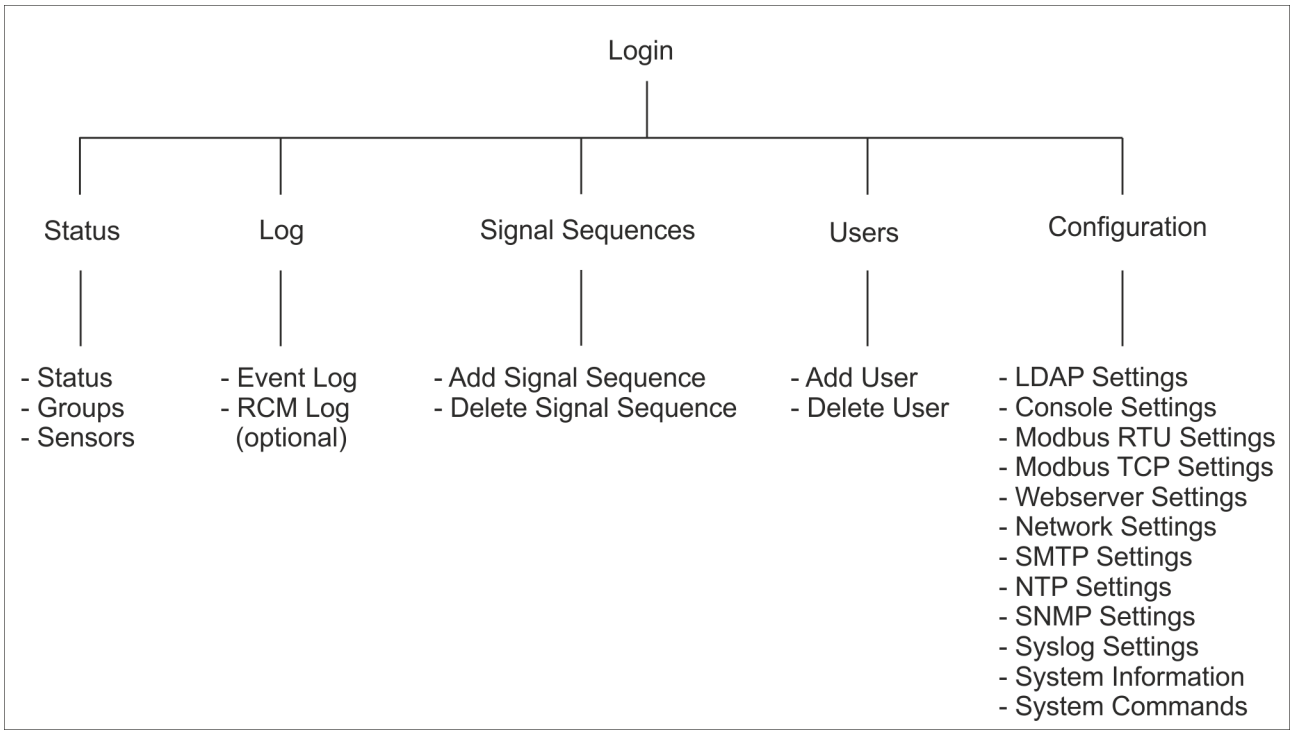


Fig. 86: Menu structure of the web interface

6.2 Login to the web interface

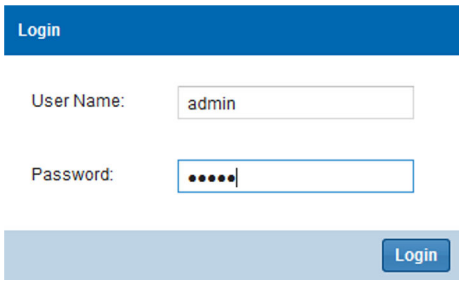


Fig. 87: Login

1. In a web browser, enter the IP address of the PDU.
   ⇨ The login information is requested (Fig. 87).
2. Enter the user name and password. Confirm the entry by clicking the *"Login"* button.

User data for the first login:
User: admin
Password: admin

After the first login, it is recommended to change the password (↬ Chapter 6.8.2 "Managing a local user" on page 88).

Login to the web interface via LDAP is possible if the PDU was connected to a directory service first (↬ Chapter 10.4.2 "Configuring LDAP settings" on page 121), if the specified groups were created in the directory service and if the directory service users were assigned to them (↬ Chapter 10.4.1 "Managing users in the directory service" on page 120).

6.3 Setting the user language

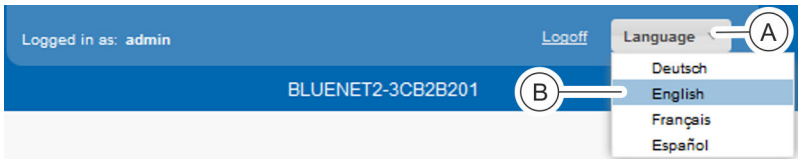


Fig. 88: Changing the language

1. Click the *"Language"* button (Fig. 88/Ⓐ) in the title line.
   ⇨ An option menu opens.
2. Select the desired language (e.g. Fig. 88/Ⓑ).
   ⇨ The language of the web interface is changed.

6.4 Explanation of the web interface

Overview of the web interface

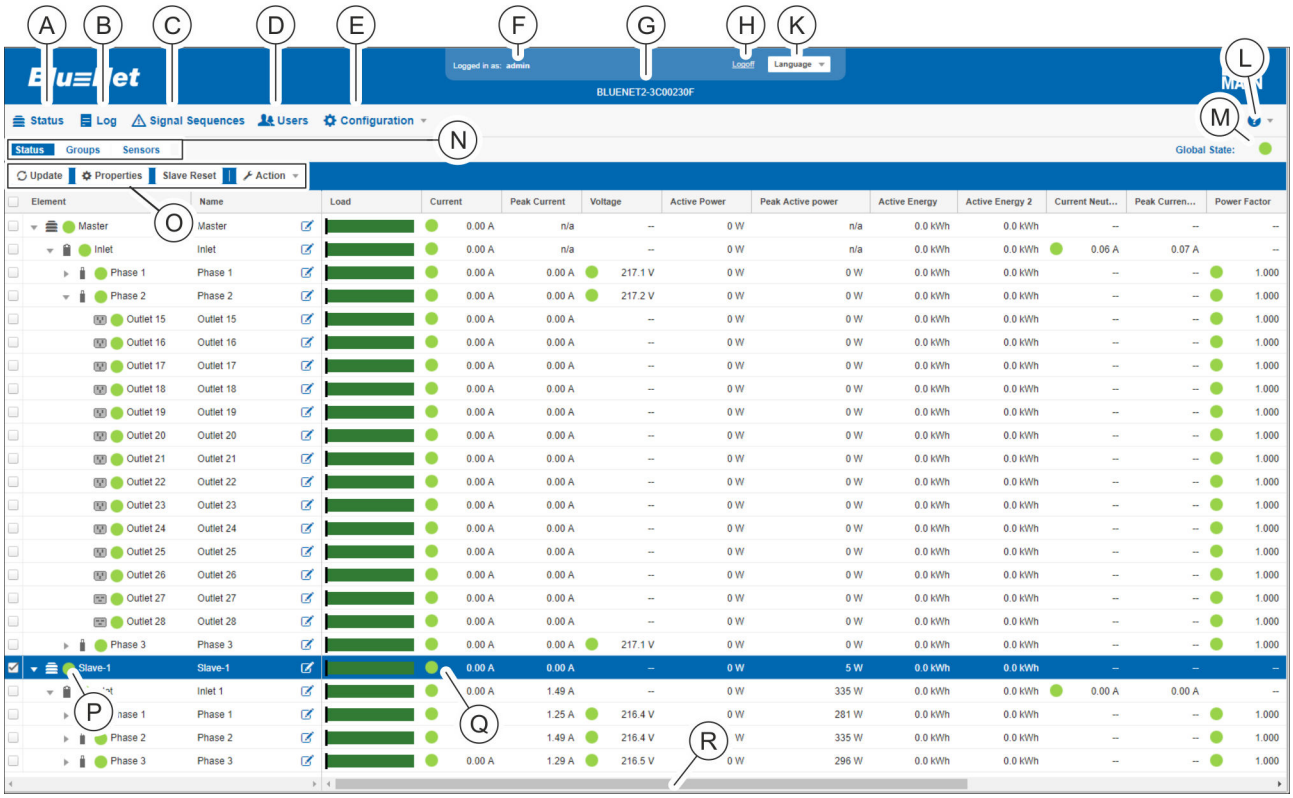


Fig. 89: Overview of the web interface

Ⓐ "Status" menu (display of the status of the PDU and connected loads) (↳ *Chapter 6.5 ""Status" menu" on page 54*)
Ⓑ "Log" menu (display of the event log)
Ⓒ "Signal Sequences" menu (management of signal sequences)
Ⓓ "Users" menu (user administration)
Ⓔ "Configuration" menu (configuration of the PDU)
Ⓕ Display of the user currently logged in
Ⓖ PDU host name
Ⓗ *"Log out"* button (for logging the user out)
Ⓚ Language option menu
Ⓛ Licence information
Ⓜ Display of the global status for all connected devices (master PDU, slave PDU, PU2) (↳ *"Explanation of the global status" on page 52*)
Ⓝ Selectable tabs of a menu
Ⓞ Menu-specific buttons
Ⓟ Status of individual elements (↳ *"Explanation of the status of individual elements" on page 52*)
Ⓠ Information field
Ⓡ Scrollbars (for scrolling within the window)

You can press the "Properties" button to display elements in the detail view (↳ "Buttons in the detail view (example for one phase)" on page 53). The detail view is displayed on the right in the window (↳ "Detail view of an element" on page 56).

Explanation of the global status

Colour	Light	State
	Continuously green	Overall status OK.
	Continuously red	One of the PDUs or socket groups has an alarm.
	Continuously orange	One of the PDUs or socket groups has a warning.
	Flashing magenta/black	An update is being imported to one of the slave PDUs.

Explanation of the status of individual elements

Colour	Light	State
"n/a" is displayed	None	Measured data is expected but is currently not available. “n/a” is displayed in the information field (Fig. 89/◎).
--	None	Measured data undefined, is only displayed in the information field (Fig. 89/◎).
None	None	The sensor or device is being identified.
	Continuously green	Measured data OK
		For sockets and fuses, indicates that they are switched on.
	800 ms dark green/ green, 200 ms dark green/white	For sockets, indicates that the relay is switched on and identification has been set.
	200 ms black/green, 800 ms dark green/black	For sockets, indicates that the relay is switched off and identification has been set
	Continuously orange	HighWarning or LowWarning measured value
		For sockets and fuses, indicates that they are switched on and a warning is present.
		Indicates a warning at one of the child elements.
	800 ms brown/orange, 200 ms brown/white	For sockets, indicates that the relay is switched on, a warning is present and identification has been set.
	200 ms black/orange, 800 ms orange/black	For sockets, indicates that the relay is switched off, a warning is present and identification has been set.
	100 ms black/orange, 400 ms orange/black	For sockets and fuses, indicates that they are switched off and a warning is present.
	Continuously red	HighAlarm or LowAlarm measured value
		For sockets and fuses, indicates that they are switched on and an alarm is present.
		Indicates an alarm at one of the child elements.

Colour	Light	State
		Indicates that one of the following devices is not available.
	Continuously dark red/ black	Measured data sensor or device is not available.
	800 ms dark red/red, 200 ms dark red/white	For sockets, indicates that the relay is switched on, an alarm is present and identification has been set.
	200 ms black/red, 800 ms dark red/black	For sockets, indicates that the relay is switched off, an alarm is present and identification has been set.
	100 ms black/red, 400 ms dark red/black	For sockets and fuses, indicates that they are switched off and an alarm is present.
	Continuously black	For sockets and fuses, indicates that they are switched off.
	Continuously blue	Firmware version of the slave PDU newer than firmware version of the master PDU. The master PDU has to be updated.
	200 ms black/magenta, 800 ms magenta/black	Signals that software/firmware is currently being updated.
	Continuously grey	Indicates that a switching operation is in progress. No alarm is displayed during the switching operation.

Buttons in the detail view (example for one phase)

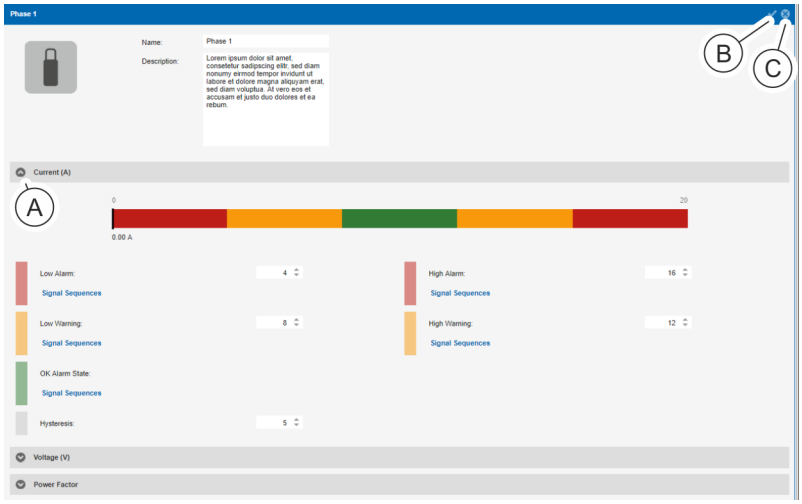


Fig. 90: Buttons in a detail view

(A) Button for expanding and collapsing an area
(B) Button for saving changes and closing the detail view
(C) Button for closing the detail view. If any changes were made previously, a security prompt appears asking whether you wish to discard the changes.

6.5 “Status” menu

6.5.1 “Status” tab

6.5.1.1 Overview

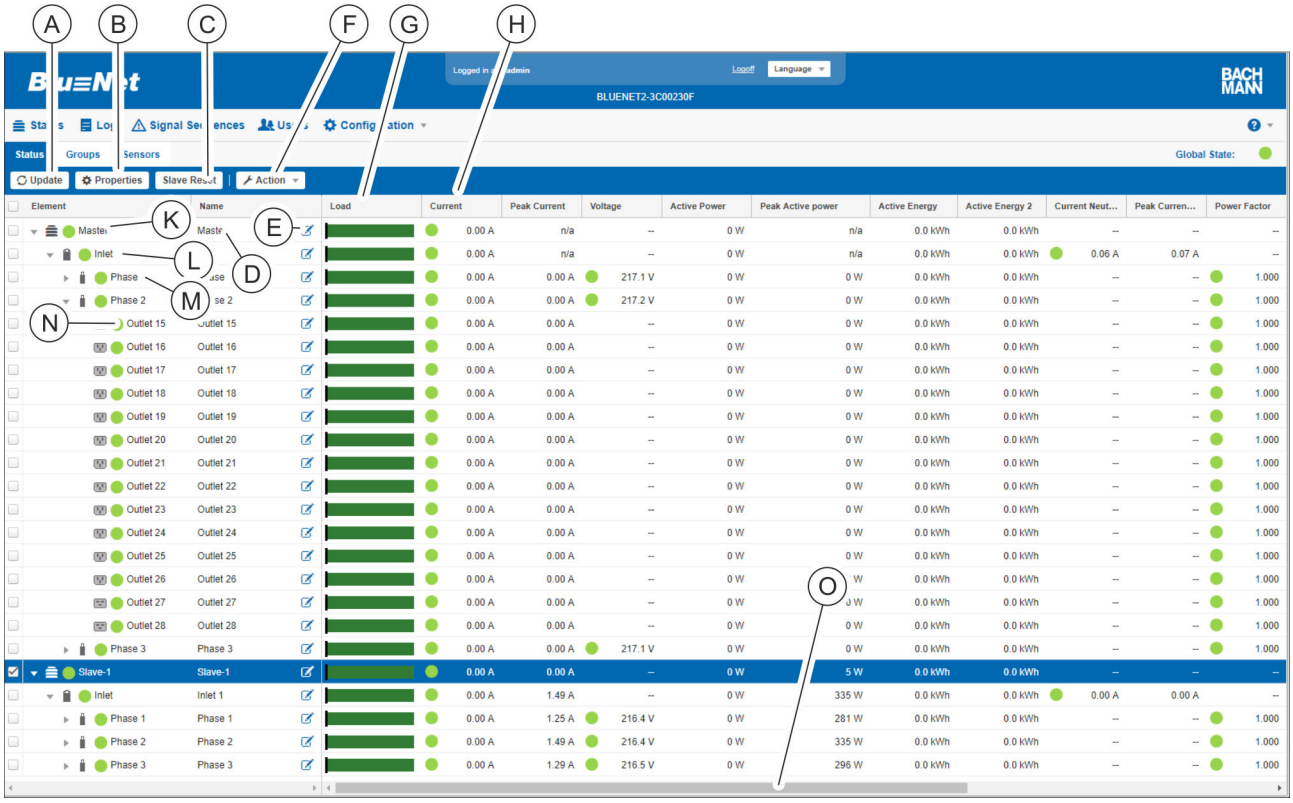


Fig. 91: “Status” menu – “Status” tab (a three-phase PDU in this example)

Ⓐ *“Update”* button for updating the display
Ⓑ *“Properties”* button for displaying details and for configuring an element (↳ *“Detail view of an element” on page 56*)
Ⓒ *“Slave Reset”* button for resetting a slave PDU. Alternatively: *“Remove device”* button for removing a slave PDU (button only appears for slave PDUs with the *“Lost”* status.)
Ⓓ Display of the name of an element
Ⓔ Button for designating an element
Ⓕ *“Action”* button for identifying and switching individual sockets (not for BN3000) and if RCM is available for starting an RCM self-test
Ⓖ Display of the load (with display of defined threshold values, ↳ *“Explanation of the load threshold value” on page 58*)
Ⓗ Display of the measured data (↳ *“Explanation of the displayed measured data” on page 55*)
Ⓚ Display of the PDU (expandable sub-elements)
Ⓛ Display of the inlet (expandable sub-elements)
Ⓜ Display of the phase (expandable sub-elements)
Ⓝ Software status of an element (↳ *“Explanation of the status of individual elements” on page 52*)
Ⓞ Scrollbars (for scrolling within the window)

In the “Status” menu, the status of the master PDU and any connected slave PDUs is displayed. The sub-elements can be expanded using the triangle next to the individual elements.

If circuit breakers are installed in a phase (Fig. 91/Ⓜ), they are displayed under the “Phase” level.

If an RCM is installed, it is displayed at the relevant level.

On the "Status" tab, you can display the performance and consumption values for the individual elements.

Explanation of the displayed measured data

Parameter	Explanation
Load	The load range is indicated in the "Load" column in the form of a bar. The present current rating value is shown in the form of a vertical line within the defined load range on the bar. Threshold values can be defined for the loads of individual elements (↬ *"Explanation of the load threshold value" on page 58*). If a defined value is exceeded or is fallen short of, a defined signal sequence can be triggered. No threshold values are defined if the entire bar is green.
Current	The "Current" parameter displays the currently measured electric current in the element in question in A. The LED in front of the value displays whether there is a warning or a critical message.
Peak current	The "Peak current" parameter displays the maximum current so far. After selecting this parameter with the cursor, a symbol appears that allows you to reset the maximum current.
Voltage	The "Voltage" parameter displays the voltage per phase.
Effective power	The "Effective power" parameter displays the current effective power of individual elements in W.
Peak effective power	The "Peak effective power" parameter displays the maximum power so far. After selecting this parameter with the cursor, a symbol appears that allows you to reset the maximum power.
Effective energy	The "Effective energy" parameter displays the effective energy of individual elements ex works in kWh (cannot be reset).
Effective energy 2	The "Effective energy 2" parameter displays the current effective energy of individual elements in kWh. After selecting this parameter with the cursor, a symbol appears that allows you to reset the effective energy 2.
Current neutral	The "Current neutral" parameter displays the current present at the neutral conductor for a 3-phase PDU.
Peak current neutral	The "Peak current neutral" parameter displays the maximum current applied to the neutral conductor for a 3-phase PDU. After selecting this parameter with the cursor, a symbol appears that allows you to reset the maximum current applied to the neutral conductor.
Power factor	The "Power factor" parameter displays whether a capacitive or inductive load is present. The LED in front of the value displays whether a message is present.
Reactive power	The "Reactive power" parameter displays the reactive power of connected devices.
Apparent power	The "Apparent power" parameter displays the apparent power of connected devices.

Parameter	Explanation
Reactive energy	The “Reactive energy” parameter displays the consumed reactive energy of connected devices in kVARh.
Apparent energy	The “Apparent energy” parameter displays the consumed apparent energy of connected devices in kVAh.
Frequency	The “Frequency” parameter displays the frequency per phase.
RCM AC	If a differential current analyser is installed, the measured differential current of the alternating voltage is displayed.
RCM DC	If a differential current analyser is installed, the measured differential current of the DC voltage is displayed.
Peak RCM AC	The “Peak RCM AC” parameter displays the maximum residual current measured so far for the alternating current voltage. After selecting this parameter with the cursor, a symbol appears that allows you to reset the maximum power.
Peak RCM DC	The “Peak RCM DC” parameter displays the maximum residual current measured so far for the direct current voltage. After selecting this parameter with the cursor, a symbol appears that allows you to reset the maximum power.

Detail view of an element

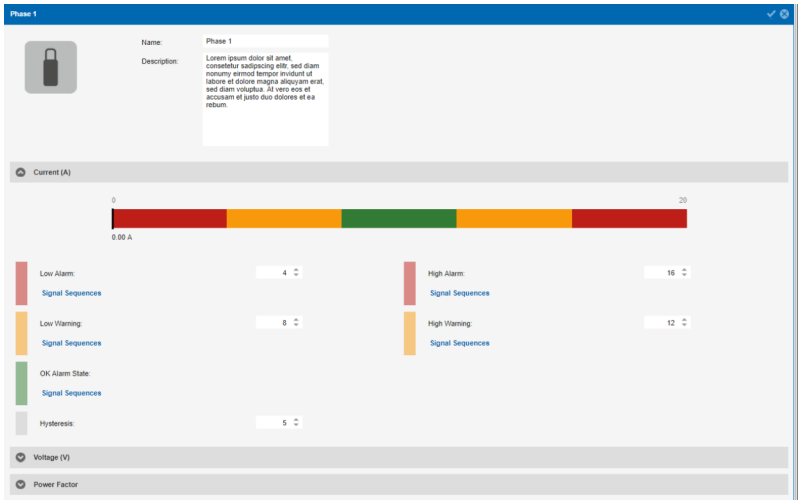


Fig. 92: Detail view for “Phase 1” (example)

In the “Status” menu, select an individual element and then click the *“Properties”* button (Fig. 91/Ⓑ) to call up the details for this element. In this window, measured data can be displayed and threshold values and signal sequences can be defined (↳ *Chapter 6.7.3 “Setting up signal sequences and threshold values for individual elements” on page 80*).

Status of the element and link to a signal sequence

In the detail view, for certain elements, a “Lost” status (loss of signal to a PDU or a connected sensor) or an “OK” status (reconnected) can be linked with a signal sequence (example: ↳ Chapter 6.7.5 “Setting up signal sequences for a GPIO module” on page 84).

In addition, threshold values can be defined for some elements (e.g. PDU, phase, inlet) and linked with a signal sequence (↳ Chapter 6.7.3 “Setting up signal sequences and threshold values for individual elements” on page 80).

Symbols in the detail view

Symbol	Explanation
	PDU
	PU2
	Inlet
	Outlet (single-phase)
	Outlet (three-phase)
	Measurement group (measured value group)
	Phase
	RCM (residual current monitor/ differential current analyser)
	Fuse
	Socket

Symbol	Explanation
	Socket group
	Sensor
	GPIO module or internal GPIO

Explanation of the load threshold value

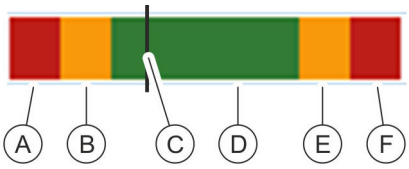


Fig. 93: Explanation of the load threshold value

Ⓐ Marking of the threshold value for the “Low Alarm” range
Ⓑ Marking of the threshold value for the “Low Warning” range
Ⓒ Display of the current load
Ⓓ Marking of the defined load range (green)
Ⓔ Marking of the threshold value for the “High Warning” range
Ⓕ Marking of the threshold value for the “High Alarm” range

For individual elements, e.g. a phase or a sensor, threshold values can be defined. The threshold values define the upper and lower limit for a defined value. If the threshold values are exceeded or fallen short of, a message may be issued by a signal sequence (↳ *Chapter 6.7.3 “Setting up signal sequences and threshold values for individual elements” on page 80*).

6.5.1.2 Modifying the grouping of the measured data

Personnel: ■ IT specialist

Proceed as follows to change the representation of individual measured data elements:

Opening the option menu

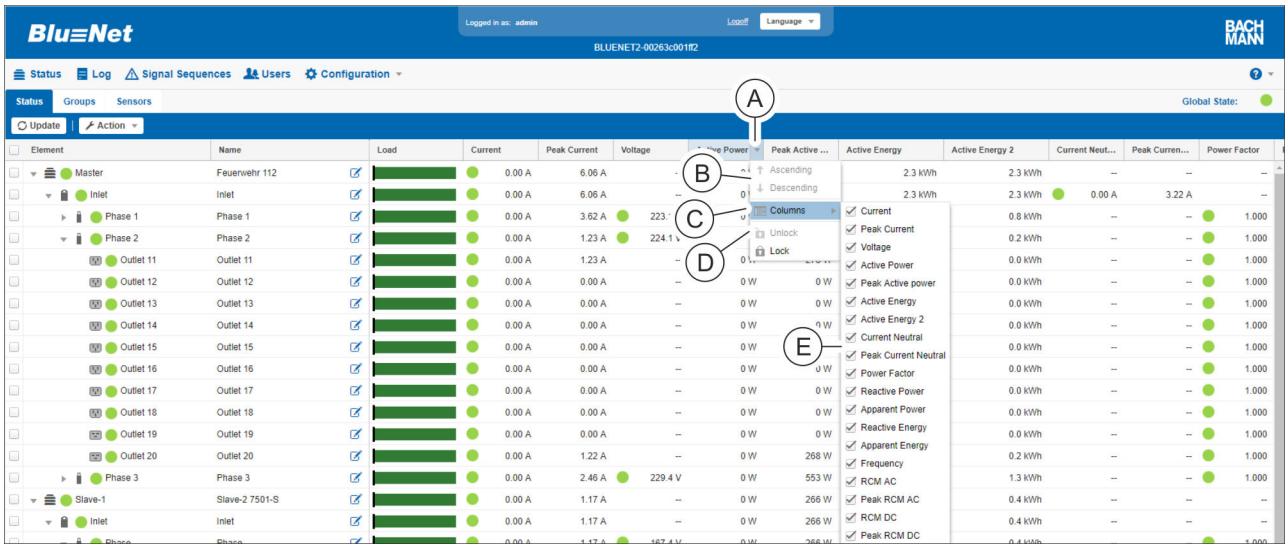


Fig. 94: Modifying the grouping of individual elements of measured data

1. Move the cursor in the title line of the measured data (Fig. 94/Ⓐ).

   ⇨ An arrow that can be used to open an option menu appears in the table.

Unlocking the column lock

2. Unlock the column lock by choosing the *"Unlock"* menu item (Fig. 94/Ⓓ).

Adjusting the width of a column

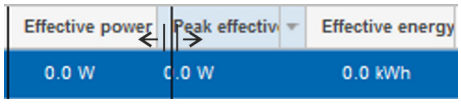


Fig. 95: Adjusting the column width

3. Move the cursor to the area between two columns and click and hold the left mouse button to adjust the width of a column (Fig. 95).

Changing the sort order

4. Change the parameter sorting by choosing the *"Ascending"* or *"Descending"* menu item (Fig. 94/Ⓑ).

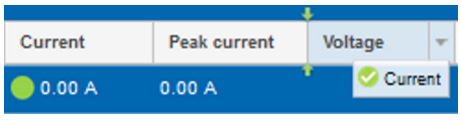


Fig. 96: Moving parameters

5. If necessary, click an individual parameter (e.g. *"Current"*) and move it within the title line (Fig. 96).

   ⇨ The selected parameter is moved within the table.

Hiding individual parameters

6. Using the *"Columns"* menu item (Fig. 94/Ⓒ), click the checkbox to hide or display the desired parameters (Fig. 94/Ⓔ).

Locking the column

7. Lock the column again by choosing the *“Lock”* menu item (Fig. 94/Ⓓ).

6.5.1.3 Modifying the names of individual elements

Personnel: ■ IT specialist

Proceed as follows to change the name of individual elements:

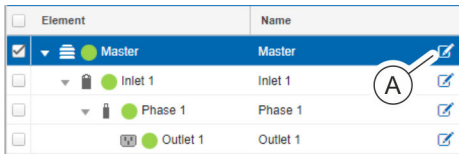


Fig. 97: Select the element

1. In the “Name” column, click on the pencil icon next to the element in question (Fig. 97/Ⓐ).
   ⇨ A text field opens (Fig. 98/Ⓐ).

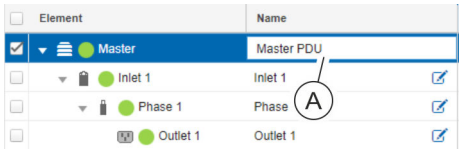


Fig. 98: Designating elements

2. Enter a name in the text field and press the *[ENTER]* button to confirm.

6.5.1.4 Resetting and removing slave PDUs

6.5.1.4.1 Resetting the slave PDU

Only active slave PDUs can be reset. The “Slave Reset” is only displayed in these cases.

Personnel: ■ IT specialist

1. Call up the “Status” menu.

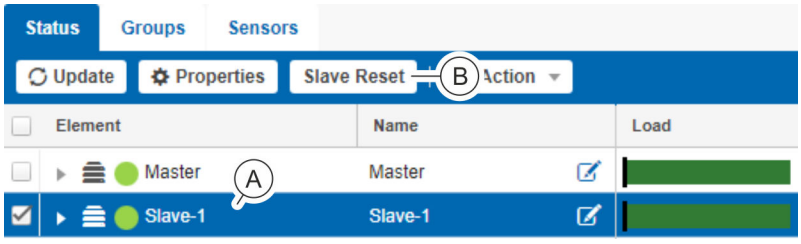


Fig. 99: “Status” menu – “Status” tab

2. Select the desired slave PDU in the “Status” tab (Fig. 99/Ⓐ).

3. Click the *"Slave Reset"* button (Fig. 99/Ⓑ).
   ⇨ The selected slave PDU is reset.

> *The set Modbus address, the energy measured data and the peak measured data are retained after the reset.*

6.5.1.4.2 Removing a slave PDU

> *Only slave PDUs to which there is no connection any more ("Lost" status) can be removed. The "Remove device" button is displayed only for slave PDUs with the "Lost" status.*

Personnel: ■ IT specialist

1. Call up the "Status" menu.

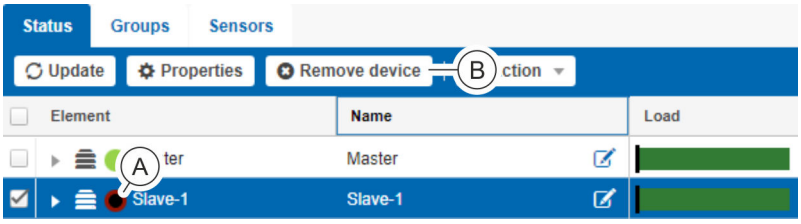


Fig. 100: "Status" menu – "Status" tab

2. Select the desired slave PDU in the "Status" tab (Fig. 100/Ⓐ).
3. Click the *"Remove device"* button (Fig. 100/Ⓑ).
   ⇨ The selected slave PDU is removed.

6.5.1.5 Switching and identifying sockets

6.5.1.5.1 Switching sockets on a PDU (BN5000/7000/7500 only)

> *Switching of individual sockets and switching of a socket group essentially function in the same way. The command for switching a socket group is forwarded to the associated sockets. A switching state is displayed on the web interface in colour with the status of individual sockets.*

Switching sockets or socket groups on and off

Personnel: ■ IT specialist

1. Call up the “Status” menu.

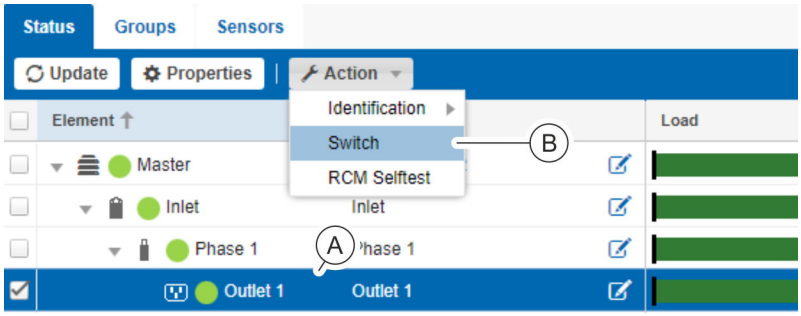


Fig. 101: “Status” menu – “Status” tab

2. Select the desired socket or socket group in the “Status” tab (Fig. 101/Ⓐ).

3. Call up the “Switch” window using *“Action ➔ Switch”* (Fig. 101/Ⓑ).

4. On the “Switch” window, go to the *“On/Off”* option menu and select the parameter *“Off”* (to switch off) or *“On”* (to switch on) (Fig. 102/Ⓐ).

Fig. 102: “Switch” window

5. **Only when switching off:** Enter a time in the *“Switch back on in (sec.)”* option menu (Fig. 103/Ⓐ).

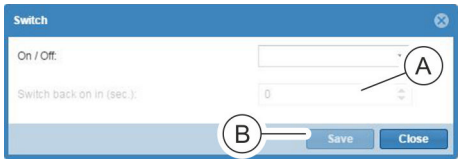


Fig. 103: Switching off a socket

In the “Switch back on in (sec.)” option menu, a value between “0” and “255” can be entered. With a value of “0”, the socket is switched off permanently. With a value of “0” or more, the socket is automatically switched back on after the entered time expires.

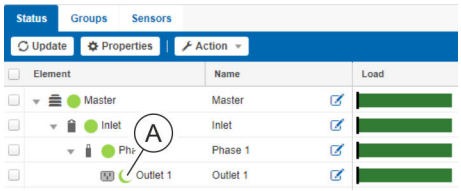


Fig. 104: "Status" menu – "Status" tab

6. Complete the operation by clicking the *"Save"* (Fig. 103/Ⓑ) button.

⇨ The software switch status of the element is displayed in the relevant colour (Fig. 104/Ⓐ).

> *If the socket has an alarm/warning state, this is indicated at the socket in the web interface (↯ "Explanation of the status of individual elements" on page 52) and at the status LEDs of the socket (↯ "Status LED on (BN3500/5000/7000/7500 only)" on page 14).*

6.5.1.5.2 Identifying sockets on a PDU (BN3500/5000/7000/7500 only)

> *Identifying individual sockets and identifying a socket group essentially function in the same way. The command for identifying a socket group is forwarded to the associated sockets. The sockets belonging to a socket group are displayed flashing in the web interface.*

Switching the identification of individual sockets or socket groups on and off

Personnel: ■ IT specialist

1. Call up the "Status" menu.

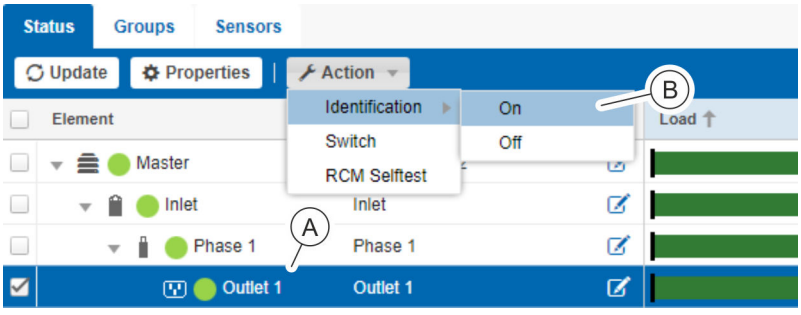


Fig. 105: "Status" menu – "Status" tab

2. Select the desired socket or socket group in the "Status" tab (Fig. 105/Ⓐ).

Switching identification on

3. Switch on the identification of the selected socket or socket group by choosing *"Action ➔ Identification ➔ On"* (Fig. 105/Ⓑ).

⇨ The socket LEDs of the selected socket or socket group flash on the PDU and on the web interface.

Switching identification off

4. Switch off the identification of the selected socket or socket group by choosing *“Action ➔ Identification ➔ Off”* (Fig. 105/Ⓑ).

   ⇨ The socket LEDs of the selected socket or socket group stop flashing on the PDU.

6.5.1.6 Carrying out an RCM self-test

Personnel: ■ IT specialist

1. Call up the “Status” menu.

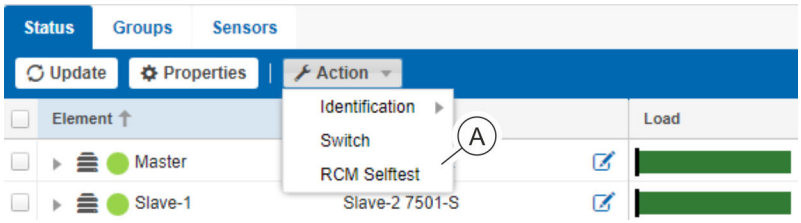


Fig. 106: “Status” menu

2. Select the RCM self-test using *“Action ➔ RCM Selftest”* (Fig. 106/Ⓐ).

   ⇨ The “RCM” window opens.

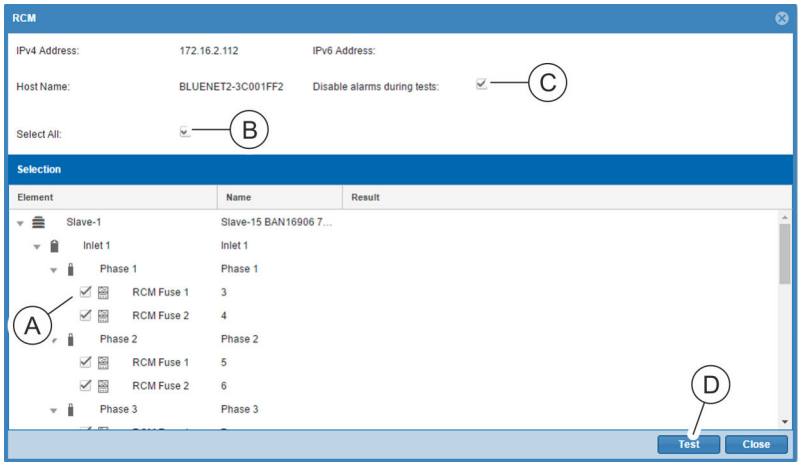


Fig. 107: “RCM” window

3. Select the individual RCM to be tested (Fig. 107/Ⓐ).

   Alternatively, select the *“Select All”* (Fig. 107/Ⓑ) checkbox to select all the available RCM for checking.

4. If necessary, uncheck the *“Disable alarms during tests”* checkbox (Fig. 107/Ⓑ) to activate the triggering of signal sequences during the test.

5. In the “RCM” window, click the *“Test”* button (Fig. 107/Ⓐ).

   ⇨ The RCM self-test is carried out.

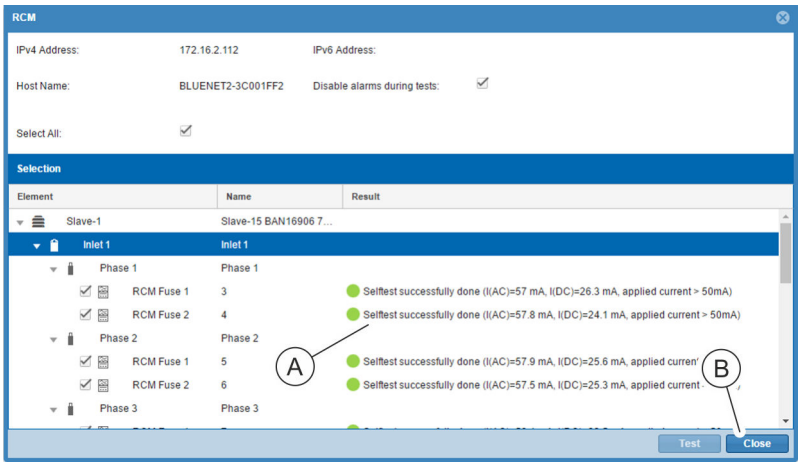


Fig. 108: “RCM” window

6. Check the results of the RCM self-test (Fig. 108/Ⓐ).

Additionally, the result of the RCM self-test is displayed in the “Log” menu – “RCM Log” tab (↳ Chapter 6.6 ““Log” menu” on page 73).

If during the conduction of several RCM self-tests, the testing of individual RCM modules cannot be started, the RCM self-test should be started individually for the RCM modules concerned.

If an RCM self-test can be carried out but is not reported back as being successful, the RCM module must be checked.

7. Exit the “RCM” window by clicking the *“Close”* button (Fig. 108/Ⓑ).

6.5.2 “Groups” tab

6.5.2.1 Overview

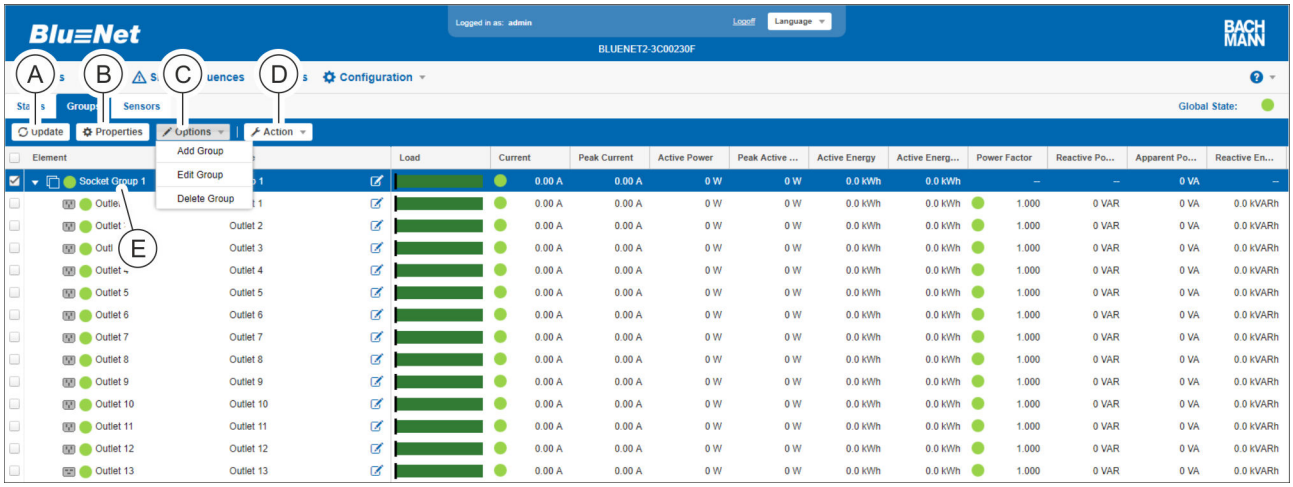


Fig. 109: “Status” menu – “Groups” tab

Ⓐ *“Update”* button for updating the display
Ⓑ *“Properties”* button for displaying details and for configuring an element (☞ *“Detail view of an element” on page 56*)
Ⓒ *“Options”* button for adding, editing and deleting groups
Ⓓ *“Action”* button for identifying and switching individual socket groups
Ⓔ Representation of a socket group

On the “Groups” tab, individual sockets can be combined into groups and managed. Groups provide the option of merging different sockets of a master/slave combination into a group. This allows, for example, all devices connected to all PDUs to be managed simultaneously.

Different sockets (switching and/or measuring) can be grouped together. If a socket group is then switched, only the sockets that support this function respond. Only the measuring sockets count towards the totalled measured data for a socket group.

If a group includes sockets for slave PDUs, and a slave PDU is temporarily not available (“Lost” status), all the group measurement data are added up without the sockets in question and switching commands for the sockets in question are ignored.

6.5.2.2 Managing socket groups (BN3500/5000/7000/7500 only)

If changes are made in this menu, it can take a while for the display on the screen to update.

Creating/modifying a group

Personnel: ■ IT specialist

1. Call up the "Status" menu.
2. Call up the "Groups" tab.

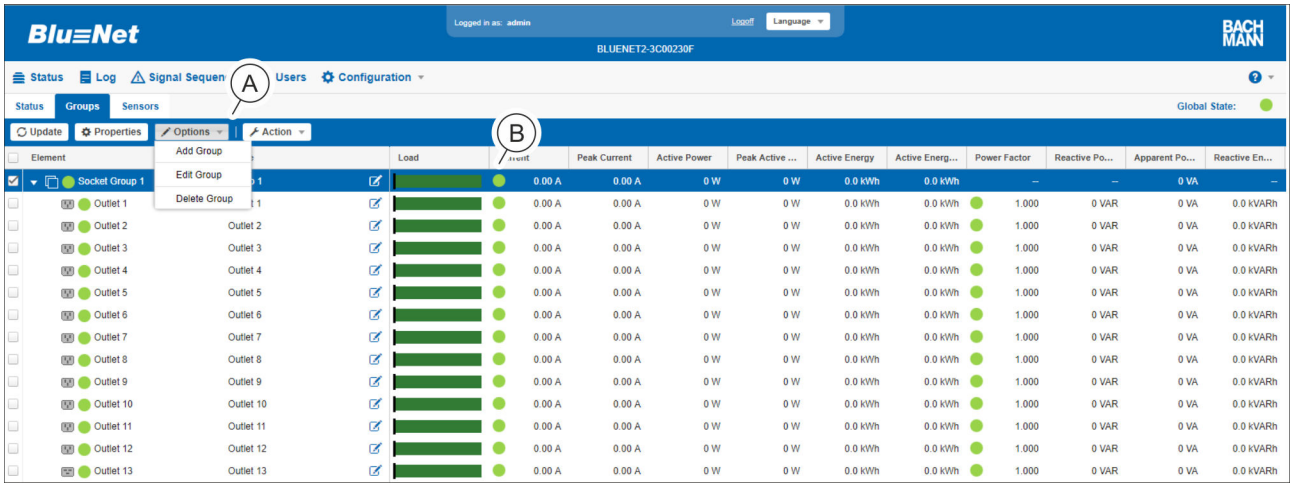


Fig. 110: "Status" menu – "Groups" tab

3. Choose *"Options ➔ Add Group"* to create a new socket group (Fig. 110/Ⓐ).

Modifying an existing group
To modify an existing group, select the desired group (Fig. 110/Ⓑ) and select the menu "Options ➔ Edit Group" (Fig. 110/Ⓐ).

⇨ The "Group" window opens (Fig. 111).

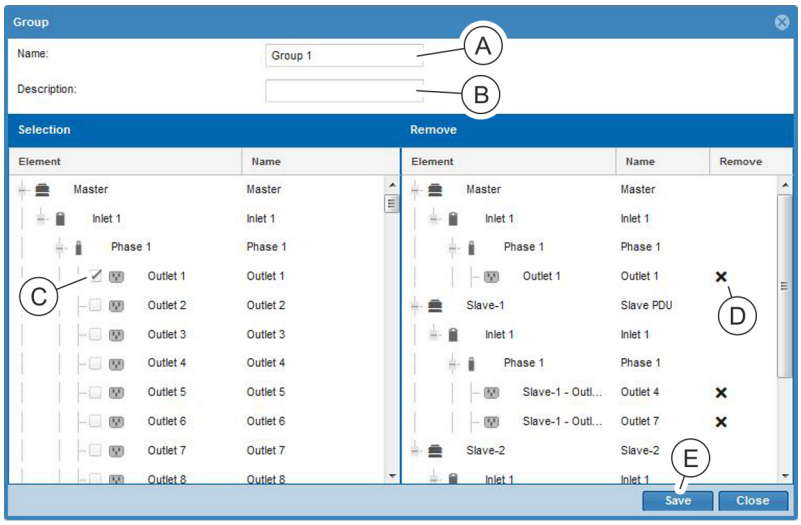


Fig. 111: “Group” window

4. In the “Group” window, add a name (Fig. 111/Ⓐ) and, if necessary, a description (Fig. 111/Ⓑ) for the group.

5. In the left-hand column, select individual sockets using the corresponding checkbox (Fig. 111/Ⓒ).

6. If necessary, remove individual sockets in the right-hand column by clicking the ✕ (Fig. 111/Ⓓ) button.

7. Press the *“Save”* button to save a socket group (Fig. 111/Ⓔ).

Deleting socket groups

To delete a socket group, select the desired socket group (Fig. 110/Ⓑ) and select the menu “Options ➔ Delete Group” (Fig. 110/Ⓐ). A security prompt appears and has to be confirmed.

6.5.2.3 Switching and identifying socket groups

Switching of individual sockets and switching of a socket group essentially function in the same way. See *Chapter 6.5.1.5 “Switching and identifying sockets” on page 61* for the procedure.

6.5.3 "Sensors" tab

6.5.3.1 "Sensors" menu view

Overview

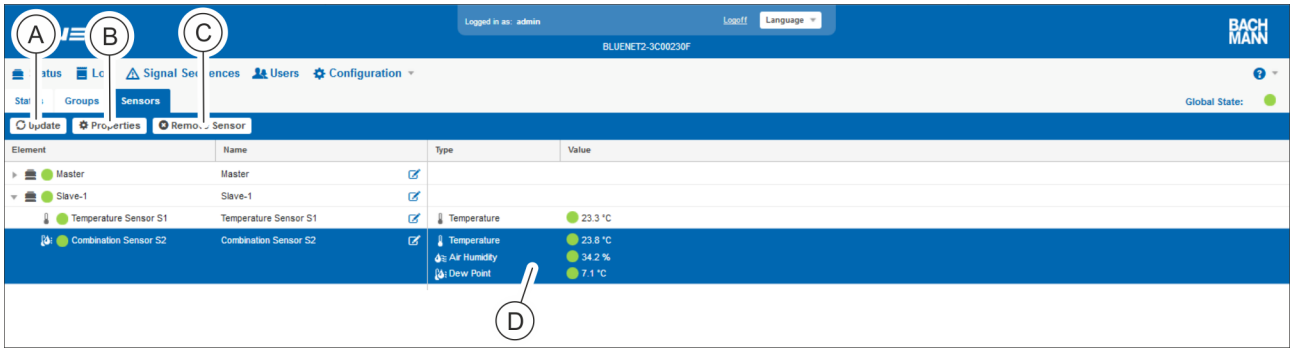


Fig. 112: "Status" menu – "Sensors" tab

Ⓐ *"Update"* button for updating the display
Ⓑ *"Properties"* button for opening the detail view
Ⓒ *"Remove Sensor"* button for removing a sensor
Ⓓ Display of the sensors for temperature and air humidity that are connected to the PDU

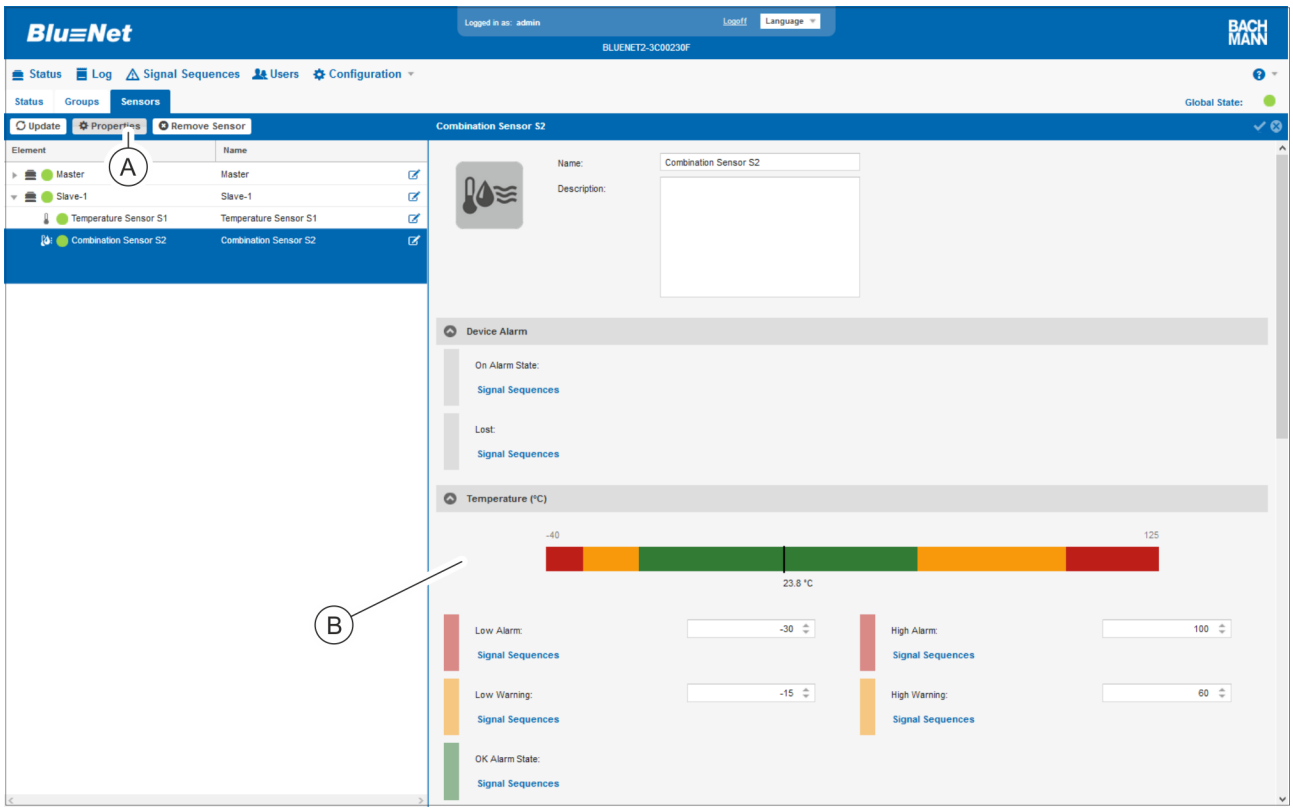


Fig. 113: "Status" menu – "Sensors" tab (sensor in detail view)

Ⓐ *"Properties"* button for opening the detail view
Ⓑ Detail view for defining alarm values and signal sequences

The values for temperature and air humidity of the connected sensors can be viewed and configured on the “Sensors” tab, and alarms, warnings and signal sequences for each sensor can be defined.

On the “Sensors” tab, you can display the measured data for the individual sensors.

6.5.3.2 “GPIO Module” menu view

Overview

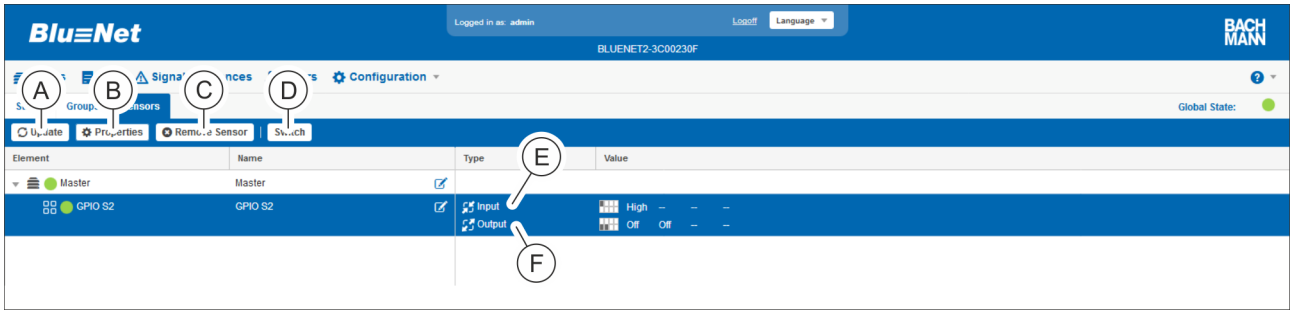


Fig. 114: “Status” menu – “Sensors” tab (GPIO module)

Ⓐ *“Update”* button for updating the display
Ⓑ *“Properties”* button for opening the detail view
Ⓒ *“Remove Sensor”* button for removing the GPIO module
Ⓓ *“Switch”* button for switching outputs
Ⓔ Status display of inputs ( )
Ⓕ Status display of outputs ( )

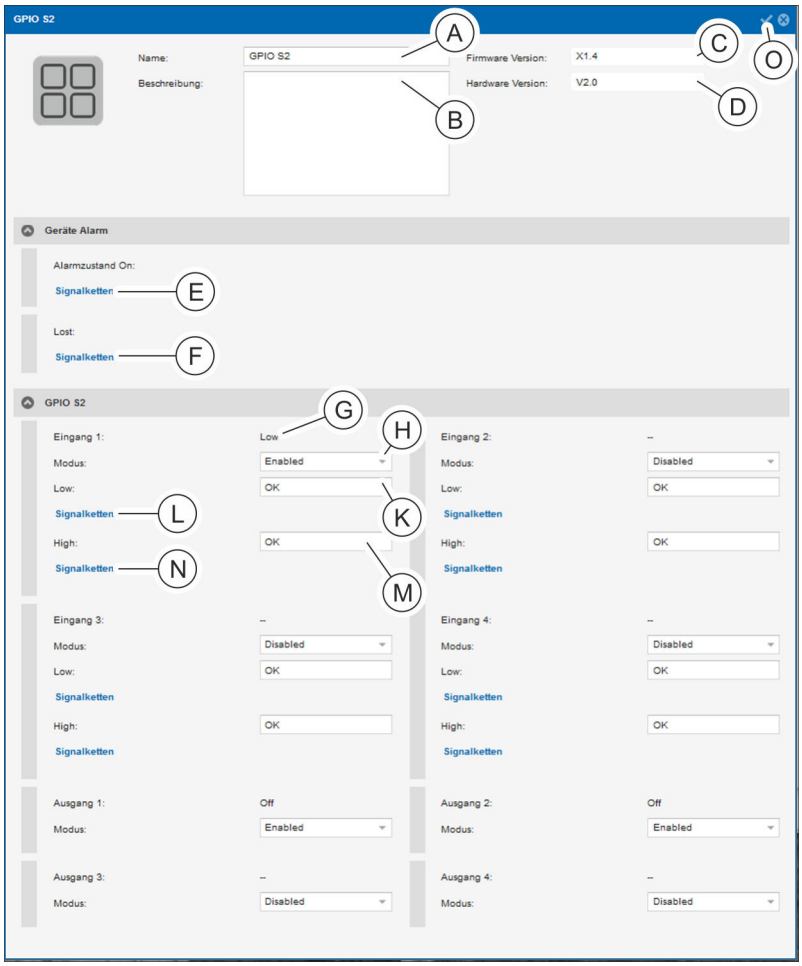


Fig. 115: "Status" menu – "Sensors" tab (GPIO module in detail view)

Ⓐ Text field for entering a name for the GPIO module
Ⓑ Text field for entering a description of the GPIO module
Ⓒ Display field for firmware version
Ⓓ Display field for hardware version
Ⓔ *"Signal Sequences"* button for assigning a signal sequence to the device alarm in the "Alarm state on" status
Ⓕ *"Signal Sequences"* button for assigning a signal sequence to the device alarm in the "Lost" status
Ⓖ *"Status"* selection field (indicates the status of the respective input and output)
Ⓗ *"Mode"* column (selection fields for activating/deactivating inputs and outputs)
Ⓚ *"Low"* column (indicates which low state has a corresponding signal sequence defined)
Ⓛ *"Signal Sequences"* button for assigning a signal sequence to a low state of an input
Ⓜ *"High"* column (indicates which high state has a corresponding signal sequence defined)
Ⓝ *"Signal Sequences"* button for assigning a signal sequence to a high state of an input
Ⓞ *"Save"* button for saving the settings

The status of a connected GPIO module can be viewed on the “Sensors” tab, where inputs and outputs can also be configured, and alarms, warnings and signal sequences for the GPIO module can be defined.

Status display for inputs and outputs

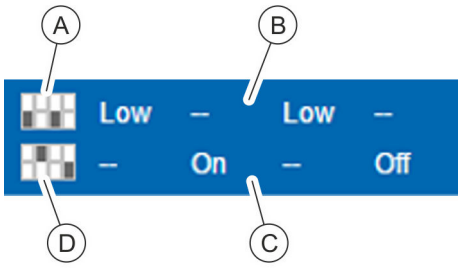


Fig. 116: Status display for inputs and outputs

Ⓐ Graph status display of inputs
Ⓑ Text status display of inputs (Signal Low/Signal High)
Ⓒ Test status display of outputs (On/Off)
Ⓓ Graph status display of outputs

The signal status at inputs 1 – 4 and the switching state of outputs 1 – 4 is displayed via the status display.

Configuring the GPIO module for the PDU

Personnel: ■ IT specialist

1. Call up the “Status” menu.
2. Call up the “Sensors” tab.
3. Select the GPIO module (Fig. 114/Ⓔ).
4. Click the *“Properties”* button (Fig. 114/Ⓑ) to call up the detail view.

Activating/deactivating an input or output

Fig. 117: Activating/deactivating an input or output

1. In the detail view (Fig. 114/Ⓒ), select the relevant input or output.
2. In the selection field (Fig. 117/Ⓐ), set the value to *“Enabled”* (to activate) or *“Disabled”* (to deactivate).
3. Adopt the settings by pressing the *“Save”* button (Fig. 115/Ⓓ).

   ⇨ The input or output is activated/deactivated.

Switching outputs

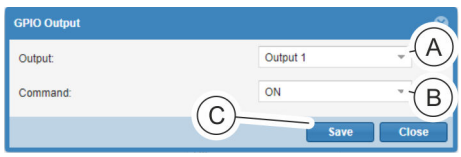


Fig. 118: “GPIO Output” window

1. Click the *“Switch”* button (Fig. 114/Ⓐ).

   ⇨ The *“GPIO Output”* window opens (Fig. 118).
2. In the *“Output”* option menu (Fig. 118/Ⓐ), select the desired output.
3. In the *“Command”* option menu (Fig. 118/Ⓑ), select the setting “ON” or “OFF”.

4. Adopt the settings by pressing the *"Save"* button (Fig. 118/Ⓟ).
   ⇨ The output is switched on or off, according to the setting.

Assigning signal sequences

How to configure signal sequences is described in ↳ Chapter 6.7.5 "Setting up signal sequences for a GPIO module" on page 84.

6.6 "Log" menu

6.6.1 "Event Log" tab

6.6.1.1 Overview of the tab

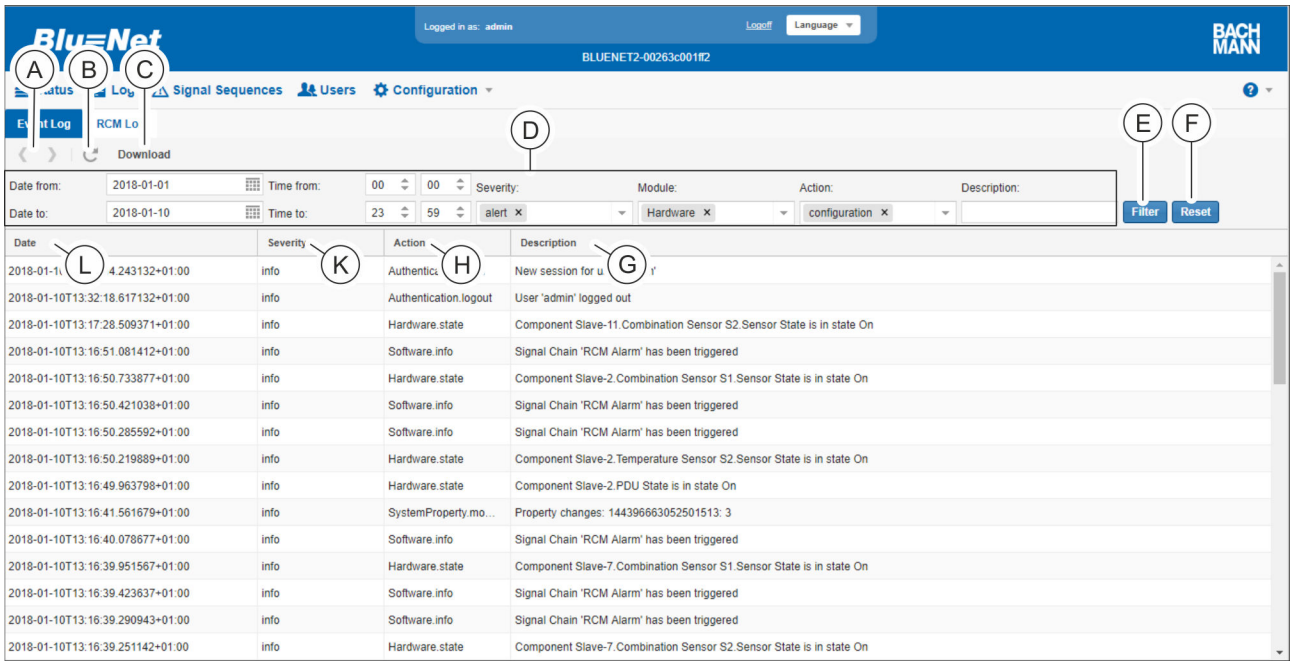


Fig. 119: "Log" menu – "Event Log" tab

Ⓐ Buttons for displaying the process
Ⓑ Button for updating the display
Ⓒ *"Download"* button for saving the event log locally
Ⓓ Filter options for the event
Ⓔ *"Filter"* button for filtering the display
Ⓕ *"Reset"* button for resetting the filter
Ⓖ Description of the action
Ⓗ Action performed by the PDU, and the corresponding module
Ⓚ Severity of the event
Ⓛ Date and time of the event

In the "Log" menu – "Event Log" tab, the event log of the PDU can be displayed. Here, individual events are displayed with the date and time, severity, action and a description. The severity levels are "Info", "Warning" and "Alarm". The event log can be filtered.

6.6.1.2 Filtering the event log

Personnel: ■ IT specialist

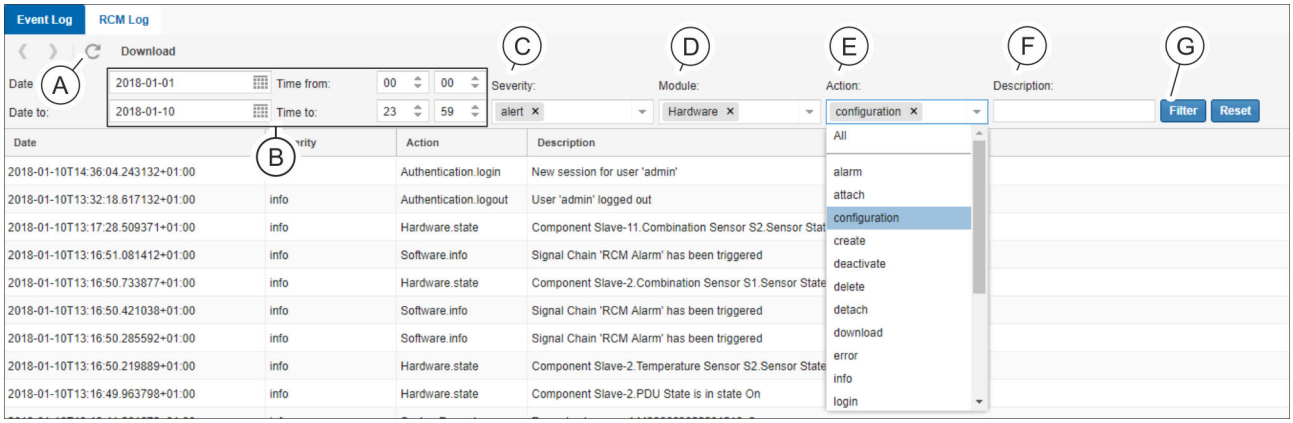


Fig. 120: Set filter

1. In the *“Filter”* area, select one or more filters by which the events are to be filtered.

> *Filtering can be carried out according to the following criteria:*
>
> – *Date and time (Fig. 120/Ⓑ)*
> – *Severity (Fig. 120/Ⓒ)*
> – *Module (Fig. 120/Ⓓ)*
> – *Action (Fig. 120/Ⓔ)*
> – *Description (Fig. 120/Ⓕ) (free text field)*

2. Click the *“Filter”* button (Fig. 120/Ⓖ).

⇨ The selected filters are applied to the event log.

6.6.1.3 Removing filters on the event log

Personnel: ■ IT specialist

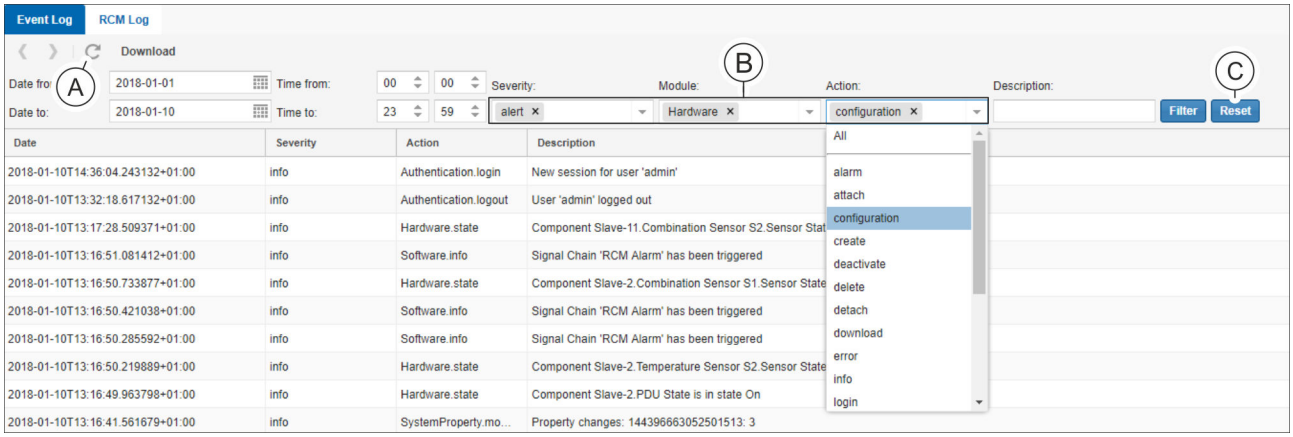


Fig. 121: Removing a filter

1. Press the × button in the corresponding filter (Fig. 121/Ⓑ) to remove the filter. Alternatively, remove all filters by clicking the *"Reset Filter"* button (Fig. 121/©).
2. Click the ↻ button (Fig. 121/Ⓐ).
   ⇨ The view of the event log is updated.

6.6.2 "RCM Log" tab (only for PDUs with RCM)

6.6.2.1 Overview of the tab

The log of the RCM self-test that was carried out can be displayed on the "RCM Log" tab (Fig. 122). For this test, it is expected that both an AC and a DC alarm are triggered. A red/green icon is displayed in the "Alarm AC" or "Alarm DC" column to indicate whether an alarm is triggered.

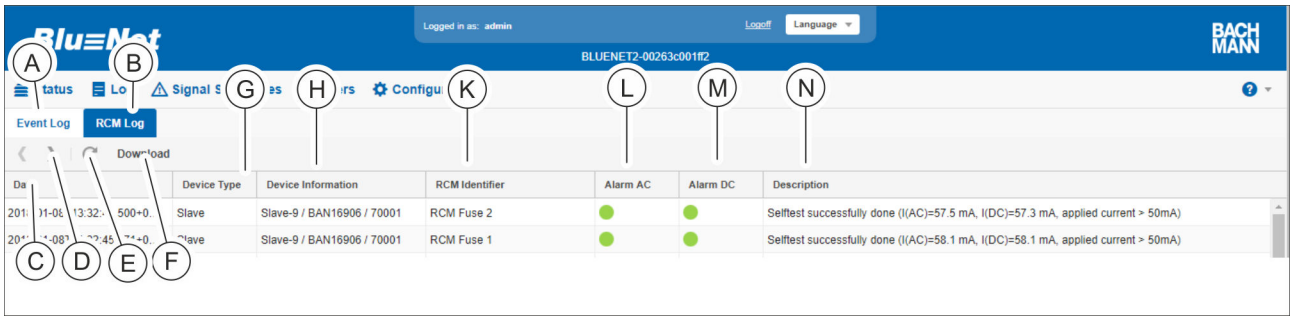


Fig. 122: "Log" menu – "RCM Log" tab

Ⓐ "Event Log" tab for calling up the event log
Ⓑ "RCM Log" tab
Ⓒ Display of the date of the event
Ⓓ Buttons for displaying the process
Ⓔ Button for updating the display
Ⓕ *"Download"* button for saving the RCM log locally
Ⓖ Display of the PDU device type (master/slave)
Ⓗ Display of the "Device Information" consisting of position in the tree (e.g. "Slave-7"), type (e.g. "802.3031-S") and serial number (e.g. "45")
Ⓚ Display of the name of the RCM
Ⓛ "Alarm AC" column to indicate whether an alarm occurred during the RCM self-test
Ⓜ "Alarm DC" column to indicate whether an alarm occurred during the RCM self-test
Ⓝ Description of the action

RCM self-tests at a slave PDU are only displayed in the RCM log if they were triggered via the web interface.

6.6.2.2 Displaying the RCM log (only for PDUs with RCM)

Personnel: ■ IT specialist

1. Call up the "Log" menu.
2. Call up the "RCM Log" tab.
   ⇨ The RCM log is displayed.

6.7 "Signal Sequences" menu

6.7.1 Overview of the menu

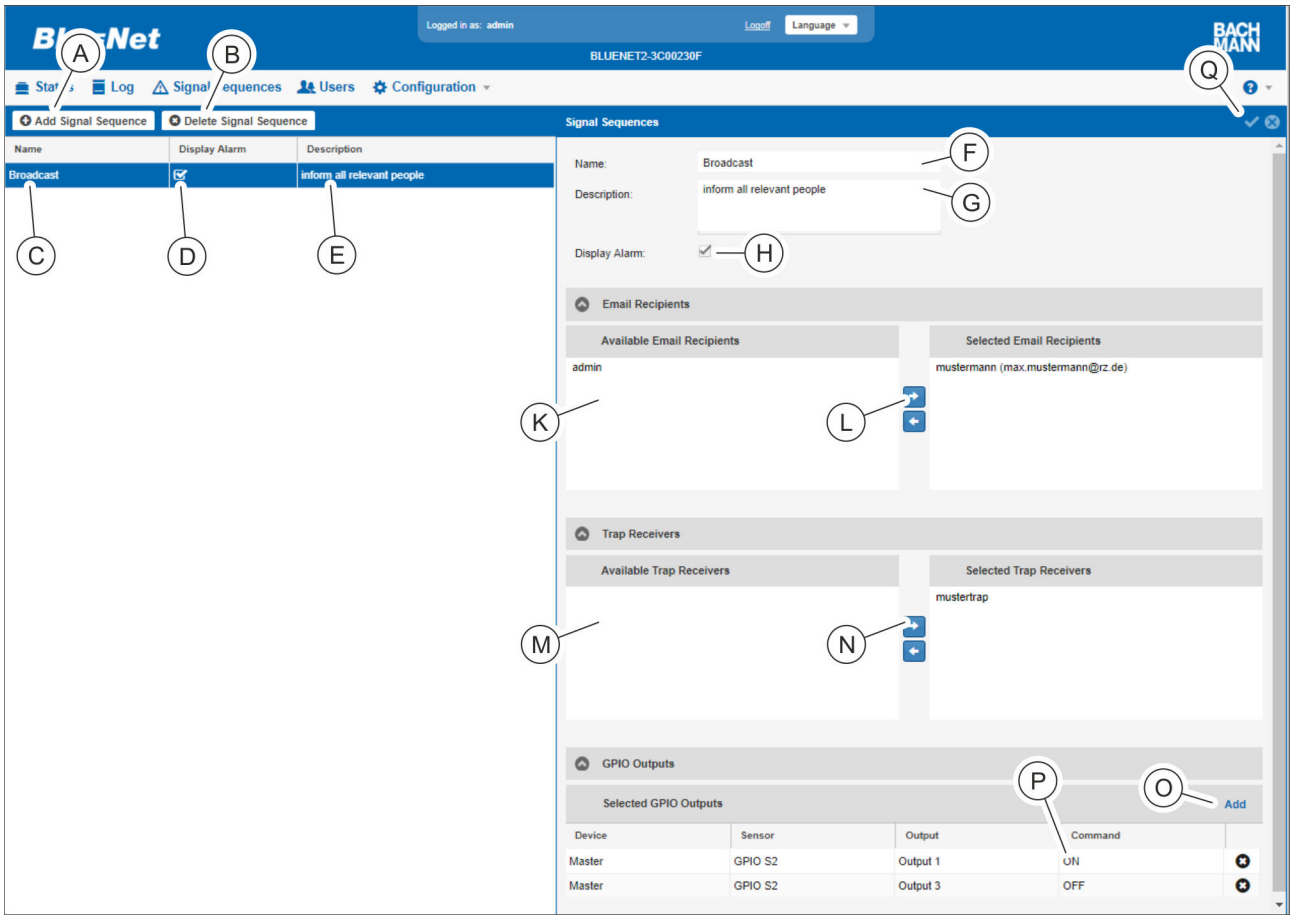


Fig. 123: "Signal Sequences" menu

Ⓐ *"Add Signal Sequence"* button for creating a signal sequence
Ⓑ *"Delete Signal Sequence"* button for deleting a signal sequence
Ⓒ *"Name"* column with designation of the signal sequence
Ⓓ *"Display Alarm"* column showing whether the display alarm is activated for the signal sequence in question
Ⓔ *"Description"* column with description of the signal sequence
Ⓕ *"Name"* text field for entering a name for the signal sequence
Ⓖ *"Description"* text field for entering a description of the signal sequence
Ⓗ *"Display Alarm"* checkbox for activating the display alarm
Ⓚ *"Available Email Recipients"* selection field for defining the email recipient of a signal sequence
Ⓛ Button for moving email recipients
Ⓜ *"Trap Receiver"* selection field for defining the trap receiver of a signal sequence
Ⓝ Button for moving trap receivers
Ⓞ *"Add"* button to add an output of a GPIO module to a signal sequence
Ⓟ List of outputs that are assigned to a signal sequence
Ⓠ *"Save"* button for saving the settings

In the “Signal Sequences” menu, signal sequences for individual events can be defined. Events are defined error states that occur when a defined measured value exceeds or falls short of the threshold value or when a connected device triggers a signal (e.g. “OK” signal or “Lost” signal).

Signal sequences indicate the error states to defined trap receivers or mail recipients (*Chapter 6.9.4 “Configuring the trap receiver” on page 95*). In addition, the error states are displayed on the display if the display alarm is active.

If a GPIO output has been assigned to a signal sequence, this output is switched if an event occurs.

When creating a signal sequence, a name, a description and a display alarm (only on a master PDU and PU2) can be defined for an error case. If the display alarm is active, the first thing that appears when the display of a master PDU is switched on is the latest error message at the PDU or PU2.

6.7.2 Configuring signal sequences

Requirements

To configure a signal sequence, a user (Chapter 6.8.2 “Managing a local user” on page 88) and a SNMP trap receiver (Chapter 6.9.4 “Configuring the trap receiver” on page 95) should be created in advance.

If an alert is to be issued via email recipients, a mail server must be set up (Chapter 6.9 ““Configuration” menu” on page 91, section on SMTP settings).

In the most basic setup for creating a signal sequence, only the entry of a name and the activation of the display alarm are necessary.

Adding/modifying a signal sequence

Personnel: ■ IT specialist

1. Call up the “Signal Sequences” menu
2. Create a new signal sequence by clicking the *“Add Signal Sequence”* button (Fig. 123/Ⓐ).

Modifying an existing signal sequence
To modify an existing signal sequence, select the relevant signal sequence in the list (Fig. 123/Ⓒ).

3. In the *“Signal Sequence”* area, enter a name for the signal sequence (Fig. 123/Ⓒ).

4. If necessary, enter a description for the signal sequence (Fig. 123/Ⓖ).
5. If necessary, activate the *"Display Alarm"* checkbox to have an alarm message displayed on the PDU display (Fig. 123/Ⓗ).
6. If necessary, select a recipient for email notification in the *"Available Email Recipients"* (Fig. 123/Ⓚ) field and use the → button to move it into the *"Selected Email Recipients"* field (Fig. 123/Ⓕ).

> *Local users and users from the directory service are listed as possible email recipients.*

7. If necessary, select a trap receiver in the *"Available Trap Receivers"* (Fig. 123/Ⓜ) field and use the → button to move it into the *"Selected Trap Receivers"* field (Fig. 123/Ⓕ).

Adding GPIO outputs (optional)

8. If you want to link the signal sequence to an output on a GPIO module, press the *"Add"* button (Fig. 123/Ⓖ).

   ⇨ The *"Available GPIO Sensor Outputs"* window opens.

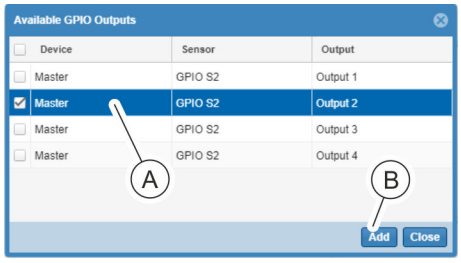


Fig. 124: "Available GPIO Outputs" window

9. Select the desired output on the GPIO module (Fig. 124/Ⓐ) and adopt the selection by pressing the *"Save"* button (Fig. 124/Ⓑ).
10. If necessary, select the corresponding output in the list and, in the *"ON"*/*"OFF"* option menu (Fig. 123/Ⓗ), define whether the relay is switched on or off when the signal sequence is triggered.
11. Confirm the selection by clicking the *"Save"* button (Fig. 123/Ⓗ).

    ⇨ The signal sequence has been created (Fig. 123/Ⓑ).

Delete Signal Sequence

> *To delete a signal sequence, select the desired signal sequence (Fig. 123/Ⓒ) and click the "Delete Signal Sequence" button (Fig. 123/Ⓑ). A security prompt appears and has to be confirmed.*

6.7.3 Setting up signal sequences and threshold values for individual elements

Overview

Signal sequences can be set up for individual elements (master PDU, slave PDU, inlets, phases, differential current analyser (RCM), fuses, sockets, socket groups, external sensors and a GPIO module). For slave PDUs, sensors and fuses, it is also possible to set up a device alarm with a signal sequence.

The setup procedure for the individual elements is essentially the same. The following explanation uses a phase as an example.

Setting up signal sequences and threshold values

Personnel: ■ IT specialist

1. Call up the “Status” menu.
2. Select the relevant element on the tab (in this case, a phase).
3. Click the *“Properties”* button to call up the properties for the element in question.

   ⇨ The properties are shown on the right in the detail view.

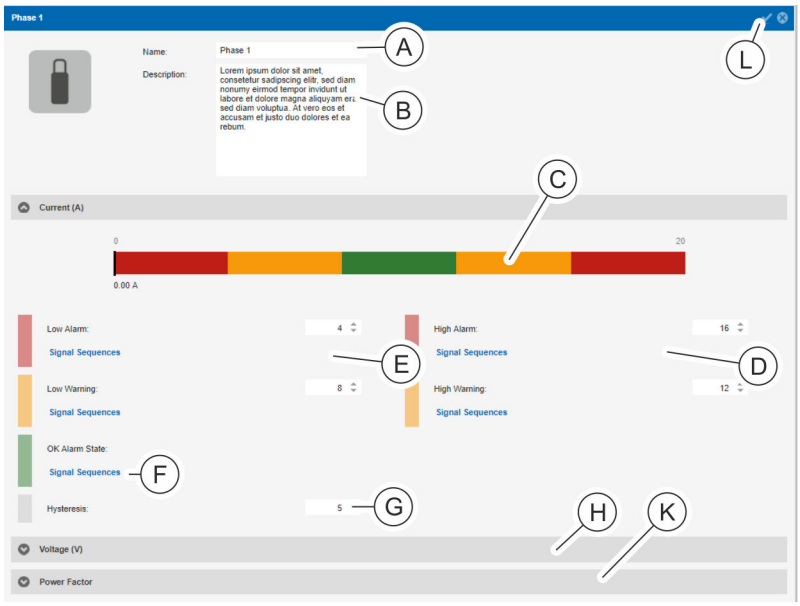


Fig. 125: Detail view

4. If necessary, adjust the name of the phase (Fig. 125/Ⓐ) in the detail view and, if necessary, add a description (Fig. 125/Ⓑ).

5. In the *"Current (A)"* area, enter a value for *"High Warning"* and *"High Alarm"* (Fig. 125/Ⓐ).

⇨ The threshold values are displayed in colour (Fig. 125/Ⓒ).

6. Assign a signal sequence to the threshold values. To do so, click the *"Signal Sequences"* button.

⇨ The "Configure alarm" window opens.

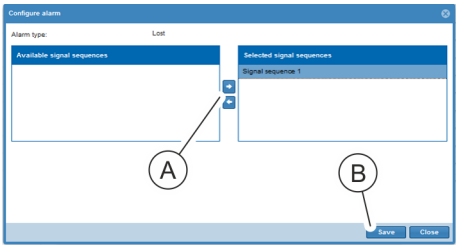


Fig. 126: "Configure alarm" window

7. Select a signal sequence in the "Configure alarm" window and use the *"→"* button (Fig. 126/Ⓐ) to move it into the *"Selected signal sequences"* field. Confirm the selection by clicking the *"Save"* (Fig. 126/Ⓑ) button.

8. In the *"Current (A)"* area, allocate a signal sequence to the *"OK Alarm State"* parameter (Fig. 125/Ⓑ) if necessary (analogous to steps 5 and 6).

9. In the *"Current (A)"* area, enter a value for *"Low Alarm"*, *"Low Warning"* and *"Hysteresis"* (Fig. 125/Ⓔ and Ⓖ) and allocate a signal sequence (analogous to steps 5 to 7).

10. Repeat steps 5 to 9 for the *"Voltage"* range to set the voltage range (Fig. 125/Ⓓ).

11. Repeat steps 8 to 9 for the *"Power Factor"* range to set the power factor (Fig. 125/Ⓔ).

12. Confirm the selection by clicking the *"Save"* (Fig. 125/Ⓑ) button.

⇨ The signal sequences and the threshold values are accepted for the PDU.

6.7.4 Setting up signal sequences and threshold values for a differential current analyser

For detailed information about RCM threshold values, see Chapter 4.2 "Residual current monitoring (RCM)" on page 21.

Personnel: ■ IT specialist

1. Call up the "Status" menu.

2. Select the relevant element on the tab.

3. Click the *"Properties"* button to call up the properties for the differential current analyser (RCM) in question.

⇨ The properties are shown on the right in the detail view.

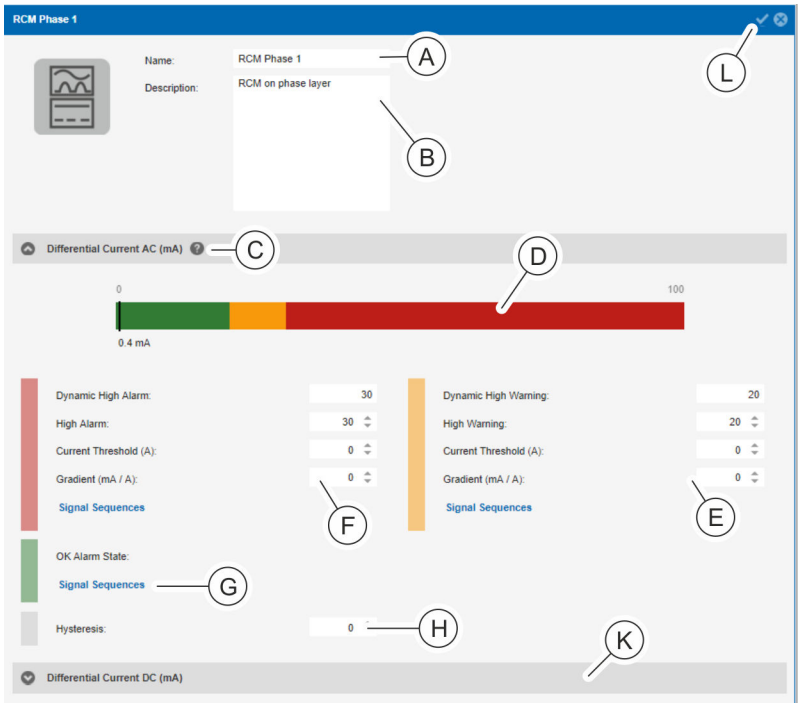


Fig. 127: Detail view

4. If necessary, adjust the name for the differential current analyser (Fig. 127/Ⓐ) in the detail view and, if necessary, add a description (Fig. 127/Ⓑ).

5. In the *“Differential Current AC (mA)”* area, enter a value for *“High Alarm”*, *“Current Threshold (A)”* and *“Gradient (mA / A)”* (Fig. 127/Ⓕ).

6. Assign a signal sequence to the threshold values. To do so, click the *“Signal Sequences”* button.

⇨ The “Configure alarm” window opens.

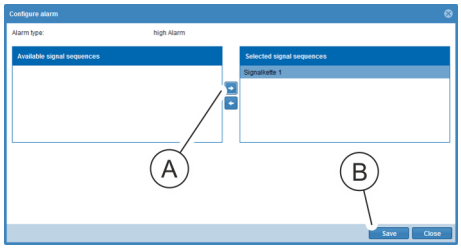


Fig. 128: “Configure alarm” window

7. Select a signal sequence in the “Configure alarm” window and use the *“→”* button (Fig. 128/Ⓐ) to move it into the *“Selected signal sequences”* field. Confirm the selection by clicking the *“Save”* (Fig. 128/Ⓑ) button.

8. In the *“Differential Current AC (mA)”* area, enter a value for *“High Warning”*, *“Current Threshold (A)”* and *“Gradient (mA / A)”* (Fig. 127/Ⓔ) and assign a signal sequence (analogous to steps 5 and 6).

9. In the *“Differential Current AC (mA)”* area, allocate a signal sequence to the *“OK Alarm State”* parameter (Fig. 127/Ⓔ) if necessary (analogous to steps 5 to 7).

10. In the *“Differential Current AC (mA)”* area, enter a value for *“Hysteresis”* (Fig. 127/Ⓓ).

11. Repeat steps 5 to 10 for the *"Differential Current DC (mA)"* range (Fig. 127/Ⓢ).

A "current threshold" and "gradient" cannot be set for "Differential Current DC (mA)". The threshold values for DC monitoring are displayed in colour (Fig. 127/Ⓒ).

12. Confirm the selection by clicking the *"Save"* (Fig. 127/Ⓑ) button.

⇨ The signal sequences and the threshold values are accepted for the PDU.

For the values "High Warning" or "High Alarm", "Current Threshold (A)" and "Gradient (mA / A)", you can enter one decimal digit. Use a full stop as the separator for the decimal digit.

The "Dynamic High Warning" or "Dynamic High Alarm" is calculated automatically. Click the question mark (Fig. 127/Ⓒ) to open a diagram explaining the dynamic RCM threshold value (Fig. 18).

6.7.5 Setting up signal sequences for a GPIO module

1. Ensure that the GPIO module is connected to the PDU.
2. Call up the “Status” menu.
3. Call up the “Sensors” tab.

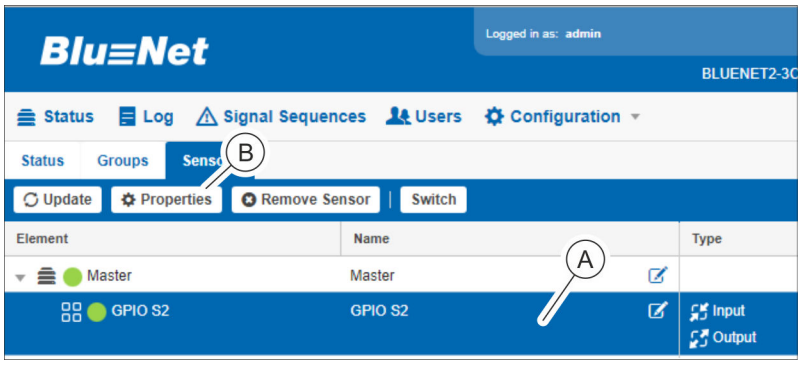


Fig. 129: “Status” menu – “Sensors” tab

4. Select the desired GPIO module in the “Sensors” tab (Fig. 129/Ⓐ).
5. Click the *“Properties”* button to call up the detail view (Fig. 129/Ⓑ).

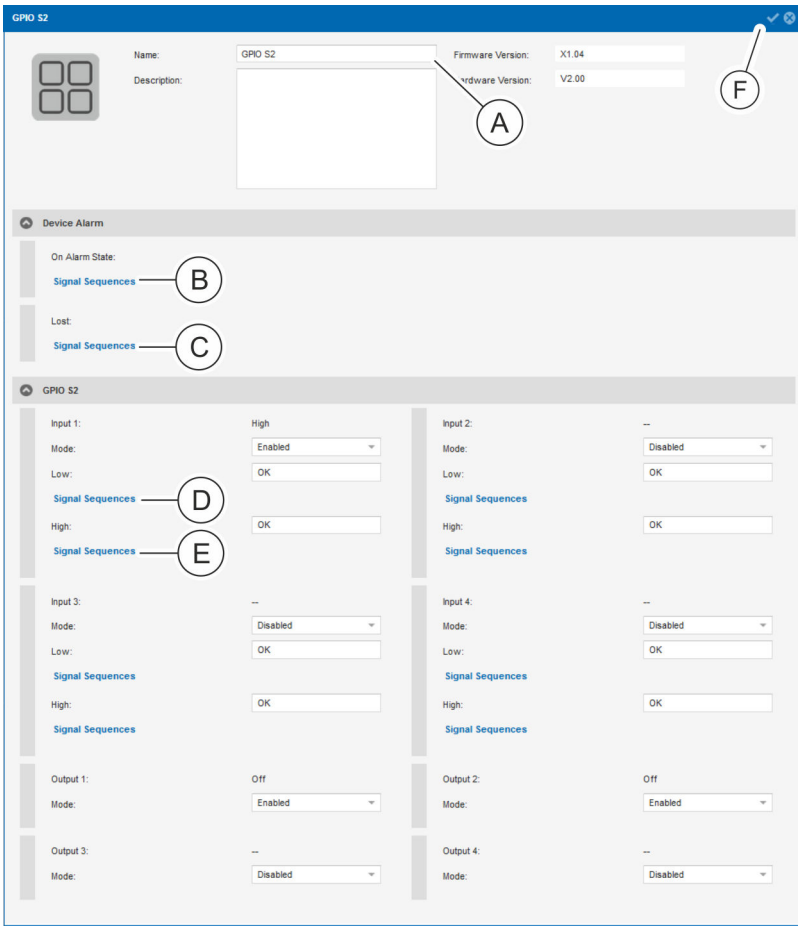


Fig. 130: "Status" menu – "Sensors" tab (detail view)

6. If necessary, change the name of the selected GPIO module and, if necessary, add a description (Fig. 130/Ⓑ).
7. If necessary, assign a signal sequence for the corresponding low signal by clicking the *"Signal Sequences"* button (Fig. 130/Ⓕ).
8. Select a signal sequence in the "Configure alarm" window and use the *"→"* button (Fig. 131/Ⓐ) to move it into the *"Selected signal sequences"* field.
9. In the *"Severity"* selection field (Fig. 131/Ⓑ), select the alarm state *"OK"*, *"Warning"* or *"Alarm"* for the input.
10. Confirm the selection by clicking the *"Save"* (Fig. 131/Ⓒ) button.

    ⇨ A signal sequence is assigned for the respective low signal state.
11. If necessary, assign a signal sequence for the corresponding high signal by clicking the *"Signal Sequences"* button (Fig. 130/Ⓕ) (analogous to steps 8 to 10).

Assigning signal sequences to input signals

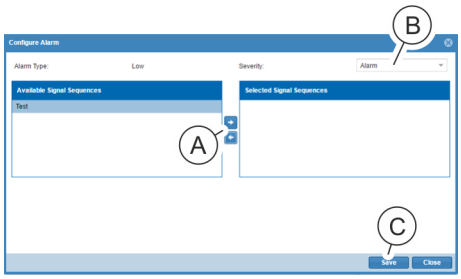


Fig. 131: "Configure alarm" window

Assigning a signal sequence for “Device Alarm”

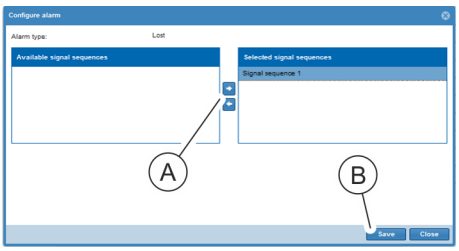


Fig. 132: “Configure alarm” window

12. If necessary, configure a signal sequence in the *“Device Alarm”* area for *“Lost Alarm State”* and *“OK Alarm State”*. To do so, click the *“Signal Sequences”* button (Fig. 130/© or Ⓓ).

⇨ The “Configure alarm” window opens.

13. Select a signal sequence in the “Configure alarm” window and use the *“→”* button (Fig. 132/Ⓐ) to move it into the *“Selected signal sequences”* field. Confirm the selection by clicking the *“Save”* (Fig. 132/Ⓑ) button.

14. Adopt the configuration by clicking the *Save* button (Fig. 130/Ⓟ).

6.8 "Users" menu

6.8.1 Overview

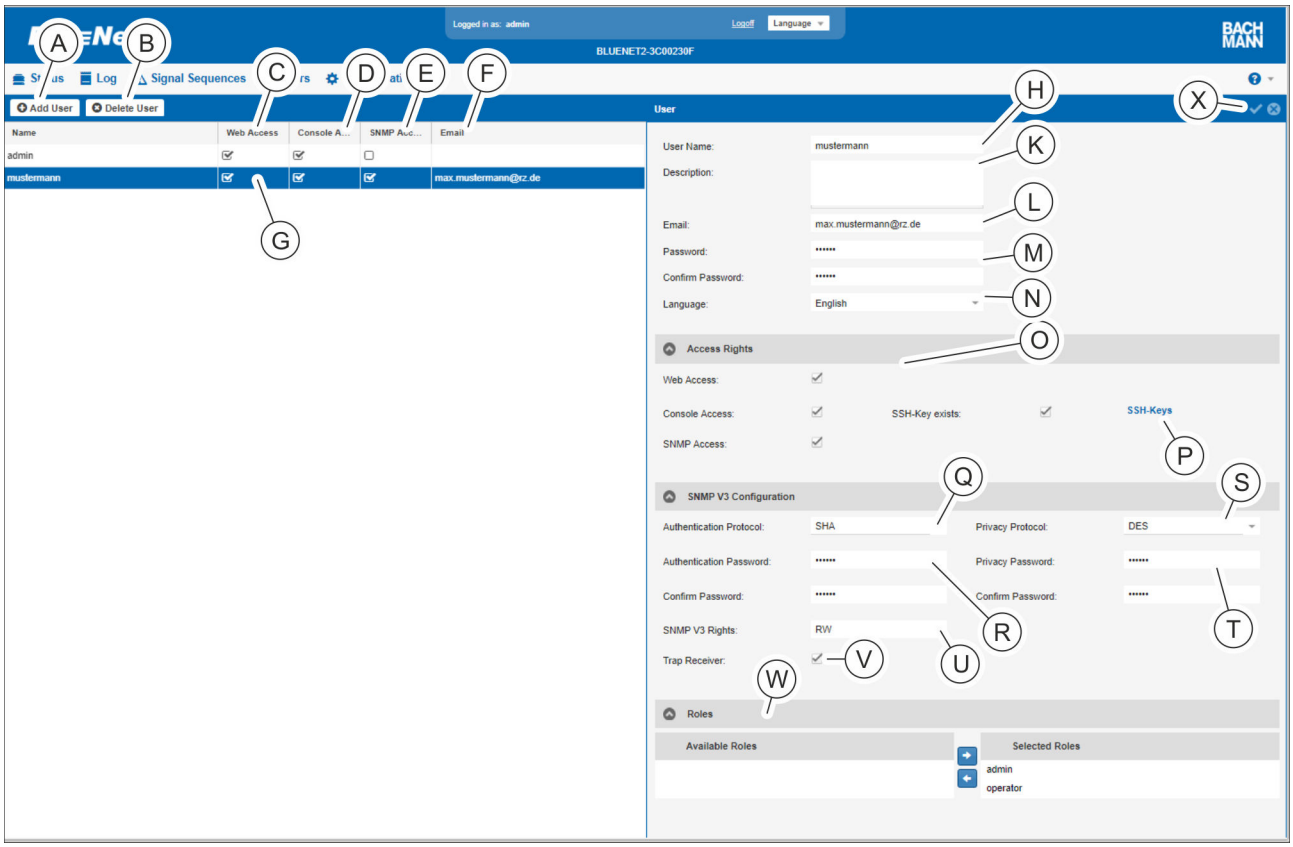


Fig. 133: "Users" menu

Ⓐ *"Add User"* button for creating a user
Ⓑ *"Delete User"* button for deleting a user
Ⓒ *"Web Access"* column for access via the web interface
Ⓓ *"Console Access"* column for access via the console
Ⓔ *"SNMP Access"* column for access via SNMP
Ⓕ *"Email"* column for displaying the defined email address
Ⓖ List of the defined users with user names, access rights and email address
Ⓗ *"User Name"* input field for entering a user name
Ⓚ *"Description"* input field for entering a description
Ⓛ *"Email"* input field for entering an email address
Ⓜ *"Password"* and *"Confirm Password"* input fields for entering a password
Ⓝ *"Language"* input field for selecting a language
Ⓞ *"Access Rights"* area for selecting access rights for *"Web Access"*, *"Console Access"*, *"SNMP Access"* and *"SSH-Key exists"*
Ⓟ *"SSH-Keys"* button for storing SSH keys
Ⓠ *"Authentication Protocol"* selection field for selecting an authentication protocol
Ⓡ *"Authentication Password"* and *"Confirm Password"* input fields for entering a password
Ⓢ *"Privacy Protocol"* selection field for selecting an authentication protocol
Ⓣ *"Privacy Password"* and *"Confirm Password"* input fields for entering a password
Ⓤ *"SNMP V3 Rights"* for assigning SNMP V3 rights
Ⓥ *"Trap Receiver"* checkbox for activating the user as a trap receiver
Ⓦ *"Available Roles"* and *"Selected Roles"* selection fields for assigning a user role
Ⓧ *"Save"* button for saving the user settings

In the “Users” menu, the users and access rights for individual users with user roles for the connected PDU can be defined. The available access rights are “Web Access” (using the web interface), “Console Access” (using the SSH console) and “SNMP Access” (using the SNMP-V3 protocol). SSH keys can be stored for key-based SSH login operations. For users, the available user roles are “operator” (with read rights in the web interface) and “admin” (with read and write rights).

In this menu, users with access rights or users with an email address only can be set up for the configuration of signal sequences (↳ *Chapter 6.8.2 “Managing a local user” on page 88*).

User names must always be written in lower case.

The “admin” user cannot be deleted.

If the PDU is reset to the factory settings, the PDU can be accessed using the “admin” user and the password “admin”.

6.8.2 Managing a local user

Creating/modifying a user

Personnel: ■ IT specialist

1. Call up the “Users” menu.
2. Create a new user by clicking the *“Add User”* button (Fig. 133/Ⓐ).

Modifying existing users
To modify an existing user, select the user in question from the list (Fig. 133/ⓖ).

⇨ The settings for the user appear on the right in the detail view.

Entering user data

3. Enter a user name (Fig. 133/Ⓑ).

The user name may only contain lower-case letters, numbers and certain special characters.

4. If necessary, enter a description for the user (Fig. 133/©).

5. Enter an email address (Fig. 133/©).

The email address may only contain letters, numbers and certain special characters.

You have to enter the email address so that the user can be assigned to a signal sequence.

6. Enter and confirm a password for accessing the PDU (Fig. 133/Ⓔ).

The password must be at least eight characters in length.

7. Select the language (Fig. 133/Ⓔ).

The languages "German", "English", "French" and "Spanish" are available.

Assigning access rights

8. Use the checkboxes to assign access rights for *"Web Access"*, *"Console Access"* and/or *"SNMP Access"* (Fig. 133/Ⓖ).

"Web Access" means access to the PDU using the web interface, "Console Access" using a console programme and "SNMP Access" using the SNMPv3 protocol.

If SNMPv3 access is not configured, the "SNMP V3 Configuration" area is greyed out.

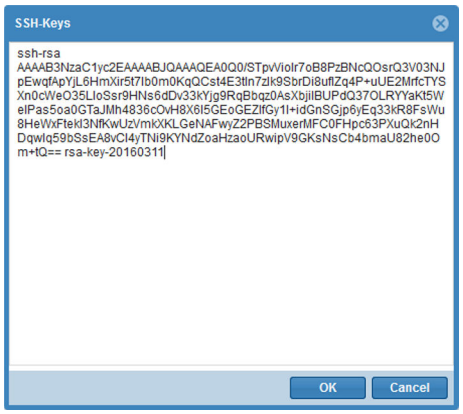


Fig. 134: Inserting an SSH key

9. The *“SSH-Keys”* button can be used to store SSH keys for key-based SSH login operations (Fig. 133/Ⓗ). Copy one or more SSH keys to the *“SSH-Keys”* window (Fig. 134) and press the *“OK”* button for confirmation.

> *A key pair must be created for key-based SSH login. The public key is stored at the PDU.*

SNMP-V3 configuration

10. In the *“SNMP V3 Configuration”* area, select an authentication protocol, if necessary (Fig. 133/Ⓒ).

> *The options “NONE”, “SHA” and “MD5” are available for selection. If “SHA” or “MD5” is selected, an authentication password can be set.*

11. Enter and confirm authentication password (Fig. 133/Ⓓ).

12. If necessary, select a privacy protocol (Fig. 133/Ⓚ).

> *The options “NONE”, “DES” and “AES” are available for selection.*
>
> *If “DES” and “AES” are selected, you can assign a privacy password.*

13. Enter and confirm a privacy password (Fig. 133/Ⓛ).

14. Assign SNMP-V3 rights (Fig. 133/Ⓞ).

> *The options “NONE”, “RO” (read rights only) and “RW” (read and write rights) are available.*

15. Select the *“Trap Receiver”* checkbox if the user is to be available as a trap receiver (Fig. 133/Ⓝ).

Assigning user roles

16. Select a user role in the *"Available Roles"* field and use the *"→"* button to move it into the *"Selected Roles"* field (Fig. 133/◎).

> *The "admin" and "operator" user roles are available. The "admin" has read and write rights in all areas of the web interface; the "operator" has read rights only. Console operations can be carried out completely by the "admin", and only to a limited extent by the "operator".*

Saving a user

17. Accept the settings using the *"Save"* (Fig. 133/Ⓟ) button.

⇨ A new user has been created or modified.

> *If the user cannot be saved, check the spelling of the user name and the email address, and/or enter the password again.*

Deleting a user

> *To delete an existing user, select the desired user (Fig. 133/ⓒ) and click the "Delete User" button (Fig. 133/Ⓑ). A security prompt appears and has to be confirmed.*

6.9 "Configuration" menu

6.9.1 Overview of the menu items

Menu item	Description
"LDAP Settings"	The "LDAP Settings" window can be opened by choosing the *"Configuration ➔ LDAP Settings"* menu. The PDU connection to a directory service can be configured here. The user accounts of the directory service can thus be used to login to the PDU. The prerequisite for this is that the user accounts are members of specified user groups, which need to be created in the directory service.
"Console Settings"	The "Console Settings" window can be opened by choosing the *"Configuration ➔ Console Settings"* menu. Access via SSH can be configured here.
"Modbus RTU Settings"	The "Modbus RTU Settings" window can be opened by choosing the *"Configuration ➔ Modbus RTU Settings"* menu. "Modbus RTU" is used for the data connection between master and slave PDUs.

Menu item	Description
"Modbus TCP Settings"	The "Modbus TCP Settings" window can be opened by choosing the *"Configuration ➔ Modbus TCP Settings"* menu. You can call up the PDU status and measuring information over the network using "Modbus TCP".
"Webserver Settings"	The "Webserver Settings" window can be opened by choosing the *"Configuration ➔ Webserver Settings"* menu. Web access to the PDU can be configured here. If access with HTTP and HTTPS is deactivated, it is no longer possible to manage the PDU using the web browser. Access with HTTP and HTTPS must be reactivated using the SSH console (↳ *Chapter 7 "Operation using the SSH console" on page 103*).
"Network Settings"	The "Network Configuration" window can be opened by choosing the *"Configuration ➔ Network Settings"* menu. Here, the network can be configured for IPv4 and IPv6 (↳ *Chapter 6.9.2 "Configuring network configuration" on page 93*).
"SMTP Settings"	The "SMTP Settings" window can be opened by choosing the *"Configuration ➔ SMTP Settings"* menu. In this window, the connection to a mail server can be configured. A mail server is required if you wish alerts to be sent out by email (↳ *Chapter 6.7.2 "Configuring signal sequences" on page 78*).
"NTP Settings"	The "NTP Settings" window can be opened by choosing the *"Configuration ➔ NTP Settings"* menu. In this menu, the date and time for the PDU can be manually set. Alternatively, one or more time servers for querying the time can be set.
"SNMP Settings"	The "SNMP Settings" window can be opened by choosing the *"Configuration ➔ SNMP Settings"* menu. Here, the SNMP settings for SNMP V1/2 can be configured, and the SNMP V3 protocol can be activated (↳ *Chapter 6.9.3 "Configuring SNMP settings" on page 95*). The "Trap Receiver List" window can be called up by clicking the *"Trap Receiver"* button. Trap receivers are servers in the network that receive and process alarm messages. In this window, trap receivers can be activated or deactivated. See ↳ *Chapter 6.9.4 "Configuring the trap receiver" on page 95* for information on setting the trap receiver.
"Syslog Settings"	The "Syslog Settings" window can be opened by choosing the *"Configuration ➔ Syslog Settings"* menu. Here, the syslog settings for the PDU can be configured. Syslog is an event log that is generated locally and is forwarded via the network to an external server for logging. In this menu, two servers can be configured with their respective ports and a facility can be selected.

Menu item	Description
"System Information"	The "System Information" menu can be displayed by choosing the *"Configuration ➔ System Information"* menu. Here, information about the PDU and current settings can be viewed. Information about the connected slave PDUs is shown in the PDU properties in the "Status" menu.
"System Commands"	The "System Commands" window can be opened by choosing the *"Configuration ➔ System Commands"* menu. In the "System Commands" window, you can: ■ Restart the PDU ■ Reset the PDU to the factory settings ■ Update the PDU software ■ Import a configuration ■ Create, restore or delete a backup ■ Collect and download diagnostic information The "collect and download diagnostic information" function is used to collect system information on the PDU and make it available as a downloadable file. After it is automatically downloaded to a local PC, the file on the PDU is deleted. Only create the diagnostic information when requested to do so by Bachmann Support, then download it and send it to Bachmann Support.

6.9.2 Configuring network configuration

The following describes an example configuration for the network settings. The other menus are configured in the same way.

Personnel: ■ IT specialist

1. Call up the network configuration by choosing *"Configuration ➔ Network Configuration"*.

⇨ The "Network Configuration" window opens.

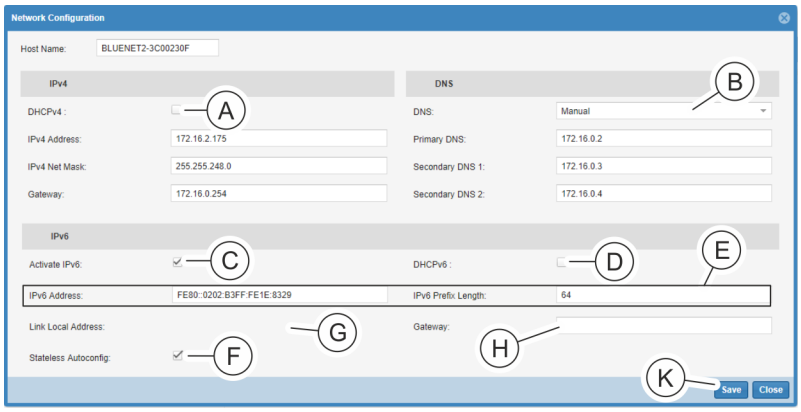


Fig. 135: “Network Configuration” window

2. In the “Network Configuration” window, select the *“DHCPv4”* checkbox in the *“IPv4”* area (Fig. 135/Ⓐ).

Alternatively, do not select the *“DHCPv4”* checkbox and enter the IP address, IPv4 net mask and gateway manually.

3.

The parameters “Prioritise DHCPv4” or “Prioritise DHCPv6” parameters can only be selected if “DHCP” or also “IPv6” are activated for each.

In the *“DNS”* (Fig. 135/Ⓑ) area, select the “Prioritise DHCPv4" or “Prioritise DHCPv6” parameter.

Alternatively, select the “Manual” parameter and manually enter the primary DNS address and the secondary DNS addresses 1 and 2.

4. If required, click the *“Activate IPv6”* checkbox in the *“IPv6”* area (Fig. 135/Ⓒ). If *“IPv6”* is selected, *“Link Local Address”* (Fig. 135/Ⓖ) is automatically set on the PDU.

5. If the *“Activate IPv6”* checkbox is checked, select the *“DHCPv6”* checkbox (Fig. 135/Ⓓ) if necessary.

Alternatively, do not select the *“DHCPv6”* checkbox and enter the IPv6 address and IPv6 prefix length manually (Fig. 135/Ⓔ).

6. If necessary, enter a gateway in the *“IPv6”* area (Fig. 135/Ⓗ).

7. If necessary, activate the *“Stateless Autoconfig”* checkbox in the *“IPv6”* area (Fig. 135Ⓖ).

8. Confirm the entry by clicking the *“Save”* (Fig. 135/Ⓚ) button.

6.9.3 Configuring SNMP settings

Personnel: ■ IT specialist

1. Call up the SNMP settings using *"Configuration ➔ SNMP Settings"* (/Ⓐ).

   ⇨ The "SNMP Settings" window opens.

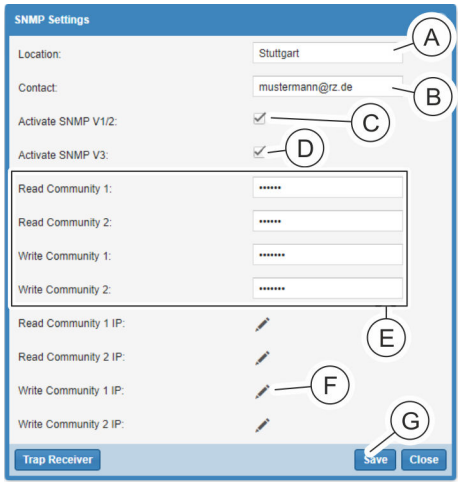


Fig. 136: "SNMP Settings" window

2. In the "SNMP Settings" window, enter the location (/Fig. 136Ⓐ) and the contact (Fig. 136/Ⓑ).
3. If necessary, click the *"Activate SNMP V1/2"* checkbox (Fig. 136/Ⓒ).
4. If necessary, click the *"Activate SNMP V3"* checkbox (Fig. 136/Ⓓ).
5. If necessary, enter an SNMP Read Community or SNMP Write Community (Fig. 136/Ⓔ).
6. If necessary, click the pencil icon (Fig. 136/Ⓕ) to configure SNMP access control.

   ⇨ The "IP Addresses" window opens (Fig. 137).

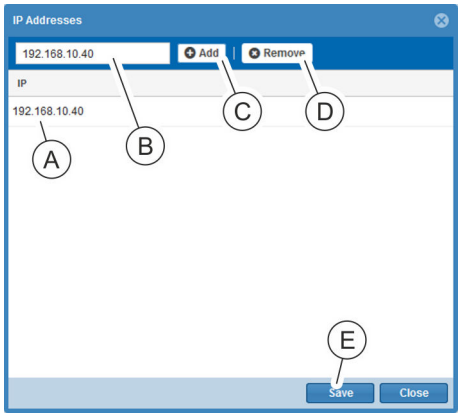


Fig. 137: "IP Addresses" window

7. Enter an IP address or host name (Fig. 137/Ⓑ) in the text box and use the *"Add"* button (Fig. 137/Ⓒ) to add it to the list (Fig. 137/Ⓐ).
8. If necessary, select an IP address or host name from the list (Fig. 137/Ⓐ) and delete it from the list by pressing *"Delete"* (Fig. 137/Ⓓ).
9. After completing the entry, close the "IP Addresses" window by clicking the *"Save"* button (Fig. 137/Ⓓ).
10. Confirm the entry by clicking the *"Save"* (Fig. 136/Ⓖ) button.

6.9.4 Configuring the trap receiver

Personnel: ■ IT specialist

1. Call up the SNMP settings using *"Configuration ➔ SNMP Settings"* (/Ⓐ).

   ⇨ The "SNMP Settings" window opens.

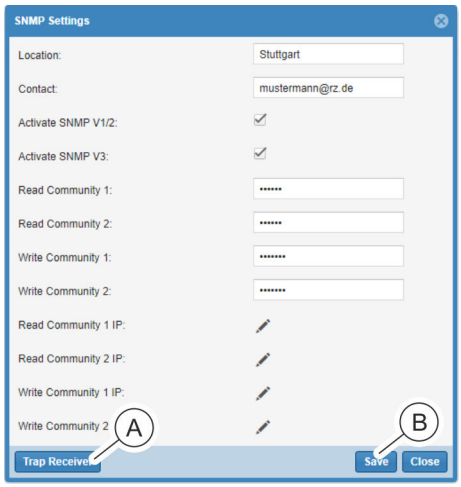


Fig. 138: “SNMP Settings” window

2. In the “SNMP Settings” window, click the *“Trap Receiver”* button (Fig. 138/Ⓐ).

⇨ The “Trap Receiver List” window opens (Fig. 139).

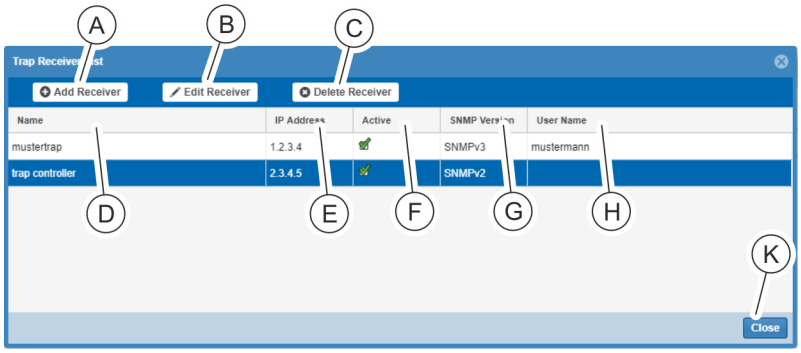


Fig. 139: “Trap Receiver List” window

Ⓐ *“Add Receiver”* button for adding a trap receiver
Ⓑ *“Edit Receiver”* button for modifying a trap receiver
Ⓒ *“Delete Receiver”* button for deleting a trap receiver
Ⓓ *“Name”* column with the name of the trap receiver
Ⓔ *“IP Address”* column with the IP address of the trap receiver
Ⓕ *“Active”* column displaying whether the trap receiver is active or not.
Ⓖ *“SNMP Version”* displaying the SNMP version of the trap receiver
Ⓗ *“User Name”* column displaying the user name
Ⓚ *“Close”* button for closing the window

3. Set up a trap receiver by clicking the *“Add Receiver”* button (Fig. 139/Ⓐ).

You can configure trap receivers with the SNMPv1/SNMPv2 protocol or trap receivers with the SNMPv3 protocol (Fig. 139).

4. After setting up the trap receiver, leave the window using the *“Close”* button (Fig. 139/Ⓚ).

Adding a receiver with SNMPv1/ SNMPv2

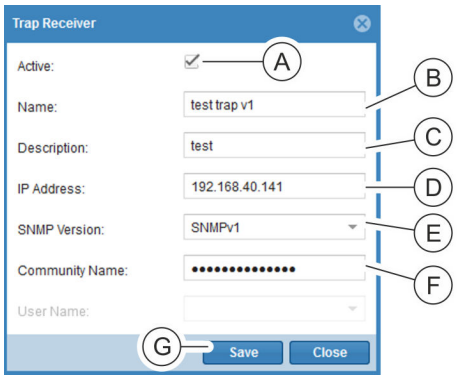


Fig. 140: "Trap Receiver" window

Personnel: ■ IT specialist

1. In the "Trap Receiver" window, click the *"Active"* button (Fig. 140/Ⓐ) to activate the trap receiver.
2. Enter a name for the trap receiver (Fig. 140/Ⓑ).
3. If necessary, enter a description (Fig. 140/Ⓒ).
4. Enter an IP address (Fig. 140/Ⓓ).
5. In the selection field, select an SNMP version ("SNMPv1" or "SNMPv2") (Fig. 140/Ⓔ).
6. Enter a community name (Fig. 140/Ⓕ).
7. After entering the data, exit the window by clicking the *"Save"* button (Fig. 140/Ⓖ) to create the configuration on the PDU.

Adding a receiver with SNMPv3

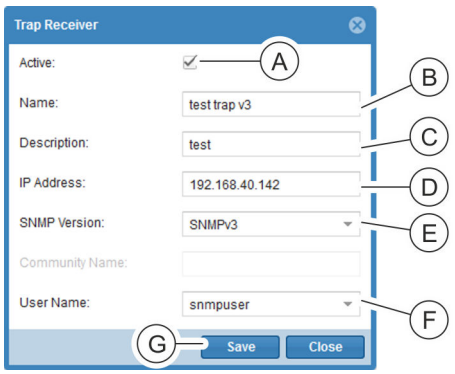


Fig. 141: "Trap Receiver" window

Personnel: ■ IT specialist

1. Configure the trap receiver as per ↳ *Adding a receiver with SNMPv1/SNMPv2*, steps 1 to 4 (Fig. 141/Ⓐ – Ⓓ).
2. In the selection field, select the SNMP version "SNMPv3" (Fig. 141/Ⓔ).
3. Select a user name (Fig. 141/Ⓕ).

> *To be able to select a user as a trap receiver, the user must be set up in the user administration as "trap receiver" (↳ Chapter 6.8.2 "Managing a local user" on page 88).*

4. After entering the data, exit the window by clicking the *"Save"* button (Fig. 141/Ⓖ) to create the configuration on the PDU.

6.9.5 Calling up system information

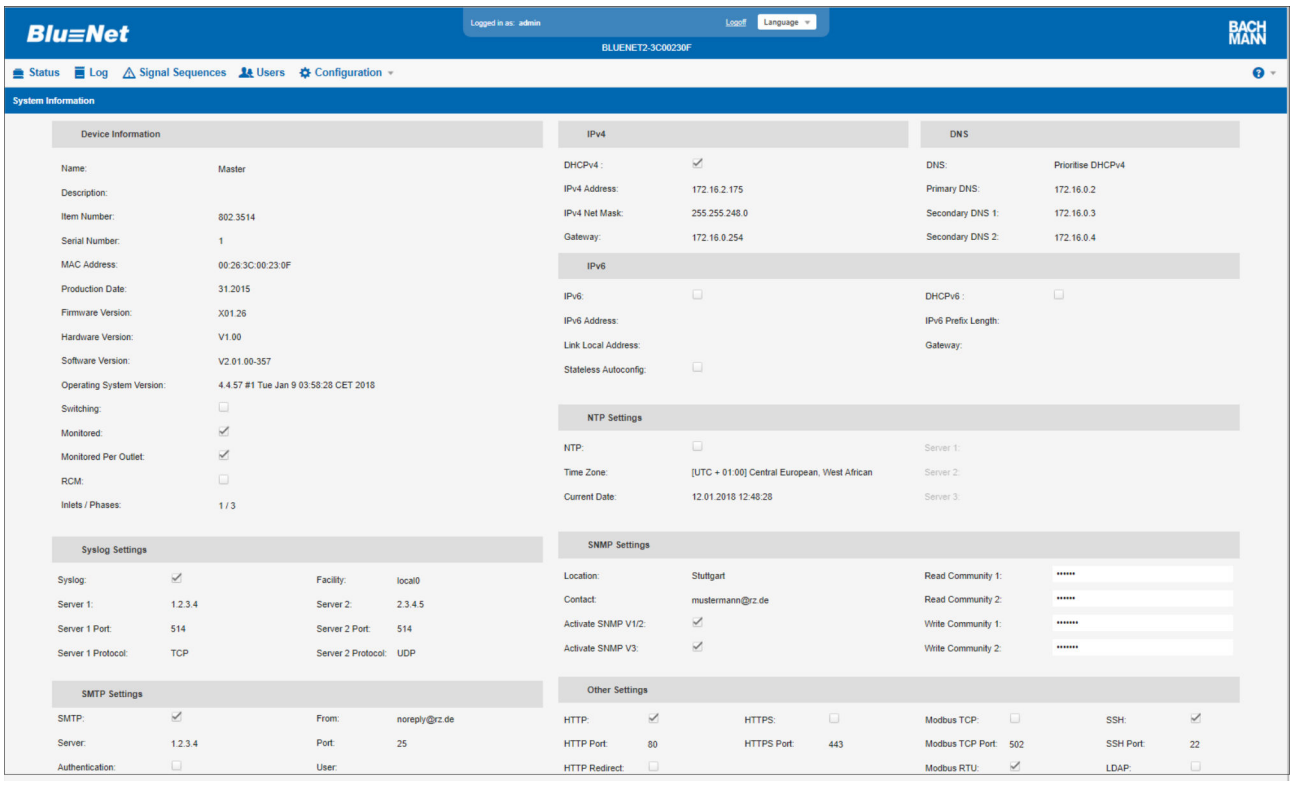


Fig. 142: “System Information” menu

→ Call up the “System Information” menu by choosing *“Configuration ➔ System Information”*.

In this menu you can view information relating to the PDU and current settings.

6.9.6 Executing system commands

Improper software updates

NOTICE!

Risk of damage if the power supply is disconnected during a software update!

If the power supply to the PDU is disconnected during a software update, the PDU could be damaged.

- The software update may only be carried out by an IT specialist.
- Never disconnect the power supply to the PDU while an update is in progress.
- Slave PDUs can be updated via the software update of the Master PDU. Never disconnect the power supply to the Slave PDUs during a software update of the Master PDU.
- GPIO modules can be updated via the software update of the Master PDU. Never interrupt the connection between the Master PDU and GPIO module during the update.

Overview

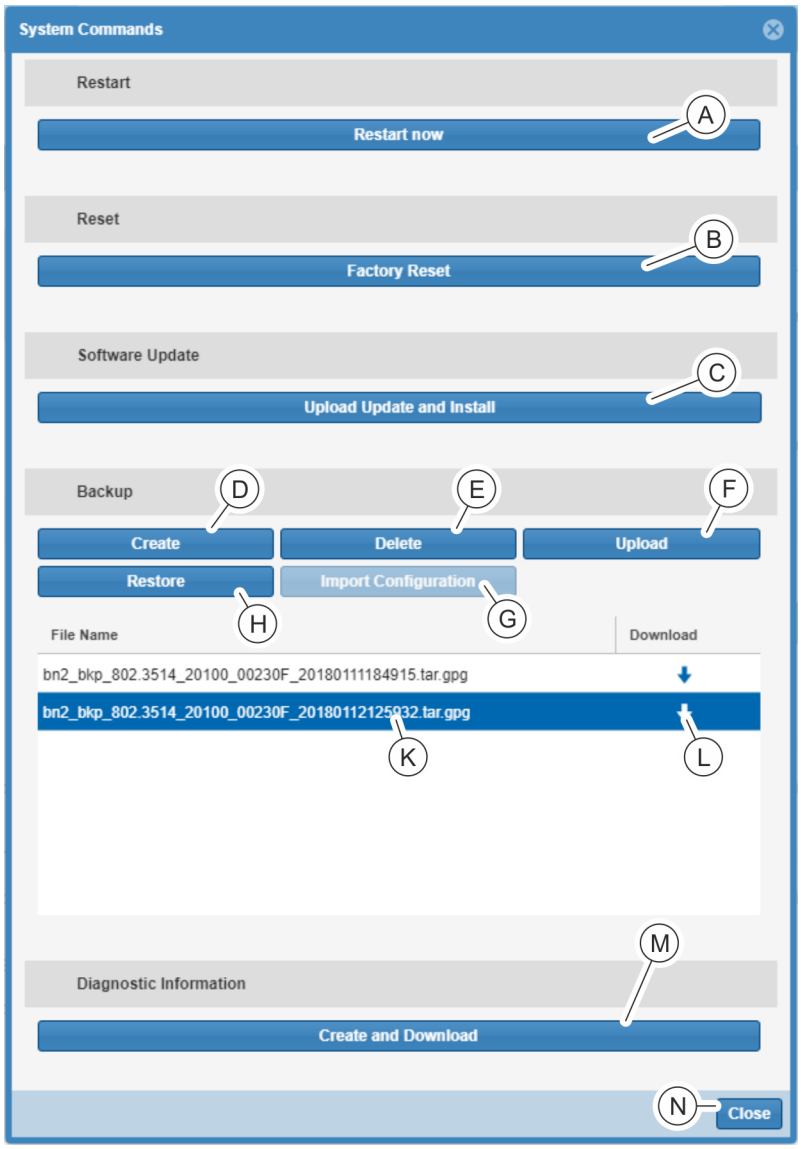


Fig. 143: “System Commands” window

Item	Button	Description
Ⓐ	*"Restart now"*	You can click this button to restart the PDU. After you click this button, you confirm a query and then the PDU restarts. The current web interface session expires. To be able to make changes to the settings using the web interface, the user must wait for the PDU to restart and log in again.
Ⓐ	*"Factory Reset"*	You can click this button to reset the PDU to the factory settings. After you click this button, you have to confirm a query to execute the operation. The current web interface session expires. To be able to make changes to the settings using the web interface, the user must wait for the PDU to restart and log in again.
Ⓐ	*"Upload Update and Install"*	You can click this button to update the PDU. After you click this button, you have to select an update in a browser dialogue and then confirm your choice. After confirming a prompt, the update is uploaded to the PDU. After uploading, the software update is installed on the PDU. This could take some time. The PDU is automatically restarted after the update is installed. The current web interface session expires. To be able to make changes to the settings using the web interface, the user must wait for the PDU to restart and log in again.
Ⓐ	*"Create"* a backup	You can click this button to create a backup of the PDU configuration. After you click this button, the settings are backed up and saved on the PDU. In the *"File Name"* field (Fig. 143/Ⓑ), the backups are displayed with a time stamp.
Ⓐ	*"Delete"* a backup	You can click this button to delete a backup of the PDU configuration. To do so, select the backup you wish to delete in the *"File Name"* field (Fig. 143/Ⓚ). Click the *"Delete"* button to execute the delete operation.
Ⓐ	*"Upload"* a backup	You can click this button to upload a backup to the PDU. After you click this button, you have to select a backup in a browser dialogue and then confirm your choice. The backup file is uploaded and is then displayed in the *"File Name"* field (Fig. 143/Ⓚ).
Ⓖ	*"Import Configuration"* of a backup	You can click this button to import a backup to the PDU. After selecting a configuration in the *"File Name"* field (Fig. 143/Ⓚ), click the *"Import Configuration"* to load the selected configuration to the PDU. After you confirm the operation, the configuration is loaded to the PDU.
Ⓖ	*"Restore"* a backup	You can click this button to restore a backup on the PDU. After selecting a backup in the *"File Name"* field (Fig. 143/Ⓚ), click the *"Restore"* button to import an earlier PDU configuration back to the PDU.
Ⓖ	*"File Name"*	A list of available backups is displayed in this field.

Item	Button	Description
Ⓖ	*“Download”* (⬇) a backup	Click this button to download a backup of the configuration. Next to each entry in the *“File Name”* field (Fig. 143/Ⓚ) there is a button that allows you to download the configuration to a local data carrier. A configuration for a PDU or PU2 that was saved on the web interface can be copied to a device of the same type (article number) and the same software version. This also applies to equivalent master-slave combinations. To do so, the user logs onto the web interface for a different PDU, imports the configuration (Fig. 143/Ⓒ) and uploads it to the PDU.
Ⓖ	*“Create and Download”*	The “create and download diagnostic information” function is used to collect system information on the PDU and make it available as a downloadable file. After it is automatically downloaded to a local PC, the file on the PDU is deleted. Only create the diagnostic information when requested to do so by Bachmann Support, then download it and send it to Bachmann Support. To create the diagnostic information, click the button and select a local target folder. A diagnostic file is then created and saved in the local target folder.
Ⓖ	*“Close”*	Click this button to close the “System Commands” window.

7 Operation using the SSH console

7.1 Description of executable commands

The commands are executed at the SSH console by users with the "admin" or "operator" role. Users with the "admin" role can use all commands. Users with the "operator" role can only use some of the commands.

For more information about possible parameter values such as "`<filter>`", call up the "`CommandLine --help`".

The following table contains the description of CLI commands. Linux commands can be used to a limited extent, depending on the role.

Command	Explanation

General	`CommandLine --help`
	`CommandLine --version`
	`CommandLine --cmd <command> [--quiet] [--verbose {0..2}] <command specific parameters>`
	An alias `cli='CommandLine --cmd'` is defined.

Entry of measured data and status of various measuring points (ReadValues)	`CommandLine --cmd readvalues [--filter <filter>]`
	The `--filter` parameter can be used to filter by the type of measured data.
	`CommandLine --cmd readvalues [--pdu {1..12}] [--inlet {1..2}] [--phase {1..3}] [--fuse {1..4}] [--outlet {1..48}] [--s-group {1..50}] [--m-group {1..4}] [--cee17-5p {1..4}]`
	The `--pdu` parameter (or similar) can be used to filter individual instances of a type.
	`CommandLine --cmd readvalues [--depth <filter>]`
	The `--depth` parameter can limit the depth of the output tree.

Output of the configuration of the various measuring points (ReadDeviceInfo)	`CommandLine --cmd readdeviceinfo [--filter <filter>]`
	The `--filter` parameter can be used to filter by the type of measured data.
	`CommandLine --cmd readdeviceinfo [--pdu {1..12}] [--inlet {1..2}] [--phase {1..3}] [--fuse {1..4}] [--outlet {1..48}] [--s-group {1..50}] [--m-group {1..4}] [--cee17-5p {1..4}]`
	The `--pdu` parameter (or similar) can be used to filter individual instances of a type.
	`CommandLine --cmd readdeviceinfo [--depth <filter>]`
	The `--depth` parameter can limit the depth of the output tree.

Set the Friendly-Name of a measuring point (WriteDeviceInfo)	`CommandLine --cmd writedeviceinfo --identifier <svid> --name <newname>`

Command	Explanation
Output of the Set-Point configuration of various measuring points (ReadSetPoint)	`CommandLine --cmd readsetpoint [--identifier <svid>] | [--name <descName>] [--filter <filter>] [--verbose]` The `--identifier` and `--name` parameters can be used to specify a concrete measuring point. The `-- filter` parameter can only be used in combination with `--name`.
Set a SetPoint configuration for a measuring point (WriteSetPoint)	`CommandLine --cmd writesetpoint (--identifier <svid>) | (--name <descName>) [--lowAlarm <n> ] [--lowWarning <n>] [--highWarning <n>] [--highAlarm <n>] [--hysteresis <n>]` The `--identifier` and `--name` parameters can be used to specify the measuring point. The `--lowAlarm` parameter (or similar) can be used to define the individual setpoint thresholds.
Output of all alarmed measuring points (ReadAlarms)	`CommandLine --cmd readalarms`

Output of relay status of all sockets (ReadRelaisState)	`CommandLine --cmd readrelaisstate [--identifier <guid> | --name <descName>]`
	The `--identifier` and `--name` parameters can be used to specify a concrete measuring point.
	`CommandLine --cmd readrelaisstate [--pdu {1..12}] [--inlet {1..2}] [--phase {1..3}] [--fuse {1..4}] [--outlet {1..48}]`
	The `--pdu` parameter (or similar) can be used to filter individual subtrees.

Set the relay status of a socket (switches a socket on/off) (WriteRelaisState)	`CommandLine --cmd writerelaisstate [--identifier <guid> | --name <descName> ] --value {off|on} [--timeout <seconds>]` The `--identifier` and `--name` parameters can be used to specify the measuring point. You can use the `--timeout <seconds>` parameter to specify a duration of time before the socket is automatically switched back on.
Deactivate an external sensor (deactivate)	`CommandLine --cmd deactivate --identifier <guid>` The `--identifier` parameter can be used to specify the sensor.
Identify an individual socket (i.e. make the LED of a socket flash) (IdentifySocket)	`CommandLine --cmd identifysocket [--identifier <guid> | --name <descName>] --value {off|on}` The `--identifier` and `--name` parameters can be used to specify the socket.
Output of a list of the configuration parameters (ReadConfig)	`CommandLine --cmd readconfig [--key <name>]` The `--key` parameter can be used to specify a concrete configuration parameter.

Command	Explanation

Set a configuration parameter (WriteConfig)	`CommandLine --cmd writeconfig --key <name> --value <value>`
	The configuration parameter must be specified using the `--key` parameter.
	The `--value` parameter specifies the related value.
	Only the setting of the IP address is supported by the current version:
	`CommandLine --cmd writeconfig --key NetworkIPv4Address --value '192.168.0.100|255.255.255.0'`

Reset values (Reset)	Resets a “peak” value or the value “Active Energy Resettable”. `CommandLine --cmd reset --identifier <svid>` The measured value must be specified using the `--identifier` parameter.
Carry out an RCM self-test (RCM selftest)	`CommandLine --cmd rcm-selftest --identifier <guid> [--alarm]` The RCM module to be tested must be specified using the `--identifier` parameter. To receive valid GUIDs as `identifier`, use the `--cmd readdeviceinfo` command. The signal sequences are triggered by the `--alarm` parameter.
Reset PDU to factory settings (FactoryReset)	`CommandLine --cmd factoryreset [--slave <slave number>] --confirm` The `--confirm` parameter prevents the command from being used unintentionally. You can use the `--slave` parameter to perform a factory reset of a slave PDU. This parameter is optional.
Configure web server settings	`CommandLine --cmd configure --service web --enable-http (on|off) --enable-https (on|off) [--http-port <port>] [--https-port <port>] [--redirect]` The `--enable-http` and `--enable-https` parameters can be used to activate or deactivate access to the web interface. The optional `--http-port` and `https-port` parameters can each be used to specify a port. The optional `--redirect` parameter can be used to activate a redirect from HTTP to HTTPS.
Display socket groups	`CommandLine --cmd list-groups [--identifier <svid>] ... [--expand]` You can use the optional `--identifier` parameter to specify the group to be displayed. If you specify the `--expand` parameter, the sockets belonging to the groups are also output.

Command	Explanation
Create or update socket groups	`CommandLine --cmd update-group --identifier <svid> [--name <name>] [--description <description>]` The `--identifier` parameter is used to specify the socket group to be created or updated. If the `identifier` has a value of `-1`, a new group is created. The optional `--name` parameter is used to specify the name of the socket group. The optional `--description` parameter is used to specify a description for the socket group.
Modify the contents of a socket group	`CommandLine --cmd modify-group --identifier <group-svid> [--add <socket-svid>[:<socket-svid>...]] [--remove <socket-svid>[:<socket-svid>...]]` The `--identifier` parameter is used to specify the socket group to be modified. The `--add` parameter is used to assign sockets. The `--remove` parameter is used to remove sockets.
Delete socket groups	`CommandLine --cmd delete-groups --identifier <svid>[:<svid>...]` You can use the `--identifier` parameter to specify the socket groups to be deleted.
List users (list users)	`CommandLine --list users`
Output of signal sequences defined for a measuring point (List signal chains)	`CommandLine --cmd list-signalchains [--identifier <svid>]` The `--identifier` parameter is used to specify the measuring point.
Assign a signal sequence to a measured value	`CommandLine --cmd associate-signalchain --identifier <svid> ... -mv-state <state> ... [--sc-name <sc-name> ...] [sc-alarm <state>]` The `--identifier` parameter is used to specify the measured value. You use the `--mv-state` parameter to specify the state that the signal sequence is assigned to. You use the `--sc-name` parameter to specify the signal sequences that are assigned to this measured value state. If you omit the parameter, all assigned signal sequences are removed. You can use the `--sc-alarm` parameter to also specify the severity of the alarm message. This is only possible for the inputs of a GPIO module.
Activate/deactivate the inputs/outputs of a GPIO module	`CommandLine --cmd configure-gpio --identifier <svid> --i1 <mode> [--i2 <mode> ...]` You use the `--identifier` parameter to specify the GPIO module. The `--i1` parameters (i1–i4 or o1–o4) specify the activation of the four inputs and the four outputs. The `<mode>` is specified by 'd' (disabled) or 'e' (enabled).

Command	Explanation
Switch an output of a GPIO module	`CommandLine --cmd switch-gpio --identifier <svid> ... --state <state>` The `--identifier` parameter is used to specify the output to be switched. The `--state` parameter is used to switch the output. The possible values are 'on' and 'off'.
Output the PDU functions (Read-Capabilities)	`CommandLine --cmd readcapabilities [--identifier <svid>] ...` The `--identifier` parameter can be used to specify a specific (slave) PDU.
Create diagnostic information (Diagnosis)	`CommandLine --cmd diagnosis [--remove]` The archive created with this command (`bn2_diag_<article number>_<SW version>_<part of MAC address>.tar.gz.gpg`) can be copied from the PDU via SCP, in order to make it available to Support. The `--remove` parameter is used to delete the archive created.
Configure Modbus TCP settings	`CommandLine --cmd configure --service modbus --enable (on|off) [--port <port>] [--spec <spec>]` The `--spec` parameter can be used to select the desired protocol specification. The default values are: Port 502, specification V2.00
Configure NTP/time settings	`CommandLine --cmd configure --service ntp --enable (on|off) [--ntp-server <server> ...] [--time <epoch>] [--tzoff <minutes>]` Up to three NTP servers can be specified here. If none is specified, “pool.ntp.org” is set as the default value. If NTP is not activated, the `--time` parameter can be used to set the time in seconds since 01.01.1970. The maximum date is 31.12.2035. If the parameter is left out, the current system time is used. The `--tzoff` parameter can be used to specify the offset of the time zone in minutes in relation to Greenwich Mean Time. The standard time zone is CET.
Configure SMTP	`CommandLine --cmd configure --service smtp --enable (on|off) --host <host> [--port <port>] --from <sender> [--auth] [--login <login>] [--password <password>]` The `--host` parameter is used to specify the mail server. This parameter has to be entered if the SMTP service is activated. The `--from` parameter is used to specify the sender address. This parameter has to be entered if the SMTP service is activated. The `--port` parameter can be used to specify the port for the mail server. If the parameter is left out, port “25” is set as the default value. The `--auth` parameter is used to specify an authentication. In this case, the two parameters `--login` and `--password` have to be used to specify a user name and password.

7.2 Restarting the PDU using the SSH console

Personnel: ■ IT specialist

1. Open an SSH session.
2. *Only users with the "admin" role can perform a restart.*

   Log in with a user name and password.
3. Enter the `sudo reboot` command in the shell.

7.3 Resetting the PDU to factory settings using the SSH console

Personnel: ■ IT specialist

1. Open an SSH session.
2. *Only users with the "admin" role can reset the PDU to the factory settings.*

   Log in with a user name and password.
3. Enter the `CommandLine --cmd FactoryReset --confirm` command in the shell.

7.4 Creating cronjobs at the PDU

Cronjobs can be used to automate recurrent tasks. Cronjobs are managed in the crontab using the `crontab [OPTION]|[FILE]` command:

OPTION

- `-l` = list of cronjobs
- `-e` = edit crontab in the editor
- `-r` = delete cronjobs

FILE

- Replaces the crontab with a specified file, e.g. "mycrontab.txt".

A cronjob is entered in the crontab in the following form:

Minute	Hour	Day	Month	Weekday	Command to be executed
0–59	0–23	1–31	1–12	0–7	e.g. script

If a cronjob is to be executed e.g. on several days, the days are listed, separated by commas.

If `*` is entered instead of a numeric value, execution is always carried out. If a `*` is entered e.g. in the “Day” column, execution takes place every day.

Editing a crontab manually

Personnel: ■ IT specialist

1. Open an SSH session.
2. Log in with a user name and password.
3. Enter the `crontab -e` command in the shell.
   ⇨ An editor with the crontab opens.
4. Enter the cronjob in the crontab.
5. Save the change and exit the editor.

Importing a crontab from a file

Personnel: ■ IT specialist

1. Open an SSH session.
2. Log in with a user name and password.
3. 
   A crontab can be imported from a previously created text file, e.g. "mycrontab.txt".

   Enter the `crontab [FILE]` command in the shell.
   ⇨ The crontab is imported.
4. To check this, use `crontab -l` to have the list of cronjobs displayed.

Deleting cronjobs

Personnel: ■ IT specialist

1. Open an SSH session.
2. Log in with a user name and password.
3. Delete all cronjobs at the shell using the command: `crontab -r`.
4. To check this, use `crontab -l` to have the list of cronjobs displayed, which should be empty.

Calling up the CommandLine interface in a cronjob

If the CommandLine interface is to be called up in a cronjob, either the library path needs to be entered or the "CLI” wrapper script needs to be used.

An example of a call of the CommandLine interface in the crontab is as follows:

with library path

```
* * * * * LD_LIBRARY_PATH=/usr/bn2/lib
Commandline --cmd readvalues >${HOME}/out.txt
```

with "CLI" wrapper script

```
* * * * * CLI --cmd readvalues >${HOME}/out.txt
```

8 Operation using the serial console

The serial console can be used for debug outputs.

An adapter can be connected with a PC via the S1 connection for a serial interface for the connection (pin assignment: 3 for RX, 6 for TX and 8 for GND).

The following settings are required for a connection of the serial console:

- Port: depends on the PC
- Baud rate: 115200
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

9 Carrying out a software update from USB stick or via SCP

Software update from USB stick

NOTICE!

Risk of damage if the power supply is disconnected during a software update!

If the power supply to the PDU is disconnected during a software update, the PDU could be damaged.

– The software update may only be carried out by an IT specialist.
– Never disconnect the power supply to the PDU while an update is in progress.
– Slave PDUs can be updated via the software update of the Master PDU. Never disconnect the power supply to the Slave PDUs during a software update of the Master PDU.
– GPIO modules can be updated via the software update of the Master PDU. Never interrupt the connection between the Master PDU and GPIO module during the update.

As an alternative to a software update using the web interface (☞ Chapter 6.9.6 “Executing system commands” on page 99), a software update can also be carried out using a USB stick or SCP.

Personnel: ■ IT specialist

Materials: ■ USB stick

1. Copy the update file to the root directory of an empty USB stick.
2. Insert the USB stick into the USB interface of the PDU.

   ⇨ The software update is automatically installed on the PDU. This could take some time. The PDU is automatically restarted after the update is installed.

   A file with the extension `.status` is created on the USB stick.

Software update via SCP

Personnel: ■ IT specialist

1. Login to a Linux PC with SSH utilities installed.
2. Enter the command `scp <update file> <user with admin role>@<pdu IP address>:/mnt/free/update` at a console.

   ⇨ The software update is installed on the PDU. This could take some time. The PDU is automatically restarted after the update is installed.

The software update can also be carried out with the corresponding tools using a Windows PC.

10 Miscellaneous

10.1 IT security

Secure passwords

We recommend complying with the following generally recognised rules:

- Use at least eight characters
- Use upper and lower-case letters, numbers and special characters
- Do not use words from the dictionary or names
- Change passwords at regular intervals
- Do not use the same password for multiple applications

https

- “https” can be activated in order to encrypt communication with the web interface.
- “http” can be deactivated or redirected to “https” with “https-redirect”.
- If necessary, a CA certificate can be loaded to the PDU.
- The following encryptions are supported:
  `EECDH+AESGCM:EDH+AESGCM:AES128+EECDH:AES128+EDH`
- An x509 certificate can be created as follows, for example:
  ```
  openssl req -nodes -newkey rsa:2048 -keyout server.key -out server.csr -subj "/O=<company name>"
  openssl x509 -req -days 10000 -in server.csr -signkey server.key -out server.crt
  cat -- server.key server.crt > server.pem
  ```
- The https encryption is via TLS 1.2 with AES 128-bit key. AES-128 is secure enough and is faster than AES-256.
- The web interface can also be used in a mode in which the user has read rights only. Here, the measured data are visible but the system configuration is not.

SSH

- Access as a root user is not possible.
- Authentication is either by means of a password or “public ssh key”.
- SSH access can be switched off for individual users or it can be completely switched off for the PDU.
- Access with read rights can also be arranged by assigning rights.

SNMP

- If SNMP is used in the version “SNMP v3”, only selected users with a password have access.
- Here, “SHA/MD5” is used for “Authentication” and “DES/AES” is used for “Privacy”.

Data backup

- The PDU allows you to create a backup of the configuration and download it on another computer.
- These backups are encrypted and therefore cannot be viewed or manipulated.
- A backup can be imported back to the PDU at any time or it can be transferred to another PDU to import the configuration there.
- In version “V2.01.yy” and higher, a backup that was created with version “V2.01.xx” (“xx” < “yy”) can be restored.

A data backup can be created in the “System Commands” window and downloaded to the local hard drive (↳ Chapter 6.9.6 “Executing system commands” on page 99).

Software update

- The software update packages in version “V2.01” and higher are encrypted and signed. They cannot be viewed or manipulated. This prevents the infiltration of harmful software.
- Due to the encryption, software update packages in version “V2.01” can only be imported from version “V2.00.04” and higher. It is not possible to directly update version “V1.02.04” or earlier to “V2.01”.

10.2 SNMP MIB

The “SNMP” function is deactivated by default. To use the function, it has to be activated and configured.

The following tables (defined in BACHMANN-BLUENET2-MIB) are relevant to monitoring of BlueNet BN3000 – BN7500 PDUs.

Table	Content
“blueNet2DeviceTable”	All devices, including the quantity of lower-level layers, such as electric circuits, fuses etc.
“blueNet2SensorTable”	All external sensors
“blueNet2CircuitTable”	All electric circuits, including the quantity of lower-level phases
“blueNet2PhaseTable”	All phases, including the quantity of lower-level fuses
“blueNet2FuseTable”	All fuses, including the quantity of lower-level sockets

Table	Content
“blueNet2SocketTable”	All sockets (blank for BN3000)
“blueNet2RcmTable”	All RCM modules
“blueNet2SocketGroupTable”	All socket groups, including the associated elements
“blueNet2VariableTable”	Less dynamic parameters for measured data (such as name, unit and scale) and their alarm status (string)
“blueNet2SensorVariableTable”	Name and description of external sensors
“blueNet2VariableSetPoint-Table”	Setpoints (alarm thresholds) for all measured data
“blueNet2VariableDataTable”	Measured data and their states (electrical and external sensor values)

SNMP numbering scheme for measured value OIDs

All OIDs start with **{ iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) bachmann(31770) }**.

The status is under **1.3.6.1.4.1.31770.2.2.8.4.1.4**

The measured data are under **1.3.6.1.4.1.31770.2.2.8.4.1.5**

The next eight characters describe the path to the individual measured data.

The following applies for electrical measured data:

Example: ..0.0.0.0.255.255.0.1

0 - number of pdu (pdu 0 -> Master PDU, 1,2,3,… -> Slave PDU)

0 - number of phase (phase 0,1,2) or 255 for PDU/Inlet layer

255 - number of fuse (fuse 0,1 / 0 if no fuse exists) or 255 for PDU/Inlet/Phase layer

255 - number of outlet (socket 0,1, …) or 255 for PDU/Inlet/Phase/Fuse layer

0.1 - two byte key definition: 1 = voltage, 4 current, …

The following applies for measured data from external sensors:

Example: ...0.1.64.4.255.2.1.0

0 - number of pdu (pdu 0 -> Master PDU, 1,2,3,… -> Slave PDU)

1 - sensor type (0: electrical, 1: external sensor, 4: rcm)

64 - sensor hardware address (64: combination sensor, 72: temperature sensor, 56: GPIO module)

4 - channel number of internal multiplexer (channel 4, 5)

255 - channel number of external multiplexer (channel 255, 1, 2, 4, 8)

2 - external sensor type (2: combination sensor, 1: temperature sensor, 3: GPIO module)

1.0 - two byte key definition:

1.0: temperature, 1.1: humidity 1.10: dewpoint

1.2-1.5 GPIO in 1-4

1.6-1.9 GPIO out 1-4

Examples

Status of voltage in the first phase of a master PDU

1.3.6.1.4.1.31770.2.2.8.4.1.4.0.0.0.0.255.255.0.1 = INTEGER: ok(2)

Measured value for voltage in the first phase of a master PDU

1.3.6.1.4.1.31770.2.2.8.4.1.5.0.0.0.0.255.255.0.1 = INTEGER: 22510

Status of the RCM residual AC current of the first phase of a master PDU

1.3.6.1.4.1.31770.2.2.8.4.1.4.0.4.0.0.255.255.0.7 = INTEGER: ok(2)

Measured value of the RCM residual AC current of the first phase of a master PDU

1.3.6.1.4.1.31770.2.2.8.4.1.5.0.4.0.0.255.255.0.7 = INTEGER: 3

SNMP numbering scheme for fuse states

Fuse states can be read from the blueNet2FuseStatus table.

They are under 1.3.6.1.4.1.31770.2.2.6.4.1.10.

The next four characters describe the path to the individual fuse states.

For the example here, the following applies: ...1.1.3.2

1 - Number of PDU (pdu 1 → Master PDU, 2, 3, … → Slave PDU)

1 - Number of inlet (inlet 1, 2 (2 only for PU2)

3 - Number of phase (phase 1, 2, 3)

2 - Number of fuse (fuse 1, 2)

Example:

Status first fuse of the second phase of a master PDU

1.3.6.1.4.1.31770.2.2.6.4.1.10.1.1.2.1 = INTEGER: on(19)

SNMP traps

Under certain circumstances, the PDU sends SNMP traps. These can be received and evaluated by trap receivers that have been configured accordingly.

Except for `blueNet2ReconfigAgentNotification`, `blueNet2ShutdownAgentNotification` and `coldStart`, it is also necessary to set up a corresponding signal sequence with trap receiver and to assign the corresponding alarm.

The following traps are supported:

- blueNet2VariableLowerAlarmTrap
  - (1) Master (Master) "Master": Current has reached a critical low state: 0.00 A (Threshold: 5.00 A)
  - (2) Master/Combination Sensor S2 (I2C Temperature-Humidity Sensor) "Combination Sensor S2": Humidity has reached a critical low state: 47.7 % (Threshold: 49.8 %)
- blueNet2VariableLowerWarningTrap
  - (1) Master (Master) "Master": Current has reached a warning low state: 0.00 A (Threshold: 5.00 A)
  - (2) Master/Combination Sensor S2 (I2C Temperature-Humidity Sensor) "Combination Sensor S2": Humidity has reached a warning low state: 47.6 % (Threshold: 58.5 %)
- blueNet2VariableStatusOkTrap
  - (1) Master (Master) "Master": Current has reached a normal state: 0.00 A
  - (2) Master/Combination Sensor S2 (I2C Temperature-Humidity Sensor) "Combination Sensor S2": Humidity has reached a normal state: 47.8 %
- blueNet2VariableUpperWarningTrap
  - (1) Master/Inlet/Phase 1 (Phase) "Phase 1": Voltage has reached a warning high state: 218.5 V (Threshold: 200.0 V)
  - (2) Master/Combination Sensor S2 (I2C Temperature-Humidity Sensor) "Combination Sensor S2": Humidity has reached a warning high state: 47.6 % (Threshold: 40.0 %)
- blueNet2VariableUpperAlarmTrap
  - (1) Master/Inlet/Phase 1 (Phase) "Phase 1": Voltage has reached a critical high state: 219.7 V (Threshold: 100.0 V)
  - (2) Master/Combination Sensor S2 (I2C Temperature-Humidity Sensor) "Combination Sensor S2": Humidity has reached a critical high state: 47.6 % (Threshold: 40.0 %)
- blueNet2SensorStatusAlarmTrap
  - (1) Master/Temperature Sensor S2 (I2C Temperature sensor) "Temperature Sensor S2" is Lost
  - (2) Master/Inlet/Phase/Fuse 1 (16A;C) "Fuse 1" is Off
- blueNet2SensorStatusOkTrap
  - (1) Master/Temperature Sensor S2 (I2C Temperature Sensor) "Temperature Sensor S2" is On
  - (2) Master/Inlet/Phase/Fuse 2 (16A;C) "Fuse 2" is Off

- blueNet2PduStatusAlarmTrap
  - Slave-1 (Slave) "Slave-1" is Lost
- blueNet2PduStatusOkTrap
  - Slave-1 (Slave) "Slave-1" is On
- blueNet2ReconfigAgentNotification
- blueNet2ShutdownAgentNotification
- coldStart

10.3 Modbus TCP

The “Modbus TCP” function can be activated or deactivated, as needed. This function is deactivated by default.

Various Modbus TCP protocols are supported. The protocol descriptions can be downloaded from the Bachmann homepage.

Modbus TCP V2.00

- Before the values of a PDU are read, the corresponding PDU ID, inlet (PDU) or outlet (PU) have to be set.
- This is not necessary for a master-only configuration without slave PDUs.
- Function code `0x03` (Read Holding Registers) for reading the measured data
- Function code `0x04` (Read Input Registers) for reading the measured value status
- Function code `0x06` for switching between PDUs, inlets or outlets

Modbus TCP V2.01

- Measured data for all PDUs cannot be read without converting the PDU ID.
- Function code `0x06` is no longer required.
- It can also be used for PowerUnit 2.
- Measured data (function code `0x03`) or status (function code `0x04`) can be read at the following registers/addresses.
  - Register 1 (address 0) - master PDU / PowerUnit 2
  - Register 2001 (address 2000) - first slave PDU
  - Register 4001 (address 4000) - second slave PDU
  - etc.
- In the sensors area, position 1 is always reserved for the internal GPIO.
- External sensors on S1 are at position 2.
- External sensors on S2 are at position 3.

After a software update to version “V2.01”, the Modbus TCP protocol in version “V2.00” is preselected.

This means that existing Modbus TCP queries can continue to be used.

Note here that the device ID (unit identifier) has to be set to the value “255”, as per the “MODBUS Messaging on TCP/IP Implementation Guide”.

10.4 LDAP

10.4.1 Managing users in the directory service

User rights

The PDU can be linked to a directory service via LDAP. The users of the directory service cannot be managed at the PDU, nor are they displayed at the PDU. The user rights for the PDU are assigned via groups specified in the directory service. The following specified groups must be created in the directory service for this purpose:

Group name	Rights at the PDU
BlueNet_adminWeb	Enables administrator login at the WEB GUI (read/write)
BlueNet_operatorWeb	Enables operator login at the WEB GUI (read-only)
BlueNet_adminSsh	Enables administrator login at the SSH console (read/write)
BlueNet_operatorSsh	Enables operator login at the SSH console (read-only)
BlueNet_emailReceiver	Enables the assignment to a signal sequence for receiving emails

In order that the user of the directory service is assigned rights for the PDU, you must add the corresponding groups.

Restrictions

To use users from a directory service, the following needs to be observed:

- The local "admin” user at the PDU has a user ID of "1000". This user ID should not be used for users from the directory service, if such a user is to be granted access to the PDU.
- All other local users at the PDU have user IDs beginning with "1001". To avoid any unexpected behaviour, both the user IDs and also the user names should not match the user IDs and user names in the directory service.
- SNMPv3 (access and trap receiver) can only be defined for local users.
- An SSH key for a user from the directory service can only be saved via SCP, because the users from the directory service are not displayed at the web interface of the PDU.

- A separate home directory is created for all users at the PDU in the path: "/home/<user name>". For users from the directory service, this is done during initial login.
- As long as the directory service is activated, further local users can login to the PDU in addition to the "admin" user. The system searches for the user and password first in the local directory and then in the LDAP.

10.4.2 Configuring LDAP settings

The "Group DN" (Fig. 144/Ⓜ), "Group Naming Attribute" (Fig. 144/Ⓝ) and "User Search Filter" (Fig. 144/Ⓟ) input fields are not supported yet by the current version and cannot be used.

Personnel: ■ IT specialist

1. Call up the LDAP settings by choosing *"Configuration ➔ LDAP Settings"*.
   ⇨ The "LDAP Settings" window opens.
2. Click the *"Active"* checkbox (Fig. 144/Ⓐ) to activate the LDAP service.
3. From the *"Server Type"* option menu, select the type of directory service server used (Fig. 144/Ⓑ).

   To connect a PDU to an MS AD server, the following LDAP Unix attributes must be integrated on the MS AD server:
   – *uidNumber*
   – *gidNumber*
4. Enter the IPv4 or IPv6 address, or alternatively, the host name of the directory service server (Fig. 144/Ⓒ).
5. Enter the port for the LDAP service (port 389 is the default setting) (Fig. 144/Ⓓ).
6. For the connection to the directory service, enter the user (User Login DN) (Fig. 144/Ⓔ) and the corresponding password (Fig. 144/Ⓕ).
7. If necessary, enter a timeout value for establishing the connection to the directory service of between 1 and 60 seconds (30 seconds is the default value) (Fig. 144/Ⓖ).
8. If necessary, enter a timeout value for searching the directory service of between 1 and 500 seconds (30 seconds is the default value) (Fig. 144/Ⓖ).
9. Enter the starting point (Base DN) (Fig. 144/Ⓚ) for the search in the directory service.

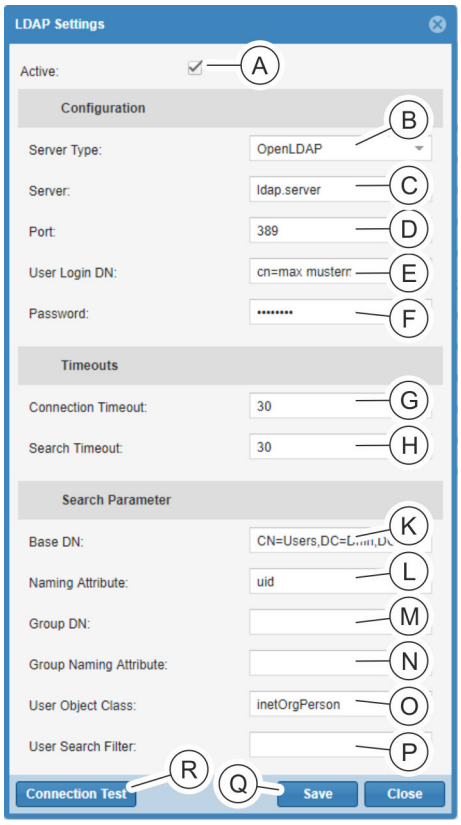


Fig. 144: "LDAP settings" window

10. If necessary, adjust the "Naming Attribute" (Fig. 144/Ⓛ). It is set automatically to "sAMAccountName" if the server type is selected for “MS Active Directory” and to “uid” for "OpenLDAP".
11. If necessary, adjust the "User Object Class" (Fig. 144/◎). It is set automatically to “user" if the server type is selected for “MS Active Directory” and to “inetOrgPerson” for "OpenLDAP".
12. Press the *“Connection Test”* button (Fig. 144/Ⓡ) to check the connection to the directory service.

    ⇨ If the connection test is successful, the "Connection test successful” message (Fig. 145) is displayed.

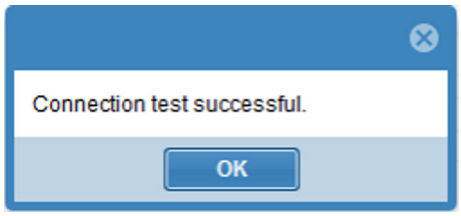


Fig. 145: Connection test successful

If the connection test failed, the "Connection test failed” message (Fig. 146) is displayed. In this case, check the entries for steps 3 – 9.

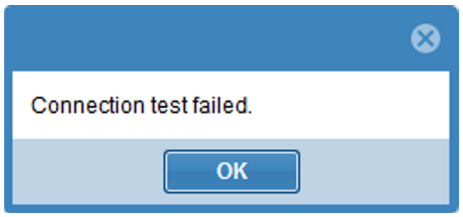


Fig. 146: Connection test failed

13. Confirm the entry by clicking the *“Save”* (Fig. 144/Ⓚ) button.

11 Troubleshooting

Fault description	Cause	Remedy
No display.	The display is switched off.	■ Press a button on the PDU to switch on the display.
	There is no voltage.	■ Check the fuses (if any). ■ Connect the on-site power supply.
	The PDU is not connected correctly.	■ Check the connections.
The status LED does not light up.	There is no voltage.	■ Check the fuse (if any). ■ Connect the on-site power supply.
	The PDU is not connected correctly.	■ Check the connections.
One ore more inlet LEDs not lighting up (PU2 only).	There is no voltage.	■ Connect the on-site power supply.
	The PU2 is not connected correctly.	■ Check the connections.
No current at one socket.	There is no voltage.	■ Check the fuse (if any). ■ Connect the on-site power supply.
When simultaneously carrying out several RCM self-tests, the test of individual RCM modules is not started.	Possible error in one or more RCM modules.	■ Individually restart the self-test of RCM modules.
The RCM self-test is reported as failed.	Possible error in one or more RCM modules.	■ The RCM modules must be checked. Contact customer service (*“Customer service” on page 3*).

12 Technical data

Specifications of the PDU or PU2

The technical specifications of the PDU or PU2 are set out on the nameplate and the data sheet.

Nameplate

The nameplate is located on the housing of the PDU or PU2 and contains the following information:

- Product name
- Item number
- Serial number
- MAC address (physical network address)
- Rated current
- Rated voltage
- Power frequency
- Manufacturer’s address
- CE marking

13 Abbreviations

AES	[**A**dvanced **E**ncryption **S**tandard]
	Encryption procedure for encrypting data
DES	[**D**ata **E**ncryption **S**tandard]
	Encryption procedure for encrypting data
DHCP	[**D**ynamic **H**ost **C**onfiguration **P**rotocol]
	Network protocol that is used in IP networks for the dynamic allocation of network configuration parameters, e.g. IP addresses.
HTTP	[**H**ypertext **T**ransfer **P**rotocol]
	File transfer protocol that is primarily used for transfer of websites
HTTPS	[**H**ypertext **T**ransfer **P**rotocol **S**ecure]
	Encrypted variant of HTTP
IP	[**I**nternet **P**rotocol]
	Mostly used with TCP protocol and is responsible for the transport of data
LDAP	[**L**ightweight **D**irectory **A**ccess **P**rotocol]
	Network protocol for access to and management of distributed directory services
MAC address	[**M**edia **A**ccess-**C**ontrol address]
	Unique hardware address of a network adaptor
MIB	[**M**anagement **I**nformation **B**ase]
	Information that can be queried or modified via a network protocol
NTP	[**N**etwork **T**ime **P**rotocol]
	Network protocol for time synchronisation between computer systems
PDU	[**P**ower **D**istribution **U**nit]
	Socket strip for 19” racks that may have additional functions such as excess-voltage protection or remote control
PoE	[**P**ower **o**ver **E**thernet]
	Energy supply via the network
RCM	[**R**esidual **C**urrent **M**onitoring]
	Monitors the residual current.
RO	**R**ead **O**nly
	Read only right
RTU	[**R**emote **T**erminal **U**nit]
	A variant of the “Modbus” transfer protocol
RW	**R**ead **W**rite

	Read and write rights
SMTP	[**S**imple **M**ail **T**ransfer **P**rotocol]
	Protocol for exchange of messages in computer networks. Is primarily used for sending and forwarding emails.
SNMP	[**S**imple **N**etwork **M**anagement **P**rotocol]
	Protocol for management of devices in networks
SSH	[**S**ecure **Sh**ell]
	Protocol and programme that creates an encrypted connection to a remote device
TCP	[**T**ransmission **C**ontrol **P**rotocol]
	Mostly used with IP protocol and is responsible for the delivery of data
Web UI	[**Web U**ser **I**nterface]
	User interface to the PDU using the web browser

14 Index

A

Access rights 88
Accessories 18
Air humidity sensor 18
Assignment of rights 88
Attachment 9

B

Backup 100, 115
Base unit 10

C

Carrying out an RCM self-test 34
Communication 15
Connections
  Modbus 16
  Network 16
  Sensors 15
  USB 16
Connector panel 7, 8
Control buttons 12
Control keys 9
Control panel 7
Copyright 3
Cronjobs 108
Customer service 3

D

Data backup 115
Diagnostic information 100
Display 9, 12
Display orientation 41

E

Earth 10
Effective energy 37
Event log 73
Explanation of symbols 19

F

Factory reset
  Carrying out using the SSH console 108
  using the buttons on the PDU 47
  using the buttons on the PU2 47
  via the menu 44
Faults 123

G

GPIO module 18
Grouping of the measured data 59
Groups 66, 67

H

https 114

I

Identification
  of individual sockets 63
Illumination time 40

K

Knurled screws 10

L

Language settings 50
LDAP
  Managing users 120
Log 73

M

Measured data
  Displaying on the PDU display 33
  Modifying the names of elements 60
Measuring unit 10, 11
Modbus address 43
Modbus LED 9, 14
Modbus TCP 119
Mounting bracket 9, 16

N

Nameplate 124
Non-heating appliance locking device 16, 17

O

Operation of the display
Resetting the PDU to factory settings using the buttons 47
Resetting the PU2 to factory settings using the buttons 47
Restarting the PDU 46
Operation using the web interface
Backing up and restoring the PDU configuration 100
Carrying out an RCM self-test 64
Configuring signal sequences 78
Configuring the GPIO module for the PDU . . . 72
Configuring the system 93, 121
Configuring the trap receiver 95
Creating and downloading diagnostic information 100
Displaying the RCM protocol 76
Filtering the event log 74
Identifying individual sockets 63
Login 50
Managing socket groups 67
Modifying the grouping of the measured data 59
Modifying the names of elements 60
Removing a slave PDU 61
Removing filters on the event log 75
Resetting the PDU to factory settings 100
Resetting the slave PDU 60
Restarting the PDU 100
Setting the user language 50
Setting up signal sequences and threshold values 80
Setting up signal sequences and threshold values for a differential current analyser 81
Setting up signal sequences for a GPIO module 84
Switching sockets 62
Uploading and installing an update on the PDU 100
User administration 88
Overview 10

P

Password rules 114
PDU restart
About the PDU 46
Using the SSH console 108
Personnel 20
Plug-in bracket 9, 16
Power supply 10
Product overview 7

R

RCM 76
RCM log 73
RCM self-test 64
Resetting to factory settings
using the buttons on the PDU 47
using the buttons on the PU2 47
Using the SSH console 108
via the menu on the display 44

S

Scope of delivery 16
Service 3
Setting up a network
with DHCP protocol 26
without DHCP protocol 28
Setting up signal sequences
GPIO module 84
Phase 80
RCM 81
Short description 11
Signal sequence
Adding 78
Slave PDU
Removing 61
Reset 60

SNMP 114
Socket groups 67
Socket LEDs 14
Socket types 7
Software update 100, 115
  Using a USB stick 112
  via SCP 112, 113
SSH 114
SSH console
  Cronjobs 108
  Description of executable commands 103
  Resetting the PDU to factory settings 108
  Restarting the PDU 108
Status LED 9, 13
Switch 62
System commands 100
System configuration
  LDAP settings 121
  Network settings 93
  SNMP settings 95
  Trap receiver 95
System information 40, 98

T

Technical data 124
Temperature sensor 18
Trap receiver 95

U

Update 100
User configuration
  Directory service 120
  Managing a local user 88
Using the display
  Carrying out an RCM self-test 34
  Displaying the measured data 33
  Displaying the system information 40
  Operating the PU2 at the display 25
  Resetting the effective energy 37
  Resetting the PDU to the factory settings via the menu 44
  Resetting the PU2 to the factory settings via the menu 44
  Setting the display orientation 41
  Setting the illumination time 40
  Setting up a network with DHCP protocol 26
  Setting up a network without DHCP protocol . 28

W

Web interface
  “Log” menu 73
  “Signal Sequences” menu 77
  “Status” menu 54
  “Users” menu 87
  Menu structure 49
  Overview 51