Rittal – The System.

Faster – better – everywhere.

IoT interface

3124300

Assembly and operating instructions

FRIEDHELM LOH GROUP

RITTAL

Foreword

Dear Customer!

We would like to thank you for choosing our IoT interface!

We wish you every success!

Your,
Rittal GmbH & Co. KG

Rittal GmbH & Co. KG
Auf dem Stützelberg

35745 Herborn, Germany
Germany

Tel.: +49(0)2772 505-0
Fax: +49(0)2772 505-2319

E-mail: info@rittal.com
www.rittal.com
www.rittal.de

We are always happy to answer any technical questions regarding our entire range of products.

Contents

Contents

1 Notes on documentation

1.1 CE labelling

Rittal GmbH & Co. KG confirms the conformance of the IoT interface to the EMC regulation 2014/30/EU and the low voltage regulation 2014/35/EU. An appropriate declaration of conformity has been prepared which can be supplied if required.

1.2 Storing the documents

The operating, installation and maintenance instructions as well as all applicable documents are an integral part of the product. They must be handed to those persons who work with the unit and must always be available and on hand for the operating and maintenance personnel.

1.3 Symbols used in these operating instructions

The following symbols are found in this documentation:

	Danger! **A dangerous situation in which failure to comply with the instructions will result in death or severe injury.**
	Warning! **A dangerous situation which may cause death or serious injury if the instructions are not followed.**
	Caution! **A dangerous situation which may lead to (minor) injuries if the instructions are not followed.**
	Note: Important notices and indication of situations which may result in material damage.

■ This symbol indicates an "action point" and shows that you should perform an operation or procedure.

1.4 Symbols on the IoT interface

	Caution: hot surface. **Do not touch!**

1.5 Associated documents

– Installation and Short User's Guide

1.6 Area of validity

This guide applies to software version ≥ V6.15.60.

This documentation uses English screenshots exclusively. The English terms are also used in the descriptions for the individual parameters on the IoT interface website. Depending on the set language, the displays on the IoT interface website may deviate (see section 8.6.2 "Units and Languages")

EN

2 Safety instructions

2.1 General safety instructions

Please observe the following general safety instructions for the installation and operation of the system:

– Assembly and installation of the IoT interface, especially wiring with mains power, may only be performed by a trained electrician.
– Please observe the valid regulations for the electrical installation for the country in which the IoT interface is installed and operated, and the national regulations for accident prevention. Please also observe any internal company regulations, such as work, operating and safety regulations.
– Use only original Rittal products or products recommended by Rittal in conjunction with the IoT interface.
– Please do not make any changes to the IoT interface that are not described in this manual or in the associated assembly and operating instructions.
– The operational safety of the IoT interface is guaranteed only for the intended use. The technical data and limit values stated in the technical specifications may not be exceeded under any circumstances. In particular, this applies to the specified ambient temperature range and IP degree of protection.
– The IoT interface must not be opened. The unit does not contain any parts that need servicing.
– Operating of the system in direct contact with water, aggressive materials or inflammable gases and vapours is prohibited.
– The IoT interface must be disconnected from the mains when it is connected with other units.
– The IoT interface is not suitable for deployment at locations where children can linger.
– The IoT interface must be installed in areas with restricted access.
– The wiring must be protected against possible misuse.
– Other than these general safety instructions, ensure you also observe the specific safety instructions when carrying out the tasks described in the following chapters.

2.2 Operating and technical staff

– The assembly, commissioning, maintenance and repair of this unit may be performed only by qualified personnel.
– Only properly instructed personnel may work on a unit while in operation.

3 Product description

3.1 Function description

The IoT interface facilitates the interconnection and administration of Rittal components (such as Blue e+ cooling units, Blue e+ chillers, Smart Monitoring System) with in-house customer monitoring systems and/or energy management systems. The generated data sets can be used for further data collection and processing. This permits a long-term recording and evaluation of device data, statuses and system messages.

The device provides an Ethernet LAN interface in conjunction with a web server for user communication. The CAN bus interface allows a wide range of sensors, actuators and systems for access monitoring to be connected. All sensors initialise themselves automatically after connection to the CAN bus system.

A 24 V $\mathrm{=}$ connection is available for the power supply. The bus cables then supply power to the connected CAN bus sensors. Alternatively, the IoT interface can also be supplied with the required operating voltage from a cooling unit connected at connection X6 (fig. 6, item 14).

3.2 Proper use, anticipated misuse

The IoT interface is exlusively for the interconnection of Rittal components in areas with restricted access in the industrial area. Any other use is not permitted.

Rittal must be contacted before using a sensor connected outside of an enclosure.

The unit is state of the art and built according to recognised safety regulations. Nevertheless, improper use can present a hazard to life and limb of the user or third parties, or result in possible impairment of the system and other property.

The unit should thus only be used properly and in technically sound condition. Any malfunctions which impair safety should be rectified immediately! Follow the operating instructions!

The intended use also includes following the accompanying documentation as well as fulfilling the inspection and maintenance conditions.

Rittal GmbH & Co. KG is not responsible for any damage which may result from failure to comply with the accompanying documentation. This also applies to failure to comply with the valid documentation for the accessories used.

Inappropriate use may result in danger. Inappropriate use may include:
– Use in areas in which children can linger.
– Use of impermissible tools.
– Improper use.
– Improper rectification of malfunctions.
– Use of accessories not authorised by Rittal GmbH & Co. KG.

3.3 Scope of supply
– IoT interface
– Accessories provided (fig. 1)
– Installation and Short User's Guide
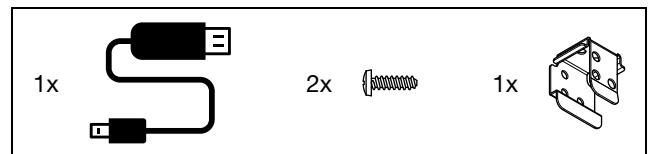
Fig. 1:   Accompanying accessories

4 Transportation and handling

4.1 Transportation

The device is supplied in one packaging unit.
- Check the packaging carefully for signs of damage.

4.2 Unpacking

- Remove the device's packaging materials.

> Note:
> After unpacking, the packaging materials must be disposed of in an environmentally friendly way. It consists of the following materials: cardboard.

- Check the device for any damage that occurred during transport.

> Note:
> Damage and other faults, e.g. incomplete delivery, should immediately be reported to the shipping company and to Rittal GmbH & Co. KG in writing.

- Check the supply contents for completeness (see section 3.3 "Scope of supply".

5 Installation

5.1 Safety notes

⚠️ **Warning!**
Work on electrical systems or equipment may only be carried out by an electrician or by trained personnel guided and supervised by an electrician. All work must be carried out in accordance with electrical engineering regulations.

The unit may only be connected after the above-named personnel have read this information!

Use insulated tools.

The connection regulations of the appropriate power company must be followed.

The unit is free from power only after all power sources have been disconnected!

The installation of the IoT interface in other units is prohibited. Only an autonomous installation is permitted.

■ Please observe the valid regulations for the electrical installation for the country in which the IoT interface is installed and operated, and the national regulations for accident prevention. Please also observe any company-internal regulations, such as work, operating and safety regulations.
■ The technical data and limit values stated in the technical specifications must not be exceeded under any circumstances. In particular, this applies to the specified ambient temperature range and the IP category.
■ If a higher IP degree of protection is required for a special application, the IoT interface must be installed in an appropriate housing or enclosure with the required IP category.

5.2 Requirements placed on the installation location

To ensure the correct operation of the device, the conditions for the installation location described in section 14 "Technical specifications" must be observed.

Electromagnetic interference
– Interfering electrical installations (high frequency) should be avoided.

5.3 Installation procedure

In general, there are two ways of installing the IoT interface:

1. Installation on a top-hat rail
2. Installation on a Blue e+ cooling unit

5.3.1 Installation on a top-hat rail

An installation on a top-hat rail is by simple attachment.
■ Attach the holder at the rear of the IoT interface at the top of the top-hat rail.
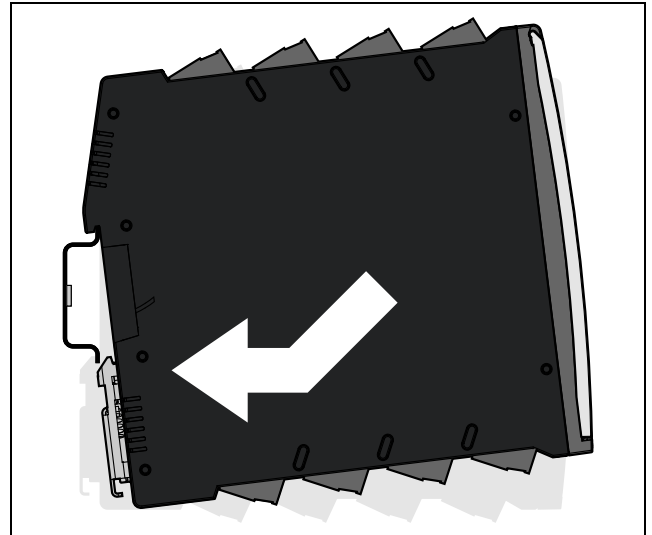
Fig. 2:   Installation on a top-hat rail

■ Push the IoT interface at the bottom completely onto the top-hat rail.
The lower, spring-loaded holder secures the IoT interface on the top-hat rail.

5.3.2 Installation on a Blue e+ cooling unit

To install the IoT interface directly on a Blue e+ cooling unit, an appropriate adaptor with the associated screws is provided with the scope of supply.
■ First fasten the adaptor with the two screws onto the cooling unit.
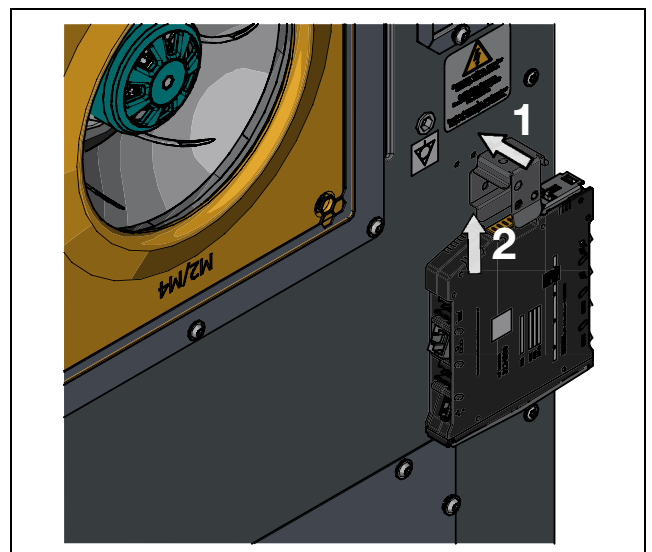
Fig. 3:   Installation on a Blue e+ cooling unit

■ Then, similar to the installation on a top-hat rail, push the IoT interface from below onto the adaptor.

5 Installation

The lower, spring-loaded holder secures the IoT interface on the adaptor.

☞ Note:
The IoT interface must not be installed directly on a Blue e+ cooling unit that is installed as full internal installation in the door of a 600 mm wide enclosure. In such a case, the enclosure door could no longer be closed.
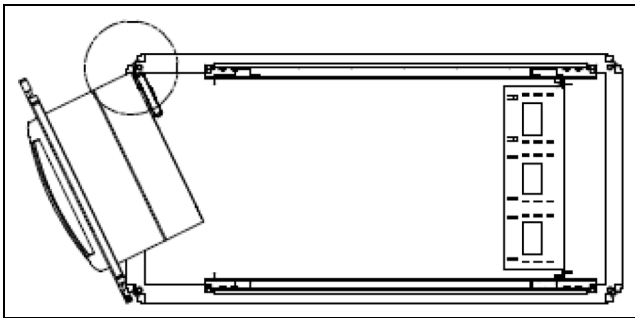
Fig. 4:   Collision for a 600 mm wide enclosure

5.4   Electrical connection

⚠ **Warning!**
The unit is free from power only after all power sources have been disconnected!

The use of open wiring (24 V direct connection) is permitted only when the IoT interface is installed in an area with restricted access.

The wiring must be protected against possible misuse.

In general, there are two ways of supplying the IoT interface with the required operational power:
1.   Direct 24 V connection
2.   Connection to a Blue e+ cooling unit
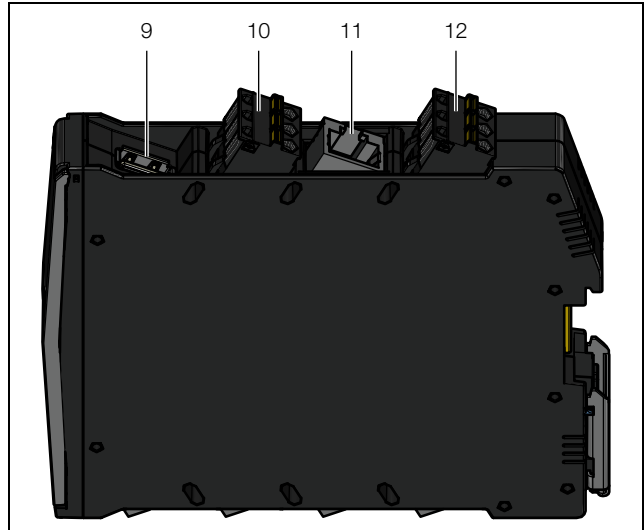
Fig. 5:   Top connections on the IoT interface

Legend
9   USB-host connection
10   Connection of an external temperature sensor
11   Ethernet interface, RJ 45
12   24 V $=$ power supply (direct connection)
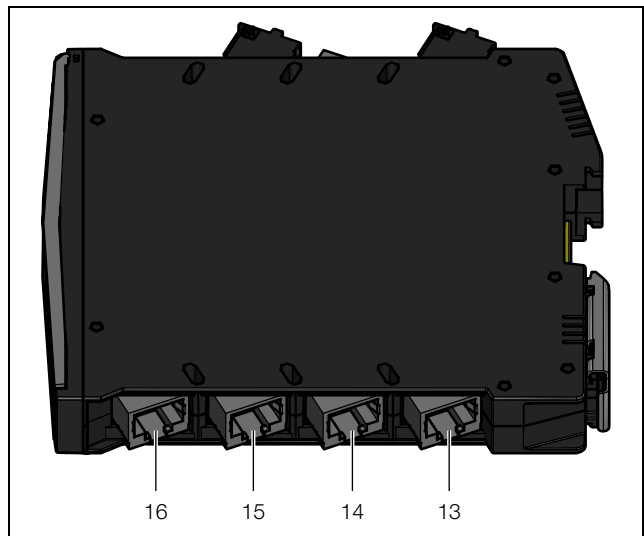
Fig. 6:   Bottom connections on the IoT interface

Legend
13   Rittal cooling unit 2 connection (climate control unit / chiller of the Blue e+ series or climate control unit with e-Comfort controller)
14   Rittal cooling unit 1 connection (climate control unit or chiller of the Blue e+ series)
15   CAN bus connection 2 (daisy-chain) for CMC III sensors or Smart Monitoring System
16   CAN bus connection 1 (daisy-chain) for CMC III sensors or Smart Monitoring System

☞ Note:
For the interconnection of climate control units with e-Comfort controller, the accessory article "Blue e IoT adaptor" (3124.310) is required in addition to the IoT interface.

* Climate control unit with e-Comfort controller

– 3273.5xx   – 3361.5/6xx
– 3303.5/6xx   – 3366.5/6xx
– 3304.5/6xx   – 3377.5/6xx
– 3305.5/6xx   – 3382.5/6xx
– 3307.7xx   – 3383.5/6xx
– 3310.7xx   – 3384.5/6xx
– 3328.5/6xx   – 3385.5/6xx
– 3329.5/6xx   – 3386.5/6xx
– 3332.5/6xx   – 3387.5/6xx
– 3359.5/6xx

Note:
The power supply to the IoT interface must not be disconnected while it is booting.

The start of the IoT interface takes approx. 1 minute. The status display flashes irregularly during this time. The device is then operational.

5.4.1 Direct connection

Warning!
Ensure that adequate clearance and reliable touch-hazard for all conductors are provided.

You can connect the IoT interface directly to the external power pack using the terminal connector.
■ To do this, connect the 24 V output (direct connection) on the power pack (DK 7030.060) to the appropriate connection of the IoT interface (fig. 5, item 12).

0.2…2.5 mm² (24…13 AWG)

7 mm
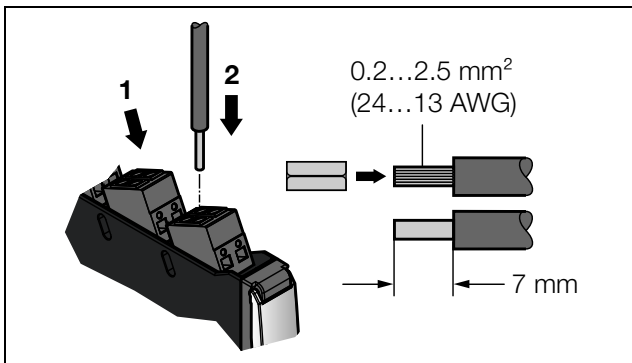
Fig. 7:   Direct connection on the IoT interface

■ Observe the pin assignment of the connection.
■ Also observe the pin assignment of the power pack (DK 7030.060). This is contained in the associated documentation.

5.4.2 Connection to a Blue e+ cooling unit

Rather than via the direct connection and an external power supply unit, you can also supply the IoT interface with the required operating voltage from a Blue e+ cooling unit connected at connection X6 (fig. 6, item 14).

Note:
The cable length between the IoT interface and the connected device must not exceed 10 m.

■ Connect connection X6 for a Rittal cooling unit with the interface of a Blue e+ cooling unit or a Blue e+ chiller.

Note:
If the electrical connection is **not** made to the direct connection, no second cooling unit can be attached to connection X5 (fig. 6, item 13) and no components (such as CMC III sensors or the Smart Monitoring System) can be connected to the CAN bus connections.

5.5 Connection of the external temperature sensor (optional)

■ If necessary, attach the external temperature sensor 3124.400 to the appropriate connection of the IoT interface (fig. 5, item 10).
■ Then route the external temperature sensor to the required measuring point.

Note:
The external temperature sensor must be connected before the IoT interface is started. If the external temperature sensor is connected during running operations, the IoT interface must be restarted so that the external temperature sensor is detected and used.

5.6 Network connection

The network connection establishes the connection to the network.
■ Connect the Ethernet interface (fig. 5, item 11) using a network cable with an RJ 45 connector to the existing network structure.

After connecting the network cable, the right Ethernet interface LED at the front of the IoT interface illuminates continually. The left LED also flashes during data transfer (see section 6.3.2 "Displays of the LEDs Ethernet interface").

5.7 Connection of sensors

A wide range of sensors, actuators and systems for access monitoring (see section 15 "Accessories") can be connected to the two CAN bus interfaces (fig. 6, item 15 and 16).

Note:
The total cable length of a CAN bus must not exceed 50 m.

5 Installation

■ For example, connect a sensor from the accessories range with a CAN bus interface of the IoT interface using a CAN bus connection cable.

The following CAN bus connection cable from the accessories range can be used:

– DK 7030.090 (length 0.5 m)
– DK 7030.091 (length 1 m)
– DK 7030.092 (length 1.5 m)
– DK 7030.093 (length 2 m)
– DK 7030.480 (length 3 m)
– DK 7030.490 (length 4 m)
– DK 7030.094 (length 5 m)
– DK 7030.095 (length 10 m)

Further components are connected as daisy chain.

■ If necessary, connect another component (e.g. another sensor type) to the second, free CAN bus interface of the first component.

■ Proceed similarly for further components.

The IoT interface automatically detects each connected sensor. After connection of the sensor, the status display of the multi-LED at the front of the IoT interface changes appropriately. The CAN bus connection LED display at the front also changes (see section 6.3.3 "Displays of the LEDs CAN bus connection").

> **Note:**
> If a sensor is added subsequently, it may have a newer firmware than the IoT interface supports. In this case, the IoT interface does not detect the sensor; the IoT interface must be updated first.

> **Note:**
> Further information concerning the connection of sensors is contained in the associated documentation of the accessory part.

6 Commissioning

6.1 Switching on the IoT interface

Once the electrical connection has been established, the IoT interface starts automatically (see section 5.4 "Electrical connection"). A separate switch-on is not required.

6.2 Operating and display elements
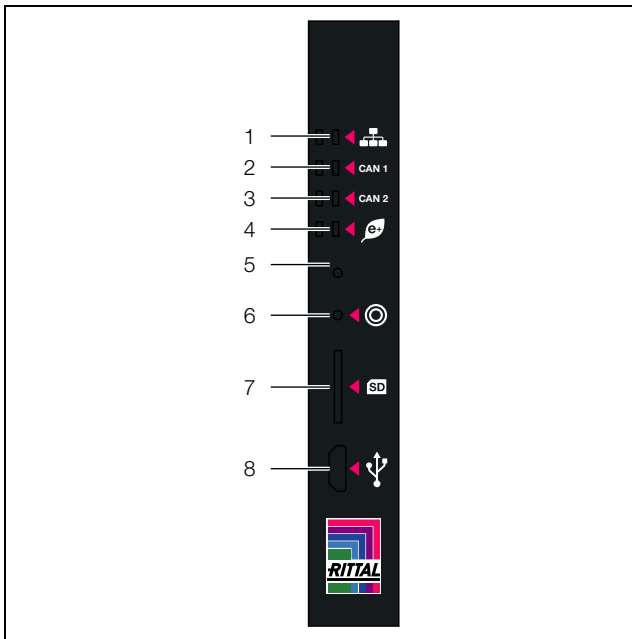
Fig. 8: Front of the IoT interface

Legend
1 Network traffic LEDs
2 CAN bus connection 1 LEDs
3 CAN bus connection 2 LEDs
4 LED data transmission climate control units (left) / multi-LED for status display (right)
5 Hidden reset key
6 Push-button for acknowledging alarms and messages
7 microSD card slot
8 Micro-USB connection for configuring

6.3 Displays of the LEDs

Various LEDs are located at the front of the IoT interface, such as for the status display and for the data transfer in the network or to the connected cooling units.

6.3.1 Multi-LED displays

Continuous lighting of the multi-LED indicates the status of the IoT interface and of the connected components.

Colour	Status
Green	All units attached and also the IoT interface have the "OK" status.
Orange	At least one unit attached to the CAN bus has the "warning" status.

Tab. 1: Continuous lighting of the multi-LED

Colour	Status
Red	At least one unit attached to the CAN bus has the "alarm" status.

Tab. 1: Continuous lighting of the multi-LED

The flashing code of the multi-LED indicates a status change of the IoT interface:

Colour	Status
Cyclically green – orange – red	At least one new device was detected on the CAN bus ("Detected" status).
Alternating red – blue	At least one device has been removed from the CAN bus or can no longer be detected over the CAN bus ("Lost" status).
Blue	The position on the CAN bus has been changed for a device ("Changed" status).
Red	Update task running (so-called heartbeat, alternating long and short).
White	Update task running for one or more sensors.

Tab. 2: Flashing codes of the multi-LED

6.3.2 Displays of the LEDs Ethernet interface

A Link and a Traffic LED for the Ethernet interface are provided at the front of the IoT interface; they indicate the status of the network connection.

LED	Status
Link (continuous light)	For 10 Mbit/s and 100 Mbit/s, the LED illuminates green; for 1000 Mbit/s, the LED illuminates orange.
Traffic (flashing light)	For 10 Mbit/s and 100 Mbit/s, the LED flashes green; for 1000 Mbit/s, the LED flashes orange.

Tab. 3: LEDs for the Ethernet interface

6.3.3 Displays of the LEDs CAN bus connection

A red and a green LED for each of the CAN bus connections 1 and 2 are provided at the front of the IoT interface; they indicate the status of the CAN bus.

Colour	Status
Green (continuous light)	Communication over the CAN bus possible.
Red (flashing)	Transfer error or no CAN bus node connected.

Tab. 4: LEDs for the CAN bus connection

6.3.4 Cooling unit data transfer LED displays

An LED for the data transfer from the cooling units is provided at the front of the IoT interface. It displays the status of the data transfer.

Colour	Status
Green (flash-ing)	Data transfer from cooling unit 1 (fig. 6, item 14)
Red (flash-ing)	Data transfer from cooling unit 2 (fig. 6, item 13)
Yellow (flash-ing)	Simultaneous data transfer from cooling units 1 and 2

Tab. 5:   Cooling unit data transfer LEDs

6.4 Acknowledgement of messages

There are generally three ways of acknowledging messages:

1. By briefly pressing the appropriate push-button (fig. 8, item 6) on the IoT interface (circle symbol). This confirms all alarm messages concurrently.
2. Via a HTTP connection by selecting a message with the right mouse button in the message display and clicking on the "Acknowledge Alarm" or "Acknowledge Devices" entry with the left mouse button in the context menu.
   If an alarm message has been selected, "Acknowledge Alarm" confirms only the currently selected message.
   If a message concerning a configuration change has been selected, "Acknowledge Devices" confirms all related messages jointly.
3. Via a HTTP connection by clicking with the right mouse button on a component entry and clicking with the left mouse button on the "Acknowledge Alarm" or "Acknowledge Devices" entry in the context menu.
   This can be used to confirm pending alarm messages for that particular component or all configuration changes.

7 Configuration

7.1 General

The base configuration of the IoT interface, in particular the (one-off) customisation of the network settings, can be performed in several ways:

1. HTTP connection via the Ethernet interface
2. Telnet connection via the Ethernet interface
3. Serial connection via the supplied USB cable

An HTTP connection is normally used to make the settings. If this is not possible, e.g. because access via HTTP or HTTPS has been deactivated, access via a Telnet connection is recommended. To do this, as for access using an HTTP connection, the IP address of the IoT interface must be known. If this address is not known, a direct access to the device can be made using the USB/serial interface at the front of the device.

The following descriptions assume that the IoT interface is in its delivered state, i.e. no changes have been made to the base configuration. In particular, the "HTTP" and "Telnet" connection types must not be blocked.

7.2 HTTP connection

7.2.1 Network connection with DHCP

As standard, automatic IP assignment is activated for the IoT interface ("DHCPv4" setting is activated).

■ Establish a connection to the network via the Ethernet interface of the IoT interface (see section 5.6 "Network connection").
■ Read the IP address assigned to the IoT interface by connecting via the USB interface. (see section 7.4 "USB/serial connection").
■ For climate control units or chillers of the Blue e+ series: Read the IP address on the display of the connected unit (Configuration > Network > Network info > IPv4).

Note:
If the device was inadvertently assigned a network address per DHCP, disconnect the device from the power supply. After reconnection, the default initialised address 192.168.0.190 is stored again.

7.2.2 Network connection without DHCP

If the IoT interface is not assigned dynamically any IP address via DHCP, the **192.168.0.190** address is preset.

■ Connect the device with a network cable using the Ethernet interface to your computer (fig. 6, item 11).

Note:
Depending on which computer is used, you may need to use a cross-over cable for this purpose.

■ Change the IP address of your computer to any address in the range 192.168.0.xxx, e.g. **192.168.0.191**. The default address **192.168.0.190** of the device must not be used.
■ Set the subnet mask to the value **255.255.255.0**.
■ If necessary, switch off the proxy server in the browser in order to permit a direct connection to the device.

7.2.3 Access to the IoT interface website

■ Enter the IP address in the browser (fig. 9, item 1). The login dialogue to log in to the device will be displayed.
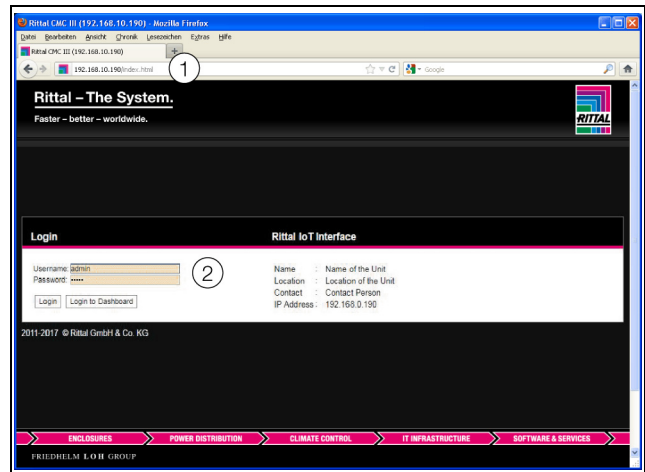
Fig. 9: Login page for an HTTP connection

■ Login as **admin** user with password **admin** (fig. 9, item 2).
■ Click the **Login** button to display the website of the device.

The overview page of the device appears (fig. 10).

Note:
Alternatively, you can also login to a dashboard directly from the login screen by clicking the **Login to Dashboard** button (see section 8.14.4 "Calling a dashboard").

7.2.4 Changing the network settings

Note:
The network settings need to be changed only when the IoT interface is integrated in the network structure **without** DHCP.

To integrate the IoT interface in your existing network structure, you can customise the network settings appropriately.

■ Click the **Processing Unit** entry in the left-hand subarea (navigation area) of the overview window (fig. 10, item 3) and the **Configuration** tab in the right-hand subarea (configuration area) (fig. 10, item 4).
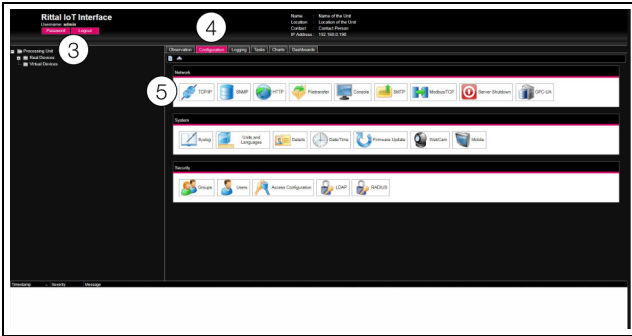
Fig. 10: Customising the TCP/IP settings

■ Click the **TCP/IP** button in the **Network** group frame (fig. 10, item 5).
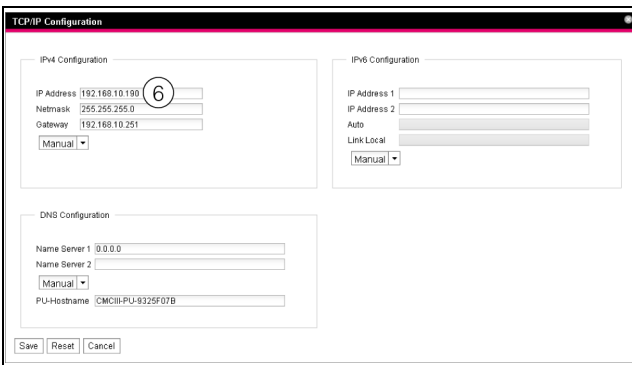
Fig. 11: Customising the TCP/IP settings

☞ Note:
The following sections describe in detail how to make the setting for the IPv4 protocol. Further notes regarding the TCP/IP configuration are contained in section 8.5.1 "TCP/IP Configuration".

■ Select the "Manual" setting rather than "DHCPv4" for a manual IP assignment.
■ Change the IP address of the device in the **TCP/IP Configuration** window in the **IPv4 Configuration** group frame to an address permitted in the network (fig. 11, item 6).
■ If necessary, set the correct net mask and gateway.
■ Click the **Save** button to save the settings.

☞ Note:
If the **Save** button cannot be clicked, an incorrect input has been made (see section 8.2.5 "Other displays"). In this case, first check and possibly correct your inputs.

■ Change the network settings of your computer to their original values of the IP address and the subnet mask.
■ Disconnect the network cable to your computer.
■ Establish a connection to the network via the Ethernet interface of the IoT interface (see section 5.6 "Network connection").

7.2.5 Configuration

All other possible IoT interface settings are described in section 8 "Operation".

7.3 Telnet connection

For a Telnet connection, the Telnet client can be used under Windows 7 and Windows 10. However, the client may need to be installed first ("Control Panel" > "Programs" > "Activate or deactivate Windows functions"). Alternatively, a suitable utility program, such as "PuTTY", can be used.

The following description assumes that a direct connection between a computer and the IoT interface is established. In this case, the same work steps as for an HTTP connection without DHCP are then required (see section 7.2.2 "Network connection without DHCP").

If the connection is established via a network with DHCP, the IP address 192.168.0.190 in the following description must be replaced with the address assigned dynamically to the IoT interface (see section 7.2.1 "Network connection with DHCP").

7.3.1 Establishing the connection

The following sections first describe establishing a connection using the Telnet client.

■ Enter the command "telnet 192.168.0.190" in the "Start" > "Search programs or files" (Windows 7) or directly in the "Search Windows" field (Windows 10). The login page appears.
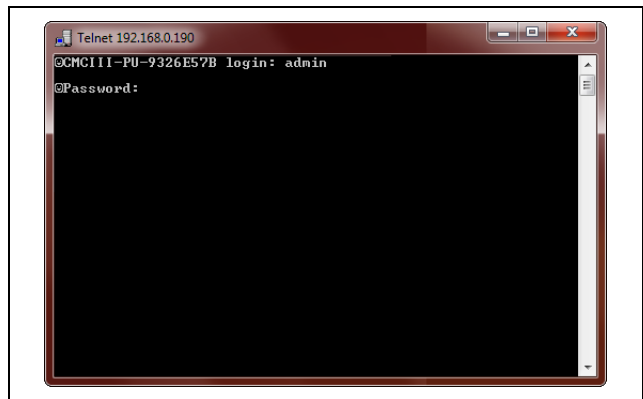
Fig. 12: Login page

Make the settings shown in the following screenshot for the "PuTTY" utility program.
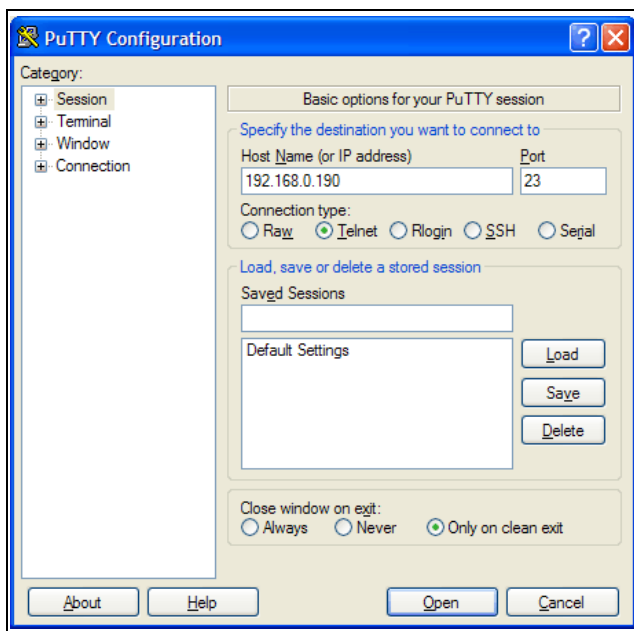
Fig. 13:   "PuTTY" connection setting

7.3.2   Changing the network settings

The changing of the network settings is described in section 7.5.4 "Input of values", example 1.

7.4   USB/serial connection

The access via the USB interface under Windows requires that an appropriate driver for the IoT interface is installed first. This driver can be downloaded from the Internet page specified in section 17 "Customer service addresses".

☞ Note:
For the driver installation under Windows 10, the driver signature must first be deactivated.

7.4.1   Determining the connection port

After the installation of the driver, a check must be made in the Control Panel to determine on which COM port the IoT interface was installed.

■ Start the Device Manager ("Control Panel" > "System" > "Hardware" > "Device Manager").
■ Expand the "Connections (COM and LPT)" entry.
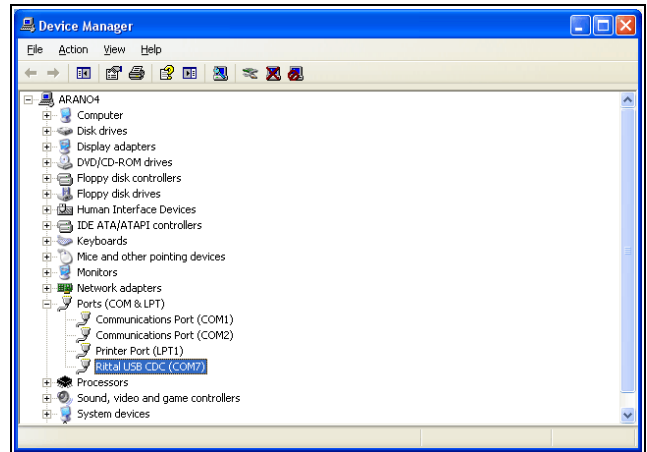
Fig. 14:   Device Manager

After the installation of the driver, the COM interface to which the IoT interface is connected is displayed.
■ Note the number of the COM port.

☞ Note:
Always connect the IoT interface to the same USB connection of your computer. If not, you will be requested to reinstall the driver and you must also specify the COM interface again.

7.4.2   Establishing the connection

A description how to establish a connection using the "PuTTY" utility program follows.
■ Start the "PuTTY" program.
■ Select the "Serial" entry for "Connection Type".
■ Then enter the COM port in the "Serial line" field that you specified previously as connection port, e.g. "COM7".
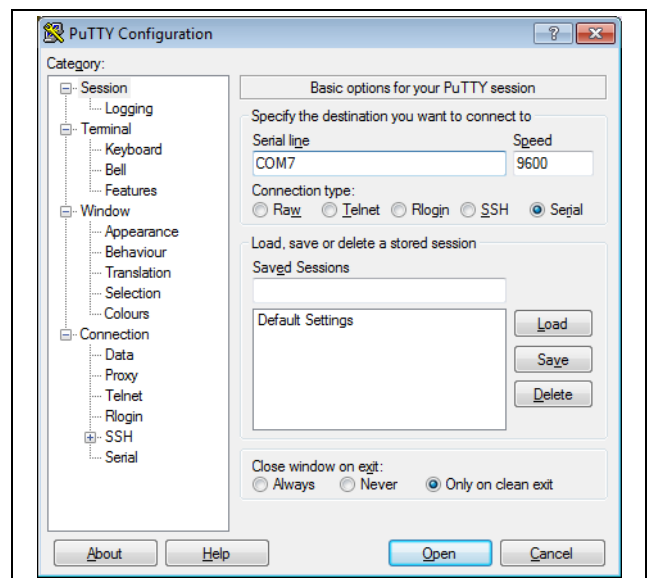
Fig. 15:   Connection setting "CMC III PU USB"

■ Select the following settings at "Connection" > "Serial":
Bits per second: 9600

Data bits: 8
Stop bits: 1
Parity: No
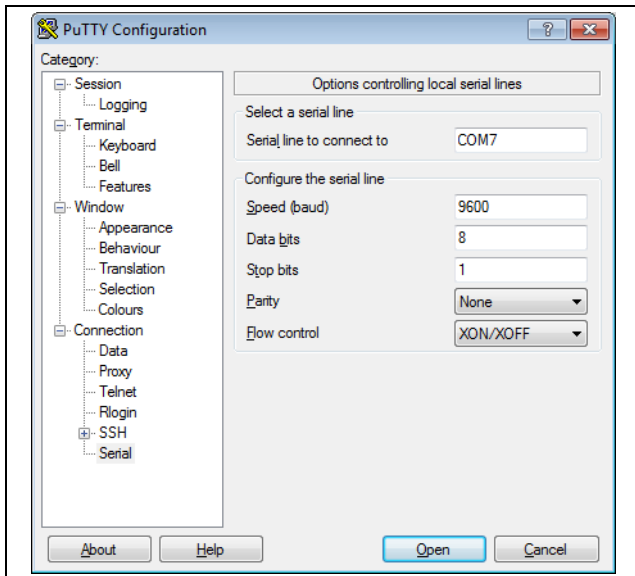
Fig. 16:   COMX properties

■ Click the **Open** button to establish the connection.
■ Press the "Return" key once to display the login page. This corresponds to the login page for a Telnet connection (fig. 12).

7.4.3   Changing the network settings
Changing of the network settings is described in section 7.5.4 "Input of values", example 1.

7.5   Basic settings
The following descriptions apply to access via "Telnet" or "USB/serial". Access via the IoT interface website is described in section 8 "Operation".

7.5.1   Login to the IoT interface
Once the connection has been established, the login page appears.
■ Enter in the line **[Hostname] login:** _ the user name.

☞ Note:
Rather than the placeholder [hostname], the host name of the IoT interface stored for the login is displayed.

■ Enter in the line **Password:** _ the associated password.

☞ Note:
The user "admin" with the password "admin" and the user "user" with the password "user" are stored as factory settings.

■ If necessary, press the "Return" key once. The **Main Menu** appears.
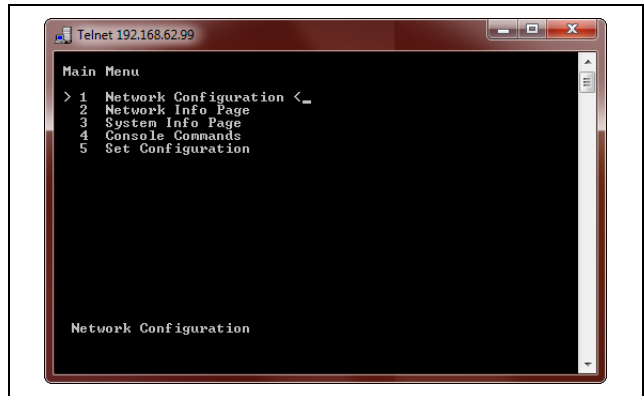
Fig. 17:   Main Menu

7.5.2   Menu structure
A Telnet or USB/serial connection can be used to make the base settings of the IoT interface using the following menu structure:

1	Network Configuration		
	1	IPv4 Configuration	
		1	IPv4 Address
		2	IPv4 Subnet mask
		3	IPv4 Gateway
		4	Enable/Disable DHCPv4
	2	IPv6 Configuration	
		1	IPv6 Address 1
		2	IPv6 Address 2
		3	IPv6 Configuration
	3	DNS Configuration	
		1	DNS Primary Server
		2	DNS Secondary Server
		3	DNS Mode
		4	Hostname
	4	LDAP Configuration	
		1	LDAP Server
		2	Enable/Disable LDAP
	5	Radius Configuration	
		1	Radius Server
		2	Enable/Disable Radius
	6	Modbus/TCP Configuration	
		1	Change Server Port
		2	Enable/Disable Modbus/TCP

	7	Settings Ethernet Port
	8	System Name
	9	System Contact
	A	System Location
	B	Actual Date
	C	Actual Time
	D	Beeper
	E	Security
		1	Change User Password
		2	Enable Web Access
		3	Change HTTP Port
		4	Change HTTPs Port
		5	Enable FTP access
		6	FTP Port
		7	Enable SSH access
		8	SSH Port
		9	Enable Telnet access
		A	Telnet Port
	F	SNMP Configuration
		1	Enable SNMP V1 & V2
		2	Read Community
		3	Write Community
		4	Trap Community
		5	Enable SNMP V3
	G	Reboot Unit
2	Network Info Page
3	System Info Page
4	Console Commands
	1	Command (by DescName)
	2	Command (by VariableName)
5	Set Configuration
	1	Set General Configuration to Default
	2	Set all Tasks to Default
	3	Set all Charts to Default

☞ Note:
The "D: Beeper" menu item has no function for the IoT interface.

You can also use the IoT interface website to access most of the parameters that can be accessed using the Telnet or USB/serial connection. Consequently, the associated descriptions are contained in section 8 "Operation". Only the few settings not available from the website are described in section 7.5.5 "Special settings and notes".

7.5.3 Navigating in the menu structure
The individual menu items are selected with the associated number shown before each menu item.
Starting at the **Main Menu**, for example, it is possible to select the following three submenus:
– Key "1": **Network Configuration** submenu
– Key "2": **Network Info Page** submenu
– Key "3": **System Info Page** submenu
– Key "4": **Console Commands** submenu
– Key "5": **Set Configuration** submenu
Alternatively, you can use the "arrow" keys, the "Return" key and the "Esc" key to navigate through the menus.

7.5.4 Input of values
The stored parameter values are displayed within pointed brackets, ">" and "<", at the end of each line. To change a value, similar to navigating in the menu structure, select the appropriate parameter using the associated number. To accept a changed value, you must always press the "Esc" key.

Example 1: Changing the network settings for IPv4
■ In the **Main Menu**, press key "1" to select the **Network Configuration** submenu.
■ Press key "1" again to select the **IPv4 Configuration** submenu.
■ Press key "1" again to select the **IPv4 Address** parameter.
■ Clear the default address stored there and enter instead a valid network address.
■ Press the "Return" key to confirm the input.
The entered address is displayed accordingly at the end of the line.
■ Press the "Esc" key to exit the **IPv4 Configuration** menu.
If the access to the device was made via Telnet, changing the IP address means that initially no further communication via the telnet client is possible.
■ First terminate the current connection.
■ Establish a new connection with the changed IP address.

Example 2: Changing the name of the contact person

■ In the **Main Menu**, press key "1" to select the **Network Configuration** submenu.
■ Press key "9" to select the **System Contact** parameter.
■ Enter the appropriate name of the contact person, e.g. **Contact person IoT interface**.
■ Press the "Return" key to confirm the input.
The entered name is displayed accordingly at the end of the line.
■ Press the "Esc" key again to exit the **Network Configuration** menu.

Note:
If after changing a value you switch to another submenu, the value is **not** accepted.

7.5.5 Special settings and notes

The following settings are not available over the website but only over a Telnet or USB/serial connection.

Parameter	Explanation
Settings Ethernet Port	Set the transmission speed and the duplex procedure or the Autonegotation for the network interface of the IoT interface.
Set General Configuration to Default	Reset all IoT interface settings to the factory settings.
Set all Tasks to Default	Reset all tasks to the delivered state (empty).
Set all Charts to Default	Reset all charts to the delivered state (empty).

Tab. 6:   Special settings

If you select the **Automatic DHCP** value via a Telnet or USB/serial connection for the **DNS Mode** parameter in the **DNS Configuration** submenu, observe the following notes:
■ Set the **Enabled** value for the **Enable/Disable DHCPv4** parameter in at least one of the **IPv4 Configuration** or **IPv6 Configuration** submenus.
■ Alternatively or additionally, set in the **IPv6 Configuration submenu** the **DHCPv6** value for the **IPv6 Configuration** parameter.
■ Under no circumstances deactivate DHCP for **both** IPv4 and IPv6 protocols after you have made the above-mentioned DNS configuration.

7.5.6 Performing switch commands

A user with administration rights can use a Telnet connection to switch the outputs for sensors connected to a IoT interface (e.g. the slots of a switchable PSM module).

■ In the **Main Menu**, press key "4" to select the **Console Commands** submenu.

You can now trigger an output using either the name (DescName) assigned to the relay output or the complete variable name.

Note:
The following representation shows a selection from the website and serves only as explanation of the "DescName", "VariableName" and "Command" terms.
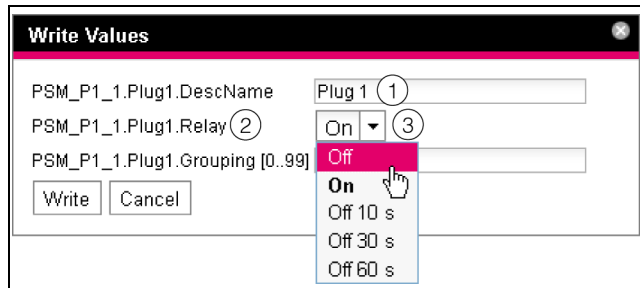
Fig. 18:   Performing switch commands

Key
1   DescName
2   VariableName
3   Command

Switching using the assigned name
■ Press key "1" to select the **Command (by Desc-Name)** command.
■ Enter the command in the "Device.DescName:Command" format.

Parameter	Explanation
Device	The device index (ID number) that is prefixed to the associated Real Device in the navigation area of the IoT interface website.
DescName	The specific description that was assigned to the output or the socket (fig. 18, item 1).
Command	The command to be performed. The following commands are supported: "Off", "On", "Off 10 s", "Off 30 s", "Off 60 s" (fig. 18, item 3).

Tab. 7:   Parameter (switch using the assigned name)

■ Press the Return key to confirm the input (e.g. "3.Plug 1:Off").

If the switching command could be performed, an appropriate message will be displayed (e.g. "Device 3.Output 'Plug 1' switched to 'Off'"). If an error occurred, an error message will be displayed (e.g. "Device 3 not available").

Switching using the complete variable name
- Press key "2" to select the **Command (by Variable-Name)** command.
- Enter the command in the "Device.Variable-Name:Command" format.

Parameter	Explanation
Device	The device index (ID number) that is pre-fixed to the associated Real Device in the navigation area of the IoT interface website (fig. 18, item 2).
Variable-Name	The variable name of the output or the socket that consists of three components each separated with a period.
Command	The command to be performed. The following commands are supported: "Off", "On", "Off 10 s", "Off 30 s", "Off 60 s" (fig 18, item 3).

Tab. 8:   Parameter (switch using the complete variable name)

- Press the Return key to confirm the input (e.g. "3.PSM_P1_1.Plug1.Relay:Off").

If the switching command could be performed, an appropriate message will be displayed (e.g. "Device 3.Output 'PSM_P1_1.Plug1.Relay' switched to 'Off'"). If an error occurred, an error message will be displayed (e.g. "Device 3 not available").

7.5.7   Logout from the IoT interface
Once you have performed all required settings on the IoT interface, logout again. To do this:
- Press the "Esc" key repeatedly until you return to the **Main Menu**.
- Press the "Esc" key again. The following message appears at the lower screen edge:
  Logout? [Y = Yes]
- Press the "Y" key to log out.
- Press any other key if you do not want to log out.

8 Operation

8.1 General

The following sections describe all settings made available via an HTTP gateway.

☞ **Note:**
If the IoT interface is deployed in an environment subject to high EMC loading, parts of the website may be displayed incorrectly. In such a case, reload the website from the browser.

8.2 General operation

8.2.1 Screen structure

After login to the IoT interface (see section 7.2.3 "Access to the IoT interface website"), the web user interface for operation of the device is displayed. The screen is generally divided into four different areas:

1. Upper area: Display of general information about the device, change of the password and logout of the current user (see section 8.2.8 "Logout and changing the password").
2. Left-hand area (navigation area): Selection of the complete system or the associated component for which the information should be shown in the right-hand area of the screen (see section 8.2.2 "Navigation area in the left-hand area").
3. Right-hand area (configuration area): Display of six tabs (see section 8.2.3 "Tabs in the configuration area") with input possibilities for all settings.
4. Lower area: Display of messages (see section 8.2.4 "Message display").
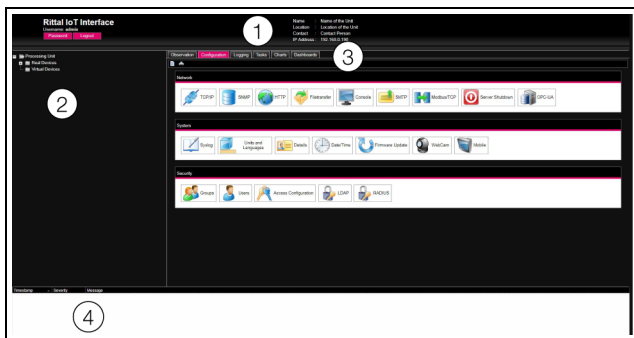
Fig. 19: Screen structure

Key
1 General information
2 Navigation area
3 Configuration area with tabs
4 Message display

8.2.2 Navigation area in the left-hand area

The complete system, including all installed components, is displayed as a tree view in the navigation area of the screen.

The Processing Unit, i.e. the complete system, is located at the top of the navigation area. Two subgroups are displayed below the complete system.

1. Real Devices: This group lists the IoT interface itself as well as all hardware-installed devices and sensors.
2. Virtual Devices: This group displays all virtual devices that were created in the IoT interface.

☞ **Note:**
A detailed description for the "Virtual Devices" topic can be found in the separate "Tasks And Virtual Devices" document.

Each device, irrespective of whether it is a real device or a virtual device, can assume various states. To quickly determine the current status, the symbol in front of the associated device is colour-highlighted:

Symbol	Explanation
	"OK" status. No warning or alarm messages are pending.
	"Warning" status. At least one warning message is pending.
	"Alarm" status. At least one alarm message is pending.
	"OK" status. The additional information flag indicates that additional status information can be displayed. This symbol is displayed only when the logged on user has at least read access to the data of the associated device (see section 8.8 "Device Rights").
	"Detected" status. The sensor has been newly added, but has not yet been confirmed. This sensor must still be confirmed by pressing the push-button to acknowledge alarms and messages on the IoT interface (circle symbol) or via the website.
	"Lost" status. The communication to a sensor is no longer possible. The connection must be checked. Alternatively, the sensor can also be deactivated by confirmation.
	"Changed" status. The sequence of the sensors has been changed, but has not yet been confirmed. This configuration change must still be confirmed by pressing the push-button to acknowledge alarms and messages on the IoT interface (circle symbol) or via the website (see section 6.4 "Acknowledgement of messages").

Tab. 9: Symbols for the status display

8.2.3 Tabs in the configuration area

Four tabs are displayed in the right-hand area of the screen:

1. Observation: The current data of the IoT interface or the connected devices (see section 8.3 "Observation tab").
2. Configuration: Configuration of the basic settings (see section 8.4 "Configuration tab").
3. Logging: The message archive for the IoT interface or the connected devices (see section 8.11 "Logging").
4. Tasks: Creation of the links for various values and the associated actions (see section 8.12 "Tasks").
5. Charts: Charts for the chronological trend of the variable values (see section 8.13 "Charts")
6. Dashboards: Creation of different views as dashboards (see section 8.14 "Dashboards").

The content of the **Observation** and **Configuration** tabs depends on whether the complete system ("Processing Unit" entry) or a single component, e.g. the "IoT interface" entry, has been selected in the left-hand area of the screen.

8.2.4 Message display

Currently pending messages are displayed in the lower area of the screen. The message display has the following structure:

1. Timestamp: Date and time when the error occurred (fig. 20, item 1).
2. Severity: The severity of the error that has occurred. A differentiation is made between warnings and alarms (fig. 20, item 2).
3. Message: Error message in plain text (fig. 20, item 3).
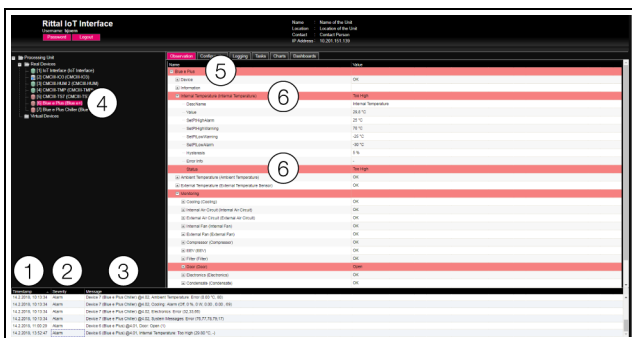
Fig. 20:   Structure of the message display

Key
1   Date and time
2   Error class
3   Error message in plain text
4   Component with error message
5   Component
6   Parameter

The occurred errors are also displayed as follows:
– Left-hand screen area (navigation area): The symbol in front of the component on which the error occurred is colour-highlighted (red for an alarm, yellow for a warn-

ing; fig. 20, item 4).
– Right-hand screen area (configuration area): The complete component as well as the special parameters for which the warning or alarm is pending is coloured red or yellow on the **Observation** tab (fig. 20, item 5 and 6).
– The multi-LED on the front of the IoT interface lights continually red or orange.

Once the cause of an error message has been corrected, the associated message can be deleted automatically from the message display. The status of the associated component can also be reset and all other displays caused by the error can disappear. This, however, depends on the selected alarm configuration (see section 8.9 "Alarm Configuration"). In some cases, error messages and the status may also remain in the overview until they have been acknowledged by pressing the push-button to acknowledge alarms and messages on the IoT interface (circle symbol) (see section 6.4 "Acknowledgement of messages").

If a permanent configuration change is made on the device, e.g. a new sensor connected to the IoT interface, it will also be output as error message of the "Alarm" type in the message display. In this case, the multi-LED in the front of the IoT interface flashes cyclically green – orange – red. Such a configuration change is deleted from the message display only when it has been confirmed by the operator (see section 6.4 "Acknowledgement of messages").

Example: Excessive temperature value
If a temperature measured for the air drawn from the enclosure at a cooling unit attached to the IoT interface exceeds the stored "SetPtHighAlarm" value, an alarm message is issued.

In this case, the following changes occur in the representation:
– The symbol in front of the Blue e Plus component in the navigation area is red-highlighted.
– The complete component as well as the "Internal Temperature" and "Status" lines have a red background on the **Observation** tab. The "Too High" alarm message is also issued.
– The appropriate warning message appears in the message display.

When the temperature again falls below the "SetPtHighAlarm" value plus the hysteresis value (see section 16 "Glossary"), it depends on the alarm configuration whether the message is deleted automatically from the message display and the associated status displays are reset again (see section 8.9 "Alarm Configuration").

8 Operation

8.2.5 Other displays

The operator inputs in the web user interface are checked automatically using specified rules depending on the entered parameter. This means changes can be saved only when all values have been previously entered correctly in a dialogue.
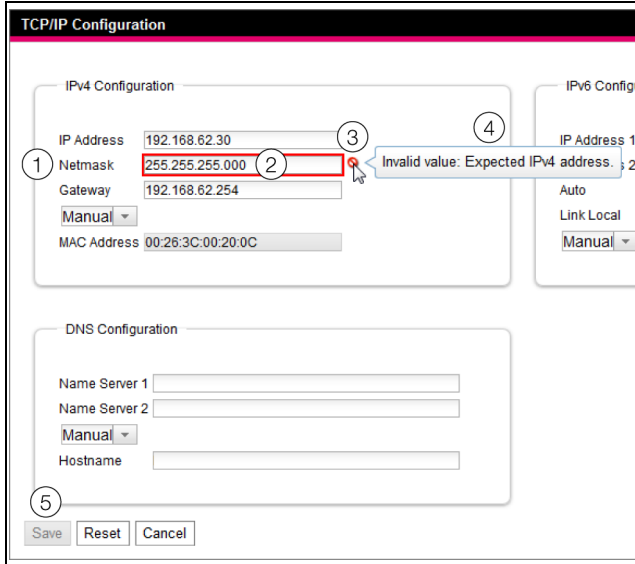
Fig. 21: Display of an incorrect input

Key
1 **Netmask**
2 Faulty entry
3 Prohibit symbol
4 Note:
5 Inactive button

The following changes result after an incorrect input in the dialogue (in this example, an incorrectly entered IP address):
– A red "prohibit symbol" (fig. 21, item 3) appears behind the faulty entry (fig. 21, item 2) in the field **Netmask** (fig. 21, item 1).
– When you place the mouse pointer over the prohibit symbol, a notice with additional information about the error appears (fig. 21, item 4).
– The **Save** button is deactivated (fig. 21, item 5) so that the currently stored values cannot be saved.

Proceed as follows to correct the error:
■ Check using the notice which incorrect input is present.
In the example shown, the value entered does not have the format of an IP address.
■ Correct the incorrect value; enter, for example, the value "255.255.255.0".
The "prohibit symbol" is hidden and the **Save** button is activated.
■ Click the **Save** button to save the settings.

8.2.6 Changing parameter values

The list representation of the **Observation** tab displays the various parameters of the associated selected com-

ponent. Whereas the operator can change some of these parameters, others have fixed values.
For all parameters that can be changed, an "edit" symbol in the form of a stylised notebook with pencil appears behind the associated parameter when you place the mouse cursor in the appropriate row (fig. 22, item 1).
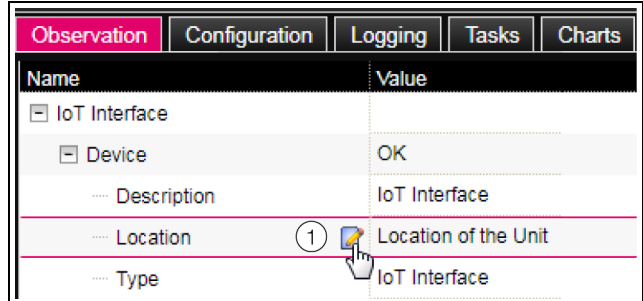
Fig. 22: Editable parameter with "edit" symbol

Key
1 "Edit" symbol

If this symbol does not appear, the associated value cannot be changed.

Example:
■ Select the "IoT interface" entry in the navigation area.
■ Click the **Observation** tab in the right-hand part of the screen.
■ Expand successively the "IoT interface" and "Device" entries by clicking the "plus" character in front of the entry (fig. 23, item 1).
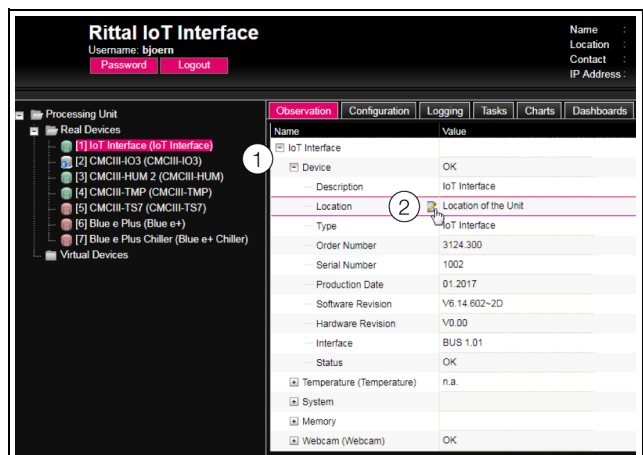
Fig. 23: Selection of a single parameter

Key
1 IoT interface and Device entries
2 "Location" parameter

■ Place the mouse cursor at the end of the first column in the "Location" row (fig. 23, item 2).
An "edit" symbol appears and the mouse cursor changes to a "hand" symbol.
■ Click the "edit" symbol.
The "Write Values" dialogue with the "Device.Location" parameter appears.
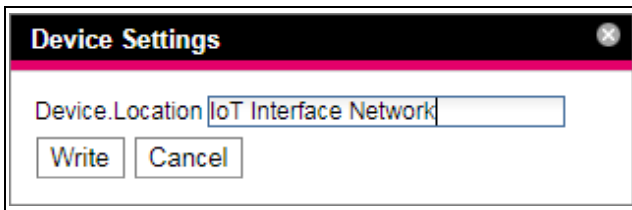
Fig. 24:   "Write Values" dialogue

■ Enter the location of the IoT interface, e.g. "IoT interface Network".
■ Confirm the entry by clicking the **Write** button.
   The dialogue closes and the new value appears in the "Location" row.
■ Now place the mouse cursor at the end of the first column in the "Type" row.
   No "edit" symbol appears, i.e. you cannot change the "IoT interface" value stored here.

Perhaps you want to change several values at once or you do not know under which entry the desired parameter is stored. In this case, you can also display in a shared window all parameter values of the lowerlevel entries to be changed.
■ Expand the "IoT interface" entry by clicking the "plus" character in front of this entry (fig. 25, item 1).
■ Place the mouse cursor at the end of the first column in the "Device" row (fig. 25, item 2).
   An "edit" symbol appears and the mouse cursor changes to a "hand" symbol.
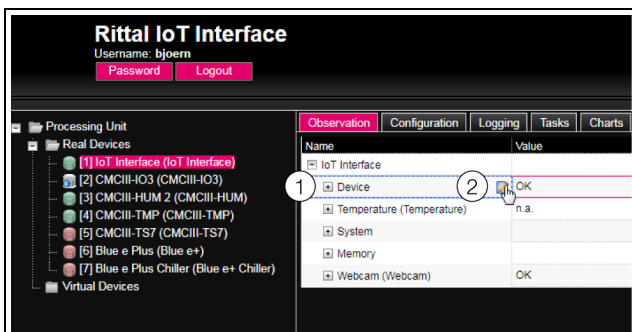
Fig. 25:   Selecting several parameters

Key
1   Device entry
2   "Edit" symbol

■ Click the "edit" symbol.
   The "Write Values" dialogue with the two "Device.Description" and "Device.Location" parameters appears.
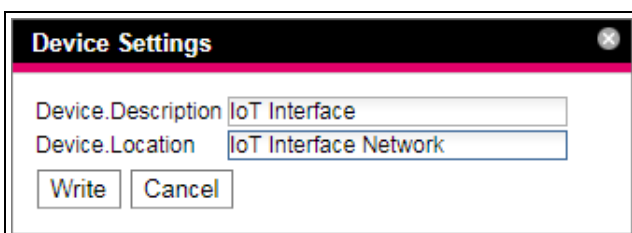
Fig. 26:   "Write Values" dialogue with several parameters

■ Save the changed values for all desired parameters.

■ Confirm the entries by clicking the **Write** button.
   The dialogue closes.
■ Expand the "Device" entry by clicking the "plus" character in front of this entry.
   You can now view all changed values.
The "Write Values" dialogue displays all the parameters that can be changed below the previously selected level. For example, if you click the "edit" symbol in the uppermost "interface IoT" level, **all** parameters that can be changed for the complete component are displayed.

☞ Note:
   If too many variables are to be changed, an error message appears. In such a case, you must switch to the next lower level.

8.2.7   Undock function
For some sensors, such as the Power Unit, a graphic overview is displayed on the IoT interface website. This overview can be remote from the current browser window and viewed in its own window.

☞ Note:
   The Undock function is not available for Internet Explorer. This button is absent.

■ Select the associated sensor, e.g. "CMCIII-POW", in the navigation area.
■ In the right-hand part of the screen, select the **Observation** tab.
■ Expand the associated entry, e.g. "CMCIII-POW", by clicking the "plus" icon in front of it.
If, after selecting the "CMCIII-POW" level, the subordinate entries "Device", "General", etc. are displayed, you can switch to the graphical representation as follows:
■ Click the coloured "graphic" icon suffixed to the "CMCIII-POW" entry in the form of a stylised chart (fig. 27).
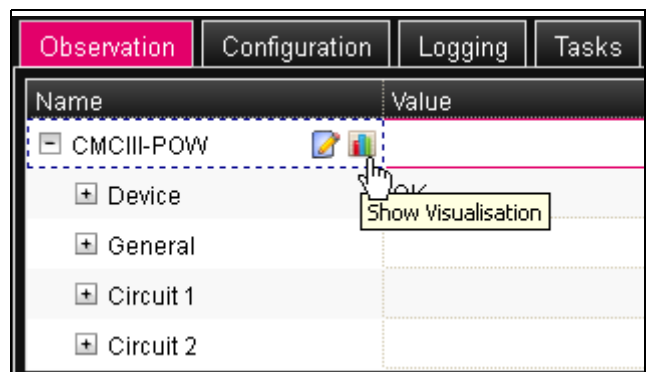
Fig. 27:   "Graphic" icon

   The display changes to the graphical representation.
■ Click the **Undock** button in the graphical representation.
   The Power Unit window is remote from the IoT interface website and the "Visualisation is undocked" message appears in the main window.

8 Operation

The remote window can be moved and altered in size independent of the window with the actual IoT interface website. This function can be used by several sensors and so a complete overview created on the PC screen.
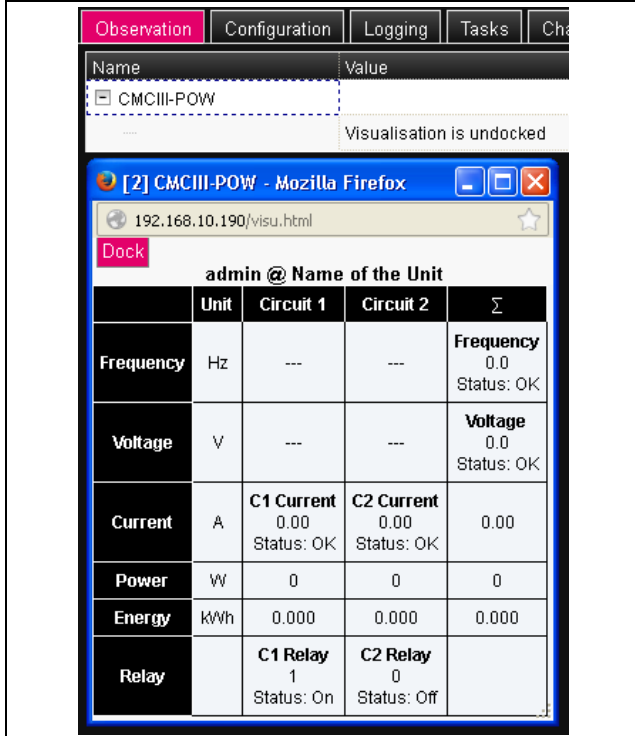
Fig. 28: Remote window of the Power Unit

■ Click the **Dock** button in the separate window or simply close the window to display the overview again in the main window.

> Note:
> If a value is in edit mode in the main window, all remote windows are darkened and no further actions can be performed there.

8.2.8 Logout and changing the password

For each user group (and thus also for each user), a time can be specified after which the user will be logged out automatically in case of inactivity (see section 8.7 "Security"). A user can, however, also logout from the web user interface.

> Note:
> After the **direct** login on a dashboard, the user is **not** logged out automatically after the predefined time. The user remains logged in to IoT interface while the dashboard is open.

■ Click the **Logout** button on the right-hand side in the upper area of the screen.
The logout is performed immediately and the Login window appears.

Users can also change their own password in the web user interface.

■ Click the **Password** button on the left-hand side in the upper area of the screen.
The "Set new password for user XXX" dialogue appears.
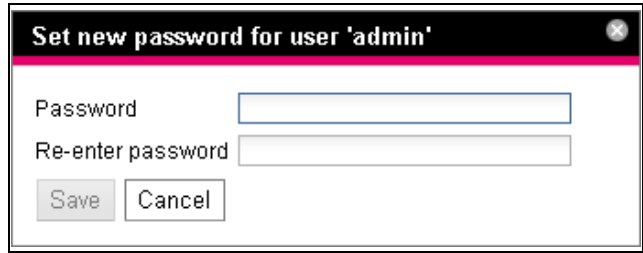
Fig. 29: Changing the password

■ Enter the new password in the "Password" line (at least three characters) and repeat it in the "Re-enter password" line.

When both entries match, you must use the new password for the next login to the system.

> Note:
> Irrespective of this change, a user with the appropriate rights can change the passwords of **all** users from the user administration (see section 8.7.2 "Users").

8.2.9 Reorganising the connected components

For the new installation of components on the IoT interface, they can be added in the navigation area at the next free location and then receive the appropriate ID number. Multiple upgrades or changes to the connected components, in particular, can mean there is no association between the position of the components on the CAN bus and the associated ID number.

The "Reorganise" function renumbers all connected components. The numbering begins with the components on CAN bus connection 1 of the IoT interface. They are then numbered in the sequence with which they are connected. Finally, all components on CAN bus connection 2 are processed similarly.

■ Click the "Processing Unit" entry in the navigation area or right-click any other connected component.

■ Left-click the "Reorganise" entry in the context menu.

A message appears stating that the reorganisation has caused the components to be reindexed. This can cause problems for the access to these components, e.g. via SNMP, so that this access must be reconfigured. The "Alarm Configuration" of the individual sensors, however, is retained.

The sensors are then registered automatically again on the IoT interface.

> Note:
> The reorganisation of the components removes, in particular, all components with the "Lost" status from the navigation area.

8.2.10 Numeric values of the states

The following table contains a list of the transferred numeric values with the associated states, for example as shown on the web user interface.

Number	Value
1	notAvail
2	configChanged
3	error
4	ok
5	alarm
6	highWarn
7	lowAlarm
8	highAlarm
9	lowWarn
10	setOff
11	setOn
12	open
13	closed
14	locked
15	unlRemote
16	doorOpen
17	service
18	standby
19	busy
20	noAccess
21	lost
22	detected
23	lowVoltage
24	probeopen
25	probeshort
26	calibration
27	inactive
28	active
29	noPower
30	readOnly
31	exchanged
32	valveOpen

Tab. 10: Numeric values and the associated states

Number	Value
33	warning
34	remote

Tab. 10: Numeric values and the associated states

8.3 Observation tab

The **Observation** tab is used to make all settings for the individual components of the system, such as limit values for warning and alarm messages. The display in the right-hand screen depends on which component was selected in the navigation area.

- If you select the "Processing Unit" (uppermost node) entry in the navigation area, the **Observation** tab, all "Real Devices" and all "Virtual Devices" are available for selection.
- If you select the "Real Devices" or "Virtual Devices" entry in the navigation area, the **Observation** tab contains only those components for selection that belong to the appropriate group.
- If you select a special component in the navigation area, e.g. the "IoT interface" entry, the **Observation** tab contains only these components for selection.

☞ Note:
It is not possible to change parameters for different components together.

In the following sections 8.3.1 "Device" to 8.3.5 "Webcam", only those parameters for which you can make changes are described in detail. There are also display values used only for information purposes.

8.3.1 Device

General settings for the IoT interface or the associated selected component are made on the "Device" level.

Parameter	Explanation
Description	Individual description of the IoT interface.
Location	Installation site of the IoT interface.

Tab. 11: Settings in the "Device" level

Parameters are also displayed that provide detailed information about the selected component, such as the version of the deployed software and hardware. You should have such information available, in particular to permit fast troubleshooting for queries with Rittal.

8.3.2 Temperature

Settings for any connected temperature sensor are performed at the "Temperature" level.

Parameter	Explanation
DescName	Individual description of the temperature sensor.
Offset	The offset value used to correct the measured temperature.
SetPtHigh-Alarm	Upper limit temperature which when overshot causes an alarm message to be issued.
SetPtHigh-Warning	Upper limit temperature which when overshot causes a warning message to be issued.
SetPtLow-Warning	Lower limit temperature which when undershot causes a warning message to be issued.
SetPtLow-Alarm	Lower limit temperature which when undershot causes an alarm message to be issued.
Hysteresis	Required percentage deviation for undershooting or overshooting of the limit temperature for a status change (see section 16 "Glossary").

Tab. 12: Settings in the "Temperature" level

The following parameters are also displayed for the temperature sensor:

Parameter	Explanation
Value	Currently measured temperature value corrected with the offset value.
Status	Current status of the sensor.

Tab. 13: Displays in the "Temperature" level

☞ Note:
If the value "0" is entered for all limit values at the "Temperature" level, the status of the temperature sensor is always "OK".

8.3.3 System

The following additional information concerning the IoT interface is displayed in the individual sublevels of the "System" level.

"CAN1 Current" and "CAN2 Current" sublevels

Settings for both CAN bus interfaces can be performed here.

Parameter	Explanation
DescName	Individual description of the associated CAN bus interface.

Tab. 14: Settings in the "CAN1 Current" and "CAN2 Current" sublevels

Parameter	Explanation
SetPtHigh-Alarm	Upper limit for the current value which when overshot causes an alarm message to be issued.
SetPtHigh-Warning	Upper limit for the current value which when overshot causes a warning message to be issued.
Hysteresis	Required percentage deviation for undershooting the limit values for a status change (see section 16 "Glossary").

Tab. 14: Settings in the "CAN1 Current" and "CAN2 Current" sublevels

The following parameters are also displayed for the CAN bus interfaces:

Parameter	Explanation
Value	Currently measured current value.
Status	Current status of the CAN bus interface.

Tab. 15: Displays in the "CAN1 Current" and "CAN2 Current" sublevels

"CAN Supply" sublevel

This indicates whether the CAN bus connections X7 and X8 have a short-circuit (fig. 6, item 15 and 16).

Parameter	Explanation
DescName	Individual description of the CAN supply.

Tab. 16: Settings in the "CAN Supply" sublevel

The following parameter is also displayed:

Parameter	Explanation
Status	Current status of the CAN buses. If no short-circuit is present, the status is OK (even when the direct connection is not supplied with 24 V). Note that the status does not provide any information whether devices can be connected to the CAN bus.

Tab. 17: Displays in the "CAN Supply" sublevel

"Supply 24V" sublevel

This displays information about the supply voltage of the IoT interface supplied via the direct connection.

Parameter	Explanation
DescName	Individual description of the supply voltage.

Tab. 18: Settings in the "Supply 24V" sublevel

The following parameters are also displayed for the supply voltage:

Parameter	Explanation
Status	This indicates whether the IoT interface is supplied with voltage from the direct connection. If the device is not supplied via the direct connection, the status is set to n.a.

Tab. 19: Displays in the "Supply 24V" sublevel

"Supply Cooling" sublevel
This displays information about the supply voltage of the IoT interface supplied via a Blue e+ cooling unit connected to connection X6 (fig. 6, item 14).

Parameter	Explanation
DescName	Individual description of the associated supply voltage.

Tab. 20: Settings in the "Supply Cooling" sublevels

The following parameters are also displayed for the power supplies:

Parameter	Explanation
Status	This indicates whether the IoT interface is supplied with voltage from a Blue e+ cooling unit. If the device is not supplied with voltage from a Blue e+ cooling unit, the status is set to n.a.

Tab. 21: Displays in the "Supply Cooling" sublevels

8.3.4 Memory
At the "Memory" level, you can view information concerning the IoT interface installed external storage media (USB stick or microSD card). These storage media may have maximum 32 GB total storage capacity, must have been formatted in the FAT32 file system and are used for recording charts (see section "8.13" Charts).

"USB stick" sublevel
Information about an installed USB stick is displayed.

Parameter	Explanation
DescName	Name of the USB stick. This name is also displayed directly on the "USB stick" sublevel.
Size	Total storage capacity of the USB stick.
Usage	Used storage capacity on the USB stick as percentage of the total storage capacity.
Command	The "Eject" command signs off the USB stick from the system. It can then be removed without any data loss.

Tab. 22: Displays in the "USB stick" sublevel

Parameter	Explanation
Status	Current status of the USB stick. "OK": USB stick installed and operational. "Inactive": USB stick installed but not signed on. "n.a.": no USB stick installed. "High Warn": Warning message when more than 80% of the storage capacity is assigned. "Too High": Alarm message when more than 90% of the storage capacity is assigned.

Tab. 22: Displays in the "USB stick" sublevel

The storage medium must first be signed off from the IoT interface before the removal of an external storage medium on which chart data is stored. Alternatively, the associated charts can be deactivated manually beforehand (see section 8.13.1 "Configuring a chart").

Note:
If an external storage medium is removed directly for activated charts, this can cause loss of chart data.

"SD card" sublevel
The same information as in the "USB stick" sublevel for a USB stick is displayed for an installed SD card.
Prior to removal from the IoT interface, an installed SD card should also be signed off with the "Eject" command in order to prevent a possible loss of chart data.

8.3.5 Webcam
At the "Webcam" level, you can view previously created images or the live stream of an Axis webcam with "VAPIX version 3" API support connected in the network. The appropriate access data for this webcam must have been entered previously (see section 8.6.6 "WebCam").

Note:
A live stream **cannot** be viewed with Internet Explorer. To view the live stream with Opera Browser, the webcam password protection must be revoked.

You have a choice between two display options for the webcam:
– Tree representation: This allows targeted and fast access to individual parameters.
– Graphical display: Graphical information (such as previously created images or a live stream) is displayed.

Note:
The switching between the two display options is described in section 8.2.7 "Undock function".

In the tree representation, the following settings for the webcam are made:

Parameter	Explanation
DescName	Specific description of the webcam.
Command	The selection of the "Trigger" manually initiates the creation of the individual images.

Tab. 23: Settings at the "Webcam" level

The following parameters are also displayed for the webcam:

Parameter	Explanation
Status	Current webcam status. "n.a.": No webcam connected or webcam not configured. "OK": A webcam is connected and operational. "Busy": The webcam creates images that were initiated by a trigger.

Tab. 24: Displays at the "Webcam" level

The actual operation and the viewing of images are performed in the graphical representation.
■ Select in the first dropdown list whether
– no image ("None" setting),
– the live stream ("Live Stream" setting) or
– a saved image of a specific date should be displayed.
■ If you want to view previously saved images, also select the start time of the sought image in the following dropdown list.
■ Click the **Backward** or **Forward** button to scroll between all individual images that were created by initiating a specific trigger.
■ Select in the last dropdown list the resolution of the image from the specified values.
For saved images, the following additional information about the trigger is displayed above the image:
– "Image X / Y": The number of the image and the total number of images (e.g. image no. 2 of 4 images).
– "Trigger caused by": The reason for initiating the trigger (e.g. Task 2).

Previously created images can be downloaded by FTP from the USB stick or the SD card to a PC where they can be viewed and saved.

Downloading the image files
■ Use preferably the "FileZilla" program to establish an FTP connection between a PC and the IoT interface (see section 12.1 "Establishing an FTP connection").
■ Switch in the "FileZilla" program in the left-hand sub-window (PC) to the folder in which you want to save the image files.

■ Switch in the right-hand subwindow (IoT interface) to the "download" folder and then to the "usb-stick/records/webcam/YYYYMMDD/hhmmss" or "sd-card/records/webcam/YYYYMMDD/hhmmss" subfolder depending on where the image files are saved in accordance with the configuration.
The "YYYYMMDD" date and the "hhmmss" timestamp represent the start time of the images.
■ Right-click the required image file and select the "Download" action.

8.4 Configuration tab

The content of the **Configuration** tab depends on which component was selected in the navigation area.
The selection of the "Processing Unit" (uppermost node) complete system provides the following configuration options:
■ **Network** group frame
– TCP/IP
– SNMP
– HTTP
– Filetransfer
– Console
– SMTP
– Modbus/TCP
– Server Shutdown
– OPC-UA
■ **System** group frame
– Syslog
– Units and Languages
– Details
– Date/Time
– Firmware Update
– WebCam
– Mobile
■ **Security** group frame
– Groups
– Users
– Access Configuration
– LDAP
– RADIUS

These configuration options are described in detail in the sections 8.5 "Network" to 8.7 "Security".

When a lower-level real device is selected, e.g. the "IoT interface" device, the following configuration options are available using the associated icons:
– Configure All Alarms (fig. 30, item 1)
– Configure Device Rights (fig. 30, item 3)

Fig. 30: Icons on the "Configuration" tab

Key
1   "Configure All Alarms" icon
2   "Configure Inputs and Outputs" icon
3   "Configure Device Rights" icon

When a virtual device is selected, the following configuration options are available:

    – Configure Inputs and Outputs (fig. 30, item 2)

These configuration options are described in detail in the sections 8.8 "Device Rights" to 8.10 "Inputs and Outputs".

If the "Processing Unit" complete system is selected, the two buttons in the lower area of the **Configuration** tab can be used to display (left-hand button; fig. 31, item. 1) or print (right-hand button; fig. 31, item. 2) a summary of the current settings.
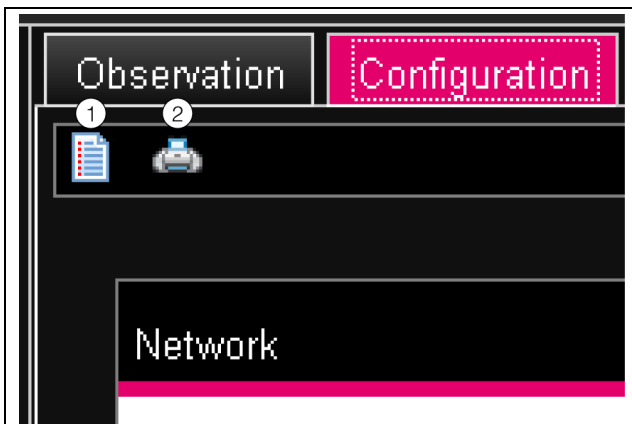
Fig. 31: Summary of the current settings

Key
1   Display
2   Pressure preview

8.5 Network

☞ Note:
In its delivered state, all protocols are activated as standard without SSL encryption. For applications with enhanced safety requirements, please note the following:
- Do not operate the system in networks directly accessible from the Internet, but only in internal networks (Intranet) that provide suitable external protection via firewalls.
- Do not use the default passwords; instead, be sure to use secure, long passwords containing numbers, a mix of upper case and lower case letters, symbols and no repetitions. For SNMP, overwrite the default community string "public".
- Only use secure, encrypted protocols, or deactivate unsecure protocols such as Telnet, FTP etc.

8.5.1 TCP/IP Configuration
The basic network settings for the TCP/IP protocol are made in the "TCP/IP Configuration" dialogue, separately for IPv4 and IPv6.

Parameter	Explanation
IP Address	IP address of the IoT interface.
Netmask	IP subnet mask.
Gateway	IP address of the router.
DHCP	Activate ("DHCPv4" entry) or deactivate ("Manual" entry) DHCP for the automatic assignment of an IP address for a server. No further inputs can be performed in this group frame when DHCP is activated.

Tab. 25: IPv4 Configuration group frame

Parameter	Explanation
IP Address 1	First IPv6 address of the IoT interface.
IP Address 2	Second IPv6 address of the IoT interface.
Auto	Displays an IPv6 address obtained automatically from the network.
Link local	Displays the permanently assigned Link Local address of the IoT interface.

Tab. 26: IPv6 Configuration group frame

Parameter	Explanation
DHCP	Basic settings for IPv6. "Disable": Deactivate IPv6. "Manual": Manual specification of the IPv6 addresses. "Stateless Auto Configuration": Activate the Autoconfiguration (in Linux networks). "DHCPv6": The address is specified using DHCPv6 (in Windows networks).

Tab. 26: IPv6 Configuration group frame

In addition to the basic network settings of the IoT interface, the address or the server name for as many as two DNS servers for the name resolution can be entered in the **DNS Configuration** group frame.

Parameter	Explanation
Name Server	IP address or name of a server for the name resolution.
DHCP	Activate ("Automatic by DHCP" entry) or deactivate ("Manual" entry) DHCP for the automatic assignment of an IP address of the DNS server. If the DHCP is activated, no further inputs can be performed in this group frame. It must, however, be activated for at least one of the IPv4 or IPv6 DHCP protocols.
PU-Hostname	DNS name of the IoT interface. If a DNS server is used for the name resolution, the IoT interface can also be accessed using its name rather than the IP address.

Tab. 27: DNS Configuration group frame

8.5.2 SNMP Configuration

The basic settings for the SNMP protocol are made in the "SNMP Configuration" dialogue.

Observe the following notes when making settings for the SNMP protocol:
– The ObjectID list for the IoT interface is a dynamically generated list that can also change when changes are made to the sensor configuration.
– If the IoT interface is integrated in an infrastructure management system via the ObjectID list, only the variable name should be used to identify the variables. Identification via the ObjectID is not recommended.

☞ Note:
The associated current version of the "OID_List.cmc3" ObjectID list can be fetched via an FTP access from the "download/docs" folder for the IoT interface and saved on a local PC (see section 12.4 "Local saving of supplementary information").
The MIB file can be downloaded at the Internet address specified in section 17 "Customer service addresses".

All trap receivers are entered and generally enabled for sending in the **Traps** group frame.

☞ Note:
– All Trap Receivers that are not enabled in this group frame ("Use" column) do not receive any traps, even if enabled in the Alarm Configuration.
– All Trap Receivers that are enabled in this group frame must also be enabled in the Alarm Configuration (see section 8.9.3 "Trap Receivers").

Parameter	Explanation
Enable Authentication Trap	Activate or deactivate the trap messages for queries with an invalid community ("Authentication Trap").
Trap Receivers	As many as 16 IP addresses or host names as possible recipients of trap messages.
Use	Activate or deactivate individual recipients.

Tab. 28: Traps group frame

You can specify special host addresses in the **Allowed Hosts** group frame that can be used to make contact to the IoT interface via SNMP.

Parameter	Explanation
Host	As many as 12 IP addresses or names as possible hosts that can make contact to the IoT interface. If **no** IP address or host name is entered here, **all** hosts in the network can make contact.
Use	Activate or deactivate individual hosts.

Tab. 29: Allowed Hosts group frame

☞ Note:
Once a host has been entered in the Allowed Hosts group frame, any other host that is not entered there can no longer query values via the SNMP protocol.

You can make special specifications for the SNMP protocol in the versions 1 and 2c in the **SNMPv1/v2c** group frame.

Parameter	Explanation
Enable	Avtivate or deactivate individual hosts.
Read Community	Name of the community with read access to the IoT interface.

Tab. 30: SNMPv1/v2c group frame

Parameter	Explanation
Write Community	Name of the community with write access to the IoT interface.
Trap Community	The name of the community with the trap receivers. Trap messages can be sent only to members of this community.

Tab. 30: SNMPv1/v2c group frame

You make special specifications for the SNMP protocol in the version 3 in the **SNMPv3** group frame.

Parameter	Explanation
Enable	Activate or deactivate SNMPv3.
SNMPv3 Username	User name for access via SNMP.
SNMPv3 Password	Associated password for access via SNMP. The password must contain at least eight characters.

Tab. 31: SNMPv3 group frame

☞ Note for the use of SNMP management systems:
The status of the IoT interface "Overload (current too high)" in the MIB is not currently supported.

8.5.3 HTTP Configuration

All settings for access via HTTP to the IoT interface are performed In the "HTTP Configuration" dialogue, subdivided into the standard access **without** SSL and the secure access **with** SSL.

In addition, it can be specified separately for each user whether or not the user has HTTP access to the IoT interface (see section 8.7.2 "Users").

Parameter	Explanation
Port	Web server port in the IoT interface.
Enable	Activate or deactivate the access via the HTTP protocol.

Tab. 32: Standard Access (without SSL) group frame

Parameter	Explanation
SSL Port	Secure web server port in the IoT interface.
Enable	Activate or deactivate the access via the HTTPS protocol.

Tab. 33: Secure Access (with SSL) group frame

☞ Note:
It is not possible to deactivate both accesses, i.e. with and without SSL, via the web user interface. This is possible only via a Telnet connection or a connection via the USB interface.

8.5.4 File Transfer Configuration

All settings for access via FTP to the IoT interface are performed in the "File Transfer Configuration" dialogue (see section 12 "Updates and data backup").

In addition, it can be specified separately for each user whether or not the user has FTP access to the IoT interface (see section 8.7.2 "Users").

Parameter	Explanation
Port	FTP server port in the IoT interface.
Enable FTP Server	Activate or deactivate the access via the FTP protocol.
Enable SFTP Server	Displays the access via the SFTP protocol. To ensure access to the IoT interface is always possible, this access cannot be deactivated.

Tab. 34: "File Transfer Configuration" dialogue

8.5.5 Console

All settings for access via Telnet and SSH (Secure Shell) are performed in the "Console Configuration" dialogue (see section 7.3 "Telnet connection").

It can also be specified separately for each user whether or not the user has Telnet or SSH access to the IoT interface (see section 8.7.2 "Users").

Parameter	Explanation
Port	Port for access via Secure Shell (SSH) to the IoT interface.
Enable	Activate or deactivate the access via Secure Shell.

Tab. 35: SSH group frame

Parameter	Explanation
Port	Port for access via Telnet to the IoT interface.
Enable	Activate or deactivate the access via Telnet.

Tab. 36: Telnet group frame

8.5.6 SMTP Configuration

The basic settings for sending mail are made in the "SMTP Configuration" dialogue.

All settings for the mail server are specified in the **Server Parameters** group frame so that the IoT interface can send an appropriate e-mail in case of pending alarms.

Parameter	Explanation
Server	IP address or name of the mail server used for sending the e-mails.
Port	Mail server port.
Authentica-tion	Setting authentication on the mail server. "No": Authentication deactivated. "Yes": Authentication activated. "Yes / TLS": Authentication activated with additional encrypted transmission of e-mails.
User name	User name for login to the mail server.
Password	Associated password for login to the mail server.
Sender Address	E-mail address of the IoT interface (sender address).
Reply to Address	Reply address when a recipient answers an e-mail of the IoT interface.

Tab. 37: Server Parameters group frame

All recipients of e-mail messages are entered and generally enabled for sending in the **Email** group frame.

Note:
– All e-mail text receivers that are not enabled in this group frame ("Use" column) do not receive any e-mails, even if enabled in the Alarm Configuration.
– All e-mail recipients activated in this group frame must also be activated in the Alarm Configuration (see section 8.9.2 "Email Receivers").

Parameter	Explanation
Send device message	Setting as to whether status changes such as "Lost", "Detected", "Changed", etc. should be sent as e-mail (checkbox activated or deactivated).
Email Address	Up to 16 e-mail addresses as possible recipients of e-mails from the IoT interface.
Use	Activate or deactivate individual recipients.

Tab. 38: Known Receivers group frame

8.5.7 Modbus/TCP Configuration

Note:
– The IoT interface supports only the "Modbus/TCP" protocol.
– The list of all variables that can be queried via Modbus can be fetched as the "ModbusMap.cmc3" file via an FTP access from the "download/docs" folder of the IoT interface and stored on a local PC (see section 12.4 "Local saving of supplementary information").

The "Modbus/TCP Configuration" dialogue is used to make the basic settings for the Modbus/TCP protocol. The following settings are made in the **Service Parameters** group frame.

Parameter	Explanation
Enable	Enable or disable access via the Modbus/TCP protocol.
Port	Port of the Modbus server in the IoT interface. Port 502 is set as default.

Tab. 39: Service Parameters group frame

The special host addresses defined in the **Allowed Hosts** group frame can be used to make contact to the IoT interface using the Modbus/TCP protocol.

Parameter	Explanation
Host	Up to 12 IP addresses or names of possible hosts that can make contact to the IoT interface. If **no** host is entered here, **all** hosts in the network can make the connection.
Access Rights	Authorisation of the associated host for access via Modbus/TCP. Possible settings are read-only access ("read" setting) or read and write access ("read/write" setting). If access via Modbus/TCP is generally disabled, this setting has no effect.

Tab. 40: Allowed Hosts group frame

Note:
Once a host has been entered in the **Allowed Hosts** group frame, any other host not entered there can no longer query values via the Modbus protocol.

8.5.8 Server Shutdown Configuration
The basic settings for the orderly download of servers via a task are made in the "Server Shutdown Configuration" dialogue. To do this, a licence of the RCCMD software (7857.421) must be installed on each of these servers.

Parameter	Explanation
Name	Name of the server.
Hostname	The IP address of the server to be downloaded.
Port	Port on which the server receives the RC-CMD signal. By default, port 6003 is set.
Delay	The time for which the alarm must be present in order to start the shutdown of the associated server.
Use	Activate or deactivate individual servers.

Tab. 41: Servers group frame

Note:
– All servers not enabled in this group frame ("Use" column) are not shutdown even if enabled in a task.
– All servers activated in this dialogue must also be activated in the associated task.

8.5.9 OPC-UA Configuration
The OPC-UA protocol is a network management protocol that can be used in control room technology. This protocol allows the sensor data of the **Observation** tab to be requested. It does not, however, provide any access to the **Configuration**, **Logging** and **Tasks** tabs. The "OPC-UA Configuration" dialogue is used to make the basic settings for this communications protocol.

Parameter	Explanation
Enable	Enable or disable access via the OPC-UA protocol.
Port	Port of the OPC-UA server in the IoT interface. By default, port 4840 is set.

Tab. 42: "OPC-UA Configuration" dialogue

8.6 System

8.6.1 Syslog
The basic settings for sending log messages to the Syslog server are made in the "Syslog Configuration" dialogue.

Parameter	Explanation
Server 1	The IP address or name of a server to which alarm and event logs are sent.
Server 2	The IP address or name of a second server to which alarm and event logs are sent.
Facility	A digit between 0 and 7 (inclusive) for prioritising the sent logs.

Tab. 43: "Syslog Configuration" dialogue

Parameter	Explanation
Enable Syslog	Activate or deactivate the sending of log messages.

Tab. 43: "Syslog Configuration" dialogue

8.6.2 Units and Languages
The "Units and Language Configuration" dialogue can be used in the **Units** group frame to switch the unit for all temperature values between "Celsius" and "Fahrenheit".

Parameter	Explanation
Temperature Format	Select the desired temperature unit ("Celsius" or "Fahrenheit").

Tab. 44: Units group frame

■ After switching the unit, check all temperature setting values (e.g. of a connected temperature sensor, of virtual devices).
The language for the website of the IoT interface can be selected in the **Language** group frame.
■ Select the required language, e.g. German, from the pull-down menu.
■ Then sign off from the IoT interface website (see section 8.2.8 "Logout and changing the password") and sign on again.
Although the names of the levels and the parameters continue to be displayed in English when the language is switched, tooltips can be displayed in the associated selected language.
■ Place the mouse cursor on the **Observation** tab, e.g. from the "Device" level, below the "IoT interface " main level.
A tooltip with the "Device" translation appears.

8.6.3 Details
Detailed information concerning the IoT interface is displayed in the "Details Configuration" dialogue. Individual parameters can be used to differentiate between multiple installations.

Parameter	Explanation
Name	Name of the IoT interface (for the more exact identification).
Location	Installation location of the IoT interface (for the more exact identification).
Contact	Contact address, typically an e-mail address.
Hardware Revision	Display of the IoT interface hardware version.
Software Revision	Display of the IoT interface software version.

Tab. 45: "Details Configuration" dialogue

Parameter	Explanation
Serial Number	Display of the IoT interface serial number.

Tab. 45: "Details Configuration" dialogue

8.6.4 Date/Time

The system date and time of the IoT interface can be changed in the "Date and Time Configuration" dialogue.

Parameter	Explanation
Time Zone	Selection of the time zone. The time zone is required when an NTP server is used.

Tab. 46: Time Zone group frame

Parameter	Explanation
Time	Current time of day.
Date	Current date.

Tab. 47: Date/Time group frame

Note:
Changing the system date or the system time can cause data loss (see section 8.13 "Charts").

The Network Time Protocol can be activated in the **NTP** group frame. The associated NTP server can also be defined here. These settings can be used to synchronize the local date and time setting of the IoT interface with a server.

Parameter	Explanation
Use NTP	Activate or deactivate the NTP function for the time and date synchronisation with an NTP server.
NTP Server 1	IP address or name of the primary NTP server.
NTP Server 2	IP address or name of the secondary NTP server.

Tab. 48: NTP group frame

8.6.5 Firmware update

Note:
Observe all advanced notes for performing an update in section 12.2 "Perform an update".

The "Firmware Update" dialogue can be used to update the IoT interface directly from the website. This is also possible with a USB storage medium, a microSD card (see section 12.2.3 "Update via USB") or via an (S)FTP

connection (see section 12.2.4 "Update via FTP or SFTP").
■ Click the diskette icon in the "Firmware Update" dialogue.
■ Navigate in the file selection dialogue to the new firmware file to be installed with the "tar" extension and select it.
The file name is displayed in the dialogue.
■ Click the **Start Update** button.

The update process starts automatically after a few seconds. This is indicated with a red flashing of the multi-LED (so-called heartbeat, alternately long and short) on the IoT interface.

8.6.6 WebCam

The access to an Axis webcam available in the network can be configured in the "WebCam Configuration" dialogue (VAPIX version 3). The webcam allows viewing of a live stream from the web user interface for the recording or saving of individual images for each task (see section 8.3.5 "Webcam").

Note:
A live stream **cannot** be viewed with Internet Explorer. To view the live stream with Opera Browser, the webcam password protection must be revoked.

The basic settings for the webcam are made in the **Network** group frame.

Parameter	Explanation
Enable	Enable or disable access to the webcam.
Host	IP address or host name of the webcam.
Username	User name for access to the webcam.
Password	Associated password for access to the webcam.

Tab. 49: Network group frame

The settings for creating individual images are made in the **Snapshot** group frame.

Parameter	Explanation
Interval	The interval in seconds between two images.
Number of Images	Total number of images created when a trigger is initiated.
Destination	Selection of the external storage medium on which the images are stored.

Tab. 50: Snapshot group frame

Note:
A trigger for creating the individual images can, for example, be initiated via tasks or manually via the website.

8.6.7 Mobile

The representation (dashboard) displayed on a mobile terminal is specified in the **Mobile Phone** group frame in the "Display Configuration" dialogue (see section 8.14 "Dashboards").

Parameter	Explanation
Dashboard	Selection of the dashboard displayed for the login with a mobile terminal.

Tab. 51: Mobile Phone group frame

The representation of a dashboard on a mobile terminal normally differs from the configured representation. The title lines of the individual components of the dashboard are initially displayed stacked on a mobile terminal. Clicking a title line displays the associated content of the component (e.g. a variable list).

Note:
Before selecting a dashboard for a mobile terminal, ensure that the dashboard has been configured appropriately.

8.7 Security

All basic settings for user groups and individual users can be specified in the **Security** group frame. These settings can be changed for individual components. If the "default" standard setting is used for the individual components, these values will be used.

8.7.1 Groups

Up to 32 different user groups can be defined in the "Groups Configuration" dialogue. The 33 users who can be created can be assigned to these groups in the "Users" dialogue (see section 8.7.2 "Users").

Parameter	Explanation
Name	Name of the user group.
Description	(Detailed) Description of the user group.
Initial Data Rights	Authorisation of the user group with regard to the parameters of the "Data" type of the devices (see section 8.8.2 "Data types"). Possible settings are no rights ("no" setting), read-only rights ("read" setting) as well as read and write rights ("read/write" setting). The authorisations set here are transferred automatically for newly signed-on devices.

Tab. 52: "Groups Configuration" dialogue

Parameter	Explanation
Initial Config Rights	Authorisation of the user group with regard to the parameters of the "Config" type of the devices (see section 8.8.2 "Data types"). Possible settings are no configuration rights ("no" setting), configuration parameters can only be read ("read" setting) and parameters can be changed ("read/write" setting). The authorisations set here are transferred automatically for newly signed-on devices.
Admin	Show or hide the **Configuration** and **Tasks** tabs. The general information for the sensors can be changed under the "Device" item only as administrator.
Auto Logout [sec]	The duration after which a user of this group with no activity is automatically logged out from the IoT interface. For the set value of "0", no automatic sign-off is performed for this user.

Tab. 52: "Groups Configuration" dialogue

Note:
The duration specified for the "Auto Logout" parameter does not apply when a user logs in directly on a dashboard. The user remains logged in to IoT interface while the dashboard is open.

For restricted user groups, it is desirable to use the setting in the "admin" column to prevent access to the **Configuration** and **Tasks** tabs (checkbox is deactivated). Otherwise there is the possibility that users reassign their own rights, change the settings for tasks or create new tasks.

Note:
The "admin" group cannot generally be changed.

If subsequent changes are made in the "Initial Data Rights" or "Initial Config Rights" columns, after clicking the "Save" button in the "Groups Configuration" dialogue, the "Initial Rights Changed" dialogue opens with a prompt.
- Click the **Yes** button to transfer the changes made in the access authorisation to the available sensors.
- Click the **No** button to retain the current access authorisations for the sensors and their parameters. The newly set access rights are then used only for sensors signed-on in future.

8.7.2 Users

Up to 33 different users can be defined in the "Users Configuration" dialogue.

Parameter	Explanation
Enabled	Activate or deactivate a user.
User	User name for login to the IoT interface.
Group	User group to which the user belongs.
File Transfer	User authorisation for access via FTP. Possible settings are "no" access, "read" access and "read/write" access. If access via FTP is generally deactivated (see section 8.5.4 "File Transfer Configuration"), this setting has no effect.
HTTP	User authorisation for access via HTTP. For activated checkbox, access via HTTP is possible; for deactivated checkbox, access via HTTP is not possible. If access via HTTP(S) is generally deactivated (see section 8.5.3 "HTTP Configuration"), this setting has no effect.
Console	User authorisation for access via Telnet or SSH. For activated checkbox, access via Telnet or SSH is possible; for deactivated checkbox, access via Telnet and SSH is not possible. If access via Telnet and SSH is generally deactivated (see section 8.5.5 "Console"), this setting has no effect.

Tab. 53: "Users Configuration" dialogue

Note:
If the access type via a specific protocol is generally deactivated, it cannot be activated for an individual user.

A user with the appropriate access rights can use the **Set Password** button to (re)assign a password for another user. To do this, the desired user must be selected beforehand, otherwise the button is inactive.

In addition, users can change their own password after login (see section 8.2.8 "Logout and changing the password").

8.7.3 Access Configuration

The stored access codes and transponder cards are displayed in the "Access Configuration" dialogue. The **Edit**, **Add** and **Delete** buttons are used to change existing entries, create new entries and delete existing entries, respectively. The detailed procedure is described in the assembly, installation and users guide for the CMC III CAN-Bus Access (DK 7030.200).

8.7.4 LDAP Configuration

The "LDAP Configuration" dialogue can be used to transfer the user administration from an LDAP server. If the access to an LDAP server is configured and activated, during the login, the user data is always checked first on the local user administration in the IoT interface. If the

user data is not found there, the LDAP server is then searched.
The basic settings for the LDAP server are specified in the **Server** group frame.

Parameter	Explanation
Enable LDAP	Enable or disable access to the LDAP server.
Hostname	The IP address or name of the LDAP server.
Bind DN	The Distinguished Name for login on the LDAP server.
Bind PW	The password for authentication on the LDAP server.

Tab. 54: Server group frame

The settings for requesting the group frame are specified in the **Group Search** group frame.

Parameter	Explanation
Search Filter	The filter for requesting the group names on the LDAP server. The expression "(&(objectClass=group)(member=%U))" is stored as standard.
Base DN	The root directory in which the information for the group administration is stored.
Attribute	The attributes returned from the LDAP server for the request.

Tab. 55: Group search group frame

Note:
"%U" can be used as placeholder for the LDAP user in the "Search Filter" mentioned above.

The settings for requesting the user names are specified in the **User Search** group frame.

Parameter	Explanation
Search Filter	The filter for requesting the user names on the LDAP server. The expression "(&(objectClass=user)(sAMAccountName=%L))" is stored as standard.
Base DN	The root directory in which the information for the user administration is stored.
Attribute	The attributes returned from the LDAP server for the request.

Tab. 56: User search group frame

Note:
"%L" can be used as placeholder for the login name in the "Search Filter" mentioned above.

Whereas the users stored in the LDAP server do not need to exist in the local user administration of the IoT interface, the groups must also be created locally. To avoid needing to use the same group names in the LDAP server and in the IoT interface, the associated names on the LDAP server can be assigned to the local group names of the IoT interface in the **Group Alias Configuration** group frame.

Parameter	Explanation
Group Name	The name of the group in the IoT interface.
LDAP Alias	The associated name of the group in the LDAP server.

Tab. 57: Group Alias Configuration group frame

8.7.5 Radius Configuration
The "Radius Configuration" dialogue performs the user administration for a Radius server. If the access to a Radius server is configured and enabled, during the login, the user data is always checked first on the Radius server. If the user data is not found there, the local user administration in the IoT interface is then searched.

The basic settings for the Radius server are specified in the **Server** group frame.

Parameter	Explanation
Enable Radius	Enable or disable access to the Radius server.
Hostname	The IP address or name of the Radius server.
Port	The port of the Radius server. Port 1812 is set as default.
Secret	The password for authentication on the Radius server.
Authentication Method	Deployed encryption method.

Tab. 58: Server group frame

The rights for a user stored on the Radius server for login to the IoT interface are specified in the **Group Search** group frame.

Parameter	Explanation
Group Selection	Assignment of the user to a group. "Manual": Each user is logged in with the user group selected in the "Group Name" field. "By Server Attribute": The user is logged in with the user group stored for the "cmc-group" attribute in the Radius server. This user group must also exist in the IoT interface.
Group Name	The selection of the associated user group for all users for login via a Radius server and a manual assignment to a user group ("Manual" setting).

Tab. 59: Group Search group frame

8.8 Device Rights
After selection of the IoT interface component from the "Real Devices" category in the navigation area, you can specify the access rights for individual user groups on the **Configuration** tab.
- Select the "IoT interface" entry in the navigation area.
- Select the **Configuration** tab in the right-hand area of the screen page.

The various parameters for the currently selected component are displayed in the list view of the **Configuration** tab. The access rights of these parameters can be customised by the operator.
- Click the "Configure Device Rights" icon.
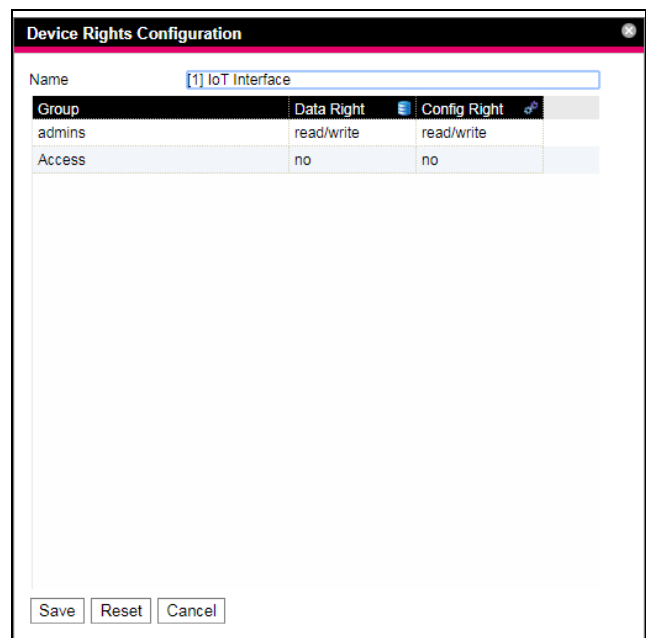 The "Device Rights Configuration" dialogue opens.

Fig. 32: "Device Rights Configuration" dialogue

The current device for which the "Device Rights Configuration" is performed is displayed above the table. The names of the user groups are listed in the "Group" column.

Parameter	Explanation
Group	The names of all user groups created previously (see section 8.7.1 "Groups").

Tab. 60: "Group" column

The access to the parameters of the "Data" device type is specified in the "Data Right" column on the **Observation** tab. The assignment of the parameters to the "Data" type can be obtained on the **Configuration** tab from the "database" icon prefixed to the associated parameter (see section 8.8.2 "Data types"). The following settings can be selected:

Parameter	Explanation
no	Members of the group have neither read nor write access to parameters of the "Data" type.
read	Members of the group have read access to parameters of the "Data" type.
read/write	Members of the group have read and write access to parameters of the "Data" type. This setting acts only when the software is permitted to change parameters of the "Data" type.

Tab. 61: "Data Right" column

The access to the parameters of the "Config" type of the device is specified in the "Config Right" column on the **Observation** tab. The assignment of the parameters to the "Config" type can be obtained on the **Configuration** tab from the "gearwheel" icon prefixed to the associated parameter (see section 8.8.2 "Data types"). The following settings can be selected:

Parameter	Explanation
no	Members of the group have neither read nor write access to the limit values. If the "no" entry is also selected in the "Data Right" column, only the "Device" level can be viewed. If some other entry is selected in the "Data Right" column, the "Value" and "Status" values can be viewed in the other levels.
read	Members of the group have read access to the limit values. This means, they can view the temperature limit values for alarms and warnings, for example.
read/write	Members of the group have read and write access to the limit values. This means, they can view and change the temperature limit values for alarms and warnings, for example.

Tab. 62: "Config Right" column

If a field does not have any caption, the "Device Rights" sublevels are different (see section 8.8.1 "Inheritance of the Device Rights").

☞ Note:
Such defined access rights always apply only for access to the associated component via the website. Access rights at door handles are controlled by the general user administration and the Access Configuration (see section 8.7.3 "Access Configuration").

8.8.1 Inheritance of the Device Rights
The rights assignment for the individual sensors is constructed parallel to the representation on the **Observation** tab. A change to a node point is also transferred automatically to all variables subordinate to this node point.
■ Select the "IoT interface" entry in the navigation area.
■ Select the **Configuration** tab in the right-hand area of the screen page.
■ Click the "Device Rights" icon suffixed to the "IoT interface" entry.
The "Device Rights Configuration" dialogue opens (fig. 32).
If a change is made in this dialogue and a different access authorisation to the variables assigned to a user group, this user group also has the same access rights for all variables subordinate to the "IoT interface" node point.
If a node point has a further node point with different subordinate variables, the inheritance also acts here. A configuration change is transferred automatically to the second node point and the subordinate variables there. If, however, the second node point is changed, only the access rights for those variables subordinate to this node point change.
If an individual subordinate parameter is customised, it can be selected and edited individually.
■ Click the "Plus" icon to open the complete structure.
■ Click the "Device Rights" icon directly behind the variable to be edited.
If the access rights of the individual parameters for a node point differ in the "Device Rights Configuration" dialogue, an empty field is shown here in the "Device Rights Configuration" of the complete sensor. Changing this empty field causes the settings there to be transferred for all subordinate parameters.

8.8.2 Data types
The parameters of the sensors are differentiated into two types:
– Data
– Config
A variable of the "Data" type provides status information and can be changed only for those sensors whose software permits this. A variable of the "Config" type contains configuration information and can be changed by a user when the software permits this.

An icon indicates the associated type. Parameters of the "Data" type are represented as a "Database" icon (with stacked blue cylinders). Parameters of the "Config" type are represented as two diagonal gearwheels.

Fig. 33: Icons of the data types

Key
1   "Gearwheel" icon ("Config" data type)
2   "Database" icon ("Data" data type)

The associated icons are displayed when a sensor is selected on the **Configuration** tab in the navigation area and this expanded down to the lowest level and also in the "Device Rights Configuration" dialogue (fig. 32, item 1). The icons emphasise the assignment to the "Data" and "Config" data types.

8.9 Alarm Configuration

After selection of the "IoT interface" entry under "Real Device" or another component under "Real Device" or under "Virtual Device", you can individually specify the alarm notification for each measured value on the **Configuration** tab.

- Select the "IoT interface" entry in the navigation area.
- Click the **Configuration** tab in the right-hand part of the screen.
- Click the "Configure All Alarms" icon.
  The "Alarm Configuration" dialogue appears.
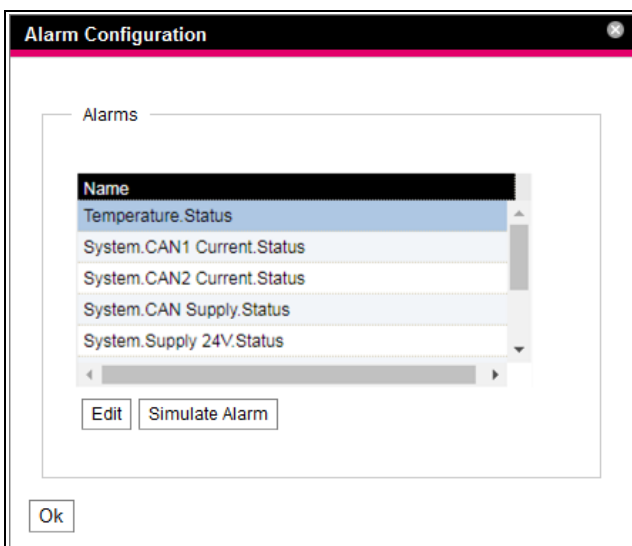
Fig. 34: "Alarm Configuration" dialogue

- In the listing, click the row of the sensor or the input/output for which you want to specify the IoT interface behaviour.
- Click the **Edit** button.

When the temperature sensor is selected, for example, the "Alarm Configuration: Temperature.Status" dialogue appears.

8.9.1 Notifications

You can make settings in the **Notifications** group frame how a pending alarm should be output.

Parameter	Explanation
Acknowledge Required	If this setting is activated, the alarm message remains displayed until it has been acknowledged. This means, even when the cause of the alarm is no longer present, e.g. when in the meantime the temperature has undershot the switching point, the "Alarm" status remains set. Only the transition to the "OK" status is blocked, i.e. other alarms as well as the transition to the "Warning" status are also displayed for activated setting.
Delay	Delay time between measured value overshot and switching to the alarm or warning status. This delay time does not apply to the switching action to the "OK" status.

Tab. 63: Notifications group frame

8.9.2 Email Receivers

You can make settings in the **Email Receivers** group frame to which recipients an e-mail should be sent when an alarm occurs.

All appropriate recipients created previously are displayed (see section 8.5.6 "SMTP Configuration"). These recipients are **deactivated** by default.

Parameter	Explanation
Email Address	E-mail addresses created in the IoT interface configuration.
Use	Activate or deactivate the associated recipient.

Tab. 64: Email Receivers group frame

☞ Note:
If an e-mail receiver was generally disabled previously, although it may be enabled for individual alarm messages, e-mails are still not sent to this receiver (see section 8.5.6 "SMTP Configuration").

8.9.3 Trap Receivers

You can make settings in the **Trap Receivers** group frame to which recipients a trap message should be sent.

All appropriate recipients created previously are displayed (see section 8.5.2 "SNMP Configuration"). These recipients are **activated** by default.

8 Operation

Parameter	Explanation
Trap Host	The trap receiver created in the IoT interface configuration.
Use	Activate or deactivate the associated recipient.

Tab. 65: Trap Receivers group frame

☞ Note:
If a trap receiver was generally disabled previously, although it may be enabled for individual alarm messages, traps are still not sent to this receiver (see section 8.5.2 "SNMP Configuration").

8.9.4 Alarm simulation

After completion of an alarm configuration, the notifications set in the "Alarm Configuration" dialogue (fig. 34) can be checked. This is done by simulating a pending alarm, such as by testing the alarm with the actual stored limit values.

■ Click in the listing the line of the sensor or the input/output for which you want to simulate the alarm behaviour.
■ Click the **Simulate Alarm** button.
If the temperature sensor is selected, for example, the "Simulate Alarm: Temperature.Status" dialogue opens.
■ You specify in this dialogue which type of alarm and for how long is to be simulated.

Parameter	Explanation
Duration	The duration for which the alarm should be simulated.
Simulation Value	The status to be simulated. The possible values depend on the type of the selected sensor or input/output.

Tab. 66: "Simulate Alarm" dialogue

■ Click the **OK** button to simulate the alarm and so check all settings (e.g. the correct sending of an e-mail to all associated receivers).

☞ Note:
The "Alarm simulation" entry created in the log information allows the simulation to be differentiated from an actual alarm.

■ After expiration of the interval for a simulated alarm, you can simulate further alarms similarly.

☞ Note:
Only one alarm simulation can be active concurrently.

8.10 Inputs and Outputs

☞ Note:
A detailed description for the "Inputs and Outputs" topic can be found in the separate "Tasks And Virtual Devices" document.

8.11 Logging

The log information of the IoT interface can be viewed on the **Logging** tab. Because this log information is generally valid, the information displayed on the **Logging** tab is independent of the component selected in the left-hand area of the screen.

☞ Note:
The associated current version of the "Logging.cmc3" log file can be fetched via an FTP access from the "download" folder of the IoT interface and stored on a local PC (see section 12.4 "Local saving of supplementary information".

■ Click the **Logging** tab in the right-hand part of the screen.

Fig. 35: Logging tab

Key
1 Define a filter
2 Reload the information
3 Delete the display
4 Printing the display

A message is initially displayed that you can either
– Define a filter in order to display only selected events
or
– Load the complete history into the display with all events.
The symbols in the toolbar below the tabs can be used for this purpose.

8.11.1 Defining a filter

To receive only a specific section from all messages, you can define a filter.
■ Click the first symbol on the left (fig. 35, item 1).
The "Set Logging Filter" dialogue appears.
The following parameters are available:

Parameter	Explanation
Date	Messages of a specific date.
Type	Error type. The selection of the "Alarm" causes, for example only alarm messages but no other messages from devices to be displayed.
Device Index	Messages of a specific device. The (internal) number of the device assigned during the initial connection is selected.
User	Messages initiated by a specific user. For example, messages when the user logs in or out are displayed.
IP Address	Messages that can be assigned to a specific IP address. All addresses used to access the IoT interface are listed.

Tab. 67: Settings in the "Set Logging Filter" dialogue

The first entry in each column is "All items". When you select this entry, the entries in the associated column are **not** filtered.

Example: All information messages on 19.01.2012
- Select the above-mentioned date "19.01.2012" in the "Date" column.
- Select the "Info" entry in the "Type" column.
- Select the "All items" entry in the three following columns.
- Click the **OK** button.

The filter is used and only those messages that satisfy the above-mentioned criterion are displayed in the list.

Note:
Several entries can be marked in the individual columns by keeping the "Ctrl" key pressed.

8.11.2 Refreshing the view
After the definition of a filter, all messages stored up to this time that satisfy the filter criterion are displayed. No subsequent automatic refresh of the display occurs when new messages arrive, i.e the display must be refreshed manually.
- Click the second symbol on the left (fig. 35, item 2).
  It takes a moment until all events have been reloaded from the IoT interface. The refreshed list with all events is then displayed.

Note:
After each refresh, only those messages that satisfy the currently stored filter criterion are displayed.

8.11.3 Printing the view
The complete history or the results selected using a filter can be printed.

- If required, first define a suitable filter in order to display only a subset of all results (see section 8.11.1 "Defining a filter").
- Click the fourth icon from the left (fig. 35, item 4).
  It takes a moment until all events have been reloaded from the IoT interface. The updated list with all events is displayed in a separate window and a "print" dialogue opens.
- Print the view or save it as PDF file.

8.11.4 Delete the display
You can delete the current display at any time.
- Click the third symbol on the left (fig. 35, item 3).
  All entries from the display are deleted and the same message as for selection of the **Logging** tab appears again.

Note:
The entries are removed only from the display. The log file remains unchanged.

8.12 Tasks

Note:
A detailed description for the "Inputs and Outputs" topic can be found in the separate "Tasks And Virtual Devices" document.

8.13 Charts
As many as 16 charts on which the chronological trend for as many as 6 variable values can be viewed on the **Charts** tab. The data of these charts can be downloaded for separate evaluation (e.g. with a spreadsheet program such as Excel) as CSV files (see section 8.13.3 "Evaluating the CSV files").
- Select the **Charts** tab in the right-hand area of the screen page.

Fig. 36:   Charts tab

Key
1   Title lines
2   Displayed chart

■ Click on the title line of the associated chart in order to display or hide the associated chart and the configuration buttons.

8.13.1 Configuring a chart

To record the variable values, each chart must first be configured and activated (once).

■ If the buttons for the configuration and the navigation of the chart are not displayed, click the title line.
  This chart now expands and it can be configured (e.g. "Chart 1").
■ Click the "Configuration" button.

The "Chart Configuration" dialogue opens.
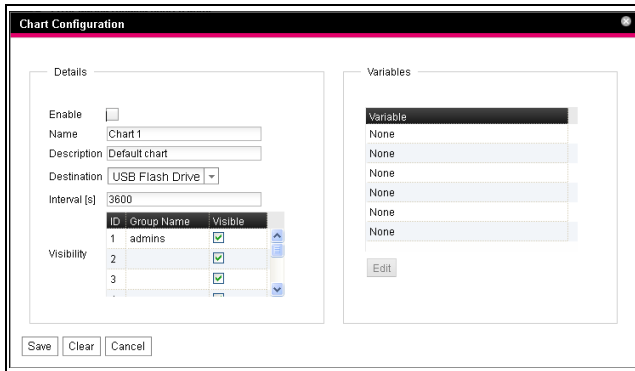
Fig. 37:   "Chart Configuration" dialogue

Make the following settings in the left-hand **Details** group frame:

Parameter	Explanation
Enable	Enable or disable the chart.
Name	Chart designation. This designation is displayed in the title line of the chart.
Description	Chart description.
Destination	Selection of the external storage medium on which the chart data is stored.
Interval	The time interval in seconds in which the current value is stored.
Visibility	Activates the user groups that can view and configure the associated chart.

Tab. 68: Details group frame

The associated charts must be deactivated before removal of the external storage medium on which chart data is stored. If this is not done, the files with the chart data may be corrupted. Alternatively, the external storage medium can also be signed-off from the system beforehand (see section 8.3.4 "Memory"). This deactivates the charts automatically.

☞ Note:
  If an external storage medium is removed directly, this can cause loss of chart data.

In the right-hand **Variables** group frame, as many as 6 variables are specified per chart, the values of which can then be shown graphically.

☞ Note:
  Changing the settings of existing charts can lead to data loss. Consequently, the associated CSV files should be saved beforehand (see section 8.13.3 "Evaluating the CSV files").

■ Select one of the 6 lines.
  If the "None" entry is not present in a line, this variable has already been assigned to the chart.
■ Click the **Edit** button.
  The "Variable Selection" dialogue opens.

The following parameters are available:

Parameter	Explanation
Device	Selection of the device for which a value should be recorded.
Variable	The variable whose value should be recorded. This list shows only those variables available for the previously selected device.

Tab. 69: Variables group frame

■ Click the **OK** button to accept the selected settings or the **Cancel** button to terminate the action.
  The "Chart Configuration" dialogue reopens.
■ If necessary, add further variables to the chart.
■ Then click the **Save** button to display the chart with the selected settings.
■ Alternatively, click the **Clear** button to reset all chart settings to their default values. All previously stored values of the chart will be deleted.

If variables with different units are assigned to a chart (e.g. temperature in °C and voltage in V), then multiple ordinate axes (Y axes) will be created.

8.13.2 Chart view

As standard, the left-hand boundary of the time axis (X axis) is fixed to the time when the chart was activated. The right-hand boundary "grows" with each refresh of the chart after the time entered in the "Interval" parameter. Similarly, the ordinate axes are adapted so that all measured values can be displayed.

As standard, the values of all represented variables at the time of activating the chart and the associated time stamp (date and time) are displayed on the right-hand side of the chart.

Display of the measured values at a specific time

Provided the chart is activated, you can display the exact measured values for a specific time.

■ Position the mouse cursor in the chart.
  A vertical line is displayed.

The values of all represented variables at the selected time are displayed in plain language together with the associated time stamp on the right-hand side of the chart.

Adapting the displayed time period
In addition, the displayed time period can be reduced, for example, to more exactly investigate the trend at a specific time.
■ Click the **Zoom In** button.
  The complete trend from activation of the chart to the current time is displayed. Each click of this button reduces the displayed time period.
■ Click the **Shift Forward** button to move the start time of the displayed area nearer the current time.
■ To move the start time of the displayed area nearer the activation time of the chart, click the **Shift Back** button.
■ Similarly, click the **Zoom Out** button to increase the displayed time period.

Displacing the charts from the browser window
As standard, the charts are displayed directly below the associated title line in the browser window. Alternatively, each chart can also be displayed in a separate window.

☞ Note:
Decoupling from the website is **not** available for Internet Explorer. This button is absent.

■ Click the **Undock** button for the desired chart.
  The chart is now displayed in a separate window; the "Chart is undocked" message appears below the title in the main window.
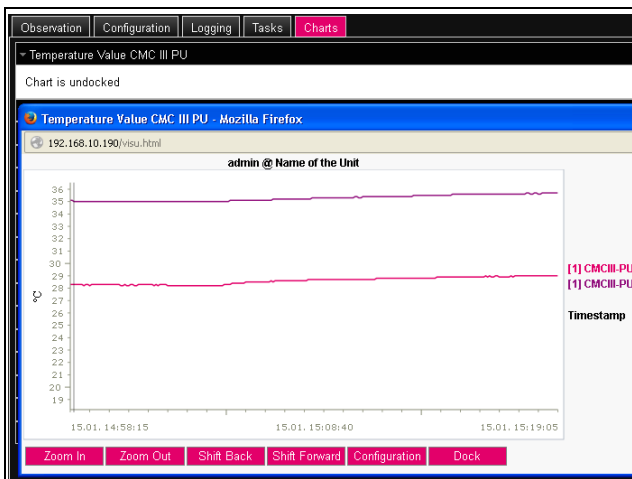
Fig. 38:   Displaced chart

Similar to the displacement of windows for various connected sensors (see section 8.2.7 "Undock function"), the separate windows of the charts can be moved independent of the actual website of the IoT interface and changed in size. This function can be used by several charts and so a complete overview created on the PC screen.

■ Click the **Dock** button in the separate window or simply close the window to display the chart again below the title line in the main window.

8.13.3 Evaluating the CSV files
The charts are created using data from the CSV files. This data can be downloaded via FTP from the IoT interface and then evaluated separately (e.g. with a spreadsheet such as Excel).
The maximum size of a CSV file is 4 GB. If this limit is reached, the CSV file will be saved as backup file and a new CSV file created automatically. If this second file also reaches the 4 GB limit, the first backup file will be overwritten when a new backup file is created.

Downloading the CSV files
■ Establish a connection between a PC and the IoT interface (see section 12.1 "Establishing an FTP connection").
■ In the left-hand subwindow (PC), switch to any folder in which you want to store the CSV files.
■ In the right-hand subwindow (IoT interface), switch to the "download" folder and to the "usb-stick/records" or "sd-card/records" subfolder depending on where the CSV files are stored as specified by the configuration of the associated chart.
■ Right-click the desired CSV file and select the "Download" action.
  The CSV files are named using the schema "chart.##.json.csv", where "##" represents the number of the associated chart ("01" to "16").

Importing the CSV files into Excel
The procedure to import a CSV file for evaluation in Excel is described below.

☞ Note:
In general, the CSV files can also be imported into another spreadsheet program, although the procedure may differ.

■ Create an empty table in Excel.
■ Use **Data** > **From text** in Excel to select the CSV file to be imported and follow the instructions of the conversion wizard.
■ Also observe the following settings:
  Step 1 of 3:
  – Data type: Separated
  – Import begins in line: 1
  – File origin: Windows (ANSI)
  Step 2 of 3:
  – Separator: Tab stop
  Step 3 of 3:
  – Data format of the columns: Standard
■ In Step 3 of 3, click the **Next...** button to specify the decimal separator (setting "point") and the 1000's separator (setting "comma") used in the CSV file. De-

pending on the country-specific settings, these settings may already be the defaults.

Note:
If different separators are set for numeric data, the time details in column 2 cannot be converted correctly later.

The display of the CSV files is divided into three areas.
– **Area 1:** General chart information in accordance with the configuration is shown in line 1 (e.g. chart name, description, start time).
– **Area 2:** Starting at line 3, information about the variables recorded in the chart is output separated by a blank line. In particular, the first two columns are important.
   Column 1: Variable designation. These designations are used as "header" in area 3.
   Column 2: The exact designation of the recorded measured values.
– **Area 3:** Finally, the time stamp and all recorded measured values are output also separated by a blank line.
   Column 1 (Time0): The UNIX time (number of elapsed seconds since 01.01.1970). Unless reformatted, this time cannot be used in Excel.
   Column 2 (Time1): The time value that can be used in Excel.
– **Columns 3 to maximum 8:** The actual measured values are output in these columns.

The time value in column 2 must be converted as follows to produce a format that can be read:
■ Mark all time values in column 2.
■ Right-click the marking and select the "Format cells" entry in the context menu.
■ Select the "User-defined" entry in the "Category" columns on the "Numbers" tab in the "Format cells" dialogue.
■ Enter the "DD.MM.YYYY hh:mm:ss" number format in the "Type" field.
   The time stamp is then output as date and time so that it can be used in a chart, for example.

8.14 Dashboards

Note:
Changes made in the dashboards described below can be made only by users who belong to the "admins" user group.

As many as 12 flexibly configurable websites can be created on the **Dashboards** tab. This makes it possible to define different views for different purposes and display only the required information. For example, the graphical representation in multiple columns similar to the structure of multiple enclosures monitored with a IoT interface is conceivable.

Note:
After the **direct** login on a dashboard, the user is **not** logged out automatically after the predefined time. The user remains logged in to IoT interface while the dashboard is open.

8.14.1 Basic settings
■ Select the **Dashboards** tab in the right-hand area of the screen page.
The following information is displayed:

Parameter	Explanation
Name	Dashboard name.
Description	Extended description of the dashboard.
Enabled	Flag whether the dashboard can be enabled ("Yes") or not ("No").

Tab. 70: Dashboards tab
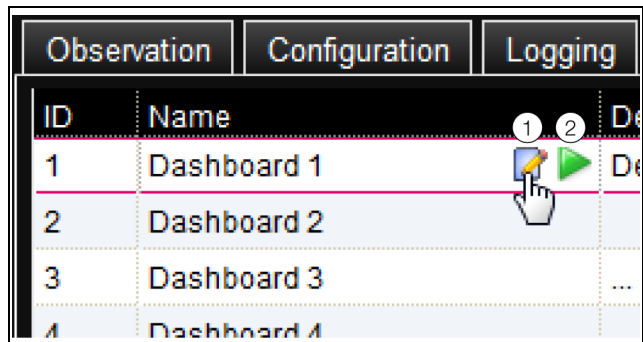
Fig. 39:   Calling the "Dashboard Configuration" dialogue

Legend
1   "Edit" icon
2   "Start" icon

The above information can be changed in the "Dashboard Configuration" dialogue.
■ Move the mouse cursor to the line of the dashboard whose information you want to change.
   An "Edit" icon appears at the end of the "Name" column and the cursor changes to the "hand" icon. If the dashboard can be enabled (the "Enabled" parameter has the value "Yes"), the green "Start" icon suffixed to the "Edit" icon can be used to enable the dashboard.
■ Click the "Edit" icon.
   The "Dashboard Configuration" dialogue opens.
■ Enter the required values for the named parameters.
■ Confirm your entry by clicking the **Save** button.
Click the **Clear** button to reset all inputs to their default values.

8.14.2 Configuring a dashboard
The contents of a dashboard must be configured (once). This requires that the dashboard is first enabled and then started.

- Check whether the "Yes" entry is displayed in the "En-abled" column for the dashboard to be configured.
- If this is not the case, first enable this setting in the "Dashboard Configuration" dialogue (see section 8.14.1 "Basic settings").
- Move the mouse cursor to the line of the dashboard to be configured.
  A "Start" icon appears next to the "Edit" icon at the end of the "Name" column and the cursor changes to a "hand" icon.
- Click the "Start" icon.
  The "Auto-Logout is Enabled" dialogue opens.
- Read the notification text and click the **OK** button to confirm.
  A new browser window opens with the actual dash-board. The dashboard is empty for the first call be-cause no boards have yet been selected.
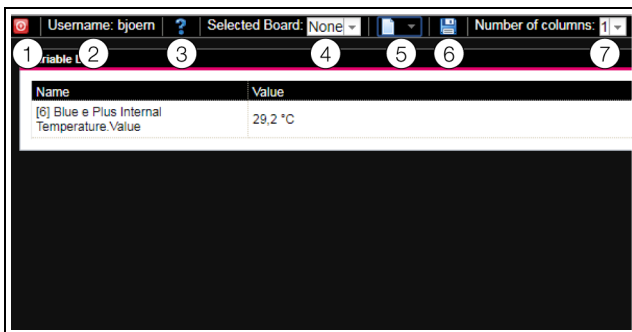
Fig. 40:   Dashboard header line

Legend
1   **Logout** button
2   "Username" column
3   Call the "Board Details" dialogue
4   Dashboard selection
5   "Edit" icon for selecting a dashboard component
6   "Save" icon
7   Number of columns

Note:
The **Logout** button is displayed only when the login is made directly on a dashboard (see section 8.14.4 "Calling a dashboard").

The following information is displayed on the header line:

Parameter	Explanation
Username	Name of the user currently logged in.
"?"	Open the "Board Details" dialogue in which the basic settings of the dashboard are dis-played.
Selected Board	Select the dashboard from a dropdown list. The names of the dashboards that can be enabled are displayed.

Tab. 71: Dashboard header line

Parameter	Explanation
"Edit" icon	Select the components to be displayed on the dashboard.
"Save" icon	Save the dashboard. The configured com-ponents and the window layout are dis-played for each login as they were configured at the time of saving. The actual display in a window is not saved.
Number of Columns	The number of columns in which the infor-mation to be displayed can be assigned (maximum nine columns).

Tab. 71: Dashboard header line

Selectable representations
The representations to be displayed on the dashboard are selected with the "Edit" icon. The following rep-resentations can be selected (depending on the type and number of components connected to the IoT inter-face).

Parameter	Explanation
Visualiza-tions	Graphical representations, such as the live stream of a connected webcam.
Device Tree	Navigation area with all connected compo-nents (see section 8.2.2 "Navigation area in the left-hand area").
Logging View	**Logging** tab (see section 8.11 "Logging").
Message View	Currently pending messages (see section 8.2.4 "Message display").
Charts	Created charts (see section 8.13 "Charts").
Variable List	Current value of individual variables, such as the current temperature value of a con-nected temperature sensor.

Tab. 72: Selectable representations

Adding representations to a dashboard
- Ensure that the dashboard to which you want to add information is selected in the "Selected Board" col-umn.
- Select in the "Number of Columns" column the num-ber of columns into which the dashboard should be di-vided.

Note:
The number of columns can also be in-creased later. To reduce the number of col-umns, the columns to be deleted must not contain any representations (e.g. in column 3 when the dashboard should be reduced to two columns).

8 Operation

■ Click the "Edit" icon and select successively all representations to be displayed on the dashboard.
Each representation newly added to the dashboard is initially always added at the end of the first column. It can be moved from there to another location within the dashboard.

Moving representations on a dashboard

Representations are moved with the "drag-and-drop" principle.

■ Place the mouse cursor on the title line of a representation.
The mouse cursor changes to a cross arrow.

■ Press the left mouse key, keep it pressed and drag the representation to the required position, e.g. into a different column.

Before being stored, the position is shown with a dashed line; the other representations are moved down correspondingly.

It is not possible to place a representation totally free on the dashboard. If a representation is set at the lower edge of a column, it will be moved automatically as far as possible upwards, to the upper edge of the dashboard or to the lower edge of a representation already placed there.
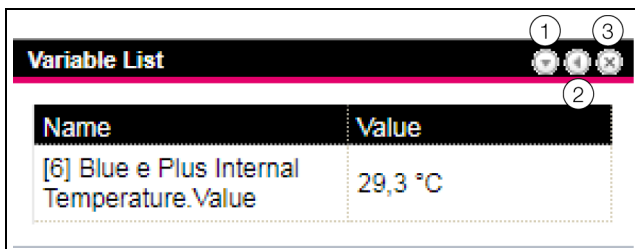
Fig. 41:   Representation icons

Legend
1   Open and close representations
2   Adapt a list with variables
3   Remove representations

Expanding and collapsing representations

Every representation can be expanded and collapsed via the title line. The representation, however, remains available, only the details are hidden.

■ Click the "Collapse" icon in the title line of a representation.
The representation on the title line is reduced.

■ To redisplay the representation: Click the "Expand" icon in the title line.
The representation reappears with all information; representations below on the dashboard are moved correspondingly.

Adapting a list with variables

Multiple, separate representations with individual variables are created. Alternatively, multiple variables can also be displayed in a representation.

■ Click the icon for adapting a list with variables (fig. 41, item 2) in the title line of a "Variable List" type representation.
The "Select Variables" dialogue is displayed.

■ Enter a meaningful name for the variable list in the "Title" field.

■ To change or delete an existing variable, click the line in which it is listed.
The "Variable Selection" dialogue is displayed.

■ Select in the "Device" field the component whose variable value you want to display.

■ Select in the "Variable" field the variable you want to display.

■ Alternatively, select the "None" entry in the "Device" field if you want to delete the variable from the representation.

■ To add another variable, click on the line with the "None" entry.
The "Variable Selection" dialogue also opens in which you can select the variable to be displayed.

■ Finally, click the "OK" button in the "Select Variables" dialogue to transfer the variable list to the representation.

☞ Note:
Changeable variable values can also changed directly from the dashboards, provided you have the appropriate user rights.

Changing the column widths

Within certain limits, the width of the individual columns can be changed. In particular for graphical representations, a minimum width is prescribed for the columns.

■ Place the mouse cursor between two columns.
The mouse cursor changes to a double arrow and the separator line between the columns is represented with a line.

■ Press the left mouse key, keep it pressed and drag the separator line to the required position.

If the minimum column width is undershot, the width is automatically changed appropriately.

Removing representations

Every representation can be removed completely from the dashboard via the title line.

■ Click the "X" icon at the far right in the title line of a representation.
The representation is removed directly from the dashboard without a prompt.

8.14.3 Saving a dashboard

To retain all changes permanently on a dashboard in accordance with section 8.14.2 "Configuring a dashboard" , the current view must be saved.

■ Click the "Save" icon in the header line of the dashboard.

The "Success" dialogue appears when the dashboard has been saved.

■ Click the "OK" button in the "Success" dialogue. The previously saved dashboard is displayed again.

☞ Note:
   – The current display of the individual components is not saved when a dashboard is saved. For example, the "Device Tree" initially appears collapsed for each call, except for the "Real Devices" and "Virtual Devices" levels.
   – When a dashboard is saved, all other dashboards are also saved automatically.
   – If (even different) dashboards are being edited concurrently by multiple users, the changes of all other users will be lost when saved (on all dashboards).

8.14.4 Calling a dashboard

After a login, similar to configuring, a dashboard can be called on a website (see section 8.14.2 "Configuring a dashboard"). In this case, the dashboard is opened in an **additional** browser window; the actual website also remains open after leaving the dashboard. The **Logout** button is then **not** displayed in the header line.

Alternatively, the login can be made directly on a dashboard when establishing an HTTP connection (see section 7.2.3 "Access to the IoT interface website").

■ After entering the login information, click the **Login to Dashboard** button.
   The dashboard view consisting only of the header line is displayed in the browser window.

■ Select in the "Select Dashboard" field the dashboard to be displayed.

The "Select Dashboard" column can be used to switch at anytime between the dashboards that can be enabled. If changes have been made to the most recently selected dashboard that have not yet been saved, the "Dashboard was Modified" dialogue opens when the dashboard is switched.

■ Click the **Yes** button if you do not want to save the changes and switch directly to the newly selected dashboard.

■ Click the **No** button to return to the still unsaved dashboard and then save it (see section 8.14.3 "Saving a dashboard").

8.14.5 Calling the website via a mobile terminal

The dashboard that was stored in the configuration is used to represent the website of the IoT interface on a mobile terminal (see section 8.6.7 "Mobile").

■ Call in the browser of your mobile terminal the address of the IoT interface, similarly as for a PC (see section 7.2.3 "Access to the IoT interface website").

■ Login with your user data.

The dashboard that was saved for the mobile terminals opens.

☞ Note:
   – If multiple variable lists with many variables are defined on the dashboard, delays when calling the mobile website can occur. This is independent of the mobile terminal power-er.
   – If a dashboard is changed, all users logged in via a mobile terminal will be logged out automatically.

8.14.6 Exiting a dashboard

A dashboard is exited by closing the browser window. If the dashboard view was enabled directly during the login by clicking the **Login to Dashboard** button, the **Logout** button is displayed at the left of the "Username" column in the header line.

■ Click the **Logout** button to log out completely from the IoT interface.
   To prevent an inadvertent logout from the website, this is not possible when the dashboard view was called for configuring a dashboard.

9 Blue e+ cooling unit

9.1 General

A maximum of two Blue e+ cooling units can be connected to the IoT interface (fig. 6, item 13 and 14). All settings, such as limit values for warning and alarm messages, are made at the "Blue e Plus" level on the **Observation** tab.

The following sections 9.2 "Device" to 9.8 "Setup" provide detailed descriptions for only the editable parameters. There are also display values provided only for information purposes.

In general, the "DescName" parameter is provided for most entries. It can contain an associated individual description.

Parameter	Explanation
DescName	Individual description of the associated value, such as a temperature value, fan.

Tab. 73: "DescName" parameter

The "Error Info" parameter is also displayed for most components. In the event of a fault, the internal error number displayed here helps Rittal Service for extended troubleshooting.

Parameter	Explanation
Error Info	Internal error number for contact with Rittal Service.

Tab. 74: "Error Info" parameter

9.2 Device

General settings for the cooling unit are configured at the "Device" level.

Parameter	Explanation
Description	Individual description of the cooling unit.
Location	Location of the cooling unit.

Tab. 75: Settings at the "Device" level

Parameters that provide detailed information about the cooling unit, such as the deployed software and hardware versions, are also displayed. It is advisable to have such information on hand, in particular, to ensure fast troubleshooting for queries with Rittal.

9.3 Information

Further information about the cooling unit is configured at the "Information" level.

Parameter	Explanation
Serial Number	Serial number of the cooling unit.

Tab. 76: Displays at the "Information" level

Parameter	Explanation
Last Update Date	Last update YYYY-MM-DD
Last Maintenance Date	Last maintenance YYYY-MM-DD
Device Operating Time	Operating hours of the cooling unit.

Tab. 76: Displays at the "Information" level

9.4 Internal Temperature

The settings for the temperature with which the air is drawn from the enclosure into the cooling unit are made at the "Internal Temperature" level.

Note that the entered limit values are stored only on the IoT interface and can be changed only there. If, for example, the upper limit temperature for an alarm message is overshot, this message is **not** displayed on the display of the cooling unit.

Parameter	Explanation
SetPtHigh-Alarm	The upper limit temperature that triggers an alarm message when overshot.
SetPtHigh-Warning	The upper limit temperature that triggers a warning message when overshot.
SetPtLow-Warning	The lower limit temperature that triggers a warning message when undershot.
SetPtLow-Alarm	The lower limit temperature that triggers an alarm message when undershot.
Hysteresis	The required percentage deviation for undershooting or overshooting the limit temperature for a status change (see section 16 "Glossary").

Tab. 77: Settings at the "Internal Temperature" level

The following parameters are also displayed for the temperature value:

Parameter	Explanation
Value	Currently measured temperature value.
Status	Current status of the temperature value.

Tab. 78: Displays at the "Internal Temperature" level

9.5 Ambient Temperature

The settings for the temperature measured with the temperature sensor located on the outer fan of the cooling unit are made at the "Ambient Temperature" level.

Note that the entered limit values are stored only on the IoT interface and can only be changed there. If, for example, the upper limit temperature for an alarm message is overshot, this message is **not** displayed on the display of the cooling unit.

Parameter	Explanation
SetPtHigh-Alarm	The upper limit temperature that triggers an alarm message when overshot.
SetPtHigh-Warning	The upper limit temperature that triggers a warning message when overshot.
SetPtLow-Warning	The lower limit temperature that triggers a warning message when undershot.
SetPtLow-Alarm	The lower limit temperature that triggers an alarm message when undershot.
Hysteresis	The required percentage deviation for undershooting or overshooting the limit temperature for a status change (see section 16 "Glossary").

Tab. 79: Settings at the "Ambient Temperature" level

The following parameters are also displayed for the temperature value:

Parameter	Explanation
Value	Currently measured temperature value.
Status	Current status of the temperature value.

Tab. 80: Displays at the "Ambient Temperature" level

9.6 External Temperature

The settings for the temperature measured with an external 3124.400 temperature sensor in the Blue e+ cooling unit, such as at a so-called hot spot in the enclosure, are made at the "External Temperature" level.

Note that the entered limit values are stored only on the IoT interface and can only be changed there. If, for example, the upper limit temperature for an alarm message is overshot, this message is **not** displayed on the display of the cooling unit.

Parameter	Explanation
SetPtHigh-Alarm	The upper limit temperature that triggers an alarm message when overshot.
SetPtHigh-Warning	The upper limit temperature that triggers a warning message when overshot.
SetPtLow-Warning	The lower limit temperature that triggers a warning message when undershot.
SetPtLow-Alarm	The lower limit temperature that triggers an alarm message when undershot.
Hysteresis	The required percentage deviation for undershooting or overshooting the limit temperature for a status change (see section 16 "Glossary").

Tab. 81: Settings at the "External Temperature" level

The following parameters are also displayed for the temperature value:

Parameter	Explanation
Value	Currently measured temperature value.
Status	Current status of the temperature value.

Tab. 82: Displays at the "External Temperature" level

9.7 Monitoring

Information about various components of the cooling unit can be displayed at the "Monitoring" level.

9.7.1 Cooling

The information that can be viewed on the start screen of the cooling unit is displayed at the "Cooling" level.

Parameter	Explanation
Operating Mode	Current cooling type (compressor operation with or without support of the heat pipe, only with heat pipe or no cooling)
Selftest	Whether or not selftest active.
Selftest Progress	Progress of an active selftest.
Capacity	Cooling capacity in watts.
Cooling Capacity	Cooling capacity in %.
EER	Current EER value.
EER 24h	Average EER value over the previous 24 hours.
Status	Current status of the cooling unit.

Tab. 83: Displays at the "Cooling" level

9.7.2 Internal Air Circuit

Information about the internal circuit is displayed at the "Internal Air Circuit" level.

Parameter	Explanation
Value	Current evaporation temperature.
Status	Current status of the internal circuit.

Tab. 84: Displays at the "Internal Air Circuit" level

9.7.3 External Air Circuit

Information about the external circuit is displayed at the "External Air Circuit" level.

Parameter	Explanation
Value	Current condensation temperature.
Status	Current status of the external circuit.

Tab. 85: Displays at the "External Air Circuit" level

9.7.4 Internal Fan

Information about the internal fan is displayed at the "Internal Fan" level.

Parameter	Explanation
Value	Current speed of the internal fan in %.
Operating Time	Operating hours of the internal fan.
Status	Current status of the internal fan.

Tab. 86: Displays at the "Internal Fan" level

9.7.5 External Fan

Information about the external fan is displayed at the "External Fan" level.

Parameter	Explanation
Value	Current speed of the external fan in %.
Operating Time	Operating hours of the external fan.
Status	Current status of the external fan.

Tab. 87: Displays at the "External Fan" level

9.7.6 Compressor

Information about the compressor is displayed at the "Compressor" level.

Parameter	Explanation
Speed	Speed of the compressor in %.
Operating Time	Operating hours of the compressor.
Status	Current status of the compressor.

Tab. 88: Displays at the "Compressor" level

9.7.7 EEV

Information about the electronic expansion valve of the cooling unit is displayed at the "EEV" level.

Parameter	Explanation
Value	Current temperature at the expansion valve.
Position	Current degree of opening of the expansion valve in %.
Status	Current status of the expansion valve.

Tab. 89: Displays at the "EEV" level

9.7.8 Filter

Information about the filter mat monitoring is displayed at the "Filter" level.

Parameter	Explanation
Status	Current status of the filter mat monitoring.

Tab. 90: Displays at the "Filter" level

9.7.9 Door

Information about the door limit switch is displayed at the "Door" level.

Parameter	Explanation
Status	"Open" or "Closed" for installed door limit switch.

Tab. 91: Displays at the "Door" level

9.7.10 Electronics

Information about the electronic unit is displayed at the "Electronics" level.

Parameter	Explanation
Status	Current status of the electronic unit.

Tab. 92: Displays at the "Electronics" level

9.7.11 Condensate

Information about the condensate evaporation is displayed at the "Condensate" level.

Parameter	Explanation
Status	Current status of the condensate evaporation.

Tab. 93: Displays at the "Condensate" level

9.7.12 System Messages

Further information about the system messages of the cooling unit is displayed at the "System Messages" level.

Parameter	Explanation
Status	Current status of the system messages.

Tab. 94: Displays at the "System Messages" level

9.7.13 Input Power

The power consumption of the cooling unit is the only value displayed at the "Input Power" level.

Parameter	Explanation
Input Power	Power consumption of the cooling unit in watts.

Tab. 95: Displays at the "Input Power" level

9.8 Setup

General settings for the cooling unit are configured at the "Setup" level.

Parameter	Explanation
Customer Name	Customer-specified designation for the cooling unit to differentiate the individual devices.
Mode	Selected control mode (internal temperature, external sensor or exhaust temperature).
Setpoint	Setpoint for the temperature control.
Alarm Threshold	The threshold used for an alarm message (overtemperature). This offset value can be set between 3…15 and is added to the setpoint.
Alarm Tolerance Filter	Alarm tolerance of the filter mat monitoring. The tolerance can be set in five levels or the filter mat monitoring deactivated. 1 = very low 2 = low 3 = medium 4 = high 5 = very high

Tab. 96:   Settings at the "Setup" level

9.8.1   Standard Control

Settings for the temperature values of the cooling unit for the "Internal temperature" and "External sensor" control modes can be performed at the "Standard Control" level.

Parameter	Explanation
Setpoint	Setpoint for the temperature control.
Alarm Threshold	The threshold used for an alarm message (overtemperature). This offset value can be set between 3…15 and is added to the setpoint.

Tab. 97:   Settings at the "Standard Control" level

9.8.2   Outlet Temperature

Settings for the temperature values of the cooling unit for the "Outlet Temperature" control mode can be performed at the "Outlet Temperature" level.

Parameter	Explanation
Setpoint	Setpoint for the temperature control.
Alarm Threshold	The threshold used for an alarm message (overtemperature). This offset value can be set between 12…24 and is added to the setpoint.

Tab. 98:   Settings at the "Outlet Temperature" level

10 Chiller Blue e+

10.1 General

A maximum of two Blue e+ chillers can be connected to the IoT interface (fig. 6, item 13 and 14). All settings, such as limit values for warning and alarm messages, are performed at the "Blue e Plus Chiller" level on the **Observation** tab.

The following sections 10.2 "Device" to 10.8 „Setup" provide detailed descriptions for only the editable parameters. There are also display values provided only for information purposes.

In general, the "DescName" parameter is provided for most entries. It can contain an associated individual description.

Parameter	Explanation
DescName	Individual description of the associated value, such as a temperature value, fan.

Tab. 99: "DescName" parameter

The "Error Info" parameter is also displayed for most components. In the event of a fault, the internal error number displayed here helps Rittal Service for extended troubleshooting.

Parameter	Explanation
Error Info	Internal error number for contact with Rittal Service.

Tab. 100: "Error Info" parameter

10.2 Device

General settings for the chiller are performed at the "Device" level.

Parameter	Explanation
Description	Individual description of the chiller.
Location	Location of the chiller.

Tab. 101: Settings at the "Device" level

Parameters that provide detailed information about the chiller, such as the deployed software and hardware versions, are also displayed. It is advisable to have such information on hand, in particular, to ensure fast troubleshooting for queries with Rittal.

10.3 Information

Further information about the chiller is displayed at the "Information" level.

Parameter	Explanation
Serial Number	Serial number of the chiller.

Tab. 102: Displays at the "Information" level

Parameter	Explanation
Last Update date	Last update YYYY-MM-DD
Last Maintenance Date	Last maintenance YYYY-MM-DD
Device Operating Time	Operating hours of the chiller.

Tab. 102: Displays at the "Information" level

10.4 Medium Outlet Temperature

The settings for the medium temperature are performed at the "Medium Outlet Temperature" level.

Note that the entered limit values are stored only on the IoT interface and can be changed only there. If, for example, the upper limit temperature for an alarm message is overshot, this message is not displayed on the display of the chiller.

Parameter	Explanation
SetPtHigh-Alarm	The upper limit temperature that triggers an alarm message when overshot.
SetPtHigh-Warning	The upper limit temperature that triggers a warning message when overshot.
SetPtLow-Warning	The lower limit temperature that triggers a warning message when undershot.
SetPtLow-Alarm	The lower limit temperature that triggers an alarm message when undershot.
Hysteresis	The required percentage deviation for undershooting or overshooting the limit temperature for a status change (see section 16 "Glossary").

Tab. 103: Settings at the "Medium Outlet Temperature" level

The following parameters are also displayed for the medium temperature:

Parameter	Explanation
Value	Currently measured temperature value.
Status	Current status of the temperature value.

Tab. 104: Displays at the "Medium Outlet Temperature" level

10.5 Ambient Temperature

Settings for the ambient temperature are performed at the "Ambient Temperature" level.

Note that the entered limit values are stored only on the IoT interface and can be changed only there. If, for example, the upper limit temperature for an alarm message is overshot, this message is **not** displayed on the display of the chiller.

Parameter	Explanation
SetPtHigh-Alarm	The upper limit temperature that triggers an alarm message when overshot.
SetPtHigh-Warning	The upper limit temperature that triggers a warning message when overshot.
SetPtLow-Warning	The lower limit temperature that triggers a warning message when undershot.
SetPtLow-Alarm	The lower limit temperature that triggers an alarm message when undershot.
Hysteresis	The required percentage deviation for undershooting or overshooting the limit temperature for a status change (see section 16 "Glossary").

Tab. 105: Settings at the "Ambient Temperature" level

The following parameters are also displayed for the temperature value:

Parameter	Explanation
Value	Currently measured temperature value.
Status	Current status of the temperature value.

Tab. 106: Displays at the "Ambient Temperature" level

10.6 External Temperature
The settings for the temperature measured with an external temperature sensor for tempering the cooling medium based on the temperature in the installation room of the chiller are performed at the "External Temperature" level.

Note that the entered limit values are stored only on the IoT interface and can be changed only there. If, for example, the upper limit temperature for an alarm message is overshot, this message is **not** displayed on the display of the chiller.

Parameter	Explanation
SetPtHigh-Alarm	The upper limit temperature that triggers an alarm message when overshot.
SetPtHigh-Warning	The upper limit temperature that triggers a warning message when overshot.
SetPtLow-Warning	The lower limit temperature that triggers a warning message when undershot.
SetPtLow-Alarm	The lower limit temperature that triggers an alarm message when undershot.
Hysteresis	The required percentage deviation for undershooting or overshooting the limit temperature for a status change (see section 16 "Glossary").

Tab. 107: Settings at the "External Temperature" level

The following parameters are also displayed for the temperature value:

Parameter	Explanation
Value	Currently measured temperature value.
Status	Current status of the temperature value.

Tab. 108: Displays at the "External Temperature" level

10.7 Monitoring
All information that can be viewed from the display of the chiller as well as several additional parameters can read directly at the "Monitoring" level.

10.7.1 Cooling
The information that can be viewed on the start screen of the chiller is displayed at the "Cooling" level.

Parameter	Explanation
Operating Mode	The current cooling type (active cooling, cooling for switched-off compressor ("Free Cooling" option), hybrid operation or no cooling).
Selftest	Whether or not selftest active.
Selftest Progress	Progress of an active selftest.
Capacity	Cooling capacity in watts.
EER	Current EER value.
EER 24h	Average EER value over the previous 24 hours.
Status	Current chiller status.

Tab. 109: Displays at the "Cooling" level

10.7.2 Evaporation Temperature
Information about the evaporation temperature is displayed at the "Evaporation Temperature" level.

Parameter	Explanation
Value	Current evaporation temperature.
Status	Current status of the evaporation temperature.

Tab. 110: Displays at the "Evaporation Temperature" level

10.7.3 Tank Level
Information about the filling level of the cooling medium is displayed at the "Tank Level" level.

Parameter	Explanation
Status	Current filling level status.

Tab. 111: Displays at the "Tank Level" level

10.7.4 Condenser Temperature

Information about the condenser temperature is displayed at the "Condenser Temperature" level.

Parameter	Explanation
Value	Current condensation temperature.
Status	Current status of the condenser temperature.

Tab. 112: Displays at the "Condenser Temperature" level

10.7.5 Flow

Settings for the flow of the cooling medium are performed at the "Flow" level.

Parameter	Explanation
SetPtLow-Warning	The lower limit value for the flow for which a warning message is issued when undershot.

Tab. 113: Settings at the "Flow" level

The following parameters are also displayed for the flow of the cooling medium.

Parameter	Explanation
Value	Current flow value.
Status	Current status of the flow.

Tab. 114: Displays at the "Flow" level

10.7.6 Pump

Information about the cooling medium pump is displayed at the "Pump" level.

Parameter	Explanation
Status	Current status of the cooling medium pump.

Tab. 115: Displays at the "Pump" level

10.7.7 Fan

Information about the condenser fan is displayed at the "Fan" level.

Parameter	Explanation
Value	Current speed of the internal fan in %.
Operating Time	Operating hours of the internal fan.
Self Adaption	Automatic adaptation of the fan speed for contaminated filter mat.
Status	Current status of the condenser fan.

Tab. 116: Displays at the "Fan" level

10.7.8 Compressor

Information about the compressor is displayed at the "Compressor" level.

Parameter	Explanation
Speed	Speed of the compressor in %.
Operating Time	Operating hours of the compressor.
Self Adaption	Automatic adaptation of the compressor for contaminated filter mat.
Status	Current status of the compressor.

Tab. 117: Displays at the "Compressor" level

10.7.9 EEV

Information about the electronic expansion valve of the chiller is displayed at the "EEV" level.

Parameter	Explanation
Value	Current temperature at the expansion valve.
Position	Current degree of opening of the expansion valve in %.
Status	Current status of the expansion valve.

Tab. 118: Displays at the "EEV" level

10.7.10 Freecooling Valve

Information about the "Free Cooling" option of the chiller is displayed at the "Freecooling Valve" level.

Parameter	Explanation
Position	Current degree of opening of the valve for free cooling in %.
Status	Current status of the expansion valve.

Tab. 119: Displays at the "Freecooling Valve" level

10.7.11 Filter

Information about the filter mat monitoring is displayed at the "Filter" level.

Parameter	Explanation
Status	Current status of the filter mat monitoring.

Tab. 120: Displays at the "Filter" level

10.7.12 Remote Input

Information about evaluation of the external enable signal (remote operation) is displayed at the "Remote Input" level.

Parameter	Explanation
Status	Current status of the remote operation.

Tab. 121: Displays at the "Remote Input" level

10.7.13 Electronics

Information about the electronic unit is displayed at the "Electronics" level.

Parameter	Explanation
Status	Current status of the electronic unit.

Tab. 122: Displays at the "Electronics" level

10.7.14 Heater

Information about the "Tank heating" option is displayed at the "Heater" level.

Parameter	Explanation
Status	Current status of the tank heating.

Tab. 123: Displays at the "Heater" level

10.7.15 System Messages

Further information about the system messages of the chiller is displayed at the "System Messages" level.

Parameter	Explanation
Status	Current status of the system messages.

Tab. 124: Displays at the "System Messages" level

10.7.16 Input Power

The power consumption of the chiller is the only value displayed at the "Input Power" level.

Parameter	Explanation
Input Power	Power consumption of the chiller in watts.

Tab. 125: Displays at the "Input Power" level

10.8 Setup

General settings for the chiller are performed at the "Setup" level.

Parameter	Explanation
Customer Name	Customer-specified designation for the chiller to differentiate the individual units.
Mode	Select the control mode (medium temperature or external sensor).
Remote	Configure how the external enabling signal should be evaluated.

Tab. 126: Settings at the "Setup" level

10.8.1 Alarm Threshold

The threshold values for the alarm messages are configured at the "Alarm Threshold" level.

Parameter	Explanation
Subnormal Command	Select whether a "too low" temperature ("On" setting) or an overtemperature ("Off" setting) should trigger an alarm.
Overtemperature	Threshold value for an overtemperature for which an alarm is triggered.
Subnormal Temp	Threshold value for a "too low" temperature for which an alarm is triggered.

Tab. 127: Settings at the "Alarm Threshold" level

10.8.2 Medium Temp Settings

The setpoint for the medium temperature is the only value specified at the "Medium Temp Settings" level.

Parameter	Explanation
Setpoint	Medium temperature

Tab. 128: Settings at the "Medium Temp Settings" level

10.8.3 External Sensor Settings

The settings for tempering the cooling medium based on the temperature in the installation room of the chiller are performed at the "External Sensor Settings" level.

Parameter	Explanation
Difference	The difference between the temperature of the cooling medium and the room temperature.
Min	Minimum temperature of the cooling medium.
Max	Maximum temperature of the cooling medium.

Tab. 129: Settings at the "External Sensor Settings" level

11   Blue e cooling unit

11.1   General
A cooling unit of the Blue e series can be connected at the IoT interface using the "Blue e IoT adaptor" (fig. 6, item 13). All settings, such as limit values for warning and alarm messages, are performed at the "Blue e Master" level on the **Observation** tab.

This cooling unit can act as master for as many as 9 further slave units. The master and the slave units can be connected to the X2 unit interface with the bus cable. The parameters and display values described below are displayed for the slave units in the "Blue e Slave 1" to maximum "Blue e Slave 9" levels (depending on the number of slave units).

The following sections 11.2 "Device" to 11.6 "Setup" provide detailed descriptions for only the editable parameters. There are also display values provided only for information purposes.

In general, the "DescName" parameter is provided for most entries. It can contain an associated individual description.

Parameter	Explanation
DescName	Individual description of the associated value, such as a temperature value, fan.

Tab. 130: "DescName" parameter

The "Error Info" parameter is also displayed for most components. In the event of a fault, the internal error number displayed here helps Rittal Service for extended troubleshooting.

Parameter	Explanation
Error Info	Internal error number for contact with Rittal Service.

Tab. 131: "Error Info" parameter

11.2   Device
General settings for the cooling unit are configured at the "Device" level.

Parameter	Explanation
Description	Individual description of the cooling unit.
Location	Location of the cooling unit.

Tab. 132: Settings at the "Device" level

Parameters that provide detailed information about the cooling unit, such as the deployed software and hardware versions, are also displayed. It is advisable to have such information on hand, in particular, to ensure fast troubleshooting for queries with Rittal.

11.3   Internal Temperature
The settings for the temperature with which the air is drawn from the enclosure into the cooling unit are made at the "Internal Temperature" level.

Note that the entered limit values are stored only on the IoT interface and can be changed only there. If, for example, the upper limit temperature for an alarm message is overshot, this message is **not** displayed on the display of the cooling unit.

Parameter	Explanation
SetPtHigh-Alarm	The upper limit temperature that triggers an alarm message when overshot.
SetPtHigh-Warning	The upper limit temperature that triggers a warning message when overshot.
SetPtLow-Warning	The lower limit temperature that triggers a warning message when undershot.
SetPtLow-Alarm	The lower limit temperature that triggers an alarm message when undershot.
Hysteresis	The required percentage deviation for undershooting or overshooting the limit temperature for a status change (see section 16 "Glossary").

Tab. 133: Settings at the "Internal Temperature" level

The following parameters are also displayed for the temperature value:

Parameter	Explanation
Value	Currently measured temperature value.
Status	Current status of the temperature value.

Tab. 134: Displays at the "Internal Temperature" level

11.4   Ambient Temperature
The settings for the temperature measured with the temperature sensor located on the outer fan of the cooling unit are made at the "Ambient Temperature" level.

Note that the entered limit values are stored only on the IoT interface and can only be changed there. If, for example, the upper limit temperature for an alarm message is overshot, this message is **not** displayed on the display of the cooling unit.

Parameter	Explanation
SetPtHigh-Alarm	The upper limit temperature that triggers an alarm message when overshot.
SetPtHigh-Warning	The upper limit temperature that triggers a warning message when overshot.
SetPtLow-Warning	The lower limit temperature that triggers a warning message when undershot.

Tab. 135: Settings at the "Ambient Temperature" level

Parameter	Explanation
SetPtLow-Alarm	The lower limit temperature that triggers an alarm message when undershot.
Hysteresis	The required percentage deviation for undershooting or overshooting the limit temperature for a status change (see section 16 "Glossary").

Tab. 135: Settings at the "Ambient Temperature" level

The following parameters are also displayed for the temperature value:

Parameter	Explanation
Value	Currently measured temperature value.
Status	Current status of the temperature value.

Tab. 136: Displays at the "Ambient Temperature" level

11.5 Monitoring
Information about various components of the cooling unit can be displayed at the "Monitoring" level.

11.5.1 Internal Air Circuit
Information about the internal circuit is displayed at the "Internal Air Circuit" level.

Parameter	Explanation
Value	Current evaporation temperature.
Status	Current status of the internal circuit.

Tab. 137: Displays at the "Internal Air Circuit" level

11.5.2 External Air Circuit
Information about the external circuit is displayed at the "External Air Circuit" level.

Parameter	Explanation
Value	Current condensation temperature.
Status	Current status of the external circuit.

Tab. 138: Displays at the "External Air Circuit" level

11.5.3 Internal Fan
Information about the internal fan is displayed at the "Internal Fan" level.

Parameter	Explanation
Value	Current switching state of the internal fan ("On" or "Off").
Status	Current status of the internal fan.

Tab. 139: Displays at the "Internal Fan" level

11.5.4 External Fan
Information about the external fan is displayed at the "External Fan" level.

Parameter	Explanation
Value	Current switching state of the external fan ("On" or "Off").
Status	Current status of the external fan.

Tab. 140: Displays at the "External Fan" level

11.5.5 Compressor
Information about the compressor is displayed at the "Compressor" level.

Parameter	Explanation
Value	Current switching state of the compressor ("On" or "Off").
Status	Current status of the compressor.

Tab. 141: Displays at the "Compressor" level

11.5.6 Filter
Information about the filter mat monitoring is displayed at the "Filter" level.

Parameter	Explanation
Status	Current status of the filter mat monitoring.

Tab. 142: Displays at the "Filter" level

11.5.7 Door
Information about the door limit switch is displayed at the "Door" level.

Parameter	Explanation
Status	"Open" or "Closed" for installed door limit switch.

Tab. 143: Displays at the "Door" level

11.5.8 Condensate
Information about the condensate evaporation is displayed at the "Condensate" level.

Parameter	Explanation
Status	Current status of the condensate evaporation.

Tab. 144: Displays at the "Condensate" level

11.5.9 System Messages
Further information about the system messages of the cooling unit is displayed at the "System Messages" level.

Parameter	Explanation
Status	Current status of the system messages.

Tab. 145: Displays at the "System Messages" level

11.6 Setup

General settings for the cooling unit are configured at the "Setup" level.

Parameter	Explanation
Setpoint	Setpoint for the temperature control.
Alarm Threshold	The threshold used for an alarm message (overtemperature). This offset value can be set between 3…15 and is added to the setpoint.
Hysteresis	Switching difference (hysteresis) that can be set between 2…10.

Tab. 146: Settings at the "Setup" level

12 Updates and data backup

Because FTP access to the IoT interface is required only to perform software updates and for data backup, the access should be generally blocked and briefly activated only for these tasks (see section 8.5.4 "File Transfer Configuration").

12.1 Establishing an FTP connection

To establish an FTP connection, you require the IP address of the IoT interface. If this address is not known, because, for example, the DHCP function is activated, read the IP address from the display of a connected cooling unit or chiller. Alternatively, you can first establish a connection via the USB interface (see section 7.4.2 "Establishing the connection"). This access is made directly so that you can use this connection to determine the IP address of the IoT interface.

An appropriate FTP client program is also required to establish an FTP connection (or SFTP connection). Rittal recommends the use of FileZilla.

- Install an FTP client program on the computer to be used to establish the FTP connection to the IoT interface.
- Establish the network connection between the IoT interface and the computer.
- Ensure that the IoT interface and the computer have the same address space.
- Enter the appropriate access data in the FTP program. The following access data is entered by default:
  – Host: 192.168.0.190
  – Username: admin
  – Password: admin
  – Port: 21 (FTP) or 22 (SFTP)
- Start the connection between the computer and the IoT interface; you may need to activate the setting: "Bypass Proxy settings".
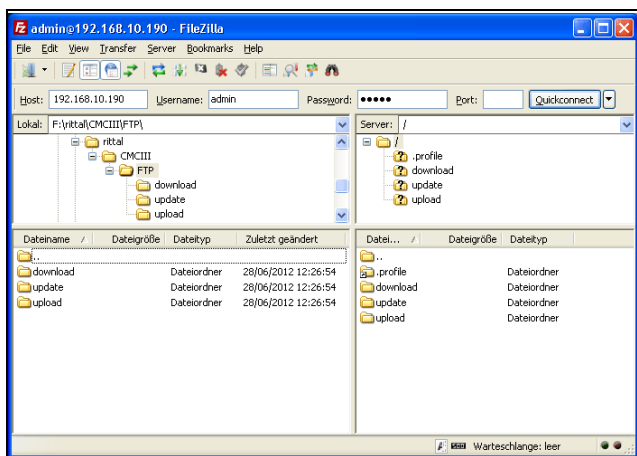

Fig. 42:   FileZilla

The left-hand subwindow now shows the folder structure and the content of the PC; the right-hand subwindow contains the equivalent content of the IoT interface.

12.2 Perform an update

12.2.1 Notes for performing an update

Observe the following security notes for performing an update.

☞ Note:
The user is responsible for performing the update in the associated network environment.

Before starting an update, ensure that the security application connected to the IoT interface can be interrupted for the duration of the update.

Ensure that you have access to the IoT interface, because, for example, you will need to check the current status on-site.

During the update process, the power to the IoT interface must not be interrupted under any circumstances.

If the update is performed using the USB connection, the USB device must not be removed during the update process.

None of the connected components for the IoT interface may be disconnected during the update process.

Under some circumstances, an update can reset the IoT interface settings to their factory state.

In addition to the two possibilities described in this section to update via USB or (S)FTP, an update is also possible via the IoT interface website (see section 8.6.5 "Firmware update").

12.2.2 Downloading the software update

A software update for the IoT interface can be downloaded from the Internet address specified in section 17 "Customer service addresses". The update will be provided as a tar archive.

- Download the current software version from the website and save it on your computer.

12.2.3 Update via USB

Observe the following notes for updating the IoT interface via USB:

– The USB storage medium used for the update must be formatted as FAT.
– In addition to the file for the software update, any other data may be present on the USB storage medium.

Proceed as follows to perform the update:

- Copy the downloaded tar file into the root directory of the USB storage medium.
- Start the IoT interface if necessary.
- Wait until the multi-LED on the front lights green, orange or red continually or is flashing.
- Then insert the USB storage medium in the appropriate USB slot of the IoT interface.

The update process starts automatically after a few minutes. This is indicated with a red flashing of the multi-LED (so-called heartbeat, alternately long and short).

If the current software version (or a later version) is already installed on the IoT interface, no update will be performed.

Depending on the number of connected sensors that are also updated, the complete update process takes approx. 15 minutes.

12.2.4 Update via FTP or SFTP

Proceed as follows to perform the update:
- Establish a connection between a PC and the IoT interface (see section 12.1 "Establishing an FTP connection").
- Switch to the "update" folder in the right-hand subwindow (IoT interface).
- In the left-hand window (PC), switch to the folder in which you stored the update file previously.
- Right-click the update file and select the "Upload" action.

The update process starts automatically after a few seconds. This is indicated with a red flashing of the multi-LED (so-called heartbeat, alternately long and short).

12.2.5 Perform the update

The system reboots automatically when the IoT interface update has completed. On completion of the booting, the LED on the front indicates the IoT interface status: green, orange or red.

An update of the connected sensors may then be performed. During this process, the status LED of the sensors flashes fast, the status LED of the IoT interface flashes white. The sensor currently being updated also flashes violet.

> **Note:**
> Under no circumstances may the sensors be disconnected from the IoT interface during the update.

The update of the IoT interface is completed when the following conditions are satisfied:
1. The LED on the front of the IoT interface lights to indicate the status: green, orange or red.
2. The LEDs on the bus connection of the sensors light green.
3. The multi-LEDs of the sensors behind the front cover flash blue.

The progress of the update is logged in the "*.status" file. Depending on the type of the update process, this file is located either in the root directory of the USB storage medium or in the Update folder of the IoT interface. The status file is a text file that can be opened with an editor or a text processing program.
- For an update via (S)FTP or the website: Transfer this file using an FTP connection from the Update folder of the IoT interface to a PC.
- For an update via USB: Copy instead from the USB storage medium to a PC.
- Open the file with an editor and check whether the update was performed successfully or whether error messages have been issued.

> **Note:**
> Finally press the "Ctrl"+"F5" key combination in the browser to reload the complete website from the IoT interface. All the changes now act.

12.3 Performing a data backup

Rittal recommends that a data backup of the IoT interface configuration is made regularly (see section 12.2 "Perform an update").

Proceed as follows to perform a data backup:
- Establish an FTP connection between a PC and the IoT interface (see section 12.1 "Establishing an FTP connection").
- In the left-hand subwindow (PC), switch to any folder in which you want to store the data backup.
- Switch to the "download" folder in the right-hand subwindow (IoT interface).
- Right-click the "cmcIIIsave.cfg" file and select the "Download" action.

The settings and configurations of all connected components as displayed currently for the individual sensors on the **Observation** (see section 8.3 "Observation tab") and **Configuration** (see section 8.4 "Configuration tab") tabs are stored in this file.

For a second IoT interface, this configuration file can be placed for transfer similarly in the upload directory. All general settings (other than the TCP/IP settings) are then taken from this file. If the same sensors, etc. are also installed in the same sequence on the second IoT interface, all limit values of these sensors are also transferred.

> **Note:**
> A configuration file which was saved by a IoT interface with an older software version cannot be transferred to a IoT interface with a more recent software version.

12.4 Local saving of supplementary information

Folder "download"

Similar to a data backup, you can download further files from the "download" folder to the PC. This is a text file with the following content:

1. "Devices.cmc3": The configurations of all connected components as displayed for the individual sensors on the **Observation** (see section 8.3 "Observation tab") and **Configuration** (see section 8.4 "Configuration tab") tabs.
2. "Logging.cmc3": Complete, i.e. unfiltered, log information of the IoT interface (see section 8.11 "Logging").
3. "cmcIIIsave.cfg": Settings and configurations for all connected components (see section 12.3 "Performing a data backup").
4. "syslog.cmc": File for transferring the syslog information.

■ After the download to the PC, if necessary, rename the files to uniquely identify the various file versions.

Folder "download/docs"

Further files can be downloaded from the "download/docs" folder. Text files are also involved:

1. "Configuration.cmc3": Configuration of the "Processing Unit" complete system as can also be displayed on the **Configuration** tab (see section 8.4 "Configuration tab").
2. "Configuration.cmc3.history": List of all configuration changes. Every change is identified with the revision version as well as with the date and time of the predecessor version and the current version.
3. "OID_List.cmc3": Listing of all OIDs of the IoT interface variables and the connected components as required for query via SNMP.
4. "OID_List.changes": List of changes to all OIDs during the last update.
5. "OID_List.old": List of changes to all OIDs before the last update.
6. "sysinfo.txt": Information on the software versions of both file systems in the IoT interface, and which of the two file systems is active.
7. "system.log": Log information on all system actions such as configuration changes.
8. "ModbusMap.cmc3": List of all variables that can be queried via Modbus.

Folder "download/docs/Configuration.cmc3.repository"

This folder additionally contains individual files for all the configuration changes implemented (patch files).

Folder "download/docs/lists"

The "download/docs/lists" folder contains CSV files, which may be viewed after downloading e.g. with a spreadsheet program such as Excel.

1. "cmcIIIDevList.csv": List of all sensors and units connected to the system.
2. "cmcIIIVarList.csv": List of all variables provided by the system.

Folder "download/usb-stick" or "download/sd-card"

If you have connected an external storage medium (USB stick or SD card) to the IoT interface, data from the charts (see section 8.13 "Charts") and from a webcam, if connected (see section 8.3.5 "Webcam") will be recorded there.

■ Download the data from these directories for further evaluation.

13 Storage and disposal

13.1 Storage

If the device is not used for a long period, Rittal recommends that it is disconnected from the mains power supply and protected from dampness and dust.

13.2 Disposal

Because the IoT interface consists mainly of the "housing" and "circuit board" parts, the device must be given to the electronic waste recycling system for disposal.

14   Technical specifications

Technical specifications		IoT interface
Model No.		3124300
W x H x D (mm)		18 x 117 x 120
Temperature range		0°C…+70°C
Operating humidity range		10%…90% relative humidity, non-condensing
Degree of protection		IP 20 to IEC 60 529
Sensors / CAN bus connection units		max. 32
Max. overall cable length for CAN bus		2 x 50 m
Interfaces	Network interface (RJ 45)	Ethernet in accordance with IEEE 802.3 via 10/100/1000BaseT
	USB interface (front)	Micro USB for setting the system
	USB interface (top)	for USB stick for data recording and SW updates up to 32 GB
	Front SD-HC slot	1 to 32 GB for data recording
Inputs and outputs	CAN bus (RJ 45)	Two, each with maximum 16 sensors = 32 sensors in total
Operation/signals	Keys	One acknowledge key
	Hidden reset key	One service key
	LED displays	OK / warning / alarm / network status
Protocols	Ethernet	SNMP, SNMPv1, SNMPv2c, SNMPv3, OPC-UA, Modbus/TCP, Radius, Telnet, SSH, (S)FTP, HTTP(S), NTP, DHCP, DNS, SMTP, Syslog, LDAP
Power supply	Input 24 V ⎓ (terminals)	One for direct connection or for connecting the CMC III power pack
	Connector X6	One for the connection at a Blue e+ cooling unit or Blue e+ chiller
Functions	User administration	LDAP, Radius
	User interface	Integral web server
	Control desk connection	Integral OPC server (OPC-UA)

Tab. 147: Technical specifications

15   Accessories

A wide range of Rittal sensors, actuators and systems for access monitoring can be connected via the CAN bus interface. A selection of sensors and systems for access monitoring follows. A complete overview of all sensors is available at the Internet address in section 17 "Customer service addresses".

Model No.	Description
7030.110	CMC III temperature sensor Monitor the ambient temperature in the enclosure (internal or external sensor). An external sensor must be used for applications without active air flow.
7030.111	CMC III temperature/humidity sensor Monitor the ambient temperature and humidity in the enclosure. Unlike 7030.110, no external connection.
7030.120	Infrared access sensor Monitor using infrared light (infrared diode with receiver and reflector) whether the enclosure door is open or closed.
7030.130	Vandalism sensor Monitor the enclosure for any applied acceleration forces (vibrations, etc.). Installation on the enclosure frame.
7030.140	Analogue air flow sensor (synergy with cooling units) Monitor the air flow using an externally mounted sensor in the air flow. The detection of flow fluctuations is useful for climate control applications.
7030.150	Analogue differential pressure sensor Measure the air pressure at two points in the room and calculate the difference. Connect a thin hose that defines the two points.
7030.190	Universal sensor Sensor with two digital and one analogue input. Digital inputs: Potential-free contacts, S0 bus, Wiegand interface.
7030.400	Smoke detector Monitor the air in the enclosure for smoke particles. Installation in the upper area of the enclosure.
7030.430 / 7030.440	Leakage sensor / leakage sensor 15 m Monitor the floor of an enclosure for conductive liquids. External sensor with two contacts.

Model No.	Description
7030.200	CMC III CAN bus access Connect a handle and a reader unit for monitoring a door. Integrated infrared access sensor (can replace 7030.120). Required for 7030.220, 7030.230 and 7320.721.
7030.220	Number-coded lock Release the door of the enclosure using a number code. Authorisation configuration using the IoT interface software. Installation on an enclosure door. CMC III CAN bus access energy supply. Requires a comfort handle with master key function 7320.721.
7030.230	Transponder reader Release the door of the enclosure using a transponder card. Authorisation configuration using the IoT interface software. Installation on an enclosure door. CMC III CAN bus access energy supply. Requires a comfort handle with master key function 7320.721.
7320.721	Comfort handle with master key function Automatic locking when closing the handle lever. Release via IoT interface or 7030.220 or 7030.230. Emergency opening with the master key (must be installed subsequently).

16 Glossary

IoT interface:

The IoT interface facilitates the interconnection and administration of Rittal components (such as Blue e+ cooling units, Blue e+ chillers, Smart Monitoring System) with in-house customer monitoring systems and/or energy management systems. The generated data sets can be used for further data collection and processing. This permits a long-term recording and evaluation of device data, statuses and system messages.

Hysteresis:

If an upper limit value is overshot (SetPtHigh) or a lower limit value is undershot (SetPtLow) a warning or an alarm will be output **immediately**. For a hysteresis of x%, the warning or alarm for undershooting an upper limit value or overshooting a lower limit value clears only for a difference of x/100*limit value to the limit value.

LDAP:

The Lightweight Directory Access Protocol (LDAP) is an application protocol from network technology. It permits information of a directory service to be requested via an IP network. In the IoT interface, the user administration can be transferred from an LDAP server.

MIB (Management Information Base):

The MIB was developed to fetch and change network elements. The MIB for SNMP was defined in the RFC 1157; the MIB-II for TCP/IP was defined in the RFC 1213. The MIBs have been registered as the OID for the IANA (Internet Assigned Numbers Authority). Once an object has been assigned to an OID, the meaning may no longer be changed. An overlapping with other OIDs is not permitted.

Modbus:

Modbus is a de-facto standard in industrial automation. Since 2007, Modbus/TCP is defined in the IEC 61158 standard.

OPC-UA:

OPC Unified Architecture (OPC-UA) is an industrial machine-to-machine communications protocol. It permits, for example, the sensor data to be requested from a control room system.

SNMP (Simple Network Management Protocol):

The SNMP is a simple network management protocol based on TCP/IP. It was developed to allow network components to be monitored and controlled at a central management station.

SSH:

SSH (Secure Shell) is a command line interface and protocol that can establish a secure encrypted network connection with a remote device.

Telnet:

Telnet is a protocol to allow guest access to a remote server. The Telnet program provides the required client functions of the protocol.

Trap:

Trap is the unrequested sending of SNMP messages.

Trap receiver:

The trap receiver is the recipient of SNMP messages.

17   Customer service addresses

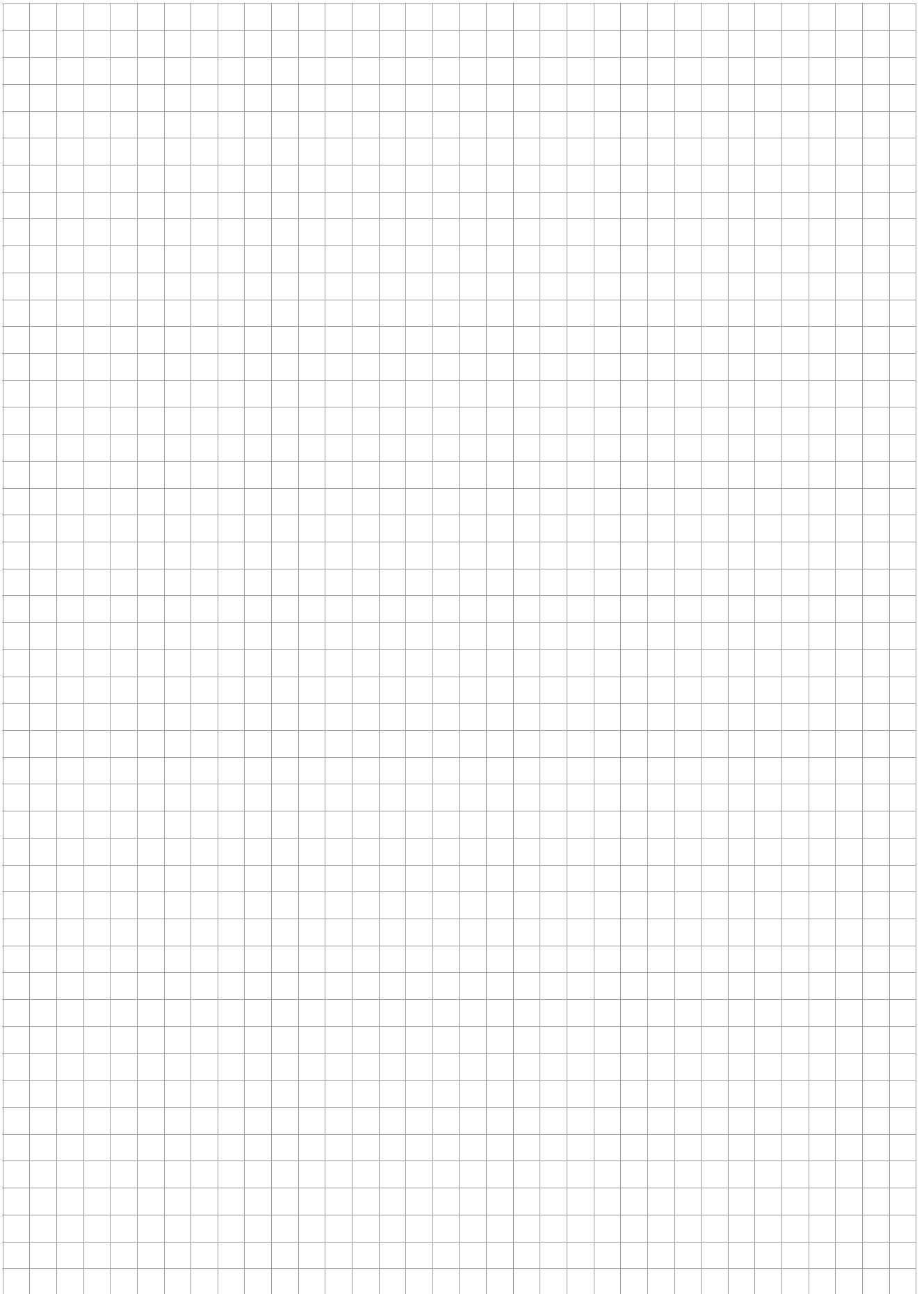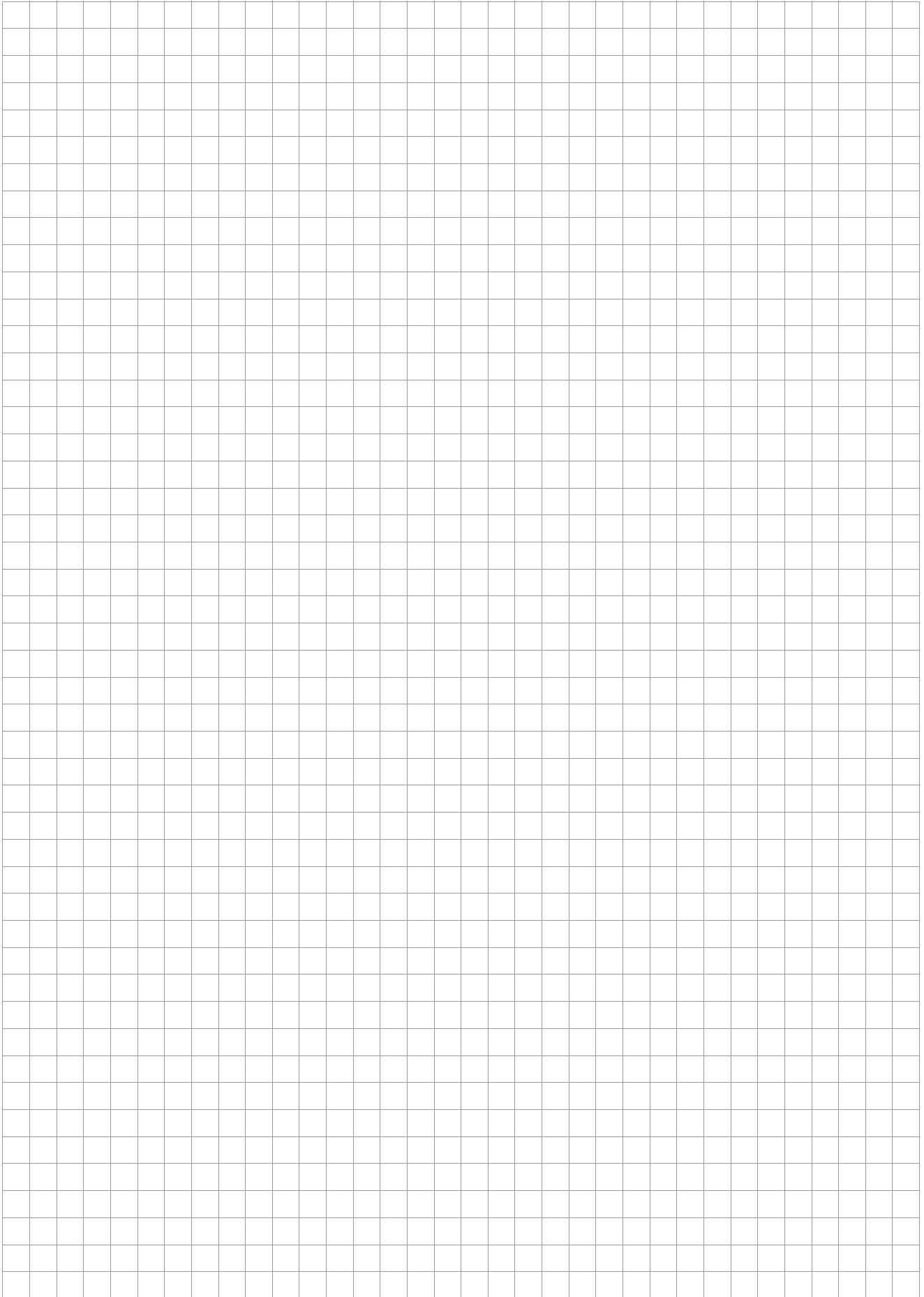For technical questions, please contact:
Tel.: +49(0)2772 505-9052
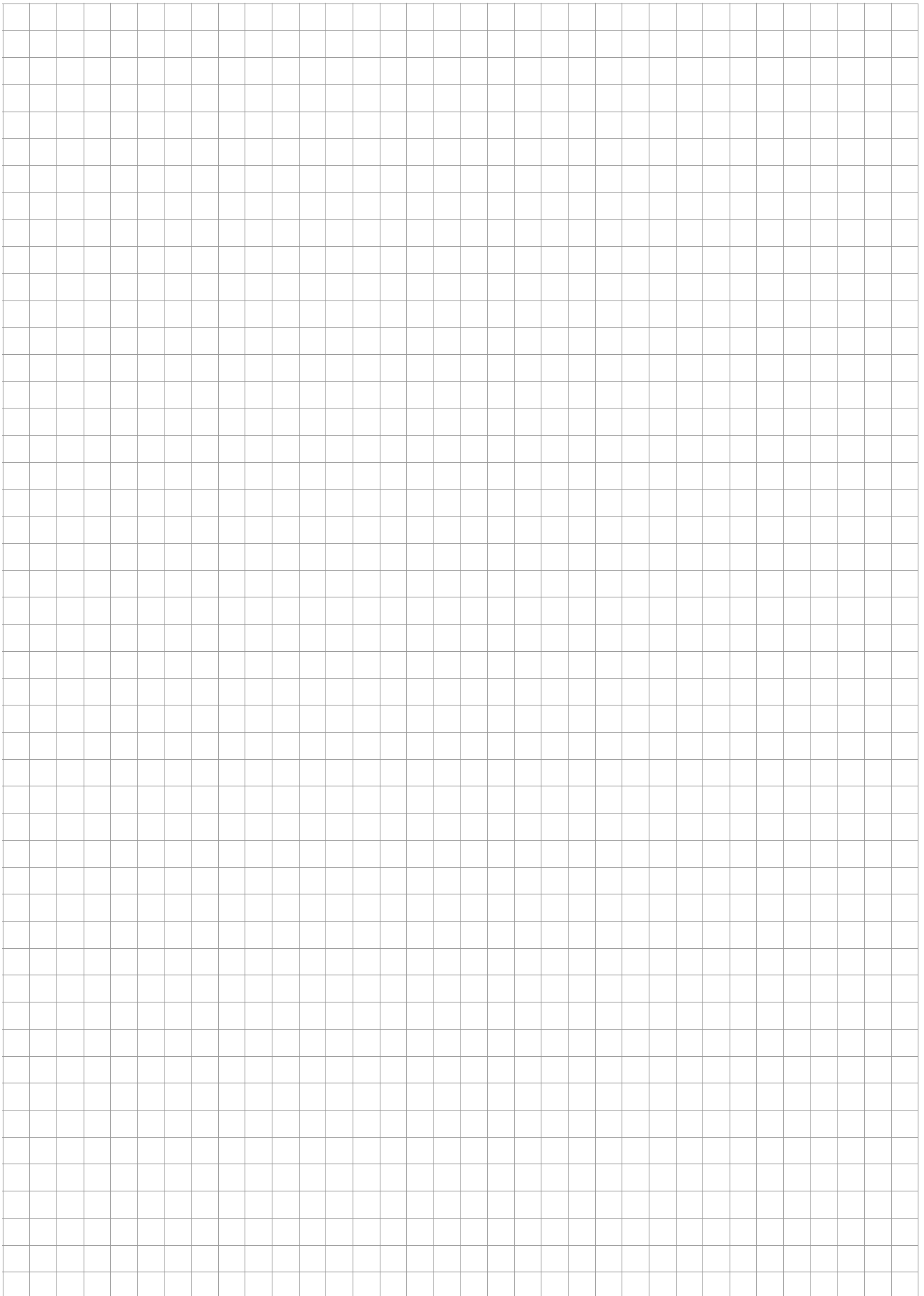E-mail: info@rittal.com
Homepage: www.rittal.com

For complaints or service requests, please contact:
Tel.: +49(0)2772 505-1855
E-mail: service@rittal.de

Notes

Rittal IoT interface

Rittal – The System.

Faster – better – everywhere.

- Enclosures
- Power Distribution
- Climate Control
- IT Infrastructure
- Software & Services

You can find the contact details of all
Rittal companies throughout the world here.

www.rittal.com/contact

RITTAL GmbH & Co. KG
Postfach 1662 · D-35726 Herborn
Phone +49(0)2772 505-0 · Fax +49(0)2772 505-2319
E-mail: info@rittal.de · www.rittal.com

ENCLOSURES POWER DISTRIBUTION CLIMATE CONTROL IT INFRASTRUCTURE SOFTWARE & SERVICES

RITTAL

FRIEDHELM LOH GROUP