

Movement by Perfection



ZAcCore

Operating manual

for pre-programmed controllers CMB..., CMP...

Issue 2026/20

Operating manual
Store for future use!

Table of contents

1	Introduction	4
1.1	Liability	4
1.2	Applicable documents	4
2	Safety instructions	4
2.1	Intended use	4
2.2	Remote control of products	4
2.3	Requirements placed on the personnel	4
2.4	Safety guidelines for operation	4
3	Product overview	6
3.1	Properties	6
3.2	System requirements for using the website	6
4	How the WEB user interface is designed and structured	7
4.1	Menu structure	8
4.2	The dashboard	10
4.3	Overview of protocols	10
4.4	User management	12
5	Operation	13
5.1	Establishing a connection to ZAcCore	13
5.2	Setting up ZAcCore	14
6	Bus systems	14
6.1	MODBUS client	15
6.2	MODBUS server	17
6.3	MODBUS RTU gateway	18
6.4	Grouping functions	20
7	Interfaces	22
7.1	Serial interface	23
7.2	Ethernet interface	23
7.3	Sockets	24
7.4	Wi-Fi	26
7.5	USB	28
8	IO system	28
8.1	Performing an IO scan	28
8.2	Configuring IO devices	29
9	Alarm management	31
9.1	Signals	34
10	ZAbulegalaxy gateway cloud connection	34



10.1	Setting up the cloud connection	36
11	Application management	37
11.1	Available applications	38
11.2	Fan controller 0-10V application	38
12	Displaying device information	40
13	System	40
13.1	Localisation	40
13.2	Update management	41
13.3	Maintenance	42
13.4	Exporting and importing data	42
14	Integrating ZAcCore into networks	43
14.1	Use within a LAN	43
14.2	Use within a Wi-Fi network	47
14.3	Connecting to the Internet via a mobile network	48
15	Notes and troubleshooting	49
16	Description of the fan controller application	51
16.1	System architecture	52
16.2	Application functions	55
16.3	Safety and specific operating conditions	55
16.4	Options for expanding the application	56
16.5	Start-up and commissioning	56
16.6	Examples	56

1 Introduction

1.1 Liability

Compliance with the following specifications serves to ensure product safety. Should the information specified especially with regard to general safety, transport, storage, assembly, operating conditions, start-up, service, maintenance, cleaning and disposal/recycling not be observed, safe operation of the product may not be guaranteed posing a possible danger to life and limb of users and third parties. Thus, deviations from the specifications below can lead to the loss of legal materials defect liability as well as to the buyer's liability for the product rendered unsafe by deviation from the specifications.

1.2 Applicable documents

Observe the following documents for instructions:

- Technical product specification
- Order confirmation
- Connection diagram
- Operating instructions for the product to be controlled

All instructions for the products to be controlled can be downloaded from: <https://www.ziehl-abegg.com/bal>

2 Safety instructions

2.1 Intended use

The product is intended for controlling, regulating and visualising systems in the heating, ventilation, air conditioning and refrigeration sector.

The operating instructions are part of the product. The product is only intended for use according to these instructions.

2.2 Remote control of products

The ZAcCore is used to operate electrical devices that may not be within sight.

- ▷ During use, make sure that nobody is located within the product's danger area.

2.3 Requirements placed on the personnel

The operator must be able to assess the risks and hazards arising from controlling individual devices or the entire system. The operator must be familiar with the entire system.

- ▷ Observe the instructions for the device being controlled.
- ▷ Make sure that only people who are familiar with the controlled device operate the ZAcCore.

2.4 Safety guidelines for operation

Safe and reliable operation

Specific safety measures are required for the safe and reliable operation of the ZAcCore.

This includes protection against:

- Unauthorised access
- Tampering
- Harmful environmental influences



ZAcore meets the requirements of relevant standards such as EN 18031-1:2024:08 and takes into account recommended data protection guidelines.

Data protection breaches may lead to recourse claims.

- Avoid connecting the ZAcore to open networks or the Internet without any firewalls.
- For remove access, use additional layers of data protection, such as VPN.
- Install firewalls to protect against unauthorised access.
- Only allow access to authorised persons.
- Change any passwords during start-up and then at specified intervals.

Compliance with these specifications is important for the system's functionality and safety. Failure to comply may render standard conformity and product liability provisions void.

Set up a fault monitoring system and performance monitoring system with an alarm signal function to prevent personal injury and damage to property in the event of malfunction or product failure.

Network security

Network segmentation and access restriction:

- Connect the product to a dedicated, isolated network segment, which is segregated from IT networks and internet-enabled systems. Use VLANs or firewalls.

Encryption and secure protocols:

- Use secure communication protocols such as TLS, VPN or encrypted industrial protocols. Disable unsecure protocols such as Telnet and FTP.

Firewall rules:

- Use a firewall to restrict data traffic to and from ZAcore. Only allows the required minimum ports and services.

Port and network isolation:

- Open ports only when needed and use isolated networks for fieldbus communication.

Guidelines for wireless communication:

- Use secure bandwidth for wireless communication and do not implement any critical routings over wireless channels. See manual for further details.

Authentication and authorisation

User authentication:

- Configure user accounts for WEB UI with passwords that are at least 8 characters long and contain a mix of upper and lower case letters, numbers and special characters.

Role-based access control (RBAC):

- Assign permissions based on job roles such as Operator, Service and Administrator.

Log-in information:

- Regularly update passwords and disable unused accounts.

Local access control:

- Limit physical access to programming interfaces such as USB and serial ports.

Recommendations for physical media and interfaces:

- Do not store any critical data on portable media such as SD cards or USB drives.
- Access to device interfaces, such as SD card slots, must be limited to authorised personnel.

Monitoring protocols

Protocol and categorisation:

- The protocol records all actions performed on the system, such as user logins, user logouts, configuration changes, operational activities and system errors, warnings, and information messages.
- The entries are categorised so that critical events requiring special attention can be identified quickly.

Logging and categorisation:

- Authorised personnel regularly review log entries to identify and correct potential safety issues, system malfunctions, or operating anomalies. After it has been reviewed and edited as necessary, each log entry is confirmed to ensure accountability and document the fact that the appropriate team is aware of the entry.
- Unconfirmed critical log entries such as errors or warnings must trigger follow-up warnings to make sure they are not missed.

Response to incidents

Define and document procedures for responding to safety and security incidents. Train staff to recognise and report suspicious activity.

3 Product overview

ZAcore is a platform for controlling and managing fans and offers functions such as monitoring and cloud connectivity.

3.1 Properties

- Connection to MODBUS-compatible devices via MODBUS TCP/IP or MODBUS RTU.
- Various network structures and connections can be established and used MODBUS TCP/IP or RS485, also simultaneously.
- Data recording: ZAcore functions
- MODBUS device overview in tree structure. Free allocation of MODBUS devices in groups within the structure.
- Patented auto-addressing for large MODBUS networks via TCP/IP or MODBUS RS485, which means that 247 MODBUS participants can be addressed when ZIEHL-ABEGG MODBUS gateways and repeaters are used.
- Group monitoring and control of fans
- Automatic update possible with active internet connection.
- Connection of fan systems to higher-level systems, e.g. plant controllers, building management with BACnet

Software bill of materials SBOM

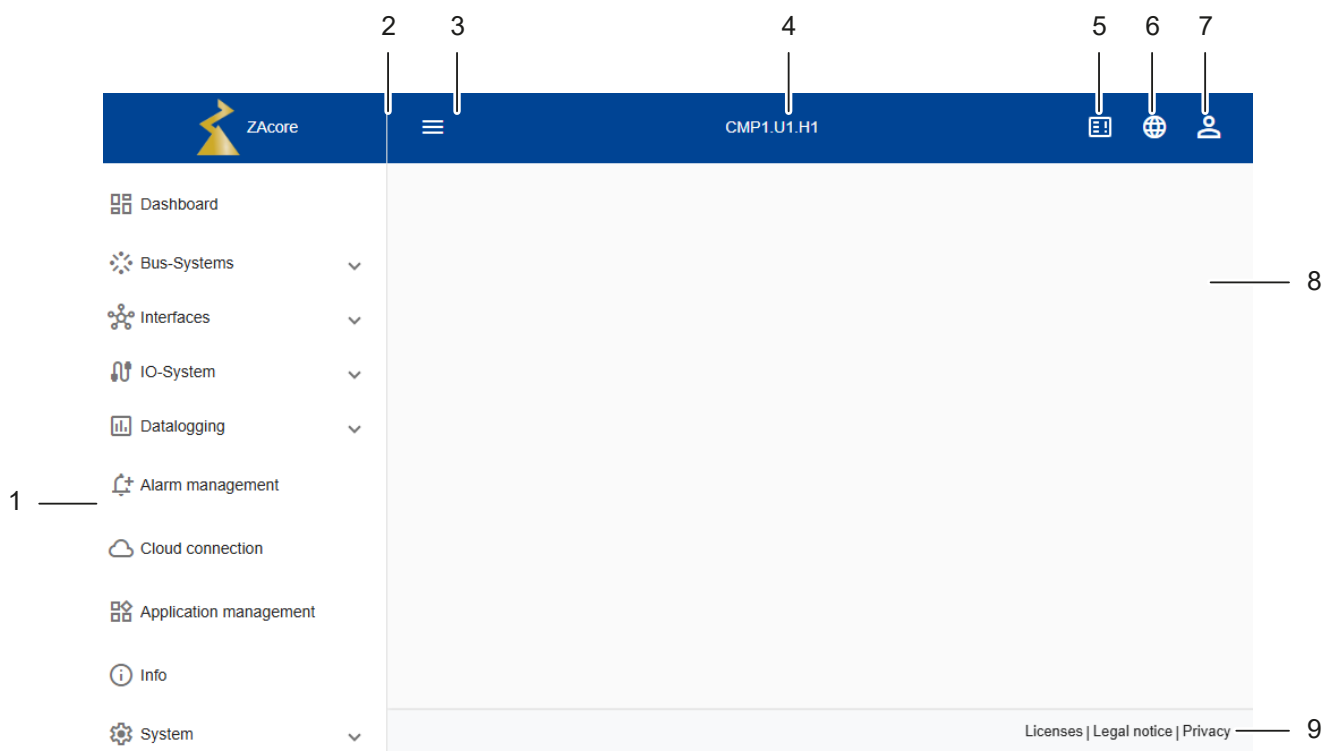
The SBOM is a detailed list of all components, modules, libraries, and dependencies contained in a software product, including their respective versions, origins, and licence information. For more information, please contact fan-controls-service@ziehl-abegg.de

3.2 System requirements for using the website

- End device with up-to-date web browser (Chrome, Edge or Firefox)
- HTML5, CSS3 and JavaScript support
- Enabled cookies



4 How the WEB user interface is designed and structured



1	Menu	2	Navigation menu Opens and closes the side navigation menu.
3	Breadcrumb Shows which menu the user is currently in.	4	Shows the ZAcCore device type.
5	Overview of protocols	6	Change of system language
7	Edit user settings Log out	8	Content for the selected menu item
9	Footer Contains the navigation links to the licence information, legal notice and data protection page.		

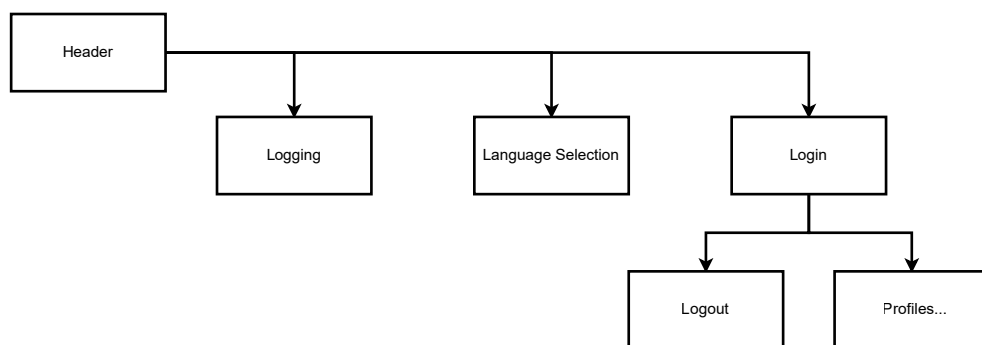
Menu

Menu point	Explanation
The dashboard	Overview of device and component, see <i>The dashboard</i> , page 10.
Bus systems	MODBUS client, MODBUS server, MODBUS RTU gateway, group management, BACnet, see <i>Bus systems</i> , page 14.
Interfaces	Serial interface, Ethernet, sockets, WLAN, see <i>Interfaces</i> , page 22.
IO system	Manages the settings for the IO modules. IO devices, IO scan, see <i>IO system</i> , page 28.

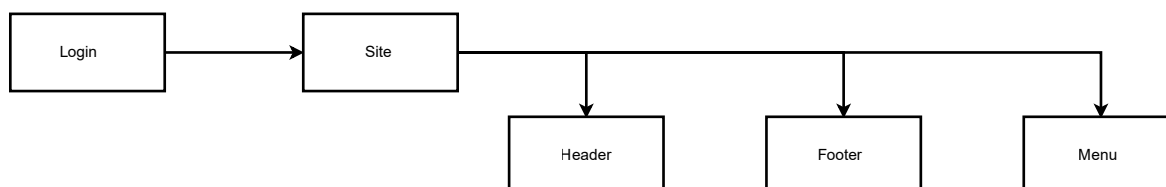
Menu point	Explanation
Data recording	Contains various options for logging specific values and displaying them graphically. Charts, configuration
Alarm management	Manages alarm groups and alarm signals, see <i>Alarm management, page 31</i> .
Cloud connection	Provides various options for setting up the cloud connection with the help of a wizard, as well as an overview of the devices reporting to the cloud, see <i>ZAbue-galaxy gateway cloud connection, page 34</i> .
Application management	For installing and managing applications, see <i>Application management, page 37</i> .
Info	Displaying device information, see <i>Displaying device information, page 40</i> .
System	For localisation, update manager, maintenance, component manager, import/export, see <i>System, page 40</i> .

4.1 Menu structure

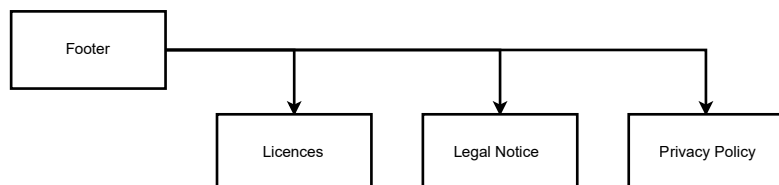
Header



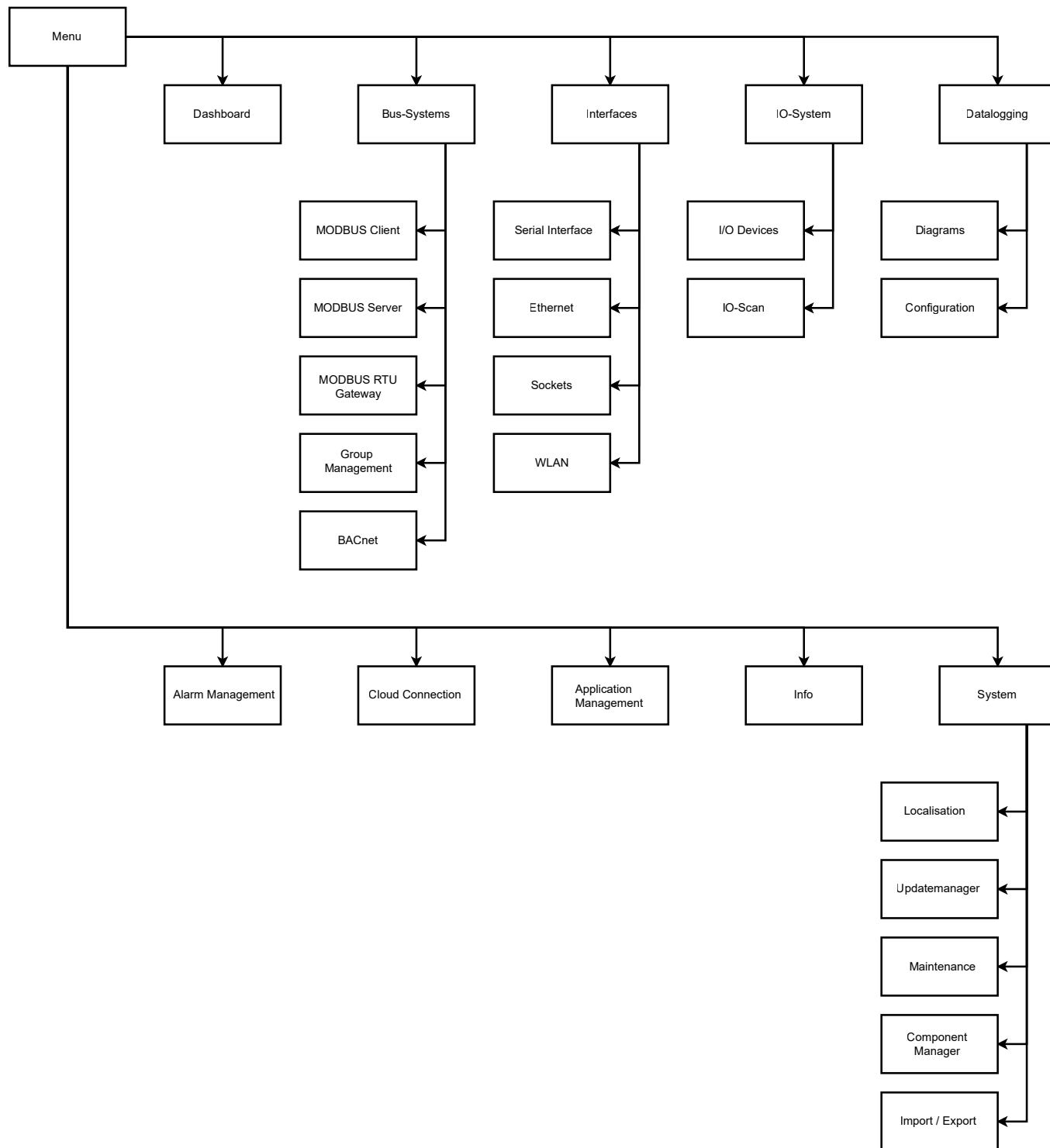
Login



Footer



Menu

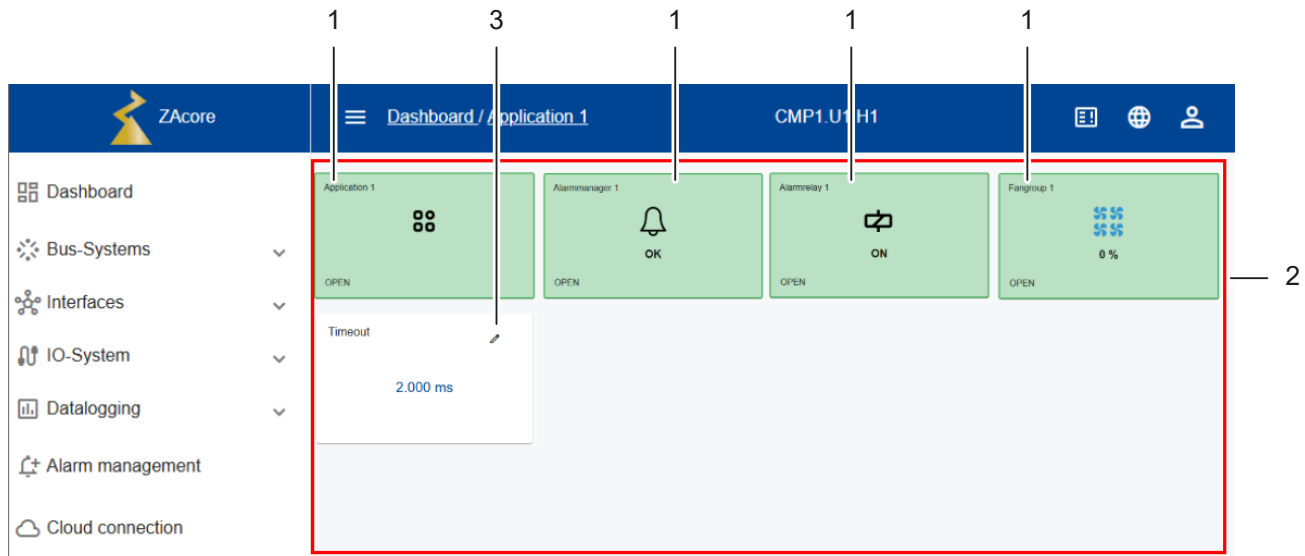


4.2 The dashboard

The dashboard (2) is the entry point after the user has logged in. It provides a personalised overview of the device and components, as well as quick access to relevant functions.

The tile-based layout can be customised. Each tile (1) shows the status of an object, highlighted in a colour for quick detection.

- Grey: No status/inactive
- Green: Ok
- Yellow: Warning
- Red: Error



The dashboard (2) is updated dynamically and shows all available values from the selected object in individual tiles. Some values can be edited directly using the pencil symbol (3).

Tile variants

The dashboard can display almost all objects and parts of the device, e.g.

- Applications
- Interfaces
- Connected components, e.g. devices integrated into MODBUS
- Product pictures
- Live data values, e.g. motors, fans or device groups

Adding an object to the dashboard

1. Open the settings for the object.
2. Check the box for **Show on dashboard**.

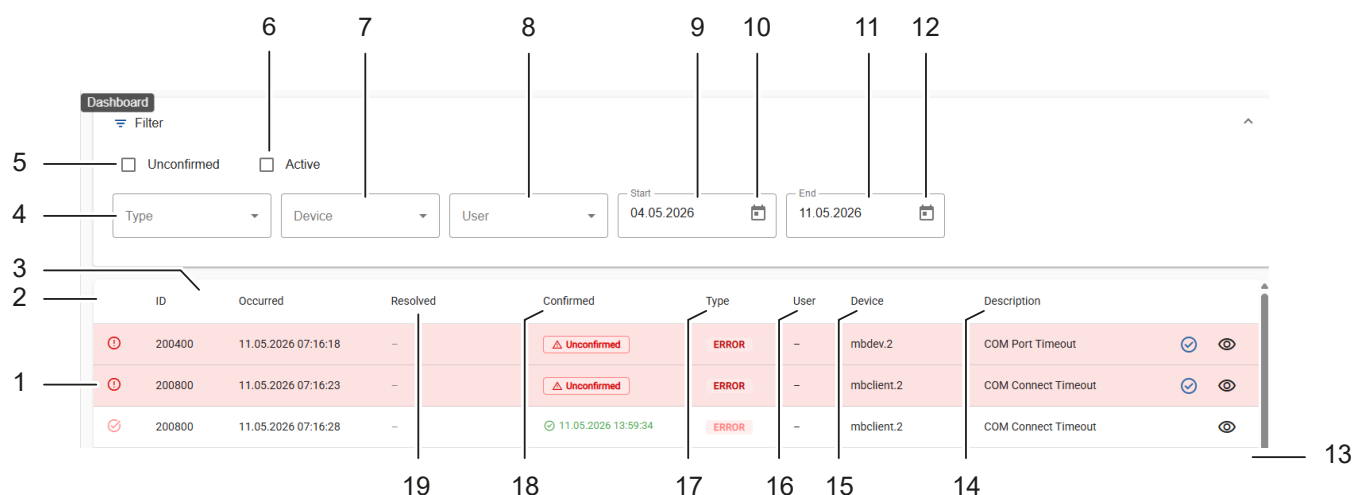
Second-generation ECblue devices have an interactive display with improved graphics for more detailed, user-friendly operation.

4.3 Overview of protocols

The system protocol records all system activities in chronological order, including procedures, restarts, and important events. The entries can be filtered according to various criteria.

By default, the protocol displays all unacknowledged and active entries sorted by type, starting with errors. Within each type group, entries are sorted by time stamp from newest to oldest. Clicking on a column heading enables the user to modify the sorting order.



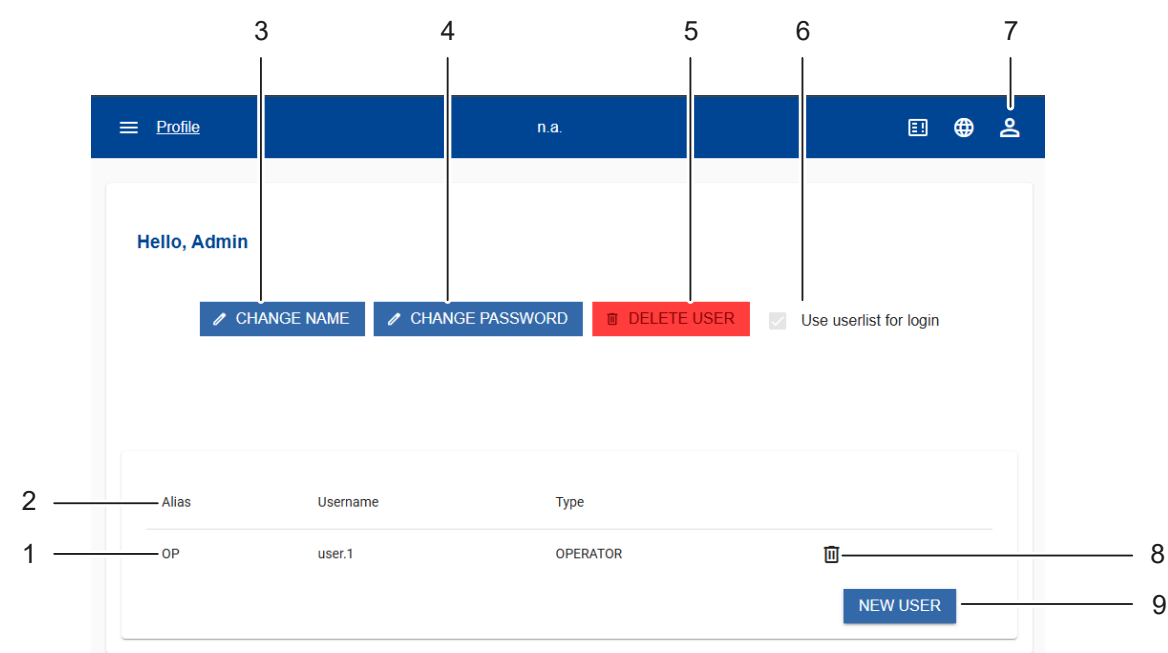


1	Event entry Click for more information. Events with the type Warning and Error can be confirmed in the pop-up with CONFIRM. The background then turns white and the font colour continues to match the type.	2	ID
3	Occurred Timestamp event occurred.	4	Types Filter with drop-down list for event types.
5	Unconfirmed Filter for already acknowledged events.	6	Active Filter for active events. ON - active events only OFF - all events
7	Device Filter with drop-down list for devices.	8	Users Filter with drop-down list for users.
9	Start Filter for start date.	10	Calendar icon For easy selection of the start date (10).
11	End Filter for end date.	12	Calendar icon For easy selection of the end date (11).
13	Next/Back	14	Description Description of the event.
15	Device ID of the device.	16	Users The user's ID.
17	Types Event type INFO - no colour, e.g. login, restart, changed settings, ... WARNING - orange font, e.g. bus connection interrupted, temperature too high, ... ERROR - red, e.g. bus connection timeout, temperature too high, ...	18	Confirmed Timestamp message confirmed or edited.
19	Resolved Timestamp message no longer present.		

4.4 User management

The following actions can be carried out in the user management sub-menu:

- Modifying the username
- Changing the password
- Deleting users
- Modifying the use of user lists, for administrators only
- Overview of user accounts
- Creating additional users



1	Overview of user accounts	2	Overview of user accounts table header
3	Modify the name of the current profile	4	Modify the password of the current profile
5	Delete current user	6	When enabled, a list of all available users is displayed during login.
7	Open profile Log out	8	To delete a user
9	Create a new user		

Overview of user accounts

Below the user actions is a table of all users, depending on the current user type. It shows all users with the same type or a lower type, starting with the highest user role.

Type	Description
ADMIN	Can view all types and create all user types. Can also delete other users by clicking on the trash can symbol on the right-hand side of the row in the table.
SERVICE	Can view and create all service, operator and guest accounts.
OPERATOR	Can view and create all operator and guest accounts.
GUEST	Can view other guest accounts, but cannot create new accounts.



5 Operation

Before the ZAcore can be used, it must be connected and set up.

5.1 Establishing a connection to ZAcore

The setup wizard of the integrated touchpanel displays information about the connection process. Devices without a touchpanel can be set up via Wi-Fi. The connection information is printed on the device, see *Accessing the browser-based interface via Wi-Fi*, page 13.

Browser-based interface via Wi-Fi	Browser-based interface in the local network
	

Accessing the browser-based interface via Wi-Fi

The SSID follows the **ZAcore-XXXXXXXXXX** schema, where XXXX... corresponds to the device's Ethernet MAC address.

Default web address: <https://192.168.4.10/>.



1	QR code Contains the default web address: https://192.168.4.10/ .	2	QR code Contains the masterkey.
3	Masterkey	4	MAC address

Procedure:

Establish a Wi-Fi connection to the ZAcore access point:

1. Select the device to be connected. If multiple devices are displayed, read the MAC address on the label on the device in the network.
2. The access point is secured, the default password is ZAcore&74653.
3. Call up the default web address: <https://192.168.4.10/>.
4. Set up the ZAcore.



Accessing the browser-based interface in the local network

Prerequisite:

- The network makes DHCP available.
- IP address of the ZAcCore is known.

The IP address is displayed on the setup page after connecting to the access point.

If only one ZAcCore is available in the network and the router or switch is set up as a DNS server, the host name ZAcCore can be used.

Alternatives for finding the IP address of the ZAcCore:

1. Use ping zacore in a command line interface, such as Windows cmd.
2. Search for connected devices in the router's user interface.

Procedure:

1. Open the Web UI: IP address of the ZAcCore <https://192.168.X.XX/>
2. Set up the ZAcCore.

5.2 Setting up ZAcCore

1. Select the system language.
2. Read the masterkey from the device and enter it in the WEB interface.
3. Enter a secure password: at least 8 characters, including upper and lower case letters, numbers and special characters
4. Repeat the password and log in.

Setup wizard

After login, the setup wizard starts automatically. You must run through the wizard.

1. Download the password recovery file and keep it in a safe place.
2. Enter a new password for the access point.
3. Set up localisation.
4. Disable or enable use of the user list.
5. Disable or enable an external touchpanel.
6. Save the settings.
7. Log in to the dashboard.

Versatile use of the ZAcCore

The ZAcCore is designed to be a versatile platform and supports different types of use. ZAcCore can be used in a wide variety of ways, depending on the application, system configuration and user role. Consequently, there is no uniform standard operation. To accommodate this versatility, the user interface has a modular design.

The following chapters describe the individual areas and sub-pages of the Web UI in detail in order to provide a structured overview of the available functions.

6 Bus systems

Bus systems permit and regulate data exchange. The following systems are available:

- MODBUS client
- MODBUS server
- MODBUS RTU gateway
- BACnet server



6.1 MODBUS client

MODBUS is a bus system commonly used for fans and IO nodes. Data can be transferred via a serial interface RS-485 or TCP Ethernet. A client is a bus actor that requests data from other devices.

Adding a MODBUS client

1. Open MODBUS Client via Menu/Bus systems.
2. Add the client by clicking on the + button and select MODBUS Client Standard.
3. Configure and save the client's device settings.
4. Add MODBUS devices to the client.

Configuring the client device settings

Available interfaces

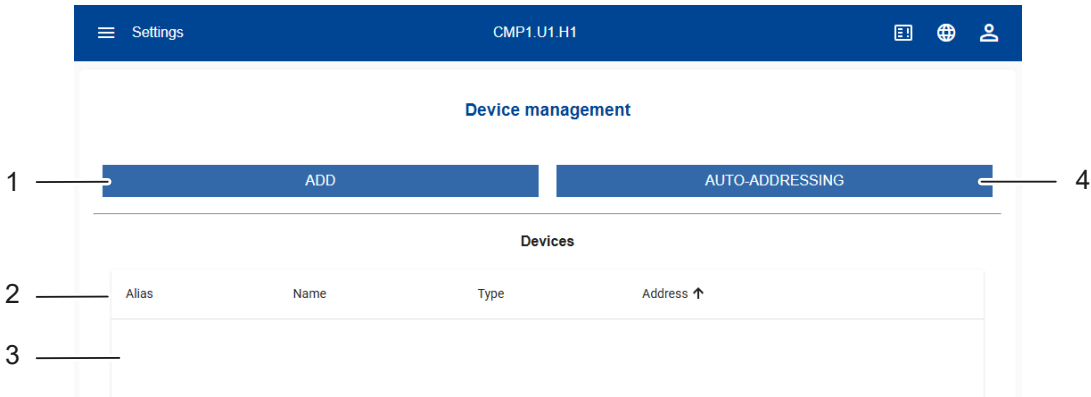
Interface	Explanation
comm.0	RS485 connection 1 to the left of the USB connection
comm.1	Isolated RS485 connection 2 to the left of the Ethernet connection
comm.2-comm.5	EM-C1 extension
comm.10-comm.19	USB serial converter ttyUSB0-9
comm.20-comm.29	USB serial converter ttyACM0-9
socket.x	Software-side interface

1	Interface comm.x interface: The MODBUS RTU protocol is used. Configuring the comm.x interface: <i>Serial interface, page 23</i> socket.x interface: The MODBUS TCP protocol is used. Configuring the socket.x interface: <i>Sockets, page 24</i>	2	Alias Name of the client that is displayed in the user interface. Max. character length: 32
3	Timeout (ms) Time in milliseconds that the client waits for the response requested by the server.	4	Restart The client is restarted.

5	Show on dashboard	6	Time between polls (ms) Waiting time in milliseconds between client requests.
7	Info To display the descriptions in the browser.		

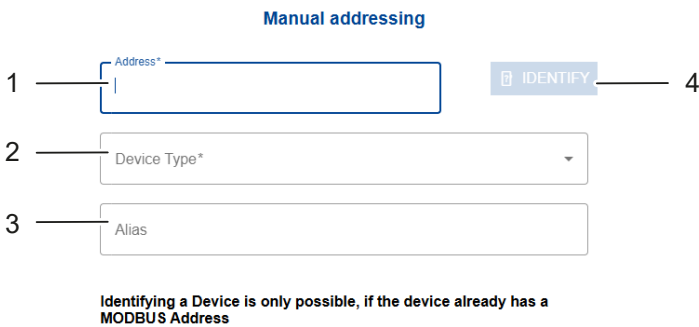
Adding devices to the client

There are two ways to add devices to the client, manually and using auto-addressing.



1	Manual addition of devices	2	Added devices table header
3	Added devices	4	Automatic addition of devices

Adding a device manually



1	MODBUS address of the device to be added. Valid range: 1 to 247. Must be unique for the client; there cannot be two devices with the same address.	2	Selecting a device type The device must have the address from the address field.
3	Alias Name of the client that is displayed in the user interface. Max. character length: 32	4	Identification After filling in the address field, the address entered can be used to identify the device type. The remaining fields are filled in automatically. This only works for devices that support MODBUS device identification.



Adding a device automatically

Prerequisite: Auto-addressing is supported by the device, e.g. ZIEHL-ABEGG ECblue fans.

Auto-addressing enables devices to be identified automatically and their addresses to be created automatically.

Auto-addressing overwrites all devices already addressed.

Auto-addressing

1 — Mode (Auto/Flex)*

2 — Optional: Start address

Flex address

3 —  4

1	Auto - The devices are addressed consecutively, starting with 1 or the address in the start address field. Flex - The devices are addressed based on the entries in the Flex Address field, which are separated by commas.	2	Start address for Auto mode.
3	Input of flexible address assignment. Addresses must be separated by a comma or semicolon.	4	Upload .CSV file type Addresses must be separated by a comma or semicolon.

6.2 MODBUS server

A server is a bus actor that provides data to MODBUS clients.

Adding a MODBUS server

1. Open MODBUS Server via Menu/Bus systems.
2. Add the server by clicking on the + button and then select MODBUS Server.
3. Configure the server.

Configuring a MODBUS server

Available interfaces

Interface	Explanation
comm.0	RS485 connection 1 to the left of the USB connection
comm.1	Isolated RS485 connection 2 to the left of the Ethernet connection
comm.2-comm.5	EM-C1 extension
comm.10-comm.19	USB serial converter ttyUSB0-9
comm.20-comm.29	USB serial converter ttyACM0-9
socket.x	Software-side interface

1	Interface comm.x interface: The MODBUS RTU protocol is used. Configuring the comm.x interface: <i>Serial interface, page 23</i> socket.x interface: The MODBUS TCP protocol is used. Configuring the socket.x interface: <i>Sockets, page 24</i>	2	Alias Name of the server displayed in the user interface. Max. character length: 32
3	Address Address of the server. MODBUS Gateway ON: The address must be unique within the MODBUS network and contain all addresses of the devices connected to the ZAcCore.	4	Restart The server is restarted.
5	Show on dashboard	6	MODBUS Gateway ON: The server also accepts requests to other addresses and forwards them to connected devices provided that a MODBUS device with this address exists in a client. External clients must only send valid requests. The server interprets each incoming MODBUS message and attempts to send them to the respective device with the specified address and payload. Device addresses must not conflict with the server address. OFF: The server responds only to its configured address and provides the data points defined in the register description of the respective server type.
7	Info To display the descriptions in the browser.		

6.3 MODBUS RTU gateway

The MODBUS RTU gateway enables seamless communication between MODBUS clients and MODBUS servers. It acts as a protocol converter and translates messages between Ethernet and serial networks.

Key functions

- Protocol conversion: Converts MODBUS TCP requests to MODBUS RTU frames and vice versa.



- Network bridging: Allows MODBUS TCP clients to access and control MODBUS RTU devices as if they were on the same network.
- Transparent communication: Ensures MODBUS function codes and data are forwarded without changes, ensuring compatibility with standard MODBUS devices.
- Multi-client support: Some gateways support multiple TCP clients accessing multiple RTU servers at the same time.
- Serial master or slave mode: Depending on the configuration, the gateway can act as a MODBUS RTU client for querying RTU servers or as a server for replying to a MODBUS TCP client.

Typical use cases

- Integration of older MODBUS RTU devices into modern Ethernet-based control systems.
- Remote monitoring and control of serial devices over IP networks.
- Industrial automation systems in which serial and Ethernet devices coexist.

Example of a communication process

1. A MODBUS TCP client sends a request via Ethernet.
2. The gateway receives the request and converts it into a MODBUS RTU frame.
3. The RTU frame is sent to the corresponding RTU server via the serial interface.
4. The server responds and the gateway converts the RTU response back to TCP format.
5. The response is sent back to the MODBUS TCP client.

Adding a MODBUS RTU gateway

1. Open MODBUS RTU gateway via Menu/Bus systems.
2. Add the gateway by clicking the + button and select MODBUS TCP/RTU gateway.
3. Configure the gateway.

Configuring a MODBUS RTU gateway

Available interfaces

Interface	Explanation
comm.0	RS485 connection 1 to the left of the USB connection
comm.1	Isolated RS485 connection 2 to the left of the Ethernet connection
comm.2-comm.5	EM-C1 extension
comm.10-comm.19	USB serial converter ttyUSB0-9
comm.20-comm.29	USB serial converter ttyACM0-9
socket.x	Software-side interface

Settings CMP1.U1.H1

mbgateway.0 +

1 Alias
mbgateway.0

2 Timeout
2000

3 Poll tries
3

☐ Show on dashboard

5

6 Time between polls
0

Addressing

4 Interface* Serial interface*

7

8 ADDRESS

9 RESET DELETE SAVE

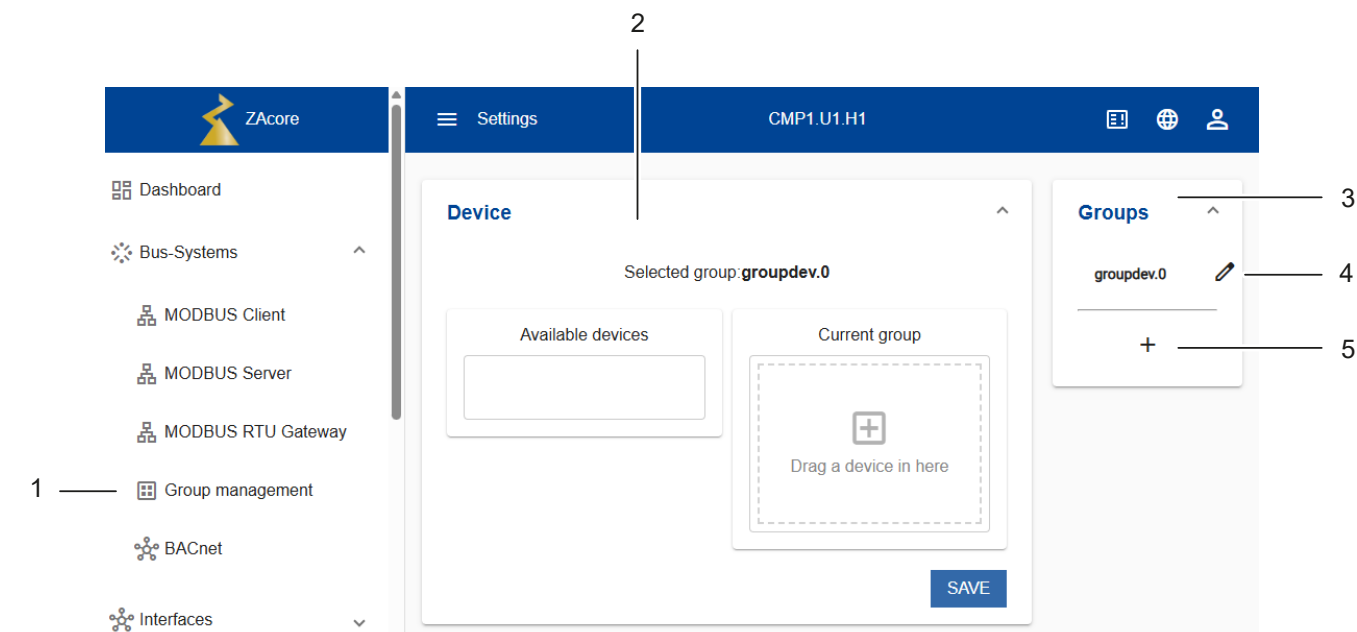
1	Alias Name of the gateway that is displayed in the user interface.	2	Timeout (ms) Time in milliseconds that the client waits for the response requested by the server.
3	Poll attempts Number of retry attempts after failed communication with a server. Typical range: 1–3	4	Interface socket.x interface: The MODBUS TCP protocol is used. Configuring the socket.x interface: <i>Sockets, page 24</i>
5	Show on dashboard	6	Time between polls (ms) Waiting time in milliseconds between gateway requests. Typical range: 10-100 ms
7	Serial interfaces comm.x interface: The MODBUS RTU protocol is used. Configuring the comm.x interface: <i>Serial interface, page 23</i>	8	Addressing is started.
9	Info To display the descriptions in the browser.		

6.4 Grouping functions

The group function can be used to group devices into logical units so that they can be controlled using shared settings and status data points and alarm messages can be read out centrally, e.g. common alarm.

There are different group types that support specific device types, such as fan groups for fans from different manufacturers. The group handler manages the MODBUS interfaces so that control takes place independently of device-specific differences. This simplifies handling and provides a standardised interface that also includes devices from different MODBUS clients and bus systems.





1	Group management Menu for grouping functions.	2	Available devices List of all detected or manually added devices that are compatible with the group type and are not assigned to a group.
3	Current group The devices can be dragged and dropped from the Available devices list to the group.	4	Select group / Edit group To configure a group.
5	Add groups Create a new group.		

Adding a new group

1. Open the group management sub-menu via **Menu/Bus systems**.
2. Add a group by clicking the + button (5) and then + Fangroup, see 6.4, page 20.
3. Drag and drop devices from the list of available devices into the current group. Remove any unnecessary devices using drag and drop.
4. Save the group.
5. Configure the group.

Configuring a group

Configuring a fan group enables fan groups to be adapted individually and controlled with a high level of precision.

Device Edit

1

Alias

groupdev.0

☐ Show on dashboard

6

2

Group setpoint %

0

Fancontroller link

7

3

Enable Switch DI

Out of service

OFF

8

4

Group password

0

Group Controlbits

0

9

5

Group Controlvalue

0

1	Alias The name of the device displayed in the user interface. Max. character length: 32	2	Group activation % Actual speed setpoint for the group Range: 0-100%
3	DI release switch The data point object ID of a digital input DI used to activate or deactivate the fan group, e.g. iodev.0.xxx. Enables external control for activating or deactivating the group, for example via a switch or a PLC.	4	Group password, optional
5	Groups control value A standardised rotational speed setpoint used for external or automatic control. Value range: 0–32767 corresponds to 0–100% of the group member's maximum rotational speed.	6	Show on dashboard
7	Fan controller link Communication connection or reference to ZAcore fan controller device that is assigned to this group. A fan controller can be used to control a group with 0-10V or similar signals.	8	Inactive ON: Marks the group as inactive, e.g. during maintenance. Devices in this group will not be queried or controlled as long as they are marked as inactive.
9	Groups control bits Bit mask or set of control flags used to define specific behaviours or modes for the group. Currently unavailable.		

7 Interfaces

The following interfaces are available:

- Serial interface COM ports RS-485
- Ethernet
- Sockets
- Wi-Fi
- USB



7.1 Serial interface

ZAcore has RS-485 as standard and can be expanded to include additional RS-485 interfaces via the EM-C1 module and also via FTDI-compatible USB serial adapters.

The operating system detects all compatible interfaces and displays them as tabs; it is not possible to add them manually.

Serial interfaces are assigned to communication applications such as MODBUS RTU, BACnet MS/TP or external touchpanels. The communication parameters can be configured in this menu, but may be overwritten by some applications.

Available interfaces

Interface	Explanation
comm.0	RS485 connection 1 to the left of the USB connection
comm.1	Isolated RS485 connection 2 to the left of the Ethernet connection
comm.2-comm.5	EM-C1 extension
comm.10-comm.19	USB serial converter ttyUSB0-9
comm.20-comm.29	USB serial converter ttyACM0-9

Configuring a serial interface

1	Alias Name of the client that is displayed in the user interface. Max. character length: 32	2	Baud rate
3	Tabs Selection of available interfaces.	4	Show on dashboard
5	Mode Configuration of the data frame.	6	Info To display the descriptions in the browser.

7.2 Ethernet interface

ZAcore has an integrated Ethernet-10/100-Base-T interface and can be expanded with one further Ethernet interface via a USB Ethernet adapter with a Realtek chipset, see *USB*, page 28.

The interfaces are called eth followed by a number, whereby the integrated interface is eth.0. Ethernet can be used for various TCP/IP applications running in parallel on a local network. The interface must match the local network settings and is configured by default for automatic IP assignment via DHCP.

SettingsCMP1.U1.H1

1

DHCP

2

IPv4 Static Address*

0.0.0.0

3

IPv4 Subnetmask*

0.0.0.0

4

IPv4 Gateway*

0.0.0.0

5

IPv4 DNS1

0.0.0.0

6

IPv4 DNS2

0.0.0.0

UNDO CHANGES

SAVE

1	DHCP ON: Interface obtains IP address from a DHCP server in the network. OFF: Interface uses static settings according to the settings.	2	IPv4 static address
3	IPv4 subnet mask Factory setting 255.255.255.0	4	IPv4 gateway The gateway address is only relevant if ZAcore is due to be connected to the internet. Recommendation: Use the router's IP address.
5	IPv4 DNS1 DNS addresses (DNS1/DNS2) are only required if network servers are due to be accessible via host name or URL. Recommendation: Use the IP4 gateway router's IP address as DNS1 – this automatically routes DNS requests to a DNS server obtained from the router.	6	IPv4 DNS2 see (5) Fallback to IPv4 DNS1

7.3 Sockets

Sockets are interfaces used with bus system applications via the TCP/IP protocol. For example:

- MODBUS-TCP
- BACnet/IP
- MQTT

Sockets can be assigned when creating this type of application.

The following socket types are available:

- Simple TCP client socket
- Simple TCP server socket for simple, unencrypted local TCP/IP communication, e.g. MODBUS TCP server and client, MODBUS gateway.
- UDP server socket, e.g. BACnet IP



Add a socket.

1. Open sockets via Menu/Interfaces.
2. Add the socket by clicking the + button and select the appropriate type.
3. Configure the socket.

Configuring a simple TCP client socket

Interface	Explanation
eth.0	Ethernet connection

1	Interface eth.x interface: Configuring the eth.x interface: <i>Ethernet interface</i> , page 23	2	Alias Name of the client that is displayed in the user interface. Max. character length: 32
3	Host address	4	Connection timeout (sec)
5	Tabs Selection of available interfaces.	6	Show on dashboard
7	Port number MODBUS-TCP default: 502; 501-509 allowed	8	Info To display the descriptions in the browser.

Configuring a simple TCP server or UDP server socket

Interface	Explanation
eth.0	Ethernet connection
eth.1	Ethernet connection via USB Ethernet adapter

The screenshot shows the 'Device settings' for an interface named 'socket.0'. The settings are as follows:

Label	Value
Alias	socket.0
Interface	Interface (dropdown)
Portnumber	502
Show on dashboard	☐

At the bottom, there are three buttons: 'UNDO CHANGES' (yellow), 'DELETE' (red), and 'SAVE' (blue). To the right of these buttons is a document icon.

1	Interface eth.x interface: Configuring the eth.x interface: <i>Ethernet interface</i> , page 23	2	Alias Name of the client that is displayed in the user interface. Max. character length: 32
3	Port number MODBUS-TCP default: 502; 501-509 allowed	4	Tabs Selection of available interfaces.
5	Show on dashboard	6	Info To display the descriptions in the browser.

7.4 Wi-Fi

ZAcore offers an integrated Wi-Fi interface, which enables:

- Wireless connection to mobile devices (access point mode)
- Wireless connection to a Wi-Fi network

Upon delivery, the Wi-Fi interface is set to Access Point Mode.

Additional Wi-Fi interfaces cannot be added manually.

In case of a static network configuration: Contact the network administrator of the Wi-Fi network. In Station Mode, only DHCP or DHCP with static addressing based on the MAC address are recommended.



The screenshot shows the 'WiFi intern' settings page. At the top, there's a blue header with 'Settings', 'CMP1.U1.H1', and icons for a list, globe, and user. Below the header, the title 'WiFi intern' is centered. The settings are organized into two columns. On the left column: 1. 'Mode' dropdown menu set to 'Access Point'. 2. 'Passphrase*' text field. 3. 'DHCP' toggle switch, currently turned off. 4. 'IPv4 Subnetmask*' text field with value '255.255.255.0'. 5. 'IPv4 DNS1' text field with value '0.0.0.0'. 6. 'IPv4 DNS2' text field with value '0.0.0.0'. On the right column: 7. 'SSID' text field with value 'ZAcCore-70B3D56980DE'. 8. 'Channel' dropdown menu set to '1'. 9. 'IPv4 Static Address*' text field with value '192.168.4.10'. 10. 'IPv4 Gateway*' text field with value '192.168.4.10'. 11. 'IPv4 DNS2' text field with value '0.0.0.0'. At the bottom, there are two buttons: 'UNDO CHANGES' (orange) and 'SAVE' (blue). A magnifying glass icon (4) is shown over the 'Passphrase*' field.

1	Mode Off, AccessPoint	2	SSID SSID is the name of the Wi-Fi network that ZAcCore should connect to in Station Mode. Clicking on the icon (4) scans available networks and displays them as a list under SSID. Select the Wi-Fi network that the ZAcCore should connect to. In Access Point Mode, the name is pre-specified: ZAcCore MAC address
3	DHCP ON: Interface obtains IP address from a DHCP server in the network. OFF: Interface uses static settings according to the settings.	4	Network scan for existing access points see Point 2
5	IPv4 subnet mask Factory setting 255.255.255.0	6	IPv4 DNS1 DNS addresses (DNS1/DNS2) are only required if network servers are due to be accessible via host name or URL. Recommendation: Use the IP4 gateway router's IP address as DNS1 – this automatically routes DNS requests to a DNS server obtained from the router.
7	Password The password for logging into the ZAcCore in Access Point Mode (factory setting: ZAcCore&74653) or into a Wi-Fi network in Station Mode. The saved password is not displayed in Station Mode.	8	Channel 1-13 Factory setting is channel 1 Recommendation: Channel 1 or 6
9	IPv4 static address	10	IPv4 gateway The gateway address is only relevant if ZAcCore is due to be connected to the internet. Recommendation: Use the router's IP address.

11	IPv4 DNS2 see Point 6 Fallback to IPv4 DNS1		
----	---	--	--

7.5 USB

ZAcCore supports various standard USB devices, but not every model available on the market. USB-RS-485/RS-232 adapters must use an FTDI chipset, USB-Ethernet adapters must use a Realtek chipset. Only one additional Ethernet extension is possible via USB.

8 IO system

The ZAcCore IO system is used to connect and control sensors, actuators and motors/control circuits. The ZAcCore has various physical connections.

- UIO channels can be used as analogue inputs, analogue outputs and digital inputs, see *Configuring IO devices*, page 29.
- DI channels, digital inputs, are intended for counting inputs, frequency inputs or switching signals.
- DO channels, digital outputs, are used to switch or control actuators.

8.1 Performing an IO scan

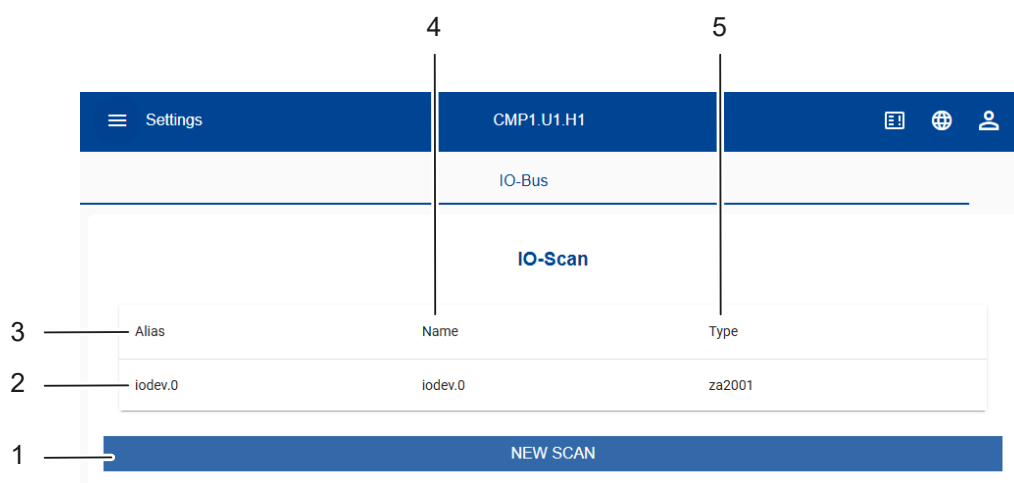
Upon initial start-up, ZAcCore detects all existing add-on modules. If new modules are added later, a new IO scan must be triggered.

ATTENTION Damage to property

- ▷ Only connect or remove IO add-on modules when switched off.

Triggering an IO scan

1. Open IO-Scan via **Menu/IO-System**.
 2. Start a scan by clicking the **RE-SCAN** button.
- The new modules can be used once the scan is complete.



1	RE-SCAN To trigger an IO scan. The process can be stopped with CANCEL IO-SCAN.	2	Found modules
---	--	---	---------------



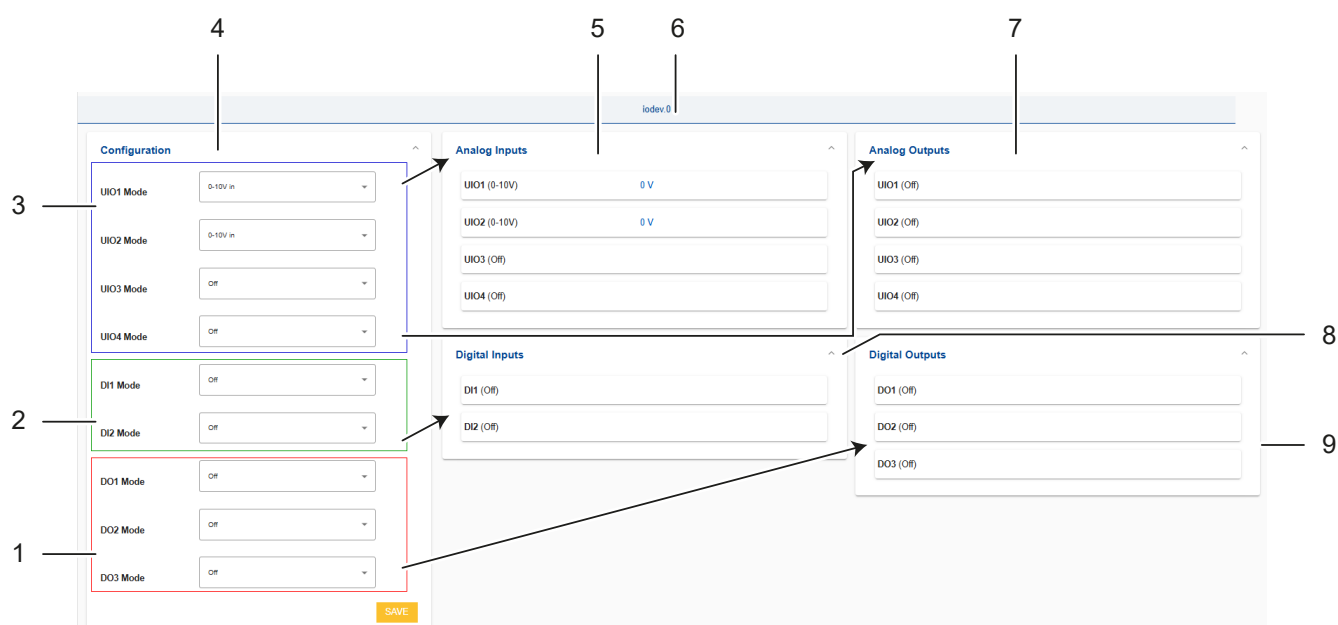
3	Display name on dashboard Standard: Alias = Instance name	4	Name Instance name of the device to connect other system components to the IO module.
5	Type Module type za20XX		

8.2 Configuring IO devices

1. Open IO devices via Menu/IO system.
2. Configure the inputs/outputs (4).
3. Save the configuration.
4. Adjust the analogue and digital outputs (7, 9) if necessary.

Available modes

Universal inputs/outputs UIO	Digital inputs DI	Digital outputs DO
Off	Off	Off
0-10V output	Digital	Digital logic
0-20mA output	S0 counter	
0-10V input	Frequency	
0-20mA input	Counter	
0-20mA input, series connection		
Resistor		
Digital logic		
Digital logic, series connection		



1	Configuration of digital outputs	2	Configuration of digital inputs
3	Configuration of universal inputs/outputs	4	Configuration window
5	Analogue inputs Depending on the configuration of the universal inputs/outputs.	6	Tab Available modules can be selected here.

7	Analogue outputs Depending on the configuration of the universal inputs/outputs.	8	Digital inputs
9	Digital outputs		

Digital inputs DI

- Isolated digital inputs are isolated from GND via optocouplers
- Inputs are suitable for logic signals and frequency measurement up to 5 kHz
- Max. voltage 30 VDC
- Min. voltage 5 VDC
- Impedance 4 KOhm
- Max. frequency 5 kHz
- Compatibility with DIN 43 864 or connection examples in EN 62053-31

Digital outputs DO

- Quantity is dependent on add-on module
- Function depends on the programming
- Short-circuit-proof
- The maximum cable length allowed is 30 m
- Max. collector voltage (U_{ce}) 30 VDC
- Min. collector voltage (U_{ce}) 5 VDC
- Max. current load 50 mA
- V+ device-side voltage 24 VDC +/- 10%

Universal inputs/outputs UIO

- Quantity is dependent on add-on module
- Basic function must be selected to match the signal type

Off

- No function

0-10V output

- Resolution: 13 bit
- Load allowed per channel: 500 - 100 K
- Short-circuit current per channel: 29 mA (source), 3.8 mA (sink)

0-20mA output

- Resolution: 13 bit
- Allowed load per channel: 25 mA
- Output impedance: 4 M

0-10V input

- Resolution: 16 bit
- Max. allowed voltage: 10 V
- Typical input impedance: 195 K

0-20mA input

- Resolution: 16 bit
- Max. allowed current: 25 mA
- Max. short-circuit current 35 mA
- Typical input impedance 200



0-20mA input, series connection

- Resolution: 16 bit
- Max. allowed current: 25 mA
- Max. short-circuit current 24.5 mA
- Measuring resistance 100
- Min. required voltage: 5 V
- Resistance measurement 0–1 M
- Measuring range accuracy: 0 to 80 0.5% ± 0.5 ± % of measured value ± offset 80 to 200 0.3% ± % of measured value 200 to 1 k 0.2% ± % of measured value 1 k to 10 k 0.2% ± % of measured value 10 k to 20 k 0.3% ± % of measured value 20 k to 100 k 0.8% ± % of measured value 100 k to 200 k 1.0% ± % of measured value 200 k to 1 M 8% ± % of measured value

Digital logic

- Max. allowed voltage: 40 V
- Max. allowed frequency: 5 KHz
- Programmable threshold voltage: 0.5–1.6 V

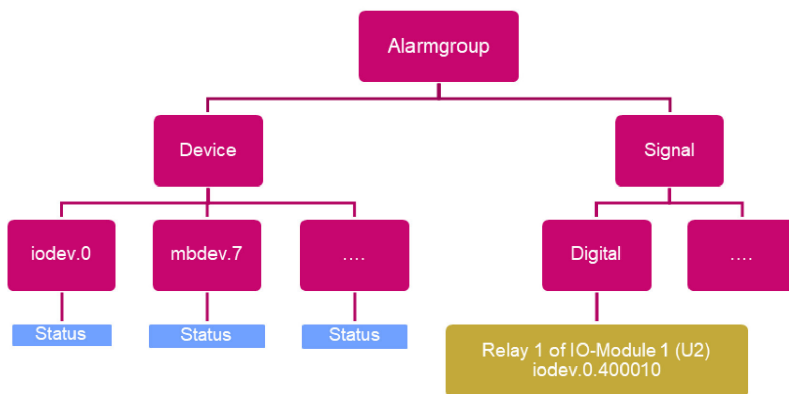
Digital logic, series connection

- Min. required voltage: 5 V
- Max. allowed frequency: 5 KHz
- Programmable wetting bridging current for potential-free contacts: 0.5–24.5 mA

9 Alarm management

Alarm management can be used to create alarm groups to which devices can be assigned. Alarm groups can only be created and configured via the WEB UI.

Structure

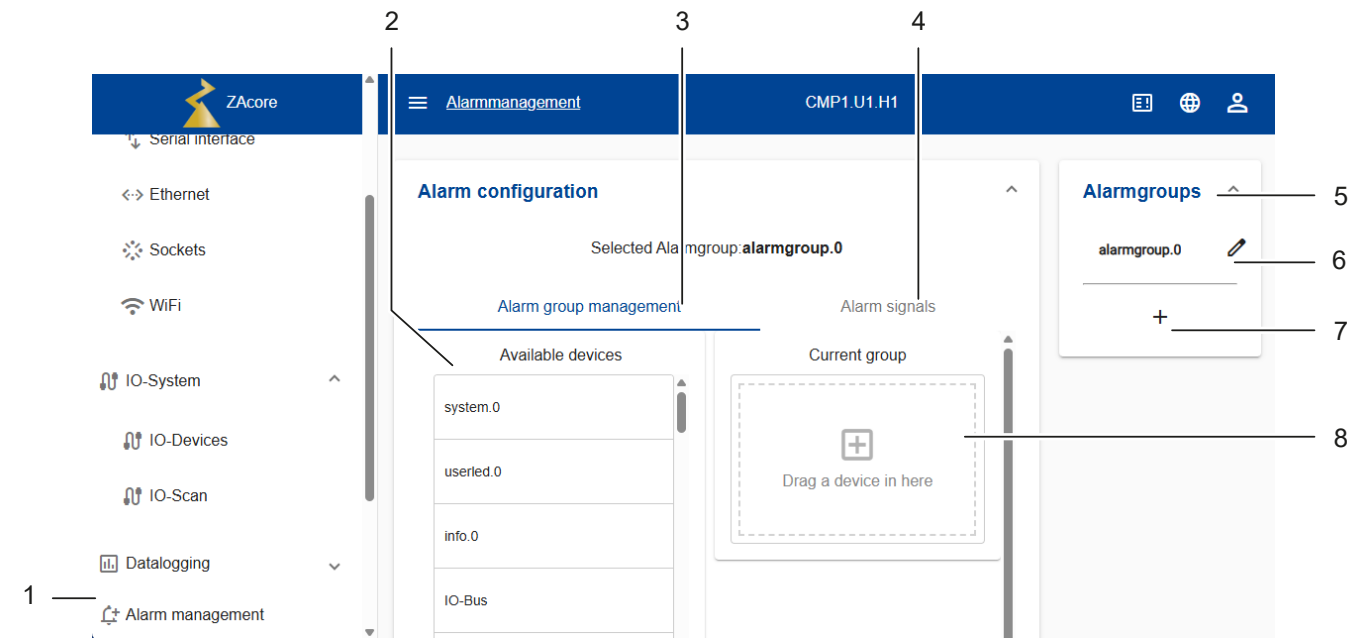


The status of the devices within an alarm group is monitored. A device can have the following statuses:

- Inactive
- Okay
- Warning alarm status
- Error/fault alarm status

An alarm group can contain several alarm signals. If a device assumes an alarm status, this is passed on to the group's alarm signals.

Alarm signals can be used, for example, to switch outputs based on an alarm condition.



1	Alarm management Menu for alarm management.	2	Available devices Displays a list of all detected or manually added devices that are compatible with the group type and are not currently assigned to a group.
3	Alarm group management Open the alarm group management tab	4	Alarm signals Open the alarm signals tab.
5	Current group The group currently selected by the user.	6	Select group / Edit group Select and edit an existing group.
7	Add groups Create a new group.	8	Add groups Create a new group.

Add an alarm group

1. Open the alarm management sub-menu via the menu.
2. Add a group by clicking on the + button (7).
3. Drag and drop devices from the list of available devices into the current group. Remove any unnecessary devices using drag and drop.
4. Save the group.
5. Configure the group.
6. Add the alarm signals.

Configuring an alarm group

Device Edit

1 Alias
alarmgroup.0

2 Out of service
Off

☐ Show on dashboard 3



1	Alias The name of the device displayed in the user interface. Max. character length: 32	2	Inactive ON: Marks the group as inactive. Devices in this group will not be queried or controlled as long as they are marked as inactive.
3	Show on dashboard		

Add an alarm signal

1. Open the alarm signals tab (4).
2. Add the alarm signal by clicking on the + button and alarm signal binary.
3. Configure the alarm signal.

Configuring an alarm signal

Signal type	Designation 2	Description
OFF NC	Inactive Normally closed	Alarm signal is always on.
ERROR NC	Error open Normally closed	Alarm signal is on as long as no error status occurs in the group. Example: Error = Relay off
WARNING NC	Warning open Normally closed	Alarm signal is on as long as no warning status occurs in the group Example: Warning = Relay off
BOTH NC	Error/warning open Normally closed	Alarm signal is on as long as no warning status or error status occurs in the group. Example: Warning or error = Relay off
OFF NO	Inactive Normally open	Alarm signal is always off.
ERROR NO	Error closed Normally open	Alarm signal is off as long as no error status occurs in the group. Example: Error = Relay on
WARNING NO	Warning closed Normally open	Alarm signal is off as long as no warning status occurs in the group. Example: Warning = Relay on
BOTH NO	Error/warning closed Normally open	Alarm signal is off as long as no warning status or error status occurs in the group. Example: Warning or error = Relay on

Device Edit

1 ☐ Show on dashboard 4

2 5

3 6

1	Alias The name of the device displayed in the user interface. Max. character length: 32	2	Inactive ON: Marks the alarm signal as inactive. Alarm signal will not be queried or controlled for as long as it is marked as inactive.
---	---	---	--

3	Deceleration sec Time in seconds before an alarm is forwarded to the signal.	4	Show on dashboard
5	IO object link Link to IO data point link, string, e.g. io-dev.0.40005.	6	Function Selection of how the alarm signal works, see <i>Digital signal functions, page 34</i> .

9.1 Signals

9.1.1 Digital signals

Digital signals can be used to switch digital outputs according to an alarm condition.

Digital signal functions

Number	Name 1	Name 2	Description
0	OFF NC	Inactive Normally closed	Alarm signal is always on.
1	ERROR NC	Error open Normally closed	Alarm signal is on as long as no error status occurs in the group. Example: Error = Relay off
2	WARNING NC	Warning open Normally closed	Alarm signal is on as long as no warning status occurs in the group. Example: Warning = Relay off
3	BOTH NC	Error/warning open Normally closed	Alarm signal is on as long as no warning status or error status occurs in the group. Example: Warning or error = Relay off
4	OFF NO	Inactive Normally open	Alarm signal is always off
5	ERROR NO	Error closed Normally open	Alarm signal is off as long as no error status occurs in the group. Example: Error = Relay on
6	WARNING NO	Warning closed Normally open	Alarm signal is off as long as no warning status occurs in the group. Example: Warning = Relay on
7	BOTH NO	Error/warning closed Normally open	Alarm signal is off as long as no warning status or error status occurs in the group. Example: Warning or error = Relay on

10 ZAbulegalaxy gateway cloud connection

The ZAbulegalaxy gateway enables ZAcure to be connected to the ZAbulegalaxy cloud service. ZAcure can send data securely via this connection, which facilitates central data exchange, monitoring and further cloud-based functions. Communication forms the basis for the overarching management, analysis and integration of the connected systems.

Collected data is defined and managed on a device-specific basis. Every 5 minutes, the current data points from



the devices added to the application and cloud connection are transferred to ZAbulegalaxy.

Status, fault codes and information

Status	LED flashing code	Action	Description
OK	Green light on	Sets the text on the dash-board to Connected	The application runs without problems.
Info	Green light flashing	Sets the text on the dash-board to Starting...	The application is booting up.
Info	No impact	Sets the text on the dash-board to Connecting ZABG...	Info
Info	No impact	Sets the text on the dash-board to Setup Communication...	Info
Info	No impact	Sets the text on the dash-board to No Devices	Info
Error	Red light flashing	Sets the text on the dash-board to Unknown Error	An error that cannot be rectified has occurred. This may cause the application to restart.
Info	1 x green, 1 x red	The application is executing a command	The application is executing a command.
Error	1 x green, 2 x red	The cloud connection is not initialised or settings are missing	Settings are missing or have not been specified.
Error	1 x green, 3 x red	Settings contain incorrect information	Settings contain the wrong syntax or incorrect information.
Error	1 x green, 4 x red	Cloud settings contain incorrect information	Cloud settings contain data points that are not part of the device.
Error	1 x green, 5 x red	Failure to read cloud settings	Cloud settings cannot be read correctly.
Error	1 x green, 6 x red	Cloud configuration missing	No cloud settings could be found for the device.
Error	2 x green, 1 x red	Not possible to connect to ZAbulegalaxy due to network problems	It is not possible to connect to ZAbulegalaxy due to network problems.
Error	3 x green, 1 x red	Sets the text on the dash-board to Gateway Wrong Password	The password for the cloud endpoint is incorrect.
Error	3 x green , 2 x red	Sets the text on the dash-board to Gateway not Found/Deactivated	The ID for the cloud endpoint could not be found
Error	3 x green, 3 x red	Sets the text on the dash-board to Gateway ID/Password empty	The device ID or password for the cloud endpoint has not been specified.
Error	3 x green, 4 x red	Sets the text on the dash-board to Gateway Deactivated/Quota	The cloud endpoint organisation has reached the maximum message limit or has been manually disabled.
Error	3 x green, 5 x red	Sets the text on the dash-board to Manually Deactivated in Cloud	The cloud endpoint has been manually disabled.
Error	3 x green, 6 x red	Sets the text on the dash-board to Quota Exceeded	The cloud endpoint organisation has reached the maximum message limit.

Status	LED flashing code	Action	Description
Error	3 x green, 5 x red	Sets the text on the dash-board to Network Issue	A network problem occurred. ▷ Use another ntp server under Localisation.
Error	5 x green, 1 x red	Sets the text on the dash-board to Modbus Error	There is a communication problem with one or more devices.
Info	Blue light on	Sets the text on the dash-board to Stopped	The application has been stopped.

MQTT

An MQTT connection to ZAbuegalaxy can be established. This can be disabled in the cloud connection settings with **Allow Modbus Mqtt: No**.

The application is able to establish an MQTT connection to the MQTT broker in ZAbuegalaxy.

Requirements:

A connected ZAbuegalaxy Gateway application is available.

Procedure:

1. Log in to ZAbuegalaxy.
2. Select the appropriate gateway.
3. Click Connect to **MQTT Broker**.

10.1 Setting up the cloud connection

A setup wizard guides you through the steps to configure and manage the gateway and MODBUS devices in the cloud environment.

Requirements:

- Active internet connection.
- Information is available regarding the organisation, location and device specifications.
- The MODBUS devices are ready for configuration.
- The user has access to zabuegalaxy.io and has the rights to create or connect to a cloud endpoint. The user is logged in to ZAbuegalaxy.

If access is not available, please send an access request to ZIEHL-ABEGG.

Procedure:

1. Open the cloud connection window via the menu.
2. Initialisation
3. Copy the displayed DeviceCode.
4. Open the website <https://login.microsoft.com/device> and paste in the DeviceCode.
5. Select the Microsoft account for the corresponding ZAbuegalaxy login and log in.
6. Select a new gateway or an existing gateway.
7. Run the cloud setup wizard.
8. Save the configuration.



Configuring the device settings for the cloud connection

The screenshot shows a configuration window titled 'Cloud' for device 'CMP1.U1.H1'. It contains several input fields and buttons. Numbered callouts are as follows:

- 1: Device ID (ZAcCoreGateway-34369599/0021)
- 2: Device password (masked with dots)
- 3: Authentication URL (https://zabg-app-prod-devicemanagement.azurewebsites.net)
- 4: Heartbeat Interval (min) (0)
- 5: START, STOP, and RESTART buttons
- 6: Device key
- 7: Authentication mode (ZABG)
- 8: MQTT Control Restriction (OFF)
- 9: SAVE button

1	Device-ID	2	Device password
3	Authentication URL URL of the authentication interface. Filled in by the system. Do not modify manually without in-depth knowledge.	4	Heartbeat interval (min) Time between two availability checks.
5	START STOP RESTART	6	Device key Unique key for identifying the data target in the ZABlue- galaxy.
7	Authentication mode Indicates the way in which the ZAcCore cloud connection is authenti- cated with the ZABluegalaxy	8	MQTT control restriction Allows/deactivates control of ZAcCore data recording with MQTT via the ZABluegalaxy.
9	Info To display the descriptions in the browser.		

1 1 Application management

Application management enables applications to be installed, configured and managed on the ZAcCore.

Adding an application

1. Open the application management sub-menu via the menu.
2. Select the application type, version and configuration; these affect how the application works.
3. Install the application.
4. If necessary, adjust the application settings.

ApplicationCMP1.U1.H1

Select application type

1

Select application type

2

Version

3

Configuration

INSTALL

1	Select an application	2	Application version
3	Version configuration		

Configuring an application

- 1. Open the application management sub-menu via the menu.
- 2. Select the pencil symbol next to the application.
- 3. Configure the application.
- 4. Save the configuration.

11.1 Available applications

Applications are developed on a continuous basis. The following applications are currently available:

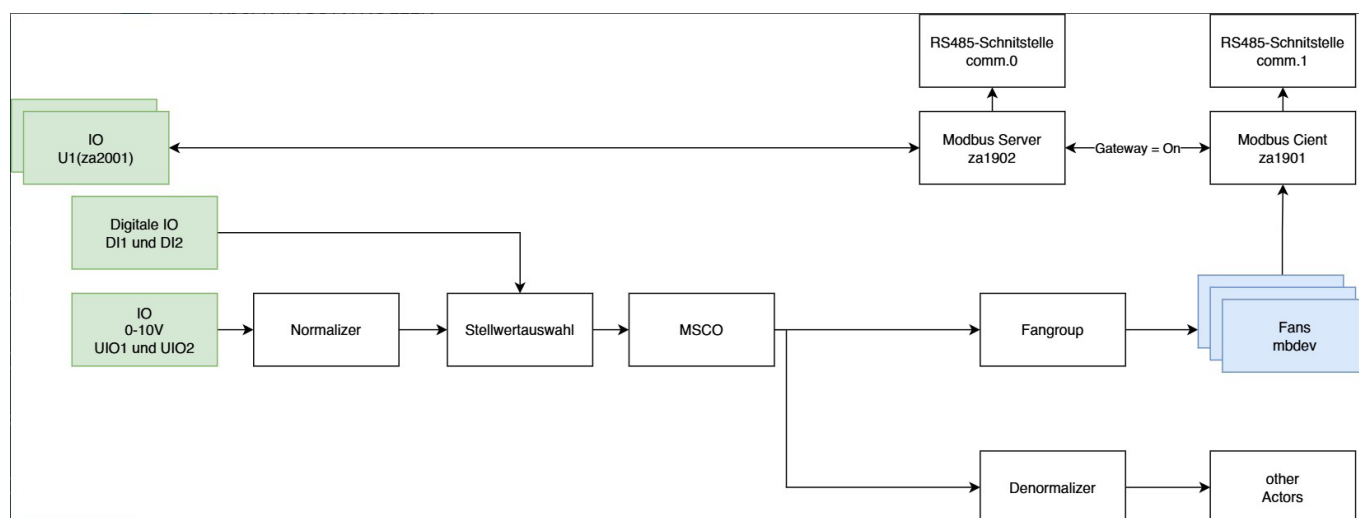
- Fan controller 0-10V, see *Fan controller 0-10V application, page 38*

11.2 Fan controller 0-10V application

The 0-10V fan controller application is a simple controller application with internal and external setpoints, one of which is selected to control fans or fan groups. In addition, a MODBUS server with gateway function and registers is available for reading and writing two U1-IO modules (MB server za1902), see *Description of the fan controller application, page 51*

The application is available for all product variants.





Procedure:

1. Install the application.
2. Fill the automatically created group **Fangroup 1** with appropriate devices, see *Grouping functions*, page 20.

Data points

Parameter/Data point	Description	Default value
MB address	MODBUS server address	246
Input 1 device ID (data point link)	Input device 1 to select the IO value	normalizer.0 --> Reference to UIO1 (in 0-10V mode) from the first IO module as standard
Input 2 device ID (data point link)	Input device 1 to select the IO value	normalizer.1 --> Reference to UIO2 (in 0-10V mode) from the first IO module as standard
DI input select	Input device for digital input signal: Switchover 1/2	iodev.0.300005
External/internal DI	Input device for digital input signal: External/internal switchover	
DI limit	Input device for digital input signal: Switch on limit	
DI full speed	Input device for digital input signal: Switch on full speed	
Freeze DI	Input device for digital input signal: Switch on freeze	
Output scaler ID	Output device for setting: Output	denormalizer.0
Set Intern1	Parameter specification in percent	80%
Set Intern2	Parameter specification in percent	50%
Min. setting	Minimum parameter specification in percent	0%
Max. setting	Maximum parameter specification in percent	100%
Limit	Maximum parameter specification in percent	100%
Selection setting		1 (1 or 2)
Internal/external selection		External(internal or external)
Input 1/2 function		S2 = INTERNAL
MSCO		2%

Parameter/Data point	Description	Default value
Output		Read value %
Specification 1		Read value %
Specification 2		Read value %
Current specification		Read value (1 or 2)
Input limit		Read value (0/1)
Input full speed		Read value (0/1)
Input freeze		Read value (0/1)
MSCO status		Read value (0/1)

12 Displaying device information

▷ Open Info via the menu.

Designation	Explanation	Designation	Explanation
Product code	Describes the device type.	WebUI Ethernet	Web address via Ethernet
RTS version	Runtime system version ZAcCore software version	Wi-Fi WebUI	Web address via Wi-Fi
App version	-	Local time	Device time and date
Masterkey	-	Free RAM memory	Free memory space
MAC address	-	Local UI version	Version of the integrated touchpanel UI
IP address ETH0	IP address of the ZAcCore Ethernet port	Remote UI version	Version of the remote display UI
Manufacturer	-	Web UI version	Version of the Web UI
Device type	-	Serial number	Serial number of the device

13 System

The maintenance area of the ZAcCore includes central settings for localising, updating, maintaining and managing components and importing/exporting content.

13.1 Localisation

The language/date/time of the ZAcCore and Web UI are managed under Localization.

Adjusting the language/date/time

1. Open the localisation sub-menu via Menu/System.
2. Configure the language/date/time.
3. Save settings.

Configuring localisation

Automatic time synchronisation with an NTP server is active when there is an active internet connection.



SystemCMP1.U1.H1

1Timezone*(UTC+01:00) Amsterdam, Berlin, Rome

7Format imperial/metric*metric

2Date formatdd.mm.yy

812h24h

3Select date*1.1.1970

9Select time*09:45

4

10

5Automatic summer time changeover

6Time server 10.pool.ntp.org

11Time server 21.pool.ntp.org

SAVERESET

1	Time zone	2	Date format dd.mm.yy - day.month.year mm.dd.yy - month.day.year
3	Select date	4	Calendar icon For easy selection of the date (3).
5	Automatic switch to daylight saving time ON: Automatic summer/winter time. OFF: No automatic summer/winter time.	6	Time server 1 Specification of the NTP server for automatic time synchronisation of the system.
7	Imperial/metric format Selection of the unit system.	8	12h/24h Selection of the time display.
9	Select time	10	Clock icon For easy selection of time (9).
11	Time server 2 Specification of the NTP server for automatic time synchronisation of the system if the first time server cannot be reached.		

13.2 Update management

The ZAcCore supports automatic and manual updates and enables the secure provision of signed update packages.

Performing an automatic update

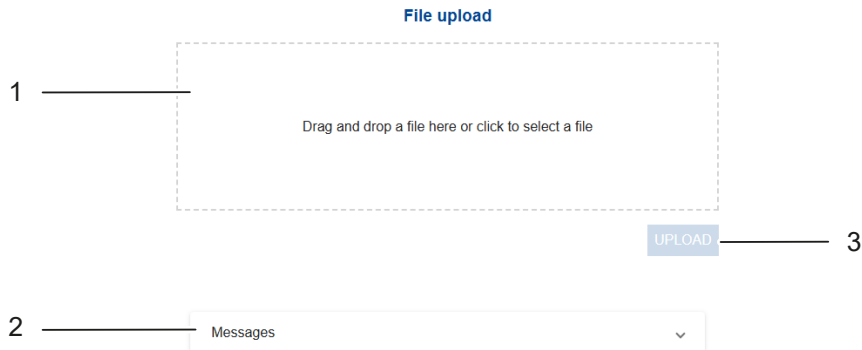
1. Open the update manager via Menu/System.
2. Check for updates by clicking the CHECK ONLINE button.
3. Start the update.



Checking whether an update is available online

Manual Update via file upload from Host

Manual update of the system using a update file from the host



1. Open the update manager via Menu/System.
2. Drag and drop the update file into the field (1).
3. Start the update (3).
4. During the update, messages are displayed at the bottom (2).

13.3 Maintenance

The following functions can be performed in the Maintenance window:

- Restart
- Factory settings
- Reset the app
- Restart the network
- Restart RTS Runtime System is restarted
- Activate SSH
- Deactivate SSH
- Ext. COM 0 touchpanel
- Ext. USB touchpanel
- Ext. touchpanel off
- Database backup
- Restore database

Executing a function

1. Open the Maintenance window via Menu/System.
2. Click on the corresponding function.
3. Execute the function.

13.4 Exporting and importing data

The import and export area enables central system data to be uploaded and downloaded securely. This includes data such as databases and password recovery files for backing up, transferring or restoring configurations in the event of service.

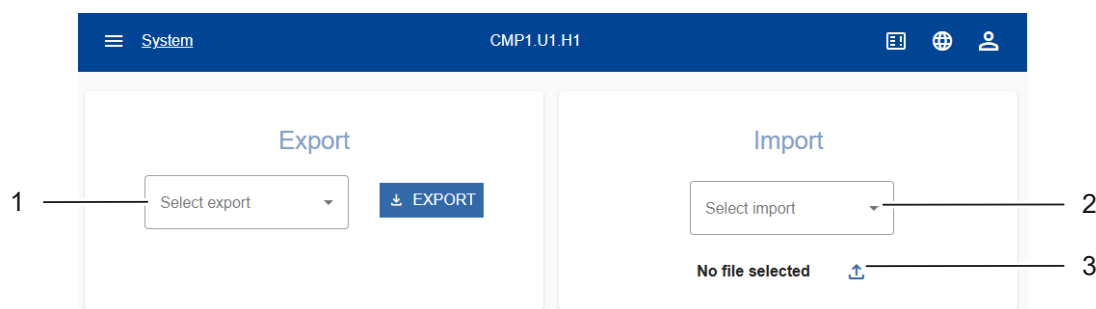
Exportable files



Designation	Explanation
Database	Exports the device's current database. It contains all data configured at the time of export, e.g. users, passwords (encrypted), devices, interfaces, etc.
BACnet EDE	Exports an EDE file based on the current BACnet configuration.
Password recovery file	Exports the password recovery file for the user currently logged-in.

Importable files

Designation	Explanation
Database	Imports a ZAcCore database (plcdata.db), e.g. from another ZAcCore. After a restart, the device is started up with this database, which means that the users, passwords, etc. from the imported database can be used.
Web server certificate	Imports a web server certificate that confirms the identity of a website and enables an encrypted connection to be established between the server and browser.
Description of the device	Device descriptions can be imported here later so that devices that are currently not known to the ZAcCore can be added at a later date.



Exporting a file

1. Open the Import/Export window via Menu/Systems.
2. Select the file to be exported (1).
3. Start the export.

Importing a file

1. Open the Import/Export window via Menu/Systems.
2. Select the file to be imported (2).
3. Select the file by clicking on the button (3).
4. Start the import.

14 Integrating ZAcCore into networks

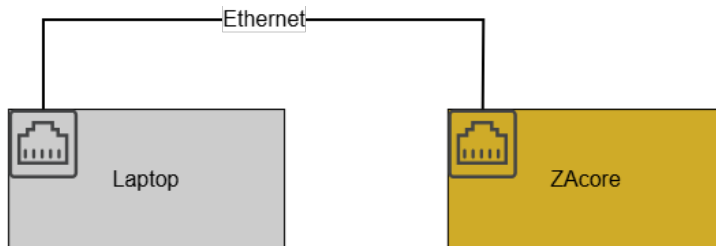
14.1 Use within a LAN

Local networks are defined as an Ethernet network consisting of several computers and peripheral devices, typically within one building. The network may also be significantly smaller in size, for example within one room or control cabinet. An Ethernet cable RJ-45, Cat. 5 or higher, is used for the connection. The length of the cable must not exceed 100 m. The transmission rate is 10 Mbit/sec or 100 Mbit/sec for a ZAcCore device.

There are 3 types of local network:

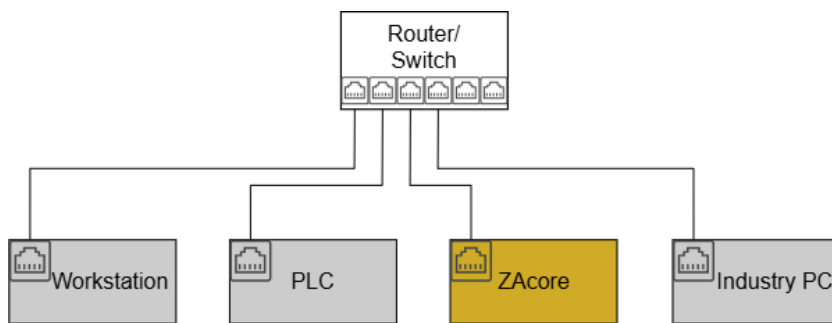
- Direct connection, consisting of 2 members connected directly to one another.
- Simple local networks consist of several members connected via a switch.
- Local networks with internet access, almost identical to simple networks. The switch is also connected to a router that enables access to the internet.

Direct connection



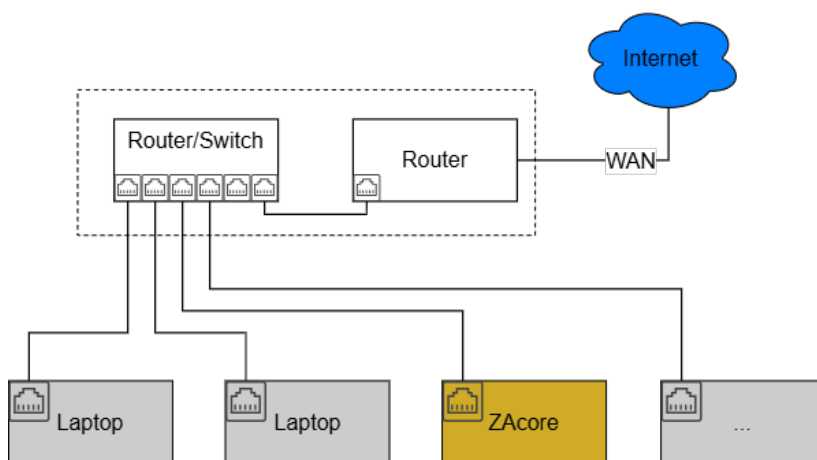
Direct connection
Local Area Network with only two devices

Simple local network



Simple local network

Simple local network with internet access



Local network with internet access



Setting options

Name	Name 2	Description
DHCP	Dynamic Host Configuration Protocol	Function that automatically takes care of the network setup. When DHCP is enabled, the following settings are set automatically: ▫ IP address ▫ Subnet mask ▫ Gateways ▫ DNS DHCP only works if the router on the network supports DHCP. Most common routers, such as FritzBox, Teltonika or company networks, support DHCP by default.
IP address	Internet Protocol address IPv4 static address	Unique identification/address of the device in the form of 4 numbers separated from one another by a dot. Common addresses are: ▫ 192.168.1.x ▫ 192.168.10.x ▫ 192.168.178.x ▫ ... Within a local network, the first 3 numbers must be the same for all members in most cases, dependent on the subnet mask. Addresses ending with 1 should be avoided, except for routers for private or proprietary networks (RFC 1918): ▫ 10.0.0.0 to 10.255.255.255 ▫ 192.168.0.0 to 192.168.255.255 ▫ 172.16.0.0 to 172.31.255.255
Subnet mask	Subnet	Sets the size of the local network and limits the number of possible network members. The most commonly used value is 255.255.255.0 ▫ 255.0.0.0: Large networks, classic Class A network 16 million hosts. ▫ 255.255.0.0: Medium networks, Class B network 65,536 hosts. ▫ 255.255.255.0: Small networks, Class C network 256 hosts. ▫ 255.255.255.255: Special mask for communication with a single host (broadcast).
Gateway IP	IPv4 gateway	Address of the device that connects to the internet (router). Often an IP address that ends in x.x.x.1. The remaining digits often correspond to the same numbers that are in the proprietary IP address.
DNS IP	Domain name System IPv4 DNS1 IPv4 DNS2	Address of the device that handles the hostname resolution. Convert the website name in the URL to the IP address, usually the same IP address as the gateway.
WAN	Wide Area Network	Connects networks and PCs across national or continental borders (internet).

14.1.1 Local networks with switch

For networks with switches or routers, e.g. Teltonika routers, FritzBoxes or company networks, we recommend activating DHCP so that no further IP settings need to be configured on the ZAcCore control system.

Notice: This may lead to the IP address of the ZAcCore control system changing.

To prevent this, a fixed IP for the ZAcCore control system can be stored in the router (DHCP) settings (web interface

of the router) (IP leasing).

Settings like this may have to be configured by the IT department if the ZAcCore control system is connected to a (company) network and this network is managed by the IT department.

For configuration without DHCP, all settings must be configured manually.

- IP4 address
- Subnet mask
- Gateways
- DNS1 (optional)
- DNS2 (optional)

Please also see: *Direct connection*, page 46

Potential problems in company networks

Problem	Root cause	Solution
MAC address of the ZAcCore control unit is blocked	Control unit cannot be reached and has not been assigned with an IPv4 address (DHCP).	▷ Release MAC address in the network, see name plate.
Ports are locked	A service, such as a Modbus (TCP) server or BACnet server, cannot be reached.	▷ Enable ports on the network. ▫ Modbus TCP standard port: 502 ▫ BACnet Server (UDP) standard port: 47808

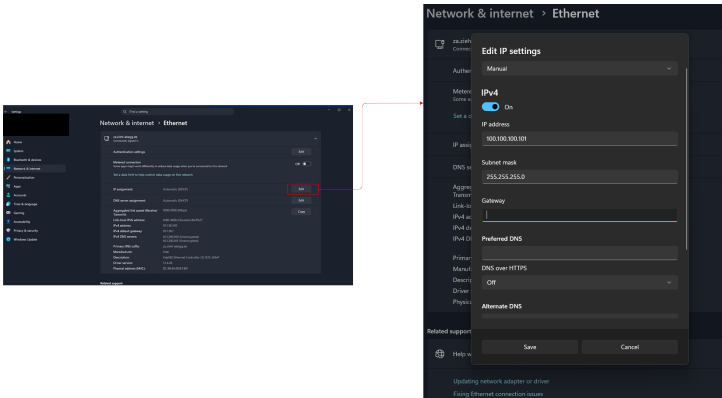
14.1.2 Direct connection

Procedure:

1. Connect the PC or laptop to ZAcCore via an Ethernet cable.
2. Turn off the PC or laptop's Wi-Fi function.
3. Adjust the Ethernet setting of the PC or laptop and the ZAcCore PLC, see *Windows settings*, page 46 and *WEB UI settings*, page 47.

Windows settings

Open the Ethernet settings via Settings/Network and Internet/Ethernet/Ip assignment.



- Laptop DHCP: Manual
- Laptop IP: 10.10.10.11
- Laptop subnet: 255.255.255.0 (typical subnet setting Class C network with up to 256 members)



WEB UI settings

For Ethernet settings, see *Ethernet interface*, page 23

- ZAcCore DHCP: Off
- ZAcCore IP: 10.10.10.12
- ZAcCore subnet: 255.255.255.0 (typical subnet setting Class C network with up to 256 members)

14.2 Use within a Wi-Fi network

The ZAcCore's Wi-Fi network allows for wireless connection to mobile end devices or the internet within a limited geographical area.

A typical Wi-Fi network structure consists of Internet access, a router with an integrated or separate access point, and various wireless end devices. Security and scalability are ensured through the targeted use of encryption, access points, mesh systems and other components.

Central components of a Wi-Fi network

- Internet connection: The Wi-Fi network is usually connected to internet access, e.g. via DSL, a cable or fibre glass.
- Wi-Fi router: The router is the central device responsible for distributing the internet connection and managing the network. In Station Mode, the ZAcCore connects to a Wi-Fi router.
- Access Point: The access point provides the actual wireless network. ZAcCore is an access point in the factory settings and thus provides a small network for access to itself.

End devices

End devices that connect to the ZAcCore Wi-Fi network (AP Mode) include, for example:

- Laptops and desktop PCs
- Smartphones and tablets
- IoT devices, e.g. smart sensors

Network architecture

The typical Wi-Fi network architecture is based on a star topology: all end devices connect directly to the central access point or router. In more extensive environments, multiple access points can be strategically placed to improve network coverage and performance. These access points are usually connected to the central router or switch via cables.

Security in a Wi-Fi network

An important component of a Wi-Fi network structure is the security concept. Typically, the following measures are used:

- Encryption using WPA2 or WPA3
- Creation of a secure Wi-Fi password
- Optional: Guest networks with separate access
- MAC address filtering optional

Extensions and special features

- Mesh networks: Mesh systems are often used in modern systems to avoid signal dead zones. They consist of several interconnected access points that seamlessly forward the Wi-Fi signal.
- Repeaters: Repeaters can be used to extend the range of an existing Wi-Fi network by amplifying and forwarding the signal.

14.3 Connecting to the Internet via a mobile network

There are different approaches to connecting the ZAcord to the internet via mobile communications, depending on the bandwidth required and the requirements of the local network. Mobile communication modems, gateways/bridges and routers are available on the market for different mobile communication standards.

Mobile communication gateway

A mobile communication gateway connects a local network to the internet via mobile communications. It is an independent device that manages the mobile communications connection itself. A mobile communication gateway has its own user interface. ZAcord is a network member and is connected to the gateway via LAN. The internet connection can be shared by several members.

Mobile communication router

In terms of functions, a mobile communication router is comparable to a gateway and connects a local network to the internet via mobile communications. Routers often have an integrated switch and other interfaces such as Wi-Fi network.

14.3.1 Mobile communication standards

In addition to the fast LTE standards with LTE CAT1 and above, there are the LTE-NB1, LTE-NB2 and LTE-M standards developed for the Internet of Things (IoT). These standards are designed for low transfer rates but are better suited for building applications.

The decision as to which solution should be used is dependent on the application, the volume of data generated and availability at the installation site.

From a cost and energy consumption perspective, LTE-NB1, LTE-NB2 and LTE-M are the optimal solutions.

Characteristic	LTE NB1	LTE NB2	LTE-M LTE CAT-M1	LTE CAT1	LTE CAT4 and above
Transmission rate	250 kbit/s uplink/downlink	156 kbit/s uplink 127 kbit/s downlink	up to 1 mbit/s uplink/downlink	up to 10 mbit/s uplink/downlink	50 mbit/s uplink 150 or more mbit/s downlink
Mobile	no	no	yes	yes	yes
Building penetration	Very good	Very good	Good	Moderate	Poor
Energy efficiency	Very good	Very good	Good	Moderate	Poor

14.3.2 Mobile network solutions for ZAcord

- ▷ When selecting a mobile communications solution, observe the regional regulations and specifications of the respective mobile network provider.

Recommended solution for mobile communications connection

Type	Equipment	Connection
Teltonika TRB140	LTE CAT-4 with one Ethernet port and USB, 9-30 VDC voltage supply https://www.teltonika-networks.com/products/gateways/trb140	Ethernet, USB possible via RNDIS
Teltonika TRB256	LTE CAT-M (LTE-M), LE-NB1, LTE-NB2 Dual SIM, Ethernet port, RS-485, RS-232, IO, 9-30 VDC voltage supply https://www.teltonika-networks.com/products/gateways/trb256	Ethernet



Type	Equipment	Connection
Teltonika TRB247	LTE CAT-1, Dual SIM, Ethernet port, RS-485, RS-232, IO, 9-30 VDC voltage supply https://www.teltonika-networks.com/products/gateways/trb247	Ethernet

Modems

ZAcore does not currently support mobile communications modems.

The max. power of the USB interface is 2.5 W, which in most cases is not sufficient for supplying mobile modems via USB, especially with LTE CAT1 and higher. Modems with an additional voltage supply are difficult to acquire.

15 Notes and troubleshooting

Fault codes

No.	Text	Remedy
1	Master key required	▷ Enter the correct master key. This is assigned when the ZAcore is set up for the first time.
2	Password required	▷ Enter password - field cannot be left empty.
3	Username required	▷ Enter username - field cannot be left empty.
4	Password must contain at least 8 characters with upper/lower case letters, numbers and special characters (apart from: '-')	▷ Use a password with at least 8 characters including upper and lower case letters, numbers and special characters. ▷ DO NOT use the character "-".
5	The password does not meet the password rules	▷ Adapt the password to comply with the password rules. At least 8 characters, upper and lower case letters, numbers and special characters. ▷ DO NOT use the character "-".
6	Passwords do not match	▷ Make sure the passwords in both fields are identical
7	The string is incorrectly formatted.	▷ Check input for the correct format, e.g. only numbers, no special characters or correct IP format.
8	Mode required	▷ Select addressing mode from the drop-down list.
9	A maximum of 64 addresses are allowed	▷ Reduce the number of flex addresses entered to no more than 64.
10	Invalid separator, allowed: (',' & ';')	▷ Use only a comma or semicolon as a separator.
11	Addresses must be between 1 and 247	▷ Use only flex addresses in the range 1-247.
12	Invalid address found	▷ Use only whole numbers in the range 1-247.
13	Invalid combination of separators found	▷ Use only a comma or semicolon as a separator.
14	There are duplicate addresses:	▷ Remove duplicate addresses from the entry.
15	Interface is required!	▷ Select the interface from the drop-down list.
16	Timeout is required!	▷ Enter timeout value.
17	IPv4 address required	▷ Enter a valid IPv4 address, e.g. 192.168.1.1.
18	Subnet mask required	▷ Enter valid subnet mask, e.g. 255.255.255.0.
19	Wrong format	▷ Check that the format of the input is correct, e.g. valid IPv4 format.
20	Gateway address required	▷ Enter a valid gateway address.
21	Baud rate is required	▷ Select baud rate from the list.
22	Address too small	▷ Enter an address greater than 0.
23	Address too large	▷ Enter an address lower than 255.



No.	Text	Remedy
24	Address is required	▷ Enter MODBUS address - the field must not be left empty.
25	Device type is required	▷ Select the device type from the drop-down list.
26	No file selected	▷ Select the file via the File dialogue.
27	Passwords do not match	▷ Fill out both password fields so they are identical.
28	Incorrect file format. Please select a CSV file.	▷ Select file in CSV format.
29	Password recovery failed. Call parameters may be missing!	▷ Specify the correct username and recovery file.
30	The recovery file does not match the specified user.	▷ Use the correct recovery file for the username entered.
31	The recovery file does not match this ZAcCore device.	▷ Use the recovery file created for this specific ZAcCore device.
32	An error occurred during the installation process	▷ Check the network connection and restart the installation process.
33	Access to cloud service denied	▷ Check cloud credentials and permissions.
34	Device code could not be copied	▷ Check browser permissions for the clipboard function. ▷ Copy the code manually.
35	An error occurred during the saving process	▷ Check the connection to the device and restart the saving process.
36	An error occurred while adding the device to the cloud	▷ Check the cloud connection and make sure the device is configured correctly.
37	An error occurred while removing the device from the cloud	▷ Check the cloud connection and try again.
38	Error: The cloud connection could not be started.	▷ Check the cloud connection and try again.
39	Error: No cloud connection object found.	▷ Correctly configure the cloud connection object
40	Unable to install app	▷ Check the network connection and cloud configuration.
41	Internet connection available, but Hawkbit server cannot be reached.	▷ Check the network's Hawkbit server configuration and firewall rules.
42	ZAcCore is not connected to the internet, but the Hawkbit server can be reached via the host computer.	▷ Establish a direct connection to the internet. ▷ Use host connection.
43	ZAcCore is not connected to the internet and the Hawkbit server cannot be reached.	▷ Establish a connection to the internet. ▷ Check Hawkbit server accessibility.
44	No network SSIDs found. Please run a network scan.	▷ Start the network scan using the corresponding button and wait until SSIDs are detected.
45	An error occurred. Please try again.	▷ Please try again.
46	Unable to add new device	▷ Please try again. ▷ Check the connection to the device.
47	The RDI did not deliver any results. Please enter the device data manually.	▷ Enter the device information address and device type manually.
48	An error occurred while running the RDI.	▷ Check the connection to the device and restart the RDI query.
49	An error occurred!	▷ Please try again.
50	Maximum number of MODBUS masters reached	1. Remove an existing MODBUS master. 2. Add a new MODBUS master.
51	No operating manual found	-



No.	Text	Remedy
52	An error occurred while saving the alarm group	▷ Check the alarm group configuration and try again.
53	An error occurred while removing a device from the group	▷ Check device assignment and try again.
54	An error occurred while initialising the cloud connection.	▷ Check the cloud configuration and try again.
55	The part or serial number is missing.	▷ Enter missing part number and/or serial number in the device profile.
56	The device must have a part and serial number to be added to the cloud	▷ Enter the part number and serial number before adding the device to the cloud.
57	An error occurred during the saving process:	▷ Check the configuration and restart the saving process.
58	An error occurred while deleting:	▷ Please try again.
59	The address at position [x] is not allowed. Addresses can only be in the range 1-247.	▷ Correct the invalid address in the CSV file to a value in the range 1-247.
60	Too many addresses available in the file. A maximum of 64 addresses are allowed.	▷ Reduce the number of addresses in the CSV file to a maximum of 64.
61	Error	▷ Please check the entered values and try again.
62	Incorrect master key	▷ Enter the correct master key.
63	An error occurred during login!	▷ Check access data and try again.
64	Error code: [code] / Message: [msg]	▷ Check the connection to the device and log in again.
65	An error occurred! - The file was not transferred in full (file size is not compatible)	▷ Check that the file is complete and restart.
66	An error occurred! - An error occurred while importing the file!	▷ Check the file and network connection and try again.
67	An error occurred! - This profile could not be deleted because it is the last administrator account.	▷ Create another administrator account before deleting the first one.
68	An error occurred! - [Cloud connection error]	▷ Check cloud connection settings.
69	An error occurred! - Unable to install app	▷ Check the network connection ▷ Restart ZAcCore.
70	Device could not be deleted	▷ Check the connection and permissions and try again.
71	Unable to create gateway. Do you want to remain in the wizard or exit?	▷ Check the gateway configuration and network connection.
72	Unable to close setup wizard. Do you want to remain in the wizard or exit?	▷ Attempt the saving process again. ▷ Restart the wizard later.
73	Unable to restart cloud connection. Do you want to remain in the wizard or exit?	▷ Check the cloud configuration and restart manually.
74	An error occurred! - Failed to save	▷ Check the connection and restart.
75	An error occurred! - An error occurred during removal	▷ Please try again.
76	Automatic logout due to inactivity	▷ Log in again.
77	Unauthorised action - The current user either has no rights to perform this action or the login token has expired.	▷ Log in again. ▷ Use a user account with sufficient permissions.

16 Description of the fan controller

application

The application is responsible for addressing, control, diagnostics, communication and long-term data collection and can be easily integrated into existing systems via open protocols. The application supports ZIEHL-ABEGG EC fans with integrated control and external fan types via open and standardised interfaces such as MODBUS or analogue input signals.

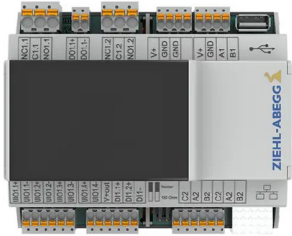
16.1 System architecture

16.1.1 Hardware components

- The ZAc core controller is responsible for control, diagnostics and communication of EC or AC fans.
 - With EC: integrated motor control, digital parameter communication
 - With AC: control via external frequency inverters
- Communication interfaces
 - Analogue industry standard signals 0-10 V or 4-20 mA
 - MODBUS RTU / MODBUSTCP
 - BACnet MS/TP or IP
- Optional sensors: Temperature, pressure, air flow, vibration sensors
- Options for modular expansion: additional inputs, outputs and interfaces

16.1.2 HMI and visualisation

Parameterisation and diagnosis via ZAc core touchpanels, webpanels or mobile terminals.

HMI	Picture
2.4" ZAc core panel - capacitive touch ▫ Integrated in ZAc core controller with type key H1 ▫ Display of ZAc core touchpanel UI	
4.3" Flexi Panel - capacitive touch ▫ Voltage supply 24 V ▫ Standard display of ZAc core touchpanel UI ▫ Alternative Renu Flexisoft HMI solution ▫ Communication: RS-485 - Optional USB, Ethernet	
7" Webpanel - capacitive touch ▫ Voltage supply 24 V ▫ Integrated chrome browser ▫ Display of ZAc core WebUI or CODESYS webvisu ▫ Communication: Ethernet	



HMI	Picture
Any web-enabled device, e.g. PC, mobile devices, etc.	

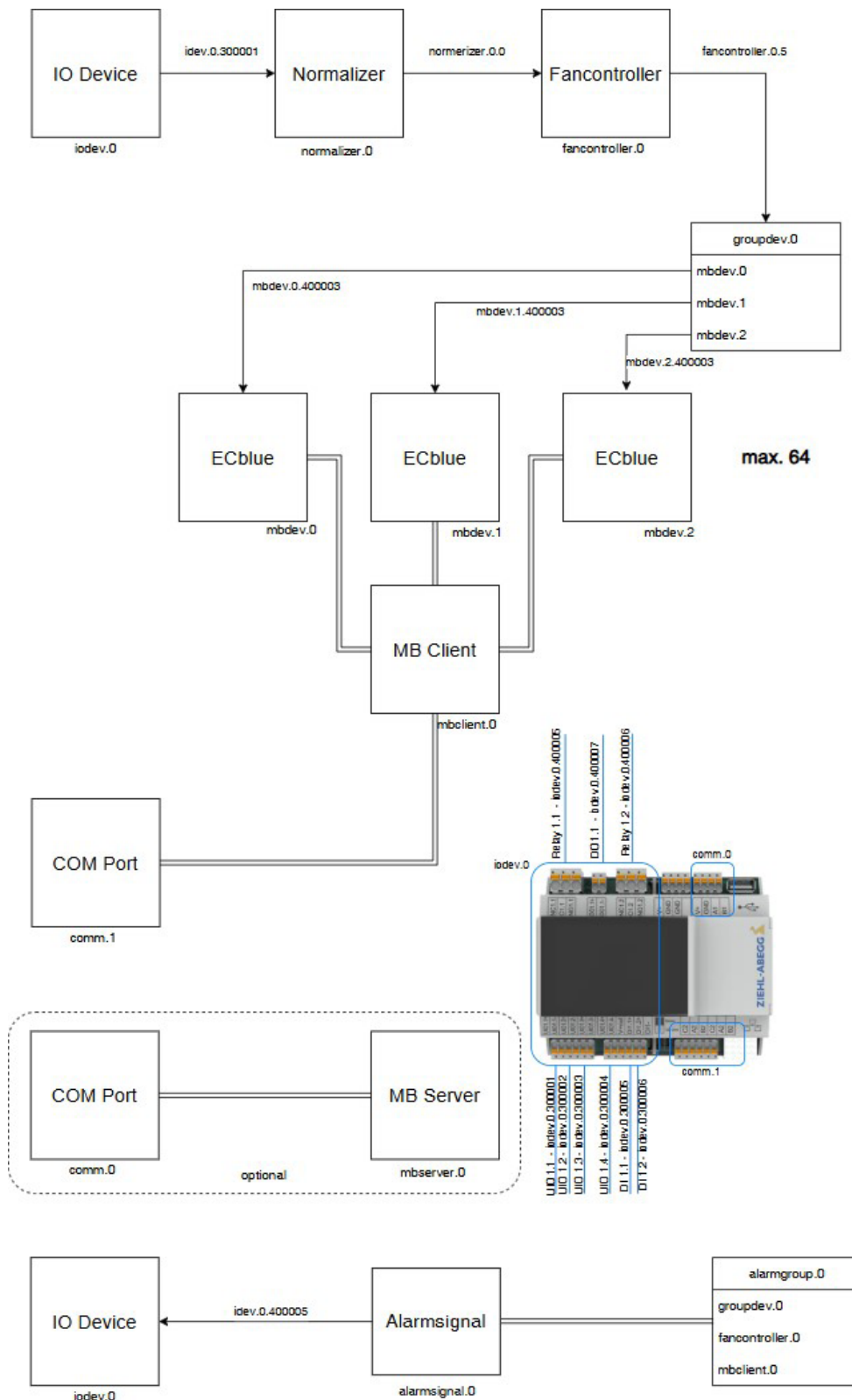
16.1.3 Software components

ZAcCore offers a ready-to-use application for controlling fans and fan walls and various prepared configurations with connection templates for different applications. This fan controller application is built from ZAcCore function block components. As standard, up to 6 fan controller applications can be installed in parallel on a ZAcCore device.

ZAcCore function block	Description
IO device (iodev)	Provides signal values (AI, AO, DI, DO) for one or more IO modules
Normaliser (normaliser)	Standardises an IO signal for use with ZAcCore. Function blocks e.g. 0-10V -> 0-1. A normaliser is required for every signal.
Fan controller (fan controller)	The core of the application provides fan or a fan group control functions that are familiar from other ZIEHL-ABEGG devices, e.g. UNIcon Master Mode 1.01: ▫ 2 external setpoints (0-10V, MODBUS, etc.), can be switched by the user ▫ Interface or digital input ▫ 2 internal setpoints, can be adjusted in the user interface, can be switched by the user ▫ Interface or digital input, can be switched to external setpoints via digital input ▫ Minimum and maximum limitation ▫ Limit function ▫ Freeze function ▫ Maximum output function ▫ Anti-jamming function
Fan group (groupdev)	Grouping of fans with a shared control system, e.g. a fan wall. Supports ZIEHL-ABEGG fans and third-party models. Grouping takes place on the user interface.
ECblue (mbdev)	Fan connected to ZAcCore via a MODBUS RTU network. Can also be a supported third-party model.
MB Client (mbclient)	MODBUS Communication Manager (MODBUS Master), which exchanges data with connected devices and monitors the devices.
MB Server (mbserver)	Optional. Provides data for higher-level controls or building management. Used to control fans with ZAcCore via MODBUS. An MB server supports MODBUS RTU (RS-485) and MODBUS TCP. The selection is made via the assigned interface.
COM Port (comm)	Serial RS-485 interface of the ZAcCore through which MODBUS communication flows.
Socket (socket)	An Ethernet connection through which MODBUS communication flows. A socket is required for MODBUS TCP communication.
Alarm group (alarmgroup)	An alarm group monitors all components for errors and warnings assigned to this alarm group. An alarm group is usually linked to at least one alarm signal to signal an alarm to users.
Alarm signal (alarmsignal)	An alarm signal is used to report an alarm to the user. There are several types of signals. The fan controller application is set up for digital alarms to be indicated via a relay output. A digital alarm signal can also be placed on a MODBUS register or a BACnet object. An alarm group can be connected to several alarm signals. If technically feasible, alarms can be sent by email or SMS.

Each ZAcCore function block can be instantiated multiple times. The instance number is the first number in a ZAcCore object name. The 2nd number is the number of a data point in a function block.

16.1.3.1 Application diagram for the ZAc core fan controller application



16.1.4 Communication and control concept

Automatic addressing & device detection

In the case of fan walls or multiple MODBUS members, the ZAc core function block `mbclient` can perform auto-addressing for connected fans. The following are read out automatically:



- Fan type
- Article and serial number
- Communication status in relation to auto-addressing and data collection

Modes

The fan controller application supports the following control modes:

- Speed control via analogue signals 0-10V or 0-20mA
- Speed control via MODBUS register
- Manual setting via user interface
- Optional operating point monitoring and optimization using characteristic curves or internal motor data

Communication with GLT / building automation

- Provision of all operating data via MODBUS RTU/TCP or BACnet
- Status and fault codes
- Future provision of operating data collection and digital history

16.2 Application functions

Operational control

ZAcore controls:

- The speed of fans, even those from other manufacturers
- Synchronous group or individual control of several fans
- Response to communication failure or fan failure, error management and responses

Diagnostics & fault processing

- Monitoring of current, voltage, temperature, speed
- Detection of typical errors such as:
 - Fan is not rotating
 - Supply phase failure
 - Overvoltage / undervoltage
 - Resonance ranges / fault diagnosis and remedies according to technical documents

Data logging & history

- Logging of selected operating parameters
- Event and error logs
- Export of log data, e.g. JSON, CSV or GLT query

16.3 Safety and specific operating conditions

Operation in humid environments

- Anti-jamming function - regular run-up to avoid moisture Notice regarding operation in humid environments

Resonance prevention

- Automatic suppression of critical speed ranges
- Fast transition through these ranges, recommendations for avoiding resonance

16.4 Options for expanding the application

The solution can be expanded with:

- Control functions, e.g. air flow
- ZABluegalaxy cloud connection
- MQTT cloud connection
- OPC-UA interface under preparation
- Additional external sensors
- Future control algorithms for vibration optimisation

16.5 Start-up and commissioning

1. Log in to the ZAcCore WebUI via Wi-Fi or LAN connection, see *Operation, page 13*.
2. For the selection, adaptation and installation of applications via the ZAcCore application manager based on prepared configurations, see *Application management, page 37*.

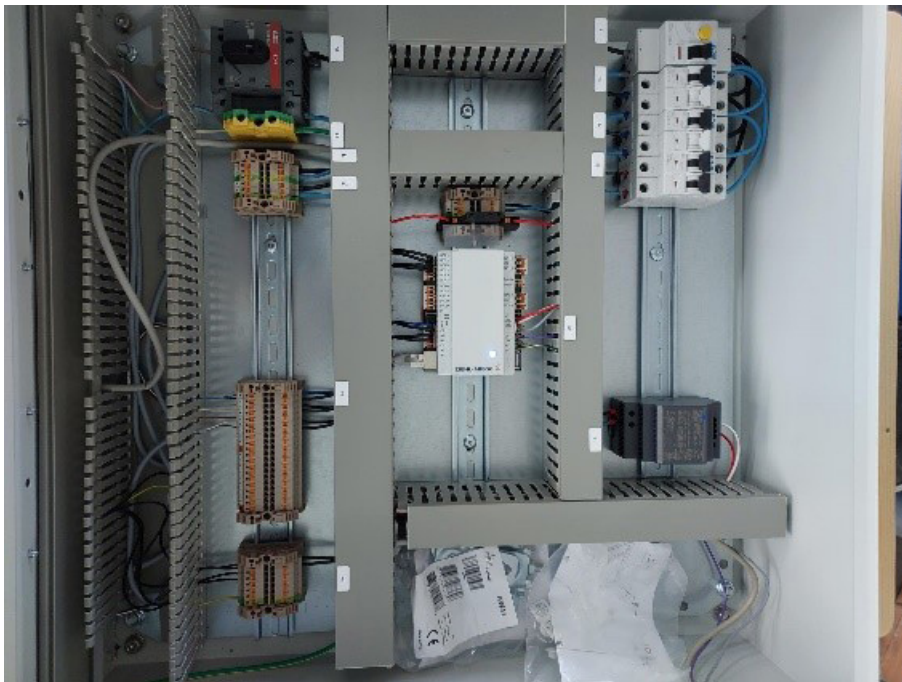
These include:

- Fan controller, comparable to UNIcon MODBUS master 1.01
- Automatic network detection for fans
- Creation of a fan wall fan group
- Creation of an alarm manager

16.6 Examples

Retrofit solutions

The replacement of large single fans with EC fan walls enables air to be guided with greater efficiency and flexibility. ZAcCore looks after all the services required for smooth integration into existing systems and expands the system with additional functions found in modern ventilation systems



[illegible]

Service

+49 7940 16 800

fan-controls-service@ziehl-abegg.de



ZIEHL-ABEGG SE Heinz-Ziehl-Straße D-74653 Künzelsau +49 7940 16-0 info@ziehl-abegg.de www.ziehl-abegg.com

© by ZIEHL-ABEGG - 2026/20 - Index 001 - Subject to technical changes