WAGO
TECHDOCS

Manual

WAGO

WAGO I/O System 750

750-8214

PFC200; G2; 2ETH RS CAN
Controller PFC200; 2nd Generation; 2 x ETHERNET,
RS-232/-485, CAN, CANopen

WAGO GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 844 169

E-Mail: info@wago.com

Web: www.wago.com

Technical Support

Phone: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

E-Mail: support@wago.com

Every conceivable measure has been taken to ensure the accuracy and
completeness of this documentation. However, as errors can never be fully
excluded, we always appreciate any information or suggestions for improving the
documentation.

E-Mail: documentation@wago.com

We wish to point out that the software and hardware terms as well as the
trademarks of companies used and/or mentioned in the present manual are
generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Notes about this Documentation

> ### Note
>
> **Always retain this documentation!**
> This documentation is part of the product. Therefore, retain the documentation during the entire service life of the product. Pass on the documentation to any subsequent user. In addition, ensure that any supplement to this documentation is included, if necessary.

1.1 Validity of this Documentation

This documentation is only applicable to the "PFC200; G2; 2ETH RS CAN" controller (750-8214).

This documentation is only applicable from FW Version 04.02.13(24).

1.2 Copyright

This Manual, including all figures and illustrations, is copyright-protected. Any further use of this Manual by third parties that violate pertinent copyright provisions is prohibited. Reproduction, translation, electronic and phototechnical filing/archiving (e.g., photocopying) as well as any amendments require the written consent of WAGO GmbH & Co. KG, Minden, Germany. Non-observance will involve the right to assert damage claims.

1.3   Property rights

Third-party trademarks are used in this documentation. This section contains the trademarks used. The "®" and "TM" symbols are omitted hereinafter.

• Adobe® and Acrobat® are registered trademarks of Adobe Systems Inc.

• Android™ is a trademark of Google LLC.

• Apple, the Apple logo, iPhone, iPad and iPod touch are registered trademarks of Apple Inc. registered in the USA and other countries. "App Store" is a service mark of Apple Inc.

• AS-Interface® is a registered trademark of the AS-International Association e.V.

• BACnet® is a registered trademark of the American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).

• *Bluetooth*® is a registered trademark of Bluetooth SIG, Inc.

• CiA® and CANopen® are registered trademarks of CAN in AUTOMATION – International Users and Manufacturers Group e.V.

• CODESYS is a registered trademark of CODESYS Development GmbH.

• DALI is a registered trademark of the Digital Illumination Interface Alliance (DiiA).

• EtherCAT® is a registered trademark and patented technology licensed by Beckhoff Automation GmbH, Germany.

• ETHERNET/IP™ is a registered trademark of the Open DeviceNet Vendor Association, Inc (ODVA).

• EnOcean® is a registered trademark of EnOcean GmbH.

• Google Play™ is a registered trademark of Google Inc.

• IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.

• KNX® is a registered trademark of the KNX Association cvba.

• Linux® is a registered trademark of Linus Torvalds.

• LON® is a registered trademark of the Echelon Corporation.

• Modbus® is a registered trademark of Schneider Electric, licensed for Modbus Organization, Inc.

• OPC UA is a registered trademark of the OPC Foundation.

- PROFIBUS® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).

- PROFINET® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).

- QR Code is a registered trademark of DENSO WAVE INCORPORATED.

- Subversion® is a trademark of the Apache Software Foundation.

- Windows® is a registered trademark of Microsoft Corporation.

1.4   Symbols

⚠ **DANGER**

Personal Injury!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will
result in death or serious injury.

⚠ **DANGER**

Personal Injury Caused by Electric Current!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will
result in death or serious injury.

⚠ **WARNING**

Personal Injury!
Indicates a moderate-risk, potentially hazardous situation which, if not avoided,
could result in death or serious injury.

⚠ **CAUTION**

Personal Injury!
Indicates a low-risk, potentially hazardous situation which, if not avoided, may
result in minor or moderate injury.

NOTICE

Damage to Property!
Indicates a potentially hazardous situation which, if not avoided, may result in
damage to property.

NOTICE

Damage to Property Caused by Electrostatic Discharge (ESD)!
Indicates a potentially hazardous situation which, if not avoided, may result in
damage to property.

Note

Important Note!
Indicates a potential malfunction which, if not avoided, however, will not result in
damage to property.

Information

Additional Information:
Refers to additional information which is not an integral part of this
documentation (e.g., the Internet).

1.5   Number Notation

Table 1: Number Notation

Number Code	Example	Note
Decimal	100	Normal notation
Hexadecimal	0x64	C notation
Binary	'100' '0110.0100'	In quotation marks, nibble separated with dots (.)

1.6   Font Conventions

Table 2: Font Conventions

Font Type	Indicates
italic	Names of paths and data files are marked in italic-type. e.g.: *C:\Program Files\WAGO Software*
Menu	Menu items are marked in bold letters. e.g.: **Save**
>	A greater-than sign between two names means the selection of a menu item from a menu. e.g.: **File** > **New**
Input	Designation of input or optional fields are marked in bold letters, e.g.: **Start of measurement range**
"Value"	Input or selective values are marked in inverted commas. e.g.: Enter the value "4 mA" under **Start of measurement range**.
[Button]	Pushbuttons in dialog boxes are marked with bold letters in square brackets. e.g.: **[Input]**
[Key]	Keys are marked with bold letters in square brackets. e.g.: **[F5]**

2   Important Notes

This section includes an overall summary of the most important safety requirements and notes that are mentioned in each individual section. To protect your health and prevent damage to devices as well, it is imperative to read and carefully follow the safety guidelines.

2.1   Legal Bases

2.1.1   Subject to Changes

WAGO GmbH & Co. KG reserves the right to provide for any alterations or modifications. WAGO GmbH & Co. KG owns all rights arising from the granting of patents or from the legal protection of utility patents. Third-party products are always mentioned without any reference to patent rights. Thus, the existence of such rights cannot be excluded.

2.1.2   Personnel Qualifications

All sequences implemented on WAGO I/O System 750 devices may only be carried out by electrical specialists with sufficient knowledge in automation. The specialists must be familiar with the current norms and guidelines for the devices and automated environments.

All changes to the coupler or controller should always be carried out by qualified personnel with sufficient skills in PLC programming.

2.1.3   Use of the 750 Series in Compliance with Underlying Provisions

Fieldbus couplers, controllers and I/O modules of the modular WAGO I/O System 750 receive digital and analog signals from sensors and transmit them to actuators or higher-level control systems. Using controllers, the signals can also be (pre-) processed.

This product fulfills the requirements of protection type IP20 and is designed for use in dry interior spaces. There is protection against finger injury and solid impurities up to 12.5 mm diameter is assured; protection against water damage is not ensured.
The product represents an open-type device. It may only be installed in enclosures (tool-secured enclosures or operating rooms) which fulfil the listed requirements specified in the safety instructions in chapter "Safety Advice (Precautions)". Use without additional protective measures in environments within which dust, corrosive fumes, gases or ionized radiation can occur is considered improper use.

The product is intended for installation in automation systems. It does not have its own integrated separator. A suitable separator must therefore be created on the plant side.

The operation of the product in residential areas without further measures is only permitted if the product complies with the emission limits (interference emissions) according to EN 61000-6-3.

Operating the product in home applications without further measures is only permitted if it meets the emission limits (emissions of interference) according to EN 61000-6-3. Please observe the installation regulations!
You will find the relevant information in the section "Device Description" > "Standards and Guidelines" in the manual for the used product.

Appropriate housing (per 2014/34/EU) is required when operating the WAGO I/O System 750 in hazardous environments. Please note that a prototype test certificate must be obtained that confirms the correct installation of the system in a housing or switch cabinet.

The implementation of safety functions such as EMERGENCY STOP or safety door monitoring must only be performed by the F I/O modules within the modular WAGO I/O System 750. Only these safe F I/O modules ensure functional safety in accordance with the latest international standards. WAGO's interference-free output modules can be controlled by the safety function.

2.1.3.1 Improper Use

Improper use of the product is not permitted. Specifically, improper use occurs in the following cases:

- Non-observance of the intended use.

- Use without protective measures in an environment in which moisture, salt water, salt spray mist, dust, corrosive fumes, gases, direct sunlight or ionizing radiation can occur.

- Use of the product in areas with special risk that require flawless continuous operation and in which failure or operation of the product can result in an imminent risk to life, limb or health or cause serious damage to property or the environment (such as the operation of nuclear power plants, weapon systems , aircraft and motor vehicles).

2.1.3.2 Warranty and Liability

The terms set forth in the General Business & Contractual Conditions apply to deliveries and services of WAGO GmbH & Co. KG, and the WAGO Software License Contract applies to software products and products with integrated software. Both are available at www.wago.com. In particular, the warranty is void if:

- The product is improperly used.

- The deficiency (hardware and software configurations) is due to special instructions.

- Modifications to the hardware or software have been made by the user or third parties that are not described in this documentation and that has contributed to the fault.

Individual agreements always have priority.

2.1.3.3   Obligations of Installers/Operators

The installers and operators bear responsibility for the safety of an installation or a system assembled with the products. The installer/operator is responsible for proper installation and safety of the system. All laws, standards, guidelines, local regulations and accepted technology standards and practices applicable at the time of installation, and the instructions in the the products' Instructions for Use, must be complied with. In addition, the Installation regulations specified by Approvals must be observed. In the event of non-compliance, the products may not be operated within the scope of the approval.

2.2   Safety Advice (Precautions)

For installing and operating purposes of the relevant device to your system the following safety precautions shall be observed:

⚠ **DANGER**

Do not work on devices while energized!
All power sources to the device shall be switched off prior to performing any installation, repair or maintenance work.

⚠ **DANGER**

Install device in a suitable enclosure!
The device is an open system. Install the device in a suitable enclosure. This enclosure must:

- Guarantee that the max. permissible degree of pollution is not exceeded.
- Offer adequate protection against contact.
- Prevent fire from spreading outside of the enclosure.
- Offer adequate protection against UV irradiation.
- Guarantee mechanical stability
- Restrict access to authorized personnel and may only be opened with tools

⚠ **DANGER**

Ensure disconnect and overcurrent protection!
The device is intended for installation in automation technology systems. Disconnect protection is not integrated. Connected systems must be protected by a fuse.
Provide suitable disconnect and overcurrent protection on the system side!

⚠ **DANGER**

Ensure a standard connection!
To minimize any hazardous situations resulting in personal injury or to avoid failures in your system, the data and power supply lines shall be installed according to standards, with careful attention given to ensuring the correct terminal assignment. Always adhere to the EMC directives applicable to your application.

⚠ WARNING

Power from SELV/PELV power supply only!
All field signals and field supplies connected to the controller „PFC200; G2; 2ETH RS CAN" (750-8214) must be powered from SELV/PELV power supply(s)!

⚠ CAUTION

Inadequate wire cross sections can cause temperature increases!
To avoid increasing thermal risks, only use conductor cross-sections sufficient for the required maximum load current. The conductor cross-sections specified in the technical data refer exclusively to the mechanical connection capacity of the clamping points.

NOTICE

System supply only with appropriate fuse protection!
Without overcurrent protection, the electronics can be damaged.
For 24 V system supply input voltage an external fuse, rated max. 2 A, slow acting, min. 30 VDC shall be used.

NOTICE

Field supply only with appropriate fuse protection!
Without overcurrent protection, the electronics can be damaged.
For 24V field supply input voltage an external fuse, rated max. 10 A, slow acting, min. 30 VDC shall be used.

NOTICE

Do not exceed maximum values via power contacts!
The maximum current that can flow through the power jumper contacts is 10 A. The power jumper contacts can be damaged and the permissible operating temperature can be exceeded by higher current values.

When configuring the system, do not exceed the permissible maximum current value. If there is a higher power requirement, you must use an additional supply module to provide the field voltage.

NOTICE

Do not exceed the maximum total current for I/O modules (5 VDC) via data contacts!
The maximum permissible total current for internal system supply of the I/O modules may not be exceeded. The permissible total current is specified in the technical data of the head station and power supply. The data contacts for internal system supply can be damaged and the permissible operating temperature can be exceeded by higher values.
When configuring the system, do not exceed the permissible total current. If there is a higher power requirement, you must use an additional supply to provide the system voltage (5 VDC)!

NOTICE

Ensure proper contact with the DIN-rail!
Proper electrical contact between the DIN-rail and device is necessary to maintain the EMC characteristics and function of the device.

NOTICE

Replace defective or damaged devices!
Replace defective or damaged device/module (e.g., in the event of deformed contacts).

NOTICE

Protect the components against materials having seeping and insulating properties!
The components are not resistant to materials having seeping and insulating properties such as: aerosols, silicones and triglycerides (found in some hand creams). If you cannot exclude that such materials will appear in the component environment, then install the components in an enclosure being resistant to the above-mentioned materials. Clean tools and materials are imperative for handling devices/modules.

NOTICE

Clean only with permitted materials!
Clean housing and soiled contacts with propanol.

NOTICE

Do not use any contact spray!
Do not use any contact spray. The spray may impair contact area functionality in connection with contamination.

NOTICE

Do not reverse the polarity of connection lines!
Avoid reverse polarity of data and power supply lines, as this may damage the devices involved.

NOTICE

Avoid electrostatic discharge!
The devices are equipped with electronic components that may be destroyed by electrostatic discharge when touched. Please observe the safety precautions against electrostatic discharge per DIN EN 61340-5-1/-3. When handling the devices, please ensure that environmental factors (personnel, work space and packaging) are properly grounded.

NOTICE

Do not use in telecommunication circuits!
Only use devices equipped with ETHERNET or RJ-45 connectors in LANs. Never connect these devices with telecommunication networks.

2.3   Licensing Terms of the Software Package Used

The firmware for the "PFC200; G2; 2ETH RS CAN" controller (750-8214) contains open-source software.

The licence conditions of the software packages are stored in the controller in text form. They can be accessed via the WBM page "Legal Information" > "Open Source Software."
You can obtain the source code with licensing terms of the open-source software from WAGO GmbH & Co. KG on request. Send your request to support@wago.com with the subject "Controller Board Support Package."

2.4   Special Use Conditions for ETHERNET Devices

If not otherwise specified, ETHERNET devices are intended for use on local networks. Please note the following when using ETHERNET devices in your system:

•   Do not connect control components and control networks directly to an open network such as the Internet or an office network. WAGO recommends putting control components and control networks behind a firewall.

•   In the control components (e.g., for WAGO I/-CHECK and CODESYS) close all ports and services not required by your application to minimize the risk of cyber attacks and to enhance cyber security.
Only open ports and services during commissioning and/or configuration.

•   Limit physical and electronic access to all automation components to authorized personnel only.

•   Change the default passwords before first use! This will reduce the risk of unauthorized access to your system.

•   Regularly change the passwords used! This will reduce the risk of unauthorized access to your system.

•   If remote access to control components and control networks is required, use a Virtual Private Network (VPN).

•   Regularly perform threat analyses. You can check whether the measures taken meet your security requirements.

•   Use "defense-in-depth" mechanisms in your system's security configuration to restrict the access to and control of individual products and networks.

•   Please note the risks of using cloud services!
If you use third-party cloud services, sensitive data is transferred to the cloud service provider at one's own responsibility. External access may result in manipulated data and/or unwanted control commands affecting the

performance of your control system.

Use encryption methods to protect your data and observe the information provided by the Federal Office for Information Security – "Cloud: Risks and Security Tips".

Observe comparable publications of the competent, public institutions of your country.

3   Overview

The controller 750-8214(PFC200; G2; 2ETH RS CAN) is an automation device
that can perform control tasks of a PLC. It is suitable for mounting on a DIN rail
and stands out on account of its various interfaces.

This controller can be used for applications in mechanical and systems
engineering, in the processing industry and in building technology.

You can connect all available I/O modules of the WAGO-I/O-SYSTEM 750 (750
and 753 Series) to the controller, enabling it to internally process analog and
digital signals from the automation environment, or to supply these signals to
other devices via one of the available interfaces.

Automation tasks can be executed in all IEC 61131-3-compatible languages with
the CODESYS V3 programming system.
The implementation of the task processing in the runtime system for Linux® has
been optimized with real-time extensions in order to provide maximum
performance for automation tasks. Web visualization is also provided as
visualization in addition to the development environment.

For IEC-61131-3 programming in CODESYS applications, the controller provides
32 MB of program memory (flash), 128 MB of data memory (RAM) as well as
128 kB of retentive memory (retain and flag variables in an integrated NVRAM).

The controller has a slot for an SD card. The SD card can be used to transfer
device parameters, boot projects and other files from one controller to another.
The SD card can be accessed via FTP as an additional drive.

> **Note**
>
> **Memory card is not included in the scope of delivery!**
> Note, the controller is delivered without memory card.
> To use a memory card, you must order one separately. The controller can also
> be operated without memory card expansion, the use of a memory card is
> optional.

> **Note**
>
> **Only use recommended memory cards!**
> Use only the SD memory cards available from WAGO (item No. 758-879/000-
> 001 and 758-879/000-2108) as these are suitable for industrial applications
> subjected to environmental extremes and for use in this device.
> Compatibility with other commercially available storage media cannot be
> guaranteed.

Two ETHERNET interfaces and the integrated, configurable switch enable wiring
in all necessary configurations with one common network where both ports share

a common IP address or with two separate networks where each port has its own IP address.

The physical interfaces (ports) are assigned via logical bridges and can be e.g., configured via the WBM.

Both of these interfaces support:

•   10BASE-T / 100BASE-TX

•   Full/Half duplex

•   Autonegotiation

•   Auto-MDI(X) (automatic uplink and crossover switching)

The following fieldbus circuits are implemented for exchange of process data:

•   CANopen Master/Slave

In the controller, all input signals from the sensors are combined. After connecting the controller, all of the I/O modules on the bus node are detected and a local process image is created from these. Analog and specialty module data is sent via words and/or bytes; digital data is sent bit by bit.

Note

No direct access from fieldbus to the process image for I/O modules!
Any data that is required from the I/O module process image must be explicitly mapped in the CODESYS program to the data in the fieldbus process image and vice versa! Direct access is not possible!

CODESYS V3 makes configuring the fieldbus possible.

A Web-based management system (WBM) is also available as a configuration aid. This system includes various dynamic HTML pages from which, among other things, information about configuration and the status of the controller can be called up. The WBM is already stored in the device and is presented and operated using a web browser. You can also save your own HTML pages in the implemented file system, or call up programs directly.

In the controller's initial state, the installed firmware is based on Linux[®], with special real-time extensions of the RT-Preempt patch. In addition, the following application programs are also installed on the controller, along with a number of different auxiliary programs:

•   a SNMP server/client

•   a FTP server, a FTPS server (explicit connections only)

•   a SSH server/client

- •   a Web server

- •   a NTP client

- •   a BootP and DHCP client

- •   a DHCP server

- •   a DNS server

- •   a CODESYS V3 Runtime Environment

Based on IEC-61131-3 programming, data processing takes place on site in the controller. The logical process results can be output directly to the actuators or transmitted via a connected fieldbus to the higher level controller.

4   Properties

4.1   Hardware Description

4.1.1   View
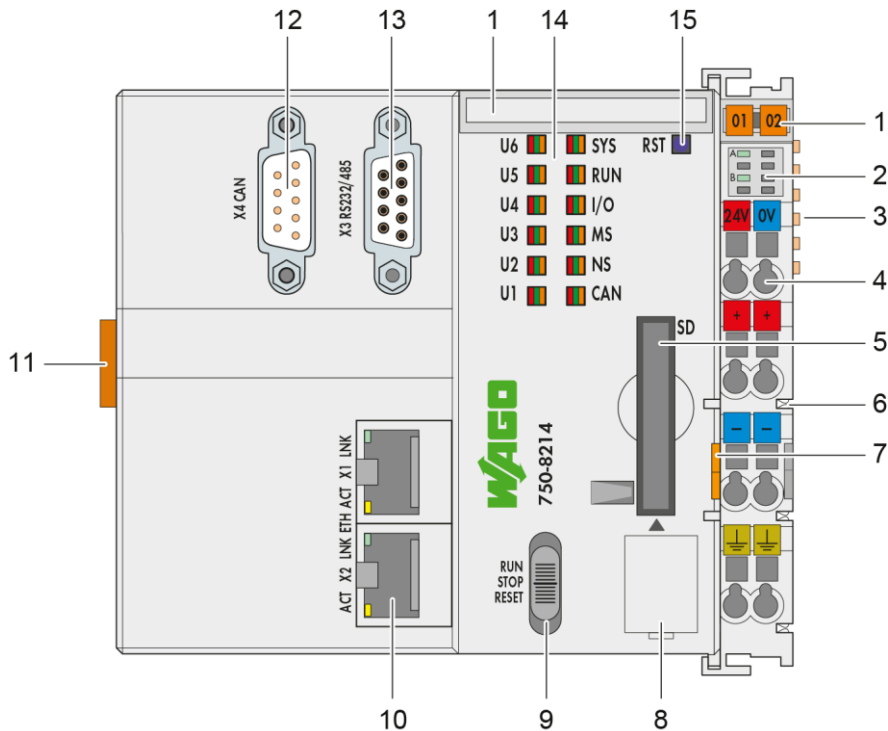
Figure 1: View

Table 3: Legend for Figure "View"

Item	Description	See section
1	Marking options (Mini WSB)	---
2	LED indicators – power pupply	"Display Elements" > "Power Supply Indicating Elements"
3	Data contacts	"Connectors" > "Data Contacts/Local Bus"
4	CAGE CLAMP® connectors for power supply	"Connectors" > "CAGE CLAMP® connectors"
5	Slot for memory card	"Slot for Memory Card"
6	Power contacts for power supply of down-circuit I/O modules	"Connectors" > "Power Jumper Contacts/Field Supply"
7	Releasing strap	"Mounting" > "Inserting Devices" "Removal" > "Removing Devices"

8	Service Interface (behind the flap)	"Connectors" > "Service Interface"
9	Mode selector switch	"Operating elements" > "Operating Mode Switch"
10	ETHERNET connectors – X1, X2	"Connectors" > "Network connectors"
11	Safe locking feature	"Mounting" > "Inserting Devices" "Removal" > "Removing Devices"
12	Fieldbus connector – CANopen – X4	"Connecors" > "CANopen"
13	Communication interface – X3	"Connectors" > "Communication Interface"
14	LED indicators – system	"Display Elements" > "Fieldbus/System Indicating Elements"
15	Reset button (in hole)	"Operating Elements" > "Reset Button"

4.1.2   Labeling

The front labeling includes:
- Device designation
- Name of the display elements, connections and control elements
- Serial number with hardware and firmware version

The side labeling includes:
- Manufacturer's identification
- Connector pin assignment
- Serial number
- Approval information

4.1.2.1   Production Code

The serial number indicates the delivery status directly after production.
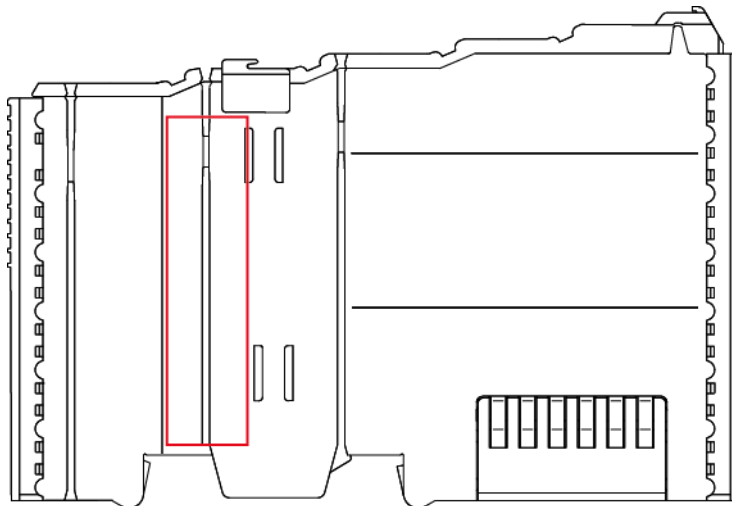
Figure 2: Marking Area for Serial Numbers

There are two serial numbers in two rows in the side marking. They are left of the release tab. The first 10 positions in the longer row of the serial numbers contain version and date identifications.

Example structure of the rows: 0114010101…

01	14	01	01	01	(additional positions)
WW	**YY**	**FW --**	**HW**	**FL**	**-**
Calendar week	Year	Firmware version	Hardware version	Firmware loader version	Internal information

The row order can vary depending on the production year, only the longer row is relevant. The back part of this and the shorter row contain internal administration information from the manufacturer.

4.1.3   Connectors

4.1.3.1   Wiring Level
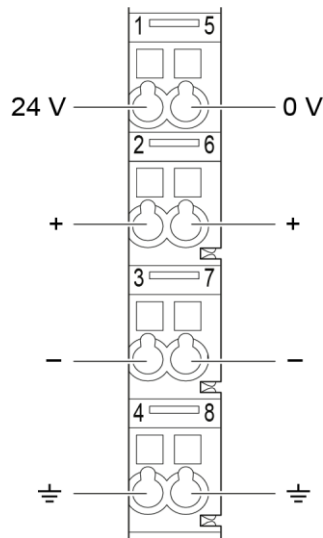
Figure 3: CAGE CLAMP® connections

Table 4: Legend for figure "CAGE CLAMP® connections"

Contact	Description	Description
1	24 V	System power supply voltage +24 V
2	+	Field-side power supply voltage U_V
3	-	Field-side power supply voltage 0 V
4	Ground	Field-side power supply voltage, ground
5	0 V	System power supply voltage 0 V
6	+	Field-side power supply voltage U_V
7	-	Field-side power supply voltage 0 V
8	Ground	Field-side power supply voltage, ground

→ **Note**

Observe supplementary power supply regulations for use in shipbuilding!
Observe supplementary power supply regulations for shipbuilding and the supply
voltage in Section "Connect Devices" > … > "Supplementary Power Supply
Regulations"!

4.1.3.2   Service Interface

The service interface is located behind the flap.

The Service interface is used for communication with WAGO-I/O-*CHECK* and "WAGO Ethernet Settings".
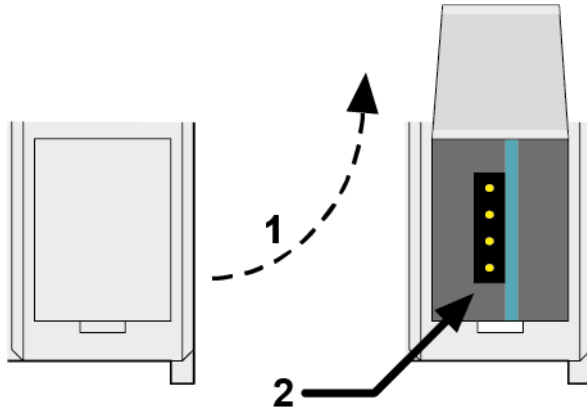
Figure 4: Service Interface (Closed and Open Flap)

Table 5: Service Interface

Number	Description
1	Open flap
2	Service interface

NOTICE

Device must be de-energized!
To prevent damage to the device, unplug and plug in the communication cable only when the device is de-energized!

The connection to the 4-pin header under the cover flap can be realized via the communication cables with the item numbers750-920 and 750-923 or via the WAGO radio adapter with the item number 750-921.

4.1.3.3 Network Connectors
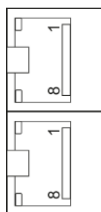
Figure 5: Network Connections – X1, X2

Table 6: Legend for Figure "Network Connections – X1, X2"

Contact	Signal	Description
1	TD +	Transmit Data +
2	TD −	Transmit Data −
3	RD +	Receive Data +
4	NC	Not assigned
5	NC	Not assigned
6	RD −	Receive Data −
7	NC	Not assigned
8	NC	Not assigned

4.1.3.4   CANopen
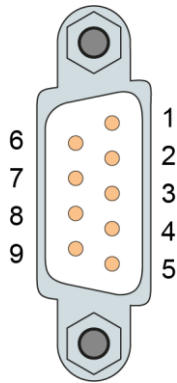
Figure 6: CANopen – X4 Fieldbus Connection

Table 7: Legend for Figure "CANopen – X4 Fieldbus Connection"

Contact	Signal	Description
1	-	Not used
2	CAN_L	CAN Signal Low
3	GND	Ground
4	-	Not used
5	Drain Shield	Shield termination
6	-	Not used
7	CAN_H	CAN Signal High
8	-	Not used
9	CAN_V+	Not used

DC/DC converters and optocouplers in the fieldbus interface provide electrical isolation between the CANopen bus system and the electronics.

The cable shield must be applied to the CAN shield. This is terminated to ground in devices with 1 MΩ (DIN rail contact). A low-impedance connection of the shielding to ground is possible only from the outside (e.g., by a supply module). We recommend using central ground contacts for the entire CANopen bus line shielding.

To minimize reflection at the end of the line, the CANopen line must be terminated at both ends by a cable termination.

Note

Attention - bus termination!

The CANopen bus segment must be terminated at both ends!
No more than 2 terminations per bus segment may be used!
Terminations may not be used in stub and branch lines!
Operation without proper termination of the CANopen network may result in transmission errors.

> **Note**
>
> **Observe permissible resistor power loss!**
> For normal operation, 1/4 Watt resistors are sufficient. In the event of a short circuit (24 V power supply to a bus line), the resistor is subjected to a power loss of (short-circuit output current from transceiver * power supply voltage). The resistor must be designed to withstand this power loss level.
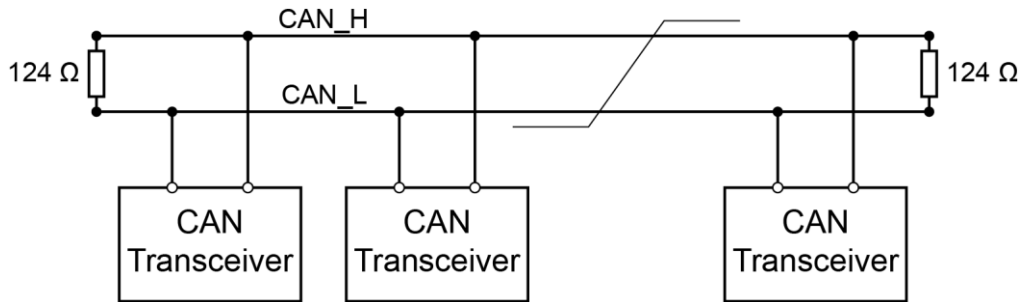
Figure 7: CANopen Standard Bus Termination

4.1.3.5   Communication Interface
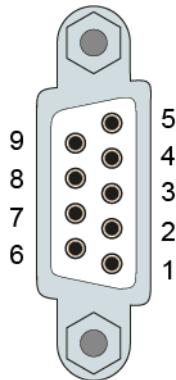
Figure 8: RS-232/RS-485 – Communication Interface – X3

Table 8: Legend for Figure "RS-232/RS-485 – Communication Interface – X3"

Contact	RS-232 (DCE)		RS-485	
	Signal	Description	Signal	Description
1	NC	Not assigned	NC	Not assigned
2	RxD (out)	Receive Data	NC	Not assigned
3	TxD (in)	Transmit Data	A (Tx/Rx+)	Transmit/receive data +
4	NC	Not assigned	NC	Not assigned
5	FB_GND	Ground	FB_GND	Ground
6	NC	Not assigned	FB_5V	Power Supply
7	RTS (in)	Request to Send	NC	Not assigned
8	CTS (out)	Clear to Send	B (Tx/Rx−)	Transmit/receive data −
9	NC	Not assigned	NC	Not assigned
Enclosure	Shield	Shielding	Shield	Shielding

If the communication interface is opened as an RS-232 interface, the controller represents data communication equipment (DCE). The RxD and CTS signals are sent to the communication partner (out), and the TxD and RTS signals are received by the communication partner (in).

NOTICE

Incorrect parameterization can damage the communication partners!
The voltage levels are −12 V and +12 V for RS-232, and −5 V and +5 V for RS-485.
If the controller interfaces differ from those of the communication partners (RS-232 <> RS-485 or RS-485 <> RS-232), this may damage the interface of the communication partner.
Therefore, always ensure that the controller interface matches those of its communication partners when configuring these items!

DC/DC converters and optocouplers in the fieldbus interface electrically isolate the fieldbus system and the electronics.

4.1.3.5.1 Operating as an RS-232 Interface

Depending on the device type DTE (Data Terminal Equipment, e.g., PC) or DCE (Data Communication Equipment, e.g., PFC, modem), the RS-232 signals have different data directions.

Table 9: Function of RS-232 Signals for DTE/DCE

Contact	Signal	Data Direction	
		DTE	DCE
2	RxD	Input	Output
3	TxD	Output	Input
5	FB_GND	---	---
7	RTS	Output	Input
8	CTS	Input	Output

For a DTE-to-DCE connection, the signals are connected directly (1:1).
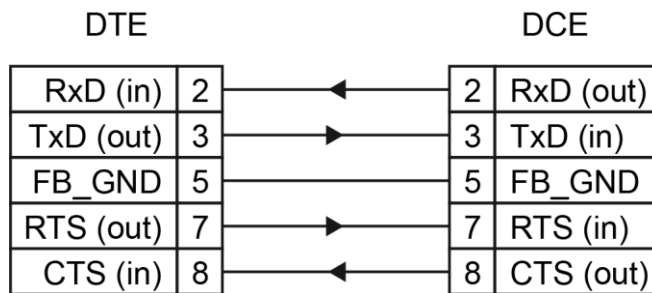
Figure 9: Termination with DTE-DCE Connection (1:1)

For a DCE-to-DCE connection, the signal connections are crossed (cross-over).
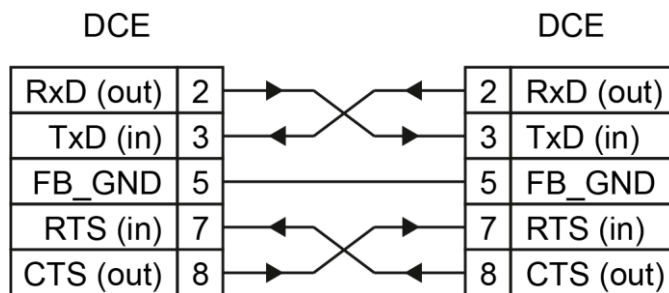
Figure 10: Termination with DCE-DCE Connection (Cross-Over)

4.1.3.5.2 Operating as an RS-485 Interface

To minimize reflection at the end of the line, the RS-485 line must be terminated at both ends by a cable termination. If required, one pull-up or pull-down resistor may be used. These resistors ensure a defined level on the bus when no subscriber is active, i.e., when all subscribers are in "Tri-state".

> **Note**
>
> **Attention — bus termination!**
> The RS-485 bus must be terminated at both ends!
> No more than two terminations per bus segment may be used!
> Terminations may not be used in stub and branch lines!
> Drop cables must be kept as short as possible!
> Operation without proper termination of the RS-485 network may result in transmission errors.
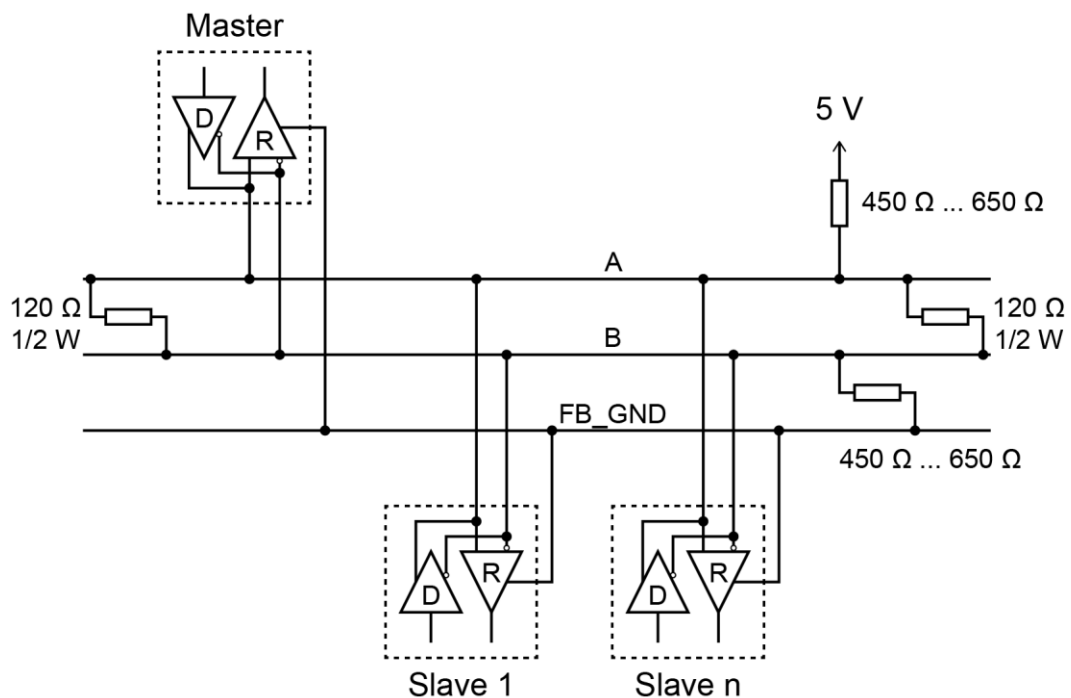
Figure 11: RS-485 Bus Termination

> **Note**
>
> **Transmission error with ineligible RS-485 configuration!**
> For baud rates lower than 115200 baud, configure the RS-485 interface with two stop bits and enabled parity (even or odd) to avoid transmission errors.

4.1.4   System Contacts

4.1.4.1   Data Contacts

Communication between the controller and the I/O modules and system power
supply for the I/O modules is provided via the local bus, which consists of 6 data
contacts designed as self-cleaning gold spring contacts.
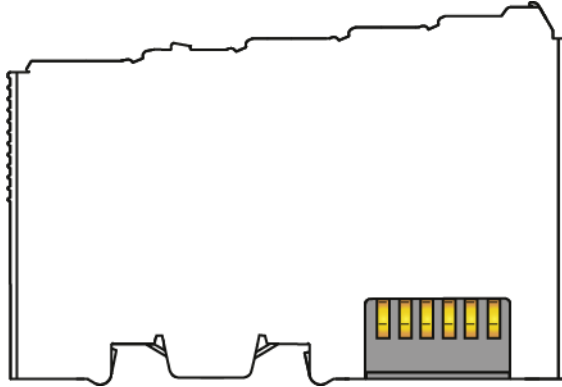
Figure 12: Data Contacts

NOTICE

Do not place the I/O modules on the gold spring contacts!
Do not place the I/O modules on the gold spring contacts in order to avoid soiling
or scratching!

NOTICE

Pay attention to potential equalization from the environment!
The devices are equipped with electronic components that may be destroyed by
electrostatic discharge. When handling the devices, please ensure that
environmental factors (personnel, work space and packaging) are properly
equalized. Do not touch any conducting parts, e.g., data contacts.

NOTICE

**Do not exceed the maximum total current for I/O modules (5 VDC) via data
contacts!**
The maximum permissible total current for internal system supply of the I/O
modules may not be exceeded. The permissible total current is specified in the
technical data of the head station and power supply. The data contacts for
internal system supply can be damaged and the permissible operating
temperature can be exceeded by higher values.
When configuring the system, do not exceed the permissible total current. If there
is a higher power requirement, you must use an additional supply to provide the
system voltage (5 VDC)!

4.1.4.2   Power Jumper Contacts

The controller 750-8214is equipped with 3 self-cleaning power contacts for transferring of the field-side power supply to down-circuit I/O modules. These contacts are designed as spring contacts.
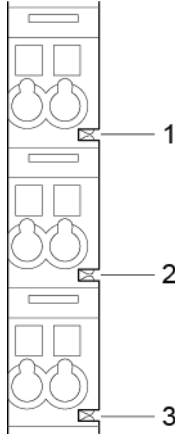
Figure 13: Power Jumper Contacts

Table 10: Legend for Figure "Power Jumper Contacts"

Contact	Type	Function
1	Spring contact	Potential transmission (U_V) for field supply
2	Spring contact	Potential transmission (0 V) for field supply
3	Spring contact	Potential transmission (ground) for field supply

⚠ **CAUTION**

Risk of injury due to sharp-edged blade contacts!
The blade contacts are sharp-edged. Handle the I/O module carefully to prevent injury. Do not touch the blade contacts.

NOTICE

Do not exceed maximum values via power contacts!
The maximum current that can flow through the power jumper contacts is 10 A. The power jumper contacts can be damaged and the permissible operating temperature can be exceeded by higher current values.

When configuring the system, do not exceed the permissible maximum current value. If there is a higher power requirement, you must use an additional supply module to provide the field voltage.

4.1.5   Display Elements

4.1.5.1   Power Supply LEDs
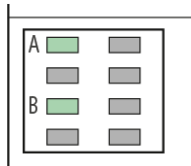
Figure 14: Power Supply Indicating Elements

Table 11: Legend for Figure "Power Supply Indicating Elements"

Designation	Color	Description
A	Green/off	Status of system power supply voltage
B	Green/off	Status of field-side power supply voltage

4.1.5.2   System/Fieldbus LEDs

Figure 15: Indicating elements for fieldbus/system

Table 12: Legend for Figure "Fieldbus/System Indicating Elements"

Designation	Color	Description
SYS	Red/Green/ Orange/Off	System status
RUN	Red/Green/ Orange/Off	PLC program status
I/O	Red/Green/ Orange/Off	Local bus status
MS	Red/Green/ Orange/Off	Module status
NS	Red/Green/ Orange/Off	Without function
CAN	Red/Green/ Orange/Off	CANopen status
U6	Red/Green/ Orange/Off	User LED 6, programmable using function blocks from the WAGO libraries to control the LEDs
U5	Red/Green/ Orange/Off	User LED 5, programmable using function blocks from the WAGO libraries to control the LEDs
U4	Red/Green/ Orange/Off	User LED 4, programmable using function blocks from the WAGO libraries to control the LEDs
U3	Red/Green/ Orange/Off	User LED 3, programmable using function blocks from the WAGO libraries to control the LEDs
U2	Red/Green/ Orange/Off	User LED 2, programmable using function blocks from the WAGO libraries to control the LEDs
U1	Red/Green/ Orange/Off	User LED 1, programmable using function blocks from the WAGO libraries to control the LEDs

4.1.5.3   Network Connector LEDs
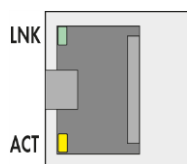
Figure 16: Indicating Elements, RJ-45 Jacks

Table 13: Legend for Figure "Indicating Elements, RJ-45 Jacks"

Designation	Color	Description
LNK	Green/Off	ETHERNET connection status
ACT	Yellow/Off	ETHERNET data exchange

4.1.5.4   Memory Card Slot LED
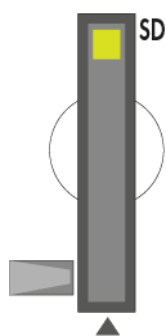
Figure 17: Indicating Elements, Memory Card Slot

Table 14: Legend for Figure "Indicating Elements, Memory Card Slot"

Designation	Color	Description
SD	Yellow/Off	Memory card status

4.1.6   Operating Elements

4.1.6.1   Operating Mode Switch

Figure 18: Mode Selector Switch

Table 15: Mode Selector Switch

Position	Actuation	Function
RUN	Latching	**Normal operation** CODESYS V3 applications running.
STOP	Latching	**Stop** All CODESYS V3 applications have stopped.
RESET	Spring-return	**Reset warm start** or **Reset cold start** (depending on length of actuation, see Section "Starting" > "Initiating Reset Functions")

Other functions can also be initiated using the reset button.

4.1.6.2   Reset Button
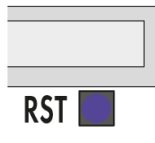
Figure 19: Reset Button

The Reset button is installed behind drilling to prevent operating errors. It is a shortstroke button with a low actuating force of 1.1 N … 2.1 N (110 gf … 210 gf). The button can be actuated using a suitable object (e.g., pen).

You can initiate different functions using the Reset button depending on the position of the mode selector:

*   Temporarily set a fixed IP address ("Fixed IP Address" mode, see section "Commissioning" > "Setting an IP Address" > "Temporarily Setting a Fixed IP Address")

*   Perform a software reset (restart, see section "Commissioning" > "Initiating Reset Functions" > "Software Reset")

*   Restore factory setting (factory reset, see section "Service" > "Firmware Changes" > "Factory Reset")

4.1.7   Memory Card Slot
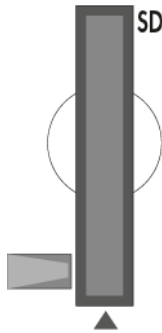
Figure 20: Slot for SD Memory Card

The slot for the SD memory card is located on the front of the housing. The memory card is locked in the enclosure by a push/push mechanism. Inserting and removing the memory card is described in the Section "Service" > "Inserting and Removing the Memory Card."
The memory card is protected by a cover flap. The cover cap is sealable.

> **Note**
>
> **Memory card is not included in the scope of delivery!**
> Note, the controller is delivered without memory card.
> To use a memory card, you must order one separately. The controller can also be operated without memory card expansion, the use of a memory card is optional.

> **Note**
>
> **Only use recommended memory cards!**
> Use only the SD memory cards available from WAGO (item No. 758-879/000-001 and 758-879/000-2108) as these are suitable for industrial applications subjected to environmental extremes and for use in this device.
> Compatibility with other commercially available storage media cannot be guaranteed.

4.2   Schematic Diagram
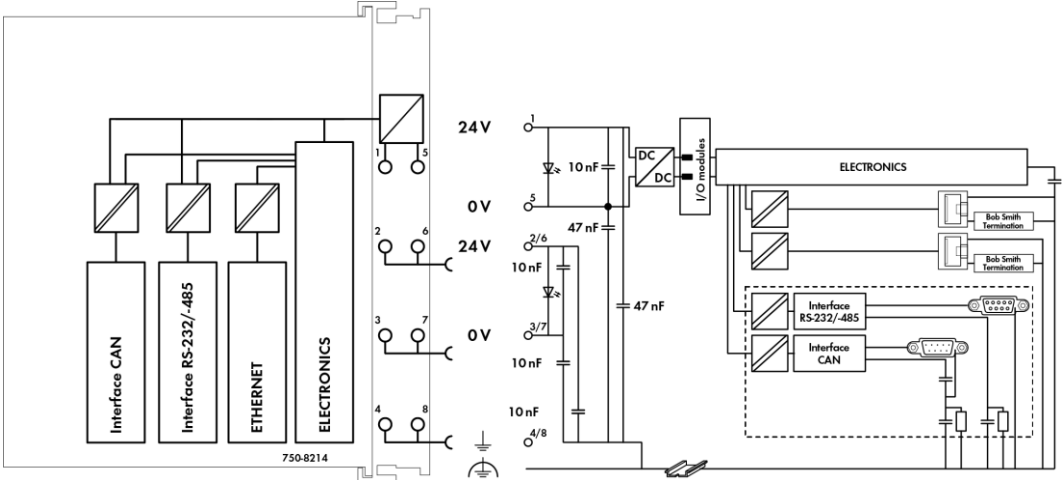
Figure 21: Schematic diagram

4.3 Technical Data

4.3.1 Mechanical Data

Table 16: Technical Data – Mechanical Data

Width	112 mm / 4.409 inch
Height	100 mm / 3.937 inch
Depth	71.9 mm / 2.831 inch
Depth from upper edge of DIN-rail	64.7 mm / 2.547 inch
Weight	256.9 g

4.3.2 System Data

Table 17: Technical Data – System Data

CPU	Cortex A8, 1 GHz
Operating System	Real-time Linux® with RT Preemption Patch
Memory card slot	Push-push mechanism, sealable cover lid
Type of memory card	SD and SDHC up to 32 Gbytes (All guaranteed properties are valid only in connection with the WAGO memory cards 758-879/000-001 and 758-879/000-2108.)

4.3.3 Power Supply

Table 18: Technical Data – Power Supply

Power supply	24 VDC (-25 % … +30 %)
Max. input current (24 V)	550 mA
Power failure time acc. IEC 61131-2	Depending on external buffering
Total current for I/O modules (5V)	1700 mA
Isolation	500 V system/supply

![→] **Note**

Buffer for system power supply!
The system power supply and, if necessary, the field supply must be buffered to bridge power outages.
As the power demand depends on the respective node configuration, buffering is not implemented internally.
To achieve power outages of 1 ms to 10 ms according to IEC61131-2, determine the buffering appropriate for your node configuration and structure it as an external circuit.

4.3.4   Clock

Table 19: Technical Data – Clock

Drift - system clock (25 °C)	20 ppm
Drift - RTC (25 °C)	3 ppm
Buffer time RTC (25 °C)	30 days

4.3.5   Programming

Table 20: Technical Data – Programming

Programming	CODESYS V3
IEC 61131-3	LD, FBD (CFC), ST, FC
Program memory (Flash)	32 Mbytes
Data memory (RAM)	128 Mbytes
Non-volatile memory (NVRAM)	128 Kbytes

4.3.6   Local Bus

Table 21: Technical Data – Local Bus

Number of I/O modules (per node)	64
with bus extension	250
Input and output process image (max.)	Not specified

4.3.7 ETHERNET

Table 22: Technical Data – ETHERNET

ETHERNET	2 x RJ-45 (switched or separated mode)
Transmission medium	Twisted Pair S-UTP, 100 Ω, Cat 5, 100 m maximum cable length
Baud rate	10/100 Mbit/s; 10Base-T/100Base-TX
Protocols	DHCP, DNS, SNTP, FTP, FTPS (only explicit connections), SNMP, HTTP, HTTPS, SSH

> **Note**
>
> **No direct access from fieldbus to the process image for I/O modules!**
> Any data that is required from the I/O module process image must be explicitly mapped in the CODESYS program to the data in the fieldbus process image and vice versa! Direct access is not possible!

4.3.8 CANopen

Table 23: Technical Data – CANopen

CANopen input and output process image max.	2000 words

> **Note**
>
> **No direct access from fieldbus to the process image for I/O modules!**
> Any data that is required from the I/O module process image must be explicitly mapped in the CODESYS program to the data in the fieldbus process image and vice versa! Direct access is not possible!

4.3.9 Communication Interface

Table 24: Technical Data – Communication Interface

Interface	1 x serial interface per TIA/EIA 232 and TIA/EIA 485 (switchable), 9-pole D-sub female connector
Protocols	WAGO Service Communication, Linux console as well as application-specific protocols (Modbus RTU, etc.)

4.3.10   Connection Type

Table 25: Technical Data – Field Wiring

Connection technology	CAGE CLAMP®
Conductor cross-section	0.08 mm² … 2.5 mm², AWG 28 … 14
Strip length	8 mm … 9 mm / 0.33 in

Table 26: Technical Data – Power Jumper Contacts

Power jumper contacts	Spring contact, self-cleaning

Table 27: Technical Data – Data Contacts

Data contacts	Slide contact, hard gold plated, self-cleaning

4.3.11   Climatic Environmental Conditions

Table 28: Technical Data – Climatic Environmental Conditions

Surrounding air temperature, operation	0 … 55 °C
Surrounding air temperature, storage	−25 … +85 °C
Relative humidity without condensation	5 … 95 % without condensation
Operating altitude above sea level without temperature derating with temperature derating max.	0 … 2000 m 2000 … 5000 m: 0,5 K per 100 m 5000 m
Pollution degree	2
Overvoltage category	II
Protection type	IP20
Resistance to harmful substances	Acc. to IEC 60068-2-42 and IEC 60068-2-43
Maximum pollutant concentration at relative humidity < 75 %	$SO_2 \leq 25$ ppm $H_2S \leq 10$ ppm
Special conditions	• Ensure that additional measures for components are taken, which are used in an environment involving: – dust, caustic vapors or gases – ionizing radiation • The permissible temperature range of the connecting cable must be dimensioned based on the mounting position and current intensity, as the temperature of the terminal connection can be up to 25 °K above the maximum expected surrounding air temperature (at 10 A).

4.4   Approvals

For current approvals, please go to: www.wago.com/<Item number>.

The following approvals have been granted to the "PFC200; G2; 2ETH RS CAN" controller (750-8214):

C E	Conformity Marking	
c(UL)us	Ordinary Locations	UL61010-2-201
KC	Korea Certification	MSIP-REM-W43-PFC750

The following Ex approvals have been granted to the "PFC200; G2; 2ETH RS CAN" controller (750-8214):

c(UL)us	Hazardous Locations	UL 121201 for Use in Hazardous Locations Cl I Div 2
⟨Ex⟩	TÜV 14 ATEX 148929 X	
	II 3 G Ex ec IIC T4 Gc	
IECEx	IECEx TUN 14.0035 X	
	Ex ec IIC T4 Gc	
(CCC) Ex nA IIC T4 Gc	2020312310000213	
	Ex nA IIC T4 Gc	
EAC Ex	EAC RU C-DE.AM02.B.00163/19	
	2Ex e IIC T4 Gc X	

The following ship approvals have been granted to the "PFC200; G2; 2ETH RS CAN" controller (750-8214):

ABS (American Bureau of Shipping)

BV (Bureau Veritas)

DNV GL
[Temperature: B, Humidity: B, Vibration: B, EMC: B, Enclosure: (*)]
(*)   Required protection according to the rules shall be provided upon installation on board.

LR (Lloyd's Register)   Env. 1, 2, 3, 4

PRS (Polski Rejestr Statków)

RINA (Registro Italiano Navale)

Information

For more information about the ship approvals:
Note the "Supplementary Power Supply Regulations" section for the ship approvals.

4.5   Standards and Guidelines

The "PFC200; G2; 2ETH RS CAN" controller (750-8214) fulfills the following standards and regulations:

Electrical Equipment For Measurement, Control, and Laboratory Use; Part 1: General Requirements	UL61010-1
Electrical Equipment For Measurement, Control, and Laboratory Use; Part 1: General Requirements	CAN/CSA C22.2 No. 61010-1-12

The "PFC200; G2; 2ETH RS CAN" controller (750-8214) fulfills the following safety standards:

Safety requirements for electrical equipment for measurement, control and laboratory use Part 2-201: Particular requirements for control equipment	UL61010-2-201
Safety requirements for electrical equipment for measurement, control and laboratory use Part 2-201: Particular requirements for control equipment	CAN/CSA-IEC 61010-2-201:14

The "PFC200; G2; 2ETH RS CAN" controller (750-8214) fulfills the following EMC standards:

EMC CE-Immunity to interference	EN 61000-6-2
EMC CE-Emission of interference	EN 61000-6-3

5   Function Description

5.1   Network

5.1.1   Interface Configuration

The X1 and X2 network interfaces of the controller are connected with an integrated configurable 3-port switch, in which the third port is connected to the CPU.

The two interfaces and configurable switch enable wiring for:

•   One common network where both ports share a common IP address.

•   Two separate networks where each port has its own IP address.

The physical interfaces (ports) are assigned via logical bridges and can be e.g., configured via the WBM.

Figure 22: Example of Interface Assignment via WBM

For network interfaces X1 … X<n>, fixed IP addresses can be set temporarily ("Fix IP Address" mode). The setting is carried out with the Reset button (see Section "Commissioning" > … > "Temporarily Setting Fixed IP Addresses").

Setting a fixed IP address has no effect on the mode previously set.

5.1.1.1   Operation in Switch Mode

For operation in Switch mode, the TCP/IP settings such as the IP address or subnet mask apply to both X1 and X2.

When switching to Switch mode, the X1 settings are applied as a new common configuration for X1 and X2.
The device is then no longer accessible via the IP address previously set for X2. This must be taken into account for CODESYS applications that use X2 for communication.

5.1.1.2   Operation with Separate Network Interfaces

When operating with separate network interfaces, both ETHERNET interfaces can be configured and used separately.

When switching to operating with separate interfaces, interface X2 is initialized with the setting values last valid for it. The connections on the X1 interface persist.

When operating with separate interfaces and fixed IP address, the device can still be accessed via the interface X2 via the regular IP address.

5.1.1.3   MAC ID and IP Address Assignment Examples

One common network with one common IP address for both ports
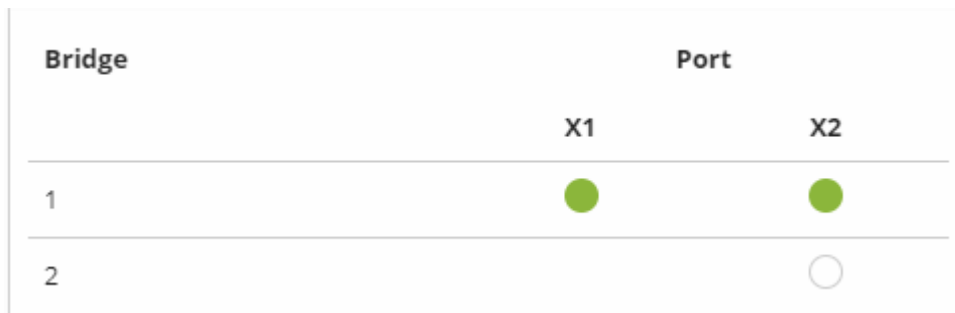
Figure 23: One Bridge with Two Ports

Table 29: MAC ID and IP Address Assignment for One Bridge with Two Ports

Bridge	MAC ID	IP Addr.	Port	MAC ID	Port	MAC ID
1	01	1	X1	02	X2	03

Two separate networks where each port has its own IP address
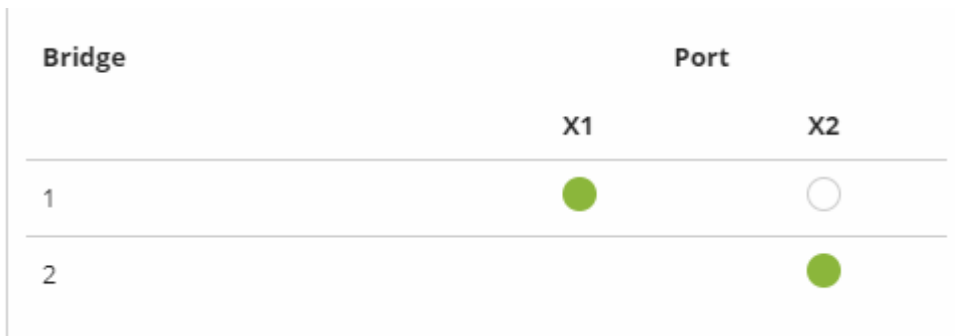
Figure 24: Two Bridges with One/One Ports

Table 30: MAC ID and IP Address Assignment for Two Bridges with One/One Ports

Bridge	MAC ID	IP Addr.	Port	MAC ID	Port	MAC ID
1	01	1	X1	01		
2	02	2			X2	02

5.1.2   Network Security

5.1.2.1   Users and Passwords

Several groups of users are provided in the controller which can be used for various services.

Default passwords are set for all users. We strongly recommend changing these passwords on startup!

→

Note

Change passwords
Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.

5.1.2.1.1   Services and Users

All password-protected services and their associated users are listed in the following table.

Table 31: Services and Users

| Service | Users | | | |
| | Linux | | | SNMP |
	root	admin	user	
Web Based Management (WBM)	X	X	X	
Linux console	X	X	X	
Console Based Management (CBM)	X			
CODESYS		X		
Telnet	X	X	X	
FTP	X	X	X	
FTPS	X	X	X	
SSH	X	X	X	
SNMP				X

5.1.2.1.2 Linux User Group

The Linux user group includes the actual users of the operating system, which is likewise used by most services.

Table 32: Linux Users

User	Special Feature	Home Directory	Default Password
root	Super user	/root	wago
admin	CODESYS user	/home/admin	wago
user	Normal user	/home/user	user

You can configure passwords for these users via a terminal connection.

→ **Note**

Change passwords
Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.

→ **Note**

Note password length!
For CODESYS, the password length must be greater than or equal to 1 character and less than 60 characters!

5.1.2.1.3 SNMP User Group

The SNMP service manages its own users. In its initial state, no users are stored in the system.

5.1.2.2   Web Protocols for WBM Access

The HTTP and HTTPS web protocols can be used to access the WBM pages for the controller. HTTPS is preferred because it uses the SSL/TLS protocol. The SSL/TLS protocol ensures secure communication through encryption and authentication

The default setting for the controller allows strong encryption, but uses only simple authentication methods. As authentication for any secure communication channel plays a central role, it is strongly recommended that you use secure authentication. The security certificate saved on the controller is the basis for authentication. The default location for the security certificate is: /etc/lighttpd/https-cert.pem

As delivered, the controller uses a generic security certificate based on x509. To allow secure authentication, you must replace the generic security certificate with a security certificate specific for the individual device.

5.1.2.2.1   TLS Encryption

When an HTTPS connection is established, the Web browser and Webserver negotiate what TLS version and what cryptographic method are to be used.

The "TLS Configuration" group of the WBM page "Security" can be used to switch the cryptographic methods allowed for HTTPS and the TLS versions that can be used.

The settings "Strong" and "Standard" are possible.
If "Strong" is set, the Webserver only allows TLS Version 1.2 and strong algorithms.
Older software and older operating systems may not support TLS 1.2 and encryption algorithms.
If "Standard" is set, TLS 1.0, TLS 1.1 and TLS 1.2 are allowed, as well as cryptographic methods that are no longer considered secure.

Information

BSI Technical Guidelines TR-02102
The rules for the "Strong" setting are based on technical guidelines TR-02102 of the German Federal Office for Information Security.
You can find the guidelines on the Internet at: https://www.bsi.bund.de > "Publications" > "Technical Guidelines."

Information

BSI Guidelines on Migration to TLS 1.2
The German Federal Office for Information Security guidelines on migration to TLS 1.2 contain "compatibility matrices" that show what software is comparable with TLS 1.2.
You can find the guidelines on the Internet at: https://www.bsi.bund.de > "Topics" > "Standards and Criteria" > "Minimum Standards".

5.1.2.3   Root Certificates

For communication encrypted with TLS, root certificates are used to verify the authenticity of the communication partner.
A root certificate, which is signed by a certificate authority, serves to verify the validity of all certificates issued by this certificate authority.

The root certificates stored on the controller (root CA bundle) form the basis for authentication of services hosted on the Internet (e.g., email providers and cloud services).

The standard storage location for the root certificates is /etc/ssl/certs/ca-certificates.crt.

This file contains the certificates provided by Mozilla. A list of the included root certificates and their respective validity periods can be requested from the following address:

https://hg.mozilla.org/releases/mozilla-release/raw-file/79f079284141/security/nss/lib/ckfw/builtins/certdata.txt

The root certificates can be updated on the controller by updating the file /etc/ssl/certs/ca-certificates.crt (see section "Service" > "Updating Root Certificates").

5.1.3   Network Configuration

5.1.3.1   Host Name/Domain Name

Without a host name configuration, the controller is assigned a default name which includes the last three values of the controller's MAC address, e.g., "PFCx00-A1A2A3." This name is valid for as long as a host name was not configured, or host name was not supplied to the controller via DHCP (for configuration of the controller see Section "Startup" > "Configuring"). When the host name is set, a host name supplied by a DHCP response is immediately active and displaces the configured or default host name.

For multiple network interfaces with DHCP, the hostname is taken from the network interface (bridge or Wwan) with the highest priority. The priority is specified alphanumerically by the name of the network interface. Thus, Bridge1 has the highest priority, followed by Bridge2, Bridge3, ..., Wwan0.

If only the configured name is to be valid, the network administrator must adjust the configuration of the active DHCP server so that no host names are transferred in the DHCP response.

The default host name or the configured name is active again if the network interfaces are set to static IP addresses or if a host name is not received via the DHCP response.

A similar mechanism is used for a domain name as for the host name. The difference is that a default domain name is not set. As long as a domain name is not configured or supplied by DHCP, the domain name is empty.

5.1.3.2   Routing

As part of the TCP/IP configuration, the controller allows you to configure static routes, IP masquerading and port forwarding. Default gateways are configured via static routes, since default gateways are a special case of static routes.

A network station transmits to a gateway all network data packets for systems outside of its local network. This gateway is responsible for the appropriate routing of the data packets so that they reach the target system. To allow access to different target systems, it may be necessary to configure multiple gateways. This is configured by adding routing entries.
A routing entry consists of the following information:

•   Destination address,

•   Destination mask,

•   Gateway address,

•   Gateway metric.

•   Interface

On the basis of the target system configuration, consisting of the destination address and destination mask, a decision is made about which gateway a network data packet should be forwarded to. The target system can be specified through an individual IP address or an IP address range. For a network data packet to forward, the routing entry with the most specific destination address and destination mask entries is always selected. The default gateway corresponds to the least specific routing entry. All network data packets such that no specific routing entry exists for their destination address and destination mask are sent to this default gateway.

Default gateway:
Default gateways, also called default routes, are always set in connection with the IP configuration.
Each default gateway has a metric that is unique among all default gateways. Bridge <n> has the metric 19+<n>.
A default gateway can also be defined via the routing configuration, e.g., to define an individual metric. The value "default" must be set for "Destination Address" and the value "0.0.0.0" for Destination Mask.

Route:
If an IP address or IP address range is entered in the "Destination Address" field, then all network data packets that are directed to the network address or network address range are sent to the gateway address corresponding to the entry. Alternatively, a bridge, a modem or a VPN interface can be specified in the "Interface" field, via which all data packets that are directed to the destination address are routed. Specifying an interface is optional. However, either a gateway address, an interface or both must be specified.

If the IP address of the gateway is outside the IP address space that the controller can reach, the associated route is not enabled. This also applies to routes in which an interface is specified, which e.g., is not enabled in the current bridge configuration.

A metric is assigned to each routing entry. If multiple routing entries are configured for the same destination address and destination mask, the metric specifies how the routing entries are prioritized. In this case, routing entries with a lower value for the metric are preferred over routing entries with a higher metric value. The metric value of the configured routing entries can be specified for the controller.

Besides the manually configurable routes, default gateways can also be set via DHCP replies. A unique metric is assigned to all default gateways assigned by DHCP.

The metric is assigned starting at 10 and depends on the network interface via which the DHCP response was received. The metric is assigned in ascending order based on the alphanumeric sorting of the network interface names (e.g., br0, br1, … wwan0).

Metric example:
A controller obtains its IP configuration via a DHCP server and receives both the

IP address and the network mask 192.168.1.10/24. Furthermore, a gateway with IP address 192.168.1.2 and metric value 20 is set up on the controller. Therefore, when no specific routing entry exists for the target address of network data packets, the controller sends them to gateway 192.168.1.2. Besides the IP address and network mask, the DHCP server is now instructed to allocate a default gateway of 192.168.1.1. The controller gives this default gateway a metric value of 10. Therefore, the default gateway received via DHCP is preferred over the manually configured gateway.

The routing entries are used to specify which gateways the network data packets are sent. If the controller is running in switched mode and only has one network interface, all network traffic passes through this network interface. If the controller is running in separated mode or contains a modem, it has more than one network interface. Therefore, it is possible for a network data packet to arrive at the controller on one network interface and depart on a different network interface. This forwarding between different network interfaces must be explicitly enabled; it is disabled when the controller is delivered. To enable the forwarding, "Enabled" must be enabled in the "IP Forwarding through multiple interfaces" group. In this case, the controller can function as a router.

For forwarding network communication through a router, it is necessary to note that corresponding routing entries must be provided not only for the router, but also for the respective endpoints of the communication. The routing entries of the endpoints must ensure that the desired network data packets are sent via the router, both when the connection is established and with the replies.

Host route example:
A host route is a route to an individual host. In the following example, a route to a host with IP address 192.168.1.2 is to be specified. The route passes through a gateway that can be reached via address 10.0.1.3. To configure a host route to the destination host on a controller connected to the gateway, the following settings must be made:

Destination Address: 192.168.1.2   IP address of the destination host
Destination Mask: 255.255.255.255   Subnet mask of an individual host
Gateway Address: 10.0.1.3   IP address of the gateway
Gateway Metric   20   Route priority

Network route example:
A network route is a route to a subnet, which can contain multiple hosts. In the following example, a route to a subnet should be specified with network address 192.168.1.0. The route passes through a gateway that can be reached via address 10.0.1.3. To configure a network route to the destination network on a controller connected to the gateway, the following settings must be made:

Destination Address: 192.168.1.0   IP address of the destination network
Destination Mask: 255.255.255.0   Subnet mask of the destination network
Gateway Address: 10.0.1.3   IP address of the gateway
Gateway Metric   20   Route priority

Example of a route via an interface:
In the following example, a route to a host with IP address "192.168.1.2" is to be specified. The route runs via the br1 interface, which corresponds to Bridge 2. To configure a host route to the target host via Bridge 2 on a controller with an activated Bridge 2, the following settings must be made.

Destination address:	192.168.1.2	IP address of the target host
Destination mask:	255.255.255.255	Subnet mask of an individual host
Gateway Metric	20	Route priority
Interface	br1	Interface through which the packet is to be routed

Besides configuration of static routes, the controller also supports IP masquerading. This can be enabled for selected network interfaces of the controller. Network data packets that depart the controller through a network interface for which IP masquerading has been enabled are given the IP address of the network interface as their sender address. If network data packets are forwarded through the controller, the network behind the controller is encapsulated under a single address.

Furthermore, the controller permits configuration of port forwarding entries. For port forwarding, the destination address and, if relevant, destination port of a network data packet that arrived at the controller via a previously configured network interface are overwritten. This makes it possible to forward network data packets through the controller to other addresses and ports. Forwarding can be configured for the TCP or UDP protocols.

5.1.4   Network Services

5.1.4.1   DHCP-Client

The controller can get network parameters from an external DHCP master via the DHCP Client service.

The following parameters can be obtained:

- IP address

- SubNet mask

- Router/gateway

- Hostname

- Domain

- DNS server

- NTP server

For the IP address, SubNet mask and router/gateway parameters, the entries are stored per ETHERNET port.

For multiple network interfaces with DHCP, the hostname is taken from the network interface (bridge or Wwan) with the highest priority. The priority is specified alphanumerically by the name of the network interface. Thus, Bridge1 has the highest priority, followed by Bridge2, Bridge3, ..., Wwan0.

5.1.4.2   DHCP Server

The controller provides the DHCP server service for the automatic configuration of IP addresses of network stations on the same subnet.
Generally, only one DHCP server can be active on a subnet at one time.

The following can be set for the DHCP server:

- The service itself (active/not active)

- The range of dynamically assigned IP addresses

- The lease time of the dynamically assigned IP addresses

- A list with static assignments of IP addresses to MAC addresses

In "switched" mode, these settings are possible for both interfaces together and in "separated" mode for each interface separately.

The settings are made, for example, in the WBM via the "DHCP Configuration" page.

The DHCP server also passes other parameters in addition to the IP address. The following table shows the complete list.

Table 33: List of Parameters Transmitted via DHCP

Parameters	Explanation
IP address	An IP address from the range of permitted address; the range can be configured in the WBM. The DHCP server determines the IP address to be passed to the requesting network subscriber (client) from the MAC address of the network subscriber and the range of addresses to be assigned. As long as the configured address range does not change and no bottlenecks occur when assigning IP addresses, the DHCP server continuously reassigns the same IP addresses to requesting network subscribers. When a subscriber connects to the network, for whose MAC address a fixed IP address has been configured in the WBM, this address is passed to it. Such a fixed IP address can also be outside the range of freely-assignable IP addresses. A hostname can also be specified instead of the MAC address for identifying the requesting network subscriber.
Subnet mask	The subnet mask configured in the network settings of the DHCP server for the local network concerned is passed. The subnet mask and IP address determine the range of valid IP addresses on the local network.
Broadcast address	IP address with which an IP packet can be sent to all network subscribers on the subnet at the same time
Lease time	Determines the validity period of the DHCP parameters passed to a network subscriber: Per protocol, the network subscriber is required to request the network settings again after half the period of validity. The lease time is configured in the WBM.
Host name	The network name is passed to the network subscriber. The network subscriber normally sends its own name with its request for the IP address. It is then used by the DHCP server in its response.
Name server	The DHCP server passes its own IP address as the DNS name server to the network subscriber.
Default gateway	The DHCP server passes its own IP address as the default gateway to the network subscriber. The default gateway is required to communication with subscribers outside the local network.

Not all parameters can be set in the WBM. If you want to set other values for the existing parameters or want to pass other parameters via DHCP, the DHCP server must be manually configured. For the controller, the DHCP server service is handled by the program "dnsmasq".

From a Linux® command line, an editor must be used to change the file "/etc/dnsmasq.d/dnsmasq_default.conf" to set the configuration.

5.1.4.3   DNS Server

The controller offers the DNS server service for the automatic assignment of hostnames to IP addresses of network stations.
The DNS server takes over the names and IP addresses of local network stations from the DHCP server. This DNS server routes requests for non-local names, such as from the Internet, to higher-level DNS servers if configured and accessible.

The following settings are possible for the DNS server:

*   The service itself (enabled/disabled)

*   Access type to the assignments
        The requests are buffered in "Proxy" mode (throughput optimized).
        In Relay mode the requests are routed directly to higher-level name servers.

*   A list with up to 15 static assignments of IP addresses to hostnames
        If only the hostname is used, the configured or default domain is added to the hostname automatically to ensure FQDN name resolution.

The settings are made, e.g., in the WBM, via the "Configuration of DNS Service" page.

5.1.5   Cloud Connectivity Functionality

With the cloud connectivity functionality and an IEC library, the controller is available as a gateway for Internet-of-Things (IoT) applications. This means the controller can collect the data from all the connected devices, access the Internet via the built-in Ethernet interface or the mobile communications module and send the data to the cloud.

You can specify the cloud service to use: Microsoft Azure, Amazon Web Services and IBM Cloud are available.
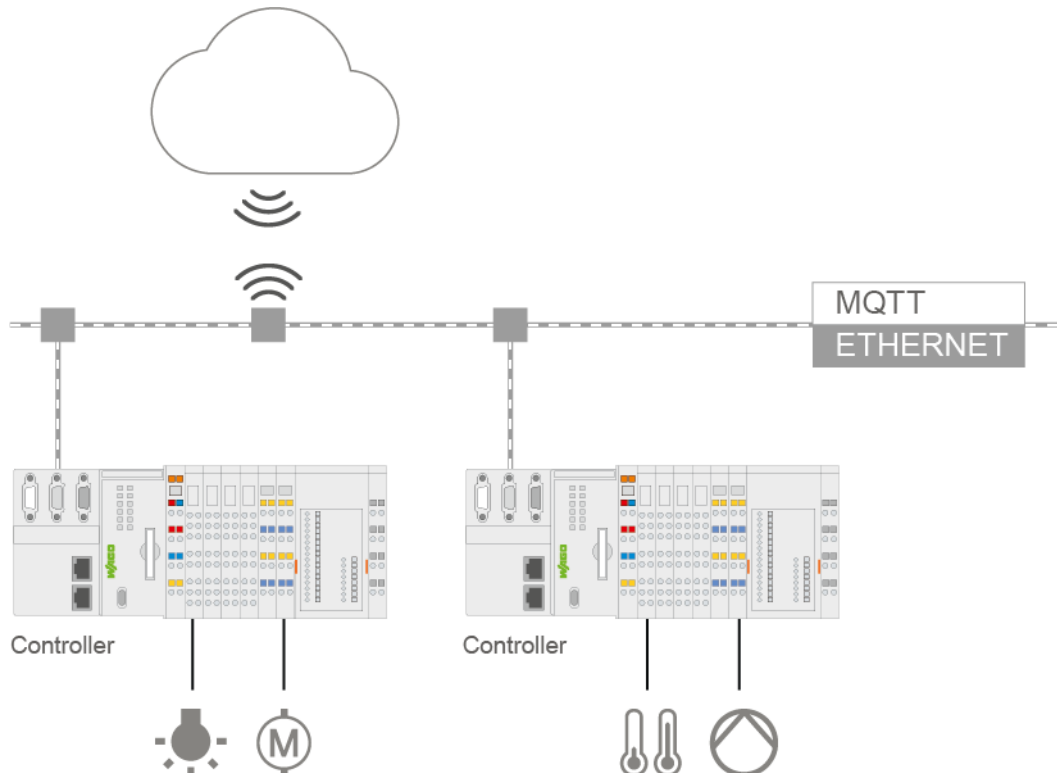
Figure 25: Connecting the Controller to a Cloud Service (Example)

Data is transmitted from the controller to the cloud service as JSON files. The connection can be encrypted with TLS; see the section "Functional Description" > … > "TLS Encryption."

You can find the settings that must be configured in the controller in order to use the cloud connectivity functionality in the section "Start-Up" > … > "Configuration Using Web-Based Management.

The communication parameter is configured in the WBM; the data to exchange between the cloud and controller is configured with the "WagoAppCloud" library for CODESYS V3.

> **Note**
>
> **Please note the risks of using cloud services!**
> If you use third-party cloud services, sensitive data is transferred to the cloud service provider at one's own responsibility. External access may result in manipulated data and/or unwanted control commands affecting the performance of your control system.
>
> Use encryption methods to protect your data and observe the information provided by the Federal Office for Information Security – "Cloud: Risks and Security Tips".
> Observe comparable publications of the competent, public institutions of your country.

> **Information**
>
> **Observe the additional documentation!**
> You can find a detailed description of the cloud connectivity software package with a controller and information on PLC programming in Application Note A500920 in the Downloads area: www.wago.com.

> **Information**
>
> **Observe the necessary data protection and security settings!**
> Before using the cloud connectivity functionality, consult the corresponding handbook and familiarize yourself with data protection and security issues.
> You will find this in the Downloads area at www.wago.com.

5.1.5.1   Components of the Cloud Connectivity Software Package

Table 34: Components of the Cloud Connectivity Software Package

Components	Description
CODESYS V3: WagoAppCloud	IEC library to create the PLC application; function blocks make it possible to exchange data between the PLC and cloud service. The data transmission variables are definable.

5.2   Memory Card Function

> **Note**
>
> **Only use recommended memory cards!**
> Use only the SD memory cards available from WAGO (item No. 758-879/000-001 and 758-879/000-2108) as these are suitable for industrial applications subjected to environmental extremes and for use in this device.
> Compatibility with other commercially available storage media cannot be guaranteed.

The memory card is optional and serves as an additional memory area in addition to the internal memory or drive in the controller. The user program, user data, source code of the project or device settings can be saved to the memory card, and thus already existing project data and programs can be copied to one or more controllers.

> **Note**
>
> **Deactivate write protection!**
> In order to be able to write data to the memory card, you must deactivate the write protection using the small push switch for the write protection setting. This switch is on one of the long sides of the memory card.

If the memory card is inserted, this is incorporated under /media/sd in the directory structure of the file system inside the controller. This means that the memory card can be addressed like a removable medium on a PC.

The function of the memory card in normal operation and possible faults that may occur when the memory card is used are described in the following sections for different operating modes.

5.2.1   Formatting

> **Note**
>
> **Note the pre-formatting of the memory card!**
> Please note that memory cards ≤ 2 GB are often formatted with the "FAT16" file system type and can generate up to 512 entries in the root directory. For over 512 entries create these in a subdirectory or format the memory card with "FAT32" or "NTFS."

> **Note**
>
> **Memory card access from CODESYS only possible with FAT16, FAT32 or NTFS!**
>
> If the CODESYS user "admin" (see the section "Network" > "Network Security" > "Users and Passwords" > "Services and Users") is supposed to be able to access files created on the memory card, the memory card must be formatted with FAT16, FAT32 or NTFS.
>
> If the Linux® file system formats EXT2 or EXT3 are used, "root" rights are required for data access. Therefore, access via CODESYS is not possible.

5.2.2   Data Backup

The controller has a backup function and a restore function.

In the WBM, the required settings can be made in the "Configuration" tab on the "Package Server" > "Firmware Backup" or "Firmware Restore" pages and the functions can be executed.

Settings can also be made in the CBM menu "Package Server" > "Firmware Backup" or "Firmware Restore".

The storage medium (internal memory or SD card) and, if applicable, the storage location on the network can be set.

The data to be backed up and restored can also be selected:

*   the CODESYS project ("PLC Runtime project," boot project)
*   the device settings ("Settings")
*   the controller operating system and the root file system ("System")
*   all of the above ("All," only visible if not saved on the network)

> ![Note icon]
>
> ### Note
>
> **Note the firmware version!**
> Restoring the controller operating system ("System" selection) is only permissible and possible if the firmware versions at the backup and restore times are identical.
> If necessary, skip restoring the controller operating system, or match the firmware version of the controller to the firmware version of the backup time beforehand.

5.2.2.1   Backup Function

The backup function enables the data of the internal memory and device settings to be saved on the memory card during operation.

The backup function can be called up the WBM page "Firmware Backup" in the "Configuration" tab, selection "Package Server" > "Firmware Backup" or in the CBM menu "Package Server" > "Firmware Backup".

The network or the inserted memory card can be selected as the target medium.

The files of the internal drive are stored on the target medium in the directory media/sd/copy and in the corresponding subdirectories.
The information that is not present as files on the controller is stored in XML format in the directory media/sd/settings/.

If the memory card is selected as the target medium, the LED above the memory card slot flashes yellow during the save operation.

The device settings and files of the internal drive are then saved on the target medium.

The controller has an automatic update function. If this function is activated on a memory card before the data backup and a controller is booted from this memory card, this data is restored automatically on the internal memory of the controller.

> **Note**
>
> **Only one package may be copied to the network!**
> If you have specified "Network" as the storage location, only one package may be selected for each storing process.

> **Note**
>
> **No backup of the memory card!**
> Backup from the memory card to the internal flash memory is not possible.

> **Note**
>
> **Account for backup time**
> Generation of backup files can take several minutes. Stop the CODESYS program before you start the backup procedure to help shorten the time required.

5.2.2.2   Restore Function

The restore function is used to load the data and device settings from the memory card to the internal memory during operation.

The restore function can be called up the WBM page "Firmware Restore" in the "Configuration" tab, selection "Package Server" > "Firmware Restore" or in the CBM menu "Package Server" > "Firmware Restore".

The network or, if it is inserted, the memory card can be selected as the source medium.

If the memory card is selected as the source medium, the LED above the memory card slot flashes yellow during the load operation.

When loading the data, the files are copied from the directory media/sd/copy/ of the source medium to the appropriate directories on the internal memory.

The device has an active and an inactive root partition. The system backup is stored on the inactive partition. Startup is then performed from the newly written partition. If the startup process can be completed, the new partition is switched to active. Otherwise, booting is performed again from the old active partition during the next boot process.

The boot project is loaded automatically and the settings automatically activated after a restart. The "Home directory on memory card enabled" setting determines whether the boot project of the internal drive or the memory card is loaded. This setting can be called up on the WBM page "PLC Runtime Configuration" in the "Configuration" tab, selection "PLC Runtime".

> **Note**
>
> **File size must not exceed the size of the internal drive!**
> Note that the amount of data in the media/sd/copy/ directory must not exceed the total size of the internal drive.

> **Note**
>
> **Restoration only possible from internal memory!**
> If the device was booted from the memory card, the firmware cannot be restored.

> **Note**
>
> **Reset by restore**
> A reset is performed when the system or settings are restored by CODESYS!

> **Note**
>
> **Connection loss through restore**
> If the restore changes the parameters of the ETHERNET connection, the WBM may then no longer be able to open a connection to the device. You must call the WBM again by entering the correct IP address of the device in the address line.

> **Note**
>
> **Note the restore time!**
> The restore process takes approx. 2 … 3 minutes.
> After the restore process, the controller is restarted and is then ready for use again.

5.2.3   Inserting a Memory Card during Operation

The fieldbus nodes and the PLC program are running.

Insert a memory card during ongoing operation.

During normal operation, the memory card is incorporated into the file system of the controller as a drive.
No automatic copy procedures are triggered.

The LED above the memory card flashes yellow during the access.

The memory card is then ready for operation and available under /media/sd.

5.2.4   Removing the Memory Card during Operation

The fieldbus node and the PLC program are in operation and the memory card is plugged in.

Remove the memory card during ongoing operation.

> **Note**
>
> **Data can be lost during writing!**
> Note that if you pull the memory card out during a write procedure, data will be lost.

The LED above the memory card flashes yellow during the attempted access.

The controller then works without a memory card.

5.2.5   Setting the Home Directory for the Runtime System

The home directory for the runtime system is located in the controller's internal memory by default. An existing boot project may be saved in the home directory.

You can use the WBM to move the home directory for the runtime system to the memory card, e.g., to make more memory available for a large boot project or other files.

This setting can be activated using the check box "Home directory on memory card enabled" on the WBM page "PLC Runtime". Click the **[Submit]** button to apply the setting, which takes effect after the next restart.
No files are applied from the old to the new home directory.

After moving the directory, a project must be loaded and a boot project created.

It should be noted that the memory card may not be removed under any circumstances as long as the home directory is there. If an application is running, system safety can be endangered by an uncontrolled controller crash.

Switching the home directory has no effect if the controller was botted from a memory card. The configuration state is saved, but only takes effect if the content of the memory card is copied to the internal memory.

5.2.6   Load Boot Project

If a boot project exists, it may be loaded, depending on the home directory setting for the runtime system. The following table shows the possible results:

Table 35: Loading a Boot Project

Boot Project Stored in Internal Flash Memory	Memory Card with Boot Project Inserted	"Home Directory on Memory Card Enabled" Checked	Boot Project is Loaded ...
No	No	No	No, no boot project exists
		Yes	No, no boot project exists
	Yes	No	No, no boot project exists in the internal flash memory
		Yes	Yes, from memory card
Yes	no	No	Yes, from internal flash memory
		(Yes) invalid	No, invalid combination, since no boot project is allowed to exist in the internal flash memory for this setting
	Yes	No	Yes, from internal flash memory
		(Yes) invalid	No, invalid combination, since no boot project is allowed to exist in the internal flash memory for this setting

5.3   Licensed Software Components

The *e!RUNTIME* runtime system software components that are subject to license verification (runtime licenses) are available for 2nd generation controllers (750-821x/xxx-xxx).

The *e!COCKPIT* software can be used for licensing. You can find corresponding instructions in the documentation of *e!COCKPIT*.

A license key is required for productive use without time restriction of a software component that is subject to licensing. Full use of the software component is possible even without a license key for 30 days. This trial period only includes the days of actual use. Access without a license key is no longer possible after the trial period.

The license status ("Evaluation period not yet expired" or "Evaluation period has expired") is displayed by the controller via the SYS LED.

When loading a program with licensed components, *e!COCKPIT* displays the number of days remaining.

6   Mounting

6.1   Installation Position

Along with horizontal and vertical installation, all other installation positions are allowed.

Note

→ **Use an end stop in the case of vertical mounting!**
In the case of vertical assembly, an end stop has to be mounted as an additional safeguard against slipping.
WAGO order no. 249-116   End stop for DIN 35 rail, 6 mm wide
WAGO order no. 249-117   End stop for DIN 35 rail, 10 mm wide

---

6.2   Overall Configuration

The maximum total length of a fieldbus node without fieldbus coupler/controller is 780 mm including end module. The width of the end module is 12 mm. When assembled, the I/O modules have a maximum length of 768 mm.

Examples:

- 64 I/O modules with a 12 mm width can be connected to a fieldbus coupler/controller.

- 32 I/O modules with a 24 mm width can be connected to a fieldbus coupler/controller.

Exception:

The number of connected I/O modules also depends on the type of fieldbus coupler/controller is used. For example, the maximum number of stackable I/O modules on one PROFIBUS DP/V1 fieldbus coupler/controller is 63 with no passive I/O modules and end module.

NOTICE

Observe maximum total length of a fieldbus node!
The maximum total length of a fieldbus node without fieldbus coupler/controller and without using a 750-628 I/O Module (coupler module for internal data bus extension) may not exceed 780 mm.
Also note the limitations of individual fieldbus couplers/controllers.

> **Note**
>
> **Increase the total length using a coupler module for internal data bus extension!**
> You can increase the total length of a fieldbus node by using a 750-628 I/O Module (coupler module for internal data bus extension). For such a configuration, attach a 750-627 I/O Module (end module for internal data bus extension) after the last I/O module of a module assembly. Use an RJ-45 patch cable to connect the I/O module to the coupler module for internal data bus extension of another module block.
> This allows you to segment a fieldbus node into a maximum of 11 blocks with maximum of 10 I/O modules for internal data bus extension.
> The maximum cable length between two blocks is five meters.
> More information is available in the manuals for the 750-627 and 750-628 I/O Modules.

6.3   Mounting onto Carrier Rail

6.3.1   Carrier Rail Properties

All system components can be snapped directly onto a carrier rail in accordance with the European standard EN 60175 (DIN 35).

NOTICE

Do not use any third-party carrier rails without approval by WAGO!
WAGO Kontakttechnik GmbH & Co. KG supplies standardized carrier rails that are optimal for use with the I/O system. If other carrier rails are used, then a technical inspection and approval of the rail by WAGO Kontakttechnik GmbH & Co. KG should take place.

Carrier rails have different mechanical and electrical properties. For the optimal system setup on a carrier rail, certain guidelines must be observed:

- The material must be non-corrosive.

- Most components have a contact to the carrier rail to ground electro-magnetic disturbances. In order to avoid corrosion, this tin-plated carrier rail contact must not form a galvanic cell with the material of the carrier rail which generates a differential voltage above 0.5 V (saline solution of 0.3 % at 20°C).

- The carrier rail must optimally support the EMC measures integrated into the system and the shielding of the I/O module connections.

- A sufficiently stable carrier rail should be selected and, if necessary, several mounting points (every 20 cm) should be used in order to prevent bending and twisting (torsion).

- The geometry of the carrier rail must not be altered in order to secure the safe hold of the components. In particular, when shortening or mounting the carrier rail, it must not be crushed or bent.

- The base of the I/O components extends into the profile of the carrier rail. For carrier rails with a height of 7.5 mm, mounting points are to be riveted under the node in the carrier rail (slotted head captive screws or blind rivets).

- The metal springs on the bottom of the housing must have low-impedance contact with the DIN rail (wide contact surface is possible).

6.3.2   WAGO DIN Rails

WAGO carrier rails meet the electrical and mechanical requirements shown in the table below.

Table 36: WAGO DIN Rails

Item No.	Description
210-112	35 × 7.5; 1 mm; steel; bluish, tinned, chromed; slotted
210-113	35 × 7.5; 1 mm; steel; bluish, tinned, chromed; unslotted
210-197	35 × 15; 1.5 mm; steel; bluish, tinned, chromed; slotted
210-114	35 × 15; 1.5 mm; steel; bluish, tinned, chromed; unslotted
210-118	35 × 15; 2.3 mm; steel; bluish, tinned, chromed; unslotted
210-198	35 × 15; 2.3 mm; copper; unslotted
210-196	35 × 8.2; 1.6 mm; aluminum; unslotted

NOTICE

Observe the mounting distance of the DIN rail when the load is increased!
With increased vibration and shock load, mount the DIN rail at a mounting
distance of max. 60 mm.

6.4   Spacing

The spacing between adjacent components, cable conduits, casing and frame
sides must be maintained for the complete fieldbus node.
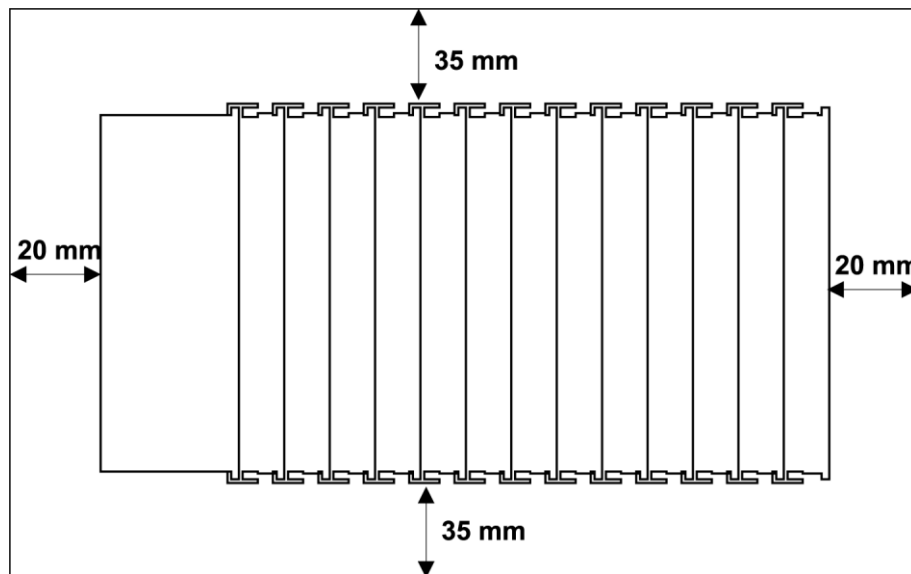
Figure 26: Spacing

The spacing creates room for heat transfer, installation or wiring. The spacing to
cable conduits also prevents conducted electromagnetic interferences from
influencing the operation.

6.5   Mounting Sequence

Fieldbus couplers, controllers and I/O modules of the WAGO I/O System 750 are snapped directly on a carrier rail in accordance with the European standard EN 60175 (DIN 35).

The reliable positioning and connection is made using a tongue and groove system. Due to the automatic locking, the individual devices are securely seated on the rail after installation.

Starting with the fieldbus coupler or controller, the I/O modules are mounted adjacent to each other according to the project design. Errors in the design of the node in terms of the potential groups (connection via the power contacts) are recognized, as the I/O modules with power contacts (blade contacts) cannot be linked to I/O modules with fewer power contacts.

⚠ CAUTION

Risk of injury due to sharp-edged blade contacts!
The blade contacts are sharp-edged. Handle the I/O module carefully to prevent injury. Do not touch the blade contacts.

NOTICE

Insert I/O modules only from the proper direction!
All I/O modules feature grooves for power jumper contacts on the right side. For some I/O modules, the grooves are closed on the top. Therefore, I/O modules featuring a power jumper contact on the left side cannot be snapped from the top. This mechanical coding helps to avoid configuration errors, which may destroy the I/O modules. Therefore, insert I/O modules only from the right and from the top.

Note

Don't forget the bus end module!
Always plug a bus end module (e.g. 750-600) onto the end of the fieldbus node! You must always use a bus end module at all fieldbus nodes with WAGO I/O System 750 fieldbus couplers or controllers to guarantee proper data transfer.

6.6   Inserting Devices

⚠ **DANGER**

Do not work when devices are energized!
High voltage can cause electric shock or burns.
Switch off all power to the device prior to performing any installation, repair or maintenance work.

6.6.1   Inserting the Controller

1.   When replacing the controller for an already available controller, position the new controller so that the tongue and groove joints to the subsequent I/O module are engaged.

2.   Snap the controller onto the carrier rail.

3.   Use a screwdriver blade to turn the locking disc until the nose of the locking disc engages behind the carrier rail (see the following figure). This prevents the controller from canting on the carrier rail.

With the controller snapped in place, the electrical connections for the data contacts and power contacts (if any) to the possible subsequent I/O module are established.
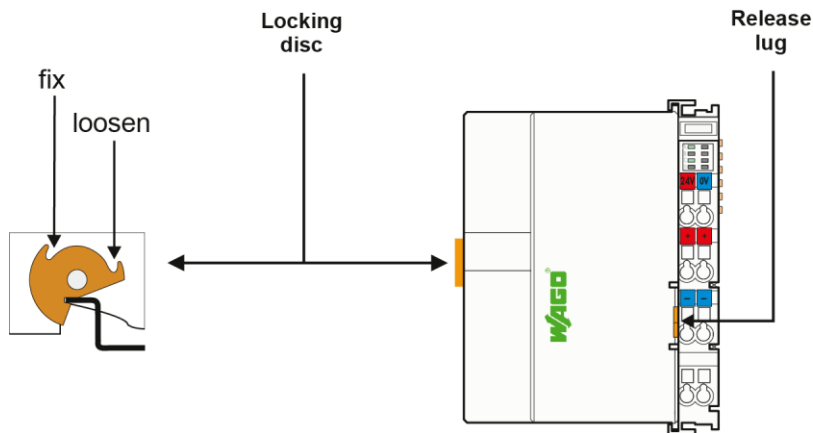
Figure 27: Release Tab of Controller (Example)

7   Connect Devices

7.1   Connecting a Conductor to the CAGE CLAMP®

The WAGO CAGE CLAMP® connection is appropriate for solid, stranded and finely stranded conductors.

NOTICE

Select conductor cross sections as required for current load!
The current consumed for field-side supply may not exceed 10 A. The wire cross sections must be sufficient for the maximum current load for all of the I/O modules to be supplied with power.

Note

Only connect one conductor to each CAGE CLAMP® connection!
Only one conductor may be connected to each CAGE CLAMP® connection.
Do not connect more than one conductor at one single connection!

If more than one conductor must be routed to one connection, these must be connected in an up-circuit wiring assembly, for example using WAGO feed-through terminals.

1.   To open the CAGE CLAMP® insert the actuating tool into the opening above the connection.

2.   Insert the conductor into the corresponding connection opening.

3.   To close the CAGE CLAMP® simply remove the tool - the conductor is then clamped firmly in place.
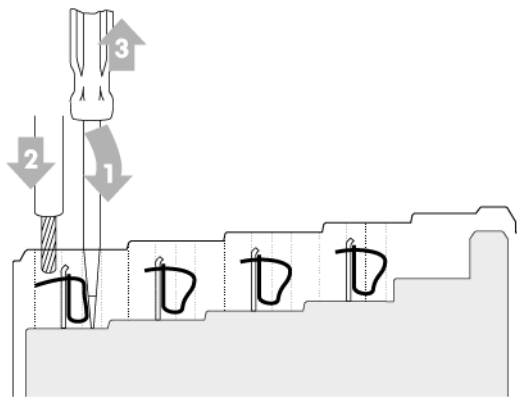
Figure 28: Connecting a Conductor to a CAGE CLAMP®

7.2   Power Supply Concept

7.2.1   Overcurrent Protection

⚠ **WARNING**

Possible fire hazard due to insufficient overcurrent protection!
In the event of a fault, insufficient overcurrent protection can present a possible
fire hazard. In the event of a fault, excessive current flow in the components can
cause significant overheating. Therefore, you should always dimension the
overcurrent protection according to the anticipated power usage.

The system and field voltage of the WAGO-I/O-SYSTEMs 750 is supplied on the
head stations and bus supply modules.
For components that work with extra low voltage, only SELV/PELV voltage
sources should be used.

A single voltage source supplying multiple components must be designed
according to the component with the strictest electrical safety requirements.
For components which are only allowed to be supplied by SELV voltage sources,
these requirements are listed in the technical data.

Most components in the WAGO-I/O-SYSTEM 750 have no internal overcurrent
protection. Therefore, appropriate overcurrent production must always be
implemented externally for the power supply to these components, e.g. via fuses.
The maximum permissible current is listed in the technical data of the
components used.

NOTICE

System supply only with appropriate fuse protection!
Without overcurrent protection, the electronics can be damaged.
If you implement the overcurrent protection for the system supply with a fuse, a
fuse, max. 2 A, slow-acting, should be used.

NOTICE

Field supply only with appropriate fuse protection!
Without overcurrent protection, the electronics can be damaged.
If you alternatively implement the overcurrent protection for the field supply with
an external fuse, a 10 A fuse should be used.

7.2.2   Supplementary Power Supply Regulations

The WAGO-I/O-SYSTEM 750 can also be used in shipbuilding or offshore and onshore areas of work (e. g. working platforms, loading plants). This is demonstrated by complying with the standards of influential classification companies such as Germanischer Lloyd and Lloyds Register.

Filter modules for 24 V supply are required for the certified operation of the system.

Table 37: Filter Modules for 24 V Supply

Order No.	Name	Description
750-626	Supply Filter	Filter module for system supply and field supply (24 V, 0 V), i. e. for fieldbus coupler/controller and bus power supply (750-613)
750-624	Supply Filter	Filter module for the 24 V field supply (750-602, 750-601, 750-610)

Therefore, the following power supply concept must be absolutely complied with.
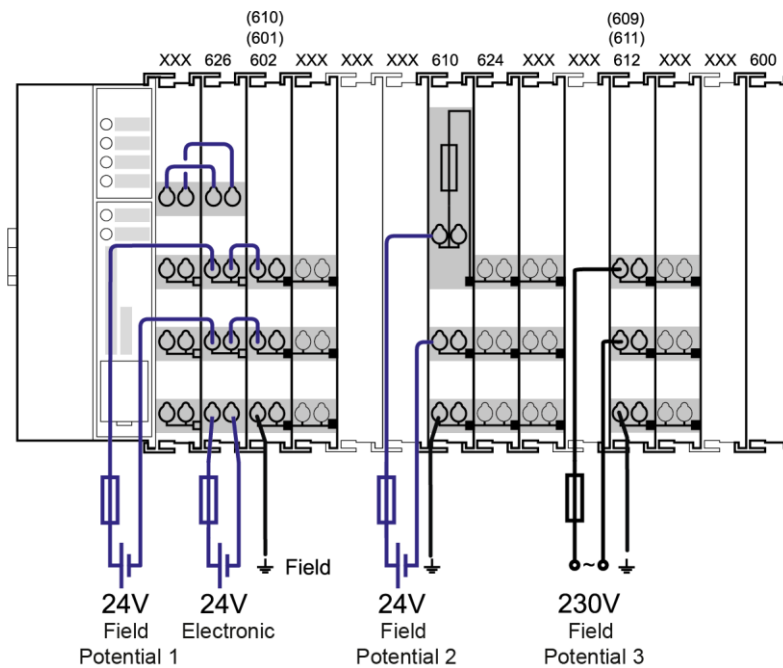
Figure 29: Power Supply Concept

> **Note**
>
> **Use a supply module for equipotential bonding!**
> Use an additional 750-601/ 602/ 610 Supply Module behind the 750-626 Filter Module if you want to use the lower power jumper contact for equipotential bonding, e.g., between shielded connections and require an additional tap for this potential.

8   Commissioning

> **Note**
>
> **Close any ports and services that you do not need!**
> Unauthorized persons may gain access to your automation system through open ports.
> To reduce the risk of cyber attacks and thus increase cyber security, close all ports and services not required by your application in the control components (e.g., port 6626 for WAGO-I/O-*CHECK* and port 11740 for CODESYS V3).
> Only open ports and services during commissioning and/or configuration.

8.1   Switching On the Controller

Before switching on the controller ensure that you

- have properly installed the controller
  (see section "Installation"),

- have connected all required data cables (see section "Connections") to the corresponding interfaces and have secured the connectors by their attached locking screws,

- have connected the electronics and field-side power supply
  (see section "Connections"),

- have mounted the end module
  (see Section "Installation"),

- have performed appropriate potential equalization at your machine/system
  (see System Description for 750-xxx) and

- have performed shielding properly (see System Description for 750-xxx).

To switch on both the controller and the connected I/O modules, switch on your power supply unit.

Starting of the controller is indicated by a brief orange flashing of all LEDs. After a few seconds the SYS LED will indicate successful boot-up of the controller.
The runtime system CODESYS V3 is started at the same time.

Once the entire system has been successfully started, the SYS and I/O LEDs light up green.

If there is an executable IEC 61131-3 program stored and running on the controller, the RUN LED will light up green.

If no executable program is stored on the controller, or the mode selector switch is set to STOP, this is likewise indicated by the RUN LED (see Section "Diagnostics"> … > "Fieldbus/System Indication Elements").

8.2   Determining the IP Address of the Host PC

To ensure that the host PC can communicate with the controller via ETHERNET, both devices must be located in the same subnet.

To determine the IP address of the host PC (with the Microsoft Windows® operating system) using the MS DOS prompt, proceed as follows:

1.   Open the MS DOS prompt window.
     To do this, enter the command "cmd" in the input field under **Start** >
     Execute… > **Open:** (Windows® XP) or **Start** > **Search programs/files**
     (Windows® 7) and then click **[OK]** or press **[Enter]**.

2.   In the MS DOS prompt enter the command "ipconfig" and then press
     [Enter].

3.   The IP address, subnet mask and standard gateway, including the
     appropriate parameters, are displayed.

8.3   Setting an IP Address

In the controller's initial state, the following IP addresses are active for the ETHERNET interface (Port X1 and Port X2):

Table 38: Default IP Addresses for ETHERNET Interfaces

ETHERNET Interface	Default Setting
X1/X2 (switched mode)	Dynamic assignment of IP address using DHCP ("Dynamic Host Configuration Protocol")

Adapt IP addressing to your specific system structure to ensure that the PC and the controller can communicate with one another using one of the available configuration tools (see section "Configuration").

Example for incorporating the controller (192.168.2.17) into an existing network:

- The IP address of the host PC is **192.168.1.2**.

- The controller and host PC must be in the same subnet (regardless of the IP address of the host PC).

- With a subnet mast of **255.255.255.0**, the first three digits of the IP address of the host PC and controller must match so that they are located in the same subnet.

Table 39: Network Mask 255.255.255.0
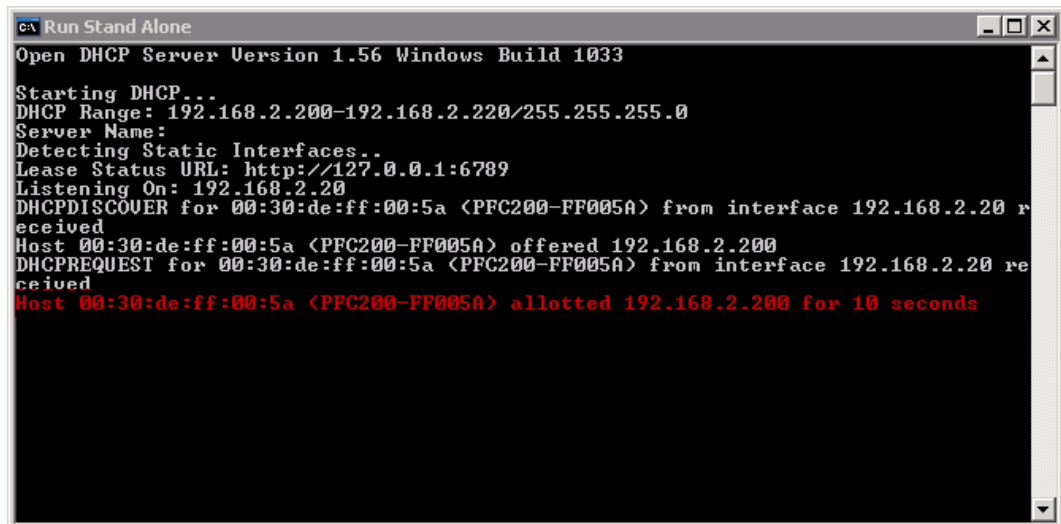
Host PC	Subnet Address Range for the Controller
192.168.1.2	**192.168.1**.1 or **192.168.1**.3 … **192.168.1**.254

8.3.1 Assigning an IP Address using DHCP

The Controller can obtain dynamic IP addresses from a server (DHCP/BootP).
In contrast to fixed IP addresses, dynamically assigned addresses are not stored permanently. Therefore, a BootP or DHCP server must be available each time the controller is restarted.

If an IP address has been assigned by means of DHCP (default setting), it can be determined through the settings and the output of the specific DHCP server.

In the example figure shown here, the corresponding output of "Open DHCP" is presented.

Figure 30: "Open DHCP", Example Figure

In conjunction with the DNS server associated with DHCP, the device can be reached using its host name.
This name consists of the prefix "PFCx00-" and the last six places of the MAC address (in the example shown here: "00:30:DE:FF:00:5A"). The MAC address of the device can be printed on the label on the side of the device.

The host name of the device in the example shown here is thus "PFC200-FF005A".

8.3.2   Changing an IP Address Using the "CBM" Configuration Tool and a Terminal Program

You can also assign a new IP address to the ETHERNET interfaces X1 and X2 using the "CBM" configuration tool provided on the Linux® console. More information about "CBM" is given in the Section "Configuration."

1. Connect a PC to the ETHERNET interface X1 of the controller using an SSH terminal program.

2. Start the terminal program.

3. Select "SSH" as the connection type, and enter the IP address of the controller and port 22 as the connection parameters.

Alternatively, you can also connect the controller via a serial interface:

1. Connect a PC to the X3 serial interface of the controller using a terminal program.

2. Start the terminal program.

3. Select "Serial" as the connection type and enter a baud rate of 115200 bauds as the connection parameter. The settings for data bits, stop bits and parity do not need to be adjusted.

4. Log in to the Linux® system as a "super user."
The user name and the password are provided in the Section "Users and Passwords" > "Linux® User Group."

5. Start the configuration tool by entering the command "cbm" (case sensitive) on the command line and then press **[Enter]**.

```
=======================================================================
WAGO Console Based Management Tool
=======================================================================
Main Menu
-----------------------------------------------------------------------
 0. Quit
 1. Information
 2. PLC Runtime
 3. Networking
 4. Firewall
 5. Clock
 6. Administration
 7. Package Server
 8. Mass Storage
 9. Software Uploads
 10. Ports and Services
 11. SNMP
 12. PROFIBUS DP
-----------------------------------------------------------------------
 Select an entry or Q to quit
-----------------------------------------------------------------------
```
Figure 31: CBM main menu (example)

6. In the **Main menu** use the keyboard (arrow keys or numeric keypad) to
    move to and select **Networking** and then press **[Enter]**.

```
========================================================================
WAGO Console Based Management Tool
========================================================================

Main Menu
------------------------------------------------------------------------
0. Quit
1. Information
2. PLC Runtime
3. Networking
4. Firewall
5. Clock
6. Administration
7. Package Server
8. Mass Storage
9. Software Uploads
10. Ports and Services
11. SNMP
12. PROFIBUS DP
------------------------------------------------------------------------
Select an entry or Q to quit
------------------------------------------------------------------------
```

Figure 32: CBM – Selecting "Networking"

7. In the **Networking** menu select **TCP/IP** and press **[Enter]**.

```
========================================================================
WAGO Console Based Management Tool
========================================================================

Networking
------------------------------------------------------------------------
0. Back to Main Menu
1. Host-/Domain Name
2. TCP/IP
3. Ethernet
------------------------------------------------------------------------
Select an entry or Q to quit
------------------------------------------------------------------------
```

Figure 33: CBM – Selecting "TCP/IP"

8. In the menu **TCP/IP** select **IP Address** and press **[Enter]**.

```
========================================================================
WAGO Console Based Management Tool
========================================================================

TCP/IP
------------------------------------------------------------------------
0. Back to Networking Menu
1. IP Address
2. Default Gateway
3. DNS Server
------------------------------------------------------------------------
Select an entry or Q to quit
------------------------------------------------------------------------
```

Figure 34: CBM – Selecting "IP address"

9. In the menu **TCP/IP Configuration** select **IP Address** and press **[Enter]**.

```
========================================================================
WAGO Console Based Management Tool
========================================================================
TCP/IP Configuration of X1
------------------------------------------------------------------------
0. Back to TCP/IP Menu
1. Type of IP Address Configuration....Static IP
2. IP Address.........................192.168.1.18
3. Subnet Mask........................255.255.255.0
------------------------------------------------------------------------
Select an entry or Q to quit
------------------------------------------------------------------------
```

Figure 35: CBM – Selecting the IP Address

10. In the menu **Change IP Address** enter the new IP address and confirm by clicking **[OK]**. If you want to return to the main menu without making changes, click **[Abort]**.

```
========================================================================
WAGO Console Based Management Tool
========================================================================
Change IP Address
------------------------------------------------------------------------

Enter new IP Address:
+---------------+
|192.168.1.17   |
+---------------+

< OK >    <Abort>

------------------------------------------------------------------------
OK: confirm value, Abort: quit without changes
------------------------------------------------------------------------
```

Figure 36: CBM – Entering a New IP Address

8.3.3   Changing an IP Address using "WAGO Ethernet Settings"

The Microsoft Windows® application "WAGO Ethernet Settings" is a software
used to identify the controller and configure network settings.

→ **Note**

Observe the software version!

To configure the controller use at least Version 6.4.1.1 dated 2015-06-29 of
"WAGO Ethernet Settings"!

You can use WAGO communication cables or WAGO radio adapters or even the
IP network for data communication.

1.   Switch off the power supply to the controller.

2.   Connect the 750-923 communication cable to the Service interface on the
      controller and to a serial interface of your PC.

3.   Switch the power supply to the controller on again.

4.   Start the "WAGO Ethernet Settings" program.
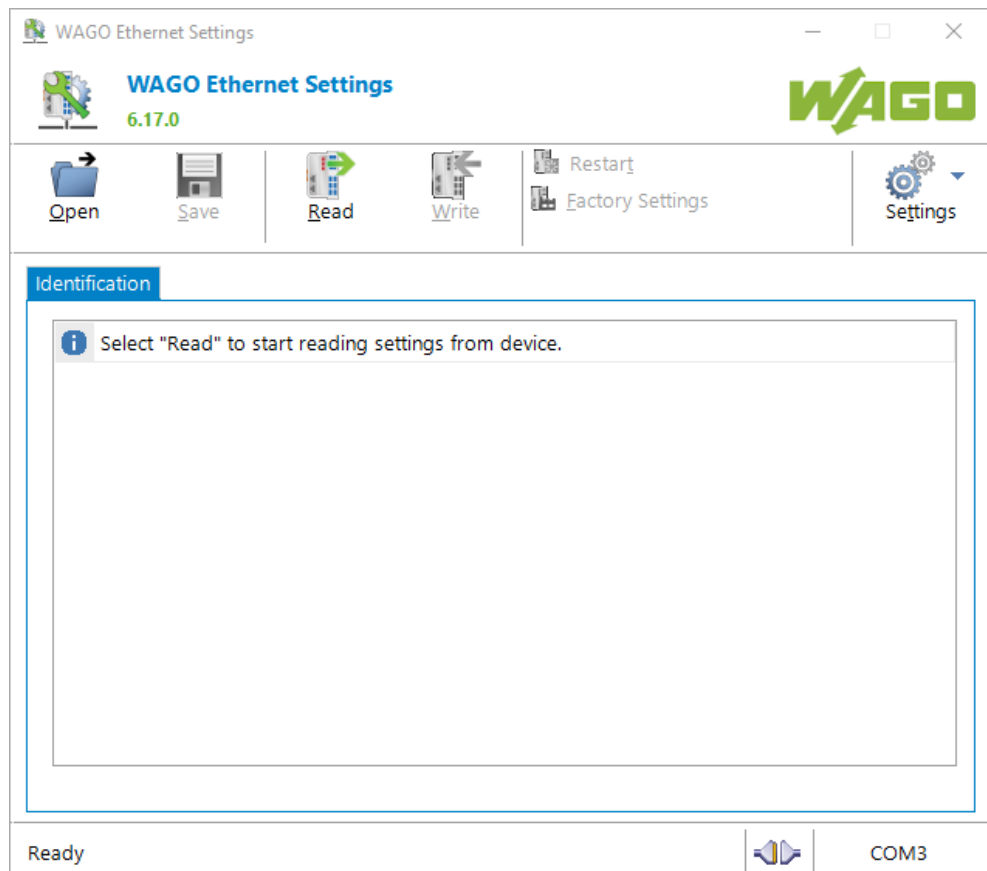
Figure 37: "WAGO Ethernet Settings" – Starting Screen (Example)

5.   Click **[Read]** to read in and identify the connected controller.

---

6.   Select the "Network" tab:

Figure 38: "WAGO Ethernet Settings" – "Network" Tab

7.   To assign a fixed address, select "Static configuration" on the "Source" line under "Input". DHCP is normally activated as the default setting.

8.   In the column "Input" enter the required IP address and, if applicable, the address of the subnet mask and of the gateway.

9.   Click on **[Write]** to accept the address in the controller. (If necessary, "WAGO Ethernet Settings" will restart your controller. This action may require about 30 seconds.)

10.   You can now close "WAGO Ethernet Settings", or make other changes directly in the Web-based Management system as required. To do this, click on **[Run WBM]** at the right in the window.

8.3.4   Temporarily Setting Fixed IP Addresses

This process temporarily sets the IP addresses for the network interfaces
X1 … X<n> to fixed IP addresses.
For each bridge used, the assigned interfaces are assigned their own address,
whereby bridge 1 receives the IP address "192.168.1.17", bridge 2 the IP
address "192.168.2.17" and so on.

No reset is performed.

To set temporary fixed IP addresses, proceed as follows:

1.   Set the mode selector switch to STOP and

2.   Press and hold the Reset button (RST) for longer than 8 seconds.

Execution of the setting is signaled by the "SYS" LED flashing orange.

If you make changes to the IP configuration of a bridge after activating the
temporary IP addresses, the new settings are permanently adopted and applied
immediately. The configured bridge exits the temporary IP address mode. The
other bridges keep the temporarily set IP address until restart / reset.

To cancel this setting, proceed as follows:

•   Perform a software reset or

•   Switch off the controller and then switch it back on.

8.4 Testing the Network Connection

Carry out a ping network function to check whether you can reach the controller at the IP address you have assigned in the network.

1. Open the MS DOS prompt window.
   To do this, enter the command "cmd" in the input field under **Start** > **Execute…** > **Open:** (Windows® XP) or **Start** > **Search programs/files** (Windows® 7) and then click **[OK]** or press **[Enter]**.

2. In the MS DOS window, enter the command "ping" and the IP address of the controller (for example, `ping 192.168.1.17`) and then press **[Enter]**.

→ **Note**

Host entries in the ARP table!

It may also be useful to delete the current host entries in the ARP table with the command "arp -d *" before executing the "ping" command (as administrator in Windows® 7). This ensures that older entries will not impair the success of the "ping" command.

---

3. Your PC sends out a query that is answered by the controller. This reply appears in the MS DOS prompt window. If the error message "Timeout" appears, the controller has not responded properly. You then need to check your network settings.

Figure 39: Example of a Function Test

4. If the test is completed successfully, close the MS DOS window.

8.5   Changing Passwords

→
Note

Change standard passwords
The standard passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs!

To increase security all passwords should contain a combination of lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), spaces and special characters: (]!"#$%&'()*+,./:;<=>?@[\^_`{|}~-). Passwords should not contain generally known names, dates of birth and other information that is easy to guess.

Change the standard passwords before commissioning the controller. Standard passwords are issued for the user groups "WBM Users" and "Linux® Users."

The table in the Section "Function Description" > ... > "Users and Passwords" > "WBM Users Group" shows the standard passwords for the WBM users. Proceed as follows to change these passwords:

1.   Connect the controller to a PC via one of the network interfaces (X1, X2).

2.   Start a web browser program on the PC and call up the WBM of the controller (see Section "Commissioning" > … > "Configuration via Web-Based-Management (WBM)").

3.   Log in on the controller as "admin" user with the standard password.

4.   Change the password for all users on the WBM "Configuration of the users for the WBM" page.

5.   Select each user and enter a new password and confirm it.

The table in the Section "Functional Description" > ... > "Users and Passwords" > "Linux® Users Group" shows the standard passwords for the Linux® users. Proceed as follows to change these passwords:

1.   Connect the controller to a PC via the network interfaces X1.

2.   Start a terminal program on the PC (see Section "Commissioning" > … > "Configuration via Console-Based-Management-Tool (CBM) using a Terminal Program").

3.   Log in on the controller as user "root" with the standard password.

4.   Change the password for all users with the "passwd root," "passwd admin" and "passwd user" commands.

8.6   Shutdown/Restart

Switch off the power supply to shut down the controller.

To perform a controller restart, press the Reset button as described in the
Section "Triggering Reset Functions" > "Software Reset (Restart)."
Alternatively, you can switch off the controller and switch it back on again.

Note

Do not power cycle the controller after changing any parameters!
Some parameter changes require a controller restart for the changes to apply.
Saving changes takes time.
Do not power cycle the controller to perform a restart, i.e., changes may be lost
by shutting down the controller too soon.
Only restart the controller using the software reboot function. This ensures that
all memory operations are completed correctly and completely.

8.7   Initiating Reset Functions

You can initiate various reset functions using the mode selector switch and the Reset button (RST).

8.7.1   Warm Start Reset

All CODESYS V3 applications are reset with a warm start reset. All global data is set to its initialization values. This corresponds to the CODESYS V3 IDE "Reset warm" command.

To perform a warm start reset, set the mode selector switch to "Reset" and hold it there for two to seven seconds.
Execution of the reset is signaled by the red "RUN LED" briefly going out when the mode selector switch is released.

8.7.2   Cold Start Reset

All CODESYS V3 applications are reset with a cold start reset. All global data and the retain variables are set to their initialization values.
This corresponds to the CODESYS V3 IDE "Reset Cold" command.

To perform a cold start reset, set the mode selector switch to "Reset" and hold it there for more than seven seconds.
Execution of the reset is signaled after seven seconds by the "RUN" LED going out for an extended period. You can then release the mode selector switch.

8.7.3   Software Reset

The controller is restarted on a software reset.

To perform a software reset, set the mode selector switch to RUN or STOP and then press the Reset button (RST) for one to eight seconds.

Reset completion is indicated by a brief orange flashing of all LEDs. After a few seconds the SYS LED will indicate successful boot-up of the controller.

8.7.4   Controller Reset

NOTICE

Do not switch the controller off!
The controller can be damaged by interrupting the controller reset process.
Do not switch the controller off during the controller reset process, and do not disconnect the power supply!

→ *Note*

Parameters and passwords are overwritten!
Parameters and passwords for the Linux® and WBM users of the controller are
overwritten by a controller reset.
Stored boot projects are deleted, including existing web visualizations.
Subsequently installed firmware functions are not overwritten.
Software licenses are retained.
The inactive system is not changed by the reset.
If you have any questions, contact WAGO Support.

The controller is restarted after the controller reset.
Proceed as follows to reset the controller:

1.   Press the Reset button (RST).

2.   Set the mode selector switch to the "RESET" position.

3.   Press and hold both buttons until the "SYS" LED alternately flashes
     red/green after approx. 8 seconds.

4.   When the "SYS" LED flashes red/green alternately, release the mode
     selector switch and Reset button.

→ *Note*

Do not interrupt the reset process!
If you release the Reset button (RST) too early, then the controller restarts
without performing the controller reset.

8.8   Configuration

→ **Note**

Check firmware version and update if required!
At the beginning of initial configuration check to ensure that you have the latest firmware version for the controller.
The firmware version installed on the controller is given on the WBM page "Status Information", or in the CBM menu "Information" under "Controller Details". Perform an update to install the latest firmware version.
To do this, follow the instructions given in section "Service" > "Firmware Changes" > "Perform Firmware Upgrade".

The following methods are available for configuring the controller:

• Access to the Web-based management system via the PC using a web browser (section "Configuration Using Web-Based Management [WBM]")

• Access to the "Console-Based Management" tool via the PC using a terminal program (section "Configuration Using a Terminal Program [CBM]")

• Access via the PLC program CODESYS using the "WagoAppConfigTool.lib" library.

• Access via the PC using "WAGO Ethernet Settings" (section "Configuration Using 'WAGO Ethernet Settings'").

The CBM is basically for the initial configuration and startup of the controller. Therefore, it only provides a subset of the WBM parameters. For example, parameters that cannot be displayed in a terminal window in a reasonable way and are not necessary for initial startup are not displayed. You can find the explanations of the parameters starting with the section "'Information' Page."

8.8.1   Configuration via Web-Based-Management (WBM)

The HTML pages (from here on referred to as "pages") of the Web-Based Management are used to configure the controller. Proceed as follows to access the WBM using a web browser:

1. Connect the controller to the ETHERNET network via the ETHERNET interface X1.

2. Start a Web browser on your PC.

3. Enter "https://" followed by the controller's IP address and "/wbm-ng" in the address line of your web browser, e.g., "https://192.168.1.17/wbm-ng".
    Note that the PC and the controller must be located within the same subnet (see Section "Setting an IP Address").
    If you do not know the IP address and cannot determine it, switch the controller temporarily to the pre-set address "192.168.1.17" ("Fixed IP address" mode, see Section "Commissioning" > … > "Temporarily Setting a Fixed IP Address").

> **Note**
>
> **Take usage by the CODESYS program into account**
> If the controller is at capacity due to a CODESYS program, this may result in slower processing in the WBM. As a result, timeout errors are sometimes reported in some circumstances. It is therefore important to stop the CODESYS application prior to performing complicated configurations using WBM.

→   When the connection has been established, a login window opens.

Figure 40: Entering Authentication

4. Enter the username and password.

5. Click the **[Login]** button.

→   Depending on the user selected, the navigation bar and the tabs of the
     WBM are displayed.

If you have disabled cookies in your web browser, you can continue to use the
WBM as long as you move directly inside it. However, if you fully reload the
website (e.g., with **[F5]**), you must log in again since the web browser is then not
able to store the data of your login session.

8.8.1.1 WBM User Administration

To allow settings to be made only by a select number of users, limit access to WBM functions through User Administration.

Note

Change passwords
Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.

If you do not change these passwords, a warning will appear each time you call up a website after logging in.

⚠ Warning

Password Expired

Security message: your password has expired!

Cancel   Change now
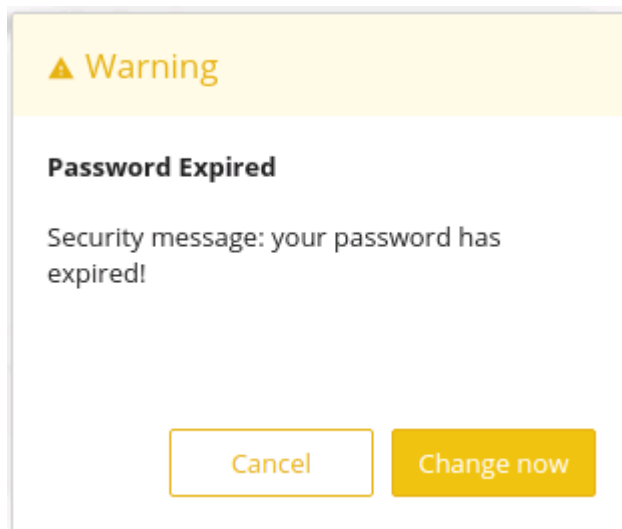
Figure 41: Password Reminder

Table 40:User Settings in the Default State

Users	Permissions	Default Password
root	All (administrator)	wago
admin	All (administrator)	wago
user	Supported to a limited extent	user

Note

General Rights of WBM Users
The WBM users "root", "admin" and "user" have rights beyond the WBM to configure the system and install software.

User administration for controller applications is configured separately.

Access rights for the WBM pages are shown in the table below.
The "root" user has the same rights as the "admin" user and is therefore not listed separately.

Table 41: Access Rights for WBM Pages

Tab/Navigation	WBM Page Title	User
Information		
Device Status	Device Status	user
Vendor Information	Vendor Information	user
PLC Runtime	PLC Runtime Information	user
Legal Information		
WAGO Licenses	WAGO Software License Agreement	user
Open Source Licenses	Open Source Licenses	user
WBM Licenses	WBM Third Party License Information	user
Trademarks Information	Trademarks Information	user
WBM Version	WBM Version Info	user
Configuration		
PLC Runtime	PLC Runtime Configuration	user
Networking		
TCP/IP Configuration	TCP/IP Configuration	user
Ethernet Configuration	Ethernet Configuration	user
Host/Domain Name	Configuration of Host and Domain Name	user
Routing	Routing	user
Clock	Clock Settings	user
Administration		
Serial Interface	Configuration of Serial Interface RS232/RS485	admin
Service Interface	Configuration of Service Interface	admin
Create Image	Create bootable Image	admin
Package Server		
Firmware Backup	Firmware Backup	admin
Firmware Restore	Firmware Restore	admin
Active System	Active System	admin
Mass Storage	Mass Storage	admin
Software Uploads	Software Uploads	admin
Ports and Services		
Network Services	Configuration of Network Services	admin
NTP Client	Configuration of NTP Client	admin
PLC Runtime Services	PLC Runtime Services	admin
SSH	SSH Server Settings	admin
DHCP Server	DHCP Server Configuration	admin
DNS	Configuration of DNS Service	user
Cloud Connectivity		
Status	Overview	admin

Table 41: Access Rights for WBM Pages

Tab/Navigation		WBM Page Title	User
	Connection 1	Configuration	admin
	Connection 2	Configuration	admin
	SNMP		
	General Configuration	Configuration of general SNMP parameters	admin
	SNMP v1/v2c	Configuration of SNMP v1/v2c parameters	admin
	SNMP v3	Configuration of SNMP v3 Users	admin
	Docker	Docker Settings	admin
	Users	WBM User Configuration	user
Fieldbus			
	OPC UA	OPC UA Configuration	admin
	BACnet		
	Status	BACnet Status	admin
	Configuration	BACnet Configuration	admin
	Storage Location	BACnet Storage Location	admin
	Files	BACnet Files	admin
Security			
	OpenVPN / IPsec	OpenVPN / IPsec Configuration	admin
	Firewall		
	General Configuration	General Firewall Configuration	admin
	Interface Configuration	Interface Configuration	admin
	MAC Address Filter	Configuration of MAC Address Filter	admin
	User Filter	Configuration of User Filter	admin
	Certificates	Certificates	admin
	Boot Mode	Boot mode configuration	admin
	TLS	Security Settings	admin
	Integrity	Advanced Intrusion Detection Environment (AIDE)	admin
	WAGO Device Access	WAGO Device Access	admin
Diagnostic			
	Log Message	Log Message Viewer	user
	Download	Download	admin
	Network Capture	Network Capture	admin

8.8.1.2 General Information about the Page

The IP address of the active device is displayed in the entry line of the browser window.

The WBM pages are only displayed after logging in. To log in, enter your username and password in the login window and click the **[Login]** button.
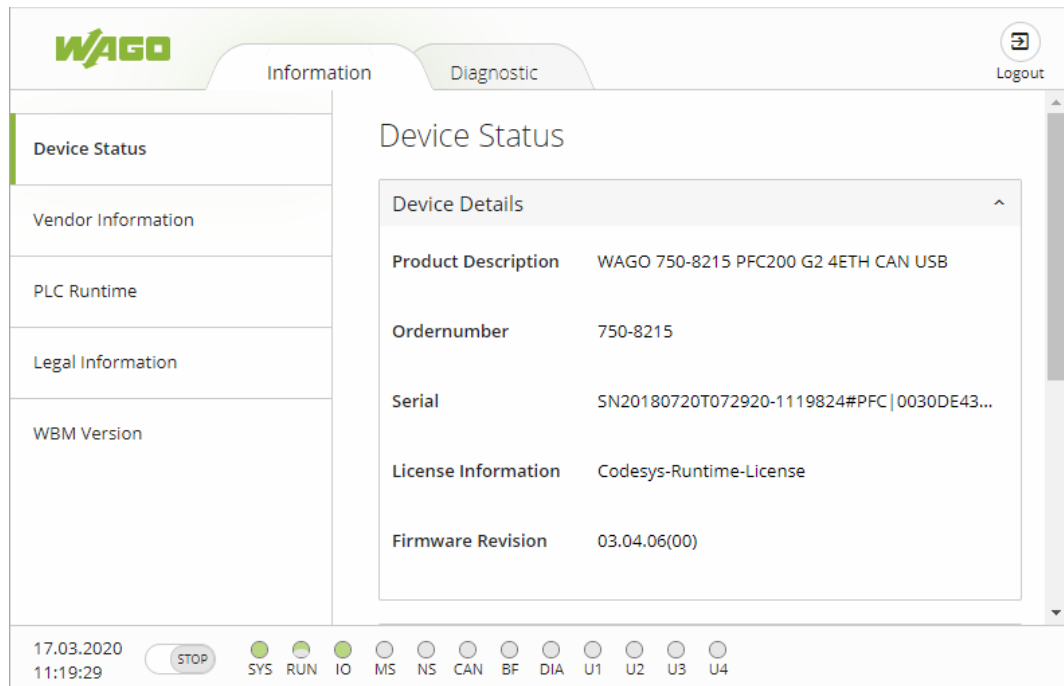
Figure 42: WBM Browser Window (Example)

The tabs for the various WBM areas and the **[Reboot]** and **[Logout]** buttons are displayed in the header of the browser window. The **[Reboot]** button only appears if you are logged in as an administrator.

If not all tabs can be displayed in the selected width of the window, a tab with ellipsis (...) is displayed instead of the tabs that cannot be displayed. This allows you to select the tabs (not shown) using a pull-down menu.
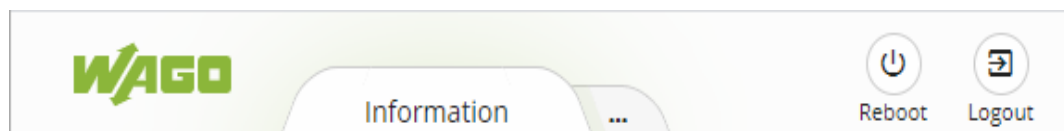
Figure 43: WBM Header with Tabs that Cannot be Displayed (Example)

The navigation tree is shown on the left of the browser window. The content of the navigation tree depends on the selected tab.
You can use this navigation tree to go to the individual pages and, where provided, subpages included in these pages.

The current device status is displayed in the status bar.
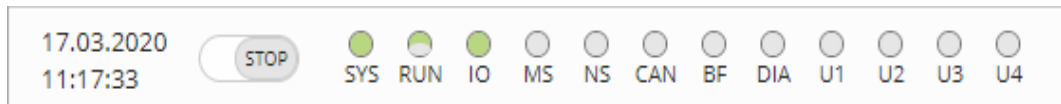
Figure 44: WBM Status Bar (Example)

- Date and Time - Local date and local time and on the device

- Setting of the mode selector switch

- LED status of the Device:
  All LEDs are graphically represented and are labeled with their particular designation (e.g., SYS, RUN, …). The following colors are possible:

  - gray: LED is off.
  - full color (green, red, yellow, orange): The LED is activated in the particular color.
  - half color:
    The LED is flashing in the corresponding color. The other half of the surface is then either gray or also colored. The latter case indicates that the LED is flashing sequentially in different colors.

  A tooltip containing more detailed information opens as long as the cursor is positioned over an LED. The text that is displayed also contains the message that put the LED into its current status. The time of the message is also shown.
  The states displayed in the WBM will not always correspond at the precise time to those on the controller. Data has a runtime during transmission and can only be queried at a certain interval. The time period between two queries is 30 seconds.

> ## Note
>
> **Do not power cycle the controller after changing any parameters!**
> Some parameter changes require a controller restart for the changes to apply.
> Saving changes takes time.
> Do not power cycle the controller to perform a restart, i.e., changes may be lost by shutting down the controller too soon.
> Only restart the controller using the software reboot function. This ensures that all memory operations are completed correctly and completely.

A description of the WBM pages and the respective parameters can be found in the appendix in Section "Configuration Dialogs" > "Web-Based Management (WBM)".

8.8.2   Configuration via Console-Based-Management-Tool (CBM) using a Terminal Program

The Console-Based Management Tool (CBM) is basically used for the initial configuration and startup of the controller via a terminal program.
Therefore, it only provides a subset of the controller parameters. For example, parameters that cannot be displayed in a terminal window in a reasonable way and are not necessary for initial startup are not displayed.

1.   Connect a PC to the ETHERNET interface X1 of the controller using an SSH terminal program.

2.   Start the terminal program.

3.   Select "SSH" as the connection type, and enter the IP address of the controller and port 22 as the connection parameters.

Alternatively, you can also connect the controller via a serial interface:

1.   Connect a PC to the X3 serial interface of the controller using a terminal program.

2.   Start the terminal program.

3.   Select "Serial" as the connection type and enter a baud rate of 115200 bauds as the connection parameter. The settings for data bits, stop bits and parity do not need to be adjusted.

4.   Log in to the Linux® system as a "super user."
      The user name and the password are provided in the Section "Users and Passwords" > "Linux® User Group."

5.   Start the configuration tool by entering the command "cbm" (case sensitive) on the command line and then press **[Enter]**.

```
=====================================================================
 WAGO Console Based Management Tool
=====================================================================
 Main Menu
 --------------------------------------------------------------------
 0. Quit
 1. Information
 2. PLC Runtime
 3. Networking
 4. Firewall
 5. Clock
 6. Administration
 7. Package Server
 8. Mass Storage
 9. Software Uploads
 10. Ports and Services
 11. SNMP
 12. PROFIBUS DP
 --------------------------------------------------------------------
 Select an entry or Q to quit
 --------------------------------------------------------------------
```

Figure 45: CBM main menu (example)

Note

Do not power cycle the controller after changing any parameters!
Some parameter changes require a controller restart for the changes to apply. Saving changes takes time.
Do not power cycle the controller to perform a restart, i.e., changes may be lost by shutting down the controller too soon.
Only restart the controller using the software reboot function. This ensures that all memory operations are completed correctly and completely.

8.8.3 Configuration using "WAGO Ethernet Settings"

The "WAGO Ethernet Settings" program enables you to read system information about your controller, make network settings and enable/disable the Web server.

→ **Note**

Observe the software version!
To configure the controller, use at least Version 6.4.1.1 dated 2015-06-29 or newer of "WAGO Ethernet Settings"!

You must select the corresponding interface after launching the "WAGO ETHERNET Settings".

A connection can be established via the service interface using configuration cable 750-923 or 750-923/000-001 or via the ETHERNET interfaces.
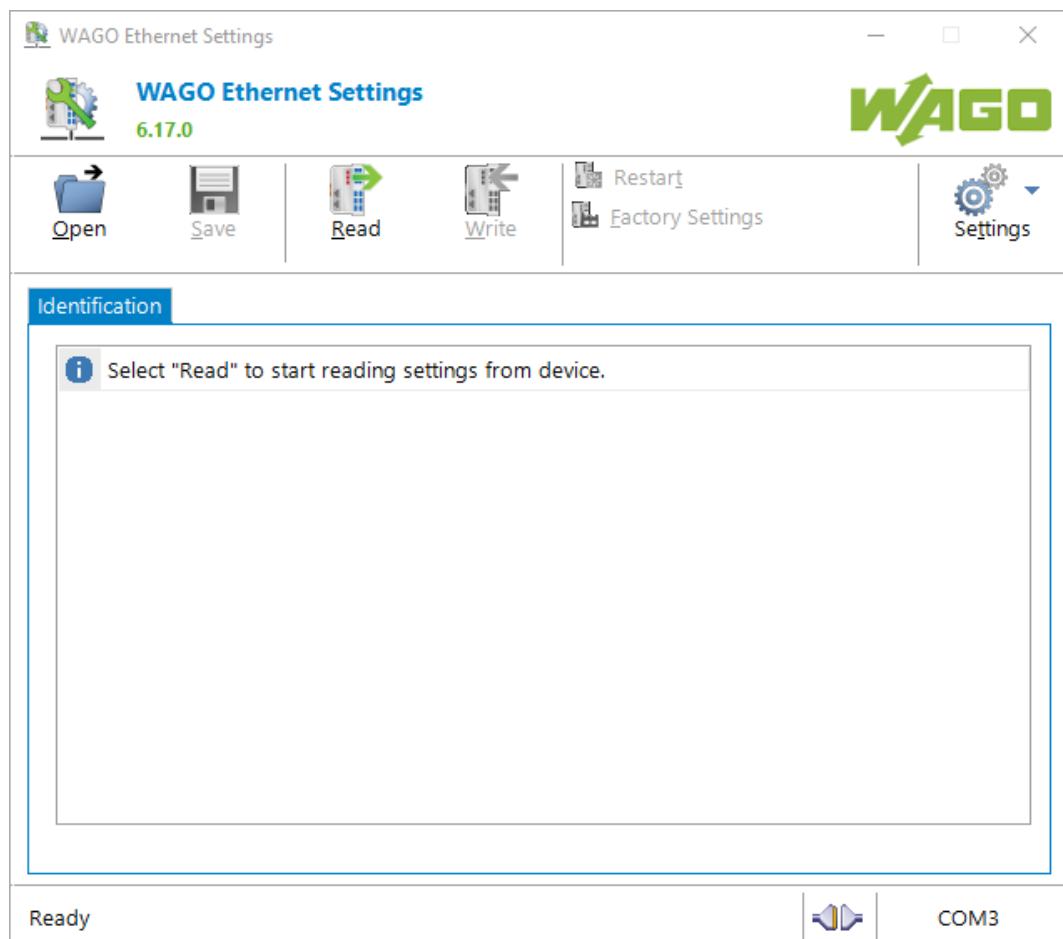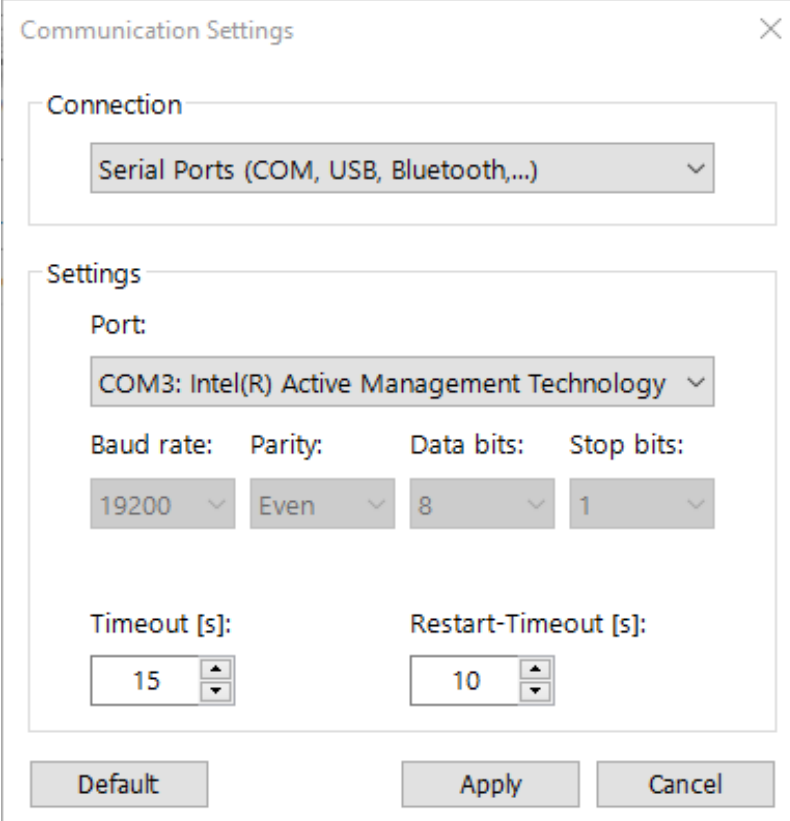
Figure 46: "WAGO Ethernet Settings" – Start Screen

For this, click "Settings" and then "Communication".

In the "Communication settings" window that then opens, adapt the settings to your needs.

Figure 47: "WAGO Ethernet Settings" – Communication Link

Once you have configured "WAGO Ethernet Settings" and have clicked **[Apply]**, connection to the controller is established automatically.

If "WAGO Ethernet Settings" has already been started with the correct parameters, you can establish connection to the controller by clicking **[Read]**.

8.8.3.1   Identification Tab

An overview of the connected device is given here.

Besides some fixed values — e.g., item No., MAC address and firmware version — the currently used IP address and the configuration method are also shown here.

Identification	Network	PLC	Status

Item Number	750-8210
Description	WAGO 750-8210 PFC200 G2 4ETH
FW Version	04.01.09(00)
HW Version	01
FWL Version	2021.10.0w04.00.00 IDX=14
Serial Number	37SUN31564010260372744+9999999999999999
MAC address	0030DE46C828
IP address	192.168.1.10 (Static Configuration)
Runtime system	CODESYS V3

Figure 48: "WAGO Ethernet Settings" – Identification Tab (Example)

8.8.3.2   Network Tab

This tab is used to configure network settings.

Values can be changed in the "Input" column, while the parameters in use are shown in the "Currently in use" column.

Figure 49: "WAGO Ethernet Settings" – Network Tab

Address Source
Specify how the controller will determine its IP address: Static, via DHCP or via BootP.

IP address, subnet mask, gateway
Specify the specific network parameters for static configuration.

> **Note**
>
> **Restricted setting for default gateways!**
> Only the default gateway 1 can be set via "WAGO Ethernet Settings."
> The default gateway 2 can only be set in the WBM!

Preferred DNS server, alternative DNS server
Enter the IP address (when required) for an accessible DNS server when identifying network names.

Time server
Specify the IP address for a time server if setting the controller's system time via NTP.

Hostname
The host name of the controller is displayed here. In the controller's initial state, this name is composed of the string "PFCx00" and the last three bytes of the

MAC address.
This standard value is also used whenever the chosen name in the "Input" column is deleted.

Domain name
The current domain name is displayed here. This setting can be automatically overwritten with dynamic configurations, e.g., DHCP.

8.8.3.3   PLC Tab
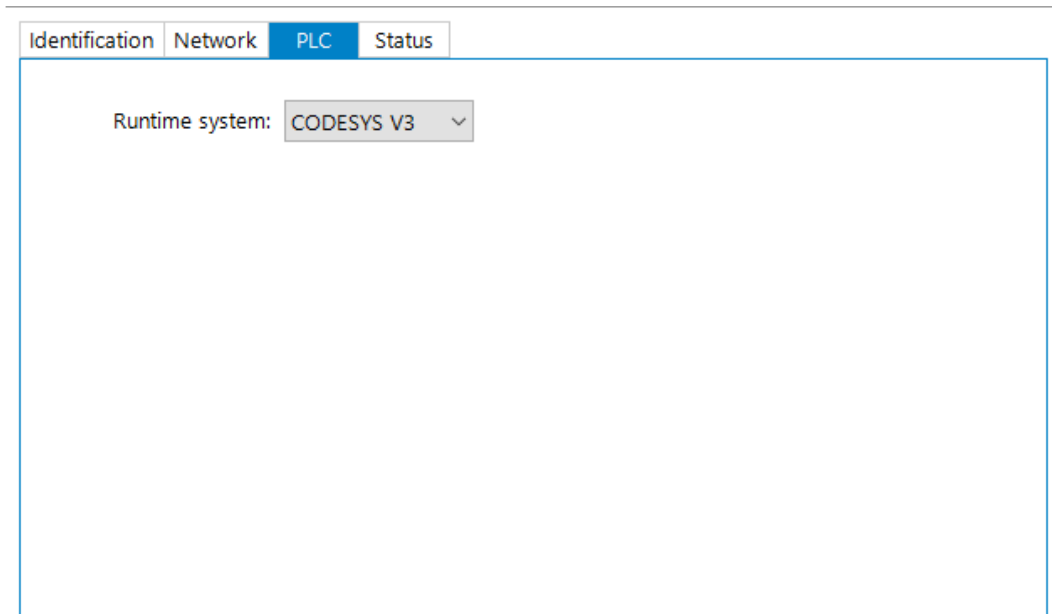
Figure 50: "WAGO Ethernet Settings" – PLC Tab

Here you can select the runtime system.

8.8.3.4   Status Tab
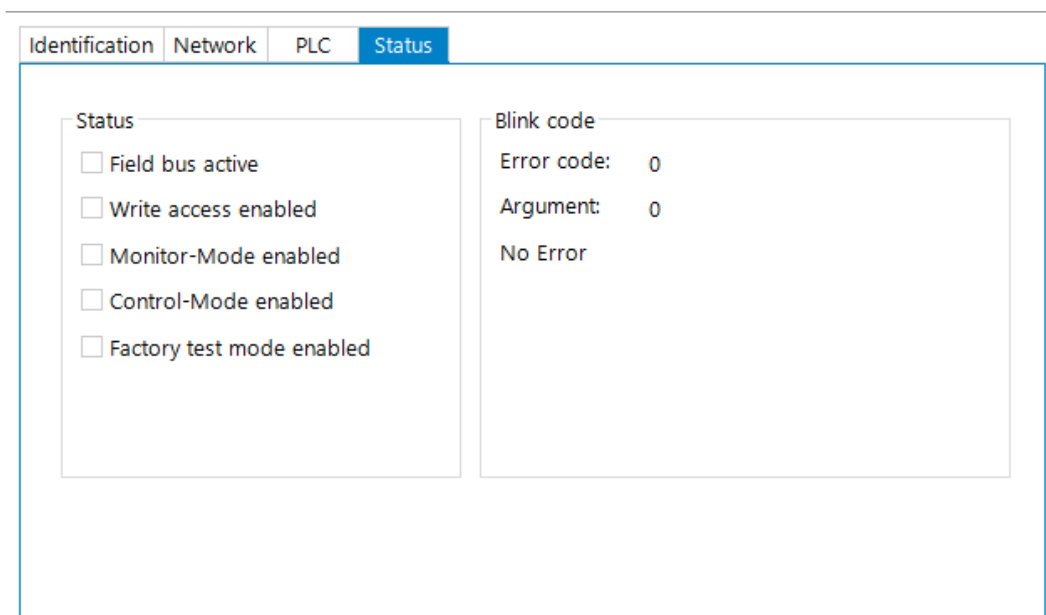
Figure 51: "WAGO Ethernet Settings" – Status Tab

General information about the controller status is displayed here.

8.8.4   Configuring with WAGO Device Access (WDA)

WAGO Device Access (WDA) is a central service in the system used for accessing the device configuration and its settings.

This service provides a REST-API via HTTP. WDA-REST-API is available at "https://<IP>/wda" or "https://<Hostname of the controller>/wda".

The English online documentation for your installed version is available at "https://<IP>/openapi/wda.openapi.html" or "https://<Hostname of the controller>/openapi/wda.openapi.html". You can call up the online documentation in the address line of your Internet browser.

9   Run-time System CODESYS V3

9.1   General Notes

> **Note**
>
> **Additional Information**
> Information on the installation, startup and programming is provided in the
> CODESYS V3 documentation.

9.2   CODESYS V3 Priorities

A list of priorities implemented for the controller is provided below as supplementary information to the CODESYS V3 documentation.

Table 42: CODESYS V3 Priorities

Scheduler	Task	Linux® Priority	IEC Priority	Remark
Preemptive scheduling - Real-time range	Local bus or fieldbus - HIGH	-95 … -86		Local bus (-88)
	Mode selector switch monitoring	-85		Task registers changes to the mode selector switch and changes the state of the PLC application. (start, stop, reset warm/cold)
	CODESYS watchdog	-83		Execution of the watchdog functions
	Cyclic and event-controlled IEC task	-55 … -53	1 … 3	For real-time tasks which must not be influenced in execution by external interfaces (e.g., fieldbus).
	Local bus or fieldbus - MID	-52 … -43		CAN (-52 … -51) PROFIBUS (-49 … -45) Modbus® slave/master (-43)
	Cyclic and event-controlled IEC task	-42 … -32	4 … 14	For real-time tasks which must not influence fieldbus communication during execution.
	Local bus or fieldbus – LOW	-13 … -4		
Fair scheduling - None real-time range	CODESYS communication	Back-ground (20)		Communication with the CODESYS development environment
	Cyclic, event-controlled and freewheeling IEC task		15	Incl. standard priority of the visualization task

9.3   Memory Spaces under CODESYS V3

The memory spaces in the controller under CODESYS V3 have the following sizes:

- •   Program memory: 32 Mbytes
- •   Data memory: 128 Mbytes
- •   Input data: 64 kbytes
- •   Output data: 64 kbytes
- •   Retain/Persistent: 128 kbytes
- •   Function block limitation: 12 * 4096 bytes = 48 kbytes

9.3.1   Program and Data Memory

The program memory (also code memory) has a maximum size of 32 MB.
The data memory has a maximum size of 128 MB.
Both areas are separate from each other and are requested when downloading to the system depending on the scope of the program. If the size limit is exceeded, it is displayed as an error.

9.3.2   Function Block Limitation

Together with the data memory to be used by the application, memory is required for the individual program function blocks in the system.

The size of the administration space is calculated from the function block limitation * 12 (i.e., 4096 Byte * 12).

The actual size of the main memory required in the system for data is the sum of global program and data memory and function block limitation memory.

9.3.3   Remanent Memory

A total of 128 kbytes of remanent memory is available for the IEC-61131 application.
The remanent area is divided into the retain area and the persistence area. The areas are automatically distributed by CODESYS V3.

10   Modbus

A direct Modbus connection is not supported by the current firmware version.

Modbus connection is possible via the CODESYS V3 functionality and the CODESYS V3 libraries.

11   CANopen Master and Slave

Based on IEC 61131-3 programming, data processing occurs on site in the controller. The process results can be output directly to the actuators, or transmitted via the bus.

Process data is exchanged with PDOs and SDOs. The controller supports 512 TX PDOs and 512 RX PDOs and 128 SDOs to send process data via the CANopen fieldbus.

In the local process image, a range of 4096 bytes serves as each input and output range for data exchange via the CANopen interface. Direct access to the I/O modules via the fieldbus is not provided.

All entries of the process image can be mapped as required to the RX PDOs and TX PDOs. The entire input and output data area can be read and written via SDOs.

After initialization, CANopen communication runs independently of the IEC application.

When used as a CANopen slave, the baud rate and the bus address can be changed according to the CANopen LSS protocol.

11.1   Object Directory

All CANopen communication and process data objects are compiled in the object directory.

The following table gives a general overview of the CANopen definition:

Table 43: Overview of Addresses in the Object Directory

Index Range	Use
0000	Not used
0001-009F	Data types
00A0-0FFF	Reserved (addresses used for other services)
1000-1FFF	Communication profile
2000-5FFF	Vendor-specific range
6000-9FFF	Up to eight standardized device profiles
A000-AFFF	Process images from IEC 61131 devices
B000-BFFF	Process images from CANopen gateways acc. CiA 302-7
C000-FFFF	Reserved

The relevant objects available on the controller are described below.

11.2   Communications Profile

0x1000 Device Type

The stack responds on the bus as the DS-405 device (IEC 61131-3 programmable device), regardless of being configured as the master or slave. As direct access to the I/O modules via the bus is prohibited, the bits for information about inputs and outputs are 0.

Entry 0x000191 = DS 405 for master and slave

0x1001 Error Register

This entry contains an 8-bit item of information about the error status. At present, bit 4 is used specifically for communication and bit 5 for the device profile. Bit 0 is set for each error.

0x1003 Pre-defined Error Field

This entry contains the list of accumulated errors which were signaled in error register 0x1001. Sub-index 0 contains the number of entries. If a new error occurs, it is added to sub-index 1 and all existing errors are moved down one sub-index. A maximum of 20 error entries is supported. If more than 20 errors occur, the error at sub-index 20 is overwritten. By writing a "0" into sub-index 0, the complete error memory is deleted.

Standard values: 0 in all entries

0x1005 COB IB Sync

This objects defines the COB ID for the synchronization message.

Default: 0x80

0x1006 Communication Cycle Period

The duration of the synchronization cycle given in µs, or 0 for cyclic synchronization. Internal resolution is 1 ms. If this value is 0, SYNC monitoring does not occur.

Default: 0

0x1008 Manufacturer Device Name

This object specifies the device name.

Entry: Item No. for the PFC200, e.g., "750-8206"

0x1009 Manufacturer Hardware Version

Entry: "V 1.0" or higher

0x100A Manufacturer Software Version

Entry: "04.02.05(00)" or higher

0x100C Node Guarding Time

The object specifies the "Guarding Time" in milliseconds. An NMT master requests the state of the NMT slave in a cyclical manner. The time between two requests is the "Guarding Time."

Default: 0 (Node guarding disabled)

0x100D Life Time Factor

The "Life Time Factor" is part of the node guarding protocol. The NMT slave checks whether it was queried within the node lifetime (guarding time multiplied by the lifetime factor). If not, the slave must assume that the NMT master is no longer in normal operation; it then initiates a "life guarding event".

Default: 0 (Node guarding off)

0x1012h COB-ID Time Stamp Object

The time stamp object enables every device's clock on the bus to be synchronized. The ID for this object is indicated here. Although the synchronization signal is not evaluated by the runtime, it may be used with library functions.

Default: 0x100 (Time Stamp Consumer)

0x1014h Emergency COB ID

An emergency message is transmitted in the event of CANopen device errors. The ID for this object is indicated here.

Default: 0x80 + Device ID

0x1015h Emergency Inhibit Time

This object specifies the minimum time that must elapse before another emergency object is sent. An entry equal to zero disables delayed sending. One time unit amounts to 100µs.

Default: 0

0x1016h Consumer Heartbeat Time

This entry can be used for monitoring of other devices on the bus. A check is made to determine whether each module defined in this object has generated a heartbeat within the set time. If the set time has been exceeded, a heartbeat event is triggered. The "Heartbeat Time" is entered in milliseconds. If the time is 0, monitoring is deactivated. The number of devices to be monitored is entered in index 0, the heartbeat time is entered in ms in the bottom 16 bits and the ID of the bus device in the 8 bits above that.

Default:

Index 0: 0 (currently still 127 = Number of possible entries)

All other entries are 0 (this function is not yet supported by the CAN master in Firmware 1.0).

0x1017h Producer Heartbeat Time

This object defines the time (in milliseconds) between two transmitted heartbeat messages. No heartbeat is sent if the time is set to 0.

Default: 0

0x1018h Identity

This object specifies the device being used. The manufacturer ID contains a unique number for each vendor. WAGO has been assigned an ID of 33.

The product code contains the device identifier.

The Rev. No. contains a specific CANopen behavior. The Major Rev. No. contains the CANopen functionality. If the functionality is changed, the Major Rev. No. is increased. You can use the Minor Rev. No. to distinguish between different versions with the same CANopen behavior.

The number is independent of the firmware revision.
When used as a CANopen slave with CODESYS 3.5, the vendor ID, product code and revision number can be freely defined in the slave configuration.

Sub-index 0 No. of entries:	4
Sub-index 1 vendor ID:	33
Sub-index 2 product_code:	e.g., 8216 for 750-8216
Sub-index 3 revision_number:	0x00010003 or higher
Sub-index 4 serial_number:	corresponds to the last 4 bytes of the MAC address.

0x1200, 0x1201 Server SDO Parameter Channels

The communication parameters for an SDO as the server are entered here. Two server SDO channels are supported.

0x1280 … 0x128E Client SDO Parameter Channels

The communication parameters for an SDO transfer as the client are entered here. 16 client SDO channels are supported.

0x1029h Error Behavior

This object defines how the slave responds in the event of an error.

Sub-index 0 No. of entries: 1

Sub-Index 1 Communication Error:

1	No change (Standard)
0	Change from operational to preoperational
2	Change to stop

0x1F51 Program Control

The status of the PLC can be read out using this object. Writing is prohibited.

Entries: 0 = Stop 1 = Run 2 = Reset 3 = Clear

11.2.1   Master Configuration

These objects are only available at the bus end when the master has been configured.

0x102A NMT Inhibit Time

This object indicates the minimum time that must elapse before another NMT telegram is sent. An entry equal to zero deactivates delayed sending. One unit of time is 100 µs.

Default: 0

0x1F80 NMT Start-up

This object contains the configuration bits for the master status. If automatic startup is deactivated, the master can be started by writing of 0x1F to this object.

0x1F81 … 0x1F8A Slave Configuration

The configured slaves are entered in these lists. All of the entries are checked when the master is started and transferred to the slaves.

0x1F81 NMT Slave-Assignment

Subindex 0:	128 = Number of possible entries
Subindex 1 … 128:	Bit 0: Slave present
	Bit 2: Slave required for start
	Bit 3: Slave reset performed on start
	Bit 8 … 15: Guard Retry Factor
	Bit 16 … 31: Guard Time
Subindex 128:	Total network (write only)

0x1F82 Request-NMT

Sub-Index 0: 127 = Number of possible entries

Sub-Index = Master Node ID NMT state of the master

0x1F84 Device Type Identification

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 … 127: Slave device type

0x1F85 Vendor Identification

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 … 127: Slave device type (not used by default)

0x1F86 Product Code

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 … 127: Slave device type (not used by default)

0x1F87 Revision number

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 … 127: Slave device type (not used by default)

0x1F88 Serial Number

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 … 127: Slave device type (not used by default)

0x1F89 Boot Time

Time in ms between the start of slaves and operational readiness of all slaves.

Default: 0 = deactivated

0x1F8A Restore Configuration

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 … 127: Bit 0 = 1 Send restore configuration to slave on start

11.3   Data Exchange

Process data exchange occurs via the communication objects with the CANopen fieldbus controller.

Each object consists of a CAN telegram with a maximum of 8 bytes process data and a COB (Communication Object Identifier) ID that is unique within the network.

These communication objects transmit data, trigger events, signal error statuses, etc.

The parameters required for the communication objects, as well as CANopen device parameters and data are stored in an object directory.

11.3.1   Controller Communication Objects

The PFC200 supports the following communication objects:

512 Tx-PDOs for process data exchange from input data of the fieldbus node

512 Rx-PDOs for process data exchange from output data of the fieldbus node

Synchronization objects (SYNC) for network synchronization

Emergency objects (EMCY)

Network management objects

-       Module Control Protocols

-       Error Control Protocols

-       Boot-up Protocol

11.3.2   Fieldbus-Specific Addressing

The CODESYS variable for the CAN bus are mapped to an object directory after configuring the CAN interface as a master or slave (initialization). A CANopen fieldbus device uses the 16-bit indices and 8-bit sub-indices of the object directory to address data via PDOs or SDOs and to access the data. The position of the data in the process image is therefore not directly significant for the CANopen user at the fieldbus end.

The variables entered into the object directory are distinguished by data type (Integer8, Unsigned8, Boolean, Integer16, etc.) and by input/output. Access via PDOs can be either for reading or writing.

As CANopen does not transfer data by bits, the variable data is combined from a Boolean data type to bytes and assigned to the corresponding index; Boolean input variable data is assigned to index 0xA080, Boolean output variable data to index 0xA500.

Variable data that has a data width of 1 byte or more is assigned to the corresponding indices in a similar manner.

→ **Note**

Observe the direction of data flow!
The IEC 61131-3 input variables are defined from the perspective of the CAN bus. These are output variables from the perspective of the PFC. Accordingly, the IEC 61131-3 output variables are input variables for the PFC.

This table provides an overview of the indices of "IEC 61131-3" variables.

Table 44: Indexing of "IEC 61131-3" Variable Data in the Object Directory

Data Type	IEC 61131-3 Output Variables	IEC 61131-3 Input Variables
	Index	
Integer8	0xA000	0xA480
Unsigned8	0xA040	0xA4C0
Boolean	0xA080	0xA500
Integer16	0xA0C0	0xA540
Unsigned16	0xA100	0xA580
Integer24	0xA140	0xA5C0
Unsigned24	0xA180	0xA600
Integer32	0xA1C0	0xA640
Unsigned32	0xA200	0xA680
Float32	0xA240	0xA6C0
Unsigned40	0xA280	0xA700
Integer40	0xA2C0	0xA740
Unsigned48	0xA300	0xA780
Integer48	0xA340	0xA7C0
Unsigned56	0xA380	0xA800
Integer56	0xA3C0	0xA840
Integer64	0xA400	0xA880
Unsigned64	0xA440	0xA8C0

Using the associated indices for data types with a data width of 1 byte (Integer8, Unsigned8 and Boolean), read-only byte-by-byte access is possible from the fieldbus to data in the controller memory.

The sub-index is utilized to select a specific byte.

In contrast, when the indices for larger data blocks are used, several bytes can be accessed simultaneously.
For example, the described PFC output variable data can be accessed in a word-by-word manner using the index for Integer16 (0xA0C0) or for Unsigned16 (0xA100), three bytes can be accessed using index 0xA140 for Integer24, etc.

Example:

The first three bytes of the PFC output data for the data type integer or unsigned are accessed from the fieldbus:

Table 45: Fieldbus Access to PFC Output Data

Access	PFC Output Data	Reading with Index (Integer / Unsigned)	Sub-Index
By byte (with Integer8 / Unsigned8)	Byte 6000	(0xA000 / 0xA040)	1
	Byte 6001	(0xA000 / 0xA040)	2
	Byte 6002	(0xA000 / 0xA040)	3
By word (with Integer16 / Unsigned16)	Word 3000 (Byte 6000/6001)	(0xA0C0 / 0xA100)	1
	Word 3001 (Byte 6002/6003)	(0xA0C0 / 0xA100)	2
3 bytes (with Integer24 / Unsigned24)	Bytes 6000 … 6002	(0xA140 / 0xA180)	1

The following tables give an overview of addressing data with different data widths.

In this case, the corresponding indexing is assigned to the memory space for fieldbus variables (byte 6000 to byte 9999) as a function of the data width.

The indexing indicated in the tables continues up to the respective maximum index and sub-index.

Note

Observe the direction of data flow!
The PFC output variables are defined from the perspective of the controller; from the perspective of the CAN fieldbus these are input variables. Accordingly, the PFC input variables for IEC 61131-3 access are output variables for the fieldbus.

Thus: IEC 61131-3 input variable = PFC output variable

PFC input variable = IEC 61131-3 input variable.
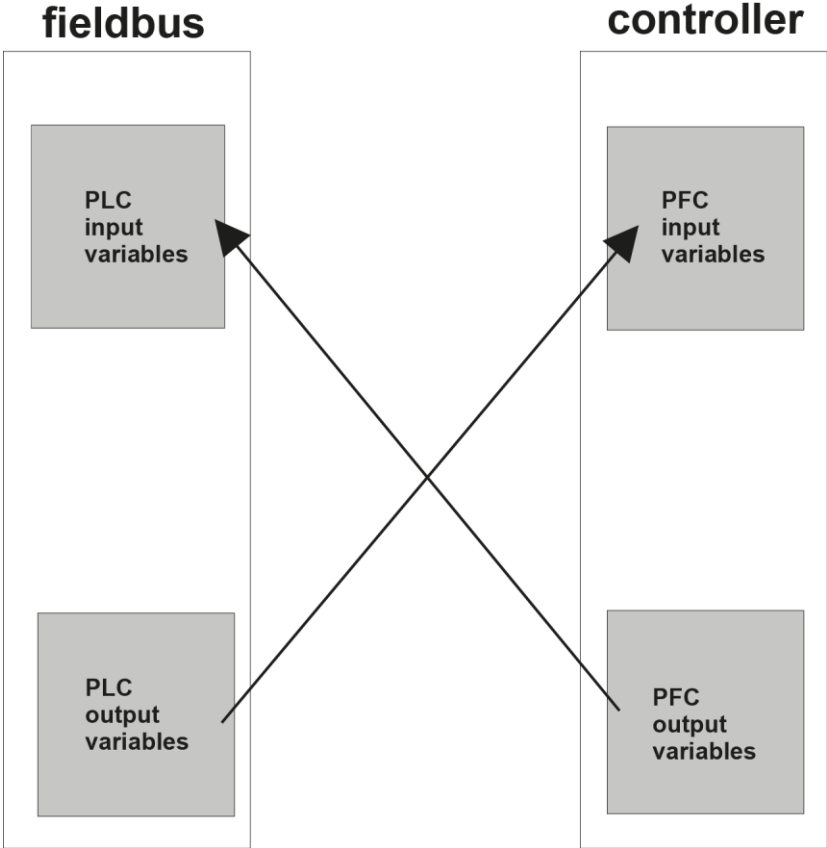
Figure 52: Correlation Between "IEC 61131-3" Variables and PFC Variables

11.3.3   Examples for the Definition of PFC Fieldbus Variables

The examples below show the allocation of several definitions for PFC variables with different data types to the associated object directory entries.

11.3.3.1   CODESYS Access to PFC Variables

Table 46: Examples for CODESYS Access to PFC Variables

Data Type of PFC Variables	PFC Input Variables		PFC Output Variables	
	Definition based on IEC 61131-3	Index/sub-index	Definition based on IEC 61131-3	Index/sub-index
Unsigned8	InByte0 AT %IB6000: BYTE;	0xA4C0/1	OutByte0 AT %QB6000: BYTE;	0xA040 /1
	InByte0 AT %IB6001: BYTE;	0xA4C0/2	OutByte0 AT %QB6001: BYTE;	0xA040 /2
Integer16	InInt0 AT %IW3000: INT;	0xA540 /1	OutInt0 AT %QW3000: INT;	0xA0C0/1
	InInt1 AT %IW3001: INT;	0xA540 /2	OutInt1 AT %QW3001: INT;	0xA0C0/2
Unsigned16	InWord0 AT %IW3000: WORD;	0xA580 /1	OutWord0 AT %QW3000: WORD;	0xA100 /1
	InWord0 AT %IW3001: WORD;	0xA580 /2	OutWord0 AT %QW3001: WORD;	0xA100 /2
Unsigned32	InDWord0 AT %ID1500: DWORD;	0xA680 /1	OutDWord0 AT %QD1500: DWORD;	0xA200 /1
	InDWord0 AT %ID1501: DWORD;	0xA680 /2	OutDWord0 AT %QD1501: DWORD;	0xA200 /2

11.3.3.2   Maximum Indices

The maximum indices and sub-indices are yielded from the memory size of the fieldbus controller at 4096 bytes and the corresponding data width for the data types.

The table below provides an overview of the maximum indices and sub-indices of the IEC 61131-3 variables.

Table 47: Maximum Indices and Sub-Indices for "IEC 61131-3" Variables

Data Type	IEC 61131-3 Input Variables		IEC 61131-3 Output Variables	
	Max. index	Max. sub-index	Max. index	Max. sub-index
Integer8	0xA00F	0xFF	0xA487	0xFF
Unsigned8	0xA04F	0xFF	0xA4C7	0xFF
Boolean	0xA08F	0xFF	0xA507	0xFF
Integer16	0xA0C7	0xFF	0xA543	0xFF
Unsigned16	0xA107	0xFF	0xA583	0xFF
Integer24	0xA145	0x55	0xA5C0	0x55
Unsigned24	0xA185	0x55	0xA600	0x55
Integer32	0xA1C3	0xFF	0xA643	0xFF
Unsigned32	0xA203	0xFF	0xA683	0xFF
Float32	0xA243	0xFF	0xA6C3	0xFF
Unsigned40	0xA283	0x33	0xA703	0x33
Integer40	0xA2C3	0x33	0xA743	0x33
Unsigned48	0xA302	0xAA	0xA780	0xAA
Integer48	0xA342	0xAA	0xA7C0	0xAA
Unsigned56	0xA382	0x49	0xA802	0x49
Integer56	0xA3C2	0x49	0xA842	0x49
Integer64	0xA401	0xFF	0xA880	0xFF
Unsigned64	0xA441	0xFF	0xA8C0	0xFF

Example:

514 bytes of output variables are addressed by word by the data type Unsigned16.

Addressing of 257 data words then occurs with:

- Index 0xA580, sub-index 1 to 255
- Index 0xA581, sub-index 1 and 2.

Table 48: Example of "IEC 61131-3" Output Variables

Index	Sub-Index	Contents	Description
0xA580	1	D1 *)	1st output variable block
	2	D2 *)	2nd output variable block
	...	...	...
	255	D255 *)	255th output variable block
0xA581	1	D256 *)	256th output variable block
	2	D257 *)	257th output variable block

*) D1 = Data word output variable 1, D255 = Data word output variable 255, etc.

11.3.4 Using the CANopen Slave (Device) under CODESYS V3

The CODESYS 3.5 slave configurator uses other object addresses for the process data than defined in the CANopen CiA 405 standard for IEC 61131 devices. Therefore, when operating as a CODESYS V3 slave, these CODESYS V3 object numbers are used:

0x3000 .. 0x31FF	Receive process data (master => slave)
0x3800 .. 0x39FF	Send process data (slave => master)
0x5000 .. 0x507F	SDO read/write access
0x5800 .. 0x587F	SDO read access

A more detailed description on how to use the CANopen interface is provided in the CODESYS V3 online manual. The WAGO-specific functions can be used via the WagoAppCanOpen and WagoAppCanLayer2 libraries.

11.3.5   Use as a CAN Layer 2 Device

As an alternative to the CANopen master or slave function, a pure Layer2 stack is also available on the PFC. This can be used when no CANopen functions are required. It offers higher data throughput with a lower CPU load.

It is possible to set 127 receive filters with a total buffer of 127 telegrams or to use an unfiltered receive buffer of 255 telegrams.

The WAGO CanLayer2 device is selected on CAN for use with CODESYS V3. This functionality is used via the WagoAppCanLayer2 library.

12   Diagnostics

12.1   Operating and Status Messages

The following tables contain descriptions of all operating and status messages for the controller which are indicated by LEDs.

12.1.1   Power Supply LEDs
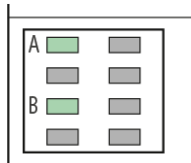
Figure 53: Power Supply Indicating Elements

12.1.1.1   A LED

The A LED (system power supply) indicates following diagnostics:

Table 49: System Power Supply Diagnistics

Status	Explanation	Solution
Green	24V system power supply voltage present	---
Off	No 24V system power supply voltage present	Switch on the power supply. Check the supply voltage.

12.1.1.2   B LED

The B LED (field-side power supply) indicates following diagnostics:

Table 50: Field-Side Supply Diagnostics

Status	Explanation	Solution
Green	24V field-side supply voltage present	---
Off	No 24V field-side supply voltage present	Switch on the power supply. Check the supply voltage.

12.1.2   System/Fieldbus LEDs

U6 ▮▮ ▮▮ SYS
U5 ▮▮ ▮▮ RUN
U4 ▮▮ ▮▮ I/O
U3 ▮▮ ▮▮ MS
U2 ▮▮ ▮▮ NS
U1 ▮▮ ▮▮ CAN

Figure 54: Indicating elements for fieldbus/system

12.1.2.1   SYS LED

The SYS LED indicates following diagnostics:

Table 51: Diagnostics via SYS LED

Status	Explanation	Remedy
Green	Ready to operate - System start completed without errors	---
Orange	Device is in startup/boot process and the RST button is not pressed.	---
Orange flashing	"Fix IP Address" mode, temporary setting until the next reboot	Connect to the device via the standard address (192.168.1.17) or restart the device to restore the original value set.
Green/red flashing	Firmware update mode	---
Orange/red flashing	No license; evaluation period not yet expired	Activate the associated licenses before the evaluation period ends, or remove the libraries or device functions from your application. The device has unrestricted functionality until the evaluation period ends.
Red flashing	No license; evaluation period has expired	Activate the associated licenses promptly, or remove the libraries or device functions from your application. Otherwise, the application can no longer be started after being downloaded again or started as a boot application after the device is restarted.

WAGO

12.1.2.2 RUN LED

The RUN LED indicates following diagnostics:

Table 52: RUN LED Diagnostics

Status	Explanation	Remedy
Green	Applications loaded and all in the "RUN" status	---
Green flashing	No application and now boot project loaded	Load an application or boot project.
Red	Applications loaded and all in the "STOP" status	Set the mode selector switch to "RUN" to start the application.
Green/red flashing	At least one application in the "RUN" status and one in the "STOP" status	Start the stopped application.
Red, goes out briefly	Warm start reset completed	---
Red, goes out longer	Cold start reset completed	---
Red, flashing	At least one application after in the "STOP" status after exception (e.g., memory access error)	Start the application with a reset via the mode selector switch or in the connected IDE. If the application cannot be started, restart the controller. Contact WAGO Support if the error occurs again.
Orange/green flashing	Load above threshold value 1	Try to reduce the load on the system: - Change the CODESYS program. - End any fieldbus communication that is not essential, or reconfigure the fieldbuses. - Remove any non-critical tasks from the RT area. - Select a longer cycle time for IEC tasks.
Orange	Runtime system in debug state (breakpoint, single step, individual cycle)	Resume the application in the connected IDE with single step or start. Remove the breakpoint if necessary. If the connection has been interrupted, set the mode selector switch to "STOP" and then back to "RUN" to enable the application to continue
OFF	No runtime system loaded	Enable a runtime system, e.g., via the WBM.

12.1.2.3 I/O LED

The I/O LED indicates following diagnostics:

Table 53: Diagnostics I/O LED

Status	Explanation	Solution
Green	Data cycle on the local bus, normal operating status.	---
Orange flashing	Startup phase; the local bus is being initialized. The startup phase is indicated by rapid flashing for about 1 ... 2 seconds.	Wait until initialization has been completed.
Red	A hardware fault is present.	Contact WAGO Support.
Red flashing (2 Hz)	An error which may be able to be eliminated is present.	First, try to eliminate the error by switching the device (power supply) off and then back on. Check the entire node structure for any errors. If you cannot eliminate the error, contact WAGO Support.
Red flashing (flashing sequence)	A local bus error is present.	An explanation of the flashing sequence is given in the section "Diagnostics Messages via Flashing Sequences".
Off	A library was not loaded, or a library function was not called up.	Restart the device. If you cannot eliminate the error, contact WAGO Support.

12.1.2.4   MS LED

The MS LED indicates following diagnostics:

Table 54: MS-LED Diagnostics

Status	Explanation	Remedy
Off	No error	---
Red flashing (flashing sequence)	A configuration error exists.	An explanation of the flashing sequence is given in the section "Diagnostics via Flashing Sequences."

12.1.2.5 CAN LED

The CAN LED indicates following diagnostics:

Table 55: Diagnostics CAN LED

Status	Explanation	Solution
Off	The CAN interface has not been configured	---
Alternating red 50 ms / green 50 ms	Configuration in progress	---
Alternating red 200 ms / green 200 ms	Configuration invalid	Check the configuration in the CODESYS Configurator.
Green 200 ms / off 800 ms	The CANopen interface has the status "Stop".	---
Green 200 ms / off 200 ms	The CANopen interface has the status "Preoperational".	---
Green	The CANopen interface has the status "Operational".	---
Red	The CANopen interface has the status "Bus Off" (short-circuit or other major fault).	Check the bus connections and the baud rate.
Error in the status "Preoperational"		
1* red flashing / 2 * green flashing	"Bus Warning Level" exceeded.	Check the wiring for the CAN bus.
2* red flashing / 2 * green flashing	"Guarding Error", slave incorrectly configured or not available.	Check the slaves and the configuration.
3* red flashing / 2 * green flashing	"Sync Error"	Change the time interval for the synchronization message.
Error in the status "Operational"		
1* red flashing / green 800 ms on	"Bus Warning Level" exceeded.	Check the wiring for the CAN bus.
2* red flashing / green 800 ms on	"Guarding Error"	Check the slaves and the configuration.
3* red flashing / green 800 ms on	"Sync Error"	Change the time interval for the synchronization message.

12.1.3   Network Connection LEDs
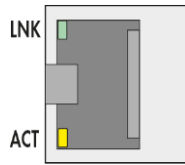
Figure 55: Indicating Elements, RJ-45 Jacks

12.1.3.1   LNK LED

The LNK LED indicates following diagnostics:

Table 56: LNK-LED Diagnostics

Status	Explanation	Remedy
Off	10 Mbit/s	---
Green	100 Mbit/s	---

12.1.3.2   ACT LED

The ACT LED indicates following diagnostics:

Table 57: ACT-LED Diagnostics

Status	Explanation	Remedy
Off	No network communication via port	Check network connections and network settings.
Yellow flashing	Network communication via port	---

12.1.4   Memory Card Slot LED
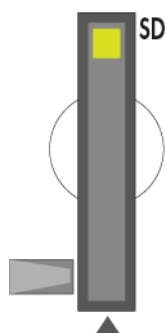
Figure 56: Indicating Elements, Memory Card Slot

The memory card slot LED indicates following diagnostics:

Table 58: Diagnostics via Memory Card Slot LED

Status	Explanation	Remedy
Off	No memory card access	---
Yellow	Memory card access	---
Yellow flashing		

12.2   Diagnostics Messages via Flashing Sequences

12.2.1   Flashing Sequences

A diagnosis (fault/error) is always displayed as three flashing sequences in a cyclic manner:

1.   The first flashing sequence (flickering) initiates reporting of the fault/error.

2.   After a short break (approx. 1 second), the second flashing sequence starts. The number of blink pulses indicates the **error code**, which describes the type of error involved.

3.   After a further break the third flashing sequence is initiated. The number of blink pulses indicates the **error argument**, which provides an additional description of the error, e.g., which of the I/O modules connected to the controller exhibits an error.
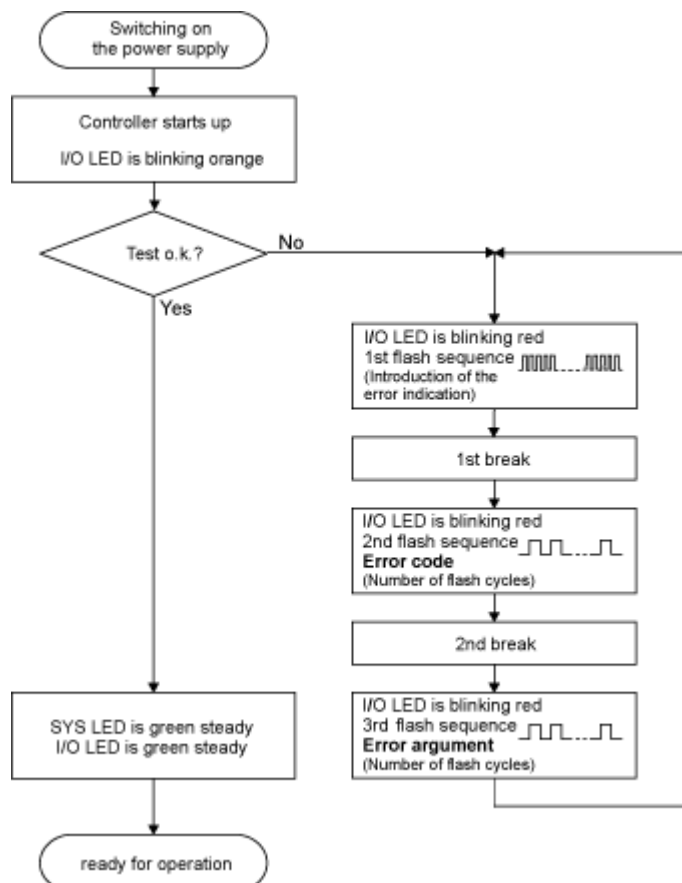
Figure 57: Flashing Sequence Process Diagram

12.2.2   Example of a Diagnostics Message Indicated by a Flashing Sequence

The example below illustrates the representation of a diagnostics message via a flashing sequence. The I/O LED indicates a data error on the local bus. The data error is caused by the removal of an I/O module located at the 6th position of the bus node.

Initiation of the Start Phase

1.   The I/O LED flashes for 1 cycle at about 10 Hz (10 flashes/second).

2.   This is followed by a pause of about one second.

Error Code 4: Data Error in the Local Bus

3.   The I/O LED flashes for 4 cycles of about 1Hz.

4.   This is followed by a pause of about 1 second.

Error Argument 5: I/O Module at the 6th Slot

5.   The I/O LED flashes for 5 cycles at 1 Hz.
      This indicates that a disruption has occurred at the local bus downcircuit of the 5th I/O module.

6.   The blink code starts flickering when the start phase is initiated again. If there is only one error, this process is repeated.

12.2.3   Meaning of Blink Codes and Procedures for Troubleshooting

This section describes the diagnostics presented as blink codes via the I/O LEDs.

If the diagnostics cannot be cleared by the measured specified for them, contact WAGO support. Be ready to explain to them the blink code that is displayed.

Phone: +49 571 887 44 55 5
Fax: +49 571 887 84 45 55
E-mail: support@wago.com

Table 59: Overview of Error Codes, I/O LED

Error code	Explanation
1	Hardware and configuration error
2	Configuration error
3	Local bus protocol error
4	Physical error on the local bus
5	Local bus initialization error
6	Not used
7	Not supported I/O module
8	Not used
9	CPU exception error

Table 60: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
-	Invalid parameter checksum for local bus interface	- Switch off the power to the controller and replace it. - Then switch the power back on.
1	Internal buffer overflow (max. amount of data exceeded) during inline code generation.	- Switch off the power to the controller. - Reduce the number of I/O modules. - Switch the power back on.
2	Data type of the I/O module(s) is not supported	- Update the controller firmware. If this error persists, there is an error in the I/O module. Identify the error as follows: - Switch off the power supply. - Place the end module in the middle of the I/O modules connected to the system. - Switch the power back on. - If the I/O flashes red switch off the power supply again and place the end module in the middle of the first half of the I/O modules (toward the controller). - If the LED is no longer flashing, switch off the power supply and place the end module in the middle of the second half of the I/O modules (away from the controller). - Switch the power back on. - Repeat this procedure until you establish which I/O module is defective. Then replace that module.
3	Unknown module type of the flash program memory	- Switch off the power to the controller and replace it. - Then switch the power back on.
4	Error occurred while writing to the flash memory	- Switch off the power to the controller and replace it. - Then switch the power back on.
5	Error occurred while erasing a flash sector	
6	The I/O module configuration after a local bus reset differs from the one after the last controller startup.	- Restart the controller by first switching off the power supply and then switching it back on, or by pressing the Reset button on the controller.

Table 60: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
7	Error occurred while writing to the serial EEPROM	- Switch off the power to the controller and replace it. - Then switch the power back on.
8	Invalid hardware/ firmware combination	
9	Invalid checksum in the serial EEPROM	
10	Fault when initializing the serial EEPROM.	
11	Error occurred while reading from the serial EEPROM	- Switch off the power supply to the controller and reduce the number of I/O modules. - Then switch the power back on.
12	Time to access the serial EEPROM exceeded	- Switch off the power to the controller and replace it. - Then switch the power back on.
14	Maximum number of gateway or mailbox modules exceeded.	- Switch off the power to the controller. - Reduce the number of gateway or mailbox modules. - Then switch the power back on.
16	Maximum number of I/O modules exceeded	- Switch off the power to the controller. - Reduce the number of I/O modules. - Then switch the power back on.

Table 61: Error Code 2, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
2	Maximum size of the process image exceeded	- Switch off the power to the controller. - Reduce the number of I/O modules. - Switch the power back on.

Table 62: Error Code 3, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
--	Local bus communication error; defective I/O module cannot be identified	If a power supply module (e.g., 750-602) is connected to the controller, ensure that this module functions properly (see Section "LED Signaling"). If the supply module does not exhibit any errors/faults, the I/O module is defective. Identify the defective I/O module as follows: - Switch off the power supply. - Place the end module in the middle of the I/O modules connected to the system. - Switch the power back on. - If the I/O LED continues to flash red switch off the power supply again and place the end module in the middle of the first half of the I/O modules (toward the controller). If only one I/O module is left and the LED continues to flash, either this module or the controller local bus interface is defective. Replace the defective module or the controller. - If the LED is no longer flashing, switch off the power supply and place the end module in the middle of the second half of the I/O modules (away from the controller). - Switch the power back on. - Repeat this procedure until you establish which I/O module is defective. Then replace that module.

Table 63: Error Code 4, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
--	Maximum permissible number of I/O modules exceeded.	- Switch off the power to the controller. - Reduce the number of I/O modules to an acceptable value. - Switch the power back on.
n*	Local bus disruption after the nth process data module.	- Switch off the power to the controller. - Replace the $(n+1)^{th}$ process data module. - Switch the power back on. I/O modules that do not provide any data are ignored (e.g., supply module without diagnostics).

Table 64: Error Code 5, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
n*	Register communication error during local bus initialization	- Switch off the power to the controller. - Replace the $(n+1)^{th}$ process data module. - Switch the power back on. I/O modules that do not provide any data are ignored (e.g., supply module without diagnostics).

Table 65: Error Code 7, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
n	First unsupported I/O module in place of n.	- Switch off the power to the controller. - Replace the nth I/O module containing process data or reduce the number of modules to the number of n-1. - Switch the power back on.

Table 66: Error Code 9, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
1	Invalid program statement	Malfunction of the program sequence: - Contact WAGO Support.
2	Stack overflow	Malfunction of the program sequence: - Contact WAGO Support.
3	Stack underflow	Malfunction of the program sequence: - Contact WAGO Support.
4	Invalid event (NMI)	Malfunction of the program sequence: - Contact WAGO Support.
5	Local bus watchdog has triggered.	For CODESYS V3 applications: - Check the system load by IEC tasks with priorities 1 ... 14 in the runtime system (see Section "CODESYS V3" Runtime Environment > "CODESYS V3 Priorities"). For C applications: - Check the time monitoring settings.

12.2.4   Meaning of Blink Codes and Procedures for Troubleshooting

This section describes the diagnostics presented as blink codes via the MS LEDs.

If the diagnostics cannot be cleared by the measured specified for them, contact WAGO support. Be ready to explain to them the blink code that is displayed.

Phone: +49 571 887 44 55 5
Fax: +49 571 887 84 45 55
E-mail: support@wago.com

Table 67: Overview of MS-LED Error Codes

Error Code	Explanation
1	Configuration error

Table 68: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
5	Error when synchronizing the controller configuration with the local bus	- Check the information of the connected I/O modules in the CODESYS controller configuration. - Adjust this to match the I/O module that is actually inserted. - Recompile the project. - Reload the project into the controller.

13   Service

13.1   Inserting and Removing the Memory Card

13.1.1   Inserting the Memory Card

1.   Use an actuating tool or a screwdriver to open the transparent cover flap by flipping it upwards. The point where to position the tool is marked with an arrow.

2.   Hold the memory card so that the contacts are visible on the right and the diagonal edge is at the top, as depicted in the figure below.

3.   Insert the memory card in this position into the slot provided for it.

4.   Push the memory card all the way in. When you let go, the memory card will move back a little and then snap in place (push-push mechanism).

5.   Close the cover flap by flipping it down and pushing it in until it snaps into place.

6.   You can seal the closed flap through the hole in the enclosure next to the flap.
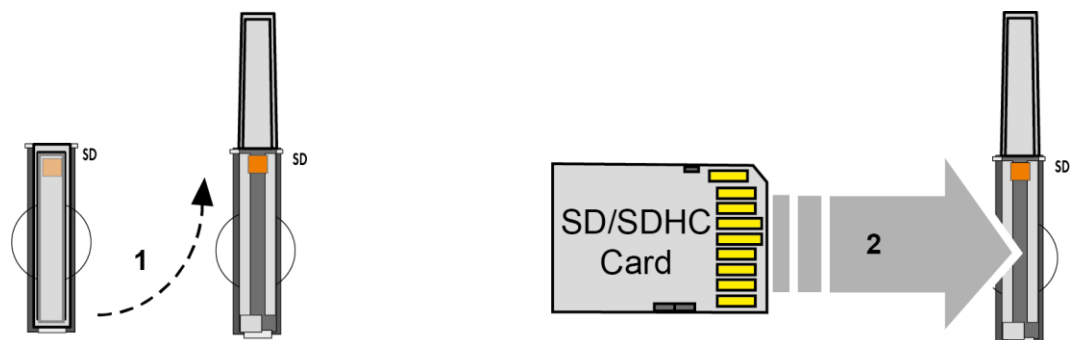
Figure 58: Inserting the Memory Card

13.1.2   Removing the Memory Card

1.   First, remove any seal that may be in place.

2.   Use an actuating tool or a screwdriver to open the transparent cover flap by flipping it upwards. The point where to position the tool is marked with an arrow.

3.   To remove the memory card you must first push it slightly into the slot (push-push mechanism). This releases the mechanical locking mechanism.

4.   As soon as you let go of the memory card, the memory card is pushed out a bit and you can remove it.

5.   Remove the memory card.

6. Close the cover flap by flipping it down and pushing it in until it snaps into place.

13.2 Firmware Changes

NOTICE

Do not switch the controller off!
The controller can be damaged by interrupting the factory reset process.
Do not switch the controller off during the factory reset process, and do not
disconnect the power supply!

Note

Obtain documentation appropriate for the firmware target version!
A firmware change can modify, remove or add controller properties and
functions. As a result, described properties or functions of the controller may not
be available or available properties or functions may not be described in the
documentation.

Therefore, use only documentation appropriate for the target firmware after a
firmware change.

If you have any questions, feel free to contact our WAGO Support.

Note

Note the firmware version
For devices with a factory installation of a firmware >= FW 05, a simple
downgrade to a version <= FW 04 is not possible!
Use a special downgrade image.

You can update the firmware in two different ways using:

• WAGOupload

• Memory card and WBM

13.2.1   Use WAGOupload to Update/Downgrade the Firmware

1.   Launch WAGOupload.

2.   Click the **[Update Firmware]** action.

3.   In the "Select Target Controllers" dialog, enter the IP address of your controller in the "Transfer via TCP/IP" option.

4.   Click **[Find Controller]**.

     Your controller is now displayed in the list.

5.   Select the displayed controller and click **[Next]**.

6.   In the "Select Update File" dialog, select the *.wup firmware file for the required firmware.

7.   Click **[Next]**.

8.   Click **[Next]** to confirm the summary.

9.   Wait until the operation ends with a status message and only then click **[Exit]** to close the window.

The newly installed firmware is now available on your controller.

13.2.2   Perform Firmware Update/Downgrade

Proceed as follows if you want to update the controller to a later firmware version or to downgrade the controller to an earlier firmware version:

1.   Copy the firmware image (*.img file) of the required firmware to the memory card using a suitable PC tool.

2.   Save your application and the controller settings.

3.   Switch off the controller.

4.   Insert the memory card with the new firmware image into the memory card slot. Use a special downgrade image if necessary (see above).

5.   Switch on the controller.

6.   After booting the controller, launch the WBM "Create Boot Image" page (you may have to temporarily change the IP address).

7.   Create a new boot image on the internal memory.

8.   Switch off the controller after completing the process.

9.   Remove the memory card.

10.   Switch on the controller.

The controller can now be started with the new firmware version.

13.3   Updating Root Certificates

If you want to update the root certificates on the controller, proceed as follows:

1.   Download the current root CA bundle from https://curl.haxx.se/ca to your PC.

2.   Rename the file "ca-certificates.crt."

3.   Transfer the file to the /etc/ssl/certs directory on the controller with an SFTP or FTP client.

4.   Restart the controller. To do so, use the reboot function in WBM or CBM.

14   Removal

> ⚠ **CAUTION**
>
> **Risk of injury due to sharp-edged blade contacts!**
> The blade contacts are sharp-edged. Handle the I/O module carefully to prevent
> injury. Do not touch the blade contacts.

14.1   Removing Devices

> ⚠ **DANGER**
>
> **Do not work when devices are energized!**
> High voltage can cause electric shock or burns.
> Switch off all power to the device prior to performing any installation, repair or
> maintenance work.

14.1.1   Removing the Controller

1.   Use a screwdriver blade to turn the locking disc until the nose of the locking
      disc no longer engages behind the carrier rail.

2.   Remove the controller from the assembly by pulling the release tab.

Electrical connections for data or power contacts to adjacent I/O modules are
disconnected when removing the controller.
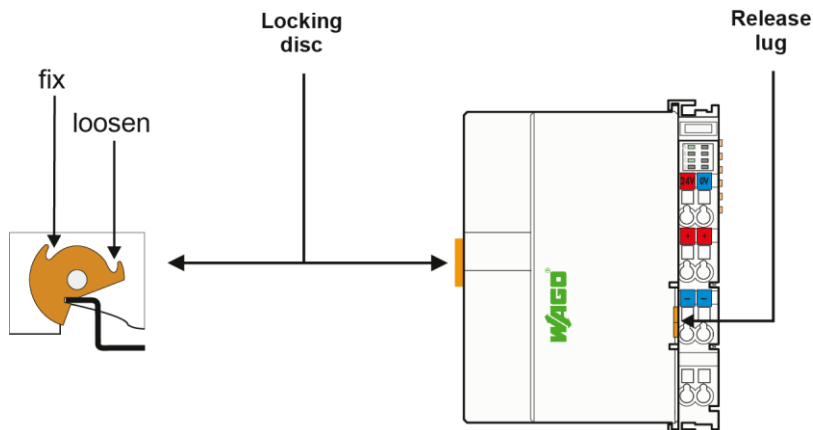
Figure 59: Release Tab of Controller (Example)

> **Note**
>
> **Do not take the controller enclosure apart!**
>
> The enclosure sections are firmly joined. The feed-in section with the CAGE
> CLAMP® connections cannot be separated from the other enclosure section.

15   Disposal

15.1   Electrical and electronic equipment
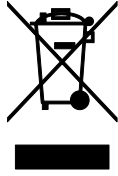
Electrical and electronic equipment may not be disposed of with household waste. This also applies to products without this symbol.

Electrical and electronic equipment contain materials and substances that can be harmful to the environment and health. Electrical and electronic equipment must be disposed of properly after use.
WEEE 2012/19/EU applies throughout Europe. Directives and laws may vary nationally.
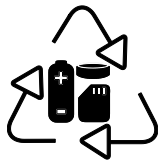
Environmentally friendly disposal benefits health and protects the environment from harmful substances in electrical and electronic equipment.

- Observe national and local regulations for the disposal of electrical and electronic equipment.

- Clear any data stored on the electrical and electronic equipment.

- Remove any added battery or memory card in the electrical and electronic equipment.

- Have the electrical and electronic equipment sent to your local collection point.

Improper disposal of electrical and electronic equipment can be harmful to the environment and human health.

15.2   Packaging

Packaging contains materials that can be reused.
PPWD 94/62/EU and 2004/12/EU packaging guidelines apply throughout Europe. Directives and laws may vary nationally.

Environmentally friendly disposal of the packaging protects the environment and allows sustainable and efficient use of resources.

- Observe national and local regulations for the disposal of packaging.

- Dispose of packaging of all types that allows a high level of recovery, reuse and recycling.

Improper disposal of packaging can be harmful to the environment and wastes valuable resources.

16   Use in Hazardous Environments

The **WAGO I/O System 750** (electrical equipment) is designed for use in Zone 2 hazardous areas and shall be used in accordance with the marking and installation regulations.

The following sections include both the general identification of components (devices) and the installation regulations to be observed. The individual subsections of the "Installation Regulations" section must be taken into account if the I/O module has the required approval or is subject to the range of application of the ATEX directive.

16.1 Marking Configuration Examples

## 16.1.1 Marking for Europe According to ATEX and IECEx
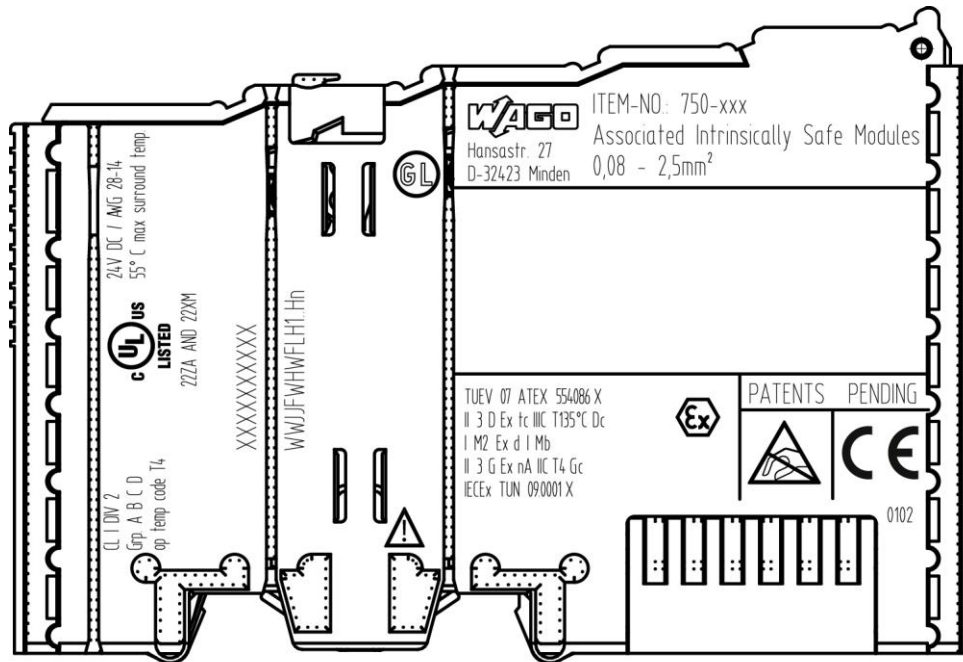
Figure 60: Marking Example According to ATEX and IECEx


```
TUEV 07 ATEX 554086 X
II 3 D Ex tc IIIC T135°C Dc
I M2 Ex d I Mb
II 3 G Ex nA IIC T4 Gc
IECEx TUN 09.0001 X
```

Figure 61: Text Detail – Marking Example According to ATEX and IECEx

Table 69: Description of Marking Example According to ATEX and IECEx

| Marking	Description
TUEV 07 ATEX 554086 X IECEx TUN 09.0001 X	Approving authority resp. certificate numbers
Dust	
II	Equipment group: All except mining
3 D	Category 3 (Zone 22)
Ex	Explosion protection mark
tc	Type of protection: Protection by enclosure
IIIC	Explosion group of dust
T135°C	Max. surface temperature of the enclosure (without a dust layer)
Dc	Equipment protection level (EPL)
Mining	
I	Equipment group: Mining
M2	Category: High level of protection
Ex	Explosion protection mark
d	Type of protection: Flameproof enclosure
I	Explosion group for electrical equipment for mines susceptible to firedamp
Mb	Equipment protection level (EPL)
Gases	
II	Equipment group: All except mining
3 G	Category 3 (Zone 2)
Ex	Explosion protection mark
nA	Type of protection: Non-sparking equipment
IIC	Explosion group of gas and vapours
T4	Temperature class: Max. surface temperature 135 °C
Gc	Equipment protection level (EPL)
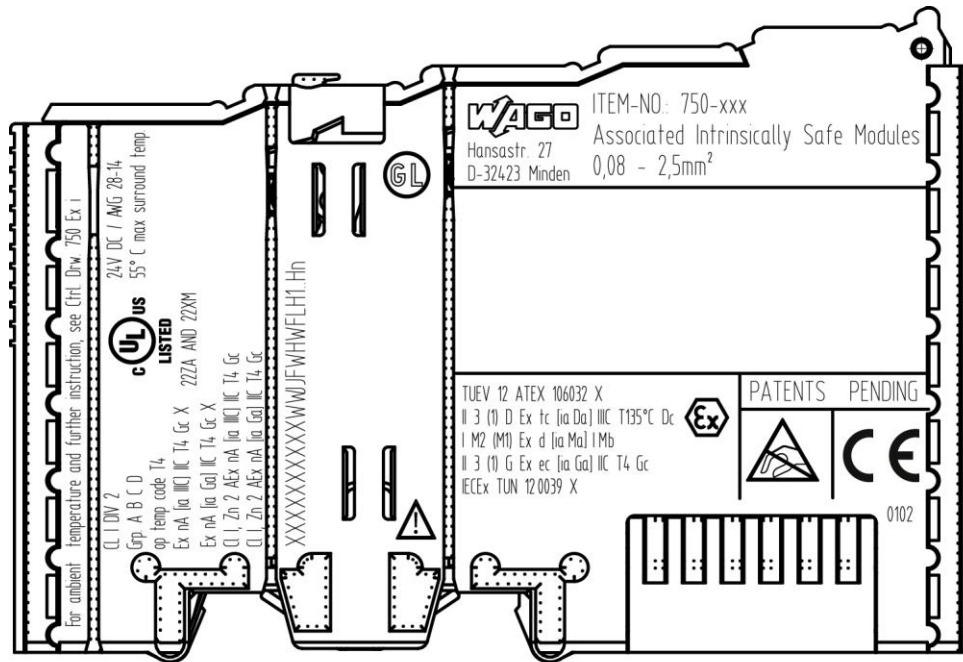
Figure 62: Marking Example for Approved I/O Module Ex i According to ATEX and IECEx

TUEV 12 ATEX 106032 X
II 3 (1) D Ex tc [ia Da] IIIC T135°C Dc
I M2 (M1) Ex d [ia Ma] I Mb
II 3 (1) G Ex ec [ia Ga] IIC T4 Gc
IECEx TUN 120039 X

Figure 63: Text Detail – Marking Example for Approved I/O ModuleEx i According to ATEX and IECEx

Table 70: Description of Marking Example for Approved I/O Module Ex I According to ATEX and IECEx

Marking	Description
TUEV 12 ATEX 106032 X IECEx TUN 12 0039 X	Approving authority resp. certificate numbers
Dust	
II	Equipment group: All except mining
3 (1) D	Category 3 (Zone 22) equipment containing a safety device for a category 1 (Zone 20) equipment
Ex	Explosion protection mark
tc	Type of protection: Protection by enclosure
[ia Da]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20
IIIC	Explosion group of dust
T135°C	Max. surface temperature of the enclosure (without a dust layer)
Dc	Equipment protection level (EPL)
Mining	
I	Equipment Group: Mining
M2 (M1)	Category: High level of protection with electrical circuits which present a very high level of protection
Ex	Explosion protection mark
d	Type of protection: Flameproof enclosure
[ia Ma]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety electrical circuits
I	Explosion group for electrical equipment for mines susceptible to firedamp
Mb	Equipment protection level (EPL)
Gases	
II	Equipment group: All except mining
3 (1) G	Category 3 (Zone 2) equipment containing a safety device for a category 1 (Zone 0) equipment
Ex	Explosion protection mark
ec	Equipment protection by increased safety "e"
[ia Ga]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 0
IIC	Explosion group of gas and vapours
T4	Temperature class: Max. surface temperature 135 °C
Gc	Equipment protection level (EPL)

## 16.1.2 Marking for the United States of America (NEC) and Canada (CEC)
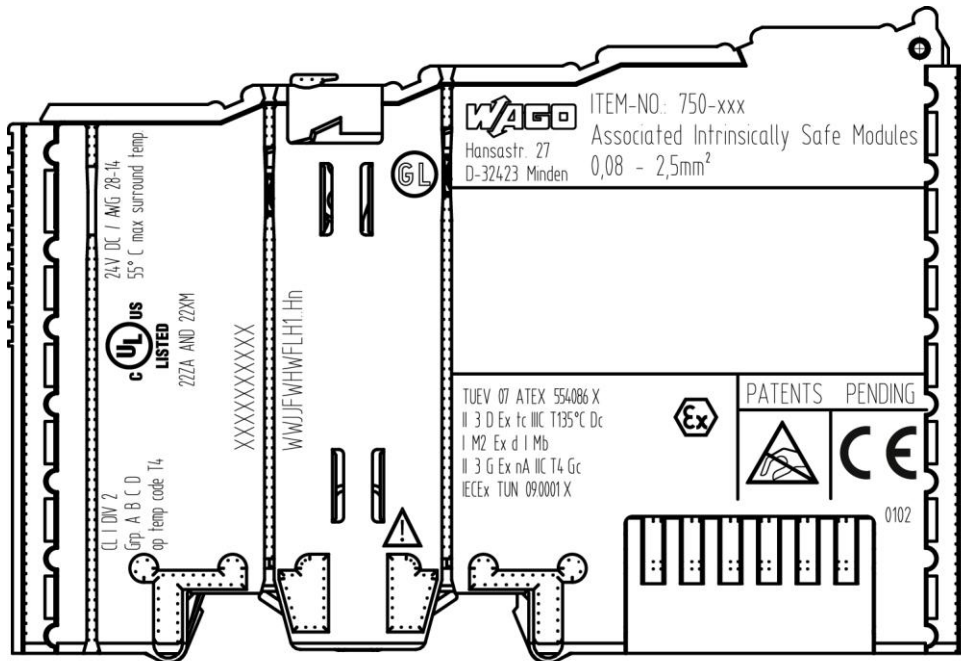
Figure 64: Marking Example According to NEC

Figure 65: Text Detail – Marking Example According to NEC 500

Table 71: Description of Marking Example According to NEC 500

Marking	Description
CL I	Explosion protection (gas group)
DIV 2	Area of application
Grp. A B C D	Explosion group (gas group)
op temp code T4	Temperature class

CI I, Zn 2 AEx nA [ia Ga] IIC T4 Gc

Figure 66: Text Detail – Marking Example for Approved I/O Module Ex i According to NEC 505

Table 72: Description of Marking Example for Approved I/O Module Ex i According to NEC 505

Marking	Description
CI I,	Explosion protection group
Zn 2	Area of application
AEx	Explosion protection mark
nA	Type of protection
[ia Ga]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20
IIC	Group
T4	Temperature class
Gc	Equipment protection level (EPL)

CI I, Zn 2 AEx nA [ia IIIC] IIC T4 Gc

Figure 67: Text Detail – Marking Example for Approved I/O Module Ex i According to NEC 506

Table 73: Description of Marking Example for Approved I/O Module Ex i According to NEC 506

Marking	Description
CI I,	Explosion protection group
Zn 2	Area of application
AEx	Explosion protection mark
nA	Type of protection
[ia IIIC]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20
IIC	Group
T4	Temperature class
Gc	Equipment protection level (EPL)

Ex nA [ia IIIC] IIC T4 Gc X
Ex nA [ia Ga] IIC T4 Gc X

Figure 68: Text Detail – Marking Example for Approved I/O Module Ex i According to CEC 18 attachment J

Table 74: Description of Marking Example for Approved I/O Module Ex i According to CEC 18 attachment J

Marking	Description
Dust	
Ex	Explosion protection mark
nA	Type of protection
[ia IIIC]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20
IIC	Group
T4	Temperature class
Gc	Equipment protection level (EPL)
X	Symbol used to denote specific conditions of use
Gases	
Ex	Explosion protection mark
nA	Type of protection
[ia Ga]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 0
IIC	Group
T4	Temperature class
Gc	Equipment protection level (EPL)
X	Symbol used to denote specific conditions of use

16.2   Installation Regulations

For the installation and operation of electrical equipment in hazardous areas, the valid national and international rules and regulations which are applicable at the installation location must be carefully followed.

16.2.1   Special Notes including Explosion Protection

The following warning notices are to be posted in the immediately proximity of the WAGO I/O System 750 (hereinafter "product"):

WARNING – DO NOT REMOVE OR REPLACE FUSED WHILE ENERGIZED!

WARNING – DO NOT DISCONNECT WHILE ENERGIZED!

WARNING – ONLY DISCONNECT IN A NON-HAZARDOUS AREA!

Before using the components, check whether the intended application is permitted in accordance with the respective printing. Pay attention to any changes to the printing when replacing components.

The product is an open system. As such, the product must only be installed in appropriate enclosures or electrical operation rooms to which the following applies:

*   Can only be opened using a tool or key

*   Inside pollution degree 1 or 2

*   In operation, internal air temperature within the range of 0 °C ≤ Ta ≤ +55 °C or −20 °C ≤ Ta ≤ +60 °C for components with extension number …/025-xxx or −40 °C ≤ Ta ≤ +70 °C for components with extension number …/040-xxx

*   Minimum degree of protection: min. IP54 (acc. to EN/IEC 60529)

*   For use in Zone 2 (Gc), compliance with the applicable requirements of the standards EN/IEC/ABNT NBR IEC 60079-0, -7, -11, -15

*   For use in Zone 22 (Dc), compliance with the applicable requirements of the standards EN/IEC/ABNT NBR IEC 60079-0, -7, -11, -15 and -31

*   For use in mining (Mb), minimum degree of protection IP64 (acc. EN/IEC 60529) and adequate protection acc. EN/IEC/ABNT NBR IEC 60079-0 and -1

*   Depending on zoning and device category, correct installation and compliance with requirements must be assessed and certified by a "Notified Body" (ExNB) if necessary!

Explosive atmosphere occurring simultaneously with assembly, installation or repair work must be ruled out. Among other things, these include the following activities

- Insertion and removal of components

- Connecting or disconnecting from fieldbus, antenna, D-Sub, ETHERNET or USB connections, DVI ports, memory cards, configuration and programming interfaces in general and service interface in particular:

  - Operating DIP switches, coding switches or potentiometers

  - Replacing fuses

Wiring (connecting or disconnecting) of non-intrinsically safe circuits is only permitted in the following cases

- The circuit is disconnected from the power supply.

- The area is known to be non-hazardous.

Outside the device, suitable measures must be taken so that the rated voltage is not exceeded by more than 40 % due to transient faults (e.g., when powering the field supply).

Product components intended for intrinsically safe applications may only be powered by 750-606 or 750-625/000-001 bus supply modules.

Only field devices whose power supply corresponds to overvoltage category I or II may be connected to these components.

16.2.2   Special Notes Regarding ANSI/ISA Ex

For ANSI/ISA Ex acc. to UL File E198726, the following additional requirements apply:

- Use in Class I, Division 2, Group A, B, C, D or non-hazardous areas only

- ETHERNET connections are used exclusively for connecting to computer networks (LANs) and may not be connected to telephone networks or telecommunication cables

- **WARNING** – The radio receiver module 750-642 may only be used to connect to external antenna 758-910!

- **WARNING** – Product components with fuses must not be fitted into circuits subject to overloads!
  These include, e.g., motor circuits.

- **WARNING** – When installing I/O module 750-538, "Control Drawing No. 750538" in the manual must be strictly observed!

![i] **Information**

Additional Information
Proof of certification is available on request.
Also take note of the information given on the operating and assembly instructions.
The manual, containing these special conditions for safe use, must be readily available to the user.

---

17   Appendix

17.1   CODESYS V3 Compatibility

Table 75: CODESYS V3 Compatibility

Device Description	Firmware *)	Compiler	Visualization Profile
6.0.0.15	10.01.04(23)	3.5.17.30	CODESYS V3.5 SP17 Patch 3
6.1.0.16	04.02.13(24)	3.5.18.10	CODESYS Visualization 4.1.1.0

*) Notes on firmware versions:

•   Not every new firmware contains a new version of the runtime environment,
     which is why the compiler version and visualization profile may remain
     unchanged.

•   In principle, there is also compatibility with the respective hotfix and patch
     versions of the firmware. Only the bugfix point of the firmware version must
     be different (example: "FW:01.02.xx(03)").

17.2   Configuration Dialogs

17.2.1   Web-Based-Management (WBM)

17.2.1.1   "Information" Tab

17.2.1.1.1 "Device Status" Page

The "Device Status" page shows information about product identification and the most important network properties.

"Device Details" Group

This group shows information about product identification.

Table 76: WBM "Device Status" Page – "Device Details" Group

Parameters	Explanation
Product Description	Product Designation
Order Number	Product Item Number
Serial	Unique Product Serial Number
License Information	Notification that the CODESYS runtime system is available
Firmware Revision	Firmware Version

"Network TCP/IP Details" Group

The network and interface properties of the product are displayed in this group.

Table 77: WBM "Device Status" Page – "Network TCP/IP Details" Group

Parameter	Meaning	
Bridge <n>	Bridge currently configured; the properties are displayed in a separate area for each configured bridge.	
MAC Address	MAC address used for product identification and addressing	
IP Source	Current reference type of the IP address	
	None	No IP allocation method is selected; this occurs, for example, if a bridge was added due to changes to the bridge configuration. Select a source in the **Configuration** tab on the **Networking** > **TCP/IP Configuration** page.
	static IP	Static IP address assignment
	dhcp	Dynamic IP address assignment via DHCP
	bootp	Dynamic IP address assignment via BootP (if BootP is supported)
	external	The IP address may be assigned by the fieldbus application; this occurs e.g., if the IP address is controlled by the application.
IP Address	Current product IP address	
Subnet Mask	Current product subnet mask	

17.2.1.1.2 "Vendor Information" Page

You can find the manufacturer and address on the "Vendor Information" page.

17.2.1.1.3 "PLC Runtime Information" Page

All information about the enabled runtime system is provided on the "PLC Runtime Information" page. You will also find a link here to open WebVisu.

"Runtime" Group

Table 78: WBM "PLC Runtime Information" Page – "Runtime" Group

Parameter	Explanation
Version	The version of the enabled runtime system is shown. If the runtime system is disabled, "None" is displayed and the subsequent fields of this group are hidden.

"WebVisu" Group

You will find a link that you can use to open WebVisu.

17.2.1.1.4 "WAGO Software License Agreement" Page

The "WAGO Software License Agreement" page lists the license terms for the WAGO software used in the product.

17.2.1.1.5 "Open Source Licenses" Page

The license conditions for the open source software used for the product are listed in alphabetical order on the "Open Source Licenses" page.

17.2.1.1.6 "WBM Third Party License Information" Page

On the "WBM Third Party License Information" page, you can find the license text of the open source licenses that apply to the WBM itself.

17.2.1.1.7 "Trademarks Information" Page

On the "Trademarks Information" page you will find a list of property and trademark rights.

17.2.1.1.8 "WBM Version" Page

On the "WBM Version" page, you can find the version information for the various sections ("Plug-ins") that the WBM contains. This information may be useful for support if an error is found in the WBM.

17.2.1.2 "Configuration" Tab

17.2.1.2.1 "PLC Runtime Configuration" Page

On the "PLC Runtime Configuration" page, you will find the settings for the boot
project created with the programming software and the settings for the web
visualization created in the runtime system.

"General PLC Runtime Configuration" Group

Table 79: WBM "PLC Runtime Configuration" Page – "General PLC Runtime Configuration" Group

Parameter	Meaning	
PLC runtime version	Select here the PLC runtime system to be enabled.	
	None	No runtime system is enabled.
	CODESYS V3	CODESYS V3 runtime system is enabled.
Home directory on memory card enabled	Define if the home directory for the runtime system should be moved to the memory card.	
	Disabled	The home directory is stored in the internal memory.
	Enabled	The home directory is moved to the memory card.

Note

All data is deleted when switching the runtime system!
The runtime system's home directory is completely deleted when switching the
runtime system!

Note

Only the first partition can be used as the Home directory!
Only the first partition of a memory card can be accessed at **/media/sd** and used
as the home directory.

Click **[Submit]** to apply the change. The runtime system change is effective
immediately.
The home directory change only takes effect after the product restarts. For this
purpose, use the WBM reboot function. Do not switch off the product too early!

"Webserver Configuration" Group

Table 80: WBM "PLC Runtime Configuration" Page – "Webserver Configuration" Group

Parameter	Meaning	
CODESYS V3 Webserver State	This displays the status (enabled/disabled) of the CODESYS V3 Webserver.	
Default Webserver	Choose here whether the Web-based Management or web visualization of the runtime system should be displayed when only entering the IP address of the controller.	
	Web-Based Management	The Web-based Management is displayed.
	WebVisu	The web visualization of the runtime system is displayed.

Click **[Submit]** to apply the change. The change takes effect immediately.

In its default setting, the WBM is called up when only entering the IP address.

To update the display after switching, enter the IP address again in the address line of the Web browser.

To display the web visualization, the Webserver must be enabled (in WBM under "Ports and Services" -> "PLC Runtime Services") and there must be a suitably configured application.

Regardless of the default Webserver setting, the WBM can be called up at any time with "https://<IP address>/wbm" and the Web visualization with "https://<IP address>/webvisu".

Note

Possible error messages when calling up the web visualization
The "500 − Internal Server Error" message indicates that the Webserver is not enabled.
A page with the header "WebVisu not available" means that no application has been loaded in the product using web visualization.

17.2.1.2.2 "TCP/IP Configuration" Page

The TCP/IP settings for the ETHERNET interfaces are shown on the "TCP/IP configuration" page.

"TCP/IP Configuration" Group

The properties are displayed in a separate area for each configured bridge.

Table 81: WBM "TCP/IP Configuration" Page – "TCP/IP Configuration" Group

Parameter	Meaning	
Network Details Bridge <n>	Settings for the bridge currently configured	
Current IP Address	This displays the current IP address.	
Current Subnet Mask	This displays current subnet mask.	
Current Default Gateway	The IP address of the current default gateway is displayed.	
IP Source	You can specify whether to use a static or dynamic IP address.	
	Static IP	Static IP addressing
	DHCP	Dynamic IP addressing via DHCP
	BootP	Dynamic IP addressing via BootP
IP Address	Enter a static IP address. This is enabled if "Static IP" is enabled in the **IP Source** field.	
Subnet Mask	Enter the subnet mask. This is enabled if "Static IP" is enabled in the **IP Source** field.	
Default Gateway	Enter the IP address of the default gateway here.	

Click the **[Submit]** button to apply a change. The change takes effect immediately.

"DNS Server" Group

Table 82: WBM "TCP/IP Configuration" Page – "DNS Server" Group

Parameters	Explanation
Active	The active DNS servers are displayed. Up to 3 active DNS servers can be used. The index reflects the query order. The first DNS server assigned via DHCP is given the highest priority.
Assigned by DHCP	The DNS servers assigned if necessary by DHCP (or BootP) are displayed. If no DNS server has been assigned by DHCP (or BootP), "No DNS Servers assigned by DHCP" is displayed.
Assigned by user	The addresses of the defined DNS servers are displayed. If no server has been entered, "No DNS Servers configured" is displayed.
New Server IP	Add additional DNS server addresses. You can enter a maximum of 3 addresses. The entries actually used result from an alternating combination of the "Assigned by DHCP" and "Assigned by user" lists.

Click the **[Delete]** button to delete the selected DNS server. The change takes effect immediately.

Click the **[Add]** button to add the entered DNS server. The change takes effect immediately.

17.2.1.2.3 "Ethernet Configuration" Page

The settings for ETHERNET are located on the "Ethernet Configuration" page.

"Bridge Configuration" Group

Table 83: WBM "Ethernet Configuration" Page – "Bridge Configuration" Group

Parameter	Meaning
Bridge 1 … \<n>	Assign the physical ports X1… X \<n> to a logical bridge. To do so, click the respective option button. The assignment is marked in color. A port can only be assigned to one bridge at a time.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

"Switch Configuration" Group

This group only appears if parameter configuration is supported.

Table 84: WBM "Ethernet Configuration" Page – "Switch Configuration" Group

Parameters	Explanation	
Port Mirror	Enable or disable mirroring of the data traffic between the ports.	
	None	Both ETHERNET ports are operating normally.
	X1	The entire data traffic between X1 and the PFC system is mirrored at port X2.
	X2	The entire data traffic between X2 and the PFC system is mirrored at port X1.
Broadcast Protection	You can set the broadcast limit for protection against overloads.	
	Disabled	No broadcast packet limit
	1 % … 5 %	Limits incoming broadcast packets to the selected percentage of the total possible data throughput (10/100 Mbit)
Rate Limit	You can set the basic limitation of the incoming data traffic.	
	Disabled	No limitation of the incoming data traffic
	64 kbps … 99 mbps	Limits the incoming data traffic to the entered value

Click **[Submit]** to apply the change. The change takes effect immediately.

"Ethernet Interface Configuration" Group

Table 85: WBM "Ethernet Configuration" Page – "Ethernet Interface Configuration" Group

Parameter	Meaning
Interface X<n>	A separate area is displayed for each interface in the controller.
Enabled	You can enable or disable the interface.
MAC Learning	You can disable or enable "MAC Learning".
Speed/Duplex	Select the transmission speed and the transmission method. The drop-down menu is generated depending on the device and interface. When "Autonegotiation" is selected, the connection modalities are negotiated automatically between the peer devices.

Click **[Submit]** to apply changes. The changes take effect immediately.

17.2.1.2.4 Configuration of Host and Domain Name" Page

The settings for the hostname and domain are displayed on the "Configuration of Host/Domain Name" page.

"Hostname" Group

Table 86: WBM "Configuration of Host and Domain Name" Page – "Hostname" Group

Parameter	Explanation
Currently used	If you have selected dynamic assignment of an IP address via DHCP, the name of the host currently being used is displayed.
Configured	Enter the product hostname here; it is then used if the network interface is changed to a static IP address or if no hostname is assigned per DHCP response.

Click the **[Submit]** button to apply a change.

Click the **[Clear]** button to reset the input field.

The change takes effect immediately.

If the controller has been assigned a host name via DHCP, it is given preference and the manually configured host name is not used.
To accept the manually configured host name, the configuration of the DHCP server may have to be reduced by assigning the host name.

"Domain Name" Group

Table 87: WBM "Configuration of Host and Domain Name" Page – "Domain Name" Group

Parameter	Explanation
Currently used	If you have selected dynamic assignment of an IP address via DHCP, the name of the domain currently being used is displayed.
Configured	Enter the product domain name here; it is then used if the network interface is changed to a static IP address or if no domain name is assigned per DHCP response.

Click the **[Submit]** button to apply a change.

Click the **[Clear]** button to reset the input field.

The change takes effect immediately.

If the controller has been assigned a domain name via DHCP, it is given preference and the manually configured domain name is not used.
To accept the manually configured domain name, the configuration of the DHCP server may have to be reduced by assigning the domain name.

202 Appendix

WAGO I/O System 750
750-8214 PFC200; G2; 2ETH RS CAN

17.2.1.2.5 "Routing" Page

On the "Routing" page you can find settings and information on the routing between the network interfaces.

"IP Forwarding through multiple interfaces" Group

Table 88: WBM "Routing" Page – "IP Forwarding through multiple interfaces" Group

Parameter	Explanation
Enabled	Specify whether forwarding of IP data packets is allowed between different network interfaces. If the box is not checked, the settings under "Static Routes" are used, without allowing IP data packets that arrive at the controller on one network interface to leave the controller on different network interface. If the box is checked, IP packets can be forwarded between the interfaces. Other settings may be necessary on this WBM page.

Click the **[Submit]** button to apply the change. The changes take effect immediately.

Manual
Version 1.11.0, valid from FW Version 04.02.13(24)

"Custom Routes" Group

Each configured static route has its own area in the display. If no static routes have been entered, "(no custom routes)" is displayed.

Table 89: WBM "Routing" Page – "Custom Routes" Group

Parameter	Explanation	
Enabled	Specify whether the selected route should be used.	
	Disabled	The route is not used.
	Enabled	The route is used.
Destination Address	Specify whether any network devices or only a specific network device or device pool should be accessible.	
	Default	Any network devices can be reached.
	Network address	Only a specific network device or device from the specified address pool can be reached.
Destination Mask	Enter the subnet mask of the device. If "default" is entered for Destination Address, the value "0.0.0.0" must be entered.	
Gateway Address	Enter the address of the gateway. If the "Interface" input field is empty, an entry is required here. If a value is entered in the "Interface" input field, the input here is optional.	
Gateway Metric	Set the number used as the metric. When there are multiple routes with the same destination address and destination mask, the metric specifies the gateway to which network data packets are first sent. Priority is given to routes with a lower value for the metric. The lowest value is 0. The highest value is $2^{32} - 1 = 4294967295$.	
Interface	Enter an interface via which the packets sent to the destination address are routed. Bridges (br0-br3) as well as modems (wwan0) or VPN interface names can be used. If the "Gateway Address" input field is empty, an entry is required here. If a value is entered in the "Gateway Address" input field, the input here is optional.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

To add a new route, click the **[Add]** button. The change takes effect immediately.

Click the **[Delete]** button to delete an existing route. The change takes effect immediately.

"Dynamic Routes" Group

All default gateways received via DHCP are displayed.
Default gateways configured via DHCP are given the metric value 10, which
means that they are normally used before the statically configured default
gateways.

Each dynamic route has its own area in the display. If no dynamic routes are
received via DHCP, "(no dynamic route)" appears.

"IP-Masquerading" Group

Each entry has its own area in the display.

Table 90: WBM "Routing" Page – "IP-Masquerading" Group

Parameters	Explanation	
Enabled	Specify whether IP masquerading should be used.	
	Disabled	IP masquerading is not used.
	Enabled	IP masquerading is used.
Interface	You can select the specified name of a network interface. Alternatively, selecting "other" allows you to specify any network interface name.	

Click the **[Submit]** button to apply the changes. The changes take effect
immediately.

Click the **[Add]** button to add a new entry. The change takes effect immediately.

Click the **[Delete]** button to delete an existing entry. The change takes effect
immediately.

An entry is only transferred to the system if "Enabled" is enabled in the "General
Routing Configuration" group. This allows you to configure a default setting that is
not applied until the general switch-on.

"Port-Forwarding" Group

Each entry has its own area in the display.

Table 91: WBM "Routing" Page – "Port Forwarding" Group

Parameters	Explanation	
Enabled	Specify whether port forwarding should be used.	
	Disabled	Port forwarding is not used.
	Enabled	Port forwarding is used.
Interface	You can select the specified name of a network interface. Alternatively, selecting "other" allows you to specify any network interface name.	
Port	Enter the port here on which the product receives network data packets to be forwarded.	
Protocol	You can select the protocol to be used for the port forwarding. The options are TCP, UDP or both protocols.	
Destination Address	Specify the network address of the destination device. This address replaces the original destination address of the network data packet.	
Destination Port	Specify the port number of the destination device. This value replaces the original destination port of the network data packet.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

Click the **[Add]** button to add a new entry. The change takes effect immediately.

Click the **[Delete]** button to delete an existing entry. The change takes effect immediately.

An entry is only transferred to the system if "Enabled" is enabled in the "General Routing Configuration" group. This allows you to configure a default setting that is not applied until the general switch-on.

17.2.1.2.6 "Clock Settings" Page

The date and time settings are displayed on the "Clock Settings" page.

"Timezone and Format" Group

Table 92: WBM "Clock Settings" Page – "Timezone and Format" Group

Parameter	Explanation	
Timezone	Select the appropriate time zone for your location. Default setting:	
	AST/ADT	"Atlantic Standard Time," Halifax
	EST/EDT	"Eastern Standard Time," New York, Toronto
	CST/CDT	"Central Standard Time," Chicago, Winnipeg
	MST/MDT	"Mountain Standard Time," Denver, Edmonton
	PST/PDT	"Pacific Standard Time", Los Angeles, Whitehouse
	GMT/BST	"Greenwich Mean Time", GB, P, IRL, IS, …
	CET/CEST	"Central European Time," B, DK, D, F, I, CRO, NL, …
	EET/EEST	"Eastern European Time," BUL, FI, GR, TR, …
	CST	"China Standard Time"
	JST	"Japan/Korea Standard Time"
TZ string	For time zones that cannot be selected with the "Time Zone" parameter, enter the name of the time zone or the country or city applicable to you. You can determine a valid name for the time zone here: http://www.timeanddate.com/time/map/	
Time Format	For switching between 12-hour and 24-hour time display	

Click the **[Submit]** button to apply a change. The change takes effect immediately.

"UTC Time and Date" Group

Table 93: WBM "Clock Settings" Page – "UTC Time and Date" Group

Parameter	Explanation
UTC Date	Set the date.
UTC Time	Set GMT time.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

"Local Time and Date" Group

Table 94: WBM "Clock Settings" Page – "Local Time and Date" Group

Parameter	Explanation
Local Date	Set the date.
Local Time	Set the local time.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

17.2.1.2.7 "Configuration of Serial Interface RS232/RS485" Page

The settings for the serial interface are shown on the "Configuration of Serial Interface RS232/485" page.

"Serial Interface assigned to" Group

The application that the serial interface is currently assigned to is displayed.

"Assign Owner of Serial Interface" Group

You can specify the application that the serial interface is to assigned after the next controller reboot.

Table 95: WBM "Configuration of Serial Interface RS232" Page – "Assign Owner of Serial Interface" Group

Parameters	Explanation
Linux® Console	Specify that the serial interface is assigned to the Linux® console.
Unassigned (usage by applications, libraries, CODESYS)	Specify that the serial interface is not to be assigned to any application and is available, so that the CODESYS program, for example, can access it via function blocks.

NOTICE

Remove RS-485 devices before switching to "Linux Console"!
Connected RS-485 devices can be damaged when switching to "Linux Console". Remove these devices before switching!

Click **[Change Owner]** to apply the change. The change only takes effect once the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

17.2.1.2.8 "Configuration of Service Interface" Page

The settings for the service interface are shown on the "Configuration of the Service Interface" page.

"Service Interface assigned to" Group

The application that the service interface is currently assigned to is displayed.

"Assign Owner of Service Interface" Group

You can specify the application to which the service interface is assigned after the next controller reboot.

Table 96: WBM "Configuration of Service Interface" Page – "Assign Owner of Service Interface" Group

Parameters	Explanation
WAGO Service Communication	Specify that the service interface is used for the WAGO Service communication or runtime system communication.
Linux Console	Specify that the service interface is assigned to the Linux® console.
Unassigned (usage by applications, libraries, CODESYS)	Specify that the service interface is not to be assigned to any application and is available, so that the CODESYS program, for example, can access it via function blocks.

Click **[Submit]** to apply the change. The change only takes effect once the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

17.2.1.2.9 "Create Bootable Image" Page

You can create a bootable image on the "Create Bootable Image" page.

"Create bootable image from boot device" Group

Once the destination has been determined and output, it is then checked and the results of this check are displayed below the settings:

Table 97: WBM "Create Bootable Image" Page – "Create bootable image from active partition" Group

Parameters	Meaning		
Boot Device	The medium from which the boot was made is displayed.		
Destination	Depending on which medium has been booted, the following destination is available for selection after boot-up for the image to be generated:		
	System was booted from		Target partition for "bootable image"
	Memory Card	→	Internal Flash
	Internal memory	→	Memory Card

- Free space on target device:
  If the available memory space is less than 5% a warning is displayed. You can still start the copy process despite the warning. If the available space is too low, a corresponding message is displayed and copying cannot be started.

- Device being used by CODESYS:
  If the device is being used by CODESYS, a warning is displayed. Although it is not recommended, you can still start the copying procedure despite this warning.

Click **[Start Copy]** to start the copying procedure. If the outcome of the test is positive, copying begins immediately. If errors have been detected, a corresponding message is displayed and copying is not started. If warnings have been issued, these are displayed again and you must then confirm that you still wish to continue.

17.2.1.2.10   "Firmware Backup" Page

You can find the controller data backup settings on the "Firmware Backup" page.

"Firmware Backup" Group

Table 98: WBM "Firmware Backup" Page – "Firmware Backup" Group

Parameter	Explanation	
Boot Device	The storage medium from which the device was booted is displayed here.	
Destination	Select the storage location for the backup here.	
	Memory Card	The data is written to the memory card. This selection only appears if a memory card is inserted and the device has not been booted from the memory card.
	Network	The data is saved in the file system and then made available as a download on the PC.
PLC runtime project	If you want to save the PLC runtime project, select this checkbox.	
Settings	If you want to save the device settings, select this checkbox.	
System	If you want to back up the operating system of the device and the root file system, select this checkbox.	
Encryption	If you want to save the data in encrypted form, select this button.	
Encryption passphrase	Enter the encryption password here. This input field only appears if the "Encryption" checkbox is selected.	
Confirm passphrase	Enter the encryption password again here to check it. This input field only appears if the "Encryption" checkbox is selected.	

Note

→ **Note the firmware version!**
Restoring the controller operating system ("System" selection) is only permissible and possible if the firmware versions at the backup and restore times are identical.
If necessary, skip restoring the controller operating system, or match the firmware version of the controller to the firmware version of the backup time beforehand.

> **Note**
>
> **Only one package may be copied to the network!**
> If you have specified "Network" as the storage location, only one package may
> be selected for each storing process.

> **Note**
>
> **No backup of the memory card!**
> Backup from the memory card to the internal flash memory is not possible.

> **Note**
>
> **Account for backup time!**
> Generation of backup files can take several minutes. Stop the CODESYS
> program before you start the backup procedure to help shorten the time required.

Click the **[Create Backup]** button to start the backup operation.

17.2.1.2.11 "Firmware Restore" Page

The settings for restoring the controller data are shown on the "Firmware Restore" page.

"Firmware Restore" Group

Table 99: WBM "Firmware Restore" Page – "Firmware Restore" Group

Parameter	Explanation	
Source	Select the data source for the restore here.	
	Memory Card	The data is read from the memory card. This selection is only enabled if a memory card is inserted and the device has not been booted from the memory card.
	Network	The data is uploaded from the PC and restored.
Boot Device	The storage medium from which the device was booted is displayed here.	
PLC runtime project	Enter the name of the backup file for the CODESYS project here. The input field only appears if the network is selected as the data source.	
Settings	Enter the name of the backup file for the settings here. The input field only appears if the network is selected as the data source.	
System	Enter the name of the backup file for the system data and the root file system here. The input field only appears if the network is selected as the data source.	
Decryption	If you have backed up the data in encrypted form, select this checkbox.	
Decryption passphrase	Enter the encryption password here. This input field only appears if the "Decryption" checkbox is selected.	

Note

→ **Note the firmware version!**
Restoring the controller operating system ("System" selection) is only permissible and possible if the firmware versions at the backup and restore times are identical.
If necessary, skip restoring the controller operating system, or match the firmware version of the controller to the firmware version of the backup time beforehand.

Note

File size must not exceed the size of the internal drive!
Note that the amount of data in the media/sd/copy/ directory must not exceed the total size of the internal drive.

Note

Restoration only possible from internal memory!
If the device was booted from the memory card, the firmware cannot be restored.

Note

Reset by restore
A reset is performed when the system or settings are restored by CODESYS!

Note

Connection loss through restore
If the restore changes the parameters of the ETHERNET connection, the WBM may then no longer be able to open a connection to the device. You must call the WBM again by entering the correct IP address of the device in the address line.

Note

Note the restore time!
The restore process takes approx. 2 … 3 minutes.
After the restore process, the controller is restarted and is then ready for use again.

Click the **[Restore]** button to start the restore operation.

17.2.1.2.12   "Active System" Page

The settings for specifying the partition from which the system is started are shown on the "Active System" page.

"Boot Device" Group

Table 100: WBM "Active System" Page – "Boot Device" Group

Parameter	Explanation
Boot Device	The storage medium from which the device was booted is displayed here.

"System <n> (Internal Flash)" Groups

Table 101: WBM "Active System" Page – "System <n> (Internal Flash)" Group

Parameter	Explanation	
Active	This shows whether the system is active.	
Configured	This shows whether the system should be active after the next reboot.	
State	The system status is displayed here.	
	good	The system is valid and can be used.
	bad	The system is not valid and cannot be used.

Click the respective **[Activate]** button to start the required system at the next reboot.

→ **Note**

Provide a bootable system!
A functional firmware backup must be available on the boot system!

17.2.1.2.13   "Mass Storage" Page

The "Mass Storage" page displays information and settings for the storage media.

The group title contains the designation for the storage media ("Memory Card" or "Internal Flash") and, if this storage medium is also the active partition, the text "Active Partition".

"Devices" Group

An area with information on the storage medium is displayed for each storage medium found.

Table 102: WBM "Mass Storage" Page – "Devices" Group

Parameter	Explanation
<Device>	The storage medium is displayed.
Boot device	This shows whether the device has booted from this storage medium.
Volume name	The name of the storage medium is displayed.

"Create new Filesystem on Memory Card" Group

Table 103: WBM "Mass Storage" Page – "Create new Filesystem on Memory Card" Group

Parameter	Meaning	
Filesystem type	You can select the format in which the filesystem should be created on the memory card.	
	Ext4	The filesystem is created in Ext4 format. The files are not readable under Windows!
	FAT	The filesystem is created in FAT format.
Label	Specify the name for the storage medium when formatted.	

Note

Data is deleted!
Any data stored in the storage medium is deleted during formatting!

To format the specified storage medium, click **[Start]**.

17.2.1.2.14   "Software Uploads" Page

On "Software Upload" page, you can install software packages on the product from your PC.

Table 104: WBM "Software Uploads" Page – "Upload New Software" Group

Parameters	Explanation
Software file	The file name of your selected software package is displayed, as long as you have not yet transferred it to the product. If you have not yet selected a package, "Choose ipk file..." appears. Click the input field and select a file with a software package on your PC.

To install the package, click **[Install]**.

The file with the software package is deleted from the device again after the installation process. If this is not possible due to a processing error, it is deleted no later than the next time the product restarts.

17.2.1.2.15   "Configuration of Network Services" Page

The settings for various services are shown on the "Configuration of Network Services" page.

> **→**   **Note**
>
> **Close any ports and services that you do not need!**
> Unauthorized persons may gain access to your automation system through open ports.
> To reduce the risk of cyber attacks and thus increase cyber security, close all ports and services not required by your application in the control components (e.g., port 6626 for WAGO-I/O-*CHECK* and port 11740 for CODESYS V3).
> Only open ports and services during commissioning and/or configuration.

"FTP" Group

Table 105: WBM "Configuration of Network Services" Page – "FTP" Group

Parameter	Explanation
Service active	Enable/disable the FTP service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

"FTPES (explicit FTPS)" Group

Table 106: WBM "Configuration of Network Services" Page – "FTPES (explicit FTPS)" Group

Parameter	Explanation
Service active	Enable/disable the FTPS service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

"HTTP" Group

Table 107: WBM "Configuration of Network Services" Page – "HTTP" Group

Parameter	Explanation
Service active	Enable/disable the HTTP service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

→ **Note**

Disconnection abort on disabling
If the HTTP service is disabled, the connection to the product may be interrupted. In that case, reopen the page.

"HTTPS" Group

Table 108: WBM "Configuration of Network Services" Page – "HTTPS" Group

Parameter	Explanation
Service active	State of HTTPS service is displayed here.

"I/O-*CHECK*" Group

This group appears if the controller supports WAGO-I/O-*CHECK*.

Table 109: WBM "Configuration of Network Services" Page – "I/O-*CHECK*" Group

Parameter	Explanation
Service active	Enable/disable the WAGO-I/O-*CHECK*-Service.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

17.2.1.2.16   "Configuration of NTP Client" Page

The settings for the NTP service are shown on the "Configuration of NTP Client" page.

"NTP Client Configuration" Group

Table 110: WBM "Configuration of NTP Client" Page – "NTP Client Configuration" Group

Parameters	Explanation
Service enabled	Enable/disabled time update.
Update interval (sec)	Specify the update interval of the time server.
Time Server <n>	Enter here the IP addresses of up to 4 time servers. Time server No. 1 is queried first. If no data is accessible via this server, time server No. 2 is queried, etc.
Additionally assigned (DHCP)	The NTP servers assigned if necessary by DHCP (or BootP) are displayed. If no NTP server has been assigned by DHCP (or BootP), "(No additional servers assigned)" is displayed.

To update the time regardless of interval, click the **[Update Time]** button.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

17.2.1.2.17 "PLC Runtime Services" Page

The settings for various services of the runtime systems are displayed on the
"PLC Runtime Services" page.

"CODESYS V3" Group

This group only appears if the controller supports the CODESYS V3 runtime
system.

Table 111: WBM "PLC Runtime Services" Page – "CODESYS V3" Group

Parameter	Explanation
CODESYS V3 State	This displays the status (enabled/disabled) of the CODESYS V3 runtime system.
Webserver enabled	Enable or disable the Webserver for the CODESYS V3 web visualization.
Port authentication enabled	Enter here whether a login is required for connecting to the device. The user name is admin and the password specified at "General Configuration."

Click the **[Submit]** button to apply the change.
The change in authentication takes effect after the next restart.
All other changes take effect immediately.

17.2.1.2.18   "SSH Server Settings" Page

The settings for the SSH service are shown on the "SSH Server Settings" page.

"SSH Server" Group

Table 112: WBM "SSH Server Settings" Page – "SSH Server" Group

Parameters	Explanation
Service active	You can enable/disable the SSH server.
Port Number	Enter the port number.
Allow root login	You can enable or inhibit root access.
Allow password login	Enable or disable the password query function.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

17.2.1.2.19   "DHCP Server Configuration" Page

The "DHCP Server Configuration" page displays the DHCP service settings.

"DHCP Server Configuration Bridge <n>" Group

Table 113: WBM "DHCP Server Configuration" Page – "DHCP Configuration Bridge <n>" Group

Parameter	Explanation
Service active	Enable or disable the DHCP service for the interface X<n>.
Start IP for Range	Enter the start value of the available IP address range.
End IP for Range	Enter the end value of the available IP address range.
Lease time (min)	Specify the lease time here in seconds. 120 minutes are entered by default.
Static Hosts	This displays the static assignments of MAC IDs to IP addresses. If no assignment was defined, "No static hosts configured" is displayed.
Add Static Host	You can add static MAC addresses or host names and IP addresses.
MAC Address or Hostname	Enter a new static assignment, e.g., "01:02:03:04:05:06=192.168.1.20" or "hostname=192.168.1.20". You can enter 15 assignments or host names.
Ip Address	Enter the IP address. You can enter 15 IP addresses.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

To accept a new assignment click the **[Add]** button. The change takes effect immediately.

Click **[Delete]** to delete an existing assignment. The change takes effect immediately.

17.2.1.2.20 "Configuration of DNS Server" Page

The "Configuration of DNS Server" page displays the DNS service settings.

"DNS Server" Group

Table 114: WBM "Configuration of DNS Server" Page – "DNS Server" Group

Parameter	Explanation	
Service active	You can enable/disable the DNS server service.	
Mode	Select the operating mode of the DNS server.	
	Proxy	Requests are buffered to optimize throughput.
	Relay	All requests are routed directly.
Static Hosts	This displays the names for IP addresses. If no assignment was defined, "No static hosts configured" is displayed.	
Add Static Host	You can add static IP addresses and host names below.	
IP Address	Enter a new static assignment, e.g., "192.168.1.20:hostname". You can enter 10 assignments.	
Hostname	Enter a host name.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

To accept a new assignment click the **[Add]** button. The change takes effect immediately.

Click **[Delete]** to delete an existing assignment. The change takes effect immediately.

17.2.1.2.21 "Status overview" Page

On the "Status overview" page, you can find information about cloud access.

"Service" Group

Table 115: WBM "Status Overview" Page – "Service" Group

Parameter	Explanation
Version	The cloud plug-in version is displayed.

"Connection <n>" Group

A group is displayed for each cloud access.

Table 116: WBM "Status Overview" Page – "Connection <n>" Group

Parameter	Explanation
Is Active	The status of the cloud connectivity application is displayed.
Data from PLC Runtime	This shows how many data collections have been registered on the IEC application side for transfer to the cloud.
Cloud Connection	The status of the connection to the cloud service is shown.
Heartbeat	This shows the current heartbeat interval setting in seconds.
Telemetry Data Transmission	This indicates whether transfer of data is enabled or disabled.
Cache fill level (QoS 1 and 2)	This shows the fill level of the memory cache for outgoing messages as a percentage.

"Diagnosis" Group

This group is visible only when diagnostic information is available.

Warnings and errors are displayed here, along with information (when available) on how to potentially eliminate the error(s).

17.2.1.2.22   "Configuration of Connection <n>" Page

You can find settings and information for cloud access on the "Configuration of Connection <n>" page.

A page is displayed for each cloud access.

"Configuration" Group

The parameters indicated depend on the cloud platform setting and, if applicable, on other settings in this group.
The dependencies are shown in a separate table.

Table 117: WBM "Configuration of Connection <n>" Page – "Configuration" Group

Parameter	Explanation
Enabled	You can enable/disable the cloud connectivity function.
Cloud platform	Select the cloud platform.
Hostname	Enter the host name or IP address for the selected cloud platform.
Port number	Enter the port here to which a connection is to be established. Typical values are 8883 for encrypted connections and 1883 for unencrypted connections.
Device ID	Enter the device ID for the selected cloud platform.
Client ID	Enter the client ID for the selected cloud platform.
Authentication	Select the authentication method. Possible settings are "Shared Key Access" or "X.509 Certificate".
Activation Key	Enter the activation key for the selected cloud platform.
Clean Session	Specify whether clean session should be enabled during the connection to the cloud service. If clean session is enabled, the information and messages on this connection are not stored persistently on the cloud service.
TLS	You can specify whether TLS encryption should be used for the connection to the cloud platform. Amazon Web Services (AWS) always uses TLS.
CA file	Enter the path here to the file encoded in PEM format that contains the trusted CA certificate to use to establish an encrypted connection. The default value is the CA certificate /etc/ssl/certs/ca-certificates.crt that is already installed on the controller.
Users	Enter the user name for cloud service authentication.
Password	Enter the password for cloud service authentication.

Table 117: WBM "Configuration of Connection <n>" Page – "Configuration" Group

Parameter	Explanation
Certification file	Enter the path here to the file encoded in PEM format that is used for cloud service authentication.
Key file	Enter the path to the file encoded in PEM format that contains the private key for cloud service authentication.
Use websockets	Here, you can specify whether the connection to the cloud platform is to be set up using the Websocket protocol via Port 443. If this checkbox is not selected, the connection to the cloud platform is set up using the MQTT protocol via Port 8883.
Proxy Type	Select which type of proxy should be used.
HTTP Proxy Host	Enter the host name or IP address of the proxy.
HTTP Proxy Port	Enter the port number of the proxy.
HTTP Proxy User	Enter the name of the proxy user.
HTTP Proxy Password	Enter the password for the proxy user.
Use compression	Here, you can set whether the data is to be compressed using GZIP compression.
Data Protocol	Here you can select the data protocol.
Cache mode	Specify in which memory the cache for the data telegrams should be created. This selection field is only enabled if a correctly formatted SD card is inserted (more information is available in Application Note A500920).
Last Will	You can specify whether a last will message should be enabled/disabled.
(Last Will) Topic	You can specify the topic under which the last will messages should be sent.
(Last Will) Message	You can enter the message you wish to use as the last will message.
(Last Will) QoS	You can specify the "Quality of Service" (QoS) of the last will message.
(Last Will) Retain	Here, you can set whether the previous last-will message sent under a topic from the broker is to be handled as a retained message.
Device info	Specify whether a device info message should be generated that informs the cloud service of the basic configuration of the controller (more information is available in the Application Note A500920).
Device status	Specify whether device state messages should be generated that inform the cloud service about changes in the mode selector switch and the LEDs (more information is available in the Application Note A500920).

Table 117: WBM "Configuration of Connection <n>" Page – "Configuration" Group

Parameter	Explanation
Standard commands	Specify whether the integrated standard commands should be supported (list of standard commands is available in the Application Note A500920). If the checkbox is disabled, only the commands defined in the IEC program are supported.
Application property template	You have the option of creating your own property for the individual MQTT messages to the Azure cloud. This parameter is optional; i.e., if the field is left blank, this property is not sent. The following placeholders are available to create this property: • <m>: Message type • <p>: Protocol version • <d>: Device ID Examples: • MyKey=HelloWorld_<m> • TestKey=<m>/<p>/<d> • DeviceId=<d>

Click the **[Submit]** button to apply a change.

The changes only take effect after the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

The following tables show the dependencies of the selection and input fields as well as the possible settings.

Table 118: Display of the Selection and Input Fields Depending on the Selected Cloud Platform

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services
Enabled	X	X	X	X	X	X
Cloud platform	X	X	X	X	X	X
Hostname	X	X	X	X	X	X
Port number			X	X	(X)	X
Device ID	X	X				
Client ID			X	X	X	X
Authentication		X				
Activation Key	X	X2				
Clean Session			X	(X)	(X)	X
TLS			X	X	(X)	X
CA file			X	X	X	X

Table 118: Display of the Selection and Input Fields Depending on the Selected Cloud Platform

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services
User			X	X		
Password			X	X		
Certification file		X2	X		X	X
Key file		X2	X		X	X
Use websockets	X	X1				
Proxy Type	X4	X4				
HTTP Proxy Host	X5	X5				
HTTP Proxy Port	X5	X5				
HTTP Proxy User	X5	X5				
HTTP Proxy Password	X5	X5				
Data Protocol		X	X	X	X	(X)
Use compression	X	X1	X1			
Cache mode	X	X	X	X	X	X
Last Will			X	X	X	X
Last Will Topic			X3	X3	X3	X3
Last Will Message			X3	X3	X3	X3
Last Will QoS			X3	X3	X3	X3
Last Will Retain			X3	X3	(X3)	X3
Device info		X1	X1	X1	X1	
Device status		X1	X1	X1	X1	
Standard commands		X1	X1		X1	
Application property template		X1				

X: Visible and enabled
(X):   Visible, but disabled
X1:   Visible and enabled, depending on the selected data protocol
X2:   Visible and enabled, depending on the selected authentication
X3:   Visible and enabled when "Last Will" is switched on
(X3):   Visible, but disabled when "Last Will" is switched on
X4:   Enabled if "Use websockets" is switched on.
X5:   Visible and enabled if "Use websockets" is switched on and if "HTTP" is set as the "Proxy Type".

Table 119: Choice of Data Protocol Depending on the Selected Cloud Platform

Data Protocol	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services
WAGO Protocol		X	X	X	X	
WAGO Protocol 1.5		X	X	X	X	
Native MQTT			X	X	X	(X)
Sparkplug payload B		X	X		X	

X: Selection possible
(X):   Fixed setting

Table 120: Display of the Selection and Input Fields Depending on the Selected Data Protocol

Selection or Input Field	Data Protocol			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
Client ID	X	X	X	X
Use compression	X	X	X	
Device info	X	X		
Device status	X	X		
Standard commands	X	X		
Application property template	X	X		

X: Visible and enabled

Table 121: Choice of Cache Mode Depending on the Selected Data Protocol

Cache Mode	Data Protocol			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
RAM	X	X	X	(X)
SD-Card	X1	X1	X1	

X: Selection possible
X1:   Selection only possible if "Compression" is not switched on
(X):   Fixed setting

Table 122: Display of the Selection and Input Fields Depending on the Selected Authentication

Selection or Input Field	Authentication	
	Shared Access Key	**X.509 Certificate**
Activation Key	X	
Certification file		X
Key file		X

X: Visible and enabled

17.2.1.2.23   "Configuration of General SNMP Parameters" Page

The general settings for SNMP are given on the "Configuration of General SNMP Parameters" page.

"General SNMP Configuration" Group

Table 123: WBM "Configuration of General SNMP Parameters" Page – "General SNMP Configuration" Group

Parameter	Explanation
Service active	Activate/deactivate the SNMP service.
Name of Device	Enter here the device name (sysName).
Description	Enter here the device description (sysDescription).
Physical Location	Enter here the location of the device (sysLocation).
Contact	Enter here the email contact address (sysContact).
ObjectID	Enter here the object ID (sysOID).

Click the **[Submit]** button to apply the changes.

17.2.1.2.24 "Configuration of SNMP v1/v2c Parameters" Page

The general settings for SNMP v1/v2c are shown on the "Configuration of SNMP v1/v2c Parameters" page.

"Communities" Group

Table 124: WBM "Configuration of SNMP v1/v2c Parameters" Page – "Communities" Group

Parameters	Explanation
Community <n>	Each configured community has its own area in the display. If no community has been configured, "(no Communities configured)" is displayed.
Name	The community name for the SNMP manager configuration is displayed. The community name can establish relationships between SNMP managers and agents who are respectively referred to as "Community" and who control identification and access between SNMP participants.
Access	This displays the access rights for the community. Possible values: "ReadOnly" or "ReadWrite".
Add new Community	In this area, you can enter a new community.
Name	Specify the community name for the SNMP manager configuration. (See above) The community name can be up to 32 characters long and must not include spaces. To use the SNMP protocol, a valid community name must always be specified. The default community name is "public."
Access	Specify the access rights for the new community. Possible values: "ReadOnly" or "ReadWrite".

Click the corresponding **[Delete]** button to delete an existing community.

Click the **[Add]** button to add a new community.

"Trap Receivers" Group

Table 125: WBM "Configuration of SNMP v1/v2c Parameters" Page – "Trap Receivers" Group

Parameters	Meaning
Trap Receiver <n>	Each configured trap receiver has its own area in the display. If no trap receiver has been configured, "(no Trap Receivers configured)" is displayed.
Host	The host name or the IP address for the trap receiver (management station) is displayed.
Community Name	This displays the community name for the trap receiver configuration. The community name can be evaluated by the trap receiver.
Version	This displays the SNMP version, via which the traps are sent.
Add new Trap Receiver	In this area, you can enter a new trap receiver.
Host	Specify the host name or the IP address for the new trap receiver (management station).
Community Name	Specify the community name for the new trap receiver configuration. (See above). The community name can be up to 32 characters long and must not include spaces.
Version	Specify the SNMP version that will send the traps. Possible values: "v1" or "v2c".

Click the corresponding **[Delete]** button to delete an existing trap receiver.

Click the **[Add]** button to add a new trap receiver.

17.2.1.2.25   "Configuration of SNMP v3 Parameters" Page

The general settings for SNMP v3 are shown on the "Configuration of SNMP v3 Parameters" page.

"Users" Group

Table 126: WBM "Configuration of SNMP v3 Parameters" Page – "Users" Group

Parameters	Meaning
User <n>	Each configured v3 user has its own area in the display. If no v3 user has been configured, "(no Users configured)" is displayed.
Security Authentication Name	The user name is displayed.
Authentication Type	The authentication type for the SNMP v3 packets is displayed. Possible values: - Use no authentication ("None") - Message Digest 5 ("MD5") - Secure Hash Algorithm ("SHA", "SHA224", "SHA256", "SHA384", "SHA512")
Authentication Key	The authentication key is displayed.
Privacy	The encryption algorithm for the SNMP message is displayed. Possible values: - No encryption ("None") - Data Encryption Standard ("DES") - Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	The key for encryption of the SNMP message is displayed. If nothing is displayed, the "authentication key" is automatically used.
Access	This displays the access rights for the user. Possible values: "ReadOnly" or "ReadWrite".
Add new v3 User	In this area, you can enter a new v3 user. You can create up to 10 users.
Security Authentication Name	Enter the user name. This name must be unique; a pre-existing user name is not accepted when entered. The name must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Authentication Type	Specify the authentication type for the SNMP v3 packets. Possible values: - Use no authentication ("None") - Message Digest 5 ("MD5") - Secure Hash Algorithm ("SHA", "SHA224", "SHA256", "SHA384", "SHA512")

Table 126: WBM "Configuration of SNMP v3 Parameters" Page – "Users" Group

Parameters	Meaning
Authentication Key	Specify the authentication key. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Privacy	Specify the encryption algorithm for the SNMP message. Possible values: - No encryption ("None") - Data Encryption Standard ("DES") - Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	Enter the key for encryption of the SNMP message. If nothing is specified here, the "authentication key" is automatically used. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Access	Specify the access rights for the new user. Possible values: "ReadOnly" or "ReadWrite".

Click the respective **[Delete]** button to delete an existing user.

Click **[Add]** to add a new user.

"Trap Receivers" Group

Table 127: WBM "Configuration of SNMP v3 Parameters" Page – "Trap Receivers" Group

Parameters	Meaning
Trap Receiver <n>	Each configured v3 trap receiver has its own area in the display. If no v3 trap receiver has been configured, "(no Trap Receivers configured)" is displayed.
Security Authentication Name	The user name is displayed.
Authentication Type	The authentication type for the SNMP v3 packets is displayed. Possible values: - Use no authentication ("None") - Message Digest 5 ("MD5") - Secure Hash Algorithm ("SHA", "SHA224", "SHA256", "SHA384", "SHA512")
Authentication Key	The authentication key is displayed.
Privacy	The encryption algorithm for the SNMP message is displayed. Possible values: - No encryption ("None") - Data Encryption Standard ("DES") - Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	The key for encryption of the SNMP message is displayed. If nothing is displayed, the "authentication key" is automatically used.
Host	The host name or the IP address of a trap receiver for v3 traps is displayed.
Add new Trap Receiver	In this area, you can enter a new v3 trap receiver. You can create up to 10 trap receivers.
Security Authentication Name	Enter the user name. This name must be unique; a pre-existing user name is not accepted when entered. The name must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Authentication Type	Specify the authentication type for the SNMP v3 packets. Possible values: - Use no authentication ("None") - Message Digest 5 ("MD5") - Secure Hash Algorithm ("SHA", "SHA224", "SHA256", "SHA384", "SHA512")

Table 127: WBM "Configuration of SNMP v3 Parameters" Page – "Trap Receivers" Group

Parameters	Meaning
Authentication Key	Specify the authentication key. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Privacy	Specify the encryption algorithm for the SNMP message. Possible values: - No encryption ("None") - Data Encryption Standard ("DES") - Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	Enter the key for encryption of the SNMP message. If nothing is specified here, the "authentication key" is automatically used. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Host	Specify the host name or the IP address for a trap receiver for v3 traps.

Click the respective **[Delete]** button to delete an existing trap receiver.

Click **[Add]** to add a new trap receiver.

17.2.1.2.26   Page "Docker Settings"

On the page "Docker Settings", see the settings for the "Docker®" service.

Group "Docker Status"

Table 128: WBM Page "Docker Settings" – group "Docker Status"

Parameter	Meaning	
Current State	The current status of the "Docker®" service is displayed.	
	stopped	The "Docker®" service is disabled.
	running	The "Docker®" service is enabled.
Service Enabled	If you want to enable the "Docker®" service, check this box.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

17.2.1.2.27 "WBM User Configuration" Page

The settings for user administration are displayed on the "WBM User Configuration" page.

"Change Password" Group

➜ **Note**

Changing Passwords
The initial passwords as delivered are documented in this manual and therefore do not provide sufficient protection. Change the passwords to meet your particular needs!

Table 129: WBM "WBM User Configuration" Page – "Change Password" Group

Parameter	Explanation
Old Password	Enter the current password here for authentication.
New Password	Enter the new password here. Permitted characters for the password are the following ASCII characters: a … z, A … Z, 0 … 9, blank spaces and special characters: ! ? % + = ( ) _ # " - / ` < > * ; , : .
Confirm Password	Enter the new password again here for confirmation.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

➜ **Note**

Note the permitted characters for WBM passwords!
If passwords with invalid characters are set for the WBM outside the WBM (e.g., from a USB keyboard), access to the pages directly on the display is no longer possible because only permitted characters are available from the virtual keyboard.

➜ **Note**

General Rights of WBM Users
The WBM users "admin" and "user" have rights beyond the WBM to configure the system and install software.

User administration for controller applications is configured and managed separately.

17.2.1.3   "Fieldbus" Tab

17.2.1.3.1 "OPC UA Configuration" Page

The settings for the OPC UA service are shown on the "OPC UA Configuration" page.

"OPC UA Server Configuration" Group

Table 130: WBM "OPC UA Configuration" Page – "OPC UA Server Configuration" Group

Parameter	Explanation
Enabled	Enable or disable the WAGO OPC UA Server here.
Log level	Select the log level. The following values can be set: Info / Debug / Warning / Error. With log level "Error," only error messages are read out; with log level "Info," status messages are read out too. The specific log level selection affects server reaction time. Therefore, select the lowest level necessary; e.g., "Debug" for in-depth analyses.
Ctrl Configuration name	Enter the configuration names the controller contains in the PLC Open Device Set.

Click the **[Submit]** button to apply the changes.

"OPC UA Server Security Settings" Group

Table 131: WBM "OPC UA Configuration" Page – "OPC UA Server Security Settings" Group

Parameter	Explanation
Anonymous Access	Permit anonymous access to the server. This requires that runtime port authentication also be deactivated.
Allow Password On Plaintext	Transfer of password in readable format
Security Modes	Security Mode of the OPC UA Server Depending on the operating mode you select, different OPC UA endpoints for setting up the connection are available: None: Only the OPC UA endpoint **None** is activated. This allows an unsecured connection to the OPC UA server to be established. None + Sign + SignAndEncrypt: The enpoints **None, Sign and SignAndEncrypt** are available. **Sign** provides an endpoint that is password protected. **SignAndEncrypt** specifies an endpoint that povides both a password and encryption. Sign + SignAndEncrypt: The **Sign** and **SignAndEncrypt** endpoints are available. SignAndEncrypt: Only the **SignAndEncrypt** enpoint is available.
Security Policies	Selection of security policies Here, you can set the encryption level for the OPC UA server. The following options are available for this: Aes128Sha256RsaOaep and better, Basic256Sha256 and better, Aes256Sha256RsaPss.

Click the **[Submit]** button to apply the changes.

17.2.1.3.2 "BACnet Status" Page

The "BACnet Status" page displays BACnet fieldbus and BACnet license specific information about your controller.

"BACnet Information" Group

Table 132: WBM Page "BACnet Status" – "BACnet Information" Group

Parameter	Meaning
State	This group shows whether the BACnet fieldbus is enabled or disabled.
Status Info	The status of the BACnet fieldbus is displayed.
Device-ID	The current device ID of the controller is displayed here.

"BACnet License" Group

Table 133: WBM Page "BACnet Status" – "BACnet License" Group

Parameter	Meaning
Type	The type of license is indicated here.
User Objects	The number of possible BACnet objects allowed by this license is displayed.

17.2.1.3.3 "BACnet Configuration" Page

You can make special settings for the BACnet fieldbus on this page.

Click the **[Submit]** button to apply a setting.
Changes made to the BACnet configuration are not applied until after a restart.
Use the WBM Reboot function to restart the stack/controller. Click the **[Restart]** button to restart the runtime. Do not shut down the controller too early!

"BACnet Service" Group

You can enable/disable the fieldbus in this group.

The "Service active" parameter must be enabled (default setting) for the BACnet fieldbus protocol to be used.

On a runtime restart a security message is displayed in a pop-up window asking if you really want to perform a restart.

Table 134: WBM Page "BACnet Configuration" – "BACnet Settings" Group

Parameter	Meaning
Service active	Enable/disable the BACnet fieldbus.
Runtime restart **[Restart]**	Use this button to restart the runtime.

"BACnet Settings" Group

The basic settings for the fieldbus are given in this group.

Table 135: WBM Page "BACnet Configuration" – "BACnet Settings" Group

Parameter	Meaning
Port number	Set the port for BACnet fieldbus communication.
Who-Is online interval time (sec)	Here, you can specify the intervals at which the controller transmits queries to the fieldbus about which other subscribers are online (minimum: 60 seconds).

"BACnet Data Reset" Group

In this group you can select the data to be deleted or reset on the next restart.

Table 136: WBM Page "BACnet Configuration" – "BACnet Data Reset" Group

Parameter	Meaning
Delete Persistence Data	Persistent BACnet data is deleted on the next restart.
Reset all BACnet Data and Settings to Default	The factory default settings for BACnet-specific settings and data is restored on the next restart.

17.2.1.3.4 "BACnet Storage Location" Page

You can specify settings for saving of BACnet-specific parameters on this page.

Changes are applied without having to restart.

"BACnet Persistence" Group

This group lets you select the storage location (SD card/internal flash) for the persistence data.

If the persistence settings are changed, a pop-up window warns that data loss may occur until the next persistence is completed.

Table 137: WBM Page "BACnet Storage Location" – "BACnet Persistence" Group

Parameter	Meaning	
Storage location	You can select the storage location for the persistence data. Selection is possible only when both storage options are available.	
	Internal-Flash	Data will be stored in the controller's internal memory.
	SD-Card	Data will be stored on the SD card. If "SD card" has been selected and the card is no longer inserted, this option is no longer enabled and only the "internal flash" option can be selected.

"BACnet Trendlog" Group

This group lets you select the storage location (SD card/internal flash) for the trend log data.

Table 138: WBM Page "BACnet Storage Location" – "BACnet Trendlog" Group

Parameter	Meaning	
Storage location	You can select the storage location for the trend log data. Selection is possible only when both storage options are available.	
	Internal-Flash	Data will be stored in the controller's internal memory.
	SD-Card	Data will be stored on the SD card. If "SD card" has been selected and the card is no longer inserted, this option is no longer enabled and only the "internal flash" option can be selected.

"BACnet Eventlog" Group

This group lets you select the storage location (SD card/internal flash) for the event log data.

Table 139: WBM Page "BACnet Storage Location" – "BACnet Eventlog" Group

Parameter	Meaning	
Storage location	Select the storage location for the event log data here. Selection is possible only when both storage options are available.	
	Internal-Flash	Data will be stored in the controller's internal memory.
	SD-Card	Data will be stored on the SD card. If "SD card" has been selected and the card is no longer inserted, this option is no longer enabled and only the "internal flash" option can be selected.

17.2.1.3.5 "BACnet Files" Page

You can exchange an override file in the controller on this page.

The changes only take effect after the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

"BACnet override.xml" Group

Table 140: WBM Page "BACnet Files" – "BACnet override.xml" Group

Parameter	Meaning
Choose file…	Select the desired file on the controller or PC here.
[Upload]	Use this button to transfer the selected file from the PC to the controller.

17.2.1.4 "Security" Tab

17.2.1.4.1 "OpenVPN / IPsec Configuration" Page

The "OpenVPN / IPsec Configuration" page displays the settings for OpenVPN and IPsec.

"OpenVPN" Group

Table 141: WBM "OpenVPN / IPsec Configuration" Page – "OpenVPN" Group

Parameter	Explanation	
Current State	The current status of the OpenVPN service is displayed.	
	stopped	The service is disabled.
	running	The service is enabled.
OpenVPN enabled	Enable or disable the OpenVPN service.	
openvpn.config	Select an OpenVPN configuration file to be transferred from PC to product or vice versa.	

Click the **[Submit]** button to apply a change.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file from the PC to the product, click **[Upload]** button.

To transfer a file from product to PC, click the **[Download]** button.

The changes only take effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

"IPsec" Group

Table 142: WBM "OpenVPN / IPsec Configuration" Page – "IPsec" Group

Parameter	Explanation	
Current State	The current status of the IPsec service is displayed.	
	stopped	The service is disabled.
	running	The service is enabled.
IPsec enabled	Enable or disable the IPsec service.	
ipsec.conf	Select an IPsec configuration file to be transferred from PC to product or vice versa.	
ipsec.secrets	Select an IPsec configuration file to be transferred from PC to product or vice versa.	

Click the **[Submit]** button to apply a change.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file from the PC to the product, click **[Upload]** button.

To transfer a file from product to PC, click the **[Download]** button.

The changes only take effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

17.2.1.4.2 "General Firewall Configuration" Page

The "General Firewall Configuration" page displays the global firewall settings.

"Global Firewall Parameter" Group

Table 143: WBM "General Firewall Configuration" Page – "Global Firewall Parameter" Group

Parameter	Explanation
Firewall enabled entirely	Enables/disables the complete functionality of the firewall. This setting has the highest priority. If the firewall is disabled, all other settings have no direct effect. The configuration of the other parameters is possible nevertheless so that you can set the firewall parameters correctly before you enable the firewall. This setting is independent of the "Filter enabled" setting in the "MAC address filter state bridge <n>" group on the "MAC address filter state bridge <n>" page.
ICMP echo broadcast protection	Enable or disable the "ICMP echo broadcast" protection.
Max. UDP connections per second	You can specify the maximum number of UDP connections per second.
Max. TCP connections per second	You can specify the maximum number of TCP connections per second.

Click **[Submit]** to apply the change. The change takes effect immediately.

17.2.1.4.3 "Interface Configuration" Page

The individual interfaces for the firewall settings are displayed on the "Interface Configuration" page.

"Firewall Configuration Bridge <n> / VPN / WAN" Group

A separate group is displayed for each configured bridge.
The settings in this group are based on the firewall configuration on the IP level.

Table 144: WBM "Interface Configuration" Page – "Firewall Configuration Bridge <n> / VPN / WAN" Group

Parameter	Explanation	
Firewall enabled for Interface	Enable or disable the firewall for the respective bridge.	
ICMP echo protection	Enable or disable the "ICMP echo" protection for the respective bridge. If you enable ICMP echo protection, all ICMP echo requests (pings) will be rejected and the ICMP echo limit per second and ICMP burst limit entries will be ineffective.	
ICMP echo limit per second	You can specify the maximum number of "ICMP pings" per second. Input is only effective when ICMP echo protection is disabled. "0" = "Disabled"	
ICMP burst limit (0 = disabled)	You can specify the maximum number of "ICMP echo bursts" per second. Input is only effective when ICMP echo protection is disabled. "0" = "Disabled"	
Service enabled	FTP/FTPES	Enable or disable the firewall for the respective service. The services themselves must be enabled or disabled separately on the "Ports and Services" page.
	FTPS (implicit)	
	HTTP	
	HTTPS	
	I/O-CHECK	
	PLC Runtime	
	PLC WebVisu – direct link (port 8080)	
	SSH	
	BootP/DHCP	
	DNS	
	SNMP	
	OPC UA (Port 4840)	
	BACnet (Port 47808)	
	PROFINET IO	
	DNP3 (port 20000)	
	IEC60870-5-104 (port 2404)	
	IEC61850 (port 102)	

Click the **[Submit]** button to apply the change. The change takes effect immediately.

17.2.1.4.4 "Configuration of MAC Address Filter" Page

The "Configuration of MAC address filter" page displays the firewall configuration on the ETHERNET level.

The "MAC Address Filter Whitelist" contains two default entries with the following values:

Description:	All WAGO devices
MAC address:	00:30:DE:00:00:00
MAC mask:	ff:ff:ff:00:00:00
Description.	Enable docker bridges
MAC address:	02:42:00:00:00:00
MAC mask:	ff:ff:00:00:00:00

If you enable the first default entry, this already allows communication between different WAGO devices in the network.

> **Note**
>
> **Enable the MAC address filter before activation!**
> Before activating the MAC address filter, you must enter and activate your own MAC address in the "MAC Address Filter Whitelist."
> Otherwise you cannot access the device via the ETHERNET. This also applies to other services that are used by your device, e.g., the IP configuration via DHCP.
> If the "MAC Address Filter Whitelist" does not contain the MAC address of your DHCP server, your device will lose its IP settings after the next refresh cycle and is then no longer accessible.
> If the "MAC Address Filter Whitelist" does not contain an entry, the activation of the filter is prevented.
> If at least one enabled address is entered, you will receive an appropriate warning before activation, which you have to acknowledge.
> The check described above is only performed in the WBM but not in the CBM!

"Global MAC address filter state" Group

Table 145: WBM "Configuration of MAC Address Filter" Page – "Global MAC address filter state" Group

Parameters	Explanation
Filter enabled	Enable or disable the global MAC address filter.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

"MAC address filter state Bridge <n>" Group

A separate group is displayed for each configured bridge.

Table 146: WBM "Configuration of MAC Address Filter" Page – "MAC address filter state Bridge <n>" Group

Parameter	Explanation
Filter enabled	Enable or disable here the MAC address filter for the specific bridge. This setting is independent of the "Firewall enabled entirely" setting on the General Firewall Configuration page.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

"MAC address filter whitelist" Group

Each list entry has its own area in the display.

Table 147: WBM "Configuration of MAC Address Filter" Page – "MAC address filter whitelist" Group

Parameters	Explanation
Description	Description of the devices or areas that can be enabled by activating the filter when the firewall is generally enabled. The description is only visible for entries initially available in the factory default settings.
MAC address	Displays the MAC address of the relevant list entry.
MAC mask	This displays the MAC mask of the relevant list entry.
Filter enabled	Enable or disable the filter for the relevant list entry.
Add filter to whitelist	Create a new list entry.
MAC address	Enter here the MAC address for a new list entry. You can enter 10 filters.
MAC mask	Enter the MAC mask for the new list entry.
Filter enabled	Enable or disable the filter for the new list entry.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

Click the appropriate **[Delete]** button to remove an existing list entry. The change takes effect immediately.

Click **[Add]** to accept a new list entry. You can enter 10 filters. The change takes effect immediately.

17.2.1.4.5 "Configuration of User Filter" Page

The "Configuration of User Filter" page displays the settings for custom firewall filters.

"User filter" Group

Each configured filter has its own area in the display.

Table 148: WBM "Configuration of User Filter" Page – "User Filter" Group

Parameters	Meaning	
Policy	This displays whether the network participant is permitted or excluded by the filter.	
Source IP address	The source IP address for the respective filter is displayed.	
Source Netmask	This displays the source netmask for the respective filter.	
Source Port	The source port number for the respective filter is displayed.	
Destination IP address	The destination IP address for the respective filter is displayed.	
Destination Netmask	The destination netmask for the respective filter is displayed.	
Destination Port	The destination port number for the respective filter is displayed.	
Protocol	The permitted protocols for the respective filter is displayed.	
Input interface	The permitted interfaces for the respective filter are displayed.	
Add new user filter	You can create up to 10 filters. You only have to enter values in the fields that are to be set for the filter. At least one value must be entered, all other fields can remain empty.	
Policy	Select here whether the network devices is to be allowed or excluded by the filter.	
	Allow	The network device is permitted.
	Drop	The network device is excluded.
Source IP address	Enter here the source IP address for the new filter.	
Source netmask	Enter here the source network mask for the new filter.	
Source port	Enter here the source port address for the new filter.	
Destination IP address	Enter here the destination IP address for the new filter.	
Destination subnet mask	Enter here the destination network mask for the new filter.	
Destination port	Enter here the destination port address for the new filter.	

Table 148: WBM "Configuration of User Filter" Page – "User Filter" Group

Parameters	Meaning	
Protocol	Enter here the protocols for the new filter.	
	TCP/ UDP	The TCP service and UDP service are filtered.
	TCP	The TCP service is filtered.
	UDP	The UDP service is filtered.
Input interface	Enter here the interfaces for the new filter.	
	Any	All interfaces are filtered.
	Bridge <n>	The interfaces assigned for bridge <n> are filtered. Only the configured bridges are displayed.
	VPN	The VPN interface is filtered.

Click **[Add]** to apply the new filter. The change takes effect immediately.

Click the **[Delete]** button to delete an existing filter. The change takes effect immediately.

17.2.1.4.6 "Certificates" Page

On the "Certificates" page, you will find options to install or delete certificates and keys.

"Installed Certificates" Group

Table 149: WBM "Configuration of OpenVPN and IPsec" Page – "Certificate List" Group

Parameters	Explanation
<certificate name>	The loaded certificates are displayed. If no certificate has been loaded. "No certificates existing" is displayed.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file PC to the product, click the **[Upload]** button. The changes take effect immediately.

The certificates are stored in the directory "/etc/certificates/" and the keys in the directory "/etc/certificates/keys/".

Click **[Delete]** to delete an entry. The changes take effect immediately.

"Installed Private Keys" Group

Table 150: WBM "Configuration of OpenVPN and IPsec" Page – "Private Key List" Group

Parameters	Meaning
<private key name>	The loaded keys are displayed. If no key has been loaded, "No private keys existing" is displayed.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file PC to the product, click the **[Upload]** button. The changes take effect immediately.

The certificates are stored in the directory "/etc/certificates/" and the keys in the directory "/etc/certificates/keys/".

Click **[Delete]** to delete an entry. The changes take effect immediately.

17.2.1.4.7 "Boot mode configuration" Page

See the "Boot mode configuration" page for boot option settings.

"Force internal boot" Group

Table 151: WBM Page "Boot mode configuration" – "Force internal boot" Group

Parameter	Meaning	
Boot mode	You set the boot option for the product.	
	Memory card or internal flash	You can boot from the internal flash or from the memory card.
	Internal flash only	You can only boot from the internal flash.

> **Note**
>
> **If you force booting from the internal flash, the device can no longer be booted from the memory card!**
> If a connection via ETHERNET is no longer possible due to problems or incorrect configuration, you have the option of making the product accessible again via the service interface and "WAGO Ethernet Settings".

Click the **[Submit]** button to apply a change. The change takes effect immediately.

17.2.1.4.8 "Security Settings" Page

The network security settings are found on the "Security Settings" page.

"TLS Configuration" Group

Table 152: "Security Settings" WBM Page – "TLS Configuration" Group

Parameters	Explanation	
TLS Configuration	You can set what TLS versions and cryptographic methods are allowed for HTTPS.	
	Standard	The Webserver allows TLS 1.0, TLS 1.1 and TLS 1.2, as well as cryptographic methods that are no longer considered secure.
	Strong	The Webserver only allows TLS Version 1.2 and strong algorithms. Older software and older operating systems may not support TLS 1.2.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

> **Note**
>
> **BSI TR-02102 Technical Guidelines**
> The rules for the "Strong" setting are based on the TR-02102 technical guidelines of the German Federal Office for Information Security (BSI).
> You can find the guidelines on the Internet at: https://www.bsi.bund.de > "Publications" > "Technical Guidelines."

17.2.1.4.9 "Advanced Intrusion Detection Environment (AIDE)" Page

The network security settings are available on the "Advanced Intrusion Detection Environment (AIDE)" page.

"Run AIDE check at startup" Group

Table 153: WBM "Advanced Intrusion Detection Environment (AIDE)" Page – "Run AIDE check at startup" Group

Parameter	Explanation
Service active	Here, you can activate/deactivate the "AIDE check" when the controller is started.

Click the **[Submit]** button to apply the changes. The changes only take effect when the controller restarts.

"Refresh Options" group

Table 154: WBM "Advanced Intrusion Detection Environment (AIDE)" Page – "Control AIDE and show log" Group

Parameter	Explanation	
Select Action	Select here the action to be executed.	
	readlog	The log data are displayed.
	init	The database is initialized and filled with the current values.
	check	The current values are compared against the values stored in the database.
	update	The current values are compared with the values stored in the database and the database then updated.
Read only the last n	Activate display of only the last n messages. You also specify the number of messages to be displayed.	
Automatic refresh interval (sec)	Select the checkbox to enable cyclic refresh. Enter the cycle time in seconds in which a cyclic refresh is performed. The label of the button ("Refresh"/"Start"/"Stop") changes depending on status.	

Click **[Refresh]** to update the display. The button is only displayed if the cyclic refresh is not enabled.

To enable cyclic refresh, click the **[Start]** button. The button is only displayed if cyclic refresh is enabled and has not yet started.

To stop cyclic refresh again, click the **[Stop]** button. The button only appears if cyclic refresh is enabled.

The cyclical refresh is performed for as long as the "Advanced Intrusion Detection Environment (AIDE)" page is open. If you change the WBM page, the

update is stopped until you call up the "Advanced Intrusion Detection Environment (AIDE)" page again.

The messages are displayed below the settings.

17.2.1.4.10   "WAGO Device Access" Page

On the "WAGO Device Access" page you will find settings for authentication when scanning the node.

→ | **Note**
Beta Status
In the present firmware version, the "WAGO Device Access" functionality is still in beta!

"Unauthenticated Requests" Group

Table 155: WBM Page "WAGO Device Access" – "Unauthenticated Requests" Group

Parameter	Meaning
Allow unauthenticated Device Scan	You set whether the node can be scanned without authentication. In the default setting, authentication is switched off. To increase the security level, you can enforce authentication for node scanning. In the current beta status, only head stations but no I/O modules are recognized when scanning!

Click the **[Submit]** button to apply a change. The change takes effect immediately.

17.2.1.5 "Diagnostic" Tab

17.2.1.5.1 "Log Message Viewer" Page

The settings for displaying diagnostic messages are shown on the "Log Message Viewer" page.

"Refresh Options" Group

Table 156: WBM "Log Message Viewer" Page – "Refresh Options" Group

Parameters	Meaning	
Read only the last	Activate display of only the last n messages. You also specify the number of messages to be displayed.	
Automatic refresh interval (sec)	Select the checkbox to enable cyclic refresh. Enter the cycle time in seconds in which a cyclic refresh is performed. The label of the button ("Refresh"/"Start"/"Stop") changes depending on status.	
Source	Select the source of the diagnostic messages. The drop-down list depends on the user who is logged in.	
	user	Default diagnostic messages only
	admin	Default diagnostic messages and all log files in the folder /var/log/*

To refresh the display or to enable cyclic refresh, click the **[Refresh]** button. This button is only displayed if the cyclic refresh is not enabled.

To enable cyclic refresh, click the **[Start]** button. The button is only displayed if cyclic refresh is enabled and has not yet started.

To stop cyclic refresh again, click the **[Stop]** button. The button only appears if cyclic refresh is enabled.

The cyclical refresh is performed for as long as the "Diagnostic Information" page is open. If you change the WBM page, the refresh is stopped until you call up the "Diagnostic Information" page again.

The messages are displayed below the settings.

17.2.1.5.2 "Download" Page

"Diagnostic Information" Group

Click the **[Download]** button to download diagnostic information from the device. An archive file is then created that contains the log messages, the firmware version and a list of the installed packages. This file is saved to the Downloads folder on your computer.

17.2.1.5.3 "Network Capture" Page

All the settings required for logging the network traffic on the device and downloading these logs are available on the "Network Capture" page.
The current status of network traffic logging is displayed.

"State" Group

Table 157: "Network Capture" Page – "State" Group

Parameter	Explanation
Current State	The current status of network traffic logging is displayed here.
Last Captured Package Count	Network packages already logged are displayed here.
Last Refresh Time	The last refresh time for Current State and Last Captured Package Count is displayed here.

"Configuration" Group

Table 158: "Network Capture" Page – "Configuration" Group

Parameter	Explanation	
Enable	Here, you can activate or deactivate logging.	
Rotate Log Files	Here, you can activate or deactivate rotating logging. When this option is activated, network traffic is recorded in up to three files of the set maximum file size. When the maximum file size for the first file is reached, the data is logged in a second file and then to a third file when the second file is full. When the maximum size of the third file is reached, the data in the first file is then overwritten.	
Max. Filesize	Specify the maximum file size for the data log file.	
Storage Location	Select the storage location for the logged data. Selection is possible only when both storage options are available.	
	Internal Flash	Data will be stored in the controller's internal memory.
	SD Card	Data will be stored on the SD card. If "SD card" has been selected and the card is no longer inserted, this option is no longer enabled and only the "Internal flash" option can be selected.
Listen On Network Interface	Here, select the network interface from which network traffic is to be logged. Any of the available network interfaces of the device can be selected.	

Click **[Submit]** to apply the change. The change takes effect immediately.

"Filter Configuration" Group

Table 159: "Network Capture" Page – "Filter Configuration" Group

Parameter	Explanation
Capture Filter	You can set capture filters here. These filters are used to log only the relevant or required data traffic. This enables you to record only the communication for one port, for example, or only from a defined IP address. More information on possible filter settings is given in the "Capture Filter" notes in the "Wireshark" documentation.

Click the **[Check]** button to check the specified "Capture Filter" for correctness.

Click **[Submit]** to apply the change. The change takes effect immediately.

"Log Download" Group

Table 160: "Network Capture" Page – "Log Download" Group

Parameter	Explanation
Select Log File	Select a log here that can be downloaded using the **[Download]** button.

Click the **[Download]** button to download the selected log from the device.

Click the **[Download All]** button to download all the logs from the device.

17.3   Process Data Architecture

The process image for the I/O modules on the local bus is built up word-by-word in the controller (with word alignment). The internal mapping method for data greater than one byte conforms to Intel formats.

The following section describes the representation for WAGO-I/O SYSTEM 750 (750 and 753 Series) I/O modules in the process image, as well as the configuration of the process values.

NOTICE

Equipment damage due to incorrect address!

To prevent any damage to the device in the field you must always take the process data for all previous byte or bit-oriented I/O modules into account when addressing an I/O module at any position in the fieldbus node.

Note

No direct access from fieldbus to the process image for I/O modules!
Any data that is required from the I/O module process image must be explicitly mapped in the CODESYS program to the data in the fieldbus process image and vice versa! Direct access is not possible!

17.3.1   Digital Input Modules

Digital input modules supply one bit of data per channel to specify the signal state for the corresponding channel. These bits are mapped into the Input Process Image.

Some digital modules have an additional diagnostic bit per channel in the Input Process Image. The diagnostic bit is used for detecting faults that occur (e.g., wire breaks and/or short circuits).

When analog input modules are also present in the node, the digital data is always appended after the analog data in the Input Process Image, grouped into bytes.

17.3.1.1   1 Channel Digital Input Module with Diagnostics

750-435

Table 161: 1 Channel Digital Input Module with Diagnostics

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						Diagnostic bit S 1	Data bit DI 1

17.3.1.2   2 Channel Digital Input Modules

750-400, -401, -405, -406, -407, -410, -411, -412, -427, -438, (and all variations), 753-400, -401, -405, -406, -410, -411, -412, -427, -429

Table 162: 2 Channel Digital Input Modules

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

17.3.1.3   2 Channel Digital Input Module with Diagnostics

750-419, -421, -424, -425,
753-421, -424, -425

Table 163: 2 Channel Digital Input Module with Diagnostics

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

17.3.1.4   2 Channel Digital Input Module with Diagnostics and Output Process Data

750-418,
753-418

The digital input module supplies a diagnostic and acknowledge bit for each input channel. If a fault condition occurs, the diagnostic bit is set. After the fault condition is cleared, an acknowledge bit must be set to re-activate the input. The diagnostic data and input data bit is mapped in the Input Process Image, while the acknowledge bit is in the Output Process Image.

Table 164: 2 Channel Digital Input Module with Diagnostics and Output Process Data

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
				Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

Output Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
				Acknowledge-ment bit Q 2 Channel 2	Acknowledge-ment bit Q 1 Channel 1	0	0

17.3.1.5   4 Channel Digital Input Modules

750-402, -403, -408, -409, -414, -415, -422, -423, -428, -432, -433, -1420, -1421, -1422, -1423
753-402, -403, -408, -409, -415, -422, -423, -428, -432, -433, -440

Table 165: 4 Channel Digital Input Modules

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
				Data bit DI 4 Channel 4	Data bit DI 3 Channel 3	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

17.3.1.6   8 Channel Digital Input Modules

750-430, -431, -436, -437, -1415, -1416, -1417, -1418,
753-430, -431, -434, -436, -437

Table 166: 8 Channel Digital Input Modules

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Data bit DI 8 Channel 8	Data bit DI 7 Channel 7	Data bit DI 6 Channel 6	Data bit DI 5 Channel 5	Data bit DI 4 Channel 4	Data bit DI 3 Channel 3	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

17.3.1.7   8 Channel Digital Input Module NAMUR with Diagnostics and Output Process Data

750-439

The digital input module NAMUR provides via one logical channel 2 byte for the input and output process image.

The signal state of NAMUR inputs DI1 … DI8 is transmitted to the fieldbus coupler/controller via input data byte D0.
The fault conditions are transmitted via input data byte D1.

The channels 1 … 8 are switched on or off via the output data byte D1.
The output data byte D0 is reserved and always has the value "0".

Table 167: 8 Channel Digital Input Module NAMUR with Diagnostics and Output Process Data

Input Process Image							
Input byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Signal status DI 8 Channel 8	Signal status DI 7 Channel 7	Signal status DI 6 Channel 6	Signal status DI 5 Channel 5	Signal status DI 4 Channel 4	Signal status DI 3 Channel 3	Signal status DI 2 Channel 2	Signal status DI 1 Channel 1
Input byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Wire break /short circuit Data bit DI 8 Channel 8	Wire break /short circuit Data bit DI 7 Channel 7	Wire break /short circuit Data bit DI 6 Channel 6	Wire break /short circuit Data bit DI 5 Channel 5	Wire break /short circuit Data bit DI 4 Channel 4	Wire break /short circuit Data bit DI 3 Channel 3	Wire break /short circuit Data bit DI 2 Channel 2	Wire break /short circuit Data bit DI 1 Channel 1

Output Process Image							
Output byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	0	0	0	0
Output byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
DI Off 8 Channel 8 *)	DI Off 7 Channel 7 *)	DI Off 6 Channel 6 *)	DI Off 5 Channel 5 *)	DI Off 4 Channel 4 *)	DI Off 3 Channel 3 *)	DI Off 2 Channel 2 *)	DI Off 1 Channel 1 *)

*)   0: Channel ON
     1: Channel OFF

17.3.1.8   8 Channel Digital Input Module PTC with Diagnostics and Output Process Data

750-1425

The digital input module PTC provides via one logical channel 2 byte for the input and output process image.

The signal state of PTC inputs DI1 … DI8 is transmitted to the fieldbus coupler/controller via input data byte D0.
The fault conditions are transmitted via input data byte D1.

The channels 1 … 8 are switched on or off via the output data byte D1.
The output data byte D0 is reserved and always has the value "0".

Table 168: 8 Channel Digital Input Module PTC with Diagnostics and Output Process Data

Input Process Image							
Input Byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Signal status DI 8 Channel 8	Signal status DI 7 Channel 7	Signal status DI 6 Channel 6	Signal status DI 5 Channel 5	Signal status DI 4 Channel 4	Signal status DI 3 Channel 3	Signal status DI 2 Channel 2	Signal status DI 1 Channel 1
Input Byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Wire break /short circuit Data bit DI 8 Channel 8	Wire break /short circuit Data bit DI 7 Channel 7	Wire break /short circuit Data bit DI 6 Channel 6	Wire break /short circuit Data bit DI 5 Channel 5	Wire break /short circuit Data bit DI 4 Channel 4	Wire break /short circuit Data bit DI 3 Channel 3	Wire break /short circuit Data bit DI 2 Channel 2	Wire break /short circuit Data bit DI 1 Channel 1

Output Process Image							
Output Byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	0	0	0	0
Output Byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
DI Off 8 Channel 8 *)	DI Off 7 Channel 7 *)	DI Off 6 Channel 6 *)	DI Off 5 Channel 5 *)	DI Off 4 Channel 4 *)	DI Off 3 Channel 3 *)	DI Off 2 Channel 2 *)	DI Off 1 Channel 1 *)

*)   0: Channel ON
     1: Channel OFF

17.3.1.9   16 Channel Digital Input Modules

750-1400, -1402, -1405, -1406, -1407

Table 169: 16 Channel Digital Input Modules

Input Process Image							
Input Byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Data bit DI 8 Channel 8	Data bit DI 7 Channel 7	Data bit DI 6 Channel 6	Data bit DI 5 Channel 5	Data bit DI 4 Channel 4	Data bit DI 3 Channel 3	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1
Input Byte D1							
Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8
Data bit DI 16 Channel 16	Data bit DI 15 Channel 15	Data bit DI 14 Channel 4	Data bit DI 13 Channel 13	Data bit DI 12 Channel 12	Data bit DI 11 Channel 11	Data bit DI 10 Channel 10	Data bit DI 9 Channel 9

17.3.2 Digital Output Modules

Digital output modules use one bit of data per channel to control the output of the corresponding channel. These bits are mapped into the Output Process Image.

Some digital modules have an additional diagnostic bit per channel in the Input Process Image. The diagnostic bit is used for detecting faults that occur (e.g., wire breaks and/or short circuits). For modules with diagnostic bit is set, also the data bits have to be evaluated.

When analog output modules are also present in the node, the digital image data is always appended after the analog data in the Output Process Image, grouped into bytes.

17.3.2.1 1 Channel Digital Output Module with Input Process Data

750-523

The digital output module delivers 1 bit via a process value Bit in the output process image, which is illustrated in the input process image. This status image shows "manual mode".

Table 170: 1 Channel Digital Output Module with Input Process Data

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						not used	Status bit "Manual Operation"

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						not used	controls DO 1 Channel 1

17.3.2.2 2 Channel Digital Output Modules

750-501, -502, -509, -512, -513, -514, -517, -535, -538, (and all variations), 753-501, -502, -509, -512, -513, -514, -517

Table 171: 2 Channel Digital Output Modules

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						controls DO 2 Channel 2	controls DO 1 Channel 1

17.3.2.3 2 Channel Digital Input Modules with Diagnostics and Input Process Data

750-507 (-508), -522,
753-507

The digital output modules have a diagnostic bit for each output channel. When an output fault condition occurs (i.e., overload, short circuit, or broken wire), a diagnostic bit is set. The diagnostic data is mapped into the Input Process Image, while the output control bits are in the Output Process Image.

Table 172: 2 Channel Digital Input Modules with Diagnostics and Input Process Data

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						controls DO 2 Channel 2	controls DO 1 Channel 1

750-506,
753-506

The digital output module has 2-bits of diagnostic information for each output channel. The 2-bit diagnostic information can then be decoded to determine the exact fault condition of the module (i.e., overload, a short circuit, or a broken wire). The 4-bits of diagnostic data are mapped into the Input Process Image, while the output control bits are in the Output Process Image.

Table 173: 2 Channel Digital Input Modules with Diagnostics and Input Process Data 75x-506

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				Diagnostic bit S 3 Channel 2	Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1	Diagnostic bit S 0 Channel 1

Diagnostic bits S1/S0, S3/S2: = '00'   standard mode
Diagnostic bits S1/S0, S3/S2: = '01'   no connected load/short circuit against +24 V
Diagnostic bits S1/S0, S3/S2: = '10'   Short circuit to ground/overload

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				not used	not used	controls DO 2 Channel 2	controls DO 1 Channel 1

17.3.2.4 4 Channel Digital Output Modules

750-504, -515, -516, -519, -531,
753-504, -516, -531, -540

Table 174: 4 Channel Digital Output Modules

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

17.3.2.5 4 Channel Digital Output Modules with Diagnostics and Input Process Data

750-532, -539

The digital output modules have a diagnostic bit for each output channel. When an output fault condition occurs (i.e., overload, short circuit, or broken wire), a diagnostic bit is set. The diagnostic data is mapped into the Input Process Image, while the output control bits are in the Output Process Image.

Table 175: 4 Channel Digital Output Modules with Diagnostics and Input Process Data

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				Diagnostic bit S 4 Channel 4	Diagnostic bit S 3 Channel 3	Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1

Diagnostic bit S = '0'   no Error
Diagnostic bit S = '1'   overload, short circuit, or broken wire

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

17.3.2.6 8 Channel Digital Output Module

750-530, -536, -1515, -1516,
753-530, -534, 536

Table 176: 8 Channel Digital Output Module

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 8 Channel 8	controls DO 7 Channel 7	controls DO 6 Channel 6	controls DO 5 Channel 5	controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

17.3.2.7   8 Channel Digital Output Modules with Diagnostics and Input Process Data

750-537,
753-537

The digital output modules have a diagnostic bit for each output channel. When an output fault condition occurs (i.e., overload, short circuit, or broken wire), a diagnostic bit is set. The diagnostic data is mapped into the Input Process Image, while the output control bits are in the Output Process Image.

Table 177: 8 Channel Digital Output Modules with Diagnostics and Input Process Data

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Diagnostic bit S 8 Channel 8	Diagnostic bit S 7 Channel 7	Diagnostic bit S 6 Channel 6	Diagnostic bit S 5 Channel 5	Diagnostic bit S 4 Channel 4	Diagnostic bit S 3 Channel 3	Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1

Diagnostic bit S = '0'   no Error
Diagnostic bit S = '1'   overload, short circuit, or broken wire

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 8 Channel 8	controls DO 7 Channel 7	controls DO 6 Channel 6	controls DO 5 Channel 5	controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

17.3.2.8   16 Channel Digital Output Modules

750-1500, -1501, -1504, -1505

Table 178: 16 Channel Digital Output Modules

Output Process Image							
Output Byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 8 Channel 8	controls DO 7 Channel 7	controls DO 6 Channel 6	controls DO 5 Channel 5	controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1
Output Byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 16 Channel 16	controls DO 15 Channel 15	controls DO 14 Channel 14	controls DO 13 Channel 13	controls DO 12 Channel 12	controls DO 11 Channel 11	controls DO 10 Channel 10	controls DO 9 Channel 9

17.3.2.9   8 Channel Digital Input/Output Modules

750-1502, -1506

Table 179: 8 Channel Digital Input/Output Modules

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Data bit DI 8 Channel 8	Data bit DI 7 Channel 7	Data bit DI 6 Channel 6	Data bit DI 5 Channel 5	Data bit DI 4 Channel 4	Data bit DI 3 Channel 3	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 8 Channel 8	controls DO 7 Channel 7	controls DO 6 Channel 6	controls DO 5 Channel 5	controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

17.3.3 Analog Input Modules

The analog input modules provide 16-bit measured data and 8 control/status bits per channel.

The controller only uses the 8 control/status bits internally for configuration/parameterization (e.g., via WAGO-I/O-*CHECK*).

Therefore, only the 16-bit measurement values for each channel are in Intel format and are mapped by word in the input process image for the controller.

When digital input modules are also present in the node, the analog input data is always mapped into the Input Process Image in front of the digital data.

Information

Information on the structure of control and status bytes
For detailed information on the structure of a particular I/O module's control/status bytes, please refer to that module's manual. Manuals for each module can be found on the Internet at www.wago.com.

17.3.3.1 1 Channel Analog Input Modules

750-491, (and all variations)

Table 180: 1 Channel Analog Input Modules

Input Process Image			
Offset	Byte Destination		Description
	High Byte	Low Byte	
0	D1	D0	Measured Value U_D
1	D3	D2	Measured Value U_{ref}

17.3.3.2 2 Channel Analog Input Modules

750-452, -454, -456, -461, -462, -464 (2-Channel Operation) -465, -466, -467, -469, -470, -472, -473, -474, -475, 476, -477, -478, -479, -480, -481, -483, -485, -487, -492, (and all variations),
753-452, -454, -456, -461, -465, -466, -467, -469, -472, -474, -475, -476, -477, -478, -479, -483, -492, (and all variations)

Table 181: 2 Channel Analog Input Modules

Input Process Image			
Offset	Byte Destination		Description
	High Byte	Low Byte	
0	D1	D0	Measured Value Channel 1
1	D3	D2	Measured Value Channel 2

17.3.3.3   2 Channel Analog Input Modules HART

750-482, -484, (and all variations),
753-482

The HART I/O module provides two different process images depending on the set operating mode.

For the pure analog values 4 mA ... 20 mA, the HART I/O module transmits 16 bit measured values per channel as an analog input module, which are mapped by word.

In operating mode "6 Byte Mailbox", the HART I/O module provides the fieldbus coupler / controller with a 12-byte input and output process image via a logical channel. For the control/status byte and the dummy byte, an acyclic channel (mailbox) for the process value communication is embedded in the process image, which occupies 6 bytes of data. This is followed by the measured values for channels 1 and 2.

HART commands are executed via the WAGO-IEC function blocks of the "WagoLibHart_0x.lib" library. The data is tunneled to the application via the mailbox and decoded by means of the library, so that the evaluation and processing takes place directly at the application level.

The operating mode is set using the WAGO-I / O-*CHECK* commissioning tool.

Table 182: 2-Channel Analog Input Modules HART

Input Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**Low Byte**		
0	D1	D0	Measured Value Channel 1	
1	D3	D2	Measured Value Channel 2	

Table 183:: 2 Channel Analog Input Modules HART + 6 bytes Mailbox

Input Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**Low Byte**		
0	Internal Use	S0	Internal used	Status byte
1	MBX_RES	MBX_RES	Response data from mailbox	
2	MBX_RES	MBX_RES		
3	MBX_RES	MBX_RES		
4	D1	D0	Measured Value Channel 1	
5	D3	D2	Measured Value Channel 2	

Output Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	-	C0	Control byte
1	MBX_REQ	MBX_REQ	Request data from mailbox
2	MBX_REQ	MBX_REQ	
3	MBX_REQ	MBX_REQ	
4	-	-	Not used
5	-	-	

17.3.3.4 4 Channel Analog Input Modules

750-450, -453, -455, -457, -459, -460, -463, -464 (4-Channel Operation), -468, -471, -468, (and all variations),
753-453, -455, -457, -459

Table 184: 4 Channel Analog Input Modules

Input Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	D1	D0	Measured Value Channel 1
1	D3	D2	Measured Value Channel 2
2	D5	D4	Measured Value Channel 3
3	D7	D6	Measured Value Channel 4

17.3.3.5   8 Channel Analog Input Modules

750-451, 750-458, 750-496, 750-497

Table 185: 8 Channel Analog Input Modules

Input Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	D1	D0	Measured Value Channel 1
1	D3	D2	Measured Value Channel 2
2	D5	D4	Measured Value Channel 3
3	D7	D6	Measured Value Channel 4
4	D9	D8	Measured Value Channel 5
5	D11	D10	Measured Value Channel 6
6	D13	D12	Measured Value Channel 7
7	D15	D14	Measured Value Channel 8

17.3.3.6   3-Phase Power Measurement Module

750-493

The above Analog Input Modules have a total of 9 bytes of user data in both the Input and Output Process Image (6 bytes of data and 3 bytes of control/status). The following tables illustrate the Input and Output Process Image, which has a total of 6 words mapped into each image.
Word alignment is applied.

Table 186: 3-Phase Power Measurement Module

Input Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	-	S0	Status byte 0
1	D1	D0	Input data word 1
2	-	S1	Status byte 1
3	D3	D2	Input data word 2
4	-	S2	Status byte 2
5	D5	D4	Input data word 3

Output Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	-	C0	Control byte 0
1	D1	D0	Output data word 1
2	-	C1	Control byte 1
3	D3	D2	Output data word 2
4	-	C2	Control byte 2
5	D5	D4	Output data word 3

750-494, -495, (and all variations)

The 3-Phase Power Measurement Modules 750-494, -495, (and all variations) have a total of 24 bytes of user data in both the Input and Output Process Image (16 bytes of data and 8 bytes of control/status).

Table 187: 3-Phase Power Measurement Modules 750-494, -495, (and all variations)

Input Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	S1	S0	Status word
1	S3	S2	Extended status word 1
2	S5	S4	Extended status word 2
3	S7	S6	Extended status word 3
4	D1	D0	Process value 1
5	D3	D2	
6	D5	D4	Process value 2
7	D7	D6	
8	D9	D8	Process value 3
9	D11	D10	
10	D13	D12	Process value 4
11	D15	D14	

Output Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	S1	S0	Control word
1	S3	S2	Extended control word 1
2	S5	S4	Extended control word 2
3	S7	S6	Extended control word 3
4	-	-	-
5	-	-	
6	-	-	-
7	-	-	
8	-	-	-
9	-	-	
10	-	-	-
11	-	-	

17.3.4   Analog Output Modules

The analog output modules provide 16-bit output values and 8 control/status bits per channel.

The controller only uses the 8 control/status bits internally for configuration/parameterization (e.g., via WAGO-I/O-*CHECK*).

Therefore, only the 16-bit measurement values for each channel are in Intel format and are mapped by word in the output process image for the controller.

When digital output modules are also present in the node, the analog output data is always mapped into the Output Process Image in front of the digital data.

Information

Information on the structure of control and status bytes
For detailed information on the structure of a particular I/O module's control/status bytes, please refer to that module's manual. Manuals for each module can be found on the Internet at www.wago.com.

17.3.4.1   2 Channel Analog Output Modules

750-550, -552, -554, -556, -560, -562, 563, -585, -586, (and all variations),
753-550, -552, -554, -556

Table 188: 2 Channel Analog Output Modules

Output Process Image			
Offset	Byte Destination		Description
	High Byte	Low Byte	
0	D1	D0	Output Value Channel 1
1	D3	D2	Output Value Channel 2

17.3.4.2   4 Channel Analog Output Modules

750-553, -555, -557, -559,
753-553, -555, -557, -559

Table 189: 4 Channel Analog Output Modules

Output Process Image			
Offset	Byte Destination		Description
	High Byte	Low Byte	
0	D1	D0	Output Value Channel 1
1	D3	D2	Output Value Channel 2
2	D5	D4	Output Value Channel 3
3	D7	D6	Output Value Channel 4

17.3.5   Specialty Modules

WAGO has a host of Specialty I/O modules that perform various functions. With individual modules beside the data bytes also the control/status byte is mapped in the process image.

The control/status byte is required for the bidirectional data exchange of the module with the higher-ranking control system. The control byte is transmitted from the control system to the module and the status byte from the module to the control system.
This allows, for example, setting of a counter with the control byte or displaying of overshooting or undershooting of the range with the status byte.

The control/status byte always is in the process image in the Low byte.

Information

Information about the structure of the Control/Status byte
For detailed information about the structure of a particular module's control/status byte, please refer to that module's manual. Manuals for each module can be found on the Internet under: www.wago.com.

17.3.5.1   Counter Modules

750-404, (and all variations except of /000-005),
753-404, -404/000-003

The above Counter Modules have a total of 5 bytes of user data in both the Input and Output Process Image (4 bytes of counter data and 1 byte of control/status). The counter value is supplied as 32 bits. The following tables illustrate the Input and Output Process Image, which has a total of 3 words mapped into each image. Word alignment is applied.

Table 190: Counter Modules 750-404, (and all variations except of /000-005), 753-404, -404/000-003

Input Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	S	Status byte
1	D1	D0	Counter value
2	D3	D2	

Output Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	C	Control byte
1	D1	D0	Counter setting value
2	D3	D2	

750-404/000-005,
753-404/000-005

The above Counter Modules have a total of 5 bytes of user data in both the Input and Output Process Image (4 bytes of counter data and 1 byte of control/ status). The two counter values are supplied as 32 bits. The following tables illustrate the Input and Output Process Image, which has a total of 3 words mapped into each image. Word alignment is applied.

Table 191: Counter Modules 750-404/000-005, 753-404/000-005

Input Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	S	Status byte
1	D1	D0	Counter Value of Counter 1
2	D3	D2	Counter Value of Counter 2

Output Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	C	Control byte
1	D1	D0	Counter Setting Value of Counter 1
2	D3	D2	Counter Setting Value of Counter 2

750-633

The above Counter Module has a total of 5 bytes of user data in both the Input and Output Process Image (4 bytes of counter data and 1 byte of control/ status). The following tables illustrate the Input and Output Process Image, which has a total of 3 words mapped into each image. Word alignment is applied.
The meaning of the output data depends on the set operating mode:
1   Up counter with enable input
2   Up/down counter with U/D input
3   Frequency counter
4   Gate time counter

Table 192: Counter Modules 750-633

Input Process Image			
Offset	Byte Designation		Description
	High Byte	Low Byte	
0	-	S	Status byte
1	D1	D0	Counter Value
2	D3	D2	

Output Process Image			
Offset	Byte Designation		Description
	High Byte	Low Byte	
0	-	C	Control byte
1	D1	D0	Counter Setting Value [1,2] watchdog time [3] reserved [4]
2	D3	D2	Counter Setting Value [1,2] reserved [3] reserved [4]

[1,2]   Up counter with enable input, Up /down counter with U / D input
[3]   Frequency counter
[4]   Gate time counter

750-638,
753-638

The above Counter Modules have a total of 6 bytes of user data in both the Input and Output Process Image (4 bytes of counter data and 2 bytes of control/status). The two counter values are supplied as 16 bits. The following tables illustrate the Input and Output Process Image, which has a total of 4 words mapped into each image. Word alignment is applied.

Table 193: Counter Modules 750-638, 753-638

Input Process Image			
Offset	Byte Designation		Description
	High Byte	Low Byte	
0	-	S0	Status byte of Counter 1
1	D1	D0	Counter Value of Counter 1
2	-	S1	Status byte of Counter 2
3	D3	D2	Counter Value of Counter 2

Output Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	C0	Control byte of Counter 1
1	D1	D0	Counter Setting Value of Counter 1
2	-	C1	Control byte of Counter 2
3	D3	D2	Counter Setting Value of Counter 2

17.3.5.2 Pulse Width Modules

750-511, (and all variations),
753-511

The above Pulse Width modules have a total of 6 bytes of user data in both the Input and Output Process Image (4 bytes of channel data and 2 bytes of control/status). The two channel values are supplied as 16 bits. Each channel has its own control/status byte. The following table illustrates the Input and Output Process Image, which has a total of 4 words mapped into each image. Word alignment is applied.

Table 194: Pulse Width Modules 750-511, /xxx-xxx, 753-511

Input and Output Process			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	C0/S0	Control/Status byte of Channel 1
1	D1	D0	Data Value of Channel 1
2	-	C1/S1	Control/Status byte of Channel 2
3	D3	D2	Data Value of Channel 2

17.3.5.3 Serial Interface Modules with Alternative Data Format

750-650, (and the variations /000-002, -004, -006, -009, -010, -011, -012, -013),
750-651, (and the variations /000-001, -002, -003),
750-653, (and the variations /000-002, -007),
753-650, -653

> **Note**
>
> **The process image of the / 003-000-variants depends on the parameterized operating mode!**
> With the freely parameterizable variations /003 000 of the serial interface modules, the desired operating mode can be set. Dependent on it, the process image of these modules is then the same, as from the appropriate variation.

The above Serial Interface Modules with alternative data format have a total of 4 bytes of user data in both the Input and Output Process Image (3 bytes of serial data and 1 byte of control/status). The following table illustrates the Input and

Output Process Image, which have a total of 2 words mapped into each image.
Word alignment is applied.

Table 195: Serial Interface Modules with Alternative Data Format

Input and Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	D0	C/S	Data byte	Control/status byte
1	D2	D1	Data bytes	

17.3.5.4   Serial Interface Modules with Standard Data Format

750-650/000-001, -014, -015, -016,
750-651/000-001,
750-653/000-001, -006

The above Serial Interface Modules with Standard Data Format have a total of 6 bytes of user data in both the Input and Output Process Image (5 bytes of serial data and 1 byte of control/status). The following table illustrates the Input and Output Process Image, which have a total of 3 words mapped into each image. Word alignment is applied.

Table 196: Serial Interface Modules with Standard Data Format

Input and Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	D0	C/S	Data byte	Control/status byte
1	D2	D1	Data bytes	
2	D4	D3		

17.3.5.5   Serial Interface Modules

750-652,
753-652

The size of the process image for the Serial Interface Module can be adjusted to 12, 24 or 48 bytes.
It consists of two status bytes (input) or control bytes (output) and the process data with a size of 6 to 46 bytes.

Thus, each Serial Interface Module uses between 8 and 48 bytes in the process image. The sizes of the input and output process images are always the same.

The process image sizes are set with the startup tool WAGO-I/O-*CHECK*.

Table 197: Serial Interface Modules 750-652, 753-652

Input and Output Process Image					
Process image size	**Offset**	**Byte Designation**		**Description**	
		High Byte	**Low Byte**		
8 bytes	0	C1/S1	C0/S0	Control/Status byte C1/S1	Control/Status byte C0/S0
	1	D1	D0	Prozess data (6-46 bytes)	
	2	D3	D2		
	3	D5	D4		
24 bytes*	4	D7	D6		
	…				
	11	D21	D20		
48 bytes	12	D23	D22		
	…				
	23	D45	D44		

*) Factory setting

17.3.5.6   Data Exchange Module

750-654, -654/000-001

The Data Exchange modules have a total of 4 bytes of user data in both the Input and Output Process Image. The following tables illustrate the Input and Output Process Image, which has a total of 2 words mapped into each image.
Word alignment is applied.

Table 198: Data Exchange Module 750-654, -654/000-001

Input and Output Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	D1	D0	Data bytes
1	D3	D2	

17.3.5.7   SSI Transmitter Interface Modules

750-630, and the variations /000-001, -002, -006, -008, -009, -011, -012, -013

> ### Note
>
> **The process image of the / 003-000-variants depends on the parameterized operating mode!**
> The operating mode of the configurable /003-000 I/O module versions can be set. Based on the operating mode, the process image of these I/O modules is then the same as that of the respective version.

The above SSI Transmitter Interface modules have a total of 4 bytes of user data in the Input Process Image, which has 2 words mapped into the image.
Word alignment is applied.

Table 199: SSI Transmitter Interface Modules

Input Process Image			
Offset	Byte Designation		Description
	High Byte	Low Byte	
0	D1	D0	Data bytes
1	D3	D2	

750-630/000-004, -005, -007

In the input process image, SSI transmitter interface modules with status occupy 5 usable bytes, 4 data bytes, and 1 additional status byte. A total of 3 words are assigned in the process image via word alignment.

Table 200: SSI Transmitter Interface I/O Modules with an Alternative Data Format (/000-004, -005, -007)

Input Process Image				
Offset	Byte Destination		Description	
	High Byte	High Byte		
0	-	S	not used	Status byte
1	D1	D0	Data bytes	
2	D3	D2		

17.3.5.8 Incremental Encoder Interface Modules

Incremental Encoder Interface Modules

750-631/000-004, -010, -011

The above Incremental Encoder Interface modules have 5 bytes of input data and 3 bytes of output data. The following tables illustrate the Input and Output Process Image, which have 4 words into each image. Word alignment is applied.

Table 201: Incremental Encoder Interface Modules 750-631/000-004, --010, -011

Input Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	-	S	not used	Status byte
1	D1	D0	Counter word	
2	-	-	not used	
3	D4	D3	Latch word	

Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	-	C	not used	Control byte
1	D1	D0	Counter setting word	
2	-	-	not used	
3	-	-	not used	

750-634

The above Incremental Encoder Interface module has 5 bytes of input data (6 bytes in cycle duration measurement mode) and 3 bytes of output data. The following tables illustrate the Input and Output Process Image, which has 4 words mapped into each image. Word alignment is applied.

Table 202: Incremental Encoder Interface Modules 750-634

Input Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	-	S	not used	Status byte
1	D1	D0	Counter word	
2	-	(D2) *)	not used	(Periodic time)
3	D4	D3	Latch word	

*)   If cycle duration measurement mode is enabled in the control byte, the cycle duration is given as a 24-bit value that is stored in D2 together with D3/D4.

Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	-	C	not used	Control byte
1	D1	D0	Counter setting word	
2	-	-	not used	
3	-	-		

750-637, (and all variations)

The above Incremental Encoder Interface Module has a total of 6 bytes of user data in both the Input and Output Process Image (4 bytes of encoder data and 2 bytes of control/status). The following table illustrates the Input and Output Process Image, which have 4 words mapped into each image. Word alignment is applied.

Table 203: Incremental Encoder Interface Modules 750-637, (and all variations)

Input and Output Process Image			
Offset	Byte Designation		Description
	High Byte	Low Byte	
0	-	C0/S0	Control/Status byte of Channel 1
1	D1	D0	Data Value of Channel 1
2	-	C1/S1	Control/Status byte of Channel 2
3	D3	D2	Data Value of Channel 2

Digital Pulse Interface module

750-635,
753-635

The above Digital Pulse Interface module has a total of 4 bytes of user data in both the Input and Output Process Image (3 bytes of module data and 1 byte of control/status). The following table illustrates the Input and Output Process Image, which have 2 words mapped into each image. Word alignment is applied.

Table 204: Digital Pulse Interface Modules 750-635, 753-635

Input and Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	D0	C0/S0	Data byte	Control/status byte
1	D2	D1	Data bytes	

17.3.5.9   DC-Drive Controller

750-636, -636/000-700, -636/000-800

The DC-Drive Controller maps 6 bytes into both the input and output process image. The data sent and received are stored in up to 4 input and output bytes (D0 ... D3). Two control bytes (C0, C1) and two status bytes (S0/S1) are used to control the I/O module and the drive.

In addition to the position data in the input process image (D0 … D3), it is possible to display extended status information (S2 … S5). Then the three control bytes (C1 … C3) and status bytes (S1 … S3) are used to control the data flow.

Bit 3 of control byte C1 (C1.3) is used to switch between the process data and the extended status bytes in the input process image (Extended Info_ON). Bit 3 of status byte S1 (S1.3) is used to acknowledge the switching process.

Table 205: DC-Drive Controller 750-636, -636/000-700, -636/000-800

Input Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	S1	S0	Status byte S1	Status byte S0
1	D1*) / S3**)	D0*) / S2**)	Actual position*) / Extended status byte S3**)	Actual position (LSB) / Extended status byte S2**)
2	D3*) / S5**)	D2*) / S4**)	Actual position (MSB) / Extended status byte S3**)	Actual position*) / Extended status byte S4**)

*)   ExtendedInfo_ON = '0'.
**)   ExtendedInfo_ON = '1'.

Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	C1	C0	Control byte C1	Control byte C0
1	D1	D0	Setpoint position	Setpoint position (LSB)
2	D3	D2	Setpoint position (MSB)	Setpoint position

17.3.5.10 Stepper Controller

750-670, -671, -672

The Stepper controller provides the fieldbus coupler/controller 12 bytes input and output process image via 1 logical channel. The data to be sent and received are stored in up to 7 output bytes (D0 … D6) and 7 input bytes (D0 … D6), depending on the operating mode.

Output byte D0 and input byte D0 are reserved and have no function assigned.

One I/O module control and status byte (C0, S0) and 3 application control and status bytes (C1 ... C3, S1 ... S3) provide the control of the data flow.

Switching between the two process images is conducted through bit 5 in the control byte (C0 (C0.5). Activation of the mailbox is acknowledged by bit 5 of the status byte S0 (S0.5).

Table 206: Stepper Controller 750-670, -671, -672

Input and Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	Reserviert	C0/S0	reserved	Control/Status byte C0/S0
1	D1	D0	Process data*) / Mailbox**)	
2	D3	D2		
3	D5	D4		
4	S3	D6	Control/Status byte C3/S3	Process data*) / reserved**)
5	C1/S1	C2/S2	Control/Status byte C1/S1	Control/Status byte C2/S2

*)   Cyclic process image (Mailbox disabled)

**)   Mailbox process image (Mailbox activated)

17.3.5.11 RTC Module

750-640

The RTC Module has a total of 6 bytes of user data in both the Input and Output Process Image (4 bytes of module data and 1 byte of control/status and 1 byte ID for command). The following table illustrates the Input and Output Process Image, which have 3 words mapped into each image. Word alignment is applied.

Table 207: RTC Module 750-640

Input and Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	ID	C/S	Command byte	Control/status byte
1	D1	D0	Data bytes	
2	D3	D2		

17.3.5.12 DALI Multi-Master Module

753-647

The DALI Multi-Master module occupies a total of 24 bytes in the input and output range of the process image.

The DALI Multi-Master module can be operated in "Easy" mode (default) and "Full" mode. "Easy" mode is used to transmit simply binary signals for lighting control. Configuration or programming via DALI master module is unnecessary in "Easy" mode.

Changes to individual bits of the process image are converted directly into DALI commands for a pre-configured DALI network. 22 bytes of the 24-byte process image can be used directly for switching of electronic ballasts (ECG), groups or scenes in "Easy" mode. Switching commands are transmitted via DALI and group addresses, where each DALI and each group address is represented by a 2-bit pair.

In full mode, the 24 bytes of the process image are used to tunnel a protocol using a mailbox interface. The process image consists of 1 byte for control / status and 23 bytes for the acyclic data.

The structure of the process data is described in detail in the following tables.

Table 208: DALI Multi-Master Module 753-647 in the "Easy" Mode

Input Process Image				
Offset	**Byte Designation**		**Note**	
	High Byte	**Low Byte**		
0	-	S	res.	Status, activate broadcast Bit 0: 1-/2-button mode Bit 2: Broadcast status ON/OFF Bit 1,3-7: -
1	DA4…DA7	DA0…DA3	Bit pair for DALI address DA0:	
2	DA12…DA15	DA8…DA11	Bit 1: Bit set = ON	
3	DA20…DA23	DA16…DA19	Bit not set = OFF	
4	DA28…DA31	DA24…DA27	Bit 2: Bit set = Error	
5	DA36…DA39	DA32…DA35	Bit not set = No error	
6	DA44…DA47	DA40…DA43	Bit pairs DA1 … DA63 similar to DA0.	
7	DA52…DA55	DA48…DA51		
8	DA60…DA63	DA56…DA59		
9	GA4…GA7	GA0…GA3	Bit pair for DALI group address GA0: Bit 1: Bit set = ON Bit not set = OFF	
10	GA12…GA15	GA8…GA11	Bit 2: Bit set = Error Bit not set = No error Bit pairs GA1 … GA15 similar to GA0.	
11	-	-	Not used	

DA = DALI address
GA = Group address

Output Process Image			
Offset	**Byte Designation**		**Note**
	High Byte	**Low Byte**	

0	-	C	res. Bit 0: Broadcast ON
			Bit 1: Broadcast OFF
			Bit 2: (1 button operation):
			- short: Broadcast ON/OFF
			- long: Broadcast dimming
			   brighter/darker
			Bit 2: (2 buttons operation):
			- short: Broadcast ON/OFF
			- long: Broadcast dimming brighter
			Bit 3: (1 button operation):
			   Broadcast ON/OFF
			Bit 3: (2 buttons operation):
			- short: Broadcast ON/OFF
			- long: Broadcast dimming darker
			Bit 4: Watchdog toggling (starting
			   from FW06 of the DALI Multi-
			   Master)
			Bit 5…7: reserved

1	DA4…DA7	DA0…DA3	Bit pair for DALI address: Bit 1 (1 button operation): - short: DA switch ON/OFF - long: dimming brighter/darker Bit 1 (2 buttons operation): - short: DA switch ON - long: dimming brighter Bit 2 (1 button operation): DA switch ON/OFF Bit 2 (2 buttons operation): - short: DA switch OFF - long: dimming darker
2	DA12…DA15	DA8…DA11	
3	DA20…DA23	DA16…DA19	
4	DA28…DA31	DA24…DA27	
5	DA36…DA39	DA32…DA35	
6	DA44…DA47	DA40…DA43	
7	DA52…DA55	DA48…DA51	
8	DA60…DA63	DA56…DA59	
9	GA4…GA7	GA0…GA3	Bit pair for DALI group address: Bit 1 (1 button operation): - short: GA switch ON/OFF - long: dimming brighter/darker Bit 1 (2 buttons operation): - short: GA switch ON - long: dimming brighter Bit 2 (1 button operation): GA switch ON/OFF Bit 2 (2 buttons operation): - short: GA switch OFF - long: dimming darker
10	GA12…GA15	GA8…GA11	
11	Bit 8…15	Bit 0…7	Switch scene 0…15

DA = DALI address
GA = Group address

Table 209: DALI Multi-Master Module 753-647 in the "Full" Mode

Input and Output Process Image				
Offset	**Byte Designation**		**Note**	
	High Byte	**Low Byte**		
0	MBX_C/S	C0/S0	Mailbox control/status byte	control/status byte
1	MBX1	MBX0	Mailbox	
2	MBX3	MBX2		
3	MBX5	MBX4		
4	MBX7	MBX6		
5	MBX9	MBX8		
6	MBX11	MBX10		
7	MBX13	MBX12		
8	MBX15	MBX14		
9	MBX17	MBX16		
10	MBX19	MBX18		
11	MBX21	MBX20		

17.3.5.13 LON® FTT Module

753-648

The process image of the LON® FTT module consists of a control/status byte and 23 bytes of bidirectional communication data that is processed by the WAGO-I/O-*PRO* function block "LON_01.lib". This function block is essential for the function of the LON® FTT module and provides a user interface on the control side.

Table 210: LON® FTT Module 753-648

Input and Output Process Image				
Offset	Byte Designation		Note	
	High Byte	Low Byte		
0	MBX_C/S	C0/S0	Mailbox control/status byte	control/status byte
1	MBX1	MBX0	Mailbox	
2	MBX3	MBX2		
3	MBX5	MBX4		
4	MBX7	MBX6		
5	MBX9	MBX8		
6	MBX11	MBX10		
7	MBX13	MBX12		
8	MBX15	MBX14		
9	MBX17	MBX16		
10	MBX19	MBX18		
11	MBX21	MBX20		

17.3.5.14 EnOcean Radio Receiver

750-642

The EnOcean radio receiver has a total of 4 bytes of user data in both the Input and Output Process Image (3 bytes of module data and 1 byte of control/status). The following tables illustrate the Input and Output Process Image, which have 2 words mapped into each image. Word alignment is applied.

Table 211: EnOcean Radio Receiver 750-642

Input Process Image				
Offset	Byte Destination		Description	
	High Byte	Low Byte		
0	D0	S	Data byte	Status byte
1	D2	D1	Data bytes	

Output Process Image				
Offset	Byte Destination		Description	
	High Byte	Low Byte		
0	-	C	not used	Control byte
1	-	-	not used	

17.3.5.15 MP Bus Master Module

750-643

The MP Bus Master Module has a total of 8 bytes of user data in both the Input and Output Process Image (6 bytes of module data and 2 bytes of control/status). The following table illustrates the Input and Output Process Image, which have 4 words mapped into each image. Word alignment is applied.

Table 212: MP Bus Master Module 750-643

Input and Output Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**Low Byte**		
0	C1/S1	C0/S0	Extended Control/ Status byte	Control/status byte
1	D1	D0	Data bytes	
2	D3	D2		
3	D5	D4		

17.3.5.16 *Bluetooth*® RF-Transceiver

750-644

The size of the process image for the *Bluetooth*® module can be adjusted to 12, 24 or 48 bytes.
It consists of one control byte (input) or status byte (output); an empty byte; an overlay able mailbox with a size of 6, 12 or 18 bytes (mode 2); and the *Bluetooth*® process data with a size of 4 to 46 bytes.
Thus, each *Bluetooth*® module uses between 12 and 48 bytes in the process image. The sizes of the input and output process images are always the same.

The first byte contains the control/status byte; the second contains an empty byte.

Process data attach to this directly when the mailbox is hidden. When the mailbox is visible, the first 6, 12 or 18 bytes of process data are overlaid by the mailbox data, depending on their size. Bytes in the area behind the optionally visible mailbox contain basic process data. The internal structure of the *Bluetooth*® process data can be found in the documentation for the *Bluetooth*® 750-644 RF Transceiver.

The mailbox and the process image sizes are set with the startup tool WAGO-I/O-*CHECK*.

Table 213: *Bluetooth*® RF-Transceiver 750-644

Input and Output Process Image					
Process image size	Offset	Byte Destination		Description	
		High Byte	Low Byte		
12 bytes	0	-	C0/S0	not used	Control/status byte
	1	D1	D0	Mailbox (0, 6, 12 or 18 words)/ Process data (4 … 46 words)	
	…	…	…		
	5	D9	D8		
24 bytes	6	D11	D10		
	…	…	…		
	11	D21	D20		
48 bytes*)	12	D23	D22		
	...	...	...		
	23	D45	D44		

*) Factory Setting

17.3.5.17 Vibration Velocity/Bearing Condition Monitoring VIB I/O

750-645

The Vibration Velocity/Bearing Condition Monitoring VIB I/O has a total of 12 bytes of user data in both the Input and Output Process Image (8 bytes of module data and 4 bytes of control/status). The following table illustrates the Input and Output Process Image, which have 8 words mapped into each image. Word alignment is applied.

Table 214: Vibration Velocity/Bearing Condition Monitoring VIB I/O 750-645

Input and Output Process Image				
Offset	Byte Destination		Description	
	High Byte	Low Byte		
0	-	C0/S0	not used	Control/status byte (log. Channel 1, Sensor input 1)
1	D1	D0	Data bytes (log. Channel 1, Sensor input 1)	
2	-	C1/S1	not used	Control/status byte (log. Channel 2, Sensor input 2)
3	D3	D2	Data bytes (log. Channel 2, Sensor input 2)	
4	-	C2/S2	not used	Control/status byte (log. Channel 3, Sensor input 1)
5	D5	D4	Data bytes (log. Channel 3, Sensor input 3)	
6	-	C3/S3	not used	Control/status byte (log. Channel 4, Sensor input 2)
7	D7	D6	Data bytes (log. Channel 4, Sensor input 2)	

17.3.5.18 KNX/EIB/TP1 Module

753-646

The KNX/TP1 module appears in router and device mode with a total of 24-byte user data within the input and output area of the process image, 20 data bytes and 2 control/status bytes. Even though the additional bytes S1 or C1 are transferred as data bytes, they are used as extended status and control bytes. The opcode is used for the read/write command of data and the triggering of specific functions of the KNX/EIB/TP1 module. Word-alignment is used to assign 12 words in the process image. Access to the process image is not possible in router mode. Telegrams can only be tunneled.

In device mode, access to the KNX data can only be performed via special function blocks of the IEC application. Configuration using the ETS engineering tool software is required for KNX.

Table 215: KNX/EIB/TP1 Module 753-646

Input and Output Process Image				
Offset	Byte Destination		Description	
	High Byte	Low Byte		
0	-	C0/S0	not used	Control/Status byte
1	C1/S1	OP	extended Control/Status byte	Opcode
2	D1	D0	Data byte 1	Data byte 0
3	D3	D2	Data byte 3	Data byte 2
4	D5	D4	Data byte 5	Data byte 4
5	D7	D6	Data byte 7	Data byte 6
6	D9	D8	Data byte 9	Data byte 8
7	D11	D10	Data byte 11	Data byte 10
8	D13	D12	Data byte 13	Data byte 12
9	D15	D14	Data byte 15	Data byte 14
10	D17	D16	Data byte 17	Data byte 16
11	D19	D18	Data byte 19	Data byte 18

17.3.5.19 AS-interface Master Module

750-655,
753-655

The length of the process image of the AS-interface master module can be set to fixed sizes of 12, 20, 24, 32, 40 or 48 bytes.
It consists of a control or status byte, a mailbox with a size of 0, 6, 10, 12 or 18 bytes and the AS-interface process data, which can range from 0 to 46 bytes.

The AS-interface master module has a total of 6 to maximally 24 words data in both the Input and Output Process Image. Word alignment is applied.

The first Input and output word, which is assigned to an AS-interface master module, contains the status / control byte and one empty byte.

Subsequently the mailbox data are mapped, when the mailbox is permanently superimposed (Mode 1).

In the operating mode with suppressible mailbox (Mode 2), the mailbox and the cyclical process data are mapped next.
The following words contain the remaining process dat.

The mailbox and the process image sizes are set with the startup tool WAGO-I/O-*CHECK*.

Table 216: AS-interface Master Module 750-655, 753-655

Input and Output Process Image					
Process image size	Offset	Byte Designation		Description	
		High Byte	Low Byte		
12 bytes	0	-	C0/S0	Not used	Control-/ Status byte
	1	D1	D0	Mailbox (0, 6, 10, 12 or 18 bytes)/ Process data (0-46 bytes)	
	…				
	5	D9	D8		
20 bytes	6	D11	D10		
	…				
	9	D17	D16		
24 bytes *	10	D19	D18		
	11	D21	D20		
32 bytes	12	D23	D22		
	…				
	15	D29	D28		
40 bytes	16	D31	D30		
	…				
	19	D37	D36		
48 bytes	12	D39	D38		
	…				
	23	D45	D44		

*) Factory Setting

17.3.6   System Modules

17.3.6.1   System Modules with Diagnostics

750-606

The modules provide 2 bits of diagnostics in the Input Process Image for monitoring of the internal power supply.

Table 217: System Modules with Diagnostics 750-606, -611

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
						Diagnostics bit S_out	Diagnostics bit S_in

750-610, -611

The modules provide 2 bits of diagnostics in the Input Process Image for monitoring of the internal power supply.

Table 218: System Modules with Diagnostics 750-610, -611

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
						Diagnostics bit S 2 Fuse	Diagnostics bit S 1 Fuse

17.3.6.2   Filter Module

750-624/020-002, -626/020-002

The Filter Module 750-624/020-002 and 750-626/020-002 equipped with surge suppression for the field side power supply have a total of 8 bits in both the Input and Output Process Image.

Table 219: Filter Modules 750-624/020-002, 750-626/020-002

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0V_MA	0V_PA	24V_MA	24V_PA	not used	PWR_DIAG	not used	VAL

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
not used	not used	not used	not used	not used	not used	not used	GFT

17.3.6.3   Binary Space Module

750-622

The Binary Space Modules behave alternatively like 2 channel digital input modules or output modules and seize depending upon the selected settings 1, 2, 3 or 4 bits per channel. According to this, 2, 4, 6 or 8 bits are occupied then either in the process input or the process output image.

Table 220: Binary Space Module 750-622 (with Behavior like 2 Channel Digital Input)

Input and Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
(Data bit DI 8)	(Data bit DI 7)	(Data bit DI 6)	(Data bit DI 5)	(Data bit DI 4)	(Data bit DI 3)	Data bit DI 2	Data bit DI 1

List of Figures

List of Tables

WAGO GmbH & Co. KG

Postfach 2880　•　D - 32385 Minden

Hansastraße 27　•　D - 32423 Minden

Phone:　　　　　+49 571 887 – 0

Fax:　　　　　　+49 571 887 – 844169

E-Mail:　　　　info@wago.com

Internet:　　　　www.wago.com