TECHDOCS

Manual

WAGO I/O System 750

750-8212(/xxx-xxx)

PFC200; G2; 2ETH RS

Controller PFC200; 2nd Generation; 2 x ETHERNET, RS-232/-485

Version 1.5.0, valid from FW Version 03.06.09(18)

WAGO Kontakttechnik GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Phone:	+49 (0) 571/8 87 – 0
Fax:	+49 (0) 571/8 87 – 1 69
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” controller (750-8212) and the variants listed in the table below.

Table 1: Variants

Item Number/Variant	Designation
750-8212	PFC200; G2; 2ETH RS
750-8212/025-000	PFC200; G2; 2ETH RS; T
750-8212/025-001	PFC200; G2; 2ETH RS; Tele; T
750-8212/025-002	PFC200; G2; 2ETH RS; Tele; T; ECO

Note

Documentation Validity for Variants
Unless otherwise indicated, the information given in this documentation applies to listed variants.

This documentation is only applicable from FW Version 03.06.09(18).

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 Kontakttechnik 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.
- AS-Interface® is a registered trademark of AS-International Association.
- BACnet® is a registered trademark of American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® is a registered trademark of the Bluetooth SIG, Inc.
- CiA® and CANopen® are registered trademarks of CAN in AUTOMATION – International Users and Manufacturers Group e. V.
- DALI is a registered trademark of Digital Illumination Interface Alliance (DiiA).
- EtherCAT® is a registered trademark and patented technology of Beckhoff Automation GmbH.
- EtherNet/IP™ is a registered trademark of Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® is a registered trademark of EnOcean GmbH.
- IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.
- KNX® is a registered trademark of KNX Association cvba.
- Linux® is a registered trademark of Linus Torvalds.
- LON® is a registered trademark of Echelon Corporation.
- Modbus® is a registered trademark of Schneider Electric, licensed to the Modbus Organization, Inc.
- PROFIBUS® is a registered trademark of Siemens AG.
- PROFINET® is a registered trademark of Siemens AG.
- Subversion® is a registered trademark of 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 2: 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 3: 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 Kontakttechnik GmbH & Co. KG reserves the right to provide for any alterations or modifications. WAGO Kontakttechnik 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.

2.1.4 Technical Condition of Specified Devices

The devices to be supplied ex works are equipped with hardware and software configurations, which meet the individual application requirements. These modules contain no parts that can be serviced or repaired by the user. The following actions will result in the exclusion of liability on the part of WAGO Kontakttechnik GmbH & Co. KG:

- Repairs,
- Changes to the hardware or software that are not described in the operating instructions,
- Improper use of the components.

Further details are given in the contractual agreements. Please send your request for modified and new hardware or software configurations directly to WAGO Kontakttechnik GmbH & Co. KG.

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 only one 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“ (750-8212) must be powered from SELV/PELV power supply(s)!

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” controller (750-8212) 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 Kontakttechnik 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 750-8212(PFC200; G2; 2ETH RS) 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.

Information

Further Information on the Use in Telecontrol Applications!
If the controller is used for telecontrol applications, observe the manuals “IEC 60870 Solution for programmable Controls of Telecontrol Technology, 759-911”, “IEC 61850 Solution for programmable Controls of Telecontrol Technology, 759-911” and “DNP3 Solution for programmable Controls of Telecontrol Technology, 759-911”.
These manuals are available in download area on the web page http://www.wago.com.

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.

Note

Number of connectable I/O modules to the controller “PFC200; 2ETH RS; Tele; T; ECO” (750-8202/025-002) is limited!
Please note the maximum number of I/O modules connected to this controller. You can operate at this controller with four I/O modules.
If the number of I/O modules is exceeded, internal bus communication cannot be held. This fault is indicated with error code 7-5 “Invalid configuration” (see section “Diagnostics”).

Automation tasks can be executed in all IEC 61131-3-compatible languages with the WAGO-*I/O-PRO* or ***e!****COCKPIT* programming system, depending on the runtime system set (CODESYS V2 or ***e!****RUNTIME*).
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.

Under CODESYS V2, the controller provides 16 MB of program memory (flash), 64 MB of data memory (RAM) as well as 128 kB of retentive memory (retain and flag variables in an integrated NVRAM) for IEC-61131-3 programming in CODESYS applications.
Under ***e!****RUNTIME*, 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) for IEC-61131-3 programming in CODESYS applications.

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:

- Modbus TCP Master/Slave
- Modbus UDP Master/Slave
- Modbus RTU Master/Slave (via RS-232 or RS-485)

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!

The fieldbus configuration can be defined with the WAGO-I/O-PRO or ***e!****COCKPIT* controller configuration, depending on the set runtime system (CODESYS V2 or ***e!****RUNTIME*).

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 Telnet server
- 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 Runtime Environment (CODESYS V2 or ***e!****RUNTIME*, selectable)

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.

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 Properties

4.1 Hardware Description

4.1.1 View

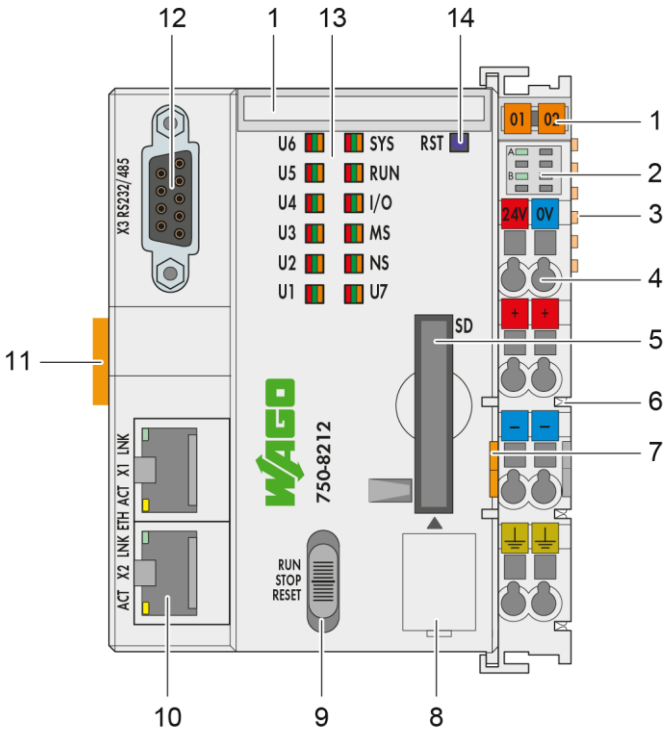


Figure 1: View

Table 4: 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	Communication interface – X3	“Connectors” > “Communication Interface”
13	LED indicators – system	“Display Elements” > “Fieldbus/System Indicating Elements”
14	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.

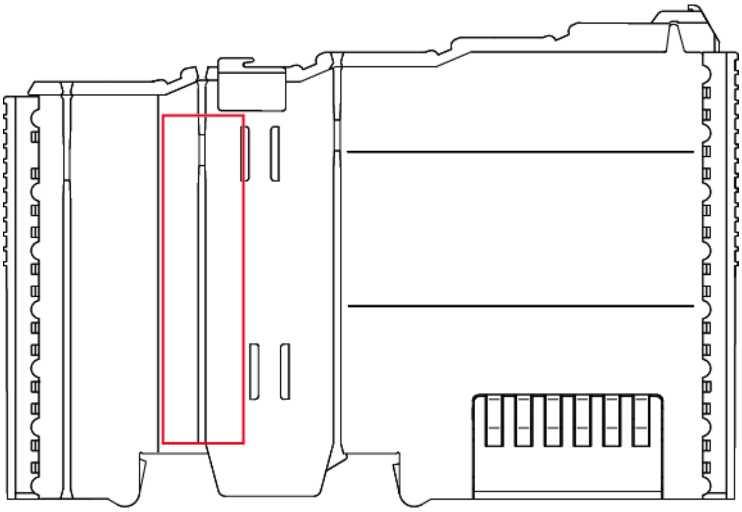


Figure 2: Marking Area for Serial Numbers

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

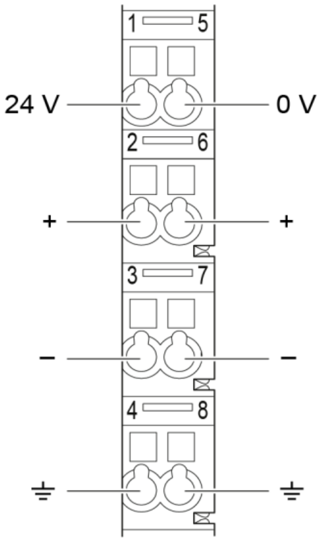


Figure 3: CAGE CLAMP® connections

Table 5: 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".

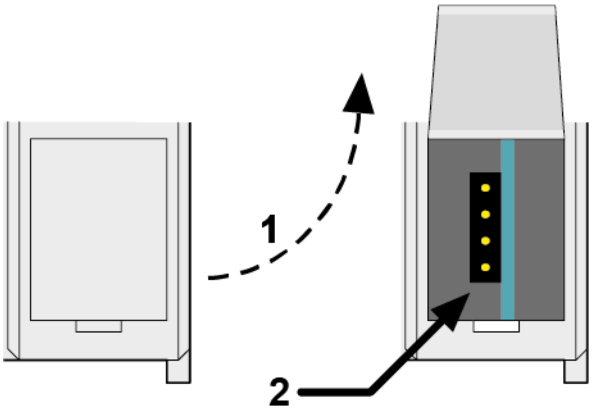


Figure 4: Service Interface (Closed and Open Flap)

Table 6: 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

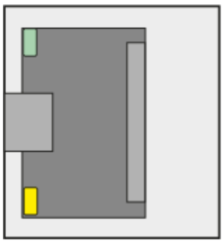


Figure 5: Network Connections – X1, X2

Table 7: 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 Communication Interface

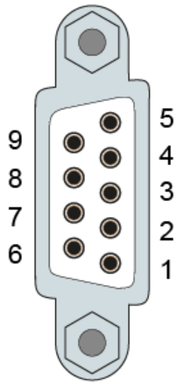


Figure 6: RS-232/RS-485 – Communication Interface – X3

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.

4.1.3.4.1 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).

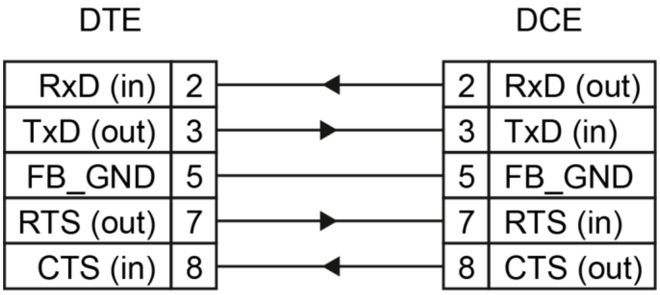


Figure 7: Termination with DTE-DCE Connection (1:1)

For a DCE-to-DCE connection, the signal connections are crossed (cross-over).

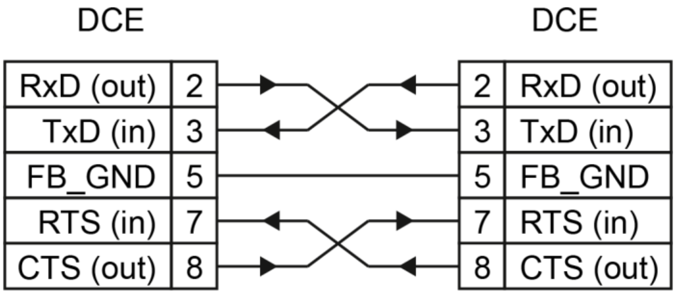


Figure 8: Termination with DCE-DCE Connection (Cross-Over)

4.1.3.4.2 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.

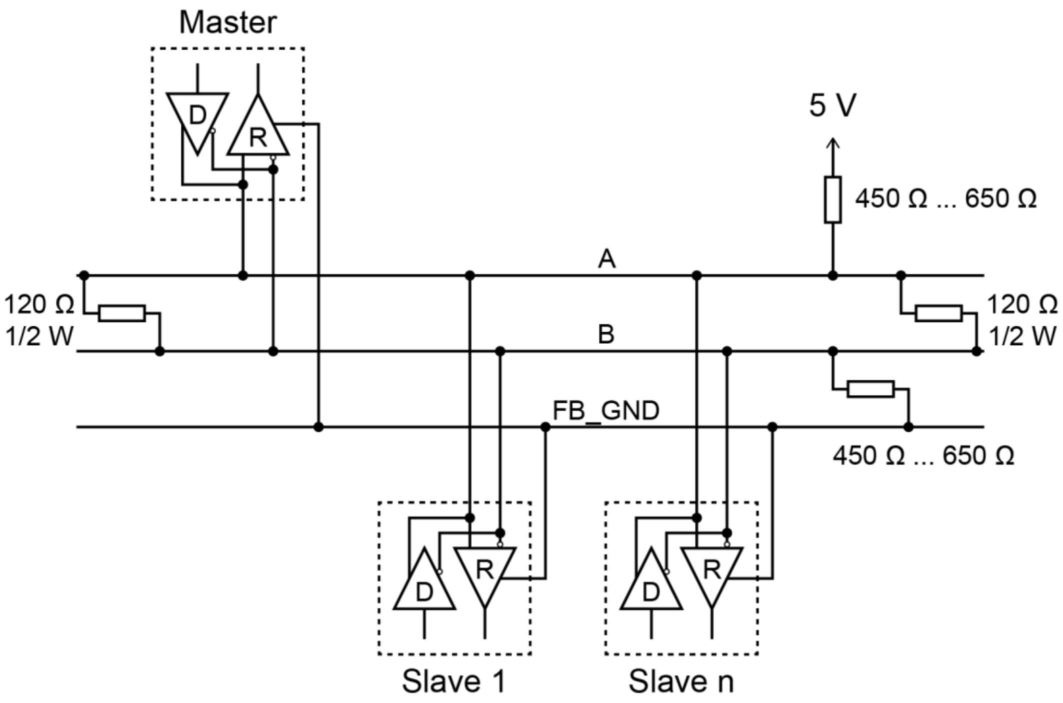


Figure 9: RS-485 Bus Termination

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.

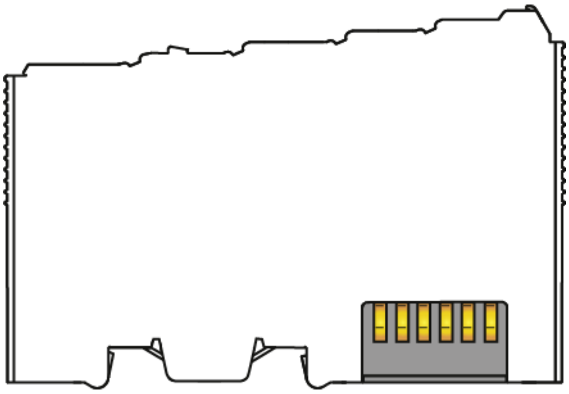


Figure 10: Data Contacts

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 750-8212is 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.

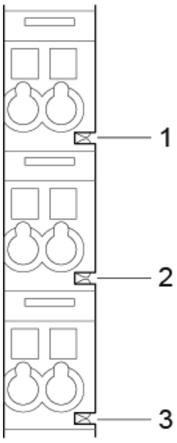


Figure 11: Power Jumper Contacts

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

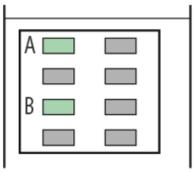


Figure 12: Power Supply Indicating Elements

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

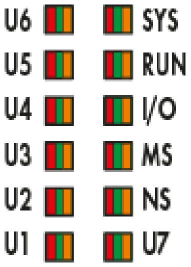


Figure 13: Indicating Elements for Fieldbus/System

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
U7	Red/Green/ Orange/Off	User LED 7, programmable using function blocks from the WAGO libraries to control the LEDs
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

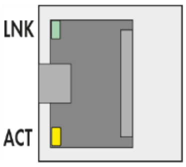


Figure 14: Indicating Elements, RJ-45 Jacks

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

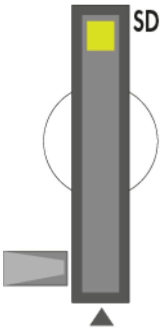


Figure 15: Indicating Elements, Memory Card Slot

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

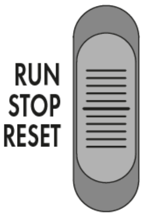


Figure 16: Mode Selector Switch

The function of the mode selector switch depends on the activated runtime system (CODESYS V2 or ***e!****RUNTIME*).

The following functions apply to the CODESYS V2 runtime system:

Table 15: Mode Selector Switch

Item	Activation	Function
RUN	Latching	**Normal mode** CODESYS V2 application runs.
STOP	Latching	**Stop** CODESYS V2 application stopped.
RESET	Spring-return	**Reset warm start** or **Reset cold start** (based on the duration of activation, see Section “Starting” > “Initiating Reset Functions”)

Other functions can also be initiated using the reset button.

The following functions apply to the ***e!****RUNTIME* runtime system:

Table 16: Mode Selector Switch

Position	Actuation	Function
RUN	Latching	**Normal operation** ***e!****RUNTIME* applications running.
STOP	Latching	**Stop** All ***e!****RUNTIME* 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

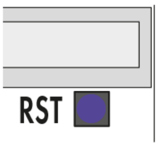


Figure 17: Reset Button

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

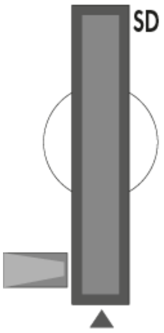


Figure 18: Slot for SD Memory Card

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

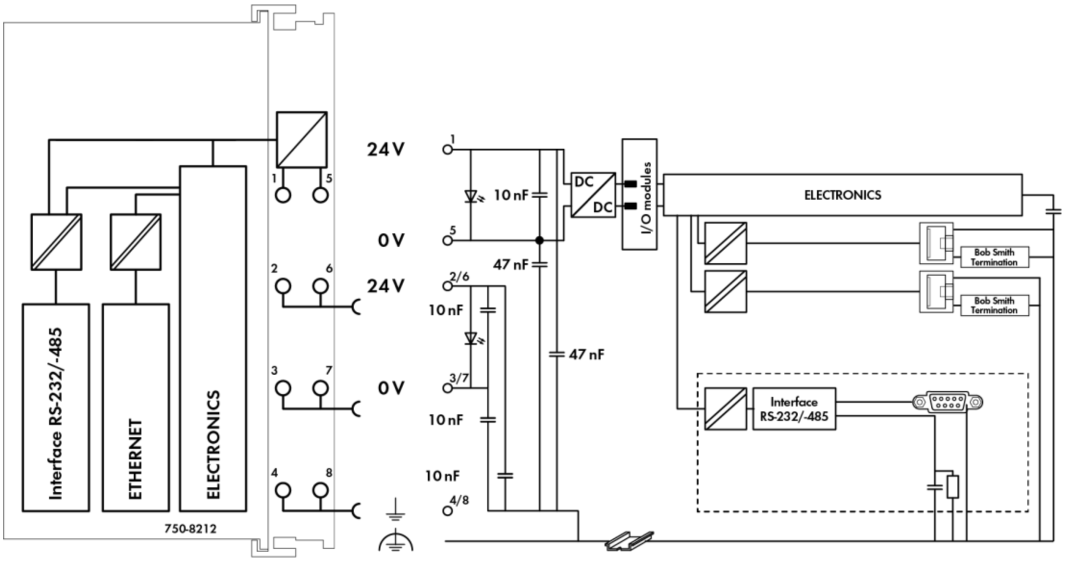


Figure 19: Schematic diagram

4.3 Technical Data

4.3.1 Mechanical Data

Table 17: Technical Data – Mechanical Data

Width	79 mm
Height (from upper edge of DIN 35 rail)	65 mm
Length	100 mm
Weight	214 g

4.3.2 System Data

Table 18: 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 19: 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 20: 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 21: Technical Data – Programming

Programming	CODESYS V2	WAGO-I/O-PRO V2.3
	***e!**RUNTIME*	***e!**COCKPIT*
IEC 61131-3		LD, FBD, ST, FC
CODESYS V2 memory configuration		
Program memory (Flash)		16 MByte
Data memory (RAM)		64 MByte
Non-volatile memory (NVRAM, Retain + Flags)		128 kByte
***e!**RUNTIME* memory configuration		
Program memory (flash)		32 MByte
Data memory (RAM)		128 MByte
Non-volatile memory (NVRAM, Retain + Flags)		128 kByte
Retain variables max.	CODESYS V2	10,000
	***e!**RUNTIME*	Not specified

4.3.6 Local Bus

Table 22: Technical Data – Local Bus

Number of I/O modules (per node)		64 (not 750-8212/025-002)
		4 (750-8212/025-002 only)
with bus extension		250 (not 750-8212/025-002)
Input and output process image (max.)	CODESYS V2	1,000 words
	***e!**RUNTIME*	Not specified

4.3.7 ETHERNET

Table 23: 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, Modbus (TCP, UDP)
Modbus input and output process image, max.	CODESYS V2	1,000 words, also with Modbus access to the flag area (see Section "Modbus" > … > "Flag Area")
	e!*RUNTIME*	32,000 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!

4.3.8 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	Modbus® RTU

4.3.9 Connection Type

Table 25: Technical Data – Field Wiring

Wire connection	CAGE CLAMP®
Cross section	0.08 mm² … 2.5 mm², AWG 28 … 14
Stripped lengths	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

4.3.10 Climatic Environmental Conditions

Table 28: Technical Data – Climatic Environmental Conditions

Surrounding air temperature (operation)	0 … 55 °C
Surrounding air temperature (operation) for components with extended temperature range (750-xxx/025-xxx)	−20 … +60 °C
Surrounding air temperature (storage)	−25 … +85 °C
Surrounding air temperature (storage) for components with extended temperature range (750-xxx/025-xxx)	−40 … +85 °C
Relative humidity	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

Information

More information about approvals.
Detailed references to the approvals are listed in the document “**Overview on WAGO I/O System 750 approvals**”, which you can find via the internet under: www.wago.com → DOWNLOADS → Documentation → System Description.

The following approvals have been granted to the basic version and the variants of the “PFC200; G2; 2ETH RS” controller (750-8212) described in this document:

Conformity Marking	
Ordinary Locations	UL61010-2-201
Korea Certification	MSIP-REM-W43-PFC750

The following Ex approvals have been granted to the basic version and the variants of the “PFC200; G2; 2ETH RS” controller (750-8212) described in this document:

Hazardous Locations	UL 121201 for Use in Hazardous Locations Cl I Div 2

TÜV 14 ATEX 148929 X

II 3 G Ex ec IIC T4 Gc

IECEx TUN 14.0035 X

Ex ec IIC T4 Gc

The following ship approvals have been granted to the basic version and the variants of the “PFC200; G2; 2ETH RS” controller (750-8212) described in this document:

ABS (American Bureau of Shipping)

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

PRS (Polski Rejestr Statków)

The following ship approvals have been granted to the basic version of the “PFC200; G2; 2ETH RS” controller (750-8212):

LR (Lloyd’s Register)	Env. 1, 2, 3, 4
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 basic version and the variants of the “PFC200; G2; 2ETH RS” controller (750-8212) described in this document fulfill 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 basic version and the variants of the “PFC200; G2; 2ETH RS” controller (750-8212) described in this document fulfill 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 basic version and the variants of the “PFC200; G2; 2ETH RS” controller (750-8212) described in this document fulfill 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

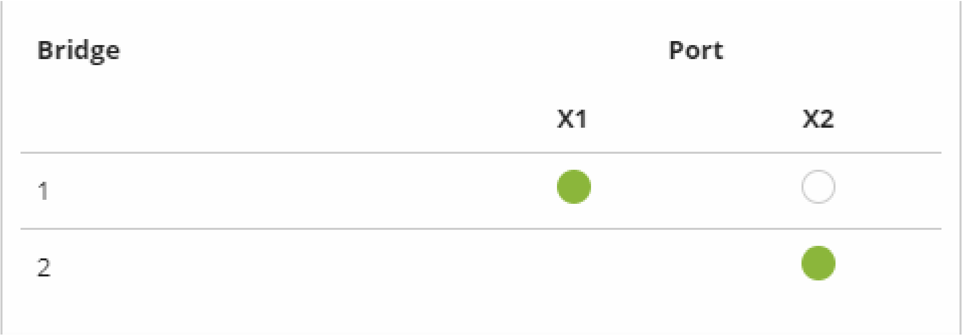
5.1.1 Interface Configuration

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.



Bridge	Port	
	X1	X2
1	●	○
2		●

Figure 20: Example of Interface Assignment via WBM

For interface X1, a fixed IP address can be set temporarily (“Fix IP Address” mode). The setting is carried out with the Reset button (see Section “Commissioning” > … > “Temporarily Setting a Fixed IP Address”).

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

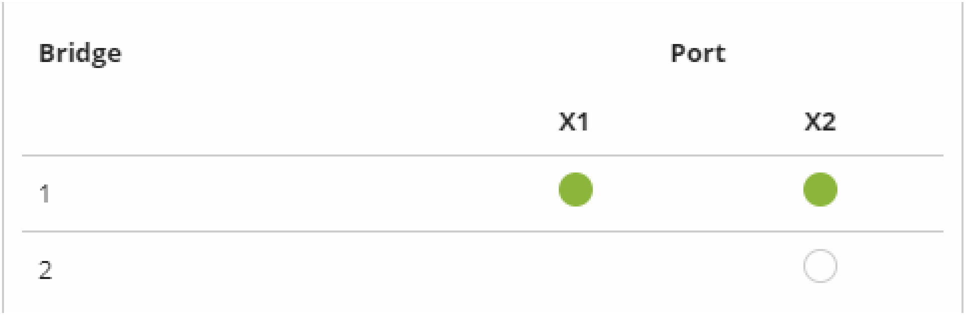
When operating with separate network interfaces, both ETHERNET interfaces can be configured and used separately.

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



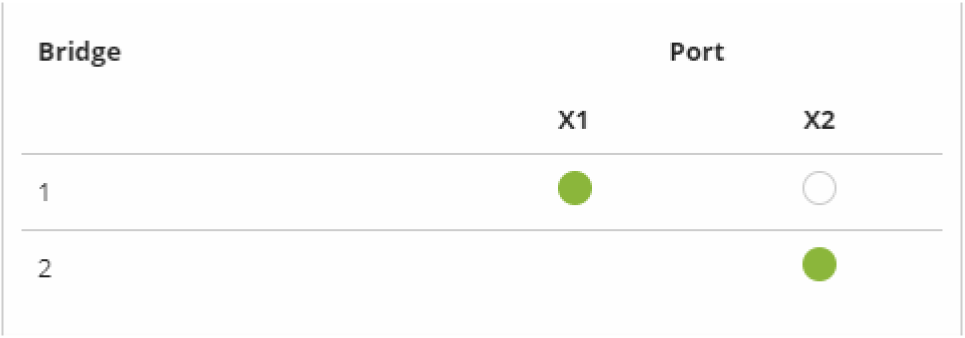
Bridge	Port	
	X1	X2
1	●	●
2		○

Figure 21: 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



Bridge	Port	
	X1	X2
1	●	○
2		●

Figure 22: 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.

	Users					
Service	**WBM**		**Linux®**			**SNMP**
	admin	**user**	**root**	**admin**	**user**	
Web Based Management (WBM)	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 WBM User Group

WBM has its own user administration system. The users in this system are isolated from the other user groups in the system for security reasons.

Detailed information about this is given in the Section “WBM User Administration”.

Table 31: WBM Users

Users	Permissions	Default Password
admin	All (administrator)	wago
user	Supported to a limited extent	user
guest	Display only	---

Note

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

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.

5.1.2.1.3 Linux® User Group

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

The passwords for these users must be configured through a terminal connection via SSH/RS-232.

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

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.

5.1.2.1.4 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. If there are multiple network interfaces with DHCP, the last received host name is valid. 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.

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:
If the value “default” is entered in the “Destination Address” field, a default gateway, also called a default route, is defined. The value “0.0.0.0” must then be set in the “Destination Mask” field.

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.

If the IP address of the gateway is outside the IP address space that the controller can reach, the associated route is not enabled.

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. The default value for the metric is 20. Besides the manually configurable routes, default gateways can also be set via DHCP replies. All default gateways transferred via DHCP are assigned a permanent metric value of 10.

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, “Routing enabled entirely” must be enabled in the “General Routing Configuration” 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

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.

The Hostname and Domain parameters are each stored according to the LIFO principle (Last In First Out). The settings from the last DHCP offer received are always used.

The DNS and NTP Server parameters are stored centrally for global use. All transmitted parameters are stored.

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.

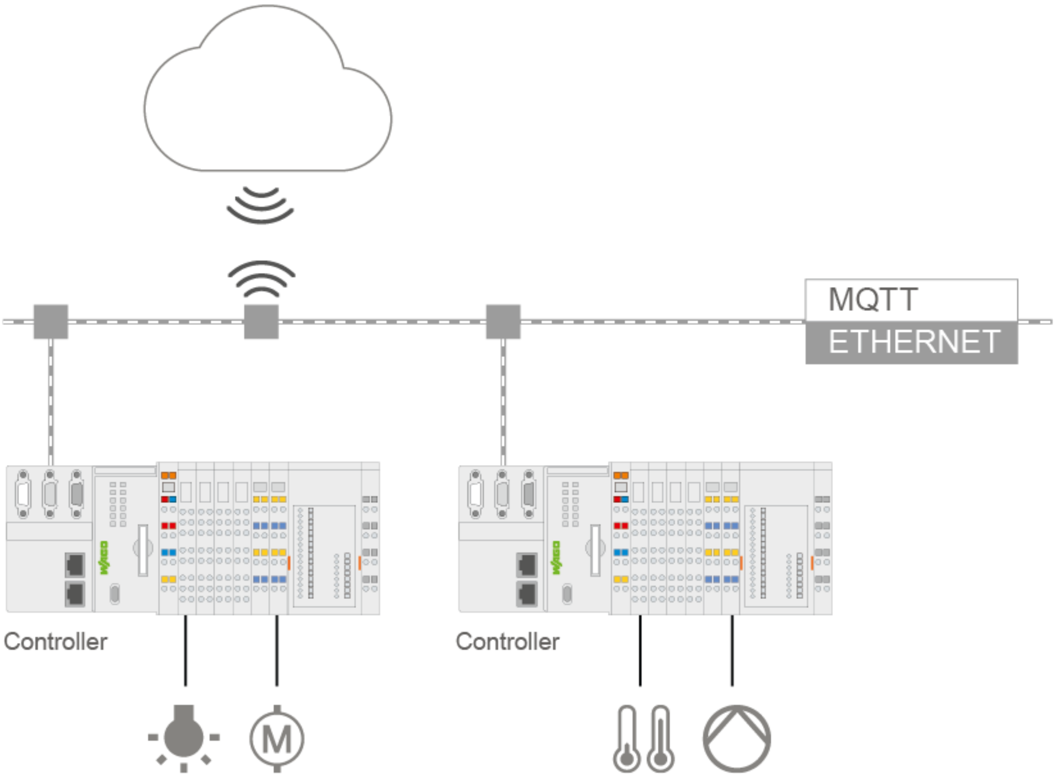


Figure 23: Connecting the Controller to a Cloud Service (Example)

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 parameters are configured in the WBM; the data to exchange between the cloud and controller is configured with the libraries for ***e!****COCKPIT* or CODESYS 2.3.

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
e!*COCKPIT*: WagoAppCloud	IEC libraries 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.
CODESYS 2.3: WagoLibCloud	

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.

The necessary settings can be made and the functions can be executed via the WBM pages or via the CBM “Backup” and “Restore” menus.

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 (“System”)
- all of the above (“All,” only visible if not saved on the network)

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 via the WBM page “Firmware Backup” or the CBM menu “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 via the WBM page “Firmware Restore” or the CBM menu “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 “Boot project location” setting on the “General PLC Runtime Configuration Web” page of the WBM determines whether the boot project of the internal drive or the memory card is loaded.

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.

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.

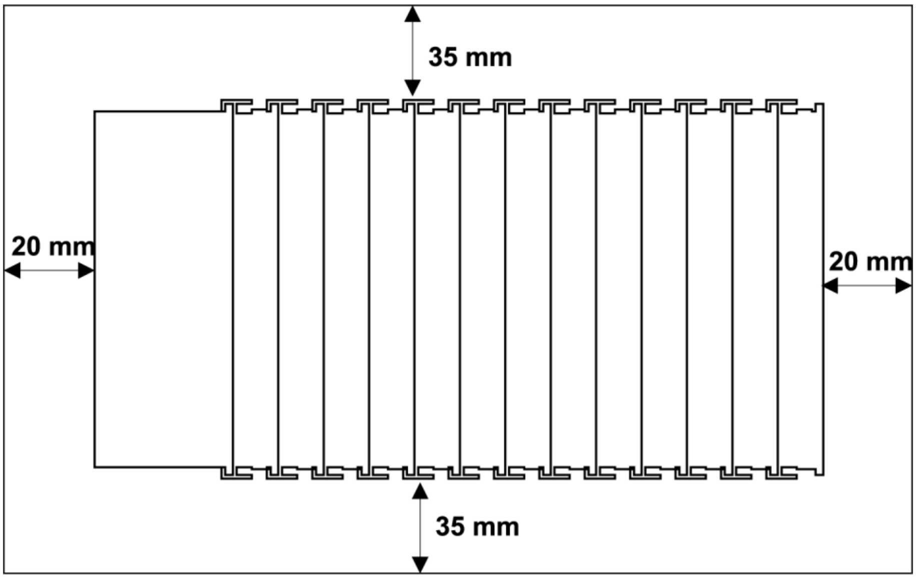


Figure 24: Spacing

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 (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.

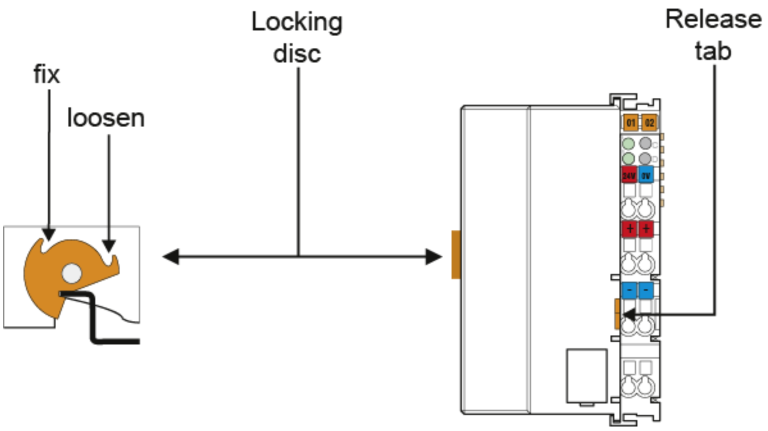


Figure 25: Release Tab of Controller

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.

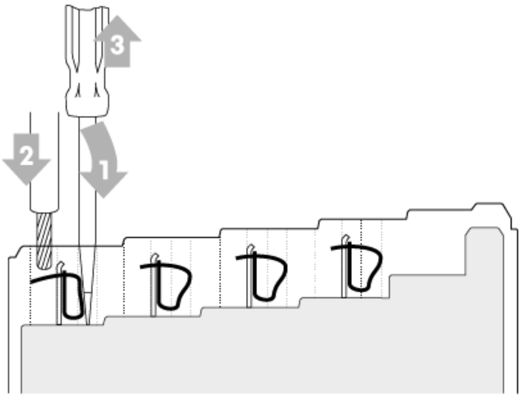


Figure 26: Connecting a Conductor to a CAGE CLAMP®

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.

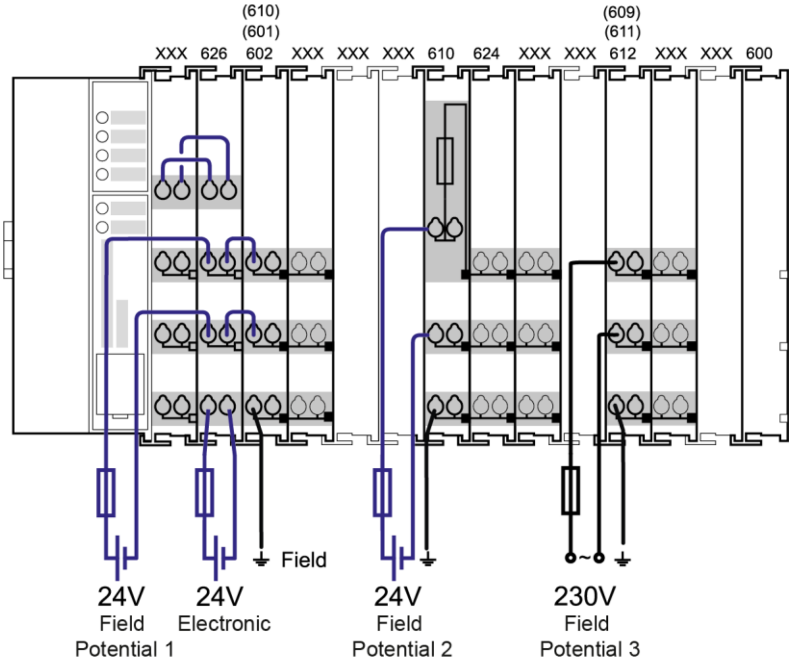


Figure 27: Power Supply Concept

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

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 (750-600)
(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 CODESYS 2.3 runtime system or ***e!****RUNTIME* 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 (WBM, WAGO ETHERNET Settings or CBM – 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

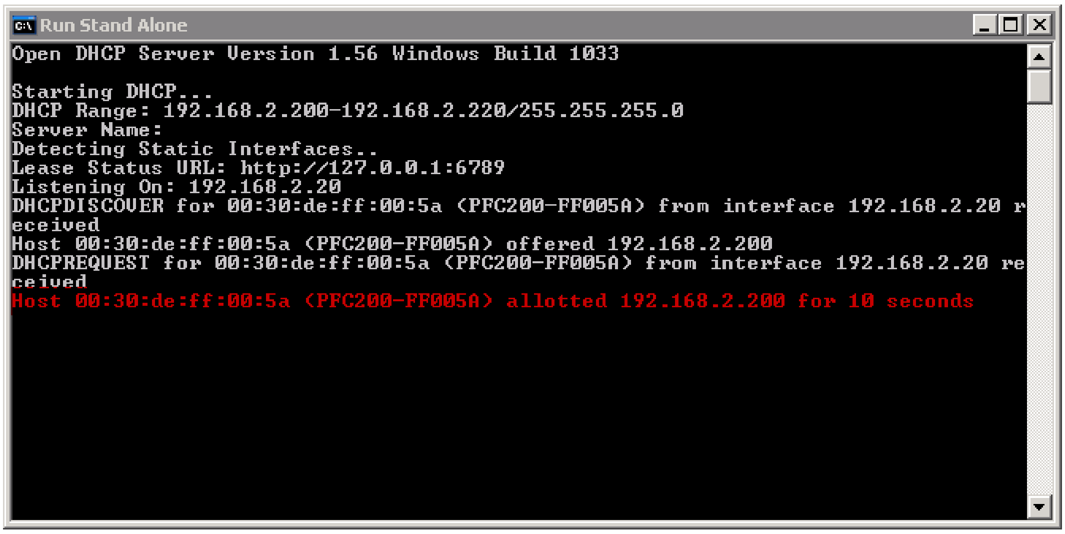
Host PC	Subnet Address Range for the Controller
192.168.1.2	**192.168.1.**1 or **192.168.1.**3 … **192.168.1.**254

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.



```
Open DHCP Server Version 1.56 Windows Build 1033

Starting DHCP...
DHCP Range: 192.168.2.200-192.168.2.220/255.255.255.0
Server Name:
Detecting Static Interfaces..
Lease Status URL: http://127.0.0.1:6789
Listening On: 192.168.2.20
DHCPDISCOVER for 00:30:de:ff:00:5a (PFC200-FF005A) from interface 192.168.2.20 r
eceived
Host 00:30:de:ff:00:5a (PFC200-FF005A) offered 192.168.2.200
DHCPREQUEST for 00:30:de:ff:00:5a (PFC200-FF005A) from interface 192.168.2.20 re
ceived
Host 00:30:de:ff:00:5a (PFC200-FF005A) allotted 192.168.2.200 for 10 seconds
```

Figure 28: “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”.

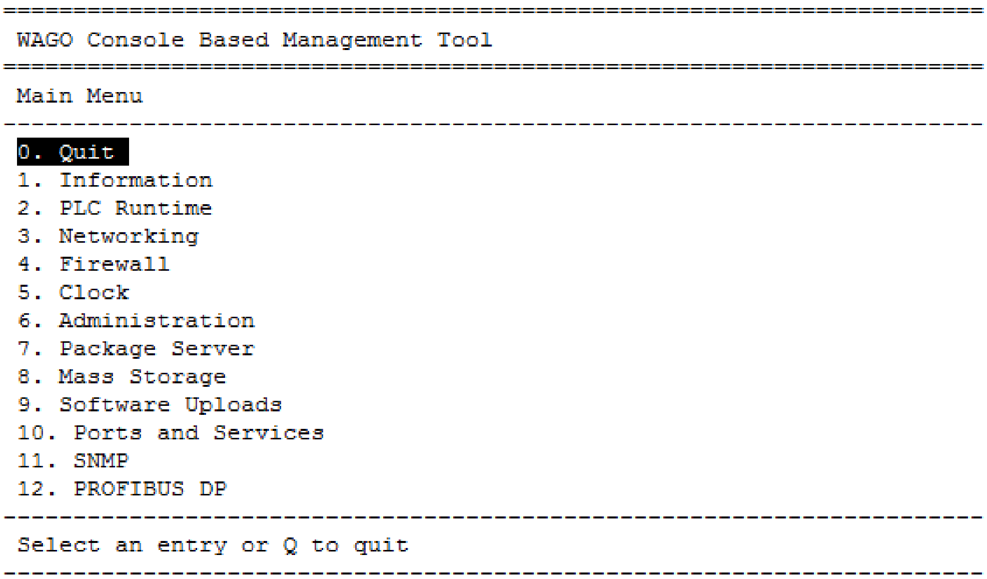
8.3.2 Changing an IP Address Using the “CBM” Configuration Tool and a Terminal Program

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:

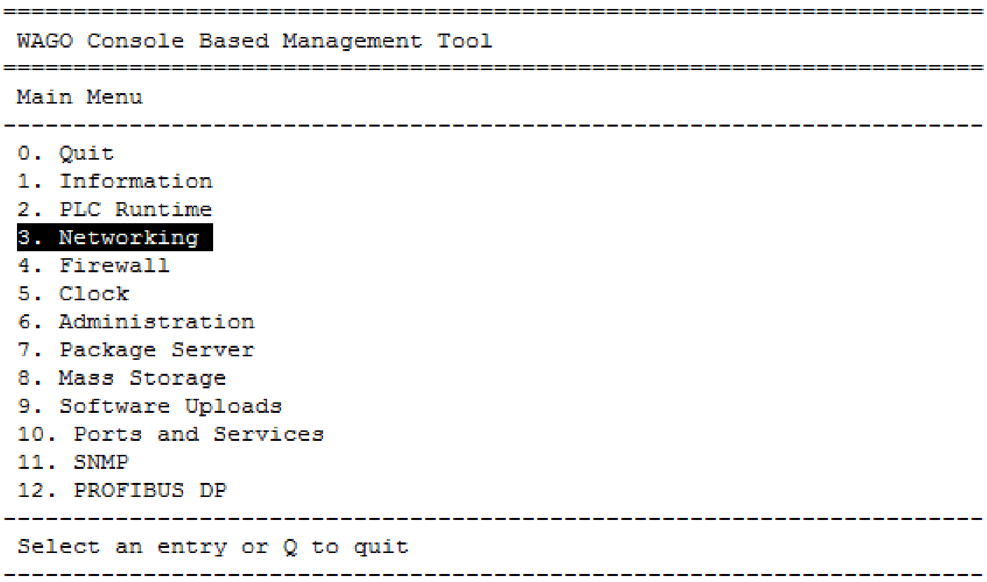
1. Connect a PC to the X3 serial interface of the controller using a terminal program.
2. Start the terminal program.
3. Select “Serial” as the connection type and enter a baud rate of 115200 bauds as the connection parameter. The settings for data bits, stop bits and parity do not need to be adjusted.
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 29: CBM main menu (example)

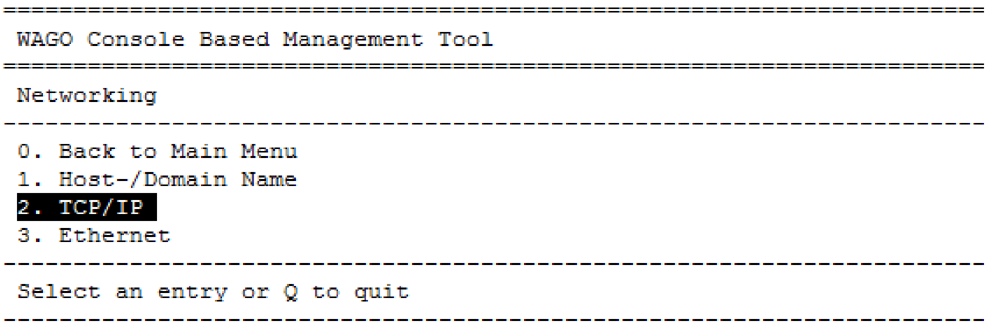
6. In the **Main menu** use the keyboard (arrow keys or numeric keypad) to move to and select **Networking** and then press **[Enter]**.



```
======================================================================
 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 30: CBM – Selecting “Networking”

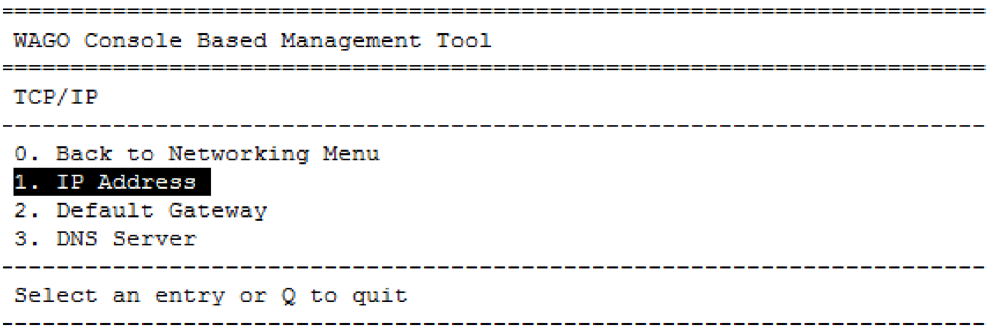
7. In the **Networking** menu select **TCP/IP** and press **[Enter]**.



```
======================================================================
 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 31: CBM – Selecting “TCP/IP”

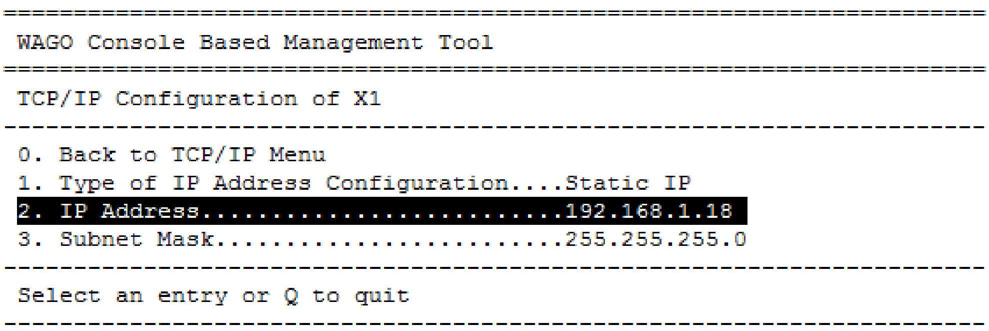
8. In the menu **TCP/IP** select **IP Address** and press **[Enter]**.



```
======================================================================
 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 32: CBM – Selecting “IP address”

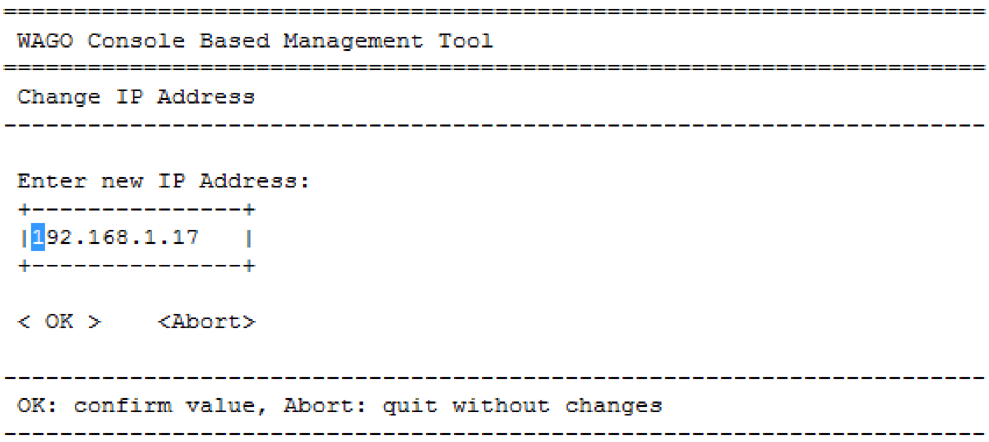
9. In the menu **TCP/IP Configuration** select **IP Address** and press **[Enter]**.



```
======================================================================
 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 33: 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 34: 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”!

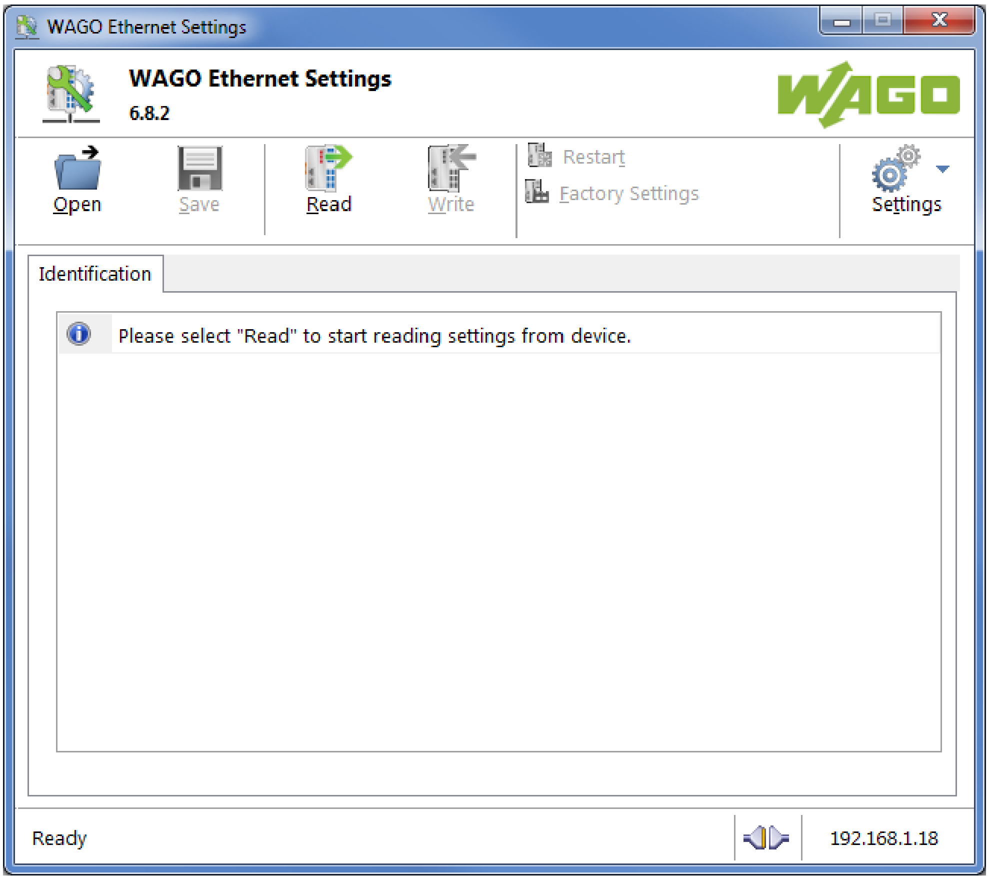
You can use WAGO communication cables or WAGO radio adapters or even the IP network for data communication.

1. Switch off the power supply to the controller.

2. Connect the 750-920 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.

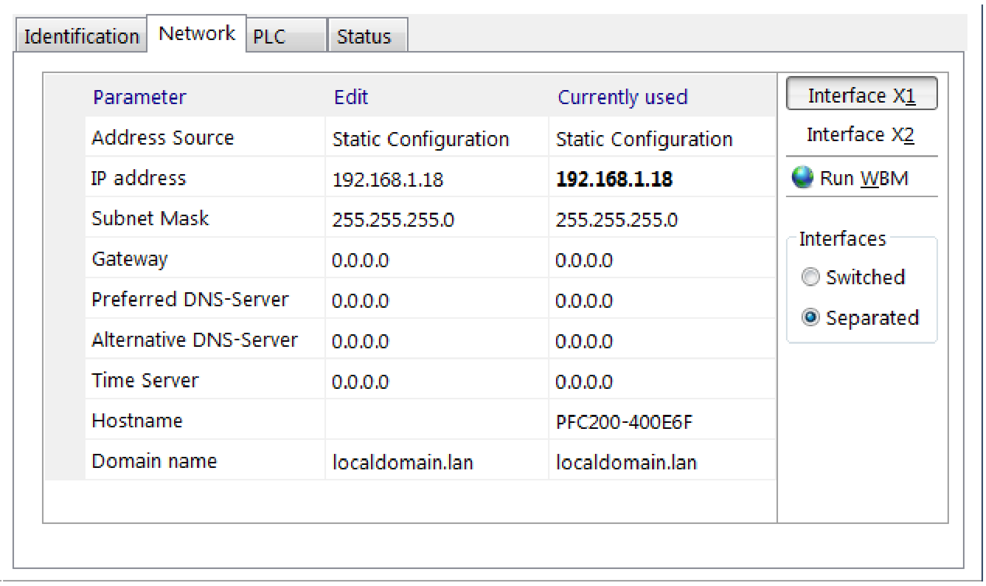


Please select "Read" to start reading settings from device.

Figure 35: “WAGO Ethernet Settings” – Starting Screen (Example)

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

6. Select the “Network” tab:



Parameter	Edit	Currently used
Address Source	Static Configuration	Static Configuration
IP address	192.168.1.18	**192.168.1.18**
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0
Preferred DNS-Server	0.0.0.0	0.0.0.0
Alternative DNS-Server	0.0.0.0	0.0.0.0
Time Server	0.0.0.0	0.0.0.0
Hostname		PFC200-400E6F
Domain name	localdomain.lan	localdomain.lan

Figure 36: “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 a Fixed IP Address

This procedure temporarily sets the IP address for the X1 interface to the fixed address “192.168.1.17”.
When the switch is enabled, the fixed address is also used for interface X2.
When the switch is disabled, the original address setting for interface X2 is not changed.
No reset is performed.

To make this setting, 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.

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]**.

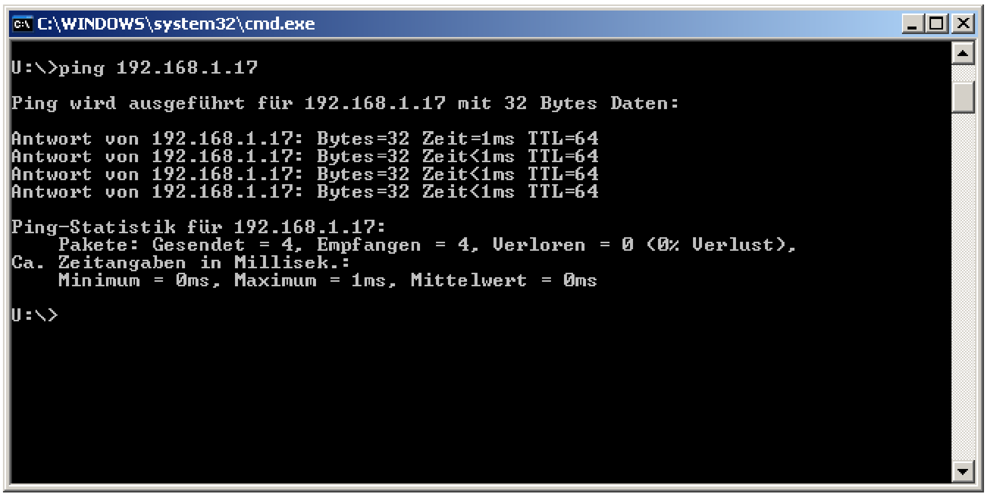
2. In the MS DOS window, enter the command “ping” and the IP address of the controller (for example, `ping 192.168.1.17)` and then press **[Enter]**.

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.



```
U:\>ping 192.168.1.17

Ping wird ausgeführt für 192.168.1.17 mit 32 Bytes Daten:

Antwort von 192.168.1.17: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 192.168.1.17:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms

U:\>
```

Figure 37: 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

The warm start reset function depends on the activated runtime system (CODESYS V2 or ***e!****RUNTIME*).

8.7.1.1 CODESYS V2 Runtime System

The CODESYS V2 application is reset on a warm start reset. This corresponds to the WAGO I/O PRO IDE “Reset” 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.

8.7.1.2 *e!RUNTIME* Runtime System

All ***e!****RUNTIME* applications are reset with a warm start reset. All global data is set to its initialization values. This corresponds to the ***e!****COCKPIT* 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

The cold start reset function depends on the activated runtime system (CODESYS V2 or ***e!****RUNTIME*).

8.7.2.1 CODESYS V2 Runtime System

On a cold start reset the CODESYS V2 application is reset and the memory containing the retain variables is cleared.
This corresponds to the WAGO I/O PRO 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.

8.7.2.2 *e!RUNTIME* Runtime System

All ***e!****RUNTIME* 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 ***e!****COCKPIT* 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 Factory Reset

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

All parameters and passwords are overwritten!
All controller parameters and passwords are overwritten by a factory reset.
Stored boot projects are deleted, including existing web visualization data.
Subsequently installed firmware functions are not overwritten.
If you have any questions, contact WAGO Support.

The controller is restarted after the factory reset.
Proceed as follows to factory 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 factory 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 CODESYS PLC program using the CODESYS V2 library WagoConfigToolLIB.lib (section “Appendix” > “WagoConfigToolLIB.lib”) or the ***e!****RUNTIME* library “WagoAppConfigTool.lib”

- 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.

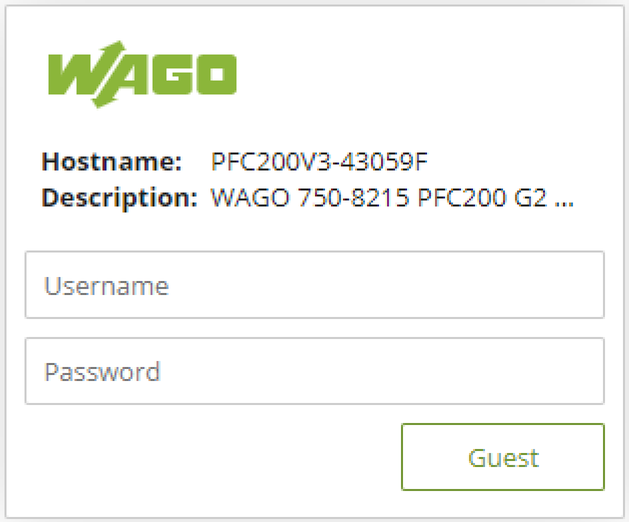
2. Start a Web browser on your PC.

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.



Hostname: PFC200V3-43059F
Description: WAGO 750-8215 PFC200 G2 ...

Figure 38: Entering Authentication

4. Enter the username and password.

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

6. If you only want to log in as a guest, click the **[Guest]** 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.

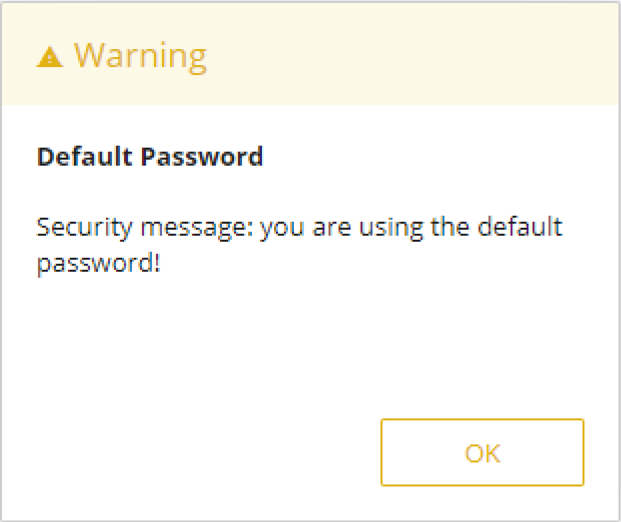
8.8.1.1 WBM User Administration

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

Default Password

Security message: you are using the default password!

Figure 39: Password Reminder

Table 40:User Settings in the Default State

Users	Permissions	Default Password
admin	All (administrator)	wago
user	Supported to a limited extent	user
guest	Display only	---

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 separately.

Access to the WBM pages is as follows:

Table 41: Access Rights for WBM Pages

Tab/Navigation	WBM Page Title	User
Information		

Table 41: Access Rights for WBM Pages

Tab/Navigation	WBM Page Title	User
Device Status	Device Status	guest
Vendor Information	Vendor Information	guest
PLC Runtime	PLC Runtime Information	guest
Legal Information		
WAGO Licenses	WAGO Software License Agreement	guest
Open Source Licenses	Open Source Licenses	user
WBM Licenses	WBM Third Party License Information	user
WBM Version	WBM Version Info	guest
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
TFTP	TFTP Server	admin
DHCP Server	DHCP Server Configuration	admin
DNS	Configuration of DNS Service	user

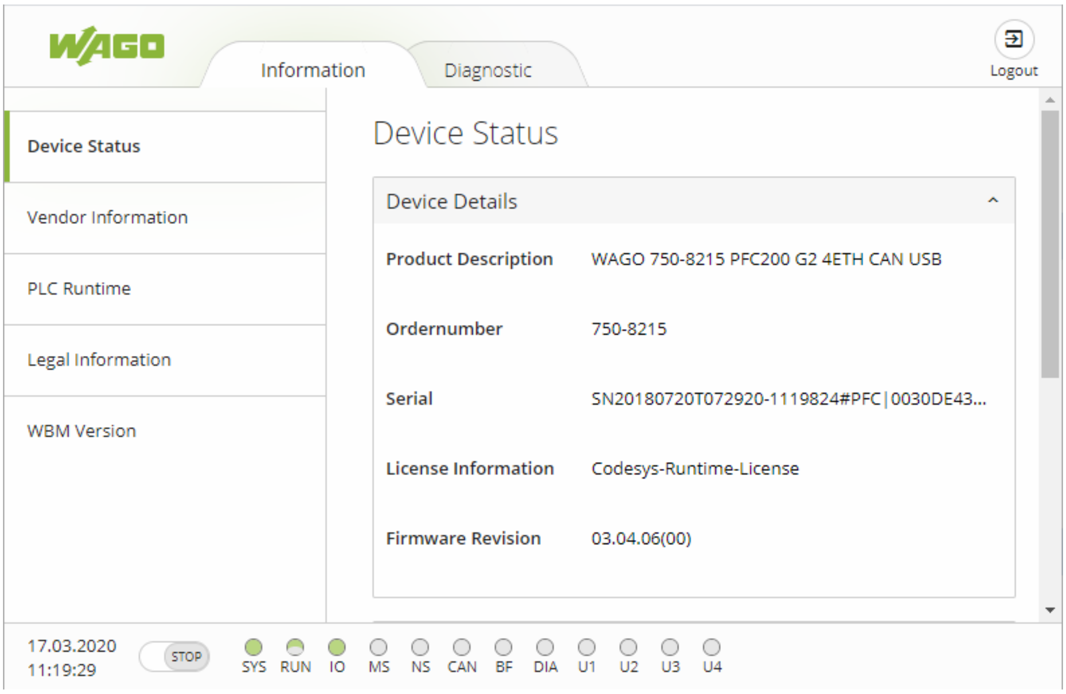
Table 41: Access Rights for WBM Pages

Tab/Navigation	WBM Page Title	User
Cloud Connectivity		
Status	Overview	admin
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
Users	WBM User Configuration	admin
Fieldbus		
OPC UA		
Status	OPC UA Status	admin
Configuration	OPC UA Configuration	admin
Information Model	OPC UA Information Model	admin
Modbus	Modbus Services Configuration	user
BACnet		
Status	BACnet Status	admin
Configuration	BACnet Configuration	admin
Storage Location	BACnet Storage Location	admin
Files	BACnet Files	admin
Diagnostic	BACnet Diagnostic	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
TLS	Security Settings	admin
Integrity	Advanced Intrusion Detection Environment (AIDE)	admin
Diagnostic	Diagnostic Information	guest

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.



Device Status

Device Details

Product Description	WAGO 750-8215 PFC200 G2 4ETH CAN USB
Ordernumber	750-8215
Serial	SN20180720T072920-1119824#PFC|0030DE43...
License Information	Codesys-Runtime-License
Firmware Revision	03.04.06(00)

17.03.2020
11:19:29

Figure 40: 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.

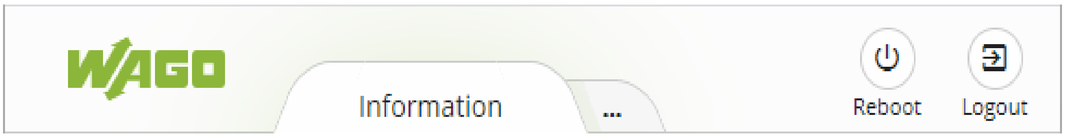


Figure 41: WBM Header with Tabs that Cannot be Displayed (Example)

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.

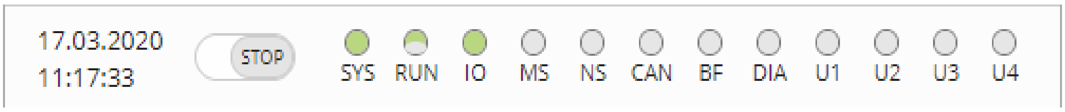


Figure 42: WBM Status Bar (Example)

- 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:

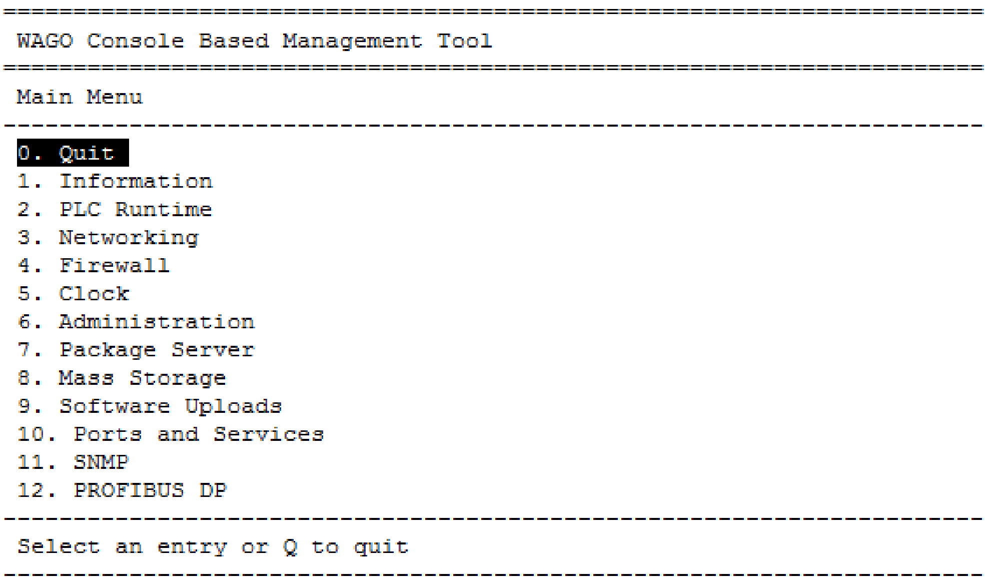
1. Connect a PC to the X3 serial interface of the controller using a terminal program.

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 43: CBM main menu (example)

8.8.2.1 CBM Menu Structure Overview

Table 42: CBM Menu Structure

Menu Hierarchy
0. Quit
1. Information
0. Back to Main Menu
1. Controller Details
2. Network Details
2. PLC Runtime
0. Back to Main Menu
1. Information
2. General Configuration
3. WebVisu
3. Networking
0. Back to Main Menu
1. Host-/Domain Name
2. TCP/IP
0. Back to Networking Menu
1. IP Address
2. Default Gateway
3. DNS Server
3. Ethernet
0. Back to Networking Menu
1. Switch Configuration
2. Ethernet Ports
0. Back to Ethernet Menu
1. Interface X1
2. Interface X2
4. Firewall
0. Back to Main Menu
1. General Configuration
2. MAC Address Filter
3. User Filter
5. Clock
0. Back to Main Menu
1. Date on device (local)
2. Time on device (local)
3. Time on device (UTC)
4. Clock Display Mode
5. Timezone
6. TZ-String
6. Administration
0. Back to Main Menu

Table 42: CBM Menu Structure

Menu Hierarchy
1. Users
2. Create Image
3. Owner of Serial Interface
4. Reboot Controller
7. Package Server
0. Back to Main Menu
1. Firmware Backup
2. Firmware Restore
3. System Partition
8. Mass Storage
0. Back to Main Menu
1. Internal Flash (active partition)
9. Software Uploads
0. Back to Main Menu
1. Update Script
10. Ports and Services
0. Back to Main Menu
1. Telnet
2. FTP
3. FTPS
4. HTTP
5. HTTPS
6. NTP
7. SSH
8. TFTP
9. DHCPD
10. DNS
11. IOCHECK PORT
12. Modbus TCP
13. Modbus UDP
14. PLC Runtime Services
11. SNMP
0. Back to Main Menu
1. General SNMP Configuration
2. SNMP v1/v2c Manager Configuration
3. SNMP v1/v2c Trap Receiver Configuration
4. SNMP v3 Configuration
5. SNMP firewalling
6. Secure SNMP firewalling

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 CBM menus and the respective parameters can be found in the appendix in Section “Configuration Dialogs” > “Console-Based Management (CBM)”.

8.8.3 Configuration using “WAGO Ethernet Settings”

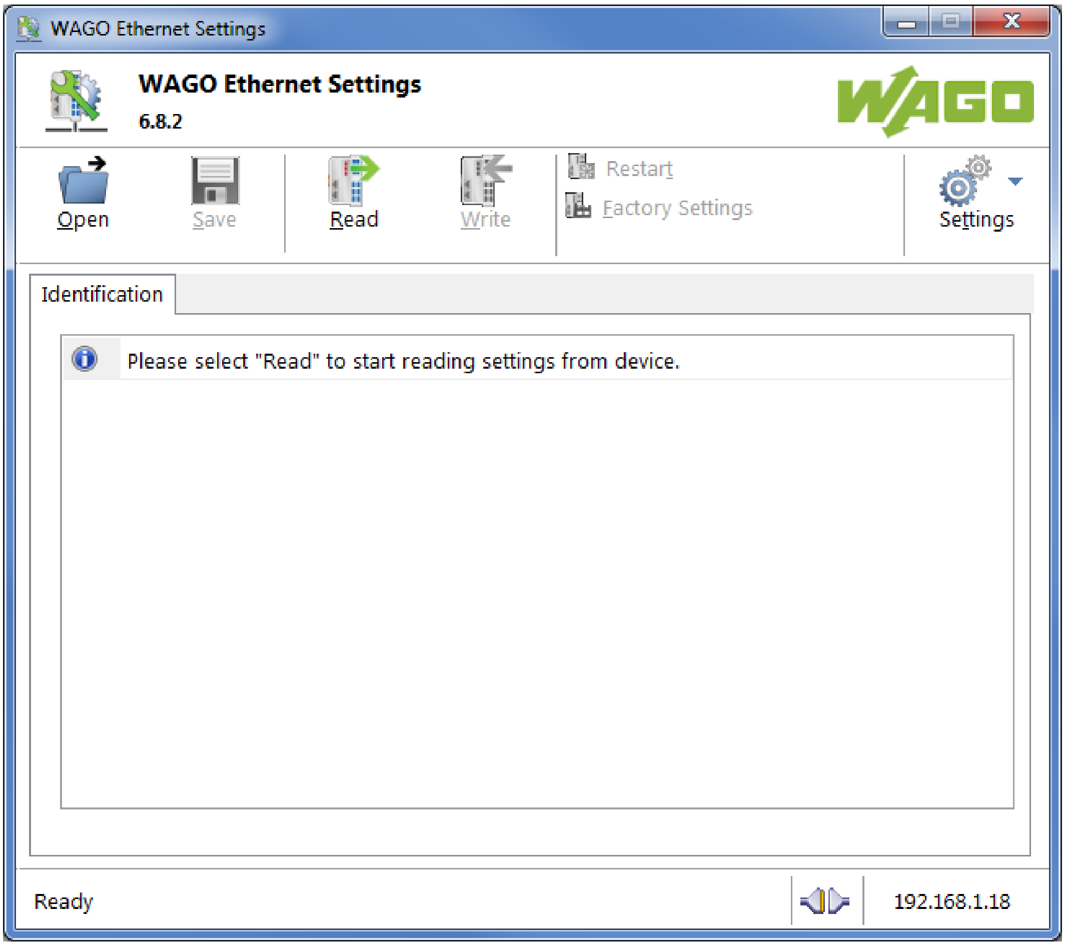
The “WAGO Ethernet Settings” program enables you to read system information about your controller, make network settings and enable/disable the Web server.

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 communication cable 750-920, *Bluetooth*® Adapter 750-921, configuration cable 750-923 or 750-923/000-001 or via the ETHERNET interfaces.



Please select "Read" to start reading settings from device.

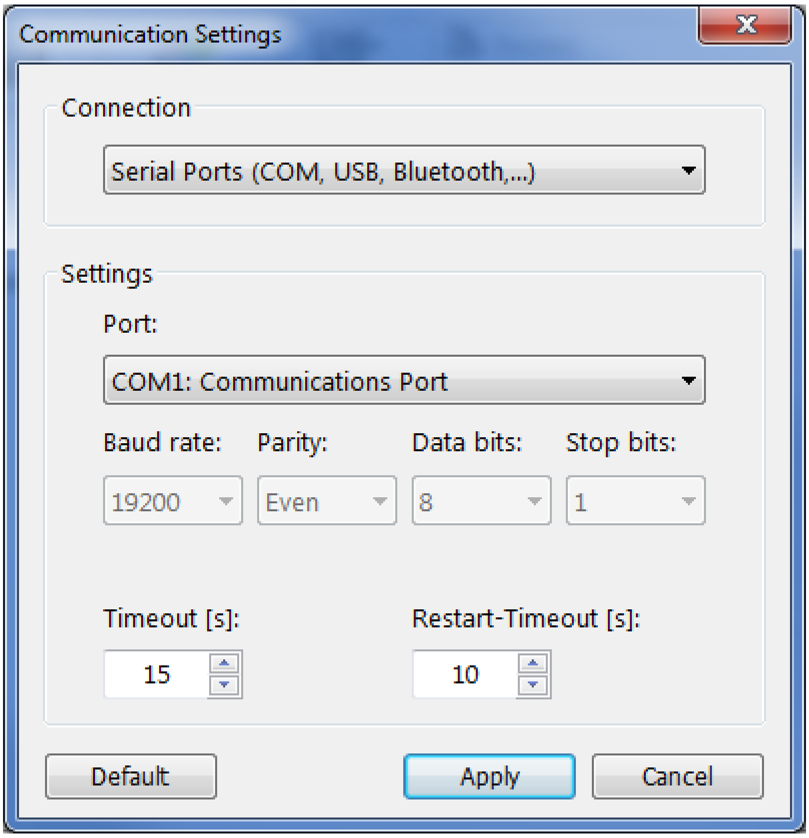
Ready

192.168.1.18

Figure 44: “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.



Communication Settings

Connection

Serial Ports (COM, USB, Bluetooth,...)

Settings

Port:

COM1: Communications Port

Baud rate: 19200

Parity: Even

Data bits: 8

Stop bits: 1

Timeout [s]: 15

Restart-Timeout [s]: 10

Figure 45: “WAGO Ethernet Settings” – Communication Link

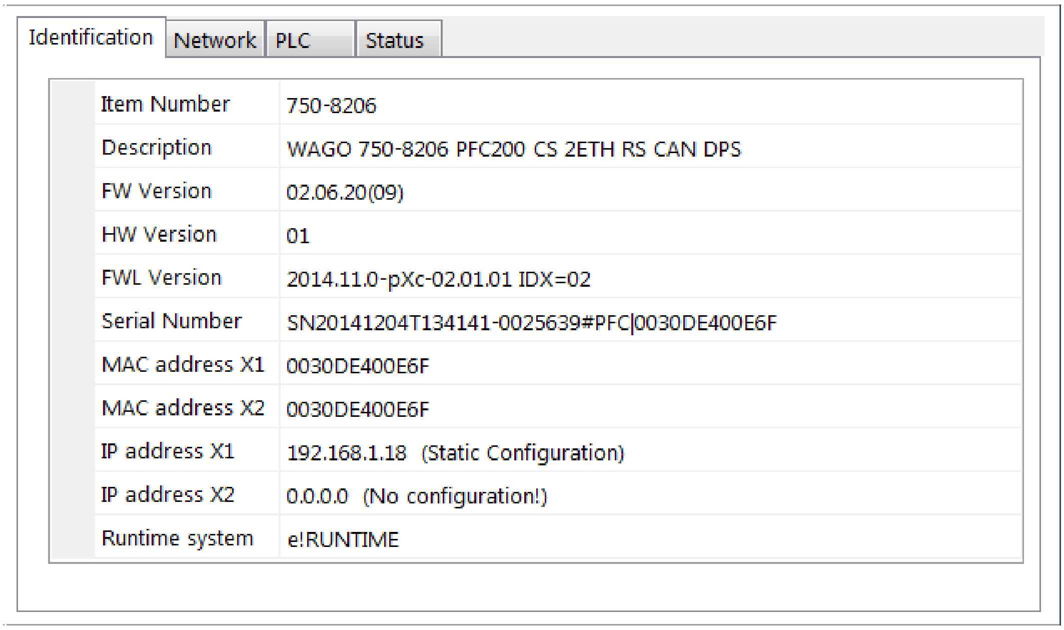
Once you have configured “WAGO Ethernet Settings” and have clicked **[Apply]**, connection to the controller is established automatically.

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.



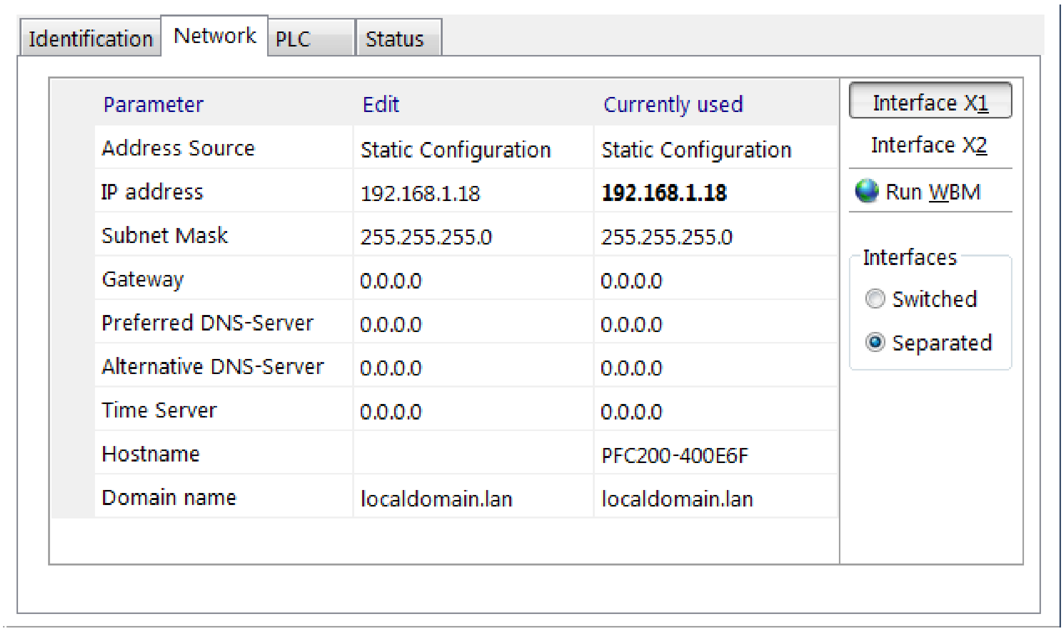
Item Number	750-8206
Description	WAGO 750-8206 PFC200 CS 2ETH RS CAN DPS
FW Version	02.06.20(09)
HW Version	01
FWL Version	2014.11.0-pXc-02.01.01 IDX=02
Serial Number	SN20141204T134141-0025639#PFC|0030DE400E6F
MAC address X1	0030DE400E6F
MAC address X2	0030DE400E6F
IP address X1	192.168.1.18 (Static Configuration)
IP address X2	0.0.0.0 (No configuration!)
Runtime system	e!RUNTIME

Figure 46: “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.



Parameter	Edit	Currently used
Address Source	Static Configuration	Static Configuration
IP address	192.168.1.18	**192.168.1.18**
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0
Preferred DNS-Server	0.0.0.0	0.0.0.0
Alternative DNS-Server	0.0.0.0	0.0.0.0
Time Server	0.0.0.0	0.0.0.0
Hostname		PFC200-400E6F
Domain name	localdomain.lan	localdomain.lan

Interfaces
○ Switched
● Separated

Figure 47: “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.

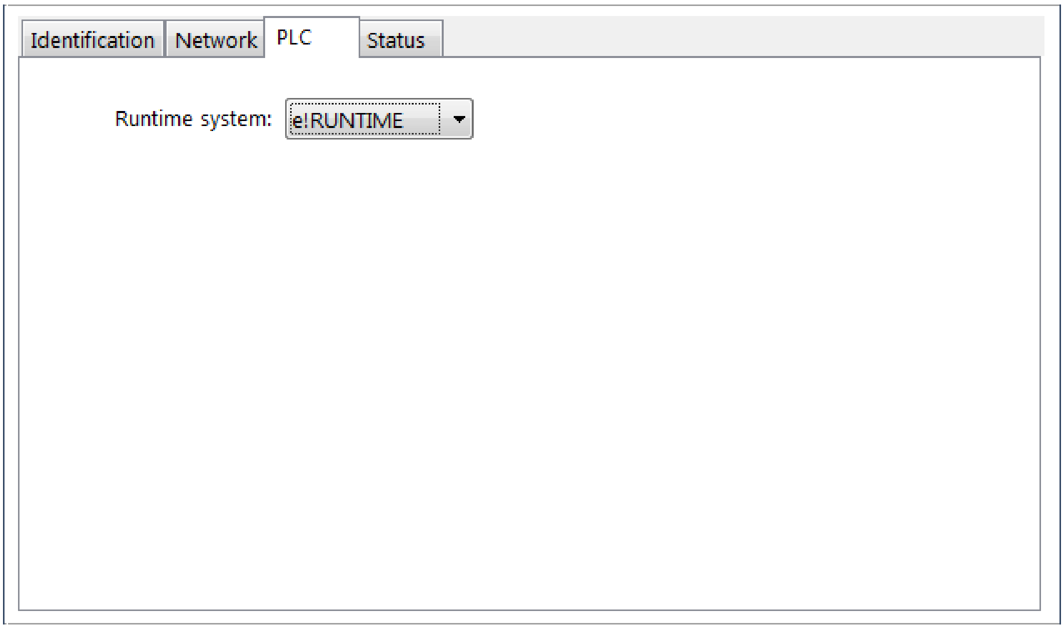
Time server
Specify the IP address for a time server if setting the controller's system time via NTP.

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

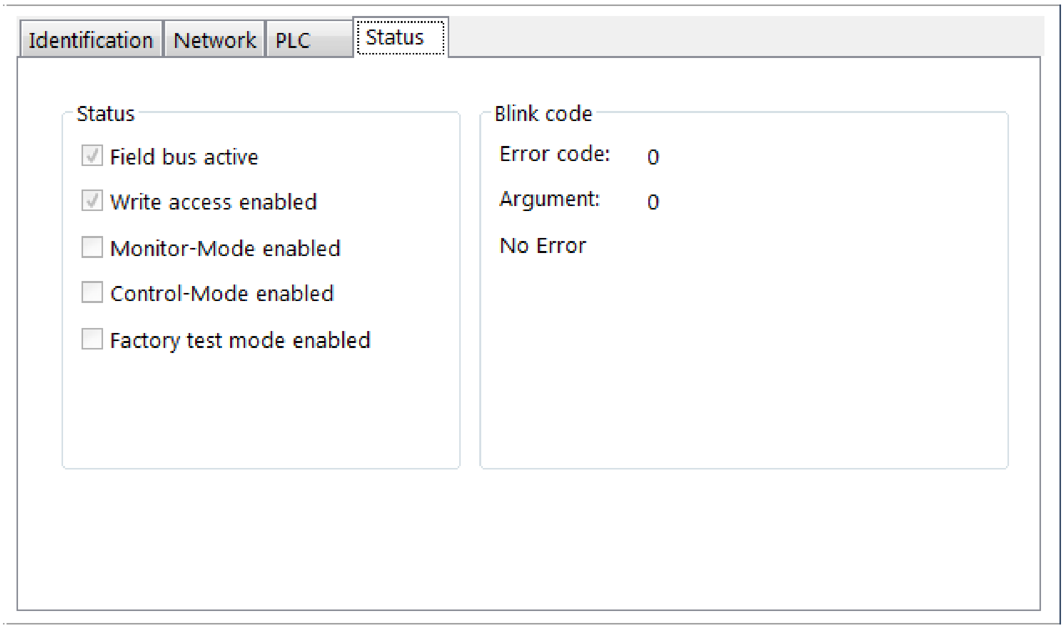


Runtime system: e!RUNTIME

Figure 48: “WAGO Ethernet Settings” – Protocol Tab

Here you can select the runtime system.

8.8.3.4 Status Tab



Status

☑ Field bus active

☑ Write access enabled

□ Monitor-Mode enabled

□ Control-Mode enabled

□ Factory test mode enabled

Blink code

Error code: 0

Argument: 0

No Error

Figure 49: “WAGO Ethernet Settings” – Status Tab

General information about the controller status is displayed here.

9 Run-time System CODESYS 2.3

9.1 Installing the CODESYS 2.3 Programming System

The WAGO target files must also be included for the installation of CODESYS. These contain all device-specific information for the WAGO 750/758 product series.

Proceed as described below to install the CODESYS 2.3 programming software on a personal computer.

1. Insert the “WAGO-I/O-*PRO*” CD into your computer drive.

2. To install the programming system, follow the instructions that appear on your screen. A successful installation is indicated by a CODESYS icon on your desktop.

9.2 First Program with CODESYS 2.3

This section uses an example to explain the relevant steps required for the creation of a CODESYS project. It is intended as a set of quick start instructions and does not address the full functional range of CODESYS 2.3.

Note

Additional information

For a detailed description of the full range of functions, refer to the “Manual for PLC Programming using CODESYS 2.3” manual available on the “WAGO-I/O-*PRO*” (759-911) CD.

9.2.1 Start the CODESYS Programming System

Start CODESYS by double clicking on the CODESYS pictogram on your desktop using the Start menu in your operating system. To do this, click on the “Start” button and choose **Programs** >
WAGO Software > **CODESYS** > **CODESYS V2.3**.

9.2.2 Creating a Project and Selecting a Target System

1. In the menu bar click on **File** and select **New**. The “Target system settings” window then opens. Here, all available target systems that can be programmed with CODESYS 2.3 are listed.

2. Open the selection box in the “Target system settings” window and select the fieldbus controller you are using. In the example shown here this is the PFC200 CS 2ETH RS “WAGO_750-8202”.

3. Click on **[OK]**. The “Target system settings” configuration window then opens.

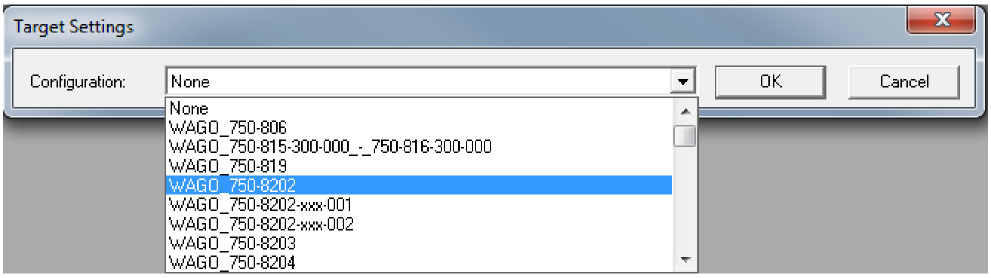
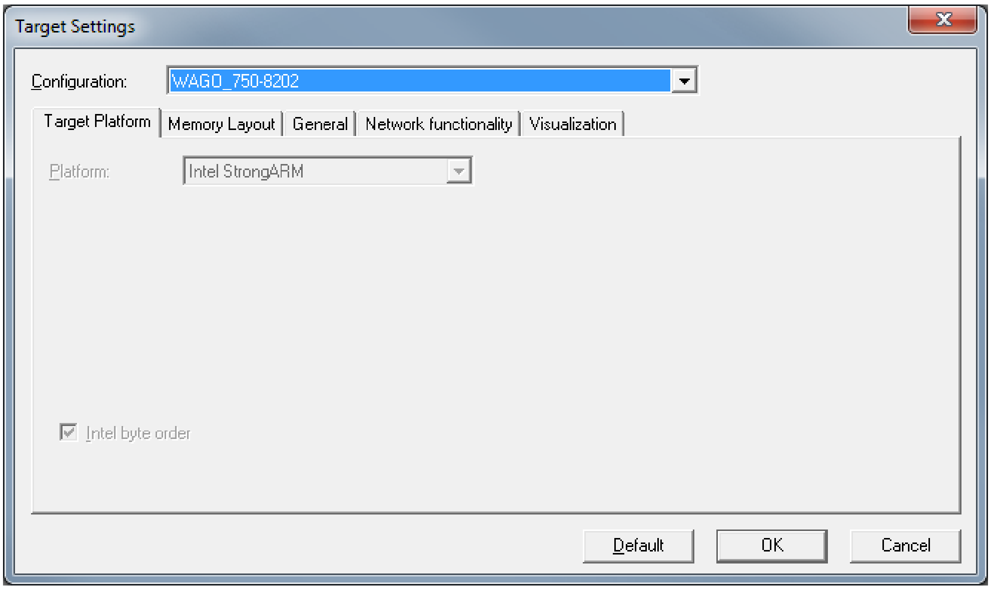


Figure 50: Target System Settings (1)

4. To accept the default configuration for the fieldbus controller click **[OK]**. The “New component” window opens.



Configuration: WAGO_750-8202

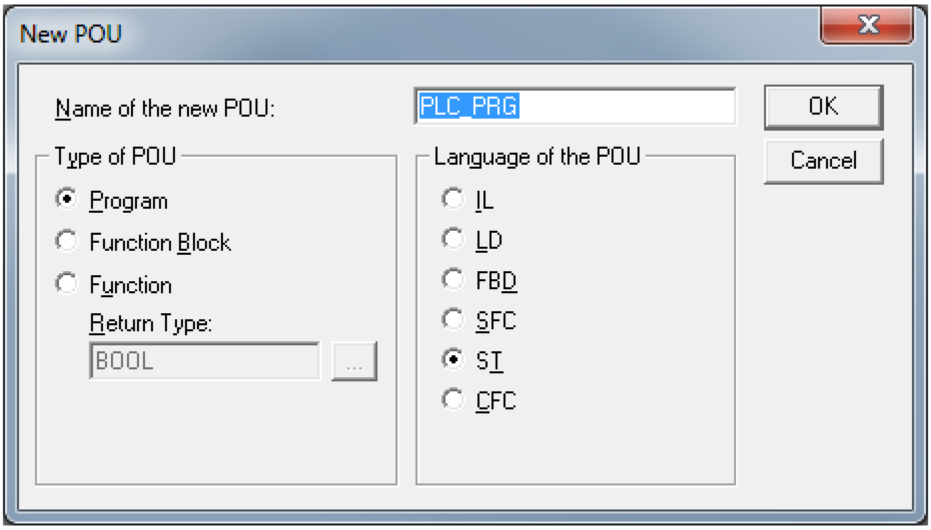
Platform: Intel StrongARM

☑ Intel byte order

Figure 51: Target System Settings (2)

5. In this “New component” window create a new program function block. In the example shown here, the new function block “PLC_PRG” is created in the “ST” programming language.

6. Click on **[OK]** to create the project. The programming interface opens.

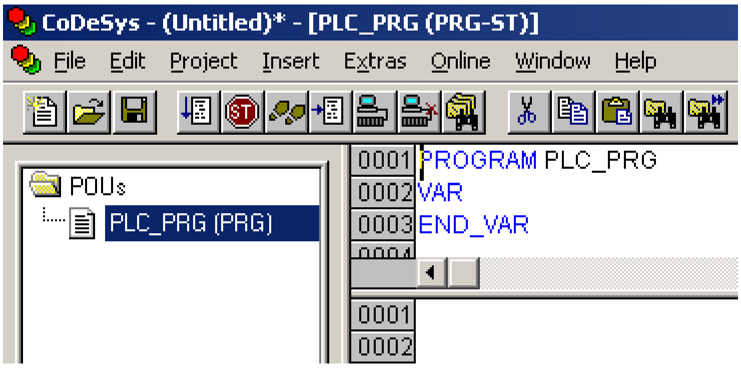


Name of the new POU: PLC_PRG

Type of POU
● Program
○ Function Block
○ Function
Return Type: BOOL

Language of the POU
○ IL
○ LD
○ FBD
○ SFC
● ST
○ CFC

Figure 52: Creating a New Function Block


CoDeSys - (Untitled)* - [PLC_PRG (PRG-ST)]
File Edit Project Insert Extras Online Window Help
POUs
PLC_PRG (PRG)

```
PROGRAM PLC_PRG
VAR
END_VAR
```

Figure 53: Programming Interface With the PLC_PRG Program Module

9.2.3 Creating the PLC Configuration

Note

Procedure for Creating the PLC Configuration

The procedure explained in this section describes the PLC configuration for the I/O modules connected to the controller.
Information about the controller function for any fieldbuses connected to the system is given in the section on the specific fieldbus.

The PLC configuration is used to configure the fieldbus controller, along with the connected I/O modules and to declare variables for accessing the inputs and outputs of the I/O modules.

1. Click on the “Resources” tab.

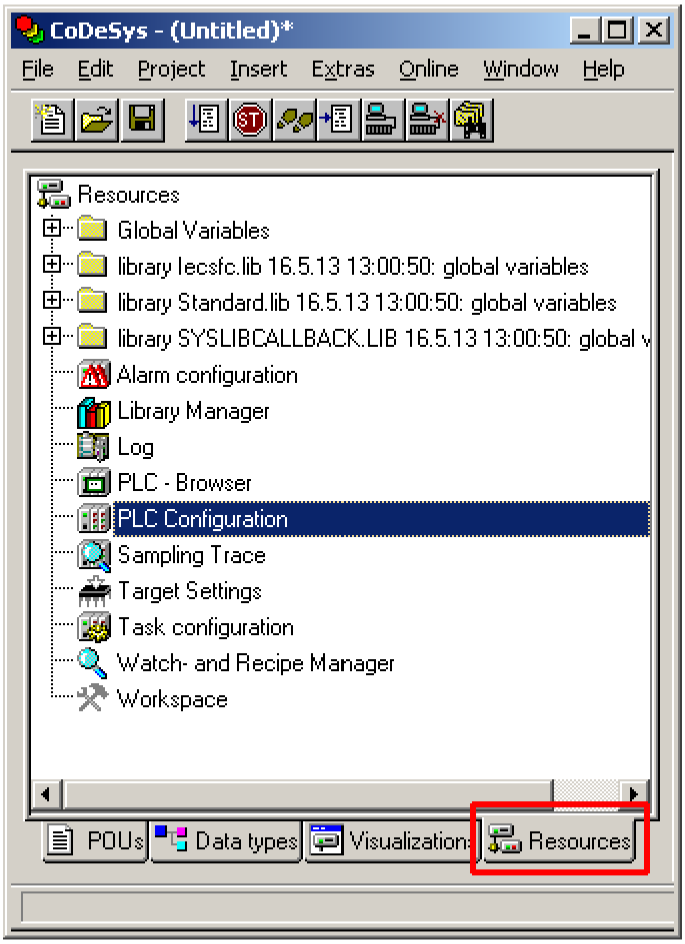

CoDeSys - (Untitled)*
File Edit Project Insert Extras Online Window Help
Resources
Global Variables
library Iecsfc.lib 16.5.13 13:00:50: global variables
library Standard.lib 16.5.13 13:00:50: global variables
library SYSLIBCALLBACK.LIB 16.5.13 13:00:50: global v
Alarm configuration
Library Manager
Log
PLC - Browser
PLC Configuration
Sampling Trace
Target Settings
Task configuration
Watch- and Recipe Manager
Workspace
POUs
Data types
Visualizations
Resources

Figure 54: “Resources” Tab

2. In the left window double-click on “PLC configuration”. The PLC configuration for the controller opens.

3. Right-click on the entry “K-Bus[FIX]” and then select “Edit” in the contextual menu. The “configuration” dialog window then opens.

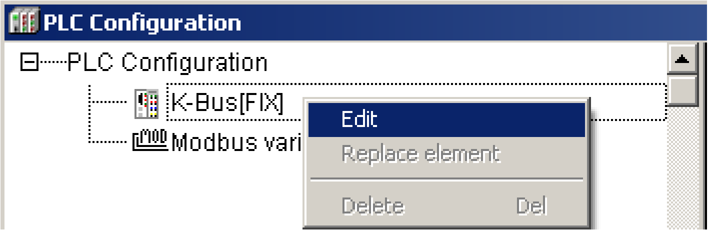


Figure 55: Control Configuration – Edit

4. There are three options for accepting the topology for the I/O modules connected to the fieldbus controller. The simplest way is to scan in the topology using WAGO-I/O-*CHECK*.
   To do this, click on the “Start WAGO-I/O-*CHECK* and scan” button.

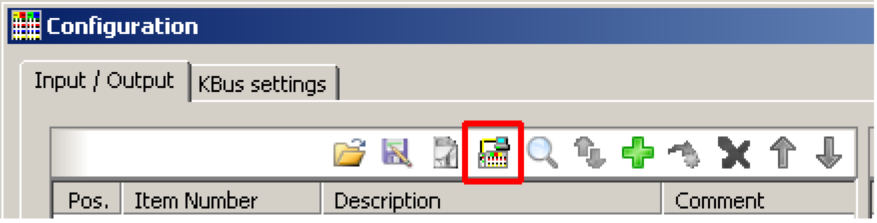


Figure 56: “Start WAGO-I/O-*CHECK* and Scan” Button

Note

Ensure proper installation of WAGO-I/O-*CHECK*!

This function requires that the latest version of WAGO-I/O-*CHECK* be installed and the IP address set under “Online > Communication parameters”, as otherwise communication will not be possible.

5. WAGO-I/O-*CHECK* is started.

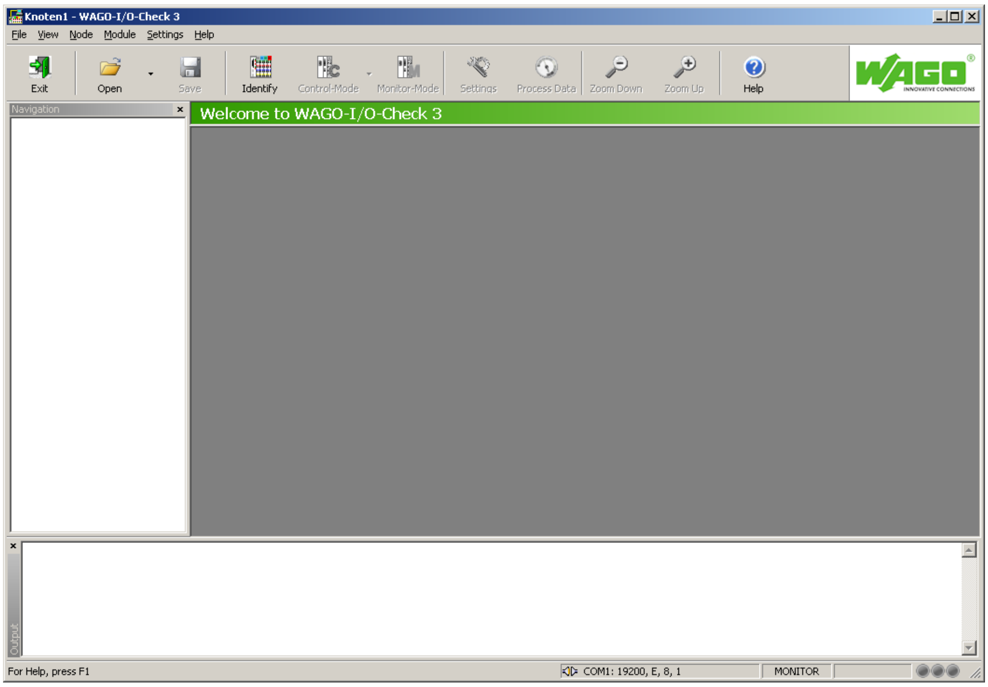


Figure 57: WAGO-*I/O-CHECK* – Starting Screen

6. To connect to the controller and read in the module configuration, click **[Identify]**.

7. If this action is successful click **[Save]** and exit WAGO-I/O-*CHECK*.

8. The detected I/O modules then appear in the configuration window.

Note

Passive I/O Modules

Remember that passive I/O modules, such as a power supply module (750-602/xxx-xxx) or end module (750-600/xxx-xxx) will not be shown in the I/O configurator.

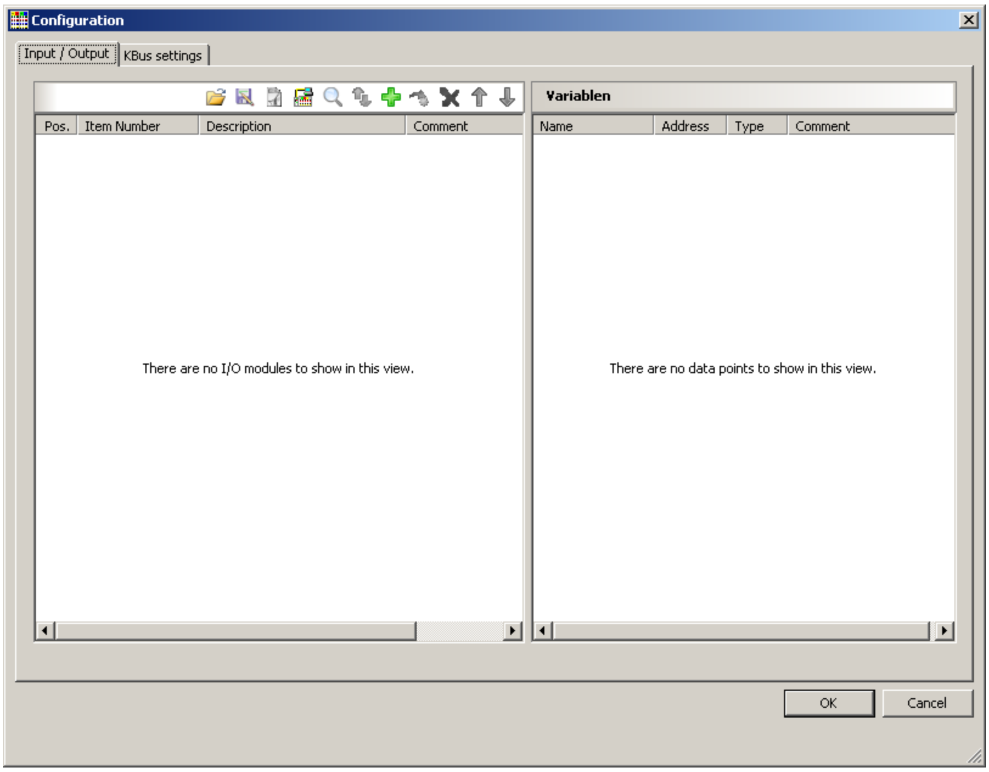


Figure 58: I/O Configurator Empty

9. You can use the **[Add]** button to add new I/O modules to manually define or change the configuration.

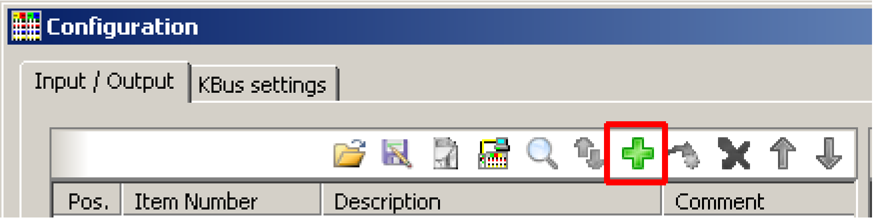


Figure 59: “Add I/O Modules” Button

10. You can select a module in the new “Module selection” window that then appears.

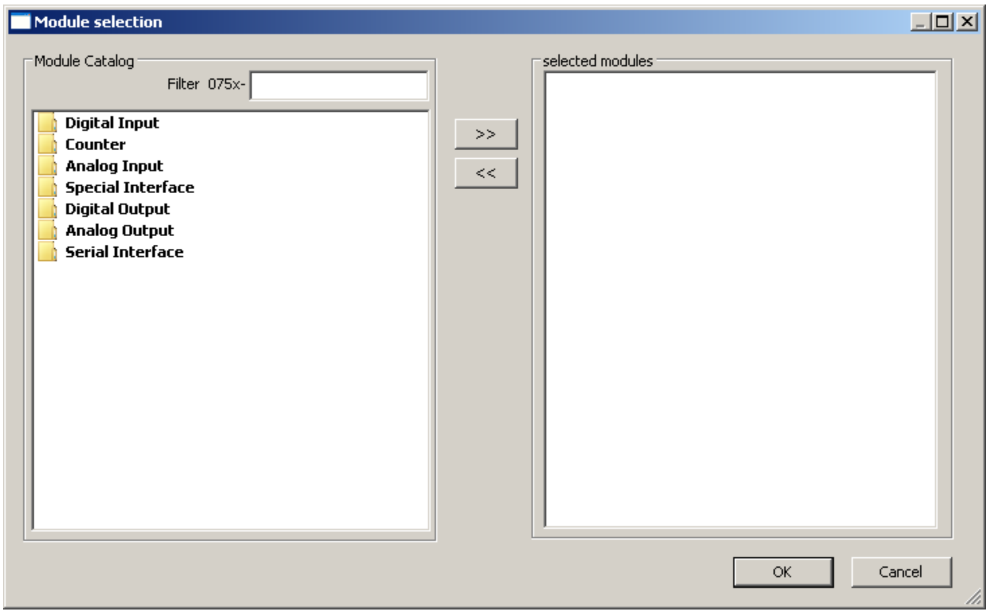
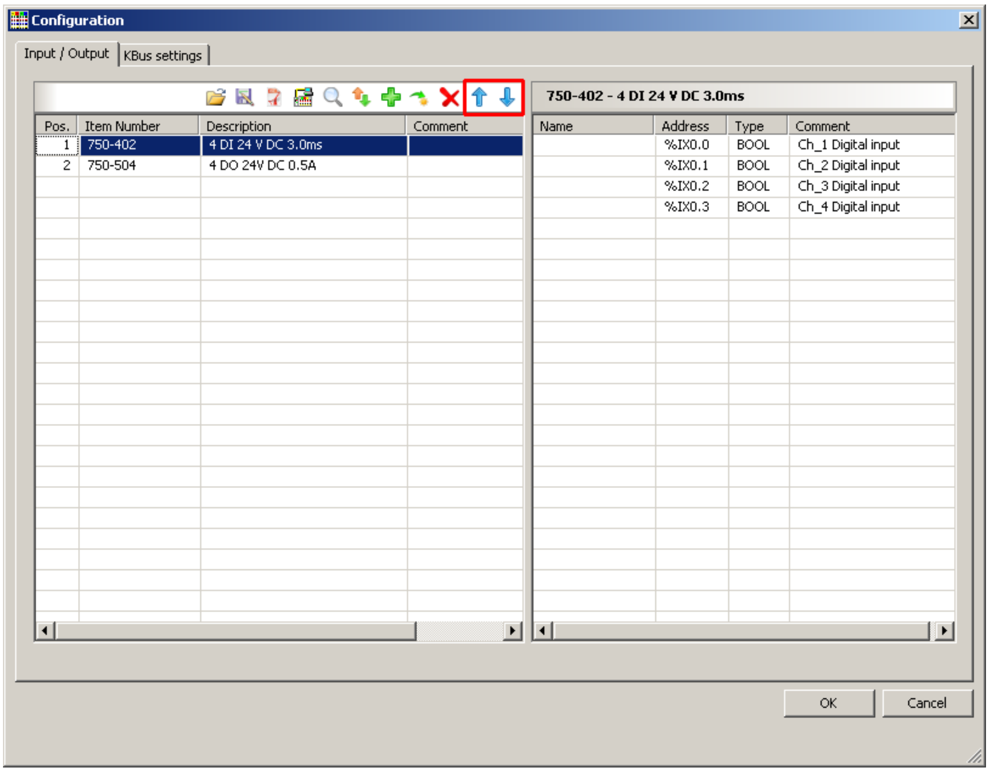


Figure 60: “Module Selection” Window

11. You can change the position of an I/O module by marking it and then using the arrow buttons at the right edge of the window to move it up or down.



Pos.	Item Number	Description	Comment
1	750-402	4 DI 24 V DC 3.0ms	
2	750-504	4 DO 24V DC 0.5A	

750-402 - 4 DI 24 V DC 3.0ms

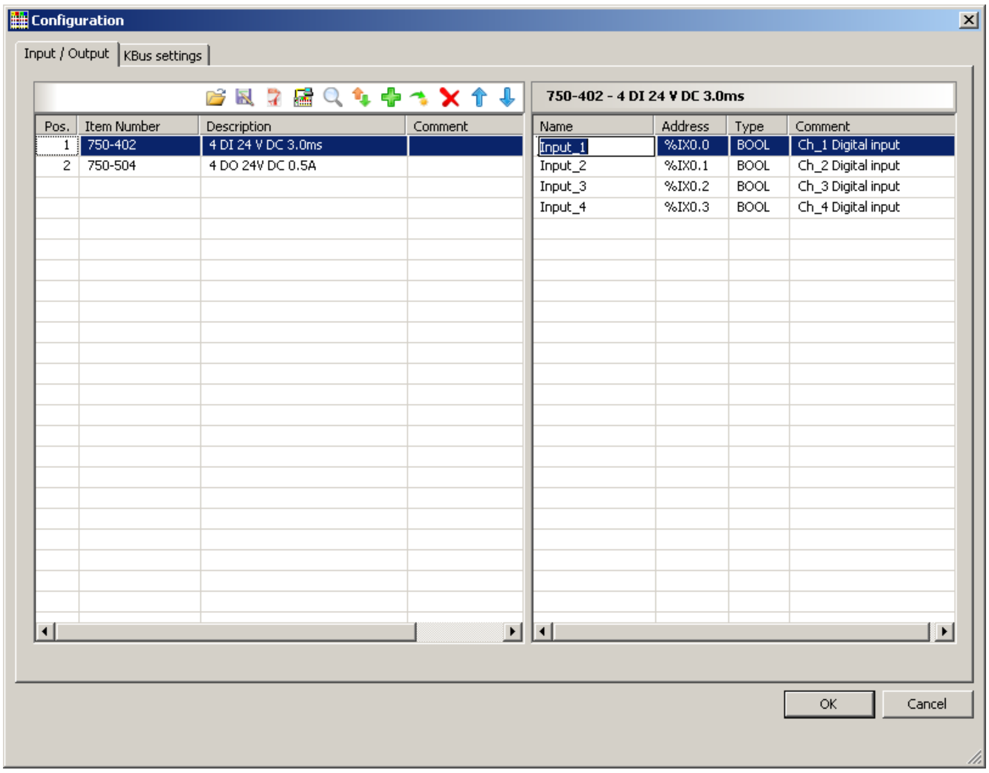
Name	Address	Type	Comment
	%IX0.0	BOOL	Ch_1 Digital input
	%IX0.1	BOOL	Ch_2 Digital input
	%IX0.2	BOOL	Ch_3 Digital input
	%IX0.3	BOOL	Ch_4 Digital input

Figure 61: I/O Configurator with Defined I/O Modules

12. Use **[Import configuration from file]** to add a configuration imported previously using WAGO-I/O-*CHECK*.

13. To close the I/O Configurator, click **[OK]**.

14. The individual inputs and outputs of the selected I/O module are displayed in the right half of the configuration window.
Here, you can declare a dedicated variable in the "Name" column for each input and output, e.g., "Output_1", "Output_2", "Input_1", "Input_2".



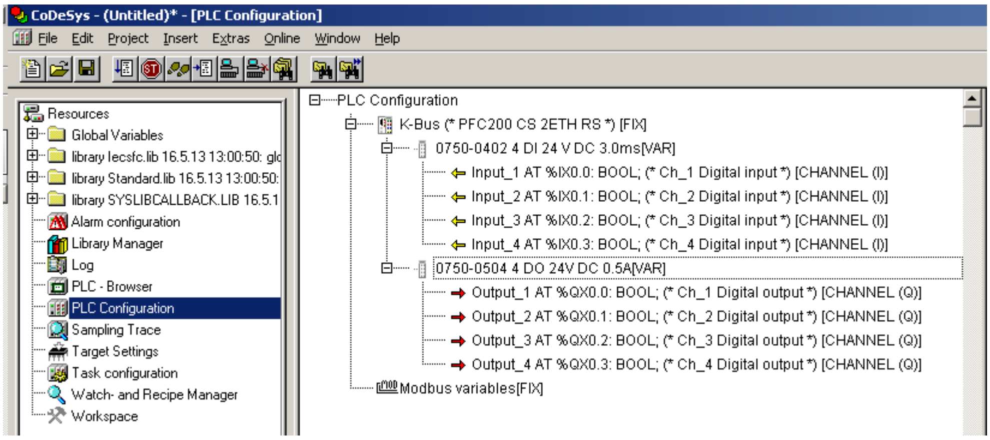
Pos.	Item Number	Description	Comment
1	750-402	4 DI 24 V DC 3.0ms	
2	750-504	4 DO 24V DC 0.5A	

750-402 - 4 DI 24 V DC 3.0ms

Name	Address	Type	Comment
Input_1	%IX0.0	BOOL	Ch_1 Digital input
Input_2	%IX0.1	BOOL	Ch_2 Digital input
Input_3	%IX0.2	BOOL	Ch_3 Digital input
Input_4	%IX0.3	BOOL	Ch_4 Digital input

Figure 62: Variable declaration

15. The added I/O modules appear in the control configuration under "K-Bus[FIX]" with their associated fixed addresses and, where applicable, their previously set variable name.

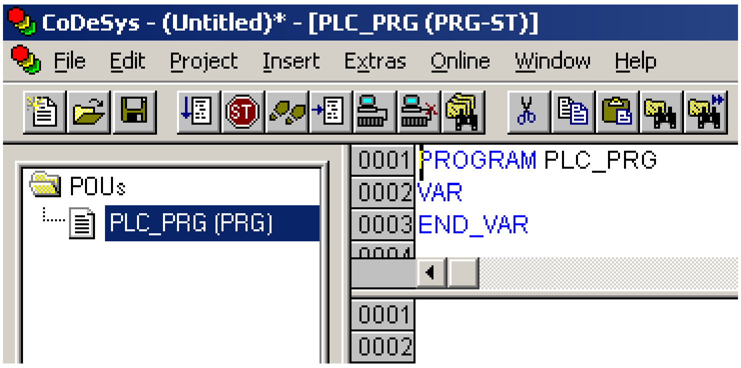


```
PLC Configuration
  K-Bus (* PFC200 CS 2ETH RS *) [FIX]
    0750-0402 4 DI 24 V DC 3.0ms[VAR]
      Input_1 AT %IX0.0: BOOL; (* Ch_1 Digital input *) [CHANNEL (I)]
      Input_2 AT %IX0.1: BOOL; (* Ch_2 Digital input *) [CHANNEL (I)]
      Input_3 AT %IX0.2: BOOL; (* Ch_3 Digital input *) [CHANNEL (I)]
      Input_4 AT %IX0.3: BOOL; (* Ch_4 Digital input *) [CHANNEL (I)]
    0750-0504 4 DO 24V DC 0.5A[VAR]
      Output_1 AT %QX0.0: BOOL; (* Ch_1 Digital output *) [CHANNEL (Q)]
      Output_2 AT %QX0.1: BOOL; (* Ch_2 Digital output *) [CHANNEL (Q)]
      Output_3 AT %QX0.2: BOOL; (* Ch_3 Digital output *) [CHANNEL (Q)]
      Output_4 AT %QX0.3: BOOL; (* Ch_4 Digital output *) [CHANNEL (Q)]
  Modbus variables[FIX]
```

Figure 63: Control Configuration: I/O Modules with Their Associated Addresses

9.2.4 Editing the Program Function Block

To edit the PLC_PRG program function block, go to the “Function block” tab and double-click on the PLC_PRG program module.

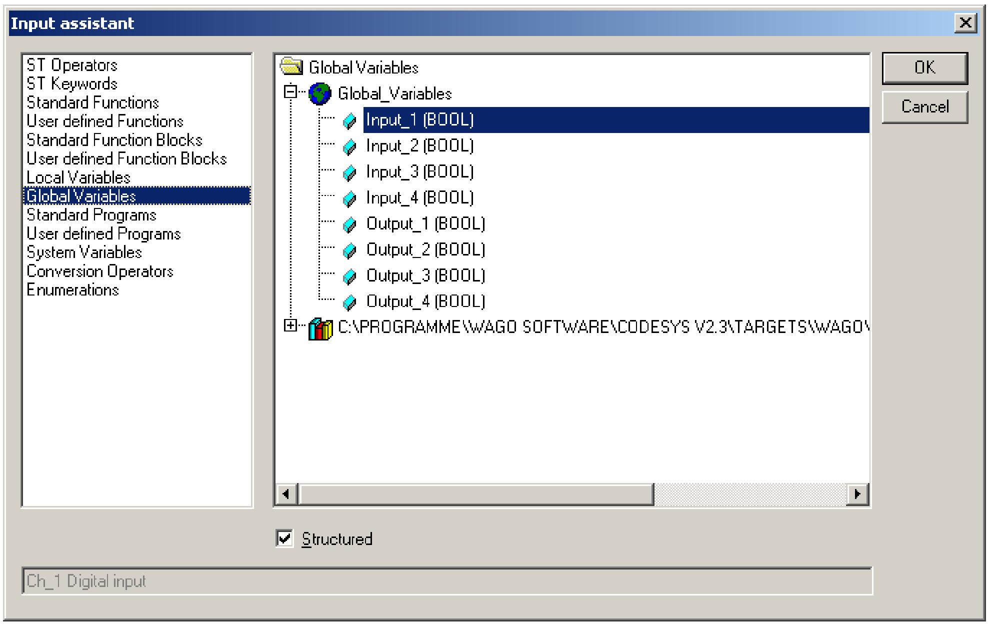

CoDeSys - (Untitled)* - [PLC_PRG (PRG-ST)]
File Edit Project Insert Extras Online Window Help
POUs
PLC_PRG (PRG)

```
PROGRAM PLC_PRG
VAR
END_VAR
```

Figure 64: Program Function Block

The following example illustrates the editing of the program function block. To do this, an input is assigned to an output:

1. Press **[F2]** to open the Input assistant, or right click and select “Input assistant” from the contextual menu.



ST Operators
ST Keywords
Standard Functions
User defined Functions
Standard Function Blocks
User defined Function Blocks
Local Variables
Global Variables
Standard Programs
User defined Programs
System Variables
Conversion Operators
Enumerations

Global Variables
Global_Variables
Input_1 (BOOL)
Input_2 (BOOL)
Input_3 (BOOL)
Input_4 (BOOL)
Output_1 (BOOL)
Output_2 (BOOL)
Output_3 (BOOL)
Output_4 (BOOL)
C:\PROGRAMME\WAGO SOFTWARE\CODESYS V2.3\TARGETS\WAGO\

☑ Structured

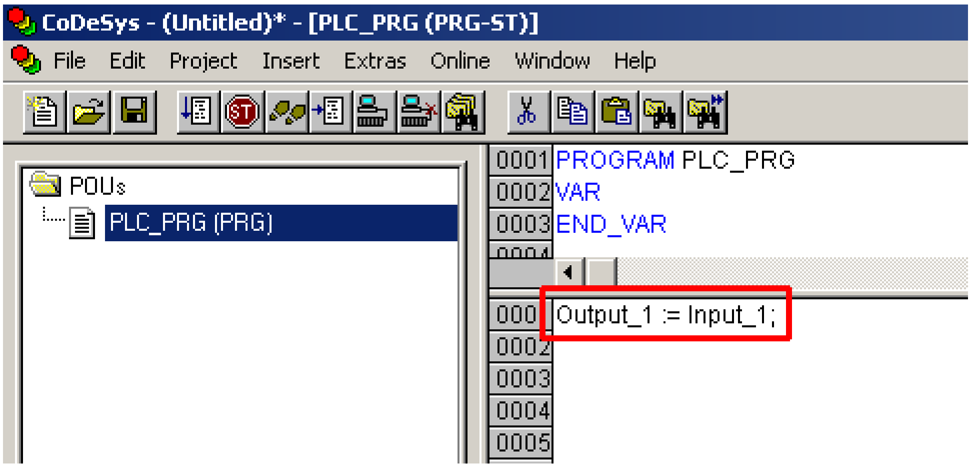
Ch_1 Digital input

Figure 65: Input Assistant for Selecting Variables

2. Under “Global variables” select the previously declared variable “Output_1” and click **[OK]** to add it.

3. Enter the allocation “=” behind the variable name.

4. Repeat Step 2 for the “Input_1” variable.


CoDeSys - (Untitled)* - [PLC_PRG (PRG-ST)]
File Edit Project Insert Extras Online Window Help
POUs
PLC_PRG (PRG)

```
PROGRAM PLC_PRG
VAR
END_VAR
```

```
Output_1 := Input_1;
```

Figure 66: Example of an Allocation

5. To compile, click on **Project > Compile all** in the menu bar.

9.2.5 Loading and Running the PLC Program in the Fieldbus Controller (ETHERNET)

Requirement:

- The simulation is deactivated (**Online > Simulation**).
- The PC is linked to the controller via ETHERNET. Refer to Section “Device Description” > …> “ETHERNET – X1, X2 Network Connection”.

Proceed as follows:

1. In the menu bar click on **Online** and select **Communication parameters …**. The “Communication Parameters” window opens.
2. To select a communication link, click on **[New …]** in the “Communication Parameters” window. A window opens in which you can define a communication link.

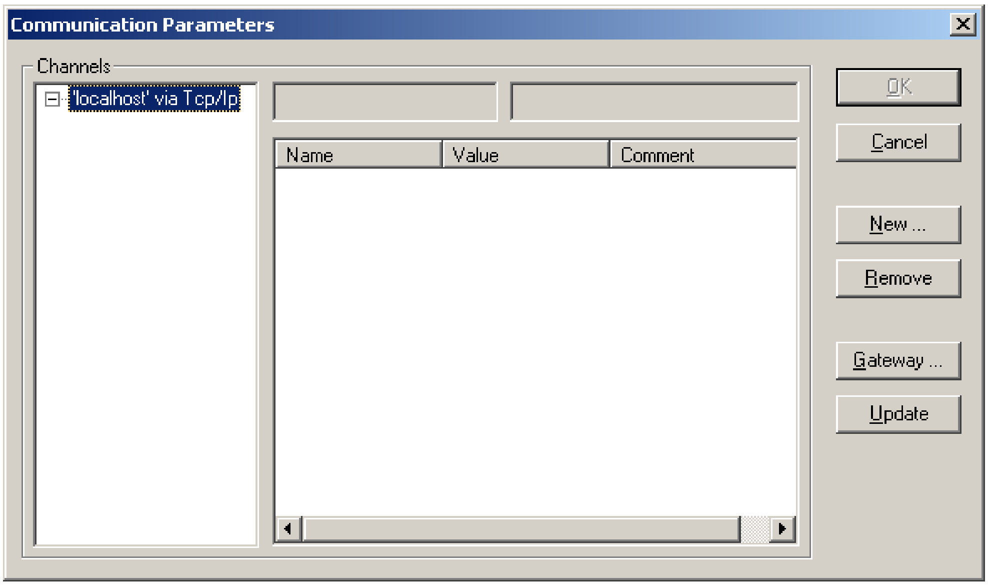
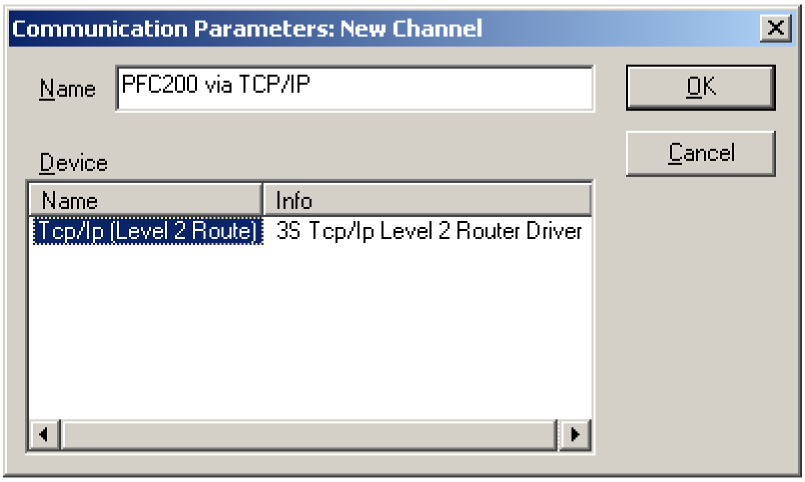


Figure 67: Creating a Communication Link – Step 1

3. In the “Name” field enter a designation for your fieldbus controller and then click on “Tcp/Ip (Level 2 Route)”. Then click **[OK]**.

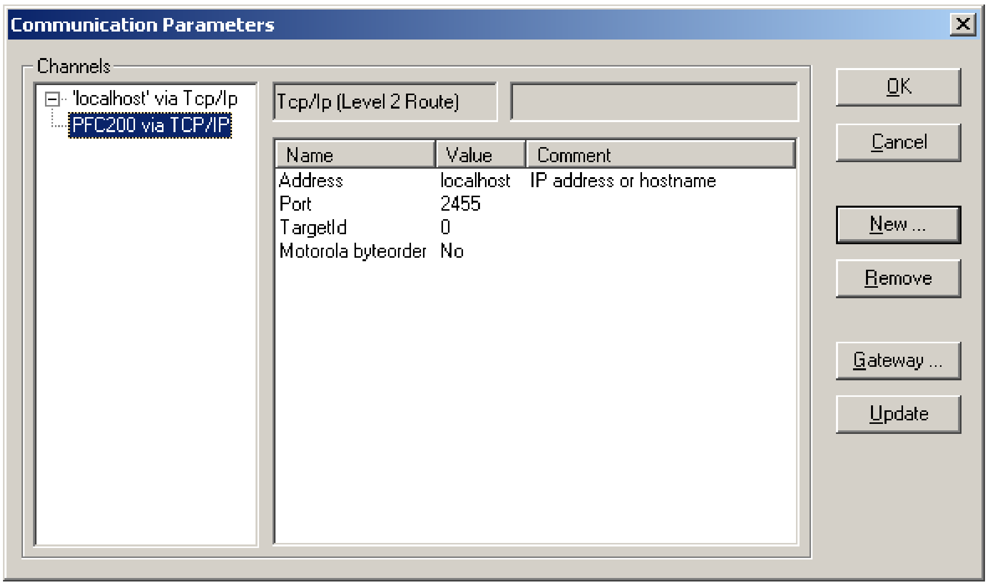


Name: PFC200 via TCP/IP

Name	Info
Tcp/Ip (Level 2 Route)	3S Tcp/Ip Level 2 Router Driver

Figure 68: Creating a Communication Link – Step 2

4. In the “Communication Parameters” window enter the **IP address of your fieldbus controller** in the “Address” field and then press Enter. To close the window, click on **[OK]**.
To select an already created controller, select it in the left window and then click on **[OK]**.



'localhost' via Tcp/Ip
PFC200 via TCP/IP

Tcp/Ip (Level 2 Route)

Name	Value	Comment
Address	localhost	IP address or hostname
Port	2455	
TargetId	0	
Motorola byteorder	No	

Figure 69: Creating a Communication Link – Step 3

5. Transfer the PLC program by clicking on **Online** in the menu bar and select **Login**.

6. Ensure that the Run/Stop switch for the fieldbus controller is set to “Run”.

7. Start the PLC program by clicking on **Online > Start** in the menu bar.

9.2.6 Creating a Boot Project

Create a boot project to ensure that the PLC program starts automatically again after a fieldbus controller restart. In the menu bar select **Online > Create boot project**. You must be logged in to CODESYS to use this function.

Note

Automatic loading of the boot project

In addition, you can load the boot project automatically when starting the fieldbus controller. Click on the “Resources” tab and open “Target system settings”. Select the “General” tab and “Load boot project automatically”.

If a boot project (DEFAULT.PRG and DEFAULT.CHK) is present under */home/codesys* and the “Run/Stop” switch of the fieldbus controller is set to “Run”, the fieldbus controller automatically starts with the processing of the PLC program. The PLC program is not started if the switch is set to “Stop”.

If a PLC program is running in the fieldbus controller, a PLC task starts with the reading of the fieldbus data (only with fieldbus controllers and fieldbus connection), the integrated input and output data and the I/O modules. The output data changed in the PLC program is updated after the PLC task is processed. A change in operating mode (“Stop/Run”) is only carried out at the end of a PLC task. The cycle time includes the time from the start of the PLC program to the next start. If a larger loop is programmed within a PLC program, the task time is prolonged accordingly. The inputs and outputs are updated during processing. These updates only take place at the end of a PLC task.

9.3 Syntax of Logical Addresses

Access to individual memory elements according to IEC 61131-3 is possible using only the following special symbols:

Table 43: Syntax of Logical Addresses

Item	Prefix	Description	Notes:
1	%	Starts the absolute address	-
2	I	Input	
	Q	Output	
	M	Flag	
3	X	Single bit	Data width
	B-	Byte (8 bits)	
	W	Word (16 bits)	
	D	Double word (32 bits)	
4		Address	

Two examples:

Addressing by word	%QW27 (28th word)
Addressing by bit	%IX1.9 (10th bit in word 2)

Enter the character string of the absolute address without empty spaces. The first bit of a word has an address of 0.

9.4 Creating Tasks

Set the time response and the priority of individual tasks in the task configuration.

Note

Watchdog

In an application program without task configuration, there is no watchdog that monitors the cycle time of the application program (PLC_PRG).

Create a task as follows:

1. Open the task configuration by double-clicking on the “Task configuration” module in the “Resources” tab.

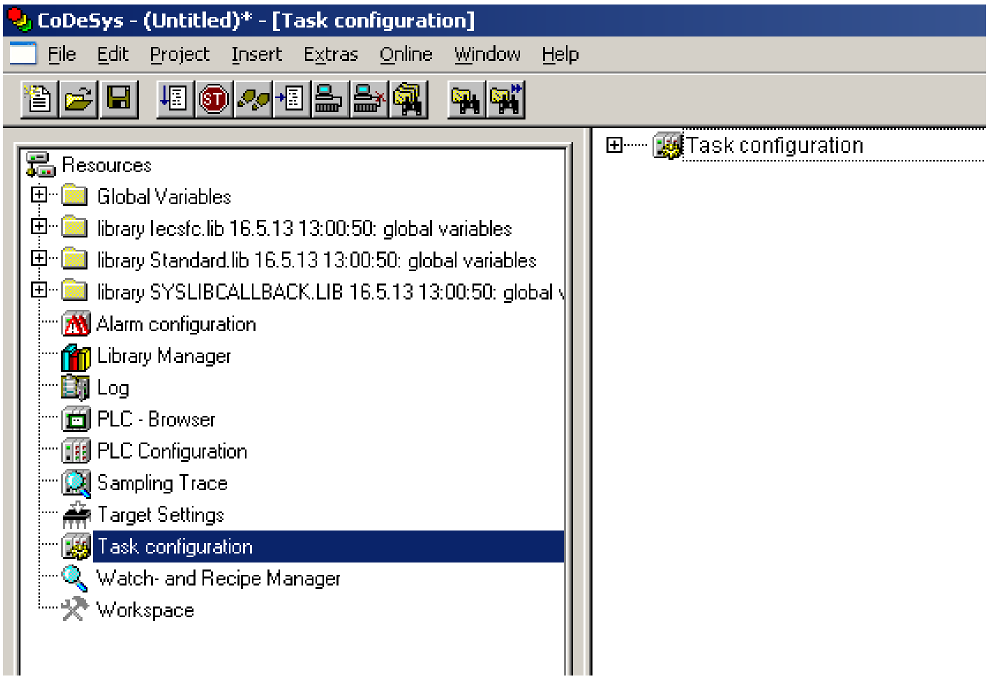

CoDeSys - (Untitled)* - [Task configuration]
File Edit Project Insert Extras Online Window Help
Resources
Global Variables
library Iecsfc.lib 16.5.13 13:00:50: global variables
library Standard.lib 16.5.13 13:00:50: global variables
library SYSLIBCALLBACK.LIB 16.5.13 13:00:50: global v
Alarm configuration
Library Manager
Log
PLC - Browser
PLC Configuration
Sampling Trace
Target Settings
Task configuration
Watch- and Recipe Manager
Workspace
Task configuration

Figure 70: Task Configuration

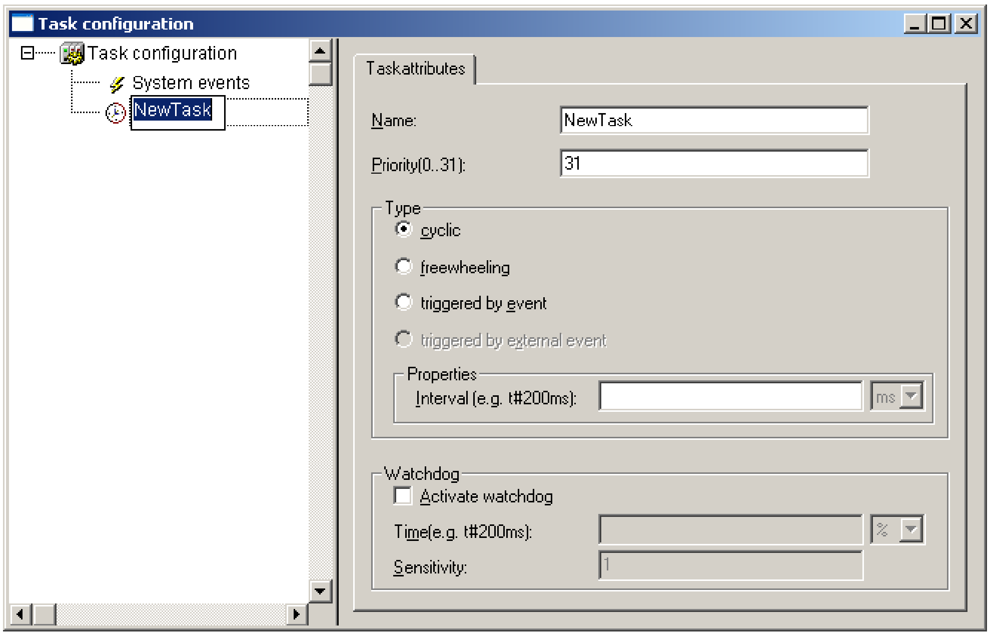
2. To create a task right-click on “Task configuration” and in the contextual menu select “Attach task”.

3. To assign a new name to the task (e.g. PLC_Prog), click on “New Task”. Then select the type of task. In this example, this is the “cyclic” type.

Note

Observe the cycle time!

The minimum cycle time for I/O-based tasks is 2 milliseconds (ms)!


Task configuration

- Task configuration
  - System events
  - NewTask

Taskattributes

Name: NewTask

Priority(0..31): 31

Type
● cyclic
○ freewheeling
○ triggered by event
○ triggered by external event

Properties
Interval (e.g. t#200ms): ms

Watchdog
□ Activate watchdog
Time(e.g. t#200ms): %
Sensitivity: 1

Figure 71: Changing Task Names 1

4. Add the program module PLC_PRG that you have just created (see Section “Editing the Program Modules”). To do this, right-clock on the “Clock” symbol and in the contextual menu select “Attach program call-up”. Then, click the **[...]** button and **[OK]**.

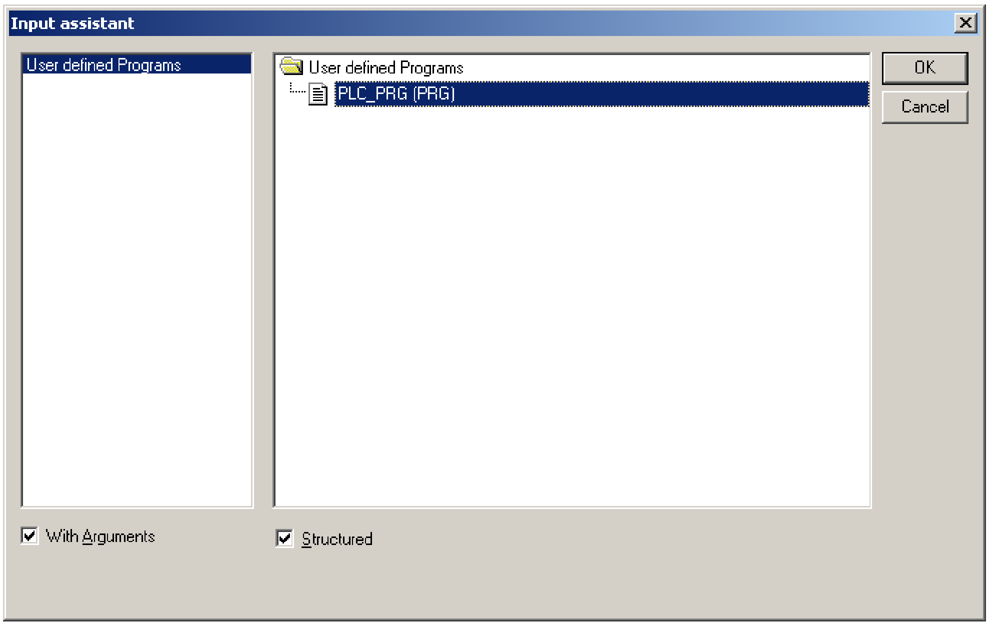
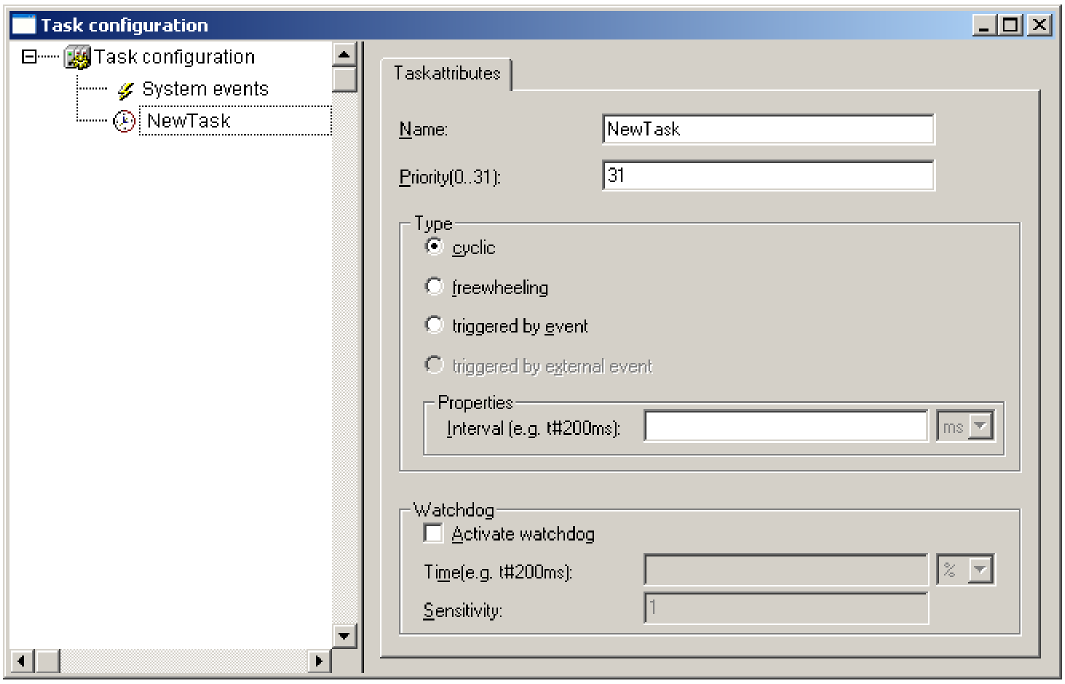


Figure 72: Call-up to Add to the Program Module

5. Compile the example program by selecting **Project > Rebuild all** in the context menu.

9.4.1 Cyclic Tasks

You can assign a priority for each task in order to establish the task processing sequence.



Name: NewTask

Priority(0..31): 31

Type

● cyclic

○ freewheeling

○ triggered by event

○ triggered by external event

Properties

Interval (e.g. t#200ms): ms

Watchdog

□ Activate watchdog

Time(e.g. t#200ms): %

Sensitivity: 1

Figure 73: Cyclic Task

Note

Order of Task Processing

The priorities given below do not specifiy the order of task processing. The tasks start in an arbitrary order.

Priority 0 … 5:
Important arithmetic operations and synchronized access to I/O module process images are to be carried out as tasks with the highest priorities 0 … 5. These tasks are processed fully according to priority and correspond to Linux® RT priorities
-79 through -74.

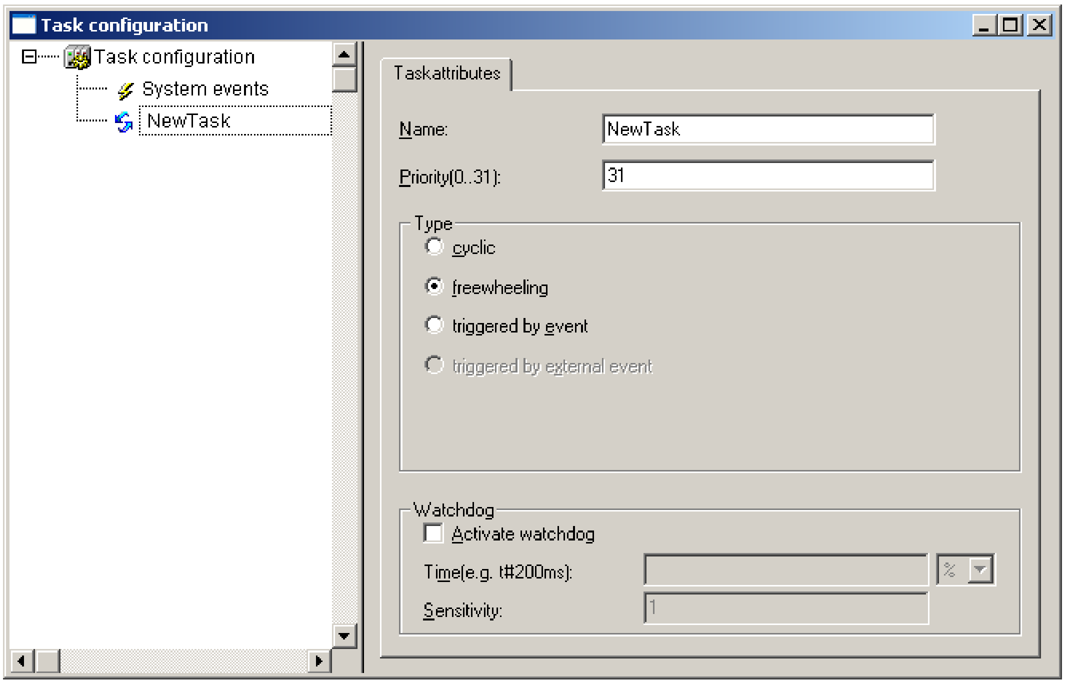
Priority 6 … 20:
Real-time access, such as access to ETHERNET and the file system, to fieldbus data and to the RS-232 interface (when available) are to be carried out as tasks with average priorities 6 … 20. These tasks are processed fully according to priority and correspond to Linux® RT priorities -40 through -26.

Priority 21 … 31:
Applications such as long-lasting arithmetic operations and non-real-time-relevant access to ETHERNET and the file system, to fieldbus data and the RS-232 interface (when provided) are to be carried out as tasks with the lowest priorities 21 … 31. No prioritiy distinction is made between tasks of priorities 21

… 31. These tasks all receive the same computing time from the operating system (“Completely Fair Scheduler” procedure).

9.4.2 Freewheeling Tasks

So-called freewheeling tasks are not processed in cycles. Their processing depends solely on the current capacity of the system. The input field “Priority (0 … 31)” is provided for freewheeling tasks without a function. These tasks are handled as tasks with priority 21 … 31.



Name: NewTask

Priority(0..31): 31

Type
○ cyclic
● freewheeling
○ triggered by event
○ triggered by external event

Watchdog
□ Activate watchdog
Time(e.g. t#200ms):
Sensitivity: 1

Figure 74: Freewheeling Task

Note

PLC-PRG as Freewheeling Task without Task Configuration

If you do not perform any task configuration, the program PLC_PRG is carried out with the lowest priority at an interval of 10 ms. The runtime of “freewheeling tasks” is not monitored by a CODESYS watchdog.

9.4.3 Debugging an IEC Program

If the IEC program is debugged with breakpoints, the behavior on actuation of the mode selector switch is defined as follows:

Provided that a task is not located on a breakpoint, RUN and STOP from the user interface (IDE) and from the mode selector switch (BAS) always have an effect on all tasks (case 1 and case 2).

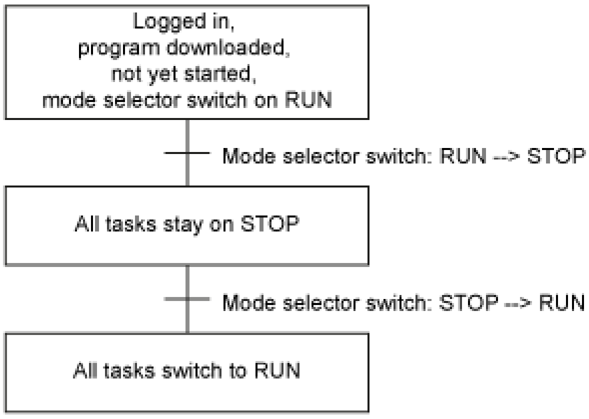

Logged in,
program downloaded,
not yet started,
mode selector switch on RUN
Mode selector switch: RUN --> STOP
All tasks stay on STOP
Mode selector switch: STOP --> RUN
All tasks switch to RUN

Figure 75: Debugging (Case 1)

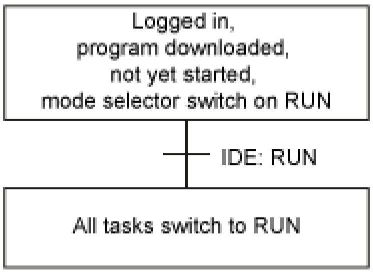


Figure 76: Debugging (Case 2)

If the mode selector switch and the STOP function of the user interface are used simultaneously, the mode selector switch has priority (case 3 and case 4).

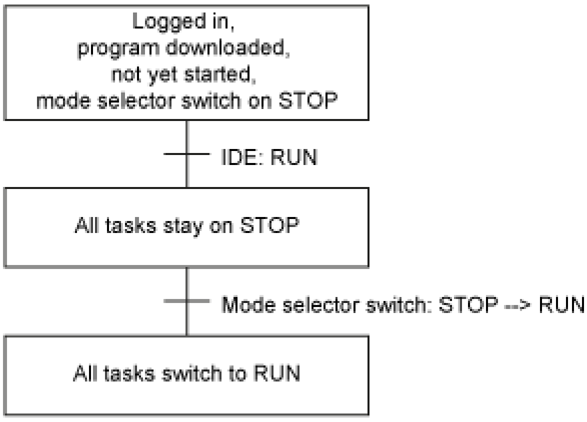


Figure 77: Debugging (Case 3)

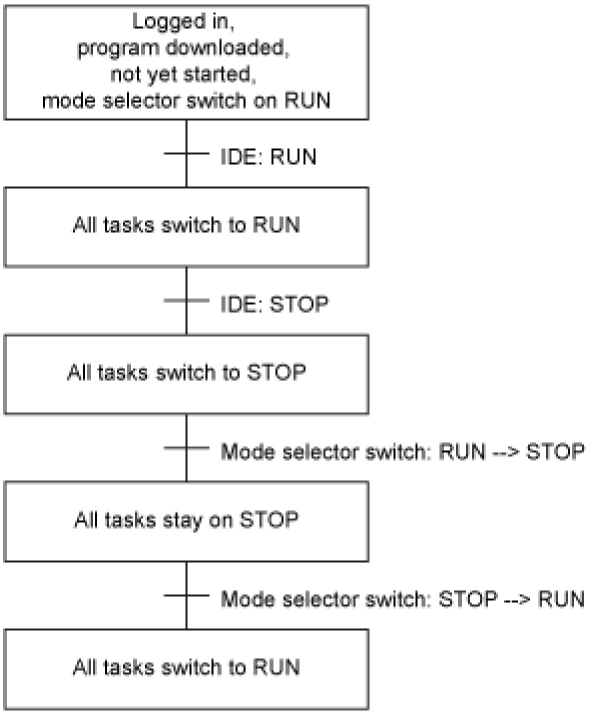


Figure 78: Debugging (Case 4)

As soon as a task is located at a breakpoint, only all other tasks can be controlled with the mode selector switch.

Exception: If the mode selector switch is on STOP, the debug task is also no longer processed.

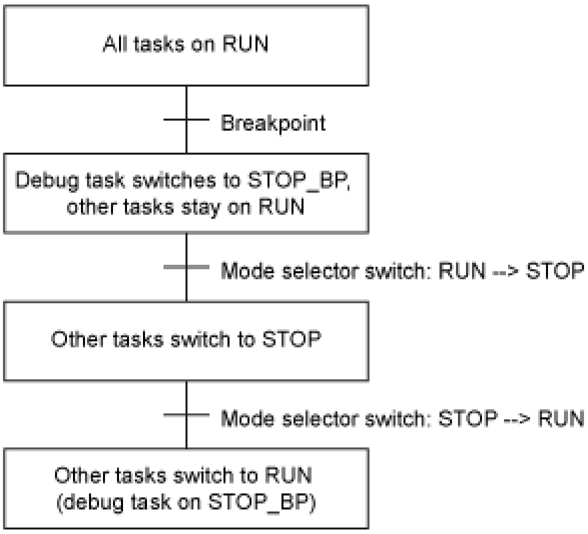

All tasks on RUN
Breakpoint
Debug task switches to STOP_BP, other tasks stay on RUN
Mode selector switch: RUN --> STOP
Other tasks switch to STOP
Mode selector switch: STOP --> RUN
Other tasks switch to RUN (debug task on STOP_BP)

Figure 79: Debugging (Case 5)

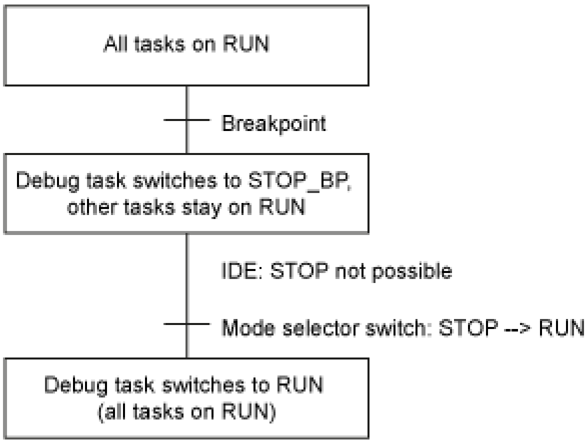

All tasks on RUN
Breakpoint
Debug task switches to STOP_BP, other tasks stay on RUN
IDE: STOP not possible
Mode selector switch: STOP --> RUN
Debug task switches to RUN (all tasks on RUN)

Figure 80: Debugging (Case 6)

If a task is at a breakpoint and the connection to the IDE is broken (e.g., by logging out), all breakpoints are deleted.
The debug task stays at the current position until the next time the mode selector switch is switched from STOP to RUN. In this case, the task continues to run from the current position (case 7).

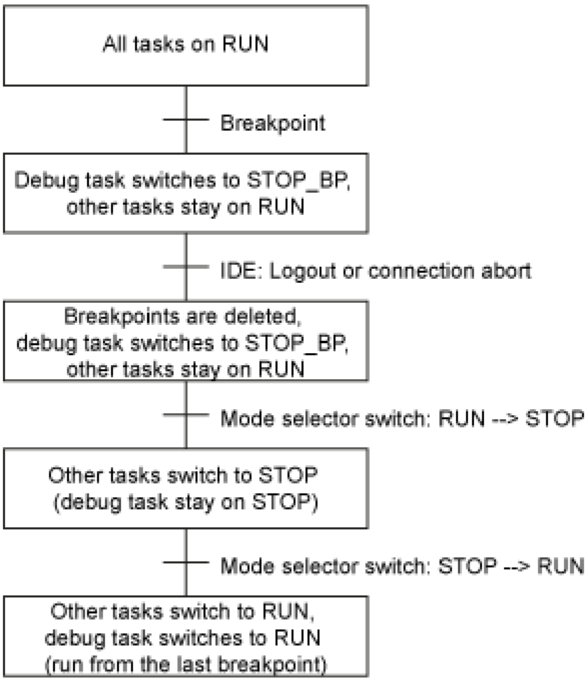
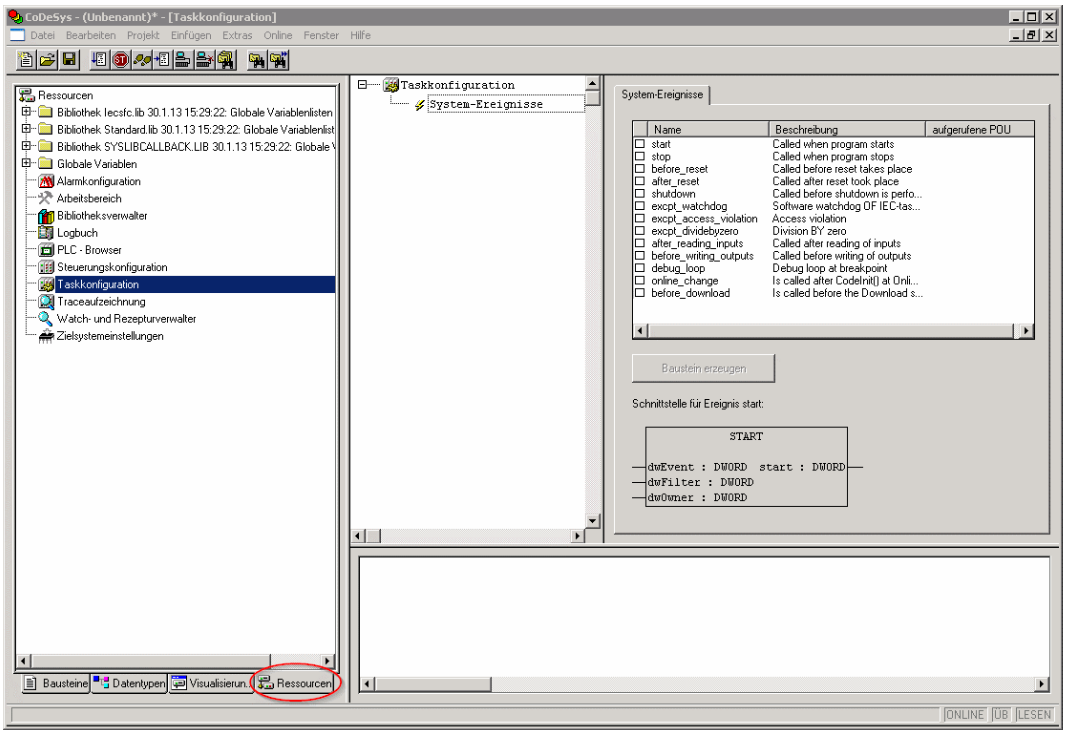

All tasks on RUN
Breakpoint
Debug task switches to STOP_BP, other tasks stay on RUN
IDE: Logout or connection abort
Breakpoints are deleted, debug task switches to STOP_BP, other tasks stay on RUN
Mode selector switch: RUN --> STOP
Other tasks switch to STOP (debug task stay on STOP)
Mode selector switch: STOP --> RUN
Other tasks switch to RUN, debug task switches to RUN (run from the last breakpoint)

Figure 81: Debugging (Case 7)

9.5 System Events

Event tasks can be used in the CODESYS task configuration in addition to cyclical tasks. Event tasks call up certain events in the device.

To activate events and define a program to be called up, open the window “Task configuration” in the “Resources” tab in the CODESYS development environment.


CoDeSys - (Unbenannt)* - [Taskkonfiguration]
Datei Bearbeiten Projekt Einfügen Extras Online Fenster Hilfe
Bausteine
Datentypen
Visualisierun...
Ressourcen
System-Ereignisse
Baustein erzeugen
ONLINE
ÜB
LESEN

Ressourcen
- Bibliothek Iecsfc.lib 30.1.13 15:29:22: Globale Variablenlisten
- Bibliothek Standard.lib 30.1.13 15:29:22: Globale Variablenlist
- Bibliothek SYSLIBCALLBACK.LIB 30.1.13 15:29:22: Globale V
- Globale Variablen
- Alarmkonfiguration
- Arbeitsbereich
- Bibliotheksverwalter
- Logbuch
- PLC - Browser
- Steuerungskonfiguration
- Taskkonfiguration
- Traceaufzeichnung
- Watch- und Rezepturverwalter
- Zielsystemeinstellungen

Taskkonfiguration
- System-Ereignisse

	Name	Beschreibung	aufgerufene POU
□	start	Called when program starts	
□	stop	Called when program stops	
□	before_reset	Called before reset takes place	
□	after_reset	Called after reset took place	
□	shutdown	Called before shutdown is perfo...	
□	excpt_watchdog	Software watchdog OF IEC-tas...	
□	excpt_access_violation	Access violation	
□	excpt_dividebyzero	Division BY zero	
□	after_reading_inputs	Called after reading of inputs	
□	before_writing_outputs	Called before writing of outputs	
□	debug_loop	Debug loop at breakpoint	
□	online_change	Is called after CodeInit() at Onli...	
□	before_download	Is called before the Download s...	

Schnittstelle für Ereignis start:

```
          START
dwEvent : DWORD   start : DWORD
dwFilter : DWORD
dwOwner : DWORD
```

Figure 82: CODESYS – System Events

Note

Do not set debug points in the event handlers!

Debug points in event handlers can lead to unforeseeable errors and must therefore not be set!

The following events can be activated:

Table 44: Events

Name	Description
start	The event is called directly after the user program starts.
stop	The event is called directly after the user program stops.
before_reset	The event is called directly before the user program is reset.
after_reset	The event is called directly after the user program is reset.
shutdown	The event is called directly before the user program is shutdown.
excpt_watchdog	The event is called if a task watchdog is recognized.
excpt_access_violation	The event is called if a memory access error to an invalid memory area is recognized. (incorrect pointer, invalid array index, invalid data descriptor)
excpt_dividebyzero	The event is called if a division by zero is recognized.
after_reading_inputs	The event is triggered after reading all of the inputs independent of the user program.
before_writing_outputs	The event is triggered before writing all of the outputs independent of the user program.
debug_loop	This event is triggered at every task call, if a breakpoint was reached in this task and the processing of this task is therefore blocked.
online_change	This event is called up after initialization of the program on an online change.
before_download	This event is always called up before a download from the IDE to the device takes place.

Note

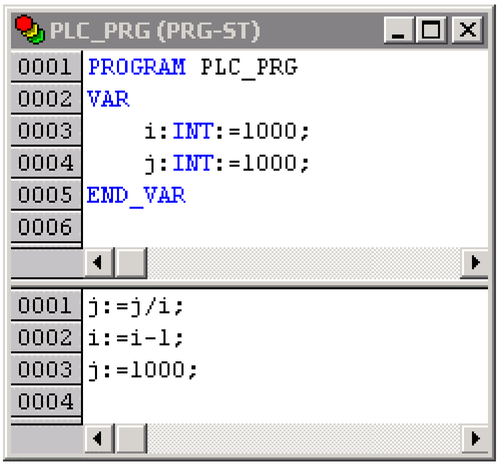
Application stops on a non-defined event handler!

If “excpt” events occur in the system and an event handler has not been defined, the application goes into the “Stop” status.

9.5.1 Creating an Event Handler

The example here is provided to illustrate how to define and use an event handler. The event handler “excpt_dividebyzero” is used in this example.

First, a program is generated in the PLC_PRG- module which provokes division by 0.



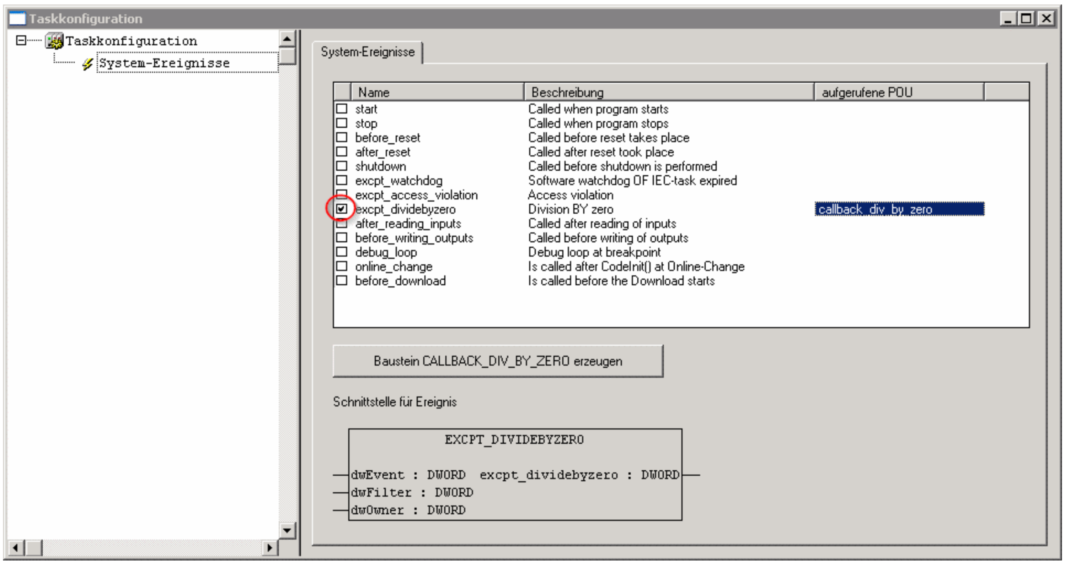
PLC_PRG (PRG-ST)

```
PROGRAM PLC_PRG
VAR
     i:INT:=1000;
     j:INT:=1000;
END_VAR

```

```
j:=j/i;
i:=i-1;
j:=1000;

```

Figure 83: CODESYS Program Provokes Division by “0”

After this, the system event “excpt_dividebyzero” is activated in the Task Configurator and the name of the event handler to be generated is entered in the column “Called POU”.



	Name	Beschreibung	aufgerufene POU
☐	start	Called when program starts	
☐	stop	Called when program stops	
☐	before_reset	Called before reset takes place	
☐	after_reset	Called after reset took place	
☐	shutdown	Called before shutdown is performed	
☐	excpt_watchdog	Software watchdog OF IEC-task expired	
☐	excpt_access_violation	Access violation	
☑	excpt_dividebyzero	Division BY zero	callback_div_by_zero
☐	after_reading_inputs	Called after reading of inputs	
☐	before_writing_outputs	Called before writing of outputs	
☐	debug_loop	Debug loop at breakpoint	
☐	online_change	Is called after CodeInit() at Online-Change	
☐	before_download	Is called before the Download starts	

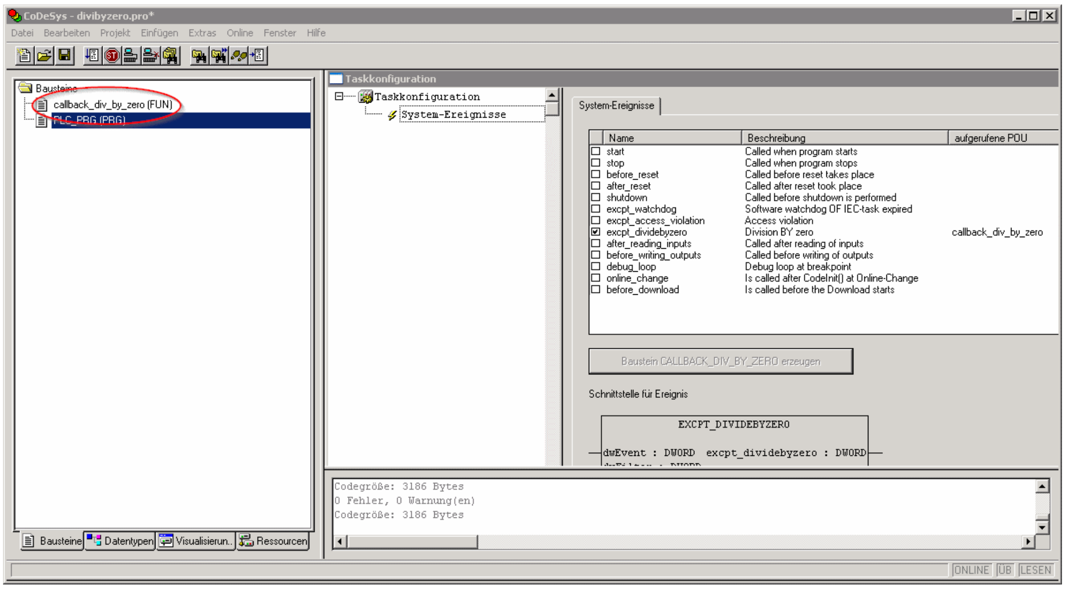
Schnittstelle für Ereignis

```
EXCPT_DIVIDEBYZERO

dwEvent : DWORD  excpt_dividebyzero : DWORD
dwFilter : DWORD
dwOwner : DWORD
```

Figure 84: CODESYS – Creating and Activating an Event Handler

To generate the event handler, click **[Generate CALLBACK_DIV_BY_ZERO function block]**.

A new function having the defined name then appears in the “Function blocks” tab.


CoDeSys - divibyzero.pro*
Datei Bearbeiten Projekt Einfügen Extras Online Fenster Hilfe
Bausteine
callback_div_by_zero (FUN)
PLC_PRG (PRG)
Bausteine
Datentypen
Visualisierun..
Ressourcen
Taskkonfiguration
Taskkonfiguration
System-Ereignisse
System-Ereignisse
Baustein CALLBACK_DIV_BY_ZERO erzeugen
Schnittstelle für Ereignis
EXCPT_DIVIDEBYZERO
ONLINE
ÜB
LESEN

	Name	Beschreibung	aufgerufene POU
☐	start	Called when program starts	
☐	stop	Called when program stops	
☐	before_reset	Called before reset takes place	
☐	after_reset	Called after reset took place	
☐	shutdown	Called before shutdown is performed	
☐	excpt_watchdog	Software watchdog OF IEC-task expired	
☐	excpt_access_violation	Access violation	
☑	excpt_dividebyzero	Division BY zero	callback_div_by_zero
☐	after_reading_inputs	Called after reading of inputs	
☐	before_writing_outputs	Called before writing of outputs	
☐	debug_loop	Debug loop at breakpoint	
☐	online_change	Is called after CodeInit() at Online-Change	
☐	before_download	Is called before the Download starts	

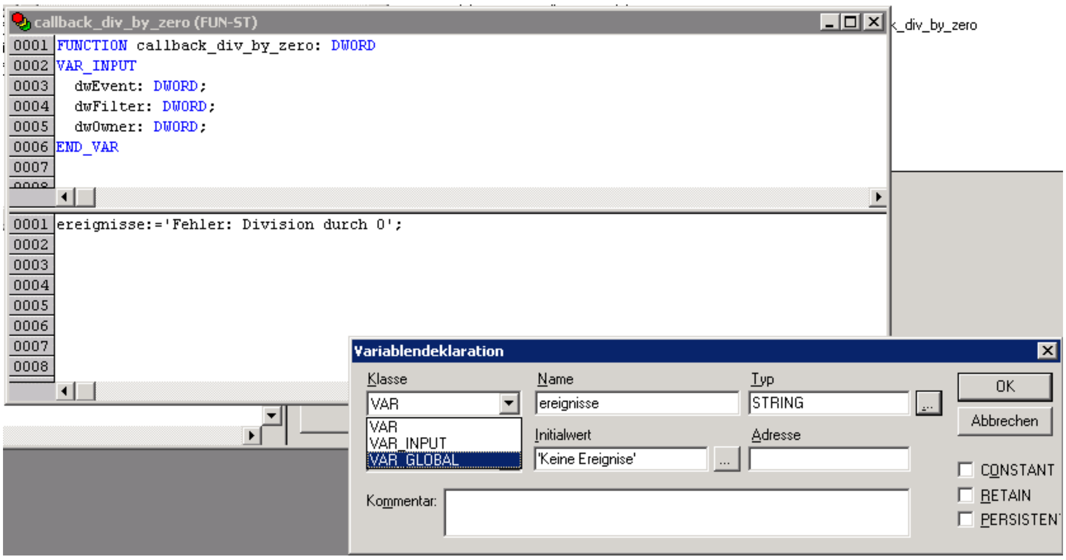
```
dwEvent : DWORD   excpt_dividebyzero : DWORD
```

```
Codegröße: 3186 Bytes
0 Fehler, 0 Warnung(en)
Codegröße: 3186 Bytes
```

Figure 85: CODESYS – New Module has been Generated

Handling for the event that has occurred is now programmed in this new function.

In the example here, the event is documented in a global variable.



```
FUNCTION callback_div_by_zero: DWORD
VAR_INPUT
  dwEvent: DWORD;
  dwFilter: DWORD;
  dwOwner: DWORD;
END_VAR
```

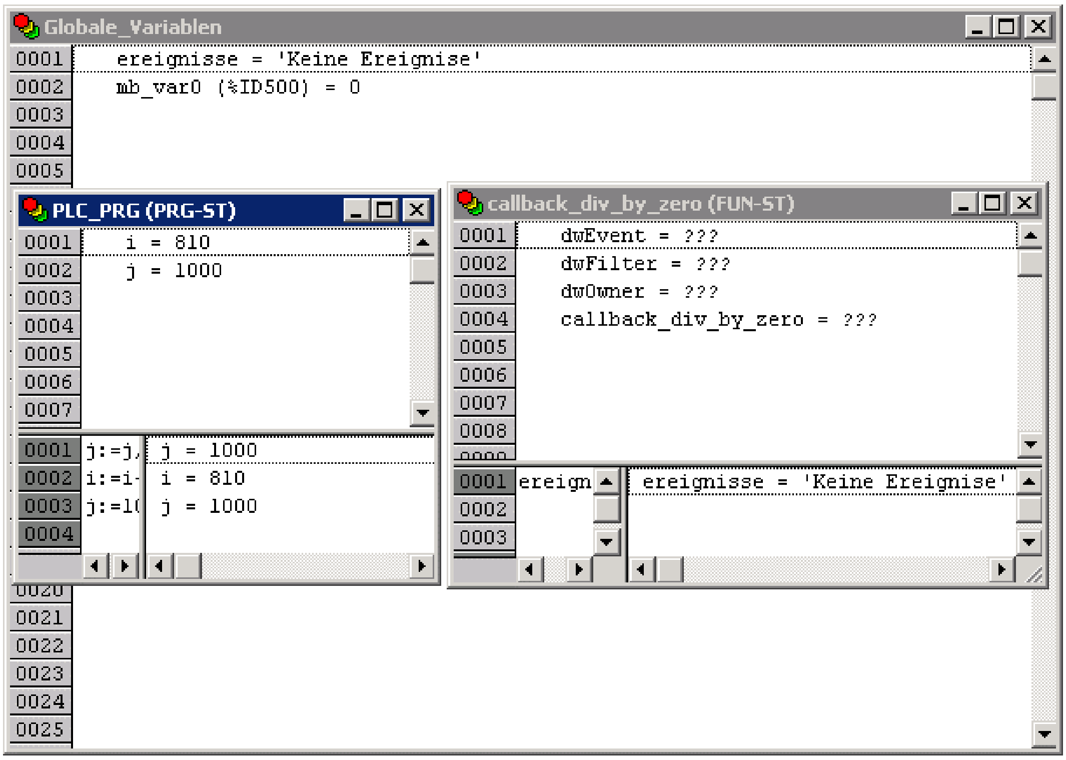
```
ereignisse:='Fehler: Division durch 0';
```

Klasse: VAR (VAR, VAR_INPUT, VAR_GLOBAL selected)
Name: ereignisse
Typ: STRING
Initialwert: 'Keine Ereignise'
Adresse:
Kommentar:
☐ CONSTANT
☐ RETAIN
☐ PERSISTENT

Figure 86: CODESYS – Enter the Event in a Global Variable

The newly created project is now supported and can be loaded to the controller.

After startup, the value of the “Events” variable changes only when counter “i” reaches the value 0, meaning that division by 0 has been performed.



```
ereignisse = 'Keine Ereignise'
mb_var0 (%ID500) = 0
```

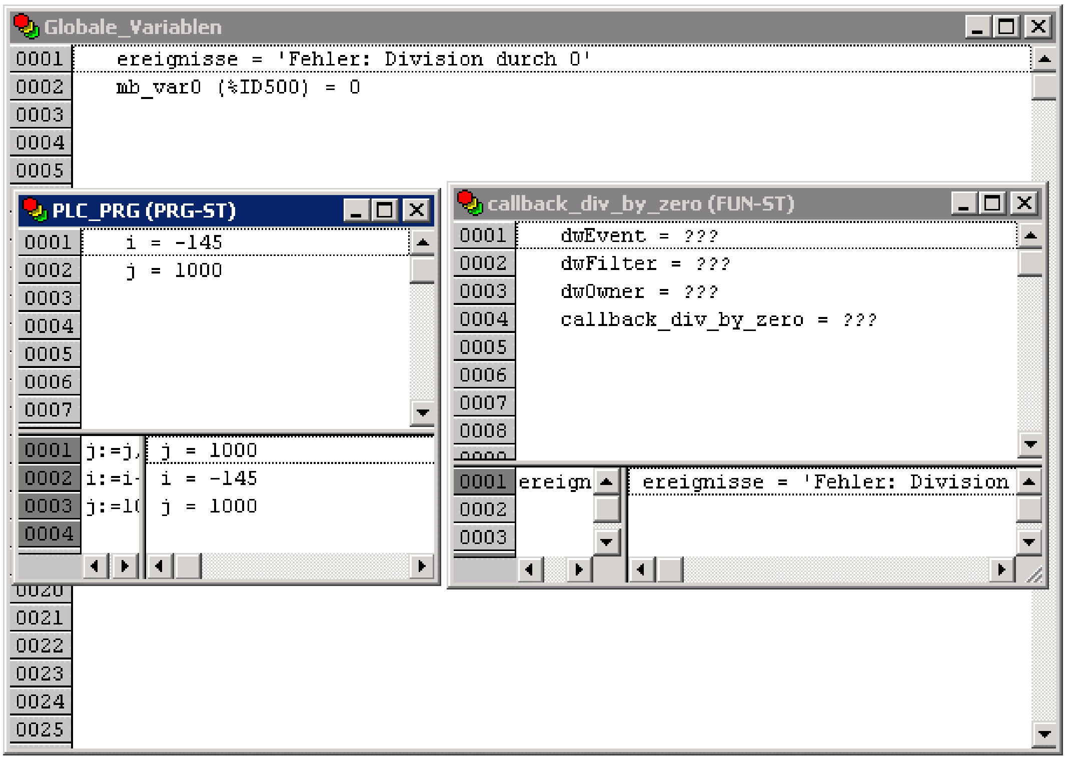
```
i = 810
j = 1000
```

```
j:=j, j = 1000
i:=i- i = 810
j:=1( j = 1000
```

```
dwEvent = ???
dwFilter = ???
dwOwner = ???
callback_div_by_zero = ???
```

```
ereign ereignisse = 'Keine Ereignise'
```

Figure 87: CODESYS – Variable Contents Prior to Division by “0”



```
ereignisse = 'Fehler: Division durch 0'
mb_var0 (%ID500) = 0
```

```
i = -145
j = 1000
```

```
j:=j, j = 1000
i:=i- i = -145
j:=1( j = 1000
```

```
dwEvent = ???
dwFilter = ???
dwOwner = ???
callback_div_by_zero = ???
```

```
ereign ereignisse = 'Fehler: Division
```

Figure 88: CODESYS – Variable Contents After Division by “0” and Call-up of the Event Handler

9.6 Process Images

A process image is a memory area in which the process data is stored in a defined sequence and consists of the I/O modules attached to the local bus, the PFC variables, the bit memory address area and the slaves attached to the fieldbus.

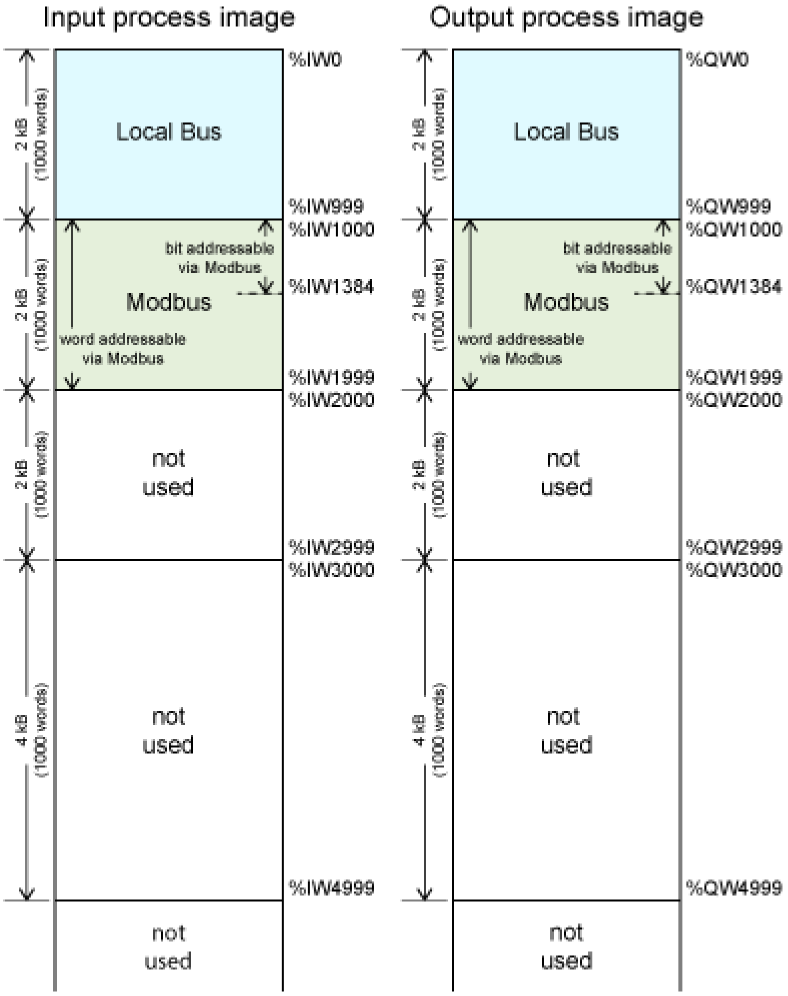


Figure 89: Process Image

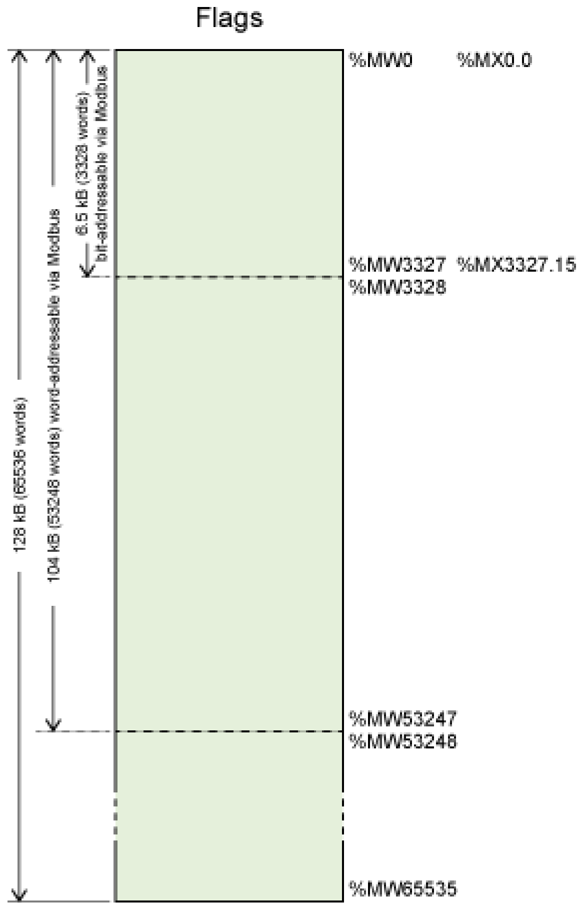

Flags
%MW0
%MX0.0
%MW3327
%MX3327.15
%MW3328
%MW53247
%MW53248
%MW65535
128 kB (65536 words)
104 kB (53248 words) word-addressable via Modbus
6.5 kB (3328 words) bit-addressable via Modbus

Figure 90: Flag Area

9.6.1 Process Images for I/O Modules Connected to the Controller

After starting the fieldbus controller, it automatically detects all connected I/O modules.
The analog input and output data is stored first word by word in the process image. Subsequent to this, come the digital input and output data bits combined to form words.

The size and structure of the process image for the I/O modules connected to the system are described in the appendix.

Note

I/O Module Data Width

The data width of an I/O module is between 0 and 48 bytes.

Note

I/O Module Process Data

Check the I/O module process data whenever you add or remove the modules to/from the fieldbus controller. Changing the I/O module topology results in an adjustment of the process image, as the process data addresses also change.

9.6.2 Process Image for Slaves Connected to the Fieldbus

The size and structure of the process image for the slaves connected to the system are described in the section for the specific fieldbus.

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!

9.7 Access to Process Images of the Input and Output Data via CODESYS 2.3

The following tables describe the possibilities with which you can access the address ranges of the process image for the inputs and outputs connected to the local bus.

Table 45: Access to the Process Images of the Input and Output Data – Local Bus

Memory Area	Description	Access via PLC	Logical Address Space
Local bus input process image	Map of the local input modules (I/O module 1 to 64*) in the RAM	Read	Word %IW0 to %IW999
			Byte %IB0 to %IB1999
Local bus output process image	Map of the local output modules (I/O module 1 to 64*) in the RAM	Read/ Write	Word %QW0 to %QW999
			Byte %QB0 to %QB1999

* The use of up to 250 I/O modules is possible with the WAGO local bus extension modules.

Table 46: Access to the Process Images of the Input and Output Data – Modbus

Memory area	Description	Access via PLC	Logical Address Space
Modbus input process image	Modbus input variables, addressed by word via Modbus	Read	Word %IW1000 to %IW1999
			Byte %IB2000 to %IB3999
	Modbus input variables, addressed by bit via Modbus	Read	Bit %IX1000.0 …%IX1000.15 to %IX1384.0 … %IX1384.15
Modbus output process image	Modbus output variables, addressed by word via Modbus	Read/ Write	Word %QW1000 to %QW1999
			Byte %QB2000 to %QB3999
	Modbus output variables, addressed by bit via Modbus	Read/ Write	Bit %QX1000.0 … %QX1000.15 to %QX1384.0 … %QX1384.15

Table 47: Access to the Process Images of the Input and Output Data – Flags

Memory Area	Description	Access via PLC	Logical Address Space
Flag variables	Total of 128 kB remanent memory (65536 words).	Read/ Write	%MW0 to %MW65535
	104 kB addressed by word via Modbus (53248 words)	Read/ Write	Word (Modbus) %MW0 to %MW3327
	6.5 kB addressed by bit via Modbus (3328 words).	Read/ Write	Bit (Modbus) %MX0.0 … %MX0.15 to %MX3327.0 … %MX3327.15
Retain variables	Retain memory addressed by symbols in the NVRAM: 128 kB	Read/ Write	-

* The use of up to 250 I/O modules is possible with the WAGO local bus extension modules.

The total size of the memory for flag and retain variables is 128 kB (131060 bytes). The size of these two sections can be customized as required, provided the total (permissible) size is not exceeded.
If you are using bit-oriented addressing, remember that the basic address is word-based. The bits are addressed from 0 to 15.

9.8 Addressing Example

The following addressing example clarifies the access to the process image:

Table 48: Arrangement of the I/O Modules for the Addressing Example

Fieldbus controller	750-400 1	750-554 2	750-402 3	750-504 4	750-454 5	750-650 6	750-468 7	750-600 8

Table 49: Addressing Example

I/O module	Input data	Output data	Description

Type	C*					
750-400	1		%IX8.0			**2DI, 24 V, 3 ms:** 1. Digital input module with a data width of 2 bits. As the analog input modules already occupy the first 8 words of the input process image, the 2 bits occupy the lowest-value bits of the 8th word.
	2		%IX8.1			
750-554	1			%QW0		**2AO, 4 – 20 mA:** 1. Analog output module with a data width of 2 words. This module occupies the first 2 words in the output process image.
	2			%QW1		
750-402	1		%IX8.2			**4DI, 24 V:** 2. Digital input module with a data width of 4 bits. These are added to the 2 bits of the 750-400 module and stored in the 8th word of the input process image.
	2		%IX8.3			
	3		%IX8.4			
	4		%IX8.5			
750-504	1				%QX4.0	**4DO, 24 V:** 1. Digital output module with a data width of 4 bits. As the analog output module already occupies the first 4 words of the output process image, the 4 bits occupy the lowest-value bits of the 4th word.
	2				%QX4.1	
	3				%QX4.2	
	4				%QX4.3	
750-454	1	%IW0				**2AI, 4 – 20 mA:** 1. Analog input module with a data width of 2 words. This module occupies the first 2 words in the input process image.
	2	%IW1				
750-650	1	%IW2				**RS-232, C 9600/8/N/1:** The serial interface module is an analog input and output module, which displays 2 words both in the input process image and in the output process image.
		%IW3				
				%QW2		
				%QW3		
750-468	1	%IW4				**4AI, 0 – 10 V S.E:** 2. Analog input module with a data width of 4 words. As the 750-454 and 750-650 analog input and output modules already occupy the first 4 words of the input process image, the 4 words of this I/O module are added behind the others.
	2	%IW5				
	3	%IW6				
	4	%IW7				
750-600						**End module** The passive 750-600 end module does not transmit any data.

▨	Analog input and output modules
□	Digital input and output modules

*C: Number of the input/output

9.9 Local Bus Synchronization

The local bus cycle and the CODESYS task cycle are optimally automatically synchronized: This depends on the number of I/O modules connected and the fastest CODESYS task cycle set in the fieldbus controller. The synchronization cases described below can therefore take place.

In this section, CODESYS task denotes only tasks within CODESYS that contain an access to the local bus. Tasks that do not access the local bus are not synchronized in the same way as described below. For this, see section “Creating Tasks.”

9.9.1 Case 1: CODESYS Task Interval Set Smaller than the Local Bus Cycle

Execution of the CODESYS tasks is synchronized with the local bus cycle time.

The CODESYS task is processed in parallel to the local bus cycle. The CODESYS task interval is extended to the local bus cycle time. This is necessary so that each CODESYS task is started with new input data from the local bus and the output values are also set at the module after each CODESYS task.

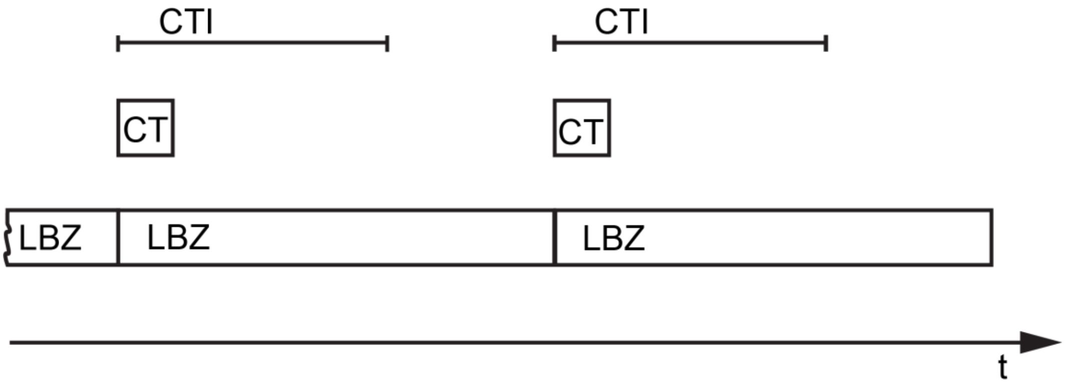


Figure 91: Local Bus Synchronization (Case 1)

CTI: CODESYS Task Interval
CT: CODESYS Task that accesses the I/O modules via the local bus
LBZ: Local Bus Cycle

Example:
CODESYS task interval (CTI): 100 µs
Local bus cycle (LBZ): 2000 µs
Result: Matching of the CODESYS task interval to the local bus cycle of 2000 µs.

9.9.2 Case 2: CODESYS Task Interval Smaller than Twice the Local Bus Cycle

Execution of the local bus is synchronized with the set CODESYS task interval.

At the end of the CODESYS task, the local bus cycle starts, which is processed synchronously with the fastest CODESYS task. This ensures that when starting each CODESYS Task, current input data are available from the local bus and the output values of each CODESYS task are also output to the I/O modules.

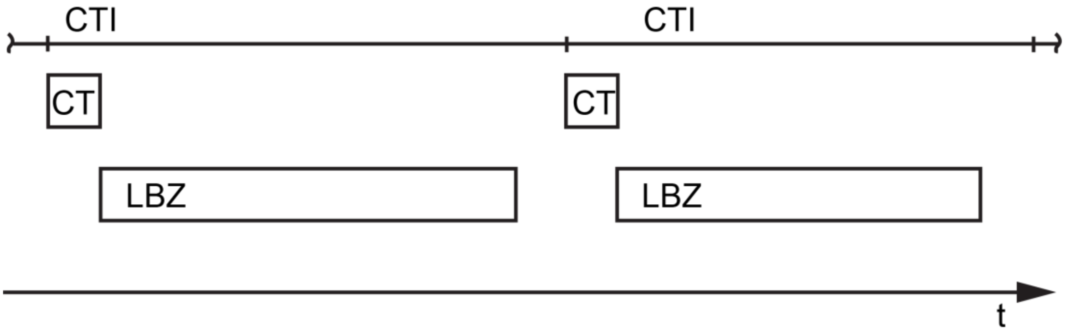


Figure 92: Local Bus Synchronization (Case 2)

CTI: CODESYS Task Interval
CT: CODESYS Task that accesses the I/O modules via the local bus
LBZ: Local Bus Cycle

Example:
CODESYS task interval (CTI): 2500 µs
Local bus cycle (LBZ): 2000 µs
Result: Execution of the local bus cycle every 2500 µs.

9.9.3 Case 3: CODESYS Task Interval Greater than Twice the Local Bus Cycle

The I/O data from the local bus are refreshed once prior to the CODESYS task and once after the CODESYS task.

Prior to processing the CODESYS task, the local bus cycle is executed, which provides the current input data for the CODESYS task. After execution of the CODESYS task, an additional local bus cycle is started, which provides the output data to the I/O modules.

This ensures that at the start of every CODESYS task, current input data are available from the local bus and the output data from each CODESYS task are quickly output to the I/O modules. This prevents processing of local bus cycles that would unnecessarily use a great deal of computing time on the CPU.

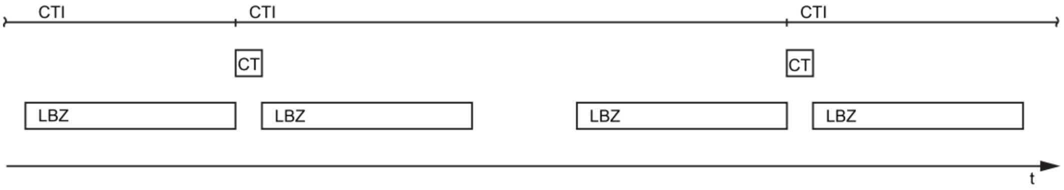


Figure 93: Local Bus Synchronization (Case 3)

CTI: CODESYS Task Interval
CT: CODESYS Task that accesses the I/O modules via the local bus
LBZ: Local Bus Cycle

Example:
CODESYS task interval (CTI): 5000 µs
Local bus cycle (LBZ): 2000 µs
Result: Execution of the local bus cycle 2000 µs prior to the CODESYS task and once directly after the CODESYS task.

9.9.4 Case 4: CODESYS Task Interval Greater than 10 ms

Synchronization takes place as in case 3; however, the output modules would be reset to their default state after 100 ms without a local bus cycle. This reliably prevents the execution of a local bus cycle after at least every 10 ms.

The I/O data from the local bus are refreshed once before the CODESYS task and once after the CODESYS task and an additional local bus cycle is also executed every 10 ms.

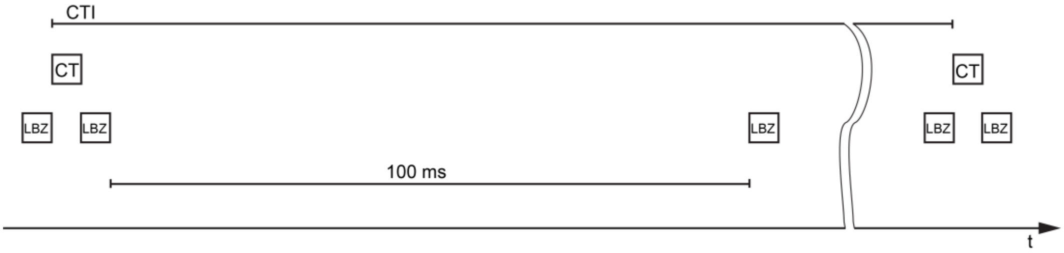
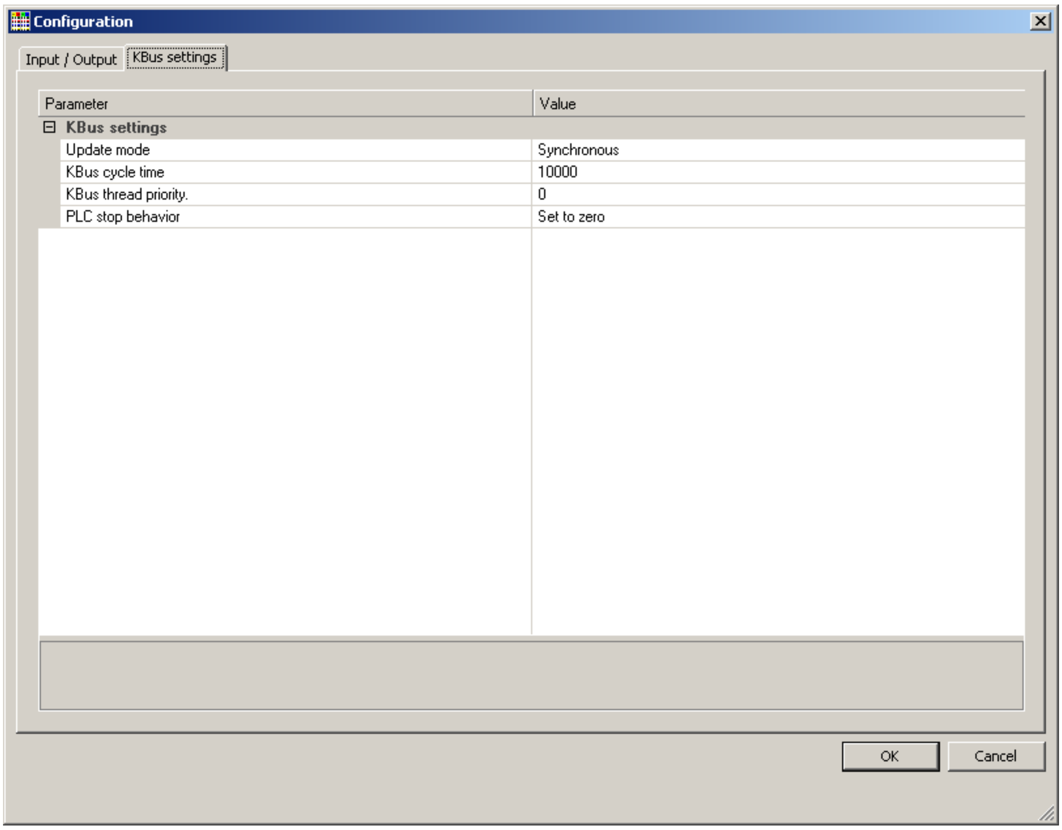


Figure 94: Local Bus Synchronization (Case 4)

CTI:	CODESYS Task Interval
CT:	CODESYS task that accesses the I/O modules via the local bus
LBZ:	Local bus cycle

Example:
CODESYS task interval (CTI): 150000 µs
Local bus cycle (LBZ): 2000 µs
Result: Execution of the local bus cycle 2000 µs prior to the CODESYS task, once directly after the CODESYS task and 10 ms after the previous local bus cycle.

9.9.5 Local Bus (KBus) Settings



Parameter	Value
⊟ KBus settings	
Update mode	Synchronous
KBus cycle time	10000
KBus thread priority.	0
PLC stop behavior	Set to zero

Figure 95: Local Bus (KBus) Settings

Table 50: Local Bus (KBus) Settings

Parameter	Explanation	
Update mode	The update mode is used to configure how the local bus process data is to be updated (refreshed).	
	Asynchronous	In the asynchronous update mode process data are refreshed in cycles at a definable interval.
	Synchronous*	In the synchronous update mode the process data are synchronized with the most rapid CODESYS task that accesses the local bus.
KBus cycle time	The update interval for the local bus is set by the cycle time. This setting is effective only in the asynchronous mode.	
	1000 µs	Minimum value 1 millisecond
	10000 µs*	Default value 10 milliseconds
	50000 µs	Maximum value 50 milliseconds
KBus thread priority	This value indicates the priority for the local bus thread. This setting is effective only in the asynchronous mode. This priority is equivalent to the priority of the cyclic CODESYS tasks (see section “Cyclic Tasks”).	
	0*	Highest priority
	15	Lowest priority
PLC stop behavior	Specifies the response of the local bus outputs when the PLC application stops.	
	Hold last value	The output states are retained.
	Set to zero*	Outputs are set to zero.

* Default setting

9.9.5.1 Effect of Update Mode on CODESYS Tasks

9.9.5.1.1 Asynchronous Update Mode

In the asynchronous update mode there is no direct influence on CODESYS task behavior.

Note

Local bus “freeze” on priority conflicts!

In the asynchronous update mode there is a risk of the local bus “freezing”, as the local bus thread operates at the same priority as the IEC tasks. The local bus thread must therefore use a priority higher than that of the IEC task to prevent this from occurring.

9.9.5.1.2 Synchronous Update Mode

In the synchronous update mode the runtime behavior of CODESYS tasks can be influenced by the local bus. The minimum task interval that can then be achieved depends on the duration of a local bus cycle. The duration of a local bus cycle, on the other hand, is based on the I/O modules connected to the bus. As a rule of thumb: The shorter the local bus structure, the shorter the cycle time and digital modules are faster than analog or complex ones.

In the event of a local bus error, the CODESYS tasks are blocked until the error is rectified, i.e., when a local bus cycle has been successfully executed again.

Note

No call-up of local bus status when local bus errors are present!

If a local bus error has occurred, it is not possible to call up the bus status using KBUS_ERROR_INFORMATION (mod_com.lib) while in the synchronous update mode.

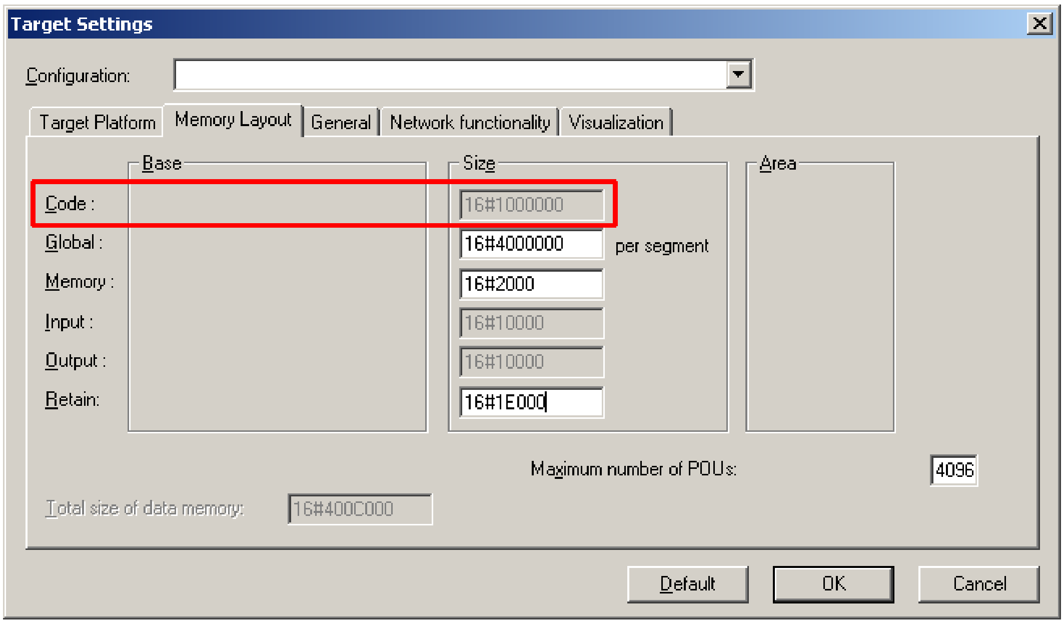
9.10 Memory Settings in CODESYS

The list below illustrates the standard memory allocation of the controller:

•	Program memory:	16 Mbyte (max.)
•	Data memory:	64 Mbytes
•	Input data:	64 kbytes
•	Output data:	64 kbytes
•	Flags:	24 kbytes
•	Retain:	104 kbytes
•	Function block limitation:	12 * 4096 bytes = 48 kbytes

9.10.1 Program Memory

The program memory (also code memory) cannot be configured and is limited to a maximum of 16 Mbytes. The memory space actually available is based on the scope of installed applications.



Code : 16#1000000

Global : 16#4000000 per segment

Memory : 16#2000

Input : 16#10000

Output : 16#10000

Retain: 16#1E000

Maximum number of POUs: 4096

Total size of data memory: 16#400C000

Figure 96: Program Memory (Example)

9.10.2 Data Memory and Function Block Limitation

The data memory is set for 64 Mbytes in the controller's initial state.

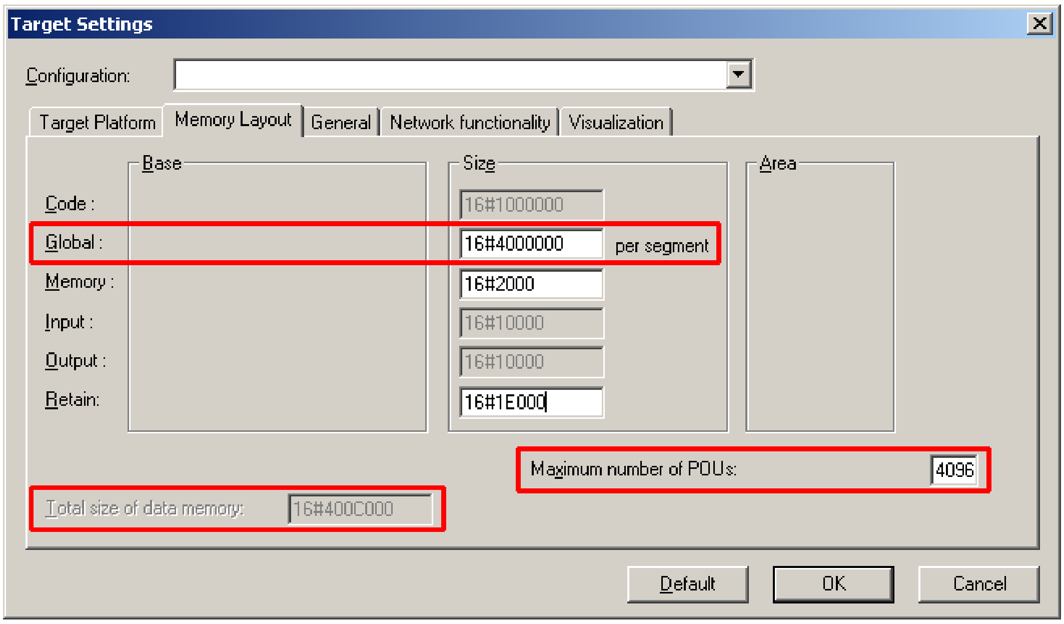
This set value has already been requested in the system after a successful program download and can be fully utilized.

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., normally 4096 * 12).

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

This value should not exceed the value specified for “Size of entire data memory.”



Configuration:

Code : 16#1000000

Global : 16#4000000 per segment

Memory : 16#2000

Input : 16#10000

Output : 16#10000

Retain: 16#1E000

Maximum number of POUs: 4096

Total size of data memory: 16#400C000

Figure 97: Data Memory and Function Block Limitation (Example)

9.10.3 Remanent Memory

A total of 128 kbytes of remanent memory is available for the IEC-61131 application.

The remanent section is subdivided into the flag area (memory) and the retain area.

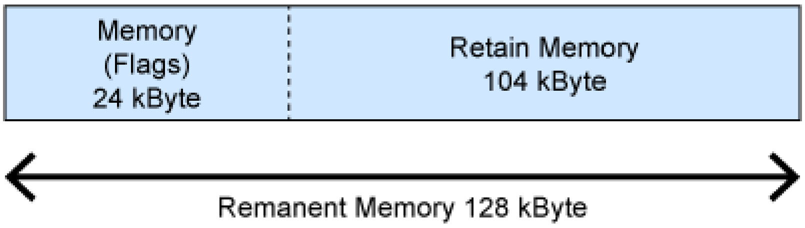
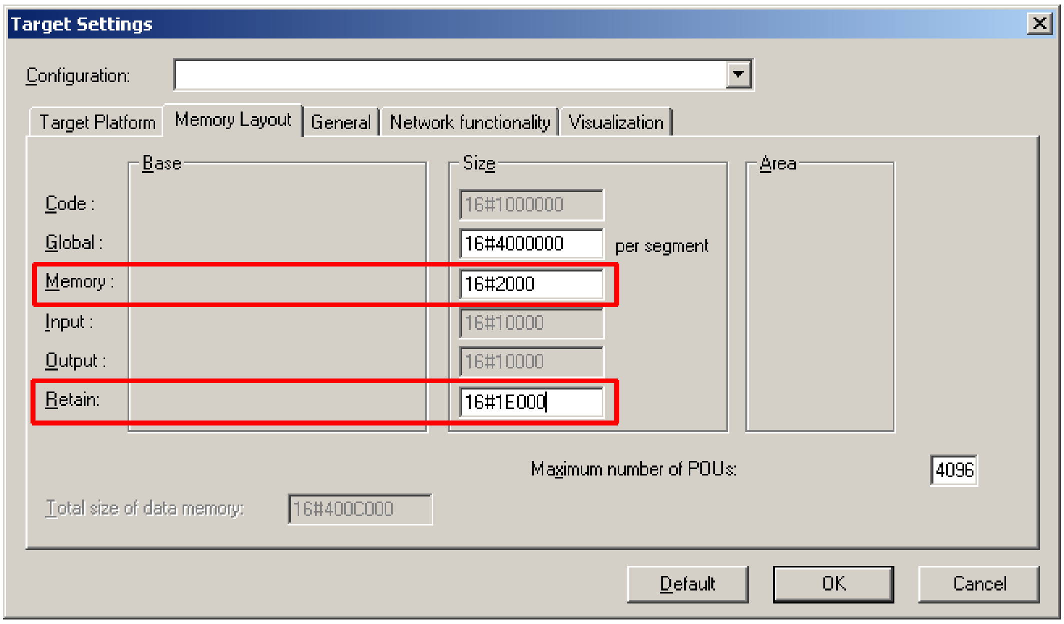


Figure 98: Remanent Main Memory (Example)

The breakdown of the flag and retain variables can be customized as required.

Note

Observe general conditions!
The sum of Memory + Retain must not exceed the maximum value of 128 kbytes (0x20000).
A maximum of 10,000 retain variables can be created.



Configuration:

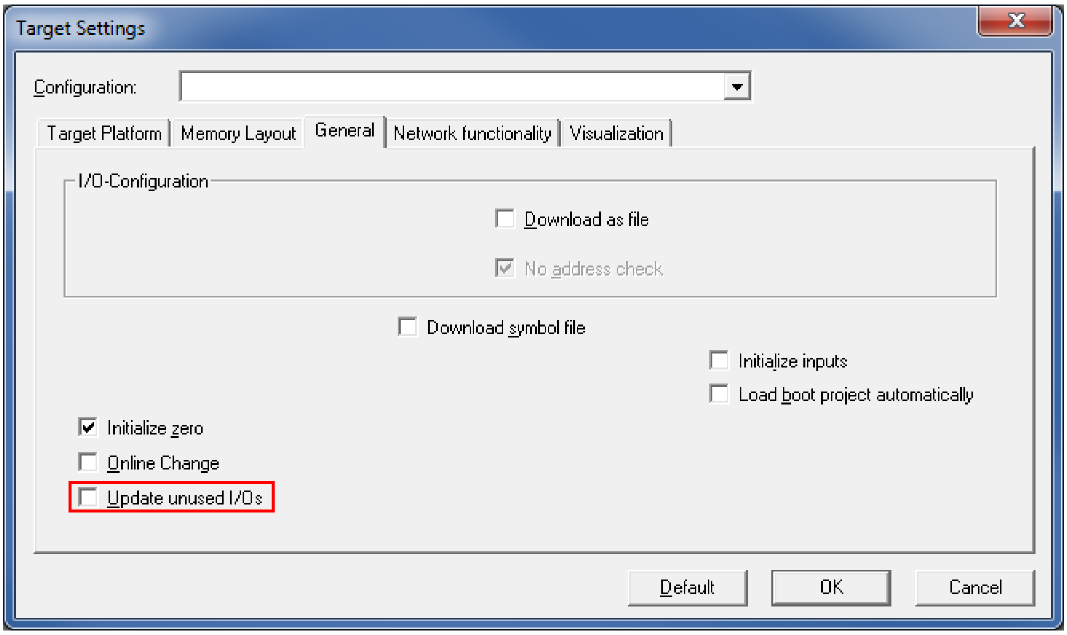
	Size	
Code :	16#1000000	
Global :	16#4000000	per segment
Memory :	16#2000	
Input :	16#10000	
Output :	16#10000	
Retain:	16#1E000	

Maximum number of POUs: 4096

Total size of data memory: 16#400C000

Figure 99: Flag and Retain Memory (Example)

9.11 General Target System Settings



I/O-Configuration

- □ Download as file
- ☑ No address check
- □ Download symbol file
- □ Initialize inputs
- □ Load boot project automatically
- ☑ Initialize zero
- □ Online Change
- □ Update unused I/Os

Figure 100: General Target System Settings

No change to the settings is necessary on the “General” tab.

The “Update unused I/Os” box can be checked for initial startup. Enabling this results in a higher CPU load and possibly a significant effect on task processing.

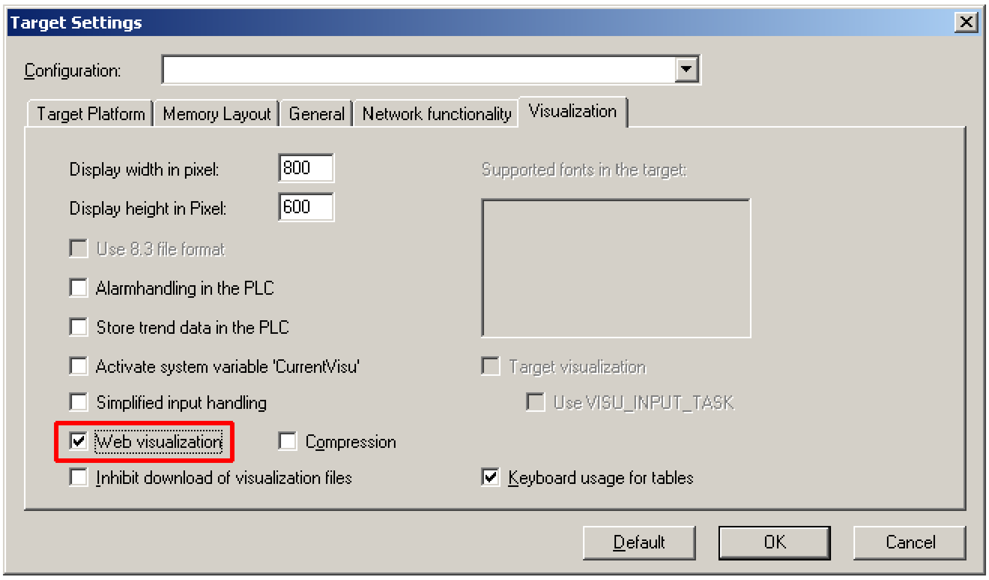
9.12 CODESYS Visualization

CODESYS Web visualization is based on Java technology. All Java programs require a Java runtime environment (JRE), which must be installed on the host PC along with a web browser. An applet is stored in the file system of a Web server and is accessible to web browsers via an HTML page.

You create all visualization types (HMI and Web visualization) with the same CODESYS graphic editor. Select the visualization type in the “Target system settings” window. A description file in XML format is generated from the information for each of these pages. You can find these files in the subfolder *“visu”* of the CODESYS installation path. The HTML home page “webvisu.htm” and the Java archive “webvisu.jar” in the applet (webvisu.class) are also saved there in a compressed format.

Once you have selected a visualization type, the following steps must be performed to execute the technique:

1. Click the “Resources” tab and open the “Target system settings.” Specify whether you wish to have visualization displayed as a “Web visualization” using a web browser.



Target Settings

Configuration:

Display width in pixel: 800

Display height in Pixel: 600

□ Use 8.3 file format

□ Alarmhandling in the PLC

□ Store trend data in the PLC

□ Activate system variable 'CurrentVisu'

□ Simplified input handling

☑ Web visualization

□ Compression

□ Inhibit download of visualization files

Supported fonts in the target:

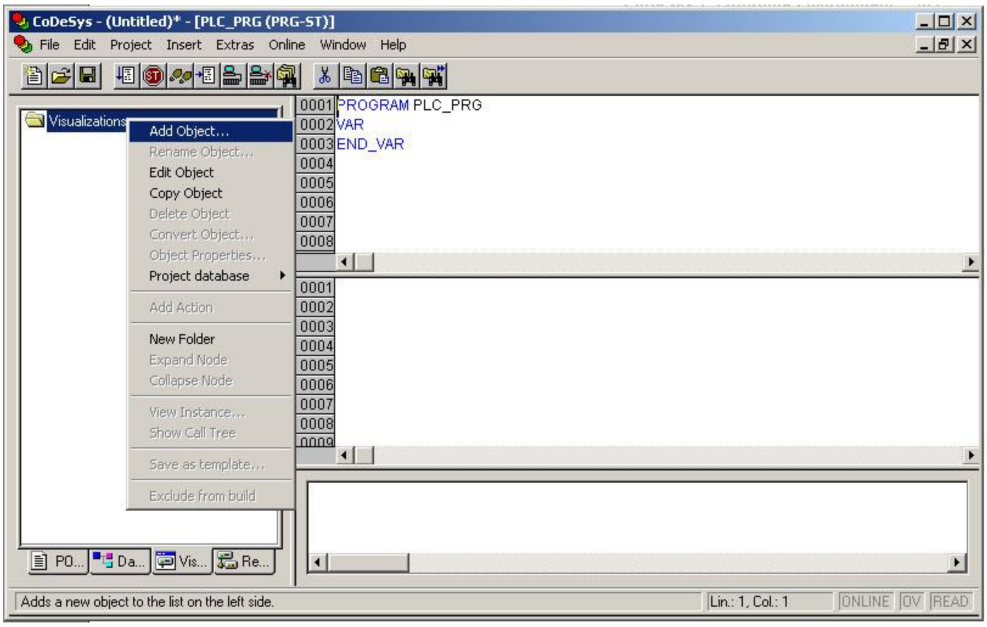
□ Target visualization

□ Use VISU_INPUT_TASK

☑ Keyboard usage for tables

Figure 101: Selecting the Visualization Technique in the Target System Settings

2. Generate a start page for the visualization. Right-click the “Visualization” folder in the “Visualization” tab. Select **Add object** ... from the contextual menu. The “New visualization” dialog box opens.



```
0001 PROGRAM PLC_PRG
0002 VAR
0003 END_VAR
```

Adds a new object to the list on the left side.

Figure 102: Creating the PLC_VISU Starting Visualization

3. In the “New visualization” dialog window, enter the name **PLC_VISU** for the start visualization. This page is then displayed as the start page upon system startup.

4. Activate the CODESYS Web server in the WBM on the “Ports and Services – CODESYS Services” page in the “CODESYS Webserver” group.

5. Activate the http service in the WBM on the “Ports and Services – Network Services” page in the “HTTP” group.

If you transfer the PLC program to the controller (**Online > Login**) and start the program (**Online > Start**), enter one of the following lines in the address line of the web browser for online visualization:

- “https://<IP address of the controller>/webvisu”, preferred method (http can also be used instead of https)
- “https://<IP address of the controller>”, if the default Web server in the WBM has been set to“WebVisu” (http can also be used instead of https)
- “http://<IP address of the controller>:8080/webvisu.htm”

You can also have Web visualization displayed via the WBM (see Section “`CODESYS - WebVisu´” Page).

Information

Frequently Asked Questions
Additional information (FAQs) on CODESYS Web visualization is also provided in the Section “Frequently Asked Questions about CODESYS Web Visualization” and in the online Help function for CODESYS 2.3.

9.12.1 Limits of CODESYS Visualization

The controller supports the “WebVisu” visualization type integrated into CODESYS. Technological limitations can be caused by the visualization type used.

Compared to “HMI”, Web visualization on the controller is performed within significantly narrower physical limits. Whereas “HMI” can access almost unlimited resources on a desktop PC, the following limitations must be observed when using Web visualization:

Adapting to the File System

The overall size of the PLC program, visualization files, bitmaps, log files, configuration files, etc. must fit into the file system.

Process Data Memory

Web visualization uses its own protocol for exchanging process data between applet and control.
The controller transfers process data with ASCII coding. The pipe symbol (“|”) is used to separate two process values. Therefore, the space requirement for a process data variable in the process data memory is dependent not only on the data type, but also on the process value itself. Thus, a variable of the “WORD” type occupies between one byte for the values 0 through 9 and five bytes for values from 10000 and greater. The selected format (ASCII + |) only permits a rough estimate of the space requirement for the individual process data in the process data buffer. If the size of the ASCII coded process data is exceeded, Web visualization no longer works as expected.

Computer Performance/Processor Time

The controller is based on a real-time operating system. This means that high-priority processes (e.g., PLC program) interrupt or block lower priority processes. The Web server responsible for Web visualization is among these lower priority processes.

Note

Processor Time
Make sure when configuring tasks, that there is sufficient processor time available for all processes.

Network Load

The controller's CPU processes both the PLC program and network traffic. ETHERNET communication demands that each received telegram is processed, regardless of whether it is intended for the controller or not.

A significant reduction of the network load can be achieved by using switches instead of hubs.

There is no measure against broadcast telegrams that can be used on the controller, however. These can only be curtailed by the sender, or blocked with configurable switches that have a broadcast limitation. A network monitor such as “wireshark” (www.wireshark.com) provides an overview of the current load in your network.

9.12.2 Eliminating Errors in CODESYS Web Visualization

If you are experiencing problems when working with the CODESYS Web visualization, use the following table to find the solution. If you cannot eliminate the problem, please contact WAGO support.

Table 51: Errors and Remedies

Error	Solution
Internet Explorer reports the error “APPLET NOT INITIATED”	Close all Internet Explorer windows and restart. If the error persists, this indicates a missing or damaged file. Using FTP, check if the entire Java archive “webvisu.jar” is available in the “/PLC” folder of the controller. The original file can be found in the installation path of CODESYS (usually under *C:\Programme\WAGO Software\CODESYS V2.3\Visu\webvisu.jar*). If necessary, replace the damaged file using FTP or force the download of all files in CODESYS with **Purge All** > Compile **All** > **Log in**.
Web visualization is not displayed	Have you installed the JRE? Check the firewall settings, e.g., if port 8080 is open.
Web visualization “freezes”. Web visualization stops after an extended period of time.	The call-up intervals selected in the task configuration are too small. As a result, the Web server of the controller — which is executed with a low priority — does not receive sufficient computer time, if any at all. If no (explicit) task configuration has been provided, the PLC_PRG is (implicitly) executed as a free running task with Priority 1. This significantly limits the Web server’s computing time. Always provide a task configuration when using Web visualization. In doing so, the call-up interval should not exceed three times the average execution time. When determining the execution time, ensure that the PLC program has reached a “steady state.” When determining the execution time, ensure that the PLC program is not “steady state.”
Web visualization cannot be loaded into the controller	Not all files may fit into the controller's file system. Delete any unneeded data (e.g., via FTP).
Bitmap is not displayed	If the name of an image file contains umlauts, the Web server cannot interpret these image names.
Java console reports: “Class not found”	The JRE does not find the entry point for the class “webvisu.class” in the Java archive “WebVisu.jar”. The Java archive is probably incomplete. Delete “WebVisu.jar” from the Java cache and/or deactivate the cache. In this case, the controller requests the archive (applet) again. If the problem persists, reload the project into the controller.
Web visualization is static, all process values are “0”	Process data communication has failed. If Web visualization is operated over a proxy server, then a SOCKS proxy is also necessary for process data exchange in addition to the actual HTTP proxy.

9.12.3 FAQs about CODESYS Web Visualization

How can I optimize the applet for special screen resolutions?

In order to optimize the Web visualization for display on a device with a fixed resolution, proceed as follows:
In the “Target system settings”, enter the pixel width and height in the tab “Visualization”. When the visualization is created, the visible area is highlighted in gray. However, the actual pixel width and height of the Web visualization is defined by the attributes “Height” and “Width” of the HTML APPLET tag in the “webvisu.htm” file. Do not forget to also adapt these parameters to the existing resolution.

Which JRE should I use?

Java2 standard edition Version 1.5.0 (J2SE1.5.0_06) or higher is recommended. This is available free of charge at www.oracle.com.
Microsoft's MSJVM3810 was also tested. For PDAs, there are runtime environments available from other manufacturers (JamaicaVM, CrEme, etc.). Please consider that for the Web visualization, these solutions can behave differently within their scope of services (e.g., stability) than those mentioned above.

Should the Java Cache be used?

This depends on the situation. After a standard installation, the cache is enabled. If the cache is enabled, the JRE uses it to store applets and Java archives. If the Web visualization is called up a second time, it requires considerably less time to start because the applet (approx. 250 kb) does not need to be reloaded via the network, but is already available in the cache. This is especially useful when network connections are slow.

Note:
The Java archives may not be completely transferred into the cache due to network failures. In this case, the cache must be cleared manually or disabled.

Why does the visualization element “TREND” in the Web visualization only work “Online”?

The following settings must be selected for visualization projects: **Resources** tab **> Target system settings**.
Activate “Web visualization” and “Trend data recording within control”. Otherwise, the trend data is stored on the hard drive of the CODESYS development PC. This makes a permanent connection between the controller and the CODESYS gateway necessary. If this connection is interrupted, this may lead to the controller behaving unpredictably.

In the TREND configuration dialog, you can choose between “Online” and “History” operating modes. The controller only supports the “Online” operating mode for visualization projects since it is not possible to configure the maximum size (quota) of the trend files (*.trd). Uncontrolled expansion of trend files can lead to unpredictable controller behavior.

In most cases, the use of the “HISTOGRAM” visualization element is the better choice, as this gives full control over the time and number of measurements and thus the amount of memory required.

What needs to be observed when the visualization element “ALARM TABLE” is used in the Web visualization?

The status of this component is best described as “Add-On”, i.e., an extra that is free of charge and not warrantied.

The following settings must be selected for visualization projects: **Resources** tab **> Target system settings**.
Activate “Web visualization” (checkmark) and “Alarm handling within control”. Otherwise, the alarm data is processed on the CODESYS development PC. This makes a permanent connection between the controller and the CODESYS gateway necessary. If this connection is interrupted, this may lead to the controller behaving unpredictably.

10 *e!RUNTIME* Runtime Environment

10.1 General Notes

Note

Additional Information

Information on the installation and startup of ***e!****COCKPIT* is provided in the corresponding manual.
Information on programming is provided in the CODESYS 3 documentation.

10.2 CODESYS V3 Priorities

A list of priorities implemented for the controller is provided below as supplementary information to the CODESYS 3 documentation.

Table 52: 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

10.3 Memory Spaces under *e!RUNTIME*

The memory spaces in the controller under ***e!****RUNTIME* have the following sizes:

• Program memory:	32 Mbytes
• Data memory:	128 Mbytes
• Input data:	64 kbytes
• Output data:	64 kbytes
• Flags:	24 kbytes
• Retain:	104 kbytes
• Function block limitation:	12 * 4096 bytes = 48 kbytes

10.3.1 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.

10.3.2 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.

10.3.3 Remanent Memory

A total of 128 kbytes of remanent memory is available for the IEC-61131 application.
The remanent section is subdivided into the flag area (memory) and the retain area.

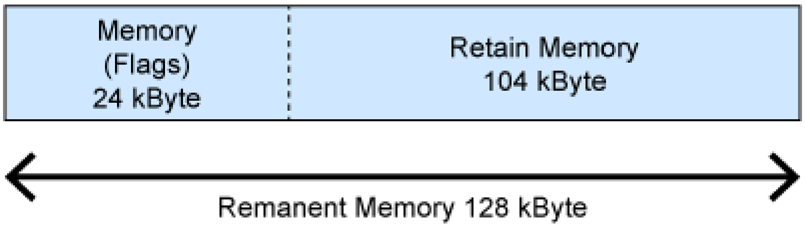


Figure 103: Remanent Main Memory

11 Modbus – CODESYS V2

11.1 General

Modbus is a non-vendor-specific, open fieldbus standard for a wide range of applications in production and process automation. The Modbus communications protocol is based on a master/slave or client/server architecture that uses function codes for execution of individual Modbus services, which have reading or writing access to individual or multiple elements of the Modbus data model simultaneously.

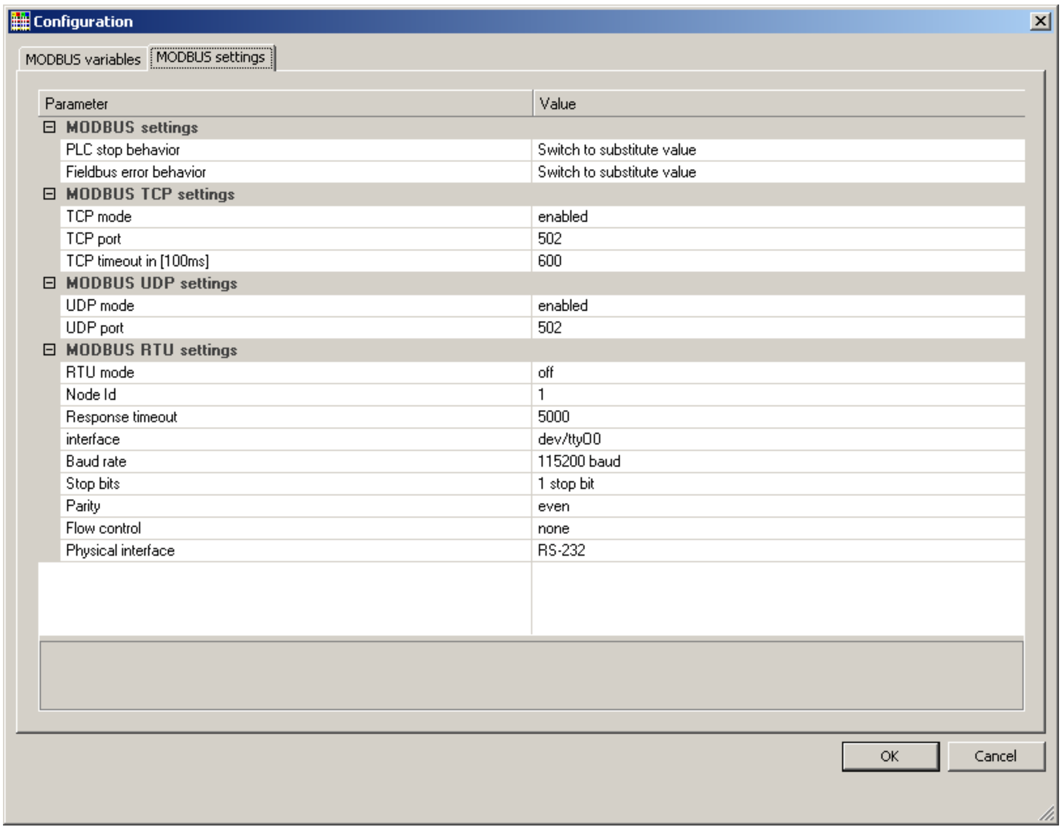
11.2 Features

The Modbus slave implemented in the PFC200 has the following features:

- 3 modes: Modbus TCP, Modbus UDP and Modbus RTU, which can be run independently of one another simultaneously
- Each mode can be configured
- 10 supported Modbus services (Function Codes): FC1 to FC6, FC15, FC16, FC22, FC23
- Data exchange via 1000 registers in each of the local Modbus process images
- 768-byte sector that can be addressed by bits in each local Modbus process image
- Access to a 104 kB flag sector (total of 53248 registers/words, with 3328 addressable bits)
- 28 Information and configuration registers
- Up to 1000 TCP connections
- Modbus communications monitoring using programmable watchdogs
- Configurable response on PLC stop
- Configurable response on disruption of Modbus communication

11.3 Configuration

All of the Modbus operating modes are configured using the CODESYS PLC configuration.



Parameter	Value
⊟ **MODBUS settings**	
PLC stop behavior	Switch to substitute value
Fieldbus error behavior	Switch to substitute value
⊟ **MODBUS TCP settings**	
TCP mode	enabled
TCP port	502
TCP timeout in [100ms]	600
⊟ **MODBUS UDP settings**	
UDP mode	enabled
UDP port	502
⊟ **MODBUS RTU settings**	
RTU mode	off
Node Id	1
Response timeout	5000
interface	dev/ttyO0
Baud rate	115200 baud
Stop bits	1 stop bit
Parity	even
Flow control	none
Physical interface	RS-232

Figure 104: CODESYS PLC Configuration - Modbus Settings

The Modbus slave configuration is composed of four basic parameter groups:

- Modbus settings,
- Modbus TCP settings,
- Modbus UDP settings,
- Modbus RTU settings.

A detailed description of all the parameter groups is given in the following sections.

11.3.1 Modbus Settings

The “Modbus settings” group contains the following configuration parameters.

Table 53: Modbus Settings

Parameters	Explanation	
PLC stop behavior	Response of the Modbus slave when the controller has halted (controller in STOP state)	
	No data exchange	No data exchange possible. Modbus requests will always be answered by the exception response “ILLEGAL FUNCTION” (0x81).
	Switch to substitute value*	Data exchange possible. Substitute values (0) are provided for Modbus read requests and the values accepted unchanged in the local Modbus process image for write requests, without passing these on to the controller.
	Hold last value	Data exchange possible. The last frozen values are provided for Modbus read requests and the values accepted unchanged in the Modbus process image for write requests, without passing these on to the controller.
Fieldbus error response	Response of the Modbus slave to detected fieldbus errors (interruption of communication).	
	No data exchange	No data exchange possible.
	Switch to substitute value*	Data exchange possible. Substitute values (0) are supplied from the Modbus process image for PLC read functions; for write access the values are accepted unchanged in the Modbus process image without passing them on to the Modbus master.
	Hold last value	Data exchange possible. The previously frozen values are supplied from the Modbus process image for PLC read functions; for write access the values are accepted unchanged in the Modbus process image without passing them on to the Modbus master.

* Default setting

11.3.2 Modbus TCP Settings

The “Modbus TCP Settings” contains the following configuration parameters for the “Modbus TCP” mode:

Table 54: Modbus TCP Settings

Parameters	Explanation	
TCP mode	Enable for the Modbus TCP mode	
	Off	Operation not permitted
	Active*	Operation possible
TCP port	Port number for the TCP link	
	1	Minimum port number
	502*	Modbus default port
	65535	Maximum port number
TCP Timeout	Time-out for a TCP link	
	1	100 ms (1 × 100 ms)
	600*	60 seconds (600 × 100ms)
	65535	1 h 49 min 13 s 500 ms (65535 × 100 ms)

* Default setting

11.3.3 Modbus UDP Settings

The “Modbus UDP Settings” group contains the following configuration parameters for the “Modbus UDP” mode:

Table 55: Modbus UDP Settings

Parameters	Explanation	
UDP mode	Enable for the Modbus UDP mode	
	Off	Operation not permitted
	Active*	Operation possible
UDP port	Port number for the UDP link	
	1	Minimum port number
	502*	Modbus default port
	65535	Maximum port number

* Default setting

11.3.4 Modbus RTU Settings

The “Modbus RTU Settings” group contains the following configuration parameters for the “Modbus RTU” mode:

Table 56: Modbus RTU Settings

Parameters	Explanation	
RTU mode	Enable for the Modbus RTU mode	
	Off*	Operation not permitted
	Active	Operation possible
Device ID	Device ID (device address) for the tty device	
	1*	min. device ID
	247	max. device ID
Maximum response time	Response timeout for a request in [ms]	
	2000	min. response time = 2 seconds. If this value is set lower than 2 seconds, it will be corrected internally to 2 seconds.
	5000*	Default = 5 seconds
	4294967295	max. response time > 71 hours.
Interface	Device name	
	“dev/…”	Name of the tty in the string
	“dev/ttyO0”*	Standard tty
Baud rate	Communication baud rate	
	1200 baud	1200 baud min. transmission speed
	2400 baud	2400 baud
	4800 baud	4800 baud
	9600 baud	9600 baud
	19200 baud	19200 baud
	38400 baud	38400 baud
	57600 baud	57600 baud
	115200 baud*	115200 baud, max. transmission speed
Stop bits	Number of stop bits	
	1 stop bit*	1 stop bit in the frame; must be used when even or odd parity has been selected.
	2 stop bits	2 stop bits in the frame; must be used when “None” has been selected for parity.
Parity	Parity check	
	None	No parity check performed; 2 stop bits must be selected in the configuration for this setting.
	Even*	Even parity
	Odd	Odd parity

Table 56: Modbus RTU Settings

Parameters	Explanation	
Flow control	Data flow control (Supported only for the setting “RS-232” for the physical interface.)	
	None*	No data flow control
	RTS/CTS	Hardware flow control
Physical interface	Mode for the physical interface	
	RS-232*	RS-232 is used as the physical interface.
	RS-485	RS-485 is used as the physical interface.

* Default setting

11.4 Data Exchange

Modbus data exchange is performed in cycles or acyclically using Modbus services. The type and number of usable Modbus services depends on the area that is addressed. There are generally four Modbus-relevant address areas in the PFC200:

- **Modbus input process image** (Modbus Input) – is an area in the PIO (PIO = Output Process Image), in which data from the PLC is provided in cycles exclusively for Modbus Read services.
- **Modbus output process image** (Modbus Output) – is an area in the PII (PII = Input Process Image), in which Modbus Write services provide data for cyclic reading by the PLC. Modbus Read services are also acceptable in this area.
- **Modbus flag area** – is an area, in which both Modbus Read and Write services can be executed.
- **Modbus register** – is an area, in which the WAGO specific information and configuration registers are contained. Only Modbus register services may be executed in this area.

11.4.1 Process Image

The main data interfaces between the PLC and the Modbus slave are the local Modbus process images in the PLC address area based on IEC 61131. The Modbus input process image (Modbus Input) is in the PIO and the Modbus output process image (Modbus Output) in the PII. Data memory blocks of 2 kB (1000 registers/word) are available for each local Modbus input and output process image. The first 768 bytes of each of these data blocks are also provided for executing bit services.

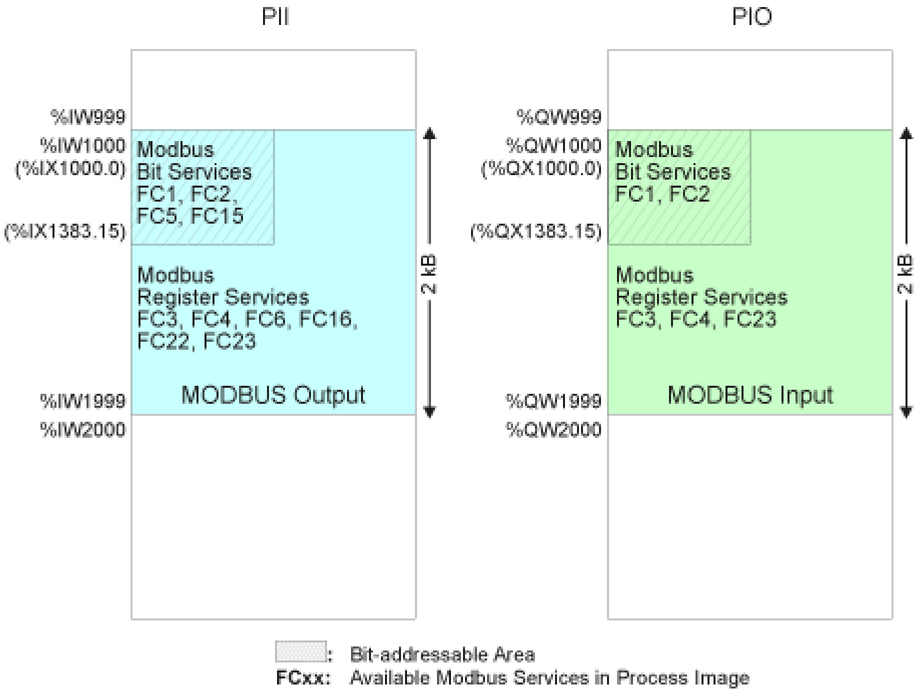


Figure 105: Modbus Process Image

As no direct access to the I/O modules is provided by the fieldbus, data can be exchanged via this interface between the PLC and Modbus for processing in the control system (PLC). Using this data in the individual I/O modules connected to the PLC can then be performed by the application.

11.4.2 Flag Area

Modbus can also exchange data and fieldbus variables with the PLC via the flag area. Caution is urged, however, when using data and/or variables in this area that is accessed by both Modbus and the PLC. This “conflicting” access is not protected from either side and could result in data inconsistency.

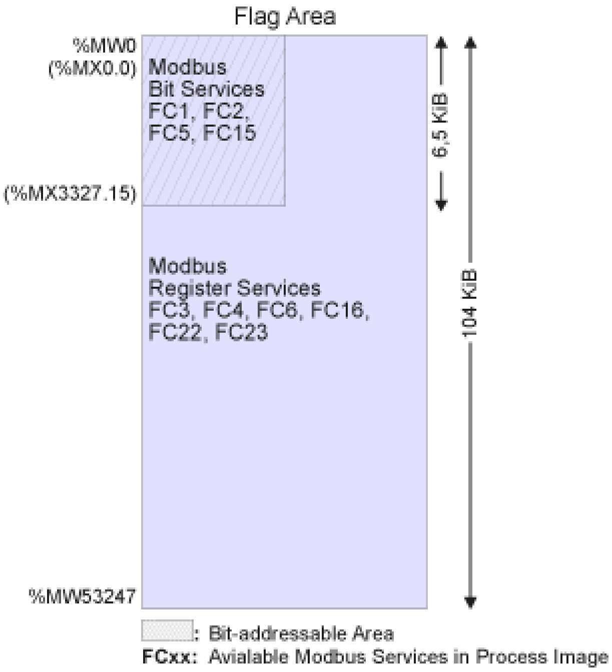


Figure 106: Flag Area

The figure shows the maximum addressable flag area with a size of 104 kB.
The actual addressable flag area depends on the current memory arrangement in the target system settings in CODESYS.
The default setting is 24 kB.

11.4.3 Modbus Registers

WAGO specific registers are implemented in the last Modbus-relevant address area; this simplifies the reading of certain system and Modbus information, as well as configuration.

The Modbus address area reserved for these registers ranging from the Modbus starting address of 4096 (0x1000) up to the Modbus end address of 12287 (0x2FFF), without any allocation to the IEC 61131 address area. These registers can be queried using the register read services FC3, FC4 and FC23 and with the register write services FC6, FC16 and FC23. A detailed description of the individual registers is given in the section “WAGO Modbus Registers”.

11.4.4 Modbus Mapping

11.4.4.1 Modbus Mapping for Write Bit Services FC1, FC2

The table below outlines the mapping for the Modbus-reading, bit-oriented services:

- FC1 – Read Single Coil,
- FC2 – Read Discrete Inputs.

Table 57: Modbus Mapping for Read Bit Services FC1, FC2

Modbus Address (hexadecimal values in parentheses)	IEC 61131 Address	Description
0 … 6143 (0x0000 … 0x17FF)	%IX1000.0 … %IX1383.15	Modbus Output: 6144 PFC input bit variables in the first 384 registers/words (768 bytes) of the 2kB Modbus output process image in the PII. Note: In this area, the read bit services return the content from the bit-addressed PII.
6144 … 12287 (0x1800 … 0x2FFF)	%QX1000.0 … %QX1383.15	Modbus Input: 6144 PFC output bit variables in the first 384 registers/words (768 bytes) of the 2 kB Modbus-input process image in the PIO.
12288 … 65535 (0x3000 … 0xFFFF)	%MX0.0 … %MX3327.15	Maximum bit-addressable flag area: 53248 bit flags (6.5 kB); the actual addressable flag area depends on the current memory arrangement in CODESYS.

11.4.4.2 Modbus Mapping for Write Bit Services FC5, FC15

The table below outlines the mapping for the Modbus-writing, bit-oriented services:

- FC5 – Write Single Coil
- FC15 – Write Multiple Coils

Table 58: Modbus Mapping for Write Bit Services FC5, FC15

Modbus Address (hexadecimal values in parentheses)	IEC 61131 Address	Description
0 … 6143 (0x0000 … 0x17FF)	%IX1000.0 … %IX1383.15	Modbus Output: 6144 PFC input bit variables in the first 384 registers/words (768 bytes) of the 2kB Modbus output process image in the PII.
6144 … 12287 (0x1800 … 0x2FFF)	~~%QX1000.0 …~~ ~~%QX1383.15~~	Modbus Output: Modbus-only area for bit-oriented write access. Bit-based write services for this area are acknowledged by the Modbus slave with the Modbus exception code “ILLEGAL DATA ADDRESS” (0x02).
12288 … 65535 (0x3000 … 0xFFFF)	%MX0.0 … %MX3327.15	Maximum bit-addressable flag area: 53248 bit flags (6.5 kB); the actual addressable flag area depends on the current memory arrangement in CODESYS.

11.4.4.3 Modbus Mapping for Read Register Services FC3, FC4, FC23

The table below outlines the mapping for the Modbus-reading, register-oriented services:

- FC3 – Read Holding Registers,
- FC4 – Read Input Registers,
- FC23 – Read/Write Multiple Registers

Table 59: Modbus Mapping for Read Register Services FC3, FC4, FC23

Modbus Address (hexadecimal values in parentheses)	IEC 61131 Address	Description
0 … 999 (0x0000 … 0x03E7)	%IW1000 … %IW1999	Modbus Output: 1000 PFC input registers/words in the 2 kB Modbus output process image in the PII. Note: In this area, the read register services return the content from the PII.
1000 … 1999 (0x03E8 … 0x07CF)	%QW1000 … %QW1999	Modbus Input: 1000 PFC output registers/words in the 2 kB Modbus input process image in the PIO. Note on FC23: Only the Read portion of this service can be executed.
2000 … 4095 (0x07D0 … 0x0FFF)		Inhibited to Modbus-only area for register-oriented read access. Register-based read services for this area are acknowledged by the Modbus slave with the Modbus exception code “ILLEGAL DATA ADDRESS” (0x02).
4096 … 12287 (0x1000 … 0x2FFF)	No IEC 61131 address	Information and configuration registers: Not all Modbus addresses in this range are valid. Valid Modbus addresses are described in the Section “WAGO Modbus Registers”. Access to invalid addresses are acknowledged by the Modbus slave with the Modbus exception code “ILLEGAL DATA ADDRESS” (0x02). Note on FC23: The Write portion of this service can only be executed for registers that data can be written to.

Table 59: Modbus Mapping for Read Register Services FC3, FC4, FC23

Modbus Address (hexadecimal values in parentheses)	**IEC 61131 Address**	**Description**
12288 … 65535 (0x3000 … 0xFFFF)	%MW0 … %MW53247	Maximum addressable flag area: 53248 register/word flags (104 kB); the actual addressable flag area depends on the current memory arrangement in CODESYS.

11.4.4.4 Modbus Mapping for Write Register Services FC6, FC16, FC22, FC23

The table below outlines the mapping for Modbus-writing, register-oriented services.

- FC6 – Write Single Register,
- FC16 – Write Multiple Registers,
- FC22 – Mask Write Register, not for information and configuration registers
- FC23 – Read/Write Multiple Registers.

Table 60: Modbus Mapping for Write Register Services FC6, FC16, FC22, FC23

Modbus Address (hexadecimal values in parentheses)	IEC 61131 Address	Description
0 … 999 (0x0000 … 0x03E7)	%IW1000 … %IW1999	Modbus Output: 1000 PFC input registers/words in the 2 kB Modbus output process image in the PII.
1000 … 1999 (0x03E8 … 0x07CF)	No access to: %QW1000 … %QW1999	Modbus Output: Inhibited Modbus area for register-oriented write access. Register-oriented write services in this area are acknowledged by the Modbus slave with the Modbus exception code “ILLEGAL DATA ADDRESS” (0x02).
2000 … 4095 (0x07D0 … 0x0FFF)		Inhibited Modbus area for register-oriented write access. Register-oriented write services in this area are acknowledged by the Modbus slave with the Modbus exception code “ILLEGAL DATA ADDRESS” (0x02).
4096 … 12287 (0x1000 … 0x2FFF) FC6, FC16, FC23 only, not FC22	No IEC 61131 address	Information and Configuration Registers: Not all Modbus addresses in this area are valid and not all registers can be written to. Valid Modbus addresses are described in the Section “WAGO Modbus Registers”. Access to invalid addresses are acknowledged by the Modbus slave with the Modbus exception code “ILLEGAL DATA ADDRESS” (0x02).

Table 60: Modbus Mapping for Write Register Services FC6, FC16, FC22, FC23

Modbus Address (hexadecimal values in parentheses)	IEC 61131 Address	Description
12288 … 65535 (0x3000 … 0xFFFF)	%MW0 … %MW53247	Maximum addressable flag area: 53248 register/word flags (104 kB); the actual addressable flag area depends on the current memory arrangement in CODESYS.

11.5 WAGO Modbus Registers

System and Modbus data can be read and some Modbus parameters configured using the WAGO Modbus registers. The following table lists all of the WAGO Modbus registers.

Table 61: WAGO Modbus Registers

Modbus Address		Data Length in Words	Access	Description
Dec.	Hex.			
4130	0x1022	1	ro	Number of registers in the Modbus input process image in the PAA
4131	0x1023	1	ro	Number of registers in the Modbus output process image in the PAE
4132	0x1024	1	ro	Number of bits in the Modbus input process image in the PAA
4133	0x1025	1	ro	Number of bits in the Modbus output process image in the PAE
4136	0x1028	1	ro	IP configuration: BootP(1), DHCP(2) or permanently coded IP address(4)
4138	0x102A	1	ro	Number of established TCP connections
4144	0x1030	1	r/w	Modbus TCP Timeout (Changes apply only to new connections)
4145	0x1031	3	ro	MAC ID of the ETHERNET interface (eth0)
4151	0x1037	1	r/w	Modbus TCP response delay
4160	0x1040	1	ro	PLC status
4352	0x1100	1	wo	Watchdog command
4353	0x1101	1	ro	Watchdog status
4354	0x1102	1	rw	Watchdog timeout (configuration register)
4355	0x1103	1	rw	Watchdog config (configuration register)
4356	0x1104	1	rw	Watchdog operation mode (configuration register)
8192	0x2000	1	ro	0x0000 (constant)
8193	0x2001	1	ro	0xFFFF (constant)
8194	0x2002	1	ro	0x1234 (constant)
8195	0x2003	1	ro	0xAAAA (constant)
8196	0x2004	1	ro	0x5555 (constant)

Table 61: WAGO Modbus Registers

Modbus Address		Data Length in Words	Access	Description
Dec.	Hex.			
8197	0x2005	1	ro	0x7FFF (constant)
8198	0x2006	1	ro	0x8000 (constant)
8199	0x2007	1	ro	0x3FFF (constant)
8200	0x2008	1	ro	0x4000 (constant)
8208	0x2010	1	ro	Revision (firmware index)
8209	0x2011	1	ro	Series code
8210	0x2012	1	ro	Device code
8211	0x2013	1	ro	Major firmware version
8212	0x2014	1	ro	Minor firmware version
8213	0x2015	1	ro	MBS version

The WAGO Modbus registers are described in more details in the following sections.

11.5.1 Process Image Properties

11.5.1.1 Register 0x1022 – Number of Registers in the Modbus Input Process Image

This register contains the number of registers available in the Modbus input process image (Modbus input).

11.5.1.2 Register 0x1023 – Number of Registers in the Modbus Output Process Image

This register contains the number of registers available in the Modbus output process image (Modbus output).

11.5.1.3 Register 0x1024 – Number of Bits in the Modbus Input Process Image

This register contains the number of bits available in the Modbus input process image (Modbus input).

11.5.1.4 Register 0x1025 – Number of Bits in the Modbus Output Process Image

This register contains the number of bits available in the Modbus output process image (Modbus output).

11.5.2 Network Configuration

11.5.2.1 Register 0x1028 – IP Configuration

This register contains information about the set IP configuration.
Possible values:

1 = BootP
2 = DHCP
4 = Fixed IP address

11.5.2.2 Register 0x102A – Number of Established TCP Connections

This register supplies the number of established TCP connections.
The maximum number of Modbus TCP connections is 1000.

11.5.2.3 Register 0x1030 – Modbus TCP Socket Timeout

This register contains the timeout value for the TCP sockets.
This value is given in units of 100ms (ticks). A new value is accepted only for new connections which have not yet been established. In the event of any changes, the already established connections will continue to operate using the previously set timeout value.

11.5.2.4 Register 0x1031 – MAC Address for ETHERNET-Interface 1 (eth0)

This register provides the MAC address for the first ETHERNET interface (eth0).
MAC may also provide a partial result.

11.5.2.5 Register 0x1037 - Modbus TCP Response Delay

This register saves the value of the Modbus response delay.
This value is specified in ms units. The maximum delay is 32 ms, default value is 0 ms (no delay).
Transmission of the response to a Modbus request is delayed from the time of processing (read and/or write register values) by the time set. In the meantime, incoming requests can only be processed when the previous response is sent. For Modbus UDP, this applies to all requests and for Modbus TCP, for each connection. The actual length of time between a Modbus request and the associated response depends on the number of parallel requests overall system utilization; it is always greater than the response delay set. Changes to the response delay become effective immediately for each subsequent request.

11.5.3 PLC Status Register

Register 0x1040 provides the status (state) that the controller is currently in. Possible values:

1 = PLC running − PLC status is RUNNING.
2 = PLC stopped − PLC status is STOPPED.

11.5.4 Modbus Watchdog

The Modbus watchdog monitors in the Modbus slave the ongoing Modbus communication with the Modbus master. All valid Modbus requests of a Modbus master from all the services supported by the Modbus slave are trigger events (see chapter “Modbus Mapping”). This does not apply to the Explicit Trigger mode and the access to the register 0x1101 (Watchdog Status), which can be configured via the 0x1103 (Watchdog Config) register.

If no trigger occurs during the watchdog within the timeout time set in the 0x1102 register (Watchdog Timeout), the “Watchdog Timeout” response is initiated. The closing of all Modbus TCP connections can be configured as a response, see register 0x1103 (Watchdog Config).

The Modbus watchdog supports two different functions STANDARD_WATCHDOG and ALTERNATIVE_WATCHDOG. The operation mode can be selected via the register 0x1104 (Watchdog Operation Mode).

The following diagrams show the possible states of the Modbus watchdog and status transitions for the particular operation mode.

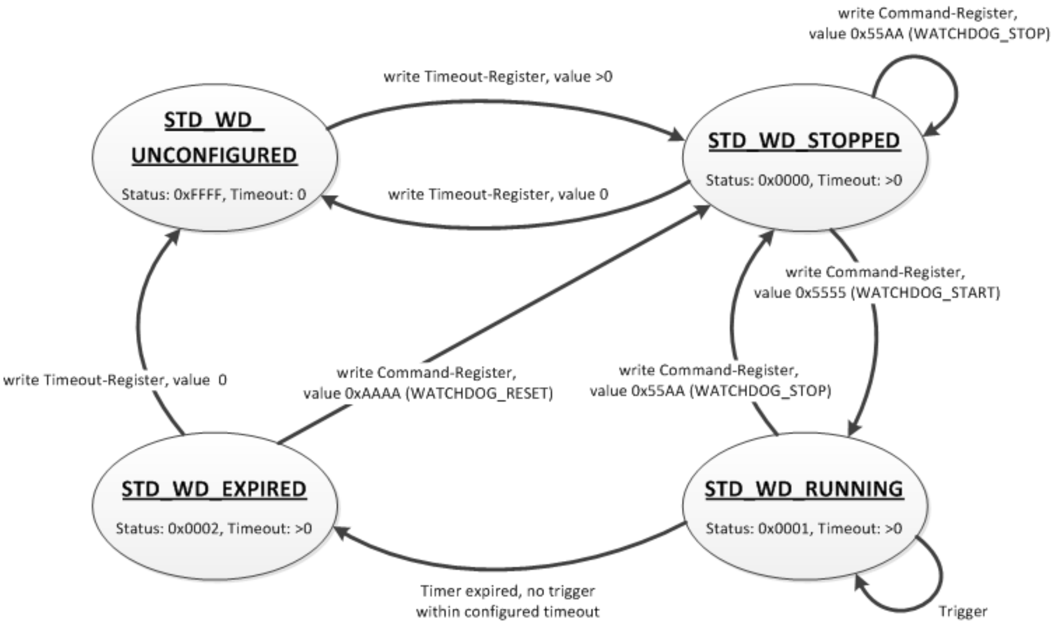

write Command-Register,
value 0x55AA (WATCHDOG_STOP)
write Timeout-Register, value >0
STD_WD_
UNCONFIGURED
Status: 0xFFFF, Timeout: 0
write Timeout-Register, value 0
STD_WD_STOPPED
Status: 0x0000, Timeout: >0
write Command-Register,
value 0x5555 (WATCHDOG_START)
write Timeout-Register, value 0
write Command-Register,
value 0xAAAA (WATCHDOG_RESET)
write Command-Register,
value 0x55AA (WATCHDOG_STOP)
STD_WD_EXPIRED
Status: 0x0002, Timeout: >0
STD_WD_RUNNING
Status: 0x0001, Timeout: >0
Timer expired, no trigger
within configured timeout
Trigger

Figure 107: State Diagram, STANDARD_WATCHDOG Operation Mode

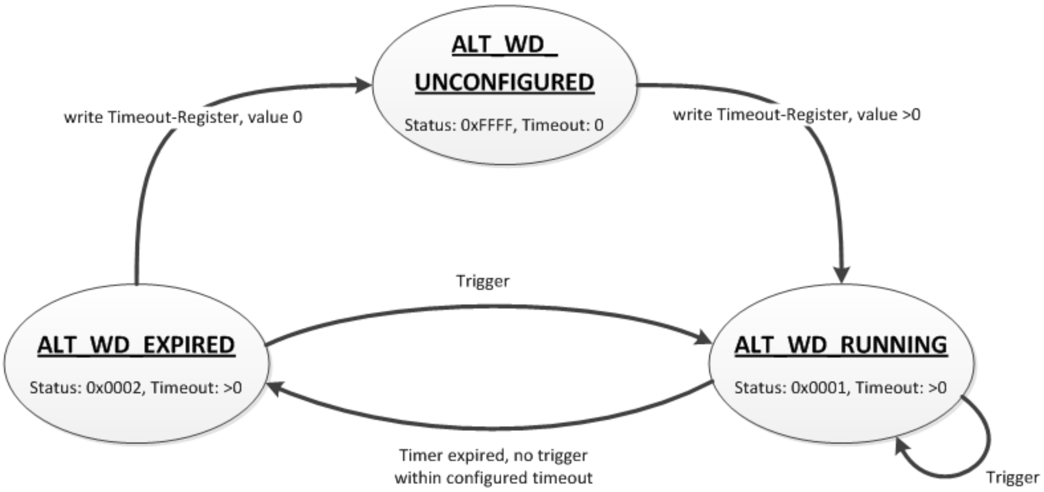

ALT_WD_
UNCONFIGURED
Status: 0xFFFF, Timeout: 0
write Timeout-Register, value 0
write Timeout-Register, value >0
Trigger
ALT_WD_EXPIRED
Status: 0x0002, Timeout: >0
ALT_WD_RUNNING
Status: 0x0001, Timeout: >0
Timer expired, no trigger
within configured timeout
Trigger

Figure 108: State Diagram, ALTERNATIVE_WATCHDOG Operation Mode

The state diagram for the ALTERNATIVE_WATCHDOG operation mode shows that the watchdog is always active as soon as a timeout time > 0 is set in the register 0x1102 (Watchdog Timeout). The writing of commands in the register 0x1100 (Watchdog Command) is limited in this operation mode. Only the WATCHDOG_START command is permitted as a possible trigger. The only possibilities to deactivate or stop the watchdog in ALTERNATIVE_WATCHDOG mode are the setting of the timeout register to 0 after the timeout has elapsed and the switching back to the STANDARD_WATCHDOG operation mode.

The following diagram shows the possible state transitions when operation modes are switched.

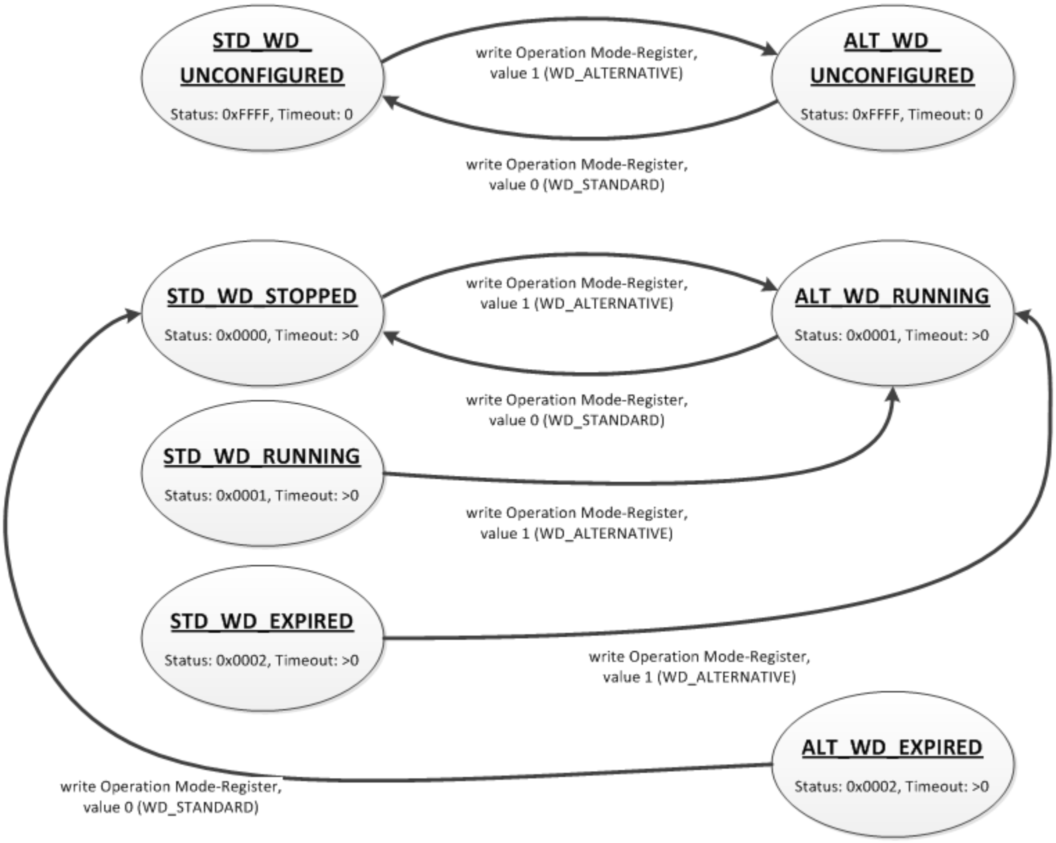

STD_WD_UNCONFIGURED
Status: 0xFFFF, Timeout: 0
write Operation Mode-Register, value 1 (WD_ALTERNATIVE)
ALT_WD_UNCONFIGURED
Status: 0xFFFF, Timeout: 0
write Operation Mode-Register, value 0 (WD_STANDARD)
STD_WD_STOPPED
Status: 0x0000, Timeout: >0
write Operation Mode-Register, value 1 (WD_ALTERNATIVE)
ALT_WD_RUNNING
Status: 0x0001, Timeout: >0
write Operation Mode-Register, value 0 (WD_STANDARD)
STD_WD_RUNNING
Status: 0x0001, Timeout: >0
write Operation Mode-Register, value 1 (WD_ALTERNATIVE)
STD_WD_EXPIRED
Status: 0x0002, Timeout: >0
write Operation Mode-Register, value 1 (WD_ALTERNATIVE)
ALT_WD_EXPIRED
Status: 0x0002, Timeout: >0
write Operation Mode-Register, value 0 (WD_STANDARD)

Figure 109: State Diagram, Switchover Operation Mode

11.5.4.1 Register 0x1100 – Watchdog Command

This register receives commands for the Modbus watchdog. It cannot be read, i.e. it is not possible to read out the last command written.
The following commands are accepted depending on watchdog status:

Table 62: Watchdog Commands

Value	Name	Explanation
0x5555	WATCHDOG_ START	Starts the configured watchdog; in the WATCHDOG_UNCONFIGURED state if no timeout is configured, the response is an ILLEGAL_DATA_VALUE (0x03) exception. In the WATCHDOG_EXPIRED state and the STANDARD_WATCHDOG operation mode the response is an ILLEGAL_FUNCTION (0x01) exception. The watchdog must in this case be reset first with the command WATCHDOG_RESET to the WATCHDOG_STOPPED state. In all other cases the watchdog is restarted and the WATCHDOG_RUNNING state is set.
0x55AA	WATCHDOG_ STOP	Stops the running watchdog; in the WATCHDOG_UNCONFIGURED state, the response is an ILLEGAL_DATA_ VALUE (0x03) exception if no timeout time is set. In the WATCHDOG_EXPIRED state and the STANDARD_WATCHDOG operation mode the response is an ILLEGAL_FUNCTION (0x01) exception. In this case the watchdog must first be reset with the WATCHDOG_ RESET command to the WATCHDOG_ STOPPED state. In operation mode ALTERNATIVE_WATCHDOG the response is an ILLEGAL_DATA_ VALUE (0x03) exception. The command is not generally permitted in this operation mode. In all other cases, the watchdog is stopped successfully and the WATCHDOG_ STOPPED state is set. In the WATCHDOG_STOPPED state, a stop command received several times in a row does not have any impact on the behavior of the watchdog and is therefore not acknowledged with an error response.
0xAAAA	WATCHDOG_ RESET	Resets the expired watchdog; the watchdog is reset in the WATCHDOG_EXPIRED state and STANDARD_WATCHDOG operation mode. The watchdog is then in the WATCHDOG_STOPPED state. In all other cases the response is an ILLEGAL_ DATA_VALUE (0x03) exception.

11.5.4.2 Register 0x1101 – Watchdog Status

This register provides the current state of the Modbus watchdog.
The following states are possible:

Table 63: Watchdog Status

Value	Name	Explanation
0xFFFF	WATCHDOG_ UNCONFIGURED	The Modbus watchdog is not configured, the “Watchdog Timeout” register (0x1102) contains the value 0. This state can only be closed by setting a timeout > 0.
0x0000	WATCHDOG_ STOPPED	The watchdog is configured, the “Watchdog Timeout” register (0x1102) contains a value >0. In the STANDARD_WATCHDOG operation mode the watchdog can be activated in this state by the WATCHDOG_START command. This state cannot be reached in the ALTERNATIVE_WATCHDOG operation mode since the watchdog is started automatically here.
0x0001	WATCHDOG_ RUNNING	The Modbus watchdog is active, i.e. configured and started. The set timeout has not yet expired.
0x0002	WATCHDOG_ EXPIRED	The timeout set in register 0x1102 (Watchdog Timeout) has expired. In the STANDARD_WATCHDOG operation mode, the watchdog in this state must be reset to the WATCHDOG_STOPPED state with the WATCHDOG_RESET command. In the ALTERNATIVE_WATCHDOG operation mode, the watchdog is automatically restarted with the next trigger.

11.5.4.3 Register 0x1102 – Watchdog Timeout

This register contains the value for the watchdog timeout. The step width is 100 ms and the maximum value is 65535 (corresponds to 6553.5 s). The default value is 0. In this case the watchdog cannot be started and will have the WATCHDOG_UNCONFIGURED state.

The register can be read and written in the states WATCHDOG_UNCONFIGURED, WATCHDOG_STOPPED and WATCHDOG_EXPIRED. However, if the watchdog is active (WATCHDOG_RUNNING state), this register can only be read. The response to a write operation is an ILLEGAL_FUNCTION (0x01) exception.

11.5.4.4 Register 0x1103 – Watchdog Config

This register contains the configuration parameters for the watchdog. The register is organized in bits, see following table.

The register can be read and written in the states WATCHDOG_UNCONFIGURED, WATCHDOG_STOPPED and WATCHDOG_EXPIRED. However, if the watchdog is active (WATCHDOG_RUNNING state), this register can only be read. The response to a write operation is an ILLEGAL_FUNCTION (0x01) exception.

Table 64: Watchdog Configuration

Bit	Name/Bit Identifier	Explanation	
0	EXPLICIT_TRIGGER_ONLY	Activates the Explicit Trigger mode	
		0*	All valid Modbus requests are considered as watchdog triggers. The only exception is the access to the register 0x1101 (Watchdog Status).
		1	Only the writing of register 0x1100 (Watchdog Command) with the value 0x5555 (WATCHDOG_START) is considered as a watchdog trigger. The access to the register 0x1101 (Watchdog Status) is also an exception here.
1	TRIGGER_ON_STATUS_REG	Activates the watchdog trigger by (read) access to register 0x1101 (Watchdog Status)	
		0*	The reading of the watchdog status is not considered as a watchdog trigger.
		1	The reading of the watchdog status triggers the watchdog.
2	CLOSE_ALL_TCP_CONNECTIONS	Activates the closing of all Modbus TCP connections with the expiry of the timeout (transition to WATCHDOG_EXPIRED state)	
		0	Existing Modbus TCP connections remain open.
		1*	All existing Modbus TCP connections are closed.
* Default setting			

The individual options are activated when the specific bit, or bit combination, is set.

11.5.4.5 Register 0x1104 – Watchdog Operation Mode

This register contains the value for the watchdog operation mode.

The register can be both read and written irrespective of the watchdog status. The following operation modes are possible:

Table 65: Watchdog Operation Modes

Value	Name	Explanation
0x0000	STANDARD_ WATCHDOG	“Standard Watchdog” operation mode; the watchdog must be controlled explicitly via commands (see register 0x1100 Watchdog Command).
0x0001	ALTERNATIVE_ WATCHDOG	“Alternative Watchdog” operation mode; the watchdog is activated immediately with a timeout > 0 s in register 0x1102 (Watchdog Timeout). Each trigger restarts both the running as well as the expired watchdog. In this operation mode the registers 0x1102 (Watchdog Timeout) and 0x1103 (Watchdog Config) are also saved retentively with the operation mode itself. After a device restart, the “Alternative Watchdog” operation mode is retained with the same configuration as before and is therefore immediately active again when the timeout is set.

11.5.5 Modbus Constants Registers

Registers 0x2000 … 0x2008 provide constants based on the table “WAGO Modbus Registers”. It is possible to read all of the constants, or a consecutive portion of them at once.

11.5.5.1 Electronic Nameplate

Registers 0x2010 to 0x2015 contain information from the electronic nameplate. It is possible to read the entire nameplate or a consecutive portion of it all at once.

11.5.5.2 Register 0x2010 – Revision (Firmware Index)

This register provides the consecutive revision index (firmware index) for the controller.

Example: 5 for Version 5.

11.5.5.3 Register 0x2011 – Series Designator

This register provides the designation (ID) for the WAGO series (Series Code) for the controller.

Example: 750 for WAGO I/O SYSTEM 750.

11.5.5.4 Register 0x2012 – Device ID

This register provides the device ID (WAGO Item No.) of the controller.

Example: 8206.

11.5.5.5 Register 0x2013 – Major Firmware Version

This register provides the major part for the firmware version.

11.5.5.6 Register 0x2014 – Minor Firmware Version

This register provides the minor part for the firmware version.

11.5.5.7 Register 0x2015 – MBS Version

This register provides the version of the Modbus slave library. The high byte contains the major version number and the low byte, the minor version number.

Example:
0x010A => Major version number = 1, Minor version number = 10.

11.6 Diagnostics

11.6.1 Diagnostics for the Modbus Master

The status of the PLC, or of the control system, can be queried by the Modbus master by reading the WAGO specific register 0x1040 – “PLC Status” using Modbus services FC3 (Read Holding Registers) or FC4 (Read Input Registers). The WAGO specific register 0x1040 – “PLC Status” is explained in the Section “PLC Status Registers”.

The status of the Modbus Watchdog can be requested using a register service (FC3 or FC4) with a query to the WAGO specific register 0x1101 – “Watchdog Status Register”. Information about this is given in the Section “Modbus Watchdog”.

The Modbus service “Get Communication Event Counter” (FC11) is not supported in the current Modbus slave Version V1.0.

11.6.2 Diagnostics for the Runtime System

Diagnostics for the Modbus slaves can be executed by integrating the CODESYS library “BusDiag.lib” via the runtime system. The required function block, “DiagGetBusState() indicates the status of the fieldbus (here Modbus) and is located in this library. Details about this function block are provided both in this document and in the online Help function for CODESYS.

11.6.3 Diagnostics for the Error Server

The Modbus slave also supports the error service implemented in the PFC and generates diagnostic messages, which are stored permanently (in a file), or temporarily (in the RAM) and can be displayed directly via the WBM client. The following diagnoses are generated by the Modbus slave:

Table 66: Diagnostics for the Error Server

Diagnostics ID	Diagnostic text	Method of saving	Explanation
0x00090000	Modbus Slave library loaded	Temporary	Modbus slave library has been successfully loaded.
0x00090001	Modbus Slave library closed	Temporary	Modbus slave library has been successfully unloaded.
0x00090002	Modbus Slave TCP started	Temporary	Modbus slave successfully started in TCP mode.
0x00090003	Modbus Slave TCP start failed	Permanent	Starting the Modbus slave in the TCP mode failed.
0x00090004	Modbus Slave TCP terminated	Temporary	Modbus slave TCP mode successfully terminated.
0x00090005	Modbus Slave UDP started	Temporary	Modbus slave successfully started in UDP mode.

Table 66: Diagnostics for the Error Server

Diagnostics ID	Diagnostic text	Method of saving	Explanation
0x00090006	Modbus Slave UDP start failed	Permanent	Starting the Modbus slave in UDP mode failed.
0x00090007	Modbus Slave UDP terminated	Temporary	Modbus slave UDP mode successfully terminated.
0x00090008	Modbus Slave RTU started	Temporary	Modbus slave successfully started in the RTU mode.
0x00090009	Modbus Slave RTU start failed	Permanent	Starting the Modbus slave in RTU mode failed.
0x0009000A	Modbus Slave RTU terminated	Temporary	Modbus slave RTU mode successfully terminated.
0x0009000B	Modbus Slave data exchange started by PLC	Temporary	Modbus slave data exchange started.
0x0009000C	Modbus Slave data exchange stopped by PLC	Temporary	Modbus slave data exchange stopped.
0x0009000F	Modbus Slave PLC watchdog timer expired	Permanent	Monitoring time for controller (PLC) expired.
0x00090100	Modbus Slave common configuration failed.	Permanent	Modbus slave configuration failed.
0x00090101	Modbus Slave TCP configured successfully.	Temporary	Modbus slave TCP configuration completed successfully.
0x00090102	Modbus Slave TCP configuration failed.	Permanent	Modbus slave TCP configuration failed.
0x00090103	Modbus Slave UDP configured successfully	Temporary	Modbus slave UDP configuration completed successfully.
0x00090104	Modbus Slave UDP configuration failed.	Permanent	Modbus slave UDP configuration failed.
0x00090105	Modbus Slave RTU configured successfully.	Temporary	Modbus slave RTU configuration completed successfully.
0x00090106	Modbus Slave RTU configuration failed	Permanent	Modbus slave RTU configuration failed.
0x00090107	Port for Modbus Slave RTU operation not free.	Permanent	Serial port for Modbus slave RTU configuration already occupied.

Table 66: Diagnostics for the Error Server

Diagnostics ID	Diagnostic text	Method of saving	Explanation
0x00090108	Modbus Slave RTU configuration in RS-485 mode failed.	Permanent	Modbus slave RTU configuration for the RS-485 mode has failed.
0x00090200	Modbus Slave Watchdog activated.	Temporary	Modbus watchdog activated.
0x00090201	Modbus Slave Watchdog deactivated.	Temporary	Modbus watchdog deactivated.
0x00090202	Modbus Slave Watchdog Timer expired.	Permanent	Modbus watchdog monitoring time expired.
0x00090203	Modbus Slave has terminated all established TCP connections.	Permanent	All Modbus TCP connections terminated due to timeout.
0x00090300	Modbus Slave: obtaining system resource failed	Permanent	Request for system resources by the Modbus slave has failed.
0x00090301	Modbus Slave: processing system resource failed.	Permanent	Access to system resources by the Modbus slave has failed.

12 Modbus – *e!RUNTIME*

12.1 Modbus Address Overview

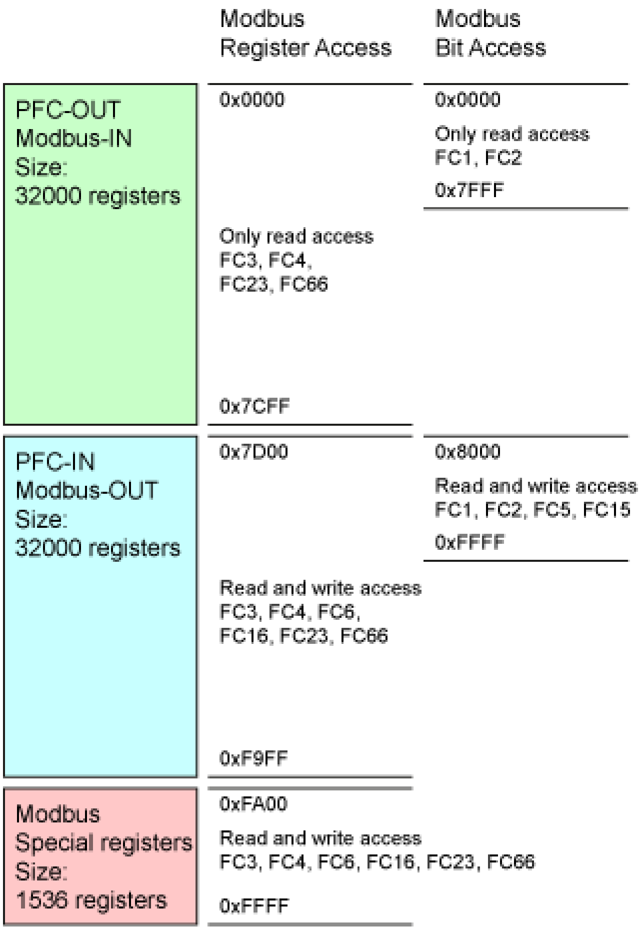


Figure 110: Modbus Address Overview

12.2 Modbus Registers

Table 67: WAGO Modbus Registers

Modbus Address		Data Length in Words	Access	Description
Dec.	Hex.			
Watchdog Configuration Registers				
64,000	0xFA00	1	w	Watchdog command register
64,001	0xFA01	1	rw	Watchdog timeout register
64,002	0xFA02	1	ro	Watchdog status register
64,003	0xFA03	1	rw	Watchdog config register
64,004	0xFA04	1	rw	Modbus TCP connection watchdog register
Status Registers				
64,010	0xFA0A	1	ro	LED flash code I/O-LED (sequence 1 of 3)
64,011	0xFA0B	1	ro	LED flash code I/O-LED (sequence 2 of 3)
64,012	0xFA0C	1	ro	LED flash code I/O-LED (sequence 3 of 3)
64,013	0xFA0D	1	ro	PLC State : 1 = Stop; 2 = Run
Electronic Type Label				
64,016	0xFA10	4	ro	Order number, e.g., 0750810100400001
64,020	0xFA14	1	ro	Firmware status
64,021	0xFA15	1	ro	Hardware version
64,022	0xFA16	1	ro	Firmware loader
Process Image Version				
64,023	0xFA17	1	ro	Version of the Modbus process image
Network Configuration				
64,032	0xFA20	3	ro	MAC-ID 1
Process Image Registers				
64,064	0xFA40	1	ro	Number of input registers, analog and digital (total size of the Modbus IN space) 0x7D00
64,065	0xFA41	1	ro	Number of input registers, analog 0x7D00
64,066	0xFA42	1	ro	Number of input registers, digital 0x8000
64,067	0xFA43	1	ro	Number of output registers, analog and digital (total size of the Modbus OUT space) 0x7D00
64,068	0xFA44	1	ro	Number of output registers, analog 0x7D00
64,069	0xFA45	1	ro	Number of output registers, digital 0x8000

Table 67: WAGO Modbus Registers

Modbus Address		Data Length in Words	Access	Description
Dec.	Hex.			
Constants Registers				
64,160	0xFAA0	1	ro	Constant 0x1234
64,161	0xFAA1	1	ro	Constant 0xAAAA
64,162	0xFAA2	1	ro	Constant 0x5555
64,250	0xFAFA	1	ro	Live register

The WAGO Modbus registers are described in more details in the following sections.

12.2.1 Modbus Watchdog

The Modbus watchdog monitors in the Modbus slave the ongoing Modbus communication with the Modbus master. All valid Modbus requests of a Modbus master from all the services supported by the Modbus slave are trigger events (see chapter “Modbus Mapping”). Exceptions here are the Explicit Trigger mode and the access to the register 0xFA02 (Watchdog Status), which can be configured via the register 0xFA03 (Watchdog Config).

The “Watchdog Timeout” response is initiated if no trigger occurs within the timeout set in the register 0xFA01 (Watchdog Timeout) with the watchdog running. The closing of all Modbus TCP connections can be configured as a response, see register 0xFA03 (Watchdog Config).

The Modbus watchdog supports two different operation modes ADVANCED_WATCHDOG and SIMPLE_WATCHDOG. The operation mode can be selected via Bit 7 in the register 0xFA03 (Watchdog Config).

The following diagrams show the possible states of the Modbus watchdog and status transitions for the particular operation mode.

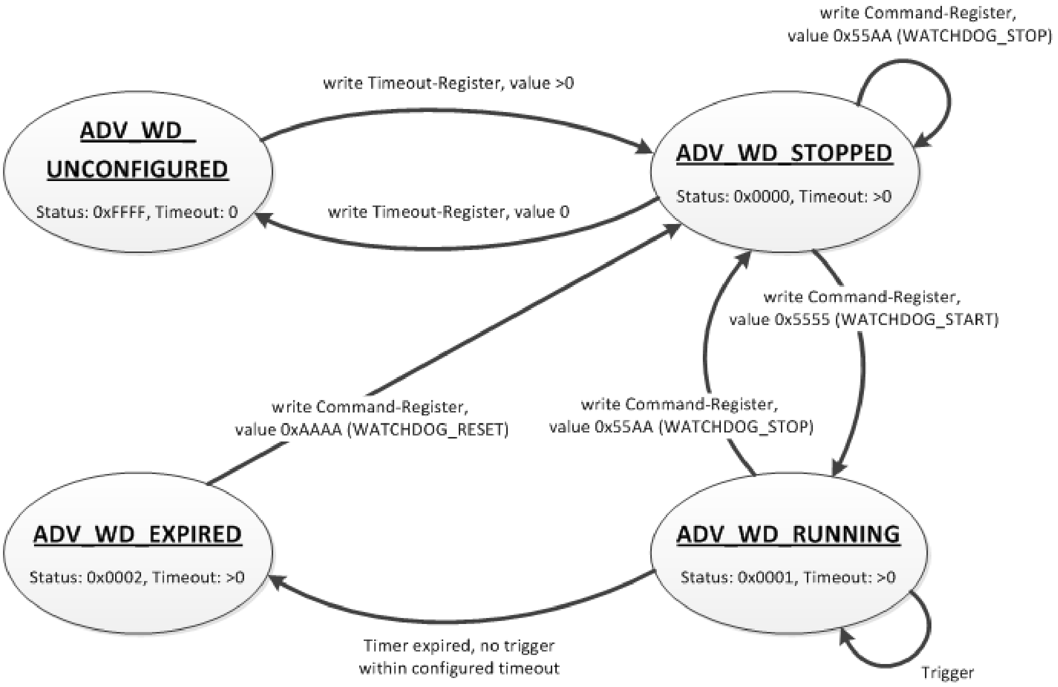

write Command-Register,
value 0x55AA (WATCHDOG_STOP)
write Timeout-Register, value >0
ADV_WD_
UNCONFIGURED
Status: 0xFFFF, Timeout: 0
ADV_WD_STOPPED
Status: 0x0000, Timeout: >0
write Timeout-Register, value 0
write Command-Register,
value 0x5555 (WATCHDOG_START)
write Command-Register,
value 0xAAAA (WATCHDOG_RESET)
write Command-Register,
value 0x55AA (WATCHDOG_STOP)
ADV_WD_EXPIRED
Status: 0x0002, Timeout: >0
ADV_WD_RUNNING
Status: 0x0001, Timeout: >0
Timer expired, no trigger
within configured timeout
Trigger

Figure 111: State Diagram, ADVANCED_WATCHDOG Operation Mode

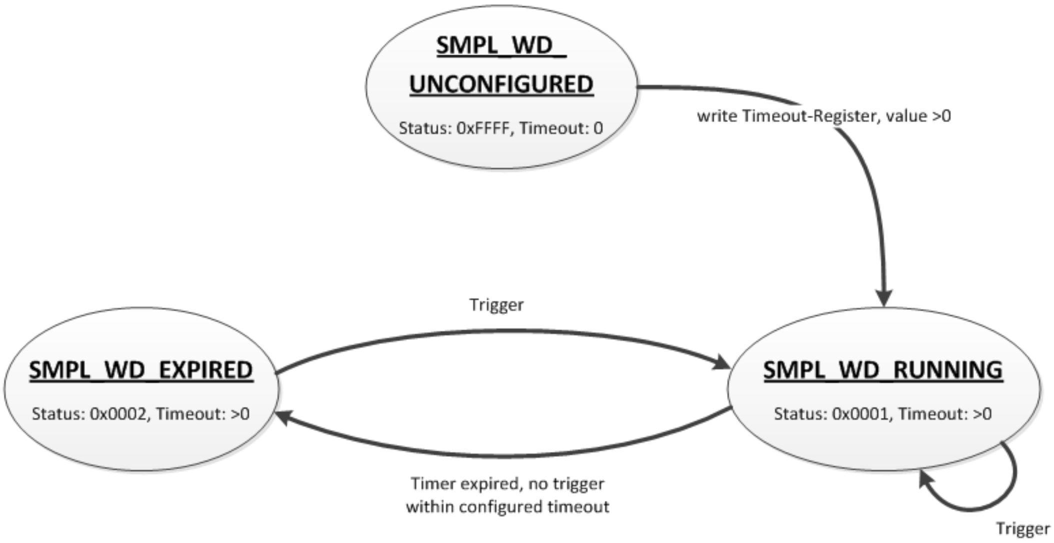

SMPL_WD_UNCONFIGURED
Status: 0xFFFF, Timeout: 0
write Timeout-Register, value >0
Trigger
SMPL_WD_EXPIRED
Status: 0x0002, Timeout: >0
SMPL_WD_RUNNING
Status: 0x0001, Timeout: >0
Timer expired, no trigger
within configured timeout
Trigger

Figure 112: State Diagram, SIMPLE_WATCHDOG Operation Mode

The state diagram for the SIMPLE_WATCHDOG operation mode shows that the watchdog is always active as soon as a timeout > 0 is set in the register 0xFA01 (Watchdog Timeout). The writing of commands in the register 0xFA00 (Watchdog Command) is restricted in this operation mode. Only the WATCHDOG_START command is permitted as a possible trigger. The only possibility to deactivate and stop the watchdog in operation mode SIMPLE_WATCHDOG, is the switching back to the operation mode ADVANCED_WATCHDOG.

The following diagram shows the possible state transitions when operation modes are switched.

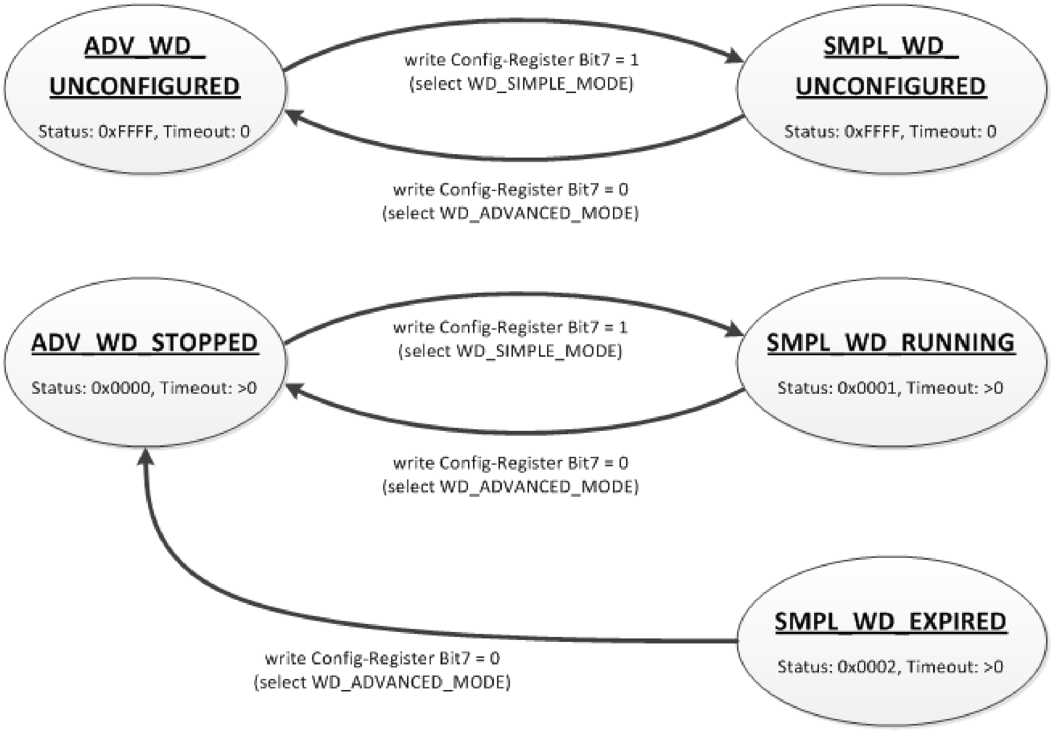

ADV_WD_UNCONFIGURED
Status: 0xFFFF, Timeout: 0
write Config-Register Bit7 = 1
(select WD_SIMPLE_MODE)
SMPL_WD_UNCONFIGURED
Status: 0xFFFF, Timeout: 0
write Config-Register Bit7 = 0
(select WD_ADVANCED_MODE)
ADV_WD_STOPPED
Status: 0x0000, Timeout: >0
write Config-Register Bit7 = 1
(select WD_SIMPLE_MODE)
SMPL_WD_RUNNING
Status: 0x0001, Timeout: >0
write Config-Register Bit7 = 0
(select WD_ADVANCED_MODE)
SMPL_WD_EXPIRED
Status: 0x0002, Timeout: >0
write Config-Register Bit7 = 0
(select WD_ADVANCED_MODE)

Figure 113: State Diagram, Switching Operation Modes

12.2.1.1 Register 0xFA00 – Watchdog Command

This register receives commands for the Modbus watchdog. It cannot be read, i.e. it is not possible to read out the last command written.
The following commands are accepted depending on watchdog status:

Table 68: Watchdog Commands

Value	Name	Explanation
0x5555	WATCHDOG_ START	Starts the configured watchdog; in the WATCHDOG_UNCONFIGURED state if no timeout is configured, the response is an ILLEGAL_DATA_VALUE (0x03) exception. The same exception is returned even if the watchdog has expired (WATCHDOG_EXPIRED) in the ADVANCED_ WATCHDOG operation mode. The watchdog must in this case be reset first with the command WATCHDOG_RESET to the WATCHDOG_STOPPED state. In all other cases the watchdog is restarted and the WATCHDOG_RUNNING state is set.
0x55AA	WATCHDOG_ STOP	Stops the running watchdog; in the WATCHDOG_UNCONFIGURED state, the response is an ILLEGAL_DATA_ VALUE (0x03) exception if no timeout time is set. The same exception is returned even if the watchdog has expired (WATCHDOG_EXPIRED) in the ADVANCED_ WATCHDOG operation mode. The watchdog must in this case be reset first with the command WATCHDOG_RESET to the WATCHDOG_STOPPED state. In the SIMPLE_ WATCHDOG operation mode the response is an ILLEGAL_DATA_VALUE (0x03) exception. The command is not generally permitted in this operation mode. In all other cases, the watchdog is stopped and the WATCHDOG_STOPPED state is set. In the WATCHDOG_STOPPED state a stop command received several times in a row does not have any impact on the behavior of the watchdog and is therefore not acknowledged with an error response.
0xAAAA	WATCHDOG_ RESET	Resets the expired watchdog; in the WATCHDOG_EXPIRED state the ADVANCED_WATCHDOG operation mode resets the watchdog. The watchdog is then in the WATCHDOG_STOPPED state. In all other cases the response is an ILLEGAL_ DATA_VALUE (0x03) exception.

12.2.1.2 Register 0xFA01 – Watchdog Timeout

This register contains the value for the watchdog timeout. The step width is 1 ms and the maximum value is 65535 (corresponds to 65.535 s). The default value is 0. In this case the watchdog cannot be started and will have the WATCHDOG_UNCONFIGURED state.

The register can be read and written in the states WATCHDOG_UNCONFIGURED and WATCHDOG_STOPPED. However, if the watchdog is active or expired (WATCHDOG_RUNNING and WATCHDOG_EXPIRED state), only read access to this register is possible. The response to a write operation is an ILLEGAL_FUNCTION (0x01) exception.

12.2.1.3 Register 0xFA02 – Watchdog Status

This register provides the current state of the Modbus watchdog.
The following states are possible:

Table 69: Watchdog Status

Value	Name	Explanation
0xFFFF	WATCHDOG_ UNCONFIGURED	The Modbus watchdog is not configured, i.e., register 0xFA01 (Watchdog Timeout) contains the value 0. Only the setting of a timeout > 0 s can close this state.
0x0000	WATCHDOG_ STOPPED	The Modbus watchdog is configured, the register 0xFA01 (Watchdog Timeout) contains a value >0. In the ADVANCED_WATCHDOG operation mode, the watchdog can be activated in this state with the WATCHDOG_START command. In the SIMPLE_WATCHDOG operation mode, this state cannot be accessed since the watchdog is automatically started.
0x0001	WATCHDOG_ RUNNING	The Modbus watchdog is active, i.e. configured and started. The set timeout has not yet expired.
0x0002	WATCHDOG_ EXPIRED	The timeout set in register 0xFA01 (Watchdog Timeout) has expired. In the ADVANCED_WATCHDOG operation mode, the watchdog in this state must be reset to the WATCHDOG_STOPPED state with the WATCHDOG_RESET command. In the SIMPLE_WATCHDOG operation mode, the watchdog is automatically restarted with the next trigger.

12.2.1.4 Register 0xFA03 – Watchdog Config

This register contains the configuration parameters for the watchdog. The register is organized in bits, see following table.

The register can be read and written irrespective of the watchdog state in the SIMPLE_WATCHDOG operation mode.
However, in the ADVANCED_WATCHDOG operation mode, the register can only be read and written in the WATCHDOG_UNCONFIGURED and WATCHDOG_STOPPED states.
If the watchdog is active (WATCHDOG_RUNNING or WATCHDOG_EXPIRED state), only a read access is permissible. The response to a write request in this case is an ILLEGAL_FUNCTION (0x01) exception.

Table 70: Watchdog Configuration

Bit	Name/Bit Identifier	Explanation	
0	EXPLICIT_TRIGGER_ONLY	Activates the Explicit Trigger mode	
		0*	All valid Modbus requests are considered as watchdog triggers. Access to register 0xFA02 (Watchdog Status) is the only exception.
		1	Only the writing of register 0xFA00 (Watchdog Command) with the value 0x5555 (WATCHDOG_START) is considered as the watchdog trigger. The exception is also here the access to the register 0xFA02 (Watchdog Status).
1	TRIGGER_ON_STATUS_REG	Activates the watchdog trigger by (read) access to register 0xFA02 (Watchdog Status)	
		0*	The reading of the watchdog status is not considered as a watchdog trigger.
		1	The reading of the watchdog status triggers the watchdog.
2	CLOSE_ALL_TCP_CONNECTIONS	Activates the closing of all Modbus TCP connections with the expiry of the timeout (transition to WATCHDOG_EXPIRED state)	
		0	Existing Modbus TCP connections remain open.
		1*	All existing Modbus TCP connections are closed.
7	SELECT_ADVANCED_SIMPLE_MODE	Determines the watchdog operation mode	
		0*	Advanced Mode: The watchdog must be controlled explicitly via commands (see register 0xFA00 Watchdog Command).
		1	Simple Mode: The watchdog is activated directly with a timeout > 0 in register 0xFA01 (Watchdog Timeout). Each trigger restarts the running as well as the expired watchdog. The watchdog can only be stopped by switching to Advanced mode.
*Default setting			

The individual options are activated if the relevant bit or bit combination is set.

12.2.1.5 Modbus TCP Connection Watchdog Register

The 0xFA04 register contains the time for the Modbus TCP connection watchdog. Time base is 10 ms. This enables the time to be set up to 655350 ms. If the register contains a value > 0 s when a new TCP connection from a Modbus master is accepted, the watchdog for this connection is started. Later changes to the register have no effect on the monitoring of existing connections. If the watchdog is started and no telegram is received from the connected Modbus master within the set time, this connection is closed from one side with a reset.

12.2.2 Status Registers

12.2.2.1 PLC Status Register

The register 0xFA0D supplies the current status of the controller.
Possible values:

1 = PLC Stop - PLC is in STOP status.
2 = PLC Run - PLC is in RUN status

12.2.3 Electronic Nameplate

Registers 0xFA10–0xFA17 contain information from the electronic nameplate. It is possible to read the entire nameplate or a consecutive portion of it all at once.

12.2.3.1 Order Number

The registers 0xFA10–0xFA13 contain the WAGO order number of the controller.

Example: 0750-8202/0025-0001.

0xFA10 = 0750,
0xFA11 = 8202,
0xFA12 = 0025,
0xFA13 = 0001

12.2.3.2 Firmware Version

The register 0xFA14 contains the firmware version of the controller.

12.2.3.3 Hardware Version

The register 0xFA15 contains the hardware version of the controller.

12.2.3.4 Firmware Loader/Boot Loader

The register 0xFA16 contains the firmware loader/boot loader version of the controller.

12.2.4 Modbus Process Image Version

The register 0xFA17 contains the Modbus process image version of the controller.

12.2.5 Modbus Process Image Registers

The registers 0xFA40–0xFA45 contain size information for the process image spaces of the controller for bit and register accesses.

12.2.6 Constant Registers

Registers 0xFAA0 … 0xFAA2 provide constants based on the “WAGO Modbus Registers” table. It is possible to read all of the constants, or a consecutive portion of them at once.

0xFAA0 = 0x1234,
0xFAA1 = 0xAAAA,
0xFAA2 = 0x5555

12.2.7 Live Register

The register 0xFAFA can only be read and contains a counter that is incremented with each cycle of a task of the runtime environment with read and write access to the Modbus process data.

12.3 Estimating the Modbus Master CPU Load

Due to the real-time characteristics of the Linux kernel used, many data points can generate many context changes.
For a one-off update (transmitting and receiving of a function code), a CPU time of approx. 800 µs can be assumed.
The CPU load (cpu_load) in percent can be estimated from the cycle time (t_z) for a query with the following rule of thumb:

cpu_load = 800 µs / t_z * 100

A cycle time of 100 ms thus results in a CPU load of 0.8%.
A maximum load of approx. 20% can be generated per connection, as this is limited by the network protocol. To minimize the CPU load:

- The cycle time must be as high as possible.
- As many data points as possible must be combined in a query.
- The minimum query interval can be increased (default value: 0 ms).

13 Diagnostics

13.1 Operating and Status Messages

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

13.1.1 Power Supply LEDs

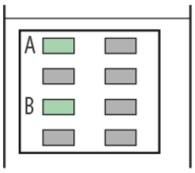


Figure 114: Power Supply Indicating Elements

13.1.1.1 A LED

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

Table 71: 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.

13.1.1.2 B LED

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

Table 72: 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.

13.1.2 System/Fieldbus LEDs

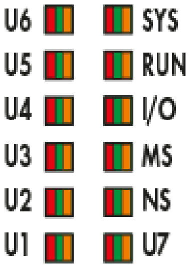


Figure 115: Indicating Elements for Fieldbus/System

13.1.2.1 SYS LED

The SYS LED indication depends on the runtime system enabled (CODESYS V2 or ***e!****RUNTIME*).

The following indications apply to the CODESYS V2 runtime system:

Table 73: 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.	---
	Load above threshold value 1 The system is at full capacity; real-time response can no longer be guaranteed.	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 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.
Red	Load above threshold value 2 The system is overloaded; real-time response can no longer be guaranteed.	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.
Green/red flashing	Firmware update mode	---

The following indications apply to the ***e!****RUNTIME* runtime system:

Table 74: 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	The libraries or device functions affected are shown in ***e!****COCKPIT*. 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	The libraries or device functions affected are shown in ***e!****COCKPIT*. 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.

13.1.2.2 RUN LED

The RUN LED indication depends on the runtime system enabled (CODESYS V2 or ***e!****RUNTIME*).

The following indications apply to the CODESYS V2 runtime system:

Table 75: Diagnostics RUN LED

Status	**Explanation**	**Solution**
Green	PLC program has the status “Run”.	---
Green flashing	PLC program at a debug point.	Resume the program in the linked IDE (Integrated Development Environment) using “Single step” or “Start”. If the connection has been interrupted, set the Run/Stop switch to “Stop” and then back to “Run” to enable the program to continue.
Green/red flashing	PLC is at a debug point and the Run/Stop switch has been set to “Stop”.	Set the Run/Stop switch to “Run” to enable the program to continue.
Red	No PLC-program loaded or PLC program has the status “Stop”.	Load the PLC program. Set the Run/Stop switch to “Run” to start the current program.

The following indications apply to the ***e!****RUNTIME* runtime system:

Table 76: 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.

13.1.2.3 I/O LED

The I/O LED indicates following diagnostics:

Table 77: 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.

13.1.2.4 MS LED

The MS LED indicates following diagnostics:

Table 78: 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.”

13.1.3 Network Connection LEDs

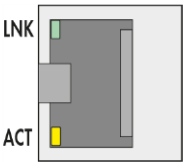


Figure 116: Indicating Elements, RJ-45 Jacks

13.1.3.1 LNK LED

The LNK LED indicates following diagnostics:

Table 79: LNK-LED Diagnostics

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

13.1.3.2 ACT LED

The ACT LED indicates following diagnostics:

Table 80: ACT-LED Diagnostics

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

13.1.4 Memory Card Slot LED

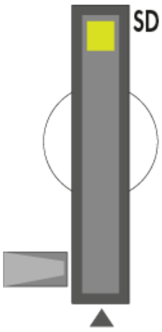


Figure 117: Indicating Elements, Memory Card Slot

The memory card slot LED indicates following diagnostics:

Table 81: Diagnostics via Memory Card Slot LED

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

13.2 Diagnostics Messages via Flashing Sequences

13.2.1 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.

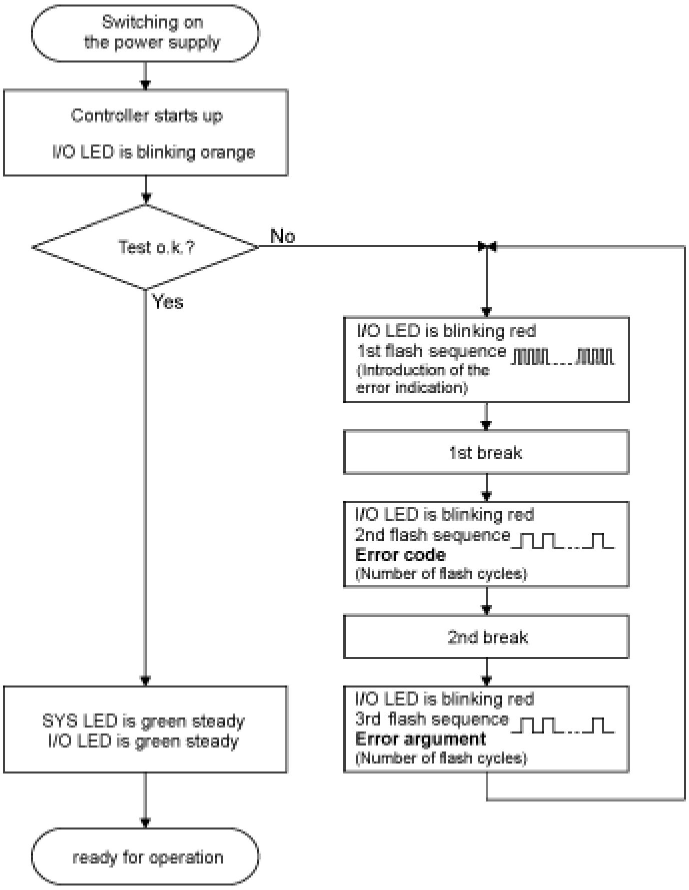


Figure 118: Flashing Sequence Process Diagram

13.2.2 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.

13.2.3 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 82: 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 83: 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 83: 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 84: 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 85: 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 86: 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 87: 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 88: 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 89: 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 V2 applications: - Contact WAGO Support. For ***e!****RUNTIME* applications: - Check the system load by IEC tasks with priorities 1 ... 14 in the runtime system (see Section “***e!****RUNTIME*” Runtime Environment > “CODESYS V3 Priorities”). For C applications: - Check the time monitoring settings.

13.2.4 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 90: Overview of MS-LED Error Codes

Error Code	Explanation
1	Configuration error

Table 91: 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.

14 Service

14.1 Inserting and Removing the Memory Card

14.1.1 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.

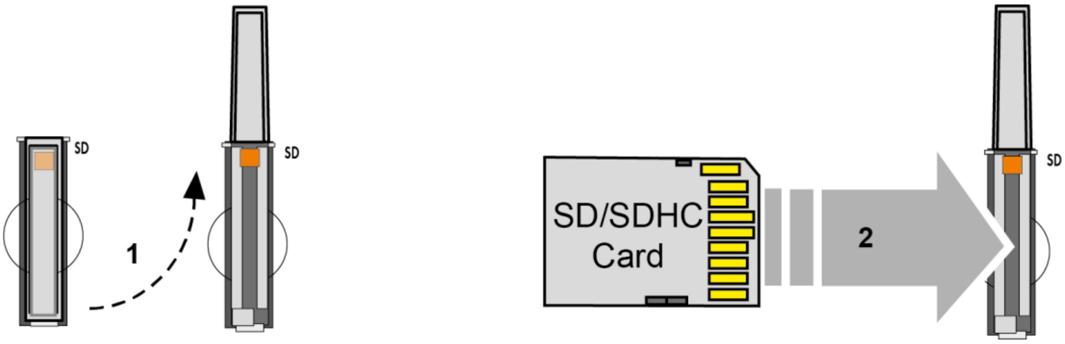


Figure 119: Inserting the Memory Card

14.1.2 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.

14.2 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:

- ***e!****COCKPIT*
- WAGOupload
- Memory card and WBM

14.2.1 Use *e!COCKPIT* to Update/Downgrade the Firmware

1. Launch ***e!****COCKPIT*.

2. Create a new project or open an existing project.

3. Add at least one controller to your ***e!****COCKPIT* project either by scanning the network or going to the device catalog and entering the IP address of your controller in the settings dialog.

   Your controller is now displayed in the Device View of the project.

4. Select the displayed controller and click “Apply Selection” in the “SCAN” tab.

5. Click **[Add]** in the dialog.

6. Then click **[Replace Firmware]**. in the “DEVICE” tab.

   The “Replace Firmware” dialog opens.

7. In the “Replace Firmware” dialog, select the required firmware under “Available firmware on the PC” or click the “Select File” entry and select the * .wup firmware file for the required firmware.

8. Click **[Replace Firmware]** to transfer the firmware to the controller.

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

The newly installed firmware is now available on your controller.

14.2.2 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.

14.2.3 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. Save your application and the controller settings.
2. Switch off the controller.
3. Insert the memory card with the new firmware image into the memory card slot. Use a special downgrade image if necessary (see above).
4. Switch on the controller.
5. After booting the controller, launch the WBM “Create Boot Image” page (you may have to temporarily change the IP address).
6. Create a new boot image on the internal memory.
7. Switch off the controller after completing the process.
8. Remove the memory card.
9. Switch on the controller.

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

14.3 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.

15 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.

15.1 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.

15.1.1 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.

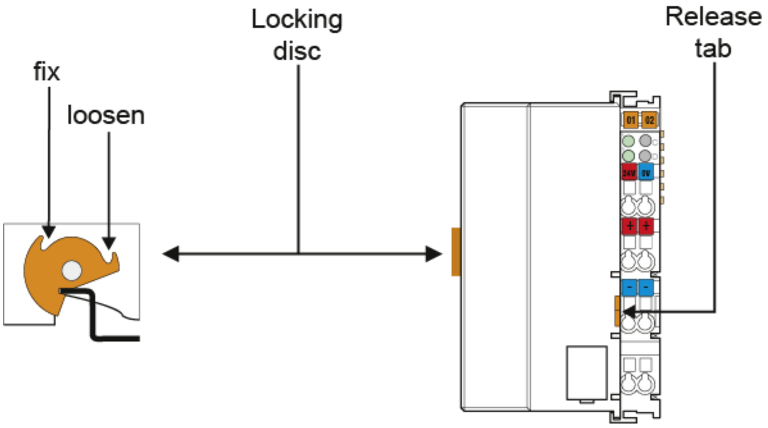


Figure 120: Release Tab of Controller

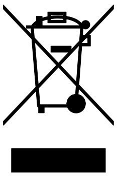
Note

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.

16 Disposal

16.1 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.

16.2 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.

17 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.

17.1 Marking Configuration Examples

17.1.1 Marking for Europe According to ATEX and IECEx

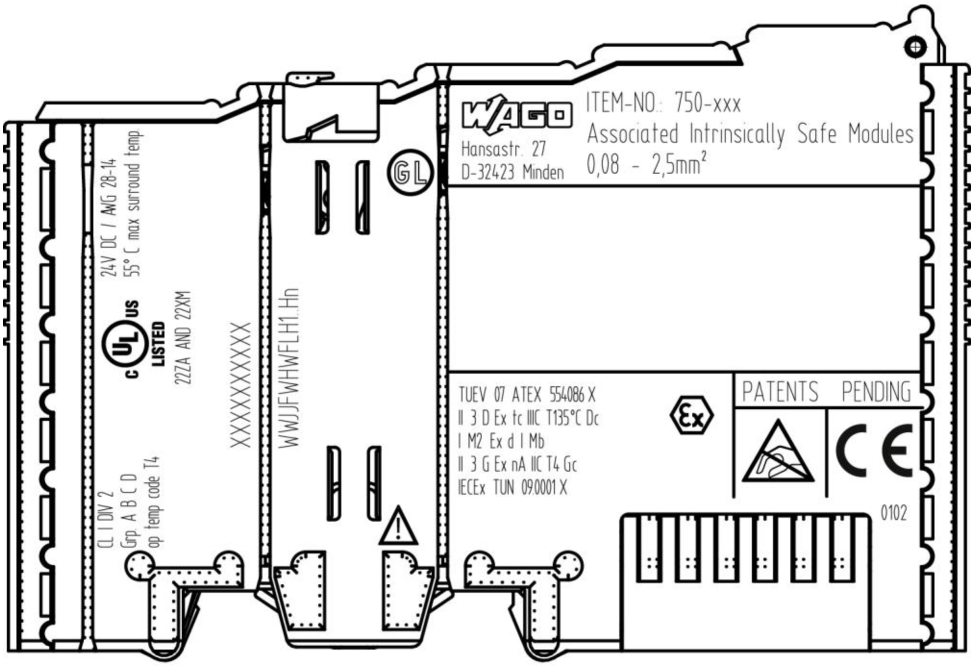


Figure 121: Marking Example According to ATEX and IECEx

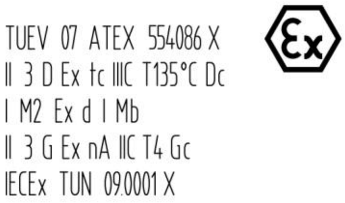

TUEV 07 ATEX 554086 X
II 3 D Ex tc IIIC T135°C Dc
I M2 Ex d I Mb
II 3 G Ex nA IIC T4 Gc
IECEx TUN 09.0001 X

Figure 122: Text Detail – Marking Example According to ATEX and IECEx

Table 92: 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)

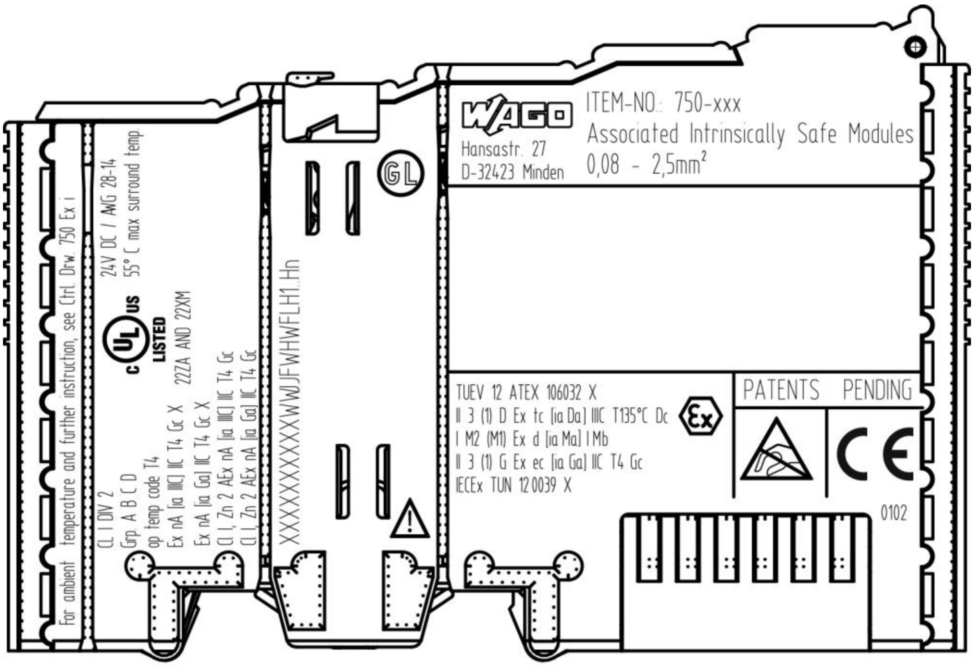

For ambient temperature and further instruction, see Ctrl. Drw. 750 Ex i
24V DC / AWG 28-14
55° C max surround temp
CL I DIV 2
Grp. A B C D
op temp code T4
Ex nA [ia IIIC] IIC T4 Gc X
Ex nA [ia Ga] IIC T4 Gc X
CL I, Zn 2 AEx nA [ia IIIC] IIC T4 Gc
CL I, Zn 2 AEx nA [ia Ga] IIC T4 Gc
c UL us
LISTED
22ZA AND 22XM
XXXXXXXXXXXWWJFWHWFLH1.Hn
GL
WAGO
Hansastr. 27
D-32423 Minden
ITEM-NO.: 750-xxx
Associated Intrinsically Safe Modules
0,08 - 2,5mm²
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 12 0039 X
Ex
PATENTS PENDING
CE
0102

Figure 123: Marking Example for Approved I/O Module Ex i According to ATEX and IECEx

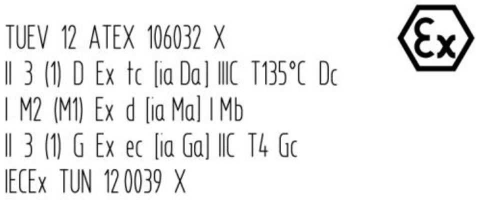

TUEV 12 ATEX 106032 X
II 3 (1) D Ex tc [ia Da] IIIC T135°C Dc
I M2 (M1) Ex d [ia Ma] I Mb
II 3 (1) G Ex ec [ia Ga] IIC T4 Gc
IECEx TUN 12 0039 X

Figure 124: Text Detail – Marking Example for Approved I/O ModuleEx i According to ATEX and IECEx

Table 93: 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)

17.1.2 Marking for the United States of America (NEC) and Canada (CEC)

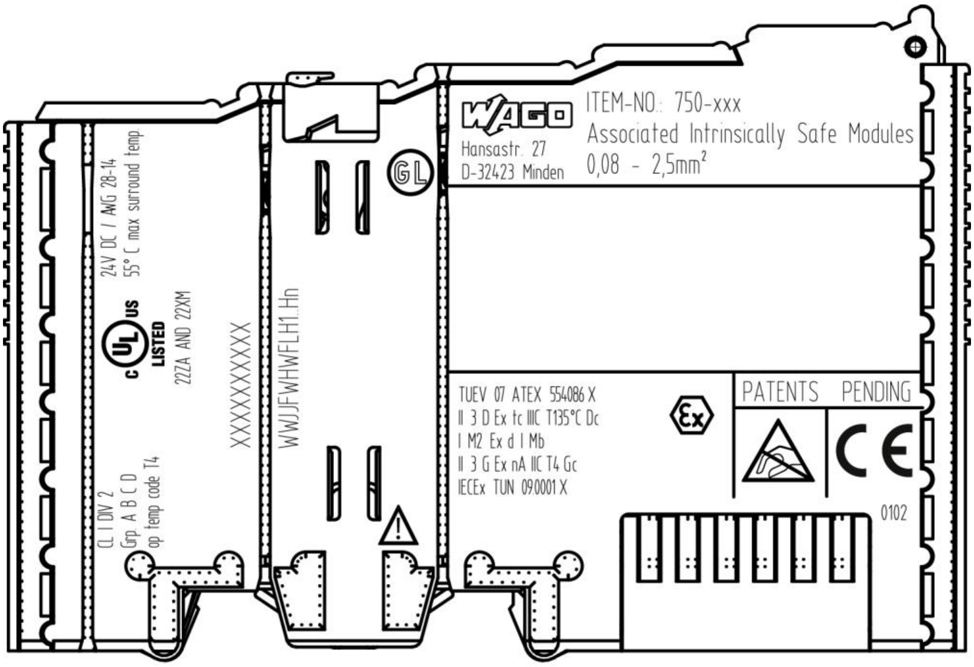


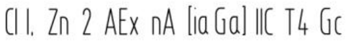
Figure 125: Marking Example According to NEC

CL I DIV 2
Grp. A B C D
op temp code T4

Figure 126: Text Detail – Marking Example According to NEC 500

Table 94: 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

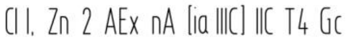


Cl I, Zn 2 AEx nA [ia Ga] IIC T4 Gc

Figure 127: Text Detail – Marking Example for Approved I/O Module Ex i According to NEC 505

Table 95: Description of Marking Example for Approved I/O Module Ex i According to NEC 505

Marking	Description
Cl 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)

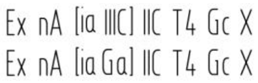


Cl I, Zn 2 AEx nA [ia IIIC] IIC T4 Gc

Figure 128: Text Detail – Marking Example for Approved I/O Module Ex i According to NEC 506

Table 96: Description of Marking Example for Approved I/O Module Ex i According to NEC 506

Marking	Description
Cl 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 129: Text Detail – Marking Example for Approved I/O Module Ex i According to CEC 18 attachment J

Table 97: 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

17.2 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.

17.2.1 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.

17.2.2 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!

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.

18 Appendix

18.1 Configuration Dialogs

18.1.1 Web-Based-Management (WBM)

18.1.1.1 "Information" Tab

18.1.1.1.1 "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 98: 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 99: WBM “Device Status” Page – “Network TCP/IP Details” Group

Parameter	Meaning	
DIP Switch Status	Status of the address selection switch; this area only appears if an address selection switch is available.	
DIP Switch Mode	Address Selection Switch	
	Off (0)	IP address assignment via e.g., WBM
	static (1 … 254)	Static IP address assignment via address selection switch
	dhcp (255)	Dynamic IP address assignment via DHCP
DIP Switch Value	Set value of the address selection switch	
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 PROFINET application.
IP Address	Current product IP address	
Subnet Mask	Current product subnet mask	

18.1.1.1.2 “Vendor Information” Page

You can find the manufacturer and address on the “Vendor Information” page.

18.1.1.1.3 “PLC Runtime Information” Page

All information about the enabled runtime system and PLC program created in the programming software is provided on the “PLC Runtime Information” page. You will also find a link here to open WebVisu.

“Runtime” Group

Table 100: WBM “PLC Runtime Information” Page – “Runtime” Group

Parameter	Explanation	
Version	The version of the currently enabled runtime system is shown. If the runtime system is disabled, “None” is displayed and the subsequent fields of this group are hidden.	
Webserver Version	This shows the version number of the Webserver. This field appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.	
State	The PLC operating state is displayed. This field appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.	
	STOP	PLC program is not executed.
	RUN	PLC program is executed.
Number of Tasks	The number of tasks in the PLC program is shown. This field appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.	

“WebVisu” Group

You will find a link that you can use to open WebVisu.

“Project Details” Group

This group appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.

Table 101: WBM “PLC Runtime Information” Page – “Project Details” Group

Parameter	Explanation
Date	The last save date of the project is displayed.
Title	The project information that the programmer has entered in the PLC program is displayed here (in the programming software under Project > Project Information ...). The information only appears in an executed PLC program. Descriptive texts up to 1024 characters long are given under “Description.”
Version	
Author	
Description	
Checksum	The calculated checksum of the project is displayed.

“Task <n>” Group(s)

One dedicated group is displayed for each task when the PLC program is executed. As a rule, only the group title is displayed with the task number, the task name and the task ID.

This group(s) appear(s) if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.

Table 102: WBM “PLC Runtime Information” Page – “Task n” Group(s)

Parameter	Explanation
Cycle count	Number of task cycles since the system start
Cycle time (µsec)	Currently measured task cycle time for the task
Cycle time min (µsec)	Minimum task cycle time for the task since the system start
Cycle time max (µsec)	Maximum task cycle time for the task since the system start
Cycle time avg (µsec)	Average task cycle time since the system start
Status	Task status (e.g., RUN, STOP)
Mode	Task execution mode (e.g., in cycles)
Priority	Set task priority
Interval (msec)	Set task interval

18.1.1.1.4 “WAGO Software License Agreement” Page

The “WAGO Software License Agreement” page lists the license terms for the WAGO software used in the product.

18.1.1.1.5 “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.

18.1.1.1.6 “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.

18.1.1.1.7 “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.

18.1.1.2 “Configuration” Tab

18.1.1.2.1 “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 103: 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 2	CODESYS V2 runtime system is enabled. This value only appears if the controller supports the CODESYS V2 runtime system.
	e!_RUNTIME_	**e!**_RUNTIME_ runtime system is enabled. This value only appears if the controller supports the **e!**_RUNTIME_ runtime system.
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 104: WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group

Parameter	Meaning	
CODESYS V2 Webserver State	This displays the status (enabled/disabled) of the CODESYS V2 Webserver. This field only appears if the controller supports the CODESYS V2 runtime system.	
e!*RUNTIME* Webserver State	This indicates the status (enabled/disabled) of the ***e!****RUNTIME* Webserver. This field only appears if the controller supports the ***e!****RUNTIME* runtime system.	
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.

18.1.1.2.2 “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 105: 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.	
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 **Configuration Type** field.	
Subnet Mask	Enter the subnet mask. This is enabled if “Static IP” is enabled in the **Configuration Type** field.	

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“DNS Server” Group

Table 106: WBM “TCP/IP Configuration” Page – “DNS Server” Group

Parameters	Explanation
New Server IP	Add additional DNS addresses. You can enter 10 addresses.
Manually Assigned	The addresses of the defined DNS servers are displayed. If no server has been entered, “No DNS Servers configured” is displayed.
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.

Click the **[Add]** button to add the entered DNS server. The change takes effect immediately.

Click the **[Delete]** button to delete the selected DNS server. The change takes effect immediately.

18.1.1.2.3 “Ethernet Configuration” Page

The settings for ETHERNET are located on the “Ethernet Configuration” page.

“Bridge Configuration” Group

Table 107: 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 108: 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.
Fast Aging	Set here the aging time of unused entries in the list of MAC addresses with a port assignment to external network stations. This field is only enabled in “switched” mode. Fast aging is only effective in this mode.	
	Disabled	An unused address entry becomes obsolete after 200 seconds.
	Enabled	An unused address entry becomes obsolete after 800 microseconds.
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 109: 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.	
Autonegotiation on	When Autonegotiation is enabled, the connection modalities are negotiated automatically with the peer devices.	
Speed/Duplex	Select the transmission speed and the duplex method:	
	10 Mbit half-duplex	Information can only be sent or received.
	100 Mbit half-duplex	
	10 Mbit full-duplex	Information can be sent and received simultaneously.
	100 Mbit full-duplex	

Click **[Submit]** to apply changes. The changes take effect immediately.

18.1.1.2.4 “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 110: 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 a hostname is supplied via a DHCP response, this is enabled in the system. If there are several network interfaces with DHCP, the last received hostname is always valid.
If only the hostname configured here is to be valid, the configuration of the DHCP server must be adapted so that no hostnames are transferred in the DHCP response.

“Domain Name” Group

Table 111: 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 a domain name is supplied via a DHCP response, this is enabled in the system. If there are several server network interfaces with DHCP, the last received domain name is always valid.

If only the domain name configured here is to be valid, the configuration of the DHCP server must be adapted so that no domain names are transferred in the DHCP response.

18.1.1.2.5 “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 112: 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.

“Default Static Routs” Group

Each configured static route has its own area in the display.

To maintain compatibility with earlier firmware versions, at least two routing entries always exist. These can be disabled, but not removed. If a route is either removed or disabled, it is no longer entered in the system.

Table 113: WBM “Routing” Page – “Default Static 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.	
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 default value for the metric is 20. The lowest value is 0. The highest value is 2^{32} - 1 = 4,294,967,295.	

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 114: 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 115: 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.

18.1.1.2.6 “Clock Settings” Page

The date and time settings are displayed on the “Clock Settings” page.

“Timezone and Format” Group

Table 116: 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 117: 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 118: 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.

18.1.1.2.7 “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 119: 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!

18.1.1.2.8 “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 120: 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!

18.1.1.2.9 “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 121: WBM “Create Bootable Image” Page – “Create bootable image from active partition” Group

<table>
<tr><th>Parameters</th><th colspan="3">Meaning</th></tr>
<tr><td>Boot Device</td><td colspan="3">The medium from which the boot was made is displayed.</td></tr>
<tr><td rowspan="4">Destination</td><td colspan="3">Depending on which medium has been booted, the following destination is available for selection after boot-up for the image to be generated:</td></tr>
<tr><td>System was booted from</td><td></td><td>Target partition for “bootable image”</td></tr>
<tr><td>Memory Card</td><td>→</td><td>Internal Flash</td></tr>
<tr><td>Internal memory</td><td>→</td><td>Memory Card</td></tr>
</table>

- 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.

18.1.1.2.10 “Firmware Backup” Page

You can find the controller data backup settings on the “Firmware Backup” page.

“Firmware Backup” Group

Table 122: 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, 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.

18.1.1.2.11 “Firmware Restore” Page

The settings for restoring the controller data are shown on the “Firmware Restore” page.

“Firmware Restore” Group

Table 123: 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 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

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.

Click the **[Restore]** button to start the restore operation.

18.1.1.2.12 “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 124: 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 125: 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!

18.1.1.2.13 “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 126: 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 127: 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]**.

18.1.1.2.14 “Software Uploads” Page

On “Software Upload” page, you can install software packages on the product from your PC.

Table 128: 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.

18.1.1.2.15 “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*, port 2455 for CODESYS V2 and port 11740 for ***e!****COCKPIT*).
Only open ports and services during commissioning and/or configuration.

“Telnet” Group

Table 129: WBM “Configuration of Network Services” Page – “Telnet” Group

Parameters	Explanation
Telnet	Enable/disable the Telnet service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“FTP” Group

Table 130: WBM “Configuration of Network Services” Page – “FTP” Group

Parameters	Explanation
FTP	Enable/disable the FTP service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“FTPS” Group

Table 131: WBM “Configuration of Network Services” Page – “FTPS” Group

Parameters	Explanation
FTPS	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 132: WBM “Configuration of Network Services” Page – “HTTP” Group

Parameters	Explanation
HTTP	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 133: WBM “Configuration of Network Services” Page – “HTTPS” Group

Parameters	Explanation
HTTPS	Enable/disable the HTTPS service.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

Note

Disconnection abort on disabling

If the HTTPS service is disabled, the connection to the product may be interrupted. In that case, reopen the page.

“I/O-*CHECK*” Group

Table 134: WBM “Configuration of Network Services” Page – “I/O-*CHECK*“ Group

Parameters	Explanation
Service active	Enable/disable the WAGO-I/O-*CHECK* service.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

18.1.1.2.16 “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 135: 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.

18.1.1.2.17 “PLC Runtime Services” Page

The settings for various services of the enabled runtime system are displayed on the “PLC Runtime Services” page.

“General Configuration” Group

Table 136: WBM “PLC Runtime Services” Page – “General Configuration” Group

Parameter	Explanation
Port Authentication Password	Specify the new password for port authentication.
Confirm Password	Enter the new password again for confirmation.

Click the **[Set Password]** button to apply the change. The change takes effect immediately.

“CODESYS V2” Group

This group only appears if the controller supports the CODESYS V2 runtime system.

Table 137: WBM “PLC Runtime Services” Page – “CODESYS V2” Group

Parameter	Explanation
CODESYS 2 State	This displays the status (enabled/disabled) of the CODESYS V2 runtime system.
Webserver enabled	Enable or disable the CODESYS V2 Webserver for the CODESYS web visualization.
Communication enabled	Enable or disable the communication between the CODESYS V2 runtime system and the CODESYS V2 programming system.
Communication Port Number	Enter here the port number for communication with the CODESYS V2 programming system. The default value is 2455.
Port authentication enabled	Define here whether port authentication is enabled. If this is enabled, the password specified under “General Configuration” must be entered when logging in via CODESYS V2 IDE.

Click the **[Submit]** button to apply the change.
The change in authentication takes effect after the next restart.
All other changes take effect immediately.

“*e!RUNTIME*” Group

This group only appears if the controller supports the ***e!****RUNTIME* runtime system.

Table 138: WBM “PLC Runtime Services” Page – “***e!****RUNTIME*” Group

Parameter	Explanation
e!*RUNTIME* State	This displays the status of the ***e!****RUNTIME* system (enabled/disabled).
Webserver enabled	Enable or disable the Webserver for the ***e!RUNTIME*** 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.

18.1.1.2.18 “SSH Server Settings” Page

The settings for the SSH service are shown on the “SSH Server Settings” page.

“SSH Server” Group

Table 139: 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.

18.1.1.2.19 “TFTP Server” Page

The settings for the TFTP service are shown on the “TFTP Server” page.

“TFTP Server” Group

Table 140: WBM “TFTP Server” Page – “TFTP Server” Group

Parameters	Explanation
Service active	Activate or deactivate the TFTP server.
Download directory	Specify the path for downloading the server directory.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

18.1.1.2.20 “DHCP Server Configuration” Page

The “DHCP Server Configuration” page displays the DHCP service settings.

“DHCP Server Configuration Bridge <n>” Group

Table 141: WBM “DHCP Server Configuration” Page – “DHCP Configuration Bridge <n>” Group

Parameter	Explanation
Service active	Enable or disable the DHCP service for the interface Xn.
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 10 assignments or host names.
Ip Address	Enter the IP address. You can enter 10 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.

18.1.1.2.21 “Configuration of DNS Server” Page

The “Configuration of DNS Server” page displays the DNS service settings.

“DNS Server” Group

Table 142: 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.

18.1.1.2.22 “Status overview” Page

On the “Status overview” page, you can find information about cloud access.

“Service” Group

Table 143: 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 144: WBM “Status Overview” Page – “Connection <n>” Group

Parameter	Explanation
Operation	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.

18.1.1.2.23 “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 145: 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 145: 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.
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).
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.

Table 145: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
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 table shows the dependencies of the selection and input fields for the selected cloud platform.

Table 146: Dependencies of the Selection and Input Fields for the Selected Cloud Platform

Selection or Input Field	Cloud Platform						Authentication		Data Protocol				Last Will
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services	Shared Access Key	X.509 Certificate	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B	
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	>					X						
Clean Session			X	(X)	(X)	X							
TLS			X	X	(X)	X							
CA file			X	X	X	X							
User			X	X									

Table 146: Dependencies of the Selection and Input Fields for the Selected Cloud Platform

Selection or Input Field	Cloud Platform						Authen tication		Data Protocol				
	WAGO Cloud	**Azure**	**MQTT AnyCloud**	**IBM Cloud**	**Amazon Web Services**	**SAP IoT Services**	**Shared Access Key**	**X.509 Certificate**	**WAGO Protocol**	**WAGO Protocol 1.5**	**Native MQTT**	**Sparkplug payload B**	**Last Will**
Password			X	X									
Certification file		>	X		X	X		X					
Key file		>	X		X	X		X					
Use websockets	X	X											
Use compression	X	X	>						X	X	X		
Data Protocol			X	X	X	(X)							
• WAGO Protocol			X	X	X								
• WAGO Protocol 1.5			X	X	X								
• Native MQTT			X	X	X	(X)							
• Sparkplug payload B			X		X								
Cache mode	X	X	X	X	X	X							
Last Will			X	X	X	X							
• Last Will Topic			>	>	>	>							X
• Last Will Message			>	>	>	>							X
• Last Will QoS			>	>	>	>							X
• Last Will Retain			>	>	(>)	>							X
Device info		X	>	>	>				X	X			
Device status		X	>	>	>				X	X			
Standard commands		X	>		>				X	X			
Application property template		X											

X: Visible and active
(X): Visible, but not active
>: Visible and active; dependent on other settings
(>): Visible, but not active; dependent on other settings

18.1.1.2.24 “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 147: 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).
Object ID	Enter here the object ID (sysOID).

Click the **[Submit]** button to apply the changes. The changes only take effect after restarting the controller. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

18.1.1.2.25 “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.

“SNMP v1/v2c Manager Configuration” Group

Table 148: WBM “Configuration of SNMP v1/v2c Parameters” Page – “SNMP v1/v2c Manager Configuration” Group

Parameters	Explanation
Protocol enabled	It is displayed the SNMP protocol for v1/v2c is enabled. The local community name is deleted when the protocol is disabled.
Local Community Name	Specify the community name for the SNMP manager configuration. 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. 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.”

Click the **[Submit]** button to apply the changes. 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!

“Actually configured Trap Receivers” Group

Table 149: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Actually Configured Trap Receivers” Group

Parameters	Meaning
Each configured trap receiver has its own area in the display. If no trap receiver has been configured, “(no trap receivers configured)” is displayed.	
IP Address	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: v1 or v2c (traps higher than v3 are displayed in a separate form).
Add new Trap Receiver	In this area, you can enter a new trap receiver.
IP Address	Specify the IP address for the new trap receiver (management station).
Community Name	Specify the community name for the new trap receiver configuration. The community name can be evaluated by the trap receiver. 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: v1 or v2c (traps higher than v3 are configured in a separate form).

Click the corresponding **[Delete]** button to delete an existing trap receiver.

Click the **[Add]** button to add a new trap receiver.

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!

18.1.1.2.26 “Configuration of SNMP v3 Users” Page

The general settings for SNMP v3 are shown on the “Configuration of SNMP v3 Users” page.

“Actually configured v3 Users” Group

Table 150: WBM “Configuration of SNMP v3” Page – “Actually configured v3 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 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”)
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”)
Privacy Key	The key for encryption of the SNMP message is displayed. If nothing is displayed, the “authentication key” is automatically used.
Notification Receiver IP	The IP address of a trap receiver for v3 traps is displayed. If no v3 traps are to be sent for this user, this field remains blank.
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.

Table 150: WBM “Configuration of SNMP v3” Page – “Actually configured v3 Users” Group

Parameters	Meaning
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”)
Authentication Key (min. 8 char.)	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”)
Privacy Key (min. 8 char.)	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.
Notification Receiver IP	Specify an IP address for a trap receiver for v3 traps. If no v3 traps are to be sent for this user, this field remains blank.

Click the respective **[Delete]** button to delete an existing user.

Click **[Add]** to add a new user.

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!

18.1.1.2.27 “WBM User Configuration” Page

The settings for user administration are displayed on the “WBM User Configuration” page.

“Change Passwords” 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 151: WBM “WBM User Configuration” Page – “Change Passwords” Group

Parameter	Explanation
Select User	Select the user (“User” or “Admin”) to whom you want to assign a new password.
Old Password	Enter the current password here for authentication.
New Password	Enter the new password here for the user selected under “Select User.” 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.

18.1.1.3 “Fieldbus” Tab

18.1.1.3.1 “OPC UA Status” Page

You can find the status information on the OPC UA service on the “OPC UA Status” page.

“OPC UA Server” Group

Table 152: WBM “OPC UA Status” Page – “OPC UA Server” Group

Parameter	Explanation
State	The current status (enabled / disabled) of the WAGO OPC UA server is displayed.
Version	The installed version of the WAGO OPC UA Server is displayed here.
License	Any existing OPC UA server license is displayed. Some features of the WAGO OPC UA server require a paid special license.

18.1.1.3.2 “OPC UA Configuration” Page

The settings for the OPC UA service are shown on the “OPC UA Configuration” page.

“General OPC UA Server Configuration” Group

Table 153: WBM “OPC UA Configuration” Page – “General OPC UA Server Configuration” Group

Parameter	Explanation	
Service enabled	Enable or disable the WAGO OPC UA Server here.	
Ctrl Configuration name	Enter the configuration names the controller contains in the PLC Open Device Set.	
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.	
Unlimited anonymous access	Access rights to the data provided by the server are set here.	
	Enabled	An unregistered user can view, read and write all variables.
	Disabled	Complete access to the data requires user logon with the appropriate rights.

Click the **[Submit]** button to apply the changes.

“OPC UA Endpoints” Group

Table 154: WBM “OPC UA Configuration” Page – “OPC UA Endpoints” Group

Parameter	Meaning
Security Policy - None	Enable or disable the OPC UA endpoint “None”. This allows an unsecured connection to the OPC UA server to be established.
Security Policy - Basic128Rsa15	Enable or disable the “Basic128Rsa15” security policy. **Note:** This policy is no longer classified as secure.
Security Policy - Basic256Sha256	The “Basic256Sha256” security policy allows a secure connection to be established with the OPC UA server.

Click the **[Submit]** button to apply the changes.

“OPC UA Security Settings” Group

Table 155: WBM Page “OPC UA Configuration” – “OPC UA Security Settings” Group

Parameter	Explanation	
Trust all clients	The verification is enabled or disabled here.	
	Enabled	A connection to all clients is permitted. → No security!
	Disabled	Connection is only allowed to clients with secure certificates.
URI Check Application	The URI check can be enable or disable here. A disabled URI check enables connection to an OPC server even if the URI on the server URI is different from the URI in the certificates.	
Error Certificate Time	The time can be enabled or disabled here. Certificates may have an expiration date. This date is checked against the current usage time on the device. The check cannot be run successfully if the time is incorrectly set on the device.	
Certificate Issuer Time Invalid	The time stamp check can be enabled or disabled here. CA certificates contain a validity time stamp from the manufacturer. This stamp is used when checking the time on the server hardware. If the time setting on the server hardware is incorrect or is missing entirely, the certificate may be indicated as invalid.	
Certificate Revocation Unknown	The accessibility check of the saving location for withdrawn certificates can be enabled or disabled here. Each certificate can have a location for withdrawn certificates. If network problems or other causes prevent access to the specified location, the certificate is not accepted.	
Certificate Issuer Revocation Unknown	The accessibility check of the storage location for withdrawn certificates can be enabled or disabled here. Each certificate of a certification location (CA certificate) can contain an entry for the withdrawn certificate saving location. If the location cannot be reached, the server will refuse the certificate.	

Click the **[Submit]** button to apply the changes.

18.1.1.3.3 “OPC UA Information Model” Page

You can find the settings for the OPC UA information module on the “OPC UA Information Model” page.
The page is only visible on 2nd generation controllers (750-821x/xxx-xxx) that support software components that are subject to a license check (runtime licenses).

“OPC UA Server Information Model” Group

Table 156: WBM “OPC UA Information Model” Page – “OPC UA Server Information Model” Group

Parameter	Meaning
Feature enabled	Enable or disable the OPC UA Server information model.
informationmodel.xml	Select an XML description file for the information model to be used. Using a specific information model requires an extended OPC UA license!

Click the **[Submit]** button to apply a change.

To transfer the selected description file to the controller, click the **[Upload]** button.

To delete the installed description file from the controller, click the **[Delete]** button. After deletion, the default PLC Open information model is used again.

18.1.1.3.4 “MODBUS Services Configuration” Page

The “Modbus Services Configuration” page displays the settings for various Modbus® services. The groups only appear if the ***e!****RUNTIME* system is enabled. Otherwise an information text is displayed.

“Modbus TCP Slave” Group

Table 157: WBM “Modbus Services Configuration” Page – “Modbus TCP” Group

Parameters	Explanation
Service active	Disable or enable the Modbus/TCP service.

Click the **[Submit]** button to apply the changes. The change takes effect immediately.

“Modbus UDP Slave” Group

Table 158: WBM “Modbus Services Configuration” Page – “Modbus UDP” Group

Parameters	Explanation
Service active	Disable/enable the Modbus UDP service.

Click the **[Submit]** button to apply the changes. The change takes effect immediately.

18.1.1.3.5 “BACnet …” Page

The WBM pages “BACnet Status”, “BACnet Configuration”, “BACnet Storage Location“, “BACnet Files” and “BACnet Diagnostic” are only fully functional for test purposes or with an installed license.

The BACnet functionality can only be used if the controller supports the ***e!****RUNTIME* runtime system and ***e!****RUNTIME* is used as the runtime system.

If you use the BACnet functionality for test purposes without a license, it is indicated by the “SYS” LED (see Section “Diagnostics” > “Fieldbus/System” Display Elements).

You can find a description of the WBM pages in the technical information on licensable “***e!****RUNTIME* BACnet/IP 300 (M)/600 (M)” functionality.

18.1.1.4 “Security” Tab

18.1.1.4.1 “OpenVPN / IPsec Configuration” Page

The “OpenVPN / IPsec Configuration” page displays the settings for OpenVPN and IPsec.

“OpenVPN” Group

Table 159: 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 160: 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!

18.1.1.4.2 “General Firewall Configuration” Page

The “General Firewall Configuration” page displays the global firewall settings.

“Global Firewall Parameter” Group

Table 161: 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.
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.

18.1.1.4.3 “Interface Configuration” Page

The individual interfaces for the firewall settings are displayed on the “Interface Configuration” page.

“Firewall Configuration Bridge <n> / VPN” 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 162: WBM “Interface Configuration” Page – “Firewall Configuration Bridge <n> / VPN” 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.	
ICMP echo limit per second	You can specify the maximum number of “ICMP pings” per second. “0” = “Disabled”	
ICMP burst limit (0 = disabled)	You can specify the maximum number of “ICMP echo bursts” per second. “0” = “Disabled”	
Service enabled	Telnet: This button is only displayed if Telnet is supported.	Enable or disable the firewall for the respective service. The services themselves must be enabled or disabled separately on the “Ports and Services” page.
	FTP	
	FTPS	
	HTTP	
	HTTPS	
	I/O-CHECK	
	PLC Runtime	
	PLC WebVisu – direct link (port 8080)	
	SSH	
	TFTP	
	BootP/DHCP	
	DNS	
	Modbus TCP	
	Modbus UDP	
	SNMP	
	OPC UA	
	PROFINET IO	

Click the **[Submit]** button to apply the change. The change takes effect immediately.

The firewall ports listed in the following table are open by default on controllers with telecontrol functionality. The corresponding telecontrol services can be executed via these ports without the firewall blocking their communication.

Table 163: Ports for Telecontrol Functionality

Protocol	Port
DNP3	20000
IEC 60870-5-104	2404
IEC 61850	102

18.1.1.4.4 “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 a default entry with the following values:

MAC address: 00:30:DE:00:00:00
MAC mask: ff:ff:ff:00:00:00

If you enable the 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 164: 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 165: 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.

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 166: WBM “Configuration of MAC Address Filter” Page – “MAC address filter whitelist” Group

Parameters	Explanation
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.

18.1.1.4.5 “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 167: WBM “Configuration of User Filter” Page – “User Filter” Group

<table>
<tr><th>Parameters</th><th colspan="2">Meaning</th></tr>
<tr><td>Policy</td><td colspan="2">This displays whether the network participant is permitted or excluded by the filter.</td></tr>
<tr><td>Source IP address</td><td colspan="2">The source IP address for the respective filter is displayed.</td></tr>
<tr><td>Source Netmask</td><td colspan="2">This displays the source netmask for the respective filter.</td></tr>
<tr><td>Source Port</td><td colspan="2">The source port number for the respective filter is displayed.</td></tr>
<tr><td>Destination IP address</td><td colspan="2">The destination IP address for the respective filter is displayed.</td></tr>
<tr><td>Destination Netmask</td><td colspan="2">The destination netmask for the respective filter is displayed.</td></tr>
<tr><td>Destination Port</td><td colspan="2">The destination port number for the respective filter is displayed.</td></tr>
<tr><td>Protocol</td><td colspan="2">The permitted protocols for the respective filter is displayed.</td></tr>
<tr><td>Input interface</td><td colspan="2">The permitted interfaces for the respective filter are displayed.</td></tr>
<tr><td>Add new user filter</td><td colspan="2">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.</td></tr>
<tr><td rowspan="3">Policy</td><td colspan="2">Select here whether the network devices is to be allowed or excluded by the filter.</td></tr>
<tr><td>Allow</td><td>The network device is permitted.</td></tr>
<tr><td>Drop</td><td>The network device is excluded.</td></tr>
<tr><td>Source IP address</td><td colspan="2">Enter here the source IP address for the new filter.</td></tr>
<tr><td>Source netmask</td><td colspan="2">Enter here the source network mask for the new filter.</td></tr>
<tr><td>Source port</td><td colspan="2">Enter here the source port address for the new filter.</td></tr>
<tr><td>Destination IP address</td><td colspan="2">Enter here the destination IP address for the new filter.</td></tr>
<tr><td>Destination subnet mask</td><td colspan="2">Enter here the destination network mask for the new filter.</td></tr>
<tr><td>Destination port</td><td colspan="2">Enter here the destination port address for the new filter.</td></tr>
</table>

Table 167: 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.

18.1.1.4.6 “Certificates” Page

On the “Certificates” page, you will find options to install or delete certificates and keys.

“Installed Certificates” Group

Table 168: 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 169: 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.

18.1.1.4.7 “Security Settings” Page

The network security settings are found on the “Security Settings” page.

“TLS Configuration” Group

Table 170: “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.”

18.1.1.4.8 “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 171: 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 172: 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.

18.1.1.5 “Diagnostic” Tab

18.1.1.5.1 “Diagnostic Information” Page

The settings for displaying diagnostic messages are shown on the “Diagnostic Information” page.

Table 173: WBM “Diagnostic Information” Page

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.

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.

18.1.2 Console-Based-Management (CBM)

18.1.2.1 “Information” Menu

This menu contains other submenus with information on the controller and network.

Table 174: “Information” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Controller Details	Opens a submenu with controller properties
2. Network Details	Opens a submenu with controller network and interface properties

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.1.1 “Information” > “Controller Details” Submenu

In this submenu, the controller properties are displayed.

Table 175: “Information” > “Controller Details” Submenu

Parameters	Explanation
Product Description	Controller identification
Order Number	Item number of the controller
License Information	Notification that the CODESYS runtime system is available
Firmware Revision	Firmware status

To return to the higher-level menu, press **[Q]** or **[Return]**.

18.1.2.1.2 “Information” > “Network Details” Submenu

In this submenu, the network and interface properties of the controller are displayed.

If the EHERNET interfaces are operated in “Switched” mode, a common table (“X1/X2”) is displayed for both connections.
If the EHERNET interfaces are operated in “Separated” mode, an individual table (“X1” / “X2”) is displayed for each connection.

Table 176: “Information” > “Network Details” Submenu

Parameters	Explanation
State	Status of the ETHERNET interface (enabled/disabled)
Mac Address	MAC address identifies and addresses the controller
IP Address	Current IP address of the controller and (in brackets) the reference type (static/bootp/dhcp)
Subnet Mask	Current subnet mask of the controller

To return to the higher-level menu, press **[Q]** or **[Return]**.

18.1.2.2 “PLC Runtime” Menu

This menu contains other submenus with information and settings for the runtime system.

Table 177: “PLC Runtime” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Information	Opens a submenu with information on the runtime system
2. General Configuration	Opens a submenu with settings for the runtime system
3. WebVisu	Opens a submenu with settings for the Web visualization

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.2.1 “PLC Runtime” > “Information” Submenu

This submenu contains other submenus with information on the runtime system and PLC program.
Menu items 2 … 6 only appear if CODESYS V2 is set as the runtime system.

Table 178: “PLC Runtime” > “Information” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Runtime Version	Opens a submenu to display the runtime version
2. Webserver Version	Opens a submenu to display the Webserver version
3. State	Opens a submenu to display the PLC operating state
4. Number of Tasks	Opens a submenu to display the number of tasks in the PLC program
5. Project Details	Opens a submenu to display the PLC program project information
6. Tasks	Opens a submenu to display the tasks in the PLC program

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.2.2 “Information” > “Runtime Version” Submenu

In this submenu, the runtime version is displayed.

Table 179: “PLC Runtime” > “Information” > “Runtime Version” Submenu

Parameters	Explanation
Version	The version of the currently enabled runtime system is shown. If the runtime system is disabled, “None” is displayed.

To return to the higher-level menu, press **[Q]** or **[Return]**.

18.1.2.2.3 “Information” > “Webserver Version” Submenu

In this submenu, the Webserver version is displayed.
The submenu only appears when CODESYS V2 is enabled as the runtime system.

Table 180: “PLC Runtime” > “Information” > “Webserver Version” Submenu

Parameters	Explanation
Version	The Webserver version is displayed.

To return to the higher-level menu, press **[Q]** or **[Return]**.

18.1.2.2.4 “Information” > “State” Submenu

In this submenu, the PLC operating state is displayed.
The submenu only appears when CODESYS V2 is enabled as the runtime system.

Table 181: “PLC Runtime” > “Information” > “State” Submenu

Parameters	Explanation	
State	The PLC operating state is shown.	
	STOP	PLC program is not executed.
	RUN	PLC program is executed.

To return to the higher-level menu, press **[Q]** or **[Return]**.

18.1.2.2.5 “Information” > “Number of Tasks” Submenu

In this submenu, the number of tasks in the PLC program are displayed. The submenu only appears when CODESYS V2 is enabled as the runtime system.

Table 182: “PLC Runtime” > “Information” > “Number of Tasks” Submenu

Parameters	Explanation
Number of Tasks	The number of tasks in the PLC program is shown.

To return to the higher-level menu, press **[Q]** or **[Return]**.

18.1.2.2.6 “Information” > “Project Details” Submenu

In this submenu, project information from the PLC program is displayed. The submenu only appears when CODESYS V2 is enabled as the runtime system and the program is executed.

Table 183: “PLC Runtime” > “Information” > “Project Details” Submenu

Parameters	Explanation
Date	Display of project information that the programmer entered in the PLC program (in the programming software under Project > Project Information ...) Descriptive text with up to 1024 characters is displayed under “Description”.
Title	
Version	
Author	
Description	

To return to the higher-level menu, press **[Q]** or **[Return]**.

18.1.2.2.7 “Information” > “Tasks” Submenu

In this submenu, tasks from the PLC program are displayed. An entry is generated for each task.
The submenu only appears when CODESYS V2 is enabled as the runtime system.

Table 184: “PLC Runtime” > “Information” > “Tasks” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
n. Task n	Opens a submenu with information on the selected task

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.2.8 “Tasks” > “Task n” Submenu

In this submenu, information on the selected task is displayed.
The submenu only appears when CODESYS V2 is enabled as the runtime system.

Table 185: “PLC Runtime” > “Information” > “Tasks” > “Task n” Submenu

Parameters	Explanation
Cycle count	Number of task cycles since the system start
Cycle time (µsec)	Currently measured task cycle time for the task
Cycle time min (µsec)	Minimum task cycle time for the task since the system start
Cycle time max (µsec)	Maximum task cycle time for the task since the system start
Cycle time avg (µsec)	Average task cycle time since the system start
Status	Task status (e.g., RUN, STOP)
Mode	Task execution mode (e.g., in cycles)
Priority	Set task priority
Interval (msec)	Set task interval

To return to the higher-level menu, press **[Q]** or **[Return]**.

18.1.2.2.9 “PLC Runtime” > “General Configuration” Submenu

This submenu contains other submenus with general settings for the runtime system.

Table 186: “PLC Runtime” > “General Configuration” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. PLC Runtime Version	Opens a submenu for the CODESYS runtime system settings
2. Home Dir On SD Card	Opens a submenu for the home directory settings

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.2.10 “General Configuration” > “PLC Runtime Version” Submenu

In this submenu, select which PLC runtime system is enabled.

Table 187: “PLC Runtime” > “General Configuration” > “PLC Runtime Version” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. None	No runtime system is enabled.
2. CODESYS 2	The CODESYS V2 runtime system is enabled.
3. e!RUNTIME	The ***e!****RUNTIME* runtime system is enabled.

Note

All data is deleted when switching the runtime system!
The runtime system’s home directory is completely deleted when switching the runtime system!

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.2.11 “General Configuration” > “Home Dir On SD Card” Submenu

In this submenu, define if the home directory for the runtime system should be moved to the memory card.

Table 188: “PLC Runtime” > “General Configuration” > “Home Dir On SD Card” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Enable	The home directory is moved to the memory card.
2. Disable	The home directory is stored in the internal memory.

Note

Insert a memory card before switching the home directory!

When moving the home directory to the memory card, insert a memory card formatted to support file system. Only the first partition of a memory card can be accessed at /media/sd and can be used as the home directory.

Note

Perform a reset before switching the home directory!
Stop IEC-61131 applications in use before switching the home directory of the runtime system.
Restore the device to its initial state using the “Reset” function. Any boot project is deleted.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.2.12 “PLC Runtime” > “WebVisu” Submenu

This submenu contains information and settings for the Web visualization.

Table 189: “PLC Runtime” > “WebVisu” Submenu

<table>
<tr><th>Menu Item</th><th colspan="2">Submenu Item / Explanation</th></tr>
<tr><td>0. Back to …</td><td colspan="2">Back to the higher-level menu</td></tr>
<tr><td>1. CODESYS 2 Webserver State</td><td colspan="2">The status of the CODESYS V2 Webserver is displayed.</td></tr>
<tr><td>2. e!RUNTIME Webserver State</td><td colspan="2">The status of the <b><i>e!</i></b><i>RUNTIME</i> Webserver is displayed.</td></tr>
<tr><td rowspan="4">3. Default Webserver</td><td colspan="2">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.</td></tr>
<tr><td>0. Back to …</td><td>Back to the higher-level menu</td></tr>
<tr><td>1. Web-based Management</td><td>The Web-based Management is displayed.</td></tr>
<tr><td>2. CODESYS WebVisu</td><td>The web visualization of the runtime system is displayed.</td></tr>
</table>

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.3 “Networking” Menu

This menu contains other submenus with settings for the network configuration.

Table 190: “Networking” Menu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. Host/Domain Name	Opens a submenu with setting options for the general TCP/IP parameters
2. TCP/IP	Opens a submenu with TCP/IP settings for the ETHERNET interfaces
3. Ethernet	Opens a submenu with settings for the ETHERNET configuration

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.3.1 “Networking” > “Host/Domain Name” Submenu

This submenu contains the “Hostname” and “Domain Name” submenu with setting options for the general TCP/IP parameters.

Table 191: “Networking” > “Host/Domain Name” Submenu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. Hostname	Opens a submenu with the hostname settings In addition to the menu item, the configured and current hostname are displayed.
2. Domain Name	Opens a submenu hostname settings In addition to the menu item, the configured and current domain name are displayed.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.3.2 “Host/Domain Name” > “Hostname” Submenu

In this submenu, you can set the hostname of the controller.

Table 192: “Networking” > “Hostname” Submenu

Parameters	Explanation
Enter new Hostname	Enter here the hostname of the controller to be used if the network interface is changed to a static IP address or if no hostname is transmitted with a DHCP response.

Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.3.3 “Host/Domain Name” > “Domain Name” Submenu

In this submenu, you can set the domain name of the controller.

Table 193: “Networking” > “Host/Domain Name” > “Domain Name” Submenu

Parameters	Explanation
Enter new Domain Name	Enter the domain name. The default entry is “localdomain.lan”.

Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.3.4 “Networking” > “TCP/IP” Submenu

This submenu contains other submenus with the TCP/IP settings for the ETHERNET interfaces.

Table 194: “Networking” > “TCP/IP” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. IP Address	Opens a submenu with settings for the IP address(es)
2. Default Gateway	Opens a submenu with settings for the default gateway
3. DNS Server	Opens a submenu with settings for the DNS server(s)

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.3.5 “TCP/IP” > “IP Address” Submenu

This submenu contains other submenus with settings for the ETHERNET interfaces.

The submenu only appears if the controller is operated in “Separated” mode. If the controller is operated in “Switched” mode, then the “IP Address” > “X1” submenu is displayed directly.

Table 195: “Networking” > “IP Address” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. X1	Opens a submenu with settings for the X1 interface
2. X2	Opens a submenu with settings for the X2 interface

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.3.6 “IP Address” > “Xn“ Submenu

This submenu contains the settings for the selected interface.

Table 196: “Networking” > “TCP/IP” > “IP Address” Submenu > “Xn”

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Type of IP Address Configuration	Select a static or dynamic IP address.	
	0. Back to …	Back to the higher-level menu
	1. Static IP	Static IP addressing When selecting static addressing, the IP address and subnet mask are then retrieved.
	2. DHCP	Dynamic IP addressing
	3. BootP	Dynamic IP addressing
2. IP Address	Enter here a static IP address.	
3. Subnet Mask	Enter the subnet mask.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.3.7 “TCP/IP” > “Default Gateway” Submenu

This submenu contains other submenus with settings for the default gateway.

Table 197: “Networking” > “TCP/IP” > “Default Gateway” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Default Gateway 1	Opens a submenu with settings for default gateway 1 In addition to the menu item, the current status of the gateway is displayed.
2. Default Gateway 2	Opens a submenu with settings for default gateway 2 In addition to the menu item, the current status of the gateway is displayed.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.3.8 “Default Gateway” > “Default Gateway n” Submenu

This submenu contains the settings for the selected gateway.

Table 198: “Networking” > “TCP/IP” > “Default Gateway” > “Default Gateway n” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Set here whether the selected default gateway is to be used.	
	0. Back to …	Back to the higher-level menu
	1. Disabled	The default gateway is not used.
	2. Enabled	The default gateway is used.
2. Gateway IP Address	Enter the address of the default gateway.	
3. Gateway Metric	Set here a number as the metric. The default value for the metric is 20, the lowest value is 0, the highest value is 4.294.967.295.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.3.9 “TCP/IP” > “DNS Server” Submenu

This submenu contains the settings for the DNS server.

Table 199: “Networking” > “TCP/IP” > “DNS Server” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
n. DNS Server n	The addresses of the defined DNS servers are displayed. Other submenus are available for the server entered.	
	0. Back to …	Back to the higher-level menu
	1. Edit	You can change the selected DNS server address.
	2. Delete	You can delete the selected DNS server address.
(n+1). Add new DNS Server	Add additional DNS server addresses. You can enter 10 addresses.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.3.10 “Networking” > “Ethernet” Submenu

This submenu contains other submenus with settings for the ETHERNET configuration.

Table 200: “Networking” > “Ethernet” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Switch Configuration	Opens a submenu with settings for the Switch Configuration
2. Ethernet Ports	Opens a submenu with settings for the ETHERNET interfaces

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.3.11 “Ethernet” > “Switch Configuration” Submenu

This submenu contains the settings for the Switch configuration.

Table 201: “Networking” > “Ethernet” > “Switch Configuration” Submenu

Submenu	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Network interfaces	Enable or disable the switch.	
	0. Back to …	Back to the higher-level menu
	1. Separated	Each interface is operated with its own IP address.
	2. Switched	Both interfaces are operated with one IP address.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.3.12 “Ethernet” > “Ethernet Ports” Submenu

This submenu contains other submenus with settings for the ETHERNET interfaces.

Table 202: “Networking” > “Ethernet” > “Ethernet Ports” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Interface X1	Opens a submenu with settings for the X1 interface
2. Interface X2	Opens a submenu with settings for the X2 interface

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.3.13 “Ethernet Ports” > “Interface Xn” Submenu

This submenu contains the settings for the selected ETHERNET interface.

Table 203: “Networking” > “Ethernet” > “Ethernet Ports” > “Interface Xn” Submenu

Submenu	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Port	Set here whether the selected port is to be used.	
	0. Back to …	Back to the higher-level menu
	1. Disabled	The port is not used.
	2. Enabled	The port is used.
2. Autonegotiation	Set here whether the Autonegotiation function is enabled for the selected port.	
	0. Back to …	Back to the higher-level menu
	1. Disabled	Autonegotiation is disabled.
	2. Enabled	Autonegotiation is enabled.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.4 “Firewall” Menu

This menu contains other submenus for the firewall functionality settings.

Table 204: “Firewall” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. General Configuration	Opens a submenu with general firewall settings
2. MAC Address Filter	Opens a submenu with MAC address filter settings
3. User Filter	Opens a submenu with user filter settings

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.4.1 “Firewall” > “General Configuration” Submenu

This submenu contains the general settings for the firewall.

Table 205: “Firewall” > “General Configuration” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Firewall enabled entirely	Enables/disables the complete functionality of the firewall.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Firewall is enabled.
	2. Disable	Firewall is disabled.
2. ICMP echo broadcast protection	Enable or disable the “ICMP echo broadcast” protection.	
	0. Back to …	Back to the higher-level menu
	1. Enable	“ICMP echo broadcast” protection is enabled.
	2. Disable	“ICMP echo broadcast” protection is disabled.
3. Max UDP connections per second	You can specify the maximum number of UDP connections per second. “0” = “Disabled”	
4. Max TCP connections per second	You can specify the maximum number of TCP connections per second. “0” = “Disabled”	
5. Interface VPN	Opens a submenu with firewall settings on the IP level for the selected interface	
6. Interface WAN		
7. Interface X1		
8. Interface X2		

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.4.2 “General Configuration” > “Interface xxx” Submenu

This submenu contains the firewall settings on the IP level for the selected interface.

Table 206: “Firewall” > “General Configuration” > “Interface xxx” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Interface state	Enable or disable the firewall for the selected interface.	
	0. Back to …	Back to the higher-level menu
	1. Open	The firewall for the selected interface is disabled.
	2. Filtered	The firewall for the selected interface is enabled.
2. ICMP Policy	Enable or disable the “ICMP echo” protection for the respective interface.	
	0. Back to …	Back to the higher-level menu
	1. Accept	The “ICMP echo” protection is disabled.
	2. Drop	The “ICMP echo” protection is enabled.
3. ICMP Limit	You can specify the maximum number of “ICMP pings” per second. “0” = “Disabled”	
4. ICMP Burst	You can specify the maximum number of “ICMP echo bursts” per second. “0” = “Disabled”	
5. Telnet	Enable or disable the firewall for the respective service. The services themselves must be enabled or disabled separately on the “Ports and Services” page.	
6. FTP		
7. FTPS		
8. HTTP		
9. HTTPS		
10. I/O-CHECK		
11. PLC Runtime		
12. PLC WebVisu – direct link (port 8080)		
13. SSH		
14. TFTP		
15. BootP/DHCP		
16. DNS		
17. Modbus TCP		
18. Modbus UDP		
19. SNMP		

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

The firewall ports listed in the following table are open by default on controllers with telecontrol functionality. The corresponding telecontrol services can be executed via these ports without the firewall blocking their communication.

Table 207: Ports for Telecontrol Functionality

Protocol	**Port**
DNP3	20000
IEC 60870-5-104	2404
IEC 61850	102

18.1.2.4.3 “Firewall” > “MAC Address Filter” Submenu

This submenu contains the settings for the MAC address filter.

Table 208: “Firewall” > “MAC Address Filter” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Global MAC address filter state	Enable or disable the global MAC address filter.	
	0. Back to …	Back to the higher-level menu
	1. Filtered	The global MAC address filter is enabled.
	2. Open	The global MAC address filter is disabled.
2. MAC address filter whitelist	Opens a submenu to edit the MAC address filter whitelist	
3. MAC address filter state X1	Enable or disable the MAC address filter for the X1 interface.	
	0. Back to …	Back to the higher-level menu
	1. Open	The MAC address filter for the X1 interface is disabled.
	2. Filtered	The MAC address filter for the X1 interface is enabled.
4. MAC address filter state X2	Enable or disable the MAC address filter for the X2 interface.	
	0. Back to …	Back to the higher-level menu
	1. Open	The MAC address filter for the X2 interface is disabled.
	2. Filtered	The MAC address filter for the X2 interface is enabled.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.4.4 “MAC Address Filter” > “MAC address filter whitelist” Submenu

This submenu displays all available filter entries.

Table 209: “Firewall” > “MAC Address Filter” > “MAC address filter whitelist” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Add new	Opens a submenu to add a new filter entry You can enter 10 filters.
2. Previous page	Displays the previous page of the list (if more than one page is filled)
3. Next Page	Displays the next page of the list (if more than one page is filled)
(n + 3.) No (n):	Opens a submenu to edit an existing filter entry

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.4.5 “MAC address filter whitelist” > “Add new / No (n)” Submenu

In this submenu, you can create, change or delete filter entries.

Table 210: “Firewall” > “MAC Address Filter” > “MAC address filter whitelist” > “Add new / No (n)” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. MAC address	Enter the MAC address.	
2. MAC mask	Enter the MAC mask.	
3. Filter state	Enable or disable the filter.	
	0. Back to …	Back to the higher-level menu
	1. on	The filter is enabled.
	2. off	The filter is disabled.
4. accept	To apply the changes for the selected filter entry, choose this menu item.	
5. delete	To delete the selected filter entry, choose this menu item.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.4.6 “Firewall” > “User Filter” Submenu

This submenu displays all available filter entries.

Table 211: “Firewall” > “User Filter” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Add new	Opens a submenu to add a new filter entry
2. Previous page	Displays the previous page of the list (if more than one page is filled)
3. Next Page	Displays the next page of the list (if more than one page is filled)
(n + 3.) No (n):	Opens a submenu to edit an existing filter entry

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.4.7 “User Filter” > “Add New / No (n)” Submenu

In this submenu, you can create, change or delete filter entries.

Table 212: “Firewall” > “User Filter” > “Add New / No (n)” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Policy	Select here whether the network devices is to be allowed or excluded by the filter.	
	0. Back to …	Back to the higher-level menu
	1. Allow	The network device is permitted.
	2. Drop	The network device is excluded.
2. Source IP address	Enter the source IP address.	
3. Source netmask	Enter the source network mask.	
4. Source port	Enter the source port number.	
5. Destination IP address	Enter the destination IP address.	
6. Destination netmask	Enter here the destination netmask.	
7. destination port	Enter the destination port number.	
8. protocol	Select the permitted protocols.	
	0. Back to …	Back to the higher-level menu
	1. tcp	The TCP protocol is permitted.
	2. udp	The UDP protocol is permitted.
	3. tcp & udp	Both protocols are permitted.
9. interface	Select the permitted interfaces.	
	0. Back to …	Back to the higher-level menu
	1. all	All interfaces are permitted.
	2. VPN	The VPN interface is permitted.
	3. WAN	The WAN interface is permitted.
	4. X1	The X1 interface is permitted.
	5. X2	The X2 interface is permitted.
10. state	Enable or disable the filter.	
	0. Back to …	Back to the higher-level menu
	1. on	The filter is enabled.
	2. off	The filter is disabled.
11. accept	To apply the changes for the selected filter entry, choose this menu item.	
12. delete	To delete the selected filter entry, choose this menu item.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.5 “Clock” Menu

This menu contains other submenus for the date and time settings.

Table 213: “Clock” Menu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Date on device (local)	Set date.	
2. Time on device (local)	Set local time.	
3. Time on device (UTC)	Set GMT time.	
4. Clock Display Mode	Select the display format for the time.	
	0. Back to …	Back to the higher-level menu
	1. 24 hours	The time is displayed in 24-hour format.
	2. 12 hours	The time is displayed in 12-hour format.
5. Timezone	Specify the appropriate time zone for your location. Basic setting:	
	0. Back to …	Back to the higher-level menu
	1. AST/ADT	“Atlantic Standard Time,” Halifax
	2. EST/EDT	“Eastern Standard Time,” New York, Toronto
	3. CST/CDT	“Central Standard Time,” Chicago, Winnipeg
	4. MST/ MDT	“Mountain Standard Time,” Denver, Edmonton
	5. PST/PDT	“Pacific Standard Time”, Los Angeles, Whitehouse
	6. GMT/BST	Greenwich Mean Time,“ GB, P, IRL, IS, …
	7. CET/ CEST	“Central European Time,” B, DK, D, F, I, CRO, NL, …
	8. EET/ EEST	“East European Time,” BUL, FI, GR, TR, …
	9. CST	“China Standard Time”
	10. JST	“Japan/Korea Standard Time”
6. TZ String	Enter the name of your time zone or country and town if the time zone is not available for selection using the “Timezone” parameter.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.6 “Administration” Menu

This menu contains settings for controller administration.

Table 214: “Administration” Menu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Users	Opens a submenu with settings for the user passwords	
2. Create Image	Opens a submenu for creating a bootable image	
3. Owner of Serial Interface	Select the serial interface assignment.	
	0. Back to …	Back to the higher-level menu
	1. Linux Console	The serial interface is assigned to the Linux® console.
	2. Unassigned	The serial interface is not assigned and is available for applications or CODESYS.
4. Reboot Controller	Restart the controller following a security challenge.	
	0. Back to …	Back to the higher-level menu
	1. Reboot	Restarts the controller

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.6.1 “Administration” > “Users” Submenu

This submenu contains settings for the user passwords.

Table 215: “Administration” > “Users” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. user	Enter a new password for the “user” user.
2. admin	Enter a new password for the “admin” user.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.6.2 “Administration” > “Create Image” Submenu

This submenu contains the selection for creating the image.

In addition to the menu item for the enabled storage medium, the current status is displayed.

Table 216: “Administration” > “Create Image” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. SD Card	To create an image on the memory card, select this menu item. Enter the reserved memory size in another step. This menu item only appears if the memory card is inserted.
2. Internal Flash	To create an image on the internal memory, select this menu item.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.7 "Package Server" Menu

This menu contains other submenus with functions for firmware backup and restore, as well as information and setting options for the current system partition.

Table 217: "Package Server" Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Firmware Backup	Opens a submenu with functions for the firmware backup
2. Firmware Restore	Opens a submenu with functions for the firmware restore
3. System Partition	Opens a submenu with information and setting options for the current system partition

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.7.1 "Package Server" > "Firmware Backup" Submenu

This submenu contains a selection option for the data to be saved.

The submenu only appears if a memory card is inserted that does not contain a bootable system. Otherwise, a message is displayed.

Table 218: "Package Server" > "Firmware Backup" Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. All	All data is saved.
2. PLC Runtime project	The PLC runtime project is saved.
3. Settings	The controller settings are saved.
4. System	The controller operating system is saved.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

You are taken to the following submenu after making the selection.

18.1.2.7.2 “Firmware Backup” > “Auto Update Feature” Submenu

This submenu contains a setting option for the Auto Update function.

The submenu only appears if the data for the firmware backup has been selected.

Table 219: “Package Server” > “Firmware Backup” > “Auto Update Feature” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. No	The Auto Update function is OFF for the selected data.
2. Yes	The Auto Update function is ON for the selected data.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

You are taken to the following submenu after making the selection.

18.1.2.7.3 “Firmware Backup” > “Destination” Submenu

This submenu contains a selection option for the backup destination drive.

Table 220: “Package Server” > “Firmware Backup” > “Auto Update Feature” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. SD Card	The selected data is copied to the memory card.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

The copy progress is displayed during the backup process.

18.1.2.7.4 “Package Server” > “Firmware Restore” Submenu

This submenu contains a selection option for the restore source drive.

In addition to the enabled partition, the current status is displayed.

Table 221: “Package Server” > “Firmware Restore” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. SD Card	The data is copied from the memory card.
2. Internal Flash	The data is copied from the internal memory.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

You are taken to the following submenu after making the selection.

18.1.2.7.5 “Firmware Restore” > “Select Package” Submenu

This submenu contains a selection option for the data to be restored.

Table 222: “Package Server” > “Firmware Restore” > “Select Package” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. PLC Runtime project	The PLC runtime project is loaded.
2. Settings	The controller settings are loaded.
3. System	The controller operating system is loaded.
4. System + Setting	The controller operating system and settings are loaded.
5. All	All data is loaded.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

The copy progress is displayed during the restore process.

18.1.2.7.6 “Package Server” > “System Partition” Submenu

This submenu contains information and setting options for the current system partition.

Table 223: “Package Server” > “System Partition” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Current active partition	The partition currently in use is displayed.
2. Set inactive NAND partition active	Select this menu item to start the system from a different partition at the next controller reboot.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.8 “Mass Storage” Menu

This menu contains information on the internal flash memory and, if inserted, on the external memory card.

In addition to the menu item, the status is displayed for the enabled partition.

Table 224: “Mass Storage” Menu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. SD Card	Opens a submenu with information on the memory card and its formatting This menu item only appears if a memory card is inserted in the controller.
2. Internal Flash	Opens a submenu with information on the internal flash memory

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.8.1 “Mass Storage” > “SD Card” Submenu

This submenu contains information on the external memory card and its formatting.

This submenu only appears if a memory card is inserted in the controller.

Table 225: “Mass Storage” > “SD Card” Menu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. Show information	Displays information on the memory card
2. FAT format medium	To format the memory card in FAT format, select this menu item. Then specify a volume name.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.9 “Software Uploads” Menu

This menu contains choices and settings for the device update.

You can select fieldbus software, program licenses and update scripts, for example, for transfer from a PC to the controller.
You can also enable transmitted packages or delete from the controller.

18.1.2.10 “Ports and Services” Menu

This submenu contains other submenus with settings for the respective services.

Table 226: “Ports and Services” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Telnet	Opens a submenu with settings for the Telnet service
2. FTP	Opens a submenu with settings for the FTP service
3. FTPS	Opens a submenu with settings for the FTPS service
4. HTTP	Opens a submenu with settings for the HTTP service
5. HTTPS	Opens a submenu with settings for the HTTPS service
6. NTP	Opens a submenu with settings for the NTP service
7. SSH	Opens a submenu with settings for the SSH server
8. TFTP	Opens a submenu with settings for the TFTP server
9. DHCPD	Opens a submenu with settings for the DHCPD service
10. DNS	Opens a submenu with settings for the DNS service
11. IOCHECK PORT	Opens a submenu with settings for the WAGO-I/O-CHECK port
12. Modbus TCP	Opens a submenu with settings for the Modbus TCP service
13. Modbus UDP	Opens a submenu with settings for the Modbus UDP service
14. OPC UA	Opens a submenu with settings for the OPC UA service
15. PLC Runtime Services	Opens a submenu with settings for the PLC runtime system services

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.1 “Ports and Services” > “Telnet” Submenu

This submenu contains the settings for the Telnet service.

Table 227: “Ports and Services” > “Telnet” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the Telnet service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The Telnet service is enabled.
	2. Disable	The Telnet service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.2 “Ports and Services” > “FTP” Submenu

This submenu contains the settings for the FTP service.

Table 228: “Ports and Services” > “FTP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the FTP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The FTP service is enabled.
	2. Disable	The FTP service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.3 “Ports and Services” > “FTPS” Submenu

This submenu contains the settings for the FTPS service.

Table 229: “Ports and Services” > “FTPS” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the FTPS service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The FTPS service is enabled.
	2. Disable	The FTPS service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.4 “Ports and Services” > “HTTP” Submenu

This submenu contains the settings for the HTTP service.

Table 230: “Ports and Services” > “HTTP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the HTTP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The HTTP service is enabled.
	2. Disable	The HTTP service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.5 “Ports and Services” > “HTTPS” Submenu

This submenu contains the settings for the HTTPS service.

Table 231: “Ports and Services” > “HTTPS” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the HTTPS service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The HTTPS service is enabled.
	2. Disable	The HTTPS service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.6 “Ports and Services” > “NTP” Submenu

This submenu contains the settings for the NTP service.

Table 232: “Ports and Services” > “NTP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the NTP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The NTP service is enabled.
	2. Disable	The NTP service is disabled.
2. Port	Enter the port number of the NTP server.	
3. Time Server 1	Enter here the IP addresses of up to 4 time servers. Time server No. 1 is requested first of all. If no data can be accessed via time server No. 1, time server No. 2 is requested.	
4. Time Server 2		
5. Time Server 3		
6. Time Server 4		
7. Update Time	Specify here the update interval of the time server.	
8. Issue immediate update	To update the time immediately, irrespective of the update interval, select this menu item.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.10.7 “Ports and Services” > “SSH” Submenu

This submenu contains the settings for the SSH service.

Table 233: “Ports and Services” > “SSH” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	You can enable/disable the SSH server.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The SSH server is enabled.
	2. Disable	The SSH server is disabled.
2. Port	Enter the port number.	
3. Allow root login	You can enable or inhibit root access.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Root access is permitted.
	2. Disable	Root access is not permitted.
4. Allow password login	Enable or disable the password query function.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Password query is enabled.
	2. Disable	Password query is disabled.
5. Status of firewalling	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.8 “Ports and Services” > “TFTP” Submenu

This submenu contains the settings for the TFTP service.

Table 234: “Ports and Services” > “TFTP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable or disable the TFTP server.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The TFTP server is enabled.
	2. Disable	The TFTP server is disabled.
2. Transfer Directory	Specify here the path for downloading the server directory.	
3. Status of firewalling	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.10.9 “Ports and Services” > “DHCPD” Submenu

This submenu contains the settings for the DHCPD service.

Table 235: “Ports and Services” > “DHCPD” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. DHCPD firewalling	Opens a submenu with firewall settings for the this service for the interfaces
2. X1	Opens a submenu with the DHCPD settings for the selected interface
3. X2	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.10 “DHCPD” > “Xn” Submenu

This submenu contains the settings for the DHCPD service for the selected interface.

Table 236: “Ports and Services” > “DHCPD” > “Xn” Submenu

<table>
<tr><th>Menu Item</th><th colspan="2">Submenu Item / Explanation</th></tr>
<tr><td>0. Back to …</td><td colspan="2">Back to the higher-level menu</td></tr>
<tr><td rowspan="4">1. State</td><td colspan="2">Enable/disable the DHCPD service for the Xn interface.</td></tr>
<tr><td>0. Back to …</td><td>Back to the higher-level menu</td></tr>
<tr><td>1. Enable</td><td>The DHCPD service is enabled.</td></tr>
<tr><td>2. Disable</td><td>The DHCPD service is disabled.</td></tr>
<tr><td>2. Range</td><td colspan="2">Enter a range of available IP addresses.</td></tr>
<tr><td>3. Lease Time (min)</td><td colspan="2">Specify the lease time here in seconds. 120 seconds are entered by default.</td></tr>
<tr><td>4. Add static hostname</td><td colspan="2">Enter a new static assignment of MAC ID to IP address,
e.g., “01:02:03:04:05:06=192.168.1.20” or “hostname=192.168.1.20”.
You can enter 10 assignments.</td></tr>
<tr><td rowspan="4">(5 + n). Static Host (n)</td><td colspan="2">This displays the static assignments.</td></tr>
<tr><td>0. Back to …</td><td>Back to the higher-level menu</td></tr>
<tr><td>1. Edit</td><td>Opens a submenu to change the selected assignment</td></tr>
<tr><td>2. Delete</td><td>Deletes the selected assignment</td></tr>
</table>

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.10.11 “Ports and Services” > “DNS” Submenu

This submenu contains the settings for the DNS service.

Table 237: “Ports and Services” > “DNS” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the DNS service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The DNS service is enabled.
	2. Disable	The DNS service is disabled.
2. Mode	Select the operating mode of the DNS server.	
	0. Back to …	Back to the higher-level menu
	1. Proxy	The requests are buffered to optimize throughput.
	2. Relay	All requests are routed directly.
3. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	
4. Add static hostname	Enter a new static assignment of IP address to hostname, e.g., “192.168.1.20:hostname”. You can enter 10 assignments.	
(5 + n). Static Host (n)	This displays the static assignments.	
	0. Back to …	Back to the higher-level menu
	1. Edit	Opens a submenu to change the selected assignment
	2. Delete	Deletes the selected assignment

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.10.12 “Ports and Services” > “IOCHECK PORT” Submenu

This submenu contains settings for the WAGO-I/O-*CHECK* port.

Table 238: “Ports and Services” > “IOCHECK PORT” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the WAGO-I/O-*CHECK* port.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The WAGO-I/O-*CHECK* port is enabled.
	2. Disable	The WAGO-I/O-*CHECK* port is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.13 “Ports and Services” > “Modbus TCP” Submenu

This submenu contains the settings for the Modbus TCP service.

Table 239: “Ports and Services” > “Modbus TCP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Disable or enable the Modbus TCP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The Modbus TCP service is enabled.
	2. Disable	The Modbus TCP service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.14 “Ports and Services” > “Modbus UDP” Submenu

This submenu contains the settings for the Modbus UDP service.

Table 240: “Ports and Services” > “Modbus UDP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Disable/enable the Modbus UDP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The Modbus UDP service is enabled.
	2. Disable	The Modbus UDP service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.15 “Ports and Services” > “OPC UA” Submenu

This submenu contains the settings for the OPC UA service.

Table 241: “Ports and Services” > “OPC UA” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Disable/enable the OPC UA service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The OPC UA service is enabled.
	2. Disable	The OPC UA service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.16 "…" > "Firewall Status" Submenu

This submenu contains firewall settings for the selected service.

Table 242: "Ports and Services" > "Firewall Status" Submenu

<table>
<tr><th>Menu Item</th><th colspan="2">Submenu Item / Explanation</th></tr>
<tr><td>0. Back to …</td><td colspan="2">Back to the higher-level menu</td></tr>
<tr><td rowspan="4">1. VPN</td><td colspan="2">Enable or disable the firewall for the VPN interface and respective service.</td></tr>
<tr><td>0. Back to …</td><td>Back to the higher-level menu</td></tr>
<tr><td>1. open</td><td>Data traffic via the VPN interface is permitted.</td></tr>
<tr><td>2. close</td><td>Data traffic via the VPN interface is not permitted.</td></tr>
<tr><td rowspan="4">2. WAN</td><td colspan="2">Enable or disable the firewall for the WAN interface and respective service.</td></tr>
<tr><td>0. Back to …</td><td>Back to the higher-level menu</td></tr>
<tr><td>1. open</td><td>Data traffic via the WAN interface is permitted.</td></tr>
<tr><td>2. close</td><td>Data traffic via the WAN interface is not permitted.</td></tr>
<tr><td rowspan="4">3. X1</td><td colspan="2">Enable or disable the firewall for the X1 interface and respective service.</td></tr>
<tr><td>0. Back to …</td><td>Back to the higher-level menu</td></tr>
<tr><td>1. open</td><td>Data traffic via the X1 interface is permitted.</td></tr>
<tr><td>2. close</td><td>Data traffic via the X1 interface is not permitted.</td></tr>
<tr><td rowspan="4">4. X2</td><td colspan="2">Enable or disable the firewall for the X2 interface and respective service.</td></tr>
<tr><td>0. Back to …</td><td>Back to the higher-level menu</td></tr>
<tr><td>1. open</td><td>Data traffic via the X2 interface is permitted.</td></tr>
<tr><td>2. close</td><td>Data traffic via the X2 interface is not permitted.</td></tr>
</table>

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.10.17 “Ports and Services” > “PLC Runtime Services” Submenu

This submenu contains the settings for the PLC runtime system services.

Table 243: “Ports and Services” > “PLC Runtime Services” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. General Configuration	Enter the password for port authentication.
2. CODESYS 2	Opens a submenu with service settings for CODESYS V2
3. e!RUNTIME	Opens a submenu with service settings for ***e!****RUNTIME*
4. Change CODESYS Runtime firewalling settings	Opens a submenu with firewall settings for the this service for the interfaces
5. Change CODESYS WebVisu firewalling settings	Opens a submenu with firewall settings for the this service for the interfaces

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.10.18 “PLC Runtime Services” > “CODESYS 2” Submenu

This submenu contains the settings for the CODESYS V2 service.

Table 244: “Ports and Services” > “PLC Runtime Services” > “CODESYS 2” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Webserver enable/disable	Enable or disable the Webserver for the CODESYS web visualization.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The Webserver is enabled.
	2. Disable	The Webserver is disabled.
2. Communication enable/disable	Enable or disable the communication between the CODESYS V2 runtime system and the CODESYS V2 programming system.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Communication is enabled.
	2. Disable	Communication is disabled.
3. Communication Port Number	Enter here the port number for communication with the CODESYS V2 programming system. The default value is 2455.	
4. Port Authentication enable/disable	Enter here whether a login is required for connecting to the device.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Authentication via login is required.
	2. Disable	Authentication is not required.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.10.19 “PLC Runtime Services” > “e!RUNTIME” Submenu

This submenu contains the settings for the *__e!__RUNTIME* service.

Table 245: “Ports and Services” > “PLC Runtime Services” > “e!RUNTIME” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Webserver enable/disable	Enable or disable the Webserver for the *__e!__RUNTIME* web visualization.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The Webserver is enabled.
	2. Disable	The Webserver is disabled.
2. Port Authentication enable/disable	Enter here whether a login is required for connecting to the device.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Authentication via login is required.
	2. Disable	Authentication is not required.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.11 “SNMP” Menu

This menu contains other submenus with the SNMP settings.

Table 246: “SNMP” Menu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. General SNMP Configuration	Opens a submenu with general SNMP settings
2. SNMP v1/v2c Manager Configuration	Opens a submenu with settings for the SNMP v1/v2c Manager
3. SNMP v1/v2c Trap Receiver Configuration	Opens a submenu with settings for the SNMP v1/v2c trap receivers
4. SNMP v3 Configuration	Opens a submenu with settings for the SNMP v3 configuration
5. SNMP firewalling	Opens a submenu with firewall settings for SNMP
6. Secure SNMP firewalling	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.1.2.11.1 “SNMP” > “General SNMP Configuration” Submenu

This submenu contains the general SNMP settings.

Table 247: “SNMP” > “General SNMP Configuration” Submenu

Parameters	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. SNMP status	Enable or disable the SNMP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The SNMP service is enabled.
	2. Disable	The SNMP service is disabled.
2. Name of device	Enter here the device name (sysName).	
3. Description	Enter here the device description (sysDescription).	
4. Physical location	Enter here the location of the device (sysLocation).	
5. Contact	Enter here the email contact address (sysContact).	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.11.2 “SNMP” > “SNMP v1/v2c Manager Configuration” Submenu

This submenu contains the SNMP v1/v2c Manager settings.

Table 248: “SNMP” > “SNMP v1/v2c Manager Configuration” Submenu

Parameters	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Protocol state	Enable or disable the SNMP v1/v2c protocol.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The SNMP v1/v2c protocol is enabled.
	2. Disable	The SNMP v1/v2c protocol is disabled.
2. Local community name	Specify here the community name for the SNMP manager configuration (max. 32 characters, no spaces).	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.11.3 “SNMP” > “SNMP v1/v2c Trap Receiver Configuration” Submenu

This submenu contains settings for the v1/v2c trap receivers.

Table 249: “SNMP” > “SNMP v1/v2c Trap Receiver Configuration” Submenu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
(n). Trap Receiver (n)	Opens a submenu with information on the selected v1/v2c trap receiver to delete the trap receiver
(n + 1). Add new Trap Receiver	Opens a series of submenus to create a new v1/v2c trap receiver You can enter 10 trap receivers. The following entries/selections are possible: • IP address of the new trap receiver (management station) • Community name for the new trap receiver configuration (max. 32 characters, no spaces) • SNMP version via which the traps are sent (v1/v2c)

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.11.4 “SNMP” > “SNMP v3 Configuration” Submenu

This submenu contains settings for SNMP v3.

Table 250: “SNMP” > “SNMP v3 Configuration” Submenu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
(n). Username	Opens a submenu with information on the selected v3 user and to delete the user
(n + 1). Add new v3 User	Opens a series of submenus to create a new v3 user You can enter 10 users. The following entries/selections are possible: • Authentication name (The name can have a min. 8 and max. 32 characters and may contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.) • Authentication type (None/MD5/SHA) • Authentication key (The key can have a min. 8 and max. 32 characters and may contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.) • Privacy type (None/DES/AES) • Privacy key (The key can have a min. 8 and max. 32 characters and may contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.) • IP address for a trap receiver for v3 traps

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

18.1.2.11.5 “SNMP” > “(Secure)SNMP firewalling” Submenu

These submenus contain the SNMP firewall settings.

Table 251: “SNMP” > “(Secure)SNMP firewalling” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. VPN	Enable or disable the firewall for the VPN interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the VPN interface is permitted.
	2. close	Data traffic via the VPN interface is not permitted.
2. WAN	Enable or disable the firewall for the WAN interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the WAN interface is permitted.
	2. close	Data traffic via the WAN interface is not permitted.
3. X1	Enable or disable the firewall for the X1 interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the X1 interface is permitted.
	2. close	Data traffic via the X1 interface is not permitted.
4. X2	Enable or disable the firewall for the X2 interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the X2 interface is permitted.
	2. close	Data traffic via the X2 interface is not permitted.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

18.2 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!

18.2.1 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.

18.2.1.1 1 Channel Digital Input Module with Diagnostics

750-435

Table 252: 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

18.2.1.2 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 253: 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

18.2.1.3 2 Channel Digital Input Module with Diagnostics

750-419, -421, -424, -425,
753-421, -424, -425

Table 254: 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

18.2.1.4 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 255: 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**
				Acknowledgement bit Q 2 Channel 2	Acknowledgement bit Q 1 Channel 1	0	0

18.2.1.5 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 256: 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

18.2.1.6 8 Channel Digital Input Modules

750-430, -431, -436, -437, -1415, -1416, -1417, -1418,
753-430, -431, -434, -436, -437

Table 257: 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

18.2.1.7 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 258: 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

18.2.1.8 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 259: 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

18.2.1.9 16 Channel Digital Input Modules

750-1400, -1402, -1405, -1406, -1407

Table 260: 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

18.2.2 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.

18.2.2.1 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 261: 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

18.2.2.2 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 262: 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

18.2.2.3 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 263: 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 264: 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

18.2.2.4 4 Channel Digital Output Modules

750-504, -515, -516, -519, -531,
753-504, -516, -531, -540

Table 265: 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

18.2.2.5 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 266: 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

18.2.2.6 8 Channel Digital Output Module

750-530, -536, -1515, -1516,
753-530, -534, 536

Table 267: 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

18.2.2.7 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 268: 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

18.2.2.8 16 Channel Digital Output Modules

750-1500, -1501, -1504, -1505

Table 269: 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

18.2.2.9 8 Channel Digital Input/Output Modules

750-1502, -1506

Table 270: 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

18.2.3 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.

18.2.3.1 1 Channel Analog Input Modules

750-491, (and all variations)

Table 271: 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}

18.2.3.2 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 272: 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

18.2.3.3 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 273: 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 274:: 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	-	-	

18.2.3.4 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 275: 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

18.2.3.5 8 Channel Analog Input Modules

750-451, 750-458, 750-496, 750-497

Table 276: 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

18.2.3.6 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 277: 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 278: 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	-	-	

18.2.4 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.

18.2.4.1 2 Channel Analog Output Modules

750-550, -552, -554, -556, -560, -562, 563, -585, -586, (and all variations),
753-550, -552, -554, -556

Table 279: 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

18.2.4.2 4 Channel Analog Output Modules

750-553, -555, -557, -559,
753-553, -555, -557, -559

Table 280: 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

18.2.5 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.

18.2.5.1 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 281: 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 282: 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 283: 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 284: 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

18.2.5.2 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 285: 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

18.2.5.3 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 286: 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	

18.2.5.4 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 287: 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		

18.2.5.5 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 288: 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

18.2.5.6 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 289: 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	

18.2.5.7 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 290: 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 291: 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		

18.2.5.8 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 292: 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 293: 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 294: 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 295: 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	

18.2.5.9 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 296: 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

18.2.5.10 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 297: 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)

18.2.5.11 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 298: 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		

18.2.5.12 DALI/DSI Master Module

750-641

The DALI/DSI Master module has a total of 6 bytes of user data in both the Input and Output Process Image (5 bytes of module data and 1 byte of control/status). The following tables illustrate the Input and Output Process Image, which have 3 words mapped into each image. Word alignment is applied.

Table 299: DALI/DSI Master Module 750-641

Input Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	D0	S	DALI Response	Status byte
1	D2	D1	Message 3	DALI Address
2	D4	D3	Message 1	Message 2

Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	D0	C	DALI command, DSI dimming value	Control byte
1	D2	D1	Parameter 2	DALI Address
2	D4	D3	Command extension	Parameter 1

Note

DALI / DSI Master can only be used with CODESYS 2!
The DALI/DSI master module is only supported by the runtime system CODESYS 2. The runtime system ***e!****Runtime* does not support the DALI/DSI master module!

18.2.5.13 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 300: 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 pairs GA1 … GA15 similar to GA0.	Bit set = Error Bit not set = No error
11	-	-	Not used	

DA = DALI address
GA = Group address

Output Process Image

Offset	Byte Designation		Note	
	High Byte	Low Byte		
0	-	S	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 301: 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		

18.2.5.14 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 302: 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		

18.2.5.15 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 303: 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	

18.2.5.16 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 304: 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		

18.2.5.17 *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 305: *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

18.2.5.18 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 306: 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)	

18.2.5.19 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 307: 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

18.2.5.20 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 308: 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

18.2.6 System Modules

18.2.6.1 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 309: 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 310: 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

18.2.6.2 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 311: 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

18.2.6.3 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 312: 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

18.3 CODESYS V2 Libraries

Additional functions for the controller 750-8212are provided using libraries.

18.3.1 General Libraries

This section contains general CODESYS libraries supported by the controller 750-8212.

18.3.1.1 CODESYS System Libraries

All of the functions of the CODESYS system libraries listed below are supported.

Table 313: CODESYS System Libraries

Library	Function	C/IEC 61131
Analyzation.lib	Analysis of boolean expressions	C and IEC 61131
AnalyzationNew.lib	Analysis of boolean expressions	C and IEC 61131
Iecsfc.lib	Provision of implicit variables in the SFC (sequential function chart)	IEC 61131
NetVarUdp_LIB_V23.lib	Implementation for network variables	IEC 61131
Standard.LIB	Offers various standard functions	C
SysLibAlarmTrend.lib	Supports alarm and trend tasks	IEC 61131
SysLibCallback.lib	For installing call-back handlers and event handlers	C
SysLibDir.lib	For accessing directories	C
SysLibDirect.lib	Access to variables using indices	C
SysLibEvent.lib	Handling of events in the system	C
SysLibFileStream.lib	File handling using ANSI-C functions	C
SysLibGetAddress.lib	Returns addresses and the size of memory segments	C
SysLibIecTasks.lib	Administration of IEC tasks	C
SysLibMem.lib	Memory administration	C
SysLibPlcCtrl.lib	Control of the PLC from outside the PLC program	C
SysLibProjectInfo.lib	Reading out of information about the CODESYS project	C
SysLibSem.lib	Handling of semaphores	C
SysLibSockets.lib	Socket handling	C
SysLibSocketsAsync.lib	Socket handling, asynchronous	C
SysLibStr.lib	String functions	C
SysLibTasks.lib	Administration of tasks	C
SysLibTime.lib	Administration of real-time clock	C
SysLibVisu.lib	Dynamic visualization	C

Table 313: CODESYS System Libraries

Library	Function	C/IEC 61131
SysTaskInfo.lib	Evaluation of task information in the Online mode	IEC 61131
Util.lib	Various logical operations	IEC 61131
Util_no_Real.lib	Various logical operations	IEC 61131

Additional information about the libraries is given in the online Help function for CODESYS-IDE.

18.3.1.2 SysLibCom.lib

The controller 750-8212supports the following function blocks of the “SysLibCom.lib” library:

- SysComClose
- SysComGetVersion2300
- SysComOpen
- SysComRead
- SysComSetSettings
- SysComSetSettingsEx
- SysComWrite

Note

Observe restrictions on the settings for stop bits!
The setting “1.5 stop bits” is not supported by controller750-8212.

Additional information about this is given in the online Help function for CODESYS-IDE.

18.3.1.3 SysLibFile.lib

The controller 750-8212supports the following function blocks of the “SysLibFile.lib” library:

- SysFileClose
- SysFileCopy
- SysFileDelete
- SysFileEOF
- SysFileGetPos
- SysFileGetSize
- SysFileGetTime
- SysFileOpen
- SysFileRead
- SysFileRename
- SysFileSetPos
- SysFileWrite

Note

Ensure that files are saved!

Files are not reliably saved on the data medium until you call up the “SysFileClose” function block!

Additional information about this is given in the online Help function for CODESYS-IDE.

Notes on the parameters of the function blocks

File and directory names distinguish between upper and lower case!

“test.txt”≠ “TEST.TXT”≠ “Test.txt”

The separator for directories is: “/.”

The file system supports:

- Absolute paths, (e.g., “/media/sd/test.txt”)
- Relative paths (e.g., “testpath/test.txt”)
- Macros (e.g., “HOME://”, “CARD://”, “TMP://”)

Table 314: Possible Macros for File Access

Macro	Booting from Internal Memory	Booting from Memory Card
HOME://	“/home/codesys/” (internal NAND memory)	“/home/codesys/” (memory card)
CARD://	“/media/sd/” (nemory card)	“/home/codesys/” (memory card)
TMP://	“/tmp/codesys/” (internal RAM memory)	“/tmp/codesys/” (internal RAM memory)

18.3.1.4 SysLibFileAsync.lib

The controller 750-8212supports the following function blocks of the “SysLibFileAsync.lib” library:

- SysFileCloseAsync
- SysFileCopyAsync
- SysFileDeleteAsync
- SysFileEOFAsync
- SysFileGetPosAsync
- SysFileGetSizeAsync
- SysFileGetTimeAsync
- SysFileOpenAsync
- SysFileReadAsync
- SysFileRenameAsync
- SysFileSetPosAsync

- SysFileWriteAsync

Note

Ensure that files are saved!

Files are not reliably saved to the data medium until you call up the “SysFileCloseAsync” function block.

Additional information about this is given in the online Help function for CODESYS-IDE.

Notes on the parameters of the function blocks

File and directory names distinguish between upper and lower case!

“test.txt”≠ “TEST.TXT”≠ “Test.txt”

The separator for directories is: “/.”

The file system supports:

- Absolute paths, (e.g., “/media/sd/test.txt”)
- Relative paths (e.g., “testpath/test.txt”)
- Macros (e.g., “HOME://”, “CARD://”, “TMP://”)

Table 315: Possible Macros for File Access

Macro	Booting from Internal Memory	Booting from Memory Card
HOME://	“/home/codesys/” (internal NAND memory)	“/home/codesys/” (memory card)
CARD://	“/media/sd/” (nemory card)	“/home/codesys/” (memory card)
TMP://	“/tmp/codesys/” (internal RAM memory)	“/tmp/codesys/” (internal RAM memory)

18.3.1.5 SysLibRtc.lib

The controller 750-8212supports the following function blocks of the “SysLibRtc.lib” library:

- SysRtcGetHourMode
- SysRtcGetTime
- SysRtcSetTime

Additional information about this is given in the online Help function for CODESYS-IDE.

18.3.1.6 BusDiag.lib

The controller 750-8212 supports the following function blocks of the “BusDiag.lib” library:

- DiagGetBusState
- DiagGetState

The document containing a description of this library and the function blocks it includes is available for download on the Internet at www.wago.com.

The values for the input variables “DEVICENUMBER” of the “DiagGetBusState” and “DiagGetState” functions are based on the particular device and bus system and are as follows for the controller “PFC200; G2; 2ETH RS” (750-8212):

Table 316: Input Variable “DEVICENUMBER”

Bus System	Value
Local bus	0
Modbus	1

18.3.1.7 mod_com.lib

The controller 750-8212supports the following function blocks of the “mod_com.lib” library:

- ADD_PI_INFORMATION
- CRC16
- FBUS_ERROR_INFORMATION
- GET_DIGITAL_INPUT_OFFSET
- GET_DIGITAL_OUTPUT_OFFSET
- KBUS_ERROR_INFORMATION
- MOD_COM_VERSION
- PI_INFORMATION
- SET_DIGITAL_INPUT_OFFSET
- SET_DIGITAL_OUTPUT_OFFSET
- SLAVE_ADDRESS

The document containing a description of this library and the function blocks it includes is available for download on the Internet at www.wago.com.

18.3.1.8 SerComm.lib

The controller 750-8212supports the following function blocks of the “SerComm.lib” library:

- SERCOMM
- SERCOMM_VERSION

The document containing a description of this library and the function blocks it includes is available for download on the Internet at www.wago.com.

18.3.1.9 WagoConfigToolLIB.lib

The following table shows call-ups that allow you to configure and parameterize the controller from the PLC program or Linux® via the “ConfigToolFB” function block (see parameter “stCallString”). In addition to WBM and the CBM, this is another variant to configure the controller for operational requirements.

The configuration directory for this under Linux® is: **`/etc/config-tools/`**

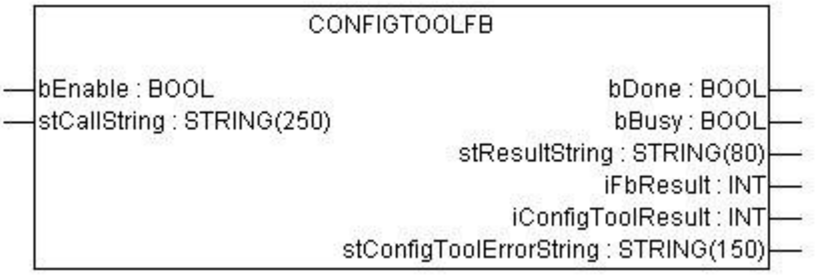

CONFIGTOOLFB
bEnable : BOOL
stCallString : STRING(250)
bDone : BOOL
bBusy : BOOL
stResultString : STRING(80)
iFbResult : INT
iConfigToolResult : INT
stConfigToolErrorString : STRING(150)

Figure 130: Graphical Representation of the “ConfigToolFB” Function Block

Table 317: Description of the Configuration Scripts for “Information”

Parameters	Status	Call-Up	Output/Input	Effective
Controller Details: Identifies various information about the controller				
Product Description	read	get_coupler_details product-description	Product description	Immediately
Order Number	read	get_coupler_details order-number	Item number of the controller	Immediately
Firmware Revision	read	get_coupler_details firmware-revision	Firmware version of the controller	Immediately
Licence Information	read	get_coupler_details license-information	CODESYS license details	Immediately
Network Details X1: Identifies the parameters currently used for the ETHERNET interface X1/X2 in “switched” mode or for the ETHERNET interface X1 in “separated” mode				
State	read	get_actual_eth_config X1 state	Status of the interface. Possible return values: - enabled - disabled	Immediately
Mac Address	read	get_actual_eth_config X1 mac-address	MAC address	Immediately
IP Address	read	get_actual_eth_config X1 ip-address	Current IP address	Immediately
Subnet Mask	read	get_actual_eth_config X1 subnet-mask	Current subnet mask	Immediately
Configuration type	read	get_actual_eth_config X1 config-type	Path via which the interface receives its IP address; Possible return values: - dhcp - static - bootp	Immediately
Cable state	read	get_actual_eth_config X1 cable-state	Connection status; Possible return values: - connected - disconnected	Immediately
Default-gateway	read	get_actual_eth_config X1 default-gateway	Default gateway currently used for interface X1 (e.g., if a default gateway was entered via a DHCP server)	Immediately
Network Details X2: Identifies the parameters currently used for the ETHERNET interface X2 in “separated” mode				
See “Network Details X1”. When calling these up, replace “X1” with “X2” (in “separated” mode only).				

Table 318: Description of the Configuration Scripts for “CODESYS”

Parameters	Status	Call	Output/Input	Effective
Information				
CODESYS Webserver Version	read	get_coupler_details codesys-Webserver-version	Version of the CODESYS Webserver	Immediately
Project Details				
Date	read	get_rts_info project date	Display of the project information specified in CODESYS (Menu > Project > Project Information)	Immediately
Title	read	get_rts_info project title		Immediately
Version	read	get_rts_info project version		Immediately
Author	read	get_rts_info project author		Immediately
Description	read	get_rts_info project description		Immediately
CODESYS State				
State	read	get_rts_info state	Display of the CODESYS status (RUN or STOP)	Immediately
Home Directory (Boot Project Location)				
Home Directory (Boot Project Location)	read	get_runtime_config homedir-on-sdcard	Storage logation for the home directory. Possible return values: - enabled: The home directory is on the SD card. - disabled: The home directory is on the boot medium.	After restart
	write	config_runtime homedir-on-sdcard=<Wert>	Storage logation for the home directory. Possible entries for the value are: - enabled: Put the home directory on the SD card. - disabled: The home directory is on the boot medium.	
Boot project location	read	get_runtime_config boot-project	Memory location for a boot project of the runtime application Possible return values: - HOME:// (saving on internal memory) - CARD:// (saving on the memory card)	After restart
	write	config_runtime boot-project=<value>	Possible entries for <value>: - HOME:// (saving on internal memory) - CARD:// (saving on the memory card)	

Table 319: Description of the Configuration Scripts for “Networking - Host/Domain Name”

Parameters	Status	Call	Output/Input	Effecti ve
Host Name				
Host Name	read	get_coupler_details hostname	Display of the host name. The return value is blank when /etc/hostname is empty. For details see the parameter “Actual Hostname.”	Immedia tely
	write	change_hostname hostname=<String>	Changing the host name. Input a host name for <String>.	Immedia tely
Actual Hostname	read	get_coupler_details actual-hostname	The actual host name (if /etc/hostname is empty, a unique host name is generated from the MAC address)	Immedia tely
Domain Name				
Domain name	read	get_coupler_details domain-name	Display of domain name	Immedia tely
	write	change_hostname dnsdomain=<String>	Change the domain name. Enter the domain name for <String>.	

Table 320: Description of the Configuration Scripts for “Networking - TCP/IP”

Parameters	Status	Call	Output/Input	Effecti ve
IP Address X1: Determines the IP parameters of the ETHERNET interfaces X1/X2 in “switched” mode and the ETHERNET interface X1 in “separated” mode				
Type of IP address configuration	read	get_eth_config X1 config-type	Path via which the interface receives its IP address Possible return values are: - static (set statically) - dhcp (per DHC) - bootp (per BootP)	Immedia tely
	write	config_interfaces interface=X1 config-type=<Value> state=enabled	Enable process, via which the interface receives its IP address Possible entries for <Value> are: - static (set statically) - dhcp (per DHC) - bootp (per BootP)	
IP address	read	get_eth_config X1 ip-address	Address set for using a static IP address (static IP).	Immedia tely
	write	config_interfaces interface=X1 ip-address=<Value>	Change IP address for static IP <Value> must have an IP address with the format “Number.Number.Number.Number.”	
Subnet Mask	read	get_eth_config X1 subnet-mask	Subnet mask set for using a static IP address (static IP)	Immedia tely
	write	config_interfaces interface=X1 subnet-mask=<Value>	Change subnet mask for static IP addresses. <Value> must have an IP address with the format “Number.Number.Number.Number.”	
IP Address X2: Determines the parameters currently used for the ETHERNET interface X2 in “separated” mode				
See “IP Address X1.” When calling these up, replace X1 with X2 (only permissible in “separated” mode).				

Table 320: Description of the Configuration Scripts for “Networking - TCP/IP”

Parameters	Status	Call	Output/Input	Effective
Default Gateway 1				
Default Gateway	read	get_default_gateway_config number=1 state	Current status of the default gateway 1. Possible return values: - enabled - disabled	Immediately
	write	config_default_gateway number=1 state=<stateval>	Possible entries for <Value>: - enabled - disabled	
Default Gateway	read	get_default_gateway_config number=1 value	Current IP address of the configured default gateway 1	Immediately
	write	config_default_gateway number=1 value=<gw>	Enter the IP address of the default gateway 1 here. <gw> is an IP address with the format “Number.Number.Number.Number.”	
Default Gateway	read	get_default_gateway_config number=1 metric	Current metric (cost factor) of the default gateway 1 The default value is “20.”	Immediately
	write	config_default_gateway number=1 metric=<n>	Enter the metric of the default gateway 1 here. <n> is a number between “0” and “4.294.967.295.”	
Default Gateway 2				
See “Default Gateway 1.” When calling the gateway number, replace 1 with 2.				
DNS Server 1				
DNS Server 1	read	get_dns_server 1	DNS server address with the consecutive number 1	Immediately
	write/ change	edit_dns_server dns-server-nr=1 change=change dns-server-name=<Value>	Set the address of the DNS server with 1 as the consecutive number. <Value> is an IP address with the format “Number.Number.Number.Number.”	
	write/ delete	edit_dns_server dns-server-nr=1 delete=delete	Delete the DNS server with the consecutive number 1.	
DNS Server 2 … n				
See “DNS Server 1.” When calling, adjust the server number (2 … n).				
Add DNS Server				
Add DNS server	write	edit_dns_server add=add dns-server-name=<Value>	Add additional DNS addresses here. <Value> is an IP address with the format “Number.Number.Number.Number.”	Immediately

Table 321: Description of the Configuration Scripts for “Networking - ETHERNET”

Parameters	Status	Call-Up	Output/Input	Effective
Switch Configuration				
Interface Mode	read	get_dsa_mode	Query the switch configuration: Possible return values: - 0 = „switched“ mode - 1 = „separated“ mode	Immediately
	write	set_dsa_mode -v <value>	Set the switch configuration: Possible entries for <value>: - 0 = „switched“ mode - 1 = „separated“ mode	
Interface X1				
Port State	read	get_eth_config X1 state	Query the port state: Possible return values: - enabled - disabled	Immediately
	write	config_ethernet port=X1 state=enabled	Activate port: enabled	
		config_ethernet port=X1 state=disabled	Deactivate port: disabled	
Autonegotiation	read	get_eth_config X1 autoneg	Query the status of the autonegotiation function: Possible return values: - on - off	Immediately
	write	config_ethernet port=X1 autoneg=on	Activate the autonegotiation function: on	
		config_ethernet port=X1 autoneg=off speed=<value> duplex=<value>	Deactivate the autonegotiation function: off Note: You must also indicate the speed and duplex value when you deactivate the autonegotiation function. Possible entries for speed: - 10M - 100M Possible entries for duplex: - half - full	
Speed and Duplex Settings	read	get_eth_config X1 speed	Display of ETHERNET speed	Immediately
	read	get_eth_config X1 duplex	Display of the Duplex mode	
	write	config_ethernet port=X1 autoneg=off speed=<value> duplex=<value>	Change the ETHERNET speed and the Duplex mode. Possible entries for speed: - 10M - 100M Possible entries for duplex: - half - full	
Interface X2				
See “Interface X1”. When calling these up, replace “X1” with “X2”.				

Table 322: Description of the Configuration Scripts for “NTP”

Parameters	Status	Call	Output/Input	Effective
Configuration Data				
State	read	get_ntp_config state	Query the status of the NTP server Possible return values are: - enabled - disabled	Immediately
	write	config_sntp state=<Value>	Possible entries for <Value>: - enabled - disabled	
Port	read	get_ntp_config port	Port number of the NTP server	Immediately
	write	config_sntp port=<Value>	Enter the port number for <Value>.	
Time Server	read	get_ntp_config time-server-<N>	Query the IP address of the time server: N = 1 … 4 for querying one of 4 time servers.	Immediately
	write	config_sntp time-server-<N>=<Value>	Enter the IP address of 4 time servers <N> can be a value from 1 to 4. <Value> is an IP address with the format “Number. Number. Number. Number.”	
Update Time (seconds)	read	get_ntp_config update-time	Query the time in seconds between two requests to the time server.	Immediately
	write	config_sntp update-time=<Value>	Specify the time-server's query cycle (in s) for <Value>.	

Table 323: Description of the Configuration Scripts for “Clock”

Parameters	Status	Call-Up	Output/Input	Effective
Clock				
Time and Date				
Date on device, local	read	get_clock_data date-local	Local time and date	Immediately
	write	config_clock type=local date=<Datum>	Change date. The format for <date> is: DD.MM.YYYY	
Time on device, UTC	read	get_clock_data time-utc	Time/UTC	Immediately
	write	config_clock type=utc time=<Time>	Change time, based on UTC time. The format for <time> is: hh:mm:ss xx	
Time on device, local	read	get_clock_data time-local	Time/local time	Immediately
	write	config_clock type=local time=<Time>	Change time, based on local time. The format for <time> is: hh:mm:ss xx	
12-Hour-Format	read	get_clock_data display-mode	Presentation format either as 12 or 24-hour format: Possible return values: - 12-hour-format - 24-hour-format	Immediately
	write	config_clock _ display_mode display-mode=<value>	Set the presentation format for the time. Possible entries for <Value>: - 12-hour-format - 24-hour-format	
Time Zone				
TZ-String	read	get_clock_data tz-string	Currently set time zone – original TZ string as stored in the operating system.	Immediately
	write	config_timezone tz-string=<String>	Change TZ string directly. Example of <String>: CET-1CEST, M3.5.0/2,M10.5.0/3	

Table 324: Description of the Configuration Scripts for "Administration"

Parameters	Status	Call	Output/Input	Effective
Administration				
Configuration of Serial Interface				
Configuration of serial interface	read	get_coupler_details RS232-owner	User of the serial interface Possible return values are: - Linux - None	immediately
	write	config_RS232 owner=<value>	User of the serial interface Possible entries for <value> are: - Linux - None	

Table 324: Description of the Configuration Scripts for "Administration"

Parameters	Status	Call	Output/Input	Effective
Configuration of Service Interface				
Configuration of Service Interface	read	get_service_interface_config mode	User of the serial interface. Active: Current value Configured: Value set, but not applied by a reboot Possible return values are: - service (WAGO-I/O-*CHECK*, WAGO-I/O-*PRO*, ***e!****COCKPIT*) - linux (Linux® console) - free (unused, free for application)	immediately
	write	config_service_interface_config mode=<value>	User of the serial interface. Possible entries for <value>: - service - linux - free	after Restart
Reboot Controller				
-	write	start_reboot	Restart the controller.	immediately

Table 325: Description of Configuration Scripts for “Package Server”

Parameters	Status	Call-Up	Output/Input	Valid
Firmware Update				
Medium for active partition	read	get_filesystem_data active-partition-medium	Specifies the medium for the active partition (sd-card, internal-flash-emmc).	Right away

Create firmware backup	write	firmware_backup
		package-settings=<Value1>
		package-codesys=<Value2>
		package-system=<Value3>
		device-medium=<Value4>
		auto-update=<Value5>
		download-dir=<Value6>
			Generates a backup of the selected packet on the specified medium.
			Parameter:
			<Value1> = 1, if the “Settings” package is to be selected.
			<Value2> = 1, if the “CODESYS Project” package is to be selected.
			<Value3> = 1, if the “System” package is to be selected.
			<Value4> = target medium for saving the backup. (sd-card, network)
			<Value5> = 1, if “Auto Update” function is to be activated.
			<Value6> = target directory for backup file, if “network” is selected as target medium.
			Parameters, which are not to be set (1) can either be set to 0 or omitted completely.
				Right away

Table 326: Description of Configuration Scripts for “Ports and Services” – “Network Services

Parameters	Status	Call-Up	Output/Input	Valid
Network Services				
Telnet				
Telnet Port	read	get_port_state telnet	Read the status of the Telnet server. Possible return values: - enabled - disabled	Right away

	write	config_port
		port=telnet
		state=<Value>
			Possible entries for <Value>:
			- enabled
			- disabled	

FTP				
FTP Port	read	config_ssl ftp-status	Read the status of the FTP server. Possible return values: - enabled - disabled	Right away
	write	config_port port=ftp state=<Value>	Possible entries for <Value>: - enabled - disabled	
FTPS				
FTPS Port	read	config_ssl ftps-status	Read the status of the FTPS port. Possible return values: - enabled - disabled	Right away
	write	config_port port=ftps state=<Value>	Activate/Deactivate FTPS. Possible entries for <Value>: - enabled - disabled	
HTTP				
HTTP Port	read	config_ssl http-status	Read the status of the HTTP port. Possible return values: - enabled - disabled	Right away
	write	config_port port=http state=<Value>	Activate/Deactivate HTTP. Possible entries for <Value>: - enabled - disabled	
HTTPS				
HTTPS Port	read	config_ssl https-status	Read the status of the HTTPS port. Possible return values: - enabled - disabled	Right away
	write	config_port port=https state=<Value>	Activate/Deactivate HTTPS. Possible entries for <Value>: - enabled - disabled	

Table 327: Description of Configuration Scripts for “Ports and Services” – “PLC Runtime Services”

Parameters	Status	Call	Output/Input	Effective
General Settings				
PLC runtime version	read	get_runtime_config running-version	Version of the enabled PLC runtime Possible return values: - 0 = no runtime enabled - 2 = CODESYS V2 enabled - 3 = ***e!****RUNTIME* enabled	Immediately
	write	config_runtime runtime-version=<value>	Setting and, if necessary, stopping of the previous runtime version and starting of required version Possible entries for <value>: - 0 = do not enable runtime - 2 = enable CODESYS V2 - 3 = enable ***e!****RUNTIME*	
Default web page	read	get_runtime_config default-webpage	Calling web page when only entering the IP address in the web browser Possible return values: - WBM (web based management) - Webvisu (web visualization)	Immediately
	write	config_runtime default-webpage=<value>	Possible entries for <value>: - WBM (web based management) - Webvisu (web visualization)	
Change authentication password	write	config_linux_user user=admin new-password=<value> confirm-password=<value>	Change the PLC runtime access password	Immediately

Table 327: Description of Configuration Scripts for “Ports and Services” – “PLC Runtime Services”

Parameters	Status	Call	Output/Input	Effective
CODESYS V2 Settings				
CODESYS2 Webserver State	read	get_runtime_config cfg-version=2 Webserver-state	Read status of the runtime-specific Webserver Possible return values: - enabled - disabled	Immediately
	write	config_runtime cfg-version=2 Webserver-state=<value>	Enable/disable runtime-specific Webserver Possible entries for <value>: - enabled - disabled	
CODESYS2 Port Authentication	read	get_runtime_config cfg-version=2 authentication	Read status of the port authentication for communication between the CODESYS V2 PC software and the controller Possible return values: - enabled - disabled	Immediately
	write	config_runtime cfg-version=2 authentication=<value>	Possible entries for <value>: - enabled - disabled	
CODESYS2 Service State	read	get_runtime_config service-state	Read status of the port for communication between the CODESYS V2 PC software and the controller Possible return values: - enabled - disabled	Immediately
	write	config_runtime service-state=<value>	Possible entries for <value>: - enabled - disabled	
CODESYS2 Communication Port	read	get_runtime_config comm-port	Read value of set network port for communication between PC and controller Default value is 2455	Immediately
	write	config_runtime comm-port=<value>	Change port number Enter the TCP/IP port number for <value>.	

Table 327: Description of Configuration Scripts for “Ports and Services” – “PLC Runtime Services”

Parameters	Status	Call	Output/Input	Effective
***e!Runtime* Settings**				
e!*RUNTIME* Webserver State	read	get_runtime_config cfg-version=3 Webserver-state	Read status of the runtime-specific Webserver Possible return values - enabled - disabled	Immediately
	write	config_runtime cfg-version=3 Webserver-state=<value>	Enable/disable runtime-specific Webserver Possible entries for <value>: - enabled - disabled	
e!*RUNTIME* Port Authentication	read	get_runtime_config cfg-version=3 authentication	Read status of the port authentication for communication between the ***e!****COCKPIT* PC software and the controller Possible return values: - enabled - disabled	Immediately
	write	config_runtime cfg-version=3 authentication= <value>	Possible entries for <value>: - enabled - disabled	

Table 328: Description of Configuration Scripts for “Ports and Services” – “SSH/TFTP”

Parameters	Status	Call-Up	Output/Input	Valid
SSH				
SSH Server				
SSH	read	get_ssh_config state	Read the status of the SSH port. Possible return values: - enabled - disabled	Right away
	read	get_ssh_config root-access-state	Indicates whether logon as root is permitted. Possible return values: - enabled - disabled	
	read	get_ssh_config password-request-state	Indicates whether authentication by password (instead of PKI key files) is permitted. Possible return values: - enabled - disabled	
	read	get_ssh_config port-number	Specifies the SSH port	
	write	config_ssh state=<Value>	Activate/Deactivate SSH service. Possible entries for <Value>: - enabled - disabled	
	write	config_ssh port-number=<Value>	Set the SSH port	
	write	config_ssh root-access-state-value=<Value>	Permit/Prohibit logon as root. Possible entries for <Value>: - enabled - disabled	
	write	config_ssh password-request-state-value=<Value>	Permit/Prohibit authentication by password. Possible entries for <Value>: - enabled - disabled	
TFTP				
TFTP Server				
TFTP	read	get_tftp_config state	Read the status of the TFTP port. Possible return values: - enabled - disabled	Right away
	read	get_tftp_config download-dir	Read the TFTP main directory.	
	write	config_tftp state=<Value>	Activate/Deactivate TFTP port. Possible entries for <Value>: - enabled - disabled	
	write	config_tftp download-dir=<Value>	Set the TFTP main directory.	

Table 329: Description of Configuration Scripts for “SNMP”

Parameters	Status	Call-Up	Output/Input	Valid
General SNMP information parameters				
Name of device	read	get_snmp_data device-name	Specifies the SNMP parameter “sysName”.	Right away
	write	config_snmp device-name=<Value>	Change the SNMP parameter “sysName” (<Value> = string).[*]	After restart
Description	read	get_snmp_data description	Specifies the SNMP parameter “sysDescr”.	Right away
	write	config_snmp description=<Value>	Change the SNMP parameter “sysDescr” (<Value> = string).[*]	After restart
Physical location	read	get_snmp_data physical-location	Specifies the SNMP “sysLocation” parameter.	Right away
	write	config_snmp physical-location=<Value>	Change the SNMP parameter “sysLocation” (<Value> = string).[*]	After restart
Contact	read	get_snmp_data contact	Specifies the SNMP “sysContact” parameter.	Right away
	write	config_snmp contact=<Value>	Change the SNMP parameter “sysContact” (<Value> = string).	After restart
[*] When entering values, the blank characters must be filled by either “+” or “%20”. If this is not done, the input is not recognized as a coherent string.				
SNMP Manager configuration for v1 and v2c				
Protocol status	read	get_snmp_data v1-v2c-state	Outputs the status of the SNMP protocol for v1/v2c as a string. Possible return values: - enabled - disabled	Right away
Local Community Name	read	get_snmp_data v1-v2c-community-name	Specifies the community name set for v1/v2c/	Right away

Protocol Status/Community Name	write	config_snmp
		v1-v2c-state=<Value1>
		v1-v2c-community-name=<Value2>
			Activates/deactivates the v1/v2c protocol (<Value1> = enabled or disabled) and assigns a community name. (<Value2> = string without spaces, min. 1, max. 32 characters).
			
			Note:
			No community name is required for deactivation.
			Activation is only possible by entering a community name. A community name can only be saved when the protocol is activated.
				After restart

Table 329: Description of Configuration Scripts for “SNMP”

Parameters	Status	Call-Up	Output/Input	Valid
SNMP Trap Receiver Configuration for v1 and v2c Any number of trap receivers can be configured. A trap receiver that has been set up is always active; the data set must be completely deleted to deactivate it.				
IP address of a trap receiver	read	get_snmp_data v1-v2c-trap-receiver-address <Nummer>	Specifies the IP address of the trap receiver that the controller is to send the v1 or v2 traps to. The <number> parameter enables consecutive reading of related data from the individually configured trap receiver for a short period of time (without interim changing of the data). This is a consecutive number that is not connected to the data. If the number is not included, the data of the first receiver are read.	Right away
Community Name	read	get_snmp_data v1-v2c-trap-receiver-community-name <Nummer>	Specifies the community name that the SNMP agent of the controller sends in the Trap Header. Parameter <number> see section “IP Address of a Trap Receiver”.	Right away
Trap version	read	get_snmp_data v1-v2c-trap-receiver-version <Nummer>	Specifies the SNMP version (“v1” or “v2c”) via which the SNMP agent sends the traps to the associated trap receiver address. Parameter <number> see section “IP Address of a Trap Receiver”.	Right away

Creating/ deleting a trap receiver	write	config_snmp
		v1-v2c-trap-receiver-edit=<Value1>
		v1-v2c-trap-receiver-address=<Value2>
		v1-v2c-trap-receiver-community-name=<Value3>
		v1-v2c-trap-receiver-version=<Value4>
			Create a new trap receiver (value1=add) or delete an already configured trap receiver (value1=delete).
			Other parameters:
			<Value2> = IP address (number.number.number.number) that the controller is to send the traps to.
			<Value3>: Community string (string), which the controller enters in the trap header.
			<Value4>: SNMP version, via which the traps are sent (v1 or v2c).
			Note:
			All parameters must also be entered when deleting a trap receiver, as this is the only means to uniquely identify the data set.
				After restart

Table 329: Description of Configuration Scripts for “SNMP”

Parameters	Status	Call-Up	Output/Input	Valid
Configuration of SNMP v3 Any number of SNMP v3 users can be created. A user that has been set up is always active; the complete data set must be deleted to deactivate a user.				
Authentication Name	read	get_snmp_data v3-auth-name <Nummer>	Specifies the user name for the v3 user. The <number> parameter enables consecutive reading of the related data from the individually configured trap receiver for a short period of time (without interim changing of the data). This is a consecutive number that is not connected to the data. If the number is not included, the data of the first user are read.	Right away
Authentication encryption type	read	get_snmp_data v3-auth-type <Number>	Specifies the type of encryption that the v3 user uses (none, MD5, or SHA). Parameter <number> see “Authentication Name”.	Right away
Authentication key	read	get_snmp_data v3-auth-key <Nummer>	Specifies the key string for authentication. Parameter <number> see “Authentication Name”.	Right away
Privacy encryption type	read	get_snmp_data v3-privacy <number>	Specifies the type of privacy encryption for the v3 user (none, DES, or AES). Parameter <number> see “Authentication Name”.	Right away
Privacy key	read	get_snmp_data v3-privacy-key <number>	Specifies the key string for privacy. If nothing is entered, the SNMP agent uses the “Authentication Key”. Parameter <number> see “Authentication Name”.	Right away
Trap receiver address	read	get_snmp_data v3-notification-receiver <number>	IP address of an SNMP manager that the agent traps for this v3 user are sent to. If nothing is entered here, no traps are sent for this user. Parameter <number> see “Authentication Name”.	Right away

Table 329: Description of Configuration Scripts for “SNMP”

Parameters	Status	Call-Up	Output/Input	Valid

Add new v3-User	write	config_snmp
		v3-edit=add
		v3-auth-name=<Value1>
		v3-auth-type=<Value2>
		v3-auth-key=<Value3>
		v3-privacy=<Value4>
		v3-privacy-key=<Value5>
		v3-notification-receiver=<Value6>
			Creating a new v3 user.
			This must be a new, unique user name.
			
			Parameters:
			User name (<Value1> = string, min. 8 and max. 32 characters, lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces)
			Encryption method. (<Value2> = none, MD5 or SHA).
			Key string for authentication, (<Value3> = String, min. 8 and max. 32 characters, lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces)
			Privacy encryption method (<Value4> = none, DES or AES).
			Privacy key string (<Value5> = String, min. 8 and max. 32 characters, lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces), can also be blank; in this case the authentication key will be used. The IP address of a trap receiver is transmitted as the notification receiver (<Value6> = number.number.number.number)
			This parameter is not required if no v3 traps are to be sent.
				After restart

Delete v3 user	write	config_snmp
		v3-edit=delete
		v3-auth-name=<Value>
			Deleting a v3 user that has been set up.
			Because the doubled allocation of the same user name is prevented when creating a user, the name is sufficient to uniquely identify a data set (<Value> = string).
				After restart

18.3.1.10 WagoLibCpuUsage.lib

The controller 750-8212supports the following function blocks of the “WagoLibCpuUsage.lib” library:

- CPU_Usage

The document containing the description of the library and the function block it includes is available for download on the Internet at www.wago.com.

18.3.1.11 WagoLibDiagnosticIDs.lib

The controller 750-8212supports the following function blocks of the “WagoLibDiagnosticIDs.lib” library:

- DIAGNOSTIC_SEND_ID
- DIAGNOSTIC_SET_TEXT_FOR_ID

The document containing the description of the library and the function block it includes is available for download on the Internet at www.wago.com.

18.3.1.12 WagoLibLed.lib

The controller 750-8212supports the following function blocks of the “WagoLibLed.lib” library:

- LED_SET_STATIC
- LED_SET_BLINK
- LED_SET_FLASH
- LED_SET_ERROR
- LED_RESET_ERROR
- LED_RESET_ALL_ERRORS
- LED_GET_STATE
- LED_GET_STATE_ASYNC

The document containing a description of this library and the function blocks it includes is available for download on the Internet at www.wago.com.

18.3.1.13 WagoLibNetSnmp.lib

The controller 750-8212supports the following function blocks of the “WagoLibNetSnmp.lib” library:

- snmpGetValueCustomOID_INT32
- snmpGetValueCustomOID_STRING
- snmpGetValueCustomOID_UINT32
- snmpRegisterCustomOID_INT32
- snmpRegisterCustomOID_STRING
- snmpRegisterCustomOID_UINT32
- snmpSetValueCustomOID_INT32
- snmpSetValueCustomOID_STRING
- snmpSetValueCustomOID_UINT32

The document containing the description of the library and the function block it includes is available for download on the Internet at www.wago.com.

18.3.1.14 WagoLibNetSnmpManager.lib

The controller 750-8212supports the following function blocks of the “WagoLibNetSnmpManager.lib” libraries:

- SNMPM_DINT_TO_TLV
- SNMPM_UDINT_TO_TLV
- SNMPM_STRING_TO_TLV
- SNMPM_TLV_TO_DINT
- SNMPM_TLV_TO_UDINT
- SNMPM_TLV_TO_STRING
- SNMPM_GET
- SNMPM_GET_V3
- SNMPM_SET
- SNMPM_SET_V3

The document containing a description of this library and the function blocks it includes is available for download on the Internet at www.wago.com.

18.3.1.15 WagoLibSSL.lib

The controller 750-8212supports the following function blocks of the “WagoLibSSL.lib” library:

- SSL_CTX
- SSL_CTX_load_verify_locations
- SSL_CTX_sess_set_cache_size
- SSL_CTX_set_client_CA_list
- SSL_CTX_set_method
- SSL_CTX_use_certificate_file
- SSL_CTX_use_PrivateKey_file
- SSL_free
- SSL_get_error
- SSL_Hndshk_Accept
- SSL_Hndshk_Connect
- SSL_load_client_CA_file
- SSL_read
- SSL_shutdown
- SSL_write

The document containing a description of this library and the function blocks it includes is available for download on the Internet at www.wago.com.

18.3.1.16 WagoLibTerminalDiag.lib

The controller 750-8212supports the following function blocks of the “WagoLibTerminalDiag.lib” library:

- GET_TERMINALDIAG

The document containing a description of this library and the function blocks it includes is available for download on the Internet at www.wago.com.

List of Figures

List of Tables

WAGO Kontakttechnik 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