SIEMENS

SIMATIC NET

LOGO! - Industrial Ethernet LOGO! CMR2020, LOGO! CMR2040

Operating Instructions

05/2015

C79000-G8976-C356-02

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C356-02
Ⓟ 05/2015 Subject to change

Preface

Validity of this manual

This document contains information on the following LOGO! products:

- LOGO! CMR2020
  Hardware product version: 1
  Firmware version: V1.1.4
  Article number: 6GK7 142-7BX00-0AX0

  Communication module for connection of LOGO! 8 to the GSM/GPRS network (2G)

- LOGO! CMR2040
  Hardware product version: 1
  Firmware version: V1.1.4
  Article number: 6GK7 142-7EX00-0AX0

  Communication module for connection of LOGO! 8 to the LTE network

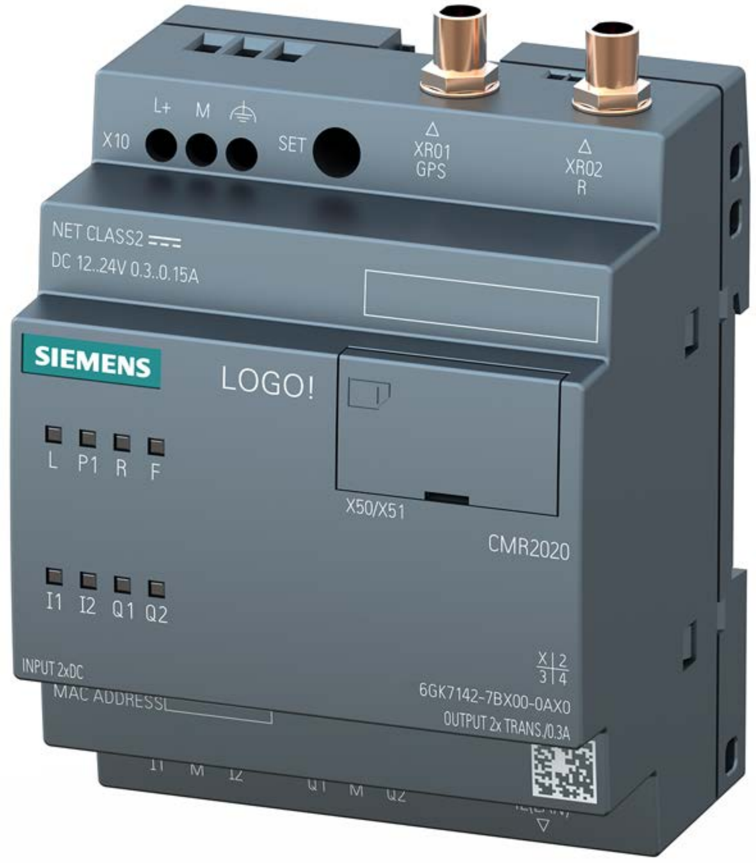


Figure 1 LOGO! CMR2020

The two devices differ in the supported mobile wireless standards. The remaining range of functions of both devices is identical.

Product names and abbreviations

- CMR or device

  In this document, the term "CMR" or "device" is also used instead of the full product name "LOGO! CMR2020 or LOGO! CMR2040. CMR is the abbreviation for Communication Module Radio.
- BM or LOGO! BM

  Basic module: LOGO! 8
- WBM

  Web Based Management; Web user interface with which the CMR is configured.
- SD card

  Below, the term “SD card" is used instead of micro SD card.

Purpose of the manual

This manual supports you during the configuration, installation, commissioning and operation of the two LOGO! wireless modules LOGO! CMR2020 and LOGO! CMR2040:

A detailed example (Page 103) supports you during commissioning.

New in this release

- Approvals ATEX, UL and US HazLoc, refer to the section Approvals (Page 129).
- Editorial revision

Replaced documentation

This manual replaces the manual release 09/2014.

Current manual release on the Internet

You will also find the current version of this manual on the Internet pages of Siemens Industry Online Support under the following entry ID:

91689511 (http://support.automation.siemens.com/WW/view/en/91689511)
> Entry list > Entry type "Manuals"

Sources of information and other documentation

You will find an overview of further reading and references in the Documentation references in this manual.

Use of the device

Connection of a LOGO! BM to an LTE, UMTS or GSM/GPRS mobile wireless network and a GPS system.

⚠ WARNING

Impairment of medical devices and data media

The device contains a wireless transmitter that could, under certain circumstances, impair the functionality of electronic medical devices such as hearing aids or pacemakers. Do not use the device in places where the operation of wireless devices is prohibited. You can obtain advice from your physician or the manufacturer of such devices.

To prevent data media from being demagnetized, do not keep disks, credit cards or other magnetic data media near the device.

License conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product.

The license conditions for open source software are stored on the device and can be read out using the WBM:

In the header of each page there is an icon with which you can download the OSS license texts.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SIMATIC NET

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD

  The DVD ships with certain SIMATIC NET products.

- On the Internet under the following entry ID:

  50305045 (http://support.automation.siemens.com/WW/view/en/50305045)

Service & Support

In addition to the product documentation, the comprehensive online information platform of Siemens Automation Customer Support supports at any time and at any location in the world. You will find the Service & Support pages on the Internet at the following address: (www.siemens.com/automation/service&support)

Apart from news, you will also find the following information there:

- Product information, Product Support, Applications & Tools
- Technical Forum
- Technical Support - Ask the Siemens experts
- Our service offer:
  - Technical Consulting, Engineering support
  - Field Service
  - Spare parts and repairs
  - Maintenance, optimization, modernization and more

You will find contact data on the Internet at the following address: (www.automation.siemens.com/partner)

SITRAIN - Siemens training for automation and industrial solutions

With over 300 different courses, SITRAIN covers the entire Siemens product and system spectrum in the field of automation and drive technology. Apart from the classic range of courses, we also offer training tailored for individual needs and a combination of different teaching media and sequences, for example self-learning programs on CD-ROM or on the Internet.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

(www.siemens.com/sitrain)

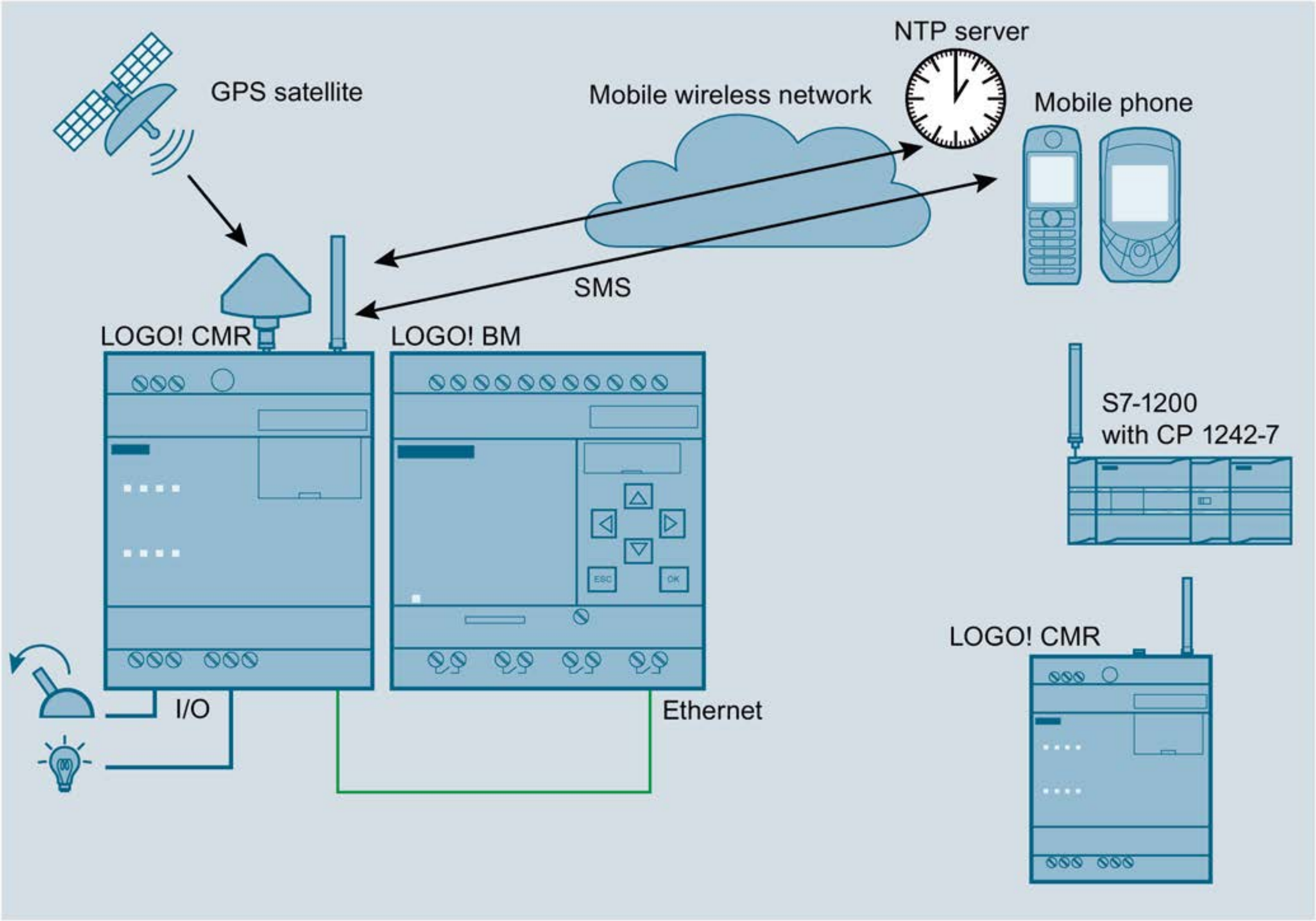
Table of contents

Properties and functions 1

1.1 Connection using mobile wireless, Internet and GPS

Configuration

Below a configuration example with LOGO! CMR is illustrated.



Supported mobile wireless standards

- LOGO! CMR2020
  - GSM/GPRS
  - GPS
- LOGO! CMR2040

  Mobile wireless standards for Europe/Australia:
  - LTE 800 (B20) / 1800 (B3) / 2600 (B7)

    If the establishment of a mobile data connection to the LTE mobile wireless network fails, the dial-in falls back automatically to the next lower mobile wireless network UMTS or GPRS.
  - 3G: HSPA+ / UMTS 900 (B8) / 2100 (B1) / 1800 (B3)
  - 2G: QB GSM/GPRS/EDGE
  - GPS

Wireless connection via the mobile wireless network

With the CMR, you establish a mobile data connection to a mobile wireless network: LTE, UMTS or GSM/GPRS mobile wireless network. You are also in a position to connect the CMR to a GPS system.

With the CMR, you can do the following:

- Read the information of a BM using SMS: Process image, inputs/outputs, memory bits and much more
- Notify event-based using SMS.

The CMR is connected locally to a BM via Ethernet and establishes the connection to a mobile wireless network.

You can also operate the CMR in stand-alone mode: in other words without a connected BM. To connect the I/O you use the two inputs and outputs of the CMR.

Requirements for operation

Mobile wireless network within reach

- To be able to send and receive SMS messages, there must be a reachable mobile wireless network.

Sending SMS messages

- You require a SIM card from a mobile wireless provider. The SIM card must be activated for sending SMS messages. This SIM card must have a telephone number.

Time-of-day synchronization with NTP

- You require a SIM card with mobile data options: This SIM card does not need to have a telephone number.
- You require a mobile wireless network within reach that supports the exchange of mobile data.

1.2 Configuration and functions

Configuring the CMR

You configure the CMR locally using a Web user interface (WBM) that can be displayed with a Web browser:

1. Connect a PC to the "X1P1 IE (LAN)" connector of the CMR. To do this, use an Ethernet patch cable.
2. Start the Web user interface as described in the section Configuration (Page 41).

Functions

The CMR supports the following basic functions:

- WBM for the configuration; protected with login and password query.
- Cyclic reading of the process image from the BM.
- From incoming events, events coming from the process or internal, suitable output reactions configured using WBM are generated: For example sending an alarm SMS message.
- Event configurations and reactions, for example trigger an alarm SMS message if a value changes in the process image.

  The process image consists of the following elements that you can use for an event or alarm configuration:

  - Digital and analog inputs
  - Digital and analog outputs
  - Digital and analog bit memory
  - Shift register
  - Operator keys
  - Function keys
- Access to variable memory (VM)

  Via the variables memory, you have access to the current values of function blocks, for example counter function blocks.
- Time-of-day synchronization
  - NTP
  - GPS
  - Mobile wireless network (depending on the mobile wireless provider)
- Forwarding the time of day to the BM
- GPS position
  - Querying position by SMS
  - Forwarding position to the BM

- The two inputs/outputs of the CMR can be configured using the WBM and read or set using SMS messages.
- Access protection when receiving SMS messages: Only SMS messages from configured telephone numbers are permitted.

Diagnostics via the local area network

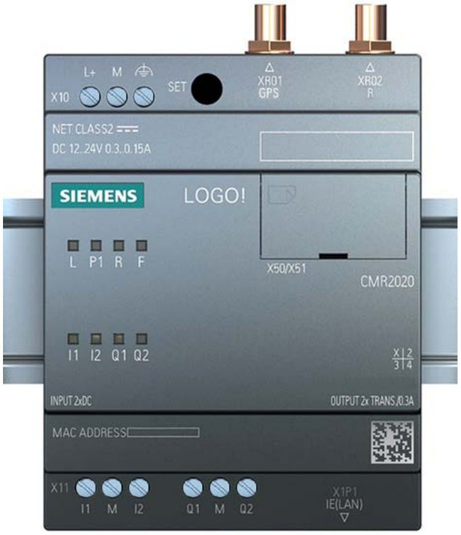
Using the WBM you can view a diagnostics buffer for diagnostics purposes. Is also possible to download and save the diagnostics buffer on an SD card or PC.

The following are logged, for example:

- Operating messages such as startup, change to the configuration.
- Establishment/interruption of the connection to the BM.
- Establishment/interruption of the connection to the mobile wireless network.
- Establishment/interruption of the mobile data connection.
- Warnings when reading in the configuration from an SD card or from the PC.
- Time-of-day synchronization

Connectors and LED display 2

2.1 Appearance of the device



Operator control/connector and display elements of the CMR

Element	Function
X10 (L+, M)	Power supply connector
SET	Service button SET, refer to the section "Functions of the SET button"
XR01	GPS antenna connector
XR02	Mobile wireless antenna connector
LED "L"	Power supply indicator
LED "P1"	LAN interface indicator
LED "R"	Mobile wireless signal strength indicator
LED "F"	Error/fault indicator
X50/X51	Slot for SIM and micro SD card
LED I1	Input 1 indicator
LED I2	Input 2 indicator
LED Q1	Output 1 indicator
LED Q2	Output 2 indicator
I1	Input 1 connector
M	Ground
I2	Input 2 connector
Q1	Output 1 connector
M	Ground
Q2	Output 2 connector
X1P1	LAN connector

Functions of the SET button

The SET button has different functions depending on how long you hold it pressed.

Operator input	Function
Keep pressed for 5 s	Restart
Keep pressed for 5 to 10 seconds	Shutting down the device to a safe status: • No LEDs are lit. • The device can be disconnected from the power supply.
Keep pressed for longer than 10 seconds	Reset to factory settings

2.2 Interfaces

Connection to a the local area network

Port X1P1 of the CMR is intended for LAN connection to the local network/PC and to connect to the BM. The IP address of port X1P1 can be configured.

Connection to the mobile wireless network and GPS

For the wireless connection, the CMR has two SMA sockets:

- SMA socket for the mobile wireless network
- SMA socket for GPS reception

2.3 LEDs to display operation

The LEDs on the CMR provide information about the operating status of the device and the two inputs/outputs.

Meaning of the LEDs

LED	Status	Meaning
All LEDs	Flashing	Fatal error
	Lit	Firmware being updated
	Not lit	• No voltage present or applied • Device shut down
L Power supply	Off □	No external power supply connected
	On 🟩	Power supply connected
	Flashing 🟩	Initialization or reconfiguration active
P1 LAN	Lit green 🟩	Link
	Part flashes yellow and part lit green 🟨	Data
	Off □	No link or no cable connected
R Signal strength (mobile wireless)	Lit green 🟩	Very good
	Lit yellow 🟨	Medium
	Off □	No signal
	Flashing 🟩	Data

LED	Status	Meaning
F Error	OFF □	No error
	ON 🟥	Error (see also "Error LED lights up red" (Page 121))
	Flashing 🟥	Duplicate IP address detected. Ethernet interface unreachable.
I1 Input 1	Off □	U < 5 V
	Lit green 🟩	U > 8.5 V
I2 Input 2	Off □	U < 5 V
	Lit green 🟩	U > 8.5 V
Q1 Output 1	Off □	No voltage at output
	Lit green 🟩	Supply voltage at output
Q2 Output 2	Off □	No voltage at output
	Lit green 🟩	Supply voltage at output

Requirements for use 3

Antennas

To operate the CMR, you require an antenna that is tuned to the frequency bands of the mobile wireless provider you have selected.

- For GSM/GPRS transmission (LOGO! CMR2020):
  - 850 MHz, 900 MHz, 1800 MHz or 1900 MHz; quad-band
- For LTE transmission (LOGO! CMR2040 only):
  - 4G: 800 MHz (B20), 1800 MHz (B3), 2600 MHz (B7)
  - Fallback* to 3G (UMTS, HSUPA and HSDPA): 900 MHz (B8), 2100 MHz (B1)
  - Fallback* to 2G (GSM/GPRS): 850 MHz, 900 MHz, 1800 MHz or 1900 MHz

  * Fallback to the next lower standard (LTE > UMTS > GSM/GPRS and EDGE)

If you want to use GPS, you require an additional GPS antenna:

- Only use antennas from the accessories program for the CMR. For more information, refer to the section Antennas (Page 135).

Power supply

You require a power supply with a voltage between 12 VDC and 24 VDC that provides adequate voltage or current. For more information, refer to the section Technical specifications (Page 125).

SIM card

You require a SIM card of your mobile wireless provider with the corresponding PIN (Personal Identification Number).

Exception: SIM cards that are only used for the data service can be used without a PIN.

Only necessary if NTP is used:

- Activation for packet-oriented data services

  The SIM card must be activated for the packet-oriented data services in the mobile wireless network by your mobile wireless provider:

  - LOGO! CMR2020: GPRS
  - LOGO! CMR2040: LTE

    As the preferred connection, LOGO! CMR2040 first attempts to establish a connection to the LTE mobile wireless network.

    If the connection to the LTE mobile wireless network fails, the CMR attempts to establish a connection to the UMTS mobile wireless network.

    If the connection to the UMTS mobile wireless network fails, the CMR attempts to establish a connection to the GSM/GPRS mobile wireless network.
  - The following access data for the mobile wireless network must be present:: Access Point Name (APN), user name and password.

For more information, refer to the section Mobile wireless settings (Page 68).

Installation, connecting up, commissioning 4

4.1 Safety notices

Safety notices on the use of the device

The following safety notices must be adhered to when setting up and operating the device and during all associated work such as installation, connecting up or replacing devices.

Overvoltage protection

> NOTICE
>
> **Protection of the external power supply**
>
> If power is supplied to the module or station over longer power cables or networks, the coupling in of strong electromagnetic pulses onto the power supply cables is possible. This can be caused, for example by lightning strikes or switching of higher loads.
>
> The connector of the external power supply is not protected from strong electromagnetic pulses. To protect it, an external overvoltage protection module is necessary. The requirements of EN61000-4-5, surge immunity tests on power supply lines, are met only when a suitable protective element is used. A suitable device is, for example, the Dehn Blitzductor BVT AVD 24, article number 918 422 or a comparable protective element.
>
> Manufacturer:
> DEHN+SOEHNE GmbH+Co.KG Hans Dehn Str.1 Postfach 1640 D-92306 Neumarkt, Germany

4.2 Notices on use in hazardous areas

> ⚠WARNING
>
> EXPLOSION HAZARD
>
> DO NOT OPEN WHEN ENERGIZED.

> ⚠WARNING
>
> The device may only be operated in an environment with pollution degree 1 or 2 (see IEC 60664-1).

External power supply

- Use only an external power supply that complies with EN 60950.
- The output voltage of the external power supply must not exceed 30 VDC.
- The output of the external power supply must be short-circuit proof.

> NOTICE
>
> **Power supply**
>
> The power supply unit to supply the CMR must comply with the requirements for a limited power source according to IEC/EN 60950-1, section 2.5.
>
> The external power supply for the CMR must meet the requirements for NEC class 2 circuits as specified in the National Electrical Code ® (ANSI/NFPA 70).

Note the information in this section and in the installation and operating instructions from the manufacturer of the power supply.

> ⚠WARNING
>
> The equipment is designed for operation with Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS).
>
> This means that only SELV / LPS complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 must be connected to the power supply terminals. The power supply unit for the equipment power supply must comply with NEC Class 2, as described by the National Electrical Code (r) (ANSI / NFPA 70).
>
> If the equipment is connected to a redundant power supply (two separate power supplies), both must meet these requirements.

> ⚠WARNING
>
> EXPLOSION HAZARD
>
> DO NOT CONNECT OR DISCONNECT EQUIPMENT WHEN A FLAMMABLE OR COMBUSTIBLE ATMOSPHERE IS PRESENT.

> ⚠WARNING
>
> EXPLOSION HAZARD
>
> SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2 OR ZONE 2.

> ⚠WARNING
>
> When used in hazardous environments corresponding to Class I, Division 2 or Class I, Zone 2, the device must be installed in a cabinet or a suitable enclosure.

4.3 Notices on use in hazardous areas according to ATEX

⚠ WARNING

Requirements for the cabinet/enclosure

To comply with EU Directive 94/9 (ATEX95), the enclosure or cabinet must meet the requirements of at least IP54 in compliance with EN 60529.

⚠ WARNING

If the cable or conduit entry point exceeds 70 °C or the branching point of conductors exceeds 80 °C, special precautions must be taken. If the equipment is operated in an air ambient in excess of 50 °C, only use cables with admitted maximum operating temperature of at least 80 °C.

⚠ WARNING

Take measures to prevent transient voltage surges of more than 40% of the rated voltage. This is the case if you only operate devices with SELV (safety extra-low voltage).

4.4 Notices on use in hazardous areas according to UL HazLoc

⚠ WARNING

EXPLOSION HAZARD

DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS.

This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D or non-hazardous locations only.

This equipment is suitable for use in Class I, Zone 2, Group IIC or non-hazardous locations only.

Connectors with LAN (Local Area Network) marking

⚠ WARNING

Safety notice for connectors with LAN (Local Area Network) marking

A LAN or LAN segment, with all its associated interconnected equipment, shall be entirely contained within a single low-voltage power distribution and within single building.
The LAN is considered to be in an "environment A" according IEEE802.3 or "environment 0" according IEC TR 62102, respectively.

Never make direct electrical connection to TNV-circuits (Telephone Network) or WAN (Wide Area Network).

4.5 Installing the device

The CMR is suitable for rail mounting on a 35 mm DIN EN 50 022 rail. On the rear of the device there is a locking mechanism with a spring catch.

Installing on a DIN rail / removing from a DIN rail

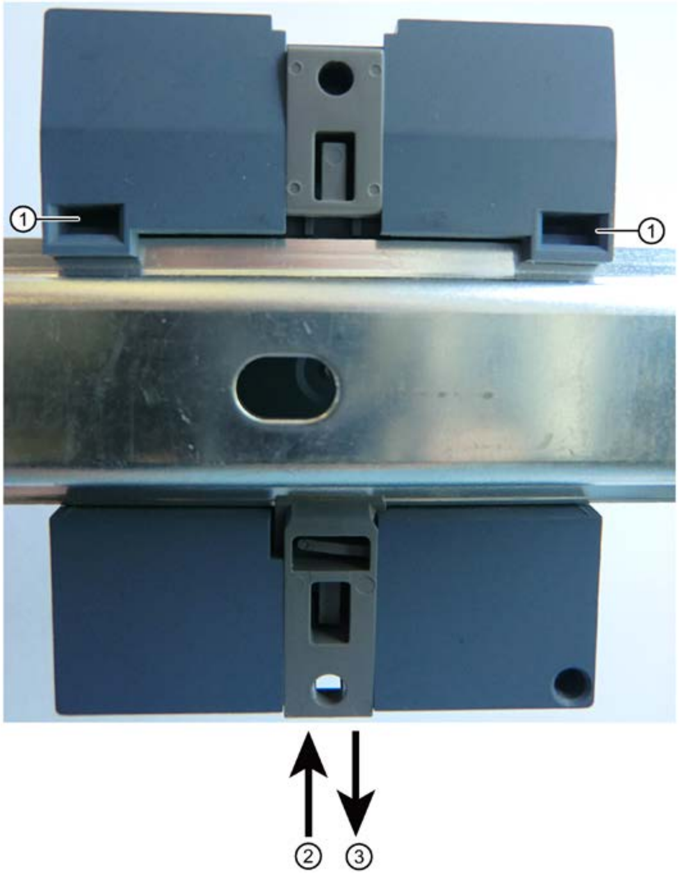


Figure 4-1 Installing on a DIN rail / removing from a DIN rail

Mounting

To mount the CMR on a DIN rail, follow the steps below:

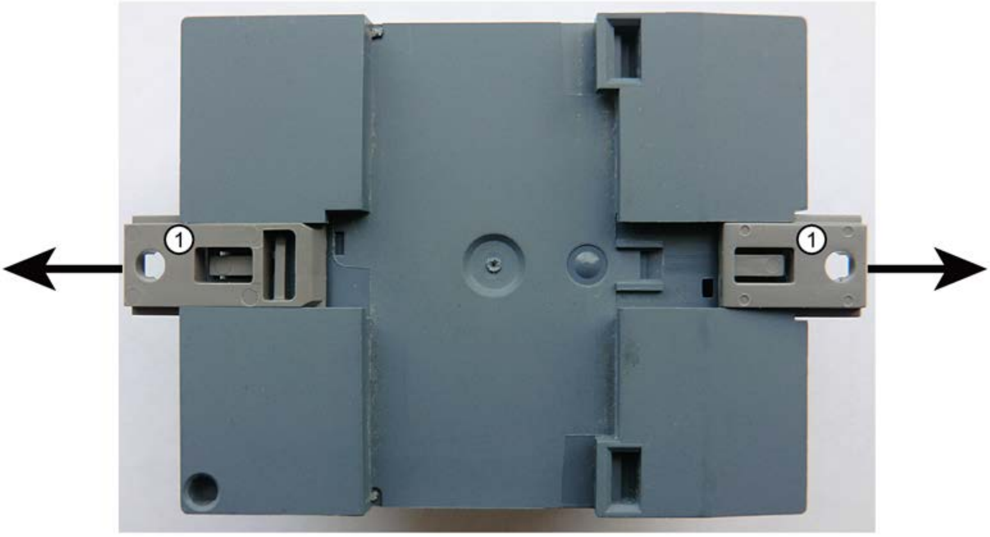
1. Fit the upper part of the locking mechanism ① of the device on to the DIN rail.
2. Press the device down against the DIN rail until the spring catch ② locks in place.

Removal

To remove the CMR from a DIN rail, follow the steps below:

1. Using a screwdriver, pull down the spring catch on the rear of the device ③.
2. Remove the device from the DIN rail.

Wall mounting



To mount the CMR on a wall, follow the steps below:

1. Using a screwdriver, pull the two spring catches ① on the rear of the device towards the outside.
2. Feed the screws through the openings in the catches and secure the device to the wall.

4.6 Connecting up the device

4.6.1 X1P1 (LAN) interface

Connecting the X1P1 (LAN) interface

The interface supports autonegotiation and autocrossing. For the connection, use a patch cable with an RJ-45 plug. You will find the properties of the X1P1 interface in the technical specifications.

- Connect your local area network, the PC or the BM to X1P1 (LAN) of the CMR.

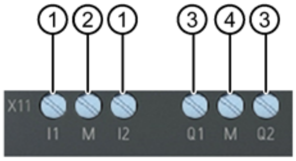
4.6.2 Inputs and outputs

Refer to the technical specifications for the load capabilities of the inputs and outputs.

Ideally, use a debounced switch to connect to a LOGO! CMR input.

Inputs and outputs

The CMR has two digital inputs and two digital outputs. The connecting terminals are on the underside of the device.



① Inputs I1 and I2

② Reference potential inputs

③ Outputs Q1 and Q2

④ Reference potential outputs

Inputs I1 and I2

The connecting terminals of the inputs are labeled I1 and I2. The reference potential for both inputs is "M".

Using the Web user interface, you can assign any function to each input, for example triggering an alarm SMS message, refer to the section Monitoring (Page 84).

The status of an input can also be read using SMS.

Outputs Q1 and Q2

The connecting terminals of the outputs are labeled Q1 and Q2. The reference potential for both outputs is "M".

You can assign any function to each output using the Web user interface see section Monitoring (Page 84). The outputs can be set and reset using SMS messages.

Note

Remember the electrical load capacity of the output.

You will find the electrical values for the inputs and outputs in the section Technical specifications (Page 125).

4.6.3 Connecting the antenna

⚠ WARNING

Risk of lightning strikes when installed outdoors

If you install an antenna outside, you need to ground the antenna to protect it from lightning strikes. This work must only be carried out by qualified personnel.

NOTICE

Damage to devices due to incorrect accessories

Select the antenna suitable for your frequency band from the accessories. Other antennas could interfere with product characteristics or lead to defects.

The CMR has two antenna sockets of the type SMA for connecting the antennas. The antennas must have an impedance of approx. 50 Ω.

Follow the operating instructions of the antennas used. See also section Antennas (Page 135).

Frequency bands in Europe and other regions

Depending on the frequency bands your mobile wireless provider uses:

- Select the antenna suitable for your frequency band. See section Antennas (Page 135).

Signal strength

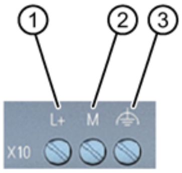
During installation make sure that there is a good signal strength:

- If the "R" LED is lit green or flashes green, the signal strength is very good.
- Lit yellow or flashing yellow signals medium quality.
- If the "R" LED is not lit, this indicates an inadequate signal strength, refer also to the section LEDs to display operation (Page 17).

Large metallic objects in the vicinity of the antennas, for example reinforced concrete, impair the signal strength.

4.6.4 Power supply

Screw terminals for the power supply



① L+ = live wire, positive pole of the DC voltage 12/24 VDC

② M = negative pole/ground of the DC voltage 12/24 VDC

③ Functional ground

- Serves to improve electromagnetic compatibility and to specify a common reference potential for all signals.
- Is achieved efficiently by a connection to the DIN rail.

Note

Power supply unit of the CMR is not electrically isolated

No electrical isolation means that the input and output circuits are not galvanically isolated.

The CMR operates with a DC voltage of 12 to 24 VDC, nominally 24 VDC. The nominal current consumption is a maximum of 250 mA at 12 V.

- Connect a suitable power supply to the screw terminals.
- Use copper wires only.
- Use only cables that are approved for at least 70 °C.

Wire:	0.5 to 3 mm² (20 to 18 AWG)
Stranded wire:	0.5 to 2.5 mm²
Tightening torque for screw terminals:	0.6 to 0.8 Nm

Turning off the CMR

NOTICE

Avoidance of sudden disconnection of the power supply

Avoid abrupt, uncontrolled disconnection of the CMR from the power supply: There is a risk of damaging the CMR!

1. Hold down the SET button for 5 to 10 seconds.

   The CMR shuts down to the safe status: All LED indicators are off.

2. Disconnect the CMR from the power supply.

The CMR can no longer be woken out of the shutdown status. Power cycling necessary.

4.7 Commissioning the device

4.7.1 Steps in commissioning

To commission the CMR, follow the steps below:

Overview of commissioning

1. Note the requirements for operating the CMR, refer to the section Requirements for use (Page 19).
2. SIM card: Before you insert the SIM card, note the information in Insert the SIM card and enter the PIN (Page 29) regarding the two different methods:
   – Method 1: For a new device
   – Method 2: Replacing the SIM card in a device that has already been in use.
3. Connect a PC with a Web browser to the local interface X1P1 of the CMR, refer to the section Establishing a connection to the CMR (Page 42).
4. Insert the SIM card, see section "Insert the SIM card and enter the PIN (Page 29)".
5. Connect the antennas.
6. Connect the CMR to the power supply.
7. Enter the PIN of the SIM card via the Web user interface of the CMR, refer to the section PIN of the SIM card (Page 70).
8. Align the antenna, refer to the section "Wireless cell (Page 73)".
9. Set up the CMR according to your requirements, refer to the section Configuration (Page 41).

4.7.2 Insert the SIM card and enter the PIN

NOTICE

Disconnecting the CMR from the power supply before inserting or removing the SIM card

Do not remove the SIM card during operation.

1. Shut the device down to a safe status.
2. Disconnect the CMR from the power supply before inserting or removing the SIM card.

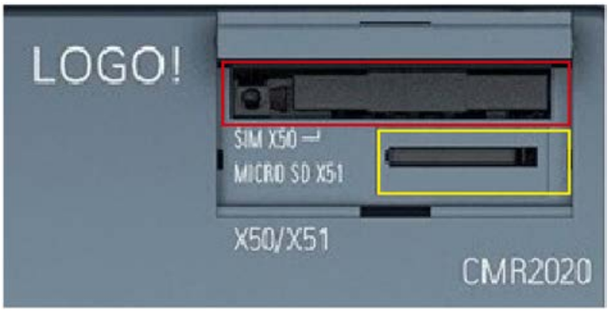


Figure 4-2 Compartment for the SIM card (red rectangle)

The compartment for the SIM card is located on the front of the CMR.

Status of the CMR before inserting/removing the SIM card

The CMR is brand new or has been reset to the factory settings:

- A SIM card is inserted for the first time.

The CMR is or has already been in operation:

- Only a different SIM card is inserted.

Inserting/removing the SIM card

1. In the WBM in "WAN", "Mobile wireless settings" tab, deselect the "Activate mobile wireless interface“ check box:
   The mobile wireless interface is turned off.
2. Shut the CMR down to the safe status: "Turning off the CMR" (Page 28).
3. Disconnect the CMR from the power supply.
4. Only if the CMR is or was in operation: Remove the SIM card and close the compartment.

   To remove the SIM card, press the left-hand sunken ejector button with a sharp object.
5. Insert the SIM card into the compartment until you can feel the card lock in place.
6. Restart the CMR by connecting up the power supply.
7. In the WBM, in "WAN", "Mobile wireless settings" tab, select the "Activate mobile wireless interface" check box:
   The mobile wireless interface is once again ready for operation.
8. Enter the PIN of your SIM card in WBM in the "WAN", Mobile wireless settings" tab.

Note

Entry of an incorrect PIN

The last entered (incorrect) PIN is saved. This means that when changing the configuration (except the PIN) or when restarting the CMR, no further PIN entry attempt is used up.

For this reason, do not change the PIN of the SIM card to the previously stored incorrect PIN outside the CMR.

9. Click the "Apply" button: the PIN of your SIM card is adopted.
10. Make the appropriate settings, see section Configuration (Page 41).

Unlocking the SIM card

If you enter the PIN incorrectly three times, the SIM card will be locked.

Unblock the SIM card as follows:

1. Shut the CMR down to the safe status: "Turning off the CMR" (Page 28).
2. Disconnect the CMR from the power supply.
3. Remove the SIM card and close the compartment.

   To remove the SIM card, press the left-hand sunken ejector button with a sharp object.
4. Insert the removed SIM card in a mobile phone.
5. Unblock the SIM card by entering the PUK or the SuperPIN.

   You will have received the PUK or SuperPIN from your mobile wireless provider along with the SIM card.

Result: The SIM card is unblocked and can be used again.

4.7.3 Inserting the micro SD card

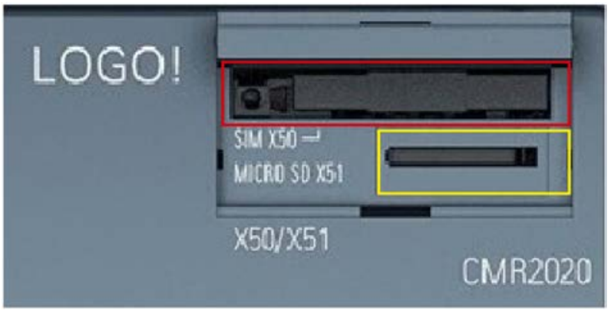


Figure 4-3 Slot for the micro SD card (yellow rectangle)

The CMR supports all normal commercially available micro SD cards.

NOTICE
Do not remove/insert an SD card during operation
You can only remove or insert the SD card when the CMR is turned off/shut down.
If you remove or insert the SD card during operation, data on the card can be damaged.

Note

Recommended SD card

For example:

- Memory: max. 4 GB
- Max speed Class 6
- FAT 32

Inserting the micro SD card

- Insert the SD card into the compartment until you can feel the card lock in place.

Removing the micro SD card

- By pressing, unlock the card and remove it from the slot.

Application examples 5

Requirement

The following applies to all application examples:

1. First familiarize yourself with the safety notices.
2. Put the CMR into operation as described in the section Installation, connecting up, commissioning (Page 21).

Possible applications

The CMR has a wide variety of possible uses in various areas of application. In this section, you will find configuration examples and use cases for the following:

- Mobile wireless communication without LOGO! BM
- Mobile wireless communication with LOGO! BM
- Position detection (GPS)
- Time-of-day synchronization with NTP

5.1 Mobile wireless communication without LOGO! BM

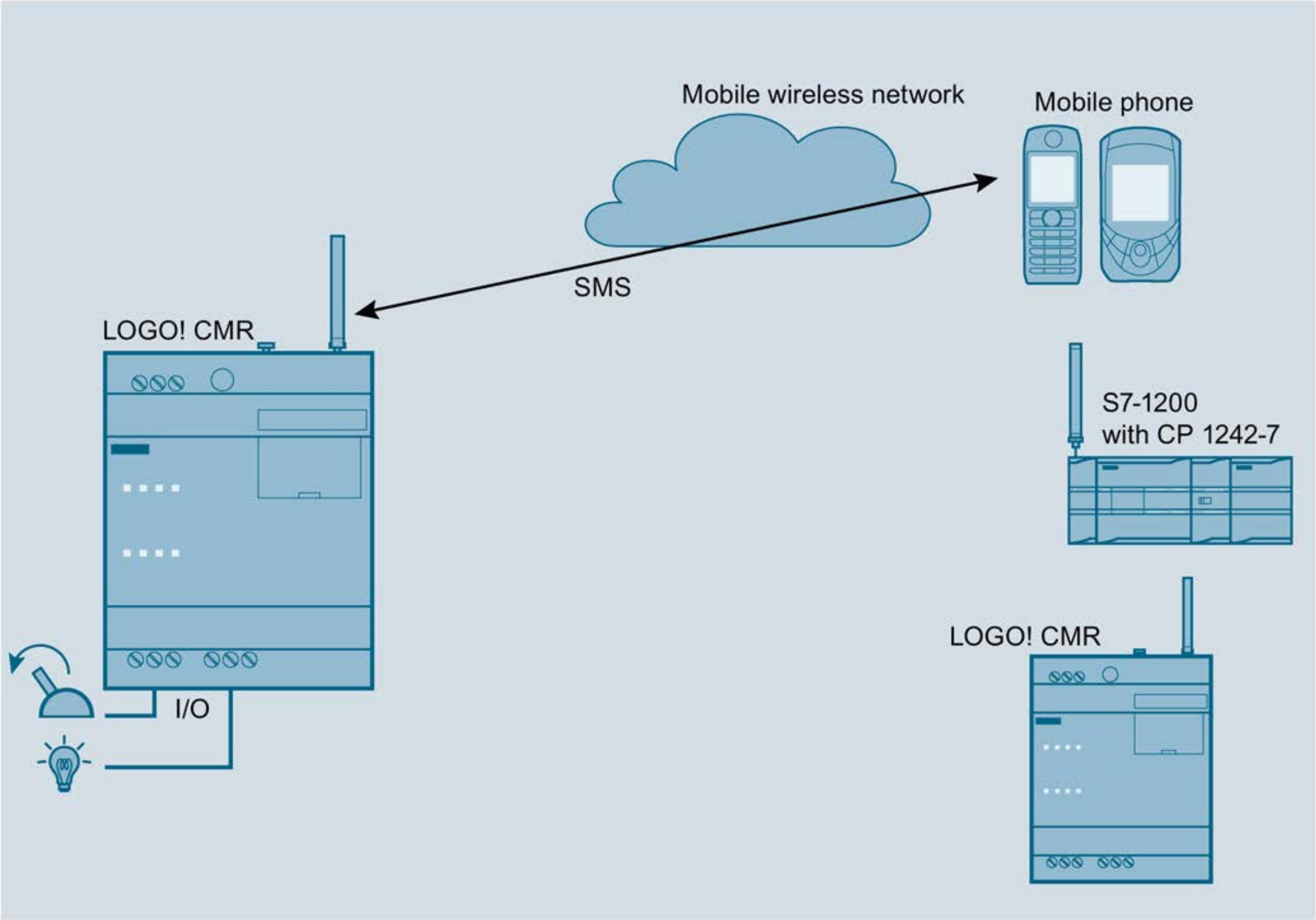


Figure 5-1 Mobile wireless communication without LOGO! BM

You can operate the CMR without a BM being connected. If the CMR is connected to a mobile wireless antenna, the following functions are available:

- Sending an SMS message due to a signal at the input of the CMR
- Receiving an SMS message:
  - Setting an output of the CMR.
  - Sending status information via the CMR using SMS messages.

Using the WBM of the CMR, you can configure events such as changing of input signals as well as actions. The actions are triggered when the events occur.

Requirements

- Installation, connecting up, commissioning (Page 21) completed.
- Antenna for mobile wireless reception connected.

Procedure

To configure access via the mobile wireless network, follow the steps below:

1. First establish a configuration connection between the CMR and a connected PC. To do this, use an Ethernet patch cable.
   See Establishing a connection to the CMR (Page 42)
2. Configure the mobile wireless connection:
   See Mobile wireless settings (Page 68)
3. Configure the device using the WBM.

5.2 Mobile wireless communication with LOGO! BM

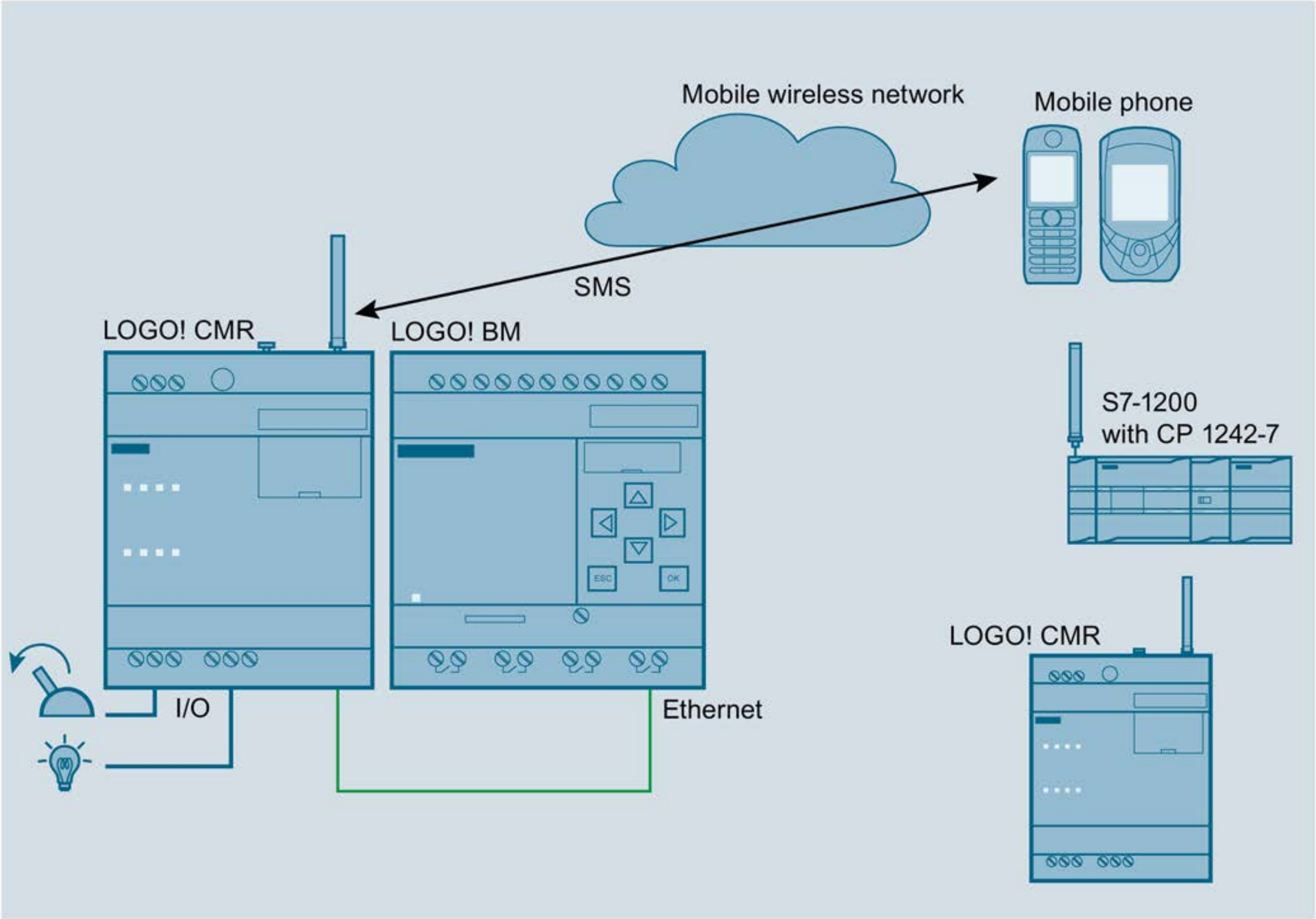


Figure 5-2 Mobile wireless communication with LOGO! BM

If the CMR is connected to the BM, and if you have a mobile wireless antenna connected, you can use all the functions available in operation without a connected BM. In addition to this, access to the LOGO! BM is expanded:

- Sending an SMS message due to an event in the connected BM.
- Receiving an SMS message:
  - Triggering an action in the connected BM.
  - Sending status information via the BM using SMS messages.

Configuration using the WBM also includes access to the components of the BM.

Requirements

1. Installation, connecting up, commissioning (Page 21) completed.
2. Antenna for mobile wireless reception connected.

Procedure

To set up access via the mobile wireless network and to establish a connection to the BM, follow the steps below:

1. First establish a configuration connection between the CMR and a connected PC. To do this, use an Ethernet patch cable.
   See Establishing a connection to the CMR (Page 42)
2. Configure the mobile wireless connection:
   See Mobile wireless settings (Page 68)
3. Configure the device using the WBM.
4. When configuration is completed, disconnect the CMR from the PC.

Note

Using a switch

When using a switch, e.g. LOGO! CSM, do not disconnect the connections: BM, CMR and PC can be operated at the same time.

5. If you do not use a switch: Connect the CMR to the BM.

5.3 Position detection (GPS)

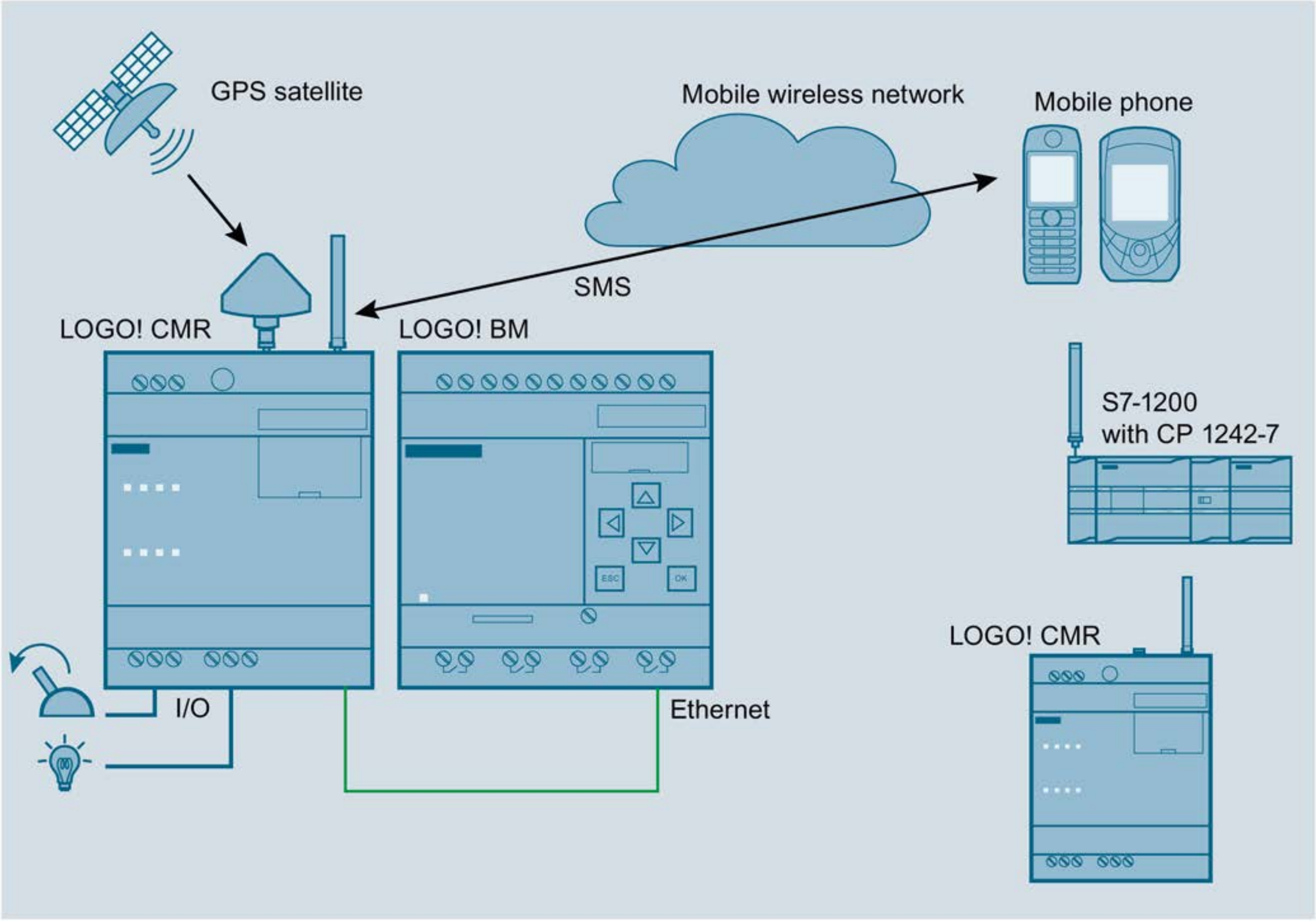


Figure 5-3 Position detection (GPS)

The CMR is equipped with a GPS interface via which the position data of the LOGO! station can be determined. If a GPS antenna is connected to the GPS interface, the following functions are available to you:

- Detecting position data:
  - Due to an event at an input of the CMR.
  - Due to an event from the BM.
  - Due to a received SMS message (with the mobile wireless antenna connected)
- Sending detected position data:
  - By SMS message
  - To the BM

To be able to use the functions listed above, you first need to activate (Page 49) the GPS interface in the WBM of the CMR. For correct position detection, the GPS signals need to be received from three satellites.

Requirements

1. Installation, connecting up, commissioning (Page 21) completed.
2. Antenna for mobile wireless reception connected.

   If only position detection using GPS is required, the mobile wireless antenna does not need to be connected. You only require a connected mobile wireless antenna when data is forwarded using SMS messages.
3. Antenna for GPS reception connected.

Procedure

To set up access via the mobile wireless network and to establish a connection to the BM, follow the steps below:

Note

Using the CMR for mobile wireless communication without BM

If you use the CMR in Mobile wireless communication without LOGO! BM (Page 34), the last two steps of the procedure described below can be omitted.

1. First establish a configuration connection between the CMR and a connected PC. To do this, use an Ethernet patch cable.
   See Establishing a connection to the CMR (Page 42)
2. Configure the mobile wireless connection:
   See Mobile wireless settings (Page 68)
3. Activate GPS reception (Page 49).
4. When configuration is completed, disconnect the CMR from the PC.

   Note

   Using a switch

   When using a switch, e.g. LOGO! CSM, do not disconnect the connections: BM, CMR and PC can be operated at the same time.
5. If you do not use a switch: Connect the CMR to the BM.

5.4 Time-of-day synchronization

Time-of-day synchronization for the CMR can be configured using three time-of-day synchronization methods.

The time-of-day synchronization method is set in the configuration on the "System" page in the "System time" (Page 51) tab:

- Synchronization with an external NTP server accessible via the mobile wireless network.
- Time of day from the GPS signal: The GPS antenna must be connected.
- Time of day from the mobile wireless network

  The availability of the time of day depends on the mobile wireless provider.

Note

The CMR does **not set itself automatically** to a time of day synchronization method. You need to select a time of day synchronization method in the configuration.

Note

If you use time-of-day synchronization of the BM via the CMR, disable the standard/daylight saving setting on the BM to ensure a consistent time.

If you enable the time of day in the WBM, you can also make a setting in the WBM so that the CMR also synchronizes the BM with the time of day (time-of-day forwarding).

"Forward time of day to LOGO! BM" is enabled:

Even if time-of-day synchronization is disabled, the time of day is forwarded to the LOGO! BM . In this case, only the manual settings are transferred to the LOGO! BM .

The following figure provides an overview:

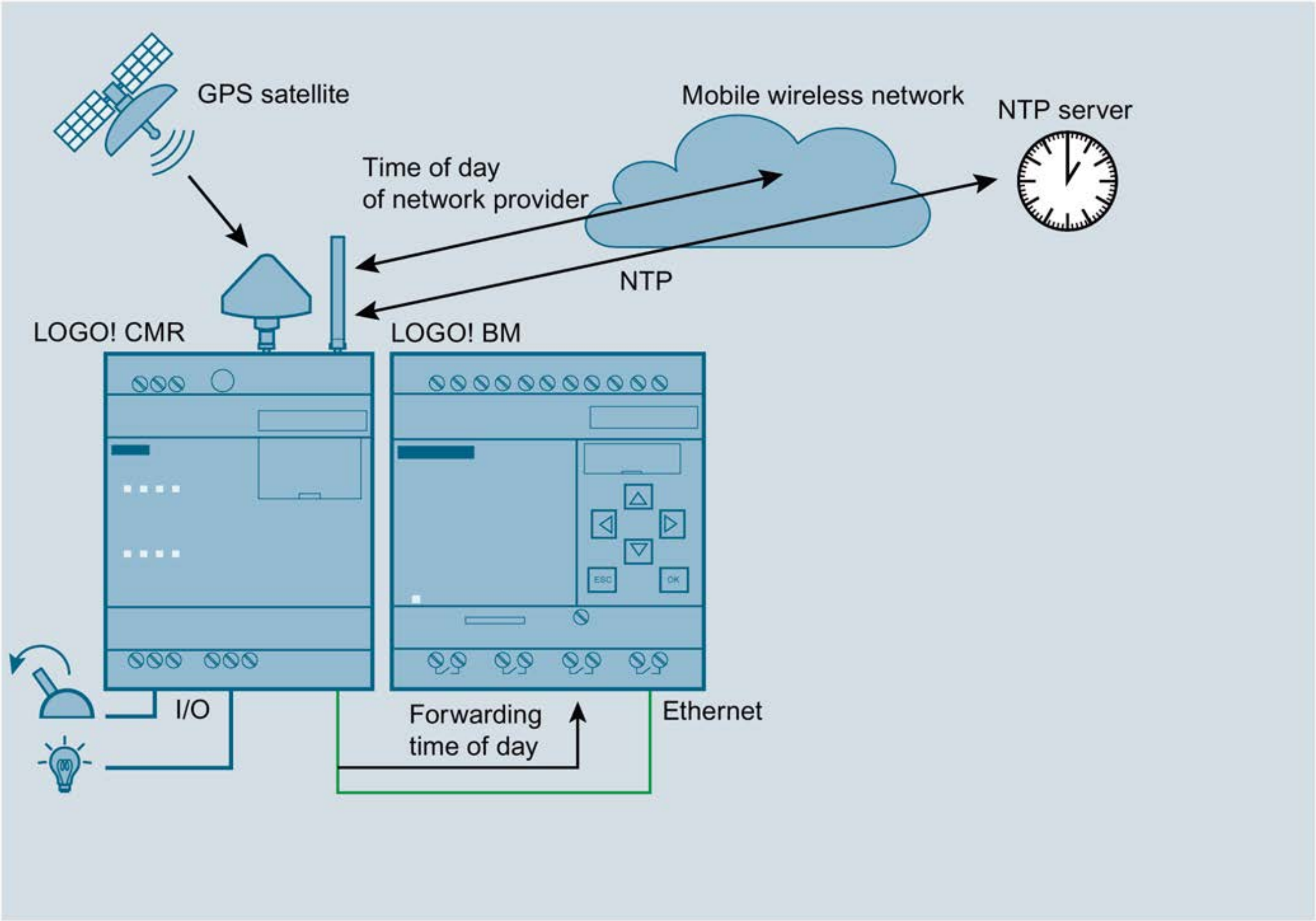


Figure 5-4 Time-of-day synchronization

The LOGO! CMR provides the option of obtaining the time of day from the following sources that can be configured in WBM:

- NTP server
- Mobile wireless network
- GPS reception

Requirements

1. Installation, connecting up, commissioning (Page 21) completed
2. Antenna for mobile wireless reception connected.
3. Only if the time-of-day synchronization method using the GPS signal was configured:

   Antenna for GPS reception connected.

Procedure

To set time-of-day synchronization, follow the steps below:

1. Establish a configuration connection between the CMR and a connected PC. To do this, use an Ethernet patch cable.
   See Establishing a connection to the CMR (Page 42)
2. Select a suitable time of day synchronization method (Page 51).

Configuration 6

6.1 Permitted characters and character lengths

When entering user names, login data, passwords etc. the following characters and character lengths are permitted.

Note

Leading and following spaces

Leading or following spaces are not permitted in names. You will be informed of the incorrect entry with a message in the WBM. Exception: Descriptions and SMS message texts.

Use of special characters

When using special characters, the maximum character length cannot be guaranteed.

Table 6- 1 **Characters/character lengths permitted and not permitted**

<table>
<tr><th>Input box</th><th>Minimum character length</th><th>Maximum character length</th><th>Permitted characters</th><th>Non permitted characters</th></tr>
<tr><td>• Names (except for modules and NTP server name)</td><td>1</td><td>20</td><td rowspan="2">All characters</td><td rowspan="2"></td></tr>
<tr><td>• Description (except for plant description)</td><td>0</td><td>50</td></tr>
<tr><td colspan="5">System</td></tr>
<tr><td>• Module name
• NTP server name</td><td>1
1</td><td>20
63</td><td>0 ... 9, a ... z, A ... Z -.
(DNS name according to RFC 1035 and RFC 1123)</td><td></td></tr>
<tr><td>• Plant description</td><td>0</td><td>20</td><td>All characters</td><td></td></tr>
<tr><td colspan="5">WAN</td></tr>
<tr><td>• SIM PIN1)</td><td>4</td><td>8</td><td>0 ... 9</td><td>a ... z, A ... Z</td></tr>
<tr><td>• APN</td><td>1</td><td>63</td><td>0 ... 9, a ... z, A ... Z -.
(DNS name according to RFC 1035 and RFC 1123)</td><td></td></tr>
<tr><td>• User name
• Password</td><td>0
0</td><td>20
20</td><td>0 ... 9, a ... z, A ... Z ! “#$%&'()*+,-./:;<=>?@[\]^_`{|}~</td><td></td></tr>
<tr><td>• SMS password</td><td>1</td><td>8</td><td>0 ... 9, a ... z, A ... Z!“#$%&'()*+,-./:<=>?@_</td><td>; [\]^`{|}~°´€</td></tr>
<tr><td colspan="5">Users / groups</td></tr>
</table>

Input box	Minimum character length	Maximum character length	Permitted characters	Non permitted characters
• Phone numbers	0	20	Digits 0 ... 9 including special characters. Typical special characters are for example + / * ( ), and spaces. Other special characters are possible.	
• Login	1	20	0 ... 9, a ... z, A ... Z, -@_.	ßäöüÄÖÜ§´€éè
• Password	8	20	0 ... 9, a ... z, A ... Z, !“#$%&'()*+,-./:;<=>?@[\\]^_`{|}~	ßäöüÄÖÜ§´€éè
Monitoring				
SMS message texts including up to 3 placeholders for process values with formatting instructions. The placeholders are replaced with real values prior to sending. The text length can then exceed the limit of 160 characters. If the maximum number of characters is exceeded, up to 2 SMS messages are generated and sent.	0	160	0 ... 9, a ... z, A ... Z ... 9,, !.#$%&'()* +,-./:<=>?@... z The characters [and] are reserved for placeholders. The following formats are permitted for the placeholders of the process values; V stands for a signal name specified in the signal definitions. The signal names must not include the characters [and]: • [V] decimal value of the signal Other placeholders: • [DATE] current date Format: yyyy-mm-dd • [GPS] value is GPS position Format: ddd:mm:ss.hs N/S ddd:mm:ss.hs W/E Alt m • [TIME] current time Format: hh:mm:ss • [DEVNAME]Module name	\\^`{|}~

[1] No PIN is also permitted.

6.2 Establishing a connection to the CMR

For the configuration of the CMR, you require a PC with a Web browser. You configure using the Web user interface (WBM) of the CMR.

Note

A maximum of 2 simultaneous logins (sessions) are possible. Both sessions have full write access. Only the "Firmware update" and "Load configuration" functions can only be used from within one session.

Configuration via the local interface

The following requirements for configuration via the local interface X1P1 must be met:

- The PC must be connected to the Ethernet socket X1P1 of the CMR or have direct access to the CMR via the local network.
- The network adapter of the PC must have the following TCP/IP configuration:
  - Same subnet; in the factory settings, e.g. the following IP address: 192.168.0.4/255.255.255.0

6.2.1 Establishing the configuration connection

To configure the CMR, you must first establish a connection to the device with a Web browser. Follow the steps outlined below:

Setting up the Web browser

1. Start the Web browser on the PC.

   The Web browsers Internet Explorer (as of version 11), Firefox (as of version 28.0) and Google Chrome (as of version33.0) are supported.
2. Set the browser so that it does not automatically select a connection when it is started.

   For example in Microsoft Internet Explorer, make the settings as follows:
   - Select the "Tools" > "Internet Options" menu command.
   - Select the "Connections" tab.
   - To delete the entries in "Dial-up and Virtual Private Network settings", click the "Remove" button.
   - Click the "Never dial a connection" radio button.

Calling up the start page of the CMR

- In the address line of the browser, enter the IP address of the CMR in full.

  In the factory setting, the IP address is: http://192.168.0.3

Entering the user name and password

1. You will be prompted to enter the user name and the password.

   The factory setting is as follows:

   User name: admin

   Passwordadmin
2. After you log in the first time, you will be prompted to change your password.

   Keep to the basic rules for a secure password (refer to the notes in the WBM)

The start page is displayed

After entering the user name and password, the start page of the CMR opens in the Web browser. The start page provides an overview of the operating status of the device.

The start page is not displayed

If, after several attempts, the browser still reports that the page cannot be displayed, try the following:

Checking the hardware connection

1. Open the DOS command prompt by selecting the menu command "Start" > "Programs" > "Accessories" > "Command Prompt".

   Result: The "Command Prompt" window appears.
2. Enter the command "ping 192.168.0.3".

   When operating correctly, you will receive four replies within a few seconds.

If you do not receive four replies within a few seconds:

- Check whether the network cable, the connectors and the network adapter are correctly connected.

Do not use a proxy server

Follow the steps outlined below depending on the operating system:

1. Select the "Tools" > "Internet Options" menu command.
2. Select the "Connections" tab.
3. Click the "LAN settings" button.

   The "Local Area Network Settings" dialog opens.
4. Under the "Proxy server" entry, disable the "Use a proxy server for your LAN" check box.

Disable other LAN connections

If other LAN connections are active on the PC, disable these LAN connections while you are setting the configuration.

Follow the steps below if working with Windows 7:

1. In the Start menu, select the command "Start" > "Control Panel" > "Network and Internet" > "Network and Sharing Center"
2. In "View your active networks" you will see the current LAN connections.
3. In "Access type: Connections", left-click on the relevant connection names.

   The dialog box associated with the connection opens.
4. Click the "Disconnect" button.

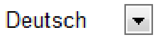
   The dialog closes, you have deactivated the required LAN connection.

6.2.2 Basics of configuration

To configure the CMR, a Web-based administration user interface (WBM) is available to you.

- At the left-hand page you will find a navigation panel.
- The main window displays the pages called according to your navigation (tabs).
- On the individual pages below the tab, you have the following options and information available:
  - Input boxes for entering text.
  - Drop-down lists for selecting entries.
  - Check boxes for enabling and disabling functions.
  - Buttons such as "Apply", "Cancel" that can be clicked.
  - Grayed out text boxes with information and instructions.

Recurring icons and displays on the pages

Symbol	Meaning
Login: 1	**Login** Login of the logged in user.
Logout	**Logout** If you click this button, you exit theWBM and go to the Login page.
2014-08-11 15:37:11	**Time of the last page update of the CMR (date and time shown)** The displayed time is the time of day of the CMR when the Web page was last updated. The date and time of the CMR is updated regularly in the WBM only if the automatic update is activated.
 Deutsch	**Language selection** Select the required language of theWBM from the drop-down list.
Number of active sessions: 1	**Number of active sessions** Shows the number of active sessions
On	**Automatic update active** Regular updating of the page content of the WBM is activated.
Off	**Automatic update inactive** Regular updating of the page content of the WBM is deactivated.
	Print By clicking this button, you can print out the content of the page you are currently viewing.
	Help By clicking this button, you go to the Internet start page of Siemens Industry Online Support.
	Open source software license information By clicking this button, you can download the OSS license texts.

Procedure for configuration

Note

After configuration: If necessary adapt the network interface

After configuration of the CMR, it may be necessary to adapt the network interface of the locally connected computer or network.

Follow the steps below to configure the CMR:

1. Select the required Web page “Configuration“ in the navigation panel.
2. Make your settings in the appropriate tab on the page you have opened.
3. If the "Apply" button is available: Always confirm your entries by clicking this button.

Result: Your settings are then adopted by the device.

Incorrect entries during configuration

The CMR checks your entries. hen you save, consistency errors and invalid characters are recognized automatically: The relevant input box is highlighted with a red boundary. With some incorrect entries an additional message is also displayed. The settings are only applied after the error has been corrected.

Saving the configuration

You can save your settings in a configuration file. This file can, when necessary, then be reloaded or transferred to other devices of the same type. For more detailed information, refer to section Configuration (Page 57).

Deleting elements

Note

Elements that are being used cannot be deleted

You can only delete an element (signal, text, user, recipient group, event, action) if the element is unused.

If the element is used, e.g. a user in a recipient group or a signal in an event, you cannot delete the element.

6.2.3 Language selection

TheWBM of the CMR is available in several languages.

At the top right you will see a drop-down list for the language selection. You can change the language setting for the entire WBM at any time.

Automatic language selection

If, for example, the Web browser is set to the English language, theWBM of the CMR is automatically displayed in English.

If the language setting of the Web browser is not supported, theWBM of the CMR is displayed in English.

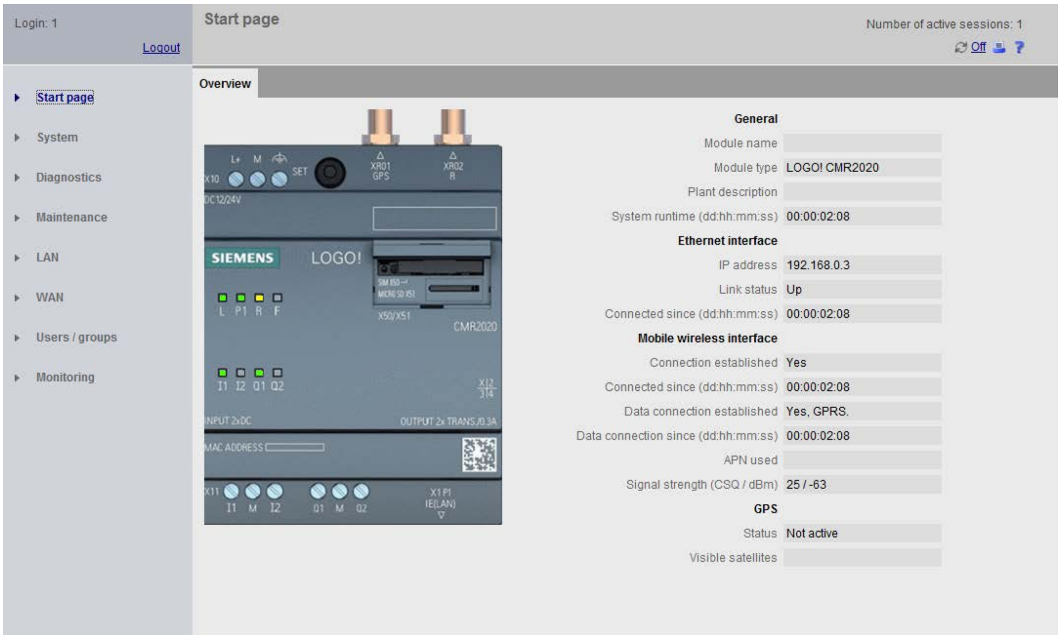
Changing the language setting

To change the language setting:

- Select the required language from the drop-down list at the top right of the start page.

  The language setting is saved and is set correctly for the next access.
- If the language is not changed immediately, update the display in your Web browser: "F5" key in the Internet Explorer.

6.3 Start page



General

Module name

Module type LOGO! CMR2020

Plant description

System runtime (dd:hh:mm:ss) 00:00:02:08

Ethernet interface

IP address 192.168.0.3

Link status Up

Connected since (dd:hh:mm:ss) 00:00:02:08

Mobile wireless interface

Connection established Yes

Connected since (dd:hh:mm:ss) 00:00:02:08

Data connection established Yes, GPRS.

Data connection since (dd:hh:mm:ss) 00:00:02:08

APN used

Signal strength (CSQ / dBm) 25 / -63

GPS

Status Not active

Visible satellites

Figure 6-1 Start page – "Overview" tab

Login

After successfully logging in (Page 43), the start page of the CMR appears.

Display of the current operating status

The start page shows an overview of the current operating status of the CMR.

General		
Module name	Display of the name you assigned on the "System" (Page 49) page.	
Module type	LOGO! CMR2020 or LOGO! CMR2040 depending on which device you are using.	
Plant description	Display of the name you assigned on the "System" (Page 49) page.	
System runtime (dd:hh:mm:ss)	Display of the system runtime of the CMR since the last restart.	
Ethernet interface		
IP address	IP address of the CMR	
Link status	• If a connection exists between the PC and the CMR "Up" is displayed. • If no connection exists between the PC and the CMR "Down" is displayed.	
Connected since (dd:hh:mm:ss)	Display of the time of the connection between the PC and the CMR.	
Mobile wireless interface		
Connection established	Display of whether or not a connection to the mobile wireless network exists (Yes/No).	
Connected since (dd:hh:mm:ss)	Displays how long the connection has been established since last booking into the mobile wireless network.	
Data connection established	• No • Yes with display GPRS (LOGO! CMR2020) or LTE (LOGO! CMR2040)	
Data connection since (dd:hh:mm:ss)	Display of the time since the last data connection.	
APN used	Display of the access point (APN) you created on the "WAN" (Page 72) page. **A**ccess **P**oint **N**ame (access point): Name of the access point for access to a mobile wireless data network.	
Signal strength	Display of the signal strength of the mobile wireless network at the location of the CMR.	
	≤ -113 dBm	No connection to the GSM network
	≥ -111 dBm	Bad signal strength
	≥ -79 dBm	Medium signal strength
	≥ -65 dBm	Good signal strength
	≥ -51 dBm	Very good signal strength
GPS		
Status	Display of whether or not GPS reception is enabled. GPS reception is enabled/disabled on the "System" page in the "General" tab (Page 49).	
Visible satellites	If GPS is active, the number of satellites from which signals are being received is displayed.	

Updating the displayed values

If you have enabled automatic updating with the On/Off button at the top right on the page, the displayed values are updated every 5 s.

To update manually, press for example the "F5" key in the Internet Explorer.

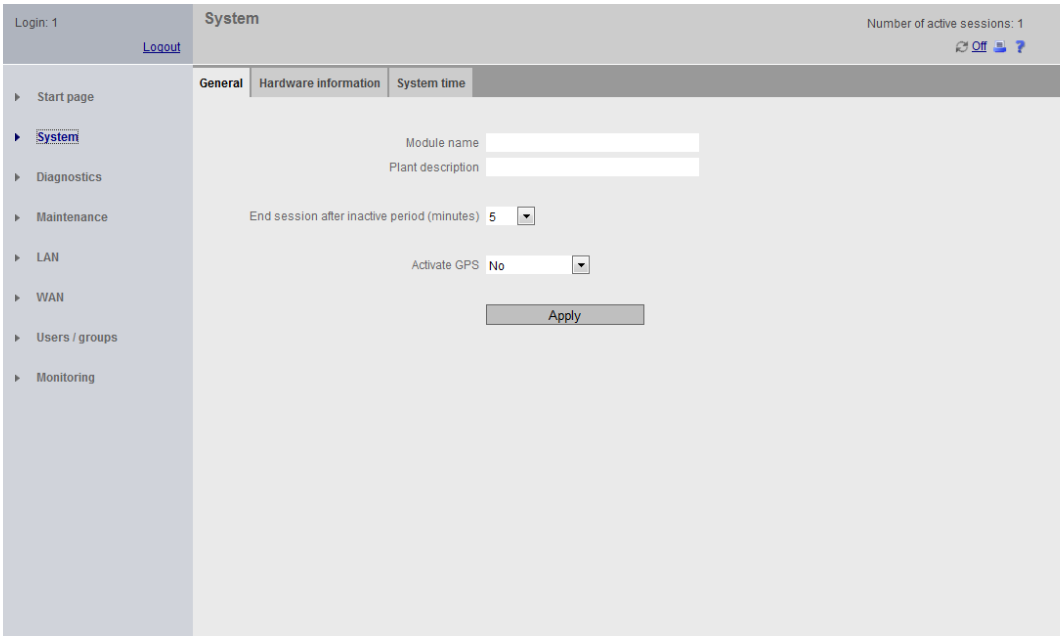
6.4 System

6.4.1 Calling the Web page

In the navigation panel, select the "System" entry and click on the available tabs:

- General
- Hardware information
- System Time

6.4.2 General



Module name

Plant description

End session after inactive period (minutes) 5

Activate GPS No

Figure 6-2 System – "General" tab

Module name

Enter any name for your module.

Only use a DNS-compliant name as the module name. DNS-compliant names are, for example, used for diagnostics.

Plant description

Enter any name for your plant.

End session after inactive period (minutes)

If you are no longer working with theWBM, set the time after which your session will be forced to close.

You then need to log in again with a user name and password.

Note

A maximum of 2 simultaneous logins (sessions) are possible. Both sessions have full write access. Only the "Firmware update" and "Load configuration" functions can only be used from within one session.

Activate GPS

Activate/deactivate GPS reception.

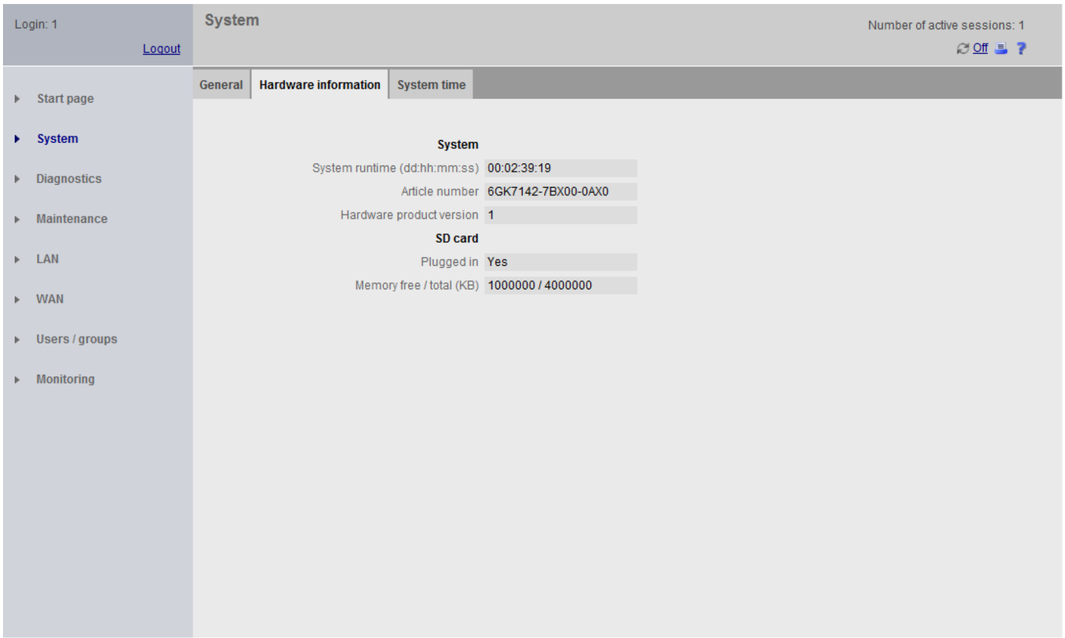
Make sure that an antenna is connected to the GPS input:

- To activate GPS, select the entry "Yes" from the "Activate GPS" drop-down list.
- To deactivate GPS, select the entry "No" from the "Activate GPS" drop-down list.

"Apply" button

If you click the "Apply" button, all the settings you made in the "General" tab are adopted.

6.4.3 Hardware information



System

System runtime (dd:hh:mm:ss) 00:02:39:19

Article number 6GK7142-7BX00-0AX0

Hardware product version 1

SD card

Plugged in Yes

Memory free / total (KB) 1000000 / 4000000

Figure 6-3 System – "Hardware information" tab

Hardware information on the CMR and the SD card.

System

- Display of the system runtime since the last restart.
- The article number and hardware product version of the CMR are also displayed.

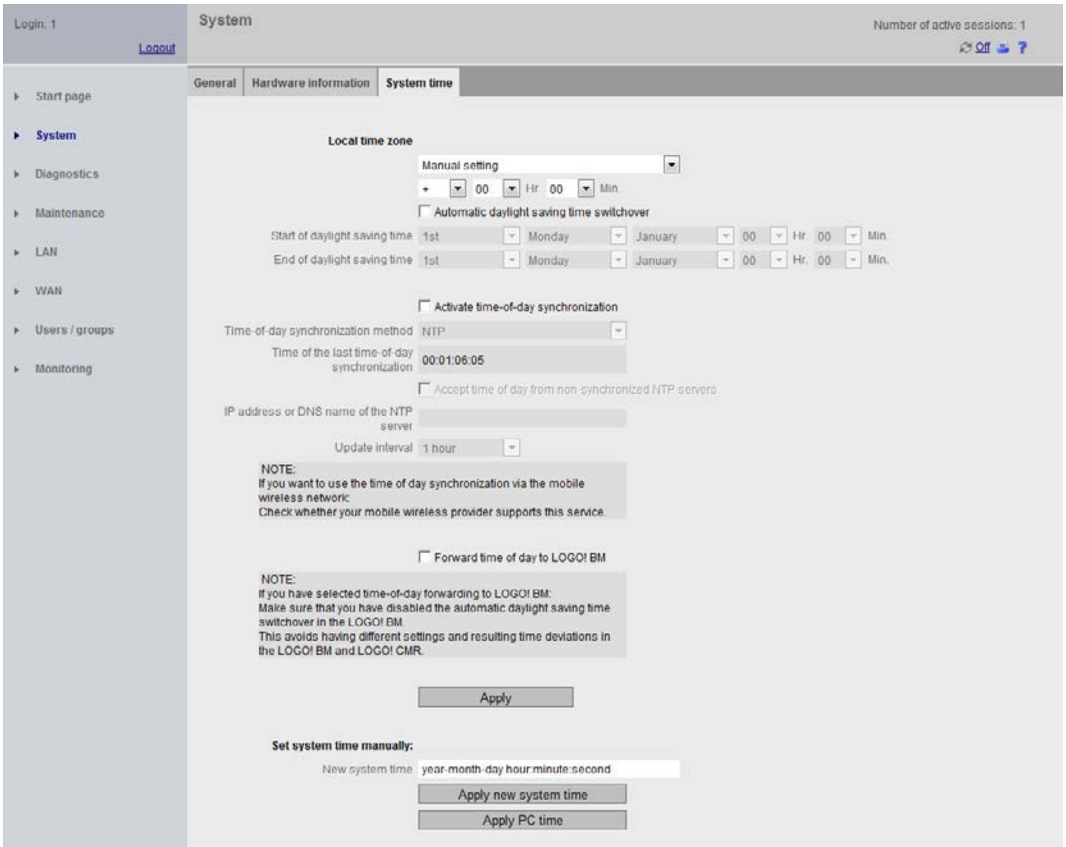
SD card

You have inserted an SD card and the CMR recognizes the card.

The following is displayed:

- Whether or not an SD card is plugged in.
- The capacity and the free memory space on the SD card.

6.4.4 System Time



Local time zone

Manual setting

+ 00 Hr 00 Min

□ Automatic daylight saving time switchover

Start of daylight saving time: 1st, Monday, January, 00 Hr. 00 Min

End of daylight saving time: 1st, Monday, January, 00 Hr. 00 Min.

□ Activate time-of-day synchronization

Time-of-day synchronization method: NTP

Time of the last time-of-day synchronization: 00:01:06:05

□ Accept time of day from non-synchronized NTP servers

IP address or DNS name of the NTP server:

Update interval: 1 hour

NOTE:
If you want to use the time of day synchronization via the mobile wireless network:
Check whether your mobile wireless provider supports this service.

□ Forward time of day to LOGO! BM

NOTE:
If you have selected time-of-day forwarding to LOGO! BM:
Make sure that you have disabled the automatic daylight saving time switchover in the LOGO! BM.
This avoids having different settings and resulting time deviations in the LOGO! BM and LOGO! CMR.

Set system time manually:

New system time: year-month-day hour:minute:second

Figure 6-4 System – "System time" tab

In this tab, you make the basic setting for the time of day and specify the following:

- The time-of-day synchronization method and the intervals at which the time of day is updated.
- The automatic daylight saving time switchover.
- The forwarding of the CMR time of day to the BM.

You have three possible time-of-day synchronization methods available:

- NTP (time server)

  If you set time-of-day synchronization using NTP, select the "Activate data connection via the mobile wireless network" (Page 71) check box.
- GPS
- GSM/LTE mobile wireless network

  Check whether your mobile wireless provider supports this function.

If you click the "Apply" button, the settings you have made for the local time zone and time-of-day synchronization are adopted.

Local time zone

- You select the time zone to match your location from the drop-down list.
- You can also set the local time zone manually.

If you click the "Applyy" button, the settings you have made for the local time zone are adopted.

Automatic daylight saving time switchover

You can only change the date and time for the time-of-day switchover using "Manual setting".

- If you select the "Automatic daylight saving time switchover" check box, the daylight saving time switchover is performed automatically.
- In the drop-down lists, you select the valid dates and times for the time switchover.

The settings are fixed for the UTC time zones and cannot be changed.

Time-of-day synchronization method

Note

Time-of-day synchronization via a mobile wireless network

If you want to use the time-of-day synchronization via the mobile wireless network:

- Check whether this service is supported by your mobile wireless provider.

The intervals of time-of-day synchronization points can deviate considerably:

The first time the device books into the mobile wireless network, the time of day is transferred by the mobile wireless provider.
After booking in, the intervals of the next time-of-day synchronization points can deviate considerably (up to several days) depending on the mobile wireless provider. Keep this in mind if you select time-of-day synchronization via the mobile wireless network.

Time-of-day synchronization with GPS

If you select time-of-day synchronization using GPS, check the following:

- Whether or not GPS is active.
- Whether or not an antenna is connected.
- Whether or not GPS reception is adequate.

1. By selecting the "Activate time-of-day synchronization" check box, you enable time-of-day synchronization.
2. Then select the required time-of-day synchronization method.

The time-of-day synchronization methods are available for selection in the "Time-of-day synchronization method" drop-down list:

Time-of-day synchronization method	Meaning
NTP	Time-of-day synchronization by an NTP server (time server). 1. In the “IP address or DNS name of the NTP server" box, enter the name of the NTP server or its IP address: – The NTP server is specified in the familiar URL format, e.g.http://www.ntpservername.de. – The IP address is specified in the format 123.123.123.123. 2. In the "Mobile wireless settings", select the "Activate data connection via the mobile wireless network (Page 71)" check box. The connection to the NTP server can only be established via the mobile wireless interface and not via the Ethernet interface.
GPS	Time of day from the GPS signal. The time of day is taken from the GPS signal and adapted according to the set time zone. • Make sure that a GPS antenna is connected and that reception is ensured.
GSM/LTE	Time of day from your mobile wireless provider. If your mobile wireless provider supports this service, the time of day is taken directly from your mobile wireless provider. Make sure this is the case before selecting this entry in the drop-down list.

- Using the "Update interval" drop-down list, you specify the intervals at which the time is synchronized using the selected time-of-day synchronization method.

  If you synchronize the time of day via the GSM/LTE mobile wireless network, you cannot specify an update interval.
- By selecting the "Forward time of day to LOGO! BM“ check box, the time of day is forwarded to the BM at the intervals you have set.

  If the time of day is synchronized via a mobile wireless network, the time of day is forwarded as soon as a new time of day is received by the CMR. The time of day is also transferred when establishing the connection to the BM.

Note

Avoid having different settings on the BM and CMR

If you have different settings on the BM and CMR and want to avoid time deviations resulting from this, you need to enable time-of-day forwarding to the BM:

1. Make sure that you have disabled the automatic daylight saving time switchover on the BM.

   This avoids having different settings and resulting time deviations in LOGO! BM and LOGO! CMR.
2. Select the "Forward time of day to LOGO! BM " check box.

The "Time of the last time-of-day synchronization" display box shows when the time of day was last synchronized successfully.

"Apply" button

If you click the "Apply" button, time-of-day synchronization is started if the parameters have been changed.

Note

The time of day is reset during a restart. To have the current time, you always need to use a time-of-day synchronization method.

Set system time manually

You can get the system time for the CMR from your PC or enter it manually.

- Click the "Apply PC time" button: The time is read from the PC and written to the CMR.
- Manual entry: Enter the system time in the “New system time" input box.
  - By clicking the “Apply new system time" button, the time is written to the CMR.

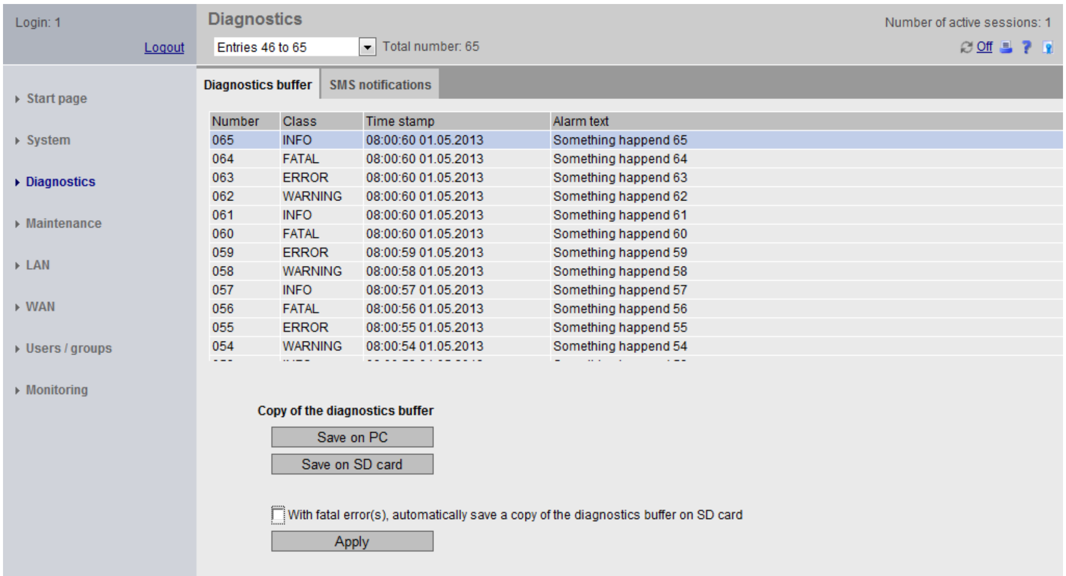
6.5 Diagnostics

6.5.1 Calling the Web page

In the navigation panel, select the "Diagnostics" entry and click on the available tabs:

- Diagnostics buffer
- SMS notifications

6.5.2 Diagnostics buffer



Entries 46 to 65 Total number: 65

Number	Class	Time stamp	Alarm text
065	INFO	08:00:60 01.05.2013	Something happend 65
064	FATAL	08:00:60 01.05.2013	Something happend 64
063	ERROR	08:00:60 01.05.2013	Something happend 63
062	WARNING	08:00:60 01.05.2013	Something happend 62
061	INFO	08:00:60 01.05.2013	Something happend 61
060	FATAL	08:00:60 01.05.2013	Something happend 60
059	ERROR	08:00:59 01.05.2013	Something happend 59
058	WARNING	08:00:58 01.05.2013	Something happend 58
057	INFO	08:00:57 01.05.2013	Something happend 57
056	FATAL	08:00:56 01.05.2013	Something happend 56
055	ERROR	08:00:55 01.05.2013	Something happend 55
054	WARNING	08:00:54 01.05.2013	Something happend 54

Copy of the diagnostics buffer

□ With fatal error(s), automatically save a copy of the diagnostics buffer on SD card

Figure 6-5 Diagnostics - "Diagnostics buffer" tab

The diagnostics buffer shows you a maximum of 20 entries of 200 possible entries.

You can do the following with the diagnostics buffer:

- Save it on your PC or the SD card.
- Have it written to the SD card automatically by the CMR if there is a fatal error.

The entries in the diagnostics buffer have time stamps and are divided into various classes:

- INFO
- WARNING
- ERROR
- FATAL

In the "Alarm text" column, you will find a brief message in plain text.

If you click the "Apply" button, all the settings you made in the "Diagnostics buffer" tab are adopted.

Events logged in the diagnostics buffer

The following events are logged during operation of the CMR:

- Operating messages such as startup, change to the configuration.
- Establishment/interruption of the connection to the BM.
- Establishment/interruption of the connection to the mobile wireless network.
- Establishment/interruption of the mobile data connection.
- Warnings when reading in the configuration from an SD card or from the PC.
- Time-of-day synchronization

Saving a copy of the diagnostics buffer

To save a copy of the diagnostics buffer on your PC:

1. Click the "Save on PC" button. You cannot assign a file name; the file name of the copy of the diagnostics buffer is preassigned: diagbuf.txt
2. Select a suitable storage location on your PC.

To save a copy of the diagnostics buffer on an inserted SD card:

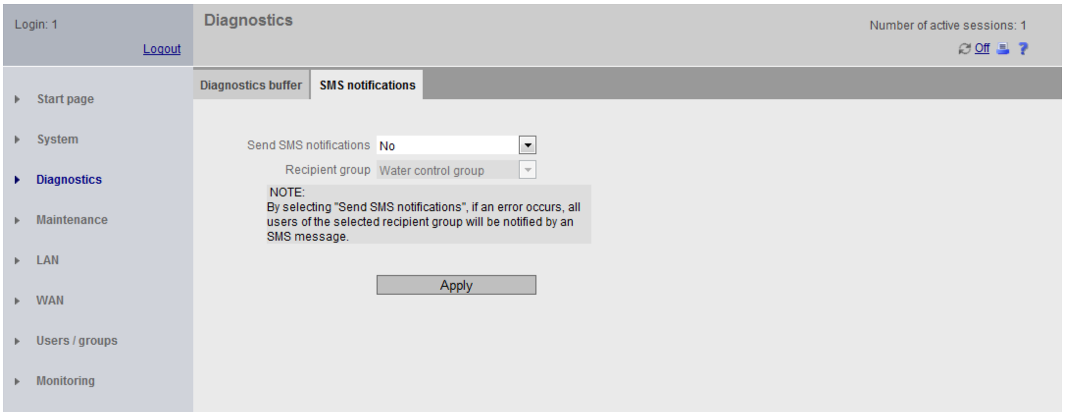
- Click the “Save on SD card" button.

  It is not necessary to specify a storage location on the SD card.

Automatic saving in the event of a fatal error

1. By selecting the "With fatal error(s), automatically save a copy of the diagnostics buffer on SD card" check box, the diagnostics buffer is automatically saved on the SD card.
2. You can then run an error analysis.

6.5.3 SMS notifications



Send SMS notifications: No

Recipient group: Water control group

NOTE:
By selecting "Send SMS notifications", if an error occurs, all users of the selected recipient group will be notified by an SMS message.

Figure 6-6 Diagnostics - "SMS notifications" tab

In the “SMS notifications" tab, you set whether or not a recipient group is notified if an error occurs (FATAL or ERROR).

Note

Messages without SMS notifications

- For messages of the type INFO or WARNING, no SMS notifications are sent.
- If the device is put out of operation by a fatal error, no SMS notifications are sent.

1. Select the entry "Yes" from the "Send SMS notifications" drop-down list.
2. Enter the group you defined in "Users / groups" in the "Recipient groups" tab in "Recipient group".

   If no recipient group has been defined yet, the notifications cannot be activated.

The plain text of the error is sent in the SMS message.

If you click the “Apply" button, all the settings you made in the “SMS notifications" tab are adopted.

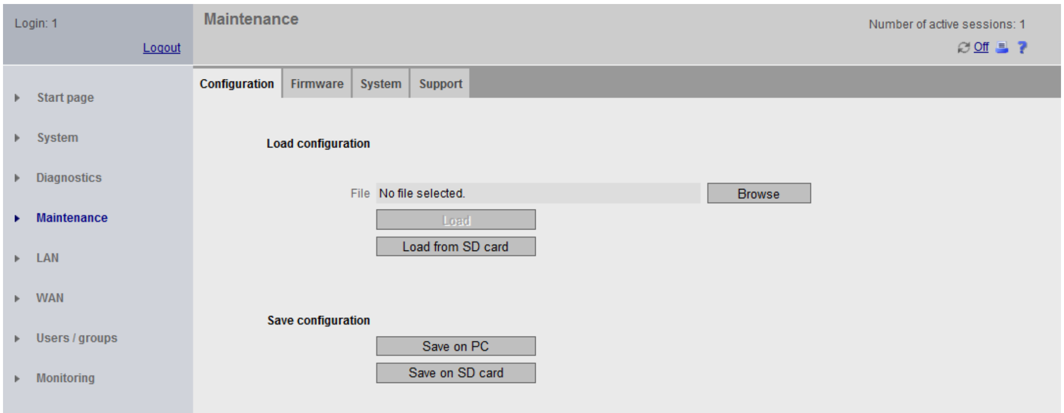
6.6 Maintenance

6.6.1 Calling the Web page

In the navigation panel, select the “Maintenance" entry and click on the available tabs:

- Configuration
- Firmware
- System
- Online support

6.6.2 Configuration



Login: 1

Number of active sessions: 1

File No file selected.

Figure 6-7 Maintenance – "Configuration" tab

Load Configuration

Load configuration from PC

With this function a configuration created previously and saved on the PC is loaded on the CMR.

Configuration files have the file extension ".cfg".

1. To search for configurations on the PC, click the "Browse" button.
2. Double-click on the required configuration file.
3. To load the configuration on the CMR, click the "Load" button.

Result: The uploaded configuration is now used.

Load configuration from SD card

With this function a configuration created previously and saved on the SD card is loaded on the CMR.

The name of the stored configuration file is "user.cfg".

- To load the configuration on the CMR, click the "Load from SD card" button.

Result: The uploaded configuration is now used.

Save configuration

Saving a configuration on PC

Note

Editing configurations with a text editor

When editing configurations with a text editor (e.g. Notepad), make sure that you save the configuration in the UTF-8 format and that you do not use any special characters; in other words only ASCII characters.

You can do the following with a configuration of the CMR:

1. Save it on the PC.
2. If necessary transfer it to other devices of the same type.

- Click the "Save on PC" button.
- Select the relevant storage location.

Save configuration on SD card

Note

Only a configuration with a fixed name is permitted on the SD card.

You can do the following with a configuration of the CMR:

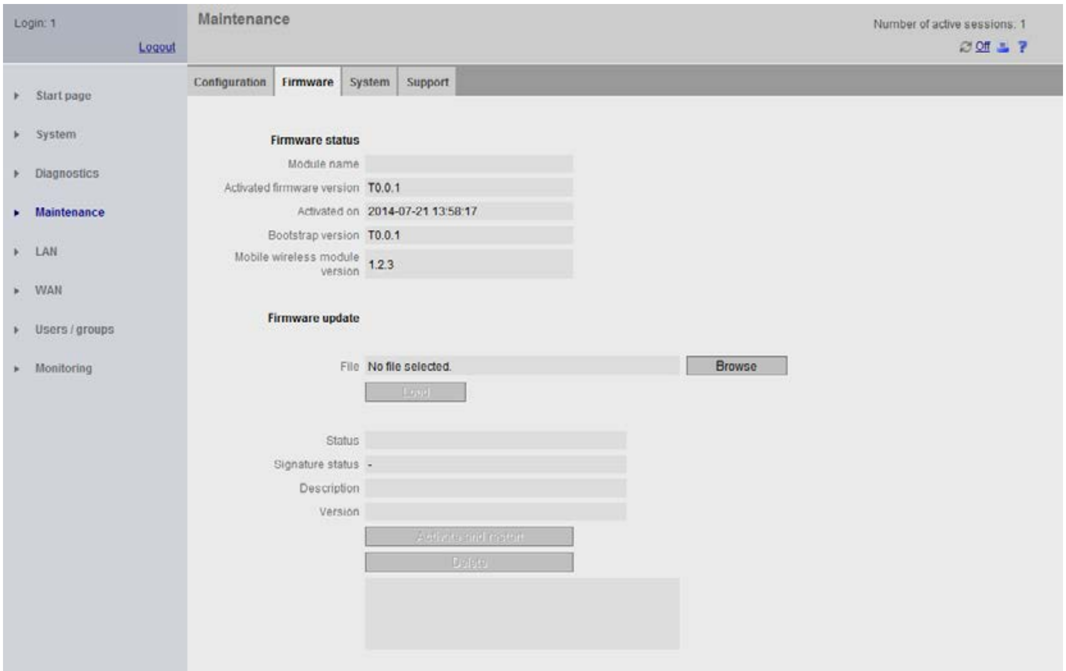
1. Save it on the SD card.
2. If necessary transfer it to other devices of the same type.

- Click the "Save on SD card" button.

Meaning of the configuration files "user.cfg" and "default.cfg"

The configuration saved using the button is stored as "user.cfg". At the same time an automatically backed up configuration file with the name "default.cfg" is stored.default.cfg is updated with every configuration change If the SD card with the "default.cfg" file is inserted in a brand-new CMR or in a CMR that has been reset to the factory settings, the "default.cfg" file will be loaded.

6.6.3 Firmware



Login: 1

Maintenance

Number of active sessions: 1

Firmware status

Module name:

Activated firmware version: T0.0.1

Activated on: 2014-07-21 13:58:17

Bootstrap version: T0.0.1

Mobile wireless module version: 1.2.3

Firmware update

File: No file selected.

Status:

Signature status: -

Description:

Version:

Figure 6-8 Maintenance – “Firmware" tab

In the “Firmware" tab:

- You will find information on the firmware currently installed on the CMR.
- Update the firmware version of the CMR.

Firmware status

The following information is shown:

- Module name that you defined on the "System" Web page
- Activated firmware version
- Activated on (date)
- Bootstrap version
- Mobile wireless module version

Firmware update

> NOTICE
>
> **Digitally signed and encrypted firmware prevents manipulation by third parties**
>
> To be able to check the authenticity of the firmware, the firmware is digitally signed by Siemens. This allows manipulation by third parties to be detected and prevented. The encryption of the firmware is intended to prevent re-engineering.

Note

During the time between unpacking the firmware and the actual update through to the restarting the CMR, the administration user interface is not blocked.

- During this time, do not make any settings in the Web user interface otherwise you cannot be certain that these settings will be adopted correctly.

Do not turn off the CMR during the update.

To load a new firmware version on the CMR, follow the steps below:

1. Before you start the update: Read the notes in “Firmware update".
2. Click the "Browse" button.
3. Select the relevant firmware file, for example "LOGO!CMR_v2.0-v2.1.sfw".
4. Click the "Load" button.
5. After successful transfer, the updated firmware version is displayed.
6. Then click the "Activate and restart" button.
7. The CMR restarts.
8. Following the restart, the firmware is updated. During this time all the LEDs light up for several seconds before the CMR starts.

Display boxes with additional information on the firmware

- Status

  Indicates errors while loading the firmware: For example format error if you load a file different from the required firmware.
- Signature status

  Shows you the result of the signature check.
- Description

  Shows you the name of the firmware.
- Version

  Shows you the version of the loaded firmware.

6.6.4 System

In the "System" tab, you can do the following:

- Shut down (Page 15) the device to a safe status.
- Run a restart.
- Reset to factory settings.

6.6.4.1 Shut down to safe status

There are two ways in which you can shut down the CMR to a safe status:

- Using the WBM with the “Shut down to safe status" button
- With theSET button on the front of the device (Page 15).

If you click the "Shut down to safe status" button, the CMR books out of the mobile wireless network. You can then disconnect the device from the power supply.

6.6.4.2 Run restart

There are two ways of running a restart with the CMR:

- Using WBM with the "Run restart“ button
- With theSET button on the front of the device (Page 15).

When restarting, existing connections are interrupted.

The settings of the current configuration do not change. The CMR continues to work using these settings after the restarting.

Restart using the WBM

- If you click the “Run restart" button in the "System" tab, the restart is executed immediately.

  Result: The CMR restarts.

Restart using the SET button

In the small opening labeledSET, there is a button that is used to restart or shut down the device.

1. Press the SET button with a flat pen-shaped object.
2. Keep the button pressed for 5 s.

   Result: The device restarts.

6.6.4.3 Reset to factory settings

There are two ways in of resetting the device to the factory settings:

- Via the WBM with the “Reset to factory settings" button.
- With theSET button on the front of the device (Page 15).

Remember the effects of resetting to factory settings

Before you reset to the factory settings: Note the following information.

NOTICE

Resetting to factory settings deletes data

If you reset to factory settings, all the configuration data of the CMR will be deleted.

Deleting involves the following data:

- Logins and passwords
- PIN of the SIM card being used
- Diagnostics buffer
- If an SD card is inserted:
  - The automatically backed up configuration (default.cfg)
  - The manually backed up configuration (user.cfg)

Following this, the CMR is restarted. After the restart, the CMR can be reached via the Ethernet interface using the default IP address 192.168.0.3.

Note

Backing up configuration data on PC or SD card

If you do not want to discard the configuration data you have entered, you can back up the data externally and load it again after resetting to factory settings.

For information on this, refer to section Configuration (Page 57)

After saving the configuration data on an SD card, note the following:

- Before resetting to factory settings, remove the SD card: see "Reusing a configuration of a CMR".
- Remove the SD card only when the power supply is disconnected.

Reset using the WBM

Follow the steps outlined below:

1. Before you start the reset: Note the information in "Effects of resetting to factory settings".
2. In the navigation panel, select "Maintenance"and the "System" tab.
3. Click the “Reset to factory settings" button.

   The device is reset to the factory settings and runs a restart.
4. Put the device back into operation as described in Steps in commissioning (Page 29) and Configuration (Page 41).

Reset using the SET button

Follow the steps outlined below:

1. Before you start the reset: Note the information in "Effects of resetting to factory settings".
2. Press the SET button with a suitable object.
3. Keep the button pressed for at least 10 s.

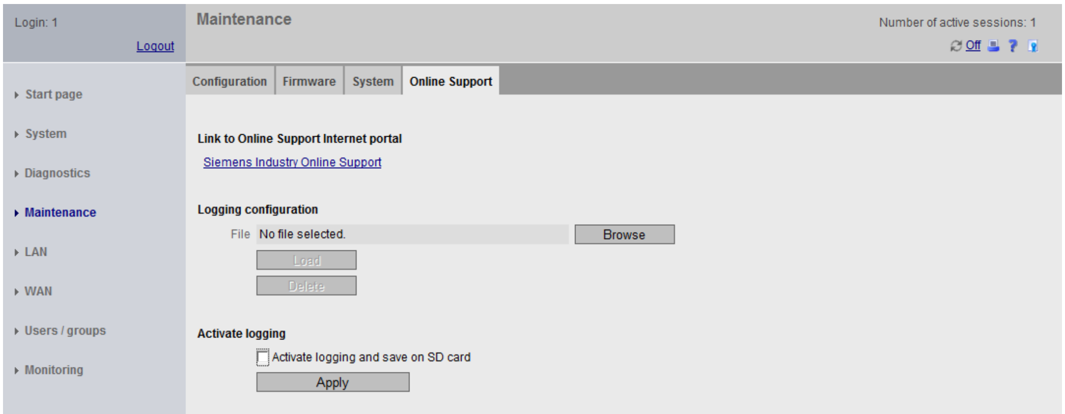
   The device is reset to the factory settings and runs a restart.
4. Put the device back into operation as described in Steps in commissioning (Page 29) and Configuration (Page 41).

Reusing a configuration of a CMR

You can transfer the configuration of a CMR any number of times to other CMRs:

1. The CMR is brand-new or was reset to factory settings (without SD card).
2. If the SD card of another CMR is inserted before starting the CMR, the automatically backed up configuration (default.cfg) of the other CMR is used.

6.6.5 Online Support



Login: 1

Number of active sessions: 1

Link to Online Support Internet portal

Siemens Industry Online Support

Logging configuration

File: No file selected.

Activate logging

□ Activate logging and save on SD card

Figure 6-9 Maintenance - "Online support" tab

In the "Online support" tab, you can obtain support and possible solutions to problems with the CMR.

If you have problems in conjunction with the CMR, you should therefore contact Siemens Industry Online Support:

1. Click on "Siemens Industry Online Support" or help ?.
   You will be connected to the Internet page of Siemens Industry Online Support.
2. To be able to configure logging of the problem handling for the particular problem, you will receive a configuration file from online support.

   To be able to log the problem handling, an SD card with ≥ 8 MB of free memory space must be inserted.

While logging is activated, the CMR saves information continuously. The saved data contains information on the configuration, active procedures and error situations. The data is saved on the SD card in a file with the name "support.bin".

The information in this file is encrypted and can therefore only be read by Siemens Industry Online Support.

To solve your problem as quickly as possible, Siemens Industry Online Support analyzes the log file.

Configuration of the logging

To load the configuration of the logging from online support onto the CMR, follow the steps below:

1. Click the "Browse" button.
2. From your local PC, select the configuration file provided by online support, for example "Ticket123456.sup".
3. Click the "Load" button.
4. After successful transfer, the "Activate logging and save on SD card" check box is enabled.

Deleting the configuration of the logging

To delete a loaded configuration again:

- Click the "Delete" button.

  The "Activate logging and save on SD card" check box is disabled and grayed out again.

  The CMR is once again in normal operation.

Activate logging

After successful transfer of the configuration file:

1. The “Activate logging and save on SD card" check box is enabled.
2. Start the logging by selecting the check box and clicking the "Apply" button.

Note

To spare the SD card: Deactivation recommended

To spare the SD card (working life), deactivate this function again after your problem has been solved:

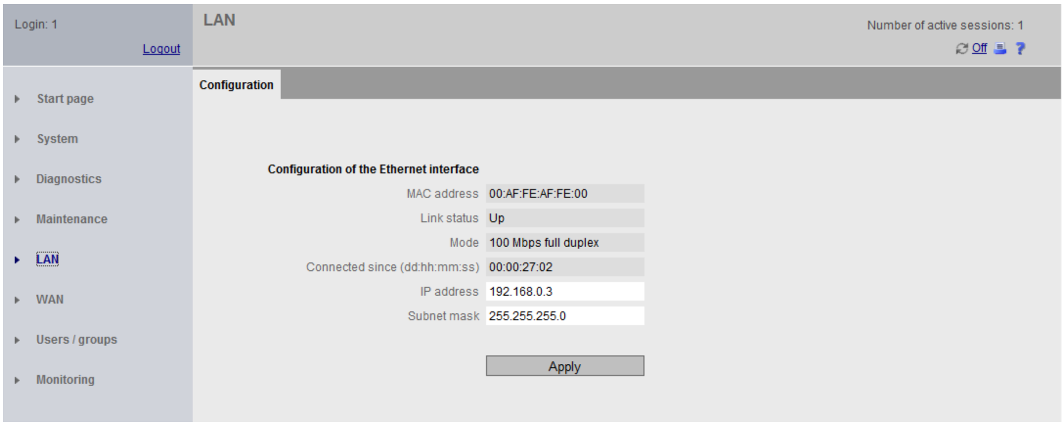
- Deselect the "Activate logging and save on SD card" check box.
- If you click the "Apply" button, you adopt this setting.

Deactivating logging

If you remove a loaded logging configuration, the check box is disabled and grayed out. The CMR is once again in normal operation.

6.7 LAN

6.7.1 Calling the Web page



Configuration of the Ethernet interface

MAC address	00:AF:FE:AF:FE:00
Link status	Up
Mode	100 Mbps full duplex
Connected since (dd:hh:mm:ss)	00:00:27:02
IP address	192.168.0.3
Subnet mask	255.255.255.0

Figure 6-10 LAN – "Configuration" tab

In the navigation panel, select the "LAN" entry.

In the "Configuration" tab, you will find the following:

- Information about the LAN interface of the CMR
- Settings for the LAN interface of the CMR

If you click the "Apply" button, all the settings you made in the "Configuration" tab are adopted.

6.7.2 Configuration

Function of the LAN interface X1P1

- The X1P1 interface (Ethernet RJ-45) of the CMR is used to connect a local PC for the configuration.
- After completed configuration, the X1P1 interface serves to connect to the BM only if the CMR is not being operated in standalone mode (Page 34).

You will find the properties of the X1P1 interface in the technical specifications (Page 125).

By using autonegotiation and autocrossing, the transmission speed, duplex and polarity are detected automatically.

Configuration of the Ethernet interface

Note

IP address and subnet mask according to RFC 1918

The factory-set IP addresses and subnet masks can be changed as required, but must keep to the specification RFC 1918. The CMR does not run any strict checks of the address bands.

- Do not set an IP address that is already assigned in your LAN, for example for other BMs.

If a duplicate IP address is detected, the red error LED starts to flash. The CMR is no longer available via the Ethernet interface. No other functions are affected: e.g. sending an SMS message due to events of the CMR itself.

Settings cannot be changed

1. MAC address
2. Link status (Up/Down)
3. Mode (current mode: 10/100 Mbps, half or full duplex
4. Connected since (dd:hh:mm:ss)

Settings can be changed

1. IP address
2. Subnet mask

If you click the "Apply" button, all the settings you made in the "Configuration" tab are adopted.

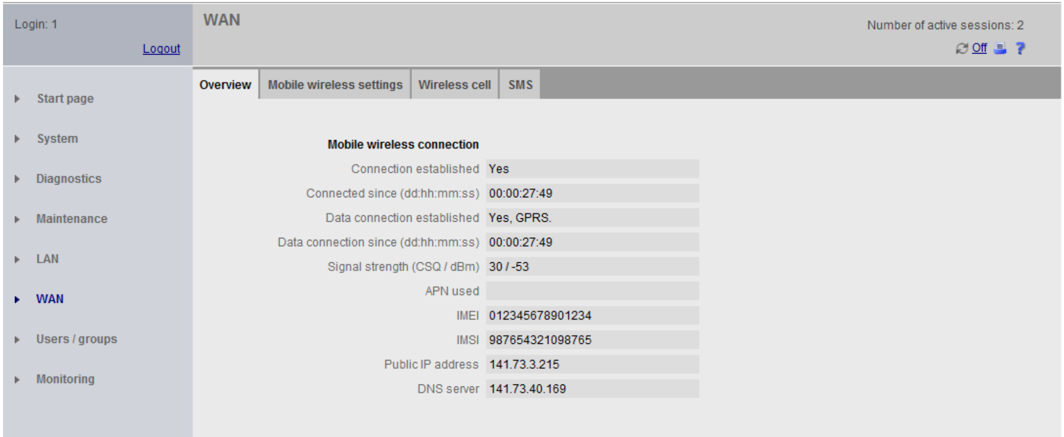
6.8 WAN

6.8.1 Calling the Web page

In the navigation panel, select the "WAN" entry and click on the available tabs:

- Overview
- Mobile wireless settings
- Wireless cell
- SMS

6.8.2 Overview



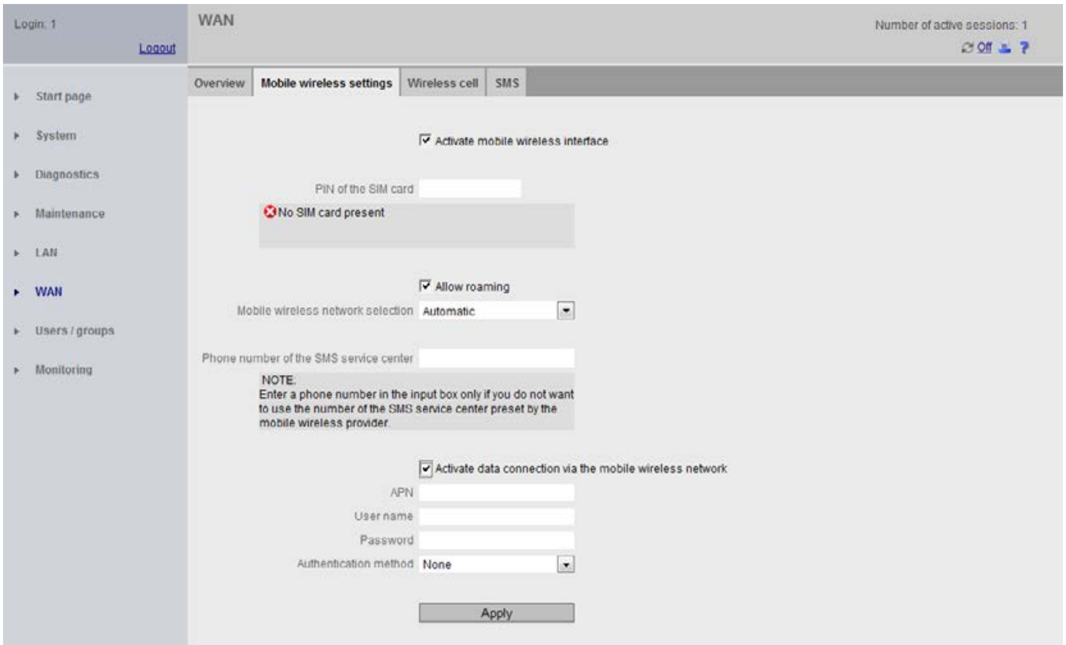
Mobile wireless connection

Connection established	Yes
Connected since (dd:hh:mm:ss)	00:00:27:49
Data connection established	Yes, GPRS.
Data connection since (dd:hh:mm:ss)	00:00:27:49
Signal strength (CSQ / dBm)	30 / -53
APN used	
IMEI	012345678901234
IMSI	987654321098765
Public IP address	141.73.3.215
DNS server	141.73.40.169

Figure 6-11 WAN – “Overview“ tab

In the "Overview" tab, you will see information about the mobile wireless interface.

6.8.3 Mobile wireless settings



☑ Activate mobile wireless interface

PIN of the SIM card

No SIM card present

☑ Allow roaming

Mobile wireless network selection: Automatic

Phone number of the SMS service center

NOTE:
Enter a phone number in the input box only if you do not want to use the number of the SMS service center preset by the mobile wireless provider.

☑ Activate data connection via the mobile wireless network

APN

User name

Password

Authentication method: None

Figure 6-12 WAN – “Mobile wireless settings" tab

The mobile wireless interface of the CMR connects the device to the mobile wireless network. The SMA antenna socket is available to allow reception of mobile wireless.

For communication, GPRS or LTE (with fallback to HSDPA, HSUPA, UMTS or GPRS) is used on the mobile wireless interface.

If you click the “Apply" button, all the settings you made in the "Mobile wireless settings" tab are adopted.

Costs of a mobile data connection

Note

Remember that both when establishing or when attempting to establish a mobile data connection and to maintain a mobile data connection, frames are exchanged that are subject to charges.

Access parameters

You configure your mobile wireless connection in the "Mobile wireless settings" tab.

For access to the GSM mobile wireless network and to the HSPA, UMTS, GPRS or LTE services, you require the following parameters:

- The PIN protects the SIM card against unauthorized use.
- APN is the name of the transition point from the mobile wireless network to other connected IP networks, at this point to the Internet.

  “User name and password are used to keep APN access secure.

You will receive these access parameters from your mobile wireless provider.

The mobile wireless network is selected automatically.

Note

Mobile wireless network connection with LOGO! CMR2020

LOGO! CMR2020 only dials into a GSM/GPRS mobile wireless network.

Mobile wireless network connection with LOGO! CMR2040

As the preferred connection, LOGO! CMR2040 first attempts to establish a connection to the LTE mobile wireless network.

1. If the connection to the LTE mobile wireless network fails, the CMR attempts to establish a connection to the UMTS mobile wireless network.
2. If the connection to the UMTS mobile wireless network fails, the CMR attempts to establish a connection to the GSM/GPRS mobile wireless network.

6.8.3.1 Activate mobile wireless interface

By selecting the “Activate mobile wireless interface" check box, you make the mobile wireless interface operational.

If the check box is not selected, the mobile wireless interface cannot be used. The mobile wireless interface is turned off.

6.8.3.2 PIN of the SIM card

Entering the PIN

Note

SIM card without PIN

The CMR also works with SIM cards without a PIN. In this case, do not make an entry in the "PIN of the SIM card" input box.

Entry of an incorrect PIN

The last entered (incorrect) PIN is saved. This means that when changing the configuration (except the PIN) or when restarting the CMR, no further PIN entry attempt is used up.

For this reason, do not change the PIN of the SIM card to the previously stored incorrect PIN outside the CMR.

Locking if the PIN is entered correctly

Enter the PIN correctly. If you enter the PIN incorrectly three times, the SIM card will be locked. You should also note the information relating to inserting the SIM card and entering the PIN (Page 29).

Unlocking the SIM card

Unlocking the SIM card is described in the section Insert the SIM card and enter the PIN (Page 29).

You have received a PIN for your SIM card from your mobile wireless provider.

1. Enter the PIN for your SIM card in the input box.

   If you use a SIM card without a PIN, do not make an entry in the box.
2. By clicking the "Apply" button, you save the PIN with the other settings.

- A green check mark below the input box indicates that the PIN was saved successfully on the device.
- A red dot with a white cross below the input box indicates that the PIN was entered incorrectly and no PIN was stored on the device.

6.8.3.3 Allow roaming

Roaming means that the mobile wireless network of your mobile wireless provider is no longer reachable and another mobile wireless provider takes over the CMR in its mobile wireless network.

If the specified mobile wireless network is no longer reachable, specify whether or not the CMR should log in to another mobile wireless network.

- Select the "Allow roaming" check box.

  If the specified mobile wireless network is not available, the device logs in to an available mobile wireless network.

  Logging in to another mobile wireless provider can lead to higher connection costs.

- Disable the "Allow roaming" check box.

  If the specified mobile wireless network is not available, no connection is established to other mobile wireless networks.

6.8.3.4 Phone number of the SMS service center

- In the input box, enter the phone number of the SMS service center of your GSM network provider.

  In most cases, you will find this phone number on the SIM card of your mobile wireless provider.

Enter a phone number in the input box only if you do **not** want to use the number of the SMS service center preset by the mobile wireless provider.

6.8.3.5 Activate a data connection via the mobile wireless network

Note

Enabling mobile data connections

Arrange for the required mobile data connections to be enabled by your mobile wireless provider.

You can turn the mobile data connection on or off for your device.

- "Activate data connection via the mobile wireless network" check box enabled:

  If you also want to use IP-based data services of your mobile wireless provider in addition to sending and receiving SMS messages, for example time-of-day synchronization using NTP.

- "Activate data connection via the mobile wireless network" check box is disabled:

  The CMR can only send and receive SMS messages.

6.8.3.6 APN / User name / Password

Note

Searching for APN, user name and password of the mobile wireless provider

You can obtain information about this access data from your mobile wireless provider or from the Internet.

- Enter, for example, the keywords "APN mobile wireless provider" in a search engine.

  The search result provides an overview of various providers with all the required access parameters.

The **APN** (Access Point Name) is the DNS host name of the access point of a mobile wireless provider to an external packet data network, e.g. LTE, UMTS, GPRS.

- APN

  Enter the APN of your mobile wireless provider in the input box.

- User name

  In the input box, enter the user name given to you by your mobile wireless provider.
  Some mobile wireless providers do without the access check with a user name. In this case, leave the input box empty.

- Password

  In the input box, enter the password of the relevant provider.
  Some mobile wireless providers do without the access check with a password. In this case, leave the input box empty.

Authentication method

Note

CHAP and PAP - meaning

CHAP: Encrypted transfer of user name and password using the Challenge Handshake Authentication Protocol.

PAP: Unencrypted transfer of user name and password using the Password Authentication Protocol.

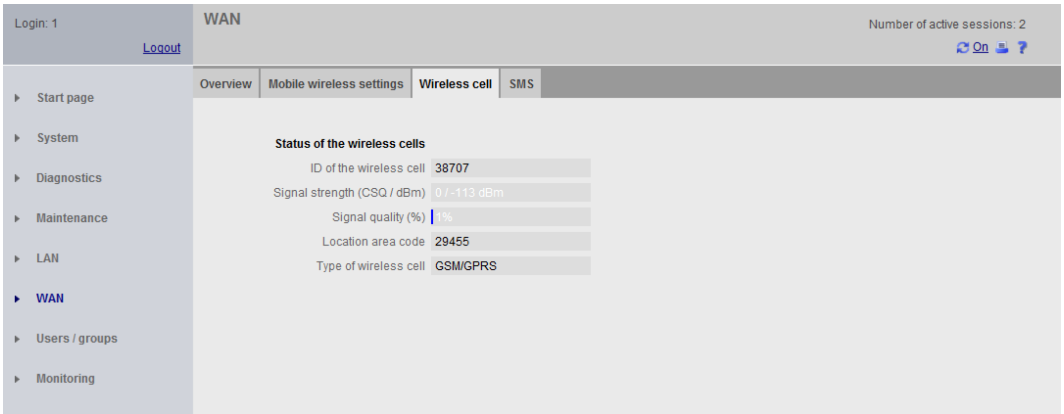
- From the "Authentication method" drop-down list, select a method with which the user name and the password of the APN will be transferred to the communications partner.
  - None

    No authentication
  - CHAP or PAP

    User name and password are transferred automatically with one of the two methods.

    CHAP has the higher priority. If the communications partner does not support CHAP, the user name and password are transferred using PAP.

6.8.4 Wireless cell



Status of the wireless cells

ID of the wireless cell	38707
Signal strength (CSQ / dBm)	0 / -113 dBm
Signal quality (%)	1%
Location area code	29455
Type of wireless cell	GSM/GPRS

Figure 6-13 WAN – "Wireless cell" tab

To obtain useful status information:

- Enable the mobile wireless interface in the Mobile wireless settings tab.

Optimum antenna alignment

To allow you to find the optimum alignment of the antenna connected to the SMA socket, you can use the "Wireless cell" tab. The "Wireless cell" tab allows you to test the signal strength at various antenna positions.

The information is updated at intervals of a few seconds. To be able to find the optimum position, you receive immediate information about the signal strength at the test positions.

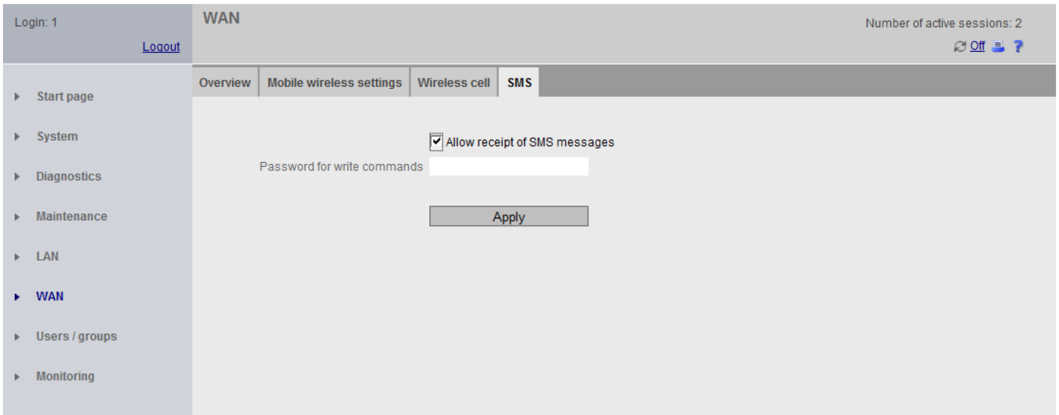
Status of the wireless cells

You will find information about the mobile wireless cell where the CMR is currently booked in:

- Signal quality: Amount of correctly transferred data/amount of all transferred data
- Signal strength
- ID of the wireless cell in the mobile wireless network: ID of the wireless cell
- Location area code

  Identifier for the current location of the CMR within the mobile wireless network.

6.8.5 SMS



☑ Allow receipt of SMS messages

Password for write commands

Figure 6-14 WAN – "SMS" tab

In the "SMS" tab, you can do the following:

- Allow or not allow receipt of SMS messages
  - Allow receipt of SMS messages: Select the check box.

    SMS messages are received and evaluated or processed further.
  - Do not allow receipt of SMS messages: Deselect the check box.

    SMS messages are received but not evaluated.

  Note

  Do not allow receipt of SMS messages: CMR does not evaluate received SMS message

  If you do not allow receipt of SMS messages in the "SMS" tab:
  Regardless of the SMS rights you have assigned on the Users / groups (Page 80) page for the users, the CMR does not evaluate received SMS messages.

  Roaming costs can still result

  The CMR receives **all** SMS messages regardless of whether the check box was disabled or enabled. For this reason roaming costs can also result in even if receipt of SMS messages is blocked.

- Define a password for SMS write commands.

  Note

  Permitted characters and character lengths for the password

  You will find the conditions that apply to passwords in Permitted characters and character lengths (Page 41).

  Only SMS write commands with the correct password are executed by the CMR.

If you click the "Apply" button, all the settings you made in the "SMS" tab are adopted.

Operation 7

7.1 Overview

In this section, you will find information about the following topics:

- Exchanging information with the BM via the CMR
- Changing values in the BM or the CMR.
- Mobile wireless communication without LOGO! BM (stand-alone operation of the CMR)
- Monitoring of the LOGO! BM.

Note

Permitted characters and character lengths for the password

You will find the characters permitted for passwords in the section Permitted characters and character lengths (Page 41).

Monitoring of a LOGO! BM

The section Monitoring (Page 84) describes the following functions:

- Monitoring of the values of the BM.
- Definition of an action depending on the value change of an event

  This can, for example, be the sending of an an SMS message to the configured phone number due to an alarm message.
- Creating recipients and recipient groups.
- Notification of a recipient or a recipient group with freely creatable SMS texts when events occur

You will find out how to configure monitoring quickly in the section Example of a monitoring configuration (Page 103).

1. You define separate events, actions and recipients.
2. You then link the events, actions and recipients as required in a list.

7.2 Reading and writing values

Reading / writing "current values" via the BM variables memory (VM)

"Current values" (e.g. flags, counters) are read and written only via the BM variables memory (VM).

For reasons of security, setting or reading of current values of the function blocks of the BM (e.g. counters) is possible only via their address in the BM variables memory.

All components of the LOGO! switching program must therefore initially be transferred to the BM-internal variables memory using the "LOGO! Soft Comfort" program. Only then are the components visible with their start addresses and length (type) for the CMR in the BM variables memory.

Data types and range of values when reading and writing

To set individual bits, the data types available must be used.

LOGO! CMR and LOGO! BM interpret all values of the data types BYTE, WORD and DWORD as being signed.

Remember this when transferring values using SMS messages.

Data type	Length in the variables memory:	Range of values
Byte	1	-128 ... 127
WORD	2	-32 768 ... 32 767
DWORD	4	-2 147 483 648 ... 2 147 483 647

Reading and writing values in the variables memory (VM) of the LOGO!! BM using SMS messages

With the LOGO! CMR, values can be written to and read from the variables memory (VM) of a LOGO! BM using SMS messages.

The parameters to be specified in SMS commands are the address and type (<address>, <data type>, refer to the section SMS commands (Page 112).

In the WBM of the LOGO! CMR, a limit this or a threshold value for a value from the LOGO! 8 can be specified on the "Monitoring" > "Events" page. If the threshold of the value in the LOGO! 8 is exceeded or fallen below, the sending of an SMS message to one or more recipients can, for example, be configured.

Note the signed interpretation of the values also in the following applications:

- Setting threshold/limit values for values in the LOGO! BM via the WBM of the LOGO! CMR
- Display of values in the LOGO! BM via the WBM of the LOGO! CMR
- Reading/writing values in the LOGO! BM using SMS messages with the LOGO! CMR

Reading and writing using LOGO!Soft Comfort

Note

Access only to the first 128 bytes of the VM (Variable Memory)

In LOGO!Soft Comfort the VM goes to address 850. Via the CMR, however, only the first 128 bytes can be accessed.

For security reasons the address in theVM can only be read or written using SMS if the address was created earlier as a signal using the WBM.

Table 7- 1 Overview of the options for accessing the LOGO! BM

Value of the LOGO! BM	Read access	Write access with action	Write access using SMS
Digital inputs (I)	x	-	-
Digital flags (M)	x	-	-
Digital outputs (Q)	x	-	-
Analog inputs (AI)	x	-	-
Analog flags (AM)	x	-	-
Analog outputs (AQ)	x	-	-
Cursor keys (C)	x	-	-
Function keys (F)	x	-	-
Shift register bits (S)	x	-	-
Variables memory (VM)	x	x [1]	x
Program status (PS)	x	x	x

[1] You only have write access to the variables memory of the LOGO! BM with the "Forward GPS position" action

1. In the program "LOGO! Soft Comfort" click "Tools" > "Parameter VM Mapping":

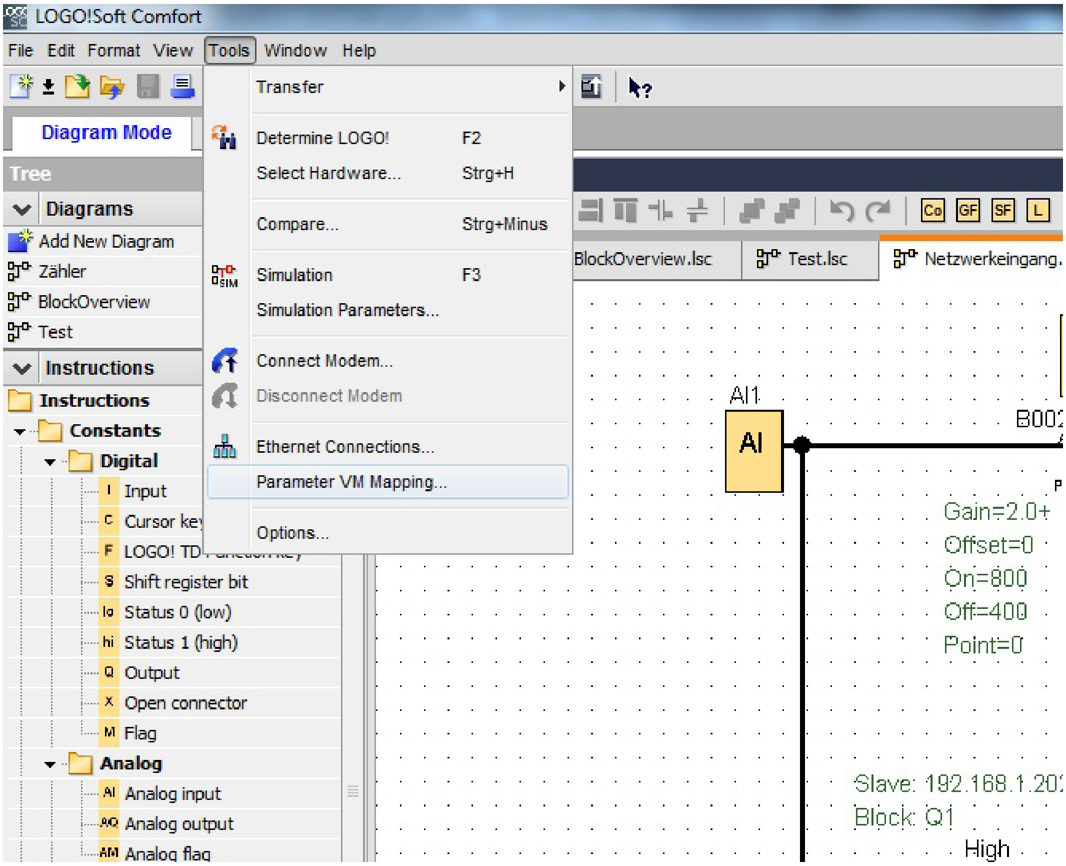
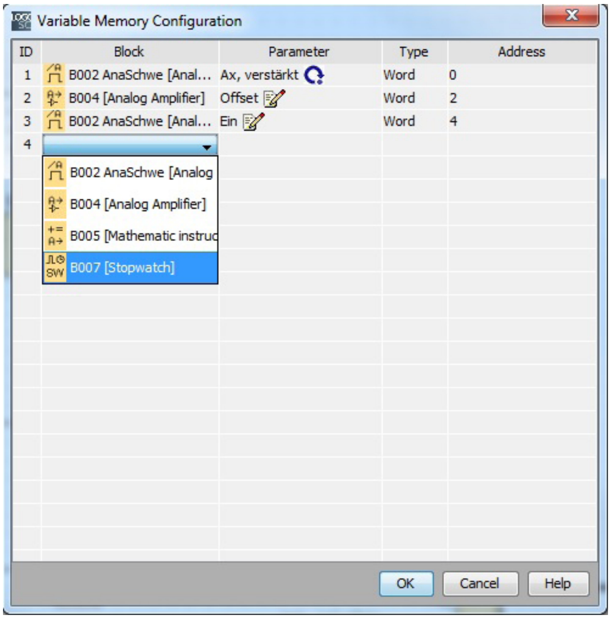


Figure 7-1 LOGO! Soft Comfort - tools

2. Select a block from your control program that you want to transfer to theVM memory.

   In the following figure, select the block B007 from your control program with the stopwatch function.



ID	Block	Parameter	Type	Address
1	B002 AnaSchwe [Anal...	Ax, verstärkt	Word	0
2	B004 [Analog Amplifier]	Offset	Word	2
3	B002 AnaSchwe [Anal...	Ein	Word	4
4				

B002 AnaSchwe [Analog
B004 [Analog Amplifier]
B005 [Mathematic instruc
B007 [Stopwatch]

Figure 7-2 Variable Memory Configuration

3. Within the B007 block then select a variable to be monitored.
4. By clicking the "OK" button, you confirm your selection.

   The selected variable is transferred to theVM.

The "Type" and "Address" of the selected variable are displayed in the VM.

For further details, refer to the LOGO! Soft Comfort description.

With the "Address" and "Type" parameters in the relevant SMS message, you can read and write the status of the variables using SMS (Page 112).

7.3 Users / groups

You can enter a maximum of 20 users in the CMR:

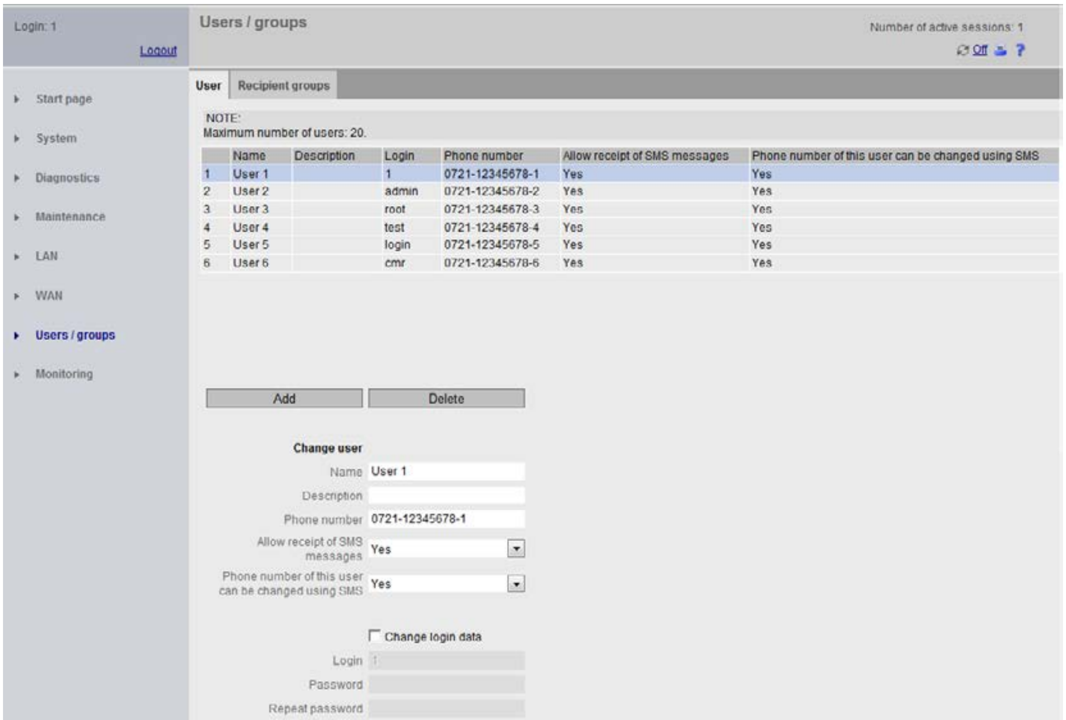
- Assign attributes to every user: Description, name, phone number and much more.
- You set up recipient groups by distributing the users you have entered:
  - Note that you can configure a maximum of five recipient groups with a maximum of ten users.
  - Recipient groups must not consist of only one recipient.

7.3.1 Calling the Web page

In the navigation panel, select the "Users / groups" entry and click on the available tabs:

- User
- Recipient groups

7.3.2 User



NOTE:
Maximum number of users: 20.

	Name	Description	Login	Phone number	Allow receipt of SMS messages	Phone number of this user can be changed using SMS
1	User 1		1	0721-12345678-1	Yes	Yes
2	User 2		admin	0721-12345678-2	Yes	Yes
3	User 3		root	0721-12345678-3	Yes	Yes
4	User 4		test	0721-12345678-4	Yes	Yes
5	User 5		login	0721-12345678-5	Yes	Yes
6	User 6		cmr	0721-12345678-6	Yes	Yes

Change user

Name	User 1
Description	
Phone number	0721-12345678-1
Allow receipt of SMS messages	Yes
Phone number of this user can be changed using SMS	Yes

□ Change login data

Login	1
Password	
Repeat password	

Figure 7-3 Users / groups - "User" tab

You can enter a maximum of 20 users in the tab. You assign attributes and rights to these users.

If you click the "Apply" button, all the settings you made in the "User" tab are adopted.

Add new user

1. Click the "Add" button.
2. Input boxes and drop-down lists are then available for the configuration.

Attributes

Enter the name, description and phone number of the user in the input boxes.

- Name

  User name you can select freely. This name is not used as a login and may contain special characters.

- Description

  Freely selectable text for a more detailed description of the user, e.g. "Service technician".

- Phone number

  Phone number at which the user can be reached.

  You can also define phone number groups by using the "*" character. For example, with the entry "+49172*", all phone numbers that start with "+49172" are authorized to send SMS messages to the CMR.

  Note

  Note the following when using phone number groups

  When using phone number groups, remember that the users of these groups cannot receive SMS messages. The users of these groups are only authorized to send SMS messages to the CMR.

Rights

- Allow receipt of SMS messages

  “Allow receipt of SMS messages" means that the created user can send SMS commands to the CMR.

  – An SMS message of the user with the specified phone number is received and evaluated (allow receipt)

  – An SMS message of the user with the specified phone number discarded: the SMS message is not evaluated (do not allow receipt).

- Phone number of this user can be changed using SMS

  You can change the phone number of this user with the "CHANGEUSER" with an SMS message.

  Changing the phone number using an SMS message can be useful in the following situations:

  – If you want to set up a substitute for a period of vacation.

  – If a phone number has changed and you cannot or do not want to make this change locally or using theWBM.

Change login data

You can change the login and the password of every user:

1. Select the required user in the list.
2. Select the "Change login data" check box.

   In the input boxes, change the login and password of the user.
3. Confirm the changed password in the "Repeat password" input box.
4. If you click the “Apply” button, the changes are adopted.

   The list is then updated with the changes.

Delete user

Note

Elements that are being used cannot be deleted

You can only delete an element (signal, text, user, recipient group, event, action) if the element is unused.

If the element is used, e.g. a user in a recipient group or a signal in an event, you cannot delete the element.

---

1. In the list, select the row with the user you want to delete.
2. Click the "Delete" button.

   A prompt for confirmation is displayed.
3. If you confirm this, the user is deleted and removed from the list.

Change user

1. In the list, select the row with the user you want to modify.
2. Change the user data with “Change user" in the lower part of the page.

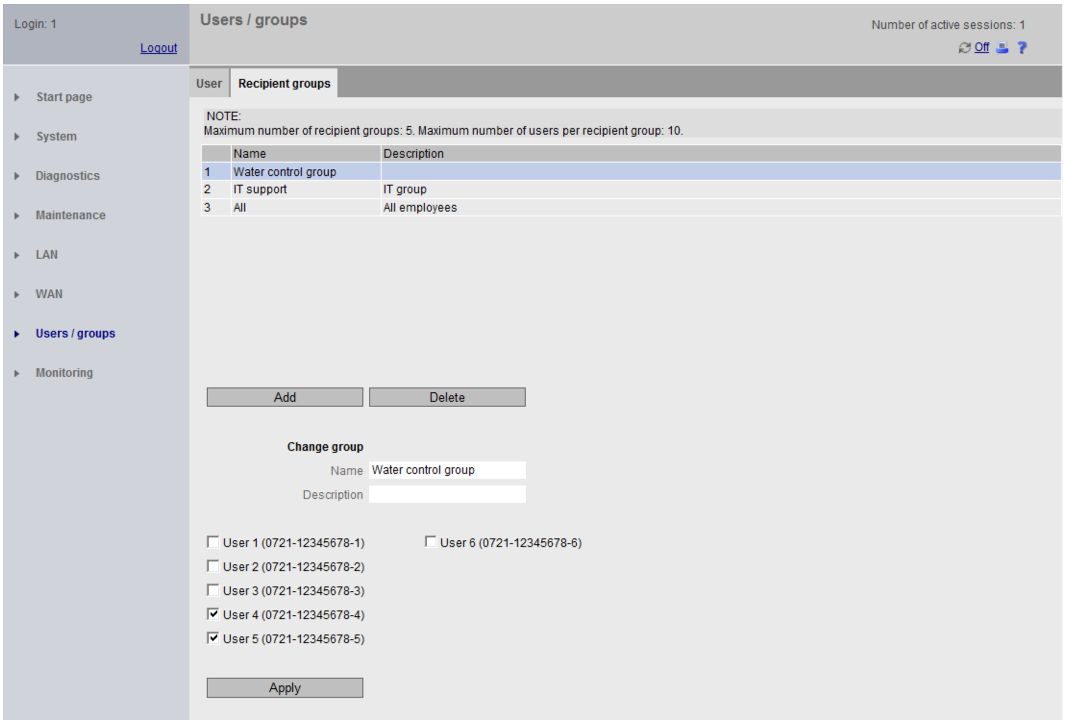
Result: When you click the "Apply” button, your change is adopted and displayed in the list.

Note

A user profile can be changed

You can change your own user profile (name, description, phone number, SMS settings) as well as the login and password. You can also change the user profiles, logins and passwords of the user entered in the "Name" column. This means that every user has administrator rights.

7.3.3 Recipient groups



NOTE:
Maximum number of recipient groups: 5. Maximum number of users per recipient group: 10.

	Name	Description
1	Water control group	
2	IT support	IT group
3	All	All employees

Change group

Name: Water control group

Description:

☐ User 1 (0721-12345678-1)
☐ User 2 (0721-12345678-2)
☐ User 3 (0721-12345678-3)
☑ User 4 (0721-12345678-4)
☑ User 5 (0721-12345678-5)
☐ User 6 (0721-12345678-6)

Figure 7-4 Users / groups - "Recipient groups" tab

In this tab, you set up your recipient groups or make changes to recipient groups that have already been set up.

You can set up a maximum of five groups each with ten users per group.

If you click the "Apply" button, all the settings you made in the "Recipient groups" tab are adopted.

Add new group

1. Click the "Add" button.
2. Enter any name and a description for the group.

   In the lower part of the page you will find all the users you have entered and their phone numbers in brackets.
3. Select the check boxes of all users you want to include in the new group.
4. If you click the "Apply" button, the settings you have made are adopted.

   Your new group is now set up and is displayed in the list.

Note

To send SMS messages, you require groups and users.

Change group

1. In the list, select the row with the group you want to modify.

   The selected group is displayed under "Change group".
2. You can now change the name and description.
   - By selecting check boxes in the lower part of the page, you add new users.
   - By deselecting check boxes in the lower part of the page, you remove users from the group.
3. If you click the "Apply" button, the settings you have made are adopted.

   Your changes are adopted and displayed in the list.

Delete group

Note

Elements that are being used cannot be deleted

You can only delete an element (signal, text, user, recipient group, event, action) if the element is unused.

If the element is used, e.g. a user in a recipient group or a signal in an event, you cannot delete the element.

1. In the list, select the row with the group you want to delete.
2. Click the "Delete" button.

   The group is deleted and removed from the list.

7.4 Monitoring

Before you start to configure monitoring of a BM or the CMR in stand-alone mode, read the following section carefully:

- The principle of monitoring and message configuration is explained below in a brief overview (Page 87).
- You will find a detailed description of the tabs in the relevant sections.
- A practical Example of a monitoring configuration (Page 103) explains the procedure.

Once you have understood the principle of monitoring and message configuration, you can create or modify configurations quickly and simply.

7.4.1 Calling the Web page

In the navigation panel, select the "Monitoring" entry and click on the available tabs:

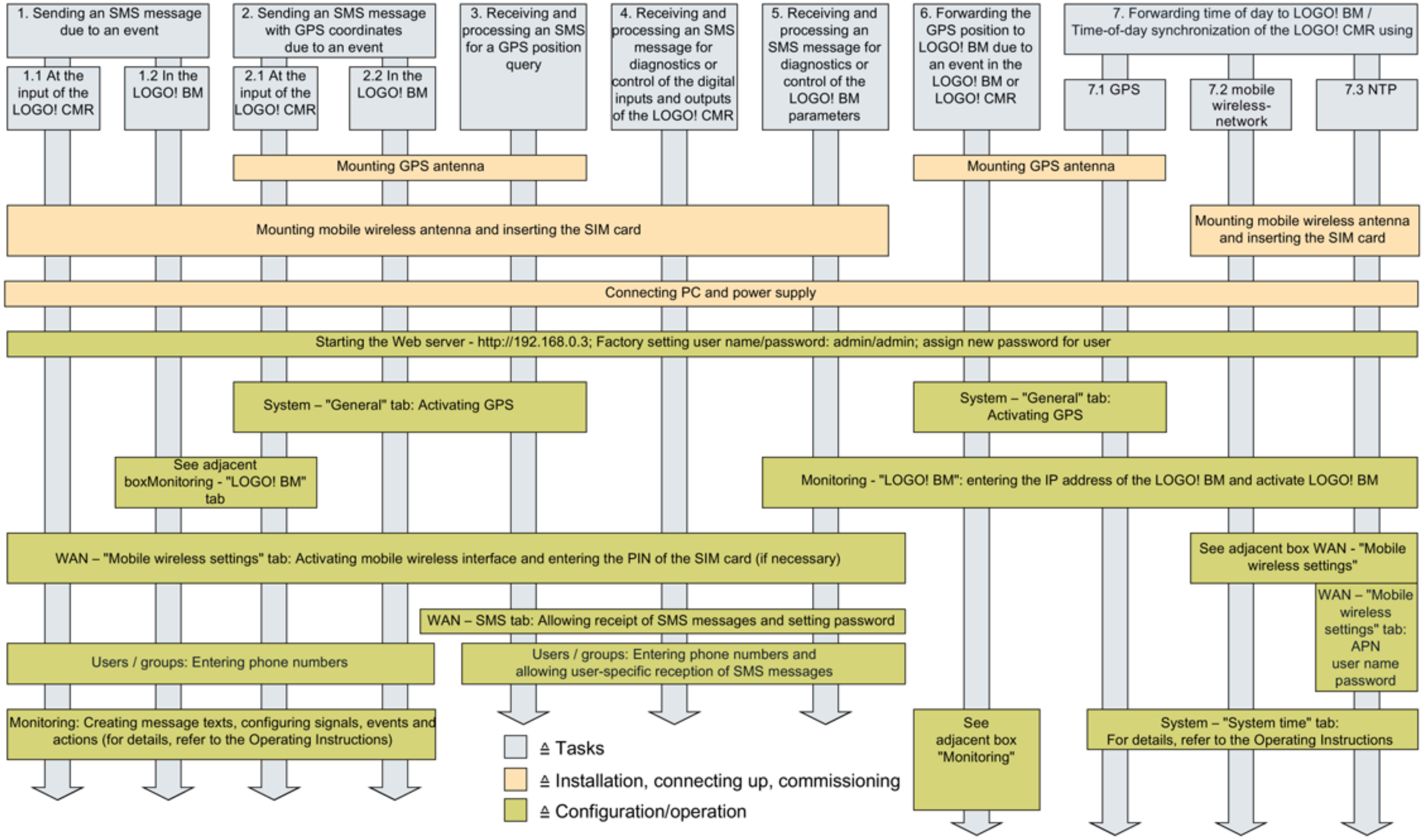
- Overview
- LOGO! BM
- Message texts
- Signal definitions
- Events
- Actions
- Assignments

You will find a brief explanation of the tasks involved on the individual tabs in the following section "Principle of monitoring and message configuration (Page 87)".

You will find a detailed description in the individual sections describing the tabs.

7.4.2 Which task needs to be completed? - Which steps are necessary for this?

To allow better orientation, you will find a graphic overview of the individual applications/tasks and the steps required here:


1. Sending an SMS message due to an event
1.1 At the input of the LOGO! CMR
1.2 In the LOGO! BM
2. Sending an SMS message with GPS coordinates due to an event
2.1 At the input of the LOGO! CMR
2.2 In the LOGO! BM
3. Receiving and processing an SMS for a GPS position query
4. Receiving and processing an SMS message for diagnostics or control of the digital inputs and outputs of the LOGO! CMR
5. Receiving and processing an SMS message for diagnostics or control of the LOGO! BM parameters
6. Forwarding the GPS position to LOGO! BM due to an event in the LOGO! BM or LOGO! CMR
7. Forwarding time of day to LOGO! BM / Time-of-day synchronization of the LOGO! CMR using
7.1 GPS
7.2 mobile wireless-network
7.3 NTP
Mounting GPS antenna
Mounting GPS antenna
Mounting mobile wireless antenna and inserting the SIM card
Mounting mobile wireless antenna and inserting the SIM card
Connecting PC and power supply
Starting the Web server - http://192.168.0.3; Factory setting user name/password: admin/admin; assign new password for user
System – "General" tab: Activating GPS
System – "General" tab: Activating GPS
See adjacent boxMonitoring - "LOGO! BM" tab
Monitoring - "LOGO! BM": entering the IP address of the LOGO! BM and activate LOGO! BM
WAN – "Mobile wireless settings" tab: Activating mobile wireless interface and entering the PIN of the SIM card (if necessary)
See adjacent box WAN - "Mobile wireless settings"
WAN – "Mobile wireless settings" tab: APN user name password
WAN – SMS tab: Allowing receipt of SMS messages and setting password
Users / groups: Entering phone numbers
Users / groups: Entering phone numbers and allowing user-specific reception of SMS messages
Monitoring: Creating message texts, configuring signals, events and actions (for details, refer to the Operating Instructions)
See adjacent box "Monitoring"
System – "System time" tab: For details, refer to the Operating Instructions
□ ≙ Tasks
□ ≙ Installation, connecting up, commissioning
□ ≙ Configuration/operation

7.4.3 Principle of monitoring and message configuration

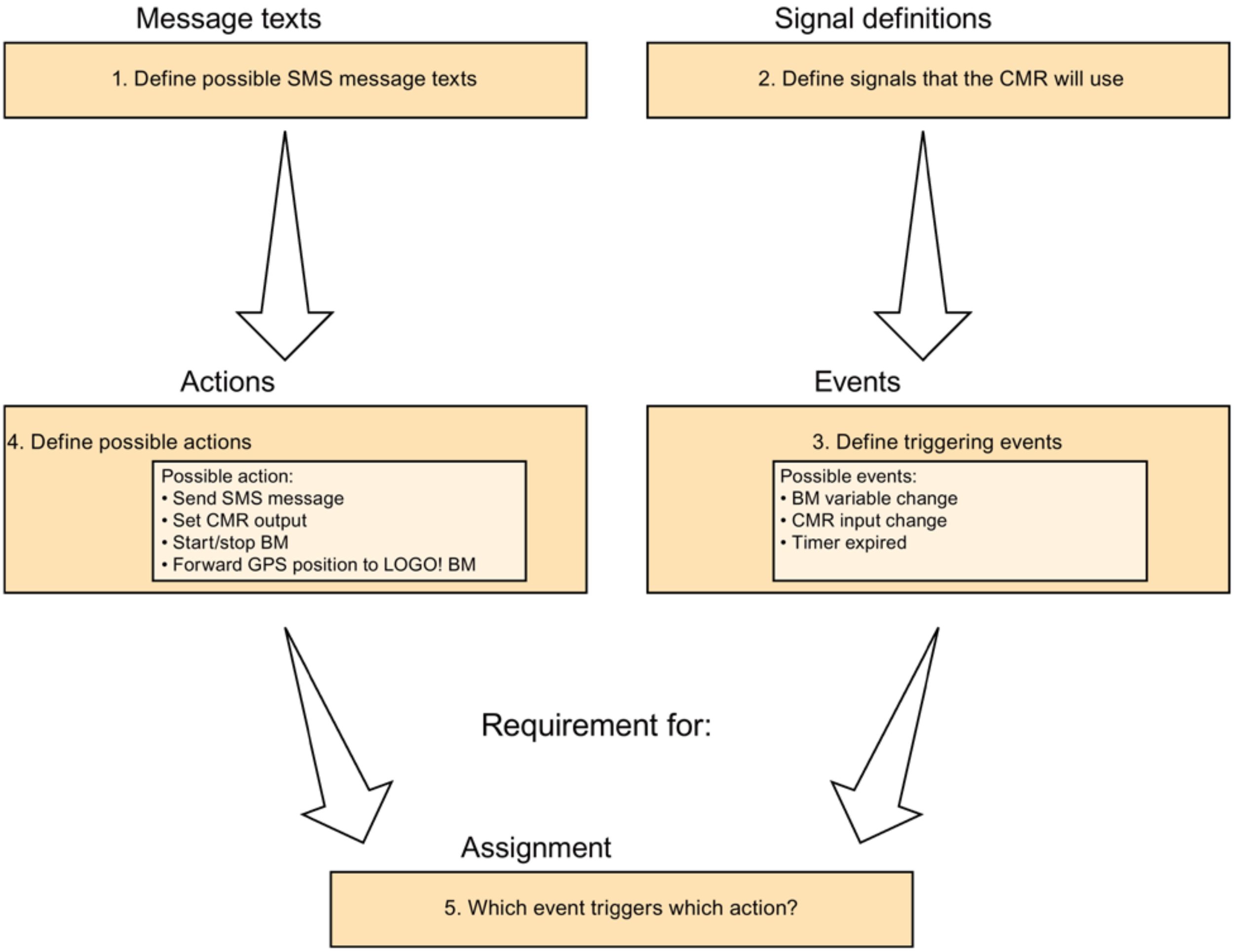


Figure 7-5 Monitoring - procedure for configuration

Overview

You will see all the configured signal definitions with their current status.

When shipped, the inputs and outputs of the CMR have already been created as signals and are displayed in the overview.

LOGO! BM

A connection between the CMR and BM is only established if you have selected the "Active" check box.

If you have deselected the "Active" check box, no connection is established to the BM.

- You enter the IP address of your BM.
- "Ping LOGO! BM" button: You test whether the entered IP address can be reached by the CMR.
- Query interval for process image: You specify the intervals at which the process image of the BM is read by the CMR.

Message texts

You create texts you want to send using SMS:

1. You define the sending of these texts to a recipient or recipient group as an action in the "Actions" tab.
2. You assign this action to an event in the "Assignments" tab.

You can assign symbolic names to the message texts.

Signal definitions

You first specify which signals from the BM or the CMR you want to monitor; e.g. the digital input 1 (I1) of the BM.

You can give all signals symbolic names ("ALIAS").

Events

For the selected signal, you define an event, for example I1 “ changes to 0".

You can give all events symbolic names ("ALIAS").

Actions

You specify one or more actions, initially not associated with an event:

- Send an SMS message to a recipient group.
- Set an output in the CMR.
- Send PI SMS message (process image SMS message).
- Forwarding a GPS position to LOGO! BM
- Change the status of the LOGO! BM .

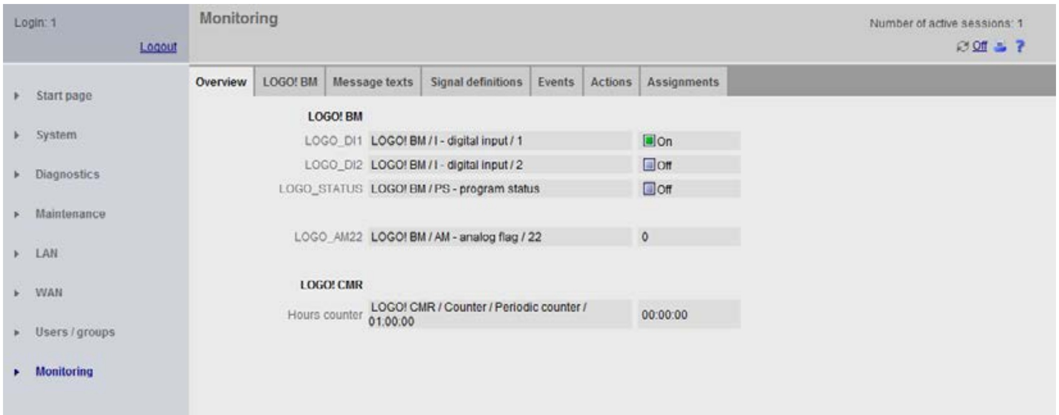
You can give all actions symbolic names ("ALIAS").

Assignments

You assign certain actions to the defined events, for example sending an SMS message to a particular recipient group if an output of the BM changes.

In the lower part of the page under “If:" and "Then:" you will see which action will be executed along with all the set parameters.

7.4.4 Overview



LOGO! BM		
LOGO_DI1	LOGO! BM / I - digital input / 1	🟩 On
LOGO_DI2	LOGO! BM / I - digital input / 2	□ Off
LOGO_STATUS	LOGO! BM / PS - program status	□ Off
LOGO_AM22	LOGO! BM / AM - analog flag / 22	0
LOGO! CMR		
Hours counter	LOGO! CMR / Counter / Periodic counter / 01:00:00	00:00:00

Figure 7-6 Monitoring – "Overview" tab

All configured signal definitions of the BM and the CMR are displayed with symbolic names and their current status.

After resetting to factory settings, the inputs and outputs of the CMR are displayed as when shipped.

Display if the connection between the CMR and BM is interrupted

- In the "LOGO! BM" tab, you have configured a connection between the CMR and BM.
- You have configured LOGO!-BM signal types in the “Signal definitions tab .

The connection between the CMR and BM is interrupted, for example by removing the Ethernet cable:

- The error LED of the CMR is lit red.
- The "Overview" tab shows all configured signal types of the BM in red characters.
- If the "LOGO! BM" signal was configured with the signal types "CS - communications status", the signal changes to the status "Off".

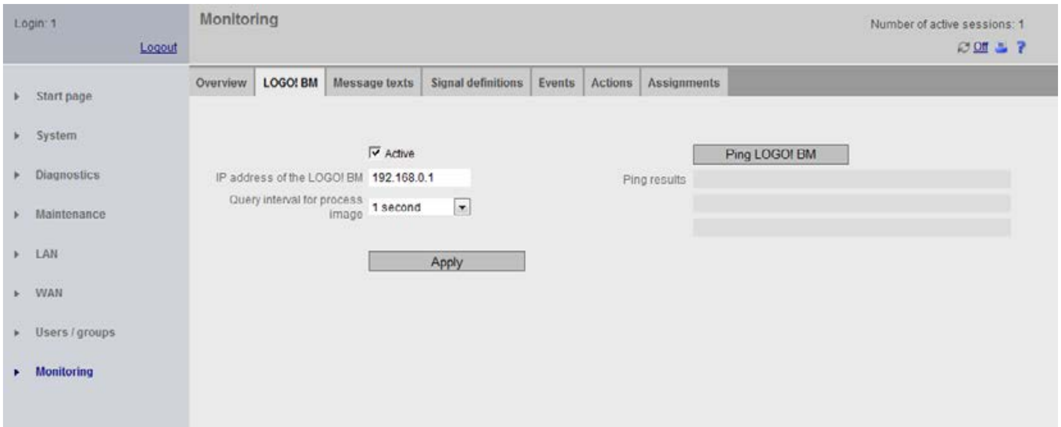
Note

Delayed display of the interrupted connection

The interrupted connection is detected by the CMR after a delay of several seconds.

7.4.5 LOGO! BM

Establishing communication between IBM and CMR



☑ Active

IP address of the LOGO! BM: 192.168.0.1

Query interval for process image: 1 second

Figure 7-7 Monitoring - "LOGO! BM" tab

1. Enter the IP address of your BM in the “IP address of the LOGO! BM" input box.
2. Select the "Active" check box. This establishes a connection between the CMR and BM.

   If the check box is disabled, there is no connection between the CMR and BM.
3. Then click the "Apply" button. The settings you have made are applied.
4. Click the “Ping LOGO! BM" button:

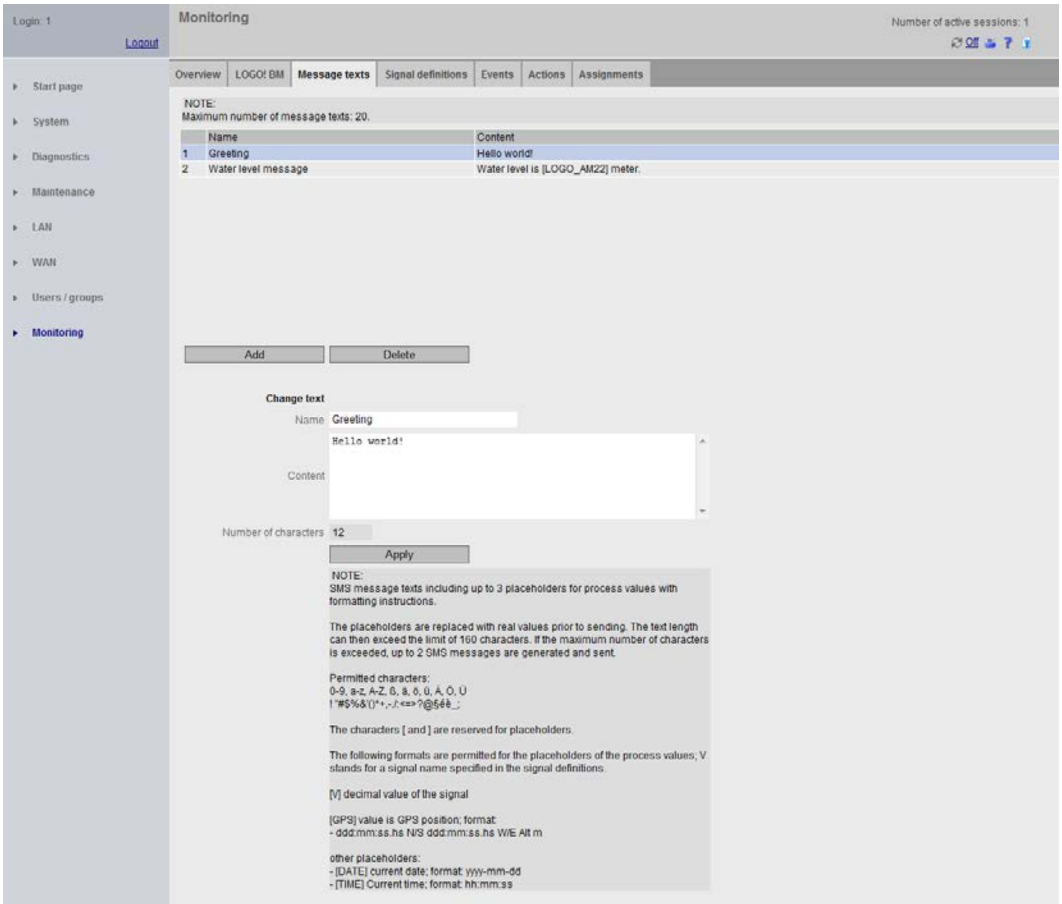
   You test whether the entered IP address can be reached by the CMR. A message is displayed indicating whether or not the IP address can be reached.

- With the "Query interval for process image" setting you specify the intervals (selection: "1 second" and "10 seconds") at which the process image of the BM will be read by the CMR:

  The CMR keeps a copy of the current process image and on request sends the process image as a reply SMS message: see SMS commands (Page 112) and Reply SMS message to the "MONITOR?" command (Page 116).

If you click the "Apply" button, all the settings you made in the "LOGO! BM" tab are adopted.

7.4.6 Message texts



NOTE:
Maximum number of message texts: 20.

	Name	Content
1	Greeting	Hello world!
2	Water level message	Water level is [LOGO_AM22] meter.

Change text

Name: Greeting

Content: Hello world!

Number of characters: 12

NOTE:
SMS message texts including up to 3 placeholders for process values with formatting instructions.

The placeholders are replaced with real values prior to sending. The text length can then exceed the limit of 160 characters. If the maximum number of characters is exceeded, up to 2 SMS messages are generated and sent.

Permitted characters:
0-9, a-z, A-Z, ß, ä, ö, ü, Ä, Ö, Ü
!"#$%&'()*+,-./:<=>?@§éè_;

The characters [and] are reserved for placeholders.

The following formats are permitted for the placeholders of the process values; V stands for a signal name specified in the signal definitions.

[V] decimal value of the signal

[GPS] value is GPS position; format:
- ddd:mm:ss.hs N/S ddd:mm:ss.hs W/E Alt m

other placeholders:
- [DATE] current date; format: yyyy-mm-dd
- [TIME] Current time; format: hh:mm:ss

Figure 7-8 Monitoring – "Message texts" tab

Adding a new message text

You can create various SMS message texts.

You can assign a symbolic name to every message text. You can create the text freely with a maximum of 160 characters per message text.

- You configure which texts are sent to which recipient groups in the "Actions (Page 97)" tab.
- If you click the "Apply" button, all the settings you made in the "Message texts" tab are adopted.

Deleting a message text

Note

Elements that are being used cannot be deleted

You can only delete an element (signal, text, user, recipient group, event, action) if the element is unused.

If the element is used, e.g. a user in a recipient group or a signal in an event, you cannot delete the element.

1. In the list, select the row with the message text you want to delete.
2. Click the "Delete" button.

   A prompt for confirmation is displayed.
3. If you confirm this, the message text is deleted and removed from the list.

Changing a message text

1. In the list, select the row with the message text you want to modify.
2. Change the message text with "Change text" in the lower part of the page.

Result: If you click the "Apply" button, your modified message text is adopted and displayed in the list.

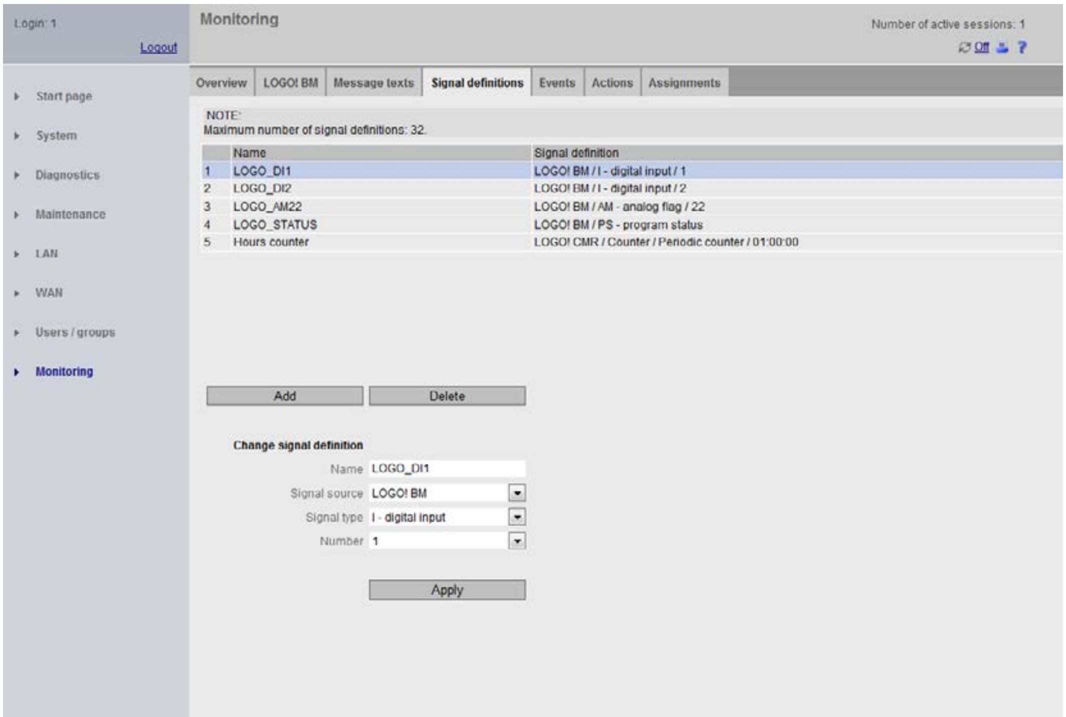
Sending process values and parameters along with the message

In the SMS message texts, you can also send process values and parameters such as time, date and GPS position.

If placeholders are used, 2 SMS messages will be sent under some circumstances.

You will find the formats permitted for the placeholders of the process values in Permitted characters and character lengths (Page 41).

7.4.7 Signal definitions



NOTE:
Maximum number of signal definitions: 32.

	Name	Signal definition
1	LOGO_DI1	LOGO! BM / I - digital input / 1
2	LOGO_DI2	LOGO! BM / I - digital input / 2
3	LOGO_AM22	LOGO! BM / AM - analog flag / 22
4	LOGO_STATUS	LOGO! BM / PS - program status
5	Hours counter	LOGO! CMR / Counter / Periodic counter / 01:00:00

Change signal definition

Name: LOGO_DI1
Signal source: LOGO! BM
Signal type: I - digital input
Number: 1

Figure 7-9 Monitoring – "Signal definitions" tab

You specify which signals of the BM or the CMR you want to monitor.

In the upper part of the page, you will see a list with the currently configured signal definitions:

- A maximum of 32 signal definitions are possible.

In the lower part of the page, under "Change signal definition", you will find the area required for signal configuration.

If you click the "Apply" button, all the settings you made in the “Signal definitions" tab are adopted and displayed in the list.

Add new signal definition

1. In the lower part of the page, click the "Add" button.
2. An input box and three drop-down lists are then available for the configuration:

   Name

   – Freely selectable symbolic signal name.

   Signal source

   – From the "Signal source" drop-down list, select the entry "LOGO! BM" for the BM or "LOGO! CMR" for the CMR.

   Signal type

   Depending on the signal source you have selected, the signal types available for the signal source are displayed.

   – With "LOGO! BM", these are all the components of the BM process image and areas of the variables memory.

   – With "LOGO! CMR", these are the inputs and outputs or counters and the mobile wireless network and data connection status.
3. Depending on the selection you have made in "Signal type" and "Signal source", further buttons will become available with which you can complete your signal definition.
4. If you click the "Apply" button, the entries you have made are adopted.

Result: Your signal definition is adopted and displayed in the list.

Deleting a signal definition

Note

Elements that are being used cannot be deleted

You can only delete an element (signal, text, user, recipient group, event, action) if the element is unused.

If the element is used, e.g. a user in a recipient group or a signal in an event, you cannot delete the element.

1. In the list, select the row with the signal definition you want to delete.
2. Click the "Delete" button.

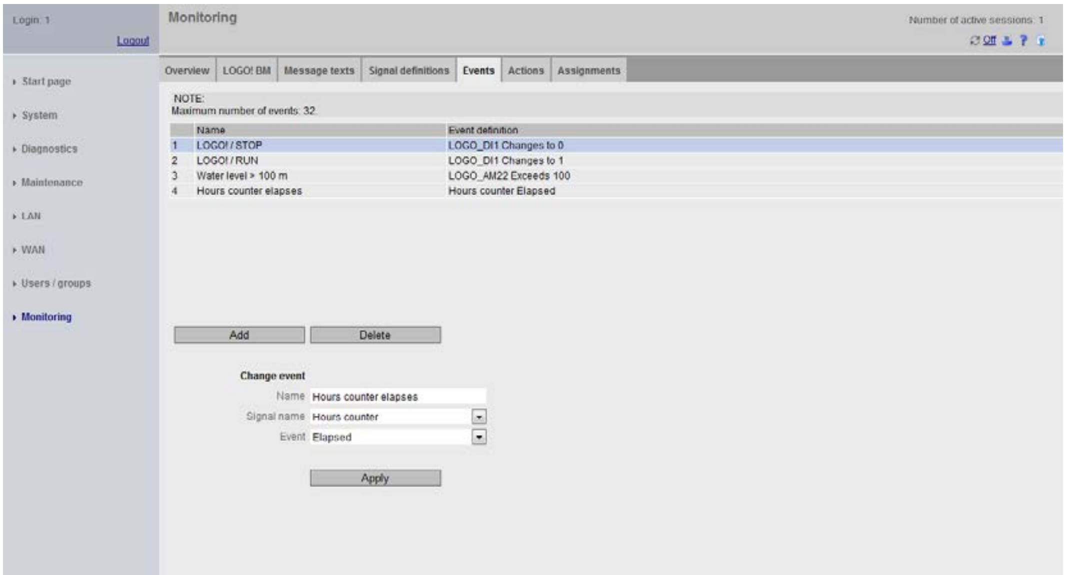
   A prompt for confirmation is displayed.
3. If you confirm this, the signal definition is deleted and removed from the list.

Change signal definition

1. In the list, select the row with the signal definition you want to modify.
2. Change the signal definition with "Change signal definition" in the lower part of the page.

Result: If you click the "Apply" button, your modified signal definition is adopted and displayed in the list.

7.4.8 Events



NOTE:
Maximum number of events: 32

	Name	Event definition
1	LOGO! / STOP	LOGO_DI1 Changes to 0
2	LOGO! / RUN	LOGO_DI1 Changes to 1
3	Water level > 100 m	LOGO_AM22 Exceeds 100
4	Hours counter elapses	Hours counter Elapsed

Change event

Name: Hours counter elapses
Signal name: Hours counter
Event: Elapsed

Figure 7-10 Monitoring – "Events" tab

For a selected signal, you define an event, for example I1 “changes to 0".

In the upper part of the page, you will see a list with the currently configured events:

- A maximum of 32 events are possible.

  If you have not yet defined an event, the list is empty.

In the lower part of the page, under "Change event", you will find the area required for event configuration.

If you click the "Apply" button, all the settings you made in the “Events” tab are adopted and displayed in the list.

Add new event

1. In the lower part of the page, click the "Add" button.
2. An input box and two drop-down lists are then available for the configuration:

   Name

   – Freely selectable symbolic name for the event.

   Signal name

   – Select the relevant signal from the drop-down list.
   All the signal definitions you have configured along with their symbolic names are available.

   Event

   – You define the event. Examples:
   The digital input changes from "1" to "0".
   The analog flag falls below or exceeds the value you specify this point.
3. Depending on the selection you have made in "Signal name" and "Event", further buttons will become available with which you can complete your event.
4. If you click the "Apply" button, the entries you have made are adopted.

Result: Your event is adopted and displayed in the list.

Deleting an event

Note

Elements that are being used cannot be deleted

You can only delete an element (signal, text, user, recipient group, event, action) if the element is unused.

If the element is used, e.g. a user in a recipient group or a signal in an event, you cannot delete the element.

1. In the list, select the row with the event you want to delete.
2. Click the "Delete" button.

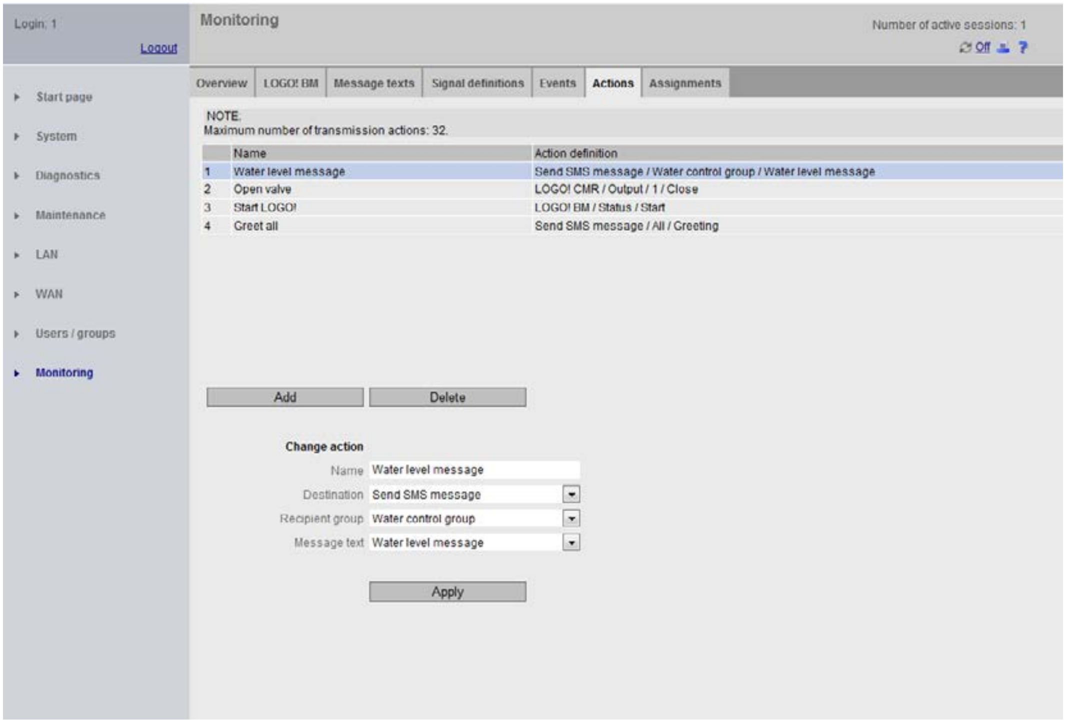
   A prompt for confirmation is displayed.
3. If you confirm this, the event is deleted and removed from the list.

Change event

1. In the list, select the row with the event you want to change.
2. Change the event with "Change event" in the lower part of the page.

Result: If you click the "Apply" button, your modified event is adopted and displayed in the list.

7.4.9 Actions



NOTE.
Maximum number of transmission actions: 32.

	Name	Action definition
1	Water level message	Send SMS message / Water control group / Water level message
2	Open valve	LOGO! CMR / Output / 1 / Close
3	Start LOGO!	LOGO! BM / Status / Start
4	Greet all	Send SMS message / All / Greeting

Change action

Name: Water level message
Destination: Send SMS message
Recipient group: Water control group
Message text: Water level message

Figure 7-11 Monitoring – "Actions" tab

You specify one or more actions, initially not associated with an event.

In the upper part of the page, you will see a list with the currently configured actions:

- A maximum of 32 actions are possible.

  If you have not yet defined an action, the list is empty.

In the lower part of the page, under "Change action", you will find the area required for action configuration.

If you click the "Apply" button, all the settings you made in the "Actions" tab are adopted and displayed in the list.

Note

First create actions then specify the assignment

1. First create all actions independently of configured events.
2. You then configure (Page 101) the assignment of an action to an event.

Add new action

1. In the lower part of the page, click the "Add" button.
2. An input box and three drop-down lists are then available for the configuration:

   Name

   – Freely selectable symbolic name for this action.

   Destination

   – Select the destination of your action from the drop-down list. Destinations can be the CMR, the BM, the SMS or the process image send function.
     If you select the CMR, you can use the two outputs of the CMR as the target element of an action: For example open an output, close or change an output.
     If you select the BM as the destination of your action you can change status of the BM or forward the GPS position data to the BM.

   Recipient group

   You can only select recipient groups and not individual users or phone numbers.

   – If you select "Send SMS message" or "Send PI SMS message" as the destination, you can choose from the recipient groups you have configured.

   Message text

   – If you select "Send SMS message" as the destination, the message texts you have created will be displayed and you can choose from them.
3. Depending on the selection you have made in "Destination", further drop-down lists will become available with which you can complete your action.
4. If you click the "Apply" button, the entries you have made are adopted.

Result: Your action is adopted and displayed in the list.

Deleting an action

Note

Elements that are being used cannot be deleted

You can only delete an element (signal, text, user, recipient group, event, action) if the element is unused.

If the element is used, e.g. a user in a recipient group or a signal in an event, you cannot delete the element.

1. In the list, select the row with the action you want to delete.
2. Click the "Delete" button.

   A prompt for confirmation is displayed.
3. If you confirm this, the action is deleted and removed from the list.

Change action

1. In the list, select the row with the action you want to modify.
2. Change the action with "Change action" in the lower part of the page.

Result: If you click the "Apply" button, your modified action is adopted and displayed in the list.

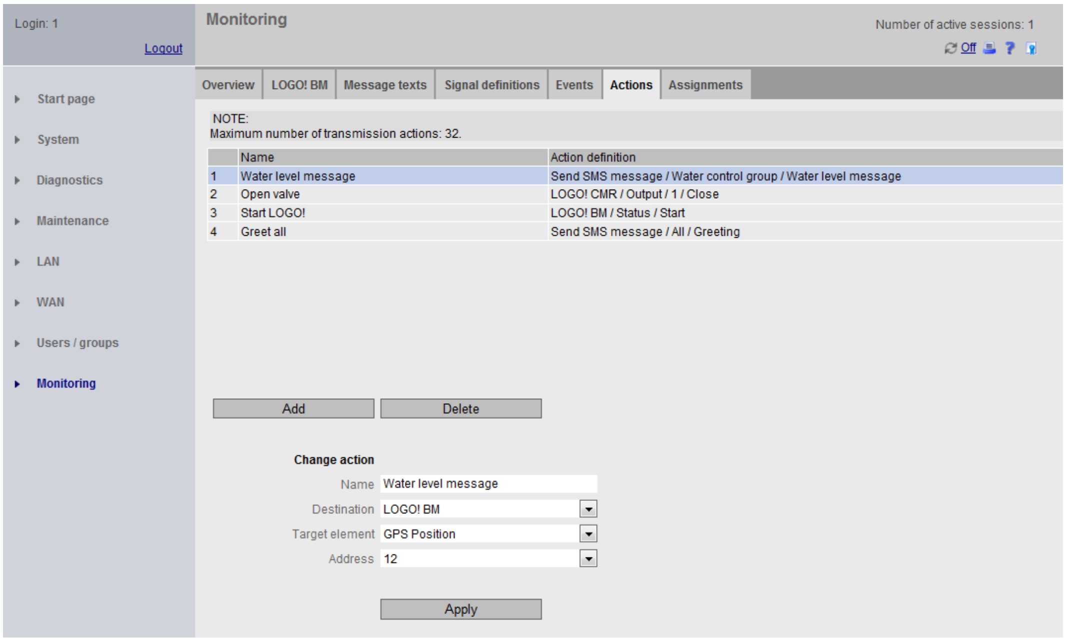
7.4.9.1 Forwarding GPS position data to LOGO! BM

You can select the transfer of the current GPS position data to LOGO! BM as an action. Triggering events can, for example be the expiry of a timer or the status change of a BM or CMR input.

The basic sequence for configuration remains unchanged:

1. Configure LOGO! BM settings
2. Configure signal
3. Configure event
4. Configure action with the destination "LOGO! BM"" and the target element "GPS position"
5. Configure assignment

The start address at which the GPS position data is stored in the VM of the LOGO! BM must be in the range 0 to 112.



NOTE:
Maximum number of transmission actions: 32.

	Name	Action definition
1	Water level message	Send SMS message / Water control group / Water level message
2	Open valve	LOGO! CMR / Output / 1 / Close
3	Start LOGO!	LOGO! BM / Status / Start
4	Greet all	Send SMS message / All / Greeting

Change action

Name: Water level message
Destination: LOGO! BM
Target element: GPS Position
Address: 12

Figure 7-12 Monitoring – "Actions" tab: Forwarding GPS position to LOGO! BM

Data structure of the GPS position data

The block of data transferred to the BM is written byte by byte and has a length of 16 bytes. The data block is structured as follows:

Note

Representation of the letters

Letters are represented as decimal ASCII characters: E.g. "78" for "N" and "83" for "S" and "69" for "E" and "87" for "W".

Note

Evaluate application on the BM: “state“ and “count“

To ensure data consistency, the BM application needs to evaluate the "state" and "count" bytes:

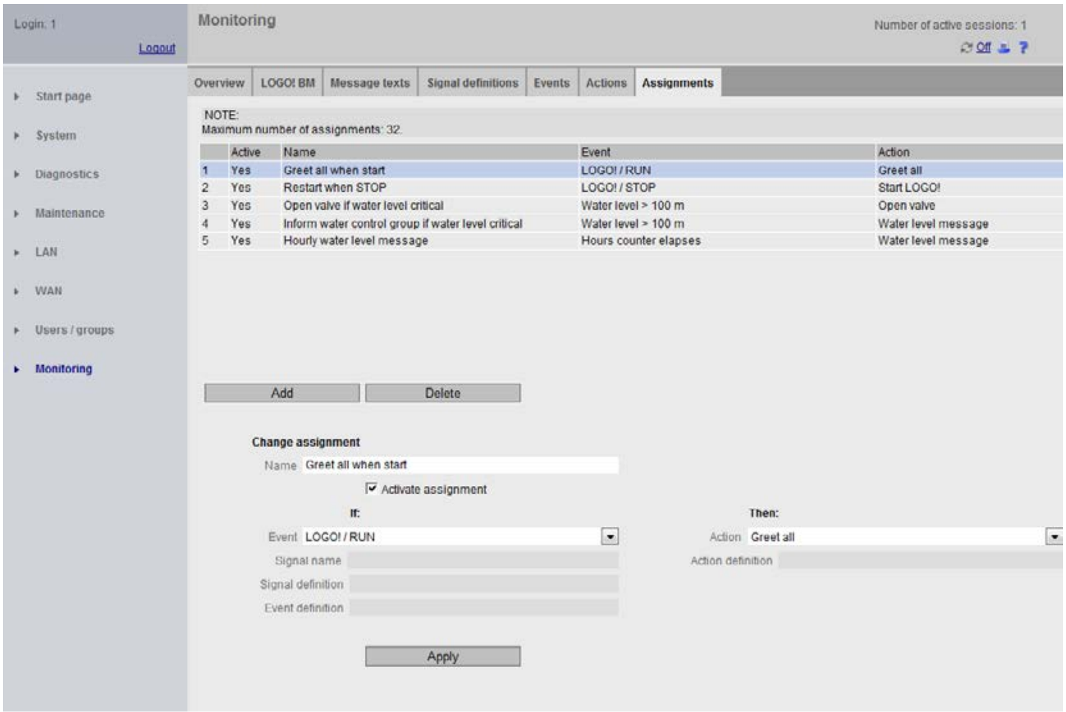
1. If "state" = "invalid": Data is currently being written by the CMR.

   Access is possible only if "state" = "valid" is set.
2. If "state" = "valid": Next, you read the Write Counter and store the value read in.
3. After you have completely read the data structure, check whether or not the Write Counter has changed its value.
   - If the value has not changed, you can continue to use the data structure.
   - If the value has changed, repeat the read cycle and start at "1.".

Byte number	Parameter	Meaning
0	latNS	North / South (N/S)
1	latD	Degrees (0 ... 179)
2	latM	Minutes (0 ... 59)
3	latS	Seconds (0 ... 59)
4	latSF	Seconds Fraction (0 ... 99)
5	lngEW	East / West (E/W)
6	lngD	Degrees (0 ... 179)
7	lngM	Minutes (0 ... 59)
8	lngS	Seconds (0 ... 59)
9	lngSF	Seconds Fraction (0 ... 99)
10 11	alt	Altitude meters (-32767 ... +32767)
12	satNum	Number of satellites in use
13	state	GPS signal state (0,1,2) • 0: invalid “invalid = 0" is set by the CMR during a write procedure. • 1: current position • 2: not current position

Byte number	Parameter	Meaning
14	count	Write Counter: This is incremented each time the GPS data is written by the CMR.
15	res1	reserved for later use

7.4.10 Assignments



NOTE:
Maximum number of assignments: 32.

	Active	Name	Event	Action
1	Yes	Greet all when start	LOGO! / RUN	Greet all
2	Yes	Restart when STOP	LOGO! / STOP	Start LOGO!
3	Yes	Open valve if water level critical	Water level > 100 m	Open valve
4	Yes	Inform water control group if water level critical	Water level > 100 m	Water level message
5	Yes	Hourly water level message	Hours counter elapses	Water level message

Change assignment
Name: Greet all when start
☑ Activate assignment

If:
Event: LOGO! / RUN
Signal name:
Signal definition:
Event definition:

Then:
Action: Greet all
Action definition:

Figure 7-13 Monitoring – "Assignments" tab

You assign an action to an event you have configured.

In the upper part of the page, you will see a list with the assignments configured up to now:

- A maximum of 32 assignments are possible.

  If you have not yet specified an assignment, the list is empty.

In the lower part of the page, under "Change assignment", you will find the area required for specifying an assignment.

If you click the "Apply" button, all the settings you made in the "Assignments" tab are adopted and displayed in the list.

Note

The monitoring of the event only becomes active with the assignment event → action

1. You have configured message texts, signal definitions, events and actions.
2. Assign the event to an action.
3. Select the "Activate assignment" check box.

   With this, you activate the assignment for monitoring.

   With the assignment of an action to an event, the relevant event is only monitored when this assignment is active.

Add new assignment

1. In the lower part of the page, click the "Add" button.
2. Following this, you will see three blocks with input boxes, drop-down lists, check boxes and grayed out text boxes for the configuration.

Name

- Freely selectable symbolic name for this assignment.
- Activate/deactivate the assignment in the "Activate assignment" check box.

If:

Event

- From the drop-down list, select the entry of the event you have created.

  The entry is displayed with the symbolic name you assigned.

  The grayed out boxes "Signal name“, "Signal definition", "Event definition" show you which event with the information shown will be used as the "If“ condition:

  – Signal name

    You have already made the setting in the Signal definitions (Page 93) tab:

    Display of the symbolic name you assigned for a signal definition.

  – Signal definition

    You have already made the setting in the Signal definitions (Page 93) tab:

    Display of the signal (signal source, signal type) that you are using under the symbolic name you selected.

  – Event definition

    You have already made the setting in the Events (Page 95) tab:

    Display of the event that you defined. The name originates from the "Event definition" column.

Then:

Action

- From the drop-down list, select the entry of the action you have created.

  The entry is displayed with the symbolic name you assigned.

  The grayed out "Action definition" allows you to check the definition of the action. The name originates from the "Action definition" column of the action list in the "Actions" tab.

"Apply" button

- If you click the "Apply" button, the entries you have made are adopted.

Result: Your assignment is adopted and displayed in the list.

Deleting an assignment

Note

Elements that are being used cannot be deleted

You can only delete an element (signal, text, user, recipient group, event, action) if the element is unused.

If the element is used, e.g. a user in a recipient group or a signal in an event, you cannot delete the element.

1. In the list, select the row with the assignment you want to delete.
2. Click the "Delete" button.

   A prompt for confirmation is displayed.
3. If you confirm this, the assignment is deleted and removed from the list.

Change assignment

1. In the list, select the row with the assignment you want to modify.
2. Change the assignment with "Change assignment" in the lower part of the page.

Result: If you click the "Apply" button, your modified assignment is adopted and displayed in the list.

7.4.11 Example of a monitoring configuration

The following simple example is intended to illustrate the steps for a monitoring configuration as explained above.

Assumptions

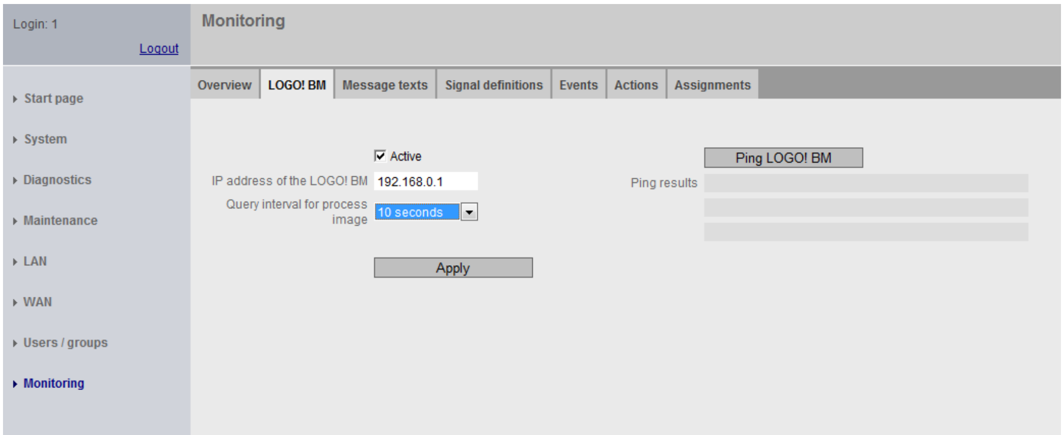
- A water tank holds 100 liters. If the 100 liters is exceeded, and alarm message will be sent to the maintenance staff in the form of an SMS message.
- The maintenance staff consists of two employees, employee "User-1" and employee "User-2" whose phone numbers are known.
- A fill level sensor is connected to input no. 1 of the LOGO! BM:

  If the measurement indicates that the amount of liquid has been exceeded (> 100 liters in the tank), the fill level sensor sets digital input no. 1 to "1".

Procedure

Requirement: The CMR and BM must be connected via an Ethernet cable.

1. In the "LOGO! BM" tab, enter the IP address of the BM in the "IP address of the LOGO! BM" input box.
2. Select the "Active" check box so that the CMR establishes a connection to the BM.



☑ Active

IP address of the LOGO! BM: 192.168.0.1

Query interval for process image: 10 seconds

Figure 7-14 Users / groups - "LOGO! BM" tab Establishing a connection to the BM

3. Following this, enter the two users User-1 and User-2 in the "User" tab with the following properties:

   User-1

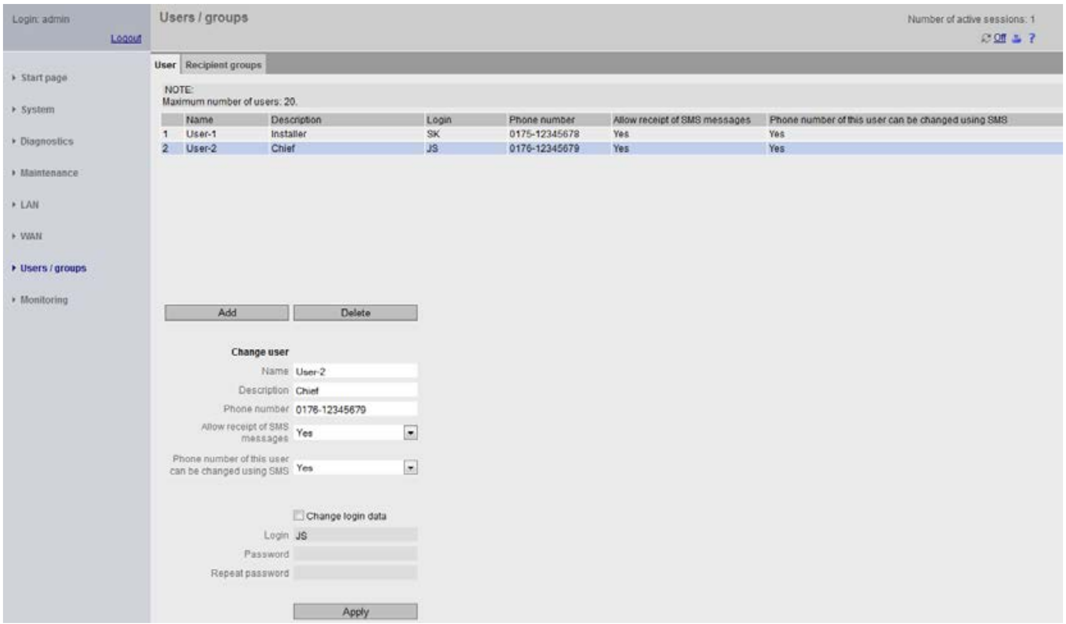
   – User-1 is the fitter with the unique login "SK".

   – The SMS message from User-1 is received from the CMR with the phone number 0175-12345678 and evaluated.

   – The phone number of User-1 can be changed using the SMS command "CHANGEUSER": For example if there is a colleague with a different phone number substituting during the user's vacation.

User-2

- User-2 is the foreman with the unique login "JS".
- The SMS message from User-2 is received from the CMR with the phone number 0175-12345679 and evaluated.
- The phone number of User-2 can also be changed using the SMS command "CHANGEUSER":



NOTE:
Maximum number of users: 20.

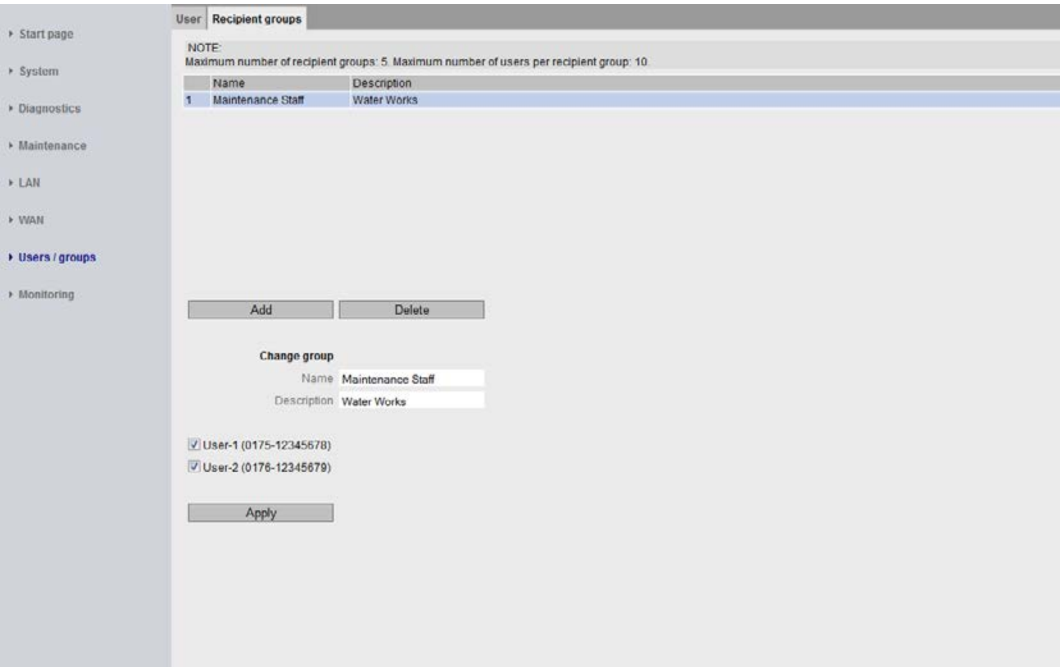
	Name	Description	Login	Phone number	Allow receipt of SMS messages	Phone number of this user can be changed using SMS
1	User-1	Installer	SK	0175-12345678	Yes	Yes
2	User-2	Chief	JS	0176-12345679	Yes	Yes

Change user

Name	User-2
Description	Chief
Phone number	0176-12345679
Allow receipt of SMS messages	Yes
Phone number of this user can be changed using SMS	Yes
	□ Change login data
Login	JS
Password	
Repeat password	

Figure 7-15 Users / groups - "User" tab: Entering users

4. You now need to assign the two employees to a recipient group "Maintenance Staff" in the Water Works ("Description"):



NOTE:
Maximum number of recipient groups: 5. Maximum number of users per recipient group: 10

	Name	Description
1	Maintenance Staff	Water Works

Change group

Name: Maintenance Staff

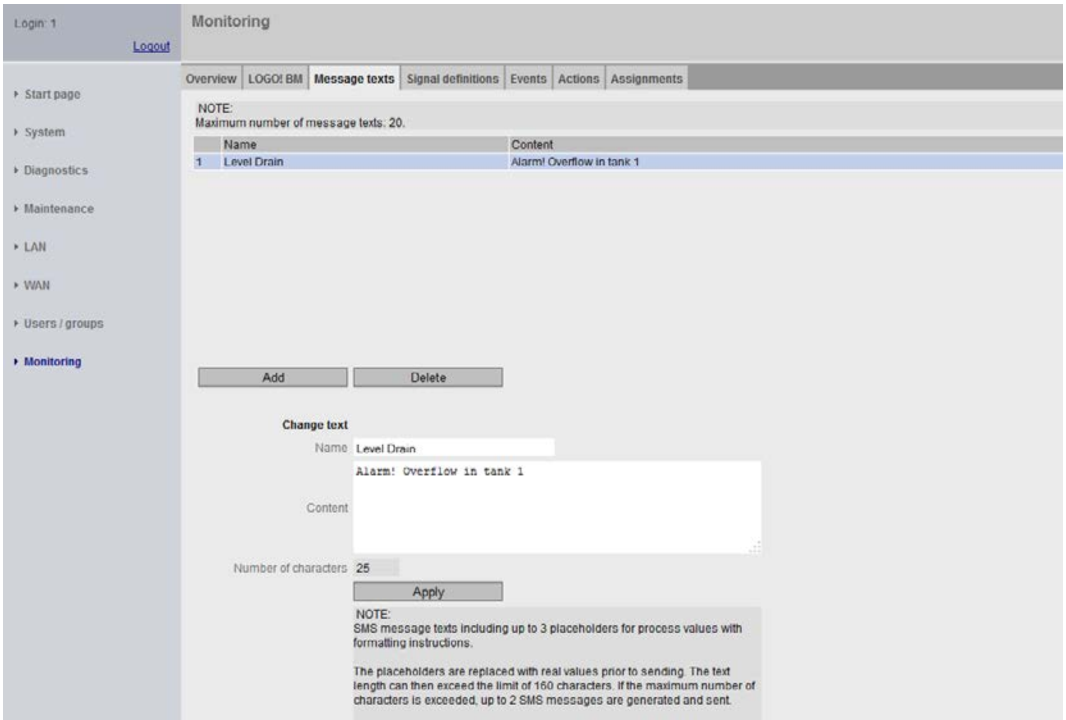
Description: Water Works

☑ User-1 (0175-12345678)

☑ User-2 (0176-12345679)

Figure 7-16 Users / groups - "Recipient groups" tab: Assigning a recipient group

5. In the "Content" input box of the "Message texts" tab, enter the text of the relevant alarm SMS message: "Alarm! Overflow in tank 1".



NOTE:
Maximum number of message texts: 20.

	Name	Content
1	Level Drain	Alarm! Overflow in tank 1

Change text

Name: Level Drain

Content: Alarm! Overflow in tank 1

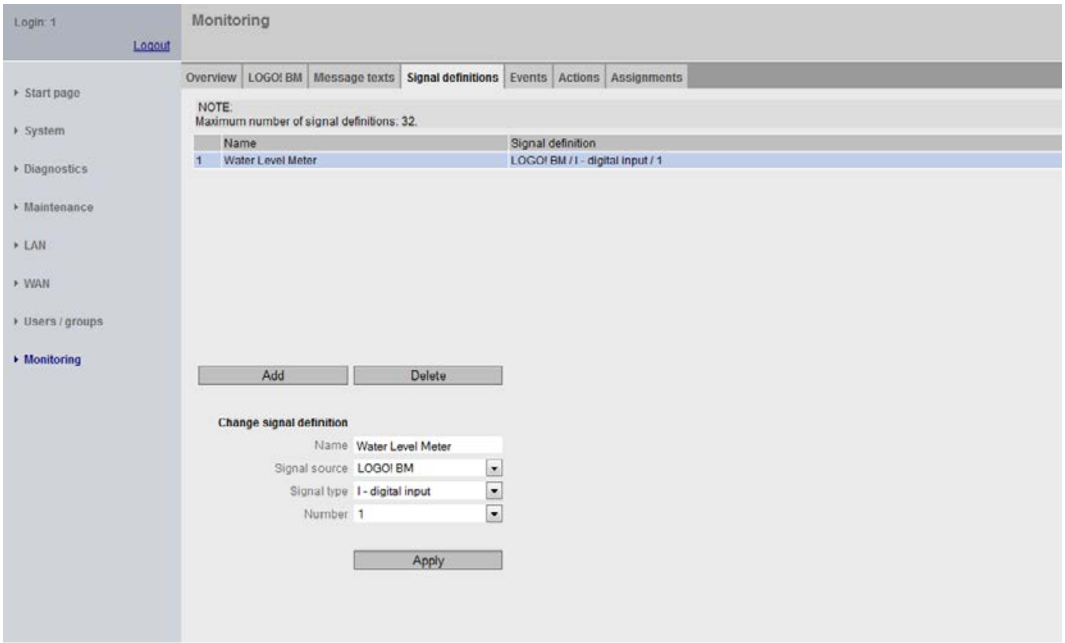
Number of characters: 25

NOTE:
SMS message texts including up to 3 placeholders for process values with formatting instructions.

The placeholders are replaced with real values prior to sending. The text length can then exceed the limit of 160 characters. If the maximum number of characters is exceeded, up to 2 SMS messages are generated and sent.

Figure 7-17 Monitoring – "Message texts" tab: Specifying the text of the alarm SMS message

6. Create the signal definition:



NOTE:
Maximum number of signal definitions: 32.

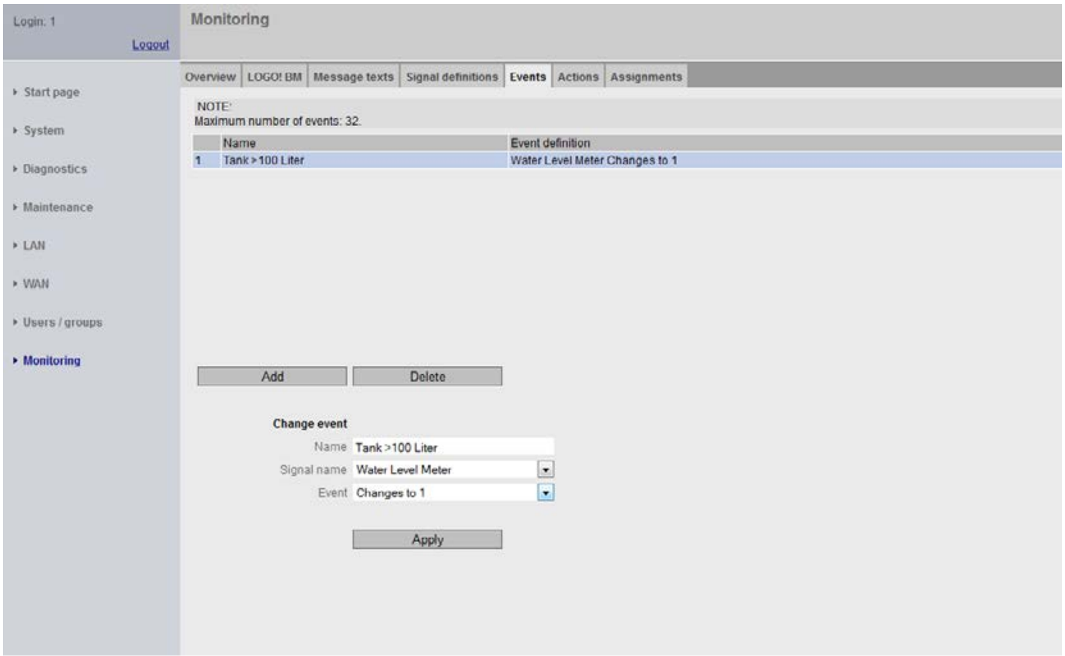
	Name	Signal definition
1	Water Level Meter	LOGO! BM / I - digital input / 1

Change signal definition

Name	Water Level Meter
Signal source	LOGO! BM
Signal type	I - digital input
Number	1

Figure 7-18 Monitoring – "Signal definitions" tab: Creating the signal definition

7. Create the event:



NOTE:
Maximum number of events: 32.

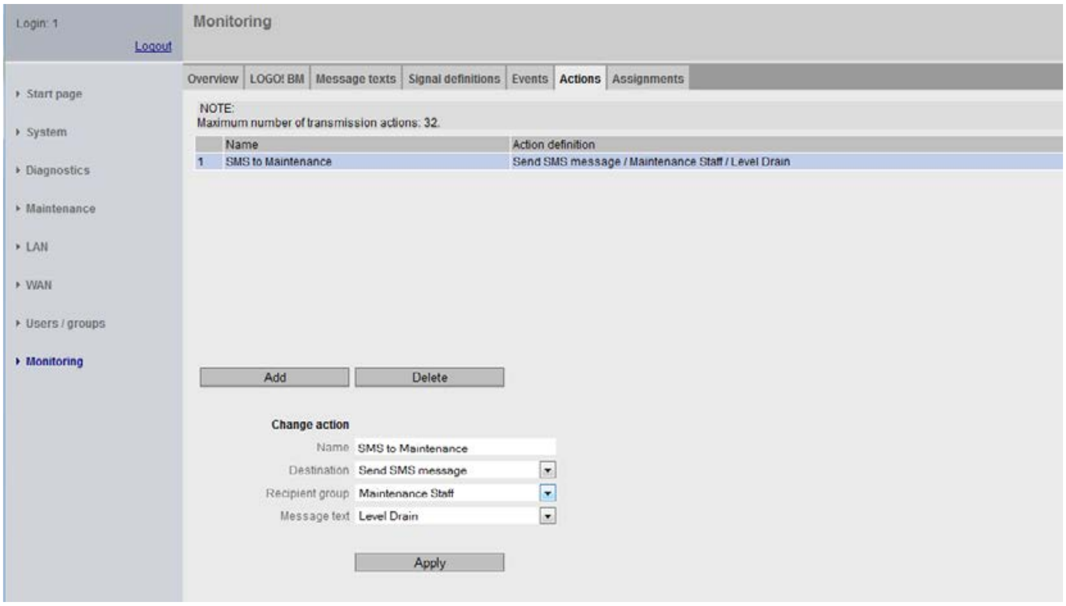
	Name	Event definition
1	Tank >100 Liter	Water Level Meter Changes to 1

Change event

Name	Tank >100 Liter
Signal name	Water Level Meter
Event	Changes to 1

Figure 7-19 Monitoring – "Events" tab: Creating an event

8. Configure an action to suit the created event.
   You can also assign this action to another event later:



NOTE:
Maximum number of transmission actions: 32.

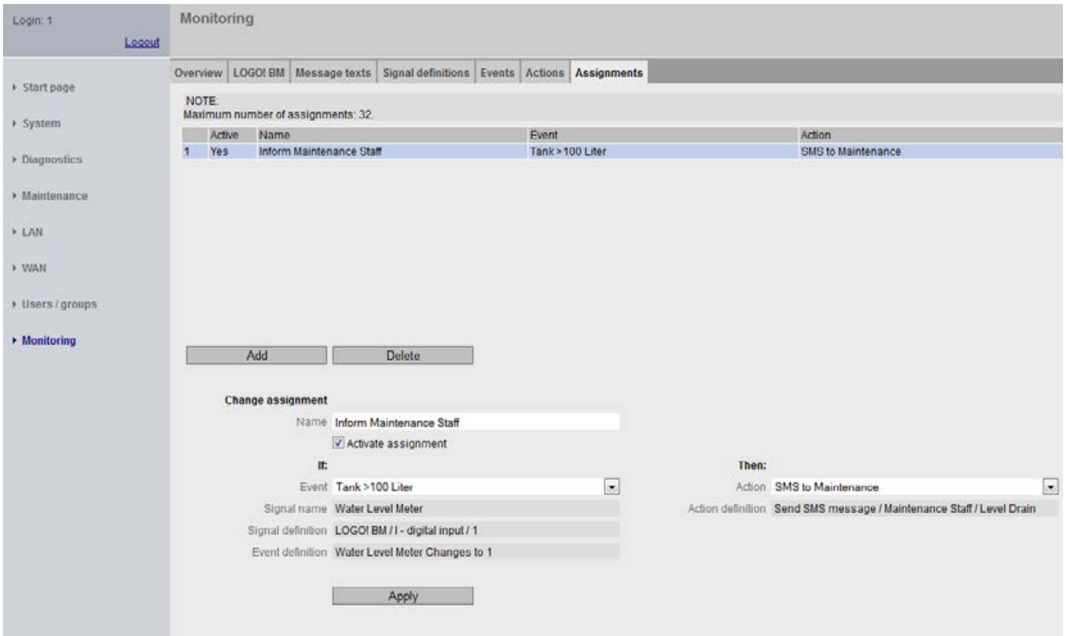
	Name	Action definition
1	SMS to Maintenance	Send SMS message / Maintenance Staff / Level Drain

Change action

Name: SMS to Maintenance
Destination: Send SMS message
Recipient group: Maintenance Staff
Message text: Level Drain

Figure 7-20 Monitoring – "Actions" tab: Configuring the action

9. Finally make the assignment (event → action):



NOTE:
Maximum number of assignments: 32.

	Active	Name	Event	Action
1	Yes	Inform Maintenance Staff	Tank > 100 Liter	SMS to Maintenance

Change assignment

Name: Inform Maintenance Staff
☑ Activate assignment

If:
Event: Tank >100 Liter
Signal name: Water Level Meter
Signal definition: LOGO! BM / I - digital input / 1
Event definition: Water Level Meter Changes to 1

Then:
Action: SMS to Maintenance
Action definition: Send SMS message / Maintenance Staff / Level Drain

Figure 7-21 Monitoring – "Assignments" tab: Specifying the assignment

Result of the configuration

The result of the configuration is as follows:

When the water level sensor I1 of the LOGO! BM changes to "1", the two employees of the maintenance staff "User-1"/fitter and "User2"/foreman are sent an SMS message with the text "Alarm! Overflow in tank 1".

7.5 SMS message structures and examples

7.5.1 Response of the CMR when receiving an SMS message/replying to SMS message

List of all permitted and non-permitted characters

You will find a list of all permitted and non-permitted characters in the section Permitted characters and character lengths (Page 41).

Checking sender numbers

When it receives an SMS message, the CMR first checks whether the sender and the sender's phone number are registered in the CMR and whether the sender has the rights to send an SMS message to the CMR (see settings in the section User (Page 80)):

- Only messages with authorized sender numbers are accepted by the CMR.
- You can also define phone number groups by using the "*" character, refer to the section User (Page 80).

Checking SMS text for keywords and password

Note

- The password must be separated from the keyword with a ";".
- Read access must not include a password.
- Write access must include a password.

Requirements:

- The sender number of the SMS message was checked against the configured phone numbers of the authorized users.
- All messages originating from unauthorized phone numbers were discarded.

The following conventions apply to queries and write access:

- The keywords must always be in uppercase letters.
- With write access, the "?" character is omitted after the keyword. You need to start with a password:
  - Write access: <password>;<key word>=<parameter>
  - Read access:<key word>?<possibly Parameter>

The CMR checks the text of the SMS message for keywords or with write SMS commands first for the password specified in the configuration:

- If the SMS message does not contain any keywords or no or an incorrect password an entry is made in the diagnostics buffer.
  - If the SMS message comes from an authorized phone number, a reply SMS message is always sent.
  - Exception: If the SMS message comes from an unauthorized phone number or “Allow receipt of SMS messages" is deactivated, the SMS message is discarded.

Password configuration for SMS messages with write access

Note

No ";" in the password

- The password must not contain ";".
- The password must be separated from the keyword with a ";".

All SMS messages with write access must be preceded by a password:

- You configure this password using the WBM.

The password counts as the authorization of the user and prevents manipulation of LOGO! BM or LOGO! CMR values.

Replying to SMS messages

SMS messages from authorized users are replied to by the CMR. With write access, this reply consists of a positive or negative acknowledgement of the write procedure.

Note

Preventing an SMS message loop with linked CMRs

To avoid several CMRs connected by mobile wireless forming an SMS loop, acknowledgement frames are received but are not replied to.

The number of SMS jobs/time is limited

The CMR stores a limited number of SMS send jobs in a job queue.

Sending an SMS message may take several seconds due to the delayed transfer in the mobile wireless network.

To make sure that all SMS messages are sent within the required time:

- Adapt the length of the interval for large amounts of data to be sent cyclically, e.g. PI-SMS messages (monitor SMS) accordingly.
- Make sure that there is enough time between different actions sending PI-SMS messages.

If, for example, a PI-SMS message requested using SMS was sent incompletely, repeat your request SMS message.

SMS error messages

You will find a list of all possible error messages in SMS error messages (Page 111).

7.5.2 SMS error messages

Message	Possible causes
OK	• The SMS command was executed successfully.
Invalid Command	• SMS keyword could not be recognized. • Check the uppercase/lower case characters and syntax.
Invalid Parameter	• Transfer parameter not correct; password not correct.
Not successful	• Values could not be set or read.
Try again	• The CMR is currently being reconfigured. The request cannot be processed.
No connection to LOGO! BM	• LOGO! BM not activated or wrong IP address set. • Cable between LOGO! BM and LOGO! CMR disconnected.
No GPS signal	• GPS not configured. • GPS signal cannot be received because there is no line of sight to the GPS satellite.

7.5.3 Syntax of all SMS commands

Syntax of the SMS commands and possible responses

What information would I like to have?	Example
Read diagnostics data from the CMR	DIAG?
Read GPS position from the CMR	GPSPOSITION?
Read process image (PI)	MONITOR?
Read status of the BM	STATUS?
Read current value	LOGO?VM125,WORD

What do I want to influence?	Example
Set the status of the BM	Password;STATUS=RUN
Write current value	Password;LOGO=VM125,1,WORD
Set digital output of the CMR	Password;OUTPUT=O1,1
Change phone number of a user	Password;CHANGEUSER="Joe","01721234567"
Configure address of an NTP server	Password;NTPSERVER="217.13.75.19"
Query mobile wireless provider using a service code	Password;SERVICECODE="*100#"

7.5.4 SMS commands

The following tables describe all the possible SMS structures of the SMS commands and these are illustrated with examples.

Note

Only 1 SMS command is possible per SMS message to the CMR.

Note

Use of prepaid SIM cards

If you use a prepaid SIM card, you can query the current credit using the appropriate service code of your provider.

If your credit has been used up, the CMR does not send an automatic warning.

Read diagnostics data from the CMR	
Function	Requesting diagnostics data from the CMR
Access	Reading, no password necessary
Structure and keyword	**DIAG?**
Return values	Diagnostics data or error message: SMS error messages (Page 111) Structure of diagnostics data:Diagnostics SMS message (Page 120)
Example	Send SMS message: DIAG? Reply SMS message: Diagnostics SMS message (Page 120)

Read GPS position from the CMR			
Function	Request current GPS position. The current GPS position is read out and returned to the sender.		
Access	Reading, no password necessary		
Structure and keyword	**GPSPOSITION?**		
Return values	GPS coordinates or error message: SMS error messages (Page 111) Structure of the SMS message: GPS position: ddd:mm:ss.hs N/S ddd:mm:ss.hs W/E Alt mmmm		
Example	Send SMS message: GPSPOSITION? Reply SMS message: GPS position: 49:0:50.4 N 8:24:15.48 E Alt 0350		
Explanation of reading the transfer data	ddd	degree	Degree
	mm	minutes	Minutes
	ss.hs	seconds	Seconds
	N/S	North/South	Degree of longitude
	W/E	West/East	Degree of latitude
	Alt mmmm	Altitude	Height above sea level in meters

Read process image	
Function	Reading out the BM process image and the status of the two inputs and outputs of the CMR.
Access	Reading, no password necessary
Structure and keyword	**MONITOR?**
Return values	Process image or error message: SMS error messages (Page 111) Structure of the process image: Reply SMS message to the "MONITOR?" command (Page 116)
Example	Send SMS message: MONITOR? Reply SMS message: Reply SMS message to the "MONITOR?" command (Page 116)

Read BM status	
Function	Query the BM status
Access	Reading, no password necessary
Structure and keyword	**STATUS?**
Return values	RUN, STOP or error message: SMS error messages (Page 111)
Example	Send SMS message: STATUS? Reply SMS message: STATUS:RUN

Set BM status	
Function	Setting the BM status to RUN or STOP
Access	Writing, password required
Structure and keyword	**<password>;STATUS=<LOGO status>**
Return values	OK or error message: SMS error messages (Page 111)
Example	Send SMS message: Password;STATUS=RUN Reply SMS message: STATUS=RUN:OK

Configure address of an NTP server	
Function	Configuring address of an NTP server. You can configure the address of an NTP server only if NTP was selected as the time-of-day synchronization method. <address> can either be the IP address in the format 123.123.123.123 or the name of the NTP server in URL format, e.g. http://www.ntpservername.de.
Access	Writing, password required
Structure and keyword	**<password>;NTPSERVER="<address>"**

Configure address of an NTP server	
Return values	OK or error message: SMS error messages (Page 111)
Example	1. Example: Send SMS message: Password;NTPSERVER="http://www.ntpservername.de" Reply SMS message: NTPSERVER=http://www.ntpservername.de:OK 2. Example: Send SMS message: Password;NTPSERVER="217.13.75.19" Reply SMS message: NTPSERVER=217.13.75.19:OK

Note

Direct access to BM variables memory

For security reasons the address in theVM memory can only be read or written using SMS if the address was created earlier as a signal using the WBM.

The two following commands access the variables memory of the BM directly:

- Set/read value in the BM variables memory.

When using these commands, remember the points made in the Overview (Page 75).

Reading the current value from the BM variables memory: Read "current values"	
Function	Reading the current value from the BM variables memory. You obtain the address from the BM variables memory. The value <data type> is BYTE, WORD or DWORD. Only the first 128 bytes of the BM variables memory can be read and written to. • BYTE: 0 ... 127 • WORD: 0 ... 126 • DWORD: 0 ... 124 You can read any value from the BM variables memory. If you know the LOGO! control program precisely, this can, for example, be useful for diagnostics purposes.
Access	Reading, no password necessary
Structure and keyword	**LOGO?VM<address>,<data type>**
Return values	Current value or error message: SMS error messages (Page 111) Structure of the returned value: VM>address>:<value>(<data type>) Output: Decimal output of the returned value
Example	Send SMS message: LOGO?VM125,WORD Reply SMS message: VM125:1(WORD)

Setting value in the BM variables memory: Write "current values"	
Function	Setting values of a component in the BM variables memory, e.g. inputs, outputs, flags. You obtain the address of the component from the BM variables memory. Only the first 128 bytes of the BM variables memory can be read and written to. • BYTE: 0 ... 127 • WORD: 0 ... 126 • DWORD: 0 ... 124 By setting a value in the BM variables memory, you can change the running of a LOGO! control program. Only use this command if you have precise knowledge of the control program! All values are processed by the CMR as signed values.
Access	Writing, password required
Structure and keyword	**<password>;LOGO=VM<address>,<value>,<data type>**
Return values	Confirmation or error message: SMS error messages (Page 111)
Example	Send SMS message: Password;LOGO=VM125,1,WORD Reply SMS message: LOGO=VM125,1,WORD: OK

Set digital output of the CMR	
Function	Setting the digital output 1 or 2 of the CMR to a value: 1 or 0.
Access	Writing, password required
Structure and keyword	**<password>;OUTPUT=O<1/2>,<1/0>**
Return values	OK or error message
Example	Send SMS message: Password;OUTPUT=O1,1 Reply SMS message: OUTPUT=O1,1:OK

Changing the phone number of a user	
Function	Changing the phone number of a user uniquely specified by the <login>. For the selected user, the corresponding release must be entered in the WBM under Users / groups in the User tabHotspot-Text (Page 80).
Access	Writing, password required, right must be configured in the WBM
Structure and keyword	**<password>;CHANGEUSER="login","phone number"**
Return values	OK or error message
Example	Send SMS message: Password;CHANGEUSER="Joe","01751234567" Reply SMS message: CHANGEUSER=Joe01751234567:OK

Querying the mobile wireless provider about the service code	
Function	Querying a service code with the mobile wireless provider, e.g. "*100#". The text transferred by the mobile wireless provider is returned unchanged as the reply in an SMS message. If you use a prepaid SIM card, and want to query the current credit: The service code can be used to query your credit. You cannot, however, use all possible service codes for queries.
Access	Writing, password required
Structure and keyword	**<password>;SERVICECODE="code"**
Return values	Original reply of the mobile wireless provider or error message
Example	Send SMS message: Password;SERVICECODE="*100#" Reply SMS message: *100# Original text of the mobile wireless provider or error message

7.5.5 Reply SMS message to the "MONITOR?" command

Process image

The process image shows the current statuses and values of the CMR and the BM with its expansion modules.

The number of I/O elements actually in the system depends on the expansion modules being used.

CMR		**Value blocks**
Digital inputs	Inputs	I1, I2
Digital outputs	Outputs	Q1, Q2

BM		**Value blocks**
Program status	Status program	PS
Communication status	Connection status BM-CMR	CS
Digital inputs	Inputs	I1 ... I24
Digital outputs	Outputs	Q1 ... Q20
Digital flags		M1 ... M64
Shift register inputs		S1.1 ... S4.8
Arrow keys		▶ ◀ ▼ ▲
Function keys		F1 ... F4
Analog inputs		AI1 ... AI8
Analog outputs		AQ1 ... AQ8
Analog flags		AM1 ... AM64

Structure of the reply SMS message of the process image (PI-SMS)

Note

A maximum of 7 SMS messages

The reply SMS includes a maximum total of 7 SMS messages. The number of SMS messages depends on the monitored signals.

Meaning of "*" in the tables

"*" correspond to spaces in the structure of the reply SMS message.

Representation of digital values, shift registers

- One digit with the logical state (0 or 1).
- Eight values per line counting from right to left.

Representation of analog values

- Analog values according to the internal representation (max. 6 characters) of the analog values of the LOGO! BM.
- The representation of the values is 6 digits with leading zeros. One analog value is output per line.

Representation of unused values and value blocks

- Unused values are represented by "x".
- If there are no used values in the remaining lines of a value block, these lines are not shown.
  Refer to "Example of a reply SMS message" below in the value block "BM I:".
- An unused values block is not displayed nor is the name.

Representation of control keys

- 4 values per line

The reply SMS message of the CMR to a process image query has the following prepared structure:

Table 7- 2 Reply SMS message: Structure

CMR I: Name of the values block for CMR inputs	
******xx	CMR input 1 and 2, values from right (I1) to left (I2)
CMR Q: Name of the values block for CMR outputs	
******xx	CMR output 1 and 2, values from right (Q1) to left (Q2)
BM PS/CS: Program and communications status of the BM	

******11	PS CS
	PS=1 BM in RUN
	PS=0 BM in STOP
	CS=1 connection to CMR
	CS=0 no connection to CMR

BM I: Name of the value block for LOGO! BM - digital inputs	
xxxxxxxx	Inputs 8 ... 1, values from right (I1) to left (I8)
xxxxxxxx	Inputs 16 ... 9
xxxxxxxx	Inputs 24 ... 17
BM Q: Name of the value block for LOGO! BM - digital outputs	
xxxxxxxx	Outputs 8 ... 1, values from right (Q1) to left (Q8)
xxxxxxxx	Outputs 16 ... 9
****xxxx	Outputs 20 ... 17
BM M: Name of the value block for LOGO! BM - digital flags	
xxxxxxxx	Flags 8 ... 1, values from right (M1) to left (M8)
xxxxxxxx	Flags 16 ... 9
xxxxxxxx	Flags 24 ... 17
xxxxxxxx	Flags 32 ... 25
xxxxxxxx	Flags 40 ... 33
xxxxxxxx	Flags 48 ... 41
xxxxxxxx	Flags 56 ... 49
xxxxxxxx	Flags 64 ... 57
BM S: Name of the value block for LOGO! BM - shift register	
xxxxxxxx	Shift register inputs S1.8 ... S1.1
xxxxxxxx	Shift register inputs S2.8 ... S2.1
xxxxxxxx	Shift register inputs S3.8 ... S3.1
xxxxxxxx	Shift register inputs S4.8 ... S4.1
BM C: Name of the value block for LOGO! BM - arrow keys	
xxxx	Keys 4 ... 1 in the symbols ▶ ◀ ▼ ▲
BM F: Name of the value block for LOGO! BM - function keys	
xxxx	Function keys F4 ... F1, F1 right justified
BM AI: Name of the value block for LOGO! BM - analog inputs	
xxxxxx	Analog input 1
xxxxxx	Analog input 2
xxxxxx	Analog input 3
xxxxxx	Analog input 4

xxxxxx	Analog input 5
xxxxxx	Analog input 6
xxxxxx	Analog input 7
xxxxxx	Analog input 8
BM AQ: Name of the value block for LOGO! BM - analog outputs	
xxxxxx	Analog output 1
xxxxxx	...
xxxxxx	...
xxxxxx	Analog output 8
BM AM: Name of the value block for LOGO! BM - analog flags	
xxxxxx	Analog flag 1
xxxxxx	...
xxxxxx	...
xxxxxx	Analog flag 64

Example of a reply SMS message

- In the CMR, input 1 and output 2 are used.
- In the BM control program I1, I2 and I6, as well as Q1, Q3,Q9 and Q17 and analog input 2 are monitored.

Assumption

- BM in RUN, CMR connection to BM
- CMR: I1=1, Q2=1
- BM: I1 = 0, I2 = 1, I6 = 0, Q1 = 1, Q3 = 0, Q9 = 1, Q17 = 0, AI2 = 3.5 V

Table 7- 3 Reply SMS message

CMR I:	
******x1	* = 6 leading spaces
CMR Q:	
******1x	* = 6 leading spaces
BM PS/CS:	
******11	BM in RUN, CMR connected to BM
BM I:	
xx0xxx10	Input 9 ... 24 in the values block not used and not displayed
BM Q:	
xxxxx0x1	
xxxxxxx1	
****xxx0	* = 4 leading spaces
BM AI:	Values blocks BM M, BM S, BM C and BM F not used and not displayed
xxxxxx	
00350	No further values in this and the following values blocks, therefore not shown in the SMS message.

Example with LOGO! BM

- The input voltage range of the analog input is 0 to 10 V:

  This range is represented by values in 1 000 steps.
- A voltage at the analog input of 3.5 V has a value of 350 [00350]:

  Input voltage in V * 100 = internal value of the LOGO!
- The representation of the values is 6 digits with leading zeros. One analog value is output per line.
- Unused values are represented by x.

  Values that cannot be read out are represented by "e".
- Remaining lines in a values block are omitted completely if there are no further used values in these lines.

7.5.6 Diagnostics SMS message

SMS command “DIAG?“

The reply SMS to a diagnostics request (SMS command "DIAG?") returns information with the following structure:

Information	SMS structure
Module name of the CMR module	From: DEVICE-Name
Type and firmware version	<CMR name> <firmware version>
Mobile wireless network status	not registered/registered/not configured/searching network/denied/unknown/roaming/invalid
Connected for (only with registered/roaming)	Attached for (ddd:hh:mm:ss) <ddd>:<hh>:<mm>:<ss>
Data service status	not registered/registered/not configured/searching network/denied/unknown/roaming/invalid
Connected for	Attached for (ddd:hh:mm:ss) <ddd>:<hh>:<mm>:<ss>
Name of the network/provider:	Network: <netname>
IP address	IP: xxx.xxx.xxx.xxx or if no IP address exists: IP: -
Signal strength	Signal Quality: invalid/good/medium/weak/no signal
Signal field strength (CSQ /dBm)	(CSQ:xx / -xxdBm)

SMS command “DIAG? Response“

If the information cannot be sent with an SMS message, there is a 2nd SMS that starts with "DIAG? Response".

Such a reply SMS message can appear as follows:

Example - the reply includes 2 SMS messages:

1. SMS

- From: DEVICE-Name
- LOGO! CMR2020 V1.0
- GSM: registered
- Attached for (ddd:hh:mm:ss): 000:00:03:36

2. SMS

- DIAG? Response
- GPRS: registered
- Attached for (ddd:hh:mm:ss): 000:00:03:36
- Network: Vodafone.de
- IP: 77.25.26.11
- Signal Quality: good (CSQ:29/-55dBm)

7.6 Disruptions and their possible causes

Disruption	Meaning	Solution
Error LED lit red	• No connection to the BM • Wrong PIN • No SIM card but the mobile wireless interface is activated To obtain information on other possible causes of error, it is best to check the log events in the diagnostics buffer.	• Check the connections/run the PING test • Unlocking the SIM card • Inserting the SIM card
Error LED flashes red	• Duplicate IP address	• Correct the IP address
No LED display	• Power supply too weak • The CMR is in the shut down status	• Correct the power supply according to the Technical specifications (Page 125)
No positioning possible	• Bad GPS reception • Antenna not or not correctly plugged in	• GPS reception is normally only possible outdoors: GPS reception is not possible in enclosed spaces. • Check the connector
Bad or no time-of-day synchronization using NTP	• Bad mobile wireless reception • Wrong configuration in the WBM • Mobile wireless interface deactivated • Incorrect NTP server name or incorrect IP address	• Correct the alignment of the antenna • Activate the mobile wireless interface in the WBM • Check the configuration of the mobile data connection in the WBM

Disruption	Meaning	Solution
No SMS reception	• SMS reception deactivated • Bad mobile wireless reception • User not registered or authorized	• Enable SMS reception in the WBM • Check user rights in the WBM and if necessary correct • Check the antenna position of the mobile wireless antenna
No dial-in to the mobile wireless network	• PIN entered incorrectly three times • Mobile wireless interface deactivated in the WBM	• See section Insert the SIM card and enter the PIN (Page 29), unlocking the SIM card • Activating the mobile wireless interface in the WBM
Monitoring not working	• Expected SMS messages configured in the WBM are not received	Check in the WBM: • Are the assignments active? • Are the inputs/outputs connected correctly? • Only if objects of the BM are monitored: Is the BM connected?
SMS message received in which there are placeholders between 2 exclamation points	• A signal name specified in the WBM does not exist or has been written incorrectly. The incorrect or non-existent signal name is then shown in the message texts as follows: [CMR_I1] becomes !CMR_I1!	• Correct placeholders in theWBM

Dimension drawings

8

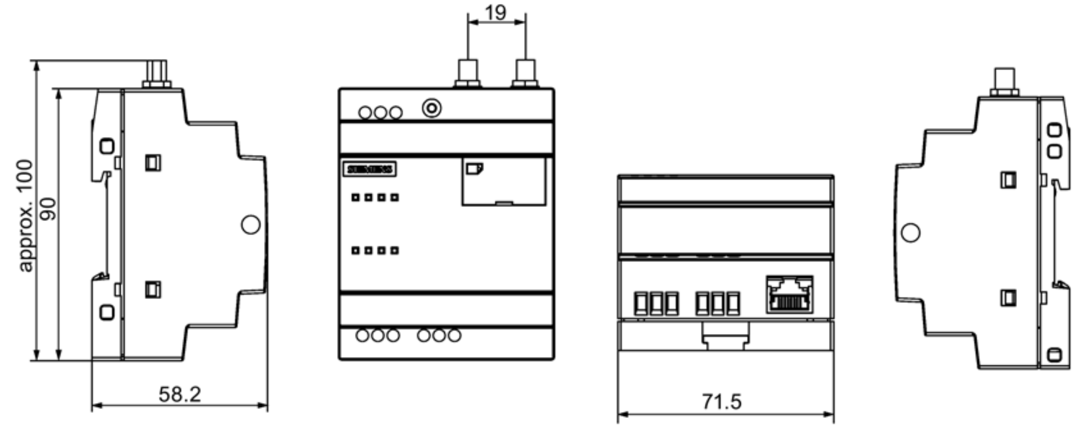


Figure 8-1 All dimensions in millimeters

Technical specifications 9

Table 9- 1 Technical specifications of LOGO! CMR2020 and LOGO! CMR2040

Technical specifications	
Article numbers	
LOGO! CMR2020	6GK7 142-7BX00-0AX0
LOGO! CMR2040	6GK7 142-7EX00-0AX0
Attachment to Industrial Ethernet	
Interface X1P1 for local applications	
• Quantity	1
• Design	RJ-45 jack
• Properties	10/100-Base-T, Ethernet IEEE 802, autocrossover, autonegotiation
• Transmission speed	10 / 100 Mbps
Permitted cable lengths (Ethernet)	**(Alternative combinations per length range) ***
0 ... 55 m	• Max. 55 m IE TP Torsion Cable with IE FC RJ45 Plug 180 • Max. 45 m IE TP Torsion Cable with IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet
0 ... 85 m	• Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable with IE FC RJ45 Plug 180 • Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord via IE FC RJ45 Outlet
0 ... 100 m	• Max. 100 m IE FC TP Standard Cable with IE FC RJ45 Plug 180 • Max. 90 m IE FC TP Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet
Electrical data	
Power supply	
• Power supply	12 to 24 VDC nominal
• Tolerance	-15 ... +20 %
• Design	3-pin terminal strip, not floating
Current consumption	
• At 12 V	Max.. 850 mA (including 2 x 300 mA for digital outputs)

Technical specifications	
• At 24 V	Max.. 725 mA (including 2 x 300 mA for digital outputs)
• I_{burst}	1050 mA (including 2 x 300 mA for digital outputs)
Effective power loss	Maximum 3 W
Digital inputs (I1, I2)	
• Quantity	2
• Design	3-pin terminal strip, not floating
• Permitted voltage range	12 to 24 V (nominal)
• Voltage in status ON	> 8.5 V
• Voltage in status OFF	< 5 V
• Current consumption	I = 5.5 mA (maximum)
Digital outputs (Q1, Q2)	
• Quantity	2
• Design	3-pin terminal strip, transistor, not floating
• Output voltage	Supply voltage
• Load capability	Max. 0.3 A
Wireless interface (mobile wireless)	
Antenna connector	
• Quantity	1
• Design	SMA socket
• Nominal impedance	50 Ω
Frequency bands	
• LTE (LOGO! CMR2040 only)	Band III (1800 MHz), band VII (2600 MHz), band XX (800 MHz)
• UMTS (LOGO! CMR2040 only)	Band I (2100 MHz), band VIII (900 MHz)
• GSM LOGO! CMR2020 and LOGO! CMR2040.	850 MHz/900 MHz, DCS 1800 MHz, PCS 1900 MHz
HSPA+	
• Transmission speeds (maximum)	• Downlink: 42 Mbps • Uplink: 5.76 Mbps
LTE	
• Transmission speeds (maximum)	• Downlink: 100 Mbps • Uplink: 50 Mbps
EDGE	
• Properties	• Multislot class 10, end device class B • Coding scheme: 1 ... 9
• Transmission speeds (maximum)	• Downlink: 236.8 kbps • Uplink: 236.8 kbps

Technical specifications	
GPRS	
• Properties	• Multislot class 10, end device class B • Coding scheme 1 ... 4
• Transmission speeds (maximum)	LOGO! CMR2020: • Downlink: 80 kbps • Uplink: 40 kbps LOGO! CMR2040: • Downlink: 85.6 kbps • Uplink: 85.6 kbps
Wireless interface (GPS)	
GPS antenna connector	
• Quantity	1
• Design	SMA socket
• Nominal impedance	50 Ω
• Power supply	• 3.8 V (nominal) • At 5 mA: 3.575 V • At 10 mA: 3.35 V • At 15 mA: 3.125 V
• Current consumption	Max. 15 mA
Design of the GPS interface	32-channel GPS standard
Frequency bands	L1 (GPS) L1, FDMA (Glonass) E1 (Galileo)
Data format	RTCM / NMEA
Transmit power • Acquisition • Navigation • Tracking	 • - 146 dBm • - 160 dBm • - 162 dBm
Accuracy • Position (CEP50) • Speed • Heading (heading)	 • 1.5 m • < 0.05 m/s • < 0,01 °
Start time at first acquisition (- 130 dBm) • Cold restart • Warm restart	 • < 35 s • 1 s

Technical specifications	
Permitted ambient conditions	
Ambient temperature • During operation • During storage	 • -20 °C to +70 °C • -40 °C ... +85 °C
Relative humidity at 25 °C	0 to 95 %, non-condensing
Design, dimensions and weight	
Design	Compact design, for DIN rail mounting
Degree of protection	IP20
Weight	160 g
Dimensions (W x H x D)	71.5 x 90 x 58.2 mm (without antenna sockets)
Materials	Plastic

* For details, refer to the IK PI catalog, cabling technology

You will find additional functions and performance data in the section Properties and functions (Page 11).

Approvals 10

Approvals issued

Note

Issued approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

EU declaration of conformity

CE

The product meets the requirements and safety objectives of the following EC directives and it complies with the harmonized European standards (EN) for programmable logic controllers which are published in the official documentation of the European Union.

- **94/9/EC (ATEX explosion protection directive)**

  Directive of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres

- **1999/5/EC (R&TTE)**

  Directive of the European Parliament and of the Council of 9 March 1999 on Radio Equipment and Telecommunications Terminal Equipment and the mutual recognition of their conformity

- **2011/65/EU (RoHS)**

  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment

The EC Declaration of Conformity is available for all responsible authorities at:

Siemens Aktiengesellschaft
Process Industries and Drives
Process Automation
DE-76181 Karlsruhe
Germany

You will find the EC Declaration of Conformity for these products on the Internet at the following address:

91689511 (http://support.automation.siemens.com/WW/view/en/91689511) → "Entry List" tab
Filter settings:
Entry type: "Certificates"
Certificate Type: “Declaration of conformity”
serach term(s):<name of the module>

IECEx

The product meet the requirements of explosion protection according to IECEx.

IECEx classification: Ex nA IIC T4 Gc

The product meets the requirements of the following standards:

- EN 60079-0

  Hazardous areas - Part 0: Equipment - General requirements
- EN 60079-15

  Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

ATEX

The product meets the requirements of the EC directive 94/9/EC "Equipment and Protective Devices for Use in Potentially Explosive Atmospheres".

Applied standards:

- EN 60079-0

  Hazardous areas - Part 0: Equipment - General requirements
- EN 60079-15

  Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

ATEX approval: II 3 G Ex nA II T4 Gc

Test number: KEMA 07 ATEX 0145 X

Over and above this, the following conditions must be met for the safe deployment of the product according to the section Notices on use in hazardous areas according to ATEX (Page 23).

You should also note the information in the document "Use of subassemblies/modules in a Zone 2 Hazardous Area" that you will find on the supplied data medium with the documentation.

For information on the EU declaration of conformity see above.

R&TTE

The CP meets the requirements of the EC directive 1999/5/EC "Radio equipment and telecommunications terminal equipment" according to the requirements of article 3 (1) a, 3 (1) b and 3 (2).

Article 3 (1) a - Health and Safety

Harmonized standards:

- EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

  Information technology equipment - Safety - Part 1: General requirements
- EN 62479:2010

  Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz ... 300 GHz)
- EN 62311:2008

  Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz ... 300 GHz)

Art. 3 (1) b - EMC

Harmonized standards:

- ETSI EN 301 489-1 V1.9.2

  Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility for radio equipment and services - Part 1: Common technical requirements
- ETSI EN 301 489-3 V1.6.1

  Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility (EMC) for radio equipment and services - Part 3 : Specific conditions for wireless devices with a low range (SRD) for use on frequencies between 9 kHz and 246 GHz
- ETSI EN 301 489-7 V1.3.1

  Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility for radio equipment and services - Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)
- ETSI EN 301 489-24 V1.5.1

  Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility for radio equipment and services - Part 24: Specific conditions for mobile and portable IMT-2000 CDMA Direct Spread (UTRA) radio and ancillary equipment
- EN 61000-6-1:2007

  Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity for residential, commercial and light-industrial environments
- EN 61000-6-2:2005+AC:2005

  Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
- EN 61000-6-3:2007+A1:2011+AC:2012

  Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments

- EN 61000-6-4:2007+A1:2011

  Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
- EN 55022:2010+AC:2011 Class A / B

  Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement
- EN 55024:2010

  Information technology equipment - Immunity characteristics - Limits and methods of measurement

Article 3 (2) Measures of efficient use of the frequency spectrum

Harmonized standards:

- ETSI EN 300 440-2 V1.4.1

  Electromagnetic compatibility and radio spectrum matters (ERM) - short range devices - radio equipment to be used in the 1 GHz to 40 GHz frequency range. Part 2: Harmonized standard covering the essential requirements of article 3.2 of the R&TTE directive.
- ETSI EN 301 511 V9.0.2

  Global system for mobile communication (GSM). Harmonized standard for mobile phones in the GSM 900 and GSM 1800 bands covering essential requirements of article 3.2 of the R&TTE directive.
- ETSI EN 301 908-1 V6.2.1

  IMT cellular networks - Harmonized standard covering the essential requirements of article 3.2 of the R&TTE directive. Part 1: Introduction and common requirements
- ETSI EN 301 908-2 V5.4.1

  IMT cellular networks. Harmonized standard covering the essential requirements of article 3.2 of the R&TTE directive. Part 2: CDMA Direct Spread (UTRA FDD) User Equipment (UE)

Maximum antenna gain

Users and installers must be provided with antenna installation instructions and transmitter operating conditions that must be followed to avoid exceeding the permitted RF exposure.

Note the technical specifications of the antenna, refer to Appendix Antennas (Page 135).

RoHS

The product meets the requirements of the EU directive 2011/65/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Applied standard:

- EN 50581:2012

UL approval

Certificate No. E85972, Report No. E85972

- Underwriter Laboratories, Inc.:
  - UL 508 Listed (Industrial Control Equipment)
  - UL 6950-1 (Information Technology Equipment - Safety - Part 1: General Requirements)
- Canadian Standards Association: CSA C22.2 No. 142

Surrounding Air Temperature: Remember the maximum permitted ambient temperature in the section Technical specifications (Page 125).

cULus approval

Certificate No. E115352, Report No. E115352

- UL 60950-1, 2nd Edition, 2011-12-19 (Information Technology Equipment - Safety - Part 1: General Requirements)
- CSA C22.2 No. 60950-1-07, 2nd Edition, 2011-12 (Information Technology Equipment - Safety - Part 1: General Requirements)

cULus Approval, Hazardous Location

Certificate No. E240480, Report No. E240480

- ANSI/ISA 12.12.01-2013, Nonincendive Electrical Equipment for use in Class I and II, Division 2 and Class III, Divisions 1 and 2 Hazardous (Classified) Locations
- CAN/CSA C22.2 No. 213-M1987, Non-incendive Electrical Equipment for use in Class I, Division 2 Hazardous Locations

FM certification

Factory Mutual Research (FM):
Approval Standard Class number 3600 and 3611
Approved for use in:
Class I, Division 2, Group A, B, C, D, Temperature Class T4A, Ta = 55 °C
Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 55 °C

Current approvals on the Internet

You will also find the current approvals for the product on the Internet pages of Siemens Industry Online Support under the following entry ID:

91689511 (http://support.automation.siemens.com/WW/view/en/91689511)
→ "Entry list" tab, entry type "Certificates"

National approvals

You will find an overview of the country-specific wireless approvals of SIMATIC NET devices with GSM, UMTS or LTE services on the IK Info Internet pages on "Industrial Communication".

ik-Info (www.siemens.com/simatic-net/ik-info)

You will find the link to the document on the following page:

Country approvals for GSM/UMTS products (www.siemens.com/mobilenetwork-approvals)

Accessories 11

11.1 Antennas

The following antennas are available and can be installed both indoors and outdoors:

Antennas

Figure 11-1 GPRS/LTE antenna, ANT794-4MR rod antenna

Article number	Explanation
6NH9 860-1AA00	Omnidirectional antenna for GSM (2G), UMTS (3G) and LTE (4G); weatherproof for indoor and outdoor areas; 5 m connecting cable connected permanently to the antenna, SMA connector, including installation bracket, screws, wall plugs.

You will find detailed information in the device manual. You will find this on the Internet on the pages of Siemens Industry Online Support under the following entry ID:

23119005 (http://support.automation.siemens.com/WW/view/en/23119005)
> Entry list > Entry type "Manuals"

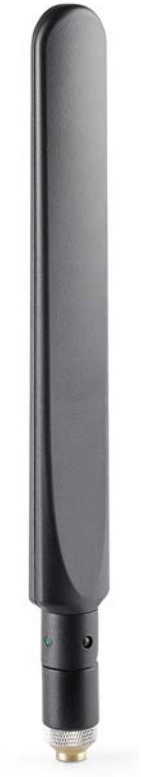


Figure 11-2 LTE antenna, ANT896-4MA, rod antenna

Article number	Explanation
6GK5896-4MA00-0AA3	IRC antenna ANT 896-4MA for GSM (2G), UMTS (3G) and LTE (4G), omnidirectional, radial swiveling, with additional joint, antenna gain: 2 dBi, incl. SMA connector, IP54, -40 ... +85 °C, for direct mounting with SMA connector; package contains: 1 x ANT896-4MA

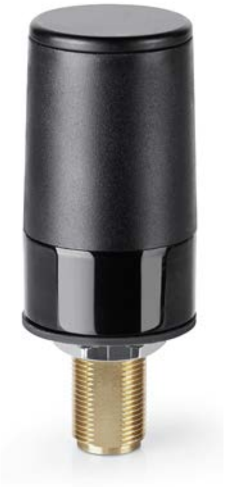


Figure 11-3 LTE antenna, ANT896-4ME, cylinder shaped antenna

Article number	Explanation
6GK5896-4ME00-0AA0	Cylinder shaped antenna ANT 896-4ME for GSM (2G), UMTS (3G) and LTE (4G), omnidirectional, incl. N female connector: 3 dBi, IP66, -40 ... +70 °C, for mounting on cabinet; package contains: 1 x ANT896-4ME

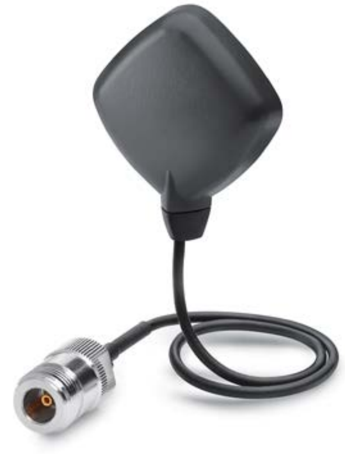


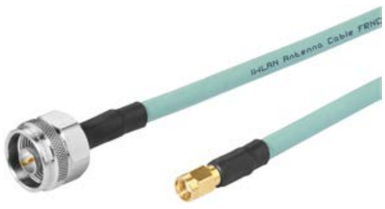
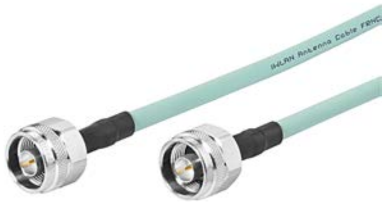
Figure 11-4 GPS antenna, ANT895-6ML, flat antenna

Article number	Explanation
6GK5895-6ML00-0AA0	Antenna ANT 895-6ML, active GPS antenna incl. connecting cable (0.3 m) and N female connector; 20 dBi; IP67, -40 ... +85 °C, mounting using magnets or screws

11.2 Antenna cable

Antenna cable

Table 11- 1 Antenna connecting cables

Article number	Cable lengths	Explanation
6XV1875-5LE30	0.3 m	 Flexible connecting cable preassembled SIMATIC NET N-Connect/SM male/male
6XV1875-5LH10	1 m	
6XV1875-5LH20	2 m	
6XV1875-5LH50	5 m	
6XV1875-5AH10	1 m	 Flexible connecting cable preassembled SIMATIC NET N-Connect/N-Connect male/male
6XV1875-5AH20	2 m	
6XV1875-5AH50	5 m	
6XV1875-5AN10	10 m	

11.3 Cabinet feedthrough / antenna coupling

Cabinet feedthrough

Cabinet feedthrough / coupling piece

Article number	Explanation
6GK5798-2PP00-2AA6	Cabinet feedthrough for wall thicknesses up to a maximum 4.5 mm, can also be used as a coupling device between two antenna connecting cables, N-Connect/N-Connect female/female connector, suitable for 0 … 11 GHz, IP68

11.4 Overvoltage protection

Overvoltage protection

Lightning protector

Article number	Explanation
6GK5798-2LP00-2AA6	Lightning protector LP798-1N, for the antennas ANT790 and ANT890, for N-Connect connectors, N-Connect/N-Connect female/female connector, suitable for 0 ... 6 GHz, IP68, also suitable for DC feed-in via the antenna cable

Documentation references A

Where to find Siemens documentation

- You will find the article numbers for the Siemens products of relevance here in the following catalogs:
  - SIMATIC NET Industrial Communication / Industrial Identification, catalog IK PI
  - SIMATIC Products for Totally Integrated Automation and Micro Automation, catalog ST 70

  You can request the catalogs and additional information from your Siemens representative.
- You will find SIMATIC NET manuals on the Internet pages of Siemens Automation Customer Support:

  Link to Customer Support (http://support.automation.siemens.com/WW/view/en)

  Enter the entry ID of the relevant manual as the search item. The ID is listed below some of the reference entries in brackets.

  As an alternative, you will find the SIMATIC NET documentation on the pages of Product Support:

  10805878 (http://support.automation.siemens.com/WW/view/en/10805878)

  Go to the required product group and make the following settings:

  "Entry list" tab, Entry type "Manuals / Operating Instructions"
- You will find the documentation for the SIMATIC NET products relevant here on the data medium that ships with some products:
  - Product CD / product DVD or
  - SIMATIC NET Manual Collection

SIMATIC NET
LOGO! CMR2020 / CMR2040
Operating Instructions
Siemens AG
91689511 (http://support.automation.siemens.com/WW/view/en/91689511)

LOGO!
System Manual
Siemens AG
Current version on the following Internet page:
13617 (https://support.industry.siemens.com/cs/ww/en/ps/13617)

Index