BOSCH

MAP 5000

ICP-MAP5000-2 / ICP-MAP5000-COM / ICP-MAP5000-S / ICP-MAP5000-SC

en Installation manual

MAP 5000   Table of contents | en   **3**

Table of contents

MAP 5000   Introduction | en   **5**

1   Introduction
1.1   Short information

This manual describes the installation, wiring, initial set-up and maintenance of the MAP 5000 system.

It is applicable for all MAP 5000 kits and the following main panels including all accessory MAP 5000 products:

– MAP Main Panel (ICP-MAP5000-2)
– MAP Main Panel with IP Communicator (ICP-MAP5000-COM) including the MAP GSM module (ITS-MAP0008).
– MAP Main Panel Small (ICP-MAP5000-S)
– MAP Main Panel Small with IP Communicator (ICP-MAP5000-SC) including the MAP GSM module (ITS-MAP0008).

1.2   Listings and approvals

The system is designed to comply with the certifications and approvals listed here.

Region	Agency	Certification
Germany	VdS	Class C, VdS G 111040
Europe	CE	Conformité Européene
Europe	EN	EN 50131-1:2006 + A1:2009 EN 50131-3:2009 EN 50131-6:2008 EN 50136-2/SP4/DP3 EN 50131-10
Switzerland	SES	Association of Swiss Installers of Security Systems Edition V3 / 01.01.2011-d
France	AFNOR / CNPP Cert.	NF&A2P Grade 3 Certificate Number ICP-MAP5000-2: 1133400003 Certificate Number ICP-MAP5000-COM: 1230200016 According to NF324-H58

1.3   Battery handling

The battery terminals must be covered after installation in order to avoid short circuits.
Suitable terminal covers are included in the scope of delivery of the power supply.

Danger!
Electrictity
Do not short-circuit the battery in the host alarm system. A short-circuited battery can deliver large currents that might result in serious burns or create a fire hazard.

Further information is available at http://www.boschsecurity.com/standards.

1.4   Installation considerations

– When installing this system, ensure that all local and national wiring codes are met.
– Only authorized service personnel is allowed to install this system.
– Use only the installation material recommended by BOSCH Security Systems to ensure error-free operation.

– Follow anti-static procedures when handling system components. Ensure that you are properly grounded to discharge any static charge before you work with system components.
– Install all components in dry, maintained interior rooms.
– Install the system in a centrally located room that is near the AC Power MAINS.
– Because the panel is permanently connected equipment, a readily accessible disconnect device must be included into the building installation wiring.

> **Danger!**
> Electric shock
> Danger of electric shock if live parts are touched. The alarm system is designed for an IT-power distribution system (230 V). Switch off the power supply of the alarm system before carrying out maintenance or installation work.

1.5 Planning the system

MAP control panel enclosure kit
The ICP-MAP0111 panel enclosure kit is the main system enclosure. This enclosure is designed to contain the following components:
– ICP-MAP5000 main panel[1]
– ICP-MAP0007 DE module[1]
– ICP-MAP0010 LSN gateway[1]
– ICP-MAP0012 CAN splitter[1]
– AT 2000 communicator[2]
– IPP-MAP0005 power supply[3]
– ICP-MAP0065 AC terminal block[4]
– ICP-MAP0050 control panel enclosure tamper switch
– Two batteries (maximum 45 Ah each)
Use the ICP-MAP0120 expansion enclosure kit when the system requirements for power and / or other remote devices exceed the capacity provided by the ICP-MAP0111 panel enclosure kit[6.].

MAP expansion enclosure kit
The ICP-MAP0120 expansion enclosure kit is designed to contain the following components:
– IPP-MAP0005 power supply[3]
– ICP-MAP0010 LSN gateway[5]
– ICP-MAP0012 CAN splitter[1]
– ICP-MAP0065 AC terminal block[4]
– ICP-MAP0055 expansion enclosure tamper switch
– Two batteries (maximum 18 Ah each)
Use the ICP-MAP0115 power enclosure kit when system power requirements exceed the power capacity of the ICP-MAP0111 panel enclosure kit[6].

MAP power enclosure kit
The ICP-MAP0115 power enclosure kit is designed to contain the following components:
– IPP-MAP0005 power supply[3]
– ICP-MAP0065 AC terminal block[4]
– ICP-MAP0050 control panel enclosure tamper switch
– Four batteries (maximum 40 Ah each)

MAP 5000

Introduction | en   **7**

[1] This module mounts on the ICP-MAP0025 hinged mounting plate.

[2] This module mounts on the ICP-MAP0020 accessory mounting plate, which mounts to the back of the enclosure.

[3] When determining the number of power supplies, it is also necessary to take into account the inrush current of loads (refer to *Planning the system with IPP-MAP0005 power supply, page 7*).

[4] This assembly is only required if the IPP-MAP0005 power supply is installed.

[5] When one or more ICP-MAP0010 LSN gateways are operated remotely, there must be one IPP-MAP0005 power supply in the same enclosure.

[6] Mount the enclosure directly under or at the side (top edge flush) of the control panel enclosure.

1.5.1 Planning the system with IPP-MAP0005 power supply

Number of power supplies

To guarantee a reliable system booting, take into account the following:

– Inrush current of the connected loads
– Current limit of the IPP-MAP0005 power supply
– Current limit of the ICP-MAP5000 main panel

Notice!

The normal operating condition is not the subject of these considerations.

Load inrush current

– IUI-MAP0001-2 control center: max. 800 mA
– ICP-MAP0010 LSN module: max. 1000 mA, AUX is switched on later
– ICP-MAP0007-2 DE module: negligible

Current limitation

– Power supply per output A / B (short-time): 3.2 A
– Main panel at external BDB: 1.6 A

Refer to *Typical configuration with ICP-MAP0111 panel enclosure, page 8*.

Definition of power supply segment

A power supply segment is a power supply with all loads supplied by the power supply.

Power supply segment
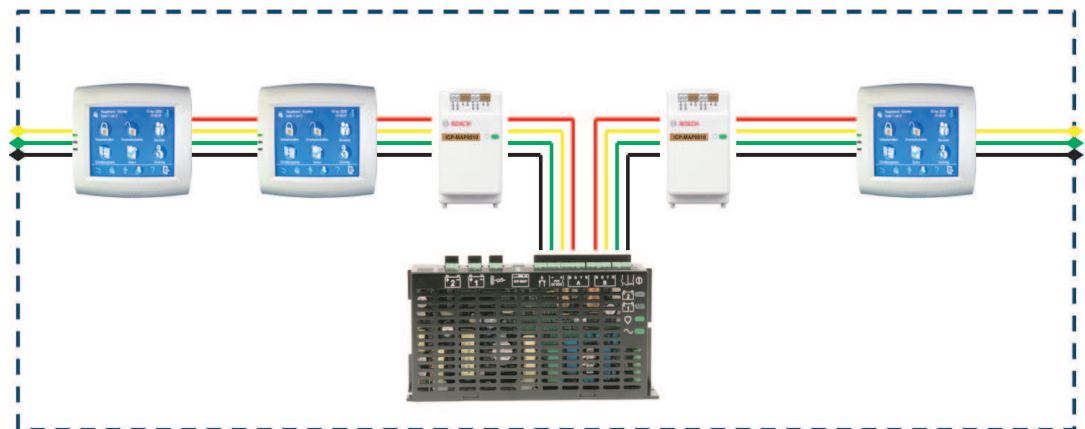
4-wire cables are used for load connection within the power supply segment.

The following conditions must be taken into account when planning in order to guarantee a reliable system booting:

Condition 1

3-wire cables are always used for connections between power supply segments (without +28 V, red wire)

Figure 1.1: Wiring of power supply segments

Condition 2

Charged batteries must be connected to the power supply to ensure reliable system start-up.
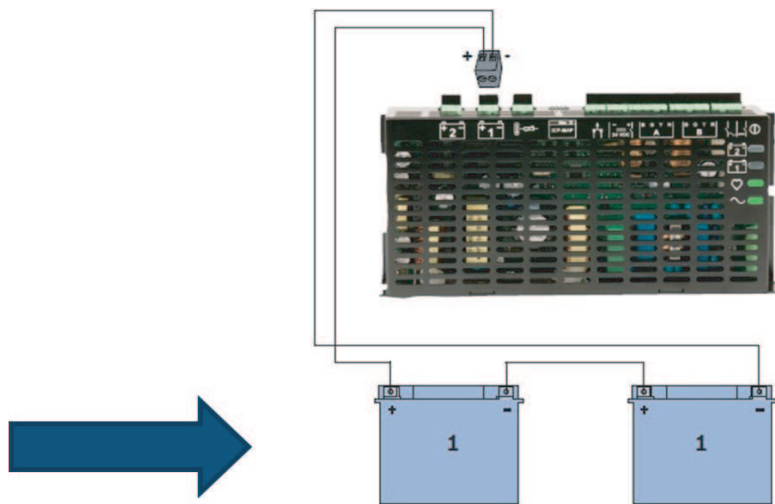
Figure 1.2: Batteries for system booting

Condition 3

To ensure reliable system start-up, it is necessary to take into account the cable length and wire gauge:

– between power supply and first control center
– between control centers

Refer to *, page 10*.

Typical configuration with ICP-MAP0111 panel enclosure

Main panel - DE module - 3 LSN gateway modules - max. 2 control centers

MAP 5000

Introduction | en   9
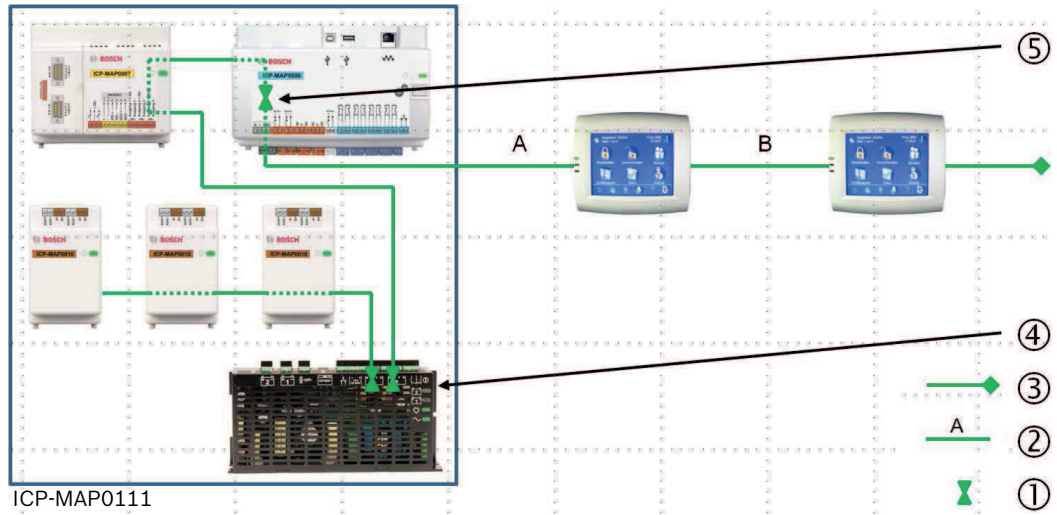
ICP-MAP0111

Figure 1.3: Wiring with ICP-MAP0111

Key	Description
1	Current limitation
2	4-wire connection, take into account cable length
3	3-wire connection to the next power supply segment
4	Short-time current limitation to 3.2 A per output A / B
5	Current limitation to 1.6 A between internal and external BDB

Remote operation with ICP-MAP0120 expansion enclosure
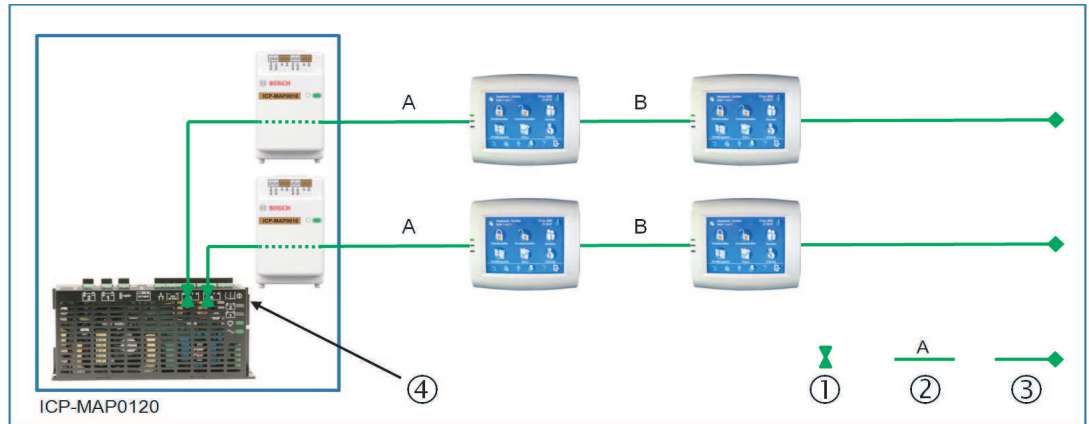
ICP-MAP0120

Figure 1.4: 2 LSN modules with up to 4 control centers
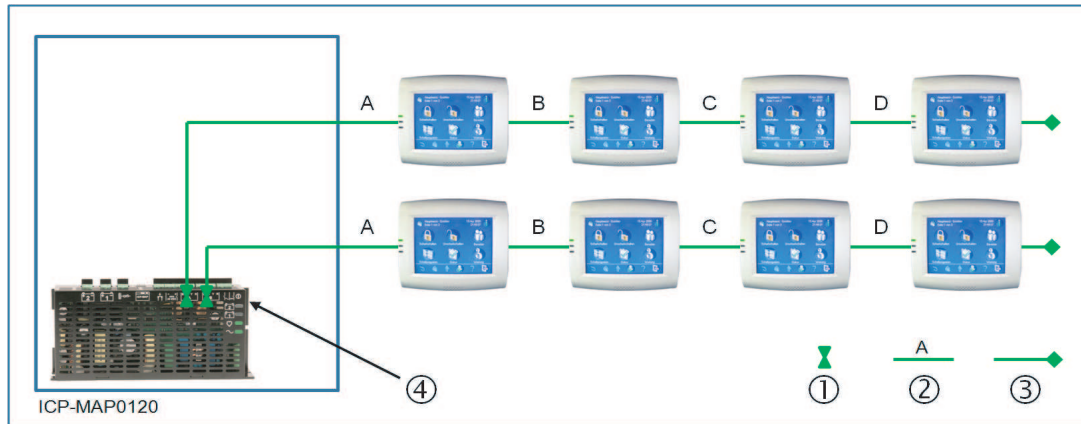
Figure 1.5: Up to 8 control centers

Key	Description
1	Current limitation
2	4-wire connection, take into account cable length, refer to , page 10
3	3-wire connection to the next power supply segment
4	Short-time current limitation to 3.2 A per output A / B

Cable length

The maximum number of control centers that can be supplied by one power supply depends greatly on the length and diameter of the cable used.

Wire diameter	Wire cross-section	Length A	Length B	Length C	Length D
0.8 mm	0.503 mm^2 .	325 m	- - -	- - -	- - -
0.8 mm	0.503 mm^2 .	100 m	135 m	- - -	- - -
0.8 mm	0.503 mm^2 .	50 m	225 m	- - -	- - -
0.8 mm	0.503 mm^2 .	50 m	50 m	50 m	- - -
1.0 mm	0.785 mm^2 .	500 m	- - -	- - -	- - -
1.0 mm	0.785 mm^2 .	175 m	175 m	- - -	- - -
1.0 mm	0.785 mm^2 .	100 m	325 m	- - -	- - -
1.0 mm	0.785 mm^2 .	100 m	75 m	75 m	- - -
1.0 mm	0.785 mm^2 .	50 m	400 m	- - -	- - -
1.0 mm	0.785 mm^2 .	50 m	125 m	125 m	- - -
1.0 mm	0.785 mm^2 .	50 m	50 m	50 m	50 m

Tab. 1.1: Cable lengths

The following applies for VdS

For remote operation of the IPP-MAP0005 power supply, a control center assigned to the same area must be provided for indication of power supply trouble (trouble in mains supply / battery).

MAP 5000

Introduction | en   **11**

| 1.5.2 | **Planning the system with ICP-MAP0012 CAN splitter module** |

▸   When using a CAN splitter module to split the external BDB into two independent areas, chose one of the following wiring possibilities:

Wiring with a CAN splitter module and a MAP LSN gateway module

ICP-MAP0012   ICP-MAP0010
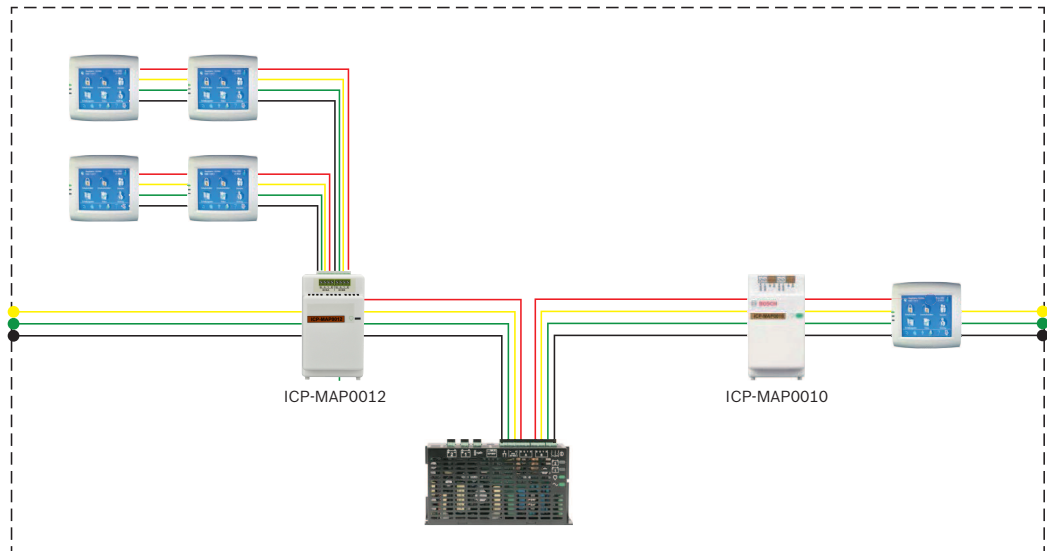
Wiring with two CAN splitter modules

ICP-MAP0012   ICP-MAP0012
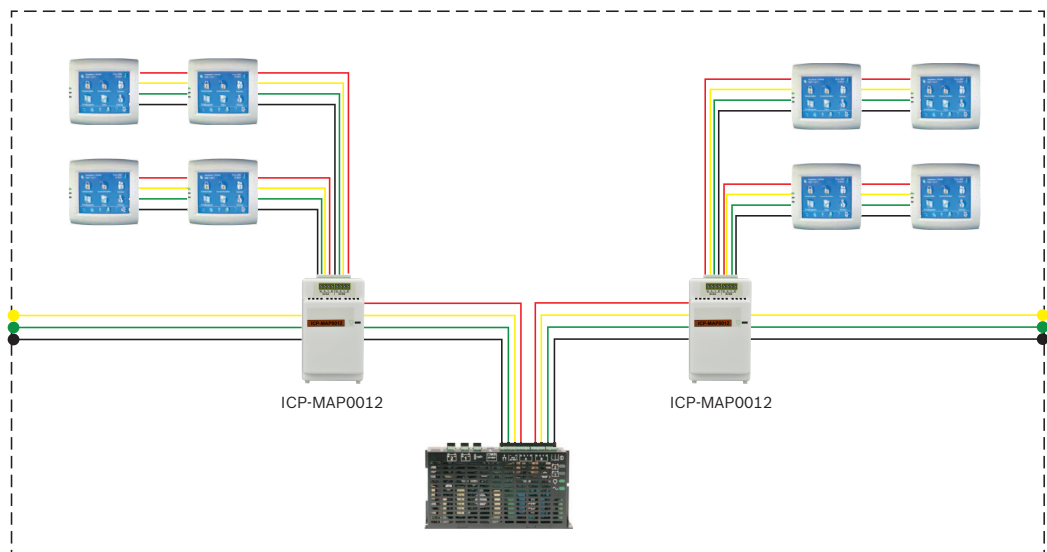
Cable length

The cable length of the splitted external BDB depends on the number of added keypads and of the cable diameter.

The maximum cable length is 500 m per BDB connector.

▸   When planning the system with one or more CAN splitter modules, ensure to use an appropriate cable length and diameter in accordance with the necessary number of keypads.

Relation of cable length, diameter and number of keypads

Cable diameter	Number of keypads					
	1	2	3	4	5	6
0.6 mm	225 m	225 m	200 m	150 m	120 m	100 m
0.8 mm	400 m	400 m	350 m	275 m	220 m	200 m
1.0 mm	620 m	620 m	550 m	450 m	360 m	300 m

Notice!
These cable lengths apply only for keypads with hardware version 1.0.2. The cable lengths of older keypads are half of the lengths displayed in the table above.

Notice!
These cable lengths apply for keypads that are mounted with an equal cable distance in between each other.

See also
– *Splitting the external data bus with a CAN splitter module, page 44*

1.6 System overview

This chapter shows an overview of the system as it is installed in the ICP-MAP0111 control panel enclosure.

System installation in ICP-MAP0111 panel enclosure (hinged mounting plate closed)
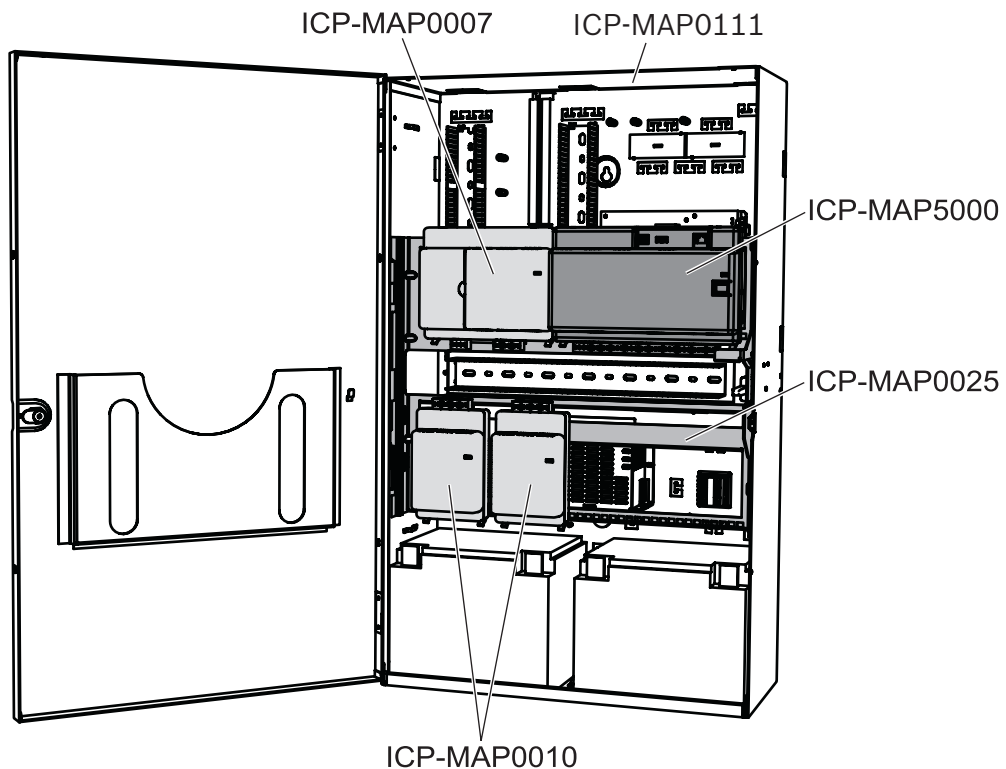
MAP 5000   Introduction | en   **13**

System installation in ICP-MAP0111 panel enclosure (hinged mounting plate open)

ICP-MAP0111

ICP-MAP0025

AT 2000

ICP-MAP0050

ICP-MAP0065

IPP-MAP0005
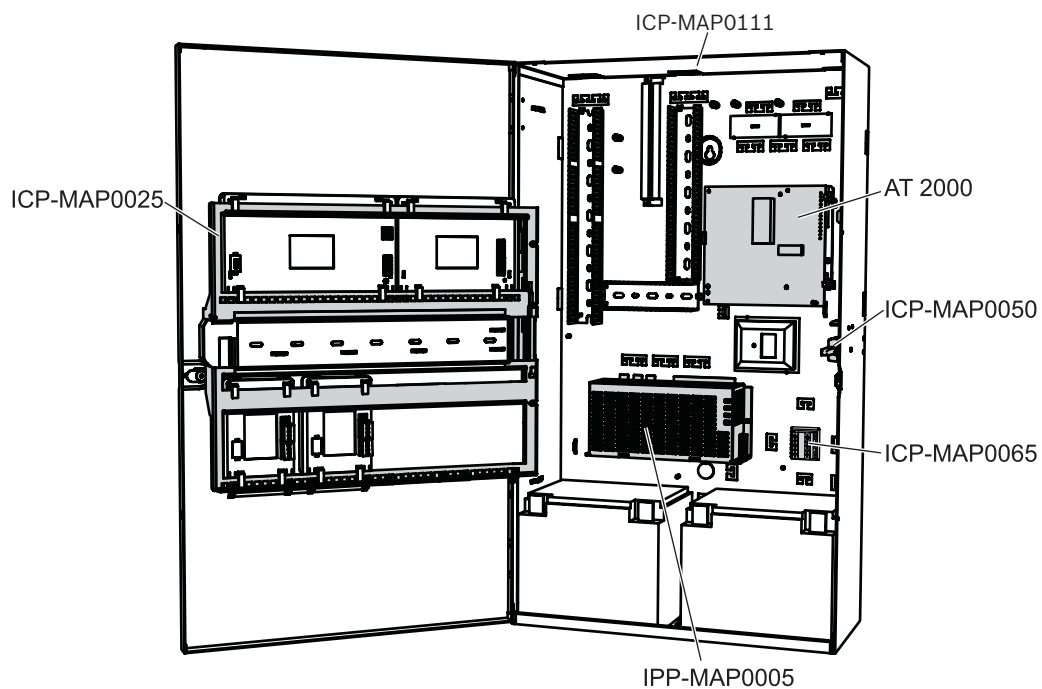
System installation in ICP-MAP0120 expansion enclosure

IPP-MAP0005   ICP-MAP0065

ICP-MAP0120   ICP-MAP0055
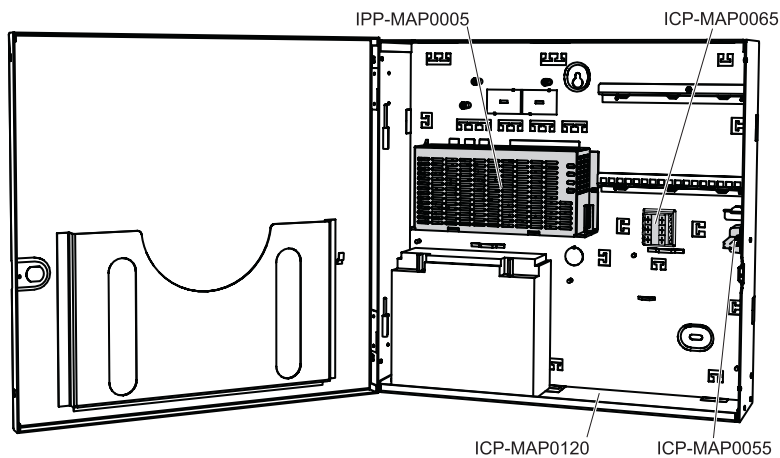
Enclosure overview

ICP-MAP0120

ICP-MAP0111
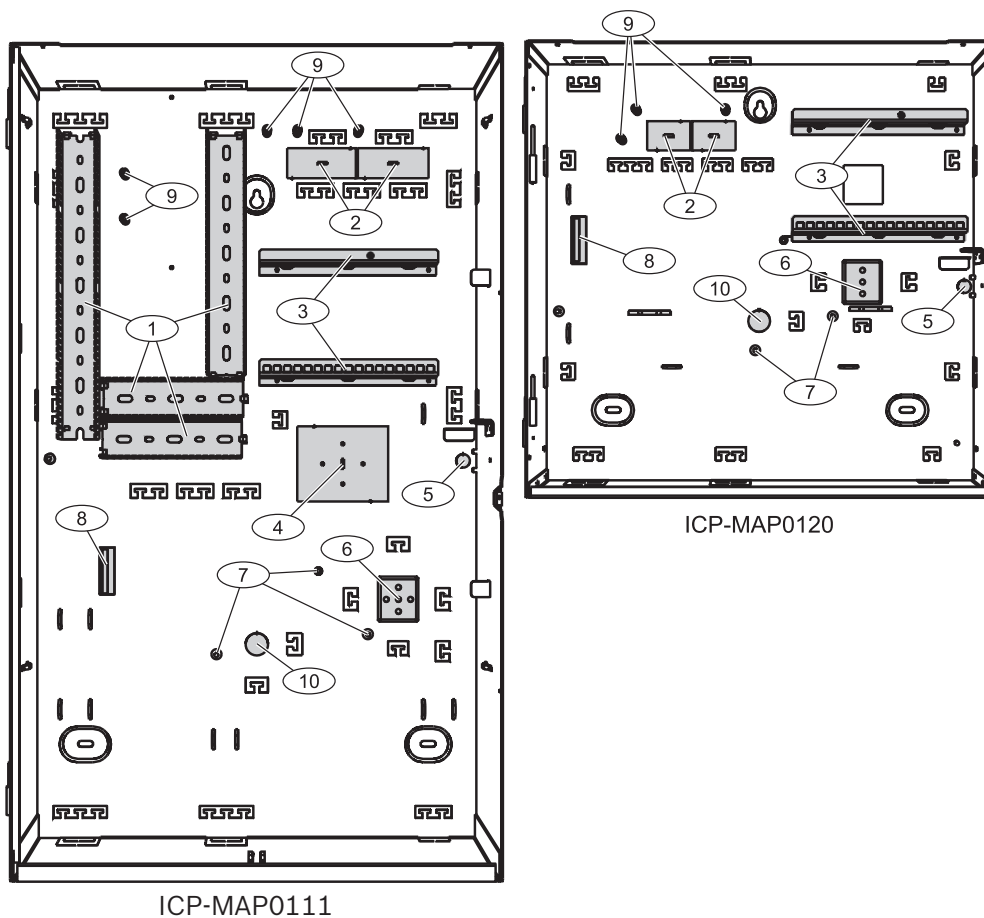
Element	Description
1	Wire trays
2	Wire knockouts
3	Mounting rails for ICP-MAP0020 accessory mounting plate
4	Mounting location for TAE box
5	Knockout for wall tamper
6	Mounting location for ICP-MAP0065 AC terminal block
7	Earth ground connection points
8	Flange for IPP-MAP0005 power supply
9	Shielding connection points
10	Knockout for AC wires (use when AC wires come in from the back of the enclosure)

MAP 5000   Installation | en   **15**

2   Installation

–   Use proper anchor and screw sets when installing the enclosure on surfaces. Refer to the drill template for detailed instructions.
–   Ensure that there is enough free space to the left of the enclosure so that the enclosure door and the ICP-MAP0025 hinged mounting plate have full range of motion. 460 mm (18 in) for a fully opened door or 32 mm (1.25 in) for 90° opened door is required.
–   Ensure that there is at least 100 mm (4 in) of space around the enclosure to allow easy access to cable conduits.
–   Leave adequate space below or next to the enclosure for an ICP-MAP0120 expansion enclosure for future additions to the system.
–   To minimize battery depletion, install the enclosure in locations at normal room temperature.
–   Use the ICP-MAP0111 installation mounting template (F.01U.076.204) or the ICP-MAP0120 installation mounting template (F.01U.076.205)

2.1   Removing the enclosure knockouts

1.   Unhinge and remove the enclosure door and set it aside.
2.   Remove the enclosure knockouts in the order shown in the figure below.

Enclosure knockouts

ICP-MAP0120

ICP-MAP0111
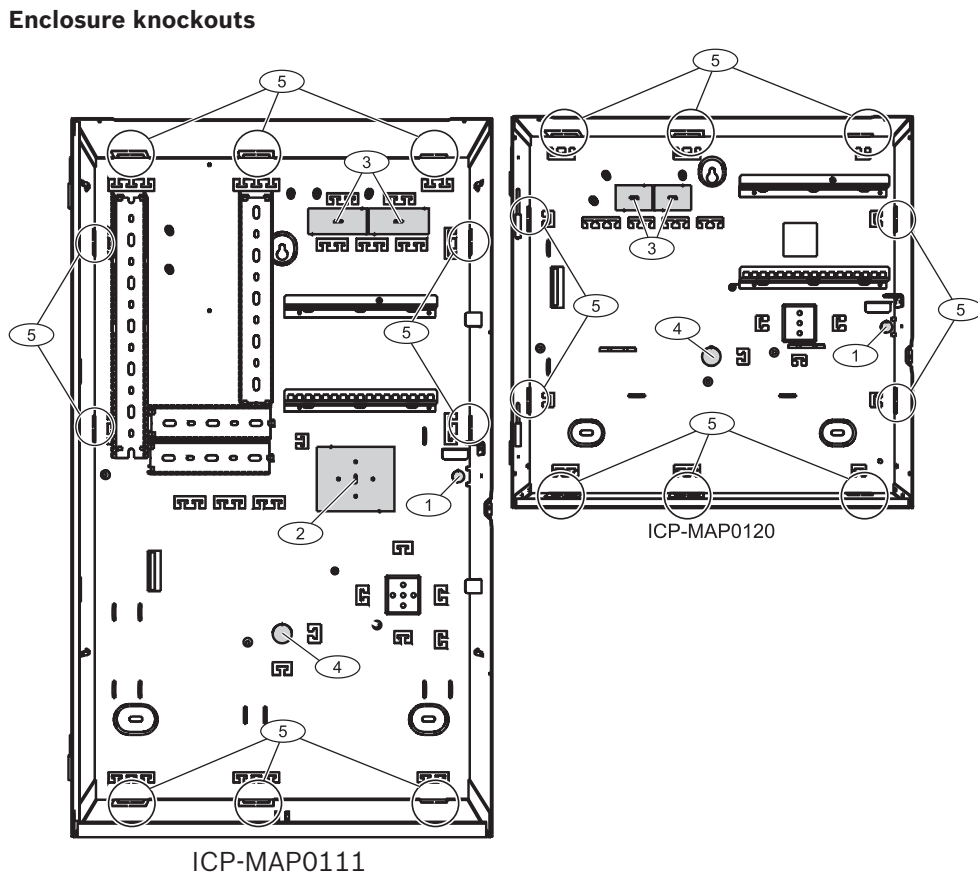
Element	Description
1	Knockout for wall tamper (required in accordance with EN50131 grade 3)
2	Knockout for TAE box
3	Knockouts for wiring

4	Knockout for AC wires (use when AC wires come in from the back of the enclosure)
5	Side wall knockouts for wiring

2.2 Installing the tamper switch rail

1. Remove the tamper switch rail from the package.
2. Mount the tamper switch rail to the inner right side of the enclosure as shown in the figure below.
3. Secure the tamper switch rail with the two supplied screws.
   Do **not** mount the tamper switch at this time.

Mounting the tamper switch rail

ICP-MAP0111

ICP-MAP0050

MAP 5000   Installation | en   **17**
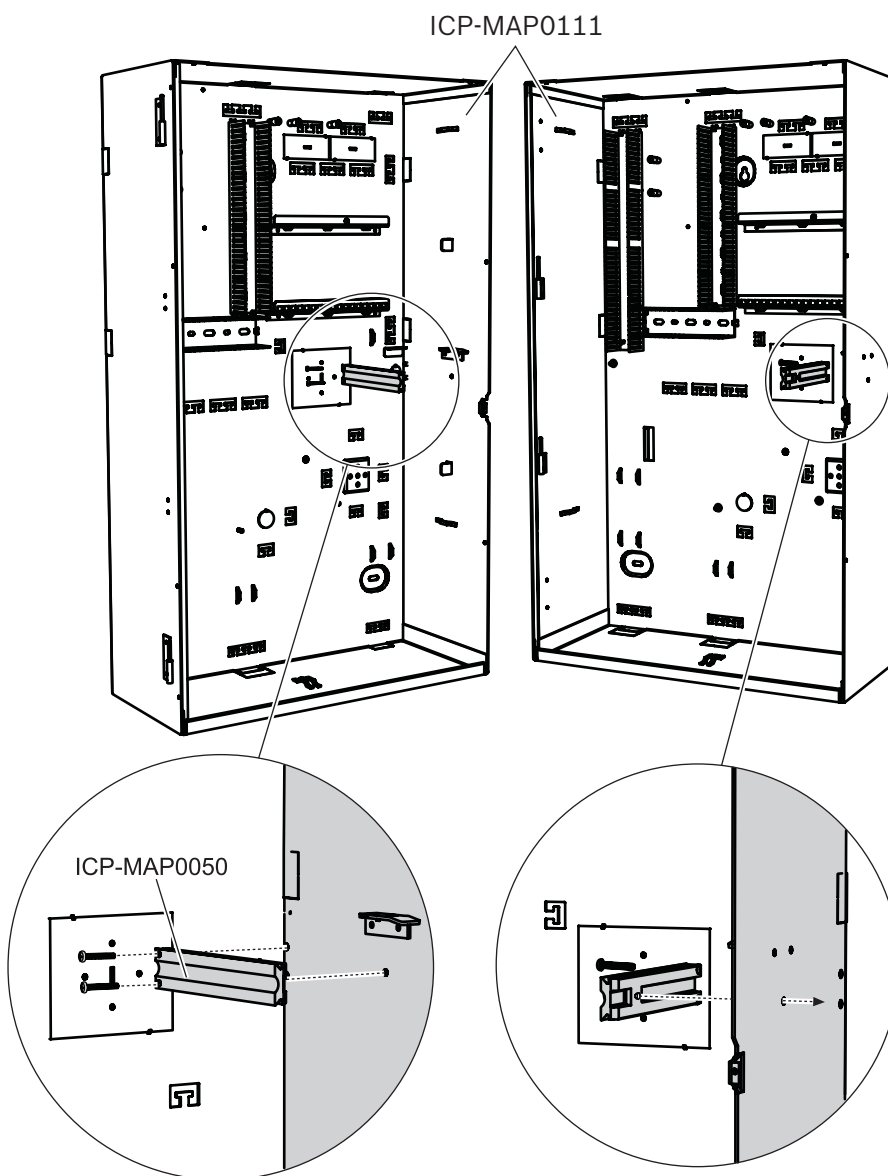
2.3   **Mounting the enclosure**

	Notice!
i	Ensure that there is enough free space to the left of the enclosure so that the enclosure door and the ICP-MAP0025 hinged mounting plate have full range of motion. - For a fully opened door, at least 460 mm (18 in) is required. - For a door opened at 90°, at least 32 mm (1.25 in) is required**.**

1. Use the supplied drill template to mark the holes on the intended surface.
   The drill template can be found in the enclosure box.
2. If a wall tamper is required, insert the plug for the tamper switch into the back of the enclosure (required in accordance with EN50131 grade 3) as shown in the figure below.
3. Secure the plug to the wall using a suitable screw (not supplied).

Inserting the wall tamper plug

ICP-MAP0111
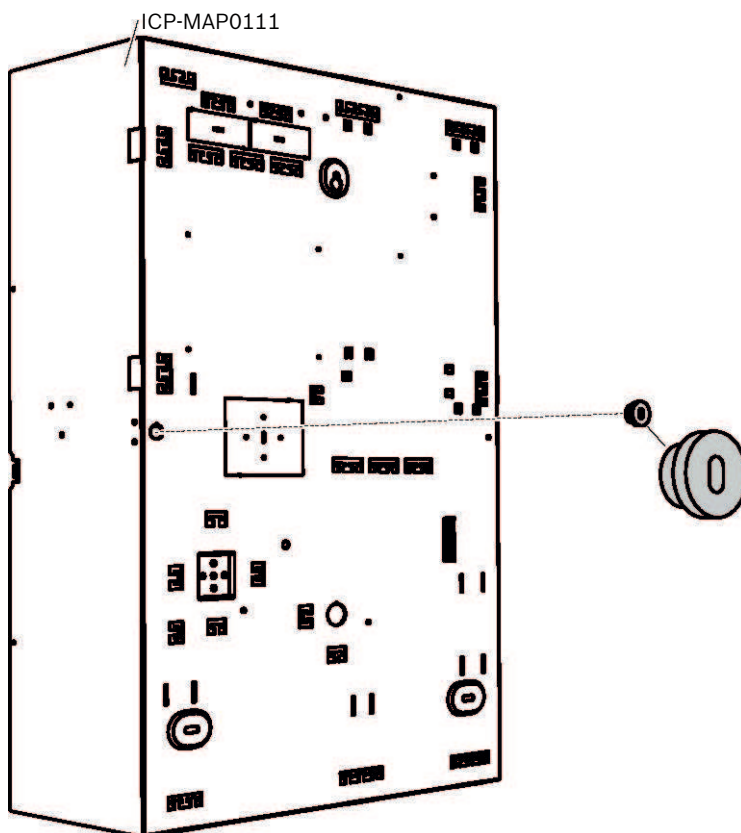
1. Mount the enclosure to the intended surface using suitable screws and anchors (not supplied). Use the mounting holes as shown in the figure below.
2. Ensure that all screws are tight and that the enclosure is securely fastened to the mounting surface.

Mounting the enclosure

ICP-MAP0111
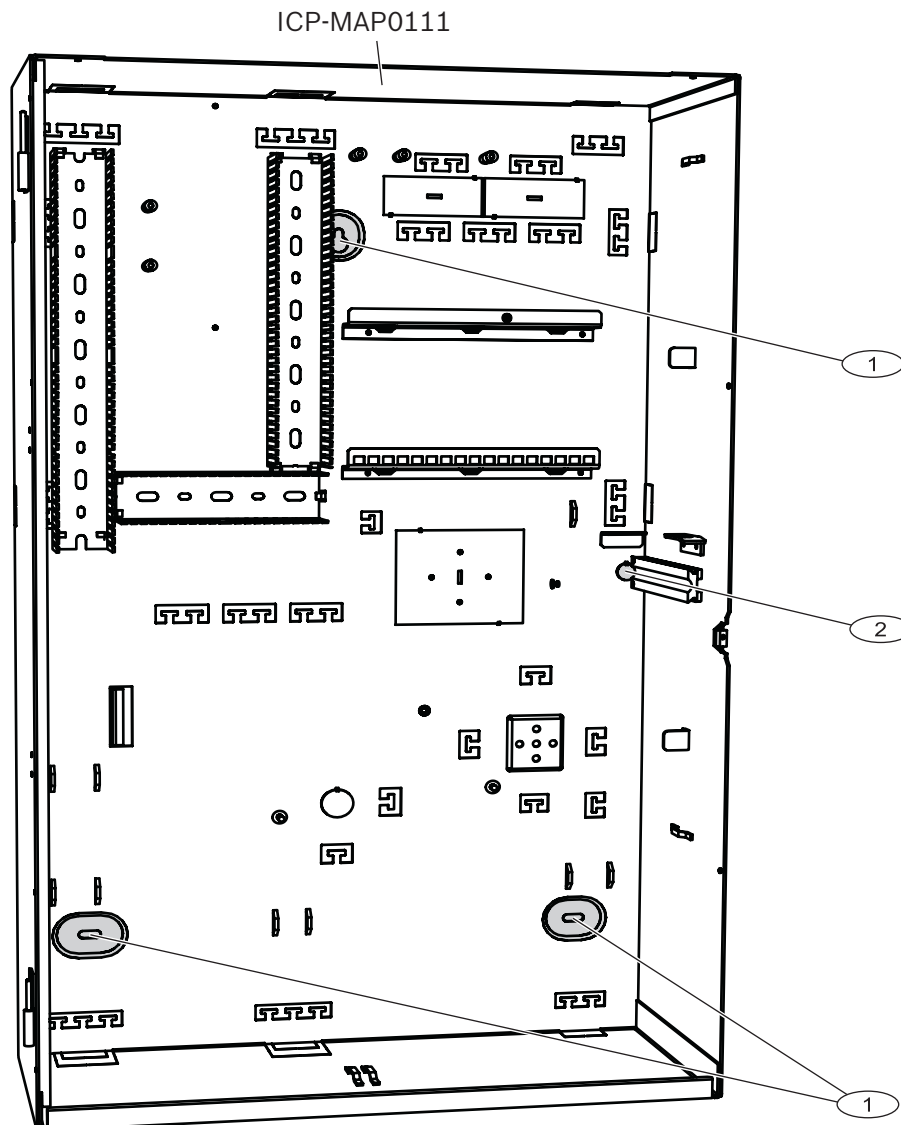
Element	Description
1	Mounting hole
2	Hole for screw to secure wall tamper plug

Mounting an edge protection profile (optional)

For an installation according to the regulations of NFa2p AFNOR certification, it is necessary to mount an edge protection profile on the upper edge of the MAP enclosure.

The edge protection profile can be ordered at http://eshop.wuerth.de/en/US/EUR/ with the article number 09610027.

1. Mount the edge protection profile on the upper edge of the MAP enclosure from the left to the right. Ensure not to leave gaps at the cut-outs.
2. Cut off the overlaying edge protection profile on the right side of the enclosure.

MAP 5000   Installation | en   **19**

Mounting an edge protection profile
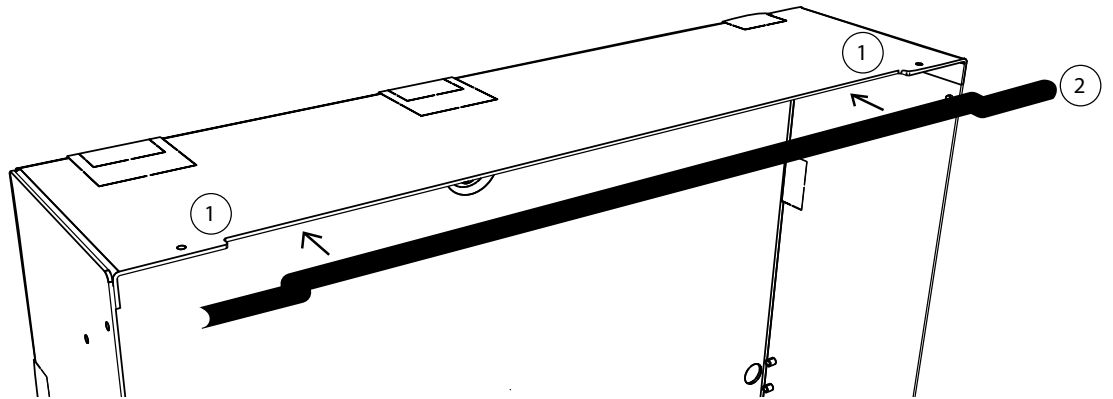
Element	Description
1	cut-outs
2	edge protection profile

2.4   Checking the AC connection

1.   Ensure that the AC circuit breaker switch is off.
2.   Connect the AC line to the AC terminal block.
3.   Switch the AC breaker on.
4.   Verify that the circuit breaker does not trip and that appropriate line voltage is present on the fused side of the AC terminal block.
5.   Switch the AC breaker off and continue with the rest of the installation.

> **Warning!**
> After ensuring the AC connection is functional, turn the AC breaker off before continuing the installation process.

2.5   Installing the power supply and power supply accessories

> **Caution!**
> Debris
> Damage to the power supply due to debris during the installation is possible.

–   To prevent damage to the power supply during installation, ensure that the supplied protective dust cover label is on top of the power supply before installing it.

1.   Slide the left side of the power supply against the flange on the left side of the enclosure back wall.
2.   Align the cut-out on the right side of the power supply.
3.   Secure the power supply to the enclosure back wall with the supplied hardware in the following order: external tooth washer, washer, hex nut

Installing the power supply

ICP-MAP0111
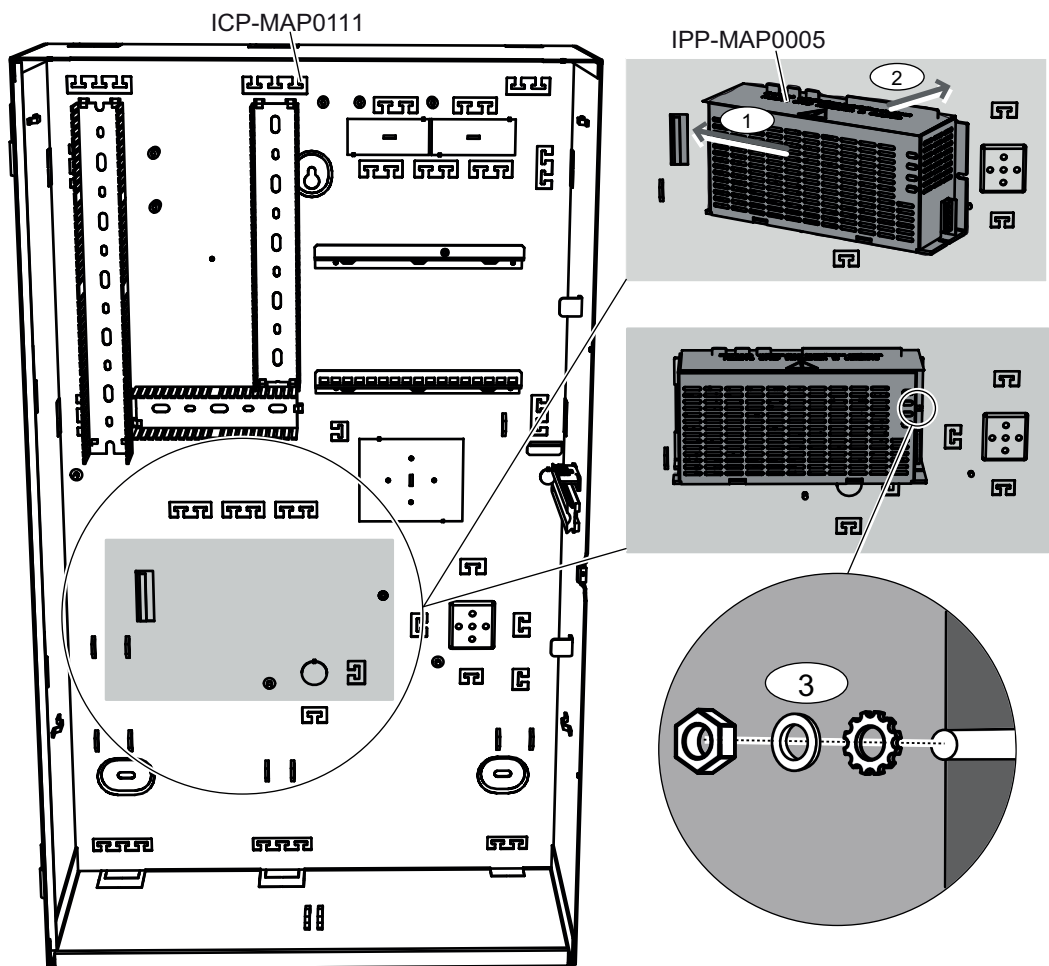
IPP-MAP0005

IPP-MAP0005 power supply ratings label

▸ Put the power supply ratings label on the side of the power supply as shown in the picture below.

MAP 5000   Installation | en   **21**
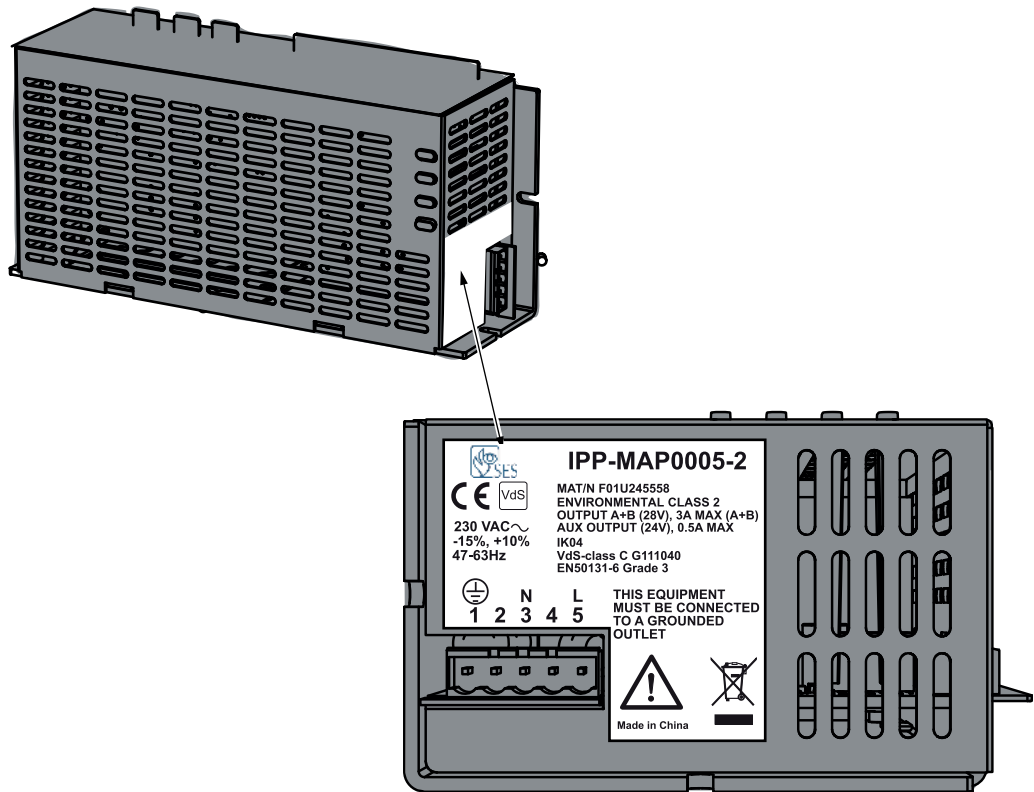
IPP-MAP0005 power supply warning label

The power supply warning label needs to be put on the enclosure back wall before installing the AC terminal block. The power supply warning label indicates that the terminal block connected to the AC terminal block may never be removed from the power supply during operation.

▸ Put the power supply warning label on the enclosure back wall at the upper right side of the power supply as shown in the pictures below.
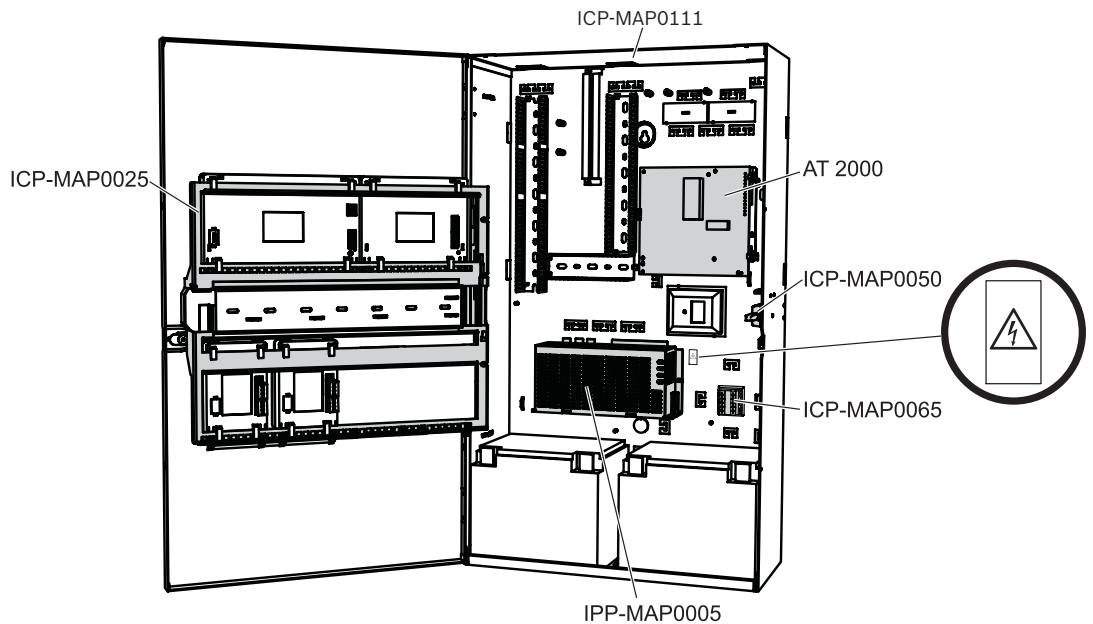
Figure 2.1: Putting the power supply warning label into the ICP-MAP0111 and ICP-MAP0115 enclosure

IPP-MAP0005   ICP-MAP0065

ICP-MAP0120   ICP-MAP0055
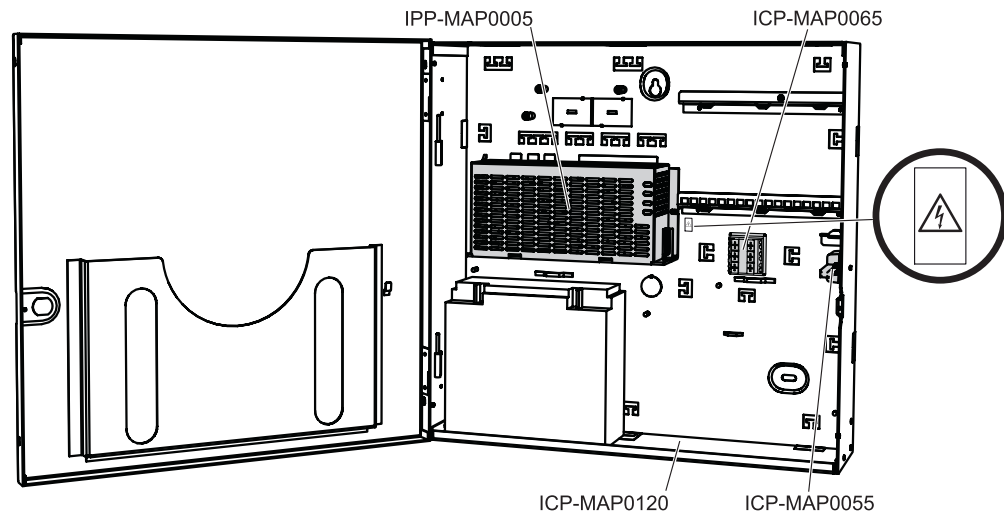
Figure 2.2: Putting the power supply warning label into the ICP-MAP0120 enclosure

▸ Refer to *Technical Specifications, page 68* for power specifications.

Installing the AC terminal block

1. Mount the AC terminal block to the enclosure back wall into the corresponding mounting holes as shown in the figure below and secure it with the supplied screws (1).
2. Plug the terminal block connected to the AC terminal block into the power supply as shown in the figure below (2).
3. Connect the ground wire to the ground connection point of the enclosure back wall as shown in the figure below (3).

MAP 5000   Installation | en   **23**
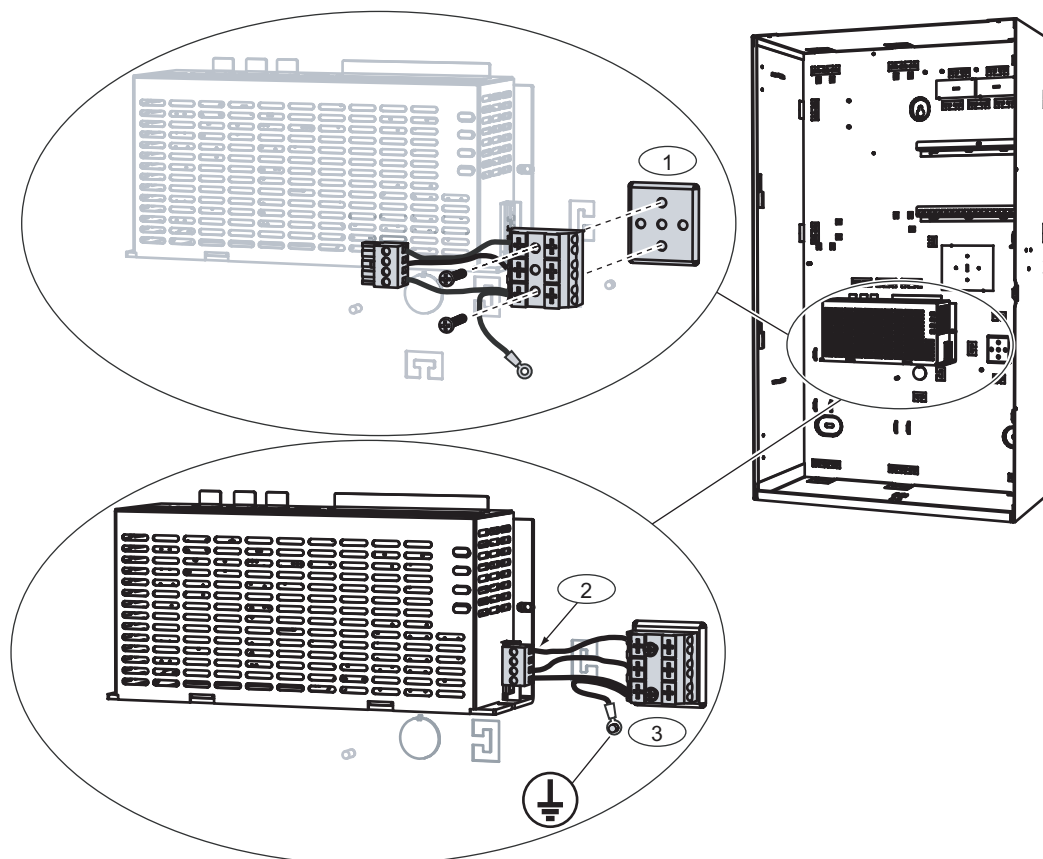
	Warning!
⚠	When installing the power supply, ensure that the ground wire from the AC terminal block is connected to the ground connection point as shown in *, page 22*. The ground wire from the AC terminal block to the power supply **does not** provide an earth ground for the enclosure. It only provides an earth ground for the power supply.

	Warning!
⚠	Electricity Once the terminal block connected to the AC terminal block has been put into the power supply, do not remove it anymore. Never remove the terminal block connected to the AC terminal block from the power supply during operation.

Installing the thermistor cable

The thermistor cable is used to adjust the battery charge voltage to compensate for the air temperature around the batteries.

1. Plug the thermistor cable into the power supply to the terminal marked ⎍⟿ .
2. Mount the thermistor on the inside rear of the enclosure right on the top of the two batteries.

	Notice!
ⓘ	In case more than one enclosure is used, mount the thermistor cable in the enclosure in which the power supply is placed.

Mounting the thermistor
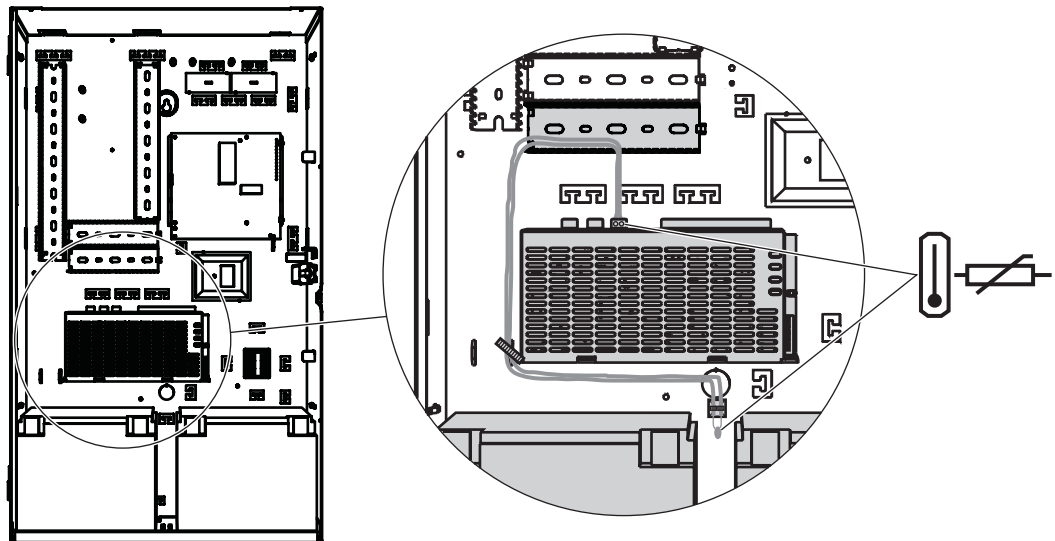
See also
– *Technical Specifications, page 68*

2.6   Installing the TAE box

▸ If the TAE Box is not mounted on the wall behind the enclosure, mount the TAE Box to the enclosure back wall either horizontally or vertically as desired.

Installing the TAE box
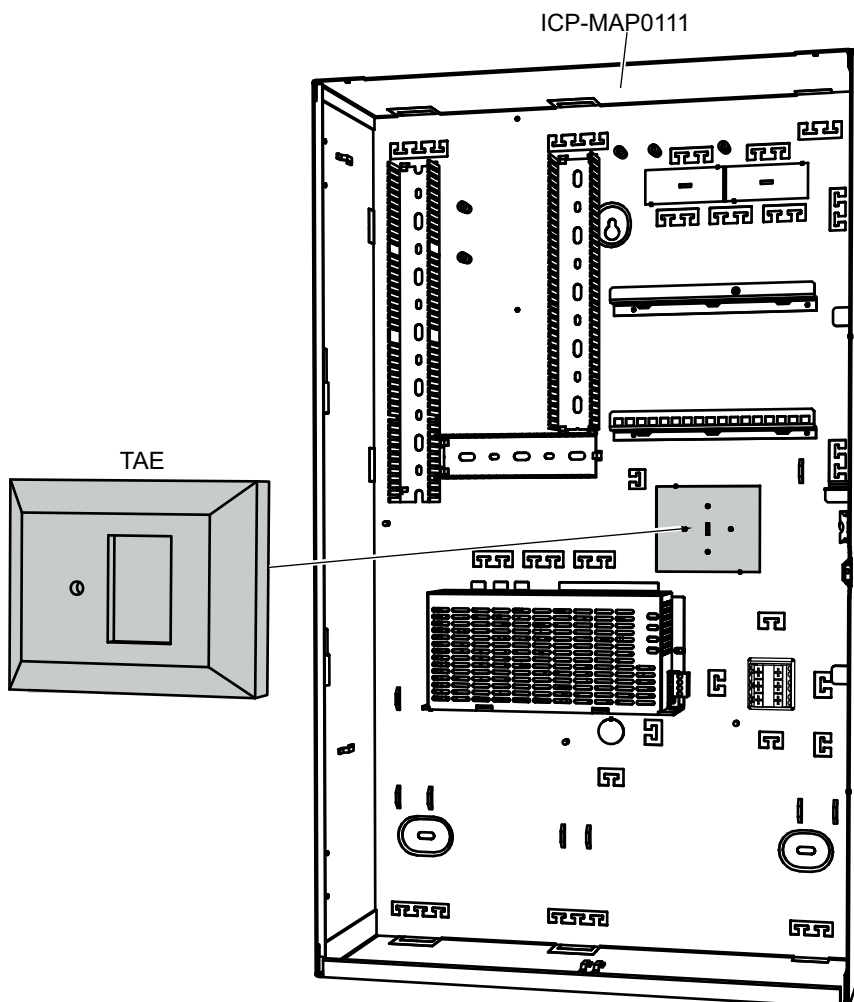
2.7 Installing the accessory mounting plate

1. Align the earth ground stud on the accessory mounting plate with the earth ground hole on the top mounting rail in the upper right side of the enclosure wall as shown in the figure below.
2. Slide the clips on the back of the accessory mounting plate onto the top and bottom mounting rails.

MAP 5000

Installation | en   25

Aligning the accessory mounting plate

ICP-MAP0111

ICP-MAP0020
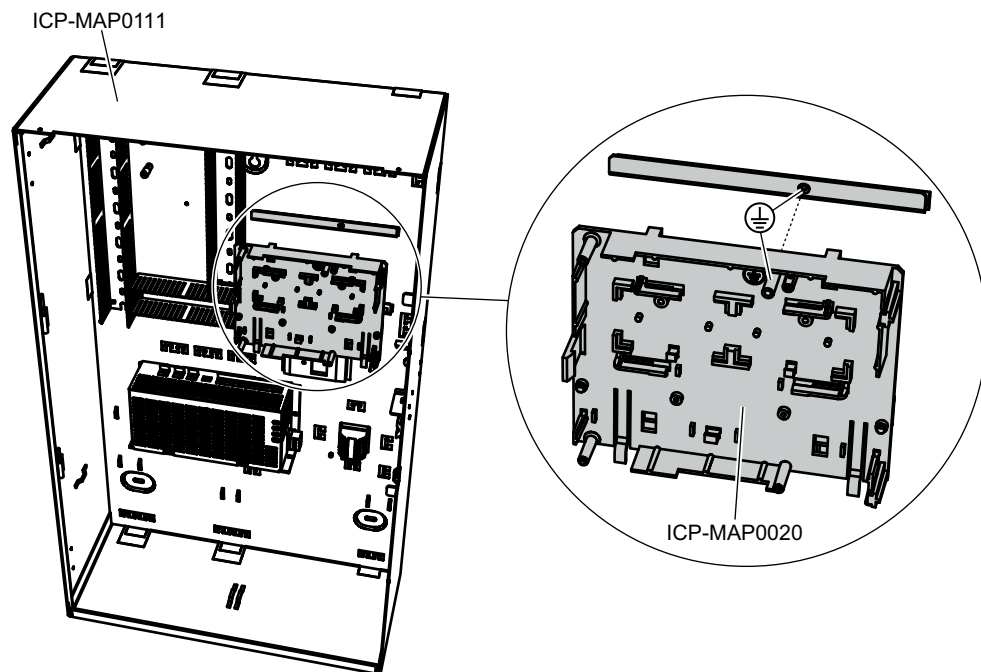
▸ Ensure that the locking clips snap into the bottom mounting rail as shown in the figure below.

Installing the accessory mounting plate
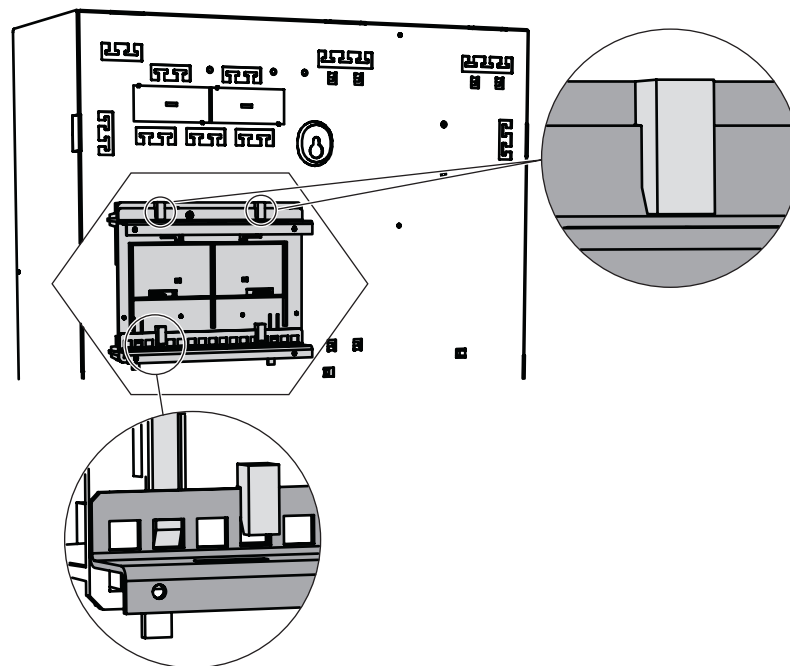
Refer to *Accessory mounting plate overview, page 26* for the locations of the modules that mount on the accessory mounting plate.

Accessory mounting plate overview
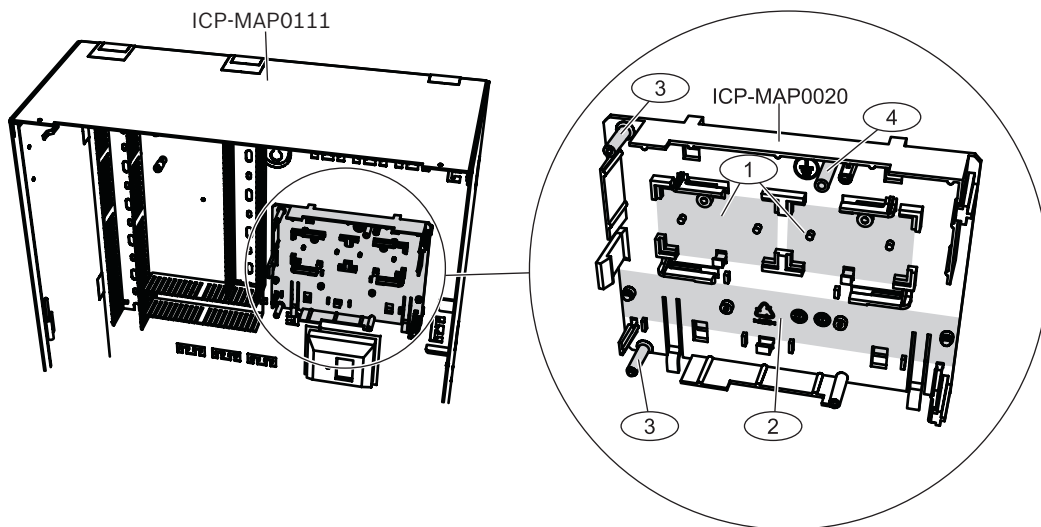
Element	Description
1	Locations for ICP-MAP0017 12 V converters (two maximum)
2	Location for fuse plate (SIV) (one maximum)
3	Screw locations for AT 2000 communicator (one maximum)
4	Screw location for AT 2000 earth ground

2.8   Installing the 12 V converter

1. Mount the ICP-MAP0017 12 V converter onto the accessory mounting plate as shown in the figure below (screws not supplied).
2. Connect the field wiring to the terminal block of the 12 V converter as shown in the figure below and leave the other ends unconnected.

MAP 5000   Installation | en   **27**

Installing the 12 V converter

M3.5 x 5

ICP-MAP0017

ICP-MAP0020
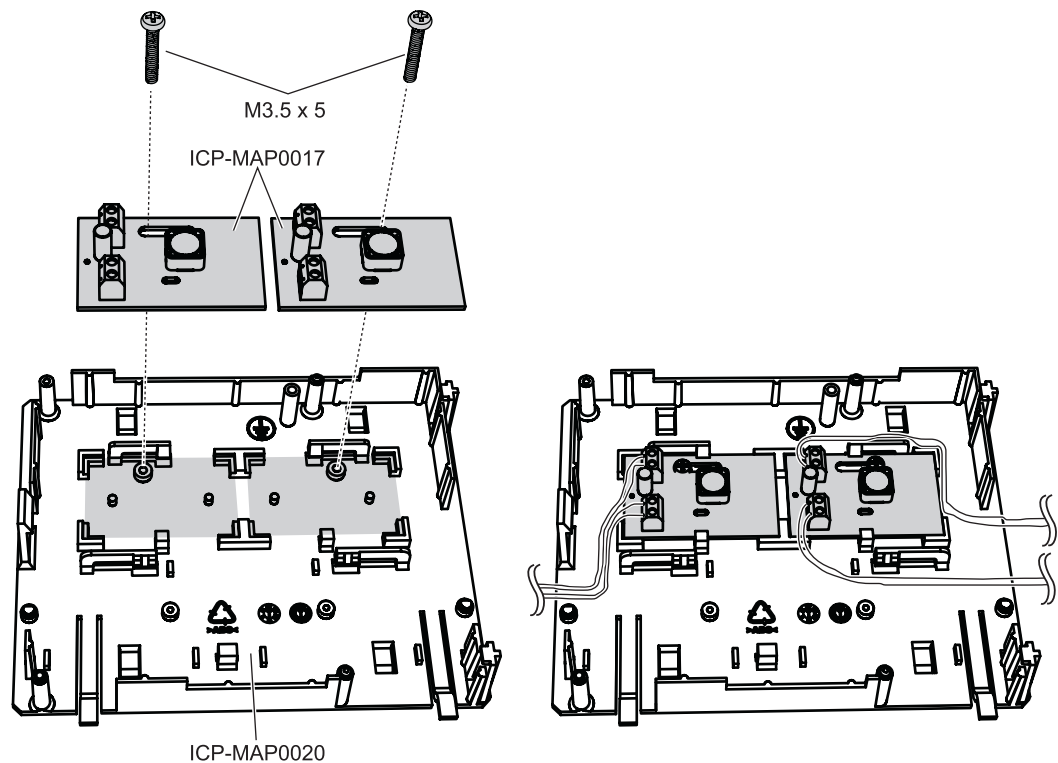
2.9   Installing the fuse plate (SIV)

1.   Mount the fuse plate (SIV) onto the accessory mounting plate as shown in the figure below (screws not supplied).
2.   Connect the field wiring to the terminal block of the fuse plate (SIV) as shown in the figure below and leave the other ends unconnected.

Notice!

Use the corresponding ratings for the fuses SI 1 ... SI 5. (minimum 250 mA, maximum 1 A depending on the connected loads).

The overall current of all SIV outputs must not exceed the available maximum current of the voltage output used.

Installing the SIV
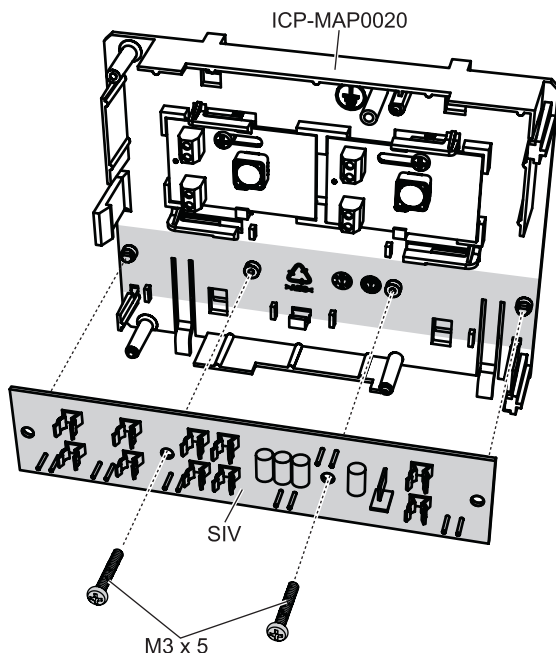
2.10 Installing the AT 2000 communicator

The AT 2000 communicator mounts onto the ICP-MAP0020 accessory mounting plate over the 12 V converter (if installed). If the fuse plate (SIV) is mounted on the accessory mounting plate, the communicator cannot be mounted on the same mounting plate.

1. Slide the right edge of the AT 2000 under the clips on the right-hand side of the accessory mounting plate.
2. Gently push down on the left edge of the AT 2000 until it snaps into place under the single clip on the left-hand side of the accessory mounting plate.
3. Insert the supplied grounding screw through the AT 2000 and the accessory mounting plate, and fasten it into the top mounting rail.

> **Notice!**
> To ensure proper system grounding, you must insert the grounding screw through the AT 2000 and the accessory mounting plate.

MAP 5000   Installation | en   **29**

Installing the AT 2000 communicator
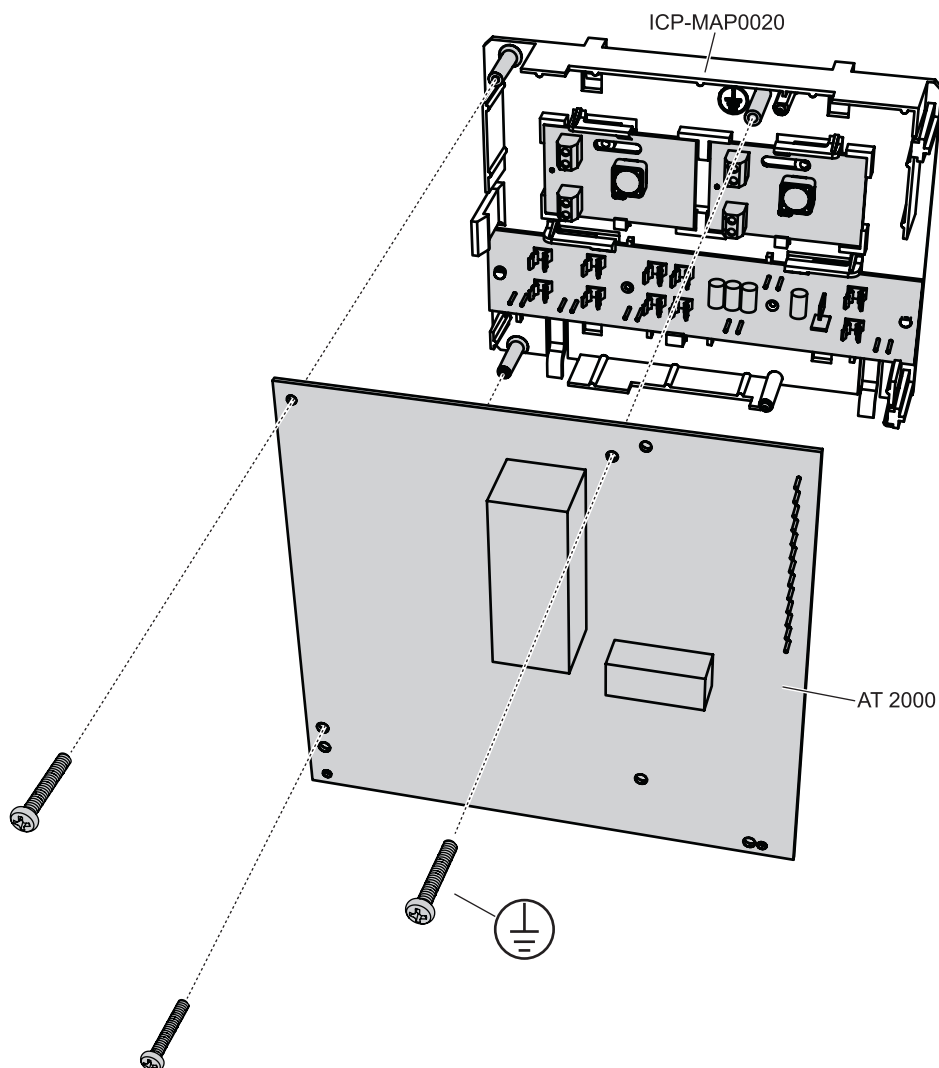
▸ Connect the AT 2000 communicator to the ICP-MAP0007 DE module using the supplied ribbon cable (P/N F01U074773).

The cable is supplied with the DE module.

The ribbon cable is used for all connections of the communicator input lines and for the "Communicator Trouble" and "Negative Acknowledgment" communicator signals. If additional signals are required for the communicator, e.g. area x armed / disarmed, these can be provided as a point-to-point connection between the panel and communicator.

i	**Notice!** The analog AT 2000 requires 12 V. Use the ribbon cable connector labeled **AT 2000 Uext**. The analog AT 2000 also requires a separate 12 V power source, such as the ICP-MAP0017 12 V converter. The ISDN AT 2000 requires 28 V. Use the ribbon cable connector labeled **AT 2000 28V**.

Analog AT 2000 to DE module connections

ICP-MAP0007

AT 2000

DE MODULE

F01U074773

P/N: F01U074773

AT2000 Uext.

AT2000 28V
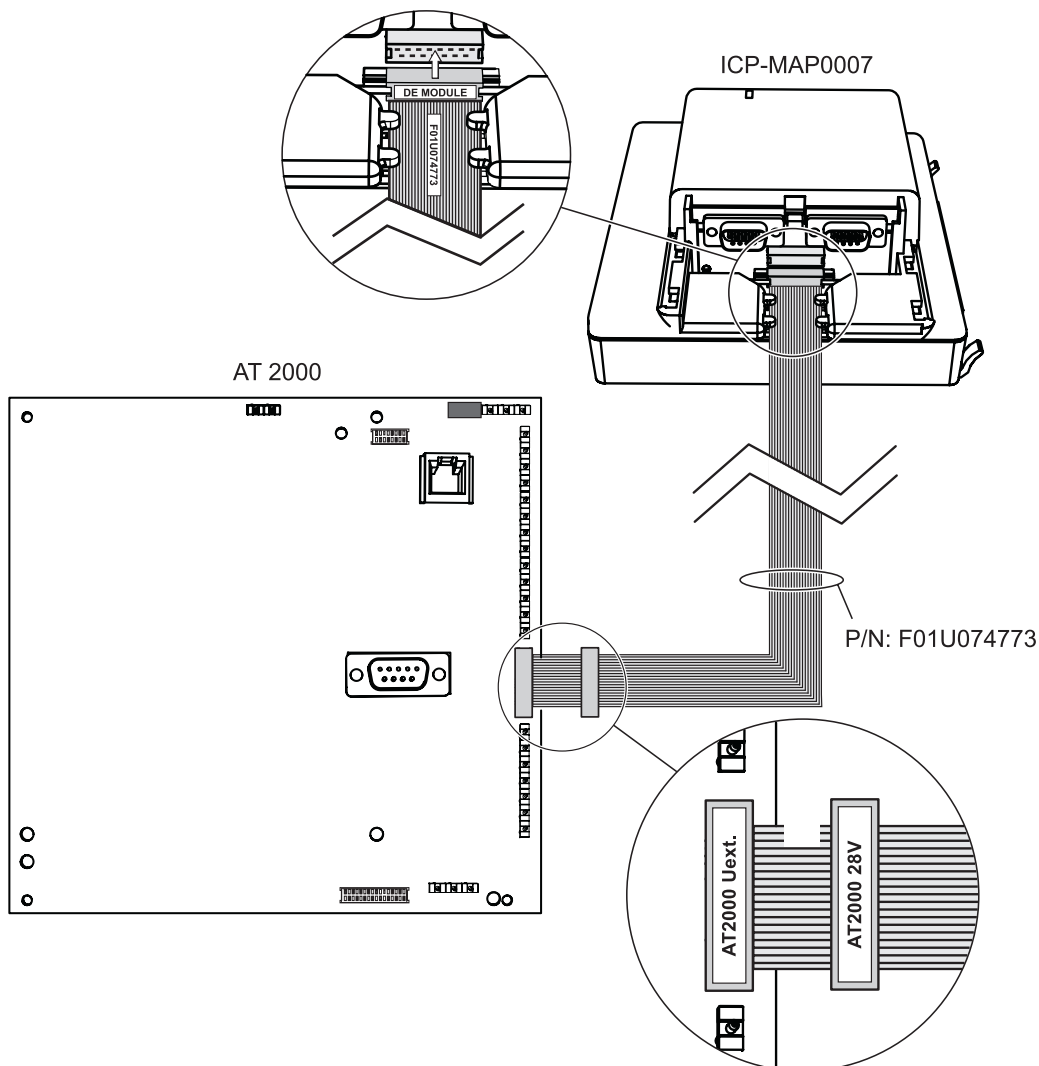
	Notice!
i	The two trouble inputs are automatically configured to "Communicator Trouble" and "Negative Acknowledgment" when "Communicator" is selected in the Remote Programming Software (RPS).

MAP 5000

Installation | en   **31**

Analog AT 2000 to ICP-MAP0017 12 V converter connections

IPP-MAP0005

(+)
(−)

ICP-MAP0017

AT 2000

+12 VDC **-12 VDC**

EXTP   EXTM
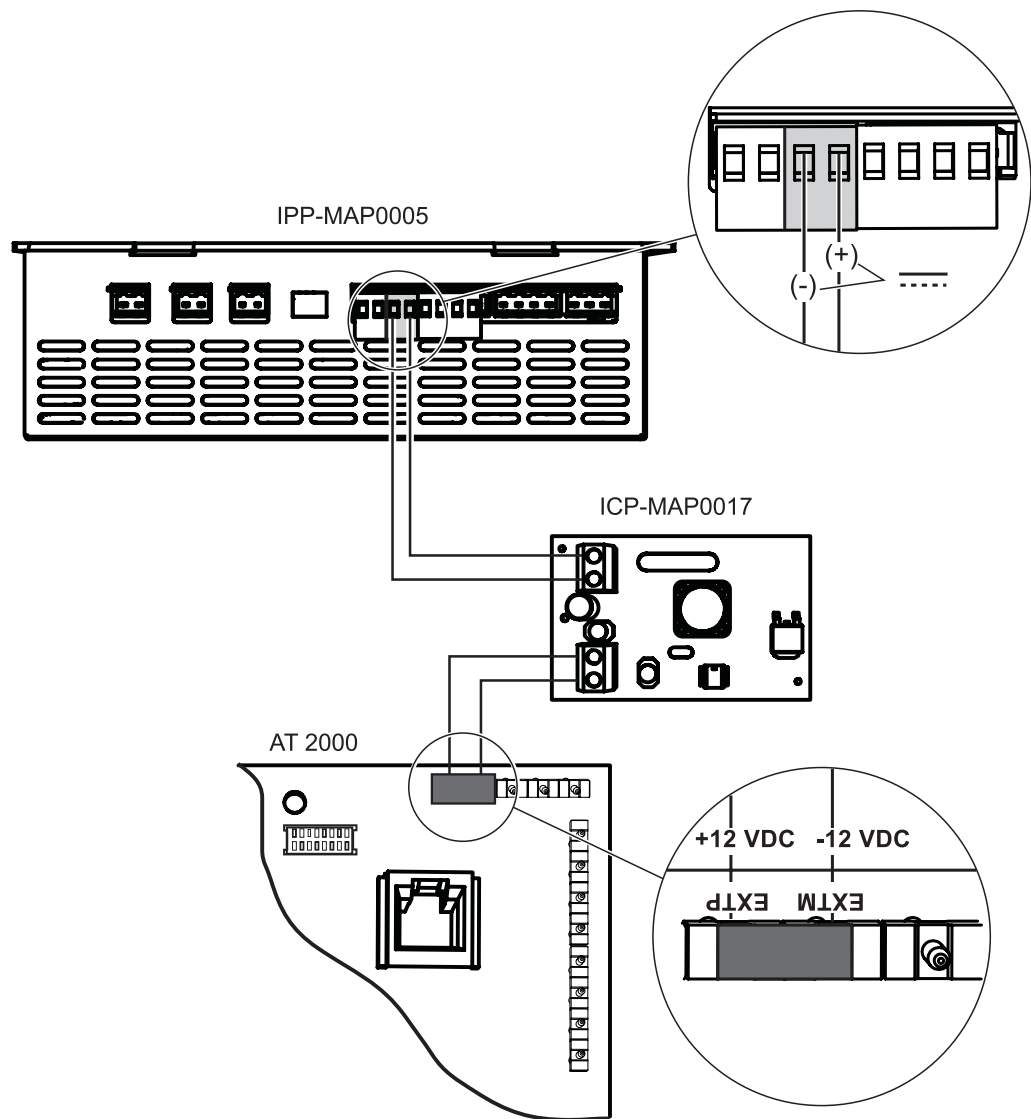
AT 2000 ISDN to DE module connections

ICP-MAP0007

DE MODULE

F01U074773

P/N: F01U074773

AT 2000 ISDN

AT2000 28V

MAP 5000   Installation | en   **33**
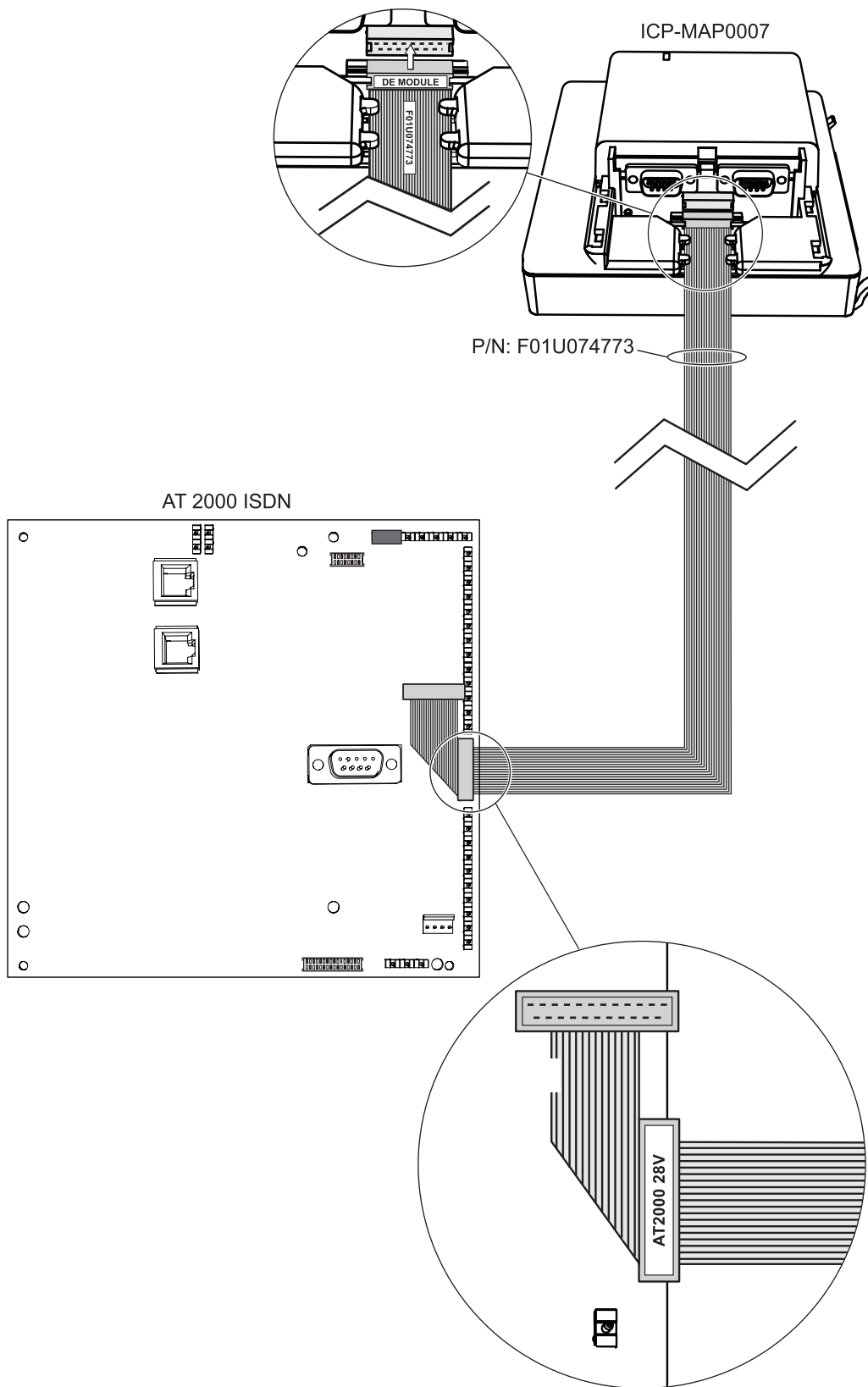
2.11   Installing the hinged mounting plate

‣   Install the ICP-MAP0025 hinged mounting plate inside the enclosure ICP-MAP0111 or ICP-MAP0120.

Installing the hinged mounting plate

ICP-MAP0111

ICP-MAP0025
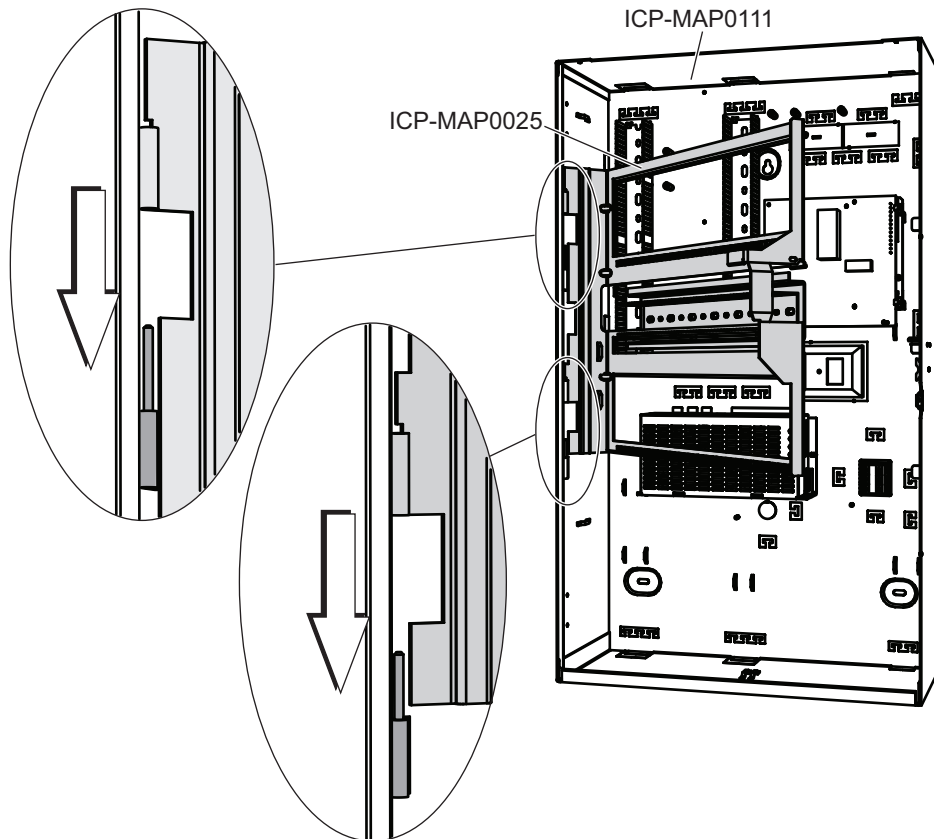
Mounting modules onto the hinged mounting plate

The following graphic shows an overview of the hinged mounting plate and the designated mounting locations of the modules.

Hinged mounting plate overview

ICP-MAP0007

ICP-MAP5000

ICP-MAP0025

ICP-MAP0010
ICP-MAP0012
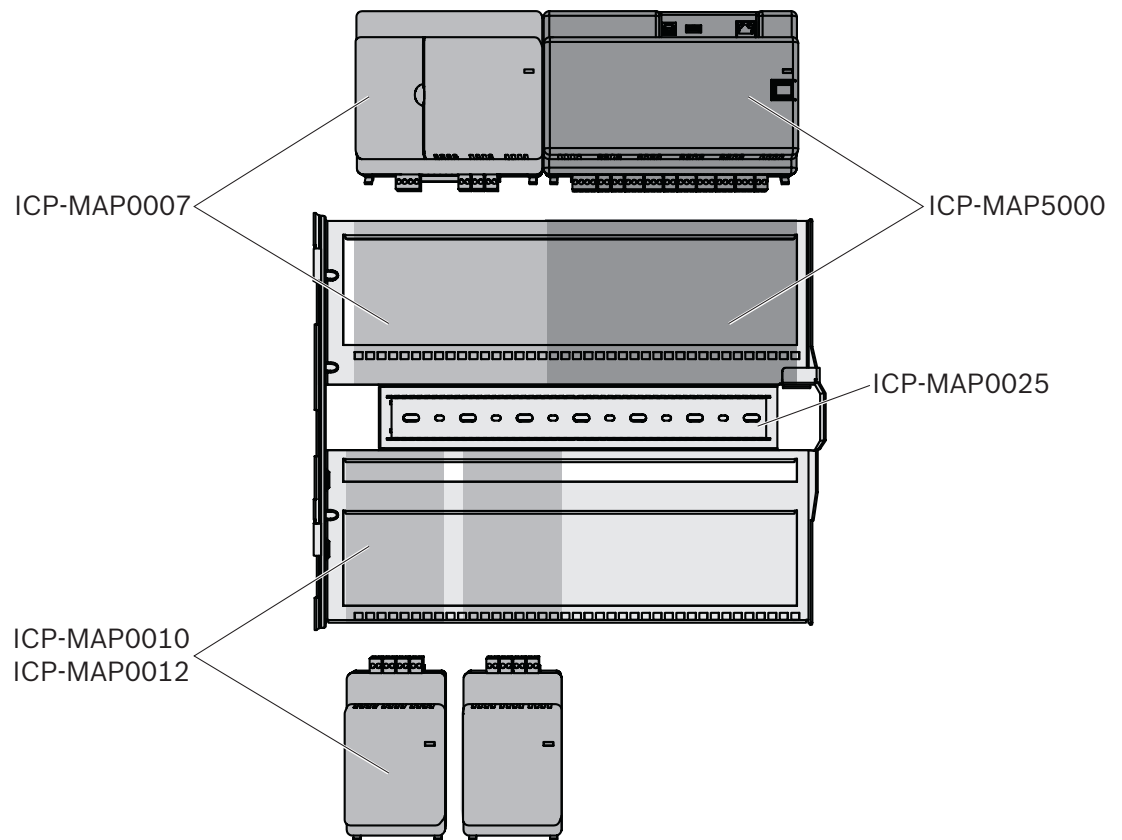
1. Slide the module onto the hinged mounting plate.
2. Ensure that the locking clips snap into a pair of rectangular openings on the bottom rail.

MAP 5000　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　Installation | en　**35**

Sliding the module onto the hinged mounting plate
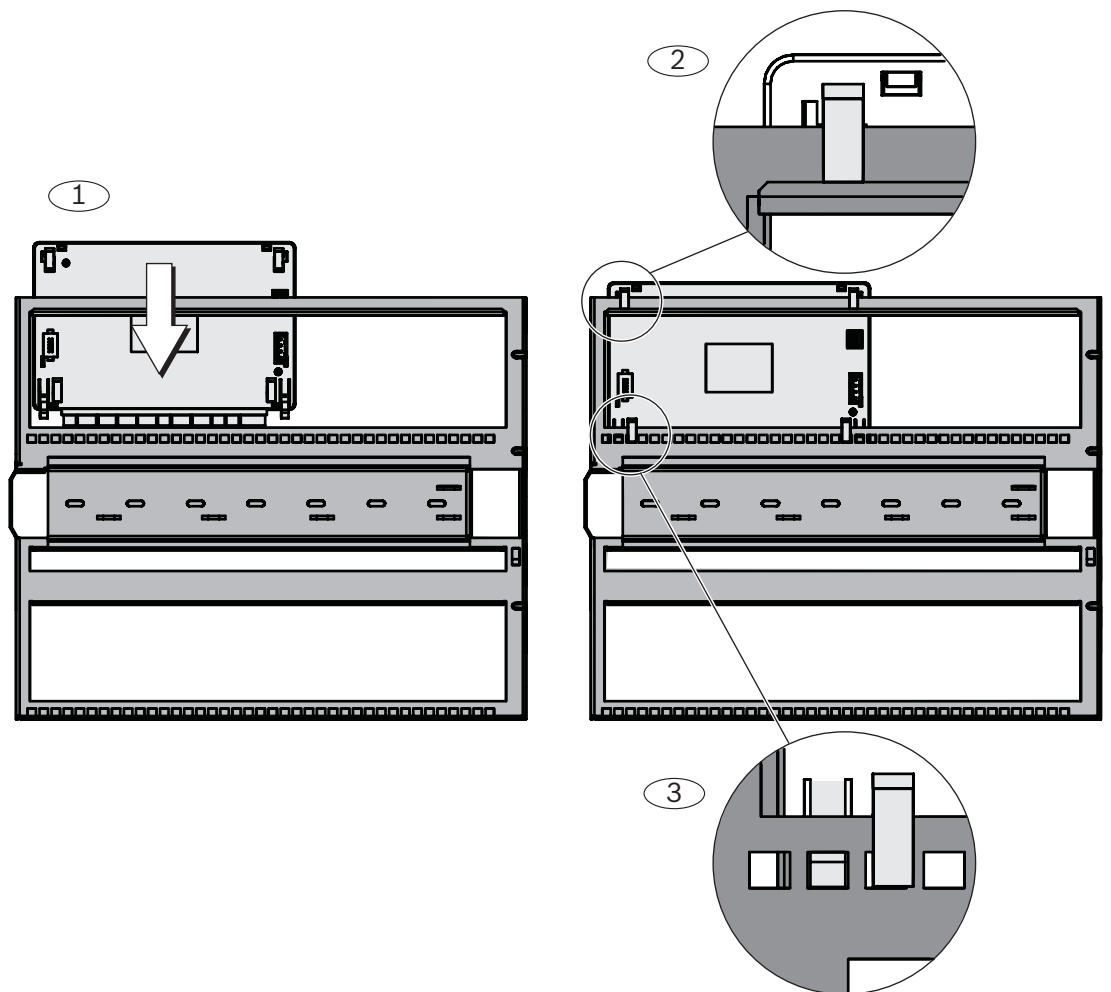
▸　Connect the grounding cable from the enclosure back wall to the hinged mounting plate.

Connecting the grounding cable to the hinged mounting plate
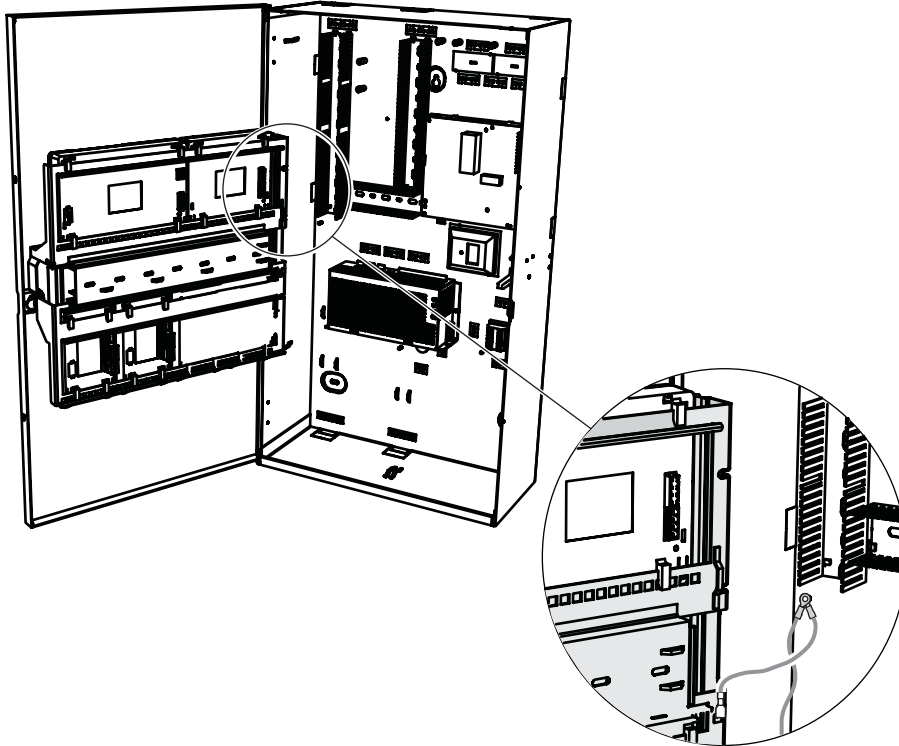
2.12 Mounting the main panel

This chapter describes the mounting of the following main panels:
– MAP Main Panel (ICP-MAP5000-2)
– MAP Main Panel with IP Communicator (ICP-MAP5000-COM) including the MAP GSM module (ITS-MAP0008).
– MAP Main Panel Small (ICP-MAP5000-S)
– MAP Main Panel Small with IP Communicator (ICP-MAP5000-SC) including the MAP GSM module (ITS-MAP0008).

How to mount the main panel
The main panel is mounted on the hinged mounting plate.
For information on how to mount modules on the hinged mounting plate, refer to *Installing the hinged mounting plate, page 33*.

Ethernet cable
The Ethernet cable is used to provide a connection via Open Intrusion Interface (OII) to a management system.
The Ethernet cable can alternatively be used for IP communication if one of the following main panels is installed:
– MAP Main Panel with IP Communicator (ICP-MAP5000-COM)
– MAP Main Panel Small with IP Communicator (ICP-MAP5000-SC)
For IP communication via an integrated IP communicator the following protocols are available:
– VdS 2465-S2
– SIA DC-09 (TCP/IP and UDP/IP)
– Conettix IP

How to mount the Ethernet cable
1. Feed the Ethernet cable through the large snap ferrite sleeve (supplied in the accessory pack of the main panel) with an additional turn.

MAP 5000   Installation | en   **37**

2.   Position the ferrite core as close as possible to the enclosure knockout inside the enclosure.

Ferrite core

2.13   Installing the ICP-COM-IF relay module

The ICP-COM-IF relay module can be mounted on the hinged mounting plate or the mounting rails of the MAP control panel enclosure.
A clearance of approx. 15 mm is required on either side for subsequent wiring. The terminal plugs can be unplugged laterally.
1.   Attach the carrier plate of the ICP-COM-IF relay module in the holes provided in the hinged mounting plate or the mounting rails.
2.   Use the screw provided to secure the carrier plate to the bottom rail.

Installing the ICP-COM-IF relay module
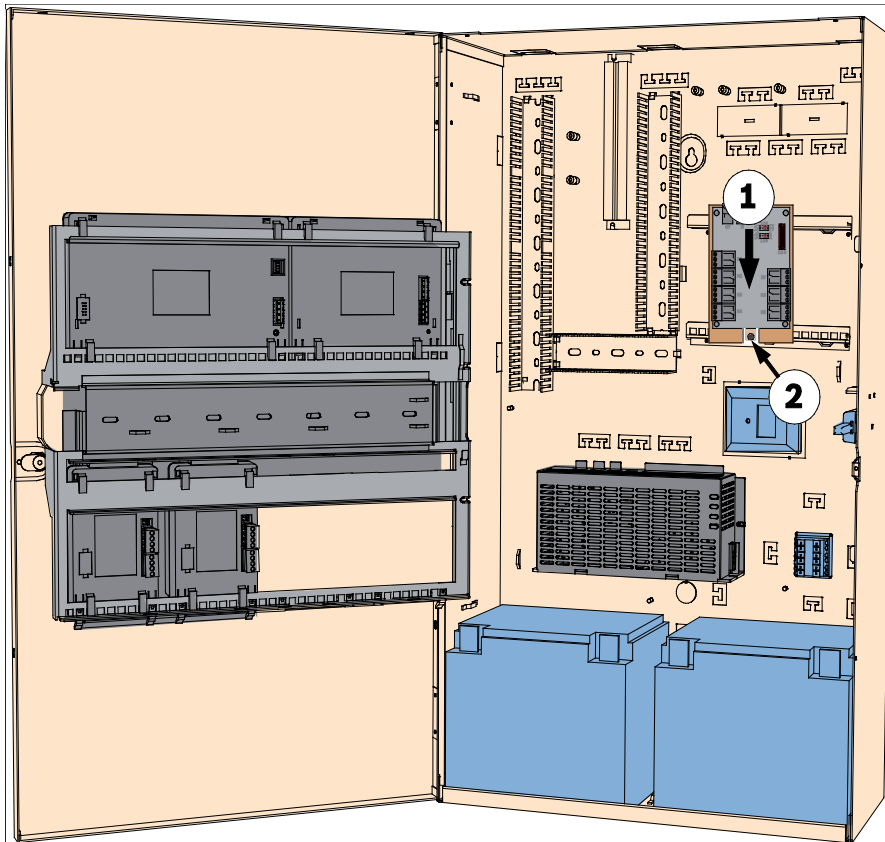
2.14   Installing and connecting the ITS-MAP0008 wireless modem

The ITS-MAP0008 wireless modem is used for wireless transmission of data via GSM/GPRS.
The ITS-MAP0008 wireless modem can only be used when one of the following main panels is installed:

–   MAP Main Panel with IP Communicator (ICP-MAP5000-COM)
–   MAP Main Panel Small with IP Communicator (ICP-MAP5000-SC)

The ITS-MAP0008 wireless modem is designed to provide the interface to GSM network to the MAP Main Panel in order to realize an integrated dual-path SPT type Z with MAP5000 according to EN 50131-10 and EN 50136-2.
The ITS-MAP0008 wireless modem is not capable of working as a standalone SPT without the connection to the MAP Main Panel.

How to install and connect the ITS-MAP0008 wireless modem
The ITS-MAP0008 wireless modem is mounted on the enclosure back wall by means of two screws (supplied with the enclosure). This means that there is no mounting location for an LSA+ strip.

1.   Insert the SIM card. Slide the card in from the top fully (card holder on the rear side of the wireless modem) until it clicks into place. Pay attention to the insertion direction.
2.   Using the cable ICP-MAP0152, connect the 9-pin SUB-D plug to the COM 1 connection of the ICP-MAP0007 DE module (not supplied).
3.   Connect the antenna to the FME female connector of the wireless modem.
4.   Connect the black-red cable at output A or B of the power supply (terminal B = black, terminal R = red), in addition to existing wires where appropriate.
5.   Mount the small snap ferrite sleeve (contained in the accessory pack of the main panel) on the black-red cable of the wireless modem close to the wireless modem.

MAP 5000   Installation | en   **39**

> **Warning!**
>
> In order to avoid data loss on the SIM card, the wireless modem must be de-energized before inserting or removing the SIM card.

Installing and connecting the ITS-MAP0008 wireless modem
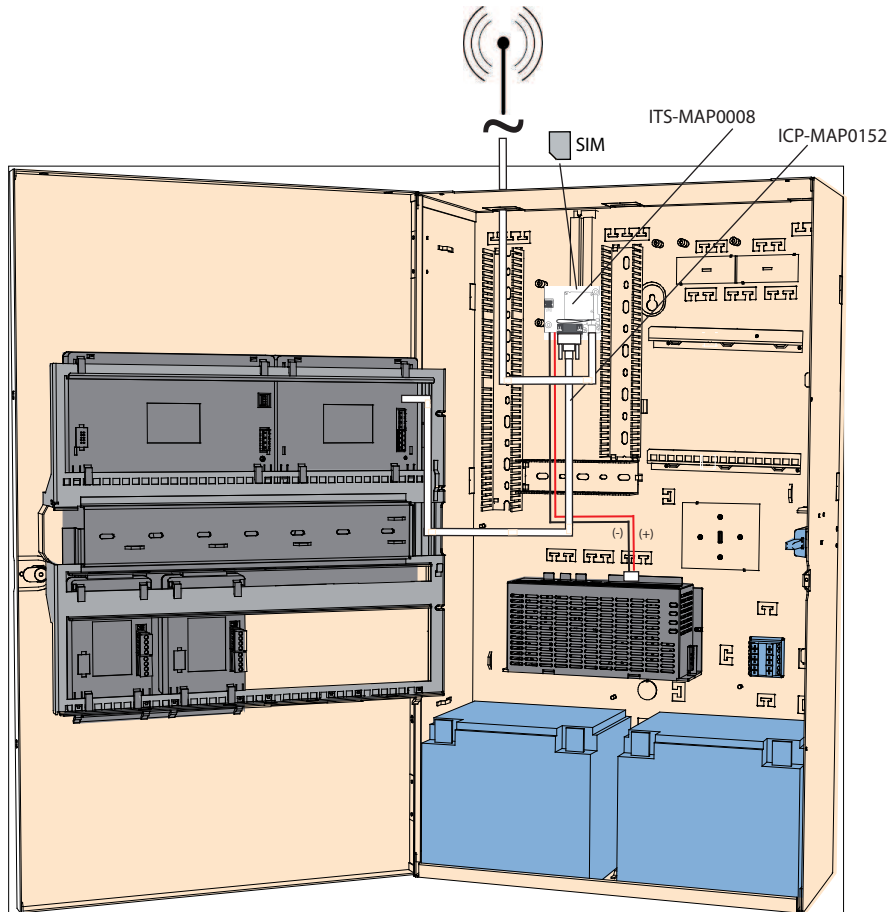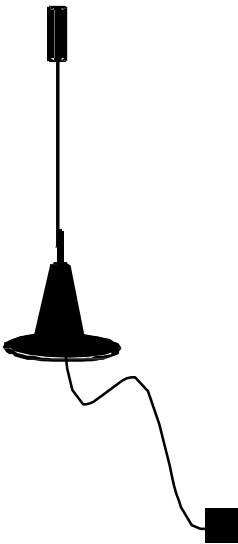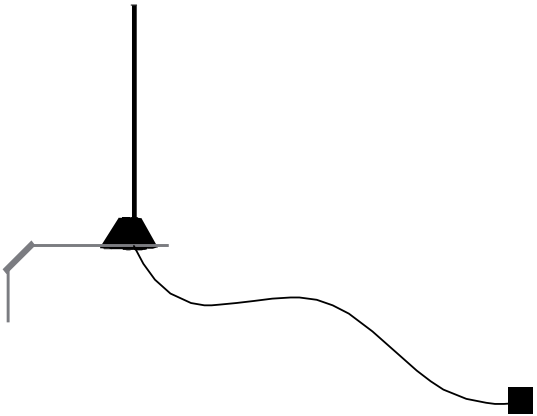
LED operating status

LED mode	Operating status of M terminal
Permanently off	M terminal is in one of the following modes: – Power down – Alarm – Non-cycling sleep – Cyclic sleep with no temporary wake-up event1 in progress
600 ms on, 600 ms off	Limited network service due to one of the following: – No SIM card inserted – No PIN entered – Network search in progress – Ongoing user authentication – Network login in progress
75 ms on, 3 s off	Idle mode: The mobile is logged to the network (monitoring control channels and user interactions). No call in progress.

LED mode	Operating status of M terminal
75 ms on, 75 ms off, 75 ms on, 3 s off	One or more GPRS contexts activated.
500 ms on, 25 ms off	Packet switched data transfer in progress.
Permanently on	Depending on type of call: – Voice call: Connected to remote party – CSD call: Connected to remote party or exchange of parameters while setting up or disconnecting a call

2.15 Antennas

Magnetic antenna mast incl. bottom[1]	
	Transmission frequency: 900 / 1800 MHz Impedance: 50 Ω Gain: 0 dBi Max power: 10 W Radiator length: 100 mm Foot: 34 mm
Magnetic antenna mast incl. bottom with 2.6 m cable. The FME female connector is preconfigured on the coaxial cable.	
Rod antenna	
	Transmission frequency: 900 / 1800 MHz Impedance: 50 Ω Gain: 3.5 dBi (without cable) Max. power: 20 W Radiator length: 250 mm Distance radiator-installation surface: 150 mm Area of use: inside, outside
Rod antenna incl. 20 m cable. The mounting bracket is designed for mounting on vertical surfaces, the FME female connector is preconfigured	

1) not for VdS

MAP 5000   Connections | en   **41**

3   Connections

⚠	**Caution!** Wiring Pinching of the wires is possible due to incorrectly hinged components.

–   Ensure that there is sufficient slack in the service wire loop to allow proper movement of
     the hinged mounting plates.
–   Ensure that the wiring to and from components on the hinged bracket is properly secured
     to the hinged mounting plates.
–   Ensure strain relief by means of the T cutouts.

Permitted cable types
For all MAP components and for all connections, only shielded cables are permitted.
▸   Ensure to connect the shield to the grounding studs.

⚠	**Caution!** Wrong cable type Using a wrong cable type can lead to malfunction of the system.

–   Use shielded cables only.

3.1   Connecting the data bus

To assist with cable connections, the terminal blocks on each system module are color-coded.

Terminal block color codes

Color	Description
White	Auxiliary power
Black	AC / battery
Blue	Inputs / tamper
Orange	Outputs
Yellow	DR2020 printer (ICP-MAP0007 only)
Brown	LSN data (ICP-MAP0010 only)
Green	Data bus

Connecting the data bus
1.   Connect the system modules via the data bus.
2.   Always use the main panel as the first device on the data bus. The 120 ohm end
      terminator is already installed on every data bus.
3.   Connect a 120 ohm end terminator to the last device on each data bus.

Data bus connections of the system modules on the internal BDB

ICP-MAP5000   ICP-MAP0007

← B

P/N: F01U074760

← A

P/N: F01U074769

ICP-MAP0010

A   B

IPP-MAP0005

P/N: F01U074761

120 Ω
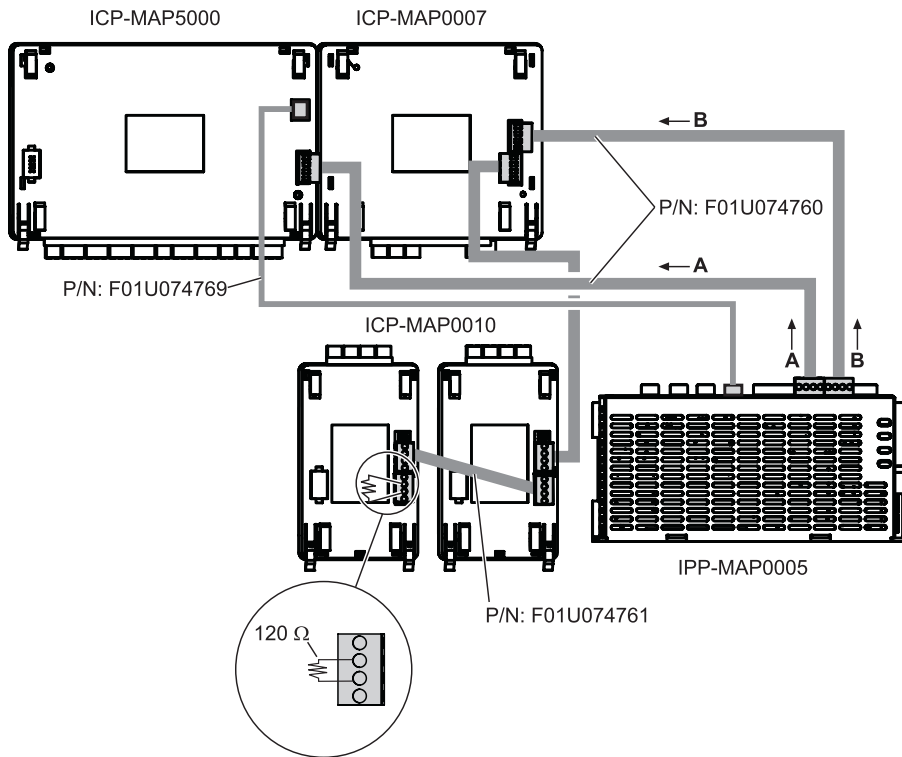
Notice!

The order of system modules on the BDB shown in the figure is not mandatory. A symmetrical load distribution to the power supply outputs A and B must be ensured as far as possible.

Data bus cable routing

120 Ω

MAP 5000

Connections | en   **43**
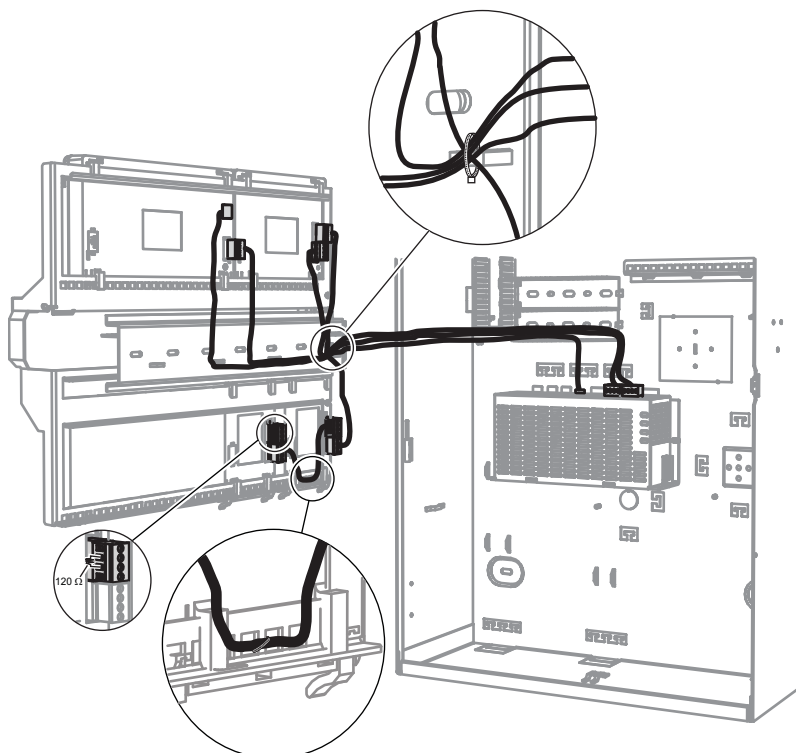
3.1.1 Internal / external data bus

The MAP 5000 system contains two data buses (BDB), which are used to connect the system modules to the main panel.

Internal BDB

The maximum length of the internal BDB is 3 m.

It is used for connecting the main panels in the control panel enclosure (*Data bus connections of the system modules on the internal BDB, page 42*).

External BDB

The maximum length of the external BDB is1000 m from the main panel.

It is used for connecting system modules in remote operation.

Requirements for data bus wiring

There are no special requirements concerning the following:

– Solid or stranded
– Twisted or untwisted
– Shielded or unshielded

The minimum wire diameter is determined on the basis of the required cable length:

– 0.6 mm up to 450 m
– 0.8 mm up to 750 m
– 1.0 mm up to 1000 m

Modules on the BDB

System module	Internal BDB	External BDB
DE module (ICP-MAP0007)	X	
LSN gateway (ICP-MAP0010)	X	X[1]
CAN splitter (ICP-MAP0012))		X
Power supply (IPP-MAP0005)	X	X
Control center (IUI-MAP0001)	X[2]	X[2]

[1]When one or more LSN gateways are operated remotely, there must be one power supply (IPP-MAP0005) installed in the same enclosure.

[2]The following applies for VdS: Control centers for different areas must not be connected on the same BDB.

3.1.2 Topology of the external data bus

▸ Mount the external BDB as shown below.

Notice!

Any other bus topology doesn't conform to the specifications of the BDB.

Bus wiring without consideration of the power supply
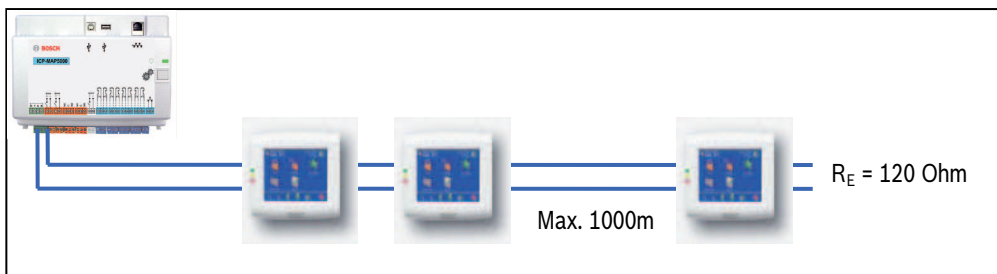
3.1.3   Splitting the external data bus with a CAN splitter module

The external BDB can be splitted into two independent and isolated stubs to connect keypads, gateways and further power supplies. This way, flexible wiring into different directions with up to 500 m cable length as well as a higher reliability can be achieved. For information on installing a CAN splitter module, refer to the correspondent installation manual and datasheet.

CAN splitter module wiring without consideration of the power supply
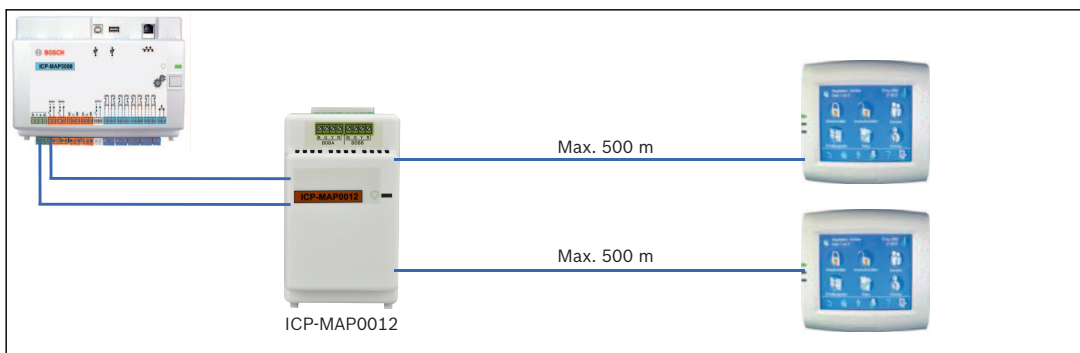
See also

3.2   Connecting the control center

The BDB supports up to 32 control centers. The power supply of remote control centers can be ensured with the expansion enclosure (power supply application).

VdS programming instruction

▸   Only assign one area (where applicable with overlapping dependent partition areas) to a control center.

Exception:

Mutually independent areas may be assigned to the control center of the control panel area.

Data bus connection of the control center on the external BDB
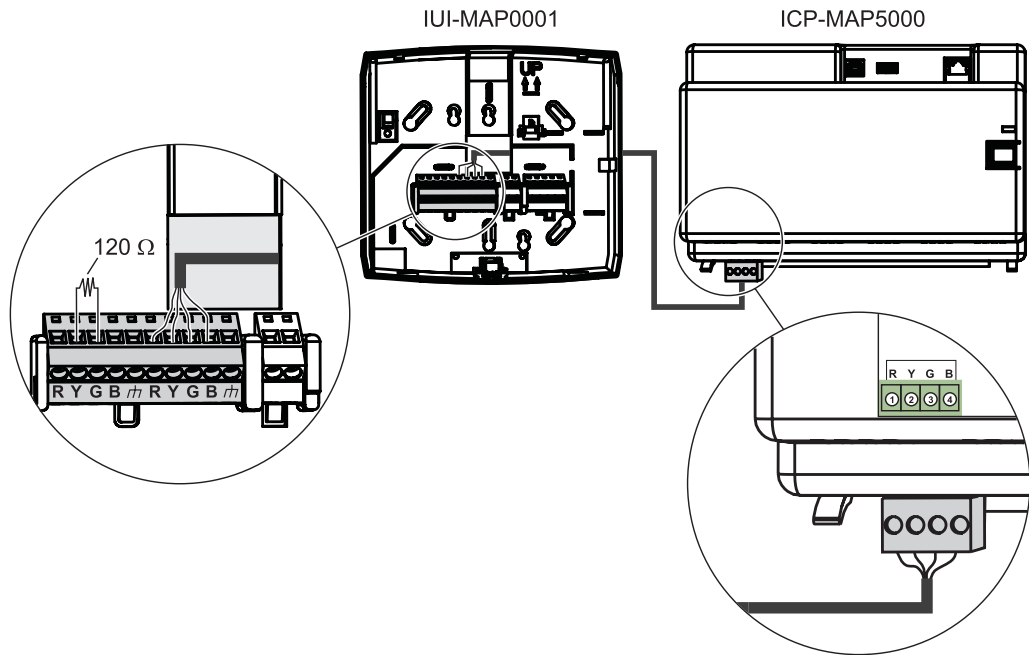
3.3 Connecting the main panel

This chapter describes the connection of the following main panels:

– MAP Main Panel (ICP-MAP5000-2)
– MAP Main Panel with IP Communicator (ICP-MAP5000-COM) including the MAP GSM module (ITS-MAP0008).
– MAP Main Panel Small (ICP-MAP5000-S)
– MAP Main Panel Small with IP Communicator (ICP-MAP5000-SC) including the MAP GSM module (ITS-MAP0008).

Connection strip of the main panel
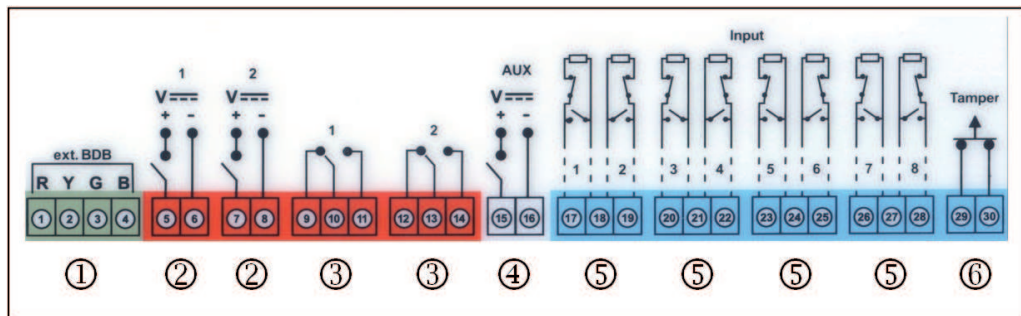
Connection	Description
1	External BDB connector
2	Two programmable voltage outputs (28 V DC / 1 A)
3	Two programmable dry relay outputs (toggle switches)
4	Voltage output AUX (28 V DC / 1 A)
5	Eight supervised inputs
6	Input for panel tamper switch

External BDB connector (1)

▸   Use this connection to connect additional system modules to the external BDB (refer to *Connecting the data bus, page 41* and *Modules on the BDB, page 43*).

Programmable voltage outputs (2)

▸   Use these connections to control devices in certain system states (refer to *Programmable output signals, page 60*).

Programmable dry relay outputs (3)

▸   Use these connections to control devices such as self-powered signaling devices in certain system states (*Programmable output signals, page 60*).

Voltage output AUX (4)

▸   Use this connection to supply voltage to devices in the panel. The voltage can be switched on/off in certain system states.

Supervised inputs (5)

▸   Use these inputs to connect supervised conventional detectors or key switches RE = 12.1 KOhm (refer to *Point types and point evaluation, page 59*).

Input for panel tamper switch (6)

▸   Use this input to connect the tamper switch of the panel (refer to *Connecting the ICP-MAP0050 tamper switch, page 53*).

3.4   Connecting the power supply

1.   Connect the AC terminal block to the power supply.
2.   Connect the power supply to the main panel using the supplied four-pin connector cable (P/N: F01U074769).

Connecting the power supply

Connection	Description

MAP 5000   Connections | en   **47**
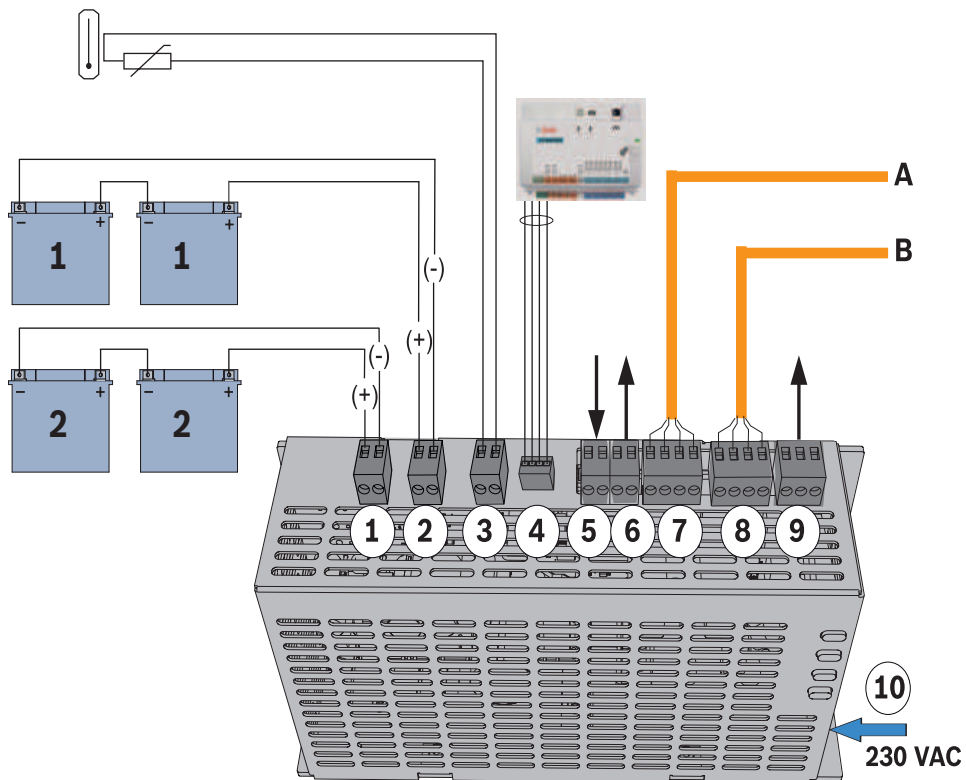
1	Battery circuit 2
2	Battery circuit 1
3	Connection for thermistor
4	Power connection to main panel
5	Input for tamper switch, is activated by configuration for remote operation of the power supply on the external BDB.
6	Output for voltage supply (switched), supervised, nominal voltage 24 V DC
7	Data bus - connection A
8	Data bus - connection B
9	Output for AC fail and summary power supply trouble (optional)
10	AC connection

3.5 Connecting the LSN gateway

Notice!

When connecting an LSN component, ensure that you follow local standards and guidelines when planning the system installation.

The following applies for VdS systems: Each area must be supplied with power independently. The outputs AUX1 and AUX2 on the LSN gateway (for max. two areas) or the voltage outputs of the fuse plate (SIV) (for additional areas) are available for this purpose.

Shielded stub and loop wiring

For both stub and loop wiring, the following additional requirements apply for shielded wires:
– Usage of an additional shielding wire from the central unit
– Routing across the shortest possible distance to the earth terminal
– Looping the shield wire through the LSN elements

Other connections of the additional shielding wire at other locations are not permitted. With loop wiring, the additional shielding wire must be connected at both loop ends.

LSN gateway loop configuration

ICP-MAP0010

ICP-MAP0111

MAP 5000   Connections | en   **49**
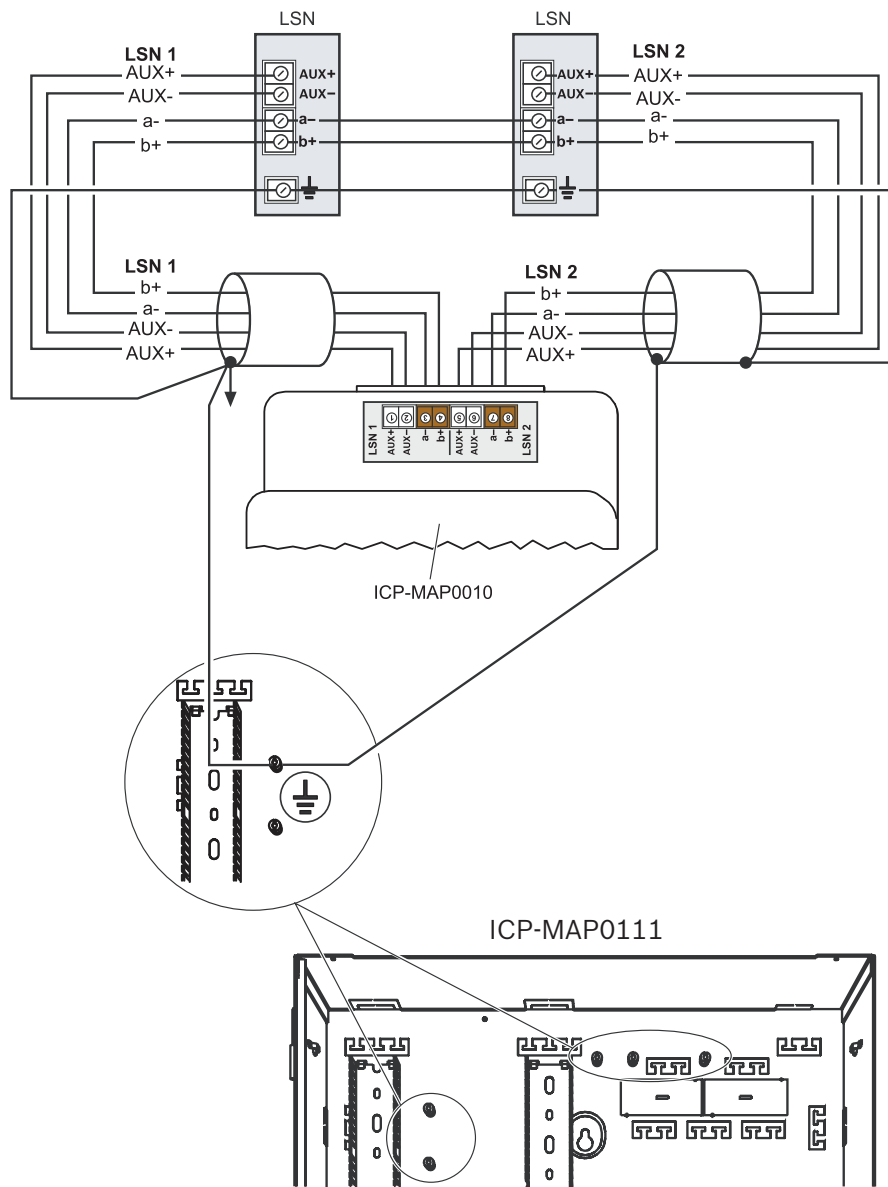
LSN gateway stub configuration

ICP-MAP0010

ICP-MAP0111
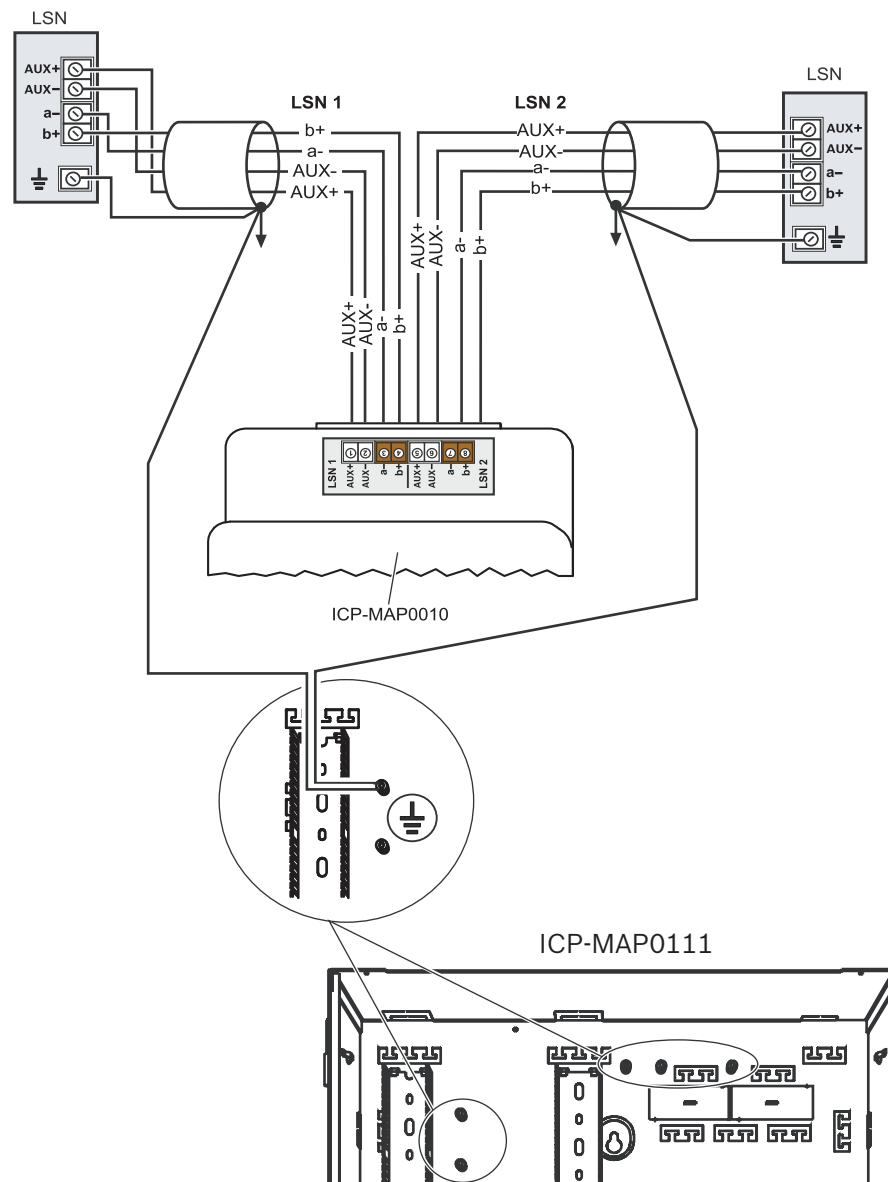
3.6 Optional connections

Optional power supply connections

1. Connect the auxiliary DC power for the 12 V converter.
2. Connect the supervision outputs. The supervision outputs monitor AC mains failure and summary power supply trouble.

Connecting the power supply
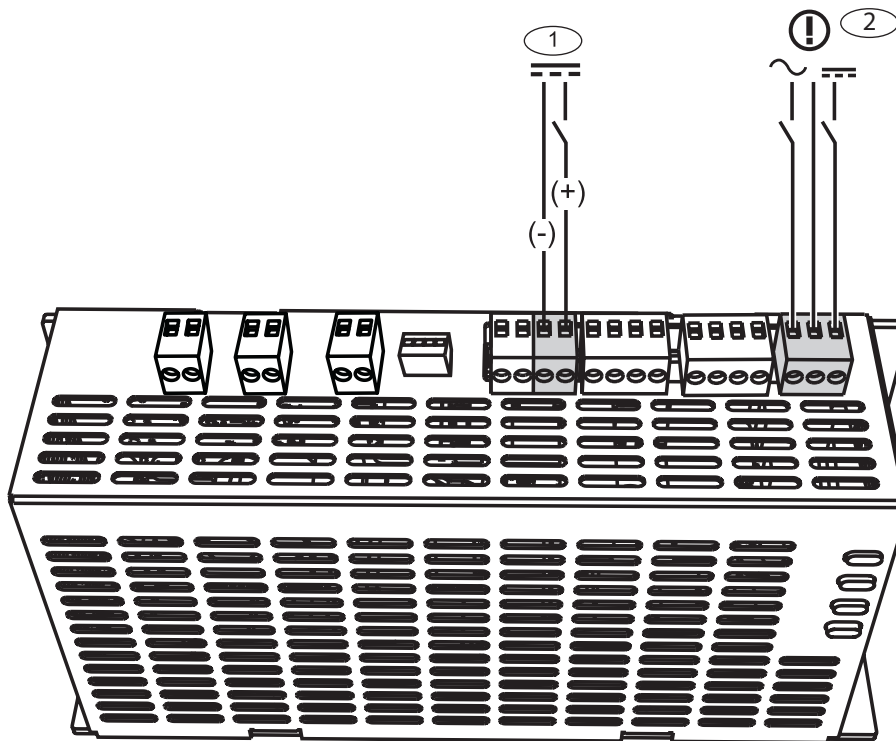
Optional DE module connections
1. If a DR2020 printer is used, connect the DE module to the DR2020.
2. Connect the supervised sirens and strobes to the DE module outputs.

MAP 5000   Connections | en   **51**

Connecting the DE module
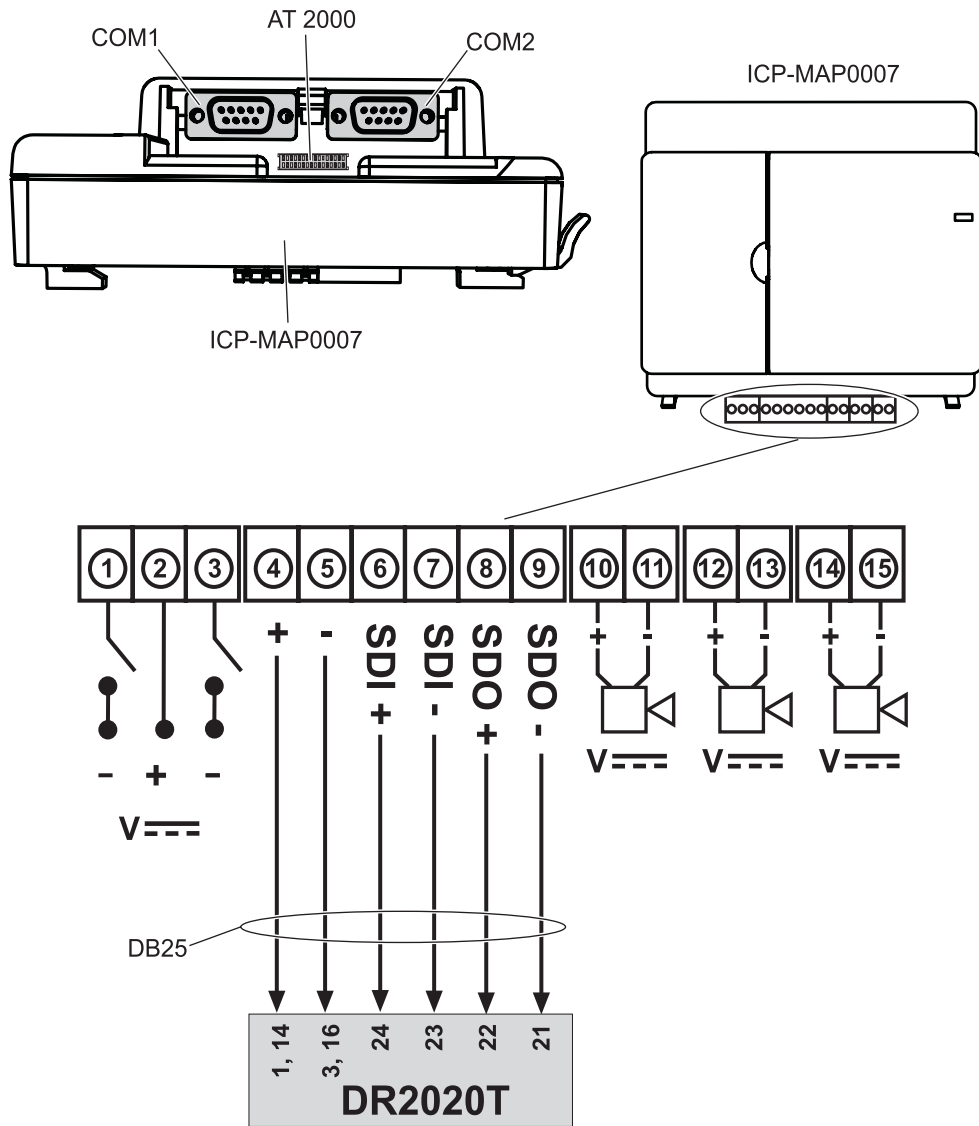
3.7   Installing and connecting the tamper switch

–   Install the ICP-MAP0050 control panel enclosure tamper switch in the ICP-MAP0111 panel
enclosure.
–   Install the ICP-MAP0055 expansion enclosure tamper switch in the ICP-MAP0120
expansion enclosure.

Installing the tamper switch onto the rail

▸   Slide the extension piece of the tamper switch to position C as shown in the figure
below.
If a wall tamper plug was installed (refer to *Mounting the enclosure, page 17*), the position
of the expansion piece of the tamper switch must be chosen in a way that lifting the
enclosure off the wall by > 5 mm leads to reliable activation of the tamper switch.

Tamper switch extension piece

ICP-MAP0050
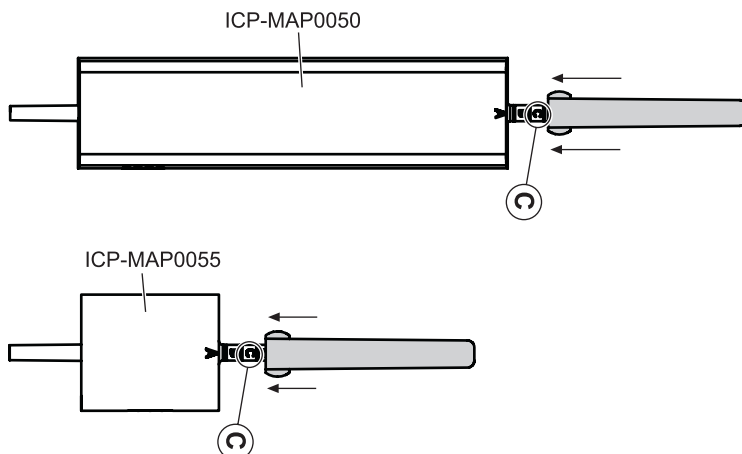
ICP-MAP0055

▸ Slide the tamper switch onto the rail as shown in the figure below.

Mounting the tamper switch onto the rail
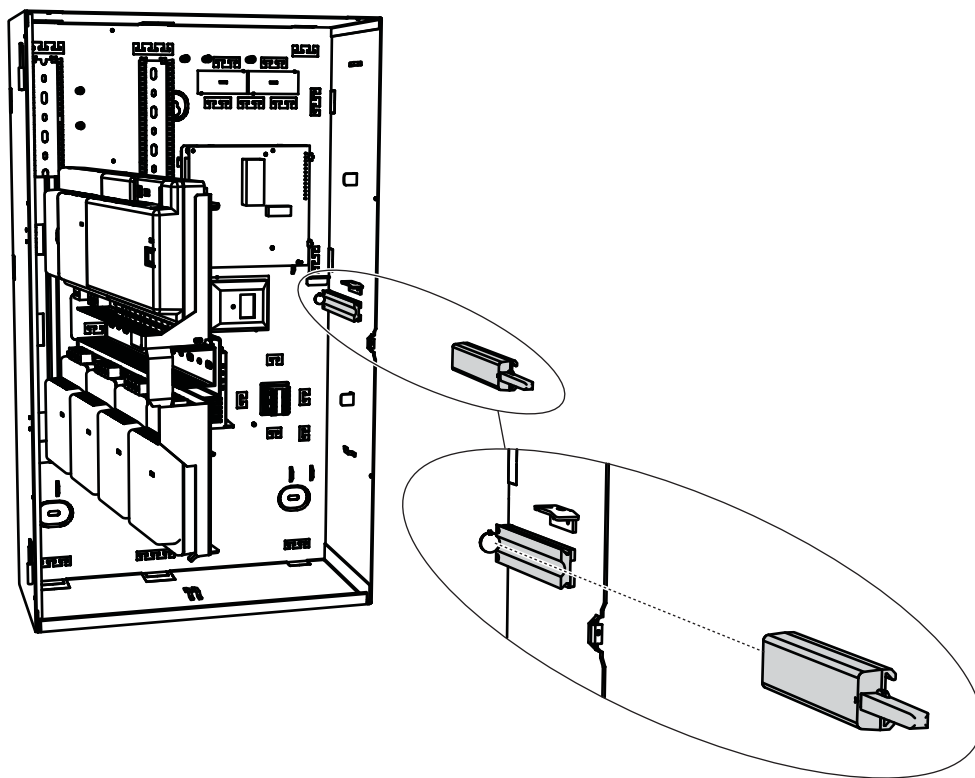
1. Clip off the connector from the cable of the tamper switch.
2. For the ICP-MAP0111 enclosure, connect the ICP-MAP0050 control panel enclosure tamper Switch to the ICP-MAP5000 main panel. Refer to *Connecting the ICP-MAP0050 tamper switch, page 53*.
3. For the ICP-MAP0120 enclosure, connect the ICP-MAP0055 expansion enclosure tamper switch to the ICP-MAP0005 power supply. Refer to *Connecting the ICP-MAP0055 tamper switch, page 53*.

MAP 5000   Connections | en   **53**

Connecting the ICP-MAP0050 tamper switch

ICP-MAP5000

ICP-MAP0050

Connecting the ICP-MAP0055 tamper switch

ICP-MAP0055

IPP-MAP0005
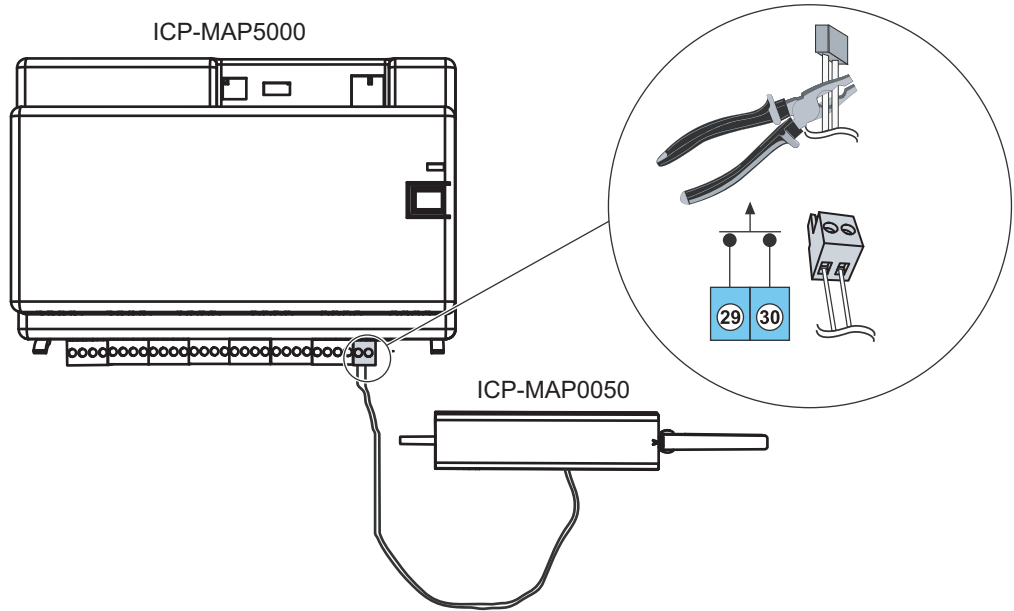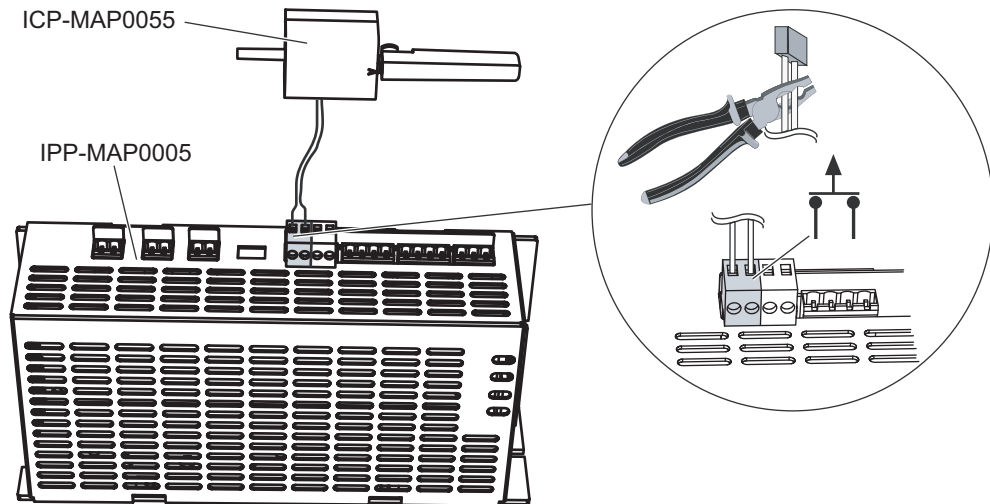
Notice!

When the enclosure door is opened, the tamper switch creates a tamper condition. To allow for a local connection between RPS and the ICP-MAP5000 panel, connect the tamper switch to the panel and not the power supply. The ICP-MAP5000 panel only allows system parameter changes via RPS if the panel tamper switch input is in open state.

3.8   Installing the ICP-MAP0060 enclosure lockset

1.   Remove the lockset knockout from the enclosure door as shown in the figure below (1).
2.   Insert the lockset into the opening on the enclosure door as shown in the figure below (2).
3.   Secure the lockset with the nut as shown in the figure below (3).

Installing the enclosure lockset
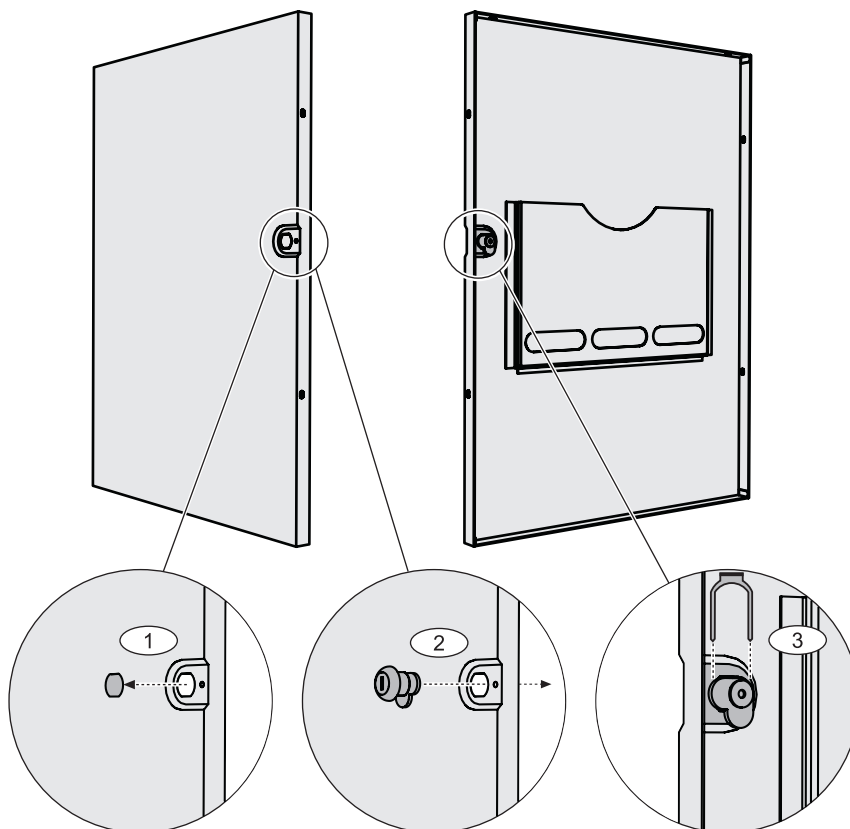
▸ Connect the long grounding cable (P/N F01U074762) to the enclosure door.

Connecting the grounding cable to the enclosure door

MAP 5000

Connections | en   55
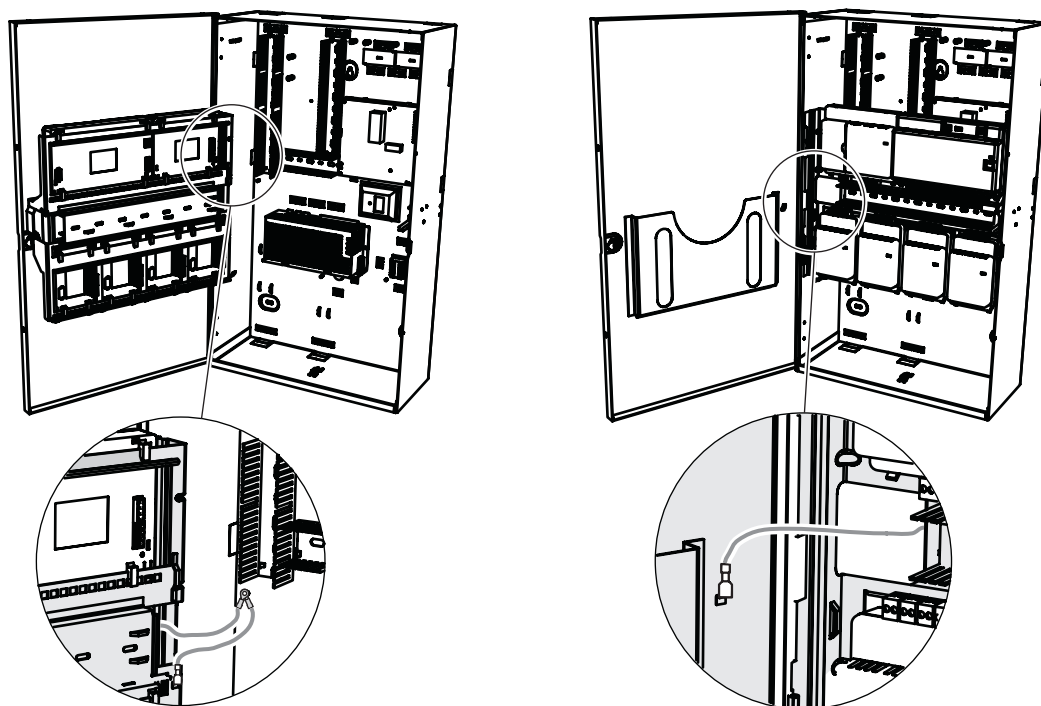
3.9   Installing the control center

Mounting location

Mount the control center onto the wall so that the user interface is at a comfortable level for the end user. Typical installations of the touchscreen are at shoulder level, which is approximately 150 to 160 cm (59 to 62 in) above the floor. It must be guaranteed by corresponding positioning of the control center or by organizational measures that only the user has an optimum view of the touchscreen.

Mounting the control center

1.   Unlock the control center base and remove the cover.
2.   Use the control center base to mark the holes on the mounting surface.
3.   Refer to *Data bus connection of the control center on the external BDB, page 45* for wiring instructions.
4.   Replace the control center cover on the base.
     The cover automatically locks to the base.
5.   Secure the cover using the two screws M3 x 20 mm (F.01U.172.636).
6.   The fed-in cable must be provided with strain relief.
7.   The adhesive seal must be attached after completion of all work.

Opening the control center
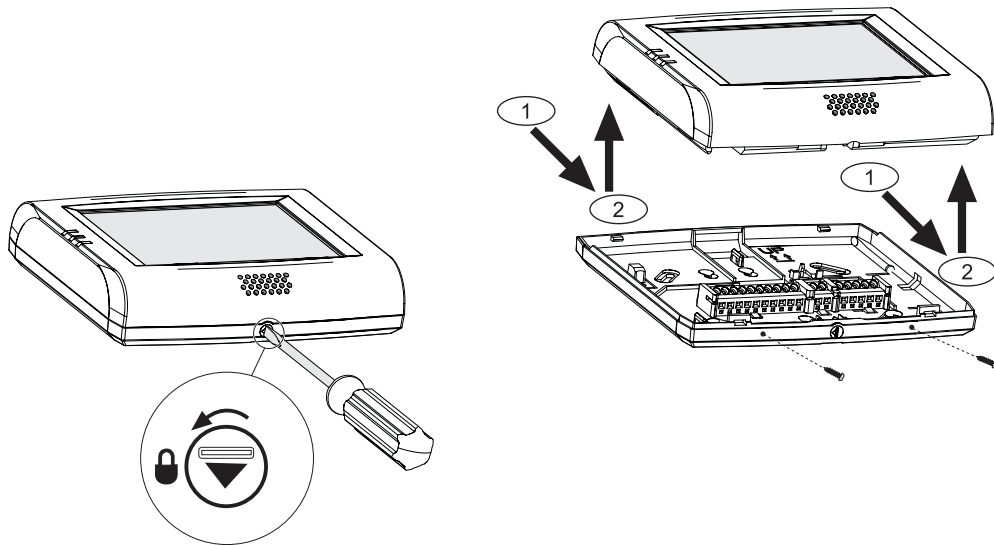
3.10   Final power connections

1.   Connect AC wires to the AC terminal block.
2.   Connect the battery wire leads to the batteries.
     Do not connect the batteries to the power supply at this time.
3.   Switch the AC breaker on.
4.   Ensure that there are no power-related trouble conditions.

> **Warning!**
> Ensure that the AC LED indicator on the power supply turns on steady before you connect the battery terminal to the power supply.

> **Warning!**
> Remove the protective dust cover label from the top of the power supply.

3.11   IP Interface

Ethernet connector
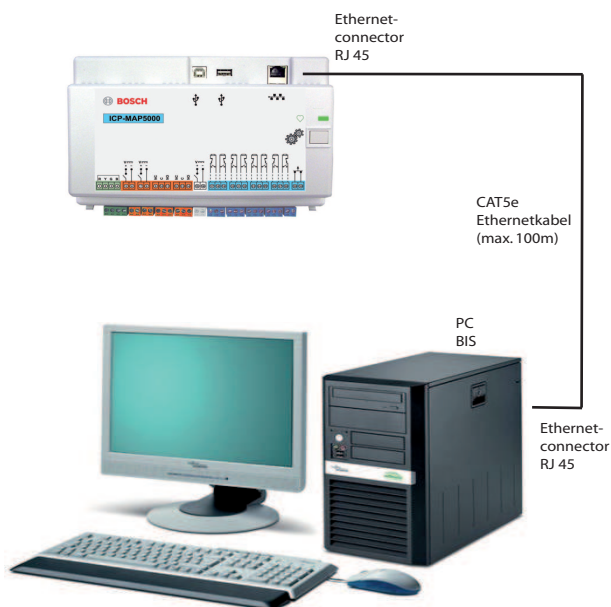
Ethernet cable type: CAT5e

VdS and EN50131: The usage of the MAP 5000 Ethernet interface is permitted if the following conditions are met.
1.   Use a direct connection (1:1 connection) for connecting the management system to MAP5000.
2.   When using repeaters (switches), ensure that no other network components are connected to the repeaters.
3.   For operation of the management system, restrict the data transfer from MAP5000 to the management system. Ensure that this does not have any influence on the panel.

VdS and EN50131 programming instruction
Settings in **RPS for MAP**:
▸   In the MAP5000 panel menu, select -> **setup: Management system as a Monitoring Station**.

> **Notice!**
> Data transfer between the MAP 5000 and the connected PC system must always take place via a secure, authenticated and encrypted connection.

MAP 5000   Initial set-up and programming | en   **57**

4   Initial set-up and programming

4.1   Initial set-up

First check the following before initial set-up:
–   Are all cables connected correctly?
–   The power supply is always in operation after the AC mains has been connected and the
     AC breaker switched on.

i	**Notice!** Remove the protective dust cover label from the top of the power supply.

Final power connections
1.   Switch the AC breaker on.
2.   Ensure that there are no power-related trouble conditions.
3.   Ensure that the AC LED indicator on the power supply turns on steady before you
     connect the battery terminals to the power supply.
4.   Connect the battery cable leads to the batteries and the power supply.

!	**Warning!** Injury due to electricity Risk of injury in the event of short circuit. Ensure the correct polarity!

Connecting the batteries
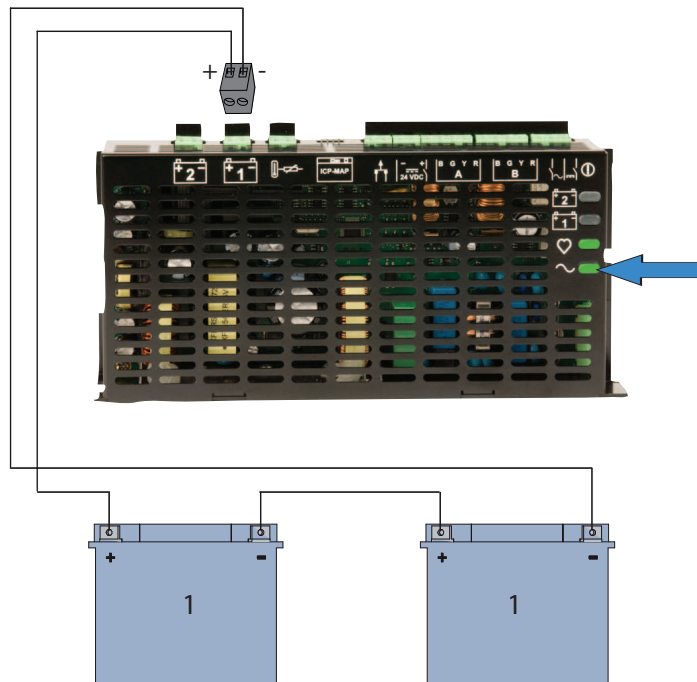
4.2   Programming

Programming is performed with the program **RPS for MAP**. A PC or laptop with Windows XP
SP3, Windows VISTA or Windows 7 is required for this. At least 256 MB RAM is needed. A
mouse is recommended for operation of the program.

Installing the programming software
1. Insert the CD in the drive and start the installation process by double-clicking on the **setup.exe** file in the **RPS** directory.
2. Follow the instructions of the installer.
✓ RPS for MAP will start automatically after installation has been completed successfully.

Logging on for the first time
The dialog box login information is displayed when the program is started for the first time after installation.
1. Enter **admin** as user name and **default** as password.
2. After successful login, the administrator password and language can be changed. To do this, change to the tab **Administration > Operators**.
✓ The password **default** is deactivated if the administrator password is changed.

4.2.1 Help for the programming software

All instructions and explanations for programming are provided online, i.e. directly on the screen.

Help texts in the properties info bar
If you mark a parameter in the **Properties** field on the **Main Page** tab, a short explanation will be displayed in the **Properties Info Bar** underneath.
Detailed information is available by pressing the F1 function key on your PC keyboard.

Help texts in the contents overview
The complete programming process with all operating steps is described in the contents overview.
▸ Click on the ? button.

4.2.2 Standard-compliant programming

If you want to perform standard-compliant programming, select the following settings in RPS before you start programming.
1. Click on the yellow RPS button and create a new panel account with the **New** button.
2. In the **Hardware Manager**, click on the **MAP 5000 Panel** node and then in the Properties field on the parameter **Default Property Values Set** and select the standard that you want to program.
3. Right-click on any parameter on the left side of the Properties window.
4. Select **Restore all properties using <selected standard> default property values set**. Confirm with **Yes**.

Compliance check / validation
During programming, you can check whether programming is compliant with the selected standard at any time.
▸ Click on the **Panel Validation** button.
✓ Any errors found will be displayed in the **Error List** window in plain text.

4.3 Panel software

Fault-free operation of the panel can be guaranteed only if **all** system modules of the panel and programming software comply with the manufacturer's specifications.

4.3.1 Checking the software version

After first start-up, you need to check whether the software versions of all system modules and the programming software are compatible with each other (refer to MAP 5000 system bundles).

MAP 5000   Initial set-up and programming | en   59

1. Make a connection to the panel.
2. Click on the **MAP 5000 Panel** node.
    The software version is displayed in the Properties field under **Control Panel Firmware Version**.
3. Click successively on the system modules in the **Hardware Manager**.
    The software version is shown in the diagnostics field under **Software Version**.
✓   The version of the programming software **RPS for MAP** is displayed during start-up or under **RPS Start>RPS Options>Resources**.

4.3.2   Software updates

All system modules are updated by means of the programming software **RPS for MAP**.

▸   To carry out updates, follow the instructions in the file **How to update** ... on the manufacturer's CD.

4.3.3   Manufacturer authorization

In order to transfer new software to the system modules with **RPS for MAP**, a manufacturer authorization may be needed on the panel side.

1. Authorize the manufacturer user by a user with corresponding permissions (see operating manual, section **Manufacturer authorization**).
2. Open the control panel enclosure.
3. Activate **Installer Mode** (*Installer button, page 66*).
4. Log on at the Installer Control Center with the manufacturer's passcode. Use the user ID **000** and password **234567** when logging on for the first time. These are entered directly in succession. The manufacturer's password can be changed after successful log-on. The password **234567** is deactivated as a result.

4.4   Completing the installation

1. Stick the type label supplied in the main panel accessory pack on the control panel enclosure at a location that is easily visible from outside.
2. Lock the enclosure door after completing all work.

Systems in accordance with VdS class C and EN 50131

1. On systems in accordance with VdS class C and EN 50131, screw the door closed on the lock side with two sheet-metal screws (3.5 mm x 10 mm) from the accessory pack in order to guarantee sufficient mechanical strength.
2. Fix the adhesive seal on the lock.

4.5   Point types and point evaluation

Overview of the Standard Point Types and their pre-set properties

Point Type	Arming state			Influences ready to arm status
	Disarmed	Internal armed	External armed	
Intrusion	No	Yes	Yes	Yes
Intrusion 24 h	Yes	No[1]	Yes	Yes
Hold-up	Yes	No[1]	Yes	Yes
Duress	Yes	No[1]	Yes	No
Tamper	Yes	No[1]	Yes	Yes
Bolt contact	No	No[1]	No	Yes

Trouble	Yes	No[1]	Yes	Yes
Technical	Yes	No[1]	Yes	No
Fire	Yes	No[1]	Yes	No

[1] Assignment to Internal Program not possible or with no effect

4.6 Output functions

4.6.1 Programmable output signals

The following functions can be programmed at outputs.

p = programmable

Behavior item type	Output is activated for ...
Hold-up alarm	Hold-up (silent) Hold-up (non silent)
Duress alarm	Duress alarm
External intrusion alarm	Intrusion alarm from unoccupied protection area
Internal intrusion alarm	Intrusion alarm from disarmed area with – activated internal program – intrusion alarm 24h
Technical alarm	Technical alarm
External system trouble	Power supply failure (p), battery trouble
Internal system trouble	Power supply failure, ground fault, printer trouble
External intrusion trouble	Detector self test trouble
Internal intrusion trouble	Anti-mask trouble
Technical trouble	Technical trouble
Summary area armed	One or more areas armed externally
Area armed	Area x armed externally
Area disarmed	Area x disarmed externally
Area ready to arm	Area x disarmed and ready to arm
Internal program ON	Internal program x switched on
Chime	Detector has tripped chime, only if chime mode is activated
Monitor (output follows Input)	Shows the actual status of the input: normal / active
Report failure panel alarm (V1.2x)	Panel has received negative acknowledgment from communicator as a result of report failure panel alarm (only for panel firmware 1.2.x)
Report failure intrusion and tamper alarm (V1.2x)	Panel has received negative acknowledgment from communicator as a result of report failure intrusion and tamper alarm (only for panel firmware 1.2.x)

MAP 5000

Initial set-up and programming | en **61**

Report failure summary alarm	Panel has received negative acknowledgment from communicator due to report failure summary alarm
Report failure summary trouble	Panel has received negative acknowledgment from communicator due to report failure trouble
Report failure duress alarm	Panel has received negative acknowledgment from communicator due to report failure duress alarm
Report failure hold-up alarm	Panel has received negative acknowledgment from communicator due to report failure hold-up alarm
Report failure intrusion and tamper alarm	Panel has received negative acknowledgment from communicator due to report failure intrusion and tamper alarm
Report failure panel alarm	Panel has received negative acknowledgment from communicator due to report failure panel alarm
Internal tamper alarm	Tamper alarm from disarmed area
External tamper alarm	Tamper alarm from armed area
Bypass	At least one device is bypassed
Disable	At least one device is disabled
Management system interface trouble	Trouble in connection to management system
Present mode ON	The area programmed as present/absent is disarmed
Blocking time active	Blocking time is active for one or more areas
Wrong login	The maximum number of permitted passcode input attempts on a control center was exceeded
User active	A defined user is logged in at a defined control center
External fire alarm	Fire alarm from armed area
Internal fire alarm	Fire alarm from disarmed area
External fire trouble	Fire device trouble from armed area
Internal fire trouble	Fire device trouble from disarmed area
Walk test	Walk test is active
Motion detector test	Motion detector test is active in one or more areas
Exit delay active	From start of exit delay until – end of exit delay – arming of the area
Entry delay active	From start of entry delay until – end of entry delay – disarming of the area
Reportable duress alarm	Reporting of duress alarm event
Reportable hold-up alarm	Reporting of hold-up alarm event

Reportable external intrusion alarm	Reporting of external intrusion alarm event, possibly also delayed if present/absent option is used
Reportable external tamper alarm	Reporting of external tamper alarm event, possibly also delayed if present/absent option is used
Reportable panel summary trouble	Reporting of panel summary trouble event, possibly also delayed if present/absent option is used
Reportable panel summary armed	Reporting of panel summary armed
Reportable external fire alarm	Reporting of duress alarm event, possibly also delayed if present/absent option is used
Anti-mask intrusion trouble	Covering of a motion detector
External tamper alarm disarmed	Tamper alarm from disarmed area with simultaneous reporting via the communicator
Transmission path fault	In the event of communication failure between communicator and receiver
Ethernet path layer1 fault	In the event of failure of connection to network connector
Wireless path layer1 fault	In the event of failure of connection to network – field strength insufficient – registration not possible – GPRS service not available – no connection to the DE module
IPC reporting failure	No acknowledgment received from the receiver within 240 sec.
S1S Transmission Path Fault	Communication failure between panel and communicator
S1S Reporting Failure	Panel has received negative acknowledgment from communicator
Open Intrusion Interface Trouble	Trouble in connection via Open Intrusion Interface
Silence Area x	Silence sirens and buzzer of area x
Reset Area x	Clear events of area x

4.6.2   Sirens and communicator in accordance with EN50131 grade 3

i	**Notice!** Sirens must be in operation for at least 90 seconds and a maximum of 15 minutes, unless local or national requirements demand a shorter duration.

The following variants are possible:

Variant A (ICP-MAP0007 DE module and ICP-COM-IF required)
–   Two supervised sirens
     Connections 10 / 11 and 12 / 13 on the ICP-MAP0007 DE module)

– One communicator (class 4)
Connections R1 – R7 on ICP-COM-IF

Variant B (ICP-COM-IF required)
– One self-powered siren
Outputs 10 / 11 or 13 / 14 on ICP-MAP5000 main panel
– One communicator class 4
Outputs R1 – R7 on ICP-COM-IF

Variant C (ICP-COM-IF required)
– One communicator class 4 (main communicator)
Outputs R1 – R7 on ICP-COM-IF
– One communicator class 3 (additional communicator)
Outputs R1 – R7 on ICP-COM-IF or other outputs on panel

ⓘ	**Notice!** Both communicators may be connected to the same outputs.

Variant D (ICP-COM-IF required)
– One communicator class 5
Outputs R1 – R7 on ICP-COM-IF

5 Enclosure options

5.1 ICP-MAP0115 power enclosure

ICP-MAP0115 power enclosure connections

ICP-MAP0111

ICP-MAP0130

IPP-MAP0005

ICP-MAP0065

P/N: F0U124597

ICP-MAP0115

(+) (-) (+) (-)

ICP-MAP0130

P/N: F0U124597

BAT1

ICP-MAP0050

BAT2

ICP-MAP0065

IPP-MAP0005

(+) (-) (+) (-)
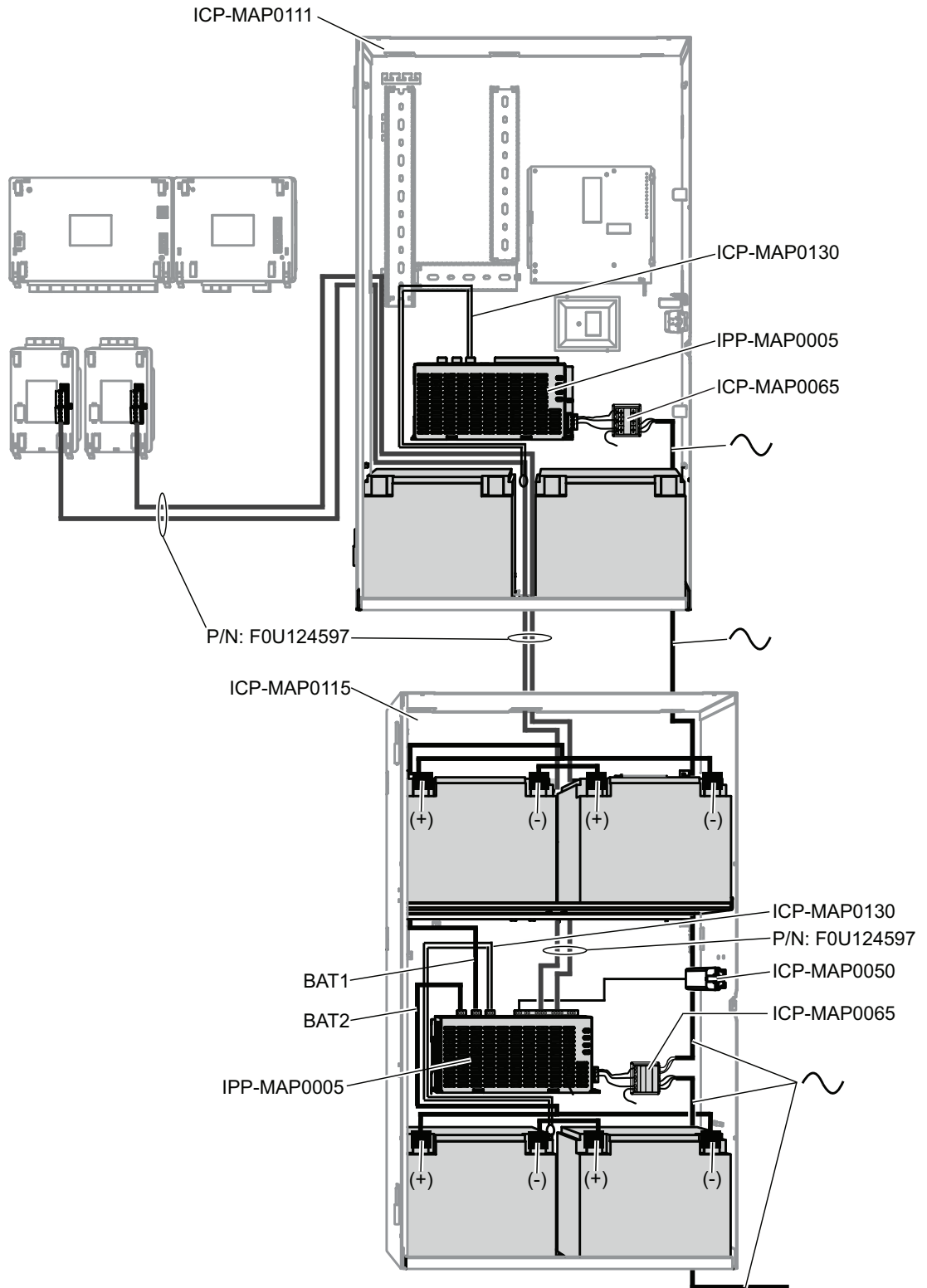
▸ Connect the ICP-MAP0115 power enclosure to the ICP-MAP0111 enclosure to provide additional power when high power capacity is required.

MAP 5000   Enclosure options | en   **65**

5.2   Rack mount option for ICP-MAP0120 expansion enclosure

‣   To install the ICP-MAP0120 expansion enclosure in a 19-inch rack, connect the ICP-MAP0035 rack mount brackets to the ICP-MAP0120 expansion enclosure.

Installing the rack mount brackets to the ICP-MAP0120 expansion enclosure
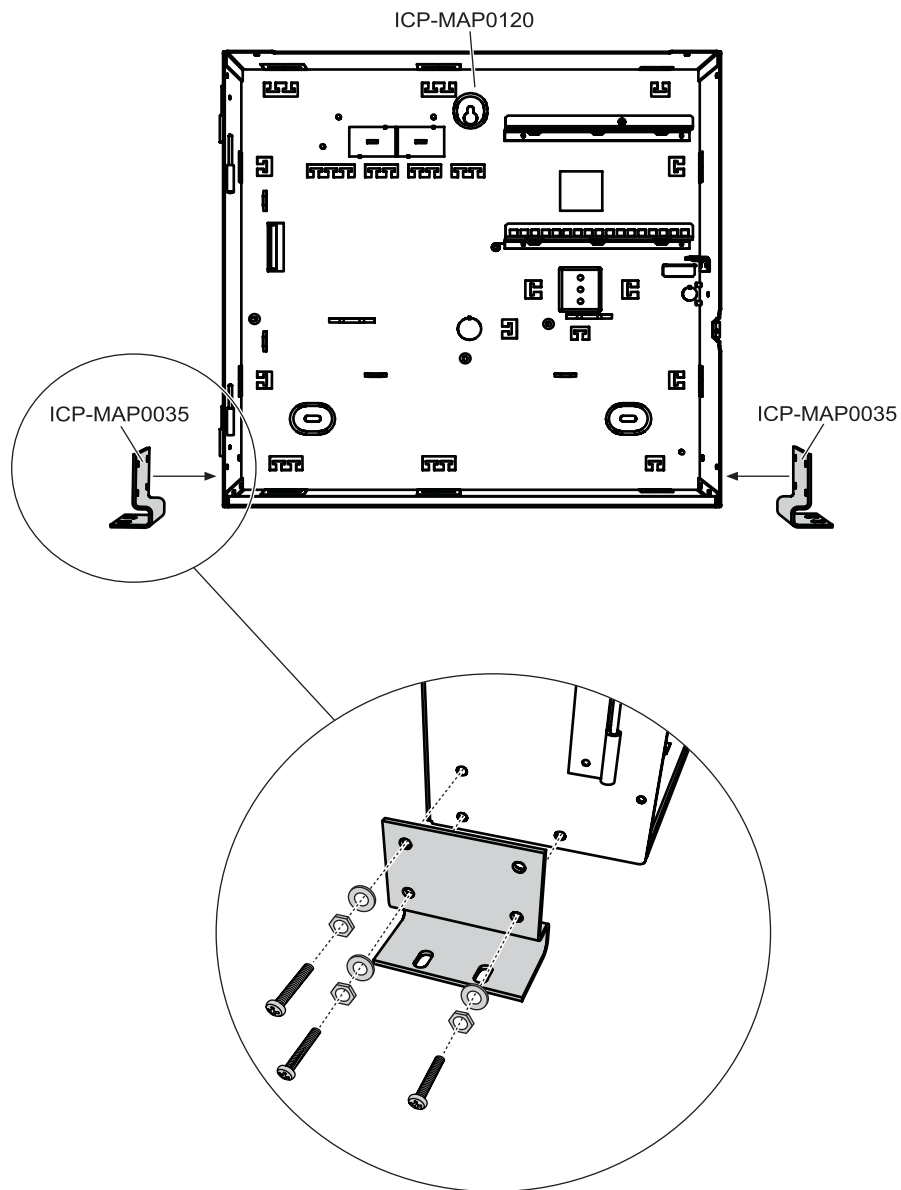
6 Maintenance and service

6.1 General information

Maintenance and inspection work must be carried out at defined intervals and by corresponding expert personnel. The regulations of DIN VDE 0833 apply additionally for all work of this kind.

i	**Notice!** Have maintenance and inspection work carried out regularly by trained expert personnel. Bosch Sicherheitssysteme GmbH recommends performing a functional and visual inspection at least once annually.

⚠	**Danger!** Danger of electric shock if live parts are touched. For your safety, you should switch off the power supply to the security system when carrying out maintenance or installation work!

6.2 Installer button

Using the installer button
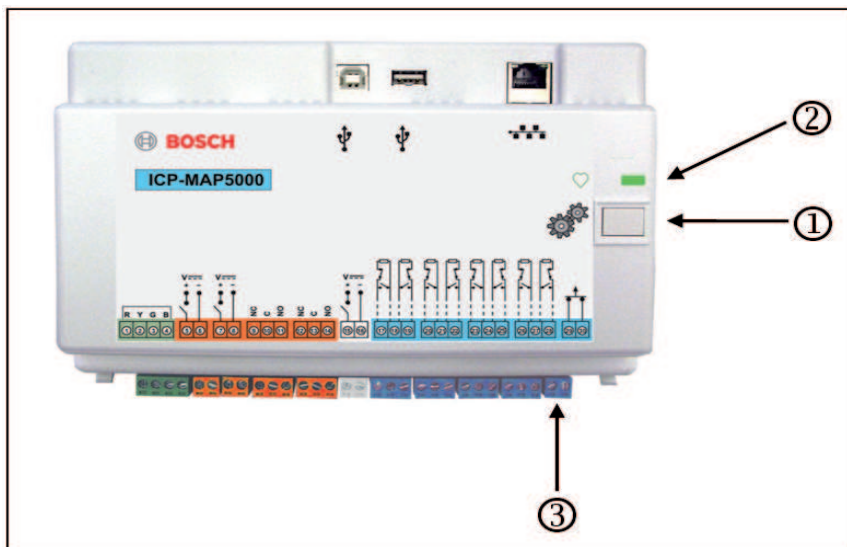
Element	Description
1	Installer button
2	Operating LED
3	Tamper switch

Switching on the installer mode
▶ Press the installer button on the main panel for three seconds.
✓ The operating LED starts blinking slowly to indicate the installer mode.

Switching off the installer mode
▶ Press the installer button on the main panel for three seconds.

System restart
The system can be restarted without being de-energized.
▶ Press the installer button on the main panel for six seconds.
The LEDs on the main panel and all other installed modules stop indicating briefly.

MAP 5000

Maintenance and service | en   **67**

The initialization phase, indicated by a blinking LED, starts.

✓   The LEDs on the main panel and all other installed modules start indicating and the system is ready for operation again.

LED status	Description
Off	No function
Fast blinking	Connection setup
Slow blinking	Data exchange
Permanently lit	Operating state

Restoring the initial state of the panel

1.   Put the panel in **Failsafe mode** (see below).
2.   Update the firmware.

Failsafe mode

Forcing failsafe mode

Programming and panel firmware are deleted and RPS passcode is reset to default settings when executing this option.

1.   Open the tamper switch.
2.   De-energize the main panel (e.g. disconnect the small white connector at the rear of the panel).
3.   Press and hold the installer button.
4.   Connect voltage (e.g. plug in small white connector again).
5.   Release the installer button after 30 seconds.
6.   Wait until operating LED is permanently lit (can take several minutes).
7.   Transfer panel firmware "MAP_Update.Cumulative ...tar.bz2" again using RPS.

Forcing extended failsafe mode

Programming, panel firmware and history are deleted and network settings are reset (DHCP, 0.0.0.0) when executing this option.

▸   Carry out steps 1 – 6 of the above, then carry out steps 2 – 7.

7 Technical Specifications

Electrical

Maximum operating voltage in VAC	230 (-15 %, + 10%)
Minimum AC line frequency in Hz	47
Maximum AC line frequency in Hz	63
Maximum power consumption in W per power supply	150
Minimum battery capacity in Ah per power supply	18
Maximum battery capacity in Ah per power supply	80
Back-up time	Determined by battery capacity and system load. Consider time or capacity limits for recharging the batteries regarding local regulations or EN standards if needed.

Refer to *, page 21* for the location of the ratings label on the power supply.

Frequency bands of operation	Power level for radio equipment
GSM900	Class 4 (2W) - GPRS Class 10
GSM1800	Class 1 (1W) - GPRS Class 10

Mechanical

Panel enclosure	
Dimension in cm (H x W x D)	65.8 x 44.3 x 19.35
Weight in g	1566
Power enclosure	
Dimension in cm (H x W x D)	65.8 x 44.3 x 19.35
Weight in g	1566
Expansion enclosure	
Dimension in cm (H x W x D)	43.6 x 44.3 x 11.2
Weight in g	780
System parameters	
Number of addresses	1500
Number of areas	500[1]
Event log capacity	4000
Users	
Number of users	1000

MAP 5000   Technical Specifications | en   **69**

Number of PINs	996 (with 9 digits, supporting a 3-digit user ID (004 - 999) and a 6-digit passcode)
Number of possible combination per PINs	1 million
Validity of PINs	Permanent validity, time-limited validity or one-time use configurable
Number of devices	
MAP LSN gateways	8
MAP control centers	32
DR2020T printer	1 (in VdS systems for service purposes only)
MAP power supplies 150W	32
MAP CAN splitter modules	8
Ethernet interface	1, RJ 45 connection
Management system connection	Via Ethernet interface and the Open Intrusion Interface OII or the MAP OPC server from Bosch - in VdS systems, only feedback-free connection as information system via exclusive transmission path
Number of inputs	
Programmable inputs on LSN Bus	Limited to maximum number of available addresses system wide
Number of inputs (on MAP main panel)	8
Number of outputs	
Programmable outputs on LSN Bus	Limited to maximum number of available addresses system wide
Power drive (on MAP main panel)	2
Dry contact (on MAP main panel)	2
Auxiliary power (on MAP main panel)	1
Supervised output (on MAP DE module)	3
Open-collector output (on MAP DE module)	2

[1]VdS system is limited to two areas, when connecting to the MAP control centers via the internal and external BDB.

Environmental

Minimum operating temperature in °C	-10
Maximum operating temperature in °C	55
Minimum storage temperature in °C	-20
Maximum storage temperature in °C	60
Minimum relative humidity in %	5

Maximum relative humidity in %	95
Protection class	IP30 IP31 (with an edge protection profile)
Security level	IK06
Environmental class	II: EN60950-1, EN50130-4, EN50131-1, VdS 2110
Usage	Indoor

MAP 5000   Appendices | en   **71**

8   Appendices

This chapter contains information and instructions for creating programming that complies with the requirements of a specific standard.

---

i

Notice!
Use the default setting for parameters that are not explicitly mentioned in this description. In addition, the instructions for panel validation in the **RPS for MAP** programming software must be followed.

8.1   Requirements in accordance with VdS class C

8.1.1   Selecting the default setting

▸   Select VdS class C as the default property values setting.

See also

–   *Standard-compliant programming, page 58*

8.1.2   Power supply for areas

Refer to *Connecting the LSN gateway, page 47*.

8.1.3   Control centers

Refer to:

–   *Connecting the control center, page 44*
–   *Planning the system with IPP-MAP0005 power supply, page 7*
–   *Planning the system with ICP-MAP0012 CAN splitter module, page 11*

8.1.4   Connection to a management system

Refer to *IP Interface, page 56*.

8.1.5   Printer connection

Connecting the DR2020T printer is permitted only for service purposes.

8.1.6   Access levels

The standard distinguishes between four access levels (AE):

–   AE 1 Access for everyone, no authorization/code required
–   AE 2 Access for users, user passcode required
–   AE 3 Access for installers via **control center** or via **RPS for MAP**
–   AE 4 Access for manufacturers via **RPS for MAP**

Selecting the access level

AE 1 Access for everyone, no authorization/code required

AE 2 Access for users, user passcode required

AE 3 Access for installers via **control center**

1.   Open control panel enclosure.
       Switch to installer mode (refer to *Installer button, page 66*).
2.   Enter installer passcode.

AE 3 Access for installers via **RPS for MAP**

---

1. Open control panel enclosure.
    or
    authorize from RPS with an AE 2 user with corresponding permissions (control center: main menu page 2 > RPS).
2. Establish a connection between the panel and RPS.

AE 4 Access for manufacturers via **RPS for MAP**

1. Authorize the manufacturer user with an AE 2 user with corresponding permissions (control center: main menu page 1 > maintenance page 3 > manufacturer permission).
2. Open control panel enclosure.
    Switch to installer mode = AE 3 (*Installer button, page 66*).
3. Login with the passcode of the manufacturer at the installer control center (*Manufacturer authorization, page 59*).
4. Establish a connection between the panel and RPS.

Functions of the access levels

The assignment of the functions to the access levels 2 and 3 can be adapted in RPS.

Further subdivisions are possible within the access levels if the owner wishes to grant the users different permissions: **User Manager > Permission Sets**

General permissions	Access level			
	1	**2**	**3**	**4**
May silence buzzer on control center		X	X	
May change own user passcode		X	X	X
May transmit/receive programming with RPS			X	
May receive history with RPS			X	
May perform diagnostics with RPS			X	
May perform software updates with RPS			X	X
Operations category permissions	**1**	**2**	**3**	**4**
May disable device			X	
May enable device			X	
May turn chime on/off		X	X	
May change schedule		X	X	
May edit blocking time		X	X	
User category permissions	**1**	**2**	**3**	**4**
May add user		X	X	
May delete user		X	X	
May change user passcode		X	X	
Event category permissions	**1**	**2**	**3**	**4**
May clear internal alarm		X	X	
May clear external alarm		X	X	

MAP 5000

Appendices | en   **73**

May clear tamper			X	
May clear trouble		X	X	
May clear battery trouble			X	
May silence			X	
Remote service category permissions	**1**	**2**	**3**	**4**
May authorize manufacturer user		X	X	
May authorize RPS user		X	X	
Arm category permissions	**1**	**2**	**3**	**4**
May arm area		X	X	
May disarm area		X	X	
Can disarm only if in alarm		X	X	
May bypass detectors			X	
May bypass detectors in area			X	
May unbypass detector		X	X	
May switch internal program on/off		X	X	
Status category permissions	**1**	**2**	**3**	**4**
May view area status		X	X	
May view device status		X	X	
May view duress alarm		X	X	
May view alarm count		X	X	
May view event memory		X	X	
May view control panel history		X	X	
May print control panel history		X	X	
May view control panel version		X	X	
Maintenance category permissions	**1**	**2**	**3**	**4**
May adjust control center volume/brightness		X	X	
May change output state		X	X	
May set date time			X	
May test bell		X	X	
May test motion detectors		X	X	
May walk test automatic points			X	
May walk test points			X	

Tab. 8.2: Permissions

8.2   Requirements in accordance with EN 50131 grade 3

i

Notice!
If not all requirements in accordance with this standard can be satisfied or only a lower grade
can be met, the compliance mark (EN 50131 grade 3) must be either removed or adapted.

8.2.1   Selecting the default setting

1.   Select EN50131 grade 3 as the default property values setting (refer to *Standard-
      compliant programming, page 58*).
2.   If the panel validation in accordance with EN 50131 grade 3 fails, do **not** proceed with
      programming the panel.

8.2.2   Connectable peripherals

To comply with the requirements for proper functioning of the panel (i.e. detection and
forwarding of intrusion, hold-up, tamper and trouble states), only peripherals may be
connected that are certified in accordance with EN 50131 grade 3 or grade 4.

8.2.3   Arming / disarming without entry / exit delay

Arming outside the secured area, e.g. with arming device
1.   Include a new area if not yet present.
2.   Connect a free input with the device key switch.
3.   Using the wizard, select the type **Static** or **Dynamic**, the user and function of the key
      switch **Arm / Disarm Area**. Now select the area that is to be armed / disarmed. For exit
      delay, select **No Delay**.
4.   Select the area in the properties field of the **Key Switch > Area**.
5.   In the properties field of the **Control Center**, include the area in the scope **Local Area** or
      Additional Areas in Scope

Programming two outputs for signaling the armed / disarmed state
1.   Connect one free output in each case with the device **LED**.
2.   Using the wizard, program one output with the behavior item **Area Armed** and a second
      output with the behavior item **Area Disarmed**.
3.   The signal must be time-limited. Enter a corresponding time (typically 10 sec. / maximum
      30 seconds) for **Activation Duration**.

**Securing access route against unauthorized entry in armed state, e.g. by installing a
blocking element**
1.   Connect a free output with the device **LED**.
2.   Variant A: Blocking element is actively controlled CLOSED. Using the wizard, program an
      output with the behavior item **Area Armed**
      or
      Variant B: Blocking element is actively controlled OPEN. Using the wizard, program an
      output with the behavior item **Area Disarmed**.
3.   The signal must be static; enter 00:00:00 for **Activation Duration**.
4.   Refer to the manufacturer's connection instructions for further information.

8.2.4   Arming / disarming with entry / exit delay

Arming inside the secured area, e.g. with control center
1.   Include a new area if not yet present.

MAP 5000   Appendices | en   **75**

2. Include a control center if not yet present.
3. Include the area in the scope of the control center: **Local Area**.
4. Program control center for arming with exit delay: **Use Area Normal Delay Time**.
5. The value for the entry / exit delay can be adapted if required: **Area Manager > Area > Timing and Delays**:
   normal entry delay (typically 45 sec. / at least 30 sec.)
   normal exit delay (typically 60 sec.)

Programming entry / exit route
1. Program all points of the entry / exit route to the point type intrusion.
2. Select the type of exit point optionally for exit route points:

Exit point type	Behavior
Initial follower [1]	Point without prevention of arming readiness, e.g. PIR that has the control center in the detection area. Important: point must be in normal state after exit, otherwise an alarm will be tripped
Follower [1]	Point that does not trip an alarm as long as the exit delay is running. Only relevant for option **MAP5000 Panel > Armed State At Exit Delay Start**
Exit	Door point that must be mandatorily tripped once upon leaving the area. The option **MAP5000 Panel > Unvacated Premises** must be activated
Interrupt	Door point that shortens the running exit delay to 10 sec. (recommended)
Restart	Point that restarts the exit delay; possible only once during the exit

Tab. 8.3: Exit point types

[1] Not for EN 50131

▸ Select the type of entry point for all entry route points.

Entry Point Type	Behavior
Delay 'Normal'	Door point that starts the entry delay with the value 'Normal'
Delay 'Extended'	Door point that starts the entry delay with the value 'Extended'
Follower	Point that does not trip an alarm as long as the entry delay is running

Tab. 8.4: Entry Point Types

Programming delayed reporting for all intrusion points of the area
1. For all points of the point type **Intrusion** and **Intrusion 24h**, set the parameter **Supports Delayed Reporting** to **Yes**.
2. For reporting **(Event Manager > Panel Event Groups > Properties > Reportable Events)**, set a **Transmission Delay** that is the same as the exit delay (typically 45 sec. / at least 30 sec.) for **External Intrusion Alarm**.

8.2.5   Arming with automatic bypass

Points that are not in normal state and therefore prevent arming can be automatically bypassed for arming. These points are automatically unbypassed again when the system is next disarmed.

1. Program point to point type **Intrusion (Bypassable)** or **Intrusion 24h (Bypassable)**.
2. Set the maximum number of points that can be bypassed on arming under **MAP5000 > Maximum Bypass Count per Area** (typically 1 - value range is not specified by the standard).
3. Set the maximum number of times that a point can be bypassed on arming under **MAP5000 > Maximum Times A Device Can Be Bypassed** (typically 1 - value range is not specified by the standard).
4. Set the permission **May Bypass Detectors In Area** for the user: **User Manager > Permission Sets > Arm Category**.

8.2.6   Automatic arming / disarming

The control center is located in the secured area.
1. Include a new area if not yet present.
2. Include a control center if not yet present.
3. Include the area in the scope of the control center: **Local Area**.

Programming two outputs for signaling the armed / disarmed state
1. Connect one free output in each case with the device **LED**.
2. Using the wizard, program one output with the behavior item **Area Armed** and a second output with the behavior item **Area Disarmed**.
3. The signal must be time-limited. Enter a corresponding time (typically 10 sec. / maximum of 30 seconds) for **Activation Duration**.

Automatic arming at a predefined time: defining the arming time
1. Start the schedule wizard and define the time of arming.
2. As action, select **Arm Area(s) Using Exit Delay**.
3. Program the duration of the acoustic warning signal before arming in the area: **Area Manager > Area > Exit Delay > Normal Delay Time**.
4. The option **Arm Only If Area Is Ready To Arm** must be deactivated.

Automatic bypassing of points can be optionally programmed. For requirements, refer to *Arming with automatic bypass, page 76*.

Automatic arming after disarming
▸ Do **not** set the option **Automatic Arming after Disarming** for an area. The procedure does not comply with the requirements of EN 50131.

Automatic disarming at a predefined time: defining the disarming time
1. Start the schedule wizard and define the time of disarming.
2. As action, select **Disarm Area(s)**.

See also
– *Arming with automatic bypass, page 76*

MAP 5000   Appendices | en   77

8.2.7 Alarm output via siren and communicator

Alarms, trouble events and other events must be output via siren and/or communicator.

‣ For possible variants, refer to *Sirens and communicator in accordance with EN50131 grade 3, page 62*.

External alarm via siren

‣ Activate the sirens at least for the following events (behavior items):
– External intrusion alarm
– External tamper alarm
‣ Set the option **Panel Wide Device**.

Additional behavior items can be optionally added.

Remote alarm via communicator

‣ Activate the communicator at least for the following events **(Event Manager > Panel Event Groups > Properties > Reportable Events)**:
– External intrusion alarm
– External tamper alarm
– Hold-up alarm
– Duress alarm
– Summary trouble

Additional reportable events can be optionally added.

8.2.8 Connection to a management system

Refer to *IP Interface, page 56*.

8.2.9 Printer connection

Connecting the DR2020T printer is permitted only for service purposes.

8.2.10 Access levels

The standard distinguishes between four access levels (AE):
– AE 1 Access for everyone, no authorization/code required
– AE 2 Access for users, user passcode required
– AE 3 Access for installers via **control center** or via **RPS for MAP**
– AE 4 Access for manufacturers via **RPS for MAP**

Selecting the access level

AE 1 Access for everyone, no authorization/code required

AE 2 Access for users, user passcode required

AE 3 Access for installers via **control center**
1. Open control panel enclosure.
   The internal warning device is activated for 3 sec.[1]
2. Switch to installer mode (refer to *Installer button, page 66*).
3. Enter installer passcode.

AE 3 Access for installers via **RPS for MAP**
1. Open control panel enclosure.
   Internal warning device is activated for 3 sec.[1]
   or
   authorize from RPS with an AE 2 user with corresponding permissions (control center: main menu page 2 > RPS).
2. Establish a connection between the panel and RPS.

AE 4 Access for manufacturers via **RPS for MAP**
1. Authorize the manufacturer user with an AE 2 user with corresponding permissions (control center: main menu page 1 > maintenance page 3 > manufacturer permission).
2. Open control panel enclosure.
   The internal warning device is activated for 3 sec.[1]
3. Switch to installer mode = AE 3 (*Installer button, page 66*).
4. Login with the passcode of the manufacturer at the installer control center (*Manufacturer authorization, page 59*).
5. Establish a connection between the panel and RPS.

1) Activation of the warning device on opening the control panel enclosure may be omitted if access to access level 3 is controlled by switches, locks (at least 15,000 variation possibilities) or other equivalent means.

Internal warning device when control panel enclosure is opened
An internal warning device must be provided that trips a time-limited audible alarm when the control panel enclosure is opened in unarmed state.
1. Assign device siren to free output.
2. In the properties> behavior item list of the device siren, activate the option **Include External Tamper Alarm Disarmed of Onboard Tamper**.

Functions of the access levels
The assignment of the functions to the access levels 2 and 3 can be adapted in RPS.
Further subdivisions are possible within the access levels if the owner wishes to grant the users different permissions: **User Manager > Permission Sets**

General permissions	Access level			
	1	2	3	4
May silence buzzer on control center		X	X	
May change own user passcode		X	X	X
May transmit/receive programming with RPS			X	
May receive history with RPS			X	
May perform diagnostics with RPS			X	
May perform software updates with RPS			X	X
Operations category permissions	**1**	**2**	**3**	**4**
May disable device			X	
May enable device			X	
May turn chime on/off		X	X	
May change schedule		X	X	
May edit blocking time		X	X	
User category permissions	**1**	**2**	**3**	**4**
May add user		X	X	
May delete user		X	X	

MAP 5000

Appendices | en   **79**

May change user passcode		X	X	
Event category permissions	**1**	**2**	**3**	**4**
May clear internal alarm		X	X	
May clear external alarm		X	X	
May clear tamper			X	
May clear trouble		X	X	
May clear battery trouble			X	
May silence			X	
Remote service category permissions	**1**	**2**	**3**	**4**
May authorize manufacturer user		X	X	
May authorize RPS user		X	X	
Arm category permissions	**1**	**2**	**3**	**4**
May arm area		X	X	
May disarm area		X	X	
Can disarm only if in alarm		X	X	
May bypass detectors			X	
May bypass detectors in area			X	
May unbypass detector		X	X	
May switch internal program on/off		X	X	
Status category permissions	**1**	**2**	**3**	**4**
May view area status		X	X	
May view device status		X	X	
May view duress alarm		X	X	
May view alarm count		X	X	
May view event memory		X	X	
May view control panel history		X	X	
May print control panel history		X	X	
May view control panel version		X	X	
Maintenance category permissions	**1**	**2**	**3**	**4**
May adjust control center volume/brightness		X	X	
May change output state		X	X	
May set date time			X	
May test bell		X	X	
May test motion detectors		X	X	

| May walk test automatic points | | | X | |
| May walk test points | | | X | |

Tab. 8.5: Permissions

See also
– *Installer button, page 66*
– *Manufacturer authorization, page 59*

8.2.11 Additional functions of the main panel

The panel has the following additional functions which do not have any influence on the intended operation of the panel.

Point type technical, fire for alarm inputs

Inputs that are assigned the device **Point** can be programmed to the point type technical or fire (refer to *Point types and point evaluation, page 59*).

Internal program

Points of the point type Intrusion can be assigned to an internal program.

When points are assigned to an internal program, and internal program is switched on, the points are capable of alarm signaling in disarmed state.

If the detector is tripped, an internal alarm is generated.

This internal alarm results in only local alarm signaling without a remote alarm.

Outputs for individual applications

Outputs of the panel can be used to control individual applications. A prerequisite for this is that no behavior item (no activation by the intended operation of the panel) is assigned to such an output.

Manual output control

▸ Select **Control Center > Behavior >Outputs Available For Direct Command.**

Automatic via schedule

1. Using the schedule wizard, enter the time when the output is to be switched on/off.
2. As action, select **Output ON** or **Output OFF**.
3. The schedule can optionally be edited at the control center. **Schedule > Behavior > May Be Edited At Control Center**.

Chime mode

If **Chime Mode** is activated on the control center in disarmed state, tripping of an intrusion point with the option **Chime Mode Capable** leads to a one-off chime tone on the control center.

▸ Assign the point to the **local area** of the control center.

8.3 Requirements in accordance with SES

The basis for this requirement is the standard EN 50131 grade 3 (refer to *Requirements in accordance with EN 50131 grade 3, page 74*). Deviations from this standard are already taken into account in the fundamental behavior of the panel and / or described below.

8.3.1 Selecting the default setting

1. Select EN50131 grade 3 as the default property values setting (refer to *Standard-compliant programming, page 58*).
2. If the panel validation in accordance with EN 50131 grade 3 fails, do **not** proceed with programming the panel.

MAP 5000   Appendices | en   **81**

See also
– *Point types and point evaluation, page 59*
– *Standard-compliant programming, page 58*

8.3.2 Automatic arming / disarming

Arming without a warning signal is permitted if it is possible to ensure by technical or organizational measures that there are no persons in the supervised area before arming.
– Refer to *Automatic arming / disarming, page 76*.

Automatic arming at a predefined time with warning signal
1. Start the schedule wizard and define the time of arming.
2. As action, select **Arm Area(s) Using Exit Delay**.
3. Program the duration of the acoustic warning signal before arming in the area: **Area Manager > Area > Exit Delay > Normal Delay Time**.
4. Deactivate the option **Arm Only If Area Is Ready To Arm**.
5. Optionally program automatic bypassing of points.

Automatic arming at a predefined time without warning signal
– Start the schedule wizard and define the time of arming.
– As action, select **Arm Area(s) Immediately**.
– Optionally program automatic bypassing of points.

Automatic arming after disarming without warning signal
– Enter the duration after disarming when automatic arming is about to take place in the area. **Area Manager > Area > Behavior > Automatic Arming after Disarming**.
– Optionally program automatic bypassing of points.

Disarming at a predefined time
Automatic disarming is **not** permitted for security reasons.

See also
– *Automatic arming / disarming, page 76*
– *Arming with automatic bypass, page 76*

8.3.3 Areas with blocking time

Disarming of an area can be optionally influenced by means of a blocking time. An external alarm from the area cancels the blocking time, i.e. disarming is possible.
1. Under **Area** (area manager), select the desired **Time Model**.
   Please note: Disarming is possible within a defined time interval.
2. A **Time Model** is made up of **Day Models** and can be adapted or created in the user manager if necessary.
3. A blocking time can be changed by the user at the control center up to seven days in advance if the user has the corresponding permissions. **User Manager > Permission Sets > Operations Category > May Edit Blocking Time**

8.3.4 Access Levels

The standard distinguishes between four access levels (AE):
– AE 1 Access for everyone, no authorization/code required
– AE 2A Access for users, user passcode required
– AE 2B Access for users, user passcode required
– AE 3 Access for installers via **control center** or via **RPS for MAP**
– AE 4 Access for manufacturers via **RPS for MAP**
Level 2A is a subset of level 2B.

Selecting the access level

AE 1 Access for everyone, no authorization/code required

AE 2A Access for users, user passcode required

AE 2B Access for users, user passcode required

AE 3 Access for installers via **control center**

1. Open control panel enclosure.
    The internal warning device is activated for 3 sec.[1]
2. Switch to installer mode (refer to *Installer button, page 66*).
3. Enter installer passcode.

AE 3 Access for installers via **RPS for MAP**

1. Open control panel enclosure.
    Internal warning device is activated for 3 sec.[1]
    or
    authorize from RPS with an AE 2 user with corresponding permissions (control center:
    main menu page 2 > RPS).
2. Establish a connection between the panel and RPS.

AE 4 Access for manufacturers via **RPS for MAP**

1. Authorize the manufacturer user with an AE 3 user with corresponding permissions
    (control center: main menu page 1 > maintenance page 3 > manufacturer permission).
2. Open control panel enclosure.
    The internal warning device is activated for 3 sec.[1]
3. Switch to installer mode = AE 3 (*Installer button, page 66*).
4. Login with the passcode of the manufacturer at the installer control center (*Manufacturer authorization, page 59*).
5. Establish a connection between the panel and RPS.

1) Activation of the warning device on opening the control panel enclosure may be omitted if access to access level 3 is controlled by switches, locks (at least 15,000 variation possibilities) or other equivalent means.

Internal warning device when control panel enclosure is opened

An internal warning device must be provided that trips a time-limited audible alarm when the control panel enclosure is opened in unarmed state.

1. Assign device siren to free output.
2. In the properties> behavior item list of the device siren, activate the option **Include External Tamper Alarm Disarmed of Onboard Tamper**.

Functions of the Access Levels

The assignment of the functions to the access levels 2 and 3 can be adapted in RPS.

Further subdivisions are possible within the access levels if the owner wishes to grant the users different permissions: **User Manager > Permission Sets**

General permissions	Access Level				
	1	2A	2B	3	4
May silence buzzer on control center	X	X	X	X	
May change own user passcode		X	X	X	X

MAP 5000　　　　　　　　　　　　　　　　　　　　　　　　Appendices | en　83

May transmit/receive programming with RPS				X	
May receive history with RPS				X	
May perform diagnostics with RPS				X	
May perform software updates with RPS					X
Operations category permissions	**1**	**2A**	**2B**	**3**	**4**
May disable device				X	
May enable device				X	
May turn chime on/off			X	X	
May change schedule			X	X	
May edit blocking time			X	X	
User category permissions	**1**	**2A**	**2B**	**3**	**4**
May add user			X	X	
May delete user			X	X	
May change user passcode			X	X	
Event category permissions	**1**	**2A**	**2B**	**3**	**4**
May clear internal alarm			X	X	
May clear external alarm			X	X	
May clear tamper				X	
May clear trouble				X	
May clear battery trouble				X	
May silence			X	X	
Remote service category permissions	**1**	**2A**	**2B**	**3**	**4**
May authorize manufacturer user				X	
May authorize RPS user			X	X	
Arm category permissions	**1**	**2A**	**2B**	**3**	**4**
May arm area		X	X	X	
May disarm area			X	X	
Can disarm only if in alarm			X	X	
May bypass detectors				X	
May bypass detectors in area			X	X	
May unbypass detector		X	X	X	
May switch internal program on/off			X	X	
Status category permissions	**1**	**2A**	**2B**	**3**	**4**
May view area status		X	X	X	

May view device status		X	X	X	
May view duress alarm		X	X	X	
May view alarm count		X	X	X	
May view event memory		X	X	X	
May view control panel history			X	X	
May print control panel history			X	X	
May view control panel version		X	X	X	
Maintenance category permissions	**1**	**2A**	**2B**	**3**	**4**
May adjust control center volume/brightness			X	X	
May change output state			X	X	
May set date time				X	
May test bell			X	X	
May test motion detectors		X	X	X	
May walk test automatic points				X	
May walk test points				X	

Tab. 8.6: SES Permissions

See also

8.3.5 Tamper surveillance of the main panel

Tamper switch with wall tamper

▸ When mounting the enclosure and installing the tamper switch, take the wall tamper of the panel into account (refer to *Mounting the enclosure, page 17* and *Installing and connecting the tamper switch, page 51*).

Location supervision of the panel

External alarm signaling by means of siren and/or remote alarm signaling with communicator must be planned in accordance with *Sirens and communicator in accordance with EN50131 grade 3, page 62*.

1. In case of variants A, B and C with communicator(s) of classes 3 and 4, provide location supervision for the panel as soon as one or more areas are armed.
   It is possible to omit location supervision for variant D with class 5 communicator.
2. Realize the location supervision as a technical solution by the intrusion alarm system itself. Therefore, ensure the EN-compliance of the requirements for disarming.
   Or:
   Realize the location supervision by security-relevant persons who guarantee that actions that pose a risk to security are detected at all times at the time of the required location supervision.

Design types of the communicators according to SES

The transmission paths for remote alarm signaling are divided into the following:

MAP 5000   Appendices | en   **85**

– Demand-driven connection with 25-hourly (AÜA-B25) or 5-hourly function monitoring (AÜA-B5)

– Existing connection with 3-minute (AÜA-S180) or 20-second function monitoring (AÜA-S20)

Types		Transmission procedure
EN 50131	**SES**	
Class 1	AÜA-B25	Demand-driven connection with 25-hourly function monitoring and voice annunciation
Class 2		Demand-driven connection with 25-hourly function monitoring and simple digital transmission
Class 3		Demand-driven connection with 25-hourly function monitoring and digital transmission
Class 4	AÜA-B5	Demand-driven connection with 5-hourly function monitoring and digital transmission
Class 5	AÜA-S180	Existing connection with 180-second function monitoring and digital transmission
Class 6	AÜA-S20	Existing connection with 20-second function monitoring and digital transmission

Tab. 8.7: Communicator types

8.4 Alarm reporting

ICP-MAP5000-COM and ICP-MAP5000-SC have an integrated alarm reporting functionality. It can be used for alarm transmission systems according to EN50136-2 SP4 or DP3. For DP3 compliant transmission, the alternate transmission path has to be wireless.

In case of a fault on the primary connection to a receiver, ICP-MAP5000-COM and ICP-MAP5000-SC are connecting to a backup receiver using the alternate transmission path.

The fault on the primary path is reported to the backup receiver and displayed on the control center.

ICP-MAP5000-COM and ICP-MAP5000-SC can report to any alarm receiver supporting the following protocols:

– Conettix IP

– SIA DC 09

– VDS 2465

Transmission path faults are directly reported to the user via the MAP 5000 control center. ICP-MAP5000-COM and ICP-MAP5000-SC have implemented layer 1 supervision for Ethernet and wireless path.

ICP-MAP5000-COM and ICP-MAP5000-SC supervise the link to Ethernet and poll the wireless network on checking for connection, signal strength and sign in status.

The communicator in ICP-MAP5000-COM and ICP-MAP5000-SC is realized as a pass-through system.

The monitoring center, to which the panel is connected to, has to provide proof of availability of the alarm transmission system.

For information security purposes, ICP-MAP5000-COM and ICP-MAP5000-SC provide the possibility of encrypted transmission (AES 128, 192, 256).

To grant anti-substitution security, the initial key has to be provided manually by typing it into the configuration software RPS for MAP.

8.5   History log

The history log of the MAP 5000 panel can be configured for 1000 to 4000 entries using RPS for MAP 5000.

For the SPT functionality, an additional history log of 1000 entries is available.

Both history logs are independent from each other and cannot influence each other.

In both history logs, the logged mandatory events cannot be deleted or overwritten by any logged optional events.

For both history logs there is no duration defined. This means, that events are stored for an unlimited amount of time and are not affected in case of power loss at the panel.