

PREGIO500 PREGIO500PL



Multi-functional hybrid control units for intrusion detection systems

PREGIO500 and PREGIO500PL are multi-functional hybrid control units that support both wired and wireless devices.

The control units give the possibility of splitting the system in 16 sectors (grouped in 1, 2 or 4 areas), which can be fully managed using the keypad menu and the BrowserOne software.

Thanks to the ULTRABUS interface, they support the connection of all EL.MO. serial devices (keypads, proximity (key) readers, power supply units, fog systems, concentrators and individual detectors).

With GATEWAY2K connection to the serial line, the control units are compatible with the NG-TRX radio technology.

Optional modules may be connected to expand their functions:

- **MDWIFIH:** it makes it possible to connect the control unit to a Wi-Fi network.
- **MDGSMI (or MDGSME):** it makes it possible to connect the control unit to the GSM/GPRS network using an internal antenna.
- **MDPSTN:** it makes it possible to connect the control unit to an analogue telephone line.
- **MDVOICE64:** voice module; it makes it possible to record up to 64 customised voice messages.

After installing the corresponding modules, MDGSMI or MDWIFIH, it is also possible to connect to e-Connect through GPRS or Wi-Fi respectively.

The control units manage:

- **inputs:** 8 on-board inputs, which can be expanded to 16 using the split function. Using the concentrators, it is possible to manage up to 24 inputs.
- **outputs:** up to 24 outputs, using optional relay modules and concentrators. There is also a fuse protected 12V output for the supply of power to the detector, and a programmable relay output.
- **users:** 32 users max.
- **control devices:** up to 16 control devices (keypads, proximity key readers) connected to the serial line.

The control units are supplied in a plastic housing protected against opening and removal from the wall.




PREGIO500 and PREGIO500PL are certified IMQ - Security Systems.

Some sections of the manual refer to options that must be selected in the BrowserOne configuration software. The following conventions apply:

• Text formatting:

- name_Function:** name of the *menu*, *page*, *tab* or *selectable function* as it appears in the BrowserOne software interface
- name_Selection:** *item that can be selected* from BrowserOne drop-down menu

• Icons:

-  BrowserOne It indicates that the subsequent operations must be carried out using BrowserOne

Warning: general warnings are outlined in chapter "10. WARNINGS" on page 24.



Please refer to the instruction manual.

1. TECHNICAL SPECIFICATIONS

GENERAL FEATURES		
Device Model	PREGIO500	PREGIO500PL
No. of on-board wired inputs	8 (16 with split)	
Max. no. of supported inputs	24	
Max. no. of supported outputs	24	
Max. no. of users	32	
Protection class	IP3X	
Operating temperature	-10 /+40 °C 93% R.H.	
Dimensions	W200 - H260 - D90 mm	W283 - H350 - D90 mm
Weight	920 g	1 kg
Certification	IMQ-SECURITY SYSTEMS and INCERT: EN50131-1, EN50131-3, EN50131-6, EN50131-10, EN50136-2, T031: grade 2, environmental class II, SP4	
POWER SOURCE		
Mains power source	230 Vac 50 Hz; 1.7 A power supply unit (mod. AL25RS15V0)	
Battery	12 V 4.2 Ah (Pb) (mod. B412I)	
Minimum operating voltage	9 V	
Maximum operating voltage	15 V	
Maximum power consumption from 230 V AC mains	290 mA	
BATTERY ELECTRIC VALUES		
Battery recharge voltage (Vdc)	13.8 V	
Exhausted battery threshold (Vdc)	10.5 V	
Exhausted battery reset (Vdc)	12.5 V	
Battery release voltage (Vdc)	9 V	
Maximum battery re-charge voltage @ 13,8 Vdc	250 mA	
14V SIR. TERMINAL ELECTRIC VALUES		
Nominal voltage (Vdc)	14.5 V	
14V SIR. anomaly voltage	9.7 V	
14V SIR. anomaly reset voltage	10.7 V	

"12V ALIM. SENS." TERMINAL ELECTRIC VALUES (electric values at the sensor power source terminal)	
Rated voltage (mains) (Vdc)	13.7 V
Minimum voltage (mains) (Vdc)	13.3 V
Maximum voltage (mains) (Vdc)	15 V
Rated voltage (battery only) (Vdc)	11.4 V
Minimum voltage (battery only) (Vdc)	8.4 V
Maximum voltage (battery only) (Vdc)	13.3 V
Fault voltage (Vdc)	10 V
Fault reset voltage (Vdc)	12 V
J12 (15 V input) TERMINAL ELECTRIC VALUES	
No power source (Vdc)	12.8 V
No power source reset (Vdc)	13.5 V
POWER CONSUMPTIONS @ 12 V	
Control unit armed-disarmed	12 mA
Relay ON	16 mA
GSM module enabled in voice mode	50 mA
GSM module enabled in GPRS mode	30 mA
GSM module, maximum power consumption	220 mA
PSTN module, idle	2 mA
PSTN module operating in digital mode	56 mA
MDWIFIH module	30 mA
MDVOICE64 module in play	10 mA
MAXIMUM NOMINAL CURRENTS AT THE OUTPUTS	
C-NA-NC relay output	3 A @ 24 V
14V SIR. output	120 mA
12V ALIM. SENS. output	1 A (880 mA if the 14V SIR terminal is used)
SIR +RIF output	120 mA

Components supplied

- Balancing resistors: 17 × 1500 Ω, 8 × 2200 Ω, 1 × 1000 Ω, 8 × 1200 Ω, 10 × 680 Ω
- Screws (4 × 30 mm) and 4 S5 nylon dowels (diam. 5 mm) for wall fixing
- Nylon cable ties
- User manual
- Quick guide

2. BEFORE INSTALLATION

- See the CEI 79-3 (installation of security systems) and CEI 64-8 (installation of low voltage systems) standards. Work following the good practice guidelines.
- Do not install the control unit and the modules in locations with extreme temperature and humidity conditions. Install the control unit away from heat sources. Avoid exposure to direct sunlight.
- Make sure that the wall is capable of supporting the weight of the control unit without damage.
- The electronic board may be damaged from electrostatic discharges. The installer must completely avoid any presence of electrostatic discharges starting from the moment of opening of the housing, both during installation and maintenance activities.
- Disconnect all mains power when connecting the switching power supply unit of the control unit to the power grid.
- The space inside the housing of the control unit (between the board and the battery) can be used to store the cables for connection to the various elements (normally a keypad, an external siren, an internal siren and up to 8 detectors). If a high number of devices must be connected, the addition of an external junction box to contain the cables is recommended.
- Connect any concentrators to the control unit serial line. Distribute them evenly along the line. Do not exceed the maximum distance of 1 km between the control unit and the last concentrator.

2.1 SYSTEM AUTONOMY CALCULATION CONSIDERATIONS

During the design stage, it will be necessary to define the autonomy of the system in case of power supply cut. This means the time during which the system will remain active, powered by one single battery, without its protection reliability being jeopardised.

The required battery capability (**C**) in Ampere hours (Ah) can be calculated as follows:

$$C = I \times A$$

where **A** is the requested autonomy in hours, **I** the total power consumption of the devices to power with the system active (which can be calculated using the power consumption data of the components as indicated in the technical specification table).

Compliance with grade 1 and 2 of the EN50131 requires a minimum autonomy of 12 hours in case of power cut: using a battery with rated capacity 4.2 Ah, the total load applicable to guarantee 12 hours of autonomy is 350 mA.

Use of power supply units

In order to ensure a high level of autonomy when installing many devices, the use of auxiliary power supply units should be considered.

EL.MO. can offer several power supply units with serial interface (e.g. C10RS and C11RS).

Connect the devices to the power supply units, splitting the load so that similar levels of autonomy are ensured for the section managed by the control unit and the rest of the system.

3. INDICATIONS FOR COMPLIANCE TO EN50131 REGULATION, GRADE 2

3.1 SYSTEM CONFIGURATION

- The minimum configuration that guarantees compliance to grade 2 requires the usage of a self-powered siren and of a MDPSTN or MDGSMI telephone dialler.
- To comply to INCERT, the automatic exclusion shall be set to 3 minimum.
- Flag all the EN50131 options available in **System Options** page > **General** tab > **EN50131 Options** pane inBrowserOne.

In particular:

▼ Activate Arming Lock

If flagged, control unit arming will be denied in case of fault or alarm. If a zone is in alarm at the end of the exit time, the control unit generates the "Arming failure" event: set the dialler activation for this event. Arming can be forced:

- pressing OK on control keypad
- moving the M4 key to the reader again
- pressing the remote control key again

See user and programming manuals for further information.

▼ Visualization protection

If flagged, the user must type the user code and then ↓ or ↑ to display status information.

3.2 POWER SUPPLY FROM MAINS AND SYSTEM AUTONOMY

- Equip the electric system with a 16 A curve C circuit breaker.
- Set a mains failure notification delay of 1 minute or below.

3.3 INTRUSION DETECTION

- Use of the following zone connection types causes certification loss: Normally closed, Normally open, Prealarm, Delayed, Auto-Bypass, Key Zone.

- Associate a remote transmission (dialler activation) to each INTRUSION-type event.

3.4 TAMPER DETECTION

- Tamper detection must not be disabled: each option whose effect is tamper detection disabling does not comply with EN 50131 regulation.
- Associate a remote transmission (dialler activation) to each TAMPER-type event.

3.5 FAULT DETECTION

- Associate a remote transmission (dialler activation) to each FAULT-type event.

3.6 ASSAULT DETECTION

- Associate a remote transmission (dialler activation) to each ASSAULT-type event.

3.7 MASKING DETECTION

- Wire the MASC output of each device that features the antimasking function to a control unit zone programmed as FAULT.
- For radio and RS-485 detectors, the fault + tamper repetition function does not comply with the EN50131 regulation.

3.8 ACCESS LEVELS

Several access levels exist to access control unit functions:

- LEVEL 1: Granted access to anybody
- LEVEL 2: User access
- LEVEL 3: Installer access
- LEVEL 4: Manufacturer access

3.12 CLASSIFICATION OF NOTIFICATIONS (ACCORDING TO TABLE 10 EN50131-1)

NOTIFICATION EQUIPMENT	A	B	C	D	E	F	GRADE
REMOTELY POWERED AUDIBLE WD	2	OP	/	OP	/	/	2
SELF-POWERED AUDIBLE WD	/	1	/	OP	/	/	2
ATS	SP2	SP2 SP4	/	SP4	/	/	2

A, B, C, D, E, F are the possible options.

For grade 2:

- SP2: MDPSTN board in VOICE PROTOCOL (periodic transmission 25h);
- SP2: MDGSME or MDGSME90 or MDGSMI or MD4GE board in VOICE PROTOCOL (periodic transmission 25h);
- SP4: MDGSME or MDGSME90 or MDGSMI or MD4GE board in SIA DC-09 or E-Connect protocol (periodic transmission 30 min or 3 min).

3.9 PERIODIC MAINTENANCE

- Perform a SYSTEM TEST periodically (see the programming manual for further details). The system test includes 4 steps: zone test, output test, dialler test (if installed and active), battery test. The test will be considered passed only if its steps are performed one after another without interruption. The SYSTEM TEST can be launched from the user or installer menu. The periodicity can be set using BrowserOne.

3.10 CURRENT DISTRIBUTION FOR IMQ - SECURITY SYSTEMS CERTIFICATION

For grade 2 (12 h autonomy), with 4.2 Ah battery:

- 0.35 A self-consumption of board and external devices;
- 0,25 A for battery recharge.

Current distributions with automatic power change (4 h), with 4.2Ah battery:

- 1.05 A self-consumption of board and external devices;
- 0.25 A for battery recharge.

Maximum current distributions (1.7 A):

- 1.45 A self-consumption of board and external devices;
- 0.25 A for battery recharge.

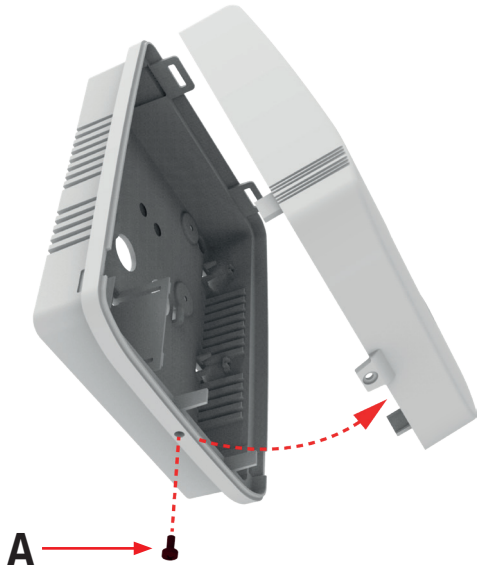
3.11 CURRENT DISTRIBUTION FOR INCERT CERTIFICATION

For grade 2 (24 h autonomy), with 4.2 Ah battery:

- 0.17 A self-consumption of board and external devices;
- 0,25 A for battery recharge.

4. PREGIO500 ASSEMBLY

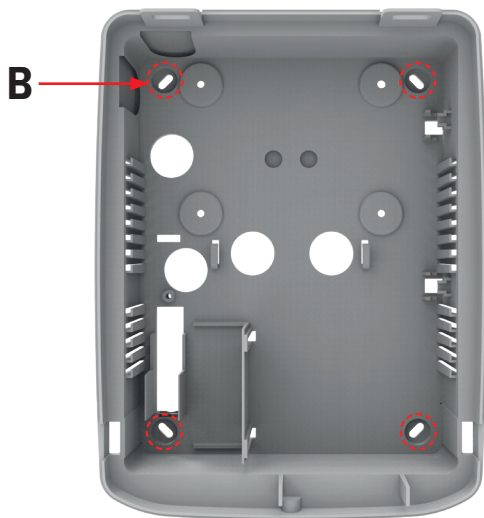
• Opening the housing



A. Closing screw

- Unscrew the screw on the bottom edge of the housing (A).
- Rotate the cover upwards and remove it.

• Wall installation

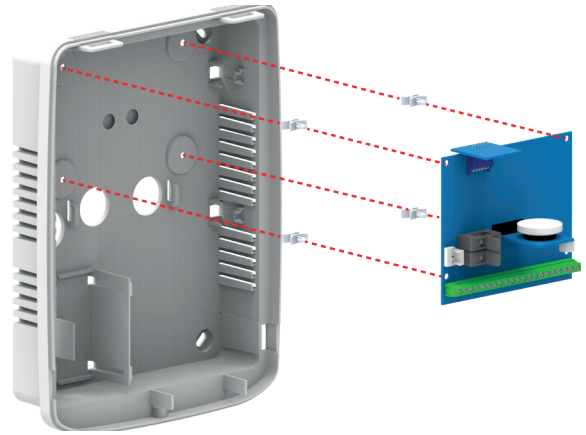


B. Fixing holes

- Place the base of the housing on the wall surface.
- Mark the fixing points (B).
- Fix the base to the wall using the screws and plugs supplied.

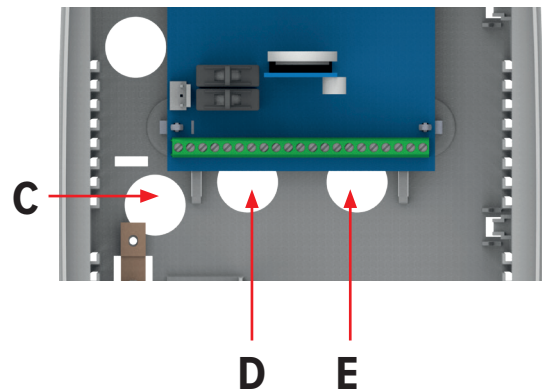
• Removing and replacing the electronic board

In order to complete the wiring and the installation of the modules, it may be necessary to remove the electronic board from the base of the housing.



- Press the end of the 4 support pins found at the corners of the control unit board.
- Remove the board.
- Install any optional modules on the control unit board as indicated in chapter “4.1 Module installation” on page 7.
- Replace the electronic board on the base, securing it with the support pins.

• Cable routing



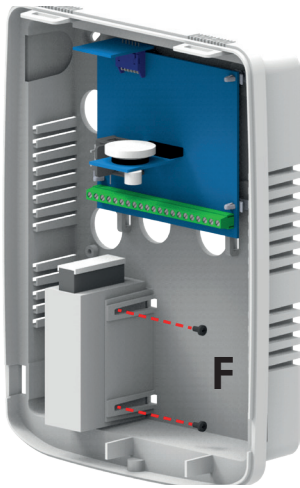
C. Mains cable

D. Powering of sensors, serial line (terminals A/B)

E. Terminal block inputs

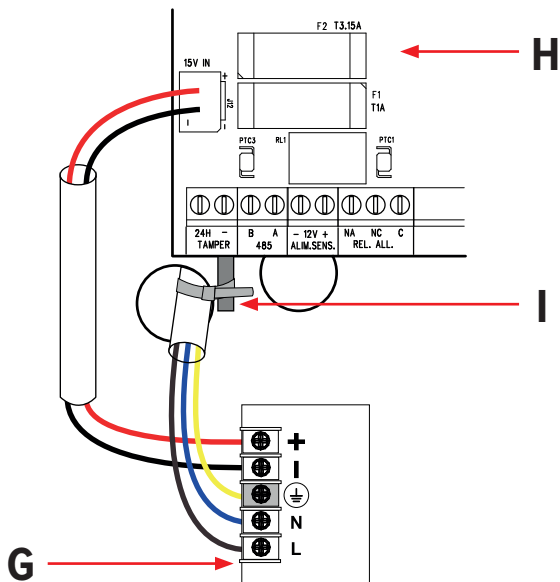
- Insert the system cables, not powered, through the two holes of the base. The image shows which holes to use.
- Complete the connections to the board terminals (see “6. WIRING” on page 12).

• **Power supply unit connection**



F. Fixing screws

- The power supply unit is fixed in position using two M3 screws.



G. Power supply unit (top view)

H. Electronic board

I. Cable fixing point

- Connect the mains cable to the power supply unit input phase and neutral terminals (terminals N and L). Connect the earth cable to the central terminal.
- Secure the mains cable at the indicated position (I) using a cable tie.
- Connect the power supply unit output cable (terminals + and -) to the board J12 connector.

To facilitate the identification of the terminals, a label at the bottom of the control unit shows the terminal block from the top.

• **Battery connection**



- Place the battery in its dedicated slot.
- Connect the black and red output cables from the control unit board to the battery terminals.

Note: The battery in use must comply with IEC 60896-21/2 and have a fire proof envelope V-2 or higher.

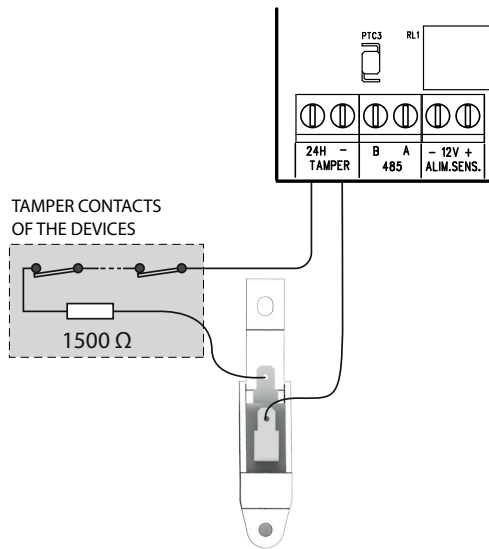
Note: The control unit will not turn on due to the battery release circuit, which is only activated when the control unit is powered from the mains using the power supply unit.

• **Tamper protection connection**

The control unit has a switch for double protection against both the opening of the cover and the removal from the wall.



- Connect the switch wires to the 24H terminals on the control unit board.



- If required, connect any device tamper contacts to the switch as shown.

• **Closing the housing**



- Place the cover on the base. Make sure that the tabs at the top of the container match the grooves of the base.
- Close the housing using the screw.

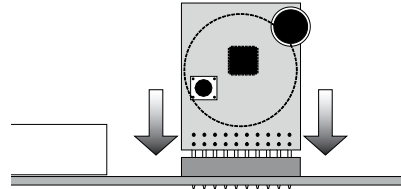
4.1 MODULE INSTALLATION

Install the modules as indicated in the following paragraphs.

Note: Before installing the modules, make sure that the power source has been disconnected from the control unit.

After installation, register each module as indicated in the programming manual.

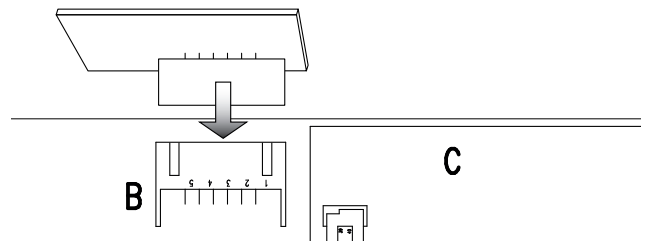
4.1.1 MDVOICE64



- Plug the module in the SINTESI A area on the control unit board. Refer to the previous image.

Note: make sure that all the feet are correctly inserted.

4.1.2 MDWIFIH

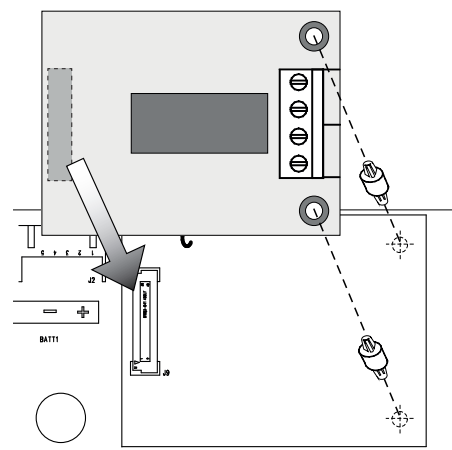


- Plug the module in the B area on the control unit board. Refer to the previous image.

4.1.3 MDPSTN

The optional MDPSTN module has a PLTM test report no. 10013, with tests carried out according to TBR21.

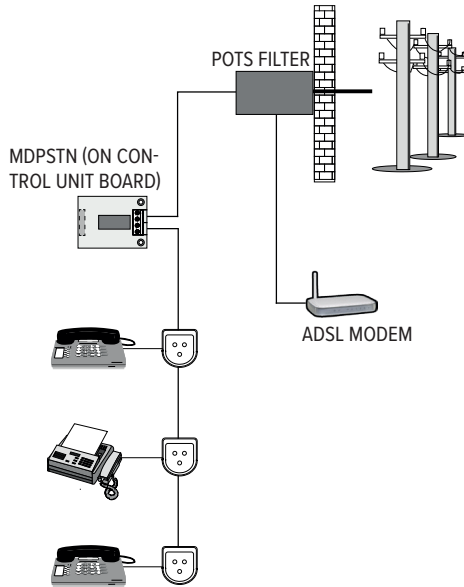
It can be used in alternative to the MDGSMI module.



- Insert the spacers (supplied with the module) in the holes of the C area. If necessary, use pliers.

- Place the module parallel to the control unit board. Align the spacer holes and the module connector with the corresponding components on the control unit board.
- Plug the module to the control unit board.
- Connect the telephone line to the terminals. See the MDPSTN technical manual.

Example of telephone system



The line goes through a POTS filter, where it is split into telephone and ADSL line.

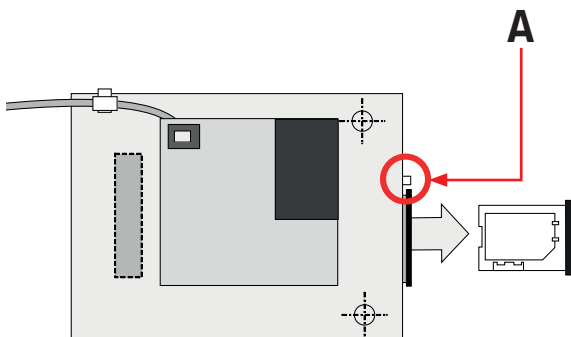
The telephone line goes through the MDPSTN module input terminals and exits through the output terminals, towards the internal telephones.

4.1.4 MDGSMI

It can be used in alternative to the MDPSTN module.

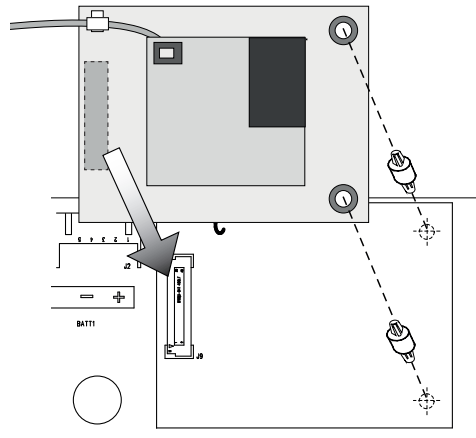
Inserting the SIM card

- Obtain a SIM card and disable the PIN code using any telephone.

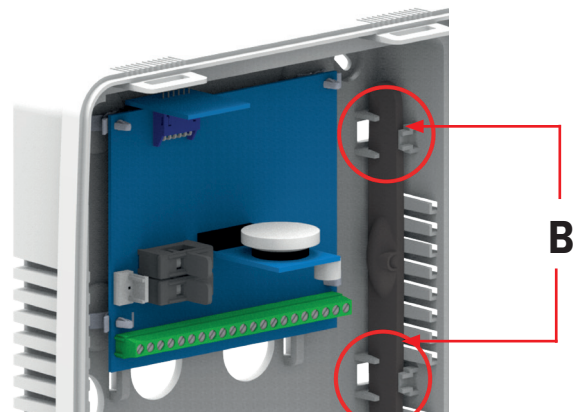


- With the tip of a pencil, press at the indicated position (A).
- Extract the SIM card holder.
- Place the SIM card in the holder.
- Place the SIM card holder with the SIM card back in its housing.

Module installation



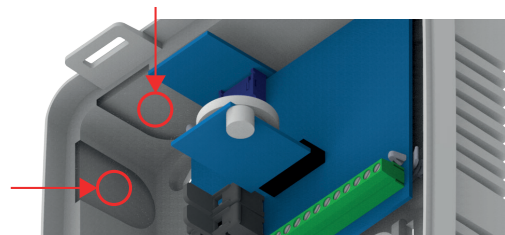
- Insert the spacers (supplied with the module) in the holes of the C area.
- Place the module parallel to the control unit board. Align the spacer holes and the module connector with the corresponding components on the control unit board.
- Plug the module to the control unit board.



- Position the antenna as indicated (B). Secure it between the supports. Pay the utmost attention when handling the cable.

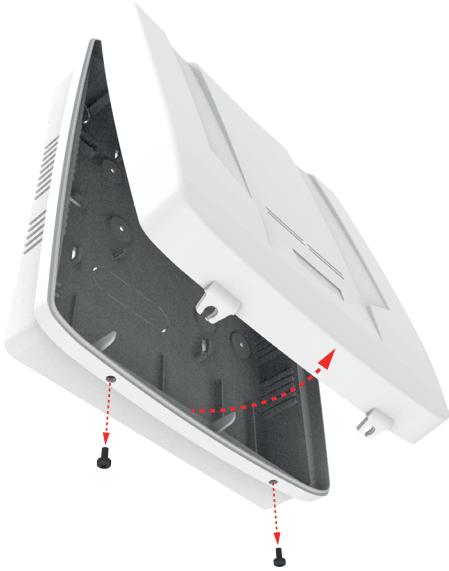
MDGSME

As an alternative to the MDGSMI module, the MDGSME module can be used together with the GSMEXA15 or GSMEXA2 antennas. We suggest using it if the control unit is installed in a position where the GSM signal is weak.

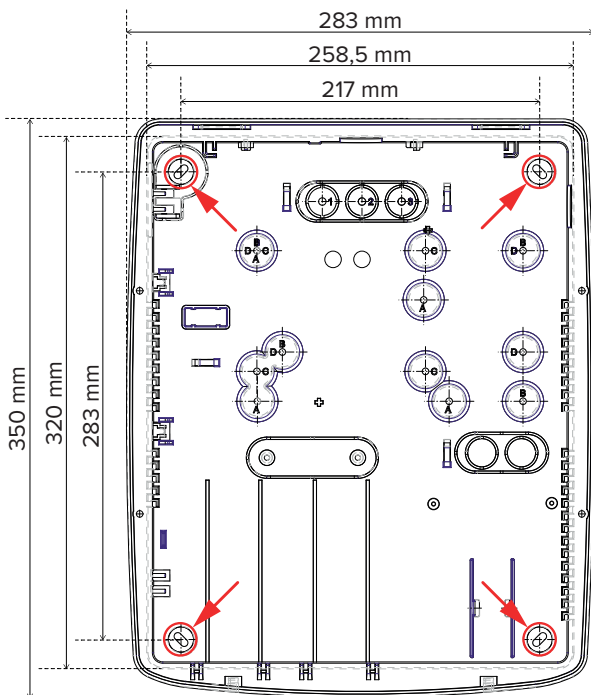


Install the module on the control unit board (area C), drill a hole in one of the areas indicated in the picture above and feed the antenna cable through that hole.

5. PREGIO500PL ASSEMBLY

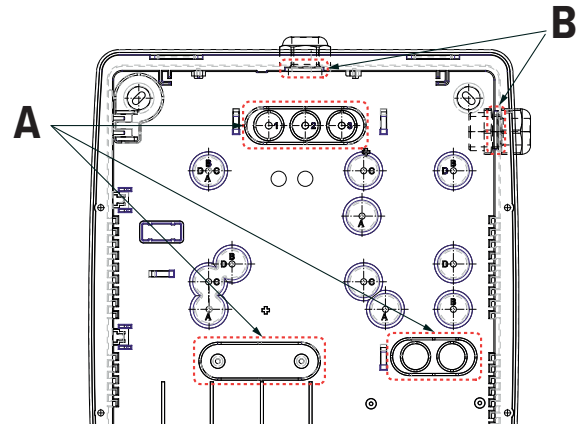


- Open control unit case unfastening the closing screws.



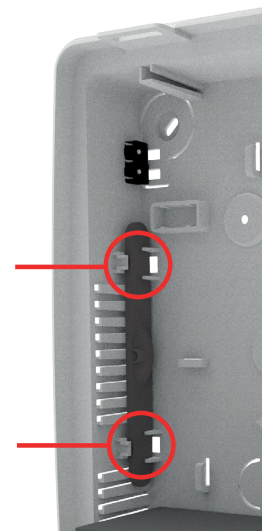
- Fix the control unit to a flat wall horizontally using the supplied screws and dowels. Use the holes on bottom indicated by the arrows.

THE WALL MUST BE ABLE TO SUSTAIN THE WEIGHT OF THE CONTROL UNIT WITHOUT FAILURE.

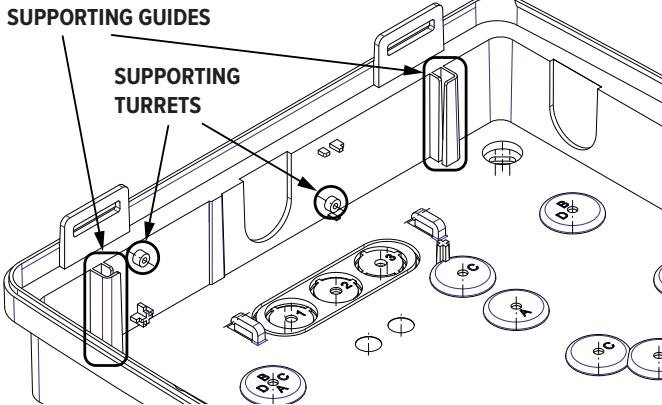
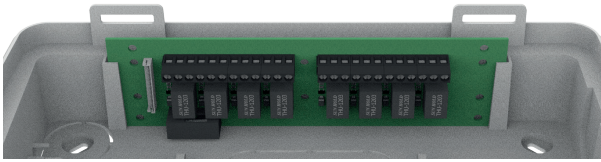


- Feed the unpowered system cables through the holes on case bottom (A), which can be obtained removing the pre-drilled plastic material. As an alternative, it is possible to use the hole for plastic cable gland (B) indicated in previous picture.
- Fix the control unit PCB to the case bottom using support pins. The holes to be used are marked with letters C.
- Connect the power supply unit as shown in the following chapter.
- Wire the output connectors of the power supply to the corresponding connectors on the main board of the control unit, using cable ties to prevent the connectors from getting pulled out when the unit gets opened. Do not let the mains cable touch the low voltage cables: use a cable tie to fix the mains cable to the base. Do not solder the wires.

Optional modules



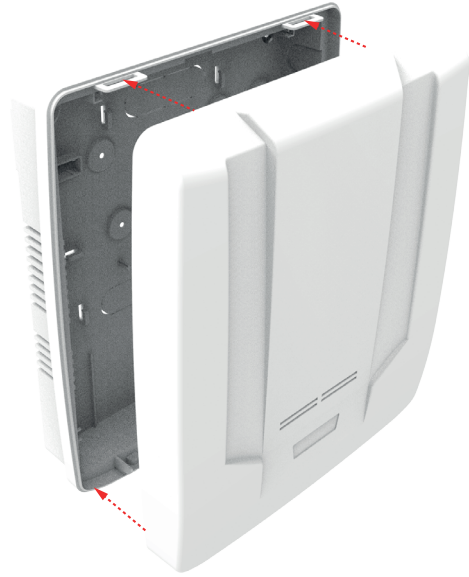
- Install optional modules on control unit board as indicated in paragraph "4.1 Module installation" on page 7. In case of installation of the MDGSMI module, arrange the antenna between the supports indicated in previous picture. Take care while handling the cable.



- The top side of the case bottom features a slot for optional PCBs. Insert the board between the guides (ETRREL type) or fix it to the supporting turrets (GATEWAY2K type), as indicated in previous picture.
- Wire the control devices and the detectors as indicated in the next chapters.
- Mark the keyboard that has been programmed as No. 1, as to facilitate the reset operations.
- Check the wirings that have been performed
- Connect the red and black cables with Faston terminals to the battery, paying attention to respecting the correct polarities. The control unit does not turn on because its battery release circuit activates only when the control unit is powered by its power supply unit.

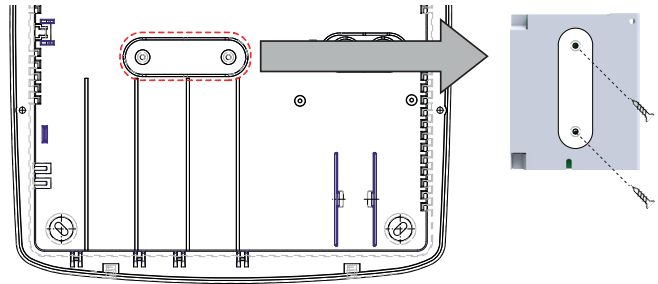
Note: The battery housing needs to have HB flammability class or higher.

- Power the unit up. Consult the brief of the various programming menus for the installer later in this manual, which will make it possible to complete the first phase of the control unit programming.
- Proceed with the M4 keys registration.
- If a PC equipped with the programming browser is available, link it to the dedicated connector of the main board by using the cable with mini-USB connector and open BrowserOne. Read the control unit configuration already stored and change it as necessary.
- Wire the sirens and perform the final testing.

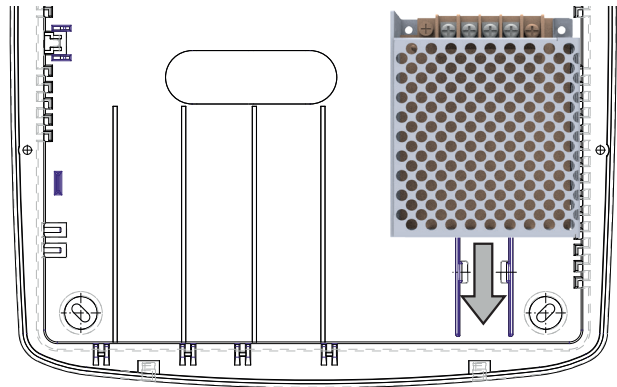


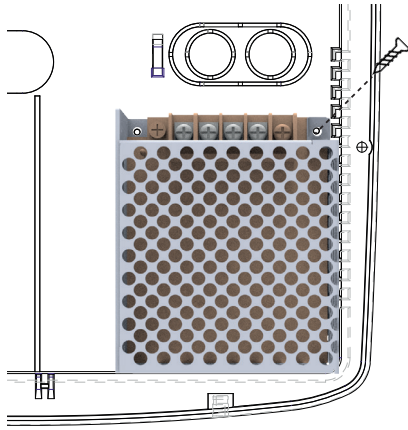
- Lean the cover on the base. Make sure that the tabs at the top of the container match the grooves of the base. Close the case using the screw.

5.1 CONNECTING THE POWER SUPPLY UNIT

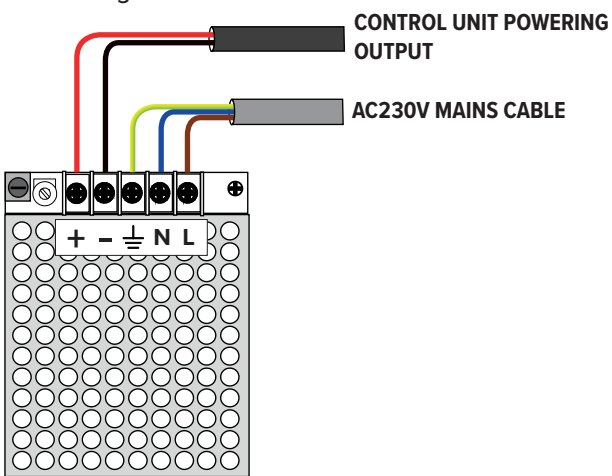


- Remove the plastic component indicated in the picture from the case bottom.
- Fix the plastic component to the power supply rear side.





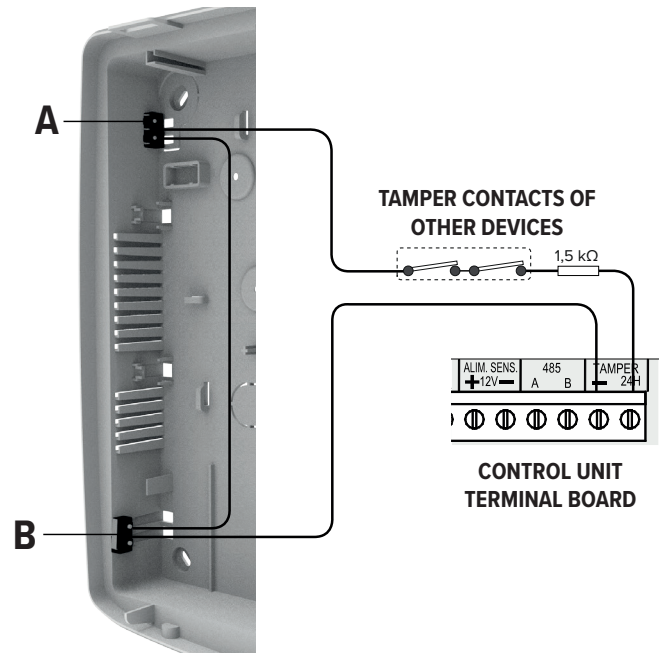
- Arrange the power supply unit making it slide between the tracks on case bottom.
- If necessary, fix the power supply unit to the case bottom using a screw.



- Wire cables as shown.

Note: the ground cable must be wired to the power supply ground terminal, and not to the faston connector on control unit board either.

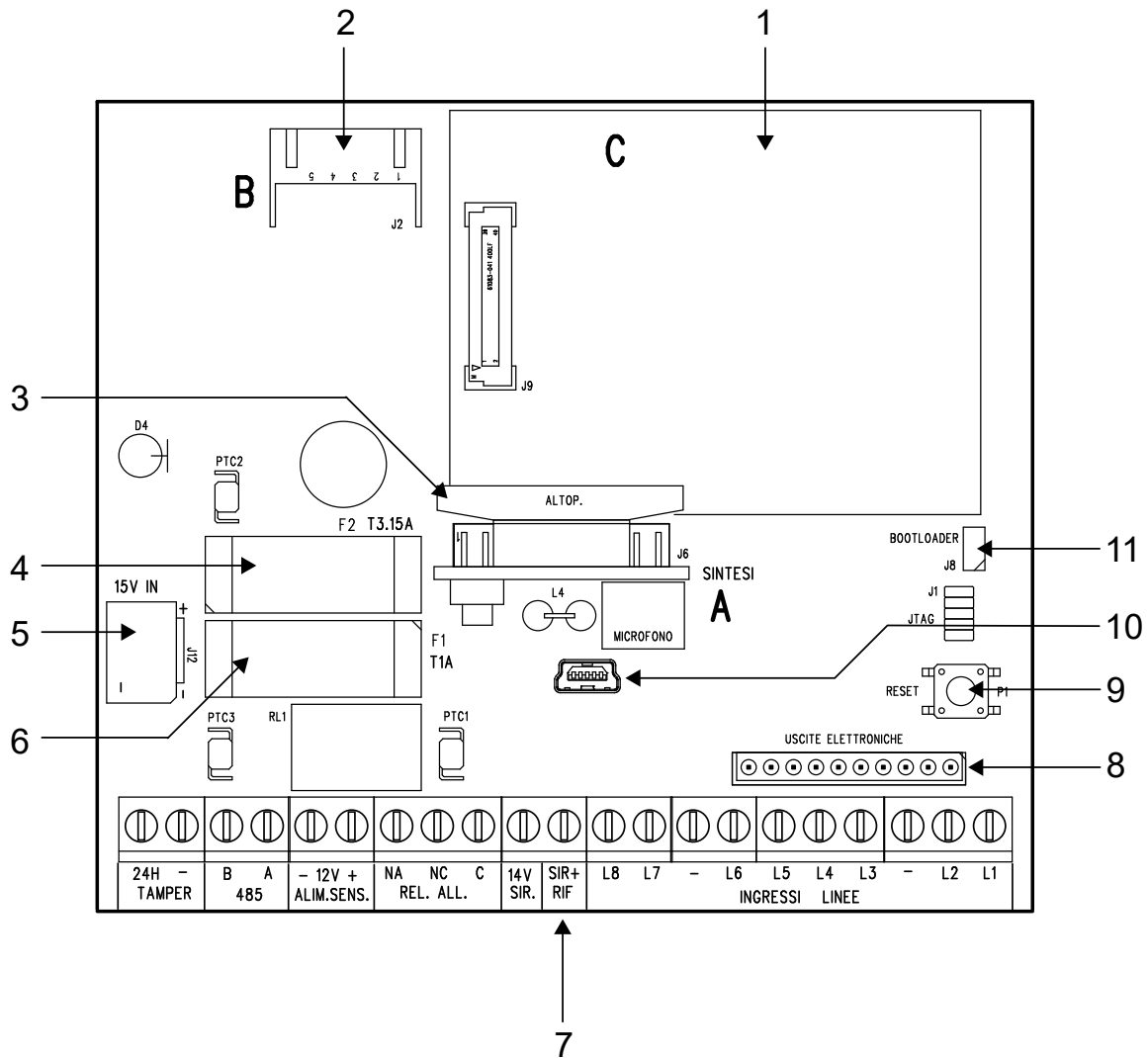
5.2 PROTECTION AGAINST OPENING AND REMOVAL FROM THE MOUNTING SURFACE



- A. Switch for protection against removal
- B. Switch for protection against opening

6. WIRING

6.1 ELECTRONIC BOARD VIEW



1. MDGSMI or MDPSTN module slot (C)
2. MDWIFIH module slot (B)
3. MDVOICE64 module slot (A)
4. **F2** fuse for battery inversion protection (3,15 A)
5. AL25RS15V0 power supply unit connector
6. **F1** fuse for the protection of the 12V ALIM. SENS. sensor power source (1 A)
7. Terminal block (see paragraph “6.1.1 Terminal block”)
8. Electronic output expansion connector
9. Reset button
10. USB connector
11. J8 jumper (bootloader)

6.1.1 Terminal block

24H TAMPER	Tamper protection line balanced input
485 (A - B)	ULTRABUS RS-485 serial line
12V SENS. POW.	Sensor power source line (12 V)
AL. RELAY	Programmable alarm relay (potential-free contacts: NA, NC, C)
14V SIR.	Self-powered siren power source
SIR+ RIF	Self-powered siren reference
LINE INPUTS	Wired sensor inputs

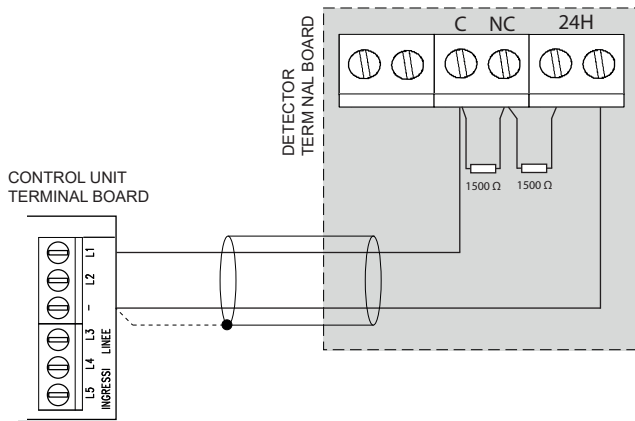
Perform wiring using shielded cables for security systems.

6.2 WIRED ZONE CONNECTION

Connect all the required wired devices using inputs 1 to 8 on the control unit terminal block.

6.2.1 Double balancing

This type of wiring is the one most commonly used for the connection of detectors: double balancing allows the control unit to monitor the idle, alarm and tampering (short circuit/cut) conditions.

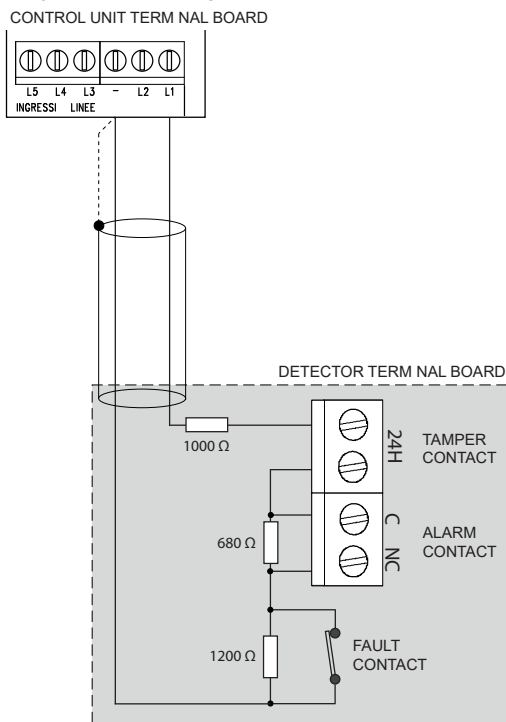


- Connect the two 1500 Ω resistors (supplied with the control unit) as shown.

Note: see the detector technical manual.

6.2.2 Triple balancing

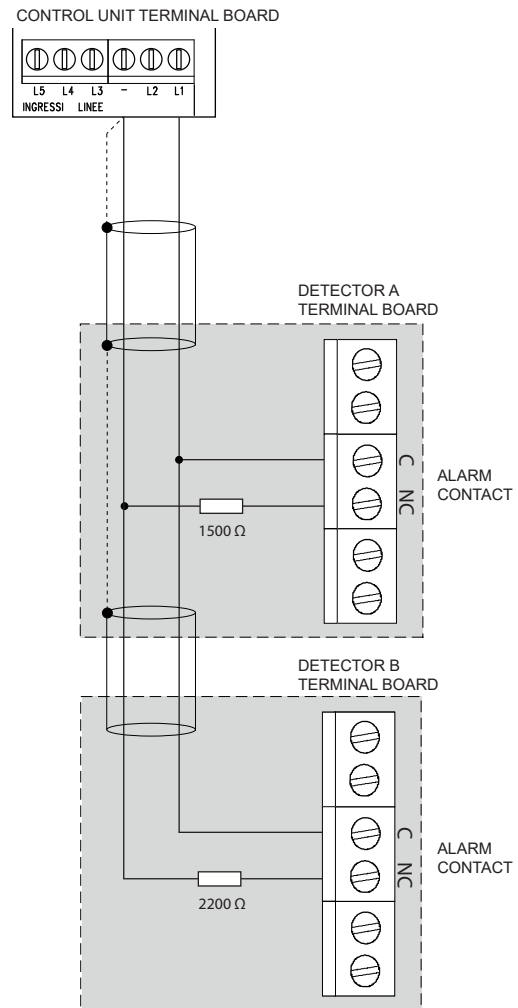
In addition to tampering, triple balancing also gives the possibility of monitoring the fault status.



- Three resistors of 1200 Ω, 680 Ω and 1000 Ω are required. Connect the three resistors as shown.

6.2.3 Split zones

Split connection gives the possibility of using the same line to connect two devices.



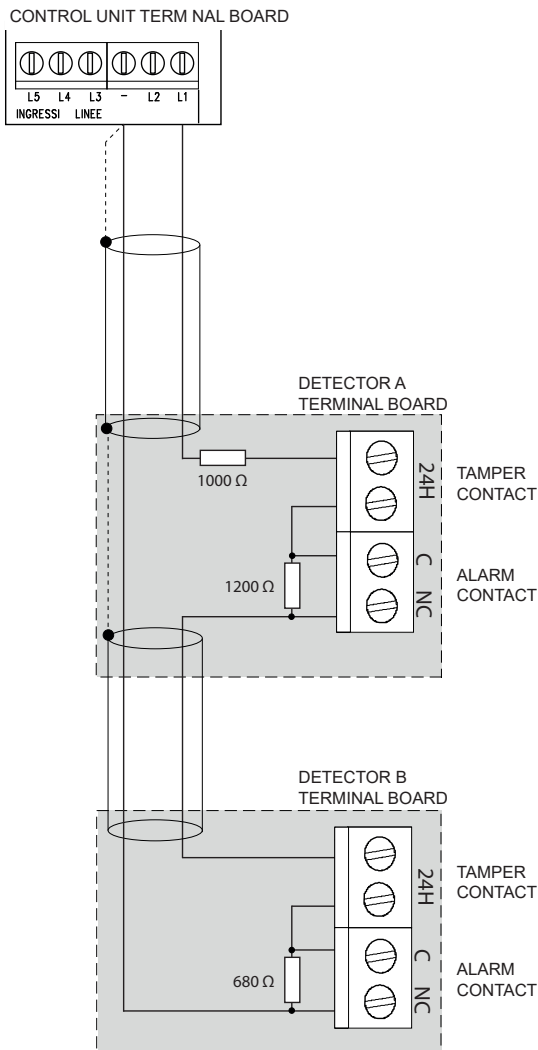
- Three resistors of 1500 Ω and 2200 Ω are required. Connect the two devices in parallel as shown in the figure.

BrowserOne

- In BrowserOne, go to **Zones > General**. In the grid, select the row of the zone n to which to connect the devices (e.g. input 2).
- In the **Zone Type** drop-down menu select *Split*. Zone n+8 (considering the example, input 10) will also automatically become a *Split* zone.

6.2.4 Extended split zone

Extended split zone mode allows to use the same line to connect two devices, also adding tamper monitoring (line cut/short circuit).



- Three resistors of 1200 Ω, 680 Ω and 1000 Ω are required. Connect the two devices as shown in the figure.

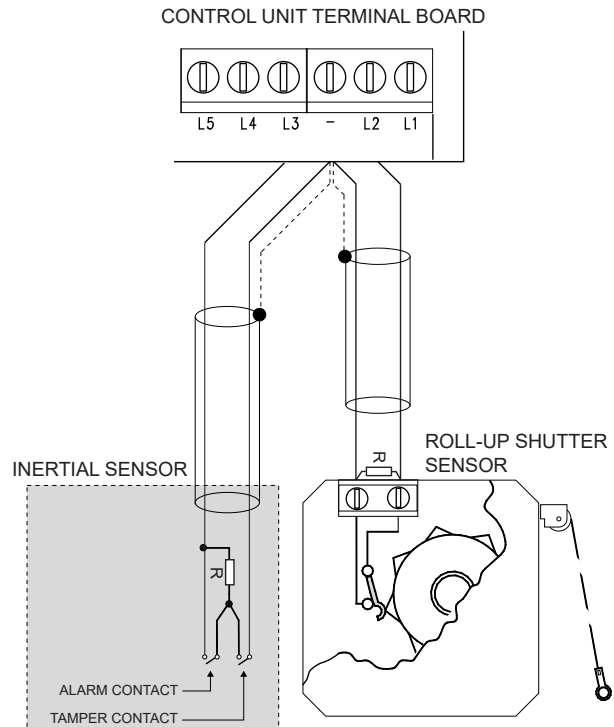
BrowserOne

- In BrowserOne, go to **Zones > General**. In the grid, select the row of the zone n to which to connect the devices (e.g. input 2).
- In the **Zone Type** drop-down menu select *Extended Split*. Input n+8 (considering the example, input 10) will also automatically become an *Extended Split* zone.

6.2.5 Fast zone

Use the following connection diagram to connect roll-up shutter or inertial sensors.

Note: Connect only one contact for roll-up shutters or only one inertial sensor for each zone, otherwise an external analysis board will be needed.



- Connect the resistor in parallel with the alarm contact, as close as possible to the sensor body.
- The resistor is supplied with the control unit: R = 1500 Ω.

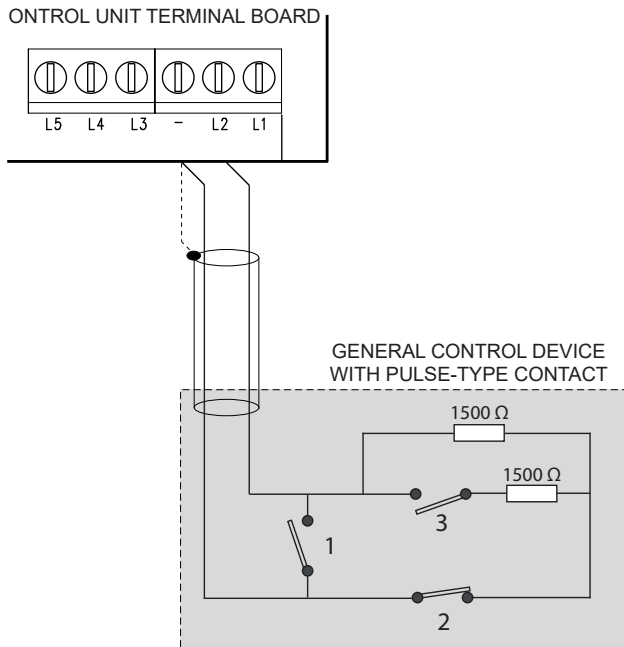
BrowserOne

- In BrowserOne, go to **Zones > General**. In the grid, select the row of the zone n to which to connect the devices (e.g. input 2).
- In the **Zone Type** drop-down menu select *Fast*.
- This will enable the **Fast** panel: set the **Sensitivity** and **Pulse Count** parameters.

6.2.6 Key zone

A "key" zone causes the switching of the arming status of its associated sectors when that zone is in anomaly state.

Use this type of wiring to connect control devices with terminal block outputs (e.g. a radio receiver of the video surveillance company) that are not directly compatible with the control unit.



1. Tamper contact (normally open)
2. Tamper contact (normally closed)
3. Device contact (NO)
 - Complete the connections as shown in the figure. The shown connections also include the necessary tamper protection.
 - Two 1500 Ω resistors are required.
 - If the control device has a power source, the idle condition must be realised with the contact open (NO) when not powered.

BrowserOne

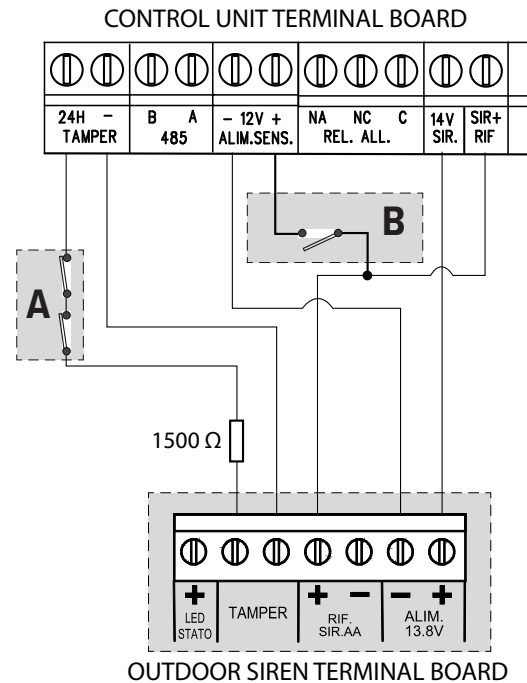
- In BrowserOne, go to **Zones > General**. In the grid select the zone row.
- In the **Zone Options** panel, tick *Key Zone* and *24H*.

6.3 SIRENS

6.3.1 Outdoor wired sirens

- Connect the outdoor wired sirens (e.g. LEDA) as shown.
- Connect the cable shield to the -12V (negative) terminal of the control unit.

Note: see the siren technical manual.

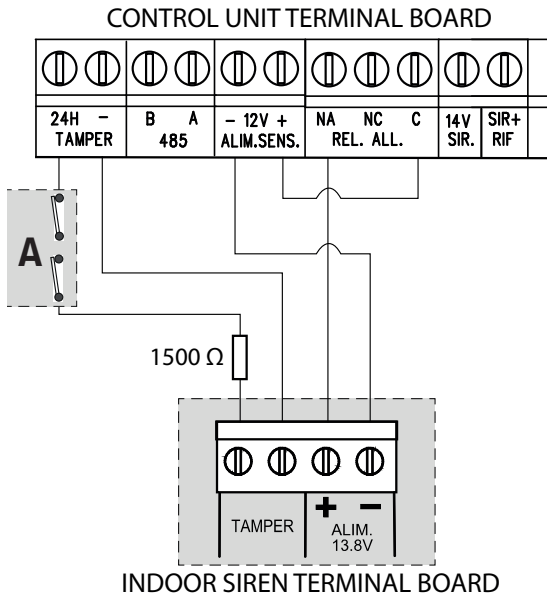


The tamper switches of all housings (control unit, remote power source boxes, detectors, etc.) must be connected in series (**A** in the figure).

Fit a manual contact to be closed in case of siren maintenance (**B** in the figure).

6.3.2 Indoor wired sirens

- Connect the indoor wired sirens (e.g. EL/7) as shown.
- Connect the cable shield to the -12V (negative) SENS. POW. terminal of the control unit.



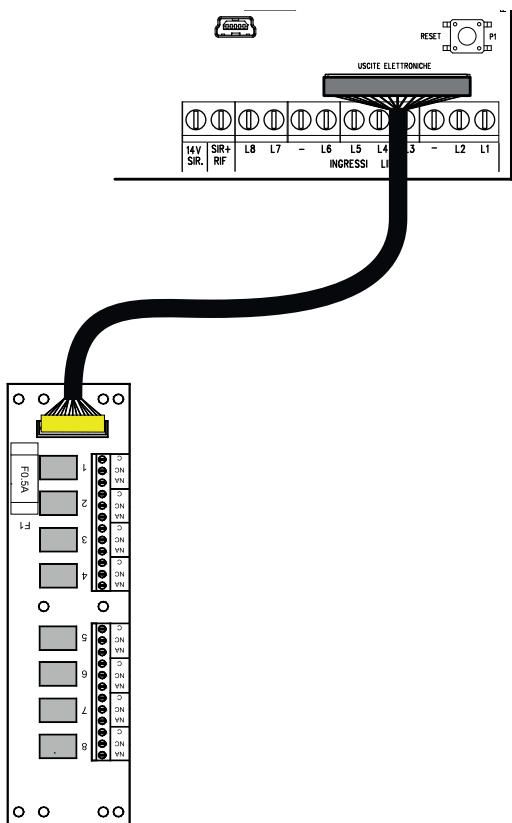
The tamper switches of all housings (control unit, remote power source boxes, detectors, etc.) must be connected in series (**A** in the figure).

BrowserOne

By default, the control unit relay is not active: it must be programmed for the requested function using BrowserOne (go to **System Options > General**, select **General Alarm Relay** from the **Programmable Relay Settings** menu).

Note: see the siren technical manual.

6.4 ELECTRONIC OUTPUTS

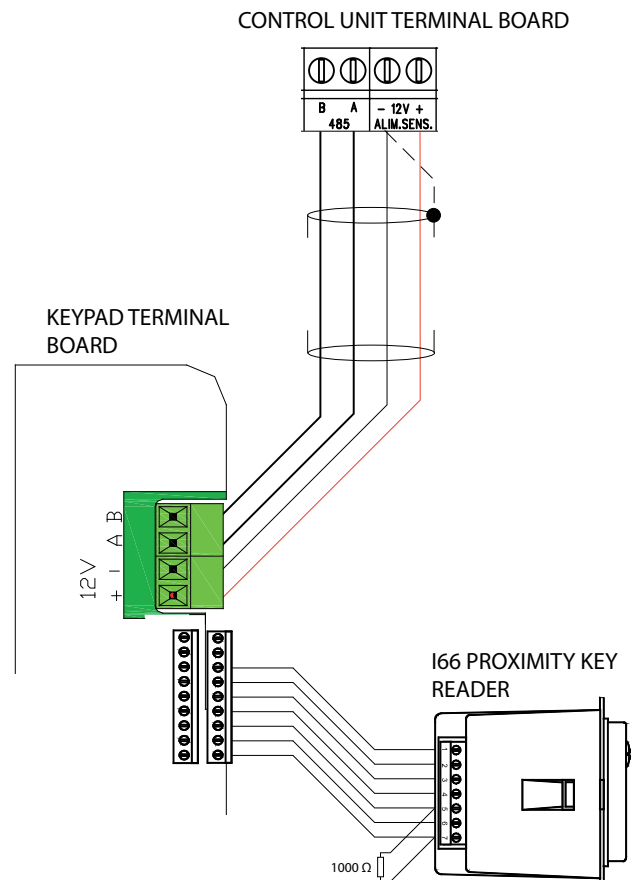


- Install ETRREL outside the control unit housing.
- Feed the cable through one of the holes at the bottom of the control unit.
- Connect the cable to the ELECTRONIC OUTPUTS connector on the control unit board.

6.5 CONTROL DEVICES

- Install the control devices (keypads, proximity key readers) as indicated in their manuals.
- Connect any keypads, 18 proximity (key) readers and key points through serial line as indicated in section “6.6 Serial line devices” on page 17.

I66 proximity key readers



- Connect any I66 proximity (key) readers to the dedicated terminals on the keypads.
- Connect a 1000 Ω termination resistor to terminals 5 and 7 of the I66 proximity (key) reader.

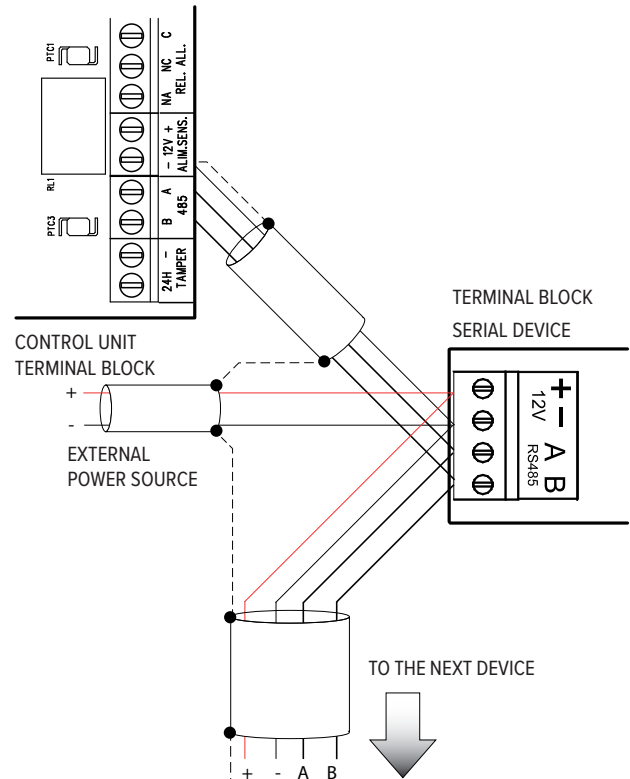
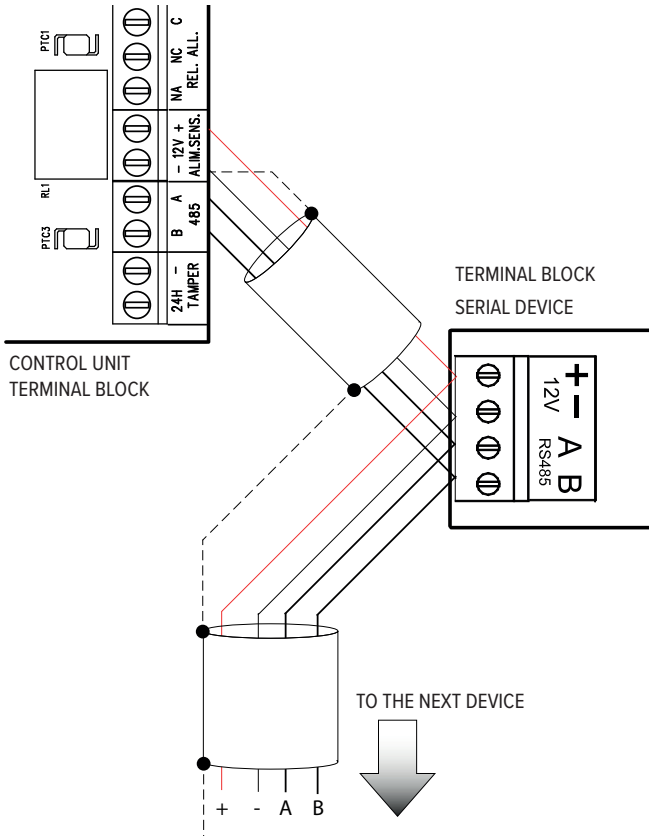
For compliance with the EN50131 standard:

- connect to each keypad only one I66 proximity (key) reader and set its presence control;
- leave the arming status display jumper connected.

6.6 SERIAL LINE DEVICES

Several types of devices may be connected with serial connection to the control unit:

- Control devices (keypad, proximity key readers)
- Concentrators, GATEWAY2K
- Sirens and detectors with serial interface
- Power supply units and fog systems

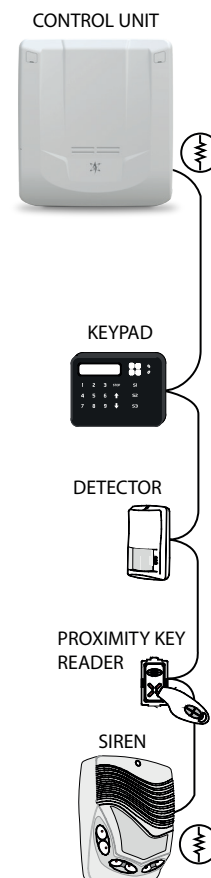


Note: Also in this case, join together the negative references of the control unit and the remote box.

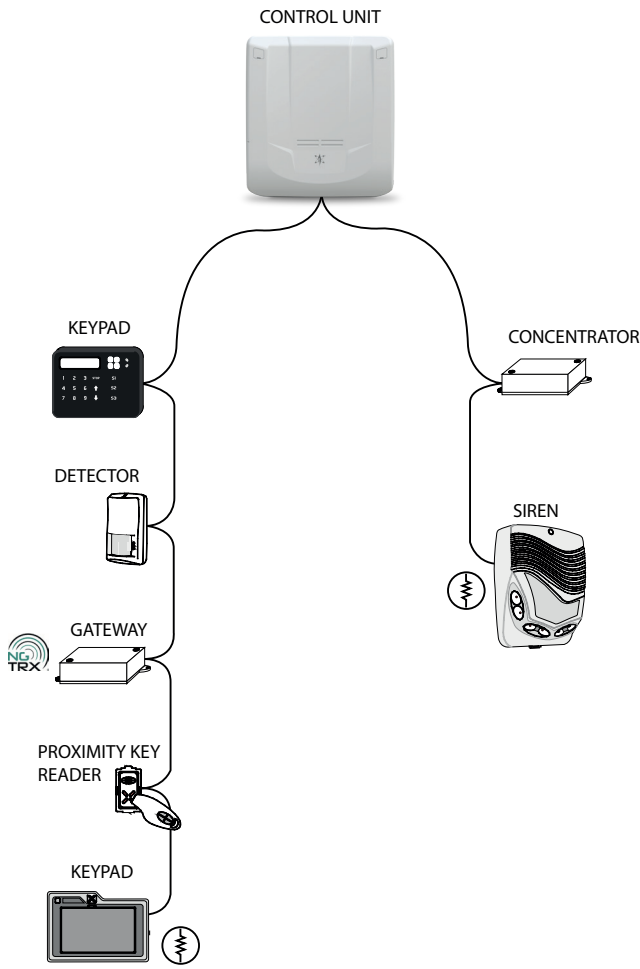
6.6.1 Simple serial line

Example: control unit at the beginning of the line

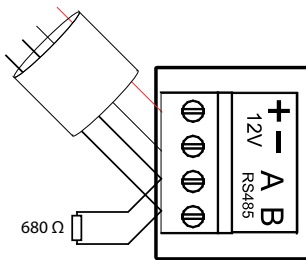
- Connect each device to the serial line using terminals A and B (in addition to the power source terminals). The line "enters" a device and, using the same terminals, "exits" towards the next device.
- Connect the cable shield (dashed line in the figure) to the 12V ALIM.SENS. negative terminal of the control unit. Isolate the cable shield on the last device.
- The +12V power source may not be directly supplied by the control unit, but rather, if required, by a separate source (for example a power supply unit):




Example: control unit at a mid point

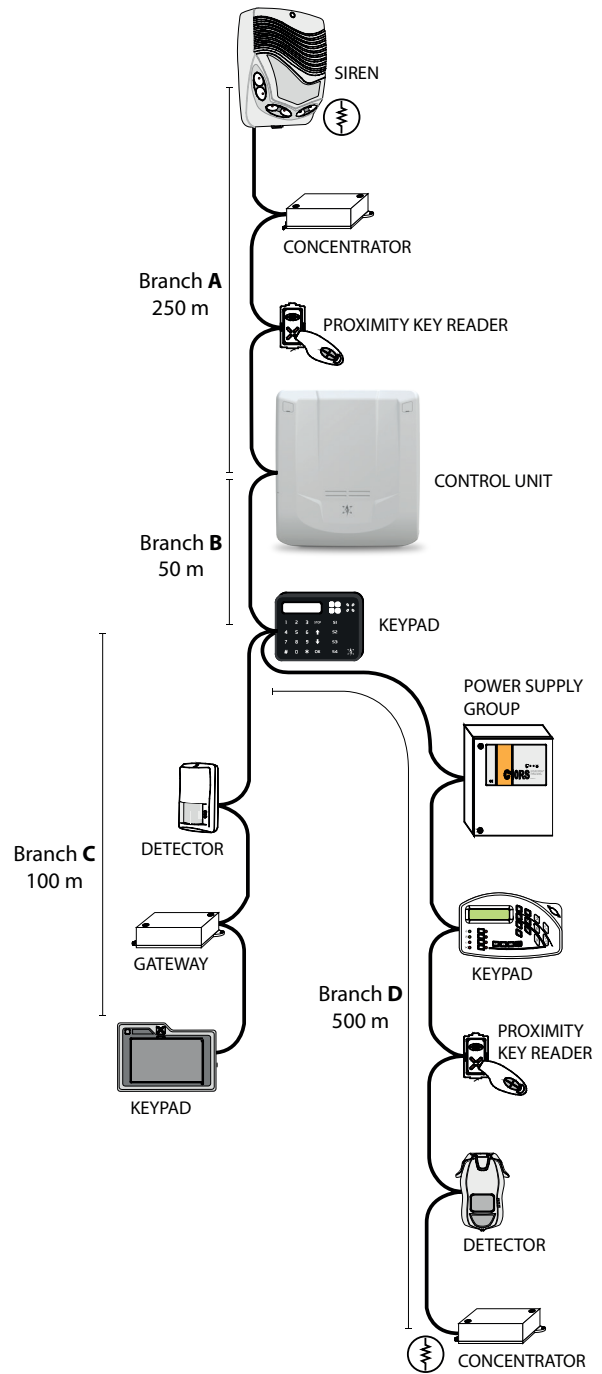


- Each serial device (including the control unit) may be positioned at any position along the bus.
- Use cables with the following sections: $2 \times 0.75 \text{ mm}^2$ (power source) + $2 \times 0.22 \text{ mm}^2$ (signal).
- The maximum number of control devices that can be connected is 16.



- Terminate the ends of the serial line: connect a 680Ω resistor to the A and B terminals of the two devices at the ends of the line (in the figure indicated with )

6.6.2 Serial line with branches



The serial line may be extended with branches, provided that the following rules are followed:

- the sum of the lengths of the branches must not exceed 1 km (in the previous image, considering the indicated values, the sum is 900 m);
- 680Ω termination resistors must be connected to the ends of the two longest branches (* in the figure).

For very long networks, consider the use of RPX485 repeaters for the repetition and isolation of the serial line. For their integration on the line, see the RPX485 manual.

6.6.3 Concentrator serial line addresses

Each concentrator takes on a set of consecutive addresses (8 for RIVER e RIVERRF, 4 for RIVERMINI4, 2 for RIVERMICRO2).

Set the address of each serial line concentrator as shown in the following tables:

• RIVERRF

Number of addresses	Dip on ON
1 - 8	1 2 3 4 5 6 7 -
9 - 16	- 2 3 4 5 6 7 -
17 - 24	1 - 3 4 5 6 7 -

• RIVER

Number of addresses	Dip on ON
1 - 8	1 2 3 4 5 6 7 -
9 - 16	- 2 3 4 5 6 7 -
17 - 24	1 - 3 4 5 6 7 -

• RIVERMINI4

Number of addresses	Dip on ON
1 - 4	1 2 3 4 5 6 - -
5 - 8	- 2 3 4 5 6 - -
9 - 12	1 - 3 4 5 6 - -
13 - 16	- - 3 4 5 6 - -
17 - 20	1 2 - 4 5 6 - -
21 - 24	- 2 - 4 5 6 - -

• RIVERMICRO2

Number of addresses	Dip on ON
1 - 2	1 2 3 4 5 6 7 -
3 - 4	- 2 3 4 5 6 7 -
5 - 6	1 - 3 4 5 6 7 -
7 - 8	- - 3 4 5 6 7 -
9 - 10	1 2 - 4 5 6 7 -
11 - 12	- 2 - 4 5 6 7 -
13 - 14	1 - - 4 5 6 7 -
15 - 16	- - - 4 5 6 7 -
17 - 18	1 2 3 - 5 6 7 -
19 - 20	- 2 3 - 5 6 7 -
21 - 22	1 - 3 - 5 6 7 -
23 - 24	- - 3 - 5 6 7 -

7. PUTTING INTO SERVICE

Once all the wiring has been completed and carefully checked, connect the power source to power the control unit.

The control unit can now be configured as indicated in the programming manual. The operations will require the use of the keypad menus and the BrowserOne software.

7.1 KEYPAD MENUS

There are two menus, which can be accessed in the following ways using the keypad:

7.1.1 Access to the user menu

- Enter the user code (6 digits, default 111111) followed by *.
- Press the arrow keys to navigate through the items.
- Press **OK** to access a menu item, or **STOP** to exit.

For a full guide to the use of the keypad menus see the programming manual.

7.1.2 Access to the installer menu

- Enter the installer code (8 digits, default 88888888) followed by **OK**.
- Press the arrow keys to navigate through the items.
- Press **OK** to access a menu item, or **STOP** to exit.

For a full guide to the use of the keypad menus see the programming manual.

Note: The authorisation for access for the installer (*TEMPORARY* or *PERMANENT*), must be granted by the user through the **INSTALLER AUTH** item of the user menu.

7.2 BROWSERONE

7.2.1 BrowserOne installation and update

See the programming manual for information on:

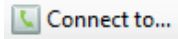
- first installation of BrowserOne: the standard installation procedure requires an Internet connection.
- BrowserOne update: instead of fully reinstalling BrowserOne on a PC where this is already installed (this causes the loss of software settings), it is possible to update to the latest software version.

7.2.2 Connecting the control unit to BrowserOne

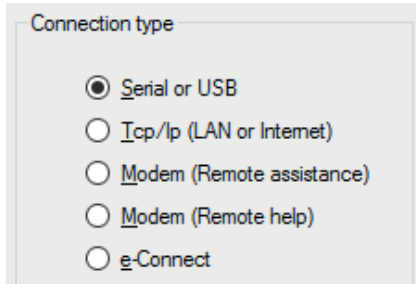
- Click the BrowserOne icon to open it.



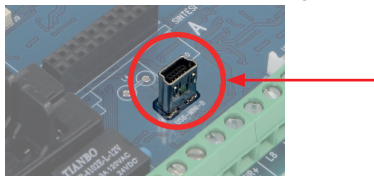
- In the top menu bar click **Connect** > **Connect to...** (also available in the control bar).




- In the page that opens select **Connection type**.



- Click **Next**. In the explanation that follows, a USB connection is used as an example.
- Connect the control unit to the PC using a mini B USB cable.



Wait for the COM port virtualisation software to load.

- In the **Serial connection** window click  to update the available communication ports. Select **ELMO Virtual COM** from the drop-down menu.
- Click **Next**: the software will attempt to establish the connection.
- Once the connection has been established, enter the installer code and click **OK**. A bar will appear at the bottom of the page.

7.2.3 Guide to the first configuration

To configure the control unit see the programming manual. In particular, follow the first section, **GUIDE TO THE FIRST CONFIGURATION** for completing the first control unit basic configuration. Below are some of the main options:

- CONNECT KEYPADS AND PROXIMITY KEY READERS
- CONNECT RIVER AND SERIAL LINE DETECTORS
- REGISTER THE INSTALLED MODULES
- PARTITION THE SYSTEM
- ACQUIRE DEVICES ON RIVERRF
- ACQUIRE DEVICES ON GATEWAY2K

- CONFIGURE A ZONE
- CONFIGURE AN USER
- ASSIGN SECTORS TO AN USER
- CONFIGURE THE OUTPUTS
- ACQUIRE AND CONFIGURE A REMOTE CONTROL
- CONFIGURE THE TELEPHONE DIALLER
- CONNECT THE CONTROL UNIT TO E-CONNECT

7.3 LEVEL OF EN50131 COMPLIANCE

The control unit was designed in compliance with the EN50131-3 standard, grade 2, environmental class 2.

Below are the options that must be enabled to ensure the required protection class.

7.3.1 Grade 2

In BrowserOne, go to **System Options** > **General** and tick the following options in the **EN50131 Options** panel:

- *Activate general alarm/siren only when system is armed.*
- *Activate arming lock.*
- *Limit Log File events.*
- *Visualization protection.*
- *Dialler delay on pre-alarm.*

7.3.2 Grade 3

This requires all the options for grade 2 to be ticked, and also that an external dialler of a compatible grade is used. The following must also be ticked:

- *Hide arming state.*
- *Required authorization of the installer for inclusion with faults/tampers.*
- *Erasing memories of fault/tamper permitted only by the installer.*
- *Zone exclusion only from installer.*

Lastly, the use of the technological event for the management of sensors with masking output is also required.

7.3.3 Grade 4 (partial)

This requires all the options for grade 3 to be ticked. The following must also be ticked:

- *Access Attempts Exceeded event as tamper event.*

Lastly, the use of the technological event for the management of sensors with range reduction output is also required.

8. MAINTENANCE

8.1 CONTROL UNIT RESET

To restore the control unit to its default configuration, complete the operations indicated below.

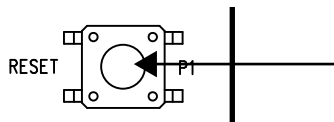
Warning: the procedure deletes all memory data. If necessary, these can be saved in BrowserOne before the reset.

8.1.1 With the control unit not in operation (first power connection)

- Press and hold **OK** on the keypad with address 1.
- Connect the power supply.
- When DEFAULT CONFIG.? Appears, release the **OK** key.
- Press **↓** and then **↑**. Wait for the REGISTER MODULES? message to appear.
- Press **OK** to register any installed modules, **#** to skip this step (it may also be completed later by accessing **REGISTER MODULES** in the installer menu). If the control unit is only powered through the power grid, after the registration of the modules, the BATTERY EXHAUSTED message will appear.

8.1.2 With the control unit already in operation

- Access the keypad installer menu: enter the installer code and press **OK**.
- Press **↓** or **↑** until **SYSTEM LOCK** is displayed. Press **OK**.
 - Press **OK** to lock the system. The LEDs of the keypads and the proximity (key) readers will flash.
- Open the control unit housing (see “4. PREGIO500 ASSEMBLY” on page 5).
- Close the (SIR +RIF) manual contact for the maintenance of any wired self-powered sirens (see “6.3.1 Outdoor wired sirens” on page 15).
- Press and hold down the RESET button (see “6.1 Electronic board view” on page 12).



- Press and hold **OK** on the keypad with address 1.
- Release the RESET button. When DEFAULT CONFIG.? appears, release the **OK** button.
- Press **↓** and then **↑**. Wait for the REGISTER MODULES? message to appear.
- The REGISTER MODULES? message will appear. Press **OK** to register any installed modules, **#** to skip this step (it may also be completed later by accessing **REGISTER MODULES** in the installer menu).

It is now possible to continue with the new programming.

Test the system and reactivate the sirens.

8.1.3 Default configuration

The reset brings the control unit back to the default configuration, which is the following:

- **Zones wired in the terminal block:** None
- **Zone configuration:** NO
- **Zone connection:** No zone connected
- **System keypad:** Keypad 1
- **Active area:** Area 1
- **Input programming:** All the zones associated to area 1
- **Active users:** User 1
- **User 1 code:** 111111
- **User 1 enabling level:** Basic maintenance
- **Installer code:** 88888888
- **Installer access authorisation:** *PERMANENT*
- **Alarm generation:** All the zones generate intrusion alarms
- **On-board relay:** Not active
- **Output time:** 15 s
- **Input time:** 10 s
- **General alarm type:** 1 min
- **Tamper alarm type:** 1 min

8.2 FIRMWARE UPDATE

The control unit firmware may be updated to add new functions.

The update can occur in two situations:

- the control unit has never been configured;
- the control unit is already configured and operational.

The update requires:

- PC with Windows 7, 8 or 10 operating system and BrowserOne installed, with PREGIO500 control unit module;
- miniB USB cable with 1 m maximum length.

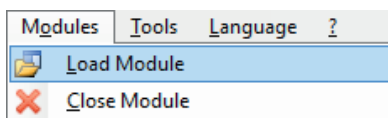
8.2.1 Preliminary operations

If the control unit is already configured, perform the following preliminary operations. If the control unit has never been configured (new installation), such preliminary operations may be ignored.

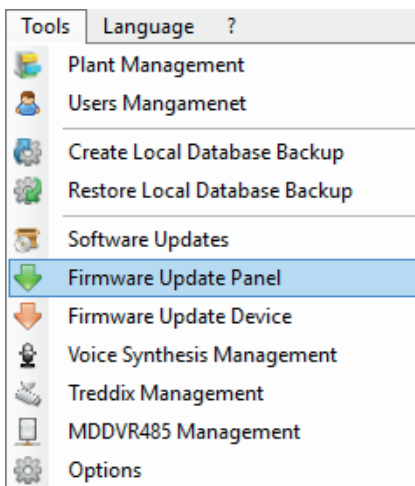
- Save the current control unit configuration: in the menu bar of BrowserOne click **File > Save As...**
- Access the keypad installer menu, enter the installer code and press **OK**.
- Press **↓** or **↑** until **SYSTEM LOCK** is displayed. Press **OK**.
 - Press **OK** to lock the system. The LEDs of the keypads and the proximity key readers will flash.
- Close the (+RIF) manual contact for the maintenance of any wired self-powered sirens (see “6.3.1 Outdoor wired sirens” on page 15).

8.2.2 Update procedure

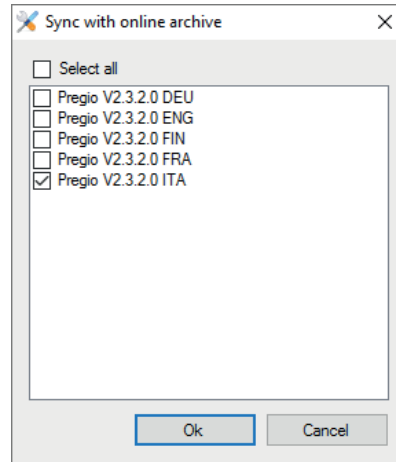
- Start BrowserOne. In the menu bar, click **Modules** and then **Load module**. Select the control unit in the list and press **OK**.




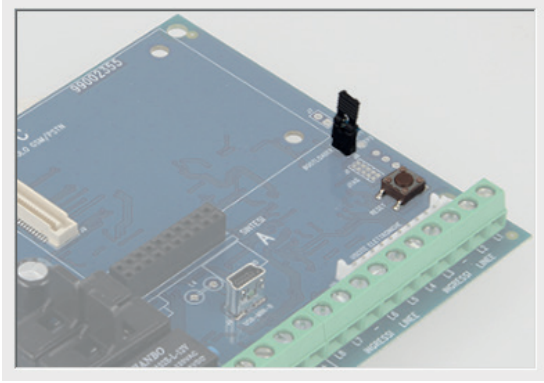
- In the menu bar, click **Tools** and then **Firmware Update Panel**.



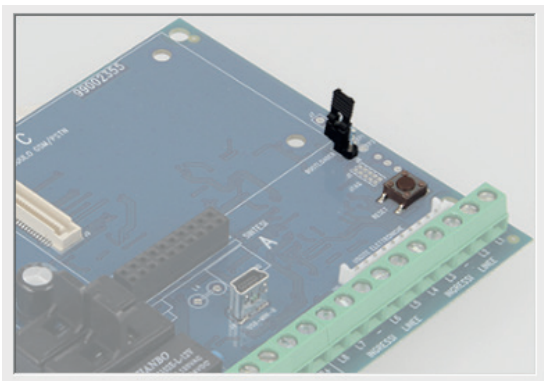
- The update file selection window will appear. Select the download location:
 - Click **Sync with online archive** to download the file from an online archive (recommended). A window will appear: tick the update file and click **OK**.



- Click **Browse** to select an update file already previously downloaded to the PC. Find the file and click **Open**.
- Click **Next** to continue.
- Open the control unit container, power the control unit and connect it to the PC using the miniB USB cable as shown in the “7.2.2 Connecting the control unit to BrowserOne” on page 20 section.
- In the **Update Settings** window just opened, enter the installer code. Click  to update the available communication ports. Select **ELMO Virtual COM** from the drop-down menu. Click **Next**.
- Select the update mode. We recommend to select **Standard Update**; **Emergency Update** should only be used in case of particular faulty situations. Click **Next**.
- Select the voice module update mode (any messages recorded by the MDVOICE64 module will not be cancelled). Click **Next**.
- The connection will be established. At the end, the summary screen will be displayed. Click **Next**.
- Switch the control unit to "firmware update" mode: close the J8 jumper and then press and release the RESET button. The BrowserOne window will show the operations to be completed. At the end click **Next**.



- The update will be completed. Click **Next**.
- Switch the control unit to operating mode: open the J8 jumper and then press and release the RESET button. The BrowserOne window will show the operations to be completed. At the end click **Next**.



- After the update procedure has been completed successfully, click **End** to terminate it.

The procedure will preserve the configuration of the control unit before the update. If this is not the case (due to update problems), it will be possible to upload the previously saved configuration: in the menu bar, click **File > Open**.

After uploading it and making any necessary changes, the configuration can be written to the control unit by clicking **Actions > Write setup**.

8.3 CHANGING THE BATTERY OF WIRELESS DEVICES

In case a device's battery is low, the anomaly and its related control unit event are signalled.

Replace the battery as follows:

- Exclude the zone on which the device is acquired: use the **BYPASS ZONES** entry in the user or installer menu. When the zone is excluded, the tamper protection is also excluded: the tamper event is logged but the tamper alarm is not triggered.
- Open the device housing and replace the battery with one of the same model.
- Close the device housing.
- Include the zone (use the **BYPASS ZONES** entry again).

9. EU DECLARATION OF CONFORMITY



The product complies with the current European EMC and LVD directives. The complete text of the EU Declaration of Conformity is available at the following Internet address: elmospa.com (simple registration required).

10. WARNINGS

Warnings for the installer

- Comply strictly with current standards governing the installation of electrical systems and security systems, and with the manufacturer's directions given in the manuals supplied with the products.
- Provide the user with full information on using the system installed and on its limitations, pointing out that there are different levels of security performance that will need to suit the user's requirements within the constraints of the specific applicable standards. See that the user looks through the warnings given herein.
- Work involved in the design, installation and maintenance of systems incorporating this product should be performed only by personnel with suitable skills and knowledge required to work safely so as to prevent any accidents. It is vital that systems be installed in accordance with current legislation. The internal parts of certain equipment are connected to the power grid and therefore there is a risk of electrocution when maintenance work is performed inside without first disconnecting the primary and emergency power supplies. Certain products include batteries, rechargeable or otherwise, as an emergency backup power supply. If connected incorrectly, they may cause damage to the product or property, and may endanger the operator (explosion and fire).

Warnings for the user

- Check the system's operation thoroughly at regular intervals, making sure the equipment can be armed and disarmed properly.
- Make sure the system receives proper routine maintenance, employing the services of specialist personnel who meet the requirements prescribed by current regulations.
- Ask your installer to check that the system suits changing operating conditions (e.g. changes in the extent of the areas to be protected, change in access methods, etc...)

General warnings

- This device has been designed, built and tested with the utmost care and attention, adopting test and inspection procedures in compliance with current legislation. Full compliance of the working specifications is only achieved in the event the device is used solely for its intended purpose, namely:

Multi-functional hybrid control unit for intrusion detection systems

- The device is not intended for any use other than the above and hence its correct functioning in such cases cannot be assured. Consequently, any use of the manual in your possession for any purpose other than those for which it was compiled - namely for the purpose of explaining the product's technical features and operating procedures - is strictly prohibited.
- Production processes are closely monitored in order to prevent faults and malfunctions. However, the componentry adopted is subject to an extremely modest percentage of faults, which is nonetheless the case with any electronic or mechanical product. Given the intended use of this item (protection of property and people), we invite you to adapt the level of protection offered by the system to suit the actual situation of risk (allowing for the possibility of impaired system operation due to faults or other problems), while reminding you that there are specific standards for the design and production of systems intended for this kind of application.
- **We hereby advise you (the system's operator) to see that the system receives regular routine maintenance, at least in accordance with the provisions of current legislation, and also check on as regular a basis as the risk involved requires that the system in question is operating properly, with particular reference to the control unit, sensors, sounders, dialler(s) and any other device connected. You must let the installer know how well the system seems to be operating, based on the results of periodic checks, without delay.**

- Work involved in the design, installation and maintenance of systems incorporating this product should be performed only by personnel with suitable skills and knowledge required to work safely so as to prevent any accidents. It is vital that systems be installed in accordance with current legislation. The internal parts of certain equipment are connected to the mains and therefore there is a risk of electrocution when maintenance work is performed inside without first disconnecting the primary and emergency power supplies. Certain products include batteries, rechargeable or otherwise, as an emergency backup power supply. If connected incorrectly, they may cause damage to the product or property, and may endanger the operator (explosion and fire).

Fundamental safety rules

- The use of the device is forbidden for children and unassisted disabled individuals.
- Do not touch the device when bare footed, or with wet body parts. Do not directly spray or throw water on the device.
- Do not pull, remove or twist the electric cables protruding from the devices even if the same is disconnected from the power source.

Disposal warnings



IT08020000001624

In accordance with Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), please be advised that the EEE was placed on the market after 13 August 2005 and must be disposed of separately from normal household waste.

For correct operation, this product requires the use of a buffer battery. The same applies to any installed additional power source units, accessories and optical-acoustic indicators installed in the system. Should the batteries need replacing, with new ones with the same characteristics, the old ones must be taken to an authorised waste disposal site. The materials used for this product are highly toxic and polluting if dispersed into the environment.

11. TABLE OF CONTENTS

1. TECHNICAL SPECIFICATIONS	2	6.2.5 Fast zone	14
2. BEFORE INSTALLATION	3	6.2.6 Key zone	15
2.1 SYSTEM AUTONOMY CALCULATION CONSIDERATIONS	3	6.3 SIRENS	15
3. INDICATIONS FOR COMPLIANCE TO EN50131 REGULATION,		6.3.1 Outdoor wired sirens	15
GRADE 2	3	6.3.2 Indoor wired sirens	15
3.1 SYSTEM CONFIGURATION	3	6.4 ELECTRONIC OUTPUTS	16
3.2 POWER SUPPLY FROM MAINS AND SYSTEM AUTONOMY	3	6.5 CONTROL DEVICES	16
3.3 INTRUSION DETECTION	3	6.6 SERIAL LINE DEVICES	17
3.4 TAMPER DETECTION	4	6.6.1 Simple serial line	17
3.5 FAULT DETECTION	4	6.6.2 Serial line with branches	18
3.6 ASSAULT DETECTION	4	6.6.3 Concentrator serial line addresses	19
3.7 MASKING DETECTION	4	7. PUTTING INTO SERVICE	19
3.8 ACCESS LEVELS	4	7.1 KEYPAD MENUS	19
3.9 PERIODIC MAINTENANCE	4	7.1.1 Access to the user menu	19
3.10 CURRENT DISTRIBUTION FOR IMQ - SECURITY SYSTEMS CERTIFICA-		7.1.2 Access to the installer menu	19
TION	4	7.2 BROWSERONE	19
3.11 CURRENT DISTRIBUTION FOR INCERT CERTIFICATION	4	7.2.1 BrowserOne installation and update	19
3.12 CLASSIFICATION OF NOTIFICATIONS (ACCORDING TO TABLE 10		7.2.2 Connecting the control unit to BrowserOne	20
EN50131-1)	4	7.2.3 Guide to the first configuration	20
4. PREGIO500 ASSEMBLY	5	7.3 LEVEL OF EN50131 COMPLIANCE	20
4.1 MODULE INSTALLATION	7	7.3.1 Grade 2	20
4.1.1 MDVOICE64	7	7.3.2 Grade 3	20
4.1.2 MDWIFIH	7	7.3.3 Grade 4 (partial)	20
4.1.3 MDPSTN	7	8. MAINTENANCE	21
4.1.4 MDGSMI	8	8.1 CONTROL UNIT RESET	21
5. PREGIO500PL ASSEMBLY	9	8.1.1 With the control unit not in operation (first power connec-	
5.1 CONNECTING THE POWER SUPPLY UNIT	10	tion)	21
5.2 PROTECTION AGAINST OPENING AND REMOVAL FROM THE MOUNTING		8.1.2 With the control unit already in operation	21
SURFACE	11	8.1.3 Default configuration	21
6. WIRING	12	8.2 FIRMWARE UPDATE	22
6.1 ELECTRONIC BOARD VIEW	12	8.2.1 Preliminary operations	22
6.1.1 Terminal block	12	8.2.2 Update procedure	22
6.2 WIRED ZONE CONNECTION	13	8.3 CHANGING THE BATTERY OF WIRELESS DEVICES	23
6.2.1 Double balancing	13	9. EU DECLARATION OF CONFORMITY	24
6.2.2 Triple balancing	13	10. WARNINGS	24
6.2.3 Split zones	13	11. TABLE OF CONTENTS	26
6.2.4 Extended split zone	14		

