

PROXIMA SERIES

Multi-functional hybrid intrusion detection system control units



1 DESCRIPTION

PROXIMA is a series of multi-functional hybrid control units that support both wired and wireless devices.

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

They are compatible with the first generation radio technology through the use of RIVERRF concentrators and with the NG-TRX radio technology after connecting a GATEWAY2K over serial line.

Optional modules may be connected to expand its functions:

- MDGSM: it makes it possible to connect the control unit to a GSM/GPRS network.
- MD4GE: makes it possible to connect the control unit to a LTE network.
- 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.
- MDRS232: allows interfacing to external devices via RS-232 serial line.

The PROXIMA control units can be managed via keypad menus and BrowserOne software.

You can also connect to e-Connect.

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

The PROXIMA control units are certified IMQ - Security

Systems.



Refer to the instruction manual.

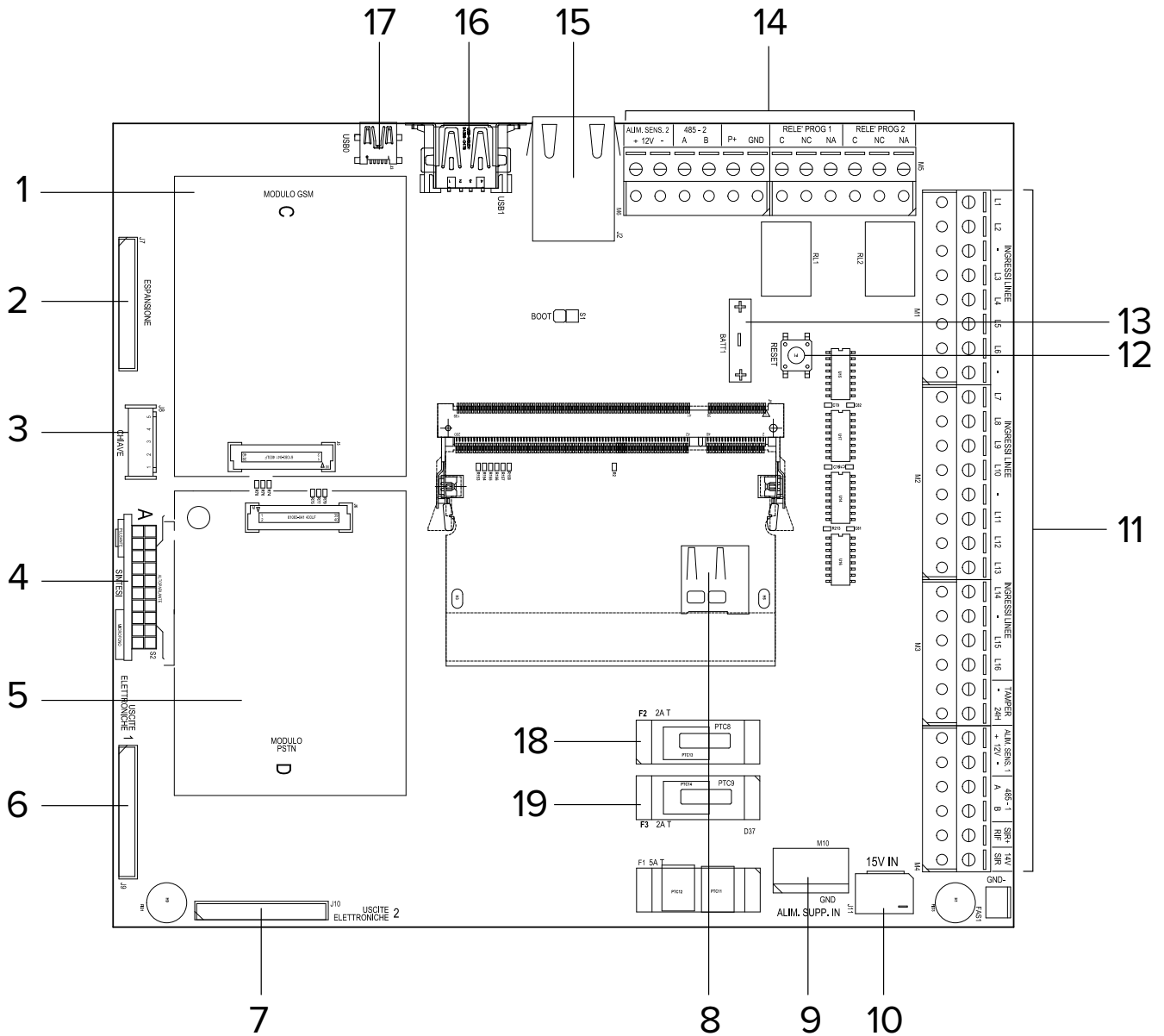
2 HARDWARE FEATURES

- On-board power source up to 5 A (of which 4 A available at loads)
- Integrated 10/100 Mbps Ethernet module
- 1 USB device port + 1 USB host port
- 1 MicroSD card slot (up to 128 GB)
- 2 expansion slots for module housing
- 1 connector for speech synthesis module
- 1 key connector
- 1 generic expansion connector
- 2 output connectors for ETRREL

Removable terminals:

- 16 on-board inputs INGRESSI LINEE, (which can be expanded to 32 using the split function), 12 fast inputs
- 2 independent outputs for sensor supply (ALIM. SENS. 1, 2)
- 2 independent RS-485 serial outputs ULTRABUS (485-1, 485-2)
- 2 programmable 3 A relays (RELE' PROG 1, 2)
- 1 programmable output for controlling a power relay (P+)
- 1 Tamper input (TAMPER)
- SIR +, 14V for siren control and power supply (SIR+, 14V)

3 PCB



- | | |
|---|---|
| <ul style="list-style-type: none"> 1 MDGSME module slot 2 Expansion connector 3 Key connector 4 Speech synthesis connector 5 MDPSTN module slot 6 ETRREL 1 electronic output expansion connector 7 ETRREL 2 electronic output expansion connector 8 MicroSD card slot module 9 Additional power supply connector 10 Power supply unit connector | <ul style="list-style-type: none"> 11 Terminal block 1 12 Reset button 13 Backup battery (for clock maintenance) 14 Terminal block 2 15 LAN connector 16 USB connector 17 USB mini-B connector 18 Fuse F2 to protect ALIM. SENS. 1 (detector supply) line 19 Fuse F3 to protect ALIM. SENS. 2 (detector supply) line |
|---|---|

Terminal block 1

Terminals	Function
INGRESSI LINEE (L1 - L16)	Wired zone connection
TAMPER	Anti-tamper protection line connection
ALIM. SENS. 1	Device power supply line 1 (12 V)
485-1	Serial line 1
SIR+ RIF	Self-powered siren reference
14V SIR	Siren power source

Terminal block 2

Terminals	Function
ALIM. SENS. 2	Device power supply line 2 (12 V)
485-2	Serial line 2
P+	Programmable output
RELE' PROG 1	Programmable relay connection 1
RELE' PROG 2	Programmable relay connection 2

4 TECHNICAL DATA


Model	PRX128	PRX256	PRX1024	
General features				
No. of on-board wired zones	16 (32 with split function)			
Max. no. of supported zones	128	256	1024	
Number of supported outputs (max)	128	256	1024	
Max. no. of users	1024			
Maximum number of controls	32 (of which a maximum of 32 advanced keyboards)			
Max no. of gateways	4			
Maximum number of serial devices	32 (to be chosen among power supplies, sirens, fog generators, GATEWAY2K etc.)			
Maximum number of supported D-Pulse devices	64			
History log capacity	5000			
Protection class	IP3X			
Working temperature	-10 / +55			°C
Certifications	IMQ-Security Systems and INCERT EN 50131-3, EN 50131-6, EN 50136-2, EN 50131-10, T031, grade 4/3/2, environmental class II, SP5-DP4			
Environmental class	II			
Dimensions	W 316 × H 305 × D 143	W 430 × H 354 × D 212		mm
Weight	4.00	6.30		kg
Ripple	200 mV peak-to-peak			
Power supply				
Mains power source	AC 230 V +10% - 15% 50 Hz 1520 mA, 50 Hz; 5 A A-type power supply (mod. AL75LRS15V0); total current available at loads: 4 A (2 A per SENS. POW. 1 and 2 A for SENS. POW. 2)			
Battery	max 18 Ah / DC12V (not supplied)	max 40 Ah / DC12V (not supplied)		
Minimum power supply	9.0			V
Maximum operating voltage	15.0			V
Maximum power absorption from mains	850 mA @ 230 Vac (1520 mA @ 100 Vac)			
Battery electrical values				
Battery recharge voltage	13.8			V
Discharged battery threshold	10.5			V
Battery restore threshold	12.5			V
Battery release voltage	9.0			V
Max battery recharging current	600			mA
14V SIR. terminal electric values				
14V SIR. terminal rated current	14.5			V
14V SIR. fault voltage	9.7			V
14V SIR. fault reset voltage	10.7			V
14V SIR. terminal maximum current	250.0			mA
SENS. POW. 12V terminal electric values				
Rated voltage (with mains)	13.7			V
Terminals 12V SENS. fault voltage	10.0			V
Terminals 12V SENS. fault reset voltage	12.0			V
12V SENS. terminal maximum current	2			A
15V power supply input terminal electric values				

Model	PRX128	PRX256	PRX1024	
No power source		12.8		V
No power source reset		13.5		V
Power consumption at 12V				
Control unit only (on or off)		82		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
Idle PSTN module		2		mA
PSTN module operating in digital mode		56		mA
Speech synthesis module in play		10		mA
LAN module in use		14		mA
Electrical output P + values				
Rated output voltage P+		13.6		V
Maximum output current P+		120		mA

Parts supplied

- Balancing resistors: 33 × 1500 Ω, 16 × 2200 Ω, 16 × 1000 Ω, 16 × 1200 Ω, 20 × 680 Ω
- 2 strips of double-sided tape for battery lock
- Cable for earth connection (only for use with MDGSME)
- Anti-tear tamper kit (for PRX128 model already pre-assembled)
- Nylon cable ties
- User manual
- Quick guide

5 BEFORE INSTALLATION

 *General warnings are at the end of this manual.*

- The electronic board may be damaged by electrostatic discharges. The installer must avoid any presence of electrostatic discharges.
- 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.
- Disconnect all mains power when connecting the switching power supply unit of the control unit to the power grid.

Note: equipment suitable for mounting at heights lower than or equal to 2 m.

5.1 System autonomy

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 18 Ah, the total load applied to guarantee 12 hours of autonomy is 1,5 A.

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.

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

5.2 Indications for compliance with EN 50131 grade 3

- The minimum configuration that guarantees compliance to grade 3 requires the mandatory use of the self-powered siren and the MDPSTN/MDGSME telephone dialler.

BrowserOne settings

Enable all EN 50131 options in the unit on page **System Options > General** of BrowserOne.

Set the following "General options":

- "Lock Dialler at Disarming Event" always OFF;
- "Deactivate Keypads Tamper" always OFF;
- "Silence Keypads during Exit Time" always OFF;
- "Disable phone numbers editing from keypad" always ON;
- "Input alarm excluded on red LED of alarm" always OFF;
- "Enable fast arming" always OFF;
- "'Fast arming/output maneuver' pressing (...)" always OFF;
- "Tampering excludable" always OFF.

Set the following timers:

- "General Alarm Relay Time", "Tamper Alarm Relay Time": 90 s minimum;
- "Mains Failure Delay": 1 h max;
- Entrance/exit time: 45 s max.

The following functions are not certified IMQ-Security Systems:

- all the functions that disable tamper protection;
- zone types NO, NC, SPLIT, OUTPUT STATUS, zones associated to domotic and fire detection functions;
- zone events: FIRE ALARM, MEDICAL ALARM, HELP REQUEST, GAS ALARM, FLOOD ALARM, FIRE ALARM FAULT, TECHNOLOGICAL, KEY ZONE

Zone options KEY ZONE, DELAYED, AUTO-BYPASS make the certification decade.

Mains supply and system autonomy

- Insert a 16 A curve C circuit breaker in the electrical system.
- Set a delay for the mains failure signal not exceeding 1 minute.
- Use a battery with a capacity not exceeding 15 Ah.

Detection

- The connections of the zones indicated below result in the decay of grade 2: Normally closed, Normally open, Pre-alarm, Delayed, Autoexclusion, Key input.
- Tamper detection must not be disabled: each option that disables tamper detection does not comply with EN50131.
- Associate a remote transmission (activation of the dialler) to all INTRUSION, TAMPER, FAULT and ROBBER (AGGRESSION) events.
- Connect the MASC output of each device that supports the anti-masking function to a control unit zone programmed as FAULT.

Fault

- Option "Delayed" with 10 s time must be associated to the zones programmed with "Fault" event.
- Set triple balance to zones programmed with "Fault", "Zone Mains Failure", "Zone low battery", "Zone siren

fault" events and associate them to fault contact in order to have them processed as fault.

- For each fault event, a notification must be triggered both when the system is armed and when it is disarmed.

Tamper

- For grade 2, option "Repeat tamper alarm to general alarm relay" must be enabled.
- Tamper must be set as excludable only by the installer.

Arming failure

- Provide for the activation of a remote notification in case of "Failed arming" event.

Inhibition and exclusion

- For inhibition function, use the user authorization levels. If a zone is intended to be used as "assault" zone, it must have an higher authorization level than the base one.
- Enabling the general option "Zone exclusion only from installer", the function becomes an ISOLATION one and no more an exclusion one, since a zone remains excluded until it is manually included again at access level 3.
- For compliance with T031, the automatic exclusion must be set to 3 minimum.

"Robbery" and "assault" zones

- The "Assault alarm" event must be associated to any "robbery" zone and "24H" option must be enabled to such zone.
- In order to force the arming of a "robbery" active zone, the general options "Enable force arming zones" and "Cancel auto-bypass at zone reset" must be enabled as well.
- The remote notification must identify the active zone.
- For an "Assault" zone, it is not possible to enable "Alarms per Zone (Max)" option.

Testing functions

- Perform a SYSTEM TEST periodically (consult the control unit programming manual for detailed information).
- Provide for an output that can be enabled remotely for device testing.

Battery recharge

The control unit reads the environmental temperature using the on-board NTC.

The battery voltage range is 13.7 V at 25°C, with -18 mV/°C compensation.

The control unit starts recharging if the battery voltage value is lower than the target.

The battery test is performed every 24 hours or upon user request.

The amount of time for 80% recharge is 24 hours.

Overvoltage protection is guaranteed by the power supply unit (125%).

5.2.1 Classification of notifications

Grade 2

Notification equipment	A	B	C	D	E	F	Grade
Remotely powered audible warning devices	2 dev.	-	-	-	-	-	2
Self-powered audible warning devices	-	1 dev.	-	-	1 dev.	-	2
ATS	SP2	SP2	DP1	-	-	DP2	2

- SP2: MDPSTN board in voice protocol (periodic transmission 25 h);
- SP2: MDGSME or MDGSME90 board in voice protocol (periodic transmission 25 h);
- SP2: MD4GE board in voice protocol (periodic transmission 25 h);
- DP1/DP2: MDPSTN board and MDGSME or MDGSEM90 or MD4GE board in voice protocol (periodic transmission set 30 min or 25 h).

Grade 3

Notification equipment	A	B	C	D	E	Grade
Remotely powered audible warning devices	2 dev.	-	-	-	-	3
Self-powered audible warning devices	-	1 dev.	-	-	-	3
ATS	SP3	SP3	DP2	SP4	DP3	3

- SP3/SP4: MDGSME or MDGSME90 or MD4GE board in SIA DC-09 or e-Connect protocol (periodic transmission 30 min or 3 min);
- SP3/SP4: LAN integrated on-board in SIA DC-09 or e-Connect protocol (periodic transmission 30 min or 3 min);
- DP2/DP3: MDGSME or MDGSME90 or MD4GE and LAN integrated on-board in SIA DC-09 or e-Connect protocol (periodic transmission 30 min or 3 min).

Grade 4

Notification equipment	A	B	C	Grade
Remotely powered audible warning devices	2 dev.	-	-	4
Self-powered audible warning devices	-	1 dev.	-	4
ATS	SP5	SP5	DP4	4

- SP5: MDGSME or MDGSME90 or MD4GE board in SIA DC-09 or e-Connect protocol (periodic transmission 90 s);

- SP5: LAN integrated on-board in SIA DC-09 e-Connect protocol (periodic transmission 90 s);
- DP4: MDGSME or MDGSME90 or MD4GE and LAN integrated on-board in SIA DC-09 e-Connect protocol (periodic transmission 90 s).

5.2.2 Current distribution for IMQ - Security Systems certification

For grade 3/4 (30 h autonomy):

- 0.1 A for board self-consumption;
- 0.5 A for external devices (18 Ah battery);
- 0.6 A for battery recharge.

For grade 2 (12 h autonomy):

- 0.1 A for board self-consumption;
- 1.4 A for external devices (18 Ah battery);
- 0.6 A for battery recharge.

Current distribution with automatic change (4 h autonomy):

- 0.1 A for board self-consumption;
- 4.3 A for external devices (18Ah battery);
- 0.6 A for battery recharge.

5 A maximum output current:

- 4.4 A for external devices and board self-consumption;
- 0.6 A for battery recharge.

5.2.3 Current distribution for INCERT certification

For grade 3/4 (autonomy 60 h or 48 h with fault transmission), with 12V 18Ah battery:

- 0.1 A for board self-consumption;
- 0.2 or 0.27 A for external devices (18Ah battery);
- 0.6 A for battery recharge.

For grade 2 (24 h autonomy):

- 0.1 A for board self-consumption;
- 0.65 A for external devices (18 Ah battery);
- 1.55 A for external devices (40 Ah battery, only for PRX1024, PRX256, PRX128M);
- 0.6 A for battery recharge.

5.2.4 Warnings concerning the electrical aspects

- The battery must be a VRLA-type (Valve Regulated Lead Acid) battery and have UL94V-1 or better flammability rating case. It must comply with IEC 60896-21:2004 and/or IEC 60896-22:2004 regulations. The battery must be replaced by experienced personnel.
- 2500 V CAT II power supply unit. The power supply unit which, once installed, is subject to transient voltages higher than those of the design overvoltage category, requires additional protection from transient voltages external to the equipment.
- All the free-from-potential contacts of the relays mounted on the control unit boards must be wired to circuits that operate with SELV voltages only.
- The end of a stranded conductor must not be bonded with soft soldering where the conductor is subjected to contact pressure.

- An easily accessible disconnecting device must be provided.

5.3 Usage with NG-TRX devices

Each PROXIMA control unit can support a maximum number of NG-TRX devices equal to the number of its zones (128 for PRX128, 256 for PRX256, 1024 for PRX1024).

The number of NG-TRX devices in use affects the minimum settable supervision time and may require multiple GATEWAY2K devices according to the indications in table below.


Number of NG-TRX devices	Minimum supervision time	Number of GATEWAY2K
Up to 64	-	1 or more
65 ÷ 128	20 minutes	1 or more
129 ÷ 256	1 h	2 or more
257 ÷ 512	2 h	3 or more
513 ÷ 1024	4 h	4

In each one of the previous cases, the maximum allowed number of volumetric detectors or magnetic contacts with frequent opening is 64.

If a great number of volumetric detectors is being used, we recommend setting the inhibition time to its maximum value (5 minutes).

If multiple GATEWAY2K devices are required, avoid installing them close to one another. Install them, if possible, so that each one will cover different parts of the system.

Note: using the option **Delay supervision anomaly** in BrowserOne might make the previous indications less essential.

 *The presence of interference or harsh environmental conditions may significantly affect the ability of the system to manage a great number of radio detectors.*

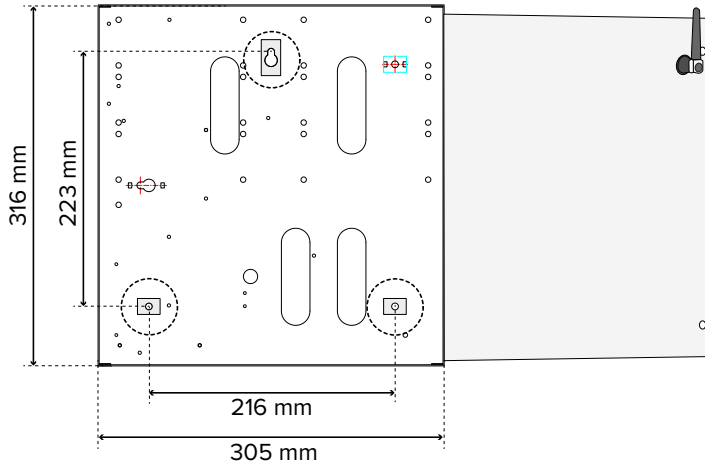
6 DEVICE MOUNTING

6.1 PRX128

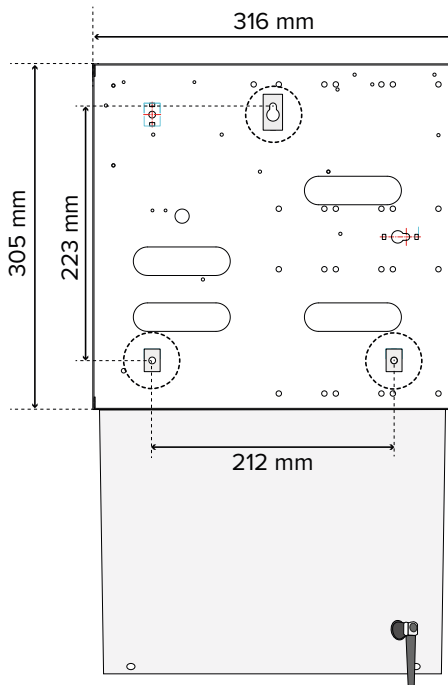
- **Opening the housing**
 - unscrew cover closing screws
 - open control unit door

- **Fixing the container**

PRX128: side opening (rear view)



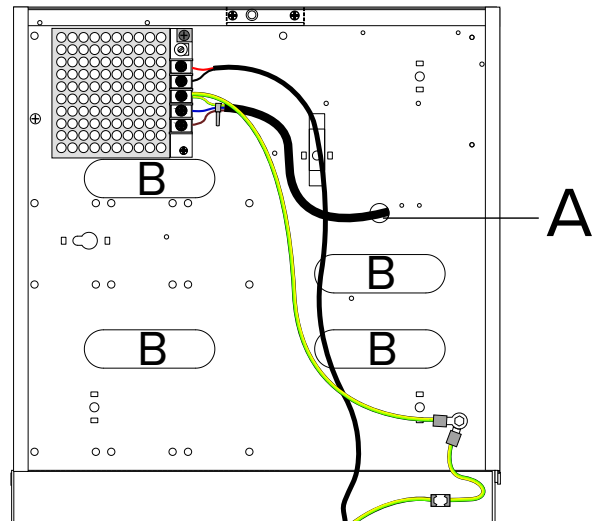
PRX128: tilt opening (rear view)



- move the fastening feet as shown in the previous figures, depending on whether the control unit is mounted so that its door opens laterally or downwards
 - place the base of the housing on the wall surface
 - mark the fixing points
 - fix the base to the wall using 8mm or larger screws and plugs (depending on the weight of the battery)
- The images presented below refer to the installation by tilting opening.

- **Cable routing**

! Make sure the cables are not connected to the power supply.



- feed 230 V mains cable through hole A
- feed system cables through holes B

Note: the entry of the cables can also be done from the top after drilling the container in the prepared areas.

- **Wirings**

- install any optional modules on the control unit board as indicated in chapter 6.3 p. 11
- wire terminals

Power supply unit connection

- wire mains cables to phase and neutral terminals of the power supply unit (N and L terminals)
- wire ground cable to central terminal \perp
- fasten the network cables together using a cable tie

! Keep a maximum distance of 2 cm between the fixing point and the terminal block.

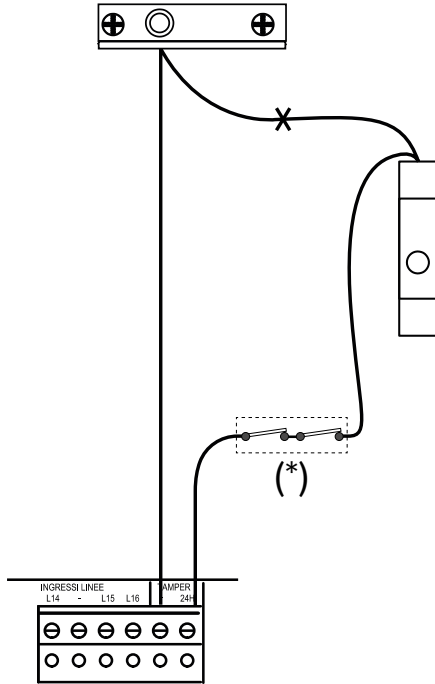
- wire power supply output cables (+ and - terminals) to connector J11 on board

Battery connection

- arrange the battery inside the case: place two double-sided adhesive tape strips (supplied) between the battery and the bearing plane on control unit bottom
- connect the black and red cables (coming from control unit board) to battery terminals

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.

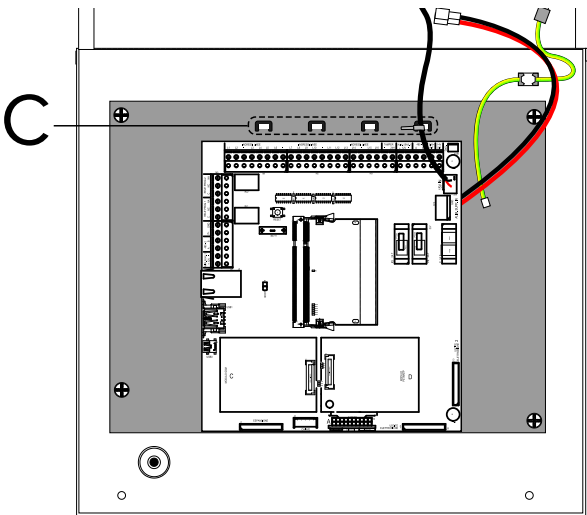
Tamper protection connection



(*) tamper contacts of the devices

- weld and insulate the two cables (one coming from the anti-opening switch, the other from the anti-tear switch) in point X in the figure
- connect the anti-opening and tear-proof switches of the container and the tamper contacts of the devices that provide it in series with the TAMPER terminals in the control unit board, as shown

• Closing the housing



- fasten all the cables connected to the board to the appropriate fixing points (C) using cable ties
- close the control unit door
- screw the screws on the container

6.2 PRX256 - PRX1024

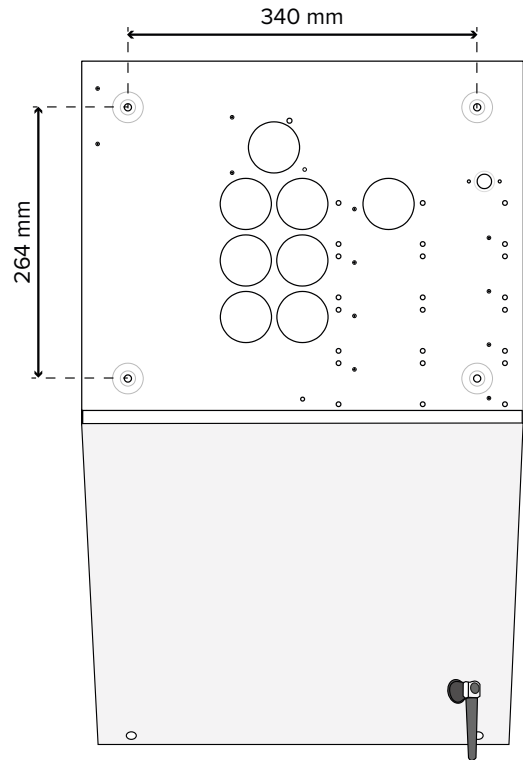
• Opening the housing

- unscrew cover closing screws

- open control unit door

• Fixing the container

PRX256 - PRX1024: tilt opening (rear view)

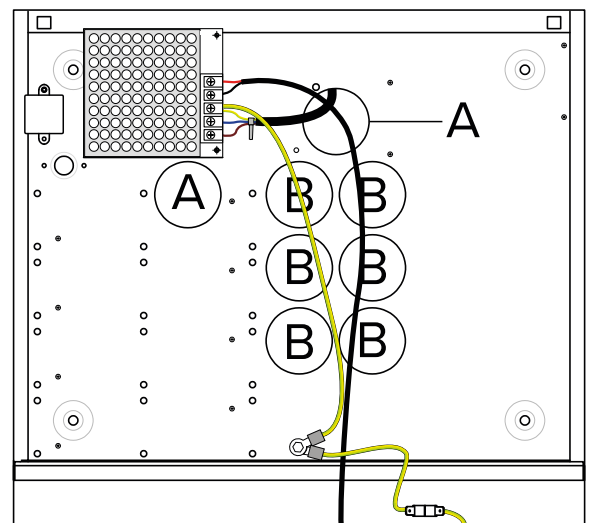


(for side opening, the fixing centre to centre distance are the same)

- place the base of the housing on the wall surface
- mark the fixing points
- fix the base to the wall using 8 mm or larger screws and plugs (depending on the weight of the battery)

• Cable routing

! Make sure the cables are not connected to the power supply.



- insert the 230 V power cable into one of the holes A
- feed system cables through holes B


Note: the entry of the cables can also be done from the top

after drilling the container in the prepared areas.

• **Wirings**

- install any optional modules on the control unit board as indicated in chapter 7 p. 13
- wire terminals

Power supply unit connection

- wire mains cables to phase and neutral terminals of the power supply unit (N and L terminals)
- wire ground cable to central terminal 
- fasten the network cables together using a cable tie

 *Keep a maximum distance of 2 cm between the fixing point and the terminal block.*

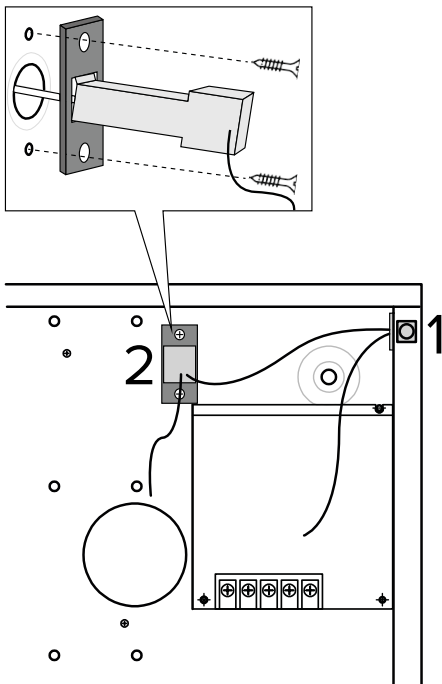
- wire power supply output cables (+ and - terminals) to connector J11 on board

Battery connection

- arrange the battery inside the case: place two double-sided adhesive tape strips (supplied) between the battery and the bearing plane on control unit bottom
- connect the black and red cables (coming from control unit board) to battery terminals

Please 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




- 1 anti-opening switch
- 2 tear-proof switch

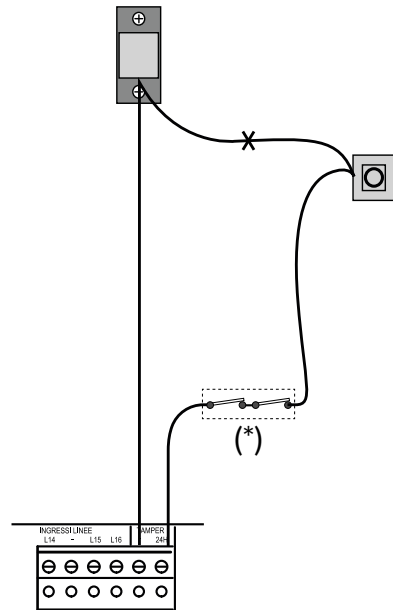
Compliance to grade 3 of the EN 50131 standard requires the container to be protected against removal from the mounting surface.

- insert the anti-tear switch in the rectangular hole of the

metal plate

 *For precise engagement, use a screwdriver if necessary.*

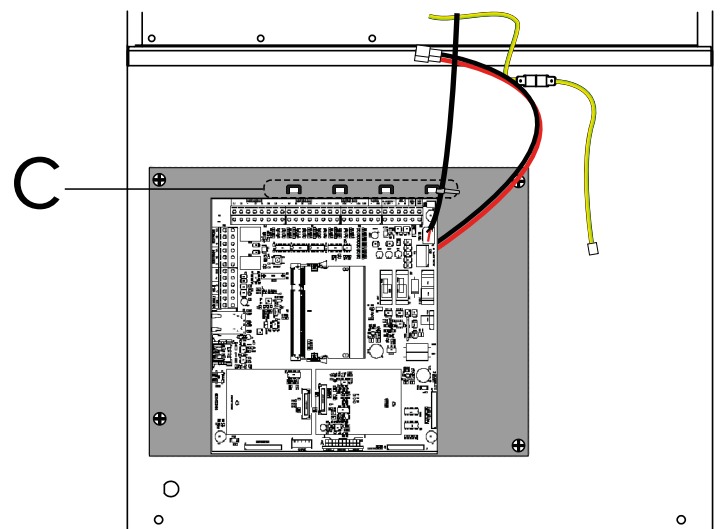
- fix the metal plate to the bottom of the container in the area indicated using the supplied screws



(*) tamper contacts of the devices

- weld and insulate the two cables (one coming from the anti-opening switch, the other from the anti-tear switch) in point X in the figure
- connect the anti-opening and tear-proof switches of the container and the tamper contacts of the devices that provide it in series with the TAMPER terminals in the control unit board, as shown

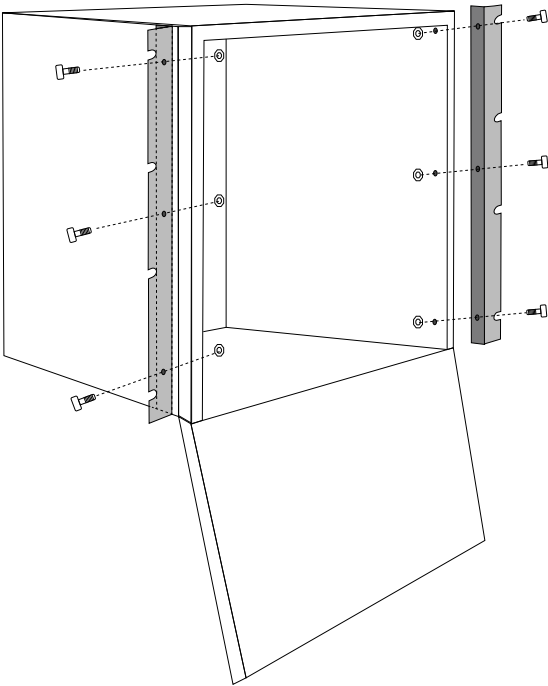
• **Closing the housing**



- fasten all the cables connected to the board to the appropriate fixing points (C) using cable ties
- close the control unit door
- screw the screws on the upper side of the container

6.2.1 Rack mounting

The container of PRX256 and PRX1024 supports rack mounting. When installed in a rack, the container can only be tilted. 19" brackets included in the optional PRXRACK kit are required.

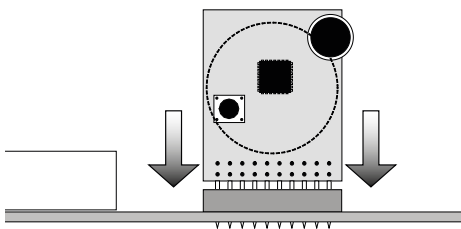


- drill 5 mm holes in the areas on the two sides of the container (3 holes per side)
- fasten the brackets to the container with the supplied screws and nuts
- fix the container with brackets to the rack cabinet using the supplied screws and nuts

6.3 Module installation

Install the modules as indicated in the following paragraphs. **Note:** before installing the modules, disconnect the control unit power source. After installation, set each module as indicated in the programming manual.

6.3.1 MDVOICE64



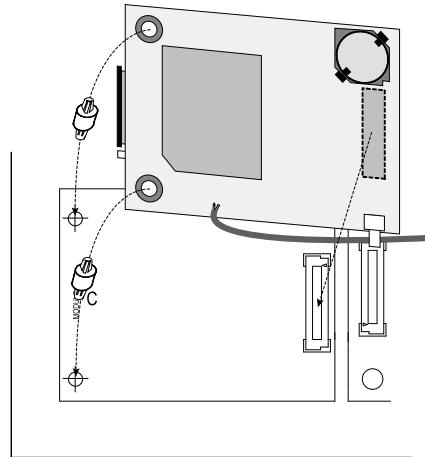
- plug the module to the control unit board connector A - SINTESI
- Refer to the previous image.

 *make sure that all the feet are correctly inserted.*

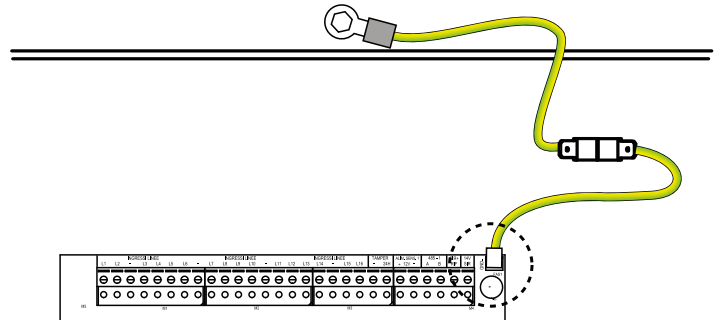
6.3.2 MDGSME and MD4GE

Follow the instructions in the respective manuals.

Installing the module



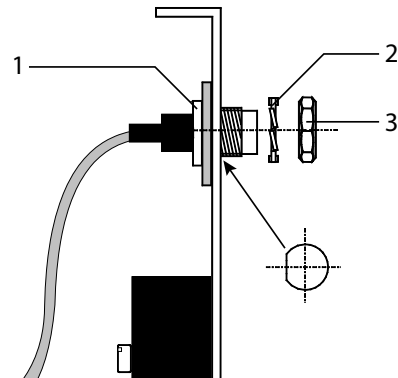
- insert the spacers (supplied) into the holes in the dedicated area on the control unit board (C)
- align the spacer holes and the module connector with the corresponding components on the control unit board
- plug the module to the control unit board



- connect the earth cable to the control unit board as shown in the previous figure

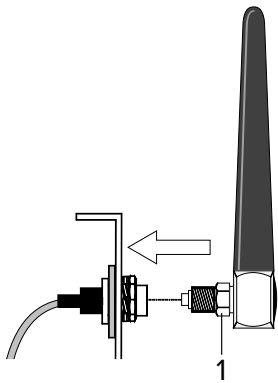
The antenna connector must be connected:

- for the module MDGSME, the 90° antenna GSMAC90;
- for the module MD4GE, the 90° antenna ANT4G90;



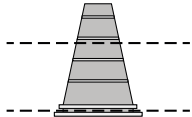
- 1 Antenna base
- 2 Lock washer
- 3 Nut (tighten with 14 mm spanner)

- remove the cap to close the hole in the door
- insert the antenna connector into the hole

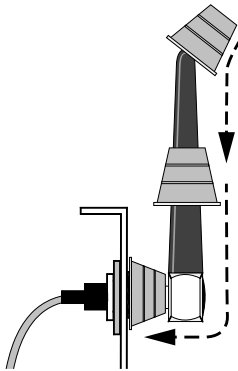


1 Nut (tighten with 8 mm spanner)

- fasten the antenna by tightening the nut

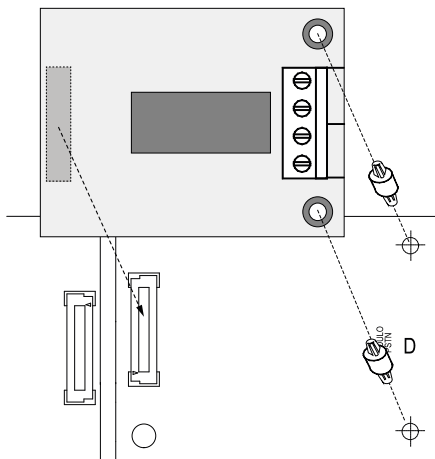


- cut the protection grommet along the indicated dashed lines



- insert the grommet on the antenna

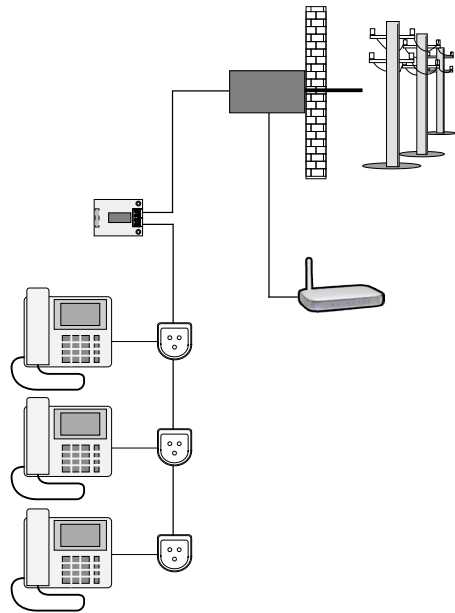
6.3.3 MDPSTN



- insert the spacers (supplied) into the holes in the dedicated area on the control unit board (D)

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



Note: See the MDPSTN technical manual.

7 WIRINGS

7.1 Wired zone connection

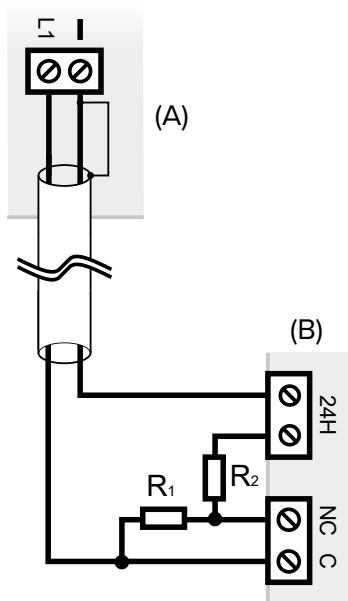
Connect all the required wired devices to inputs 1 to 16 on the control unit terminal block.

Below are some examples of balancing and configuration of the main types of zones.

A graphic editor is available in BrowserOne for each zone to freely configure the balances.

7.1.1 Double balancing

It allows the control panel to monitor rest, alarm and tamper conditions (short circuit/cut).



A Control unit
B Detector
 $R_1 = R_2 = 1500 \Omega$

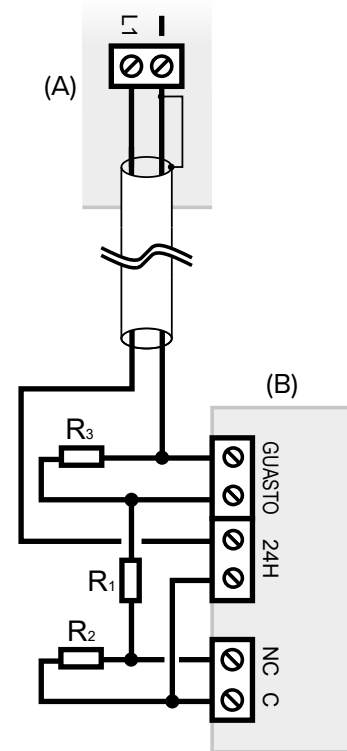
– connect the two 1500Ω resistors (supplied with the control unit) as shown

Note: see the detector technical manual.

7.1.2 Triple balancing

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

Three resistors of 1200Ω , 680Ω and 1000Ω are required.



A Control unit
B Detector
 $R_1 = 1000 \Omega$
 $R_2 = 680 \Omega$
 $R_3 = 1200 \Omega$

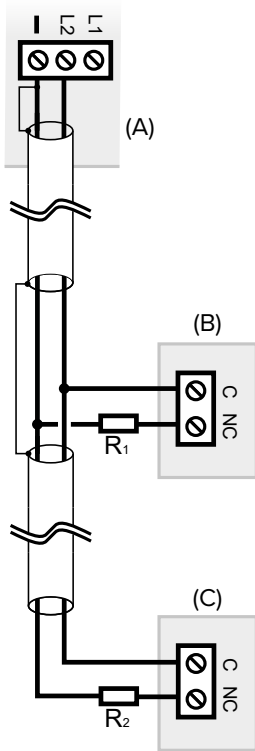
– connect the three resistors as shown

Note: by adding a resistor in parallel to the tamper contact, the **quadruple balancing scheme** is obtained, which allows to distinguish the cut-off condition from the detector tamper condition.

7.1.3 Split inputs

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

Two resistors of 1500Ω and 2200Ω are required.



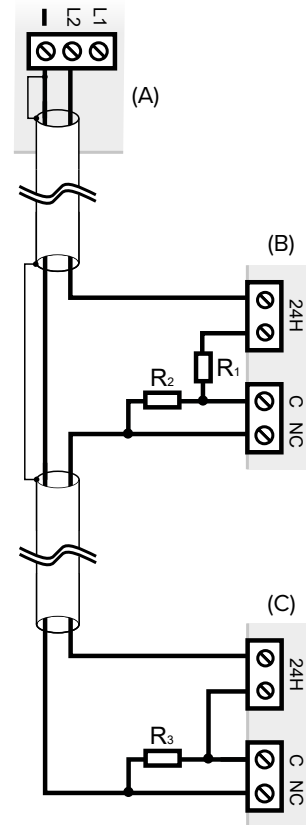
- A Control unit
- B Detector 1
- C Detector 2
- $R_1 = 1500 \Omega$
- $R_2 = 2200 \Omega$

- connect the two devices in parallel as shown in the figure In BrowserOne:
- go to page **Zones > General**
- in the grid, select the row of the input n to which to connect the devices (e.g. input 2)
- from the drop-down menu **Zone Type**, select "Split": automatically also the input n+16 (following the example: input 18) will take on the "Split" type

7.1.4 Extended split zones

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.

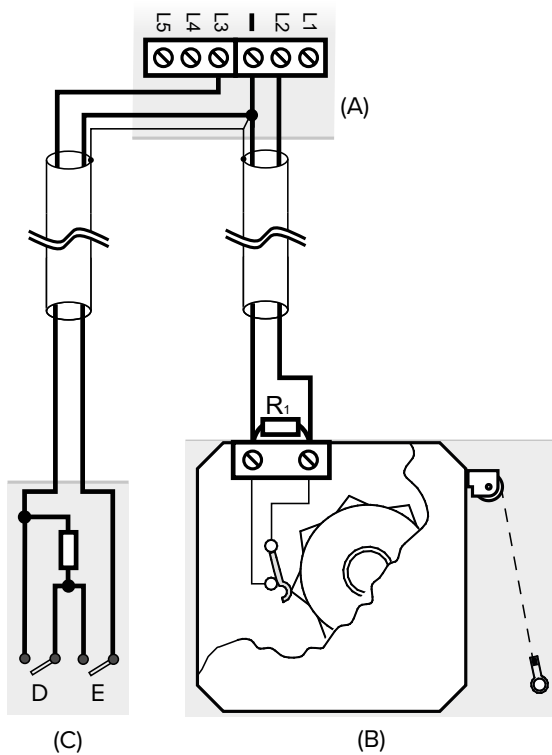


- A Control unit
- B Detector 1
- C Detector 2
- $R_1 = 1000 \Omega$
- $R_2 = 1200 \Omega$
- $R_3 = 680 \Omega$

- connect the two devices as shown in the figure In BrowserOne:
- go to page **Zones > General**
- in the grid, select the row of the input n to which to connect the devices (e.g. input 2)
- from the drop-down menu **Zone Type**, select "Extended split": automatically also the input n+16 (following the example: input 18) will take on the "Extended split" type

7.1.5 Fast inputs

Use the following connection diagram to connect roll-up shutter or inertial sensors. Only for zone 1 to 12.



- A Control unit
- B Roll-up shutter sensor
- C Inertial contact
- D Alarm contact
- E Tamper contact

Connect only one contact for roll-up shutters or only one inertial sensor for each input, otherwise an external analysis board is required.

- 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: $R = 1500 \Omega$.

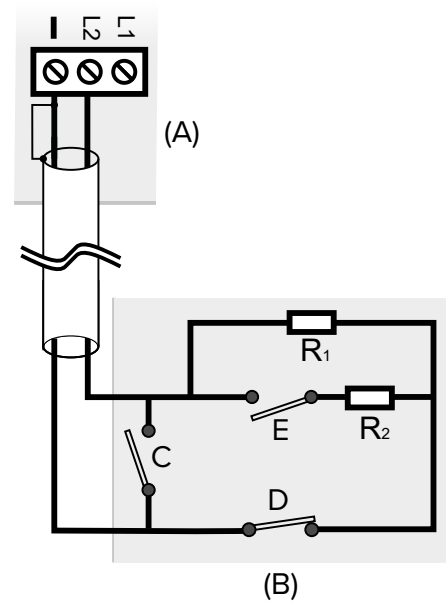
In BrowserOne:

- go to page **Zones > General**
- in the grid, select the row of the input n to which to connect the devices (e.g. input 2)
- from the drop-down menu **Zone Type**, select "Fast"
- this will enable the "Fast" panel: set the "Sensitivity" and "Integration" parameters here

7.1.6 Key zones

A "key" zone causes the switching of the associated arming conditions when a fault occurs.

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.



- A Control unit
 - B Generic control device with impulsive contact
 - C Tamper Contact (NA)
 - D Tamper Contact (NC)
 - E Device contact (NO)
- $R_1 = R_2 = 1500 \Omega$

- make the connections as shown in the figure (the connections shown also include the necessary protection against tampering)

Two 1500Ω resistors are required.

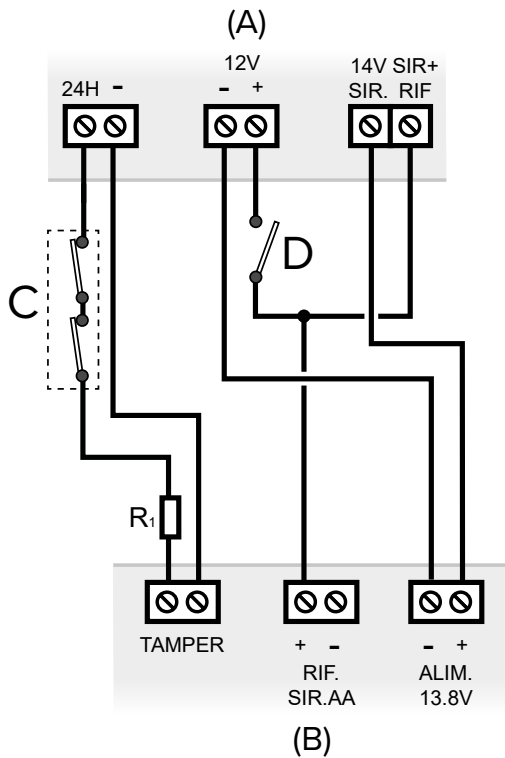
If the control device has a power source, the idle condition must be realised with the contact open (NO) in the absence of power source.

In BrowserOne:

- go to page **Zones > General**
- in the grid select the zone row
- in the panel **Zone Options**, tick "Key zone" and "24 hours"

7.2 Siren connection

7.2.1 Outdoor sirens



- A** Control unit
 - B** Siren
 - C** Tamper switches
 - D** Manual contact for maintenance
- $R_1 = 1500 \Omega$

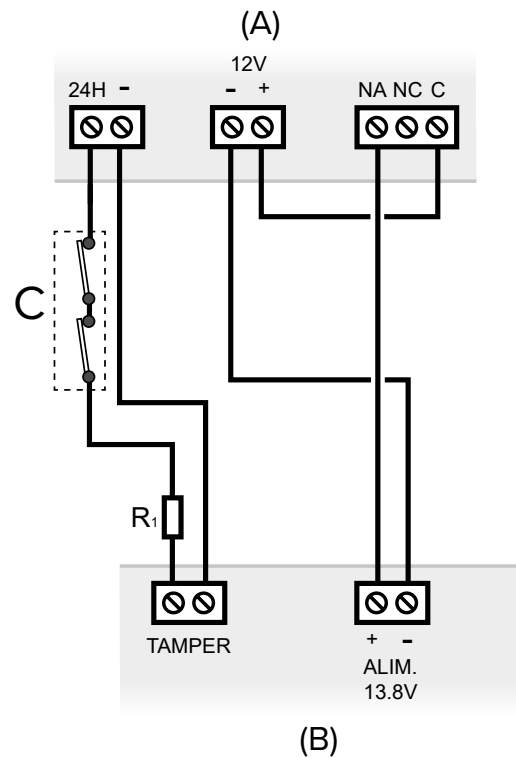
- connect the outdoor wired sirens as shown
- connect the cable shield to the -12V (negative) terminal of the control unit

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 (C).

Fit a manual contact to be closed in case of siren maintenance (D).

7.2.2 Indoor sirens



- A** Control unit
 - B** Siren
 - C** Tamper switches
- $R_1 = 1500 \Omega$

- connect the indoor wired sirens as shown
- connect the cable shield to the -12V SENS. POW. negative terminal of the control unit

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

By default, the control panel relay is not active.

Program it for the function requested through BrowserOne:

- on the **System options** > **General** page, select "General alarm relay" from the drop-down menu

Programmable Relay Settings

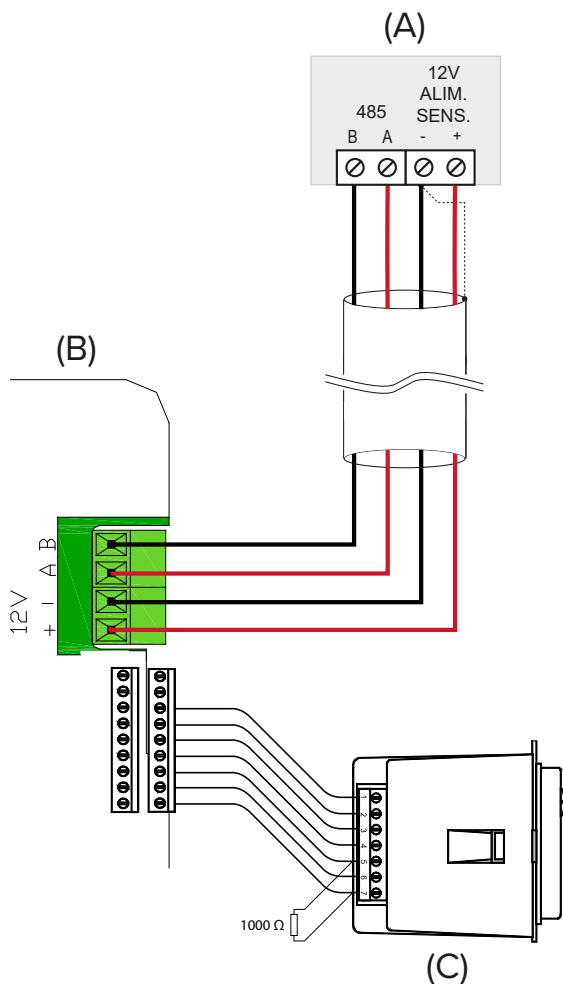
Note: see the siren technical manual.

7.3 Electronic outputs

- install ETRREL inside the container of the unit, using the holes provided on the bottom of the container
- connect the cable to the ELECTRONIC OUTPUTS connector on the control unit board

7.4 Control devices

- install the control devices (keyboards, proximity (key) readers) as indicated in their manuals
- connect any keypads, 18 proximity (key) readers and key points through serial line as indicated in paragraph 7.5 p. 17



- A** Control unit
- B** Keypad
- C** I66 proximity (key) reader

- 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

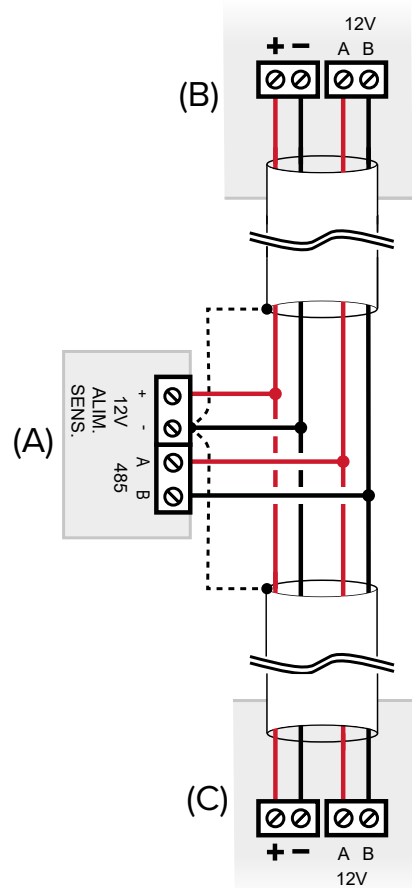
For compliance with the EN50131 standard:

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

7.5 Serial line devices

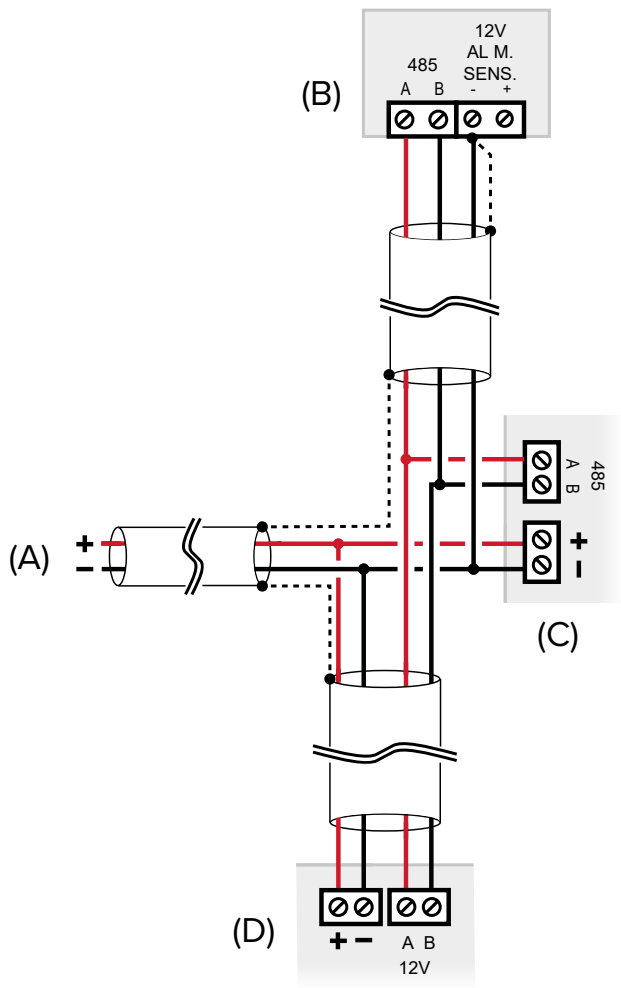
Several types of devices may be connected with serial connection to the control unit:

- control devices (keypads, proximity (key) readers);
- concentrators, GATEWAY2K;
- serial interface sirens and detectors;
- power supply units and fog systems.



- A** Control unit
- B** Previous device over serial line
- C** Next device over serial line

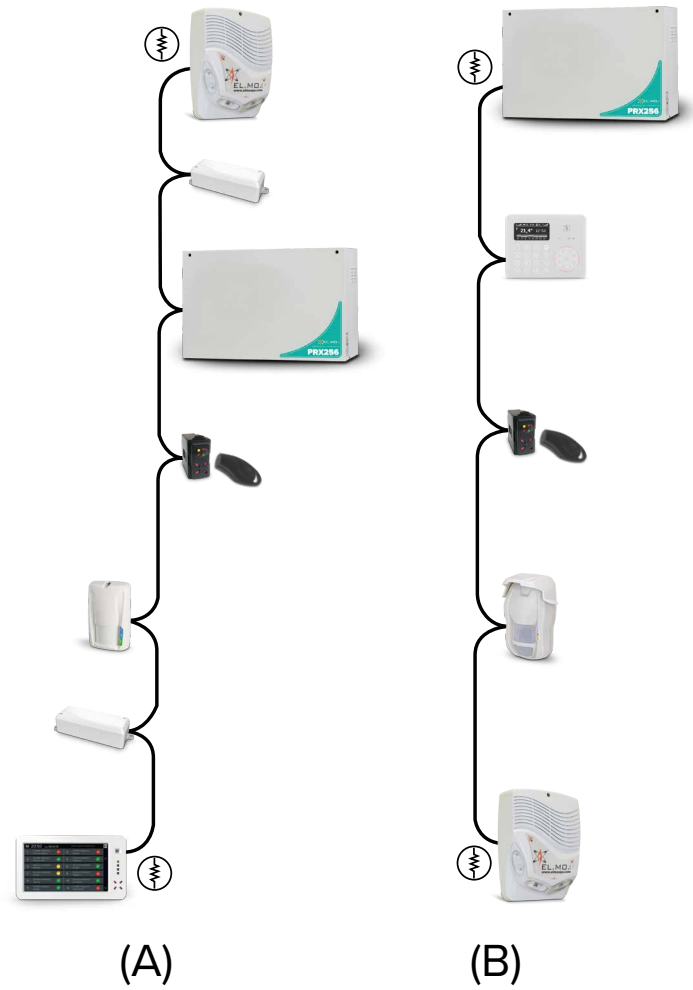
- connect each device to the serial line using terminals A and B (in addition to the power source terminals)
 - use cables with the following sections: $2 \times 0.75 \text{ mm}^2$ (power source) + $2 \times 0.22 \text{ mm}^2$ (signal)
 - connect the cable shield (dashed line in the figure) to the negative 12V ALIM.SENS. terminal of the control unit
 - insulate 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):



- A** External power source
- B** Control unit
- C** Serial line device 1
- D** Serial line device 2

Also in this case, join together the negative references of the control unit and the remote box. Each serial device (including the control unit) may be positioned at any position of the bus.

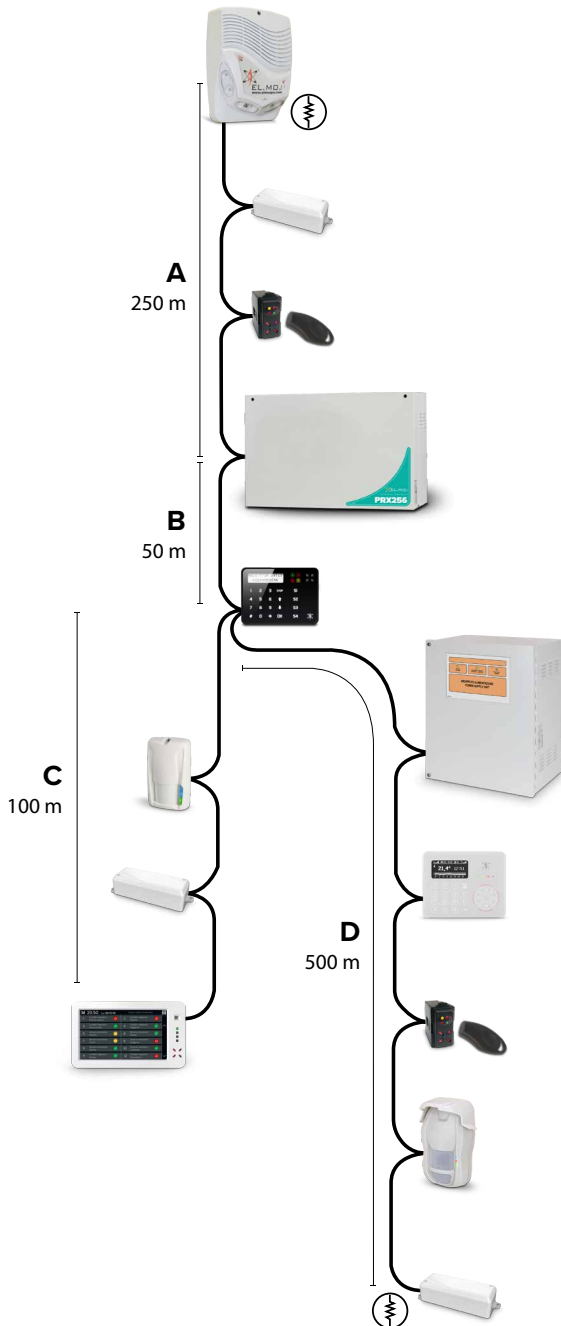
Simple serial line



- A** central unit placed at a midpoint of the line
- B** central unit placed at one end of the line

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

Branched serial line



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);
- 680 Ω 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.

7.5.1 Addressing of concentrators

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 concentrator manuals:

To know the address to assign to a concentrator:

- open BrowserOne

- go to page **Zones > Cable Devices**

- select in the grid one of the lines relating to the bank of inputs to be reserved for the concentrator

- from the drop-down menu **Zone Type**, select "Wired Concentrator" or "River RF" (depending on the case)

- in the pane **Device type** select the number of device inputs

A graphic indication of the addressing dip setting will appear: set them as shown.



The following tables report the addresses to set for each type of concentrator.

In any case, it is necessary to take into account the maximum number of addresses available for each control unit:

- PRX128: max 128;
- PRX256: max 256;
- PRX1024: max 1024.

RIVER / RIVERRF

Number of addresses	Dip on ON	Number of addresses	Dip on ON
1 - 8	1 2 3 4 5 6 7 -	513 - 520	1 2 3 4 5 6 - -
9 - 16	- 2 3 4 5 6 7 -	521 - 528	- 2 3 4 5 6 - -
17 - 24	1 - 3 4 5 6 7 -	529 - 536	1 - 3 4 5 6 - -
25 - 32	- - 3 4 5 6 7 -	537 - 544	- - 3 4 5 6 - -
33 - 40	1 2 - 4 5 6 7 -	545 - 552	1 2 - 4 5 6 - -
41 - 48	- 2 - 4 5 6 7 -	553 - 560	- 2 - 4 5 6 - -
49 - 56	1 - - 4 5 6 7 -	561 - 568	1 - - 4 5 6 - -
57 - 64	- - - 4 5 6 7 -	569 - 576	- - - 4 5 6 - -
65 - 72	1 2 3 - 5 6 7 -	577 - 584	1 2 3 - 5 6 - -
73 - 80	- 2 3 - 5 6 7 -	585 - 592	- 2 3 - 5 6 - -
81 - 88	1 - 3 - 5 6 7 -	593 - 600	1 - 3 - 5 6 - -
89 - 96	- - 3 - 5 6 7 -	601 - 608	- - 3 - 5 6 - -
97 - 104	1 2 - - 5 6 7 -	609 - 616	1 2 - - 5 6 - -
105 - 112	- 2 - - 5 6 7 -	617 - 624	- 2 - - 5 6 - -
113 - 120	1 - - - 5 6 7 -	625 - 632	1 - - - 5 6 - -
121 - 128	- - - - 5 6 7 -	633 - 640	- - - - 5 6 - -
129 - 136	1 2 3 4 - 6 7 -	641 - 648	1 2 3 4 - 6 - -
137 - 144	- 2 3 4 - 6 7 -	649 - 656	- 2 3 4 - 6 - -
145 - 152	1 - 3 4 - 6 7 -	657 - 664	1 - 3 4 - 6 - -
153 - 160	- - 3 4 - 6 7 -	665 - 672	- - 3 4 - 6 - -
161 - 168	1 2 - 4 - 6 7 -	673 - 680	1 2 - 4 - 6 - -
169 - 176	- 2 - 4 - 6 7 -	681 - 688	- 2 - 4 - 6 - -
177 - 184	1 - - 4 - 6 7 -	689 - 696	1 - - 4 - 6 - -
185 - 192	- - - 4 - 6 7 -	697 - 704	- - - 4 - 6 - -
193 - 200	1 2 3 - - 6 7 -	705 - 712	1 2 3 - - 6 - -
201 - 208	- 2 3 - - 6 7 -	713 - 720	- 2 3 - - 6 - -
209 - 216	1 - 3 - - 6 7 -	721 - 728	1 - 3 - - 6 - -

Number of addresses	Dip on ON	Number of addresses	Dip on ON
217 - 224	-- 3 -- 6 7 -	729 - 736	-- 3 -- 6 --
225 - 232	12 --- 6 7 -	737 - 744	12 --- 6 --
233 - 240	- 2 --- 6 7 -	745 - 752	- 2 --- 6 --
241 - 248	1 ---- 6 7 -	753 - 760	1 ---- 6 --
249 - 256	----- 6 7 -	761 - 768	----- 6 --
257 - 264	12 3 4 5 - 7 -	769 - 776	12 3 4 5 ---
265 - 272	- 2 3 4 5 - 7 -	777 - 784	- 2 3 4 5 ---
273 - 280	1 - 3 4 5 - 7 -	785 - 792	1 - 3 4 5 ---
281 - 288	-- 3 4 5 - 7 -	793 - 800	-- 3 4 5 ---
289 - 296	12 - 4 5 - 7 -	801 - 808	12 - 4 5 ---
297 - 304	- 2 - 4 5 - 7 -	809 - 816	- 2 - 4 5 ---
305 - 312	1 -- 4 5 - 7 -	817 - 824	1 -- 4 5 ---
313 - 320	--- 4 5 - 7 -	825 - 832	--- 4 5 ---
321 - 328	12 3 - 5 - 7 -	833 - 840	12 3 - 5 ---
329 - 336	- 2 3 - 5 - 7 -	841 - 848	- 2 3 - 5 ---
337 - 344	1 - 3 - 5 - 7 -	849 - 856	1 - 3 - 5 ---
345 - 352	-- 3 - 5 - 7 -	857 - 864	-- 3 - 5 ---
353 - 360	12 -- 5 - 7 -	865 - 872	12 -- 5 ---
361 - 368	- 2 -- 5 - 7 -	873 - 880	- 2 -- 5 ---
369 - 376	1 --- 5 - 7 -	881 - 888	1 --- 5 ---
377 - 384	---- 5 - 7 -	889 - 896	---- 5 ---
385 - 392	12 3 4 -- 7 -	897 - 904	12 3 4 ----
393 - 400	- 2 3 4 -- 7 -	905 - 912	- 2 3 4 ----
401 - 408	1 - 3 4 -- 7 -	913 - 920	1 - 3 4 ----
409 - 416	-- 3 4 -- 7 -	921 - 928	-- 3 4 ----
417 - 424	12 - 4 -- 7 -	929 - 936	12 - 4 ----
425 - 432	- 2 - 4 -- 7 -	937 - 944	- 2 - 4 ----
433 - 440	1 -- 4 -- 7 -	945 - 952	1 -- 4 ----
441 - 448	--- 4 -- 7 -	953 - 960	--- 4 ----
449 - 456	12 3 --- 7 -	961 - 968	12 3 ----
457 - 464	- 2 3 --- 7 -	969 - 976	- 2 3 ----
465 - 472	1 - 3 --- 7 -	977 - 984	1 - 3 ----
473 - 480	-- 3 --- 7 -	985 - 992	-- 3 ----
481 - 488	12 ---- 7 -	993 - 1000	12 -----
489 - 496	- 2 ---- 7 -	1001 - 1008	- 2 -----
497 - 504	1 ---- 7 -	1009 - 1016	1 -----
505 - 512	----- 7 -	1017 - 1024	-----

RIVERMINI4

Number of addresses	Dip on ON	Number of addresses	Dip on ON
1 - 4	12 3 4 5 6 --	129 - 132	12 3 4 5 ---
5 - 8	- 2 3 4 5 6 --	133 - 136	- 2 3 4 5 ---
9 - 12	1 - 3 4 5 6 --	137 - 140	1 - 3 4 5 ---
13 - 16	-- 3 4 5 6 --	141 - 144	-- 3 4 5 ---
17 - 20	12 - 4 5 6 --	145 - 148	12 - 4 5 ---
21 - 24	- 2 - 4 5 6 --	149 - 152	- 2 - 4 5 ---

Number of addresses	Dip on ON	Number of addresses	Dip on ON
25 - 28	1 -- 4 5 6 --	153 - 156	1 -- 4 5 ---
29 - 32	--- 4 5 6 --	157 - 160	--- 4 5 ---
33 - 36	12 3 - 5 6 --	161 - 164	12 3 - 5 ---
37 - 40	- 2 3 - 5 6 --	165 - 168	- 2 3 - 5 ---
41 - 44	1 - 3 - 5 6 --	169 - 172	1 - 3 - 5 ---
45 - 48	-- 3 - 5 6 --	173 - 176	-- 3 - 5 ---
49 - 52	12 -- 5 6 --	177 - 180	12 -- 5 ---
53 - 56	- 2 -- 5 6 --	181 - 184	- 2 -- 5 ---
57 - 60	1 --- 5 6 --	185 - 188	1 --- 5 ---
61 - 64	---- 5 6 --	189 - 192	---- 5 ---
65 - 68	12 3 4 - 6 --	193 - 196	12 3 4 ----
69 - 72	- 2 3 4 - 6 --	197 - 200	- 2 3 4 ----
73 - 76	1 - 3 4 - 6 --	201 - 204	1 - 3 4 ----
77 - 80	-- 3 4 - 6 --	205 - 208	-- 3 4 ----
81 - 84	12 - 4 - 6 --	209 - 212	12 - 4 ----
85 - 88	- 2 - 4 - 6 --	213 - 216	- 2 - 4 ----
89 - 92	1 -- 4 - 6 --	217 - 220	1 -- 4 ----
93 - 96	--- 4 - 6 --	221 - 224	--- 4 ----
97 - 100	12 3 -- 6 --	225 - 228	12 3 ----
101 - 104	- 2 3 -- 6 --	229 - 232	- 2 3 ----
105 - 108	1 - 3 -- 6 --	233 - 236	1 - 3 ----
109 - 112	-- 3 -- 6 --	237 - 240	-- 3 ----
113 - 116	12 --- 6 --	241 - 244	12 -----
117 - 120	- 2 --- 6 --	245 - 248	- 2 -----
121 - 124	1 ---- 6 --	249 - 252	1 -----
125 - 128	----- 6 --	253 - 256	-----

RIVERMICRO2

Number of addresses	Dip on ON	Number of addresses	Dip on ON
1 - 2	12 3 4 5 6 7 -	129 - 130	12 3 4 5 6 --
3 - 4	- 2 3 4 5 6 7 -	131 - 132	- 2 3 4 5 6 --
5 - 6	1 - 3 4 5 6 7 -	133 - 134	1 - 3 4 5 6 --
7 - 8	-- 3 4 5 6 7 -	135 - 136	-- 3 4 5 6 --
9 - 10	12 - 4 5 6 7 -	137 - 138	12 - 4 5 6 --
11 - 12	- 2 - 4 5 6 7 -	139 - 140	- 2 - 4 5 6 --
13 - 14	1 -- 4 5 6 7 -	141 - 142	1 -- 4 5 6 --
15 - 16	--- 4 5 6 7 -	143 - 144	--- 4 5 6 --
17 - 18	12 3 - 5 6 7 -	145 - 146	12 3 - 5 6 --
19 - 20	- 2 3 - 5 6 7 -	147 - 148	- 2 3 - 5 6 --
21 - 22	1 - 3 - 5 6 7 -	149 - 150	1 - 3 - 5 6 --
23 - 24	-- 3 - 5 6 7 -	151 - 152	-- 3 - 5 6 --
25 - 26	12 -- 5 6 7 -	153 - 154	12 -- 5 6 --
27 - 28	- 2 -- 5 6 7 -	155 - 156	- 2 -- 5 6 --
29 - 30	1 --- 5 6 7 -	157 - 158	1 --- 5 6 --
31 - 32	---- 5 6 7 -	159 - 160	---- 5 6 --
33 - 34	12 3 4 - 6 7 -	161 - 162	12 3 4 - 6 --

Number of addresses	Dip on ON	Number of addresses	Dip on ON
35 - 36	- 2 3 4 - 6 7 -	163 - 164	- 2 3 4 - 6 - -
37 - 38	1 - 3 4 - 6 7 -	165 - 166	1 - 3 4 - 6 - -
39 - 40	- - 3 4 - 6 7 -	167 - 168	- - 3 4 - 6 - -
41 - 42	1 2 - 4 - 6 7 -	169 - 170	1 2 - 4 - 6 - -
43 - 44	- 2 - 4 - 6 7 -	171 - 172	- 2 - 4 - 6 - -
45 - 46	1 - - 4 - 6 7 -	173 - 174	1 - - 4 - 6 - -
47 - 48	- - - 4 - 6 7 -	175 - 176	- - - 4 - 6 - -
49 - 50	1 2 3 - - 6 7 -	177 - 178	1 2 3 - - 6 - -
51 - 52	- 2 3 - - 6 7 -	179 - 180	- 2 3 - - 6 - -
53 - 54	1 - 3 - - 6 7 -	181 - 182	1 - 3 - - 6 - -
55 - 56	- - 3 - - 6 7 -	183 - 184	- - 3 - - 6 - -
57 - 58	1 2 - - - 6 7 -	185 - 186	1 2 - - - 6 - -
59 - 60	- 2 - - - 6 7 -	187 - 188	- 2 - - - 6 - -
61 - 62	1 - - - - 6 7 -	189 - 190	1 - - - - 6 - -
63 - 64	- - - - - 6 7 -	191 - 192	- - - - - 6 - -
65 - 66	1 2 3 4 5 - 7 -	193 - 194	1 2 3 4 5 - - -
67 - 68	- 2 3 4 5 - 7 -	195 - 196	- 2 3 4 5 - - -
69 - 70	1 - 3 4 5 - 7 -	197 - 198	1 - 3 4 5 - - -
71 - 72	- - 3 4 5 - 7 -	199 - 200	- - 3 4 5 - - -
73 - 74	1 2 - 4 5 - 7 -	201 - 202	1 2 - 4 5 - - -
75 - 76	- 2 - 4 5 - 7 -	203 - 204	- 2 - 4 5 - - -
77 - 78	1 - - 4 5 - 7 -	205 - 206	1 - - 4 5 - - -
79 - 80	- - - 4 5 - 7 -	207 - 208	- - - 4 5 - - -
81 - 82	1 2 3 - 5 - 7 -	209 - 210	1 2 3 - 5 - - -
83 - 84	- 2 3 - 5 - 7 -	211 - 212	- 2 3 - 5 - - -
85 - 86	1 - 3 - 5 - 7 -	213 - 214	1 - 3 - 5 - - -
87 - 88	- - 3 - 5 - 7 -	215 - 216	- - 3 - 5 - - -
89 - 90	1 2 - - 5 - 7 -	217 - 218	1 2 - - 5 - - -
91 - 92	- 2 - - 5 - 7 -	219 - 220	- 2 - - 5 - - -
93 - 94	1 - - - 5 - 7 -	221 - 222	1 - - - 5 - - -
95 - 96	- - - - 5 - 7 -	223 - 224	- - - - 5 - - -
97 - 98	1 2 3 4 - - 7 -	225 - 226	1 2 3 4 - - - -
99 - 100	- 2 3 4 - - 7 -	227 - 228	- 2 3 4 - - - -
101 - 102	1 - 3 4 - - 7 -	229 - 230	1 - 3 4 - - - -
103 - 104	- - 3 4 - - 7 -	231 - 232	- - 3 4 - - - -
105 - 106	1 2 - 4 - - 7 -	233 - 234	1 2 - 4 - - - -
107 - 108	- 2 - 4 - - 7 -	235 - 236	- 2 - 4 - - - -
109 - 110	1 - - 4 - - 7 -	237 - 238	1 - - 4 - - - -
111 - 112	- - - 4 - - 7 -	239 - 240	- - - 4 - - - -
113 - 114	1 2 3 - - - 7 -	241 - 242	1 2 3 - - - - -
115 - 116	- 2 3 - - - 7 -	243 - 244	- 2 3 - - - - -
117 - 118	1 - 3 - - - 7 -	245 - 246	1 - 3 - - - - -
119 - 120	- - 3 - - - 7 -	247 - 248	- - 3 - - - - -
121 - 122	1 2 - - - - 7 -	249 - 250	1 2 - - - - - -
123 - 124	- 2 - - - - 7 -	251 - 252	- 2 - - - - - -
125 - 126	1 - - - - - 7 -	253 - 254	1 - - - - - - -
127 - 128	- - - - - - 7 -	255 - 256	- - - - - - - -

8 STARTING THE DEVICE

Once all the wiring has been completed and carefully checked, power the control unit for the first time.

First power supply to the control unit

- press and hold OK key on keypad with address 1
- power up the control panel
- when message **FACTORY DEFAULT?** appears, release OK key
- press \uparrow and then \downarrow
- wait for message **REGIST. MODULES?** to appear
- press OK to register any installed modules, and # to skip this step (it may also be completed later by accessing **REGISTER MODULES** in the installer menu)
- wait for message **DEVICES LEARNING** to appear
- press OK to register any peripheral devices on the serial line, # to avoid this step

The registration of the peripheral devices will take 2 minutes max.

If the control unit is only powered through the power grid, after the registration of the modules, the LOW BATTERY message will appear.

Control unit configuration

Once the control unit is powered up, proceed with its configuration.

The operations will require the use of the keypad menus and the BrowserOne software.

Consult the quick guide to make a first configuration (basic) of the control unit.

8.1 Keyboard menus

Two keypad accessible menus are available.

User menu


It allows the user to perform basic maintenance and to enable the installer to perform remote assistance operations.

- enter the user code (6 digits, default 111111)
- type *
- press the \uparrow or \downarrow 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.

Installer menu

It allows more in-depth programming.

 Access authorization must be granted by a user with maintenance properties using the **AUTHORIZATION INST.** in the user menu.

- enter the installer code (8 digits, default 88888888)
- press OK
- press the \uparrow or \downarrow 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.

8.2 BrowserOne Software

Installation and update of BrowserOne


See the programming manual for information on:

- first installation of BrowserOne: the installation expects to be connected to the Internet.
- BrowserOne update: instead of fully reinstalling BrowserOne on a PC where this is already installed (this would cause the loss of software settings), it is possible to update to the latest software version.

Connecting the control unit to BrowserOne

- open BrowserOne
- click on **Connect to...** (available on controls bar too)
- select **Connection type**

Note: the following is supposed to use the USB connection (via a USB mini-B cable not included). This connection also allows updating the firmware and speech synthesis.


- click on **Next**
- connect the control unit to the PC using the mini-B USB cable
- wait for the COM port virtualization software to be loaded
- in the **Serial connection** window click  to update the available communication ports
- select "ELMO Virtual COM" from drop-down menu
- select **Next:** the software will attempt to start 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.

9 MAINTENANCE

9.1 Control unit reset

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

 *The procedure deletes all memory data. If necessary, these can be saved using BrowserOne before the reset.*

- enter keypad installer menu
- press ↑ or ↓ until SYSTEM LOCK is displayed
- press OK to enter the menu
- press OK to lock the system: the LEDs on the keypads and the key readers flash
- open the control unit container as indicated in the assembly procedure
- close the (SIR +RIF) manual contact for the maintenance of any wired self-powered sirens

- press and hold down the RESET button (see chapter 3 p. 2)
- press and hold OK key on keypad with address 1
- release the RESET button
- when the word DEFAULT CONFIG? appears, release the OK button
- press ↓ and then ↑
- wait for the REGISTER MODULES? message to appear
- press OK to register any installed modules, and # to skip this step (it may also be completed later by accessing **REGISTER MODULES** in the installer menu)
- wait for the message DEVICES LEARNING? (see paragraph 9.1.2 p. 22 for further information)
- press OK to register any peripheral devices on the serial line, # to avoid this step

The registration of the peripheral devices will take 2 minutes max.

It is now possible to continue with the new programming. Test the system and reactivate the sirens.

9.1.1 Default configuration

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

Zones wired in the terminal block: None

Zone configuration: NO

Zone connection: No zone connected

System keypad: Keypad 1

Active area: Area 1

Zone programming: All the zones associated to area 1

Active users: User 1

User 1 code: 111111

User 1 enabling level: Small maintenance activities

Installer code: 88888888

Installer access authorisation: PERMANENT

Alarm generation: All the zones generate intrusion alarms

On-board relay: Not active

Output time: 15 s

Zone time: 10 s

General alarm type: 1 min

Tamper alarm type: 1 min

9.1.2 Automatic device learning

This tool allows to scan the serial bus in order to detect the installed RS-485 ULTRABUS devices.

The control unit will search the following devices:

- RS-485 ULTRABUS control devices (keypads, proximity key readers);
- RS-485 ULTRABUS concentrators with 8, 4, 2 zones;
- detectors with RS-485 ULTRABUS interface;
- power supply units with RS-485 ULTRABUS interface;
- sirens with RS-485 ULTRABUS interface;
- GATEWAY2K devices.

The automatic device learning will be proposed after control unit reset.

9.2 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 a PC with Windows 7, 8 or 10 operating system and BrowserOne installed, with PROXIMA control unit module.


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.

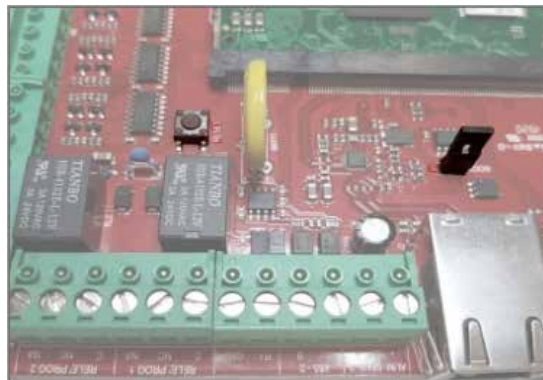
- save the current control unit configuration: in BrowserOne, in the menu bar click on **File > Save As...**
- access the keypad installer menu, enter the installer code and press **OK**
- press **↑** or **↓** until the item SYSTEM LOCK is reached
- press **OK**
- press **OK** to lock the system: the LEDs on the keypads and the key readers flash
- close the (+RIF) manual contact for the maintenance of any wired self-powered sirens

9.2.1 Firmware update via USB

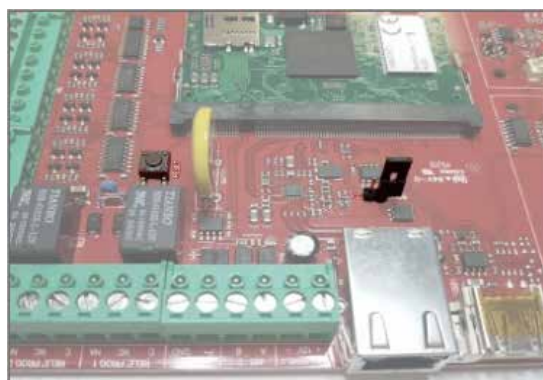
- open BrowserOne
 - connect the control unit to the PC that runs BrowserOne
 - enter menu **Tools** and select **Firmware Update Panel**
- The update file selection window will appear. Select the download location:
- click on **Sync with online archive** if the PC has an Internet connection and you want to download the file from an online archive (recommended): select the update file and then click on **Ok**
 - click on **Browse** if instead you want to select an update file already downloaded to your PC (the firmware update files are available on the site www.elmospa.com on the control unit page, after registration): search for it and click on **Open**
 - click on **Next**
 - select update mode **Update via USB**
 - open the control unit container, power the control unit and connect it to the PC using the mini-B USB cable as shown in section 8.2 p. 22
 - click on **Next**
 - in the window **Update settings** just opened, enter the installer code
 - click  to update the available communication ports
 - select "ELMO Virtual COM" from drop-down menu
 - click on **Next**
 - select the update mode: it is recommended to select the Standard Update; reserve the Emergency Update for

particular malfunctions

- click on **Next**
- select the voice module update mode (any messages recorded will not be cancelled)
- click on **Next**
- the connection will be established; at the end, the summary screen will be displayed.
- click on **Next**



- switch the control unit to "firmware update" mode: close the S1 jumper and then press and release the RESET button (the window in BrowserOne will show the operations to be performed)
- click on **Next**
- the update will be done: at the end, click on **Next**



- switch the control unit to operating mode: open the S1 jumper and then press and release the RESET button (the window in BrowserOne will show the operations to be performed)
- click on **Next**
- after the update procedure has been completed successfully, click on **End** to end the procedure

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 on **File > Open**. After uploading it and making any necessary changes, write it on the control unit by clicking on **Actions > Write setup**.

9.2.2 Remote firmware update

 *Firmware update from remote is supported from*

Note: In order to perform remote update, it is necessary to be enabled.

Enabling

- open BrowserOne
- in the menu bar, click ? » Additional features...
- click on **Add**
- send the control code to international@elmospa.com, specifying that you want to enable the update of intrusion detection control units
- once received the unlock code, come back to this screen and input it in the field below

Update

- open BrowserOne
 - load a module compatible with the control unit being used
 - enter menu **Tools** and select **Firmware Update Panel**
- The update file selection window will appear. Select the download location:
- click on **Sync with online archive** if the PC has an Internet connection and you want to download the file from an online archive (recommended): select the update file and then click on Ok
 - click on **Browse** if instead you want to select an update file already downloaded to your PC (the firmware update files are available on the site www.elmospa.com on the control unit page, after registration): search for it and click on **Open**
 - click on **Next**
 - in the **Update settings** window displayed, select update mode via LAN TCP/IP or e-Connect
 - click on **Next**
 - enter required data (control unit IP address, connection port or e-Connect credentials) and installer code
 - click on **Next**
 - select the voice module update mode (any messages recorded will not be cancelled)
 - click on **Next**
 - the connection will be established; at the end, the summary screen will be displayed.
 - click on **Next**

The update file will now be sent to the control unit.

- click on **End** to end the procedure

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 on **File > Open**. After uploading it and making any necessary changes, write it on the control unit by clicking on **Actions > Write setup**.

User confirmation

If it has been set that the update must be confirmed by the user, the user will have to:

- go to the keypad
- press Stop to delete message "**Panel update available**"
- key in user code
- type *
- press OK to confirm the update

if it has been set that the update is automatically completed, no confirmation will be required to the user.

9.3 Wireless device battery change

If the battery of a device is dead, the anomaly and the related event are signalled in the control unit.

To replace the battery proceed as follows:

- exclude the input on which the device is learned: use the item in BYPASS ZONES the user or installer menu

When the input is excluded, tampering is also excluded: the tamper event is logged but the tamper alarm is not generated.

- open the device container and replace the battery with one of the same type
- close detector case
- re-include the input (always via the menu item BYPASS ZONES)

Table of contents

1	DESCRIPTION.....	P. 1	MAIN SAFETY RULES.....	P. 28
2	HARDWARE FEATURES	P. 1	DISPOSAL WARNINGS.....	P. 28
3	PCB.....	P. 2		
4	TECHNICAL DATA.....	P. 3		
5	BEFORE INSTALLATION.....	P. 5		
5.1	System autonomy	p. 5		
5.2	Indications for compliance with EN 50131 grade 3	p. 5		
5.2.1	Classification of notifications	p. 6		
5.2.2	Current distribution for IMQ - Security Systems certification	p. 7		
5.2.3	Current distribution for INCERT certification	p. 7		
5.2.4	Warnings concerning the electrical aspects	p. 7		
5.3	Usage with NG-TRX devices	p. 7		
6	DEVICE MOUNTING	P. 7		
6.1	PRX128	p. 7		
6.2	PRX256 - PRX1024	p. 9		
6.2.1	Rack mounting	p. 11		
6.3	Module installation	p. 11		
6.3.1	MDVOICE64	p. 11		
6.3.2	MDGSME and MD4GE	p. 11		
6.3.3	MDPSTN	p. 12		
7	WIRINGS.....	P. 13		
7.1	Wired zone connection	p. 13		
7.1.1	Double balancing	p. 13		
7.1.2	Triple balancing	p. 13		
7.1.3	Split inputs	p. 13		
7.1.4	Extended split zones	p. 14		
7.1.5	Fast inputs	p. 14		
7.1.6	Key zones	p. 15		
7.2	Siren connection	p. 16		
7.2.1	Outdoor sirens	p. 16		
7.2.2	Indoor sirens	p. 16		
7.3	Electronic outputs	p. 16		
7.4	Control devices	p. 16		
7.5	Serial line devices	p. 17		
7.5.1	Addressing of concentrators	p. 19		
8	STARTING THE DEVICE	P. 21		
8.1	Keyboard menus	p. 21		
8.2	BrowserOne Software	p. 22		
9	MAINTENANCE.....	P. 22		
9.1	Control unit reset	p. 22		
9.1.1	Default configuration	p. 22		
9.1.2	Automatic device learning	p. 22		
9.2	Firmware update	p. 23		
9.2.1	Firmware update via USB	p. 23		
9.2.2	Remote firmware update	p. 23		
9.3	Wireless device battery change	p. 24		
	EU DECLARATION OF CONFORMITY	P. 28		
	GENERAL WARNINGS	P. 28		
	INSTALLER WARNINGS	P. 28		
	USER WARNINGS.....	P. 28		

EU DECLARATION OF CONFORMITY

The product complies with current European EMC and LVD directives.

The full text of the EU declaration of conformity is available at the following internet address: www.elmospa.com – registration is quick and easy.



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 units 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 components adopted are 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).

INSTALLER WARNINGS



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 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).

USER WARNINGS



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...)

MAIN 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 device 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.

This product needs batteries for correct functioning. Exhausted batteries have to be delivered to dumping grounds authorised for battery collection. The materials used for this product are very harmful and polluting if dispersed in the environment.