EL.MO. SPA

USER MANUAL

PREGIO SERIES

Multi-functional hybrid control units for intrusion detection systems

1 GENERALS

The PREGIO control units are multi-functional hybrid control units supporting both wired and wireless devices.
Control units are compatible with

- all EL.MO. series devices (keypads, readers, power groups, security fog systems, concentrators and single detectors) thanks to ULTRABUS interface;
- NG-TRX wireless technology with connection of GATEWAY2K over serial line.

Optional modules can be installed to improve unit operating mode.
It is also possible to connect to e-Connect with the installation of suitable modules.
PREGIO1000, PREGIO1000BM, PREGIO2000 are supplied in a metal housing.
PREGIO500, PREGIO500PL, PREGIO1000PL, PREGIO2000PL are supplied in a plastic housing.
All control units are protected against the cover opening and removal from wall.

Icons used in this manual

▼ **Example of messages on keypad display**

```
Fri01/09/17 9:00
Area 1
```

▼ **Keys typing**

▼ **Usage example**

Manual contents

▼ **Keypads usage**
operating mode from keypad ➔ cap. 2 *p. 1*

▼ **Proximity keys usage**
operating mode from keypad ➔ cap. 3 *p. 12*

▼ **Remote controls usage**
operating mode with remote control ➔ cap. 4 *p. 14*

▼ **GSM and phone communications**
phone calls reception, SMS texts sending and reception ➔ cap. 5 *p. 15*

▼ **Temperature monitoring**
use of built-in temperature detector ➔ cap. 6 *p. 16*

▼ **e-Connect usage**
Information on e-Connect service ➔ cap. 7 *p. 16*

▼ **Maximum security**
maximum security property, arming with maximum security ➔ cap. 8 *p. 17*

▼ **Remote interrogation and remote control**
SMS sent to the unit for status or command request ➔ cap. 9 *p. 18*

▼ **System test**
system test to check system working ➔ cap. 10 *p. 21*

▼ **Anomalies diagnostics**
anomalies check ➔ cap. 11 *p. 21*

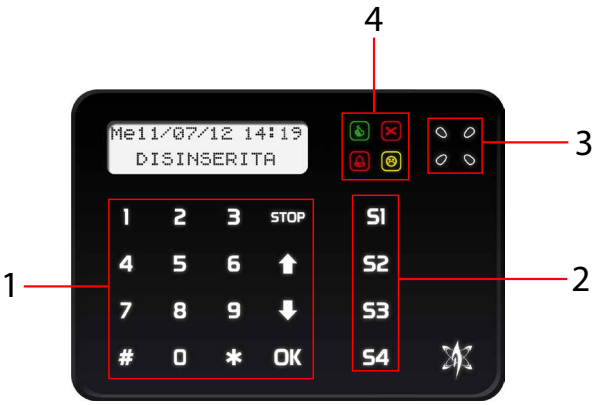
2 KEYPADS USAGE

PREGIO control units are multi-area devices capable of

managing up to 16 sectors.
During unit setup, sectors can be divided into:

- **4 areas** including **4 sectors** each;
- **2 areas** including **8 sectors** each;
- **1 area** including all **16 sectors**.

Keypads allow to perform arming and disarming operations considering such distribution.
Keypad example:



1 Number and control keys
2 Sector buttons
3 Proximity keys reader
4 LED indicators

2.1 Keypad parts

2.1.1 Sector buttons

Keypads are equipped with 4 sector keys allowing the selection of sectors to be armed/disarmed.

Sector keys indications may vary according to the distribution of sectors among areas.

4 Areas / 4 sectors mode

Each sector key is associated to a sector of the currently operating area distinctively and provides information about arming status of the corresponding sector (key S1 for sector 1, key S2 for sector 2, etc.)

Key status	Indication
OFF	Sector disarmed
ON	Sector armed
Fast blinking	Arming with Max Security
Slow blinking	Exit time in progress

8/16 Sectors per area mode

During unit configuration, sector keys are associated to **sector groups** . Each sector key provides information about arming status of corresponding sectors.

Key status	Indication
OFF	All sectors associated to the key are disarmed
ON	All sectors associated to the key are armed
Fast blinking	All sectors associated to the key are armed with maximum security
Fast blinking alternate to steady light	At least one sector associated to the key is armed (but not all)
Slow blinking	Exit time in progress

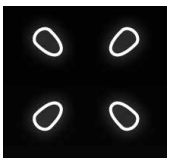
⚠ *Once the system has been armed, arming status is normally displayed on keypad display and/or sector keys: such keys will remain ON if sectors are armed. When the option* **Hide arming state** *is enabled in BrowserOne, all indications will be disabled and sector keys will remain OFF also when the system is armed.*

If the keypad is configured as “system keypad”, its sector keys will indicate arming status of one area (and not that of sectors.)

2.1.2 Number and control keys

Keypads feature number keys and also the following keys:

OK	To enter a menu/submenu or confirm an operation.
STOP	To exit a menu/submenu.
↑ ↓	To browse among menu pages and options

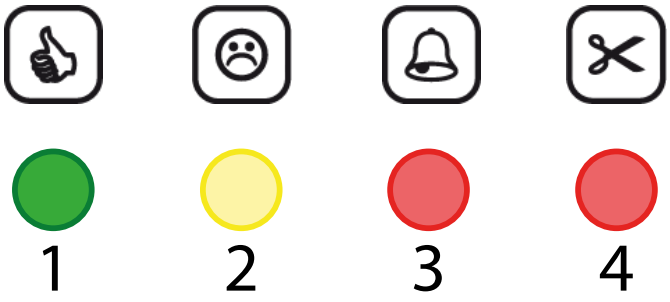


The keypads are normally equipped with a proximity keys reader.

2.1.3 LED indicators

Four LEDs indicates the status of the current area.
If the keypad has been configured as “system keypad”, LEDs will indicate system global status.

The 4 LEDs will blink simultaneously in case of setup from keypad or system locked.



1 Zones status (GREEN)
2 Anomaly (YELLOW)
3 General alarm (RED)
4 Tamper (RED)

1. Zones status LED

It indicates zones arming status.

- **ON**: no zones with alarm/tamper alarm events. The unit can be armed.
- **OFF**: at least one zone not assigned to the exit path is alarmed.
- **Blinking**: the unit is armed and at least one zone assigned to the exit path signals an anomaly event; or at least one zone signals alarm/tamper event but generates an event different from intrusion alarm.

When the LED is off or blinking, the alarmed zones can be displayed using ↓ key.

2. Anomaly status LED

It indicates anomaly status.

- **ON**: no anomalies. However, it is possible to configure the LED so as it remains off when there are no anomalies (via BrowserOne).
- **Blinking**: system anomaly (Mains failure, Low battery, open Tamper or memory anomaly, etc.) or zones anomaly. For details on how to display anomalies, please see paragraph 2.3.2 *p. 4*.

To reset memories, arm and disarm the system.

3. General alarm LED

It indicates general alarm.

- **OFF**: no alarm events.
- **ON**: alarm in progress (active relay).
- **Blinking**: alarm memories. To reset alarm memories, arm and disarm the system.

4. Tamper LED

It indicates tamper status.

- **OFF**: no tampering zones.
- **ON**: tamper alarm in progress (active relay).
- **Blinking**: tamper alarm memories. To reset alarm memories, arm and disarm the system.

⚠ *Once the system has been armed, if the option* **Visualization Protection** *is enabled in BrowserOne, all status indications from LEDs will be disabled.*

Acoustic signalling for tampered zones

The unit can be configured to emit a single or continued acoustic signal ("Din Don") when one or more zones are in anomaly condition.

2.2 Displayed information

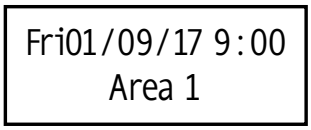
Each keypad can control one (or more) pertaining area(s) and can display its status. The display will show details of all areas, one by one.

Idle display

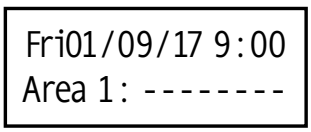
top row: date and time
bottom row: welcome message (if set)

To activate the display, press any keys. It will show the **presenting area** as defined during keypad installation.

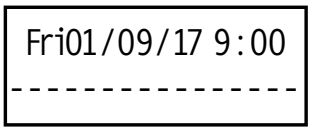
Display with 4 areas / 4 sectors mode



Display with 2 areas / 8 sectors mode

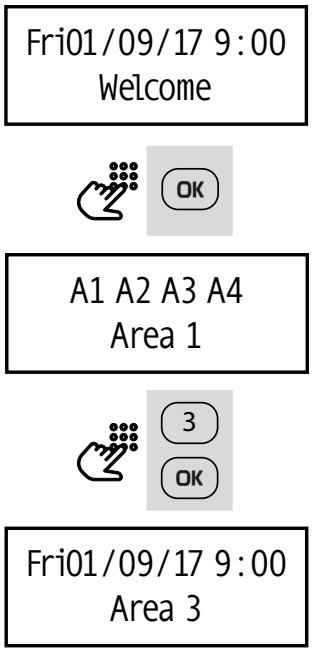


Display with 1 area / 16 sectors mode



2.2.1 Change of current operating area

To change the current operating area:



– Press **OK** while the interface is idle.

The above row shows user's pertaining areas, below row shows the currently operating area.

– Press the number key (1, 2, 3 or 4) corresponding to the desired area (such area can be accessed only if the user has sectors authorised for the area).
– Press **OK** to confirm, **STOP** to exit.

The LEDs will indicate the status of the area just set (not that of the presenting area).

⚠ *The keypad shows presenting area again one minute after the last button has been pressed.*

2.2.2 User menu

A **user menu** is available at keypad.

User menu items allow users to manage basic maintenance.

- ▼ **MAINTENANCE**
  - ➔ BYPASS ZONES
  - ➔ INSTALLER AUTH.
  - ➔ OUTPUT CONTROL
  - ➔ MANAGE SIM BAL.
  - ➔ CLOCK SETUP
  - ➔ CLOCK CALIBR.
  - ➔ WEEKLY PROGR.
  - ➔ MANAGE USERS
  - ➔ PHONE NUMBERS
  - ➔ WI-FI SETTINGS
  - ➔ CHANGE CODE
  - ➔ SYSTEM TEST
  - ➔ MANAGE CHIME
  - ➔ EVENT LOG

For more information: paragraph 2.5 *p. 8*

2.2.3 User code and keypad locked

The most part of commands from keypad requires a 6-digit user code.

If during installation the option **Enable keypad locking for error code** has been enabled, the keypad will be blocked after the wrong code has been entered for three times.

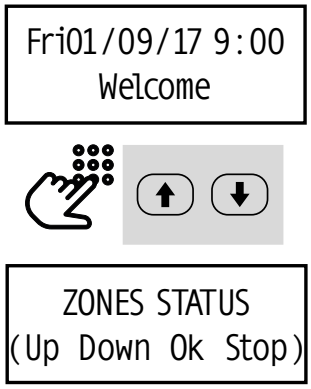
The following message will be displayed for 90 seconds:

⚠ *Further options are available for associating tamper events generation with wrong codes typing. Please see product programming manual.*

2.3 Display the status

"Status display" menu pages will display information of the operating area previously selected.

To enter the menu:



– Press arrow keys ⬆ or ⬇ while the interface is in idle mode.

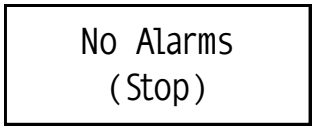
⚠ *If* **Visualization Protection** *option is enabled (for EN50131 standard compliance), the user will have to enter user code and then use arrow keys to go to "status display" menu pages.*

– Press **OK** to enter a menu/submenu, **STOP** to exit.
– When in submenu pages, use arrow keys ⬆ or ⬇ to display relevant data.

2.3.1 Check zones status

– Go to **ZONE STATUS**.
– Press **OK** to enter the menu item.
– Use arrow keys ⬆ or ⬇ to browse the reports.

If there are no reports on the page, the following message will be displayed:



2.3.2 Check anomalies status

The yellow LED will blink in case of anomalies.

To check anomalies:
– Go to **ANOMALIES STATUS**.
– Press **OK** to enter the menu item.
– Use arrow keys ↑ or ↓ to browse the reports.

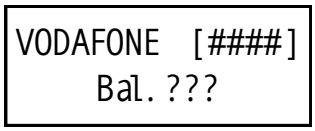
In case of more than one anomaly, an arrow → will appear in the top right corner of the display.
For more information: paragraph 11 *p. 21*.

2.3.3 Tamper and alarm memories

To check alarm and tamper memories logged on unit historic file.
– Go to **ALM/TAMP. MEMORY**.
– Press **OK** to enter the menu item.
– Use arrow keys ↑ or ↓ to browse the reports.

2.3.4 SIM Balance status

If the unit is equipped with a prepaid card, the balance can be displayed on keypad.
– Go to **GSM STATUS**.
– Press **OK** to enter the menu item.



top row: provider and signal strength
bottom row: card balance

The card balance is displayed only in case of prepaid cards; if this is not the case, the balance will not be displayed [???].

2.3.5 Check Internet connection state

Function available from firmware version 3.3.9.
To check Internet connection state:
– Go to **INTERNET STATUS**.
– Press **OK** to enter the menu item.

If there is no connection, **DISCONNECTED** will appear.
If the connection is present, **CONNECTED** will appear followed by the type of connection.

2.4 Operating mode from keypad

Different modes are available for arming from keypad.

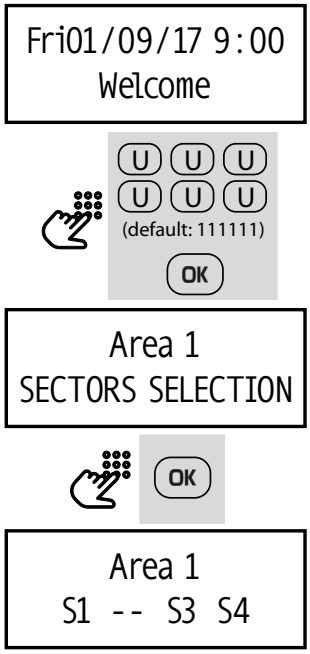
2.4.1 General information on system arming

The system will be armed per sectors.
During system configuration, each user will be assigned sectors to arm.
Each sector can include one zone (or more) that can be associated to intrusion detection devices (detectors, magnetic contacts, etc.)
During unit configuration, some zones can be included into **exit path**. After system arming, users can leave the premises within a set time (**exit time**) through the exit path without triggering an alarm event.
Exit path zones can be set as **exit door**: when users exit and close the door, the remaining exit time will reset and the unit will arm.

⚠ *The subsequent opening of the door generates an alarm.*

2.4.2 Simple arming

With simple arming, the **sectors proposed** to the user will be armed. The sectors proposed are set during system installation.



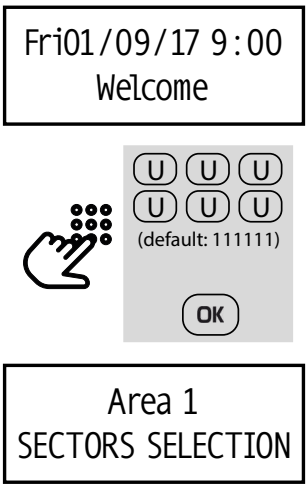
– Key in user code.
– Press **OK**.

Keys of sectors proposed for arming for a specific user will blink in the currently operating area.
– Press **OK** to start arming, **STOP** to cancel it.
– If exit time has been set, it will be marked by beep sounds: leave the protected areas within the set time walking through the path set.

At the end of exit time, sectors proposed will be armed (sector keys remains lighted unless the option **Hide arming state** is enabled).

2.4.3 System arming with sectors selection - 4 areas / 4 sectors mode

The unit features an advanced arming procedure that allows the manual selection of sectors to be armed among the sectors proposed to the user.
With 4 areas / 4 sectors mode, each sector key is associated to a sector distinctively.



– Key in user code.
– Press **OK**.

Pre-arming mode starts. Sector keys of sectors proposed for arming will start blinking (for the specific user in the currently operating area).

– Press a sector key (S1, S2, S3, S4) to change the sectors proposed (if authorised for the specific user).

⚠ *The interval between the pressure of one key and the following one must not be over 5 seconds otherwise the system will arm.*

Example

If sectors proposed for arming at the beginning are S1 and S3

when you press key S2 (if authorised) also sector 2 will be proposed for arming.

If you press key S2 again, sector 2 will be excluded from sectors proposed.

– To change area, press arrow keys ↑ or ↓, then select sectors to be armed.
– When finished, press **OK** to start arming, **STOP** to cancel it.
– If exit time has been set, it will be marked by beep sounds: leave the protected areas within the set time walking through the path set.

At the end of exit time, sectors proposed will be armed (sector keys remains lighted unless the option **Hide arming state** is enabled).

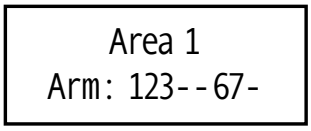
⚠ *if one selected sector cannot be armed, the arming procedure will be stopped.*

2.4.4 System arming with sectors selection - 8/16 sectors per area mode

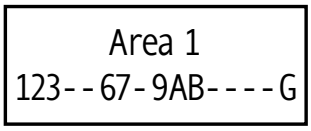
Under 8/16 Sectors per area mode, sector keys are associated to **sectors group**.
Sector keys arm/disarm sector groups. The key-sectors association is made during setup.

– Key in user code.
– Press **OK**.

Keys of sectors proposed for arming for a specific user will blink in the currently operating area.
On the keypad display, a number / letter indicates that the sector associated is proposed for arming (under 16 sectors per area mode letters A to G represent sectors from 10 to 16); hyphens indicate sectors not proposed for arming.
8 Sectors mode



16 Sectors mode



During key blinking (pre-arming time, around 5s), it is possible to change sectors proposed either per single sector, or per sectors group.

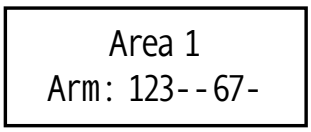
Per single sector:

Press a number key to change a single sector proposed (as long as the sector selected is authorised for the user).

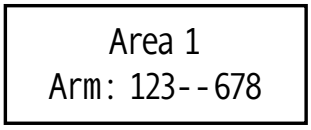
▼ **8 Sectors mode**
Press numeric keys from **1** to **8**.

▼ **16 Sectors mode**
Press numeric keys from **1** to **9**, * (= A), **0** (= B), **#** (= C). The single sector selection is not available for D, E, F, and G sectors.

If sectors proposed for arming at the beginning are number 1, 2, 3, 6, 7



when you press key 8 also sector 8 will be proposed for arming (as long as it is authorised for the user):



If you press key 8 again, sector 8 will be excluded from sectors proposed.

Per sectors group:

Press a number key to change sectors proposed for arming for that specific key according to the following table:

Status BEFORE pressing a sector key		Status AFTER having pressed a sector key
At least one sector (but not all) among those associated to that key is proposed for arming	→	All sectors associated to that key are proposed for arming (as long as they are authorised for that user)
All sectors associated to that key are proposed for arming	→	No sectors associated to that key are proposed for arming (as long as they are authorised for that user)

If sectors proposed for arming are

```
Area 1
Arm: 123--67-
```

and sector key S2 has sectors 3, 4, and 5 associated (all authorised for the user too), when you press sector key S2 items proposed for arming will change:

```
Area 1
Arm: 1234567-
```

– When finished, press **OK** to start arming, **STOP** to cancel it.
– If exit time has been set, it will be marked by beep sounds: leave the protected areas within the set time walking through the path set.

At the end of exit time, sectors proposed will be armed (sector keys remains lighted unless the option **Hide arming state** is enabled).

2.4.5 Fast arming - 4 areas / 4 sectors mode

If two specific options are enabled, sectors can be armed without entering the user code.

Arming with sector key + OK

⚠ *The option* **Enable fast arming** *in BrowserOne has to be activated.*

– Press sector key of the sector to be armed (the sector can be armed if it is authorised at least to one user). The key will start blinking.

```
Sector S1. A1
FAST ARMING?
```

– Press **OK** to confirm (if not, the procedure will be cancelled after 5s).
– If an exit time has been set, leave the protected areas within the set time.

When during the procedure another sector key is pressed, the sector to be armed will be changed.

The procedure will be cancelled if you press the key of a sector that cannot be armed.

Arming with double pressure

⚠ *The option* **"Fast arming / output maneuver" pressing sector key twice** *has to be enabled in BrowserOne.*

– Press sector key of the sector to be armed (the sector can be armed if it is authorised at least to one user). The key will start blinking.

```
Sector S1. A1
FAST ARMING?
```

– Press the key again.
– If an exit time has been set, leave the protected areas within the set time.

The procedure will be cancelled if you press the key of a sector that cannot be armed.

2.4.6 Fast arming - 8/16 sectors per area mode

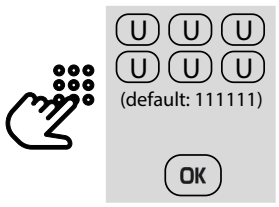
Fast arming option can be enabled under '8/16 sectors per area' mode (if checked during system configuration); to do so, press sector key + OK, or press sector key twice (as explained in the previous paragraph 2.4.5 *p. 7.*

Sectors associated to that sectors key will be armed as long as they are also authorised for the user.

2.4.7 Disarming

When system is armed:

```
Ve01/09/17 09:00
Armed       S 1234
```




```
Ve01/09/17 09:00
Disarmed
```

– Key in user code.
– Press **OK**.

System disarming will be marked by beeping sounds.

Only sectors authorised for the specific user will be disarmed.

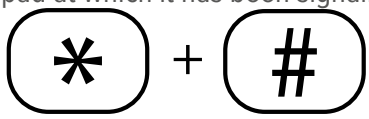
2.4.8 Disarming with duress mode.

A duress event occurs when a user is forced to disarm the

system at keypad.
In such case:
– Key in user code increasing or decreasing the last digit by one unit (example: 123450 or 123458 when the real code is 123459).
– Press **OK**.
The control unit will be disarmed and, at the same time, a "duress event" will be generated. The event will be managed via phone dialler or GSM module.

2.4.9 Panic alarm from keypad

If necessary, it is possible to generate a "Panic alarm", indicating the keypad at which it has been signalled.



– Press keys * and # on keypad simultaneously.

2.4.10 Arming advanced functions

Authorise system arm / disarm

During system configuration, the installer can set arm/disarm authorisation for each user on **Users** menu page in BrowserOne.
A user can be denied authorisation for arming or disarming or for both commands; in the latter case, the user can still check control unit status and access maintenance menu (if authorised).

⚠ *At least one user must always be authorised for system arm/disarm.*

Forced arming through keypad

If the option **Activate Arming Lock** in BrowserOne is active, system arming will be denied if some fault conditions occur. When the arming is denied due to a dialler failure or lack of supervision, users can force the arming only through the keypads controlling the areas involved in the arming denied.
– When forced arming is allowed, the following message will be displayed:

ANOMALY
FORCE ARMING?

– Press **OK** within 15 seconds to start forced arming, **STOP** to cancel it.

⚠ *Bypassed detectors will not cause system lock.*

Fast arming will automatically be performed in case of failure or lack of supervision when arming is activated by remote control via software or SMS, and by time scheduler.
Forced arming will not be allowed in case of zones with anomaly events. If the user has sent an arming command via SMS, the unit will reply with "**ARMING DENIED**".

Installer intervention

If the following option has been enabled
Required authorization of the installer for inclusion with...,
and one of the following events occur:
- system / control devices / serial devices tamper
- dialler / siren / battery fault

the installer code will be required to force system arming:

INSTALLER CODE :

The installer authorisation is required also when arming the system with a remote control or a M4 key that is not associated to the keypad.
All keypads of areas affected by the arming command will display

REQUIRED
INSTALLER AUTH.

Arming/disarming signalled from siren

Arming and disarming can be signalled by the sirens connected to the control unit. In detail:
- **arming**: single blink, acoustic signal
- **disarming**: double blink, acoustic signal

Arming from external control device

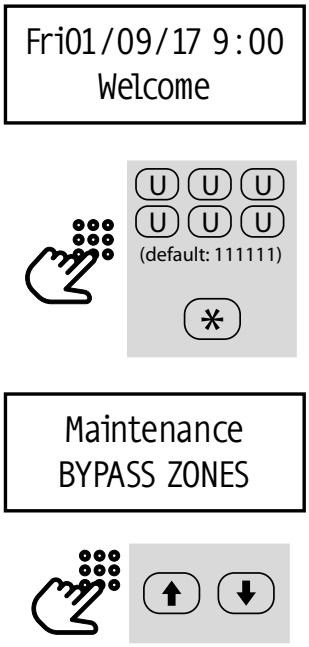
Control units can recognise arm/disarm commands sent by control devices different from the compatible ones (example: receivers already existing in the system.)
Such control devices has to be wired to control units zones conveniently and set for such purpose.
They shall feature the same performance level as the control unit.

2.5 Enter USER MENU on keypad

PREGIO units provide a **user menu** that can be accessed at keypad.
User menu items allow users to manage basic maintenance.

⚠ *The user can access the menu only if authorised by the installer (with* **Basic Maintenance** *option).*

To enter user menu:



– Key in user code (default: 111111).

⚠ *It is strongly recommended to change the code to strengthen system security level. The installer cannot see it since it is represented by asterisks.*

– Press * key.
– Use arrow keys ↑ or ↓ to browse among options.
– Press **OK** to enter a menu item, **STOP** to exit setup.
– If you press **STOP** repeatedly after an operation, you may be asked to save changes.

SAVE CHANGES?
(Ok=Yes #=No)

While in user menu, the 4 LED indicators will blink simultaneously.
The user menu lists the following items (on the right, the number of the paragraph with details on the items):

▼ **MAINTENANCE**
- ➔ **BYPASS ZONES** - § 2.5.1 *p. 9*
- ➔ **INSTALLER AUTH.** - § 2.5.2 *p. 9*
- ➔ **OUTPUT CONTROL** - § 2.5.3 *p. 10*
- ➔ **MANAGE SIM BAL.** - § 2.5.4 *p. 10*
- ➔ **CLOCK SETUP** - § 2.5.5 *p. 10*
- ➔ **CLOCK CALIBR.** - § 2.5.6 *p. 10*
- ➔ **WEEKLY PROGR.** - § 2.5.7 *p. 10*
- ➔ **MANAGE USERS** - § 2.5.8 *p. 10*
- ➔ **PHONE NUMBERS** - § 2.5.9 *p. 10*
- ➔ **WI-FI SETTINGS** - § 2.5.10 *p. 10*
- ➔ **CHANGE CODE** - § 2.5.11 *p. 11*
- ➔ **SYSTEM TEST** - § 2.5.12 *p. 11*
- ➔ **MANAGE CHIME** - § 2.5.13 *p. 12*
- ➔ **EVENT LOG** - § 2.5.14 *p. 12*

2.5.1 Zones bypass

Users can bypass zones with anomaly (example: for maintenance operations).
– Use arrow keys ↑ or ↓ to go to **BYPASS ZONES** option.
– Press **OK** to enter the menu.
– Use arrow keys ↑ or ↓ to browse among zones or enter the zone number directly (example, key in 003 for zone 3) .
– Press **OK** to bypass the zone and exit the menu, or press **STOP** to exit the menu without saving.

Zone 001 BYPASS
Zone 001

To include the zone again, repeat the steps.

Zone 001 ENABLED
Zone 001

If the installer has enabled **Zone exclusion only from installer** via BrowserOne, the menu will not be available for users and zones can be bypassed by the installer only.

2.5.2 Limits to installer access

Installers access to configuration is subject to users' authorisation.
The authorisation is valid for all access modes: from keypad, direct connection or remote assistance.
The user has to grant the authorisation to visualise its own images (via BrowserOne).
The user can use the following menu:
– Use arrow keys ↑ or ↓ to go to **INSTALLER AUTH.** option.
– Press **OK** to enter the menu.
– Press **1 (=Acc.)** repeatedly to change control unit access authorisation:

▼ **TEMPORARY**
Until the end of the connection session.

▼ **NONE**
Access denied.

▼ **PERMANENT**
Access granted.

– Press **2 (=Img.)** repeatedly to change authorisation to visualise user images in BrowserOne:

▼ **NONE**
The installer cannot view the images.

▼ **LOCAL**
The installer can view the images only via USB connection (default).

▼ **ALWAYS**
The installer can view the images only via any type of connection.

– Press **STOP** to save and exit the menu.

2.5.3 Manual control of outputs

Users can change outputs status if such outputs have been assigned "Manual control" option.

– Use arrow keys ↑ or ↓ to go to **OUTPUT CONTROL** option.
– Press **OK** to enter the menu.
– Use arrow keys ↑ or ↓ to browse among outputs or enter the output number directly (example, key in 003 for output 3) .
– Press **OK** repeatedly to change output status (**ENABLED**/**DISABLED**).

⚠ *When all outputs are disabled the message* **No Out.Available** *will be displayed. When an output is associated to an event and/ or cannot be controlled by the user, its status can be checked but it cannot be managed.*

– Press **STOP** to save and exit the menu.

2.5.4 SIM balance check

Users can enable/disable balance reading of GSM module SIM card.
This option is available only if the correct **SIM Balance Check Profile** has been selected by the installer.

– Use arrow keys ↑ or ↓ to go to **MANAGE SIM BAL.** option.
– Press **OK** to enter the menu.
– Press **OK** repeatedly to change output status (**READING ENABLED**/**READING DISABLED**).
– Press **STOP** to save and exit the menu.

⚠ *Not all telephone companies allow such operation.*

2.5.5 Date and time setup

– Use arrow keys ↑ or ↓ to go to **CLOCK SETUP** option.
– Press **OK** to enter the menu.
– Use number keys to set weekdays (**1** = Monday ... **7** = Sunday), day/month/year, hour and minute. Use arrow keys ↑ or ↓ to move cursor along the row: data which are being modified will blink.
– Press **OK** to save and exit the menu, or press **STOP** to exit the menu without saving.

2.5.6 Clock calibration

Use this menu to manually adjust the difference in time occurred over a month between the control unit clock and the standard one.

– Use arrow keys ↑ or ↓ to go to **CLOCK CALIBR.** option.
– Press **OK** to enter the menu.
– Use arrow keys ↑ or ↓ to increase/decrease seconds per month (5s/month steps).
– Press **OK** to save and exit the menu, or press **STOP** to exit the menu without saving.

2.5.7 Schedules change

The activation time of a schedule set with the programmer can be suspended or modified.

⚠ *There has to be at least one schedule set and users has to be authorised for changes.*

– Use arrow keys ↑ or ↓ to go to **WEEKLY PROGR.** option.
– Press **OK** to enter the menu.

⚠ *If there are no schedules available the message* **No prog. avail.** *will be displayed.*

– Press 1 to start modifying time: use number keys to modify time, arrow keys ↑ or ↓ to move cursor. Press **OK** to confirm.
– Press # to suspend a schedules, press 1 to restart it.
– Press **STOP** to save and exit the menu.

2.5.8 Users authorisations management

The user who has been authorised during system installation can change other users' authorisation to system access.

– Use arrow keys ↑ or ↓ to go to **MANAGE USERS** option.
– Press **OK** to enter the menu.
– Use arrow keys ↑ or ↓ to select user to manage.
– Press **OK** repeatedly to change the user's authorizations:
• **FULL**
• **ARM ONLY** (= only arming)
• **DIS. ONLY** (= only disarming)
• **SUSPENDED** (= system access denied)
– Press # key to suspend a user. The suspension can be set through weekly programmer too. However, setup from keypad has priority over other settings.
– Press **STOP** to save and exit the menu.

2.5.9 Change phone numbers

Numbers on phone numbers list can be modified.

– Use arrow keys ↑ or ↓ to go to **PHONE NUMBERS** option.
– Press **OK** to enter the menu.
– Use arrow keys ↑ or ↓ to select the number to be modified.
– Press **OK** to activate the field.
– Use number keys, * and # to key in the number: cursor will move rightwards. Press ↓ to cancel one digit. Press ↑ to enter an empty space. Press S4 to cancel the entire row.
– Press **OK** to save and exit the menu, or press **STOP** to exit the menu without saving.

2.5.10 Set the Wi-Fi connection

The user can set the connection data of the Wi-Fi network. This entry is only available if the installer enabled it and if a Wi-Fi module is installed.

– Use arrow keys ↑ or ↓ to go to WI-FI SETTINGS option.
– Press **OK** to enter the menu.
– Press **1** repeatedly to select the protection used by the

router: None; WEP, WPA2 PSK.

If 1 is not pressed, the previously chosen protection (initially "None") is used.

– Press **OK** to continue.
– Use number keys to type the network name: cursor will move rightwards. Press ⬇ to cancel one digit. Press **S4** to cancel the entire row.
– If the protection has been set to "None" or "WEP", press **OK** to save and exit the menu, or press **STOP** to exit the menu without saving.
– Otherwise, press **OK** to continue.
– Use number keys to type the network's password: cursor will move rightwards. Press ⬇ to cancel one digit. Press **S4** to cancel the entire row.
– Press **OK** to save and exit the menu, or press **STOP** to exit the menu without saving.

While the password is being saved, the **Wait Please** message appears. While it stays, you can press **STOP** to cancel saving.

Once finished, the **PSWD SAVED** message appears, press **OK** to save and exit.

Key-character correspondence

1. ., - 1 @ ? ! % # $ &	**6.** M N O 6
2. A B C 2	**7.** P Q R S 7
3. D E F 3	**8.** T U V 8
4. G H I 4	**9.** W X Y Z 9
5. J K L 5	**0.** [space] _ 0 ( ) ; : ^ /

– Press a key repeatedly to select the chosen character, cycling through characters in the shown sequence.
– Press **#** to change the last typed character form uppercase to lowercase or viceversa; the setting is kept for all following characters.

Example: to type "teST" press 8 # (T➜t) 33 (e) 7777 # (s➜S) 8 (T).

Succesful connection check

In order to verify on your own that the Wi-Fi connection works properly you can follow several procedures:

▼ **Open the router's setting pages**

Many routers list connected devices.

Open the router's configuration and check the presence of a device which name is made by three pairs of characters prefixed by GS, IMW or by the name of the Wi-Fi module installed in the control unit, e.g. MDWIFI_0F_82_AB or GS_B7_29_1A.

▼ **Test the Wi-Fi connection to e-Connect**

The control unit has to be connected to an e-Connect account.

It is necessary that Wi-Fi is the control unit's preferential method of connection to e-Connect or that all methods of connection with higher priority can be interrupted by the user without causing alarms.

Make sure that the control unit communicates with e-Connect over Wi-Fi by interrupting more prioritary methods of connection.

Access e-Connect and check that it is possible to connect to the control unit.

– If the connection is not working properly, make sure that connection credentials have been entered correctly.

2.5.11 Change user code

Users can change their codes.

– Use arrow keys ⬆ or ⬇ to go to **CHANGE CODE** option.
– Press **OK** to enter the menu.
– Use number keys to enter the code. Digits will be represented by asterisks (*).
– Enter the code again. If the two codes match, the new code is memorised and the function exits the menu automatically.

2.5.12 System test

The test includes 4 steps: ZONE TEST, OUTPUT TEST, DIALLER TEST, BATTERY TEST.

For the test to be considered valid, all four steps have to be run in sequence, without exiting the SYSTEM TEST menu: please wait for each step to be completed (with messages TEST OK, TEST EXECUTED or NOT EXECUTAB.) and go to the next one.

If users press **STOP** before the end of a step, the test will be stopped and considered invalid.

Start system test

– Enter user menu.
– Use arrow keys ⬆ or ⬇ to go to **SYSTEM TEST** option.
– Press **OK** to enter the menu.
– Use arrow keys ⬆ or ⬇ to browse among available steps. Press **OK** to start a test.

ZONE TEST

– Press **OK** to start a test.

⚠ *All connected zones with "walk test" property will be tested one by one. If no zones have the walk test property, the message* **NOT EXECUTAB.** *will appear.*

– The system shows the first zone to be tested which will be alarmed. The system beeps for confirmation and is now ready to test the following zone.
– Repeat the previous step for all zones displayed.
– Once the test is completed, press **STOP** to exit test step.
– Use arrow keys ⬆ or ⬇ to go to the next step.

OUTPUT TEST

– Press **OK** to start a test.
– The following outputs will be temporarily activated: programmable relay (if activated during setup), external siren, RS-485 and NG-TRX sirens (if present). All outputs

will be activated for 6 seconds and the activation can be interrupted by pressing # key.

Note: the NG-TRX sirens are activated on an area basis: if there are several sirens within the same area, they will all be activated at the same time. Areas with no sirens are not displayed.

– Press **OK** to go to the next output to test. Repeat for each output.
– Once the test is completed, press **STOP** to exit test step.
– Use arrow keys ↑ or ↓ to go to the next step.

DIALLER TEST

– Press **OK** to start the test. The dialler activates and the message TEST CALL will be displayed.
– Press **OK** again to start the test. Wait for test to be completed (the message NOT EXECUTAB. will be displayed if the dialler is disabled.)
– Once the test is completed, press **STOP** to exit test step.
– Use arrow keys ↑ or ↓ to go to the next step.

BATTERY TEST

– Press **OK** to start the battery test that will check battery efficiency.
– When the test is ok, the message TEST EXECUTED will appear. In case of anomalies, the corresponding events will be stored in the control panel.

⚠ *The interval between battery tests shall be at least 2 minutes.*

– Once the test is completed, press **STOP** to exit test step.

⚠ *In case of battery replacement, after the replacement it is necessary to do a battery test to reset the anomaly signal.*

2.5.13 Chime management

Users can enable/suspend chime function. The function shall be enabled for each zone individually during zones configuration.
When enabled, an acoustic signal will be emitted by the keypad when the zone is activated while its sectors are disarmed or when a zone with 24H is alarmed.

– Use arrow keys ↑ or ↓ to go to **MANAGE CHIME** option.
– Press **OK** to enter the menu.
– Press **OK** repeatedly to select **ENABLED** or **SUSPENDED**.
– Press **STOP** to save and exit the menu.

2.5.14 Events log

Users can check system events list saved.

– Use arrow keys ↑ or ↓ to go to **EVENT LOG** option.
– Press **OK** to enter the menu.
– The function will display the last event saved and the corresponding user. Press ↑ or ↓ to browse among events. Press * key to display date and time of the event.
– Press **STOP** to exit the menu.

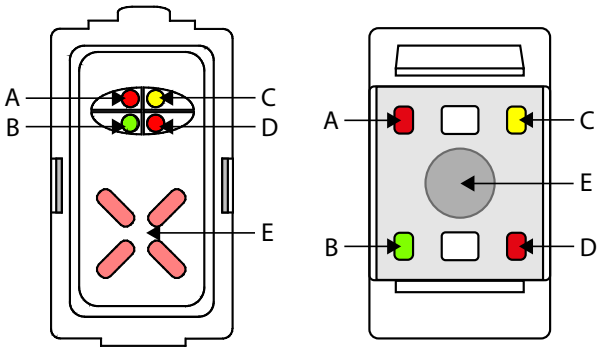
3 PROXIMITY KEYS USAGE

With proximity keys users can arm/disarm systems quickly by drawing them close to system readers (I8, I66, IZENITH).

⚠ *The keys shall be registered to the control unit.*

3.1 Readers type

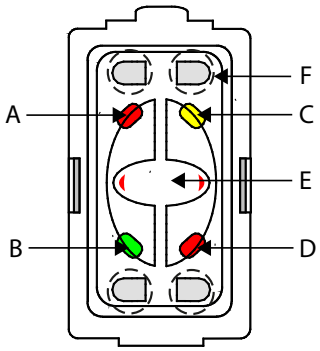
I8 - I66 - I9 - I10



A Tamper/general alarm LED (shared indication)
B Unit arming status LED (zones status)
C System anomaly LED
D System arming status LED
E Area for M4 key

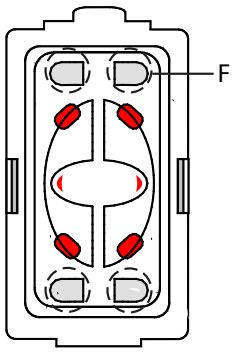
For LEDs indications, please see paragraph 2.1.3 *p. 2*.

IZENITH



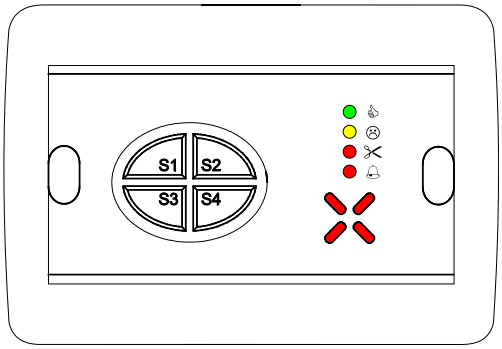
A Tamper/general alarm LED (shared indication)
B Unit arming status LED (zones status)
C System anomaly LED
D System arming status LED
E Area for M4 key
F Sectors selection keys

For LEDs indications, please see paragraph 2.1.3 *p. 2*.
IZENITH can be set for one area only.



During arming procedure, red-lighted LEDs will indicate sectors arming status.

ETRZENITH



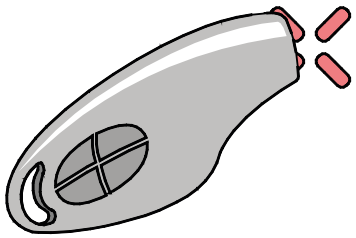
ETRZENITH includes a LED indicator, one area for arming with proximity keys, and 4 sector keys to select for sectors arming.
For LEDs indications, please see paragraph 2.1.3 *p. 2*.
ETRZENITH can be set for one area only.

3.2 Proximity keys usage

Before proceeding, please see arming general information (paragraph 2.4.1 *p. 5*).

3.2.1 System arming

– Place the proximity key near the sensitive area (onto reader or keypad).



– The pre-arming time will start (around 5s): if there are sector keys, users can modify sectors proposed for arming. Please see paragraph 2.4.3 *p. 5*.
– When the pre-arming time elapses, the exit time will start (if set). Leave the protected area within such time walking through the path set.

When exit time elapses, the unit status LED will light up.

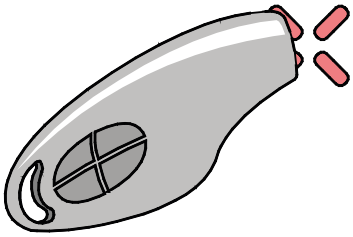
3.2.2 Disarming

When system is armed:

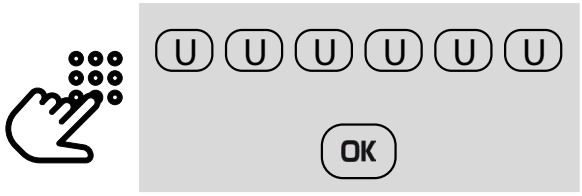
– Place the proximity key near the sensitive area (onto reader or keypad).
– Wait a few seconds until the unit status LED (on readers) or sector keys (on keypad) switches OFF.

3.2.3 Disarming with duress mode.

Users may be forced to disarm the system with a proximity key (duress event).
To protect against this possibility, users may ask installers to activate the "double confirmation" function, that is, all disarming procedures with proximity keys have to be confirmed by entering a user code (to keypad) within a set time interval.
To disarm with double confirmation function active:



– Place the proximity key near the sensitive area.
– Go to the nearest keypad within the time set during system configuration (**Double confirmation time for duress**).



– Key in user code.
– Press **OK**.

All areas feature a separate timer: if a disarming procedure involves multiple areas, timers of all involved areas will activate.
The code entered may not be of the same user that disarmed the unit; however each user can lock only timers of pertaining areas.
If the time interval elapses without the confirmation of the system disarming, a duress alarm related to the user that disarmed will be created.

3.2.4 System forced arming

If the option **Activate Arming Lock** in BrowserOne is active, system arming will be denied if some fault conditions occur. If arming is not allowed because of dialler fault or lack of supervision events, users can force system arming only using control devices that control areas involved in the arming lock.
– When arming can be forced, the red arming LED will start blinking rapidly.
– Within 15 seconds: to force arming place M4 key again near the reader or press **OK** on the keypad to which the reader is connected.

⚠ *Bypassed detectors will not cause system lock.*

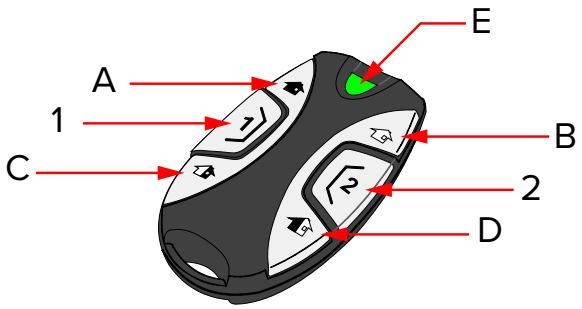
4 REMOTE CONTROLS USAGE

Remote control devices can be used to arm (either totally or partially) and disarm systems.
Remote controls have to be learned to a specific device.

Remote control	Device
ATLANTE4, ATLANTE6	RIVERRF
ATLANTE4PLUS	RIVERRFPLUS
ATLANTE2K	GATEWAY2K

4.1 Function keys

The following image refers to ATLANTE2K device. Other devices may not feature the same function keys.



A Key "TOTAL ARMING"
B Key "TOTAL DISARMING"
C Key "PARTIAL ARMING 1"
D Key "PARTIAL ARMING 2"
E Two-colour LED for data transmission status

1 Key "OUTPUT 1 CONTROL"
2 Key "OUTPUT 2 CONTROL"

Please refer to the manual of the remote control in use for information on keys and LED indications.

4.2 Operation with remote controls

Before proceeding, please see arming general information (paragraph 2.4.1 *p. 5*).

4.2.1 System arming

To arm the system, press one of the following keys:
- "Total arming" (A): arms **all sectors authorised** for the user
- "Partial arming 1" (C): arms **sectors proposed** for the user
- "Partial arming 2" (D): arms **sectors authorised but not the proposed ones**

Example

if sectors authorised are number 1, 2, 3, 4, 5, 6, and proposed ones are 1, 2, 3, 4, only the remaining sectors 5 and 6 will be armed.

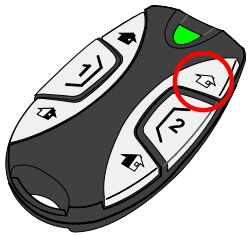
⚠ *For some remote controls, installers can modify the default configuration of "Partial arming 1" key and "Partial arming 2" key so that such keys will arm/disarm defined sectors instead of sectors proposed and sectors authorised but not the proposed ones respectively*

4.2.2 Disarming

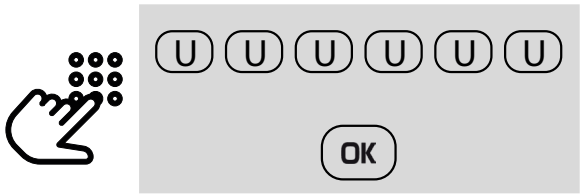
– Press "total disarming" (B) key.

4.2.3 Disarming with duress mode.

Users may be forced to disarm the system with a remote control device (duress event).
To protect against this possibility, users may ask installers to activate "Double confirmation" function, that is, all disarming procedures with remote controls have to be confirmed by entering a user code (to keypad) within a set time interval.
To disarm with double confirmation function active:



– Press "total disarming" key (B).
– Go to the nearest keypad within the time set during system configuration (**Double confirmation time for duress**).

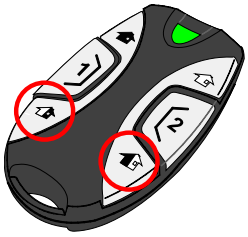


– Key in user code.
– Press **OK**.

All areas feature a separate timer: if a disarming procedure involves multiple areas, timers of all involved areas will activate.
The code entered may not be of the same user that disarmed the unit; however each user can lock only timers of pertaining areas.
If the time interval elapses without the confirmation of the system disarming, a duress alarm related to the user that disarmed will be created.

4.2.4 Panic event

When necessary, a panic alarm event can be generated by pressing "Partial arming 1" key (C) and "Partial arming 2" key (D) simultaneously.



If suitably set, sirens and phone dialler will activate upon panic event.

4.2.5 System forced arming

If the option **Activate Arming Lock** in BrowserOne is active, system arming will be denied if some fault conditions occur.
If arming is not allowed because of dialler fault or lack of supervision events, users can force system arming only using control devices that control areas involved in the arming lock.

– Within 15 seconds: to force arming press again the remote control key previously selected.

⚠ *Bypassed detectors will not cause system lock.*

5 GSM AND PHONE COMMUNICATIONS

Depending on the model, the PREGIO control units support the following modules:

- **MDPSTN**: to connect to an analogue telephone line;
- **MDGSME** or **MDGSMI**: allows connection to the GSM network to send voice and SMS messages.

PREGIO1000, PREGIO1000BM, PREGIO2000 support the MDPSTN, MDGSME modules.
PREGIO500, PREGIO1000PL, PREGIO2000PL support the MDPSTN, MDGSMI modules.

5.1 Calls reception

Users will receive calls or SMS texts when specific alarm events occur (defined during setup.)
Events can also be used for transmissions to surveillance centres.
When users receive a phone call, they can use one of the following keys on the phone keypad:

5	The call is interrupted, the unit will call the following number (if set).
0	The call is interrupted, the unit will not call other numbers until a new event occurs.
* **or #**	It activates **remote listening** function. The call will be terminated after 2 minutes automatically, or whenever users want by pressing 0 or 5 key.

5.1.1 Remote listening

⚠ *Remote listening function is available only if MDVOICE64 voice synthesis module has been installed and registered.*

The function can be activated also via remote control command.

M.ON

(see 9 *p. 18*).
When the activation request is accepted, the unit will send an SMS text to confirm

REMOTE LISTENING REQ.

and will call the number and immediately activate the remote listening function for 2 minutes.

5.2 Receiving SMS from control units

If the unit is equipped with GSM module, during configuration it is possible to activate SMS sending upon events (alarms, arming/disarming commands, anomalies).
Users with their phone number on the list will receive a SMS text from the unit upon occurrence of such events.
SMS texts contain information on system status.
The unit can send maximum 1000 events / day.
During installation it is possible to set "forwarding numbers ", that are number to which the unit will forward SMS texts not identified as remote control texts (example, SMS texts sent by phone companies, etc.)

5.3 SIM balance check

If installers activate the balance control of prepaid SIM cards installed on to GSM module, users can suspend / activate again the balance control:

- from keypad (**MANAGE SIM BAL.** in user menu) details at: 2.5.4 *p. 10*
- via SMS (texts **C.OFF** / **C.ON** messages) details at: 9 *p. 18*

5.4 Sending SMS to control units

SMS texts are used to receive information about unit status or send commands to the unit.
For details, please see 9 *p. 18*.

5.5 Change number list from keypad

Users can modify the phone number list using **PHONE NUMBERS** in user menu.
For more information: paragraph 2.5.9 *p. 10*.
Such user change can be disabled during configuration.

5.6 Advanced settings

The installer can set advanced settings using BrowserOne software.

5.6.1 Dialler block at disarming

Users can require to block phone communications (voice and digital) caused by sectors disarming.
This function is available in **System Options** menu in

BrowserOne.
If dialler block is removed, the phone dialler will activate when the first event generated after the removal occurs.

5.6.2 Limits to dialler activations

Installers can program the control unit so that it limits the number of events that trigger the dialler.
When the max number is reached, the voice/SMS dialler ignores other calls until the next day.
This function is available in **Telephone Dialler** menu in BrowserOne.

⚠ *Limits refer to events, and not to calls: the amount of calls can be higher if events cause several calls. Moreover, the limit refers only to voice dialler and not digital dialler.*

5.6.3 Disable arm/disarm commands

Installers can disable arm/disarm commands via SMS texts or voice communications (not digital ones) for each single user.
This function is available in **Users** menu in BrowserOne.

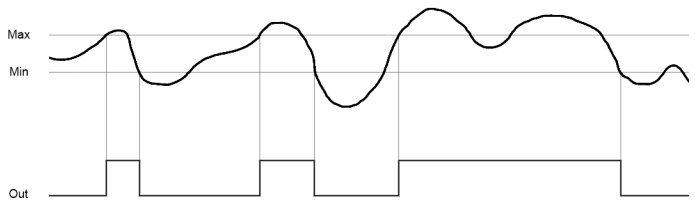
6 TEMPERATURE MONITORING

PREGIO series units are equipped with a temperature detector measuring the temperature inside the housing.

⚠ *Temperature detected from the sensor shall be considered only as a technical indication, for example for the installation of units inside technology closets. Do not use it as a thermostat.*

6.1 Temperature thresholds

The installer can set two thresholds, one minimum and one maximum:
- when the temperature goes from minimum to maximum threshold the "Maximum Temperature" event will be generated.
- when the temperature goes from maximum to minimum threshold the "Minimum Temperature" event will be generated.



Such events can be used to activate the on-board relay or an external one.

6.2 A-B temperatures management

A more advanced temperature control can be realised using output functions and alarm/pre-alarm thresholds (in **BrowserOne**: page Temperature, tab **Management of A-B temperatures**).
The installer can set four thresholds with corresponding events: two for high temperature (Pre-alarm A and Alarm A), and two for low temperature (Pre-alarm B and Alarm B.)
The installer can set an output to activate when the temperature reaches one of the thresholds and to reset when the temperature falls again within threshold ranges set.
If the temperature is not over/under thresholds set, the output can be reset also by users in the two following ways:

⚠ *It is required the installer has set one output with* **Control of A-B temperatures** *function associated to a* **SX** *sector key.*

Reset from keypad

– Key in user code.
– Press SX sector key.

Reset via SMS

– Send SMS command **S.X** (see chapter 9 *p. 18*).

Example

If S3 key has been associated to the function, the output will reset:
- with the user code keyed in and followed by S3 key, or
- sending an SMS text with **S.3**

7 E-CONNECT

e-Connect is a supervision software for EL.MO. intrusion detection systems.
e-Connect allows users to control and manage their systems via the Internet, a PC or a smartphone application.
Operations with e-Connect software:
- check control unit status (anomalies, tamper events, alarms)
- arm / disarm procedures
- read events log
- enable/disable outputs

For the correct use of the software, units have to be equipped with one of the following modules:
- MDLAN or MDGSME for PREGIO1000, PREGIO1000BM, PREGIO2000
- MDWIFIH, MDLAN or MDGSMI for PREGIO1000PL, PREGIO2000PL
- MDWIFIH or MDGSMI for PREGIO500

The installer has to configure the unit suitably and set one user account.
To access e-Connect, download the app (available for

Android and iOS systems) or login to https://connect.elmospa.com.
For more details on e-Connect, please see the user manual on www.elmospa.com site (also for download).

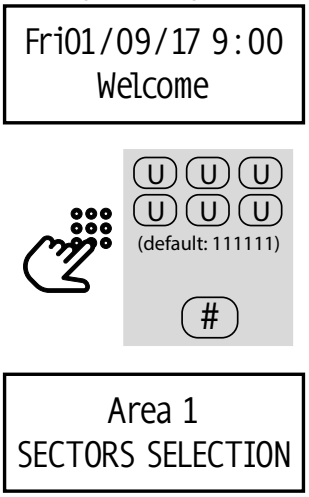
8 MAX SECURITY

Sectors can be armed with **Max Security** property.
Such property can be set by the installer during configuration.
When a sector is armed in Max Security mode it can only be disabled

- by a user with 'max security' property (enabled via BrowserOne during configuration)
- via weekly programmer
- by the installer via software.

8.1 Arming with Max Security

To arm with Max Security property:



– key in user code
– press # key
– continue as illustrated for normal arming:

- **simple arming**: press **OK** (see paragraph 2.4.2 *p. 5*).
- **arming with sectors selection**: use sector keys to modify sectors proposed (see paragraph 2.4.3 *p. 5*). When finished, press **OK**.

Sector keys corresponding to sectors armed with Max Security property will blink quickly.
Sectors armed with Max Security property will blink on keypad display.

⚠ *Users without Max Security property cannot disarm sectors until at least one of sectors authorised for them or for the keypad are armed with Max Security.*

8.2 Notes on Max Security

A sector can be armed with Max Security property:

- by a user with Max Security property: in such case the sector is armed in **User Max Security** mode;
- by the weekly programmer: in such case is armed in **Weekly Programmer Max Security** mode.

The User Max Security property is reset at any disarming; when a sector armed with Max Security property is disarmed the property is reset.
On the contrary, the Weekly Programmer Max Security property is reset by "Max security disarming" and "Max security reset" weekly programmer functions only.

⚠ *In detail, if a sector is armed in Weekly Programmer Max Security mode and a user with max security property performs a disarm, the Weekly Programmer Max Security property remains active. Therefore, at the next control unit arming it will be armed with Max Security property, even if the arming is performed by a user without the Max Security property. However, if the disarming is performed via weekly programmer Max Security Reset function, the sector property will be reset and the sector can be armed in the standard way.*

The following icons indicate sectors arming status:

	Sector disarmed, no Max Security
	Sector disarmed, Weekly Programmer Max Security
	Sector armed, no Max Security
	Sector armed, Weekly Programmer Max Security
	Sector armed, User Max Security
	Sector armed, User Max Security + Weekly Programmer Max Security

The following table illustrates Max Security operating mode for arming/disarming events:

Starting condition	Action	End status
	Arming made by user / weekly programmer without Max Security	
	Arming made by user with Max Security	
	Arming made by weekly programmer with Max Security	
	Arming made by user without Max Security	
	Arming made by user with Max Security	

	Arming made by weekly programmer with/without Max Security	
	Disarming made by user / weekly programmer	
	Disarming made by user with Max Security or weekly programmer without Max Security	
	Disarming made by weekly programmer with Max Security	
	Disarming made by user with Max Security or by weekly programmer with/without Max Security	
	Disarming made by user with Max Security	
	Disarming made by weekly programmer without Max Security	
	Disarming made by weekly programmer with Max Security	
	Reset Max Security by weekly programmer	
	Reset Max Security by weekly programmer	
	Reset Max Security by weekly programmer	
	Reset Max Security by weekly programmer	
	Set Max Security by weekly programmer	
	Set Max Security by weekly programmer	
	Set Max Security by weekly programmer	

Special cases

- A max security arming can be performed while the sectors cannot be armed or are already armed; in such case the arming is denied but the max security property is set and the corresponding event is saved on to the system log.
- When a weekly programmer activates a max security arming but the sectors cannot be armed and feature the arming lock option, the sectors will not be armed but the weekly programmer max security property will be set anyway.
- When a max security arming command is sent via remote control to already armed sectors, such sectors will remain armed and will be assigned the User Max Security property.

9 REMOTE INTERROGATION AND REMOTE CONTROL

When control units are equipped with GSM module, SMS can be used:

- to receive information about system status;
- to send commands to the unit.

An SMS text will be sent to the unit and the unit will reply with another SMS text.

⚠ *The command sent will be accepted only if sent by a number on the unit phone number list.*

9.1 SMS structure

SMS text shall be in the following form:

C.nnnnnn X.X

where
nnnnnn = code of the user sending the SMS (6 digits)
X.X = code of the command (see table)

⚠ *Leave an empty space between C.nnnnnn and X.X.*

With a single SMS text it is possible to send up to 10 commands/reports, separated by an empty space.

C.nnnnnn X.X Y.Y Z.Z

Commands will always be performed before reports.
To each SMS received, the unit will reply with one or more SMS texts (max 16) containing information on the operating status requested or on the command performed.

⚠ *The control unit will reply only if the number sending the SMS is on the unit phone list.*

The following tables contain command codes to be used in X.X. section.
Codes from R.C to R.T are report codes; the others are command codes.

Report codes

Report codes	Indication
R.C	Control unit report
R.I	Zones report
R.M	Tamper and alarm memories report
R.A	Anomalies report
R.U	Outputs report
R.E	Excluded zones report
R.S	Sectors report
R.T	Temperature report

Example

User with code 123456 requires a control unit status report.
And will text the following code:

C.123456 R.C

with an empty space between C.123456 and R.C
The user will receive the following text (example):

PANEL FULLY ARMED, INTRUSION ALARM MEMORY

Command codes

Command codes	Action
I.ON	Arm areas / sectors authorised
I.P1	Arm sectors proposed
I.P2	Arm sectors authorised but not the proposed ones
I.OFF	Disarm areas / sectors authorised
G.ON	Activate GSM module
G.OFF	Deactivate GSM module after 7 minutes
M.ON	Remote listening request
A.#	Output activation (# = 2-digit output number)
D.#	Output deactivation (# = 2-digit output number)
E.#	Exclude zone (# = 2-digit zone number)
N.#	Include zone (# = 2-digit zone number)
S.#	Output manoeuvring (# = command key number)
C.ON	Activate balance reading
C.OFF	Suspend balance reading

Example

The user with code 123456 has the following sectors authorised: all area 1 sectors and sectors 2 and 4 of area 2. The user wants to arm all the sectors authorised.
And will text the following code:

C.123456 I.ON

leaving a space between C.123456 and I.ON
The user will receive the following text (example):

[name] ARMED, [name] S12--

9.2 Answers to report request messages

After a report request message, control units will reply with one of the following codes:

9.2.1 Control unit report

The first part of the message will be one of the following 4 messages:

- **PANEL DISARMED, ready to be armed**
  All sectors authorised for the user are disarmed but can be armed.
- **PANEL DISARMED, not ready to be armed**
  All sectors authorised for the user are disarmed and there are some conditions that prevent arming.
- **PANEL FULLY ARMED**
  All sectors authorised for the user are armed.
- **PANEL PARTIALLY ARMED**
  Some sectors authorised for the user are armed (but not all).

Such data will be followed by alarm/tamper, anomaly and GSM activation information and separated by commas:

- **TAMPER ALARM**
  Tamper alarm at one of the areas authorised for the user.
- **TAMPER ALARM MEMORY**
  Tamper alarm memory at one of the areas authorised for the user.
- **INTRUSION ALARM**
  Intrusion alarm at one of the areas authorised for the user.
- **INTRUSION ALARM MEMORY**
  Intrusion alarm memory at one of the areas authorised for the user.
- **PANEL ANOMALY**
  One of the areas authorised for the user signals an anomaly (or there is a memory for such event).
- **GSM ON**
  GSM module on.
- **GSM TURNING OFF**
  GSM module is turning off.

9.2.2 Zones report

The control unit replies with SMS texts containing the status of the zones that pertain to the user (one per zone).

Replying SMS

- **zone [name] ALARM**
  The zone signals an alarm event.
- **zone [name] TAMPER**
  The zone signals a tamper event.
- **no zones alarmed**
  No zones signal tamper or alarm events.

9.2.3 Memories report

The control unit replies with SMS texts containing alarm/tamper memories, one text per each zone pertaining to the user.

Replying SMS

- **System TAMPER MEM.**
  External tamper memory at (at least) one of the areas pertaining to the user
- **zone [name] ALARM MEM.**
  Alarm memory at the zone.
- **zone [name] TAMPER MEM.**
  Tamper memory at the zone.
- **no alarm/tamper mem.**
  No alarm / tamper memories.

9.2.4 Anomalies report

The control unit replies with SMS texts containing anomalies information, one text per each zone pertaining to the user.

Replying SMS

- **ANOMALY System test**
  System test anomaly at one of the areas (at least) pertaining to the user.
- **MEMORY Mains Failure**
  Mains failure memory at one of the areas (at least) pertaining to the user.
- **MEMORY Detector Fault zone [name]**
  Detector fault anomaly at the zone.
- **No anomalies**
  No anomalies

9.2.5 Outputs report

The control unit replies with SMS texts containing outputs status, one text per each zone pertaining to the user.

Replying SMS

- **Out. [name] ENABLED**
  The output is active.
- **no enabled outputs**
  There are no outputs activated.

9.2.6 Excluded zones report

The control unit replies with SMS texts containing excluded zones status, one text per each zone pertaining to the user.

Replying SMS

- **zone [name] BYPASSED**
  The zone is excluded.
- **no zones bypassed**
  There are no excluded zones.

9.2.7 Sectors report

The control unit replies with SMS texts containing areas arming status, one text per each zone pertaining to the user.

Replying SMS

- **[name] ARMED**
  All area sectors are armed.
- **[name] DISARMED**
  All area sectors are disarmed.
- **[name] S12--**
  Some sectors of the area are armed. Numbers indicate sectors armed, hyphens sectors disarmed.

9.2.8 Temperature report

The control unit replies with an SMS text containing the unit internal temperature measured by the sensor.

Replying SMS

- **+/- XX,X degrees**
  Temperature detected.

9.3 Replies to command messages

The control unit will reply with one SMS (or more) containing the response to the command sent.

9.3.1 Arm/disarm commands

The command affects all sectors authorised for the user.
The control unit will reply with one SMS per each area authorised for the user:

Replying SMS

- **[name] ARMED**
  All area sectors are armed.
- **[name] DISARMED**
  All area sectors are disarmed.
- **[name] S12--**
  Some sectors of the area are armed. Numbers indicate sectors armed, hyphens sectors disarmed.
- **ARMING DENIED**
  Arming impossible
- **DISARMING DENIED**
  Disarming impossible

9.3.2 GSM ON/OFF

Replying SMS

- **GSM ON**
  GSM module on.
- **GSM TURNING OFF**
  GSM module is turning off.
- **G.DENIED**
  GSM on/off functions disabled or the user is not authorised for Small Maintenance

9.3.3 Remote listening request

Replying SMS

- **REMOTE LISTENING REQ.**
  Command M.ON recognised.

9.3.4 Activate/deactivate outputs

The control unit will reply with one SMS per output.

Replying SMS

- **out. [name] ENABLED**
  The output is active.
- **out. [name] DISABLED**
  The output is not active.
- **A.DENIED**
  Output activation is not allowed or the user is not authorised for Small Maintenance.

▼ **D.DENIED**
Output deactivation is not allowed or the user is not authorised for Small Maintenance.

9.3.5 Bypass/include zone

The control unit will reply with one SMS per zone.

Replying SMS

▼ **zone [name] BYPASSED**
The zone is excluded.

▼ **zone [name] ACTIVE**
The zone is active.

▼ **E.DENIED**
Zone exclusion is not allowed or the user is not authorised for Small Maintenance.

▼ **N.DENIED**
Zone inclusion is not allowed or the user is not authorised for Small Maintenance.

9.3.6 Output commands

Replying SMS

▼ **COMMAND S# EXECUTED**
The command has been executed.

SX stands for sector keys (S1 to S4). Each sector key manages one output, according to software configuration.

9.3.7 Disable balance reading

Replying SMS

▼ **SIM BALANCE READING DISABLED**
Reading disabled.

▼ **SIM BALANCE READING ENABLED**
Reading enabled.

▼ **C.DENIED**
Reading disabled or the user is not authorised for Small Maintenance.

10 SYSTEM TEST

Users shall test the system regularly in order to verify its correct working and refer to the installer in case of abnormal functioning.
For such purpose, the control unit will ask users to perform a system testat regular intervals.
Test interval is set during installation (default 4 weeks). The control unit yellow LED ON indicates the necessity of performing a system test, and the following message will be displayed among anomalies:

EXECUTE
SYSTEM TEST

⚠ *Such request does not affect system functioning. System test request will be logged and if the test is not performed will be repeated once a month.*

Items tested:
- **zones** (with Walk Test property): check of the correct functioning of detectors connected to zones, control of idle and alarm conditions
- **outputs**: temporary activation of programmable relay (when activated for general or tamper alarm), external siren, sirens on serial line or radio sirens
- **dialler** (if installed): generation of the periodic call event and dialler activation

⚠ *The DIALLER TEST requires the installation of a phone module, the presence of PSTN or GSM line and the association of at least one number to the event "Test call".*

- **battery**: check of battery status

To start system test, go to user menu and follow the procedure illustrated at 2.5.12 *p. 11*.

11 DIAGNOSTICS

In case of anomalies, the yellow LED indicator on keypads or readers will keep blinking.
Go to **ANOMALIES STATUS** menu to see current anomalies (for details, see paragraph 2.3.2 *p. 4*).
Below messages that may be displayed.

ANOMALY	CAUSE
ANOMALY Low Battery	Battery is low or absent. It may be necessary to replace battery protection fuse.
ANOMALY Mains Failure	Mains failure: the unit is powered by the battery only.
ANOMALY Tel. Line Fault	Phone line not detected or absent.
ANOMALY No GSM Registr.	SIM card missing or disabled, or PIN code active.
KEYP/RD TAMPER Keyp./Reader #	Keypad or reader (the number of which is indicated) signals a tamper event.
ANOMALY SIM Card Balance	SIM balance below 5€, or the operator has not provided the information.
ANOMALY REGISTERMODULES	One module (or more) installed have not been registered correctly.
ANOMALY Sensor low volt.	One sensor (or more) is not powered correctly. Power voltage is below set threshold.
ANOMALY Sound. low volt.	One siren (or more) is not powered correctly. Power voltage is below set threshold.
ANOMALY R.C. Low Battery	One remote control (or more) signals low battery.

12 ENERGY SAVING

Installers can activate functions for energy saving:

- **Yellow LED OFF when there are no anomalies**
  The yellow LED will be off (at keypads and readers connected) when there are no anomalies.
- **Sector keys OFF when inactive**
  Sector keys back light will be off in case of inactive system
- **Reader arming LED OFF when inactive**
  The reader LED indicating arming status will be OFF in case of inactivity.

GSM automatic switch off

Installers can also configure GSM module so that it turns off automatically after the inactive time intervalset.

Emergency light

Keypad display can be set to remain active for a defined time interval in case of mains failure (**Emergency Light Time**). When the interval expires, the display will blink for 30 secs to indicate imminent deactivation.

13 PARTS CLEANING

Clean the unit and the keypads with a damp cloth, using suitable non-corrosive cleansers.
Do not spray any liquid substance directly on the case.

Table of contents

1 GENERALS ..... P. 1

2 KEYPADS USAGE ..... P. 1
2.1 Keypad parts ..... p. 2
2.1.1 Sector buttons ..... p. 2
2.1.2 Number and control keys ..... p. 2
2.1.3 LED indicators ..... p. 2
2.2 Displayed information ..... p. 3
2.2.1 Change of current operating area ..... p. 3
2.2.2 User menu ..... p. 4
2.2.3 User code and keypad locked ..... p. 4
2.3 Display the status ..... p. 4
2.3.1 Check zones status ..... p. 4
2.3.2 Check anomalies status ..... p. 4
2.3.3 Tamper and alarm memories ..... p. 5
2.3.4 SIM Balance status ..... p. 5
2.3.5 Check Internet connection state ..... p. 5
2.4 Operating mode from keypad ..... p. 5
2.4.1 General information on system arming ..... p. 5
2.4.2 Simple arming ..... p. 5
2.4.3 System arming with sectors selection - 4 areas / 4 sectors mode ..... p. 5
2.4.4 System arming with sectors selection - 8/16 sectors per area mode ..... p. 6
2.4.5 Fast arming - 4 areas / 4 sectors mode ..... p. 7
2.4.6 Fast arming - 8/16 sectors per area mode ..... p. 7
2.4.7 Disarming ..... p. 7
2.4.8 Disarming with duress mode ..... p. 7
2.4.9 Panic alarm from keypad ..... p. 8
2.4.10 Arming advanced functions ..... p. 8
2.5 Enter USER MENU on keypad ..... p. 8
2.5.1 Zones bypass ..... p. 9
2.5.2 Limits to installer access ..... p. 9
2.5.3 Manual control of outputs ..... p. 10
2.5.4 SIM balance check ..... p. 10
2.5.5 Date and time setup ..... p. 10
2.5.6 Clock calibration ..... p. 10
2.5.7 Schedules change ..... p. 10
2.5.8 Users authorisations management ..... p. 10
2.5.9 Change phone numbers ..... p. 10
2.5.10 Set the Wi-Fi connection ..... p. 10
2.5.11 Change user code ..... p. 11
2.5.12 System test ..... p. 11
2.5.13 Chime management ..... p. 12
2.5.14 Events log ..... p. 12

3 PROXIMITY KEYS USAGE ..... P. 12
3.1 Readers type ..... p. 12
3.2 Proximity keys usage ..... p. 13
3.2.1 System arming ..... p. 13
3.2.2 Disarming ..... p. 13
3.2.3 Disarming with duress mode ..... p. 13
3.2.4 System forced arming ..... p. 13

4 REMOTE CONTROLS USAGE ..... P. 14
4.1 Function keys ..... p. 14
4.2 Operation with remote controls ..... p. 14
4.2.1 System arming ..... p. 14
4.2.2 Disarming ..... p. 14
4.2.3 Disarming with duress mode ..... p. 14
4.2.4 Panic event ..... p. 14
4.2.5 System forced arming ..... p. 15

5 GSM AND PHONE COMMUNICATIONS ..... P. 15
5.1 Calls reception ..... p. 15
5.1.1 Remote listening ..... p. 15
5.2 Receiving SMS from control units ..... p. 15
5.3 SIM balance check ..... p. 15
5.4 Sending SMS to control units ..... p. 15
5.5 Change number list from keypad ..... p. 15
5.6 Advanced settings ..... p. 15
5.6.1 Dialler block at disarming ..... p. 15
5.6.2 Limits to dialler activations ..... p. 16
5.6.3 Disable arm/disarm commands ..... p. 16

6 TEMPERATURE MONITORING ..... P. 16
6.1 Temperature thresholds ..... p. 16
6.2 A-B temperatures management ..... p. 16

7 E-CONNECT ..... P. 16

8 MAX SECURITY ..... P. 17
8.1 Arming with Max Security ..... p. 17
8.2 Notes on Max Security ..... p. 17

9 REMOTE INTERROGATION AND REMOTE CONTROL ..... P. 18
9.1 SMS structure ..... p. 18
9.2 Answers to report request messages ..... p. 19
9.2.1 Control unit report ..... p. 19
9.2.2 Zones report ..... p. 19
9.2.3 Memories report ..... p. 19
9.2.4 Anomalies report ..... p. 20
9.2.5 Outputs report ..... p. 20
9.2.6 Excluded zones report ..... p. 20
9.2.7 Sectors report ..... p. 20
9.2.8 Temperature report ..... p. 20
9.3 Replies to command messages ..... p. 20
9.3.1 Arm/disarm commands ..... p. 20
9.3.2 GSM ON/OFF ..... p. 20
9.3.3 Remote listening request ..... p. 20
9.3.4 Activate/deactivate outputs ..... p. 20
9.3.5 Bypass/include zone ..... p. 21
9.3.6 Output commands ..... p. 21
9.3.7 Disable balance reading ..... p. 21

10 SYSTEM TEST ..... P. 21

11 DIAGNOSTICS ..... P. 21

12 ENERGY SAVING ..... P. 21

13 PARTS CLEANING ..... P. 22

EU DECLARATION OF CONFORMITY ..... P. 24

GENERAL WARNINGS ..... P. 24

INSTALLER WARNINGS ..... P. 24

USER WARNINGS ..... P. 24

MAIN SAFETY RULES ..... P. 24

DISPOSAL WARNINGS ..... P. 24

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.

CE

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 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 performedonly 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 performedonly 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).

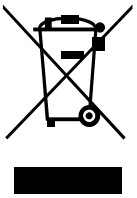
USER WARNINGS

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.

EL.MO. Spa - Via Pontarola, 70 - 35011 Campodarsego (PD) - Italy
Ph. +39 049.9203333 - Fax +39 049.9200306 - Help Desk +39 049.9200426 - www.elmospa.com - international@elmospa.com