

# SUPERIA SERIES

**Multi-functional hybrid control units  
for intrusion detection systems**



## 1 GENERALS

The SUPERIA / EXCELSA series 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;
- the first-generation wireless technology using RIVERRF concentrators and the NG-TRX wireless technology with connection of GATEWAY2K over serial line.

Optional modules can be installed to improve unit operating mode.

The control units can be connected to e-Connect.

The SUPERIA / EXCELSA control units are supplied in a metal housing protected against cover opening and removal from the wall.

### Icons used in this manual

#### ▼ Example of messages on keypad display

Ve01/09/17 09:00  
Area 1

#### ▼ Keys typing



#### ▼ Usage example



### Manual contents

#### ▼ Keypads usage

operating mode from keypad → cap. 2 p. 2

#### ▼ Proximity keys usage

operating mode from keypad → cap. 3 p. 13

#### ▼ Remote controls usage

operating mode with remote control → cap. 4 p. 15

#### ▼ GSM and phone communications

phone calls and SMS reception → cap. 5 p. 16

#### ▼ Temperature monitoring

use of built-in temperature detector → cap. 6 p. 16

#### ▼ e-Connect usage

Information on e-Connect service → cap. 7 p. 17

#### ▼ Maximum security

maximum security property, arming with maximum security → cap. 8 p. 17

#### ▼ System test

system test to check system working → cap. 9 p. 19

#### ▼ Anomalies diagnostics

anomalies check → cap. 10 p. 19

## 2 KEYPADS USAGE

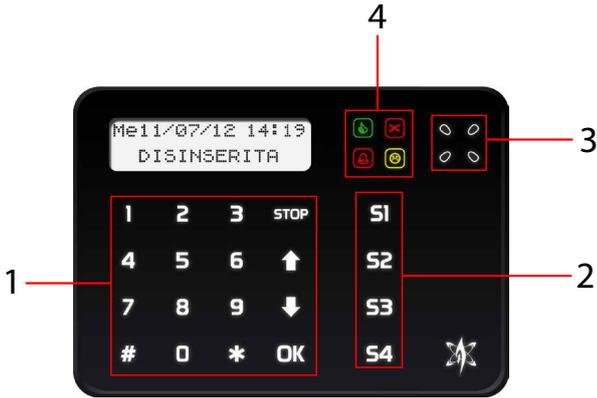
The SUPERIA control units are multi-area devices capable of managing up to 64 sectors.

During unit setup, sectors can be divided into:

- **16 areas** including **4 sectors** each;
- **8 areas** including **8 sectors** each;
- **4 areas** including **16 sectors** each;
- **2 areas** including **32 sectors** each;
- **1 area** including all **64 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

### Note: use with touch screen keypads

Some advanced keypads (i.e. the touch-screen ones, like KARMA) do not feature some of the items that will be introduced further on (sector keys, number keys and control keys).

Such keypads feature:

- dedicated menu items for arming the system and consulting system status and anomalies;
- a standard keypad interface to access user and installer menu.

See the related technical manual.

## 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.

### 16 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

### 8/16/32/64 sectors per area mode

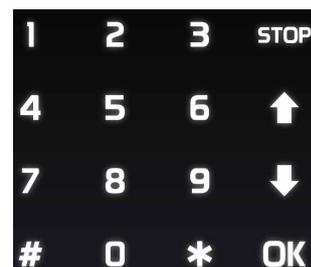
During unit configuration, sector keys are associated to **sector groups**. Each sector key provides information about arming status of corresponding sectors.

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.)

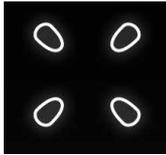
### 2.1.2 Number and control keys



Keypads feature number keys and also the following keys:

OK	To enter a menu/submenu or confirm an operation.
----	--

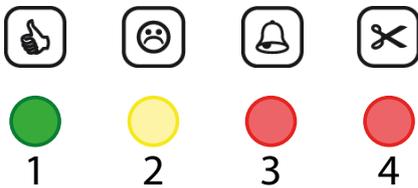
<b>STOP</b>	To exit a menu/submenu.
↑ ↓	To browse among menu pages and options



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. 5.

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

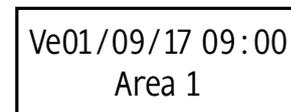


**top row**: date and time

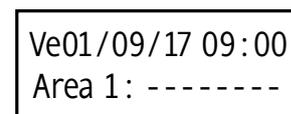
**bottom row**: welcome message (if set)

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

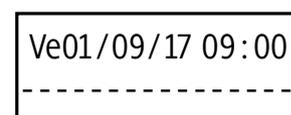
#### Display with 16 areas / 4 sectors mode



#### Display with 8 areas / 8 sectors mode



#### Display with other modes



## 2.2.1 Change of current operating area

To change the current operating area:

Ve01/09/17 09:00  
Welcome



A1 A2 A3 A4  
Area 1



Ve01/09/17 09:00  
Area 3

- 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
- AUTHORIZATION
- OUTPUT CONTROL
- DAY TYPE
- OVERTIME REQUEST
- CLOCK SETUP
- WEEKLY PROGR.
- MANAGE USERS
- PHONE NUMBERS
- CHANGE CODE
- SYSTEM TEST
- MANAGE CHIME
- EMER. DOOR TEST
- EVENT LOG

For more information: paragraph 2.5 p. 9.

## 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:

DISABILITAZIONE  
TEMPORANEA

*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:

Fri01/09/17 9:00  
Welcome



ZONES STATUS  
(Up Down Ok Stop)

- 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:

Nessun allarme  
(Stop)

### 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 10 p. 19.

### 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 Check Internet connection state

Function available from firmware version 1.1.2.

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.)

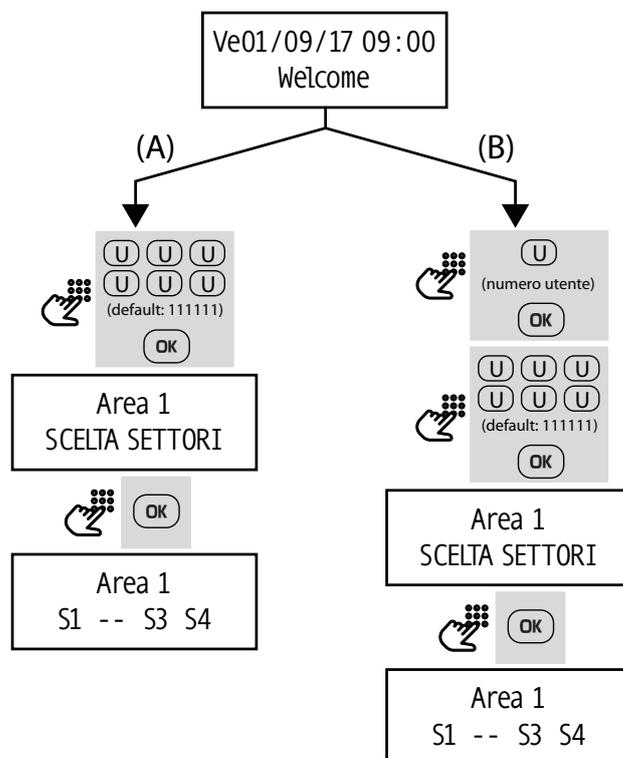
During unit configuration, some zones can be included into **exit path**. After system arming, users can leave the premises within a set time (**exit time**) through the exit path without triggering an alarm event.

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.



- A** "simplified codes" mode
- B** user number + user code mode

- If "simplified codes" mode is disabled, enter user number and then press **OK**.
- Key in user code.
- Press **OK**.

Keys of sectors proposed for arming for a specific user will blink in the currently operating area.

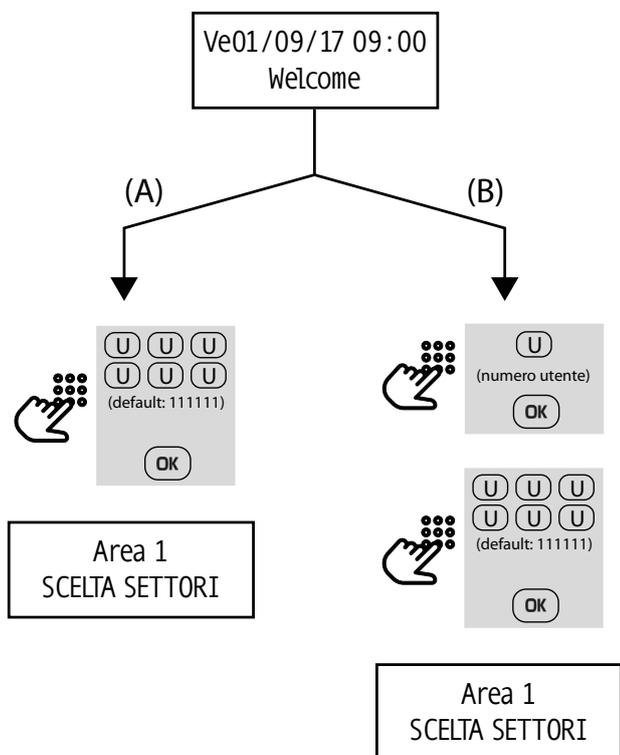
- Press **OK** to start arming, **STOP** to cancel it.
- If exit time has been set, it will be marked by beep sounds: leave the protected areas within the set time walking through the path set.

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 sectors per area 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 16 areas / 4 sectors mode, each sector key is associated to a sector distinctively.



- A** "simplified codes" mode
- B** user number + user code mode

- If "simplified codes" mode is disabled, enter user number and then press **OK**.
- 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 - 8/16/32/64 sectors per area mode

Under 8/16/32/64 sectors per area mode, sector keys are associated to **sectors group**.

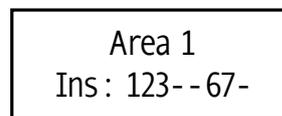
Sector keys arm/disarm sector groups. The key-sectors association is made during setup.

- Key in user code.
- Press **OK**.

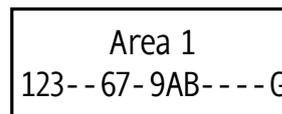
Keys of sectors proposed for arming for a specific user will blink in the currently operating area.

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

Area 1  
Ins : 123--67-

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

Area 1  
Ins : 123--678

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  
Ins : 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  
Ins : 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 sectors per area 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.

Settore S1. A1  
INSERIM. VELOCE?

- 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.

Settore S1. A1  
INSERIM. VELOCE?

- 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.

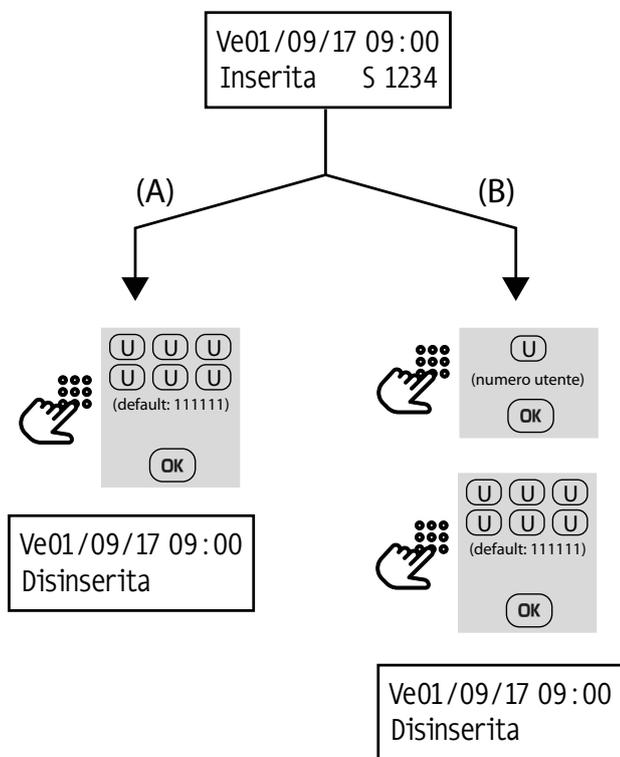
**2.4.6 Fast arming - 8/16/32/64 sectors per area mode**

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 2.4.6 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:



- A** "simplified codes" mode
- B** user number + user code mode

- If "simplified codes" mode is disabled, enter user number and then press **OK**.
- Key in user code.
- Press **OK**.

System disarming will be marked by beeping sounds. Only sectors authorised for the specific user will be disarmed. If "Euro mode" has been activated, it is possible to disarm single sectors (see paragraph 2.4.7.1 p. 8).

#### 2.4.7.1 "Euro" mode

If "Euro mode" has been activated in BrowserOne for an user, this user can use the keypad to select each single sector to disarm, with no need to disarm all allowed sectors at the same time.

**!** *Function available from control unit firmware version 1.0.5.*

When system is armed:

- If "simplified codes" mode is disabled, enter user number and then press **OK**.
- Key in user code.
- Press **OK**.

Pre-disarming mode starts.

- Press the sector keys corresponding to the sectors to disarm.

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

- When finished, press OK to start arming, STOP to cancel

it.

The pressed sector keys will switch off and the related sectors will be disarmed.

If during pre-disarming a sector key corresponding to a disarmed sector is pressed, this sector will be armed when the time expires.

**Note:** under 8/16/32/64 Sectors per area mode, each sector key is associated to a sectors group and not to a single sector (see paragraph 2.4.4 p. 6).

#### 2.4.8 Disarming with duress mode.

A duress event occurs when a user is forced to disarm the system at keypad.

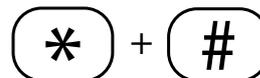
In such case:

- 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:

GUASTO  
INS. FORZATO?

- 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 by time scheduler.

Forced arming will not be allowed in case of zones with anomaly events.

### 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:

C. INSTALLATORE :  
-----

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

NECESSARIA  
AUT. INSTALLATORE

### 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.

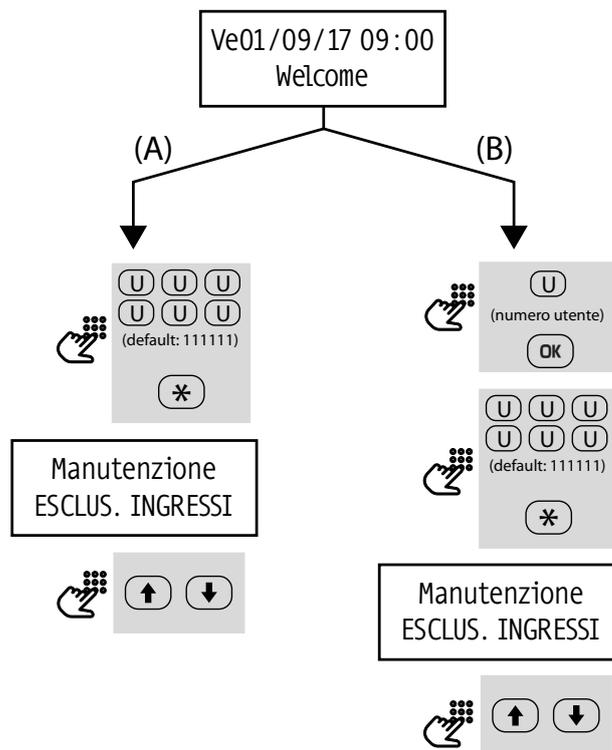
## 2.5 Enter USER MENU on keypad

SUPERIA 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:



**A** "simplified codes" mode

**B** user number + user code mode

- If "simplified codes" mode is disabled, enter user number and then press **OK**.
- 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.

SALVARE MODIF. ?  
(Ok=Si #=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. 10
- **AUTHORIZATION** - § 2.5.2 p. 10
- **OUTPUT CONTROL** - § 2.5.3 p. 10
- **DAY TYPE** - § 2.5.4 p. 11

- **OVERTIME REQUEST** - § 2.5.5 p. 11
- **CLOCK SETUP** - § 2.5.6 p. 11
- **WEEKLY PROGR.** - § 2.5.7 p. 11
- **MANAGE USERS** - § 2.5.8 p. 11
- **PHONE NUMBERS** - § 2.5.10 p. 12
- **CHANGE CODE** - § 2.5.9 p. 11
- **SYSTEM TEST** - § 2.5.11 p. 12
- **MANAGE CHIME** - § 2.5.12 p. 12
- **EMER. DOOR TEST** - § 2.5.13 p. 12
- **EVENT LOG** - § 2.5.14 p. 13

### 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.

Ing. 001 ESCLUSO  
 Ingresso 001

To include the zone again, repeat the steps.

Ing. 001 ATTIVO  
 Ingresso 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 Installer authorisations management

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 manage the authorisations using this menu:

- Use arrow keys ↑ or ↓ to go to **AUTHORIZATION** option.
- Press **OK** to enter the menu.
- Use arrow keys ↑ or ↓ to go to the authorisation you are interested in.

#### Installer Access

- Press **OK** repeatedly to change the authorisation to access the control unit:

##### ▼ TEMPORARY

Until the end of the connection session.

##### ▼ NONE

Access denied.

##### ▼ PERMANENT

Access granted.

#### Image Installer

- Press **OK** repeatedly to change the authorisation to access the user's 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.

#### Panel Update

- Press **OK** repeatedly to change the authorisation to remotely update control unit firmware:

##### ▼ USER

Each remote firmware update must be confirmed by the user.

Once the update has been launched via BrowserOne, the following message will appear on keypad display:

AGGIOR. CENTRALE  
 DISPONIBILE

To complete the update, the user has to perform the following operations:

- Press **Stop** to delete the message.
- Key in user code (default: 111111).
- Press \* key.
- Press **Ok**.

The following message will be proposed again at each access to the user menu, until the update is carried out.

AGGIOR. CENTRALE  
 Ok=Si #=No

In case # key is pressed, the update will not be carried out and it will remain pending.

##### ▼ AUTOMATIC

Each remote firmware update will be completed automatically, no authorisation will required to the user.

 *Setting the update to "AUTOMATIC" will cause the loss of the IMQ - Security Systems certification.*

- 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 Change day type

It allows to temporarily change the day type (workday, holiday etc.)

This change will only be effective on current week: next week the configuration values set in BrowserOne will be restored.

- Press **OK** to enter the menu.
- Use arrow keys ↑ or ↓ to go to the required day.
- Press \* or # to change day type.
- Press **Stop** to save and exit the menu.

#### 2.5.5 Overtime requests

The user can require "overtime" for current programs, in case he needs to temporarily change the scheduled activation / deactivation hour of a program.

For example, suppose a program has been set in an office in order to automatically arm the system at 5 pm (standard end of working time). In case one employee needs to leave the office later (e.g. at 6 pm), he/she can request "overtime" for this program: the system will be armed at 6 pm instead of at 5 pm.

The request can be repeated several times up to the maximum value set via BrowserOne.

- Press **OK** to enter the menu.
- Use arrow keys ↑ or ↓ to go to the required program.
- Press \* to enable overtime and set its time.

The overtime duration is defined according to pre-defined time steps (which can be set via BrowserOne) and it depends on how many times the \* button is pressed: each single pressure extends the duration of a quantity equal to the set time step.

For example, if the time step is set to 30 minutes, by pressing \* 3 times the overtime duration will be set to 1h 30'.

- Press # to cancel the ongoing overtime request.
- Press **OK** to save.
- Press **STOP** to exit the menu.

#### 2.5.6 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.

#### 2.5.7 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 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.

### 2.5.10 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.

### 2.5.11 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.*

### 2.5.12 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.

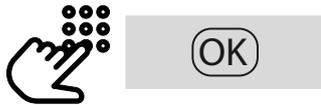
- Use arrow keys ↑ or ↓ to go to **MANAGE CHIME** option.
- Press **OK** to enter the menu.
- Press **OK** repeatedly to select **ENABLED** or **SUSPENDED**.
- Press **STOP** to save and exit the menu.

### 2.5.13 Testing "emergency exit" zones

A user can test the zones defined as "Emergency exits".

 *Function available from control unit firmware version 1.0.8.*

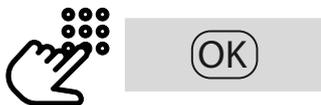
MAINTENANCE  
EMER. DOOR TEST



EMER. DOOR TEST  
(OK = Execute)

- Use arrow keys ↑ or ↓ to go to **EMER. DOOR TEST** option.
- Press **OK** to enter the menu.

EMER. DOOR TEST  
(OK = Execute)



Zones to test  
Warehouse door

- If at least one zone can be tested, press OK to enter test mode.

**!** *If no zones can be tested or if the test cannot be started manually for any zone, "Not executable" appears.*

- Make each "Emergency exit" zone to test enter alarm state and then idle state again.
- Once all the "Emergency exit" zones have been tested, the following message appears:

EMER. DOOR TEST  
Test OK

## Stopping the test

Zones to test  
Warehouse door



Test started  
(# = Stop)

- Press Stop during the test.
- Press # to stop the test, Stop to cancel the stopping attempt.

An interrupted test is considered failed for the sectors not yet tested.

### 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

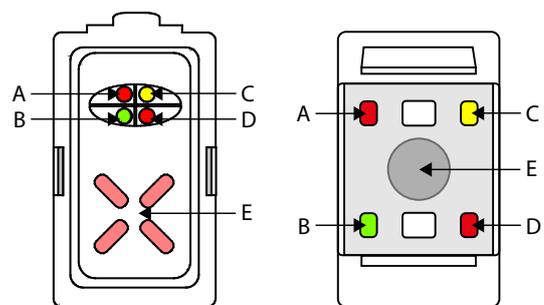
Proximity keys can be used to quickly arm and disarm the system.

Simply draw them close to system readers (I8, I66, IZENITH).

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

### 3.1 Readers type

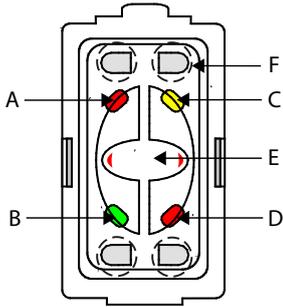
**I8 - I66 - I9 - I10**



- 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 proximity key

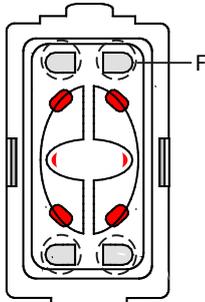
For LEDs indications, please see paragraph 2.1.3 p. 3.

## IZENITH



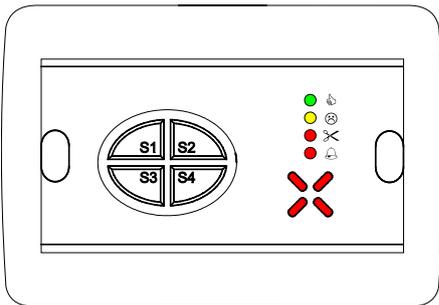
- A** Tamper/general alarm LED (shared indication)
- B** Unit arming status LED (zones status)
- C** System anomaly LED
- D** System arming status LED
- E** Area for proximity key
- F** Sectors selection keys

For LEDs indications, please see paragraph 2.1.3 p. 3.  
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. 3.  
ETRZENITH can be set for one area only.

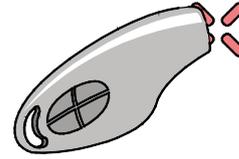
### 3.2 Proximity keys usage

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.

At the end, the unit status LED (on proximity key reader) or the sector keys (on keypad) will turn on.

#### 3.2.2 Disarming

When system is armed:

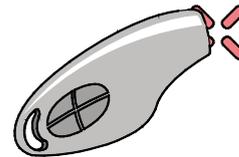
- Place the proximity key near the sensitive area (onto reader or keypad).
- Wait a few seconds until the unit status LED (on readers) or sector keys (on keypad) switches OFF.

#### 3.2.3 Disarming with duress mode.

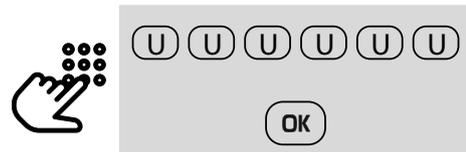
Users may be forced to disarm the system with a proximity key (duress event).

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

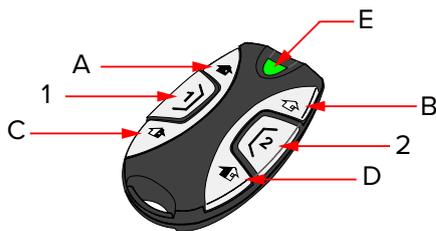
Remote control devices can be used to arm (either totally or partially) and disarm systems.

Remote controls have to be learned to a specific device.

Remote control	Device
ATLANTE4, ATLANTE6	RIVERRF
ATLANTE4PLUS	RIVERRPLUS
ATLANTE2K, ELISEO2K	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

The SUPERIA control units support the following modules:

- **MD4GE**: allows connecting the control unit to the LTE network.

### 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.

### 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 Advanced settings

The installer can set advanced settings using BrowserOne software.

### 5.3.1 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.

### 5.3.2 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

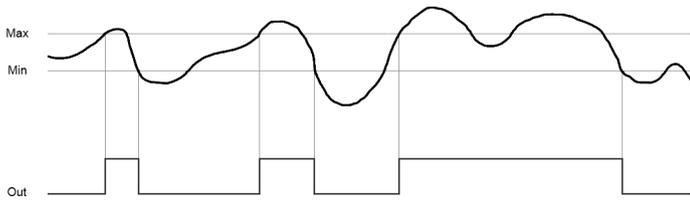
SUPERIA series units are equipped with a temperature detector measuring the temperature inside the housing.

 *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.

### Example



If S3 key has been associated to the function, the output can be reset entering user code + S3 key.

## 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



The software requires the use of the LAN integrated module or of the MD4GE optional module.

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](http://www.elmospa.com) site (also for download).

## 8 MAX SECURITY

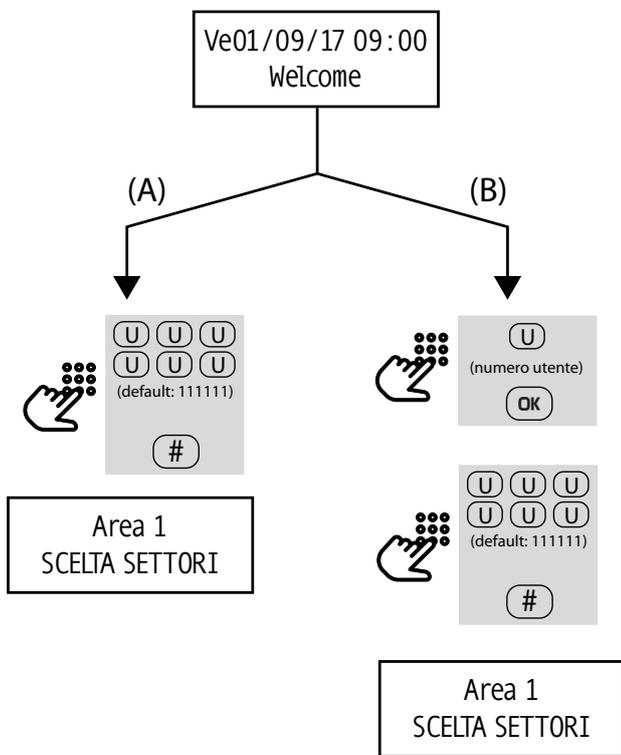
Sectors can be armed with **Max Security** property.

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:



- A** "simplified codes" mode
- B** user number + user code mode

- if "simplified codes" mode is disabled, enter user number and then press **OK**
- 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 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 test at 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:

ESEGUIRE  
TEST IMPIANTO

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 the 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 2.5.11 p. 12.

## 10 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. 5).

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 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.
EXECUTE SYSTEM TEST	It is necessary to perform a system test.

## 11 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 interval set.

### **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.

## **12 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

<b>1</b>	<b>GENERALS</b> .....	<b>P. 1</b>	5.1	Calls reception .....	p. 16
<b>2</b>	<b>KEYPADS USAGE</b> .....	<b>P. 2</b>	5.2	Receiving SMS from control units .....	p. 16
2.1	Keypad parts .....	p. 2	5.3	Advanced settings .....	p. 16
2.1.1	Sector buttons .....	p. 2	5.3.1	Dialler block at disarming .....	p. 16
2.1.2	Number and control keys .....	p. 2	5.3.2	Disable arm/disarm commands .....	p. 16
2.1.3	LED indicators .....	p. 3	<b>6</b>	<b>TEMPERATURE MONITORING</b> .....	<b>P. 16</b>
2.2	Displayed information .....	p. 3	6.1	Temperature thresholds .....	p. 16
2.2.1	Change of current operating area .....	p. 4	6.2	A-B temperatures management .....	p. 17
2.2.2	User menu .....	p. 4	<b>7</b>	<b>E-CONNECT</b> .....	<b>P. 17</b>
2.2.3	User code and keypad locked .....	p. 4	<b>8</b>	<b>MAX SECURITY</b> .....	<b>P. 17</b>
2.3	Display the status .....	p. 4	8.1	Arming with Max Security .....	p. 17
2.3.1	Check zones status .....	p. 4	8.2	Notes on Max Security .....	p. 18
2.3.2	Check anomalies status .....	p. 5	<b>9</b>	<b>SYSTEM TEST</b> .....	<b>P. 19</b>
2.3.3	Tamper and alarm memories .....	p. 5	<b>10</b>	<b>DIAGNOSTICS</b> .....	<b>P. 19</b>
2.3.4	Check Internet connection state .....	p. 5	<b>11</b>	<b>ENERGY SAVING</b> .....	<b>P. 19</b>
2.4	Operating mode from keypad .....	p. 5	<b>12</b>	<b>PARTS CLEANING</b> .....	<b>P. 20</b>
2.4.1	General information on system arming .....	p. 5	<b>13</b>	<b>NOTES</b> .....	<b>P. 21</b>
2.4.2	Simple arming .....	p. 5	<b>14</b>	<b>NOTES</b> .....	<b>P. 22</b>
2.4.3	System arming with sectors selection - 4 sectors per area mode .....	p. 5	<b>15</b>	<b>EU DECLARATION OF CONFORMITY</b> .....	<b>P. 24</b>
2.4.4	System arming with sectors selection - 8/16/32/64 sectors per area mode .....	p. 6	<b>16</b>	<b>GENERAL WARNINGS</b> .....	<b>P. 24</b>
2.4.5	Fast arming - 4 sectors per area mode .....	p. 7	<b>17</b>	<b>INSTALLER WARNINGS</b> .....	<b>P. 24</b>
2.4.6	Fast arming - 8/16/32/64 sectors per area mode .....	p. 7	<b>18</b>	<b>USER WARNINGS</b> .....	<b>P. 24</b>
2.4.7	Disarming .....	p. 7	<b>19</b>	<b>MAIN SAFETY RULES</b> .....	<b>P. 24</b>
2.4.7.1	"Euro" mode .....	p. 8	<b>20</b>	<b>DISPOSAL WARNINGS</b> .....	<b>P. 24</b>
2.4.8	Disarming with duress mode .....	p. 8			
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. 9			
2.5.1	Zones bypass .....	p. 10			
2.5.2	Installer authorisations management .....	p. 10			
2.5.3	Manual control of outputs .....	p. 10			
2.5.4	Change day type .....	p. 11			
2.5.5	Overtime requests .....	p. 11			
2.5.6	Date and time setup .....	p. 11			
2.5.7	Schedules change .....	p. 11			
2.5.8	Users authorisations management .....	p. 11			
2.5.9	Change user code .....	p. 11			
2.5.10	Change phone numbers .....	p. 12			
2.5.11	System test .....	p. 12			
2.5.12	Chime management .....	p. 12			
2.5.13	Testing "emergency exit" zones .....	p. 12			
2.5.14	Events log .....	p. 13			
<b>3</b>	<b>PROXIMITY KEYS USAGE</b> .....	<b>P. 13</b>			
3.1	Readers type .....	p. 13			
3.2	Proximity keys usage .....	p. 14			
3.2.1	System arming .....	p. 14			
3.2.2	Disarming .....	p. 14			
3.2.3	Disarming with duress mode .....	p. 14			
3.2.4	System forced arming .....	p. 15			
<b>4</b>	<b>REMOTE CONTROLS USAGE</b> .....	<b>P. 15</b>			
4.1	Function keys .....	p. 15			
4.2	Operation with remote controls .....	p. 15			
4.2.1	System arming .....	p. 15			
4.2.2	Disarming .....	p. 15			
4.2.3	Disarming with duress mode .....	p. 15			
4.2.4	Panic event .....	p. 16			
4.2.5	System forced arming .....	p. 16			
<b>5</b>	<b>GSM AND PHONE COMMUNICATIONS</b> .....	<b>P. 16</b>			

## 15 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](http://www.elmospa.com) – registration is quick and easy.



## 16 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 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).

## 17 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).

## 18 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...)

## 19 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.



Refer to the instruction manual.

## 20 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.