Mod. 1068

DS1068-045A LBT21166

REMOTE MANAGED ALARM CONTROL PANELS

Ref. 1068/005A
Ref. 1068/010A

Ref. 1068/005A

Through the following QR Code, it is possible to download the eventual new version of the manual.

http://qrcode.urmet.com/default.aspx?prodUrmet=164750&lingua=en

Ref. 1068/010A

http://qrcode.urmet.com/default.aspx?prodUrmet=165029&lingua=en

USER MANUAL

TABLE OF CONTENTS (Control panel FW Rel.: 1.050/ KP FW Rel: 1.050)

INTRODUCTION

This manual is addressed to the Users of the Intrusion Alarm System 1068A produced by Urmet S.p.A.

The document provides the Customer with a general description of the alarm system, its main features and also contains detailed instructions for proper use.

CONVENTIONS

In this manual, some conventions have been used to distinguish between different types of information:

This is the equivalent key to be pressed on the keypad.

<Master code>
<User code>
<Installer code>
<Technical Manager code>

This indicates the code to be entered using the keypad.

<Master / User code> This means that either code may be entered on the keypad indifferently.

The manual also contains symbols that provide the following information:

Warning! Warning messages highlight potential system damage, data loss or non-compliance with applicable regulations.

Notes: notes contain important information, which may be useful for better use of the system.

This symbol indicates compliance with EN50131 grade 1.

This symbol indicates compliance with EN50131 grade 2.

This symbol indicates that the function or device does not comply with the EN50131 standard.

Refer to the device's installation manual.

1 CONTROL DEVICES

This chapter contains a description of the devices which allow to interact with the alarm system, to set or unset it and to program it.

1.1 1068/005A – 1068/010A CONTROL PANEL

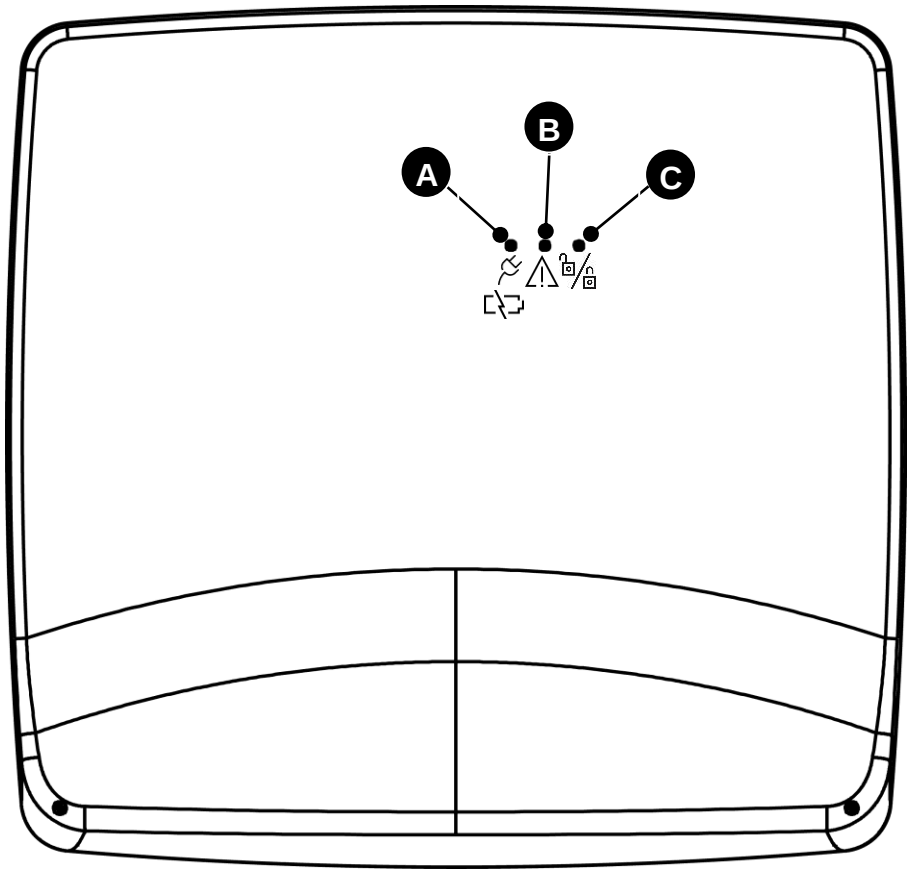


Figure 1 - 1068/005A – 1068/010A Control panel

Ref.	Description	Viewing	Supplied indications
A	Power supply	Green LED	**Steady on** = mains power present. **Slow blinking** = no mains power.
B	Notices	Yellow LED	**Steady on** = in case of Alarms or Tampering. **Fast blinking** = in case of Faults. **Slow blinking** = Open or inhibited/isolated inputs.
C	Zone status	Green LED	**Steady On** = all system Zones defined as used are active. **Slow blinking** = Some zones defined as used are active, while the rest are inactive. **Off**= all Zones defined as used are inactive.

1.2 1068/021 LCD COMMAND KEYPAD

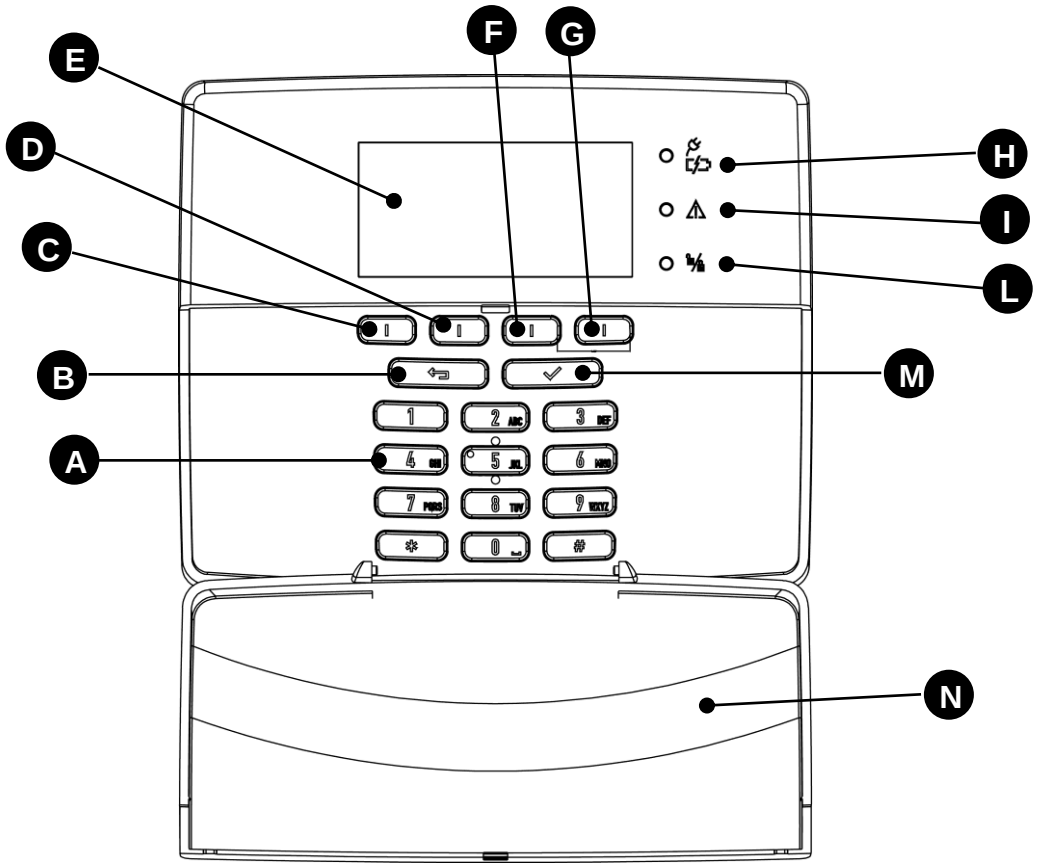


Figure 2 - 1068/021 keypad

Ref.	Description	Use or indications provided
A	Alphanumeric keys	Access code entry and system programming.
B	(**ESC**) ⮌ key	To go back to the upper menu level.
C	Function key	**Home page:** zone activation. **In Programming:** navigation of menu items.
D	Function key	**Home page:** zone deactivation. **In programming:** menu item selection/deselection.
E	Graphic Display 128x64 pixel	**Home page:** display of date and time or detailed information on system status. **In programming:** display of menus and system parameters and information.
F	Function key	**Home page:** Activation of the anti thief and emergency signalling or activation / deactivation of the outputs that can be controlled. **In programming:** menu item selection/deselection.
G	Function key	**Home page:** access to the programming menu. **In Programming:** navigation of menu items.
H	POWER LED	**Steady on:** mains power present. **Blinking:** no mains power.
I	WARNING LED	**Steady on:** alarm and/or tamper. **Fast blinking:** failure presence. **Slow blinking:** open or inhibited/isolated inputs.
L	SYSTEM STATUS LED	**Steady On:** all Zones assigned to the keypad defined as used are active. **Slow blinking:** some zones assigned to the keypad defined as used are active, while the rest are inactive. **Off:** all Zones assigned to the keypad defined as used are inactive.
M	**(OK)** ✓ key	To confirm the chosen menu and go to the submenu.
N	Slider	Key protection.

Table 1 - 1068/021 keypad elements

1.2.1 Status icons in the display

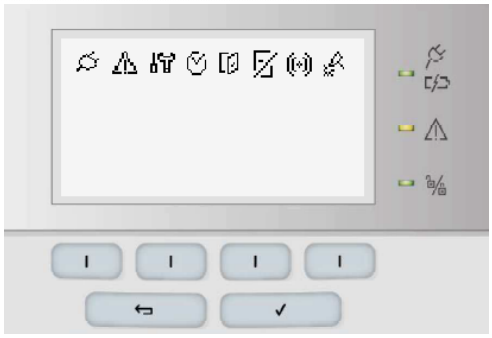


Figure 3 - 1068/021 keypad status icons

The LEDs and icons on the keypads indicate system status and alarms.

The amount of displayed information depends on the system status (set or unset), the mode of use set during programming and the access level (see paragraph *5.1 System access codes*).

Symbol	Description	Viewing	Supplied indications
	Power supply	Green LED	**On:** mains power present. **Off:** no mains power.
	Faults	Yellow LED (*)	**On:** Presence of a failure or fault. **Off:** No failures or faults. **Reverse On:** Consultation of details in progress ("ICON DETAILS" / "FAULTS" menu).
	Maintenance	----------	**On:** System under maintenance. **Off:** Normal operation.
	Time Scheduler	----------	**On:** commands present for the current day. **Off:** No command. **Reverse On:** command activation warning.
	Open inputs	Yellow LED (*)	**On:** Open input. **Off:** No open input. **Reverse On:** Consultation of details in progress ("ICON DETAILS" / "OPEN INPUTS" menu).
	Inhibited or isolated inputs	----------	**On:** Inhibited or isolated input. **Off:** No inhibited or isolated input. **Reverse On:** Consultation of details in progress ("ICON DETAILS" / "ISOLATED INPUTS" menu).
	Alarms	Yellow LED (*)	**On:** At least one alarm condition present. **Off:** No alarm condition present. Reverse On: Consultation of details in progress ("ICON DETAILS" / "ALARMS" menu).
	Tamper	Yellow LED (*)	**On:** At least one tamper condition present. **Off:** No tamper condition present. **Reverse On:** Consultation of details in progress ("ICON DETAILS" / "TAMPER" menu).

Table 2 - LED and icon indications of 1068/021 keypad

(*) The indicated failures and warnings are: GSM/GPRS module, IP interface, power supply for overvoltage, power supply for low voltage, battery (inefficient or low battery), +V voltage of control panel and expansion inputs, intrusion alarm condition, input isolation or inhibition, tamper.

The indicated alarm conditions are intrusion and warning. Technological indications are also provided (emergency, technological sustained, timed technological).

The indicated tampering conditions are: control panel tamper, devices tamper, control panel SAB input, expansion SAB input, tamper input, communication on system bus (the devices do not communicate with the control panel), imbalance of one of the inputs customised as balanced or double balancing, attempt to use a wrong access code or key (repeated 21 times).

Information is limited to the zones associated to the keypad only. The status of any configured zones which are not associated to the keypad cannot be determined.

1.2.2 Zone status

The zone status is shown on the keypad display in graphic mode.

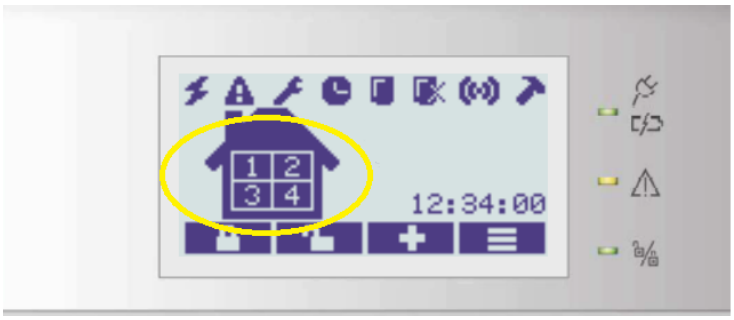


Figure 4 - Example 4-zones house - 1068/005A control panel

Inside the house there is a square for each of the zones of the control panel.

- 4 zones: 1068/005A control panel
- 8 zones: 1068/010A control panel
- Square completely white indicates:
  - Zone not associated to the keypad;
  - Zone associated to the keypad, not active and without open inputs.
- Numbered square with white background indicates:
  - Zone associated with the keypad, not active, with at least 1 input open;
- Numbered square with a black background (as in the image) indicates:
  - Zone associated with the keypad and active.

1.2.2.1 LED indications with compliance to EN50131 grade 1 and grade 2

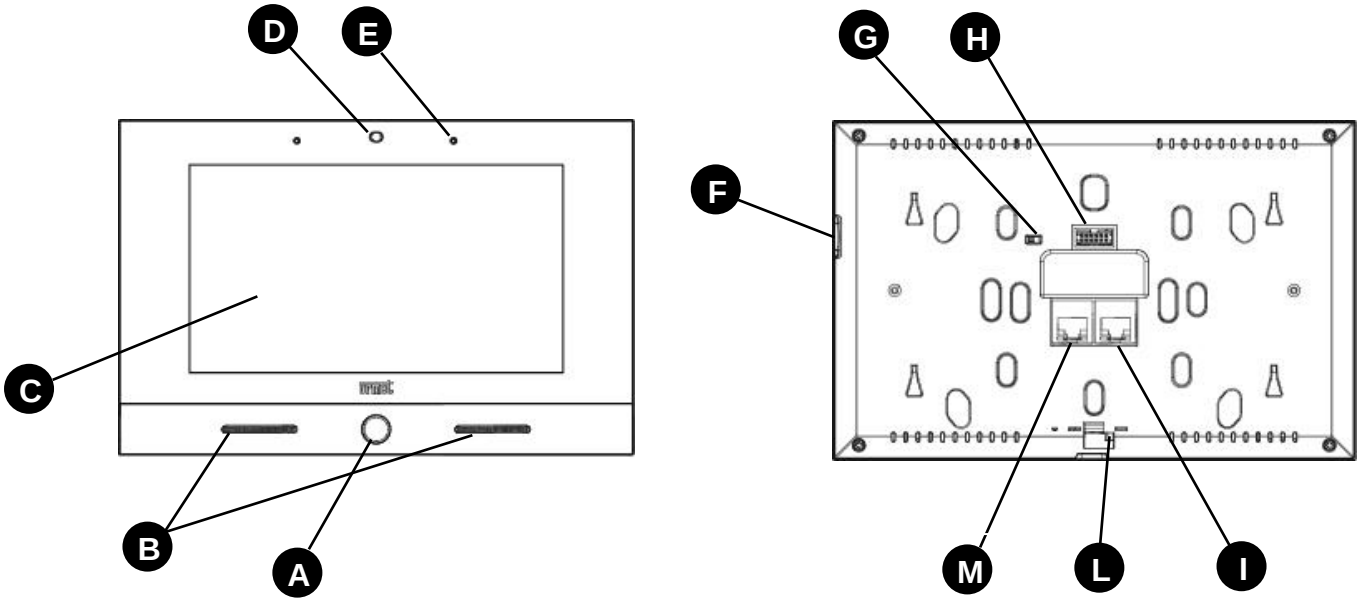
If the alarm system has been configured in operating mode compliant with EN50131-1, when active, only the following indications are visible:

- Power supply;
- Time scheduler;
- System status.

Enter a valid code to see details on the indications.

When the system is inactive, the access codes can be used to delete any type of signalling.

1.3 1068/027 TOUCH SCREEN KEYPAD



Ref.	Description
A	Backlit blue Home button
B	Speakers
C	7” touchscreen display
D	Webcam 2Mpx
E	Microphone
F	Micro SD Card
G	Switch (not used)
H	12 way for connecting the printed circuit board for external connections
I	LAN connector (not used)
L	Keypad locking latch
M	POE connector (LAN with power supply)

1.3.1 Status icons in the display

On the home page of the intrusion there is a series of icons that allow access to a series of information related to the status of the control panel.

Each of the icons must maintain a state, indicated by a color change. For example gray if there is nothing to report and white if the user must be notified of at least one event of the respective class.

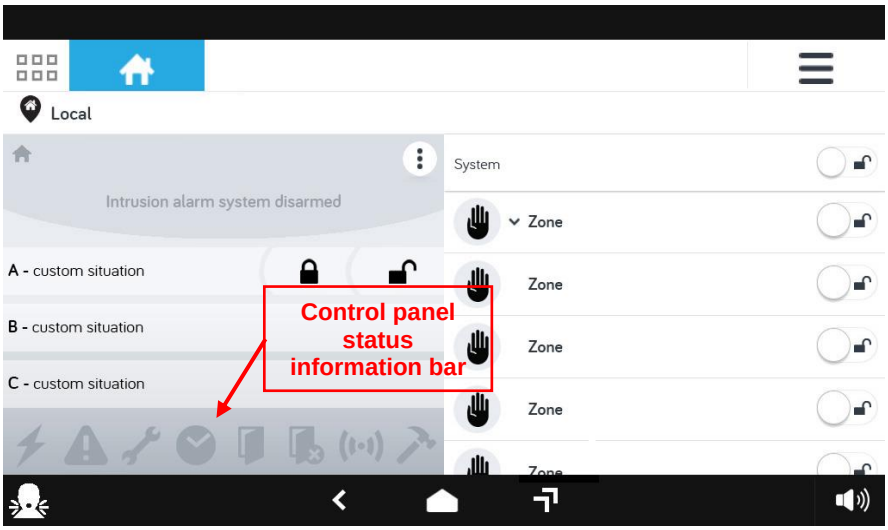


Figure 5 - 1068/027 keypad status icons

Symbol	Description	Supplied indications
	Power supply	Power supply events are displayed.
	Faults	Active fault events are displayed. It is possible to cancel the faults events.
	Maintenance	When not active, the maintenance status of the control panel is displayed. **WARNING**: the icon cannot be selected when active, as if the system is under maintenance, the touch keypad is inhibited.
	Time Scheduler	By selecting the time scheduler you can access the programming page; furthermore, programming can be postponed by entering the time by which it is to be delayed. Depending on the status, the icon takes on the following colors: • Gray: no programming available • White: there is a time schedule • Blue: there are 30 minutes left until the programming is activated
	Open inputs	The page with the list of open inputs is displayed.
	Inhibited or isolated inputs	The page containing the list of inputs excluded from security checks is displayed.
	Alarms	The page containing the list of alarm events is displayed. Alarm events can be deleted.
	Tamper	The page containing the list of tampering events is displayed. Tampering events can be deleted.

Table 3 - *1068/027 Keypad icons*

By pressing on each single icon, information can be obtained.
Power supply detail screen example:

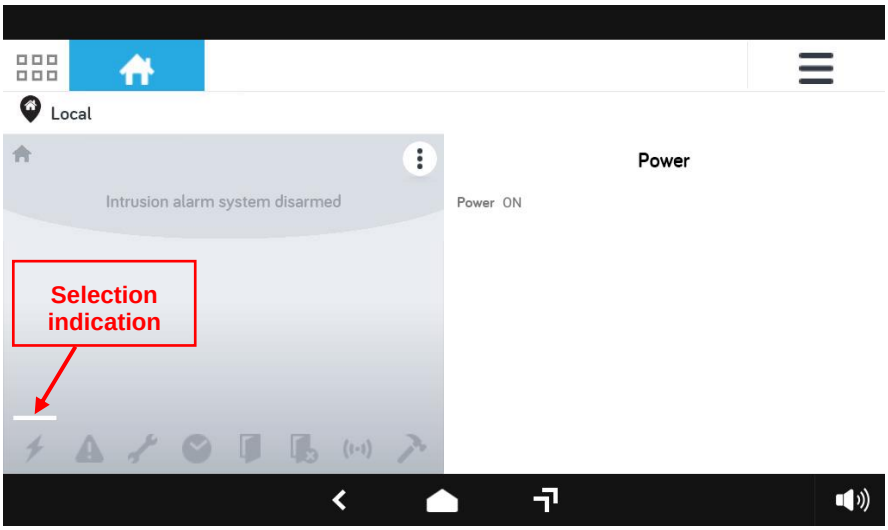


Figure 6 – Information screen example

1.4 1067/334 – 1067/335 ELECTRONIC KEY READER

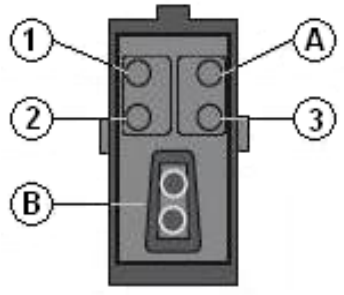


Figure 7 - 1067/334 – 1067/335 electronic key reader

Ref.	Description	Use or indications provided
1, 2, 3	LEDs (green) associated zones status	**Off** = all zones associated to the LED are unset. **On** = all zones associated to the LED are set. **Blinking** = at least one zone associated to the LED is set.
A	LED (yellow) alarm and signalling summary	**Steady on** = in case of Alarms or Tampering. **Fast blinking** = in case of Faults. **Slow blinking** = open or inhibited/isolated inputs.
B	Keyhole for electronic key	1067/334 – 1067/335 Shaped hole for inserting the electronic key.

1.5 1068/435 PROXIMITY KEY READER

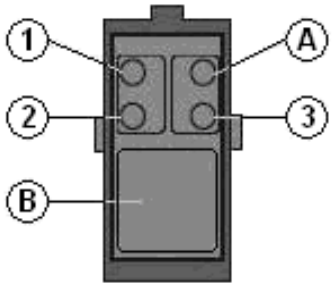


Figure 8 - 1068/435 proximity key reader

Ref.	Description	Use or indications provided
1, 2, 3	LEDs (green) associated zones status	**Off** = all zones associated to the LED are unset. **On** = all zones associated to the LED are set. **Blinking** = at least one zone associated to the LED is unset.
A	LED (yellow) alarm and signalling summary	**Steady on** = in case of Alarms or Tampering. **Fast blinking** = in case of Faults. **Slow blinking** = open or inhibited/isolated inputs.
B	Transponder	1068/435 Proximity key sensor.

2 SYSTEM BASIC MANAGEMENT

This chapter contains information for basic system management and describes how to activate and deactivate the system using keypads and electronic and proximity keys.

IMPORTANT! Users and keys must have been previously acquired, configured and enabled to set and unset the system and to clear the alarms, as explained in paragraph *5.4 Enabling and disabling.*

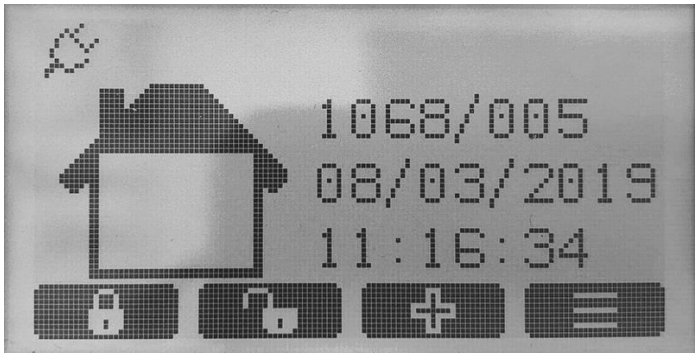
2.1 KEYPADS CUSTOMISATION

Each keypad can be independently customised by means of some parameters which can be configured locally with authorisation codes.

2.1.1 LCD Info

The keypad can display the following information in the home page with system active or not active:

- Date and time (always visible);
- Zone status (visible if configured);
- Name system (visible if configured);
- The display status of various icons of the system.



The viewing mode may be independently elected for each keypad in the system.

To enable the displaying of the **Synoptic** on the keypad, proceed as follows:

1. Access the **MASTER** / **INSTALLER** / **TECH. MANAGER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**LCD info**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Synoptic**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "SYNOPTIC ☑ " message on the display:
   - "ENABLE" ☑ : indicates the assignment to the zone.
   - "ENABLE" ☐: indicates the NON-assignment to the zone.
6. Press ✓ to confirm;
7. Press ↩ to return to the upper level menu.

To enable the displaying of the **Name system** on the keypad, proceed as follows:

1. Access the **MASTER** / **INSTALLER** / **TECH. MANAGER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**LCD info**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Name system**" by pressing the key associated with the ∨ or ∧ symbol ∧. Press ✓ to confirm;
5. Press the key associated with the "NAME SYSTEM" message ☑ on the display:
   - "ENABLE" ☑ : indicates the assignment to the zone.
   - "ENABLE" ☐: indicates the NON-assignment to the zone.
6. Press ✓ to confirm;
7. Press ↩ to return to the upper level menu.

2.1.2 How to set the Buzzer volume

Proceed as follows to adjust the Buzzer volume:

1. Access the **MASTER / INSTALLER / TECH. MANAGER** / **USER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Set buzzer**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Press | in correspondence of the character " **+** / **-** " to increase or decrease the volume;
5. Press ↩ to return to the upper level menu.

WARNING! If the control panel is used in compliance with EN50131 mode, the buzzer volume must remain active.

2.1.3 How to set the display contrast

Proceed as follows to adjust the display contrast:

1. Access the **MASTER / INSTALLER / TECH. MANAGER** / **USER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Set contrast**" by pressing the key associated with the ∨ or ∧ symbol Press ✓ to confirm;
4. Press | in correspondence of the character " **+** / **-** " to increase or decrease the contrast. Press ✓ to confirm;
5. Press ↩ to return to the upper level menu.

2.1.4 How to set backlighting

Proceed as follows to adjust the display and Leds brightness:

1. Access the **MASTER / INSTALLER / TECH. MANAGER** / **USER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Set backlight**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Press | in correspondence of the character " **+** / **-** " to increase or decrease the brightness. Press ✓ to confirm;
5. Press ↩ to return to the upper level menu.

If level 0 is set (no square on) the keys will be switched off and the display can only be read in adequate ambient lighting conditions.

Backlighting will not be switched back on even if a key is pressed.

2.2 DATE AND TIME SETTING

In addition to being shown on the keypad in the home page, date and time information is used to record events (System log) and for the Time Scheduler functions.

Proceed as follows to modify the date and time shown on the display:

1. Access the **MASTER / INSTALLER / TECH. MANAGER** / **USER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Date and Time**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Set hour**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Use the alphanumeric keypad to enter the correct time. Press ✓ to confirm;
7. Select "**Set date**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Use the alphanumeric keypad to enter the correct date. Press ✓ to confirm;
9. Press ↩ repeatedly to go back to the upper level menu.

To set the daylight saving time, follow the instructions below:

1. Access the **MASTER / INSTALLER / TECH. MANAGER** / **USER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Date and Time**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Set Daylight Saving Time**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm. Press ✓ to confirm;
6. Use the alphanumeric keypad to enter the correct time. Press ✓ to confirm;
7. Press ↩ repeatedly to go back to the upper level menu.

IMPORTANT! The time scheduler will not work properly if the date and time are not correct and the System Log time references will not be correct.

2.3 SETTING PROCEDURE

The alarm system has various setting modes, some of which are EN50131 compliant.

- **Compliant with EN50131:** setting with keypad, through time scheduler and through a customised key input.
- **Not compliant with EN50131:** setting with electronic or proximity key, remote activation via GSM module or IP module and radio remote control.

The authorisation codes which must be used with keypads are described in paragraph *5.1 System access codes.*

You can activate the entire system and only a few zones if they have been configured in programming.

The User or key must have been previously assigned to the zone during programming in order to operate on it.

2.3.1 Partial or total setting with 1068/021 keypad

EN50131 GRADO 1 EN50131 GRADO 2

System setting can be:

- Total
- Partial

2.3.1.1 Enabling direct setting

Quick direct setting is used to make the system operational without entering a code.
If the specific function is enabled, the system can be activated using the quick setting keys.

Proceed as follows to enable the function:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Direct setting**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Press the key ▯ associated with the "ACTIVATION" message ☑ on the display:
   - "ENABLE" ☑ : direct setting enabled.
   - "ENABLE" ☐ : direct setting NOT enabled.
5. Press ✓ to confirm;
6. Press ↩ repeatedly to go back to the upper level menu.

2.3.1.2 Configuration of partial setting quick keys

The **A / B / C** quick setting keys will only work if they have been previously programmed.

Proceed as follows to configure the function:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**Keypad settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**A / B / C keys**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**A key**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the zone "**ZNXX : Zone X**" by pressing the key associated with the ∨ or ∧ symbol.
6. Press the key ▯ associated with the "ASSIGNMENT" message ☑ on the display:
   - "ZN0X: Zone X" ☑ : zone associated with key A
   - "ZN0X: Zone X" ☐ : zone NOT associated with key A

   Press ✓ to confirm;
7. Perform the assignment operation for all zones you want to assign to key A;
8. Perform operations from Step 4 for all **A** / **B** / **C** keys;
9. Press ↩ repeatedly to go back to the upper level menu.

2.3.1.3 Quick total setting

Proceed as follows to set the alarm system:

1. Press the key ▯ associated with the symbol 🔒 to activate the intrusion alarm system.
2. If "direct setting" is enabled:
   - If there are programmed subzones ("**A**" / "**B**" / "**C**") - select the key ▯ associated with the symbol 🔒 again.
   - If there are no programmed subzones ("**A**" / "**B**" / "**C**") the system will be directly activated.
3. If "direct setting" is not enabled:
   - If there are programmed subzones ("**A**" / "**B**" / "**C**") - select the key ▯ associated with the symbol 🔒 again. You will be asked to enter a user code, enter the code and press ✓ to confirm.
   - If there are no programmed subzones ("**A**" / "**B**" / "**C**") you will be asked to enter a user code immediately.
   - Enter the code and press ✓ to confirm.

⚠	**IMPORTANT!** With this procedure a user will set only the relevant zones filtered by zones assigned to the keypad and not necessarily all of them. The user (MASTER / INSTALLER / TECH. MANAGER) activates all the zones without being filtered by the keypad zones assignment.

2.3.1.4 Quick partial setting

To partially set the system zones using the shortcut keys, proceed as follows:

1. Press the key associated with the symbol to activate the intrusion alarm system;
2. Select, by pressing the keys ssociated with the symbols "**A**" / "**B**" / "**C**", the desired partial setting depending on the previous configuration. The keys are NOT visible if they have not been associated with zones.
3. If the "Direct setting" function is enabled, the system will be activated directly without any user code request.
4. If the "Direct setting" function is not enabled, the keyboard will ask you to enter a user code.
5. Enter the code and press to confirm.

	IMPORTANT! With this procedure a user will set only the relevant zones filtered by zones assigned to the keypad and not necessarily all of them. The user (MASTER / INSTALLER / TECH. MANAGER) activates all the zones without being filtered by the keypad zones assignment.

2.3.1.5 Partial or total setting from the menu

This setting mode, unlike the quick mode described above, always requires a code.

A particularity of the splitting method is that it allows to set and unset the zones in the same way without needing to use two different procedures.

Proceed as follows to select the zones to be activated:

1. Access the **MASTER** / **INSTALLER / TECH. MANAGER / USER** menu by entering the access code. Press to confirm;
2. Select "**System status**" by pressing the key associated with the or symbol. Press to confirm;
3. Moving with associated with the symbol or , select with the key associated with the symbol the zones to be activated:

   "Padlock open" = Zone not active; "Padlock closed" = Zone to be activated.
4. Press to confirm, the zones will be active immediately and you will return directly to the home page of the keypad.

	IMPORTANT! With this procedure, the User will only view and activate/deactivate the zones for which he/she is responsible.

EN50131

2.3.2 Partial and total setting with electronic or proximity key

2.3.2.1 Total setting from reader

	IMPORTANT! This procedure can only be used if all zones are unset.

Proceed as follows to set all zones assigned to the reader and to the key:

1. Insert the key or approach it to the reader when all the green LEDs are off (the procedure will unset the zones if some green LEDs are on).

   The yellow LED will blink to indicate that the key is being read.

   All the green LEDs will blink rapidly if the key is not recognised.
2. Extract/move away the key when the yellow LED starts blinking.
3. The green LEDs indicate the status of the zones assigned to the reader:
   - LED steady on = zone active;
   - LED off = zone not active;
   - LED blinking = at least one zone associated to the LED is set.

	IMPORTANT! The key will set only the assigned zones and not necessarily all the zones with this procedure.

2.3.2.2 Partial setting from reader

Proceed as follows to set some of the zones assigned to the reader and to the key:

1. Insert the key or approach it to the reader when all the green LEDs are off (the procedure will set the zones if some green LEDs are on during the first cycle). The yellow LED will blink to indicate that the key is being read. All the green LEDs will blink rapidly if the key is not recognised.
2. The yellow LED will blink and after a few seconds a cycle will start during which the green LEDs turn on showing the various combinations in sequence.
3. Extract/move away the key when the combination of zones to be set is displayed by the LEDs. The possibility of setting each zone depends on the programming of the reader and on the key used.
4. The green LEDs indicate the status of the zones assigned to the reader:
   - LED steady on = zone active;
   - LED off = zone not active;
   - LED blinking = at least one zone **associated to the LED is set.**

	**IMPORTANT! The key will set only the assigned zones and not necessarily all the zones with this procedure.**

2.4 UNSETTING PROCEDURE

The alarm system may be unset in various manners, some of which are not EN50131 compliant.

- **Compliant with EN50131**: unsetting with keypad, through time scheduler and through a customised key input.
- **Not compliant with EN50131**: unsetting with electronic or proximity key, remote unsetting via GSM module or IP interface, radio remote control and 1068/027 keypad.

The authorisation codes which must be used with keypads are described in paragraph *5.1 System access codes.*

You can unset the entire system and only a few zones if they have been configured in programming.

The user or key must have been previously assigned to the zone during programming in order to operate on it.

2.4.1 Partial or total unsetting with 1068/021 keypad

EN50131 GRADO 1 EN50131 GRADO 2

2.4.1.1 Total unsetting

Proceed as follows to deactivate the entire alarm system:

1. Press the key [ ] associated with the symbol  to deactivate the intrusion alarm system;
2. Press the key [ ] associated with the symbol  ;
3. Enter the **USER** code and press [✓] to confirm.

	**IMPORTANT!** The user will unset only the assigned zones and not necessarily all the zones with this procedure.

2.4.1.2 Partial unsetting

Proceed as follows to deactivate some zones of the alarm system:

1. Access the **MASTER / INSTALLER / TECH. MANAGER / USER** menu by entering the access code. Press [✓] to confirm;
2. Select "**System status**" by pressing the key associated with the ∨ or ∧ symbol. Press [✓] to confirm;
3. Press the key [ ] associated with the symbol  to select the zones to deactivate. Pressing [✓] the zones will be immediately deactivated;
4. Press [↩] repeatedly to go back to the upper level menu.

	**IMPORTANT!** The user will unset only the assigned zones and not necessarily all the zones with this procedure.

2.4.1.3 Quick total unsetting

Proceed as follows to deactivate the alarm system:

1. Press the key associated with the symbol to deactivate the intrusion alarm system.
2. If there are programmed subzones ("A" / "B" / "C") - select the key associated with the symbol again; a user code will be requested.
3. Enter the code and press to confirm.

IMPORTANT! With this procedure a user will deactivate only the relevant zones filtered by zones assigned to the keypad and not necessarily all of them.

The user (MASTER / INSTALLER / TECH. MANAGER) deactivates all the zones without being filtered by the keypad zones assignment.

2.4.1.4 Quick partial unsetting

Proceed as follows to partially deactivate the alarm system:

1. Press the key associated with the symbol to partially deactivate the intrusion alarm system.
2. Select, by pressing the keys associated with the symbols "A" / "B" / "C", the desired partial unsetting depending on the previous configuration; a user code will be requested.
3. Enter the code and press to confirm.

IMPORTANT! With this procedure a user will deactivate only the relevant zones filtered by zones assigned to the keypad and not necessarily all of them.

The user (MASTER / INSTALLER / TECH. MANAGER) deactivates all the zones without being filtered by the keypad zones assignment.

2.4.1.5 Unsetting from keypad under hold-up

On the 1068/005A or 1068/010A control panel, if the hold-up function has been enabled if you are threatened and forced by a criminal and your life is at risk, then you can unset the intrusion alarm system while setting the hold-up alarm simultaneously, which will make the dialler send the programmed alarm messages without activating the siren sound.

To unset the system when you are under hold-up, just increase your user code of one digit. For example if your user code is 000021 you need only to enter 000022; if user code is 000029 enter 000020, if it is 000039 enter 000030, etc.

IMPORTANT! Enabling the hold-up function will cancel any compliance with EN50131 standards.

2.4.2 Partial and total unsetting with electronic or proximity key

2.4.2.1 Total unsetting from reader

Proceed as follows to deactivate all zones assigned to the reader and to the key:

1. Insert the key or approach it to the reader. The yellow LED will blink to indicate that the key is being read. All the green LEDs will blink rapidly if the key is not recognised;
2. Extract/move away the key when the yellow LED starts blinking;
3. The green LEDs indicate the status of the zones assigned to the reader:
   - LED off = zone not active;
   - LED on = key not assigned to the zone;
   - LED blinking = at least one zone associated to the LED is deactivated.

IMPORTANT!

The key will unset only the assigned zones and not necessarily all the zones even with this procedure.

2.4.2.2 Partial unsetting from reader

Follow the same procedure used for partial setting from reader to partially deactivate the system through a reader with key (see paragraph *2.3.2.2 Partial setting from reader).*

2.5 SYSTEM STATUS INFORMATION

2.5.1 How to view system status

The system status is displayed by the LED and summary synoptic provided on keypads and readers.

The number of activated and assigned zones is shown on the keypad display.

Each User can view the system status in detail for the part concerning to them (only the zones on which the user is authorised to operate will appear).

To view the system status:

1. Enter the menu by entering the access code. Press ✓ to confirm;
2. Select "**System status**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm. The display will show the status of the zone associated with the system;
3. Press ↩ repeatedly to go back to the upper level menu.

2.5.1.1 How to view open inputs

The presence of one or more open inputs is indicated by the specific LED and icon on the keypad and by the reader LED (see chapter *1 CONTROL DEVICES).*

To view input addresses:

1. Press the key ▯ associated with the symbol ☰ to enter the menu.
2. Select "**Icon details**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
   (A valid code entry is required only in compliance with EN50131 operating mode).
3. Select "**Open inputs**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm. The display shows the open inputs in the system with their technical name;
4. Press ↩ repeatedly to go back to the upper level menu.

2.5.2 How to view isolated or inhibited inputs

The presence of one or more isolated or inhibited inputs is indicated by the dedicated icon.

An input can only be isolated if it has been programmed as such.

All users can isolate an input associated with their zone of competence.

To view addresses of isolated inputs:

1. Enter the menu by entering the access code. Press ✓ to confirm;
2. Select "**Icon details**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
   (A valid code entry is required only in compliance with EN50131 operating mode).
3. Select "**Isolated inputs**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm. The display shows the isolated or inhibited inputs with their technical name;
4. Press ↩ repeatedly to go back to the upper level menu.

2.5.3 How to examine the Alarms Memory

Alarm events are indicated by the specific LEDs (on keypad and readers) and stored by the control panel. Details on the events can then be viewed on the keypad display.

Proceed as follows to view details:

1. Press the key ▯ associated with the symbol ☰ to enter the menu;
2. Select "**Icon details**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Alarms**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm. The display shows the stored alarms;
4. Press ↩ repeatedly to go back to the upper level menu.

2.5.4 How to delete the Alarms Memory

Proceed as follows to delete the Alarms Memory:

1. Enter the menu by entering the access code. Press ✓ to confirm;
2. Select "**Icon details**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Alarms**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Delete memory**" by pressing the key ▯ associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. The message "**Are you sure?**" appears on the display. Press ✓ to confirm;
6. Press ↩ repeatedly to go back to the upper level menu.

2.5.5 How to examine the Tampers Memory

Tamper events are indicated by the specific LEDs (on keypad and readers) and stored by the control panel. Details on the events can then be viewed on the keypad display.

Proceed as follows to view details:

1. Press the key associated with the symbol to enter the menu;
2. Select "**Icon details**" by pressing the key associated with the or symbol. Press to confirm;
3. Select "**Tamper**" by pressing the key associated with the or symbol. Press to confirm; The display will show the tampering events with the input that detected the event;
4. Press repeatedly to go back to the upper level menu.

2.5.6 How to delete the Tampers Memory

Proceed as follows to delete the Tampers Memory:

1. Enter the menu by entering the access code. Press to confirm;
2. Select "**Icon details**" by pressing the key associated with the or symbol. Press to confirm;
3. Select "**Tamper**" by pressing the key associated with the or symbol. Press to confirm;
4. Select "**Delete memory**" by pressing the key associated with the or symbol. Press to confirm;
5. The message "**Are you sure?**" appears on the display. Press to confirm;
6. Press repeatedly to go back to the upper level menu.

	IMPORTANT! A tamper event which is still present cannot be deleted.

2.5.7 How to examine the fault and anomaly memory

A fault, failure or anomaly (e.g. low or inefficient battery, phone line fault, detector or siren fault) will be indicated by the specific LED on the keypad and the reader LED (see chapter *1 CONTROL DEVICES).*

To examine the detected faults:

1. Press the key associated with the symbol to enter the menu;
2. Select "**Icon details**" by pressing the key associated with the or symbol. Press to confirm;
3. Select "**Faults**" by pressing the key associated with the or symbol. Press to confirm. The display shows the stored "Fault" events;
4. Press repeatedly to go back to the upper level menu.

2.5.8 How to delete the fault memory

How to delete the fault memory:

1. Enter the menu by entering the access code. Press to confirm;
2. Select "**Icon details**" by pressing the key associated with the or symbol. Press to confirm;
3. Select "**Faults**" by pressing the key associated with the or symbol. Press to confirm;. The display shows the stored "Fault" events;
4. Select "**Delete memory**" by pressing the key associated with the or symbol. Press to confirm;
5. The message "**Are you sure?**" appears on the display. Press to confirm;
6. Press repeatedly to go back to the upper level menu.

2.6 HOW TO POSTPONE AUTOMATIC SETTING

Times and actions to be performed are set by the installer during programming on the time scheduler.

For instance, automatic setting of the alarm system may be programmed but it could be necessary to delay actual setting. This can be achieved without changing the time scheduler configuration. Setting can be postponed by a minute number within 1 and 30 during the warning time (which can be configured during programming) before the intrusion alarm system is automatically set by the time scheduler. This operation can be repeated several times before midnight. The warning time is indicated on the keypads by the buzzer sounding and the time scheduler icon turning on in reverse mode.

Proceed as follows to postpone automatic setting:

1. Access the **MASTER** / **INSTALLER** / **TECH. MANAGER / USER** menu by entering the access code (*User* only for the assigned zones). Press to confirm;
2. Select "**Icon details**" by pressing the key associated with the or symbol. Press to confirm;
3. Select "**Time scheduler**" by pressing the key associated with the or symbol. Press to confirm;
4. Select "**Move command**" by pressing the key associated with the or symbol. Press to confirm;
5. Enter the minute number. Press to confirm;
6. The message "**Are you sure?**" appears on the display. Press to confirm;
7. Press repeatedly to go back to the upper level menu.

3 SYSTEM ACTIVATION FAILURE

This chapter describes the causes that prevent the activation of the alarm system, indicating any remedies to be taken.

An **EN50131 compliant** intrusion alarm system cannot be set by the User if certain blocking conditions are present.

There are also conditions that can be inhibited which may be overridden and bypassed by means of specific manual commands imparted by the User or by the Installer.

The following describes both blocking conditions and conditions that can inhibited.

3.1 BLOCKING CONDITIONS

Conditions that always automatically prevent setting (regardless of the control device that requested activation).

The conditions that block the system are:

- Open and non-excludable instantaneous intrusion input
- Open and non-excludable tamper input
- Open and non-excludable pre-alarm input
- Open and non-excludable detector failure input
- Open and non-excludable siren failure input
- Unbalanced and non-excludable balanced or double balanced input (any customisation)

Input conditions only prevent the setting of the zones associated with them.

The conditions that prevent the setting of any zone are the following:

- Bus failure
- No communication with a wired device or a communicator or lack of radio supervision
- Control panel tamper, radio device or wired device
- 24-hour inputs (open) (control panel SAB or wired expansion)
- Jamming on radio module, radio interface or GSM/GPRS module
- Control panel battery failure, radio device and additional power supply
- +SR failure
- Control panel power supply failure and additional power supply
- Bus power supply voltage failure
- +V1 failure
- +V2 failure
- Bus device failure
- Control panel mains failure and additional power supply failure
- GSM /GPRS fault
- IP interface fault

3.2 CONDITIONS THAT CAN BE INHIBITED

The conditions that can be inhibited may be overridden and bypassed by means of specific manual commands imparted by the User or by the Installer.

3.2.1 Conditions that can be inhibited on inputs

The input conditions apply to inputs associated with at least one of the zones for which activation is required.

The conditions requiring inhibition are as follows:

- Open and excludable **instantaneous intrusion** input
- Open and excludable **tamper** input
- Open and excludable **pre-alarm** input
- Open and excludable **Detector failure** input
- Open and excludable **Siren failure** input
- Unbalanced and excludable balanced or double balanced input **(any customisation**)

Inhibitions can be confirmed by any user.

If the activation command is given by a control device other than a wired keypad, that is:

- Time scheduler
- Proximity key
- Electronic key
- Remote control
- Wireless keypad
- Key customised input
- GSM phone communicator
- Via Urmet Secure App - 1068set Android App – Keypad 1068/027

Conditions that would require inhibition by the user also cause the prevention of setting, since with these control devices it is not possible to confirm the inhibition.

The electronic and proximity keys, the time scheduler and the special key input will not set the alarm system in these cases. The failure to set event caused by the block is stored in the System Log with a description of the reason.

You can attempt to override the block and set the system all the same by operating on the alarm system using the keypad. The cause or causes which prevent setting will appear on the keypad display. The User can try to eliminate the causes of the block, for example by closing the open inputs, or force the block with the keypad by checking each block and, overriding them one by one with subsequent confirmations, forcing the block.

The block override operation is stored step by step in the System Log.

	**IMPORTANT!** Furthermore, you cannot override the prevention of setting in one step. You must override the single blocks one by one.

	**IMPORTANT!** The prevention of setting will be overridden until the system is unset. The override will be ended when the system is unset and must be repeated when the system is set again. The end of the inhibition is stored in the System log.

	**IMPORTANT!** Overriding the prevention of setting is a temporary solution to allow to set the alarm system also when conditions which may compromise efficacy are present. It is advisable to remove the causes that prevent setting and to restore perfect efficiency of the system as soon as possible.

3.3 EXAMPLE OF OVERRIDING

In this example, we will describe a system with four zones, zone1 has 3 inputs and the inputs 2 and 3 of zone 1 are open.

In this case, the setting sequence performed by a normal User will be:

1. Fully activate the system by pressing the key  associated with the symbol  (only with direct setting enabled).
2. Press the key associated with the symbol  . Without direct setting enabled, a code must be entered. Press  to confirm;
3. The display shows "**Prevention of setting**" and the line below lists the inputs that are open;
4. Press  to confirm the inputs you wish to inhibit;
5. After confirming them, the system will propose **"forced setting"**. Press  to confirm;
6. At the end of this operation the system will result with the inputs inhibited.

3.3.1 Impossibility to override the prevention of setting with open inputs

The setting can be overridden with open intrusion inputs, providing that:

1. The inputs are all configured as “isolable” during programming, and
2. The open inputs are not customised as First Entry/Last Exit or Delayed.

The customised First Entry/Last Exit or Delayed inputs are ignored by the control panel when the open inputs are checked during activation. Their feature is to be able to be or remain open to allow Users to leave the protected rooms.

For this reason, you will not be asked to inhibit them and when the alarm system is eventually set at the end of the delay time, the control panel will detect an open intrusion input and trip the alarm.

4 ALARMS, EVENTS AND INDICATIONS

This chapter contains a detailed description of the alarms, events and signalling managed by 1068/005A and 1068/010A control panels.

4.1 DESCRIPTION OF SIGNALLING EVENTS IN THE LOG

The table below contains the messages that are displayed in the Log, the possible causes of the failure or malfunction that occurred, and actions to take to solve the problem. **M**= Master ; **I**= Installer; **T**= Technical Manager; **U**= User

Description on System log	Visible with code...	Event	Icon on keypad display	Suggested actions
Acquire key	**M – I – T – U**	• A key has been acquired by the system.	----------	----------
Battery failure	**I**	• Control panel battery failure • Radio device failure	Faults	Verify that: • The control panel battery is charged • The batteries of any radio devices are charged
Firmware upgrade	**I**	• Firmware upgrade is performed	----------	----------
Hold-up	**M – I – T – U**	• A customised hold-up input has been opened • A hold-up code has been entered	----------	----------
Anti thief	**M – I – T – U**	• A customised anti thief input has been opened • The function key of the keypad, wireless keypad or remote control has been pressed	Alarm	----------
System shutdown	**I**	• Control panel powered only by battery below 10.5V threshold	----------	• Check that the 220V voltage is present • Check the voltage on the control panel battery
Forced setting	**M – I – T – U**	• In EN50131 compliant operating mode the system activation was forced by the user.	----------	----------
Backup configuration	**I**	• A configuration has been backed up	----------	----------
Prevention of setting	**M – I – T – U**	• In EN50131 compliant operating mode, some zones were not activated through keypads or remote controls due to an event that blocked them.	----------	----------
Valid code	**M – I – T – U**	• A valid code has logged in to the system	----------	----------
How to delete a key	**M – I – T – U**	• A key has been deleted from the system	----------	----------
Cause of prevention of setting	**M – I – T – U**	• In EN50131 compliant operating mode, event that caused the activation of one or more zones to be blocked	----------	----------
Command	**M – I – T – U**	• A controllable output was controlled by device function keys, time scheduler, vocal call, SMS or Urmet 1068set App / Urmet Secure App	----------	----------
Alarm count	**I**	• An input has been isolated following the alarm count	----------	----------
Access control	**M – I – T – U**	• A key with ZONE CTRL function has been used	----------	----------
Date and Time	**M – I – T – U**	• The date or time of the system have been changed by the user	----------	----------

Description on System log	Visible with code...	Event	Icon on keypad display	Suggested actions
Wrong code	**M – I – T – U**	• An invalid code has been entered 21 times. • An unfinished code has been entered within 60 seconds for 21 times. • A key that has not been acquired or enabled by the system has been passed 21 times.	Tampering	----------
XX Faults	**I**	• +PS +SR +V1 +V2 VBUS faults (are signalled if present for more than 10 seconds)	Faults	• Verify that the voltages on: VBUS, +PS, +SR, +V1 and +V2 are correct.
Communicators fault	**I**	• A customised communicator fault input has been opened	Faults	Available only with 1068/010A control panel.
IP Fault	**I**	• An IP interface fault has been detected	Faults	• Perform the IP interface test to get any details about the failure
GSM Fault	**I**	• A GSM communicator fault has been detected	Faults	• Perform the GSM field test to get any details about the failure
Detector Fault	**I**	• A customised detector fault input has been opened.	Faults	----------
Siren Fault	**I**	• A customised siren fault input has been opened	Faults	----------
IDP	**I**	• A call has been made to a surveillance centre via IDP numeric protocol	----------	----------
IDP-IP	**I**	• A call has been made to a surveillance centre via IDP/IP numeric protocol	----------	----------
Fire	**M – I – T - U**	• A customised fire input has been opened	Alarm	Available only with 1068/010A control panel.
Inhibit	**M – I – T - U**	• An input with at least one active assigned zone has been inhibited following an alarm count.	Isolated	----------
Inhibit	**M – I – T - U**	• Blocking conditions that have been inhibited by the user for activation in EN50131 compliant operating mode. • No communication or bus failure, tamper open, SAB input open, jamming, loss of mains, battery failure and system failure.	----------	Verify that: • No blocking conditions are present • SAB inputs are closed • Mains power is present • All Tampers are closed • There are no system failures
Enable Start/End	**M – I – T - U**	• Master user has enabled or disabled users or keys.	----------	----------
Instantaneous intrusion	**M – I – T - U**	• A customised instantaneous input with at least one active assigned zone has been opened.	Alarm	----------

Description on System log	Visible with code...	Event	Icon on keypad display	Suggested actions
Intrusion path	**M – I – T - U**	• A customised path input with at least one active assigned zone has been opened.	 Alarm	----------
Prealarm intrusion	**M – I – T - U**	• A customised prealarm input with at least one active assigned zone has been opened.	 Alarm	----------
Delayed intrusion	**M – I – T - U**	• A customised delayed input with at least one active assigned zone has been opened.	 Alarm	----------
Isolation	**M – I – T - U**	• An input has been manually isolated by the user.	 Isolated	----------
Jamming	**I**	• The system has detected an interference on the radio part	 Tampering	----------
No dialogue	**I**	• No communication with keypads, expansions, readers, IP, GSM, radio devices (supervision enabled).	 Tampering	• Check that the BUS devices, radio devices and interfaces on the control panel are correctly connected.
Loss of mains	**M – I – T – U**	• Instantaneous and persistent loss of mains (2 different messages in the log).	----------	Verify that: • The 220V mains power is present • The control panel power supply unit is working
Tamper	**I**	• A customised tamper input has been opened • Some inputs of BAL or double BAL type have been unbalanced.	 Tampering	• Check that the BAL or double BAL inputs are correctly connected with the 2.7Kohm resistors.
Tampering in 24H	**I**	• Check that the tamper inputs are properly grounded with the 2.7Kohm resistor.	 Tampering	----------
Maintenance	**M – I – T – U**	• The system sets to maintenance mode	 Maintenance	----------
First Entry/Last Exi	**I**	• A customised first entry/last exit input with at least one active assigned zone has been opened.	 Alarm	----------
Time scheduler	**M – I – T – U**	• The activation of the system through the time scheduler has been postponed manually.	 Time scheduler	----------
Communicator progr.	**I**	• The programming of the communicator has been changed	----------	----------
Reset	**I**	• Event generated at each restart or reset (RESET jumper) of the control panel	----------	----------
Reset	**I**	• The system has been reset to the factory settings.	----------	----------
Fire Reset	**M – I – T – U**	• A customised fire reset input has been opened	----------	Available only with 1068/010A control panel.
Restoring	**I**	• A configuration backup has been restored.	----------	----------

Description on System log	Visible with code...	Event	Icon on keypad display	Suggested actions
Update result	**I**	• Result of FW upgrade of the devices	----------	• Check that the arrow next to the description is pointing upwards (positive result). If the arrow points down (negative result), repeat the system upgrade procedure.
SIM expiration date	**M – I – T – U**	• The day of the set expiration date has been reached.	----------	• Renewing or topping up your SIM Card • Updating the expiration date
Emergency	**M – I – T – U**	• A customised emergency input has been opened • The function key of the keypad, wireless keypad or remote control has been pressed	 Alarm	----------
Zone status	**M – I – T – U**	• One or more zones of the system have been activated or deactivated	----------	----------
Tamper	**I**	• Verify that all tampers of the devices in the system are closed	 Tampering	----------
Technological sustained	**M – I – T – U**	• A customised technological input has been opened	----------	----------
Timed technological	**M – I – T – U**	• A customised timed technological input has been opened	----------	----------

5 ADVANCED SYSTEM MANAGEMENT

This chapter contains information for complete system management including the procedures which are used less frequently than the system setting and unsetting procedures.

5.1 SYSTEM ACCESS CODES

Access to given system functions is permitted according to the access code type (Master, User, Installer or Technical Manager). The available codes are:

1. **Master code**. This code is always enabled and is the only code authorised to enable other users, keys, time scheduler and remote access. It can be used to reset all the other access codes to the factory default (useful if the changed access code is forgotten).
2. **Installer code**. This code must be enabled each time by the Master code and is automatically deactivated when a new valid code is entered or a valid key is used. The code is also enabled after each system reset. This is to program the system and for maintenance. This code is used by the installer. It can be used to reset all the other access codes to the factory default (useful if the changed access code is forgotten).

	**IMPORTANT!** The installer code will be automatically deactivated if any Users enter their code while the installer code is enabled. The same will occur if an electronic or proximity key is used.

3. **User code**. This code must be enabled by the Master code and will remain valid until it is deactivated by the Master code or by a time scheduler command. This code is used by users for normal operations: setting and unsetting the system, displaying system status, reading system log and changing the access code.
4. **Technical Manager code**. This code must be enabled by the Master code and is automatically deactivated when a new valid code is entered or a valid key is used. The code is also enabled after each system reset. It allows to access a limited number of system configuration functions. It can be used to reset all the other access codes to the factory default (useful if the changed access code is forgotten).

	**IMPORTANT!** The enabled Technical Manager code will be automatically deactivated if any User enters their code while the Technical Manager code is enabled. The same will occur if an electronic or proximity key is used.

Each access code is freely programmable with a variable length from a minimum of four to a maximum of six digits. Each User can change their access code at will.

 Each Users, including the Master and Installer, should change their code before commissioning the system

Always press  to confirm the entered access code to access menus or functions.

	**IMPORTANT!** Enabling the hold-up function will cancel any compliance with EN50131 standards

5.1.1 Default access codes

The 1068/005A and 1068/010A control panels is provided with default codes when leaving the factory.

The Installer and Technical Manager codes are enabled at the factory and automatically deactivated when a valid Master or User code is entered for the first time.

Code type	Level	Default code	Assigned zones	Enabled when leaving the factory	Enable time (once enabled)
Installer	3	0000	All	Yes	Temporary session
Master	2	1111	All	Yes	Permanent
User (1÷16)	2	0010-0160	Zone 1	No	Until expressly disabled
Technical Manager	3	2222	All	Yes	Temporary session

Table 4 - Default access codes for 1068/005A

Code type	Level	Default code	Default code	Enabled when leaving the factory	Enable time (once enabled)
Installer	3	0000	All	Yes	Temporary session
Master	2	1111	All	Yes	Permanent
User (1÷32)	2	0010-0320	Zone 1	No	Until expressly disabled
Technical Manager	3	2222	All	Yes	Temporary session

Table 5 - Default access codes for 1068/010A

5.1.2 Change code

Each User can change their access code freely.

Proceed as follows to change the code:

1. Enter the menu by entering the access code. Press ✓ to confirm;
2. Select "**System settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Change code**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Enter the "Old code" and press ✓ to confirm;
6. Enter the “New code” (4 to 6 digits), and press ✓ to confirm;
7. Press ✓ to confirm the new code;
8. Press ↩ repeatedly to go back to the upper level menu.

5.1.3 How to reset an access code

An access code can be reset to its default value if a user forgets it (see paragraph *5.1.1 Default access codes).*

Proceed as follows to reset a code to its default value:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Default code**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the desired user by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
7. The system asks for confirmation of the request and the message "**Are you sure**?” will be displayed. Press ✓ to confirm;
8. Press ↩ repeatedly to go back to the upper level menu.

5.1.4 Entering an invalid code or using an invalid key

An attempt to enter an invalid access code 21 consecutive times or use of an invalid key 21 consecutive times will be interpreted by the control panel as a sabotage attempt. The control panel will consequently generate a tamper alarm and activate the programmed alarm outputs and the phone call dialer.

The incorrect code count will be reset as soon as a correct code or valid key is used.

5.2 MENU

All system configuration and enabling operations are performed using menus.

The operations for accessing and navigating menus are described below.

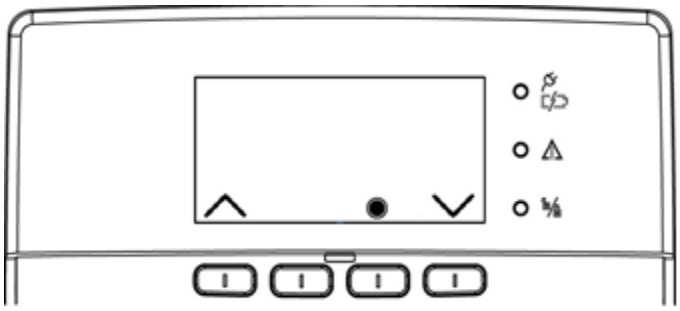
5.2.1 How to access menus

The menus can be accessed in two ways:

1. By entering an access code (Master, Installer, User or Technical Manager), then ✓;
   The displayed menu will reflect the privileges of the access code used.
2. Alternatively, press the key associated with the symbol ☰ directly.
   The free access menu described below will be opened.

5.2.2 How to navigate the menus

The menus are organised in a tree structure, i.e. with reciprocally nested submenus, each consisting of one more items. Programming is carried out using the keys and reading the messages and information which appear on the display.



IMPORTANT! The keys are associated with the respective symbols located above and shown on the display.

The submenu items differ according to the access code used and the system configuration.

For example, the respective menu items will not appear if the radio devices, interface or module radio is not installed.

Similarly, the ENABLE menu item (users, keys etc.) only appears in the Master menu and not in all the others.

The various keys used to navigate the menus are shown in the following table.

Key	Description
	It identifies a parameter and activates and deactivates a certain function associated with the relevant symbol positioned above according to the scrolling menu.
	It confirms the entered access code, accesses the displayed submenu or confirms the selection made.
	It goes back to the previous page or menu level.

Symbol shown on the display	Description
	Press the key  associated with the symbol to activate the zones.
	Press the key  associated with the symbol to deactivate the zones.
	Press the key  associated with the symbol for 3 seconds to activate the auxiliary keypad functions previously programmed (for example: "Emergency" signalling).
	Press the key  associated with the symbol to enter the menu.
	Press the key  associated with the symbol to scroll up the menu.
	Press the key  associated with the symbol to scroll down the menu.
	Press the key  associated with the symbol to scroll the menu to the right. The symbol indicates that the menu or parameter includes a submenu with multiple choice.
	Press the key  associated with the symbol to scroll the menu to the left. The symbol indicates that the menu or parameter includes a submenu with multiple choice.
 	Press the key  associated with the symbol to enable the parameter. Press the key  associated with the symbol the parameter is NOT enabled. The symbol indicates that the parameter includes a single choice.
 	Press the key  associated with the symbol to enable the parameter. Press the key  associated with the symbol the parameter is NOT enabled. The symbol indicates that the parameter includes a single choice.

A brief *beep* will be heard each time a key is pressed.

A *beep* will be heard to confirm that the entered parameter is correct, i.e. when a correct access code is entered.

A long *beep* will be heard if an incorrect parameter is entered, i.e. if an incorrect user code is entered.

5.2.3 Free access menu

Directly press the key  associated with the symbol  , to access the following menu items:

- CONTROL DEVICES
- ICON DETAIL (visible only if there are icons to be displayed)
- SYSTEM STATUS
- KEYPAD SETTING
- SYSTEM SETTING

5.2.4 Main Menu

The main menu is the first menu that is accessed after logging in. From the items in this menu you can access all the various submenus. **M =** Master – **I =** Installer – **T =** Technical Manager – **U =** User

Profile enabled for consultation	Displayed string	Additional functions		Profile enabled for consultation	Submenu Description	
M - I - T - U	System status	→	Submenu	**M - I - T - U**	This shows the system status and can be used to change the zones status.	
M - I - T - U	Keypad settings	→	Submenu	**M - I - T – U** **Attention:** the user does not see the parts marked with asterisk of the submenu on the side.	• Display Info ***** • Set Backlight • Set Contrast • Set Buzzer	• A/B/C keys ***** • Direct setting ***** • Info (KEYPAD)
M - I - T - U	System settings	→	Submenu	**M - I - T - U**	• System log This is used to read the list of events stored on the control panel, based on the entered code.	
M - I - T - U	System settings	→	Submenu	**M - I - T - U**	• Settings This is used to isolate inputs, set the current date and time, configure the users or reset codes to default value, acquire, configure and detect electronic proximity keys and transponders and configure the time scheduler.	
M - I - T - U	System settings	→	Submenu	**M - I**	• Test This is used to carry out specific tests to check perfect operation of the system. It is possible to check the inputs of the control panel inputs and of the other devices connected to the bus, the GSM signal, the phone calls and the IP interface separately.	
M - I - T - U	System settings	→	Submenu	**I**	• Programming It allows you to configure the zones of the system, the various inputs and bus peripherals, the outputs of control panel and expansions, the keypads and readers.	
M - I - T - U	System settings	→	Submenu	**I**	• Parameters - Times This is used to set the various system timers.	
M - I - T - U	System settings	→	Submenu	**M - I**	• Communicator This is used to store the phone numbers to be dialled to send alarms and indications, customise the vocal messages, associate specific alarms to each telephone number and to specify the sending methods, to set parameters of the GSM, GPRS networks and IP interface, to edit SMS messages, and to enable and configure other telephone functions.	
M - I - T - U	System settings	→	Submenu	**I**	• Maintenance This is used to carry out maintenance operations on the system, such as changing the languages, acquiring devices, deleting devices, upgrading the device firmware, resetting and saving the programmed settings. • EN50131 Event log (available only with 1068/010A control panel)	
M - I - T - U	System settings	→	Submenu	**M - I**	• SIM management It allows you to set the expiry date of the SIM card used.	
M - I - T - U	System settings	→	Submenu	**M**	• Authorisations It allows you to enable or disable a user profile to perform operations.	
M - I - T - U	Commands	→	Submenu	**M - I - T - U**	• It allows you to directly control the outputs (depending on the profile added)	
M - I - T - U	Icons detail (*)	→	Submenu	**M - I – T - U**	• Faults # • Tamper # • Time scheduler #	• Open inputs # • Isolated inputs # • Alarms #

(*) = Visible in the menu only if the (#) icons are present.

5.3 HOW TO ENTER ALPHANUMERIC CHARACTERS

The keypad can be used to enter alphanumeric characters to store descriptive names for users, zones, outputs etc. Each name can be up to 24 characters long. Press the keys to select several characters cyclically as shown on the following table. A cursor will blink on the display at the entry point of the new character.

To write a name during user configuration:

1. Press the key associated to the required character until it appears;
2. Use the key associated with the symbol < and the key associated with the symbol > to go to the previous or next string position (use the “0” key to delete characters in excess);
3. Finally, press the key ✓ to save the name or to delete everything;
4. Press the key ↩ to delete what has been entered or to quit the procedure.

Key	Character
1	. , : ; ! ? / 1
2	A B C a b c 2
3	D E F d e f 3
4	G H I g h i 4
5	J K L j k l 5
6	M N O m n o 6

Key	Character
7	P Q R S p q r s 7
8	T U V t u v 8
9	W X Y Z w x y z 9
*	*
	* " $ & ' ` { } | (characters available only for password and WiFi network name)
0	[space] + - ( ) % 0
	[space] + - ( ) % = ~ 0 (characters available only for password and WiFi network name)
#	#
	# < > @ [ ] \ ^ _ (characters available only for password and WiFi network name)

5.4 ENABLING AND DISABLING

Installers and normal users must be enabled to operate on the system. Only the Master user is always enabled. The Master can enable and disable the other users and the electronic and proximity keys and can enable and disable particular system functions.

The procedure for enabling and disabling users and key is described in detail below. During programming, users and keys are configured, i.e. it is specified what they can do. However, these "capabilities" are put on-hold until someone, namely the Master User, authorises them to use them.

Similarly, the Master User can revoke the authorisation and put the "capabilities" back on-hold at any time. Enabling and disabling means authorising and revoking authorisations.

It is important to note that disabling does not means deleting the configuration made during programming but simply suspending it. Indeed, by enabling a previously disabled User or key (electronic or proximity) these will immediately reacquire all their "capabilities".

The User code and key enabling and disabling procedures are very useful particularly in combination with the time scheduler to permit entry restricted in time to the protected rooms.

An example will help understanding the concepts of configuration, programming, enabling and disabling in greater detail.

Everyone of us has many keys: to open the gate, the garage door, the front door, the car, the basement, the utility room, the bicycle lock etc. Each key lets you open or use something. In an alarm system, you have functions which let you do something instead of keys.

A set of keys can be put on a key ring and each key ring will allow to do some things and not others. For example, we could make one set with the garage key and the bicycle padlock key and another set with the garage key and the car key. Both sets of keys will open the garage but the vehicle you can use will be different. Configuration is the equivalent for the set of keys and programming is the procedure used to make each set.

The enabling and disabling actions used for the alarm system are equivalent to giving the keys to someone or taking them away.

Enabling and disabling applies to other functions in the system, and not only users and keys. The functions can be easily made operational or not without needing to program the configurations again.

5.4.1 How to enable the Installer

The Installer must have been previously enabled to work on the system. For safety reasons, Installer enabling is cancelled whenever a User or Master code is entered or when an electronic or proximity key, remote control or wireless keypad is used.

	**IMPORTANT!** The Installer is automatically enabled each time the system is turned on.

Proceed as follows to enable the Installer:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
5. Select "**I : Installer**" by pressing the key associated with the ∨ or ∧ symbol.
6. Press the key associated with the "AUTHORISATIONS" message ☑ on the display to enable the **INSTALLER**. Press ✓ to confirm;
   ☑ = Installer enabled ; ☐ = Installer NOT enabled
7. Press ↩ repeatedly to go back to the upper level menu.

5.4.2 How to enable the technical manager

The Technical Manager must have been previously enabled to work on the system.

For safety reasons, Technical Manager enabling is cancelled whenever a User or Master code is entered or when an electronic or proximity key, remote control or wireless keypad is used.

	**IMPORTANT!** The Technical Manager is automatically enabled each time the system is turned on.

Proceed as follows to enable the Technical Manager:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Selection "**TM : Technical Manager**" by pressing the key associated with the ∨ or ∧ symbol,
6. Press the key associated with the "AUTHORISATIONS" message ☑ on the display to enable the **TECH. MANAGER**. Press ✓ to confirm;
   ☑ = Tech. Manager enabled ; ☐ = Tech. Manager NOT enabled
7. Press ↩ repeatedly to go back to the upper level menu.

5.4.3 How to enable a User

Each User must have been previously enabled to work on the system.

Proceed as follows to enable a user:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the desired user "**USXX : User X**" by pressing the key associated with the ∨ or ∧ symbol.
6. Press the key associated with the "AUTHORISATIONS" message" ☑ on the display to enable the **User**. Press ✓ to confirm;
   ☑ = User enabled ; ☐ = User NOT enabled
7. Press ↩ repeatedly to go back to the upper level menu.

5.4.4 How to enable a key

Each key must have been previously enabled to work on the system.

⚠	**IMPORTANT!** Each key must have been previously acquired to be enabled.

Proceed as follows to enable a key:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keys**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to view the available authorisations;
5. Select the key by pressing the key associated with the ∨ or ∧ symbol;
6. Press the key associated with the "AUTHORISATIONS" message on the display to enable the selected key. Press ✓ to confirm;
   ☑ = Key enabled; ☐ = Key NOT enabled
7. Press ↩ repeatedly to go back to the upper level menu.

5.4.5 How to enable the time scheduler

Proceed as follows to enable the time scheduler:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Time scheduler**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Press the key associated with the "ADVANCED" message on the display to enable the time scheduler. Press ✓ to confirm;
   ☑ = Time scheduler enabled; ☐ = Time scheduler NOT enabled
7. Press ↩ repeatedly to go back to the main menu.

5.4.6 How to enable remote access

Enabling the remote access allows access via the "Urmet secure and Urmet 1068set" Apps.

Proceed as follows to enable remote access to the system:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "ADVANCED" message ☑ on the display to enable the **"Remote access"**. Press ✓ to confirm;
   ☑ = Remote access enabled; ☐ = Remote access NOT enabled.
6. Press ↩ repeatedly to go back to the upper level menu.

5.4.7 Enabling remote unsetting

Enabling remote unsettting means being able to unset the system either totally or partially, from a distance, e.g. to allow access to the rooms even if you are not physically present.

Remote unsetting can be done through the "Urmet secure, Urmet 1068set" App, GSM answering machine.

Proceed as follows to enable remote system unsetting:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "ADVANCED" message ☑ on the display to enable the **"Remote unsetting"**. Press ✓ to confirm;
   ☑ = Remote unsetting enabled; ☐ = Remote unsetting NOT enabled
6. Press ↩ repeatedly to go back to the upper level menu.

5.4.8 Enabling anti-thieft function

Proceed as follows to enable the function anti-thieft:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "ADVANCED" message ☑ on the display to enable the **"Anti thieft"**. Press ✓ to confirm;
   ☑ = Anti thieft enabled ; ☐ = Anti thieft NOT enabled
6. Press ↩ repeatedly to go back to the upper level menu.

5.4.9 Enabling Hold-up function

Proceed as follows to enable the function Hold-up:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "ADVANCED" message ☑ on the display to enable the **"Hold-up"**. Press ✓ to confirm;
   ☑ = Hold-up enabled ; ☐ = Hold-up NOT enabled
6. Press ↩ repeatedly to go back to the upper level menu.

5.4.10 How to disable the Installer

Installer enabling is revoked whenever a User / Master code is entered or when an electronic or proximity key is used.

5.4.11 How to disable a User

Proceed as follows to disable a User:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the desired user "**USXX : User X**" by pressing the key associated with the ∨ or ∧ symbol;
6. Press the key associated with the "AUTHORISATIONS" message ☐ on the display to disable the selected user;
7. Press ✓ to confirm;
8. Press ↩ repeatedly to go back to the upper level menu.

5.4.12 How to disable a key

Proceed as follows to disable a key:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Keys**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "AUTHORISATIONS" message ☐ on the display to disable the selected key;
6. Press ✓ to confirm;
7. Press ↩ repeatedly to go back to the upper level menu.

5.4.13 How to disable the Technical Manager

Technical Manager enabling is revoked whenever a User or Master code is entered or when an electronic or proximity key is used.

5.4.14 How to disable the time scheduler

Proceed as follows to disable the time scheduler:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Time scheduler**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Press the key associated with the "ADVANCED" message ☐ on the display to disable the time scheduler;
7. Press ✓ to confirm;
8. Press ↩ repeatedly to go back to the upper level menu.

5.4.15 How to disable remote access

If you disable the remote access to the system, you will no longer be able to access the control panel via the "Urmet secure" and "Urmet 1068set" Apps.

Proceed as follows to disable remote access to the system:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "ADVANCED" message ☐ on the display to disable the **"Remote access"**. Press ✓ to confirm;
6. Press ↩ repeatedly to go back to the upper level menu.

5.4.16 Disabling remote unsetting

If you disable the remote unsetting of the system, you will no longer be able to disable the GSM answering machine via the "Urmet secure" and "Urmet 1068set" Apps.

Proceed as follows to disable remote system unsetting:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "ADVANCED" message ☐ on the display to disable the **"Remote unsetting"**. Press ✓ to confirm;
6. Press ↩ repeatedly to go back to the upper level menu.

5.4.17 Disabling anti-thieft function

Proceed as follows to disable the anti thieft function:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "ADVANCED" message ☐ on the display to disable the **"Anti thieft"**. Press ✓ to confirm;
6. Press ↩ repeatedly to go back to the upper level menu.

5.4.18 Disabling Hold-up function

Proceed as follows to disable the Hold-up function:

1. Access the **MASTER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Authorisations**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Advanced**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press the key associated with the "ADVANCED" message ☐ on the display to disable the **"Hold-up"**. Press ✓ to confirm;
6. Press ↩ repeatedly to go back to the upper level menu.

5.5 SYSTEM LOG

1068/005A Control panel

The System Log stores the last 500 events (setting, unsetting, alarm, tamper etc.) which concerned the system.

The events are stored from the most recent to the oldest, i.e. the most recent event is the one with the lowest identification number. The stored events move down by one position as a new event is added.

When the System Log reaches the maximum size (500 events), each new event will be written over the oldest stored event.

The System Log may be examined by the Master user and by the other users but may only be deleted by the Installer.

1068/010A Control panel

The System Log stores the last 1000 events (setting, unsetting, alarm, tamper etc.) which concerned the system.

The events are stored from the most recent to the oldest, i.e. the most recent event is the one with the lowest identification number. The stored events move down by one position as a new event is added.

When the System Log reaches the maximum size (1000 events), each new event will be written over the oldest stored event.

The System Log may be examined by the Master user and by the other users but may only be deleted by the Installer.

The EN50131 Event log stores the last 500 events (tamper, failures, etc.) which concerned the system.

The events are stored from the most recent to the oldest, i.e. the most recent event is the one with the lowest identification number. The stored events move down by one position as a new event is added.

When the EN50131 Event log reaches the maximum size (500 events), each new event will be written over the oldest stored event.

The EN50131 Event log can be examined only by the Installer in the maintenance menu.

IMPORTANT!

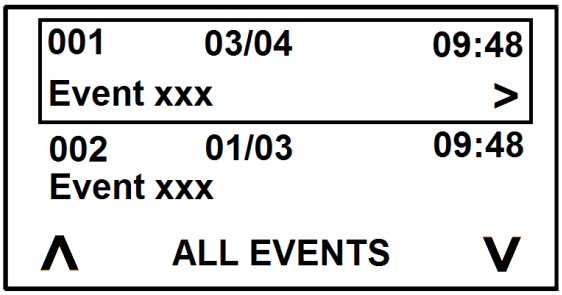
A user can only see the events related to the pertinent zones, i.e. the assigned zones.

The Master user is assigned to all zones and can always see all stored events.

Only the Installer user will be able to see technical events, such as faults and tampering.

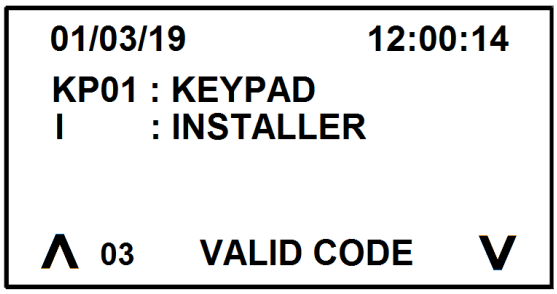
5.5.1 How to interpret viewed data

Stored event information is displayed in the Event Log as follows:



where:

- **001:** is the number of the event (001 is the most recent event, 500 is the oldest).
- **03/04:** is the date of the event;
- **09:48:** hours and minutes of the event;
- **Event xxx:** this is the type of occurred event.



where:

- **01/03/19:** it is the day, month and year of the event;
- **12:00:14:** hours, minutes and seconds of the event;
- **KP01: KEYPAD / I: INSTALLER:** detail of the individual event that occurred.

5.5.2 How to browse the System Log

Proceed as follows to browse the System Log:

1. Access the **MASTER / TECH. MANAGER / USER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**System log**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**All events**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm and view all recorded events;
5. Select "**Event filter**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm.
6. Select "**Event type**" or "**Date type**" by pressing the key associated with the ∨ or ∧ symbol to display the events according to the date or type of event. Press ✓ to confirm.
7. Press ↩ repeatedly to go back to the upper level menu.

5.5.3 How to browse the EN50131 Event Log (available only with 1068/010A control panel)

Proceed as follows to browse the EN50131 Event Log:

1. Enter the **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Maintenance**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**EN50131 Event log**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**Read event log**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select "**All events**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm and view all the details about the events;
7. Select "**Event filter**" by pressing the key associated with the ∨ or ∧ symbol; Press ✓ to confirm;
8. Select "**Event type**" or "**Data type**" by pressing the key associated with the ∨ or ∧ symbol to view events according to the date or type of event. Press ✓ to confirm;
9. Press ↩ repeatedly to go back to the upper level menu.

6 USERS

This chapter explains how to add new users.

Adding a User essentially means configuring a “User” memory of the control panel, i.e. defining whether it is associated to the entire system or only to some zones and programming a descriptive name.

The new user must be enabled after they have been created (see paragraph *5.4 Enabling and disabling).*

6.1 PREREQUISITES

6.1.1 How to assign a user

Proceed as follows to assign a User to the system (all zones):

1. Access the **MASTER / INSTALLER / TECH. MANAGER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**User configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the user you want to rename by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Zone assignment**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Select the zone(s) you wish to associate to the selected user by pressing the key associated with the ∨ or ∧ symbol.
9. Press the key associated to the ASSIGNMENT message ☐ on the display. Press ✓ to confirm;
   ☑ = assigned zone; ☐ = NOT assigned zone
10. Press ↩ repeatedly to go back to the upper level menu.

6.1.2 How to program a descriptive user name

Providing a descriptive name to a user helps to recognise the user during enabling and configuration and when reading the System Log.

Proceed as follows to assign a descriptive name to a user:

1. Access the **MASTER / INSTALLER / TECH. MANAGER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Users**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select "**User configuration**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
6. Select the user you want to rename by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Name**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Use the alphanumeric keypad to enter the name you want to associate with the selected user. Press ✓ to confirm;
9. Press ↩ repeatedly to go back to the upper level menu.

Each USER may change their name.

7 PHONE DIALER AND IP INTERFACE

IMPORTANT!

The information contained below implies that the 1068/005A or 1068/010A control panel is connected to at least one GSM phone network (via the 1068/458 module) and/or is connected to a local area network or the Internet (via the 1068/013 module).

This chapter explains how:

1. Alarm and event notifications via phone dialer and IP interface work;
2. To enter and configure a phone number or IP address so that it can receive notifications;
3. To write or delete the text that will be displayed in SMS messages (sending SMS requires the use of the 1068/458 module).

7.1 ALARM AND EVENT NOTIFICATIONS

Alarms and events can be reported via:

1. Vocal calls to suitably configured phone numbers. Vocal calls can be made from 1068/458 module;
2. SMS to suitably configured phone numbers. SMS can only be sent from the 1068/458 module;
3. Calls to surveillance centres via IDP numeric protocol. The phone numbers of the surveillance centres must be appropriately configured. IDP calls can be made from 1068/458 module. The use of module 1068/458 is not recommended, as the operation of the IDP protocol is not guaranteed on the GSM phone network;
4. Calls to surveillance centres via IDP/IP numeric protocol. The IP addresses of the surveillance centres must be appropriately configured. IDP/IP calls can be made from the 1068/458 module.
5. PUSH notifications that can be read via Urmet Secure App and Urmet 1068set App. They can only be sent from the 1068/013 module.

IMPORTANT!

It is not recommended to use the 1068/458 module to make calls with the IDP protocol. In fact, the operation of this protocol is not guaranteed on the GSM phone network.

When one or several alarms and events occur, the control panel:

1. Identifies the alarms and events with the highest priority if they are different and simultaneous;
2. Calls the numbers and IP addresses configured for that alarm event;
3. For each phone number or IP address and sending mode, in the case of different and simultaneous alarms and events, the transmitter will try to group as many as possible (in a single call or SMS). This is carried out compatibly with the restrictions of the various modes (e.g. maximum length of SMS messages);
4. In the case of vocal calls, one attempt is made for each phone number before moving to the next number. The sequence repeats up to 3 times.
5. In the case of a numeric protocol, a maximum of 3 consecutive attempts will be made for each telephone number.

The vocal call cycle can be stopped by dialling “12” on the phone which received the call after hearing the message and receiving the call block beep. When the 12 is recognised, the control panel blocks any subsequent calls.

IMPORTANT!

The sending of SMS messages and PUSH notifications and calls in numeric protocol are not affected by the entry of the code 12.

Deactivating one or more zones blocks any notification that has not been sent yet concerning intrusion alarms relating to at least one of the deactivated zones. This applies to vocal calls that have not been started yet, SMS or PUSH notifications that have not been sent yet, calls over a numeric protocol that have not been started yet.

Entering a valid code or key blocks any notification that has not been sent yet relating to at least one of the zones associated with the code or key.

7.2 PHONE NUMBERS AND IP ADDRESSES

The 1068 series control panels can store a directory of 12 elements.

Each of these elements can be configured to contain either a phone number or an IP address.

The configurations that can be modified for each of these 12 elements are as follows:

1. The phone number or the IP address and port pair;
2. Zones assignment. Only events related to the assigned zones will be reported to that element;
3. The notification sending mode;
4. The network to be used;
5. Events to be notified.

7.2.1 How to edit a phone number

Each pause lasts for 2 seconds. Simply queue pauses to obtain a longer pause. The pauses are displayed with the character "**P**".

Proceed as follows to edit a phone number:

1. Access the **MASTER / INSTALLER** menu by entering the access code**;** Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Numbers - IP address**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the number/IP address you want to change and confirm with ✓;
6. Select "**Modification**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**Number**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Enter the desired number and pauses (**P**). Press ✓ to confirm;
9. Press ↩ repeatedly to go back to the upper level menu.

7.2.2 Changing the IP address and port

An IP address is in the form xxx.xxx.xxx.xxx where xxx is a number between 0 and 255. The port is a number between 0 and 65535.

Proceed as follows to edit the IP address and port:

1. Access the **MASTER / INSTALLER** menu by entering the access code**;** Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Numbers - IP address**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the number/IP address you want to change and confirm with ✓ ;
6. Select "**Number Modification**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select "**IP address**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
8. Enter the desired IP address. Press ✓ to confirm;
9. Press ↩ repeatedly to go back to the upper level menu.

7.2.3 Zones assignment modification

The stored phone numbers may be associated to the entire system (the phone number will be used for any event) or to specific zones (the phone number will be used only for the events concerning these zones).

Proceed as follows to modify the zone assignment

1. Access the **MASTER / INSTALLER** menu by entering the access code**;** Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Numbers - IP address**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the number/IP address you want to change and confirm with ✓;
6. Select "**Zone assignment**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select the zone to be assigned and confirm by pressing the key associated with the ∨ or ∧ symbol.
8. Press the key associated to the “ASSIGNMENT" message ☐ on the display, in the box of the right column a confirmation sign ☑ will appear to indicate the assignment to the zone;
9. Press ↩ repeatedly to go back to the upper level menu.

7.2.4 Changing the sending mode

The notification sending mode can be:

1. **Vocal**. To use this mode the directory element should be configured as phone number;
2. **SMS**. To use this mode the directory element should be configured as phone number;
3. **IDP**. To use this mode the directory element should be configured as phone number;
4. **IDP backup**. An element with this programming is only used if the sending to the previous element programmed as IDP fails. To use this mode the directory element should be configured as phone number;
5. **IDP/IP**. To use this mode the directory element should be configured as IP address and port;
6. **IDP/IDP backup**. An element with this programming is only used if the sending to the previous element programmed as IDP/IP fails. To use this mode the directory element should be configured as IP address and port.

Proceed as follows to edit the sending mode:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Numbers - IP addresses**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the number/IP address you want to change and confirm with ✓;
6. Select "**Sending type**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select the desired sending type by pressing the key associated with the ∨ or ∧ symbol.
8. Press the key associated with the "SENDING TYPE" message on the display. Press ✓ to confirm;
   Sending selected = ◉ ; Sending NOT selected = ○
9. Press ↩ repeatedly to go back to the upper level menu.

7.2.5 Network modification

The networks that can be used are as follows:

1. **GSM network**. It requires the 1068/458 module and is compatible with vocal call, SMS, IDP call and IDP backup sending modes;
2. **IP network**. It requires the 1068/013 module and is compatible with IDP/IP call and IDP/IP backup sending modes.
3. **GPRS network**. It requires the 1068/458 module and is compatible with IDP/IP call and IDP/IP backup sending modes.

Proceed as follows to modify the network:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ o ∧. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Numbers - IP addresses**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the number/IP address you want to change and confirm with ✓;
6. Select "**Network type**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select the desired sending type by pressing the key associated with the ∨ or ∧ symbol.
8. Press the key associated with the "NETWORK TYPE" message on the display. Press ✓ to confirm;
   Network selected = ◉ - ; Network NOT selected = ○
9. Press ↩ repeatedly to go back to the upper level menu.

7.2.6 Changing events to be notified

To change the events that will be notified to the number or IP address proceed as follows:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Numbers - IP addresses**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the number/IP address you want to change and confirm with ✓;
6. Select "**Associated events**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
7. Select the desired event type by pressing the key associated with the ∨ or ∧ symbol.
8. Press the key associated with the "ASSOCIATED EVENTS" message on the display. Press ✓ to confirm;

   Associated event = ☑ ; NOT associated event = ☐
9. Press ↩ repeatedly to go back to the upper level menu.

7.3 SMS MESSAGES

The 1068 series control panels can send SMS messages to the programmed telephone numbers when the following alarms or events occur.

For each alarm or event it is possible to configure the descriptive text that will be added to the notification SMS.

7.3.1 Editing texts for SMS messages

Proceed as follows to edit the descriptive text of an alarm or event:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Communicator**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**SMS messages**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the type of message to edit by pressing the key associated with the ∨ or ∧ symbol.
6. Enter the desired text message and confirm with ✓;
7. Press ↩ repeatedly to go back to the upper level menu.

8 USER REMOTE CONTROL

8.1 ACTIVATION AND DEACTIVATION OF OUTPUTS WITH SMS

Outputs programmed as “commandable” can be activated or deactivated remotely by sending SMS messages. The "Incoming SMS" GSM parameter must be enabled to use this function. Furthermore, the text message must come from a known phone number, i.e. one of the 12 phone numbers stored on the control panel.

IMPORTANT!
- This number does not need to be associated to an event.
- In order for the control panel to recognise the phone number, remember to save it with the international prefix (for example 0039 for Italian numbers).

The text message to be sent to the phone number of the SIM Card of the control panel must have the following syntax:

2nns.

where:

- **nn** is the logical number from 01 to 10 of the commandable output or commandable pulse to be switched;
- **s** is a digit which represents the status that the output must assume: **1** (set) or **0** (unset). In case of pulsed commandable output only **1** (set) can be used;
- **.** (full stop) is the end of the message.

Several controls can be queued in the same text message and separated by a comma. The text message must end with a full stop (“.”).

Any spaces will be ignored, but characters other than digits, spaces, commas and full stops will be considered errors. The text message will be rejected.

EXAMPLES

SMS	Description
2031.	Correct: this message will activate logical output 03
2 03 1.	Correct: this message will activate logical output 03
2031, 2050.	Correct: this message will activate logical output 03 and deactivate logical output 05
2031	Wrong: no full stop at the end of the message
2 3 1.	Wrong: the output number is not written using two digits
2031. 2050.	Partially correct: the first command will be executed, the second one will be rejected.

The control panel will send a reply text message with the received message text and “OK” or “KO” to confirm command reception.

EXAMPLE: *Command* 2031. – *Reply*: 2031 OK. Otherwise the reply will be "2031 KO".

8.2 DEVIATION OF INCOMING SMS MESSAGES

SMS messages that are not recognised as commands can be deviated to a number in the directory by configuring the GSM parameter "SMS deviation number". The SMS can also come from numbers not present in the directory

If the GSM parameter "incoming SMS" is disabled, the commands are also deviated.

8.3 ACTIVATION OF OUTPUTS WITH FREE OF CHARGE CALLS

The outputs programmed as "commandable" can be activated remotely by means of a phone call without the caller being charged any cost. To use this function, the GSM answering machine must be enabled and the outputs that can be controlled must be associated with a known phone number, i.e. be part of the 12 phone numbers saved in the control panel.

IMPORTANT!
- The same phone number may command multiple outputs. One output cannot be commanded by multiple phone numbers.
- In order for the control panel to recognise the phone number, remember to save it with the international prefix (for example 0039 for Italian numbers).

The operating principle is the following:

1) The GSM number of the control panel is called using the phone number saved in the control panel.
2) The call is closed within the number of rings defined by the "incoming rings” GSM parameter.
3) All the associated commandable outputs are activated: the pulsed ones for the time configured (typical application of a gate opener), commutable ones or bistable ones until they are deactivated by sending the relative command via SMS.
4) To confirm reception of the command, the control panel calls the number that originally called for a few seconds, confirming the command made (eventually you must not be answered in order to avoid having the cost charged to the control panel SIM card).

8.4 REMOTE CONTROL WITH GUIDED VOICE MENU

The remote control call can be made from a landline with tone keypad (DTMF) or a mobile phone.

The GSM answering machine must be enabled to uses all functions.

If you want to use the GSM, you must program the parameter "Incoming GSM rings" to a value greater than zero.

8.4.1 Calling the GSM answering machine

Call the GSM number of the control panel and wait for a number of rings equal to the value programmed for the parameter "Incoming GSM rings". This parameter should be programmed to a value greater than zero.

8.4.2 Functions of the guided voice menu

The guided voice menu can be used to: set zones, unset zones, switch commandable outputs, isolate and enable inputs, query system status.

The system status summary sends vocal messages about: active zones, tampering or system failure status.

Proceed as follows for remote control:

1) Call the GSM phone number of the control panel from a landline or mobile phone.
2) Enter the valid code within 10 seconds on the keypad at the prompt. Enter a digit and wait for the confirmation beep before entering the next one. Enter "#" at the end of the digits.
3) You will hear a welcome message if the entered message is correct. Otherwise, try to enter the code again (up to three attempts).
4) After having been recognised you have a few seconds to enter the menu number (see *Table of List of DTMF commands*) and access the required menu directly. Otherwise, follow the vocal menu instructions to access and use the various functions.
5) Press " ***** " repeatedly to exit remote control.

	**IMPORTANT!** In remote control mode, the ***** (asterisk) key will allow you to go back to the previous menu.

8.5 LIST OF DTMF COMMANDS FOR VOCAL ANSWER MACHINE

DTMF key	Function	Accepted digits	Action
0	**Zones setting**	01-04" followed by #	Activation of entered zones (only if associated with the code used to access the answering machine).
		#	Activation of all zones associated to the code.
1	**Zones unsetting**	"01-04" followed by #	Deactivation of entered zones (only if associated with the code). "Remote unsetting" must be enabled to work.
		#	Deactivation of all zones associated to the code.
2	**Remote controls Outputs**	"01"-"99"	Selection of the output to be controlled (the output must have zones in common with the code and must be controllable).
		0 - 1	Command (0 = unset, 1 = set). If the output is pulsed commandable, the deactivation command has no effect.
4	**Input Isolation / Enabling**	"01"-"21"	Select input to be isolated / enabled (the input must have zones in common with the code and must be isolable).
		1	Input isolation.
		0	Input enabling.
9	**System status summary**		List with zone status and tamper or fault status.

Table 6 - List of DTMF commands

Examples

Key sequences	Result
0 #	System total setting.
1 0 2 0 3 0 4 #	Unsetting of zones 2, 3 and 4.
0 0 3 * 2 0 6 1 #	Setting of zone 3 and commandable output 6.

9 SYSTEM TEST

9.1 PERIODICAL TESTS

It is advisable to check perfect operation of the intrusion alarm system regularly.

The main tests are:

- Inputs
- Outputs
- Control panel Battery
- Call or SMS
- Push notification sending
- GSM field
- Radio devices (see dedicated manual)
- IP interface
- Supplementary power supply battery (available only with 1068/010A control panel)

Test the 1068 series system before prolonged absences, for example before the summer holidays.

9.1.1 Input test

Proceed as follows to test that the inputs work perfectly:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Test**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Inputs**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Press ✓ to start the test;
6. Perform a test by opening all programmed inputs;
7. Press ✓ to end the test;
8. After the control panel has performed the test, messages concerning the status of each input will be shown on the display of the keypad;
   If the *test is successful*, a "V" sign will be assigned to the input string;
   In case of *a failed test*, an "X" sign will be assigned to the input string;
9. Press ↩ repeatedly to go back to the upper level menu.

9.1.2 Output test

Proceed as follows to test that the outputs work perfectly:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Test**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Outputs**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the output you want to test by pressing the key associated with the ∨ or ∧ symbol.
6. Press the key associated with the "OUTPUT TEST" message on the display. Press ✓ to confirm and start the test;
   Test associato 1 ; NOT associated test 0.
7. Check the correct switching of the output;
8. Press ↩ repeatedly to go back to the upper level menu.

9.1.3 Control panel battery test

Proceed as follows to check the condition of the control panel battery:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Test**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select " **Control panel Battery**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;

   After the control panel has performed the test, messages concerning the status of the battery will be shown on the display of the keypad.

   In case of *failed test* one of the following text messages "Low or fault battery", "Low Battery", will be reported.

   If the *test is successful* , the message "Battery OK" will be displayed;
5. Press ↩ repeatedly to go back to the upper level menu.

9.1.4 Call test or SMS

Proceed as follows to check the sending of calls or SMS:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Test**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**Call or SMS**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Select the number to test by pressing the key associated with the symbol ∨ or ∧ symbol. Press ✓ to confirm;
6. The message "**Are you sure?**" appears on the keypad display. Press ✓ to confirm;
7. The display of the keypad will show the number that is receiving the test call, the network used and the sending type.

   For example, if the test is performed using the GSM module and the vocal sending, the following will appear on the display:

   3401234567

   GSM

   Vocal
8. Press ↩ repeatedly to go back to the upper level menu.

9.1.5 Push notification sending test

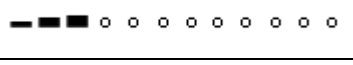
Proceed as follows to check the PUSH notification sending:

1. Access the **MASTER / INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Test**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**PUSH notification sending**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. Verify the reception of the notification on 1068set or Urmet Secure APPs;
6. Press ↩ repeatedly to go back to the upper level menu.

9.1.6 GPRS/GSM Field Test

Proceed as follows to test the GSM/GPRS field signal level:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Test**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**GSM field** " by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to start the test;
5. The system will show ***"Waiting for..."*** on the keypad display, followed by the result of the tests;
   - GSM OK / KO
   - GPRS OK / KO
   - SIM OK / KO / Not present / Invalid PIN

	Excellent signal
	Good signal
	Sufficient signal
	Poor signal

6. Press ✓ to end the test;
7. Press ↩ repeatedly to go back to the upper level menu.

9.1.7 IP interface test

Proceed as follows to check that the IP interface works perfectly:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Test**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**IP interface**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
5. The system will show ***"Waiting for..."*** followed by the result of the tests;
   - Connected or Not Connected
   - Access point or Urmet Cloud
   - IP Address
6. Press ↩ repeatedly to go back to the upper level menu.

9.1.8 Supplementary power supply battery test (available only with 1068/010A control panel)

Proceed as follows to check the condition of the control panel battery:

1. Access the **MASTER** / **INSTALLER** menu by entering the access code. Press ✓ to confirm;
2. Select "**System Settings**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
3. Select "**Test**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;
4. Select "**PS Batteries**" by pressing the key associated with the ∨ or ∧ symbol. Press ✓ to confirm;

   After the control panel has performed the test, messages concerning the status of the battery will be shown on the display of the keypad.

   In case of *failed test* one of the following text messages "Low or fault battery", "Low Battery", will be reported.

   If the *test is successful* , the message "Battery OK" will be displayed;
5. Press ↩ repeatedly to go back to the upper level menu.

10 SYSTEM SHEET

10.1 INSTALLATION DETAILS

Installation date	
Last name and first name	
Address	
Phone	

10.2 ZONES TABLE

Zone ID	Zone description	Notes
1		
2		
3		
4		
5		
6		
7		
8		

10.3 TABLE OF PROGRAMMED PHONE NUMBERS

ID	Name	Phone no.
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

11 QUICK GUIDE TO REMOTE CONTROL

Cut out the following quick reference guides along the lines to keep the list of remote control commands handy at all times. The folded guide is credit-card-sized to conveniently fit in a wallet or purse.

How to skip a telephone answering machine

Call the control panel number and hang up after the first ring.

Call the control panel back within 30 seconds.

How to manage outputs using text messages

Send a text message to the control panel in the following format: *2 nn s. ,* where *nn* is the two-digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=set; 0 =unset).

In case of pulsed commandable output only 1 (set) can be used.

Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (".").

Guided voice menu

Call the control panel from a DTMF tone phone.

Enter the valid code within 10 seconds.

Follow the vocal instructions.

Press "*****" to go back to the previous menu or to end remote control.

How to skip a telephone answering machine

Call the control panel number and hang up after the first ring.

Call the control panel back within 30 seconds.

How to manage outputs using text messages

Send a text message to the control panel in the following format: *2 nn s. ,* where *nn* is the two-digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=set; 0 =unset).

In case of pulsed commandable output only 1 (set) can be used.

Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (".").

Guided voice menu

Call the control panel from a DTMF tone phone.

Enter the valid code within 10 seconds.

Follow the vocal instructions.

Press "*****" to go back to the previous menu or to end remote control.

How to skip a telephone answering machine

Call the control panel number and hang up after the first ring.

Call the control panel back within 30 seconds.

How to manage outputs using text messages

Send a text message to the control panel in the following format: *2 nn s. ,* where *nn* is the two-digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=set; 0 =unset).

In case of pulsed commandable output only 1 (set) can be used.

Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (".").

Guided voice menu

Call the control panel from a DTMF tone phone.

Enter the valid code within 10 seconds.

Follow the vocal instructions.

Press "*****" to go back to the previous menu or to end remote control.

Cut out the following quick reference guides along the lines to keep the list of remote control commands handy at all times. The folded guide is credit-card-sized to conveniently fit in a wallet or purse.

How to skip a telephone answering machine

Call the control panel number and hang up after the first ring.
Call the control panel back within 30 seconds.

How to manage outputs using text messages

Send a text message to the control panel in the following format: *2 nn s. ,* where *nn* is the two-digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=set; 0 =unset).

In case of pulsed commandable output only 1 (set) can be used.

Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided voice menu

Call the control panel from a DTMF tone phone.
Enter the valid code within 10 seconds.
Follow the vocal instructions.
Press “*****” to go back to the previous menu or to end remote control.

How to skip a telephone answering machine

Call the control panel number and hang up after the first ring.
Call the control panel back within 30 seconds.

How to manage outputs using text messages

Send a text message to the control panel in the following format: *2 nn s. ,* where *nn* is the two-digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=set; 0 =unset).

In case of pulsed commandable output only 1 (set) can be used.

Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided voice menu

Call the control panel from a DTMF tone phone.
Enter the valid code within 10 seconds.
Follow the vocal instructions.
Press “*****” to go back to the previous menu or to end remote control.

How to skip a telephone answering machine

Call the control panel number and hang up after the first ring.
Call the control panel back within 30 seconds.

How to manage outputs using text messages

Send a text message to the control panel in the following format: *2 nn s. ,* where *nn* is the two-digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=set; 0 =unset).

In case of pulsed commandable output only 1 (set) can be used.

Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided voice menu

Call the control panel from a DTMF tone phone.
Enter the valid code within 10 seconds.
Follow the vocal instructions.
Press “*****” to go back to the previous menu or to end remote control.

Cut out the following quick reference guides along the lines to keep the list of remote control commands handy at all times. The folded guide is credit-card-sized to conveniently fit in a wallet or purse.

How to skip a telephone answering machine

Call the control panel number and hang up after the first ring.

Call the control panel back within 30 seconds.

How to manage outputs using text messages

Send a text message to the control panel in the following format: *2 nn s. ,* where *nn* is the two-digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=set; 0 =unset).

In case of pulsed commandable output only 1 (set) can be used.

Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided voice menu

Call the control panel from a DTMF tone phone.

Enter the valid code within 10 seconds.

Follow the vocal instructions.

Press “*****” to go back to the previous menu or to end remote control.

How to skip a telephone answering machine

Call the control panel number and hang up after the first ring.

Call the control panel back within 30 seconds.

How to manage outputs using text messages

Send a text message to the control panel in the following format: *2 nn s. ,* where *nn* is the two-digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=set; 0 =unset).

In case of pulsed commandable output only 1 (set) can be used.

Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided voice menu

Call the control panel from a DTMF tone phone.

Enter the valid code within 10 seconds.

Follow the vocal instructions.

Press “*****” to go back to the previous menu or to end remote control.

How to skip a telephone answering machine

Call the control panel number and hang up after the first ring.

Call the control panel back within 30 seconds.

How to manage outputs using text messages

Send a text message to the control panel in the following format: *2 nn s. ,* where *nn* is the two-digit logical number of the controllable input, *s* is a digit which represents the status that the output must assume (1=set; 0 =unset).

In case of pulsed commandable output only 1 (set) can be used.

Several controls can be queued in the same text message and separated by a comma. Each text message must end with a full stop (“.”).

Guided voice menu

Call the control panel from a DTMF tone phone.

Enter the valid code within 10 seconds.

Follow the vocal instructions.

Press “*****” to go back to the previous menu or to end remote control.

URMET S.p.A.
10154 TORINO (ITALY)
VIA BOLOGNA 188/C
Telef. +39 011.24.00.000 (RIC.AUT.)
Fax +39 011.24.00.300 - 323

Area tecnica
servizio clienti +39 011.1962.0029
http://www.urmet.com
e-mail: info@urmet.com