2CSYD0001N
2CSYD0002N

Control Unit / Control Unit with GSM

FN Installation Manual

ABB

Manual code 2CSM600500D0201 rev 00

IT

TABLE OF CONTENTS

IT

1 GENERAL INFORMATIN

1.1 Where to find information

This installation manual encompasses all information to:

- install,
- configure,
- maintain

the alarm control unit.
It also provides some suggestions to plan an intrusion alarm system, a list of the technical features of the control unit, and the procedures to be followed to isolate and solve system anomalies.
The installation manual is addressed only to the technician who will assemble the system.

Some configuration procedures are described only in the user manual.
The user manual encompasses all information for the daily usage of the control unit and for any configuration and customization that can be executed by the user as well as by the technician.

1.2 Glossary

Actuator	Electrical device that enables to indirectly operate on the working and on the control of the systems and other devices.
Buffer battery	Power source that provides power to the system for a pre-defined period of time when the mains supply is unavailable.
Home Automation	Automatic control system for home devices
I&HAS	Abbreviation for Intrusion and Hold-up Alarm System
Connector	Device that identifies a physical medium and that arms or disarms the alarm system.
Repeater	Device that receives an incoming radio signal and repeats it to increase the distance covered.
Detector	Device able to detect an anomalous condition and to generate an hazard warning signal.
Supervision	Periodic check of the correct working of the connection between the control unit and the device.
Tamper	Device that automatically detects any tampering attempts
Area	Limited area that encompasses one or more detectors in which anomalous conditions can be detected.

IT

1.3 Compliance

The control unit has been designed and manufactured according to the quality and security standards provided by the regulations and laws in force.
Qualitative requirements are certified by the affixation of the CE mark in compliance with the 1999/05/EC law.

In addition, the control unit complies with the rule EN 50131-1 grade 2 class I

Warning! Installation must be carried out only by a qualified electrician.

Remember that the above certified compliances and the product performance can be jeopardized by:

- Incorrect electrical power supply;
- Incorrect installation, or incorrect or improper usage, or anyway a usage different from the instructions explained in the installation and user manuals or from the instructions provided with the different devices;
- Replacement of original components or accessories with others not approved by the manufacturer; or replacement executed by non-authorized personnel.

In case of non-compliant configurations, the product label stating the compliance shall be changed or removed.

1.4 Disclaimer

All information in this document has been carefully selected and checked however ABB S.p.A. is not liable for any printing errors or technical inaccuracy.
ABB S.p.A. reserves the right to improve or change the products described in this user manual at any time and without any advanced notice.
Moreover, it is possible that this user manual encompasses references or information about products and services not sold yet. Such references or information do not mean in any way that ABB S.p.A. intends to sell such products or services.

1.5 Trademarks and copyright

DomusTech Free is a trademark of ABB S.p.A.
All trademarks in the document belong to the relevant owners.

CE

2 IN SHORT

This section describes the main features of the control unit and specifies the maximum sizes of the system.

2.1 Main functions

The control unit communicates with other devices of the system through radio frequencies and it provides the user with the following functions:

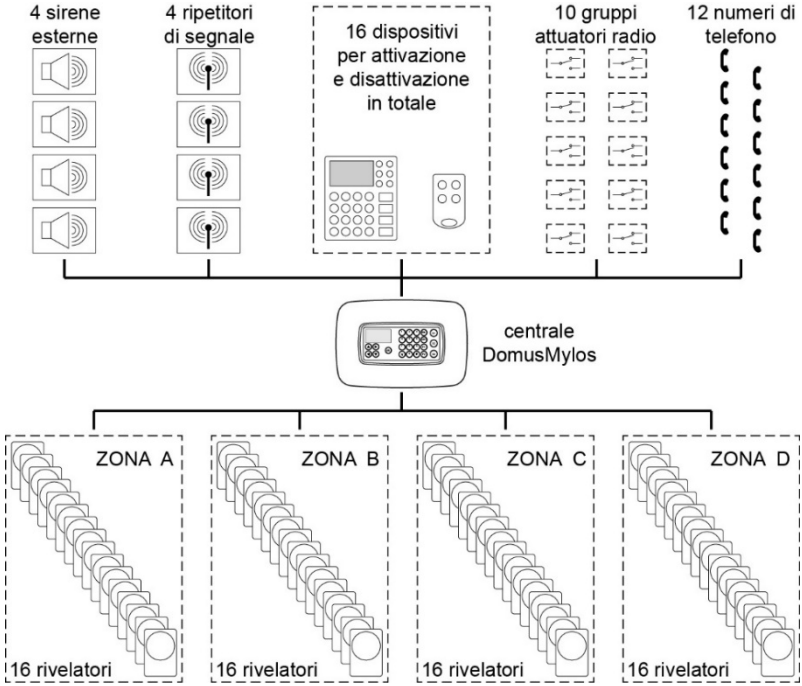
- Management of the anti-intrusion devices;
- Management of the home security devices;
- Management of anti-panic signals;
- Commands for the operation of external devices;
- Alarm notification through voice messages or SMS text messages to the programmed telephone numbers;
- Remote control of the DomusTech Free system through Home automation menu on the mobile phone or smartphone or through DTMF-tone commands;
- Gateway towards the RF Home Automation system by integrating in this way security and remote features with the Home Automation.

2.2 Main features

- Micro-processor-driven control unit with backlit 128 x 64 pixel graphic display.
- Keypad with 24 keys to program and browse the menus and the customizable quick functions.
- 4 notification LEDs.
- GSM/UMTS module for remote connection.
- 868.3 MHz radio module for bi-directional radio connection with the system devices.
- Radio communication between devices protected by a 128-bit encryption
- Cyclic supervision of the system and protection against radio jamming attempts.
- RS485 interface for the connection to optional RS485 devices.
- Built-in piezoelectric siren.
- 230 VAC power supply.
- Rechargeable NiMh buffer battery.
- Anti-tampering and anti-removal tamper.
- Compliance with the rules EN 50131-1 and EN 50131-3 Grade 2 Class I

IT

2.3 System capability



The control unit manages up to 4 programmable areas, each of them with 16 detectors for a total of max 64 detectors. The number of the actual areas is defined during the control unit configuration.
Areas can be programmed individually as:

- Intrusion alarm;
- Active H24;

The control unit manages up to:

- 4 external sirens;
- 4 signal repeaters;
- 16 devices (remote controls, radio keypads, radio connectors) to arm or disarm the intrusion alarm system;
- 10 radio actuator groups;
- 12 programmable telephone numbers to which alarm and event signals shall be sent.

IT

3 PLANNING A SYSTEM

Planning an intrusion and security alarm system with radio devices powered by a battery is simple. It is enough to follow some elementary instructions.
A good project ensures a simple installation and a good working of the system.
This section provides all information required to achieve these goals.

3.1 Information about radio waves

Systems that use radio waves to connect to devices offer the great possibility to install and connect different devices without the need for complex cabling works. Instead, they require more attention when positioning the devices in order to obtain the best radio connection.
The quality of a radio connection is directly proportional to the signal power that reaches the device. This power is affected by two factors:

- the distance between the devices (the radio signal power drops with the square of the distance),
- any signal absorption phenomena caused by obstacles along the radio wave path.

Remaining power after the radio wave absorption	Material
90-100%	Wood or plastic furniture, synthetic materials (e.g. Plexiglas), glass, hollow bricks, plasterboard
65-85%	Solid bricks, marble, aquariums
10-60%	Reinforced concrete, metallic structures (electrical household appliances, piping, railings)
0-10%	Metallic sheets, mirrors

3.2 Using areas

Areas are used to functionally group detectors for a better usage of the system. During the configuration it is possible to define the number of the areas and the relevant type.

3.2.1 Area types

Areas can be programmed as:

- Intrusion alarm: it is used to group detectors that notify intrusion attempts and that shall be activated only when it is required, usually when the area to be protected is unattended;
- active H24: it is used to group detectors that shall be always active in order to send signals related to security, e.g. flooding, smoke, and gas detectors and, in general, technological detectors;

IT

The intrusion alarm areas can be configured in the Pre-alarm, Internal Alarm (LITE) and External Alarm (FULL) modes.
In the Pre-alarm and Internal Alarm modes it is supposed that the environments are not completely disabled and therefore some signal types are not activated (external sirens and telephone messages).
Instead, in the External Alarm mode, all signals envisaged by system will be activated in case of alarm. All these activities can be configured.

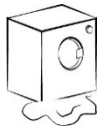
WARNING! The technical area (H24) and the Pre-alarm and Internal Alarm modes do not comply with the rule EN 50131-1.
The functions related to home security, such as flooding, smoke, and gas detectors and, in general, the technical detectors as well as the RF Home Automation functions are not covered by the rules EN 50131-1 and EN 50131-3.

3.2.2 Area subdivision

The subdivision of the intrusion alarm system into areas enables a higher management flexibility and better meets the user requirements.

For example, it is possible to link the perimeter detectors (e.g. door and window opening) to an area and the passive infrared ones to another one. In this way, the user can activate only the first area during the night, when he/she sleeps, and both areas when the house is unattended. This setting will notify the intrusion attempts when you are sleeping and, at the same time, it will enable the free movements of people within the house when necessary.

The possibility to activate or deactivate different areas is very useful also when you have a garage, a shop, an office or a lab next to your house. In this case, the possibility to link different environments to different areas enables to protect them separately with a single system by arming the anti-intrusion protection when none is in.

Example of area subdivision			
			
Area A (lab)	Area B (house)	Area C (garage)	Area D (H24)

4 INSTALLATION

This section explains how to install and connect the alarm control unit.

4.1 Positioning the Control Unit

The control unit shall be positioned:

- Indoor, in a dry place;
- At a height of about 140-160 cm on a flat wall;
- In a central position with respect to the installed devices;
- Within an area protected by anti-intrusion detectors and, if possible, not in a place of passage;
- At a distance of more than one meter from the other system devices;
- Far from any heat source (radiators, direct sun rays);
- Far from any electromagnetic interference source (electricity meter, electric engines);
- NEVER on metal surfaces.

4.1.1 Preliminary check

In case of control unit with GSM, before definitively fixing it, we suggest to execute the preliminary test related to the GSM/UMTS signal by inserting the SIM card into the control unit. For the test it is possible to use the power provided by the internal battery of the control unit.
If the level of the received signal is not proper, try to position the control unit elsewhere and execute the check again.
This preliminary test avoids to realize a new mains supply and to fix the control unit again because, after the system completion, you have discovered that the position you chose does not guarantee the proper GSM/UMTS signal level.

4.2 Connecting to the mains supply

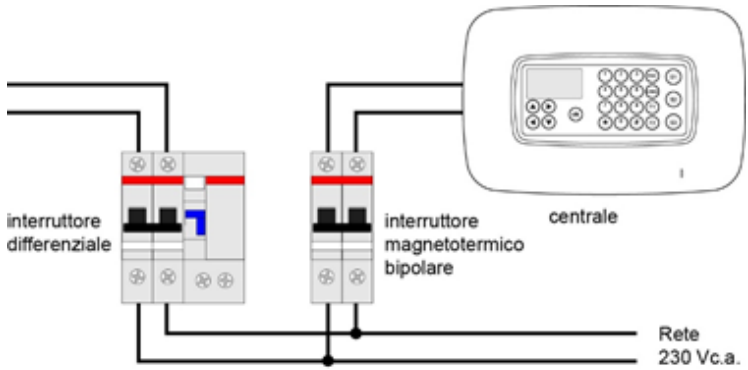
WARNING! Before executing any work on the electric system, disconnect the mains supply.

The control unit is designed to always work with the mains supply. The buffer battery guarantees up to 16 hours of operational autonomy in case of occasional power failures.

According to what specified by the rule EN 60950 related to electric security, for the 230 VAC power supply it is necessary to use a double-insulated wire (with sheathing) that shall be installed in a proper circuit-breaking device that can be easily accessed in order to protect the power supply line (bipolar magneto-thermal switch with a distance between the contacts of at least 3 mm.)

We recommend to power the control unit upstream the differential switch in order to disconnect all other electrical appliances by keeping the system operability.

IT

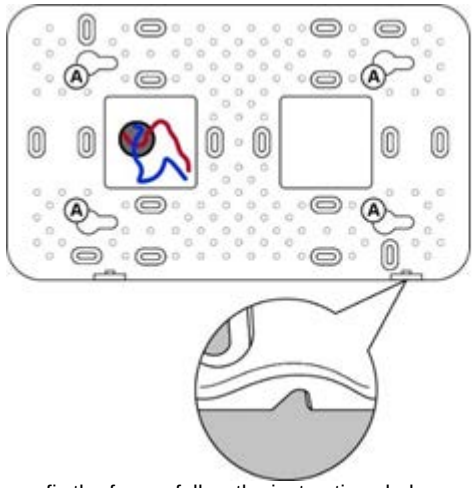


4.3 Fixing the supporting frame

Firmly fix the supporting frame of the control unit on the wall by using the prearranged slots. If the frame is placed on a wall flush-mounted box it is possible to use some slots to block it directly on the box.

WARNING! To make the fixing holes of the frame, use the drilling template provided. Once the assembly has been completed, the main part of the control unit is offset from the vertical axis of the supporting frame.

WARNING! The holes indicated with the letter A in the figure must not be used to fix the frame on the wall.



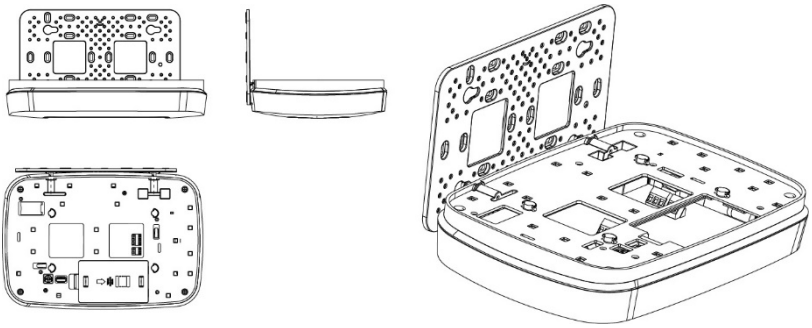
When you fix the frame, follow the instructions below:

- Place the frame horizontally, as shown in the figure, by properly positioning the top and bottom sides;

- Let the power wire and any other wires pass through the right square hole on the frame;
- Pay attention to the frame fixing direction especially to the two clamping rings that must be on the lower side when the frame is fixed.

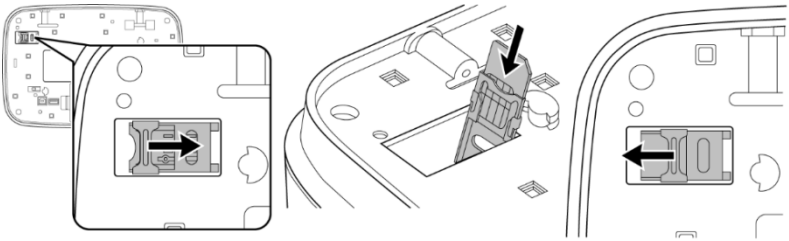
4.4 Fixing the control unit for cabling and maintenance

In order to ease the cabling and maintenance activities, the control unit can be temporarily fixed perpendicularly to the supporting frame.
In order to fix the control unit, partially extract the two fixing plugs, insert them into the two lower slots of the frame and move the control unit to right. The following figures show the end position of the control unit.



4.5 Inserting the SIM Card

The SIM Card holder is on the back of the control unit. To insert the card:

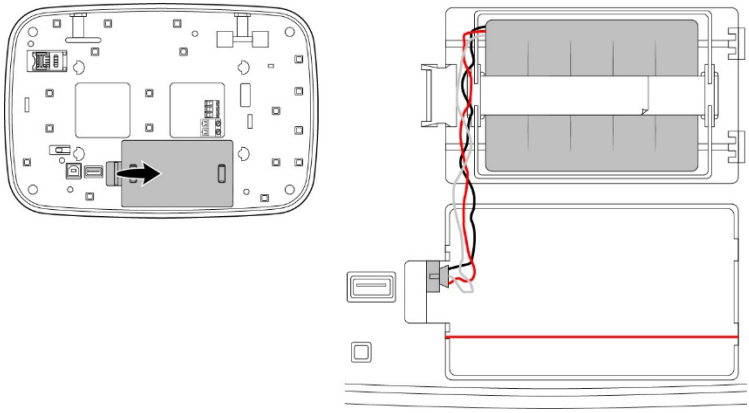


1. Unlock the SIM Card holder tray by moving the locking slide to left.
2. Raise the tray and insert the SIM Card.
3. Close the tray again and block it by moving the locking slide to right.

IT

4.6 Battery

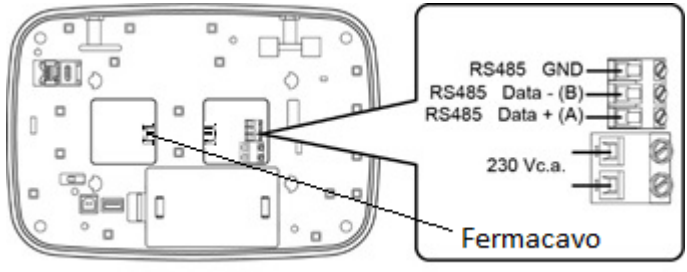
1. Open the battery holder on the back of the control unit.
2. Connect the battery pack to the polarized connector in it. The battery pack is already fixed to the cover through a Velcro strip.
3. Close the battery holder.



4.7 Mains supply and RS485 connections

The connection terminals can be easily reached from the back of the control unit.

WARNING! Be careful when you connect the mains supply (230 VAC) to the proper terminal.



Connect the control unit to the RS485 accessory device by using the RS485 terminal.

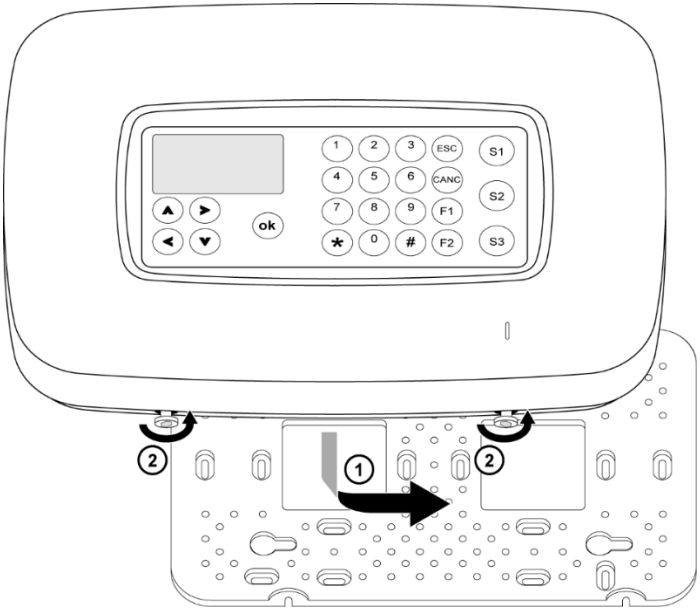
Connect the mains supply (230 VAC) to the control unit. With the clamp, fix the power supply cable to the proper cable tie as shown in the previous figure. The

control unit has a double-insulation and it does not need a PE conductor (ground connection).

4.8 Connecting the control unit to the frame

Insert the fixing pins of the control unit into the prearranged slots on the frame and let the control unit slide to the right until it stops.

Block the control unit to the frame by counter-clock rotating the two lower fixing plugs with an Allen wrench.



IT

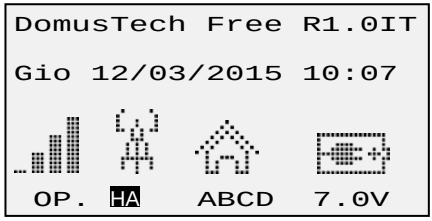
5 COMMAND INTERFACE

This section describes the control unit display and keypad, the authorization levels and how to access and browse the menus.

5.1 Display

The liquid crystal display shows information related to the configuration of the control unit and to the system working. It can encompass up to 8 text lines with 20 digits each, or a series of icons or a combination of texts and icons.
The symbol ↓ at the right bottom of the display indicates that a following page of the same section or topic is available and that it can be accessed by pressing the ⮟ key.
The symbol ↑ at the right top of the display indicates that a previous page of the same section or topic is available and that it can be accessed by pressing the ⮝ key.

Generally the display is off and it lights up when a key is pressed.



When in stand-by mode, the display shows the following information:

- firmware version and language of the control unit, at the right top (in the figure shown they are DB0.10 and IT = Italian, respectively);
- date and time;
- 4 icons that indicate - from left to right - the status of:
    - GSM/UMTS telephone,
    - Radio frequency link between devices,
    - Intrusion alarm system,
    - Control unit power supply.

IT

5.1.1 Icon meaning

Status of	Icon	Meaning
Telephone		The connection to the GSM/UMTS telephone network is working. The measured field strength is displayed through notches; the telephone service provider is also displayed.
		GSM/UMTS telephone network not identified.
		SIM Card not installed or not identified.
Radio frequency link		The radio frequency link between devices is working HA in bold: the interface to radio Home Automation is active.
		The radio frequency link between devices is not working due to jamming.
Intrusion alarm system		The intrusion alarm system is disarmed.
		The alarm system is armed in the Pre-alarm mode
		The alarm system is armed in the Internal mode (LITE). Time-bound disabled H24 area
		Alarm system armed in the External mode (FULL)
Control unit power supply		It indicates that the mains supply and the battery voltage of the control unit are available
		It indicates the battery charge status of the control unit and the relevant voltage
		Battery is missing

IT

By accessing the different menus, the display can show the following icons:

Icon	Meaning
	Arming. It enables to access the arming or disarming menu related to the whole alarm system or to single areas.
	Events. It enables to access the menu that displays the events stored by the control unit.
	System status. It enables to access the pages that summarize the working status of the alarm system.
	Panic. It enables to activate a panic alarm.
	Force block. It enables to force the block that prevents the arming of the alarm system in case of faulty detectors.
	Restore. It enables to access the menu to restore the whole system or single areas by removing any inhibition due to technical alarms, faults or tampering alarms related to the single sensors (jamming, supervision).
	Options. It enables to access the menu to adjust display, date and time.
	Programming. It enables to access the programming menu of devices and services.
	System. It enables to access the system management menu.
	Settings. It enables to access the system maintenance menu.
	Exit. It exits the main menu and brings the control unit back to the stand-by status.

5.1.2 Status of the single areas

On the display areas are identified by a letter of the alphabet in case of intrusion alarm areas or by the letter Tx for the H24 areas, where x is a numeric value (technological alarm).
If the letter (A, B, C …) is white on a black background, the intrusion alarm area is activated in the External mode (FULL). H24 areas are always white on a black background, except when they are time-bound disabled.

The lower-case letters of the alphabet (a, b, c …) on a black background indicate that the area has been activated in the Internal mode (LITE).
The lower-case letters (a, b, c …) indicate that the area has been activated in the Pre-alarm mode.

Examples

ABCT_4 Intrusion alarm areas A, B and C disarmed, technological area T4 armed.

abcT_4 Intrusion alarm areas A, B and C armed in the Pre-alarm mode, technological area T4 armed.

AbcT_4 Intrusion alarm area A armed in the External mode, B and C armed in the Internal mode, technological area T4 time-bound disabled.

ABCT4 Intrusion alarm area A, B and C armed in the External mode, technological area T4 armed.

5.2 LEDs

Next to the display, on the right, there are 4 LEDs.

	It indicates that the control unit battery is faulty.
	It indicates that there are mandatory notifications stored that have not been read yet.
	It indicates an alarm (intrusion, tampering or security). It does not indicate the Burglary alarms.
	It indicates the jamming of the system.

In case of fault or alarm the related LED is on, except when the mains supply does not work and only the battery power supply is active. In this last case, to save power, LEDs slowly blink (2 seconds on, 10 seconds off).

For transitory or temporary anomalies (e.g. lack of supervision, alarm, open entrances, etc.) LEDs automatically turned off when you read them in the attempt to arm the system.

For permanent faults (e.g. lack of mains supply or of the GSM telephone network, battery faulty etc.) the LED turns off only when the fault has been repaired (e.g. in case of mains supply return, GSM telephone network recognition, battery replacement, etc.).

5.3 Keypad

The keypad encompasses 24 keys.

IT

▲ ➤ ▼ ➤	They enable to browse menus and icons
OK	It confirms the entered or selected value. If it is pressed anywhere in the displayed menu, it saves data and goes to the higher menu level
1 2 3…0	Alphanumeric keys that enable to enter numbers or letters
*	Not used
#	It goes back to the previous menu without saving data or changes
ESC	It exits the current working session without saving. If you press it in a third-level menu it goes back to the second-level main menu from which you accessed it without losing the functions activated
F1	Contextual key that enables to activate a voice (set / reset) or to enter a configuration subpage (if the display shows the symbol ►)
F2	Contextual key used for special settings. It skips the page without saving
CANC	Deletion of a setting or of a device
S1, S2, S3	Function keys that can be customized by the user

5.4 Authentication

In order to access menus and to operate on the control unit, it is necessary to authenticate yourself by entering an ID and a password that are both numeric. The ID and the password are stored in an encrypted format. Moreover, specific authorizations, that define what a user is allowed to do, are assigned to each single user.
There are no factory default users.
The working session lasts three minutes for the 2nd level users and one hour for the 3rd level users.

5.4.1 User Identifier

The user identifier (ID) is a 1-digit numeric code ranging from 0 to 9.
ID 0 is for a 3rd level user (installer or system administrator), ID 1 is for a 2nd level user (user).
Each system envisages at least a 3rd level user and a 2nd level user.

5.4.2 Password

The password (PIN) is made up of 5 numbers and it is freely defined by the user.
The PIN can be changed only by its owner through a dedicated procedure.

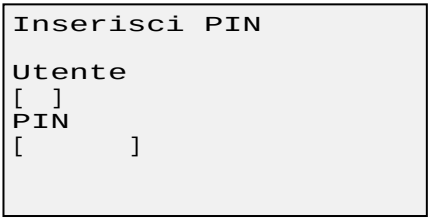
5.4.3 Authentication without existing 2nd level users

IT

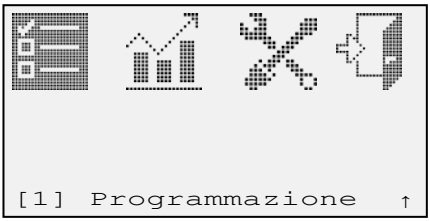
WARNING! As long as at least a 2nd level user is not created, the Installer (authorization level 3) can directly access the system without any authorization. After the creation of a 2nd level user, no 3rd level users can access the system without an authorization by a 2nd level user.

To authenticate yourself, from the stand-by window:

1. Press the **ok** key on the keypad. The authentication window is displayed.



2. Enter the ID "0" (zero). The cursor automatically moves to PIN.
3. Enter the PIN. The numbers entered are shown as asterisks (*).
4. Press the **ok** key to confirm. If the entered PIN does not encompass 5 numbers, the **ok** key is not accepted. If the user enters a wrong PIN, at the 10th attempt a tampering alarm is generated.
5. If the authentication is successful, the following screen is displayed

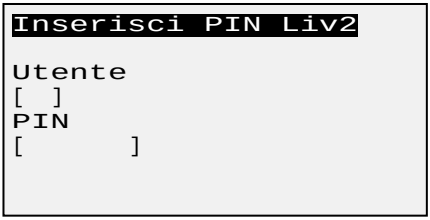


The **ESC** key enables to exit the authentication window and to go back to the stand-by window.
With the ▲ key you go back to the ID field, with the ◄ and ► keys you can browse the entered values and change them by overwriting them.

5.4.4 Authentication with existing 2nd level users

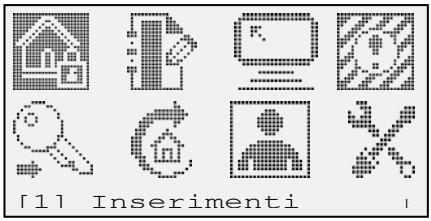
To authenticate yourself, from the stand-by window:

1. Press the **ok** key on the keypad. The authentication window is displayed.



IT

2. Enter the ID. The cursor automatically moves to PIN.
3. Enter the PIN. The numbers entered are shown as asterisks (*).
4. Press the **ok** key to confirm. If the entered PIN does not encompass 5 numbers, the **ok** key is not accepted. If the user enters a wrong PIN, at the 10th attempt a tampering alarm is generated.
5. If the authentication is successful, the following screen is displayed



The **ESC** key enables to exit the authentication window and to go back to the stand-by window.
With the ⮝ key you go back to the ID field, with the ⮜ and ⮞ keys you can browse the entered values and change them by overwriting them.

5.5 Authorization levels

The authorization level defines what a single user can do after the authentication. There are three authorization levels:

- Level 2 is divided into three sub-levels (Super-user, Standard user and Partial user) and it groups the users, i.e. those users who daily use the intrusion alarm system. The three sub-levels enable to assign different authorizations to the single users for security reasons.
- Level 3 is divided into two sub-levels (Installer and System Administrator) and it groups the users who can create or change the system configuration. The Installer is the technician who installs the system and who cannot arm or disarm the system for security reasons. There can be only one Installer for each system. The System Administrator is basically an Installer who, during the session (max 1 hour), can also arm and disarm the system to test it. In order to operate, a 3rd level user shall be previously authorized by a 2nd level user.
- Level 4. It identifies the users that can update or change the control unit firmware. As this is a critical operation required for a good working of the system, it is used to execute again and in a specific way the authentication of the user who has already authenticated himself/herself with the relevant access credentials.

The 3rd level user System Administrator and the 2nd level user Super-user correspond to the homonymous authorization levels established by the rule EN 50131-1.

The following table shows the authorizations linked to each authorization level.

Function	Access level		
	2	3	4

IT

	Super-user Type 1	Standard user Type 2	Partial user Type 3	Installer	System administrator	Maintenance man
Total arming	■				■	
Only allowed arming	■	■	■		■	
Total disarming	■				■	
Only allowed disarming	■	■	■		■	
I&HAS restoration	■	■	■	■	■	
I&HAS function check	■	■		■	■	
Event history query	■	■		■	■	
Inhibition / isolation / forcing (according to the level)	■	■		■	■	
Adding / changing single authorization codes (only the change of the personal code is allowed)	■	■	■	■	■	
Adding / removing 2nd level users and codes				■	■	
Adding / changing specific data of the site				■	■	
Changing / replacing firmware						■

IMPORTANT! As long as at least a 2nd level user is not created, the 3rd level user can directly access the system without any authorization. After the creation of a 2nd level user, no 3rd level users can access the system without an authorization by a 2nd level user.

WARNING! The access levels *2 Partial user Type 3* and *3 Installer* do not comply with the EN 50131-1 rule.

5.6 General and alarm signals

The control unit manages the alarm and anomaly situations with the following signals:

Cause	Device LED or buzzer	Control unit LED	Control unit display	Control unit buzzer	Siren	Siren flash	Voice telephone message	SMS text message
Pre-alarm	■ (1)			■				
Internal intrusion alarm	■ (1)			■	□	□		
External intrusion alarm	■ (1)			■	■	■	□	□

IT

Cause	Device LED or buzzer	Control unit LED	Control unit display	Control unit buzzer	Siren	Siren flash	Voice telephone message	SMS text message
System tampering alarm with system activated in the External mode				■	■	■	□	□
System tampering alarm with deactivated system or system activated in the Internal or Pre-alarm mode				■	□	□	□	□
Sensor tampering alarm with system activated in the External mode				■	■	■	□	□
Sensor tampering alarm with deactivated system or system activated in the Internal or Pre-alarm mode				■	□	□	□	□
Jamming alarm		■	■	■	□	□	□	□
Panic alarm				■	□	□		
Burglary alarm							□	□
Assistance alarm							□	□
Fire alarm				□	□	□	□	□
Gas alarm				□	□	□	□	□
Flooding alarm				□	□	□	□	□
Technological alarm				□	□	□	□	□
GSM is missing			■					
230 VAC mains supply is missing			■				□	□
230 VAC mains supply return			■				□	□
Low battery - devices							□	□
Device fault							□	□
Low battery – control unit		■	■				□	□
Technical assistance							□	□
Radio fault			■				□	□
Anti-theft device arming – Internal mode			■	□	□	□	□	□
Anti-theft device arming – External mode			■	■	■	■	□	□
Anti-theft device arming – Pre-alarm mode			■	□	□	□	□	□
Anti-theft device disarming			■	■	■	■	□	□
Contact ON				□			□	□
Contact OFF				□			□	□

■ factory enabled signal in compliance with the law EN 50131-1.
□ programmable optional signal

(1) if envisaged in the device

IT

6 PROGRAMMING

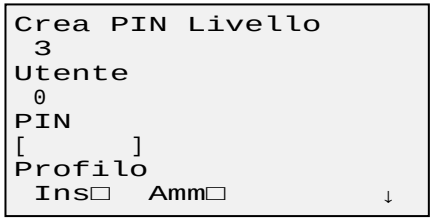
This section describes the procedures to be followed to configure the control unit. The programming is carried out by using the control unit keypad and by following the procedures described below

6.1 First switching on

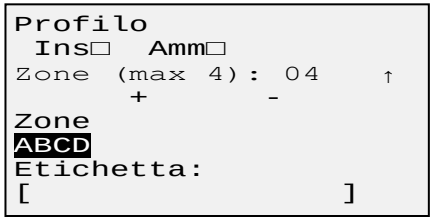
The procedure related to the first switching on is executed when you turn on the control unit for the first time or after a reset (when the factory configuration is restored). In both cases no users are stored and therefore it is necessary to create a 3rd level user (Installer or System Administrator) and a 2nd level user.

To create the first 3rd level user:

1. Press the **ok** key. The following screen is displayed



   where level (3), user ID (0) and sub-level (Profilo (Profile) Ins, i.e. Installer, or Amm, i.e. System Administrator) are already proposed.
2. With the arrow move to the field PIN and enter a 5-digit numeric code that, together with the ID 0, will represent the access credentials. The numbers entered are displayed as asterisks *.
3. If required, change the profile from Ins (Installer) to Amm (System Administrator) with the arrow keys and press the **F1** key.
4. Press the ↓ key. The following screen is displayed



   where the number of the areas that compose the system is selected. The factory settings propose 4 intrusion alarm areas.
   With the arrow keys move to + or – and change the number of the areas by pressing **F1**. To change the area type, please refer to the section System structure.

WARNING! The system must include at least an area.

IT

Tip: Keep the proposed number of areas. If you do not need an area, it is not necessary to remove it, just do not use it.
Note: also after a reset of the control unit (when the factory configuration is restored), the control unit automatically creates a configuration with 4 intrusion alarm areas.

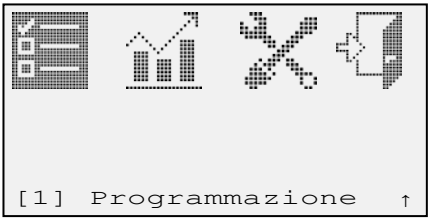
If the selected profile is Amm also the field Zone (Areas) is displayed. Area names are highlighted in negative to indicate that the user is enabled to arm and disarm them. To enable or disable an area, move on it with the arrow keys and press the **F1** key.
Through the keypad, enter a relevant name into the Etichetta (Label) field to better identify the user.

5. Press the **ok** key to confirm all selections and then create the new user.
6. After having created the 3rd level user, the control unit is in the "Installazione impianto" (System installation) mode that only enables to install and test the system and to create new users. Then the System (Impianto) screen is displayed.
   If you try to change the mode to "Operativa" (Operating) the control unit checks whether a 2nd level user has already been created and if the 2nd level user has not been created yet, it asks for the relevant creation.

WARNING! As long as a 3rd level user is not created the control unit will interpret each switching on as "first switching on" and it will behave accordingly.

6.1.1 The Impianto (System) screen

The Impianto (System) screen encompasses the accesses to the Programming, System, and Settings menus. It is the screen displayed when the 2nd level users have not been created yet and it is the second page of the main menu when 2nd level users already exist.



6.2 Following switching on

If there are not 2nd level users the "Installazione impianto" (System installation) mode is active and it enables to directly access the control unit menu as 3rd level user. To activate the "Operativa" (Operating) mode, that enables to arm and disarm the alarm system, the control unit asks to create a 2nd level user.

IT

6.3 System creation

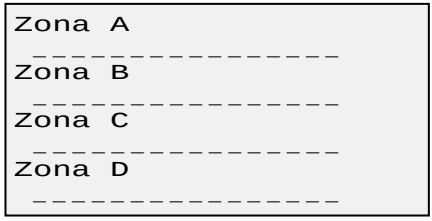
The system creation consists in the acquisition and programming of the different devices (detectors, repeaters, keypads, remote controls, connectors, control medals, sirens, actuators, chronothermostats, interfaces) and services (telephones, DTMF) required to create and configure the users and to finally test the system.
During the work session it is possible to browse backwards the menus by pressing the # key, without the need to authenticate yourself for each operation.

WARNING! If you unintentionally exit the main menu and you go back to the stand-by system screen, it will be necessary to authenticate yourself again.

6.4 Programming Detectors

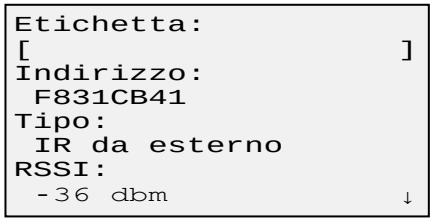
To program the detectors:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **1** or move to the Programmazione (Programming) icon by pressing the arrow keys and then confirm by pressing the **ok** key. If required, authenticate yourself again as 3rd level user.
3. Enter **1** Sensori (Sensors).
4. The list of the areas defined during the system setting is displayed. The figure shows the predefined 4 areas that can be activated.



The underscore (_) indicates a free address and the asterisks (*) a detector already entered.

5. The cursor automatically moves to the first free address. Alternatively, position the cursor on the address to be use by pressing the keys.
6. Let the control unit identify the detector by following the instructions provided with the device.
7. The underscore becomes an asterisk. Press the **ok** key to access the menu to configure the detector parameters.



The parameter list is shown on different pages. To scroll the pages use the arrow keys.
The parameters with a name displayed in negative are in read-only mode. They are:

- **Indirizzo (Address)**: detector hexadecimal address.
- **Tipo (Type)**: generic detector name.
- **RSSI**: level of the detector radio signal measured in dBm (decibel mW)
- **Ultima RX (Last RX)**: date and time of the last detector transmission received by the control unit.
- **Ripetitore (Repeater)**: ID of the used repeater, if the repeater does not directly communicate with the control unit and it communicates through a repeater. “Non impostato” (Not set) means that the detector directly communicates with the control unit.

8. Configuring parameters. The table of the following section lists all parameters for the detectors, their meaning and the relevant value.
   The alphanumeric digits are entered by using the keypad. To delete a wrong digit, by pressing the arrows position the cursor on the digit to be deleted and enter the right digit or a space to delete it. To select the value of a parameter, highlight it with the arrows and press the **F1** key.
   For the values that can be set with the buttons + and –, position the cursor on them and press the F1 key until the system displays the required value.
9. Press the **ok** key to save the configuration or the ***** key to not save the configuration. The window closes and the cursor moves to the first free address to enter the following detector.

6.4.1 Detector parameters

The table lists the possible parameters common to the different detectors. Further parameters that are specific to a single detector type are shown in the relevant detector manual.

Parameter	Meaning	Allowed values
Etichetta (Label)	It is used to better identify the detector. It is suggested to use a descriptive and unique name, e.g. KITCHEN, LIVING ROOM, BATHROOM, PORCH, etc.	Alphanumeric digits, max length 16 digits.
Escludi (Exclud)	It excludes the detector (the control unit ignores any alarm signal it sends) by keeping however the relevant configuration. It corresponds to the Insulation function as defined in the rule EN 50131-1.	SI (YES), NO
Supervisione (Supervision)	It selects the frequency at which the control unit establishes that the detector is working.	NO, 15, 30, 45, 65 minutes (1)
Ripetiz. Preallarme (Pre-alarm repetition)	Number of times that a pre-alarm is repeated if the cause that generated it persists.	3, 10, Sempre (Always)

IT

Parameter	Meaning	Allowed values
Ripetiz. Allarme (Alarm repetition)	Number of times that an (Intrusion or tampering) alarm is repeated if the cause that generated it persists. It is used to limit the number of times that the alarm beeps if the cause that generated it is not solved	3, 10, Sempre (Always)
Ritardo Ingr.(2) (Entrance delay)	Delay time between the intrusion detection and the alarm signal. It enables to enter the protected rooms and to disarm the alarm system through the control device (keypad, plug) placed within the rooms. The entrance delay time should be applied only to those detectors that cover the path between the entrance (door, garage shutter etc.) and the control device.	From 0 to 90 seconds, with a step of 10 seconds. With 0 the alarm signal is immediately activated. (2)
Ritardo Usc.(2) (Exit delay)	Delay time between the alarm system arming and the activation of the alarms in case of intrusion detection. It enables to exit the protected rooms after having armed the alarm system through a control device (keypad, plug) placed within the rooms without letting the alarm switch on. The exit delay time should be applied only to those detectors that cover the path between the exit (door, garage shutter etc.) and the control device.	From 0 to 90 seconds, with step of 10 seconds. With 0 the alarm signal is immediately activated. (2)

The underlined values are factory values.
(1) Intervals different from 15 minutes do not comply with the rule 50131-6 section 4.5.1.
(2) The programming with entrance and/or exit delay time different from 0 do not comply with the rules EN 50131-1 and EN 50131-3.

6.5 Programming Commands

To program the commands (remote controls, keypads, connectors, control medals):

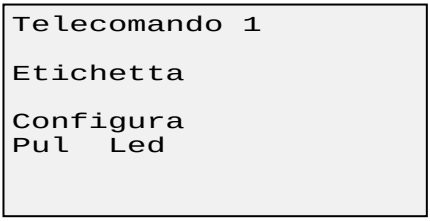
1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **1** or move to the Programmazione (Programming) icon by pressing the arrow keys and then press the **ok** key to confirm. If required, authenticate yourself again as 3rd level user.
3. Enter **1** or move to the Programmazione (Programming) icon by pressing the arrow keys and then press the **ok** key to confirm.
4. Enter **3** Comandi (Commands).
5. The command list is shown. For each command type it is possible to enter up to 16 devices.

6. The underscore (_) indicates a free address, the asterisks (*) a command already entered.
7. The cursor automatically moves to the first free address. Position the cursor on a free address of the command to be entered.
8. Let the control unit identify the command by following the instructions provided with the device.

Now you can set the command configuration that is different for each type.

6.5.1 Remote control configuration

1. Position the cursor on the asterisk (*) that identifies the remote control to be configured and then press the **ok** key. The window that enables to link a function to each key is shown.



2. With the arrows, position the cursor on the Etichetta (Label) field to set the remote control label, i.e. a name that helps to identify it more easily.
3. Position the cursor on the Pul field and press the **F1** key to set the function required for each key. Possible functions are:

Linkage type	Meaning
ZONE (AREAS)	The key arms/disarms one or more areas
FUNZIONI (FUNCTIONS)	The key activates a programmable function
N.A. (NOT ENTERED)	The key is free (it can be used for H.A.)

The selection shown on the display is the one that will be saved.

4. By selecting ZONE (AREAS) or FUNZIONI (FUNCTIONS) another screen is displayed on which it is possible to configure the required operation. Use the arrow key to move within the screen and the **F1** key to change the parameter.

IT

Areas

```
Zona A
EST INT PRE DIS CIC
Zona B
EST INT PRE DIS CIC
Zona C
EST INT PRE DIS CIC
Zona D
EST INT PRE DIS CIC
```

For each key linked to the function ZONE (AREAS) the configurations related to each single area are shown.

Display note	Description
EST	External arming (FULL)
INT	Internal arming (LITE)
PRE	Pre-alarm arming
DIS	Disarming
CIC	Cyclic: it inverts the last area status (if it is armed, it disarms it and vice versa). When the status changes from disarming to arming the last arming type of the area before the disarming is restored (FULL / LITE / Pre-alarm)

Functions

```
Rapina
NO       STA       STP
Panico
NO       STA       STP
Soccorso
NO       STA       STP
Richiesta Stato
ON       OFF
```

For each key the special function linked to it and the relevant configuration are shown.

Special function	Display note	Description
Rapina (Burglary)	STA	Alarm start
	STP	Alarm stop
Panico (Panic)	STA	Alarm start
	STP	Alarm stop
Soccorso (Assistance)	STA	Alarm start
	STP	Alarm stop

Richiesta stato (Status request)	ON	It activates the function
	OFF	It deactivates function

WARNING! For the special functions the cyclic mode is not envisaged. Therefore, it is necessary to configure two different keys on the keypad to start and stop the alarm.

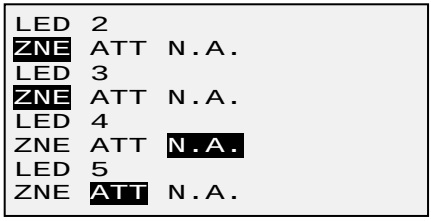
5. Configuring LEDs. It is possible to configure the LEDs 2…5 that indicate a status on the display, while LED 1 (Service) cannot be configured.
   Possible options are:
   - **ZNE**: the status of one or more areas.
   - **ATT**: the status of one or more actuators.

   The LED can light up with three different colors that are pre-defined and cannot be configured:

Color	Meaning with ZNE	Meaning with ATT
Green	Disarmed Area/s	Actuator/s OFF
Red	Armed Area/s	Actuator/s ON
Amber	Arming/disarming block	Unknown actuator status

WARNING! The control unit does not preliminary check whether there are areas, detectors, inputs or actuators.

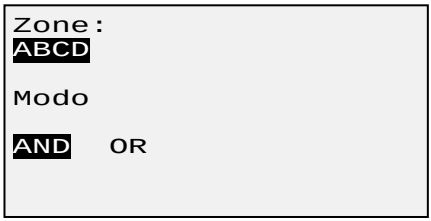
The display shows the option or the options linked to each single LED in negative (in the following figures LEDs 2 and 3 are linked to areas, LED 4 is not used and LED 5 is linked to actuators).



For each LED, position the cursor on the required option with the arrow keys and press the **F1** key to set it.

6. If more areas or detectors or actuators are linked to the same LED, it is necessary to define how it should behave. Start from the status of the single areas, detectors and actuators and combine them through the logic operators AND and OR to define the LED behavior.
   By selecting ZNE for a LED and by pressing the **F1** key a window similar to the following one is shown:

IT



On the example screen, the LED shows the status of the A, B, C and D areas by using the logic operator AND. If only an area is selected, the Modo (Modus) parameter is not shown.

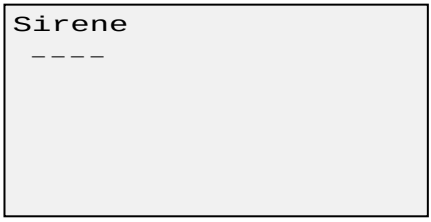
With multiple linkages and logic operators, LEDs will behave as follow:

Linkage	Logic operator	Status	LED
Zone (Areas)	AND	All disarmed areas	Green
		All armed areas	Red
		Armed and disarmed areas	Turned off
	OR	All disarmed areas	Green
		At least one armed area	Red
Actuators	AND	All actuators are OFF	Green
		All actuators are ON	Red
		Actuators ON and OFF	Turned off
	OR	All actuators are OFF	Green
		At least one actuator is ON	Red

6.6 Programming Sirens

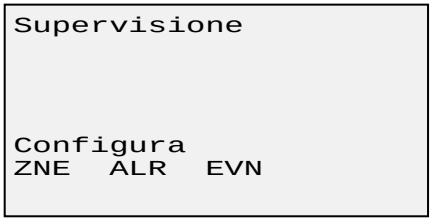
The system can manage up to 4 sirens. To program sirens:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **1** or move to the Programmazione (Programming) icon by pressing the arrow keys and then press the **ok** key to confirm. If required, authenticate yourself again as 3rd level user.
3. Enter **1** or move to the Programmazione (Programming) icon by pressing the arrow key and then press the **ok** key to confirm.
4. Enter **4** Sirene (Sirens). The siren list is shown.



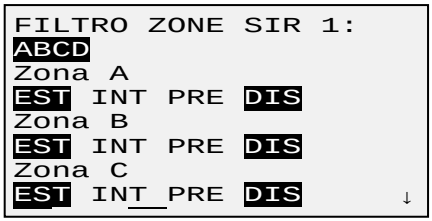
IT

5. The underscore (_) indicates a free address, the asterisk (*) a siren already entered.
6. The cursor automatically moves to the first free address. Alternatively, with the arrows, position the cursor on the address to be used.
7. Press the key Service PIN of the siren. The siren is entered.
8. With the arrow keys, select the siren just entered and press the **ok** key to configure the relevant parameters.



Supervision
It enables to select the frequency at which a control unit establishes that the siren is working. The set parameter is the time interval between a check and the following one.

ZNE
It enables to set customized filters for the siren, i.e. the conditions for which the siren emits a sound in case of alarm. The active filters are displayed in negative.



For each area (A, B, C, D in the figure) it is possible to activate different filters combined as required. The following table lists the conditions in which the sirens emits a sound.

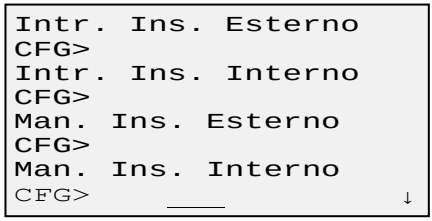
Filter	The sirens emits a sound for	Activated by the factory
EST	• Arming of the area in the External mode (FULL) • Intrusion alarm with area armed in the External mode (FULL) • Tampering alarm with area armed in the External mode (FULL)	■

IT

Filter	The sirens emits a sound for	Activated by the factory
INT	• Arming of the area in the Internal mode (LITE) • Intrusion alarm with area armed in the Internal mode (LITE) • Tampering alarm with area armed in the Internal mode (LITE)	
PRE	• Arming of the area in the Pre-alarm mode • Intrusion alarm with area armed in the Pre-alarm mode • Tampering alarm with area armed in the Pre-alarm mode	
DIS	• Area disarming • Tampering alarm related to a non-armed area	■

To change or activate a filter, position the cursor on it by pressing the arrow keys and then press **F1**.

ALR
If required, it enables to change the operating parameters, such as the sound, the duration, etc. of the siren related to alarm events (intrusion, tampering, burglary, panic, system, etc.)



It is possible to set multiple parameters for the different alarms. To configure the parameters of an alarm type, move to the corresponding CFG> with the arrows keys and press the **F1** key.
Parameters that can be changed on the displayed window are:

Alarm / event type	Sound type *	Duration / number of beeps	Volume	Warning	Warning duration	LED
Intrusion alarm – External	**1** / 2 / 3 / 4	30 s / **3 m** / 9 m **	Min / Med / **Max**	SI (YES)/ **NO**	**10** / 20 / 30 s	**SI (YES)** / NO
Intrusion alarm – Internal	1 / 2 / **3** / 4	10 s / 3 m / 9 m	Min / Med / Max / **NO**	SI (YES)/ **NO**	**10** / 20 / 30 s	**SI (YES)**/ NO

IT

Alarm / event type	Sound type *	Duration / number of beeps	Volume	Warning	Warning duration	LED
Pre-alarm	3 / **4**	3 / 10 / 20 s	Min / Med / Max / **NO**	SI (YES)/ **NO**	**10** / 20 / 30 s	SI (YES)/ **NO**
Tampering alarm – system armed in the External mode	1 / **2** / 3 / 4	30 s / **3 m** / 9 m	Min / Med / **Max**	SI (YES)/ **NO**	**10** / 20 / 30 s	**SI (YES)** / NO
Tampering alarm – system armed in the Internal mode	1 / 2 / 3 / 4	15 s / 30 s / 3 m	Min / Med / Max / **NO**	SI (YES)/ **NO**	**10** / 20 / 30 s	SI (YES)/ **NO**
Tampering alarm – disarmed system	1 / 2 / 3 / 4	15 s / 30 s / 3 m	Min / Med / Max / **NO**	SI (YES) / **NO**	**10** / 20 / 30 s	SI (YES) / **NO**
System alarm	1 / 2 / **3** / 4	15 s / **30 s** / 3 m	Min / **Med** / Max/NO	SI (YES)/ **NO**	**10** / 20 / 30 s	**SI (YES)** / NO
Panic alarm	**1** / 2 / 3 / 4	**30 s** / 3 m / 9 m	Min / Med / **Max**	SI (YES)/ **NO**	**10** / 20 / 30 s	**SI (YES)** / NO
Technological alarm	1 / 2 / 3 / 4	15 s / 30 s / 3 m	Min / Med / Max / **NO**	SI (YES)/ **NO**	**10** / 20 / 30 s	**NO**
External activation		**SI (YES)** / NO	Min / Med / **Max**			NO / **3 flashings**
Internal activation		SI (YES) / **NO**				**NO** / 3 flashings
Pre-alarm activation		SI (YES) / **NO**				**NO** / 3 flashings
Deactivation from External arming		**SI (YES)** / NO	Min / Med / **Max**			NO / **1 flashing lasting 3 s**

(*) 1 =SWEEP high frequency; 2 = SWEEP low frequency; 3 = DUAL TONE high frequency; 4 = DUAL TONE low frequency.
(**) to ensure the compliance with the rules EN 50131-1 and EN 50131-3 the activation time of the sirens shall be longer than 90 seconds and shorter than 15 minutes (except for different local or domestic regulations).
The factory settings are in bold.

IT

To change a parameter, position the cursor on it by pressing the arrow keys and then press the **F1** key.

WARNING! The ringer sound types 2, 3, 4 do not comply with the rule EN 50131-1.

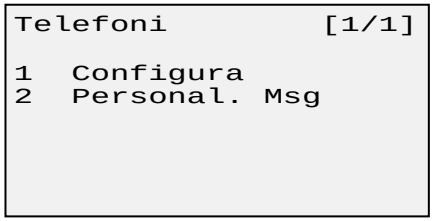
EVN
If required, it enables to change the operating parameters of the sirens related to the arming and disarming of the alarm system with a procedure similar to the previous ALR.

Press the **ok** key to save the configuration or the **#** key to not save the configuration. The window closes and the cursor moves to the first free address to enter the following siren.

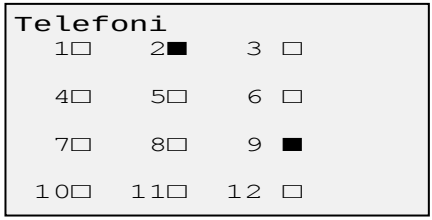
6.7 Programming Telephone numbers

The system can manage up to 12 telephone numbers. To program a telephone number:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **1** or move to the Programmazione (Programming) icon by pressing the arrow key and then press the **ok** key to confirm. If required, authenticate yourself again as 3rd level user.
3. Enter **5** Telefoni (Telephones).

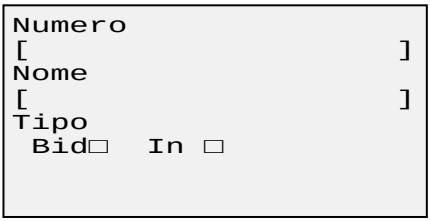


4. Enter **1** Configura (Configure). The telephone list is shown.



A non-marked square indicates a free telephone number, a marked square indicates that a telephone number is already set.

5. With the arrow keys, position the cursor on the telephone number to be set and press the **ok** key. A new window is displayed:



Configure the telephone number:

- With the keypad, enter the telephone number. The max. length is 16 digits. To delete a wrong digit go back with the arrow key and overwrite it.
- Assign a name to the telephone number in order to identify it more easily. The name can encompass up to 16 alphanumeric digits. The digits are entered by using the keypad. To delete a wrong digit, by pressing the arrows, position the cursor on the digit to be deleted and enter the correct digit or a space to delete it.
- Select the line operating type (Bid = incoming and outgoing telephone line, In = exclusively incoming telephone line) and confirm the selection with the **F1** key.

6. Press the **ok** key. If the telephone line is only for incoming calls, directly go to point 10. If the telephone line is for incoming and outgoing calls, the list of the events that can be programmed, i.e. the events that can activate the sending of a telephone message, is shown. Use the arrow keys to scroll the list.

Events that can be programmed are:

Event	Sending type	Filter
Intrusion	VOC / SMS	Alarm area
Tampering	VOC / SMS	Alarm area
Control unit tampering	VOC / SMS	
Burglary	VOC / SMS	
Assistance	VOC / SMS	
Fire	VOC / SMS	Technological area
Gas	VOC / SMS	Technological area
Flooding	VOC / SMS	
Technical assistance	VOC / SMS	

IT

Event	Sending type	Filter
230VAC is missing (*)	VOC / SMS	
230VAC return	VOC / SMS	
Technological	VOC / SMS	Technical area
Contact ON	VOC / SMS	Technical area
Contact OFF	VOC / SMS	Technical area
Low battery	VOC / SMS	
Control unit battery	VOC / SMS	
Arming	VOC / SMS	
Disarming	VOC / SMS	
Jamming	VOC / SMS	
Hardware fault	VOC / SMS	
Radio fault	VOC / SMS	

VOC indicates a voice message, SMS a text message.
(*) after 15 minutes of mains supply lack (max. delay envisaged by the rules EN50131-1 and EN50131-3 is 60 minutes)
For each event you want to program, select the sending type with the arrow keys and confirm the selection with the **F1** key. It is possible to send messages for more events to the same telephone number also with multiple sending type (voice + SMS).

WARNING! The delivery time of the SMS text message depends on how the network of the telephone service provider works and therefore it is not sure that it is sent immediately.

7. After having selected all events that can be programmed, press the **F2** key. A new window on which you can customize the sending is displayed.

```
Interrompibile
 Sì □  No □
Ritardo
 No □  20s□ 60s□
Messaggio Audio 00
  +      -
                  F2>
```

Possible options are:

- **Interrompibile (Interruptible)**: it is possible to interrupt the alarm message sending through the remote authentication of the user and the DTMF command. The factory value is No.
- **Ritardo (Delay)**: delay time between the event occurrence and the triggering of the voice call. In case of more telephone numbers the control unit executes the sequence according to the delays set in each single telephone. If for all telephone numbers there is not a delay time (setting = “immediato”(immediate)) the order followed is the one of the identification 1, 2, 3, 4 etc. The delay time enables to create a priority order according to which the telephone

numbers called can intervene and block the call sequence if required. The factory value is No (no delay).

- **Messaggio Audio (Voice Message)**: identification number of the pre-recorded personal message that will be sent. The voice message follows the generic pre-recorded message that identifies the event type that caused the message sending.

To select the value of a parameter, highlight it with the arrows and press the **F1** key.
For the values that can be set with the + and - keys, position the cursor on them and press the F1 key until the required value is displayed.

8. Press the **F2** key. A new window is displayed on which it is possible to define how events should be filtered (arming, disarming, intrusion, tampering) in order to send the telephone message.

```
Filtro Ins.
 SET►
Filtro Disins.
 SET►
Filtro Intrus.
 SET►
Filtro Manomis.
 SET►
```

9. With the arrow keys, position the cursor on the filter to be configured and press the **F1** key. A new window, that is different for the various filters, is displayed.

Arming and disarming

```
Utenti (pin)
 ..........
Tastiere
 ................
Telecomandi
 ................
Inseritori
 ................
```

The dot digit (.) indicates an empty memory position, the asterisks (*) indicates an existing and filtered user or command, the digit (-) indicates an existing and non-filtered user or command. A user or command is considered as filtered when its alarm system arming or disarming activity generates the sending of the relevant SMS text message. To filter or not filter a user or a command, select it with the arrow keys and press the **F1** key.
Press the **ok** key to save the new configuration.

Intrusion and tampering

IT

```
Allarme Esterno
 ABCD
Allarme Interno
 ABCD
Preallarme
 ABCD
```

The filtered areas are highlighted in negative. To filter or not filter an area, select it with the arrow keys and press the **F1** key.
Press the **ok** key to save the new configuration.

Go to point 12.

10. If the telephone number is enabled only for incoming calls, the following screen is displayed:

```
Feedback SMS
 Sì □  No □
Richiamata
 Sì □  No □
```

The parameters to be configured are:

- **Feedback SMS (SMS feedback)**: when an incoming call is received, the control unit confirms it by sending an SMS text message to the calling number.
- **Richiamata (Recall)**: after having received the incoming call, the control unit will recall the calling number and it will ring three times.

WARNING! The calling number shall not be hidden.

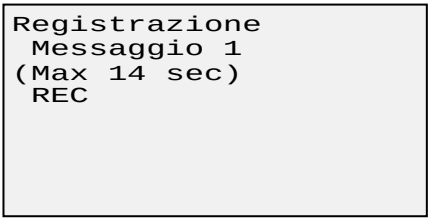
11. Select the required parameter values with the arrow keys and confirm the selection with the **F1** key. Press the **ok** key to save the new configuration.
12. Go back to the initial window.

```
Telefoni          [1/1]

1  Configura
2  Personal. Msg
```

13. Enter **2** Personal. Msg. (Customize message). A list of the messages is displayed. It is possible to record up to 9 different messages, each lasting 14 seconds.

If it is set, the personal message follows the specific pre-recorded message that the control unit sends after an event.
The message shall always indicate the place in which the event occurred. For example, a generic personalized message could be “at Mr. Smith house, Queensway 24, London”

14. Enter the number corresponding to the message to be recorded. The recording window is displayed.



15. Press the **ok** key to start recording. Wait for 2 seconds and start speaking.
16. REC becomes STP. Press the **ok** key again to interrupt the recording.
17. To check the recording quality, send the voice message from the menu Prova Sistema -> Telefoni (System test -> Telephones).

6.7.1 Sending sequence of the telephone messages

SMS text messages are sent immediately to all configured telephone numbers.

Voice calls follow the rules below:

- The numbers programmed as “voice” are called in sequence after the delay time defined through the “Ritardo” (Delay) parameter on each of them. The calling order is defined by the delay parameter. For example, if telephone 1 is programmed with a delay of 60 seconds, telephone 2 immediately, telephone 3 with a delay of 20 seconds and telephone 4 immediately, the control unit will call the telephone numbers with this sequence: 2-4-3-1.
- If the telephone number is busy or it does not answer within 4 rings, the control unit interrupts the calling and calls the following telephone number in the sequence.
- Once the first calling cycle ends (all active telephone numbers), the control unit tries to call again the numbers that did not answer. The control units

IT

executes 3 calling cycles with the numbers that did not answer before interrupting the message sending sequence. During the calling attempts the programmed delay time is not followed.

- The voice message is repeated 3 times before the control units hangs up. The sent message encompasses a pre-recorded part related to the event that caused the voice call and a variable part linked to the first one that can be a recorded personalized message or, if it does not exist, the generic indication “presso impianto antifurto” (at the anti-theft system).

6.7.2 Receipt of telephone calls by the control unit

When you connect to the control unit through a telephone, the following rules are valid:

- Tones are always accepted even if the calling telephone number does not correspond to one of the 12 numbers in the list. The unique exception is that the calling telephone number is programmed in the control unit just for incoming calls; in this last case the control unit does not manage tones.
- If during the programming of the telephone numbers with only incoming calls the function “Feedback SMS” (SMS Feedback) is enabled, the control unit executes the command linked to that telephone number without answering. Tones are actually disabled. This is, for example, an alternative to the remote control usage.
- If during the programming of the telephone numbers with only incoming calls, the function “Richiamata” (Recall) is enabled, the control unit – after having executed the linked command - let the calling telephone ring three times and in case of answer it lists the status of the executed operation.

7 HOME AUTOMATION

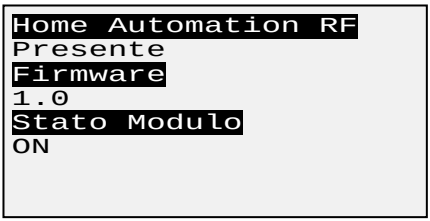
This section shows the integration of the RF Home Automation within the system.

7.1 Gateway information

To display the gateway information:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **1** or move to the Programmazione (Programming) icon by pressing the arrow keys and then press the **ok** key to confirm. If required, authenticate yourself again as 3rd level user.
3. Enter **6** Automazione (Automation).

4. Enter **2** Info Gateway (Gateway info). The relevant information is displayed (in read-only mode).



Home Automation: it identifies the Home Automation system type and it indicates whether it is present.
Firmware: it shows the installed firmware version
Stato del modulo (Module status): it indicates whether the gateway is switched on (ON) or switched off (OFF).

7.2 RF Home Automation

The radio-frequency actuators shall be programmed and linked to the commands of the control unit.
The RF Home Automation manages the devices through channels, i.e. through addresses to which an actuator or an actuator group corresponds.
The RF Home Automation programming requires two steps:

- The configuration of the channels or of the security scenario;

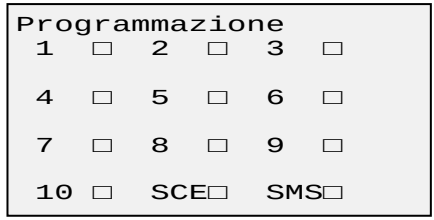
- The entry of one or more Home Automation devices.

7.2.1 Channel configuration

To configure a channel:

1. Authenticate yourself on the Impianto (System) screen.
2. Enter **1** or move to the Programmazione (Programming) icon by pressing the arrow keys and then press the **ok** key to confirm. If required, authenticate yourself again as 3rd level user.
3. Enter **6** Automazione (Automation).

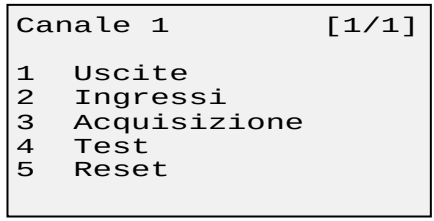
4. Enter **1** Programmazione (Programming).



With the arrows, select the channel (**1…10**) or the security scenario (**SCE**).

Press the **ok** key to confirm.

5. The following screen is displayed:



6. Enter **1** Uscite (Outputs).

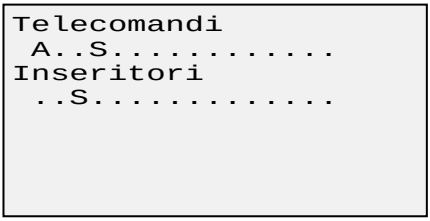
With the arrows, select the required output type and press the F1 key to confirm. The output is marked and the mark on the previous type is deleted. Press the **ok** key to confirm the selection.

7. Enter **2** Ingressi (Inputs).

By linking an input to the channel the activation mode or the control mode of the outputs linked to the relevant channel is defined.
It is possible to link different input types to a channel, each of them will have the same effects on the output.
By entering the number of one of the menu items, the system displays the relevant configuration screens explained below.

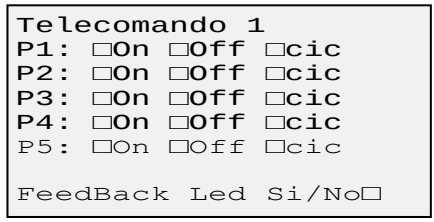
Commands
It enables to set the remote controls and the connectors as input for the channel.
The first screen enables to select the command type:

- **.** (dot) indicates a free address (device not entered);
- **A** indicates a command available for the Home Automation;
- **S** indicates a command completely linked to areas or to security functions (panic or silent alarms) that are therefore not available for the Home Automation.



With the arrows, select the required command (it shall be marked by the letter A) and confirm the selection by pressing the **ok** key. The configuration window is displayed:

IT

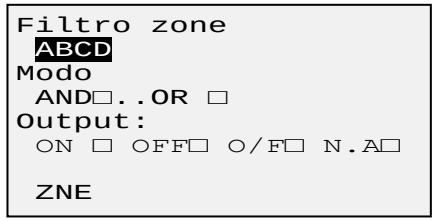


Only free keys or keys already used for the Home Automation are displayed. The set operation type is highlighted by a tick.
Select the required key and the operation type with the arrow keys and press the **F1** key to confirm the selection. The possible selections depends on the actuator type:

- **On**: it "switches on" the actuator.
- **Off**: it "switches off" the actuator.
- **Cic**: it inverts the actuator status (if it is switched off, it switches it on and vice versa). It is displayed only with the switches.
- **SU (UP)**: it lifts the shutter or it increases the dimmer.
- **GIU (DOWN)**: it lowers the shutter or it decreases the dimmer.

If you set FeedBack Led to Sì (Yes) the remote control will light up enough to receive the answer by the actuator.
Press the **ok** key to confirm the selections.

Status
It enables to set the status change of the control unit as input for the channel.

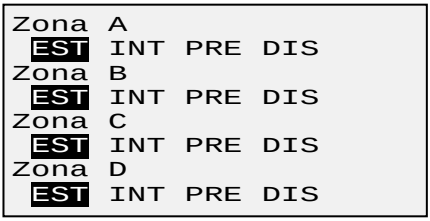


The parameters that can be configured are:

- **Filtro zone (Area filter)**: it highlights the reference anti-intrusion areas with a white digit on a black background. As pre-defined option all areas have been selected.
- **Modo (Modus)**: it indicates how the area status shall be in order to activate the output. With AND all relevant areas shall have the programmed status, with OR just a single area is enough.
- **Output**: it dynamically indicates the possible operation type (ON it switches it on; OFF it switches it off; O/F it switches it on when the anti-intrusion alarm is armed, it switches it off when the anti-intrusion alarm is disarmed; SU (UP) it lifts the shutter or it increases the dimmer, GIU (DOWN) it lowers the shutter or it decreases the dimmer).

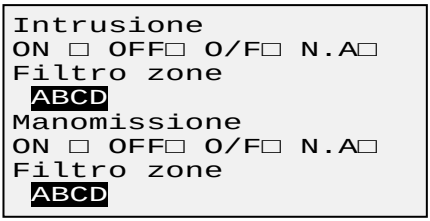
With the arrow keys, select the relevant parameter and press the **F1** key to change its status.

By selecting ZNE and by pressing **F1** a new screen is displayed on which only the selected areas with Filtro zone (Area filter) are shown.



By pressing the arrow keys and the **F1** key**,** for each area it is possible to select the status change type that causes the actuator activation (EST = External alarm arming, INT = Internal alarm arming, PRE = pre-alarm arming, DIS = disarming).
Press the **ok** key to store the changes made.

Alarms
It enables to set the alarms generated by the control unit as input for the channel.

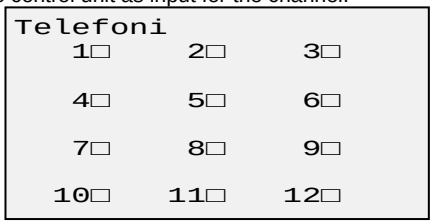


Alarms that can be configured are Intrusion, Tampering, Technological, System alarm, Panic, Assistance. Use the arrow keys to scroll the alarm list.
For each alarm type it is possible to define the operation type of the actuator (ON it switches it on; OFF it switches it off; O/F it switches it when the anti-intrusion alarm is armed, it switches it off when the anti-intrusion alarm is disarmed; SU (UP) it lifts the shutter or it increases the dimmer, GIU (DOWN) it lowers the shutter or it decreases the dimmer, N.A ignores the alarm). The available operation type dynamically depends on the output type
You can set multiple selections, i.e. more alarm types can control the channel actuator also in a different way.
For the Intrusion, Tampering and Technological alarms, through the function Filtro Zona (Area Filter) it is also possible to select the alarm of what areas shall be considered.
To configure an alarm, select the relevant operation type with the arrow keys and confirm the selection by pressing the **F1** key (with Filtro zone (Area filter) the F1 key includes or excludes the area).
Press the **ok** key to store the changes made.

Ring

IT

It enables to set the calls received by one or more telephone numbers stored in the control unit as input for the channel.



When a call is received, the command type selected - ON, OFF or CIC - is sent to the actuators.
To configure the ring input, select the telephone number and press the **F1** key to change the relevant setting. Repeat the operation for the other telephone numbers.
Scroll the screen with the arrow keys, select the required command type (ON, OFF or CIC) and confirm the selection with the **F1** key.
Press the **ok** key to store the changes made.

7.2.2 SMS linkage

It is possible to enable or disable the linkage of a channel to the received SMS through the domotic menu. The linkage between the SMS and the channel is fix.

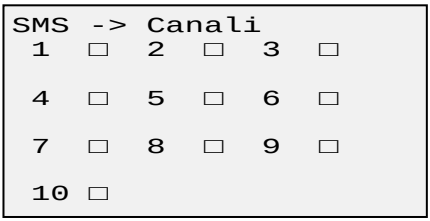
SMS	Control unit
Com1	1
Com2	2
Com3	3
Com4	4
Com5	5

SMS	Control unit
Com6	6
Com7	7
Com8	8
Com9	9
Com10	10

The operation type activated by the SMS is defined by the output configuration (switch or shutter or dimmer or scenario) of the linked channel:

Parameter	Output type			
	Switch	Shutter	Dimmer	Scenario
1	ON	Su (Up)	Increases	ON
0	OFF	Giù (Down)	Decreases	-
2	Status	-	-	-

To enable or disable the SMS-channel linkage, select **SMS** with the arrow keys on the Programmazione (Programming) screen (please refer to the section Channel configuration, point 4) and press the **ok** key to confirm. The following screen is displayed:



The enabled linkages are marked. The control unit is issued by the fabric with all linkages disabled.
With the arrow keys, select the SMS-channel linkage to be enabled or disabled and press the **F1** key to change the status. Repeat the operation if there are other linkages whose status has to be changed.
At the end, press the **ok** key to confirm the changes made.

7.2.3 Entry of Home Automation devices

To link a Home Automation device to a channel of the control unit:

1. Prepare the device to be programmed by following the instructions provided in the device manual.
2. Open the channel programming menu (follow the section Channel configuration up to point 5).
3. Enter **3** Acquisizione (Entry).
4. The control unit sends the Reset Canale (Channel reset), Config(urazione) (Configuration) and Link commands one after the other by displaying the answer received by the device: OK indicates that the command has been successfully executed, ERR indicates that an error occurred.

Possible error causes are: switched off device, faulty device, device too close to the control unit (< 50 cm), etc.

7.2.4 Test

To execute the Home Automation actuator test:

1. Open the channel programming menu (follow the section Channel configuration up to point 5).
2. Enter **4** Test.
3. The control unit executes the diagnostic analysis of the channel and sends the command set for the output in order to visually enable the correct working (e.g. the light turns on, the shutter is lifted etc.) of all actuators belonging to the channel.

7.2.5 Change

To change an output or an input, follow the channel configuration procedure by using the relevant sub-menus.

IT

7.2.6 Channel reset

To reset the Home Automation channel:

1. Open the channel programming menu (follow the section Channel configuration up to point 5).
2. Enter **5** Reset.
3. The control unit deletes all linkages related to the channel

WARNING! The channel reset cannot be cancelled.

8 SYSTEM CONFIGURATION

IT

This section describes the procedures used to configure the system, to test it, to manage and change the access codes, to check the SIM Card credit and to set the supervision.

8.1 Control unit adjustments

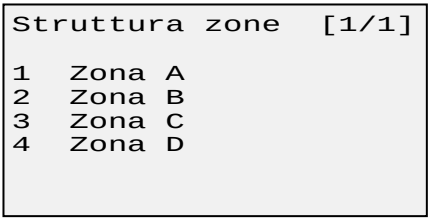
For the procedures used to adjust the date and time, the display lightness, siren volumes and duration, please refer to the User manual.

8.2 System structure

The system structure is defined when you switch on the system for the first time. However, it is possible to change the structure in a later moment by changing the relevant type. Changes executed after the programming can cause the re-alignment of the configuration, where possible, or the deletion of all configurations executed with regard to the changed area(s).

To change the system structure:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **2** or move to Sistema (System) icon with the arrow keys and then press the **ok** key to confirm.
3. Enter **1** Struttura impianto (System structure).



4. Enter the number of the relevant area.

Assign a name to the area (Etichetta (Label)) in order to identify it more easily. The name can encompass up to 16 alphanumeric digits. Digits are entered by using the keypad. To delete a wrong digit, by pressing the

IT

arrows position the cursor on the digit to be deleted and enter the correct digit or the space to delete it.
Select the area type (24h = technical area, Ins = intrusion alarm area) and confirm the selection with the **F1** key.

5. Press the **ok** key to save the changes or the # key to delete them and to go back to the previous menu.
6. Repeat from point 4 to change the other areas.

WARNING! The technical area (24h) does not comply with the rule EN 50131.

8.3 System test

The whole system shall be tested at the end of the installation activity and also later on a regular basis, at least every 6 month, in order to check that all relevant devices and functions properly work.

It is possible to test only one sub-system or only some sub-systems to check if they work. The partial test is useful in case of limited changes to the system that are relevant for only one device or one of its functions.

The inactivity allowed for the System test function is 10 minutes. After 10 minutes the system goes back to its standard working. Each time you execute a test, e.g. you check a detector that sends a replay signal to the control unit, the countdown starts again from 10 minutes.

To test the alarm system:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **2** or move to the Sistema (System) icon by pressing the arrow keys and then press the **ok** key to confirm.
3. Enter **2** Prova Sistema (System test).

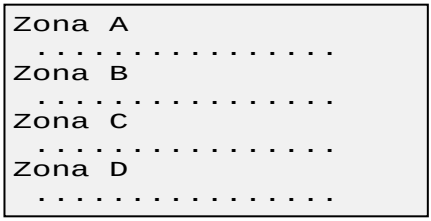
```
Prova Sistema  [1/2]

1  Sensori
2  Ripetitori
3  Comandi
4  Sirene
5  Telefoni
6  DTMF
```

Select the sub-system to be tested by entering the relevant number. If the sub-system does not encompass devices the selection is ignored.

4. According to the sub-system selected, new windows will be displayed and it could be necessary to execute some operations to activate the relevant devices.

Detectors
After having selected **1** Sensori (Sensors) as sub-system, properly perform the following activities on the various detectors, i.e. pass by the IR

detectors, open and close doors and windows for the magnetic contacts, spill water for the flooding detectors, etc.



All possible detectors are listed for each area. The digits displayed have the following meaning:

- **.** (dot): free address (detector not present).
- **1**…**9**: successful test. The number indicates the quality of the radio connection.
- **!** (exclamation mark): an anomaly has been detected.

By highlighting with the arrow keys the position of the detector and by pressing the **ok** key**,** a new detail window is displayed that - for diagnostic purposes - shows:

- The hexadecimal address of the detector.
- The signal level.
- The detector name.
- The detector status. The meaning of the abbreviations displayed is:
  - ALRM Detector in alarm status
  - ON Detector open contact
  - OFF Detector closed contact
  - MAN. Anti-opening tampering
  - RIM. Anti-removal tampering
  - BATT Low battery
  - GST Generic fault
  - SVIS Supervision anomaly
  - ESCL Detector excluded (it corresponds to the “isolated detector” as defined by the rule EN 50131)
- Re-creation date and time.

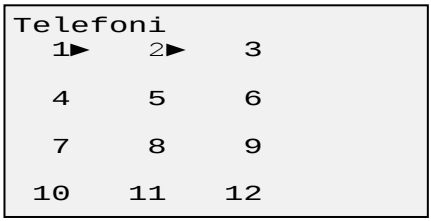
Sirens

After having selected **4** Sirene (Sirens) as sub-system, select the relevant device from the list and press the **ok** key.
The selected siren emits a bi-tonal sound, with a medium volume, for 10 seconds and the relevant LEDs blink.

Telephones

After having selected **5** Telefoni (Telephone numbers) the list of all available telephone numbers is displayed. The configured numbers are highlighted by the symbol ►.

IT



Select the required telephone number and press the **ok** key.

With the arrow keys, select the event type and the sending type to be tested.
The activated sending types for the different alarm signals are highlighted in negative. With the arrow keys, position the cursor on the required one and press the **ok** key. The control unit will send the specific alarm communication to the telephone number with the selected modality.

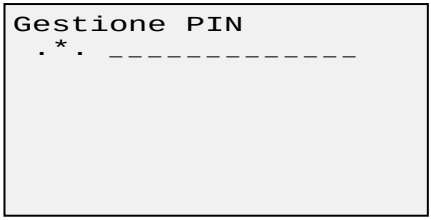
8.4 User management

It is possible to create new users and to delete existing ones. For further information about the authentication criteria of the users and about the authorizations linked to them, please refer to the sections Authentication e Authorization levels.

8.4.1 Creating a new user

To create a new user:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **2** or move to the Sistema (System) icon by pressing the arrow keys and then press the **ok** key to confirm.
3. Enter **3** Gestione PIN (PIN management).



Each dot (.) indicates an already used position, the asterisk (*) the current memory position, the underscore (_) a free position.

4. Move to a free position with the arrow keys and press the **ok** key. Authenticate yourself as 3rd level user.

The used positions are indicated by an * (asterisk).

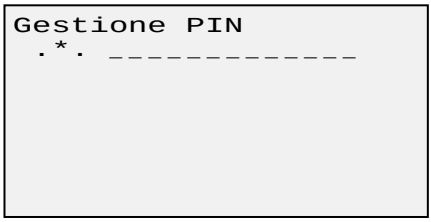
5. Select a free position (_) and press the **ok** key. On the following windows select or enter the following parameters:
   - **Crea PIN Livello (Create Level PIN)**: select a user level (2, 3 or 4) by entering the number of the level, and confirm it by pressing the **ok** key. The control unit automatically assigns the ID to the user.
   - **PIN**: enter a user-defined password encompassing 5 numbers.
   - **Profilo (Profile)**: within the same level, it identifies the users with different authorizations. The 2nd level profile can be of type Sup = Super-user, Nor = Standard user, Par = Partial user. The 3rd level user can be Amm = System administrator or Ins = Installer. The Ins profile is available only if it has not been created yet (the system can encompass only one Ins profile). Highlight the required profile with the arrow keys and confirm it by pressing the **F1** key.
   - **Zone (Areas)**: they are areas on which the user you are creating can operate. As predefined condition, the user can operate on all areas. With the arrow keys move to the required areas and enable or disable them with the **F1** key.
   - **Etichetta (Label)**: Assign a specific name to the user (e.g. name, surname or both) in order to identify him/her more easily. The name can encompass up to 16 alphanumeric digits. The digits are entered by using the keypad. To delete a wrong digit, by pressing the arrows, position the cursor on the digit to be deleted and enter the right digit or a space to delete it.
6. Press the **ok** key to save the new user or the **#** key to exit without saving.

8.4.2 Changing an existing user

To change an existing user:

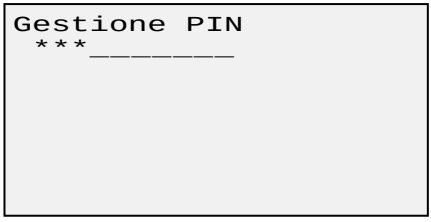
1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **2** or move to the Sistema (System) icon by pressing the arrow keys and then press the **ok** key to confirm.
3. Enter **3** Gestione PIN (PIN management).

IT



Each dot (.) indicates an already used position, the asterisk (*) the current memory position, each underscore (_) a free position.

4. With the arrows move to the required memory position and press the **ok** key. Authenticate yourself as 3rd level user.



The used positions are indicated by an * (asterisk).

5. Select the required memory position displayed by an * (asterisk) and press the **ok** key. On the following windows it is possible to change the parameters below:
   - **Profilo (Profile)**: within the same level, it identifies the users with different authorizations. The 2nd level profile can be of type Sup = Super-user, Nor = Standard user, Par = Partial user. The 3rd level user can be Amm = System administrator or Ins = Installer. The Ins profile is available only if it has not been created yet (the system can encompass only one Ins profile). Highlight the required profile with the arrow keys and confirm it by pressing the **F1** key.
   - **Zone (Areas)**: they are areas on which the user you are creating can operate. As predefined condition, the user can operate on all areas. With the arrow keys move to the required areas and enable or disable them with the **F1** key.
   - **Etichetta(Label)**: Assign a specific name to the user (e.g. name, surname or both) in order to identify him/her more easily. The name can encompass up to 16 alphanumeric digits. The digits are entered by using the keypad. To delete a wrong digit, by pressing the arrows position the cursor on the digit to be deleted and enter the right digit or a space to delete it.

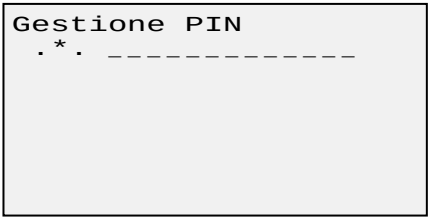
WARNING! The changing procedure does not enable to change the authorization level of the user or his/her password (e.g. in case he/she forgot it). To execute such changes the only possibility is to delete the existing user and to create it again with the new configurations.

6. Press the **ok** key to save the new user or the # key to exit without saving.

8.4.3 Deleting a user

To delete a user:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **2** or move to the Sistema (System) icon by pressing the arrow keys and then press the **ok** key to confirm.
3. Enter **3** Gestione PIN (PIN management).

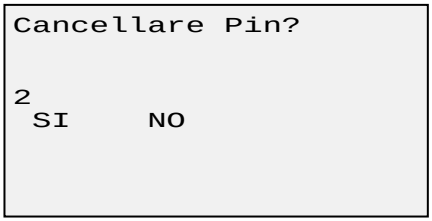


Each dot (.) indicates an already used position, the asterisk (*) the current memory position, each underscore (_) a free position.

4. With the arrows move to the required memory position and press the **ok** key. Authenticate yourself as 3rd level user.

The used positions are indicated by an * (asterisk).

5. Select the required memory position to be deleted that is displayed by an * (asterisk), and press the **CANC** key.



The PIN identification is shown (in the example figure is number 2) and the system asks to confirm the deletion. With the arrow keys, select SI (YES) to confirm the deletion and NO to cancel it. The selected option is highlighted in negative. Press the **ok** key to confirm the selection.

IT

8.5 Supervision cycles

For a detailed description of this function, please refer to the user manual.
The factory-preset control unit envisages supervision cycles equal to 1 and, for a device linked to it, the supervision time is 15 minutes.

WARNING! Any value different from the specified ones does not comply with the rules EN 50131-1 and 50131-3.

9 POWER SUPPLY MANAGEMENT

9.1 Battery

The control unit continuously measures the battery voltage.
When the voltage is lower than:

- 6.9 VDC the control unit recharges it;
- 5.5 VDC, the control unit notifies the event “Batteria scarica” (Low battery) and switches off all power supplies. The RTC calendar keeps updating itself. When the mains supply returns the control unit restarts the system;
- 1.5 VDC, the control unit notifies the event “Batteria guasta” (Battery fault) and the battery LED lights up.

9.2 Mains supply

In the event of a mains supply lack (230 VAC):

- The backlight of the control unit display immediately switches off (the display switches on again if you press a key on the keypad).
- The Home Automation Gateway is deactivated (intelligent switching off after having checked that all electrical nodes are without power supply).
- The GSM module management follows the battery charge trend.
- After 15 minutes in a raw of voltage lack the control unit notifies the mains supply lack event.
- The USB terminal is always active.

When the mains supply returns the GSM module completely starts to work again.
15 minutes following the mains supply return the control unit notifies the mains supply return event. The 15-minute interval can be changed by programming it.

IT

10 MAINTENANCE

10.1 Putting into maintenance status

To put the system into maintenance status it is enough to activate the Prova Sistema (System test) function.
To exit the maintenance status it is enough to exit the menu.

10.2 Replacing the battery of the control unit

WARNING! The exhausted battery shall be replaced with an identical one with UL94HB flammability rating or higher.

To replace the battery of the control unit:

1. Put the system into maintenance status.
2. Unhook the control unit from the supporting frame and fix it in the maintenance position.
3. Open the battery holder and extract the exhausted battery.
4. Insert the new battery and close the battery holder.
5. Unhook the control unit from the maintenance position and fix it again to the supporting frame.
6. Exit the maintenance status of the system.

10.3 Control unit reset

To restore the factory values of the control unit and to delete the executed programming and configurations:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **3** or move to the Impostazioni (Settings) icon by pressing the arrow keys and then press the **ok** key to confirm.
3. On the new screen, enter **4** Ripristina Default (Restore Default).

4. Authenticate yourself as 4th level user.
5. Press the **ok** key. The control unit restores the factory settings.
6. Exit the maintenance status of the system.

WARNING! The control unit reset operation cannot be cancelled and it implies a new and complete system configuration.

10.4 Adding devices

To add new devices after having put the system into operation, follow the instructions described for programming the different devices that are encompassed in the section Programming.

10.5 Removing devices

To remove a no longer required device:

1. Authenticate yourself and go to the Impianto (System) screen.
2. Enter **1** or move to the Programmazione (Programming) icon by pressing the arrow keys and then press the **ok** key to confirm. If required, authenticate yourself again as 3rd level user.
3. Select the device group of the device to be removed. A list of the entered devices, highlighted by * (asterisk), is displayed.
4. With the arrow keys, select the device to be removed and press the **ok** key.
5. The detail window, that enables to verify that the selected device is the required one, is displayed. Press the # key to go back to the previous screen.
6. If the selected device is the required one, press the **CANC** key to remove it or repeat the operation from point 10.
7. If you pressed the **CANC** key the control unit asks to confirm the removal. Select SI (YES) to remove the device, NO to not remove it, and press the **ok** key to confirm the selection.
8. Press the **ESC** key to exit the menu.

10.6 Replacing devices

To replace a device, first of all remove the old device and then add a new one.

WARNING! The removal of the device implies the loss of all configuration parameters. Before definitively remove the device, write down the relevant parameter values that are listed in the detail window.
Then, when you add a new device, use the values previously written down to program it.

10.7 Updating the control unit firmware

WARNING! For the update use the provided USB stick. Other devices could not be recognized.

To update the control unit firmware:

1. Put the system into maintenance status.

IT

2. Go back to the Impianto (System) screen by pressing the # key.
3. Enter **3** or move to the Impostazioni (Settings) icon by pressing the arrow keys and then press the **ok** key to confirm.
4. On the new screen, enter **2** Aggiorna FW da USB (Update FW from USB).

5. Authenticate yourself as 4th level user.
6. Unhook the control unit from the supporting frame.
7. Insert the USB stick with the new firmware into the USB port on the back of the control unit and press the **ok** key.
8. The control unit uploads the new firmware and, at the end of the uploading, it displays a message showing the successful result of the operation.
9. Remove the USB stick and fix again the control unit to the supporting frame.
10. Exit the maintenance status of the system.

10.8 Troubleshooting

Trouble	Cause	Solution
Icon 	The SIM Card is missing.	Insert a SIM card
	The SIM Card is inserted but it is not making contact.	Insert the SIM Card properly after having cleaned the contacts.
	The SIM Card credit is finished.	Reload the SIM Card, if it is a reloadable one.
Icon 	GSM/UMTS network not identified.	Check that there is coverage by the telephone network signal
Icon 	The battery is not connected.	Connect the battery or check the relevant connection.
Icon 	The battery is exhausted	Check if there is a mains supply and wait until the battery is recharged. If the signal persists, replace the battery.
LED  turned on	The battery is faulty	Replace the battery

IT

Trouble	Cause	Solution
Icon  LED  turned on	Jamming on the radio channels	Check if an electric device or an electromagnetic interference source is preventing the radio communication between the control unit and the device.
LED  turned on	There are alarm notifications not read yet.	Read the notifications
LED  turned on	There are mandatory notifications not read yet.	Read the notifications.
You do not remember the PIN		Delete the user and create a new one
The sirens beep 4 times when the system is activated	A door or a window is open	Check that doors and windows are closed
	The siren battery charge is running low	Replace the low battery
	A tampering occurred.	Check if a tampering occurred and, if possible, solve the problem
	The telephone network does not work properly	Check if there is credit in the SIM card and if there is the telephone network signal

IT

11 TECHNICAL SPECIFICATIONS

MODEL		Control unit Control unit with GSM
PRODUCT CODE		2CSYD0001N 2CSYD0002N
APPLICATION SCOPE		Household security, anti-intrusion and Home Automation
PERFORMANCE LEVEL	Security level	2
	Environmental class	I
	Notification rules	Option B
COMMUNICATION TECHNOLOGY	Security & Safety between devices	Bi-directional transmission - FM 868.3 MHz Range: 300 m in free field
	Telephone network	GSM/UMTS Dual band Module (900 MHz / 1800 MHz) Max transmission power 2 W Internal Antenna
	With RS485 devices	RS485 interface, 3-wire terminal blocks
	With PC	USB port – type A USB port - type B
ELECTRICAL FEATURES	Power supply	230 VAC ± 10%, frequency 50/60 Hz
	Current	45 mA max
	Buffer battery	NiMh Rechargeable, 6 V, 1600 mAh It ensures the compliance with the rule EN 50131-1 section 9
PHYSICAL FEATURES	Protection level	IP20
	Sizes (L x H x W)	274 x 185 x 53 mm
	Weight	0.85 kg
USAGE CONDITIONS	Environmental class	I (internal)
	Usage temperature	-5…+45 °C (*)
	Relative humidity	Medium 75% not condensing, peak 90%
	Installation	On the wall
SPECIFIC FUNCTIONS	Control unit	Micro-processor with 64 kB RAM and 128 kB flash memory
	Graphic display	Backlit LCD - 128 x 64 pixel
	Keypad	16 keys for programming 5 keys for browsing 3 keys for quick functions that can be customized at user level
	Horn	Built-in piezoelectric siren, 95 dB power at 1 m
	Protection	Anti-tampering and anti-removal tamper

(*) Test in the interval +5…+40 °C for the requirements of the Environmental class I according to the rule 50130

ABB S.p.A. –
An ABB SACE Division
Viale dell'Industria, 18
20010 Vittuone (MI) - Italy

For further information and assistance:

Numero Verde
800.55.1166

from Monday to Saturday
from 8:00 a.m. to 7:00

Printed in Italy

Power and productivity for a better world ™