



Installer manual



By-alarm Plus burglar alarm system

By-alarm Plus Manager Software



BY-ALARM PLUS

Index

1. Minimum hardware and software requirements	4
2. By-alarm Plus Manager software installation procedure	4
2.1 Select installation language	4
2.2 Select destination location	4
2.3 Select additional tasks	5
3. Transferring the software to the panel	6
4. Procedure for creating and managing a new system	6
4.1 Creating a new project	6
4.2 Check connection	8
4.3 Managing an existing project	8
4.4 Replacing a panel	9
4.4.1 REPLACEMENT with one OF THE SAME SIZE	9
4.4.2 REPLACEMENT with A LARGER SIZE one	10
4.5 Creating a project from a custom template	11
5. Design guide	12
5.1 Introduction	12
5.2 Configuring via system software	12
6. Structure of the By-alarm Plus Manager software	13
6.1 Section A	13
6.1.1 Connection	13
6.1.2 Read	13
6.1.3 Write	13
6.1.4 Save	13
6.1.5 Save with name	13
6.1.6 Save as template	13
6.1.7 Migrate	13
6.1.8 Audio Files	13
6.1.9 Logger	13
6.1.10 Monitor	14
6.1.11 Update Firmware	14
6.1.12 Panel Info	14
6.2 Section B	14
6.3 Section C	15
6.4  key	15
6.5  key	15
7. Design	16
8. SYSTEM	17
8.1 SYSTEM – Panel	17
8.1.1 SYSTEM – Panel – GENERAL	17
8.1.2 SYSTEM – Panel – COMMUNICATION	18
8.1.3 SYSTEM – Panel – INTRUSION	19
8.1.4 SYSTEM – Panel – SOUNDERS	20
8.1.5 SYSTEM – Panel – REGULATION	20
8.2 SYSTEM – Partitions	22
8.3 SYSTEM – Temporal exceptions	23
9. TERMINALS	24
9.1 TERMINALS – Zones	24
9.2 TERMINALS – Outputs	29
10.USER	34
10.1 USER – Profiles	34
10.2 USER – Users	35
10.3 USER – User notifications	38
10.4 USER – ARCs	39
10.5 USER – USER - Surveillance notifications	40
10.6 PIN and key management	41
11.AUTOMATION	42
11.1 AUTOMATION – Activation Lines	42
11.2 AUTOMATION – Activation Scenarios	42
11.3 AUTOMATION – Auto-insertions (and Automatismes)	43
12.EXPANSIONS	45
12.1 BUS EXPANSIONS – Expansions	45
12.2 BUS EXPANSIONS – Keyboards	46
12.3 BUS EXPANSIONS – Readers	48
12.4 BUS EXPANSIONS – Radio receivers	49
12.5 BUS EXPANSIONS – (LTE dialer art. 03810/03820)	50
12.6 BUS EXPANSIONS – Sounders	51
12.7 RADIO PERIPHERALS – Sensors and detectors	53
12.8 RADIO PERIPHERALS – Radio keys (remote controls)	54
12.9 RADIO PERIPHERALS – Sounders	55
13.SYSTEM MONITOR	56
13.1 RADIO MAP	64
APPENDIX - Updating the panel and device firmware	65

Minimum hardware and software requirements - By-alarm Plus Manager software installation procedure

1. Minimum hardware and software requirements

Hardware

- PC

Software

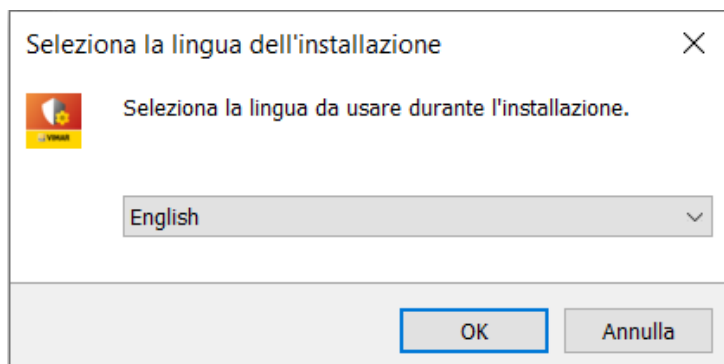
- Microsoft Windows ver. 10 and later operating system.

2. By-alarm Plus Manager software installation procedure

After downloading the software from the www.vimar.com website, run the By-alarmPlusManager-Setup.exe program.

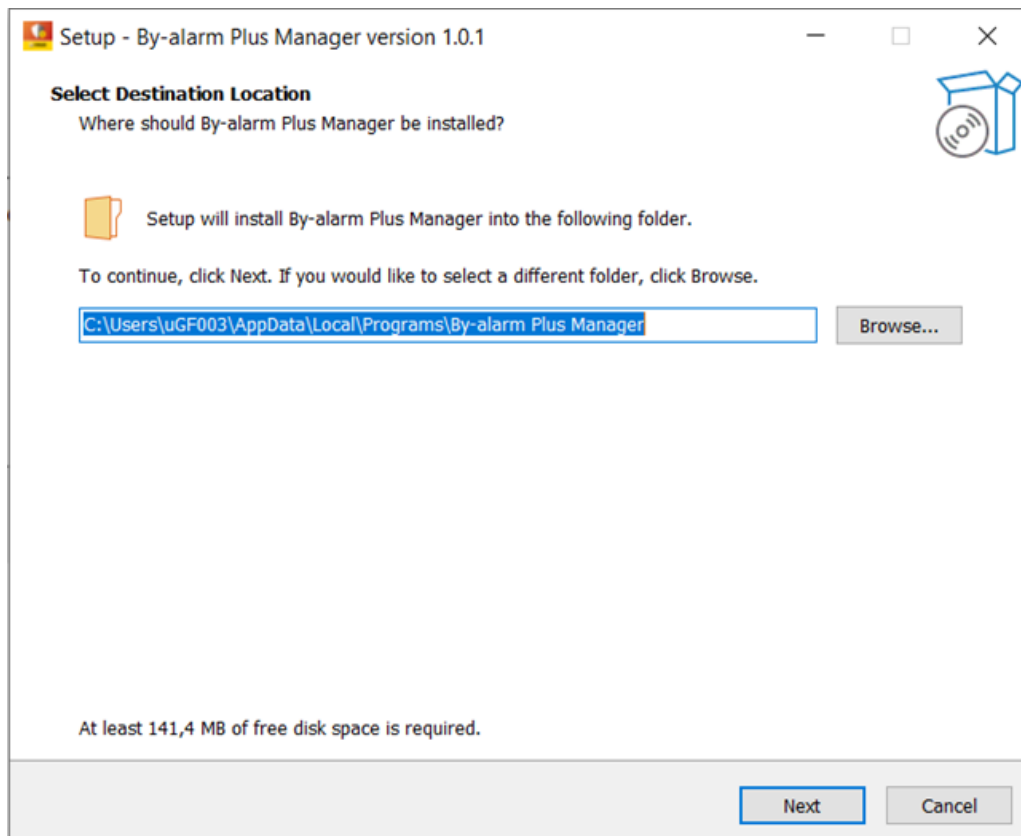
The installation procedure must be carried out by an Administrator user.

2.1 Select installation language



Press OK to proceed.

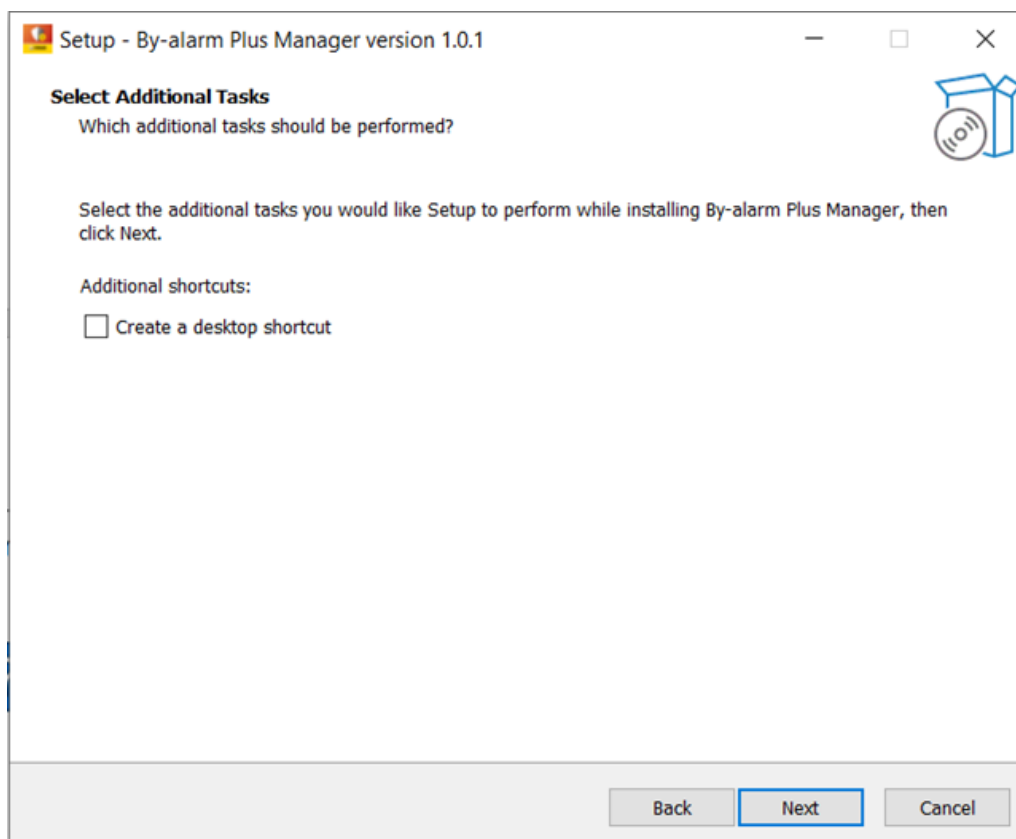
2.2 Select destination location



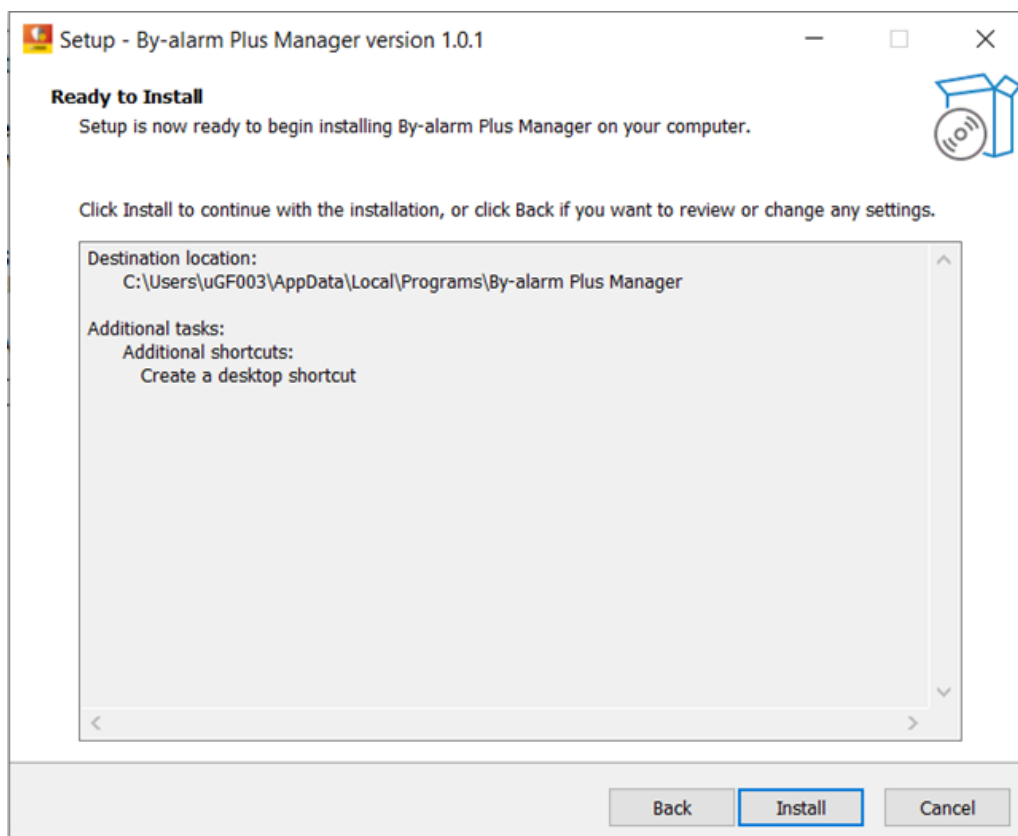
Press Next to proceed.

By-alarm Plus Manager software structure

2.3 Select additional tasks



Press Next to proceed.



Press **Install** to start the procedure that transfers the files to the PC and prepares the By-alarm Plus Manager environment to manage the burglar alarm system.

Connecting the software to the panel - Procedure for creating and managing a new project

3. Connecting the software to the panel

The By-alarm Plus software can be connected to the panel board as described below.

With a USB cable

Use a USB-microUSB cable to connect a USB port on the PC to the corresponding connector on the board. Set the following fields in the connection configuration window of the By-alarm Plus Manager software:

- Connection type: select “USB serial”
- COM port: select the port being used

With gateway art. 03812

Use the View Pro app to create the project and add the burglar alarm system gateway 03812.

Set the following parameters in the connection configuration window of the By-alarm Plus Manager software:

- Connection type: select “Gateway”
- IP address: enter the IP address of the gateway, which you can get from the View Pro app
- Port: enter the port number associated with the gateway IP, which you can get from the View Pro app

For all details, refer to the “By-alarm Plus Burglar Alarm System Gateway art. 03812” chapter in the VIEW IoT Smart System platform manual.

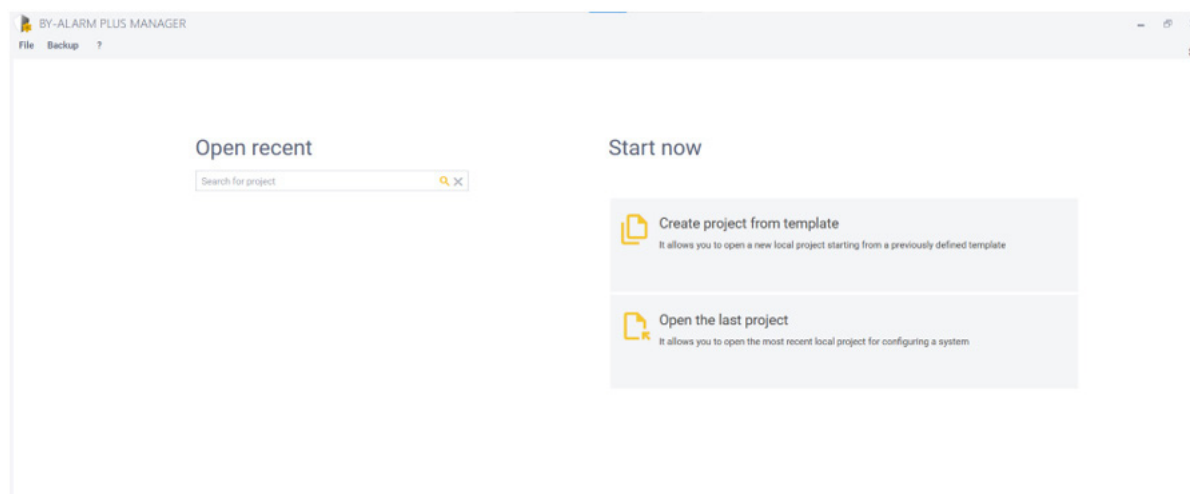
4. Procedure for creating and managing a new project

The software displays recent projects and the following options:

- Create project from template
- Open the last project
- Import database

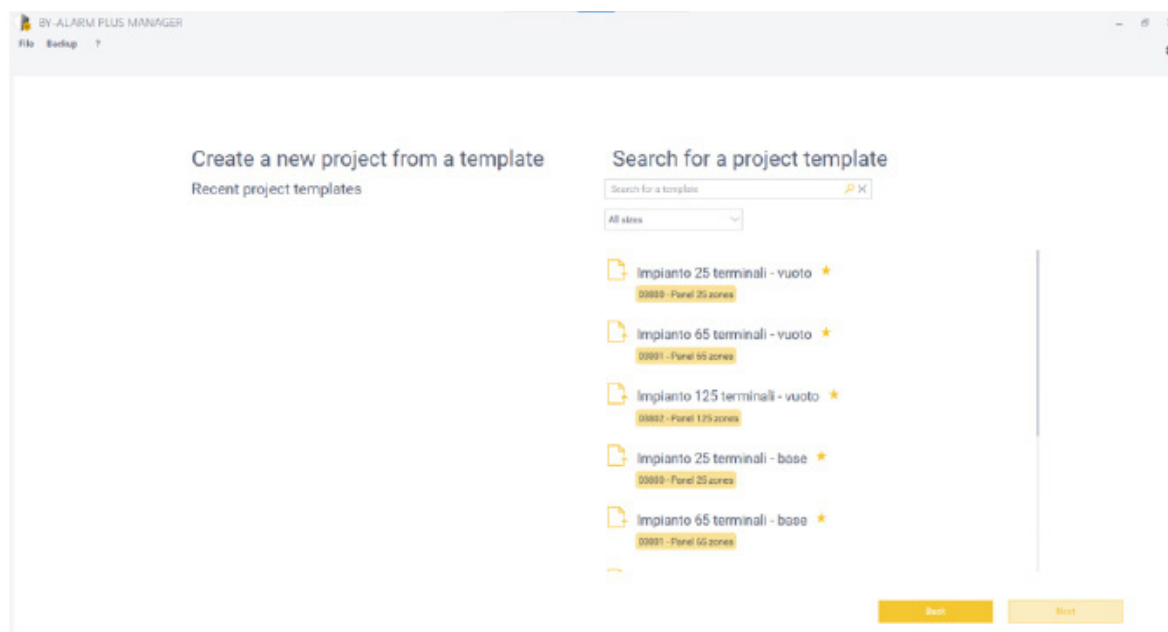
4.1 Creating a new project

Select the “Create project from template” option.



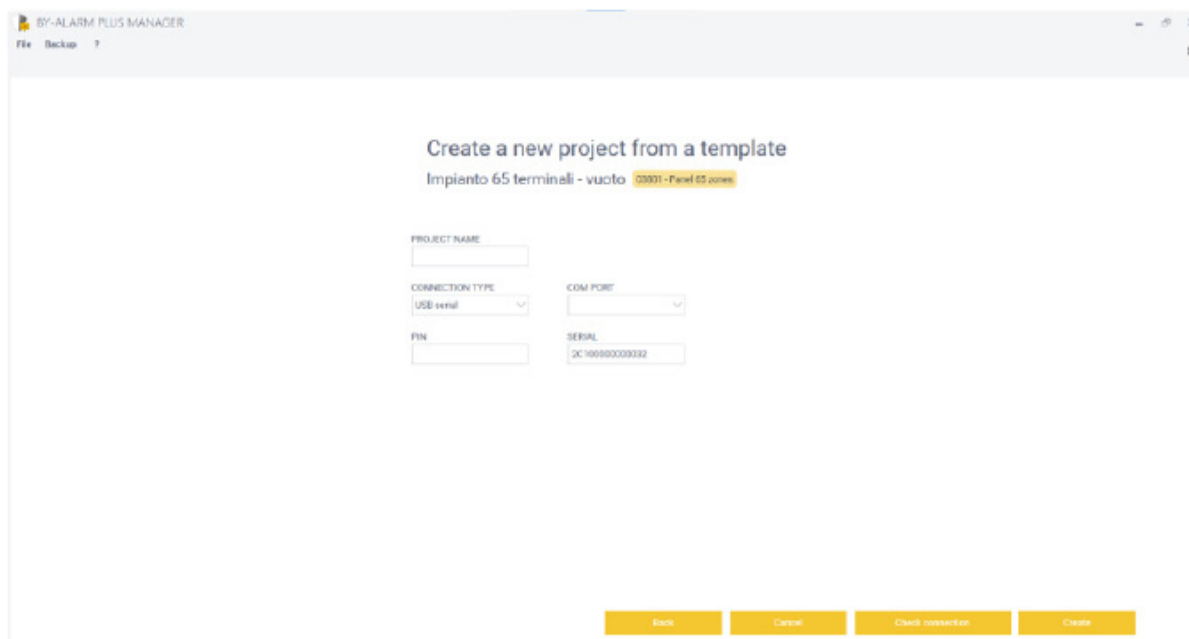
Procedure for creating and managing a new project

Choose the panel type (25, 65 or 125 zones)



Set the following parameters:

- Project name;
- Connection type: refer to the previous "Transferring the software to the panel" chapter;
- PIN for connecting to the board: enter the installer's code.
N.B. The default installer's PIN is "9999" when accessing the system for the first time (i.e. until it is changed)
- Serial number of the board (given on the label with QRCode in the packaging).



N.B. A panel can only be read/written if the QR code entered in the software matches the QR code in the panel.
In fact, the panel QR code is used as an integral part of some encryption algorithms.

Procedure for creating and managing a new project

4.2 Check connection

This function checks that the board can be connected. The check confirms that the serial number is valid; a message will inform the installer if this check fails during the connection procedure.

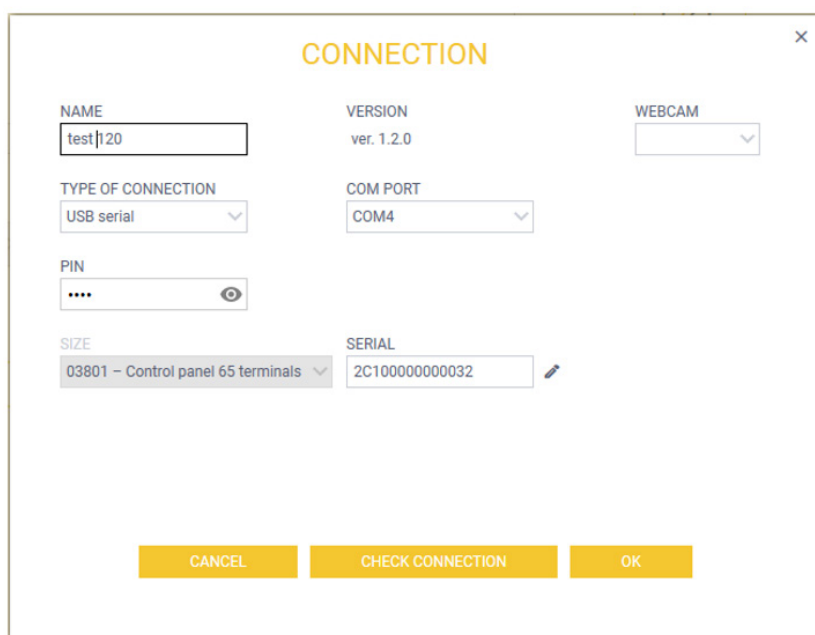
Error cause	Message
Wrong COM	Physical error
Wrong PIN	Unrecognised user
Wrong IP/Port	Unable to establish a connection with the panel

4.3 Managing an existing project

Select "Open" from the "File" menu to recall any system project created previously.

Connection

This window displays information about the connection made in the last session.



The screenshot shows a window titled "CONNECTION" with a close button (X) in the top right corner. The window contains several fields and buttons:

- NAME:** A text box containing "test120".
- VERSION:** A text box containing "ver. 1.2.0".
- WEBCAM:** A dropdown menu.
- TYPE OF CONNECTION:** A dropdown menu showing "USB serial".
- COM PORT:** A dropdown menu showing "COM4".
- PIN:** A text box with four dots and an eye icon.
- SIZE:** A dropdown menu showing "03801 - Control panel 65 terminals".
- SERIAL:** A text box containing "2C100000000032" with an edit icon (pencil) to its right.
- Buttons:** At the bottom, there are three yellow buttons: "CANCEL", "CHECK CONNECTION", and "OK".

Specifically:

- VERSION: indicates the firmware version of the control unit
- WEBCAM: designed to assign the WEBCAM to use to read QR Codes to the software
- SIZE: designed to display the size of the panel indicated when creating the system via the SERIAL entered

Note: Use  to update the SERIAL when replacing the panel. The panel type (number of zones) cannot be changed.

Procedure for creating and managing a new project

4.4 Replacing a panel

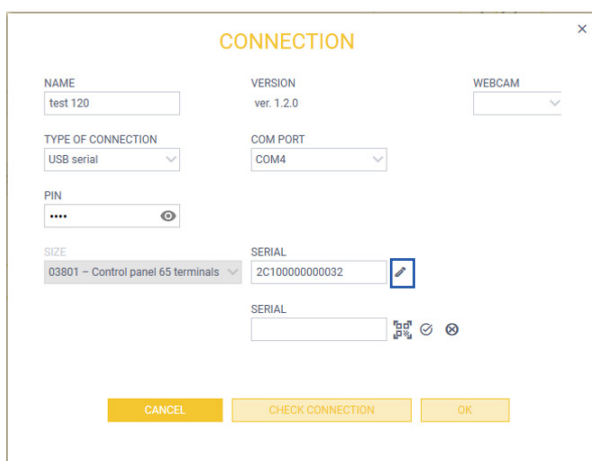
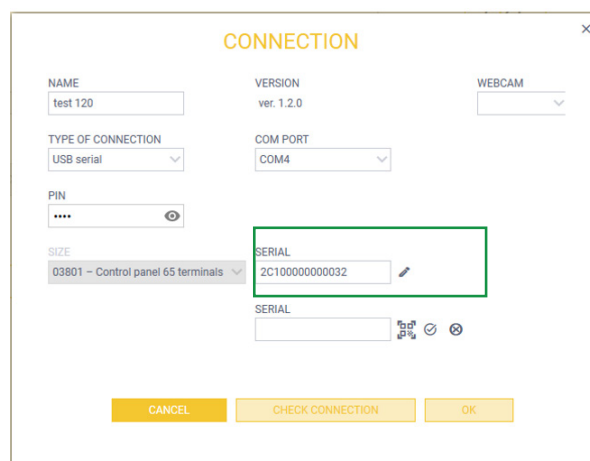
Caution: Any changes made by users to PINs and keys after the last panel reading with the software (programming backup and PINs and keys) will not be recovered; it is therefore always advisable to read the panel before you begin the procedure.

4.4.1 REPLACEMENT with one OF THE SAME SIZE

The procedure is as follows:

- Replace the panel with a new one of the SAME SIZE
- Restore the factory data in the panel (if the panel is not brand new)
- Enrol at least one keypad, log in as user 1 (default PIN 0001) and enable "Enable writing PINs/KEYS from SW"
- From the By-alarm Plus Manager software on the PC, open the saved project programming that you want to transfer to the new panel
- View the CONNECTION option in the software, activate QR code editing, enter the QR code of the new panel and confirm

The  key activates the QRCode scanning using the camera associated with the software.

- The software will ask whether you are "Replacing a panel" or "Installing a new system"; select "Replacing a panel"
- Press the "Write" key to write to the panel
- Writing PINs/KEYS is AUTOMATICALLY DISABLED when the software has finished writing

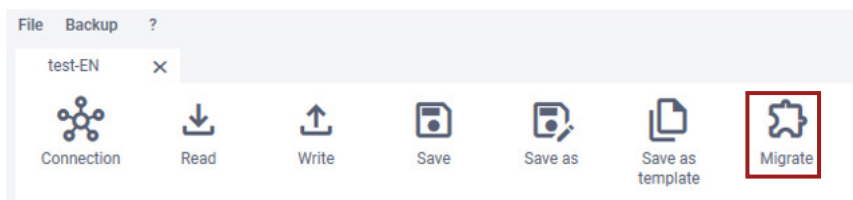
Procedure for creating and managing a new project

4.4.2 REPLACEMENT with A LARGER SIZE one

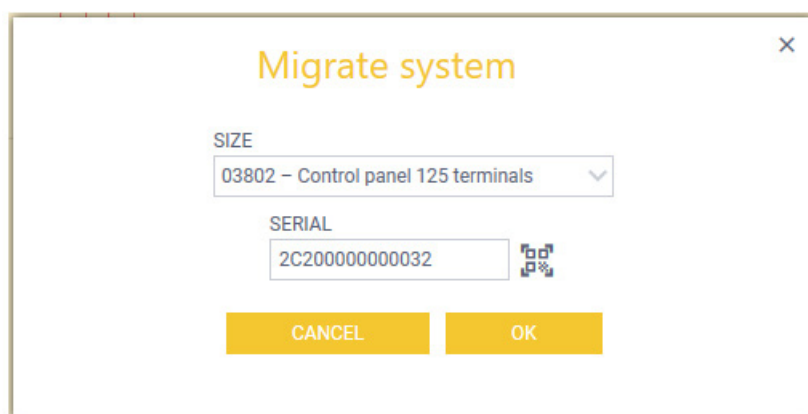
N.B. The software only allows you to transfer from a smaller panel to a larger one and NOT vice-versa.

The procedure is as follows:

- a. Replace panel A (SMALLER SIZE) with panel B (LARGER SIZE)
- b. In the By-alarm Plus Manager software, press "Migrate" to launch the procedure



- c. The software will display the window for choosing the new size of panel B and its QR code

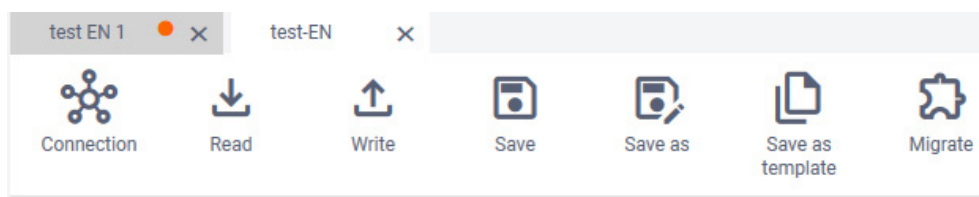


- d. Once you have chosen the size and inserted the correct QR code (you can leave it on default and change it later, but you must change it BEFORE you communicate with panel B) press OK.

- e. To save these settings to the software database one of the following operations must be carried out:

- (1) "Save as", if you want to keep a system for panel A as backup and have a new system for panel B (this is RECOMMENDED, the old system of panel A can be deleted later)
- (2) "Save" if you want to overwrite the current system

If you carry out operation (1) you will therefore have a new system for panel B with the chosen name. For example:

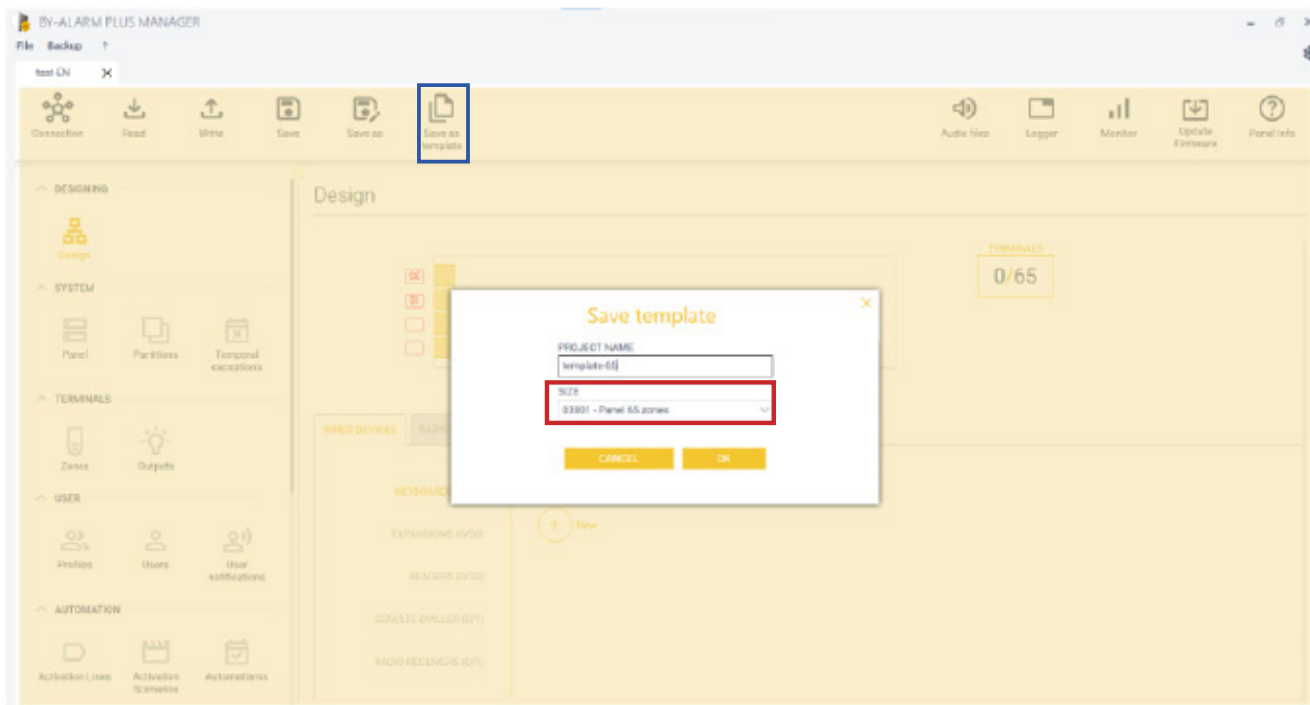


- f. Restore the factory data in panel B (if the panel is not brand new).
- g. Enrol at least one keyboard, log in as user 1 (default PIN 0001) and enable "Enable writing PINs/KEYS from SW".
- h. Check you have correctly inserted the QR code of panel B (as set out in point "d") then write the new system on panel B.
- g. Writing PINs/KEYS is AUTOMATICALLY DISABLED when the software has finished writing.

Procedure for creating and managing a new project

4.5 Creating a project from a custom template

- a. Starting from a software project with the panel size you want for the new project to be created, press “Save as template”.




The template created will contain the structure of the original project, i.e. terminals and their programming, user notifications, users and their programming (but with default PINs, without keys enrolled and without sensitive information), wired and radio devices and their programming (but with default QR codes - all 0s for the panel part) and all other general panel programming.

- b. Create a new project, selecting the custom template created in the previous step as the starting point.

Search for a project template

🔍 ✕

All sizes
▼


template-65

03801 - Panel 65 zones

- ALWAYS assign the QR code of the panel to be installed (of the right size).
- ALWAYS replace all QR codes with those of the devices to be installed.
- Finally, complete and/or change the programming as required for the specific installation site.

5. Design guide

5.1 Introduction

When choosing the installation method, refer to chapter 2 “How to create a system” in the By-alarm Plus Installation Manual, which illustrates the available procedures:

- 2.1 Off-line installation;
- 2.2 Installation on-site and addressing wired and radio peripherals/devices using the By-alarm Plus manager software;
- 2.3 Installation on-site and addressing wired peripherals without software.

5.2 Configuring via system software

After creating the project, the installer has to define a range of information.

The installer can get an overview of the current configuration in the “Design” section.

The sequence of operations to perform in order to configure the system for the first is suggested below.

1. Panel: define the languages included, communication attributes, intrusion, regulations. For full details, see chapter 8 in this manual.
2. Peripherals: define the devices (keyboards, expansions, readers, etc.), description, attributes. For full details, see chapter 12 in this manual.
3. Partitions: define the partitions, keyboard associations (see par. 12.2 in this manual) and readers (see par. 12.3 in this manual) and switch-on options. For full details, see para. 8.2 in this manual.
4. Zones: define the zones, description, peripheral types. For full details, see para. 9.1 in this manual.
5. Outputs: define the outputs, description, peripheral types. For full details, see para. 9.2 in this manual.
6. Profiles: define the user profiles for the system, description, attributes. For full details, see para. 10.1 in this manual.
7. User: define the users, description, associated profile, language, attributes. For full details, see para. 10.2 in this manual.

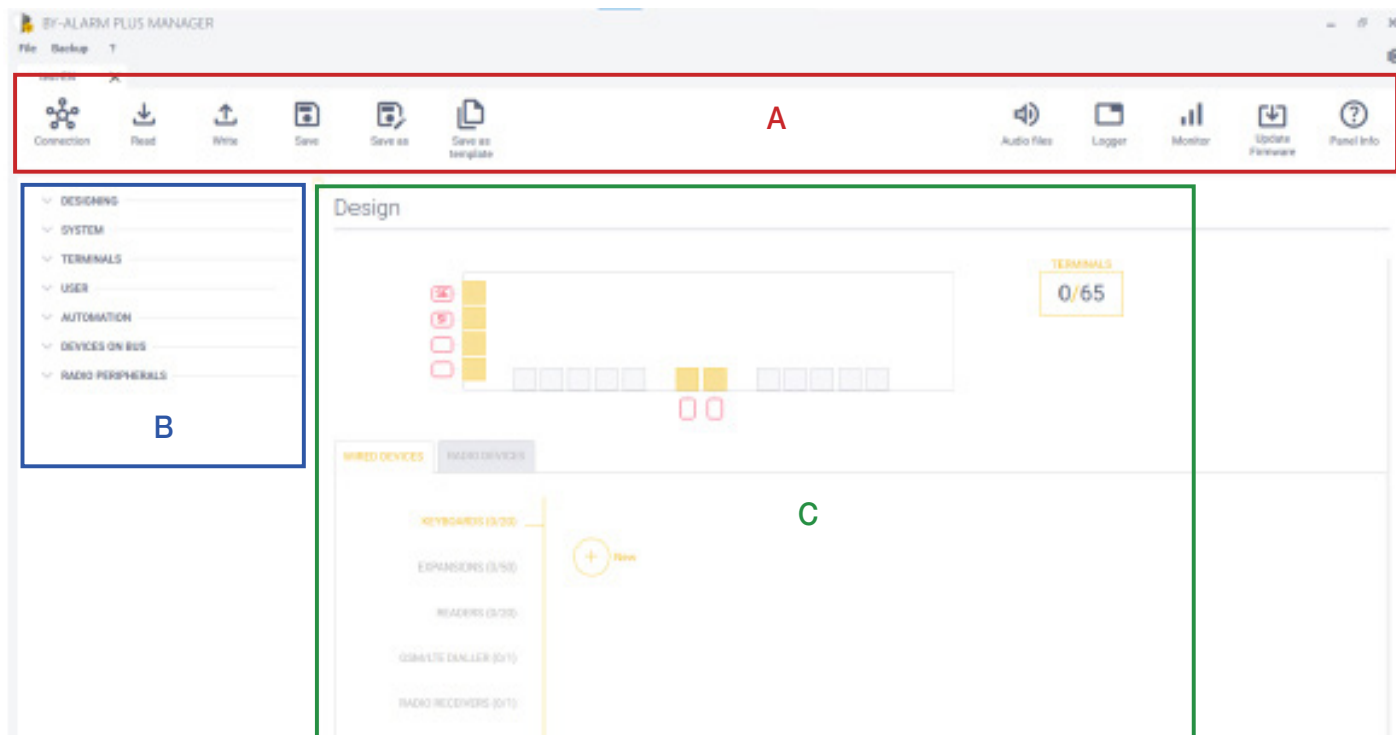
After setting all the system parameters, press **Save** followed by **Write** to transfer all the information to the panel. The system has now been configured with the By-alarm Manager Plus software.

By-alarm Plus Manager software structure

6. By-alarm Plus Manager software structure

The main screen of the *By-alarm Plus Manager* contains three sections, as identified by the following three boxes:

- Section A
- Section B
- Section C



6.1 Section A

This contains general controls and information related to reading and writing system parameters, accessing the logger, saving the project, monitoring, etc. Each key may open a dialogue box to enter or confirm certain information.

6.1.1 Connection

Contains parameters related to the connection between the software and panel via USB or gateway art. 03812.

6.1.2 Read

Control to display all system parameters on the panel.

6.1.3 Write

Control to set all system parameters on the panel.

6.1.4 Save

Control to save the project with the current name.

6.1.5 Save with name

Control to save the project with a name other than the current one.

6.1.6 Save as template

Control to save a custom template based on the current project.

6.1.7 Migrate

Control for replacing the panel with a larger size one, while retaining the programming of the system.

6.1.8 Audio Files

Controls to convert the Descriptions entered by the user into voice files. The procedure can send all the files generated to the connected panel.

When the system is fully operational, the notifications sent by the panel via the GSM/LTE dialer will consist of several concatenated voice files in order to provide information on the burglar alarm system status on a remote device.

Pressing the key opens a wizard that:


1. Uses a "natural text to speech" engine to generate all the audio files with the voice call notifications in the selected panel language, for both common texts and descriptions of its characteristics (zones, partitions, users, etc.). An icon displays date of the last generation performed.

Note: the audio files must be regenerated and sent to the panel whenever a characteristic is added or a description is changed.

2. Send the most recent set of audio files generated to the panel


By-alarm Plus Manager software structure

6.1.9 Logger

Control to read the system logger. After pressing the  "READ" key to read all the panel events, a window appears to display them.

The  key can be used to export the list of events just displayed.

6.1.10 Monitor

Control to open the screen in which the entire system can be monitored in real time. After pressing the  key to start monitoring, a window appears in which all the information is updated in real time.


6.1.11 Update Firmware

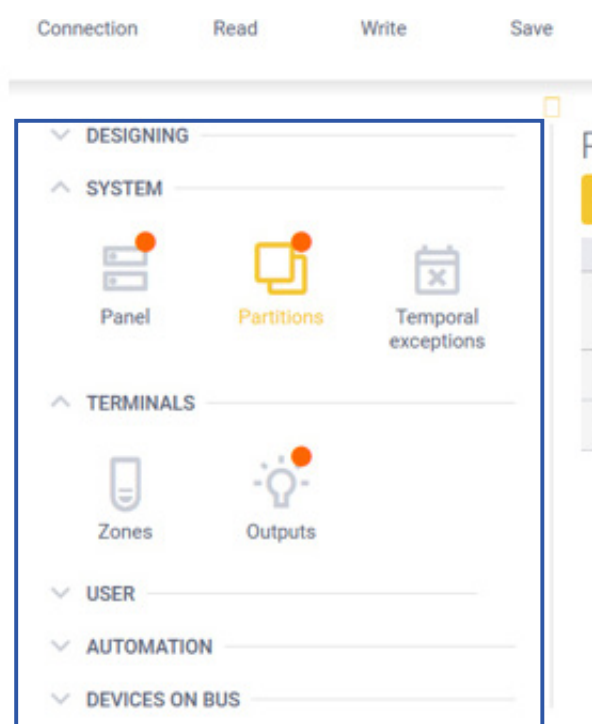
Control to update the panel and device firmware after selecting the required files.

6.1.12 Panel Info

Control to display the data that characterises the panel (QR code, firmware panel, model, etc.).

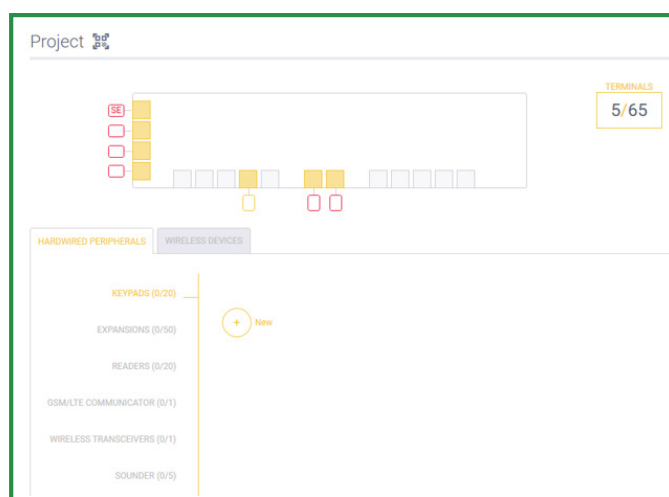
6.2 Section B

This contains the logical sections for all functional parameters of the panel and system. Each name generically identifies the parameter type it contains. An orange dot  indicates that one or more parameters in this section have been changed.



6.3 Section C

This contains parameters and specific details related to the part of section B selected previously.

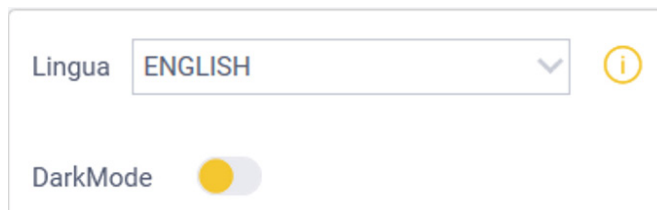


Clicking on the stylised symbol of a QR code next to "Design" allows you to open a window to facilitate the "rapid" acquisition of any type of peripheral device serial number, both via optical detection and entry on the keypad.

By-alarm Plus Manager software structure

6.4 key

The Configuration key  serves to customise the **Language** and program Background (**DarkMode**).



The screenshot shows a configuration panel with two settings. The first is 'Lingua', which is a dropdown menu currently displaying 'ENGLISH' with a downward arrow and an information icon to its right. The second is 'DarkMode', which is a toggle switch currently in the 'off' position, indicated by a yellow circle on the left and a grey bar on the right.

Restart the By-alarm Plus manager software to apply the selected language.

DarkMode selects a dark or light background in the By-alarm Plus manager software.

6.5 button

Designed to disconnect the current user.

Design

7. Design

This is the initial screen for designing a project, and serves to:

- Add or delete BUS peripherals in the **WIRED DEVICES** box (this is also possible from the **DEVICES ON BUS** menu) and radio devices in the **RADIO DEVICES** box (this is also possible from the **RADIO DEVICES** menu).

To add a peripheral, click the peripheral type you want to add (e.g. **ESPANSIONI (1/50)**) — click the  **Nuova** key to display the peripheral).

Double-click the peripheral to open its page directly and set its parameters (this page and the parameters for each peripheral are illustrated in the **DEVICES ON BUS** and **RADIO DEVICES** paragraphs).

- Configure the input/output terminals and access their programming directly (this is also possible from the **TERMINALS** menu). For peripherals that have terminals, you can set the type.

Double-click the terminal to open its page directly and set its parameters (this page and the parameters for each peripheral are illustrated in the **TERMINALS** paragraph).


- View how many terminals have been used compared to those available; the  box is updated automatically as the terminals are added/removed.



- Use the **RADIO DEVICES** box to add or remove radio devices; click the  **Nuova** key to open the window in which you can enrol a new radio device.

- Use the **Model** menu to select which of the displayed devices you want to enrol.

You then have to enter the alphanumeric code of the QR code on each device in the **Serial** box; you can enter the device name in the **DESCRIPTION** box.

Then press the  key to add the device to the system.

Consider that the radio devices are managed as BUS peripherals (e.g. expansions); so add the device and then “connect” the corresponding signals you want to use. For example, the magnetic contact art. 03833 is a device that can handle 3 distinct signals: magnetic reeds and terminals T1 and T2. For each device, the available signals/terminals are identified with icons (see the  boxes):

-  the signal is used/enabled
-  the signal is NOT used

Some radio devices, such as the detector art. 03836, have a single signal; in that case, the signal is always enabled by default and CANNOT be disabled.

To enable/disable a signal on a radio device, right-click the  /  symbol and select the signal you want from those listed.

The zone or output enabled on the radio device will also be displayed in **TERMINALS – Zones** and **TERMINALS – Outputs**, where you can set its parameters.

All details are described in the **RADIO DEVICES** paragraph and in the manual for the radio interface art. 03831.

System

8. SYSTEM

This section consists of a number of general menus and parameters for the entire system. From here you can set the system options, define the partitions (and their parameters) to be used in the system, and the temporal exceptions.

8.1 SYSTEM – Panel

This is composed of four menus: **GENERAL – COMMUNICATION – INTRUSION – REGULATION**

8.1.1 SYSTEM – Panel – GENERAL

Section C (green):

Panel Name is the name assigned by the installer.

The **SERIAL** is not editable because it contains the unique for each panel.

The four languages can be set.

Certain DATE/TIME parameters can be set, namely:

- the display format (the date and time can be changed the keypad as described in the user manual or in the software);
- the TIMEZONE, to set the UTC zone adopted by with the relevant rules for managing the automatic time change*, which is useful when the panel is a gateway (this setting will be ignored if a gateway is present);
- synchronisation from SIA-IP, to allow the panel to time based on the time references of the SIA-IP (tamps) transmitted by the Alarm Receiving Centre ignored if a gateway is present).

(*) The specific DST rules of each world zone are verified by the SW after they have been taken from the operations; we therefore recommend you keep your PC to receive any new government directives in each state.

You can then set the *options* for:

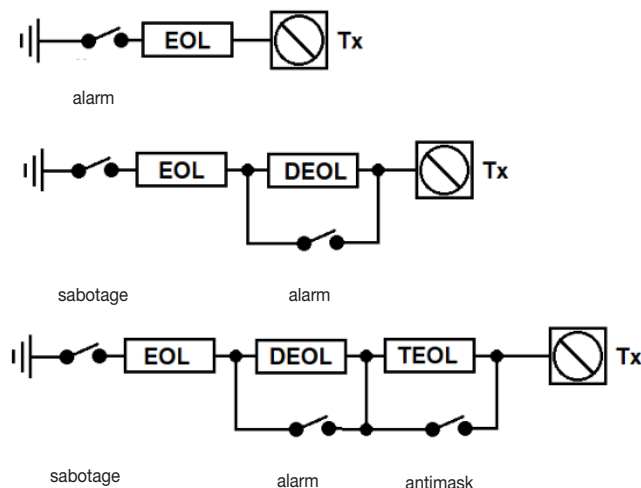
- the **BUS Speed** (default 125 kbps);
- **reactivate outputs on impulsive activations**: when a put already activated in PULSE mode by a programmed new trigger PULSE will restart its on time count from zero; otherwise it will ignore the new trigger and continue counting the current on time.

You can set the *radio options* for:

- **Radio peripheral supervision time**: this is the time used to check whether a radio device has disappeared. If a radio device does not communicate for longer than the programmed time, it will be notified as disappeared in the panel. The regulations state the following for both wired and radio devices:
 - for security grade 2, the supervision time cannot exceed 120 minutes;
 - for security grade 3, the supervision time cannot exceed 100 seconds.

The default supervision time in the software is 30 minutes for radio devices, and can be set up to a maximum of 250 minutes.

The **REFERENCE IMPEDANCES FOR THE SYSTEM** can be set (default 3.3kΩ, 4.7 kΩ, and 15 kΩ). These are the values used whenever adding a new wired zone, with reference to the balancing diagrams in the figure below.



(N.B. The sabotage signal is wired to a terminal configured as TAMPER).

Caution: The impedances shown do not change the status threshold in wired zones already configured. They will only be considered to recalculate the thresholds when a balancing change is made in each zone.

8.1.2 SYSTEM – Panel – COMMUNICATION

Max number of voice recall:

this is the number of call attempts (with voice messages) to the telephone numbers, after which the call is considered to have failed.

Call with voice recognition online:

This starts playing the voice message after recognising the voice online. When this option is not enabled, the voice message is played immediately after dialling the number.

NOTIFICATION DELAY

- Power failure notification delay
- Delay for notification of communication failures
- Delay for notification of other faults

The times are set in s and indicate for how long the failure must persist before notification. It is a filter to prevent false notifications; for example, if the power failure delay is set to 180 s, a power failure event notification is sent if the mains voltage is missing continuously for longer than 180 s, while no notification is sent if the mains voltage returns within 180 s.

AREA CODE

Delete digits at the top of the selection: this removes digits from the user's telephone number before dialling the call or sending a text message. The number of digits to be removed is programmable.

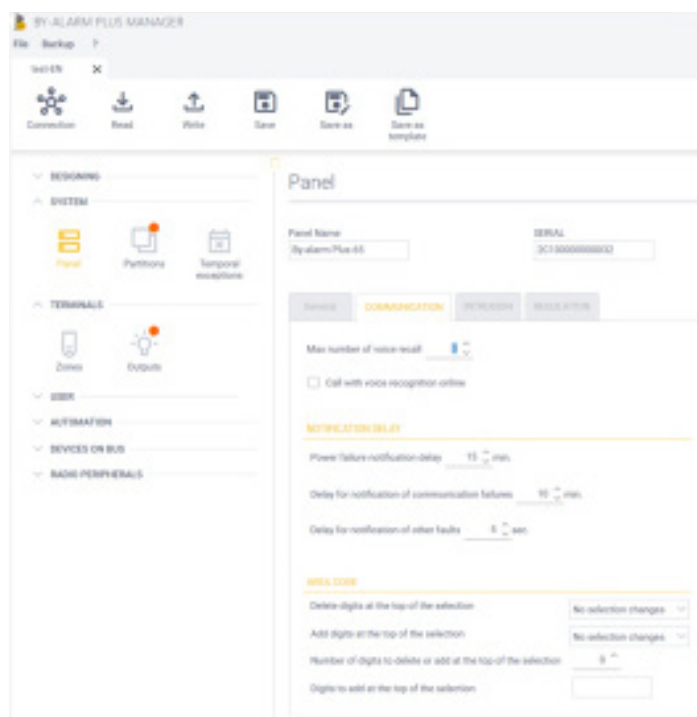
Add digits at the top of the selection: this adds digits from the user's telephone number before dialling the call or sending a text message. The digits to be added are programmable.

Number of digits to delete or add at the top of the selection: when *Delete digits at the top of the selection* is enabled, this is the number of digits to be removed.

Digits to add at the top of the selection: when *Add digits at the top of the selection* is enabled, these are the digits that will be added.

SECURITY

The "SIA CODES" button grants access to the advanced settings of the panel SIA-IP protocol to allow the customisation of the codes sent to security for certain categories of events. They should be edited by the installer only where requested by the reception and control centre manager in charge of the ARC.



ID	DESCRIPTION	SIA-IP CODE ACTIVATION	SIA-IP CODE RESTORING
0	Detector dusty or not calibrated	AS	AN
1	No AC	AT	AR
2	Violated intrusion zone in armed status	BA	BR
3	Intrusion zone bypassed	BB	BU
4	Intrusion alarm deleted	BC	--
5	Intrusion zone fault	BT	BJ
6	Intrusion alarm confirmed	BV	--
7	Auto-arming delayed	CE	--
8	Forced arming (zones not ready)	CF	--
9	Arming failed (not armed after zones made ready)	CI	--
10	Partition armed/disarmed automatically	CA	OA
11	Partition armed/disarmed by user	CI	OP

NOTES:

1. If a code in the table is "--", the SIA-IP notification it uses is not sent to the ARC
2. The panel autonomously manages the sending or not of the restoring of a notification, depending on whether the triggering cause was an ON/OFF type or a simple occurrence (for instance "Intrusion alarm confirmed"), so a possible code programmed for restoring may be ignored by the panel

8.1.3 SYSTEM – Panel – INTRUSION

Observation time to generate a confirmed alarm:

When there is intrusion/sabotage for a zone/peripheral in a partition, a **confirmed intrusion/sabotage** event is generated if intrusion/sabotage occurs for another zone/peripheral in the same partition within the set time (in minutes).

Pre-alert time for auto-insertions:

When automatic time-based arming is programmed, this is the time (in minutes) before arming the partitions at which the arming is notified acoustically and on the keyboard displays. An extraordinary request can be made to delay auto-arming.

Persistence time of sabotage in the control panel:

When the panel is subject to sabotage, this event persists for at least the time set here. If the sabotage condition remains after this time, it will not be reset.

Maximum number of activations for sabotage in the control panel:

When set to "0", the control panel sabotage event will be generated whenever it occurs.

When set to a number "n" other than "0", the sabotage event is generated "n" times and then no more. It is a filter that prevents continuous repetition of sabotage events. A user reset will reset the counter.

User log time on keyboard:

This is the time (in s) for which the user login remains valid (after entering a valid PIN) in order to use the keyboard without having to enter the PIN again. Once this time lapses without pressing any key, the user will have to enter the PIN again before accessing the keyboard.

GENERIC OPTIONS

Arming a zone in a multi-area even with only one partition armed:

This is a system option that allows alarms to be generated by zone in multiple partitions when only one of them is armed. It is often described as partition OR. When it is not selected, the alarm for a zone in multiple partitions can only be generated when all of its partitions are armed.

Treat antimask as broken:

Masking is normally considered to be sabotage. When this option is selected, a fault event is generated instead of sabotage.

See the disappearance as sabotage as well as a breakdown:

Disappearance of a peripheral is a fault. When this option is selected, a sabotage event is also generated.

In disarmed, no indoor siren for tampering:

If all partitions are disarmed, a sabotage/tampering event does not activate the "indoor siren" output.

Stop sirens when entering code:

All siren outputs are deactivated as soon as a valid PIN is recognised.

Stop calls to code entry:

All notifications are stopped as soon as a valid PIN is recognised.

Disarm partitions in alarm upon entering the code:

All partitions in the alarm state are disarmed as soon as a valid PIN is recognised.

System reset upon code entry:

A system reset is performed as soon as a valid PIN is recognised. The alarm and sabotage memories are erased (not faults); clearly the end result will depend on the profile of the user performing the operation (partitions and profile options), and on the active regulation grade (see the REGULATION paragraph).

Activates alternative mode of the area status light signalling reader:

Using this option will activate each LED in the following ways:

- fixed, if all the programmed areas for the related INTRUSION function are in the total arming or at least partially configured status;
- flashing slowly, if all the areas programmed for the related INTRUSION function are disabled and at least one alarm memory is present for at least one of the areas;
- flashing quickly, if at least one of the areas programmed for the related INTRUSION function is in alarm.

Activates alternative mode of the area status light signalling reader:

If this option is active, the reader LEDs do not show the partition states and remain off. They only turn on when a valid transponder key is brought close to select the operation.

Exclude area also for sabotage:

If this option is active, disabling/isolating a zone disables both alarm and sabotage signalling. If the option is not active, disabling/isolating a zone enables sabotage signalling only (not alarm).

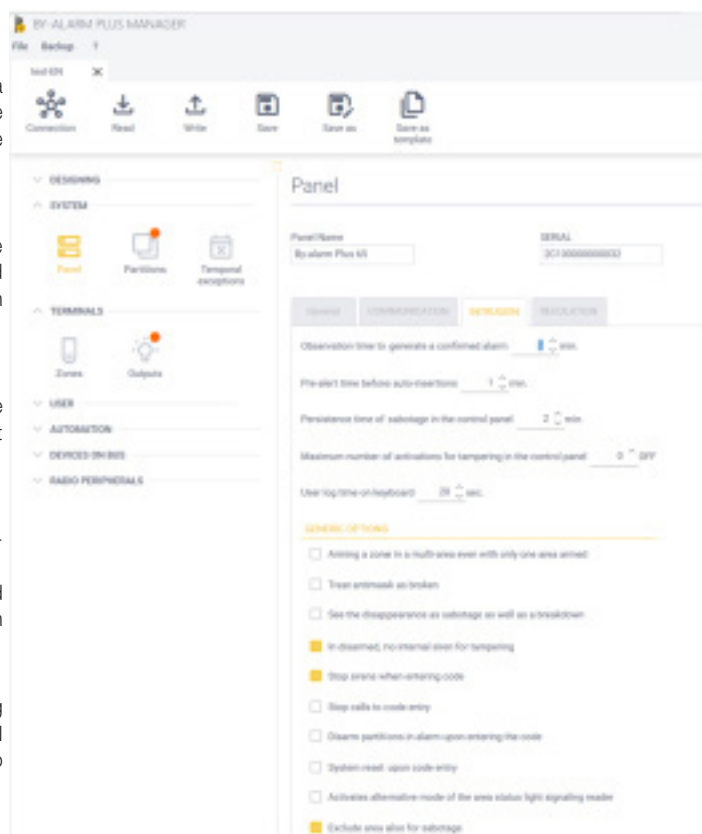
USER

Code digit number.

It establishes the number of digits which each user/installer PIN created or edited in the system should have.

Confirm code with OK.

Prompts you to press the "OK" key on the keyboard to confirm the selection of the PIN entered.



System

Choose code.

Allows the user to edit their PIN by typing in the desired PIN directly. Shows the possibility that a code from another user already in the system may be revealed if the same PIN is typed in. If this option is not active, when the PIN is changed, the user will instead have to choose from the PINs suggested randomly by the system.

Names for partial arming

In each of the 4 text entry boxes, you can specify the description of each one of the 4 partial system arming modes.

8.1.4 SYSTEM – Panel – SOUNDERS

This section illustrates the activation modes associated with each category of event configurable for the bus sounders art. 03826. Depending on the category(ies) of events chosen as the causes of activation, the sounder will be activated by ringing and/or blinking in one of the modes specified in this section.

For each category of events, you can set the following parameters associated with the sounders:

Blinking

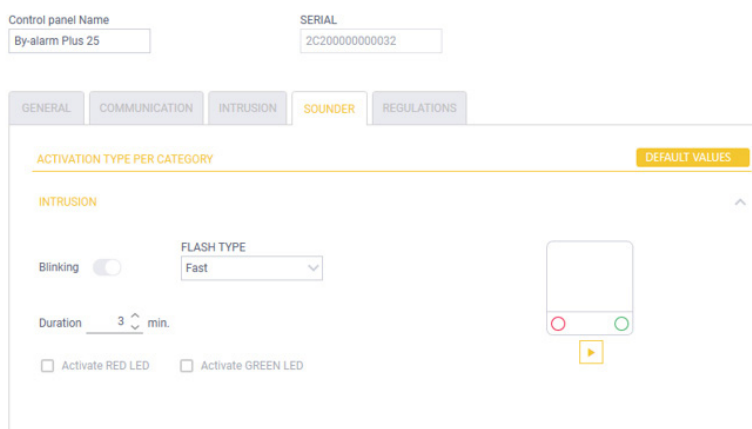
- Switch for enabling or disabling the blinking
- Drop-down menu to choose the type of blinking (slow or fast)
- Checkbox to ensure the blinking remains active even after the sounder has stopped (ignores the “duration” parameter)

Duration

- Activation time

Checkbox for the selective activation of the red and green status LEDs

There is also a simulation of the sounder's behaviour depending on the configuration, which can be activated by pressing the  button.



8.1.5 SYSTEM – Panel – REGULATION

Section C (green) contains a drop-down menu to set the regulation with which you want to validate the system.

NONE:

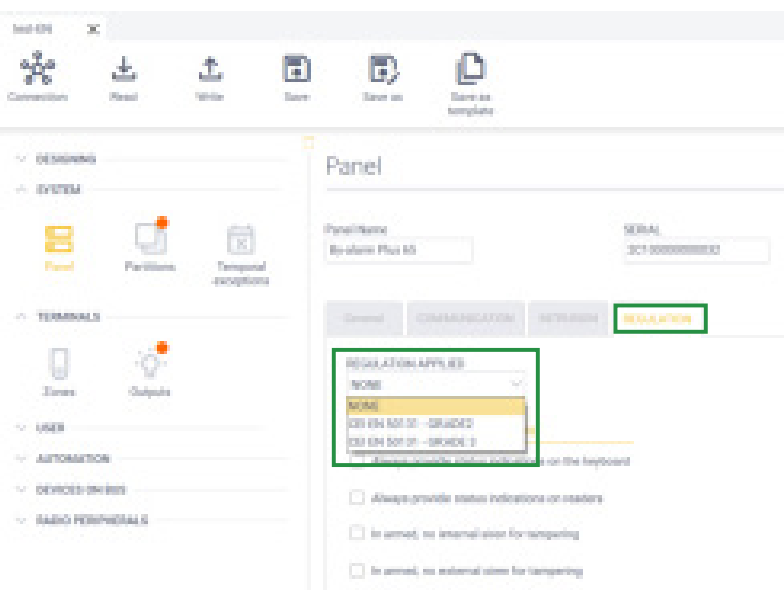
The system does not require any grade of the EN50131 standard.

CEI EN 50131 – GRADE2:

CEI EN 50131 – GRADE3:

The system has to have security grade 2 or security grade 3. This selection alone is not sufficient to guarantee the protection grade, but other specific settings are required for grade 2 and grade 3, as described below. Selecting grade 2 or 3 affects some functional behaviour of the panel as required for the selected grade (e.g. for GRADE 3, the keyboard will not display the partition arming status unless previously authenticated with a user PIN).

The paragraph below provides detailed instructions for programming the panel in accordance with the regulation.



8.1.4.1 Compliance with EN50131 standard grade 2 and grade 3

Follow the instructions below to ensure that the devices comply with the regulations in force.

DEVICE ANTI-SABOTAGE

The peripherals on the bus must have enabled the tamper-proof devices.

If possible, the devices listed below must have been installed inside the panel enclosures, or they must be equipped with a device to protect against opening the casing (EN50131 grade 2) and against removal (EN50131 grade 3):

- Readers
- Expansions
- Dialer
- Radio receiver

All bus peripherals installed outside the panel enclosure must have the “no sabotage” attribute set to DISABLED

BALANCED ZONES

The lines for intrusion detection zones must be balanced:

- for EN50131 grade 2, with two termination resistors (double balancing), or they must be balanced with a single termination resistor(balanced) and have a device that ensures protection against opening the casing;
- for EN50131 grade 3, with three termination resistors (triple balancing) for grade 3 sensors with masking and fault function or, as for grade 2, with a terminal to manage a sensor fault separately.

CONTROL ZONES

This type of zone cannot be used because it does not comply with EN50131 grade 2 and 3, except when connected to key devices with more than 10000 combinations.

TYPE OF ZONE

The zones that comply with EN50131 grade 2 and 3 are INSTANT, PATH, DELAYED (or variants thereof), ANTI-MASKING, TAMPER, FAULT (or variants thereof).

The zones must be configured with SENSOR PARAMETERS - "Pulse duration" set to 400 ms (40 cs), and ALARM PARAMETERS - "Activation cycles" set from 3 to 10.

If the zones are of the DELAYED type (or variants thereof), they must be configured with ALARM PARAMETERS - "Input time" set to no longer than 45 s.

SABOTAGE EVENTS

Sabotage events must activate acoustic signalling (siren) for at least 3 minutes.

The PANEL - INTRUSION - "Maximum number of activations for sabotage" must be set to 0 (OFF).

PIN

All PIN codes must be 6-digit.

AUTO-INSERTIONS

When using automatic arming, the auto-arming warning times must be at least 1 minute.

PROFILES AND USERS

For EN50131 grade 3, the installer can only disarm a zone or erase fault and sabotage events if enabled by a level 2 user. If an operational user other than the installer is needed to perform these operations, at least one profile must be configured with "level 3" (mandatory), "Exclude zones" and/or "System recovery" attributes ENABLED, and at least one user must have that profile in order to perform the operations (all or some, depending on the attributes enabled in the profile) when enabled by a level 2 user from the corresponding keyboard menu (permissions).

REGULATION

The option PANEL - REGULATION - "Applied regulation" must be configured for the required grade, EN50131 grade 2 or grade 3. The panel will change some functions to comply with the regulation (limiting the indications on the keyboard and readers for unauthenticated users, requiring the right user level to erase fault and sabotage events, managing permissions for different user types for some operations).

MANDATORY OPTIONS

Some panel options must have a fixed configuration in order to comply with the regulation:

PANEL - COMMUNICATION: All notification delay options must be less than 1 minute.

PANEL - INTRUSION - GENERIC OPTIONS: The following options must remain disabled:

GENERIC OPTIONS

- ☐ Arming a zone in a multi-area even with only one area armed
- ☐ Treat antimask as broken
- ☐ See the disappearance as sabotage as well as a breakdown
- ☒ In disarmed, no internal siren for tampering
- ☒ Stop sirens when entering code
- ☐ Stop calls to code entry
- ☐ Disarm partitions in alarm upon entering the code
- ☐ System reset upon code entry
- ☐ Activates alternative mode of the area status light signaling reader
- ☒ Exclude area also for sabotage

PANEL - INTRUSION - REGULATION: The following options must remain disabled:

ADHERENCE TO THE REGULATION

- ☐ Always provide status indications on the keyboard
- ☐ Always provide status indications on readers
- ☐ In armed, no internal siren for tampering
- ☐ In armed, no external siren for tampering

System

The software has a section to perform the automatic check of all the above-listed indications. If you select one of the regulation levels of the APPLIED REGULATION parameter, you can click on the adjacent symbol to open a window; press the "Check" key to highlight any criticalities to be addressed to ensure the system is compliant with a red or yellow symbol, and possibly even a sub-list.

8.2 SYSTEM – Partitions

This section serves to arm the partitions used and set all the parameters.

A single partition is enabled *by default*

To add a partition, click the  key and enter the ID and description.

After creating the partition, you can set the parameters described below.

Description of the partition

ATTRIBUTES

Erase memories upon insertion:

As soon as the partition is armed in any mode, the alarm/sabotage memories for the partition are automatically erased (not faults). Clearly the end result will depend on the profile of the user performing the operation (partitions and profile options), and on the active regulation grade (see the REGULATION paragraph).

Clear phone queue on disarming:

The notification queue is cleared as soon as the partition is disarmed.

Disables pre-alarm on keypad

Disables the signal on the keypad which warns of an imminent self-start.

If this option is not selected, the self-starts are signalled on the keypad with an alert time equal to the pre-alert time for self-starts parameter (see para. 8.1.3 SYSTEM – Panel – INTRUSION).

Minimum group of cross zones:

Number of zones that must be in the alarm state to actually activate the alarm. (*)

Enable the zone cross function:

The zone cross function (AND) is enabled for the partition: Two or more zones with the **Zone Cross** function activated only generate an alarm if at least the **Minimum group of cross zones** are actually in the alarm state within **Max time between 2 cross zones** (*).

Max time between 2 cross zones:

This is the time (in seconds) within which at least the **Minimum group of cross zones** are actually in the alarm state. (*)

(*) The cross zones (AND) and the conditions for generating the corresponding alarms constitute a precise function. Normally, when a zone enters the alarm state, it generates the corresponding alarm event, which activates outputs, notifications, etc.

The zone cross function serves to define:

- a group of zones (united by the **Zone Cross** option); for example, 6 zones have this option
- the time **Max time between 2 cross zones**; for example, 40 seconds
- the number **Minimum group of cross zones**; for example, 3

In this case, if one (of the 6 zones) enters the alarm state, the zone alarm event is NOT generated, but a 40 second timer is activated; if another 2 zones (of the 6, making a total of 3 zones) enter the alarm state within these 40 seconds, alarm events are then generated for all 3 zones.

Patrol time:

The partition **Patrol** function serves to simultaneously disarm the zones in a patrol user's partition after entering the PIN (to allow an inspection round). This does not apply to zones with the "ignore patrol" attribute (the partitions will remain armed, but the zones will not generate an alarm if triggered). The zones automatically return to the armed state at the end of the Patrol time (expressed in minutes) (the patrol user can in any case manually restore the armed state from the keypad before this time lapses)

Auto-arming delay time:

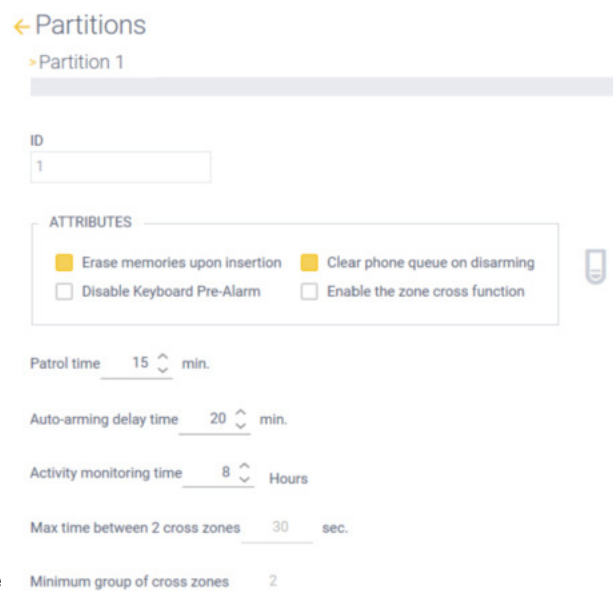
This is the time (in minutes) by which the programmed auto-arming will be delayed. In practice, for example, it is the time required when working overtime.

Activity monitoring time:

If a partition contains zones with the "Activity test" option enabled, when the partition is not armed, a lack of activity in those zones for longer than the time programmed for that parameter (in minutes) generates a "no activity" event, which serves to send notifications and/or control a terminal programmed as an output (e.g. the sensors in a partition of a shop should always detect activity during opening hours with the alarm disarmed). The time measurement restarts whenever the partition is disarmed.

Integration with the By-me system

For full details, see para. "Integration of By-alarm and video door entry devices with By-me Plus applications" in the By-me Plus system manual.



8.3 SYSTEM – Time exceptions

This section serves to define the time exceptions (i.e. time programs) for arming partitions, automations and weekly user access plans.

The time exceptions serve to define the dates on which the auto-arming and/or the automations do not need to be performed.

To create a new time exception, click the  key and set the parameters.

A time exception has the following parameters:

- exception start month and day
- exception end month and day

Once you have defined the time exceptions, then enable them for them to become active, as specified in para. 11.3 AUTOMATION – Auto-arming (and Automations).

Terminals

9. TERMINALS

This section serves to set the zone and output parameters.

In general, zones are system input signals, i.e. wired and/or radio signals generated by the following devices:

- unauthorised intrusion
 - infrared detectors
 - dual technology detectors
 - magnetic contacts
- robbery
- fire sensors
- environment sensors

In general, outputs are signals that the system generates to activate:

- acoustic signalling
 - sirens
 - buzzers
- light signalling
- generic actuators
 - relays
 - gate openers

9.1 TERMINALS – Zones

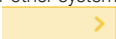
This serves to program, create or delete system zones.

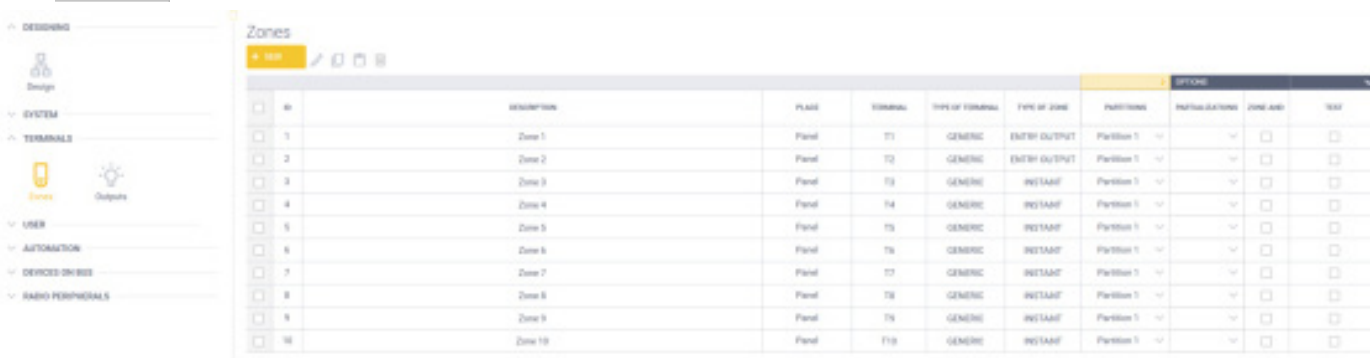
Each zone can be in one of the following states:

- Armed: zone monitored when the system is activated, if it is in the selected partition(s);
- Disarmed: zone not monitored when the system is activated. The zone is disarmed permanently until it is explicitly rearmed by a user with sufficient rights;
- Inhibited: zone not monitored when the system is activated. The zone is disarmed temporarily, and is rearmed automatically after the next time it is disarmed


In the main screen, all configured zones are displayed in a grid in which some columns contain display-only parameters and others contain parameters that are both displayed and can be edited.

As for other system options, double-clicking a zone opens a page containing details about that zone.

Click  just above the PARTITIONS column to expand the column and show details of all available partitions.



ID	DESCRIPTION	PLACE	SIGNAL	TYPE OF SIGNAL	TYPE OF ZONE	PARTITIONS	PARTITION ACTIONS	ZONE AND	TEST
1	Zone 1	Panel	T1	GENERIC	ENTER OUTPUT	Partition 1			
2	Zone 2	Panel	T2	GENERIC	ENTER OUTPUT	Partition 1			
3	Zone 3	Panel	T3	GENERIC	INSTANT	Partition 1			
4	Zone 4	Panel	T4	GENERIC	INSTANT	Partition 1			
5	Zone 5	Panel	T5	GENERIC	INSTANT	Partition 1			
6	Zone 6	Panel	T6	GENERIC	INSTANT	Partition 1			
7	Zone 7	Panel	T7	GENERIC	INSTANT	Partition 1			
8	Zone 8	Panel	T8	GENERIC	INSTANT	Partition 1			
9	Zone 9	Panel	T9	GENERIC	INSTANT	Partition 1			
10	Zone 10	Panel	T10	GENERIC	INSTANT	Partition 1			

Click  to add a new zone, and the window will present the parameters to be set in order to configure it correctly in sequence. Specifically, the sequence will show where the new zone is to be located (on a panel, expansion, keyboard or radio device terminal) and the type of zone you want.

PARAMETERS

Description: text that identifies the zone in notifications and in its status display.

Place: Defines where you want to create the zone. The available choices depend on what peripherals have actually been created in the project. The panel will always be available, while Expansion, Keyboard and Sensor (radio) will be available if at least one device is installed in the system.

Terminal: This serves to select a precise peripheral, either wired or radio, on which to create the zone. All peripherals of the previously selected type will be displayed. The image above shows a list of available expansions or radio sensors.

Type of terminal: **ONLY IF THE PERIPHERAL TYPE is Panel/Expansion/Keyboard**, i.e. a wired peripheral; it is the step that sets for which of the available peripheral terminals the zone will be created. Only the peripheral terminals that are actually available will be displayed.

Type of terminal: **ONLY IF THE PERIPHERAL TYPE is Sensor (radio)**; it is the step in which you set for which of the radio peripheral signal/terminals the zone will be created. Only the peripheral terminals that are actually available will be displayed.

Terminals

Type of zone: This serves to set the terminal/zone type to be added. Once this parameter has been set, it CANNOT be changed later.

Note that only options that apply the device for which you are creating the zone will be displayed; the options are as follows:

- **ZONE:** generic input able to detect slow variations in the detector signal; this type is suitable, for example, for magnetic contact or detector. Typically, an alarm signal is generated if the input is active/unbalanced continuously for 300 ms.
- **SHUTTER:** input able to detect the fast variations typical of rope detectors applied to shutters. The alarm signals consist of numerous very short “clicks” in quick succession.
- **INERTIAL:** similar to **SHUTTER**, input able to detect the fast variations typical of the vibration detectors or accelerometers that can be applied to windows. In this case, the alarm signals typically consist of short, sharp pulses.
- **CONTROL:** the detected signal is slow (similar to **ZONE**), but does not generate alarm signals. This input is intended to perform control functions.

N.B. Consider that, in general, the zone parameters screen adapts automatically to the zone type; radio zones also adapt to the type of “sensor” in the zone (e.g. only the applicable parameters will be shown, depending on whether the zone sensor is a magnetic contact or passive infrared sensor).

The zone details page is described below.

You can edit the zone description in the “**Zone x**” box.

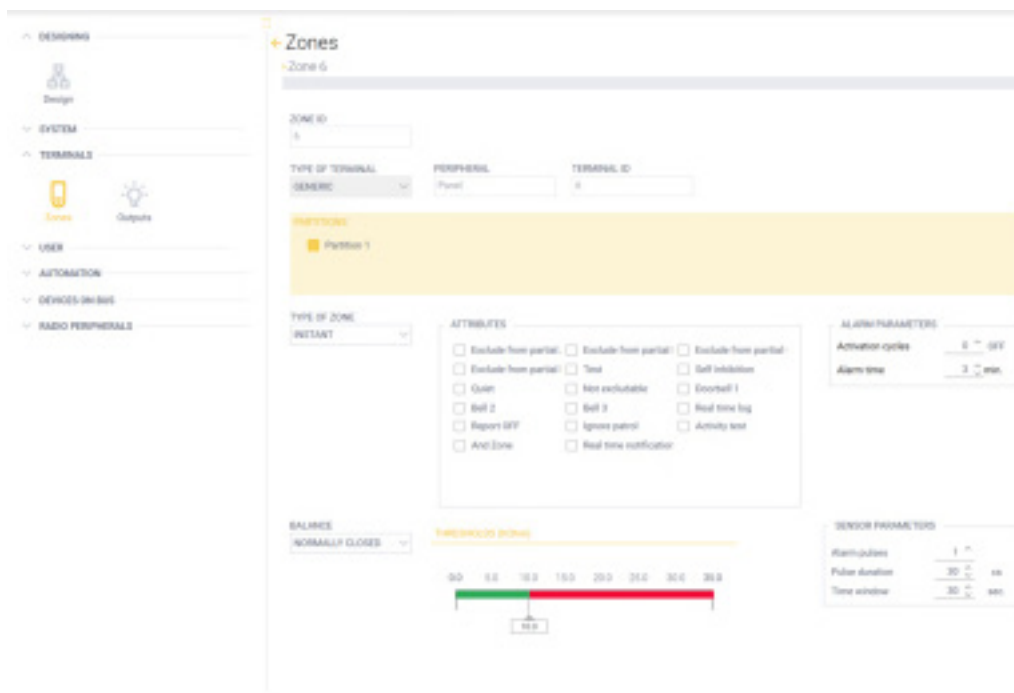
ZONE ID is NOT editable. It indicates the zone location.

PARTITIONS.

This serves to set the partition to which the zone belongs.

TYPE OF ZONE.

The drop-down menu that appears depends on how the *Type of zone* parameter is set when creating the new zone; it therefore depends on whether **ZONE**, **SHUTTER**, **INERTIAL** or **CONTROL** was selected.



The **ATTRIBUTES** option also depends on the selection made in the drop-down menu.

• *Type of zone* = **ZONE**

The drop-down menu will contain:

NOT USED
 INSTANT
 PATH
 INSTANT PATH
 INSTANT RESTART OUTPUT TIME
 DELAYED
 INSTANT/DELAYED
 DELAYED/PATH
 INSTANT/EMERGENCY EXIT
 ANTI-MASKING
 ORE24
 TAMPERING
 PANIC
 ROBBERY
 FIRE
 FLOODING
 GAS
 CO
 HIGH TEMPERATURE
 LOW TEMPERATURE
 TECHNICAL
 FAULT
 ROBBERY FAULT
 SIGNALLING DEVICE FAULT

Terminals

• **Type of zone = SHUTTER or INERTIAL**

The drop-down menu will contain:

NOT USED

INSTANT

PATH

INSTANT PATH

INSTANT RESTART OUTPUT TIME

DELAYED

INSTANT/DELAYED

DELAYED/PATH

INSTANT/EMERGENCY EXIT

ORE24

TAMPERING

TECHNICAL

The table below illustrates the meanings of the attributes when *Type of zone* = ZONE, SHUTTER or INERTIAL

Type of zone = ZONE/SHUTTER or INERTIAL		
Type	Alarms generated	Description
NOT USED	-	Not considered in any processing by the panel, even if the terminal remains where it is housed as configured (occupied).
INSTANT	INTRUSION	If the zone is activated electrically, the panel will generate a zone open event . If the partition to which the zone belongs is armed and the zone is activated, the panel will generate an intrusion alarm .
PATH	INTRUSION	If an output time or input time is running in the partition to which the zone belongs and the zone is activated, the panel will generate a zone open event . If there are no output/input times running in the partition to which the zone belongs, the zone will behave as an <i>instant</i> zone.
INSTANT + PATH	INTRUSION	If the partition to which the zone belongs is armed, the zone will behave as a <i>path</i> zone. If the partition to which the zone belongs is partially armed, the zone will behave as an <i>instant</i> zone.
INSTANT RESTART OUTPUT TIME	INTRUSION	If an output time is running in the partition to which the zone belongs and the zone is activated, the panel will restart the output time. When the output time lapses, the zone will behave as an <i>instant</i> zone.
DELAYED	INTRUSION	If the zone is activated/restored electrically, the panel will generate a zone open/restored event . If the partition to which the zone belongs is armed, the panel will generate an output time started event regardless of the electrical state of the zone. If an input time is running in the partition to which the zone belongs and the zone is activated, the panel will generate an input time started event , and if the zone is activated during this time, the panel will generate a zone open event . If the partition has not been disarmed when the input time lapses, the panel will generate an intrusion alarm , regardless of the zone activation state.
INSTANT/DELAYED	INTRUSION	If the partition to which the zone belongs is armed, the zone will behave as a <i>delayed</i> zone. If the partition to which the zone belongs is partially armed, the zone will behave as an <i>instant</i> zone.
DELAYED/PATH	INTRUSION	If the partition to which the zone belongs is fully armed, the zone will behave as a <i>path</i> zone. If the partition to which the zone belongs is partially armed, the zone will behave as a <i>delayed</i> zone.
INSTANT/EMERGENCY EXIT	- INTRUSION - EMERG OUTPUT	Suitable for managing EMERGENCY OUTPUTS. If the partition to which the zone belongs is armed, the zone will behave as an <i>instant</i> zone. If the partition to which zone belongs is armed and the zone is activated, the panel will generate an emergency output alarm .
ANTI-MASKING	- SABOTAGE - FAULT	The zone is managed as a <i>tamper</i> zone, except that a system option (*) is enabled to interpret the alarm as a fault. (*) "Process masking as fault"
ORE24	INTRUSION	If the zone is activated, the panel will generate an intrusion alarm , regardless of the armed state of the partition to which the zone belongs.
TAMPERING	TAMPERING	If the zone is activated, the panel will generate a tamper alarm , regardless of the armed state of the partition to which the zone belongs.
PANIC	PANIC	If the zone is activated, the panel will generate a panic alarm , regardless of the armed state of the partition to which the zone belongs.
ROBBERY	ROBBERY	If the zone is activated, the panel will generate a robbery alarm , regardless of the armed state of the partition to which the zone belongs.
FIRE	FIRE	If the zone is activated, the panel will generate a fire alarm , regardless of the armed state of the partition to which the zone belongs.
FLOODING	FLOODING	If the zone is activated, the panel will generate a flooding alarm , regardless of the armed state of the partition to which the zone belongs.
GAS	GAS	If the zone is activated, the panel will generate a gas alarm , regardless of the armed state of the partition to which the zone belongs.

Terminals

Type	Alarms generated	Description
CO	CO	If the zone is activated, the panel will generate a CO (carbon monoxide) alarm , regardless of the armed state of the partition to which the zone belongs.
HIGH TEMPERATURE	HIGH TEMPERATURE	If the zone is activated, the panel will generate a high temperature alarm , regardless of the armed state of the partition to which the zone belongs.
LOW TEMPERATURE	LOW TEMPERATURE	If the zone is activated, the panel will generate a low temperature alarm , regardless of the armed state of the partition to which the zone belongs.
TECHNICAL		Does not belong to any alarm category. If the zone is activated, the panel will generate a zone open event , regardless of the armed state of the partition to which the zone belongs.
FAULT	- FAULT	If the zone is activated, the panel will generate a zone fault event , regardless of the armed state of the partition to which the zone belongs.
ROBBERY FAULT	- FAULT	If the zone is activated, the panel will generate a zone robbery fault event , regardless of the armed state of the partition to which the zone belongs.
FAULT SIGNALLING DEVICE	- FAULT	If the zone is activated, the panel will generate a signalling device fault event , regardless of the armed state of the partition to which the zone belongs.

• **Type of zone = CONTROL**

The drop-down menu will contain:

NOT USED

PULSE CONTROL

ON/OFF CONTROL

PULSE DELAY CONTROL

ON/OFF DELAY CONTROL

The table below illustrates the meanings of the attributes when *Type of zone = CONTROL*

Type of zone = CONTROL		
Type	Alarms generated	Description
NOT USED		Not considered in any processing by the panel, even if the terminal remains where it is housed as configured (occupied).
PULSE CONTROL		Suitable for managing a pulse keyswitch. If the partition to which the zone belongs is disarmed and the zone is activated, the panel will generate a total partition arming command. If the partition to which the zone belongs is armed and the zone is activated, the panel will generate a partition disarming command.
ON/OFF CONTROL		Suitable for managing a two-position stable keyswitch. If the zone is set to the active state, the panel will generate a total partition arming command. If the zone is set to the standby state, the panel will generate a partition disarming command.
PULSE DELAY CONTROL		Suitable for managing a pulse keyswitch. If the zone is activated, the panel will generate a command to delay the next programmed auto-arming event by a preset time.
ON/OFF DELAY CONTROL		Suitable for managing a two-position stable keyswitch. If the zone is set to the active state, the panel will generate a command to disable all programmed auto-arming events for the partition. If the zone is set to the standby state, the panel will generate a command to re-enable all programmed auto-arming events.

NOTE: When arming with a control zone, it will be of the TOTAL type (NOT IMMEDIATE), i.e. it will include normal operation of any delayed zones.

The table below lists all the zone attributes.

N.B. ATTRIBUTES will only show the attributes that are consistent with the previous selections, depending on the type of zone.

ZONE ATTRIBUTES	
Attribute	Description
PARTIAL A	With this attribute, if the partition to which the zone belongs is armed in Partial A, B, C or D mode, the panel will not process a zone activation as an alarm.
PARTIAL B	
PARTIAL C	NOTE: "Instant/Delayed", "Instant/Path" and "Delayed/Path" zones cannot activate the internal A/B/C/D attributes simultaneously. Dual operation will only apply to partial arming of zones that have not been defined as internal.
PARTIAL D	

Terminals

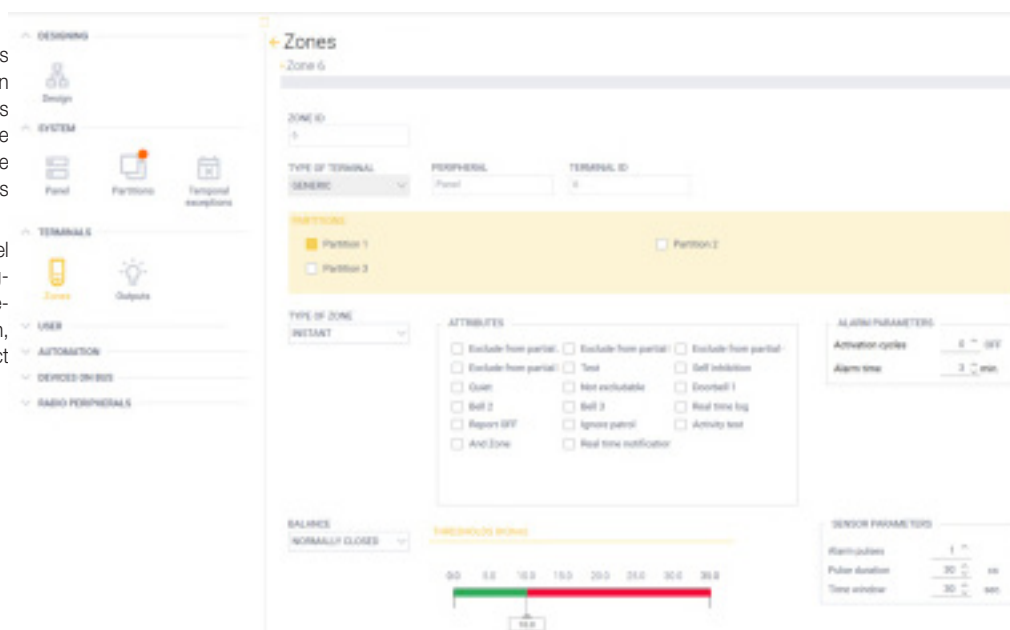
Attribute	Description
TEST	With this attribute, the panel will process all changes of zone state, compatibly with the zone type. However if the zone triggers an alarm, it will not be notified via the physical units, but just logged in the event memory and sent to the monitoring station or a specific user via the communication channels (with a suitable code specifying the test status of the detector).
INPUT ONLY	With this attribute, the zone behaves exclusively as a delayed input. NOTE: this attribute CANNOT be used together with the following attributes: <ul style="list-style-type: none"> • Output only • Last output • Viewable
OUTPUT ONLY	With this attribute, the zone behaves exclusively as a delayed output. NOTE: this attribute CANNOT be used together with the “Input only” attribute.
Output termination	This attribute applies if the zone changes from an active state to a standby state, while the output times are active in the partition to which it belongs. In this case, all partition output times are reset and the partition will be armed within 5 seconds. NOTE: this attribute CANNOT be used together with the “Input only” attribute.
VIEWABLE	This attribute applies if the zone is active and the partition to which it belongs is disarmed or being armed. In this case, the keyboard explicitly indicates the zone open state.
SELF INHIBIT	This attribute applies if the partition to which the zone belongs is armed when the zone is active. In this case, the zone is inhibited until the next time the partition to which it belongs is disarmed.
QUIET	This attribute applies if when the zone is activated, it should generate an alarm that is consistent with the type of zone activated. In this case, the zone alarm will not be notified via the physical outputs, but just to the user or an ARC (if the “Report OFF” attribute is not selected) via the communication channels. The zone is in any case recorded in the event log if the “Disable Log” attribute is not selected.
NOT EXCLUDABLE	The intrusion zone cannot be inhibited and/or disabled by the user (even if it belongs to a user profile enabled to do so).
BELL 1	This attribute applies if the zone is active and the partition to which it belongs is disarmed. In this case, the panel will sound the buzzer with the appropriate pattern on the keyboard belonging to the partition. NOTE: the three doorbell types are mutually exclusive.
BELL 2	
BELL 3	
REAL TIME LOG	With this attribute, any change of electrical state in the zone will be recorded in the internal event memory.
Report OFF	With this attribute, zone events relevant to the type and armed state of the partition to which the zone belongs will not be sent remotely to a monitoring station.
PATROL	This attribute applies when the partition to which the zone belongs is disarmed by a patrol user. In this case, only the zones with the patrol attribute will be disarmed for up to the preset time
ACTIVITY TEST	This attribute only applies if the partition to which the zone belongs is disarmed. In this case, the panel generates a NO ACTIVITY ALARM if the zone is not activated at least once within a programmable time window (*). (*) System option
SELF TEST	With this attribute, the panel generates a ZONE FAULT signal if the zone is not activated at least once within a week.
ARMING ONLY	For pulse key arming control zones, this indicates that the action is arming only. NOTE: this attribute CANNOT be used together with the following attributes: <ul style="list-style-type: none"> • Disarming only
DISARMING ONLY	For pulse arming control zones, this indicates that the action is arming only. NOTE: this attribute CANNOT be used together with the following attributes: <ul style="list-style-type: none"> • Arming only • Forced arming
FORCED ARMING	For arming control zones, this indicates that the arming action must take place even when a partition is not ready. Arming is forced in the event of faults or sabotage; however arming does not take place if there is an open zone that would cause an alarm when armed EN50131 does not allow the use of a control zone, so these cases do not apply when regulation is active. NOTE: this attribute CANNOT be used together with the following attributes: <ul style="list-style-type: none"> • Disarming only
And Zone	With this attribute, the zone is part of a group zones that will only generate an alarm if at least G zones in the group are activated not more than T seconds apart. The alarm type is defined by the nature of the first zone activated. G and T are partition parameters.
REAL TIME NOTIFICATION	Users with zone RT in their notifications profiles can receive real time zone notifications. They are in any case replicated in the Cloud.

Terminals

ALARM PARAMETERS.

Activation cycles: the number alarms that can be generated by the zone when armed. If, for example, this parameter is set to 4, the zone can generate no more than 4 alarms once it has been armed. The counter is reset the next time the zone is disarmed.

Alarm time: the time for which the panel considers the alarm to be active. If a magnetic contact is opened then closed immediately and this parameter is set to 1 min, the panel will keep the magnetic contact "logically violated" for 1 minute.



BALANCE.

The following balancing options are available:

- NORMALLY OPEN
- NORMALLY CLOSED
- SINGLE BALANCING
- DOUBLE BALANCING
- TRIPLE BALANCING
- CUSTOM

SENSOR PARAMETERS.

These are advanced parameters that set how the signal is processed in order to generate the alarm event.

An alarm signal is normally generated when a detector is activated for about 300 ms.

In this case:

- Alarm pulses = 1
- Pulse duration = 30 cs (30 cs = 300 ms)
- Time window = not used

In some situations, it may be useful to filter the alarm generation further; for example, for an infrared detector in an environment that could generate false alarms, the alarm can be generated if three 700 ms pulses are "detected" no more than 40 seconds apart; in that case:

- Alarm pulses = 3
- Pulse duration = 70 cs (70 cs = 700 ms)
- Time window = 40 sec

Integration with the By-me system

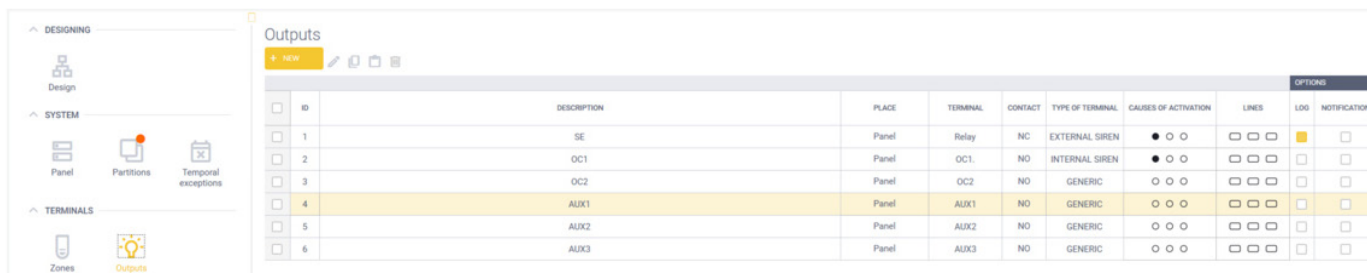
For full details, see para. "Integration of By-alarm and video door entry devices with By-me Plus applications" in the By-me Plus system manual.

9.2 TERMINALS – Outputs

This section serves to program, create or delete outputs.

In the main screen, all configured outputs are displayed in a grid in which some columns contain display-only parameters and others contain parameters that are both displayed and can be edited.

As for other system options, double-clicking an output opens a page containing details.



ID	DESCRIPTION	PLACE	TERMINAL	CONTACT	TYPE OF TERMINAL	CAUSES OF ACTIVATION	LINES	LOG	NOTIFICATION
1	SE	Panel	Relay	NC	EXTERNAL SIREN	● ○ ○	□ □ □	□	□
2	OC1	Panel	OC1	NO	INTERNAL SIREN	● ○ ○	□ □ □	□	□
3	OC2	Panel	OC2	NO	GENERIC	○ ○ ○	□ □ □	□	□
4	AUX1	Panel	AUX1	NO	GENERIC	○ ○ ○	□ □ □	□	□
5	AUX2	Panel	AUX2	NO	GENERIC	○ ○ ○	□ □ □	□	□
6	AUX3	Panel	AUX3	NO	GENERIC	○ ○ ○	□ □ □	□	□

Click  **NUOVA** to add a new output, and the window will present the parameters to configure it correctly in sequence.

Terminals

Place, *Terminal* and *Terminal type* are the same as the settings made when creating a new zone.

Type of terminal: Services to set the output type and, unlike for zones, it can also be changed later.

The output details page is described below.

You can edit the output description in the **Outputs** box.

OUTPUT ID is not editable in this page.

TYPE OF TERMINAL: as explained previously, this can be *GENERIC*, *OUTDOOR SIREN*, *INDOOR SIREN*

CATEGORY: is a parameter that may be useful for apps. Possible values are:

- GENERIC
- GATE
- SIGNALLING DEVICE

ATTRIBUTES

Log: if enabled, every output activation/deactivation will be saved in the event logger.

Notification: if enabled, every output activation/deactivation will be notified.

CONTACT AT REST: is the output state, which can be NC=normally closed or NO=normally open.

OUTPUT DRIVE CLASS: is a parameter to set which users can activate/deactivate this output manually. (See the description of Profiles in the USER section, and specifically the OUTPUT DRIVE CLASS). A profile with an OUTPUT DRIVE CLASS higher than or equal to the OUTPUT DRIVE CLASS of the output can activate/deactivate it.

LINES

These are the lines to which the output belongs. If a line is "activated" (with the PIN on the keyboard, transponder key, etc.) and the output belongs to this line, the output will be activated.

ACTIVATION DEFAULT

This is the default mode with which the output is activated:

• CONTINUOUS

The output is activated by an ON command and deactivated by an OFF command.

BLINK: if enabled, the output is ON for 0.5 s and OFF for 0.5 s when it is active.

IGNORE RESTORE: if enabled, the output is NOT deactivated when the event that activated it ends. To deactivate it, the user must do so manually or perform a system/memory reset

• PULSE

The output is activated by an ON command and will be deactivated automatically after the set time or following an OFF command.

BLINK: if enabled, the output is ON for 0.5 s and OFF for 0.5 s when it is active.

CAUSES OF ACTIVATION

This section serves to set the events that activate the output.

Click **+ NUOVA** to create the activation causes; up to three can be set.

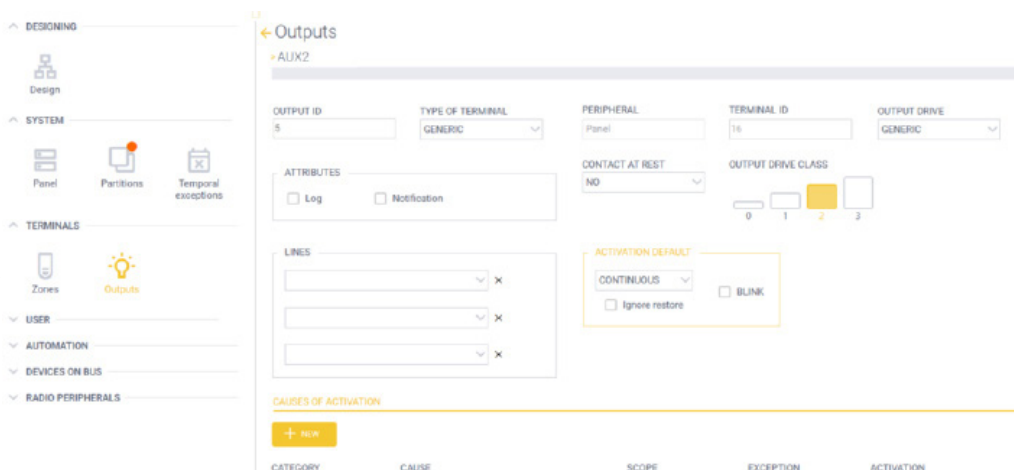
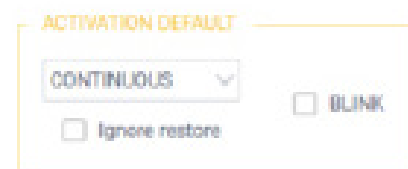
CATEGORY

This section serves to set the generic event that activates the output.

The **CAUSE** and **EXTENT** menus will adapt to selection made here.

The **X** symbol serves to delete the **CAUSE OF ACTIVATION**.

The **EXCEPTION** and **ACTIVATION** options are common to all **CATEGORIES**.

Terminals

The table below lists all possible configurations.

CATEGORY	CAUSE	EXTENT
INTRUSION_ALARM	<input type="checkbox"/> INTRUSION <input type="checkbox"/> SABOTAGE <input type="checkbox"/> SYSTEM SABOTAGE <input type="checkbox"/> ROBBERY <input type="checkbox"/> INTRUSION (CONF) <input type="checkbox"/> ROBBERY (CONF) <input type="checkbox"/> PANIC	<input type="checkbox"/> All <input type="checkbox"/> Partition 1 <input checked="" type="checkbox"/> Partition 2 <input checked="" type="checkbox"/> Partition 3
EMERGENCY_ENVIRONMENTAL_ALARM	<input type="checkbox"/> FIRE <input type="checkbox"/> FLOODING <input type="checkbox"/> GAS <input type="checkbox"/> CO <input type="checkbox"/> HIGH TEMPERATURE <input type="checkbox"/> LOW TEMPERATURE <input type="checkbox"/> EMERGENCY <input type="checkbox"/> MEDICAL AID	<input type="checkbox"/> All <input type="checkbox"/> Partition 1 <input checked="" type="checkbox"/> Partition 2 <input checked="" type="checkbox"/> Partition 3
PARTITION_STATE ⁽¹⁾	STATUS ENTERED TOTAL ARMED STATUS PARTIAL ARMED STATE STATUS DISARMED ARMING PHASE STATUS READY TO ARM STATUS NOT READY TO INSERT PRESENCE OF ZONES EXCLUDED PRESENCE OF ALARM MEMORIES EMERGENCY EXIT OPENING LACK OF ACTIVITY AREA INSERTION FAILED	<input type="checkbox"/> All <input type="checkbox"/> Partition 1 <input checked="" type="checkbox"/> Partition 2 <input checked="" type="checkbox"/> Partition 3
INDICATORS	IN SERVICE IN PROGRAMMING PIN / KEY RECOGNIZED WRONG KEY CODE	//
OUTPUT_ZONE_STATE	ZONE ALARM ZONE SABOTAGE REAL TIME ZONE OUTPUT REAL TIME	<input type="checkbox"/> Zone 1 <input type="checkbox"/> Zone 2 <input type="checkbox"/> Zone 3 <input type="checkbox"/> Zone 4 <input type="checkbox"/> Zone 5 <input type="checkbox"/> Zone 6 <input type="checkbox"/> Zone 7 <input type="checkbox"/> Zone 8 <input type="checkbox"/> Zone 9 <input type="checkbox"/> Zone 10
FAULT ⁽²⁾	<input type="checkbox"/> LACK OF AC <input type="checkbox"/> PANEL POWER SUPPLY PROBLEM <input type="checkbox"/> PANEL BATTERY PROBLEM <input type="checkbox"/> BUS PROBLEM <input type="checkbox"/> SYS PERIPHERAL PROBLEM ON BUS <input type="checkbox"/> PROBLEM ON OUTPUTS AND AUX <input type="checkbox"/> RADIO BLACKOUT <input type="checkbox"/> GSM LINK DOWN <input checked="" type="checkbox"/> LINK MONITORING STATION DOWN <input type="checkbox"/> Loss of date / time <input type="checkbox"/> ZONE FAILURE <input type="checkbox"/> BUS PERIPHERAL PROBLEM	//

(1) The PARTITION_STATE category serves to select specific partition conditions as causes of output activation. The state is recognised/signalled when the partition actually enters the state given in the description:

STATUS ENTERED	the partition is armed in any mode, TOTAL or PARTIAL A/B/C/D
TOTAL ARMED STATUS	the partition is armed in TOTAL mode
PARTIAL ARMED STATE	the partition is armed in PARTIAL A/B/C/D mode
STATUS DISARMED	the partition is disarmed

Terminals

ARMING PHASE	the partition is currently being armed/disarmed; an input time or output time is running
STATUS READY TO ARM	in the partition, all zones to be armed in TOTAL mode are in the standby state; therefore, the partition can be armed in TOTAL mode
STATUS NOT READY TO INSERT	in the partition, at least one of the zones to be armed in TOTAL mode is not in the standby state; therefore, the partition cannot be armed in TOTAL mode
PRESENCE OF ZONES EXCLUDED	in the partition, there is at least one inhibited/isolated zone
PRESENCE OF ALARM MEMORIES	in the partition, there is an alarm memory that has not yet been erased
EMERGENCY EXIT OPENING	in the partition, there is at least one EMERGENCY EXIT zone in the alarm state
LACK OF ACTIVITY AREA	in the partition, no zone has changed state within the <i>Activity monitoring time</i> . It indicates a potentially abnormal condition because the detectors should detect activity in the partition within the <i>Activity monitoring time</i> .
INSERTION FAILED	in the partition, arming was not possible (total or partial) because of conditions that prevented it (e.g. faults, sabotage, disappearances, etc.)

(2) The FAULT category serves to select one or more faults detected by the system as causes of output activation:

LACK OF AC	there is no primary mains power supply (230V~)
PANEL POWER SUPPLY PROBLEM	the power supply unit in the panel has various faults
PANEL BATTERY PROBLEM	the lead backup battery in the panel is disconnected, not working or low
BUS PROBLEM	the BUS has overcurrents, overvoltages or short-circuits.
SYS PERIPHERAL PROBLEM ON BUS	at least one of the peripherals without partitions: - art. 03808/03819 expansions - art. 03810/ 03820 LTE dialers - art. 03831/03832/03840 radio transceivers and repeaters - art. 03827/03830 BUS and radio sirens has disappeared
PROBLEM ON OUTPUTS AND AUX	at least one output terminal or AUX is not activated or has overcurrents or short-circuits
RADIO BLACKOUT	radio jamming has been detected on the transceiver or on a repeater
GSM LINK DOWN	the LTE dialer is not connected to an operator
LINK MONITORING STATION DOWN	the SIA-IP receiver (monitoring stations) is unreachable
LOSS OF DATE / TIME	the panel may have lost the correct date/time following a reboot
ZONE FAILURE	the following conditions generate a ZONE FAILURE signal: - a FAULT, ROBBERY FAULT or SIGNALLING DEVICE FAULT zone has been violated - both contacts are unbalanced in a TEOL (triple) balancing zone - the antimask contact is unbalanced in a TEOL (triple) balancing zone and the Treat antimask as broken system option is selected (see the SYSTEM – Panel – INTRUSION) paragraph
BUS PERIPHERAL PROBLEM	at least one of the peripherals to which partitions can be assigned: - art. 03817/03818 keyboards - art. 03824 readers has disappeared
RADIO PERIPHERAL PROBLEM	at least one radio device has disappeared
RADIO SENSOR LOW BATTERY	the battery in at least one radio device is almost flat

EXCEPTION

NONE: No exception is applied. The output is activated as soon as the activation command is received.

DELAY: The output is activated the set number of seconds after receiving the activation command.

STAY_ONLY_DELAY: This exception only has effect if the CATEGORY is INTRUSION_ALARM. In this case, the output is only activated after the specified delay if one of the partitions was armed in STAY/PARTIAL mode.

DO_NOT_ACTIVATE_STAY: This exception only has effect if the CATEGORY is INTRUSION_ALARM. The output is NOT activated in the event of an alarm from at least one partition armed in STAY/PARTIAL mode. For example: the siren will not be activated if an intrusion alarm occurs and the partition is armed in STAY/PARTIAL mode (someone is at home).

ACTIVATION TYPE

This parameter serves to select the output activation mode.

DEFAULT: the output will follow the default programming.

CUSTOM: the output will activate in the mode specified here, ignoring the set default output programming.

N.B. If there are 2 or 3 ACTIVATION CAUSES, the 2 or 3 causes are considered to be in order of priority. The first cause at the top has the highest priority. If there are 2 or 3 causes, **AND **OR** can be selected at the top right**

OR: when any of the ACTIVATION CAUSES occurs, the corresponding output action is performed.

Considering the adjacent figure, if a FAULT occurs due to a PANEL BATTERY PROBLEM, the output will be activated as a 3 s PULSE. If an INTRUSION ALARM occurs in Partition 1 during this time, since this cause has a higher priority, the output will be activated in its default mode, “overwriting” the FAULT mode.

Terminals

AND: the output action is only performed when all of the ACTIVATION CAUSES occur, following the setting of the first cause at the top.

CAUSES OF ACTIVATION

AND

OR

1

new

CATEGORY	CAUSE	SCOPE	EXCEPTION	ACTIVATION
INTRUSION ALAR	INTRUSION	Partition 1	NONE	DEFAULT <input checked="" type="radio"/> CUSTOM <input type="radio"/>
EMERGENCY EN	GAS	Partition 1	NONE	DEFAULT <input checked="" type="radio"/> CUSTOM <input type="radio"/> <div>CONTINUOUS</div> <div><input type="checkbox"/> ignore restore <input type="checkbox"/> BLINK</div>
BROKEN DOWN	PANEL POWER SUPPLY PROBLEM		NONE	DEFAULT <input checked="" type="radio"/> CUSTOM <input type="radio"/> <div>PULSE</div> <div>3 sec. <input type="text"/></div> <div><input type="checkbox"/> BLINK</div>

10. USER

This section serves to create and define:

- Profiles (of users)

A profile is a set of data and permissions that define how a user can operate in the system.

- Users

A user generally identifies a person with whom a profile has been associated; in addition to the characteristics of their profile, a user is associated with other more strictly personal parameters (such as the PIN) that determine the available functions and identify the user.

- Alarm Receiving Centres (ARCs)

For each reception and control centre with which the panel has to interact, configuration parameters can be programmed, as agreed with the ARC managers.

- Notifications that the system sends

When events occur, the burglar alarm system can send various types of notification to users and reception/control centres (ARCs).

The characteristics of each user can be configured according to what that user is authorised to do in the system.

Notifications can be sent to users via text messages, voice messages and push notifications (on dedicated applications). Notifications can also be sent to reception/control centres (ARCs) via SIA-IP (a data transmission protocol dedicated to burglar alarm systems).

10.1 USER – Profiles

The summary screen lists all the profiles that have been created, and the various columns show the most significant parameters for each profile.

The summary table can also be used to edit the displayed parameters by clicking directly on the parameter.

DESIGNING

Design

SYSTEM

TERMINALS

USER

Profiles

Users

User notifications

Profiles

NEW

					OPTIONS						
<input type="checkbox"/>	ID	DESCRIPTION	PARTITIONS	CLASS	TOTAL	PARTIAL ARMING	DISARMING	RESTORATION	EXCLUDE ZONES	LOGGER	ENABLING
<input type="checkbox"/>	3	ADMINISTRATOR	Partition 1	3	<div></div>	EXCLUDE FROM PARTIAL A...	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<input type="checkbox"/>	4	NORMAL	Partition 1	0	<div></div>		<div></div>	<div></div>	<div></div>	<div></div>	<div></div>

To create a new profile, click the **+ NUOVA** key and set the description and output drive class (the meaning of which will be explained in the parameters below).

To open the full profile page, double-click anywhere on the line of the profile you want.

The individual parameters are described below.

Description: description of the profile (ADMINISTRATOR in the example shown in the figure)

Enabling: This is an option that the installer sets when programming the panel. Then it will be managed by the users.

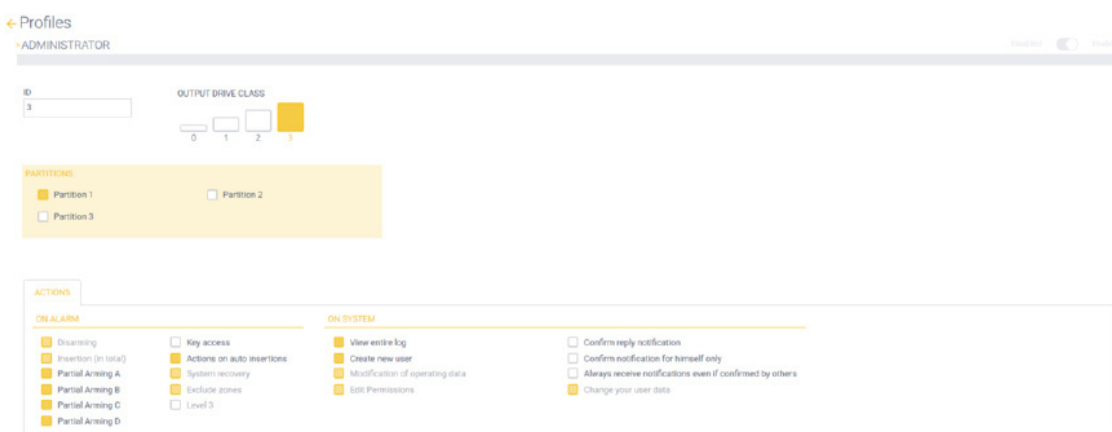
If a profile is enabled/disabled, all users with that profile are enabled/disabled for system management. It is therefore a high level enable/disable. Each user will also be enabled/disabled individually.

ID: Numeric index assigned to the profile

OUTPUT DRIVE CLASS:

Mode that allows users to manage the outputs. Each output terminal also has its own OUTPUT DRIVE CLASS; the user will only be able to manage (manually activate/deactivate) an output (an output terminal) if the OUTPUT DRIVE CLASS in their profile is greater than or equal to the OUTPUT DRIVE CLASS of the output they want to manage.

PARTITIONS: The partitions in which the profile (and therefore the users associated with that profile) is enabled to operate.



Profiles
ADMINISTRATOR

ID: 3

OUTPUT DRIVE CLASS: 3

PARTITIONS: ☒ Partition 1 ☐ Partition 2 ☐ Partition 3

ACTIONS

ON ALARM

- ☒ Disarming
- ☒ Insertion (in total)
- ☒ Partial Arming A
- ☒ Partial Arming B
- ☒ Partial Arming C
- ☒ Partial Arming D
- ☐ Key access
- ☐ Actions on auto insertions
- ☐ System recovery
- ☐ Exclude zones
- ☐ Level 3

ON SYSTEM

- ☒ View entire log
- ☒ Create new user
- ☒ Modification of operating data
- ☒ Edit Permissions
- ☐ Confirm reply notification
- ☐ Confirm notification for himself only
- ☐ Always receive notifications even if confirmed by others
- ☒ Change your user data

ACTIONS - ON ALARM.

There are several options, each of which enables/disables the profile to perform the described action.

Disarming, Arming (total), Partial Arming A, Partial Arming B, Partial Arming C, Partial Arming D: If the option is enabled, the profile can perform the related partial arming.

Key access: If enabled, this allows the user to use transponder keys or remote controls.

Actions on auto insertions: If enabled, this allows the user to change partition auto-arming.

System recovery: If enabled, this erases the system, detector and partition alarm memories.

Exclude zones: If enabled, this allows zones to be armed/disarmed manually.

Level 3: If enabled, the user is classified as a level 3 user in accordance with the EN50131 standard, and can therefore erase system, detector and partition sabotage memories.

ACTIONS - ON SYSTEM

There are several options, each of which enables/disables the profile to perform the described action.

View entire log: If enabled, this allows the event log to be displayed on the keyboards.

Create new user: If enabled, this allows the user to create new users using the keyboard.

Modification of operating data: If enabled, the user can edit certain system operating data, for example to change the date/time, enables/disables and auto-arming, and to run diagnostic procedures.

Edit permissions: If enabled, this allows the user to authorise/deny the installer to edit parameters and update the system.

Edit permissions: If enabled, this allows the user to authorise/deny the installer to edit parameters and update the system.

Confirm reply notification: If enabled, the user confirms the notification call simply by answering, and therefore does not need to press the “*” key.

Confirm notification for himself only: If enabled, when the user receives a notification, the notification confirmation is only valid for that specific user. N.B. If no profile has this option enabled, any event programmed to notify a large number of users will stop sending the notifications as soon as one of the users has been successfully notified.

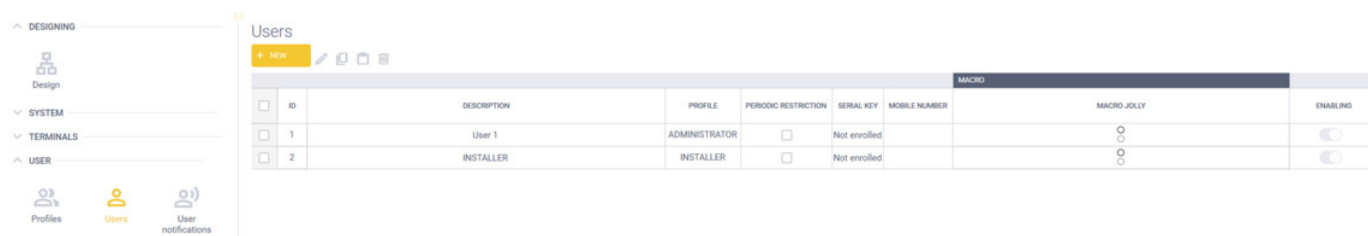
Always receive notifications even if confirmed by others: If enabled, users with this profile will always receive event notifications, even if they have already been confirmed by others. This is the opposite of the previous option.

Change your user data: If enabled, users with this profile can edit certain personal data such as the PIN, phone number, etc.

10.2 USER – Users

The summary screen lists all the users that have been created, and the various columns show the most significant parameters for each user.

The summary table can also be used to edit the displayed parameters by clicking directly on the parameter.



ID	DESCRIPTION	PROFILE	PERIODIC RESTRICTION	SERIAL KEY	MOBILE NUMBER	MACRO	MACRO JOLLY	ENABLING
1	User 1	ADMINISTRATOR	<input type="checkbox"/>	Not enrolled			<input type="radio"/>	<input type="checkbox"/>
2	INSTALLER	INSTALLER	<input type="checkbox"/>	Not enrolled			<input type="radio"/>	<input type="checkbox"/>

To create a new user, click the **+ NUOVA** key and set the desired description and profile.

To open the full user page, double-click anywhere on the line of the user you want.

User

The individual parameters are described below.

Description: description of the profile (ADMINISTRATOR in the example shown in the figure)

Enabling: This is an option that the *installer* sets when programming the panel. Then it will be managed by the users.

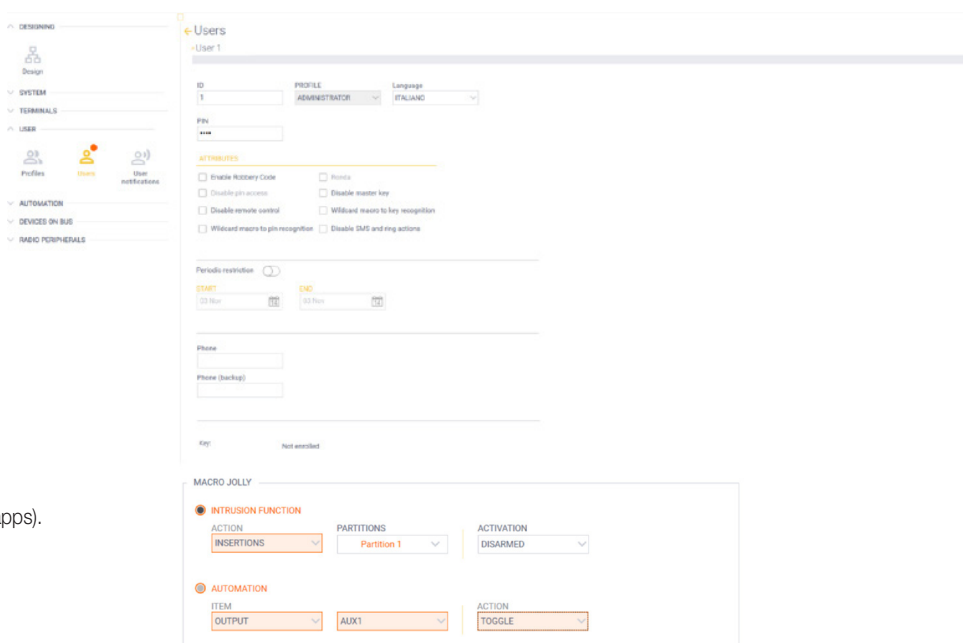
A disabled user cannot access system management.

ID: a numeric index assigned to the user.

PROFILE: this is the profile with which the user is associated.

LANGUAGE: this is the language in which the keyboard strings will be displayed once the user has been identified.

PIN: this is the 4-, 5- or 6-digit numeric code that uniquely identifies the user accessing the system via the available interfaces (keyboards, apps).



The Installer PIN is 9999 by default and is required to connect the By-alarm Plus manager software to the panel.

For security reasons and to prevent access to the panel by an unauthorised installer, we recommend changing the Installer PIN. Therefore, the installer performing the programming MUST change the default PIN.

This PIN can be used to access keyboard menus reserved for installers; press and hold the  key on the keyboard to access these menu sections.

Caution: The Installer PIN is not valid for daily use of the keyboard and the burglar alarm system; after entering the Installer PIN, the keyboard will not allow access to the user menus. When the timeout lapses, the display will show "Caution! Not allowed".

To increase security after creating a user, we recommend changing the assigned PIN using the keyboard.

ATTRIBUTES

There are several options, each of which enables/disables the user to perform the described action.

Enable robbery code: If enabled, the user can enter the PIN with 1 added to the last digit in order to operate normally while simultaneously alerting a robbery attempt under duress. For example, if the user PIN is 12345, the user under duress will enter 12346 so that a "robbery" event will be generated to alert law enforcement without raising suspicion.

Disable PIN access: If enabled, the user cannot use the numeric PIN and will only be able to manage the system with transponder keys and remote controls.

Wildcard macro to key recognition: If enabled, the WILDCARD MACRO (described in the WILDCARD MACRO paragraph) will be run as soon as the user's key is recognised.

Disable SMS and ring actions: If enabled, text messages and/or calls to the LTE dialer from this user will be ignored.

Patrol: If enabled, the partitions will be disarmed for the patrol time (for that partition) as soon as the user is recognised; once the patrol time has lapsed, will be rearmed to their previous modes.

Disable master key: If enabled, the user cannot use the transponder key.

Disable remote control: If enabled, the user cannot use the remote control.

Wildcard macro to PIN recognition: If enabled, the WILDCARD MACRO (described in the WILDCARD MACRO paragraph) will be run as soon as the user's PIN is recognised.

Periodic restriction.

If enabled, this serves to define the start-end time within which the user can operate. Outside this period, the user is not allowed to operate in the system.

Phone.

This is the phone number used to send text messages and voice calls to the user and accept text messages and ringing for running macros. When programming text message notifications, this must be the number of a device that can receive text messages.

Phone (backup).

This is an optional second phone number used to send voice calls to the user if there is no answer to the first phone number.

Key.

This parameter is not programmable, but displays whether the user has a transponder key.

Key and remote control.

These parameters are not programmable, but display whether the user has a transponder key and remote control.

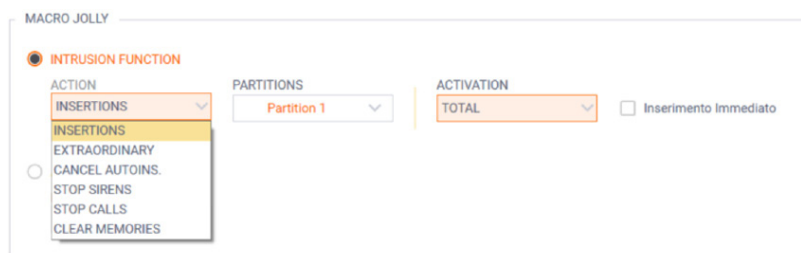
WILDCARD MACRO.

THE WILDCARD MACRO identifies two programmable actions associated with the user, which are performed if at least one of the above options is enabled: *Wildcard macro on recognising the key or Wildcard macro on recognising the PIN.*

The possible WILDCARD MACRO functions are described below.

Dual authentication: To execute commands, the user must authenticate with both the transponder key and the remote control.

The WILDCARD MACRO can enable two functions independently of each other; INTRUSION FUNCTION and AUTOMATION.

INTRUSION FUNCTION


If enabled, the ACTION can be selected from the following options:

- **INSERTIONS** – arming/disarming partitions in various modes.
This selection allows you to set which partitions to operate on and in which mode.
- **EXTRAORDINARY** – overtime work request, which postpones the partition auto-arming time by x minutes.
This action will be extended to all partitions common to the profile and keyboard on which the user is operating.
- **CANCEL AUTOINS.** – does not perform the next partition auto-arming (from the time at which the WILDCARD MACRO is activated).
This action will be extended to all partitions common to the profile and keyboard on which the user is operating.
- **STOP SIRENS** – deactivates all “siren” outputs.
- **STOP CALLS** – stops all ongoing notifications.
- **CLEAR MEMORIES** – erases the alarm memories (and sabotage memories if the profile allows).
This action will be extended to all partitions common to the profile and keyboard on which the user is operating.

The *Immediate arming* option arms the partitions immediately, ignoring all output delay times.

AUTOMATION

If enabled, the ACTION can be selected from the following options:

- **OUTPUT** – output activation/deactivation and corresponding output activation mode.
- **LINE** – line activation/deactivation and corresponding line activation mode.
- **SCENARIO** – activation operations of an activation scenario.

USER CODE (PIN)

The system manages these as follows:

- **ID 1; PIN = 0001** is reserved for the ADMINISTRATOR
This is the only profile included by default and cannot be deleted. The default PIN is therefore 0001.
- **ID 2; PIN = 0002** is reserved for the INSTALLER
It is the code intended for the installer and has a hidden profile, i.e. it is not visible and therefore cannot be deleted.
IMPORTANT: the installer's default PIN is not 0002, but 9999.

When creating a new user in the software, its initial PIN is “derived” from its ID, i.e. from the identification number; for example:

- if ID=4, the PIN will be 0004;
- if ID=15, the PIN will be 0015;
- if ID=27, the PIN will be 0027.

Therefore, apart from ID 2 whose default PIN is 9999, all other PINs will match the ID number (PIN 0002 can never be used).

10.3 USER – User notifications

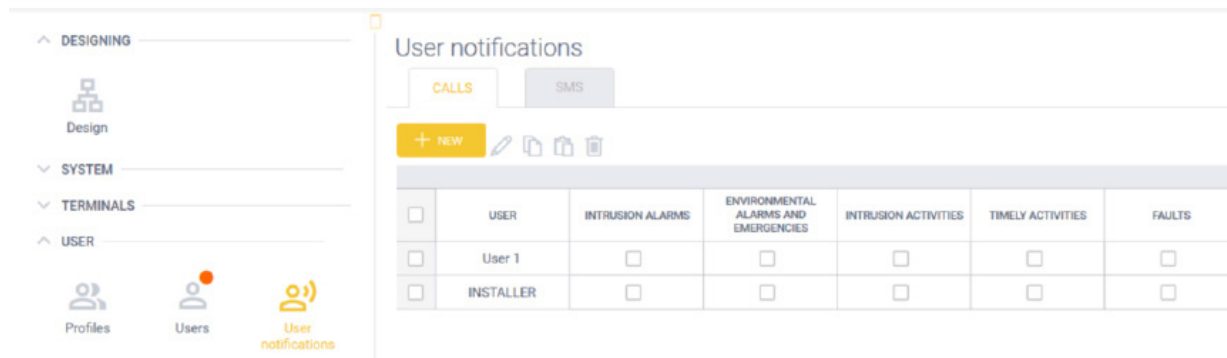
The summary screen lists all user notifications that have been created, and the various columns show the most significant parameters for each user.

The summary table can also be used to edit the displayed parameters by clicking directly on the parameter.

This programming is system related; go to the relevant screen for details.

There are two sections: **CALLS** and **SMS**. The **CALLS** section is dedicated to voice message notifications and the **SMS** section is dedicated to text message notifications.

The two sections have the same settings, so only one will be described.



To create a new notification, at least one user must have been created in the system; click the **+ NUOVA** key and select the user to whom the notifications will be sent.

To open the full notification details page, double-click anywhere on the line of the user you want.

The individual parameters are described below.

The details page is divided into five columns:

- INTRUSION ALARMS
- ENVIRONMENTAL ALARMS AND EMERGENCIES
- INTRUSION ACTIVITIES
- TIMELY ACTIVITIES
- FAULTS

INTRUSION ALARMS			ENVIRONMENTAL ALARMS AND EMERGENCIES			INTRUSION ACTIVITIES			TIMELY ACTIVITIES			FAULTS		
All	A	R	All	A	R	All	A	R	All	A	R	All	A	R
Intrusion	<input type="checkbox"/>	<input type="checkbox"/>	Fire	<input type="checkbox"/>	<input type="checkbox"/>	Insertion (in total)	<input type="checkbox"/>	<input type="checkbox"/>	Zone Alarm / Sabotage	<input type="checkbox"/>	<input type="checkbox"/>	Mains power supply	<input type="checkbox"/>	<input type="checkbox"/>
Intrusion confirmed	<input type="checkbox"/>	<input type="checkbox"/>	Flooding	<input type="checkbox"/>	<input type="checkbox"/>	Arming (partially)	<input type="checkbox"/>	<input type="checkbox"/>	Real time zone	<input type="checkbox"/>	<input type="checkbox"/>	Panel Power Supply	<input type="checkbox"/>	<input type="checkbox"/>
Sabotage	<input type="checkbox"/>	<input type="checkbox"/>	Gas	<input type="checkbox"/>	<input type="checkbox"/>	Disarming	<input type="checkbox"/>	<input type="checkbox"/>	Output real time	<input type="checkbox"/>	<input type="checkbox"/>	Panel Battery	<input type="checkbox"/>	<input type="checkbox"/>
System sabotage	<input type="checkbox"/>	<input type="checkbox"/>	CO	<input type="checkbox"/>	<input type="checkbox"/>	Failed to insert	<input type="checkbox"/>	<input type="checkbox"/>	Line activity	<input type="checkbox"/>	<input type="checkbox"/>	Device disappeared	<input type="checkbox"/>	<input type="checkbox"/>
Robbery	<input type="checkbox"/>	<input type="checkbox"/>	High temperature	<input type="checkbox"/>	<input type="checkbox"/>	Auto-arming delayed / canceled	<input type="checkbox"/>	<input type="checkbox"/>				Outputs and Aux	<input type="checkbox"/>	<input type="checkbox"/>
Robbery confirmed	<input type="checkbox"/>	<input type="checkbox"/>	Low temperature	<input type="checkbox"/>	<input type="checkbox"/>	Emergency exit	<input type="checkbox"/>	<input type="checkbox"/>				Bus	<input type="checkbox"/>	<input type="checkbox"/>
Panic	<input type="checkbox"/>	<input type="checkbox"/>	Emergency / Rescue	<input type="checkbox"/>	<input type="checkbox"/>	Lack of activity	<input type="checkbox"/>	<input type="checkbox"/>				Zone	<input type="checkbox"/>	<input type="checkbox"/>
						Exclusions	<input type="checkbox"/>	<input type="checkbox"/>				Gas link	<input type="checkbox"/>	<input type="checkbox"/>
						Delete memories / calls or stop sirens	<input type="checkbox"/>	<input type="checkbox"/>				Link to the Monitoring Station	<input type="checkbox"/>	<input type="checkbox"/>
						Maintenance	<input type="checkbox"/>	<input type="checkbox"/>				Radio Blanking	<input type="checkbox"/>	<input type="checkbox"/>
						Codes / keys / time management	<input type="checkbox"/>	<input type="checkbox"/>				Device problems	<input type="checkbox"/>	<input type="checkbox"/>
						Code / key not allowed	<input type="checkbox"/>	<input type="checkbox"/>				Low battery devices	<input type="checkbox"/>	<input type="checkbox"/>
												Loss of data / time	<input type="checkbox"/>	<input type="checkbox"/>
												Other faults	<input type="checkbox"/>	<input type="checkbox"/>

Each column is in turn composed of two additional columns, **A** and **R**, which serve to set the notification when the event starts/activates/occurs (**A**) and when the event resets/deactivates/ends (**R**).

N.B. In general, each event will only be notified if it occurs in partitions for which the user is enabled. If, for example, a user is to be notified for **INTRUSION ACTIVITIES – Disarming**, they will only be notified when a partition is disarmed if their user profile is enabled for that partition.

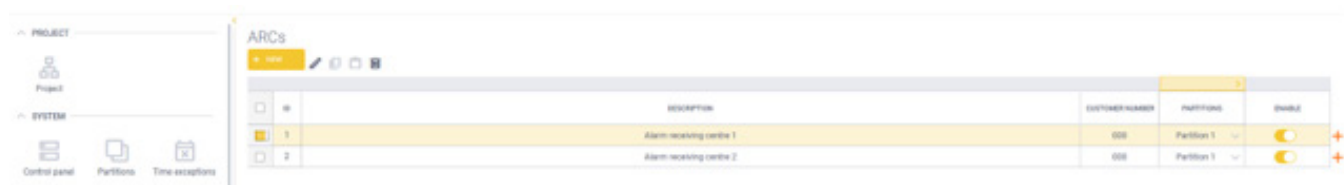
Not all fault events correlate with partitions (for example a **FAULT – Zone** correlates with partitions, but **FAULT – Mains power supply** does not); the notification will therefore follow that correlation.

The procedure to enable the system to receive call and/or text message notifications is as follows:

1. Install the LTE dialer art. 03810-03820
2. Install the voice synthesis board 03813 (for receiving call notifications only)
3. Use the By-alarm Plus Manager software to:
 - a) Add the LTE dialer to the system (see para. 12.5);
 - b) Configure user notifications (see this paragraph)
 - c) (For receiving call notifications only) - use the "Audio Files" control, as described in para. 6.1, execute "Generate audio file" and "Send audio file to panel" in that order.

10.4 USER - ARCs

The summary screen lists all the ARCs that have been created, and the various columns show the most significant parameters for each one.



ID	Description	Customer number	Partitions	Enabled
1	Alarm receiving centre 1	000	Partition 1	<input checked="" type="checkbox"/>
2	Alarm receiving centre 2	000	Partition 1	<input type="checkbox"/>

To create a new ARC, click on the “NEW” button and set the description (the TYPE parameter is a non-editable value)

To open the full ARC page, double-click anywhere on the row.

The individual parameters are described below.

Profile description: (in the example in the figure, “Alarm receiving centre 1”)

Disabled Enabled: This is an option that the installer sets when programming the panel. It allows the installer to disable the use of an ARC without deleting its programming.

ID: Numerical index assigned to the ARC

TYPE: non-editable internal parameter

Work as a back-up (of): in the presence of more than one programmed ARC, you can define for one to act as the back-up of the other. An ARC configured as a back-up will have the connection monitored with the polling programmed (see related parameter below) but it will receive notifications from the panel only if the panel is unsuccessful in sending notifications to the main one, specified in the field on the right of this attribute.

Partitions: Partitions associated with the ARC. No notifications will be sent relating to the non associated partitions.

CONNECTION: network, IP and port parameters of the ARC, provided to the installer by the reception and control manager in charge of the ARC.

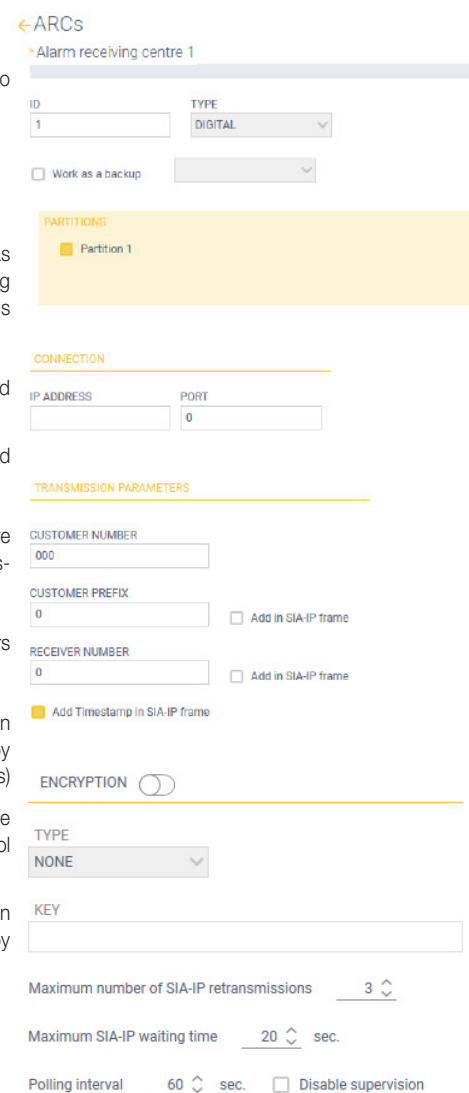
TRANSMISSION PARAMETERS: these parameters are used for the panel SIA-IP communication. They are provided to the installer by the reception and control manager in charge of the ARC and are tied to the customer where the panel is installed.

ENCRYPTION: if the reception and control centre manager in charge of the ARC requires it, these parameters are provided to the installer to encrypt the communication between the panel and the ARC

Maximum number of SIA-IP retransmissions: Number of repeated notification sending attempts. This is an advanced parameter of the SIA-IP protocol, which should be edited by the installer only where requested by the reception and control centre manager in charge of the ARC (in the event of problems receiving notifications)

Maximum SIA-IP waiting time: Waiting for a response to the notification. This is an advanced parameter of the SIA-IP protocol, which should be edited by the installer only where requested by the reception and control centre manager in charge of the ARC (in the event of problems receiving notifications)

Polling interval: Connection supervision time between the panel and the ARC (0 means disabled). This is an advanced parameter of the SIA-IP protocol, which should be edited by the installer only where requested by the reception and control centre manager in charge of the ARC.



← ARCs
Alarm receiving centre 1

ID: 1 TYPE: DIGITAL

☐ Work as a backup

PARTITIONS
Partition 1

CONNECTION
IP ADDRESS: PORT: 0

TRANSMISSION PARAMETERS
CUSTOMER NUMBER: 000
CUSTOMER PREFIX: 0 ☐ Add in SIA-IP frame
RECEIVER NUMBER: 0 ☐ Add in SIA-IP frame
☒ Add Timestamp in SIA-IP frame

ENCRYPTION ☐

TYPE: NONE

KEY:

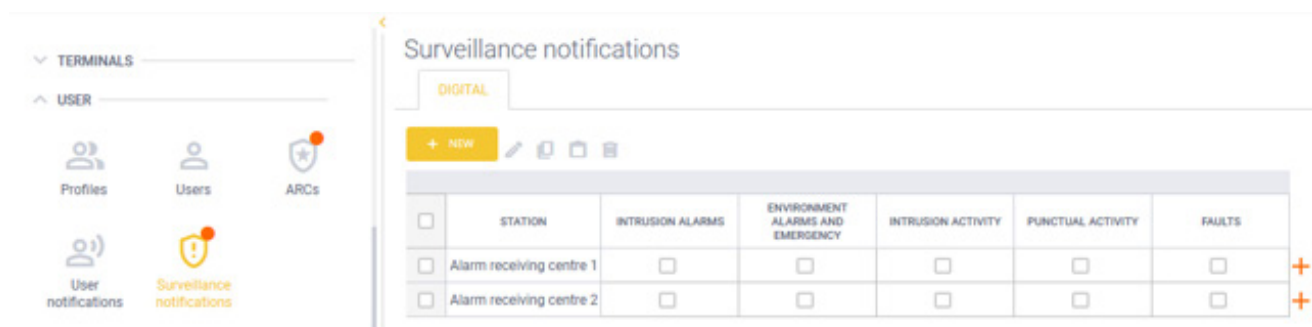
Maximum number of SIA-IP retransmissions: 3

Maximum SIA-IP waiting time: 20 sec.

Polling interval: 60 sec. ☐ Disable supervision

10.5 USER - Surveillance notifications

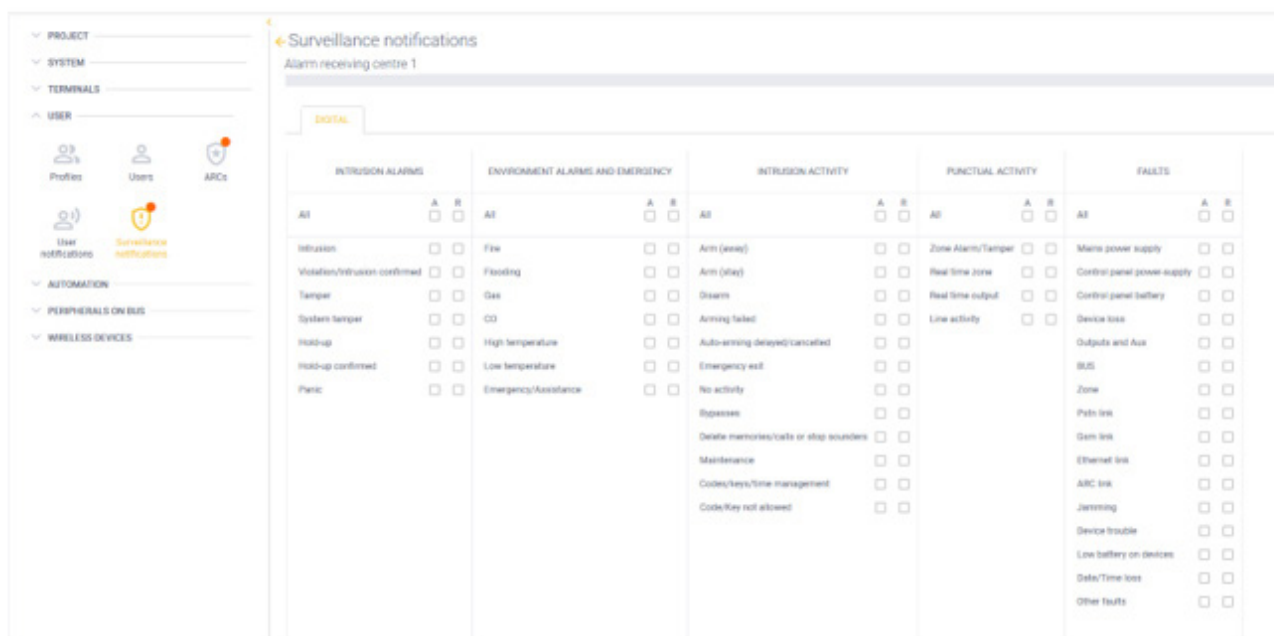
The summary screen lists all ARC notifications that have been created, and the various columns show the most significant parameters for each one. The summary table can also be used to edit the displayed parameters by clicking directly on the parameter. This programming is system related; go to the relevant screen for details.



<input type="checkbox"/>	STATION	INTRUSION ALARMS	ENVIRONMENT ALARMS AND EMERGENCY	INTRUSION ACTIVITY	PUNCTUAL ACTIVITY	FAULTS
<input type="checkbox"/>	Alarm receiving centre 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Alarm receiving centre 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

To create a new notification, at least one ARC must have been created in the system; click on the “NEW” button and select the recipient ARC of notifications. To open the full page of notifications to a specific ARC, double-click anywhere on the row.

For a description of individual parameters, please refer to the section “USER – User notifications”: the parameters have the same meaning.



INTRUSION ALARMS			ENVIRONMENT ALARMS AND EMERGENCY			INTRUSION ACTIVITY			PUNCTUAL ACTIVITY			FAULTS		
All	A	R	All	A	R	All	A	R	All	A	R	All	A	R
Intrusion	<input type="checkbox"/>	<input type="checkbox"/>	Fire	<input type="checkbox"/>	<input type="checkbox"/>	Arm (delay)	<input type="checkbox"/>	<input type="checkbox"/>	Zone Alarm/Tamper	<input type="checkbox"/>	<input type="checkbox"/>	Main power supply	<input type="checkbox"/>	<input type="checkbox"/>
Violation/Intrusion confirmed	<input type="checkbox"/>	<input type="checkbox"/>	Flooding	<input type="checkbox"/>	<input type="checkbox"/>	Arm (delay)	<input type="checkbox"/>	<input type="checkbox"/>	Real time zone	<input type="checkbox"/>	<input type="checkbox"/>	Control panel power supply	<input type="checkbox"/>	<input type="checkbox"/>
Tamper	<input type="checkbox"/>	<input type="checkbox"/>	Gas	<input type="checkbox"/>	<input type="checkbox"/>	Disarm	<input type="checkbox"/>	<input type="checkbox"/>	Real time output	<input type="checkbox"/>	<input type="checkbox"/>	Control panel battery	<input type="checkbox"/>	<input type="checkbox"/>
System tamper	<input type="checkbox"/>	<input type="checkbox"/>	CO	<input type="checkbox"/>	<input type="checkbox"/>	Arming failed	<input type="checkbox"/>	<input type="checkbox"/>	Line activity	<input type="checkbox"/>	<input type="checkbox"/>	Device loss	<input type="checkbox"/>	<input type="checkbox"/>
Hold-up	<input type="checkbox"/>	<input type="checkbox"/>	High temperature	<input type="checkbox"/>	<input type="checkbox"/>	Auto-arming delayed/cancelled	<input type="checkbox"/>	<input type="checkbox"/>				Outputs and Aux	<input type="checkbox"/>	<input type="checkbox"/>
Hold-up confirmed	<input type="checkbox"/>	<input type="checkbox"/>	Low temperature	<input type="checkbox"/>	<input type="checkbox"/>	Emergency exit	<input type="checkbox"/>	<input type="checkbox"/>				BUS	<input type="checkbox"/>	<input type="checkbox"/>
Panic	<input type="checkbox"/>	<input type="checkbox"/>	Emergency/Assistance	<input type="checkbox"/>	<input type="checkbox"/>	No activity	<input type="checkbox"/>	<input type="checkbox"/>				Zone	<input type="checkbox"/>	<input type="checkbox"/>
						Bypasses	<input type="checkbox"/>	<input type="checkbox"/>				Path link	<input type="checkbox"/>	<input type="checkbox"/>
						Delete memories/calls or stop sounders	<input type="checkbox"/>	<input type="checkbox"/>				Gen link	<input type="checkbox"/>	<input type="checkbox"/>
						Maintenance	<input type="checkbox"/>	<input type="checkbox"/>				Ethernet link	<input type="checkbox"/>	<input type="checkbox"/>
						Codes/keys/time management	<input type="checkbox"/>	<input type="checkbox"/>				ARC link	<input type="checkbox"/>	<input type="checkbox"/>
						Code/Key not allowed	<input type="checkbox"/>	<input type="checkbox"/>				Jamming	<input type="checkbox"/>	<input type="checkbox"/>
												Device trouble	<input type="checkbox"/>	<input type="checkbox"/>
												Low battery on devices	<input type="checkbox"/>	<input type="checkbox"/>
												Date/Time loss	<input type="checkbox"/>	<input type="checkbox"/>
												Other faults	<input type="checkbox"/>	<input type="checkbox"/>

10.6 PIN and key management

The PIN and keys associated with each user are stored securely in the panel and software projects. They are encrypted using the highest security standards (AES 256bit) with a unique encryption key for each panel.

Users manage PINs and enrol keys from the panel, so they may change over time.

The software updates user PINs and keys by reading the panel. It is therefore good practice for the installer to periodically read the panel to keep the project up to date with the changes made by users.

Writing PINs and keys to the panel is protected and requires explicit authorisation by the end user; even if the user data in the software is not aligned (in terms of PINs and keys) and the installer does not read from the panel first, writing to the project DOES NOT overwrite the user data

Periodically backing up user PINs and keys

The installer just has to read the project from the panel and save it to keep a secure backup of the user data (PINs and keys) on the PC. The list of projects in the software always contains the date and time of the last save

Restoring user PINs and keys from a backup

There may be situations in which user PINs and keys need to be restored to a panel from those available in the last backup saved. In order for the software to overwrite the PINs and keys on the panel, a user with the "Edit permissions" attribute enabled in their profile must use the PERMISSIONS – INSTALLER – "Enable writing PINs/KEYS from SW" keyboard menu to enable the operation in advance.

IMPORTANT: After writing the project to the panel, overwriting the user PIN and keys, the write enable is AUTOMATICALLY DISABLED at the end of the operation (reading with the software does not change the enable status)

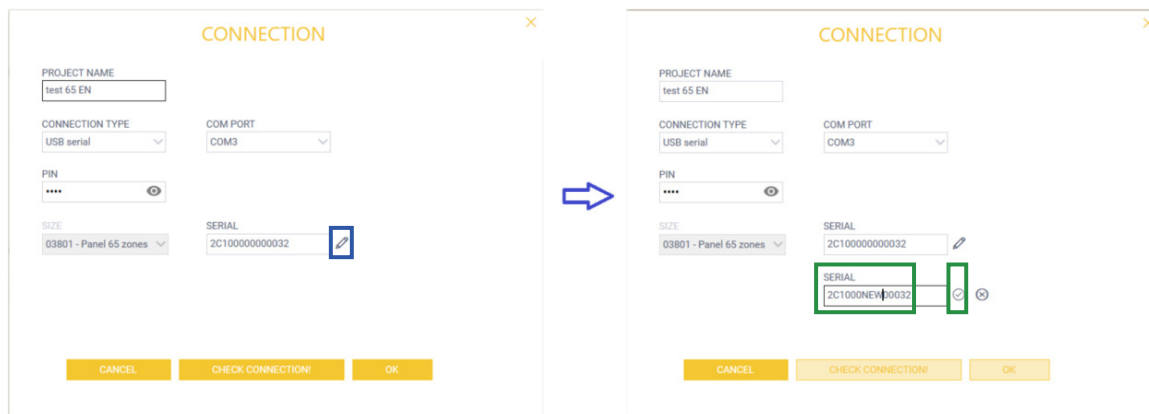
Operationally, there are two common situations and corresponding procedures:

1. The need to restore the factory settings in the panel

- Read the panel with the software
- Restore the factory settings in the panel
- Enrol at least one keyboard, log in as user 1 (default PIN 0001) and select "Enable writing PINs/KEYS from SW"
- Write to the panel with the software
- Writing PINs/KEYS is AUTOMATICALLY DISABLED when the software has finished writing

2. The need to replace a damaged panel

- In this case, use the last project saved followed by the PIN and key backup from a specific date. CAUTION: any changes made by users to PINs and keys on the damaged panel after this backup CANNOT be recovered
- Replace the panel with a new one of the SAME SIZE
- Restore the factory data in the panel (if the panel is not brand new)
- Enrol at least one keyboard, log in as user 1 with the default PIN 0001, and enable "Enable writing PINs/KEYS from SW"
- View CONNECTION in the software, activate QR code editing (in BLUE), enter the QR code of the new panel and confirm (in GREEN)



f. Write to the panel with the software

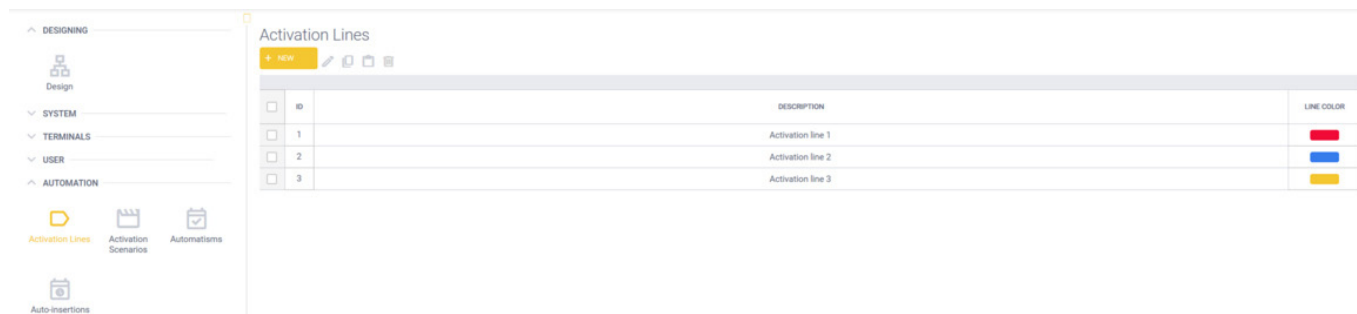
g. Writing PINs/KEYS is AUTOMATICALLY DISABLED when the software has finished writing

11. AUTOMATION

This paragraph is about the automation features, and is therefore not always related to intrusion protection.

11.1 AUTOMATION – Activation Lines

Activation lines serve to group multiple outputs together in order to manage them in a single block. The summary screen lists all the lines. There is no additional details page for the activation lines.



ID	DESCRIPTION	LINE COLOR
1	Activation line 1	Red
2	Activation line 2	Blue
3	Activation line 3	Yellow

An activation line can be controlled directly by the following devices:

- Readers
- Keyboard with transponder
- Radio keys (remote controls)

or indirectly using the following panel configurations:

- Activation scenarios
- Automatisms

The commands sent include:

- ON
- OFF
- TOGGLE
- SET percentage value
- INC/DEC (only on T4 and T5 of the expansions to control the 0–10V output)

For direct control by a reader, keyboard with transponder or remote control, it is possible to combine AUTOMATION actions that use device outputs to control relays or 0–10V voltage ranges in the burglar alarm system.

Specifically, the controls can be associated as follows: LED ACTIONS in the reader; KEY ACTIONS in the keyboard with transponder; devices KEYS in the radio key. Alternatively, they can be used for integration with the By-me Plus system.

To create a new line, click the **+ NUOVA** key and set the line description.

Integration with the By-me system

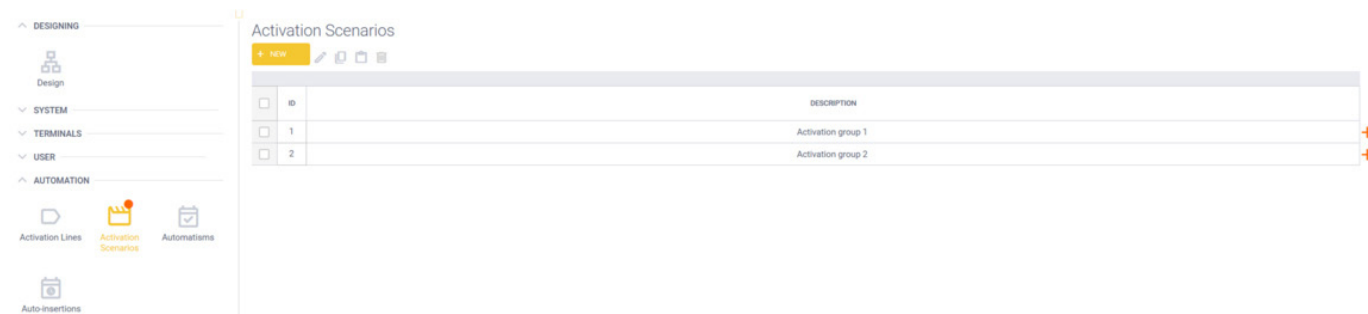
For full details, see para. "Integration of By-alarm and video door entry devices with By-me Plus applications" in the By-me Plus system manual.

11.2 AUTOMATION – Activation Scenarios

The summary screen lists all the scenarios.

To program each activation scenario, open the details page.

An *Activation Scenario* is a feature that allows lines and individual outputs to be activated/deactivated in a programmable manner



ID	DESCRIPTION
1	Activation group 1
2	Activation group 2

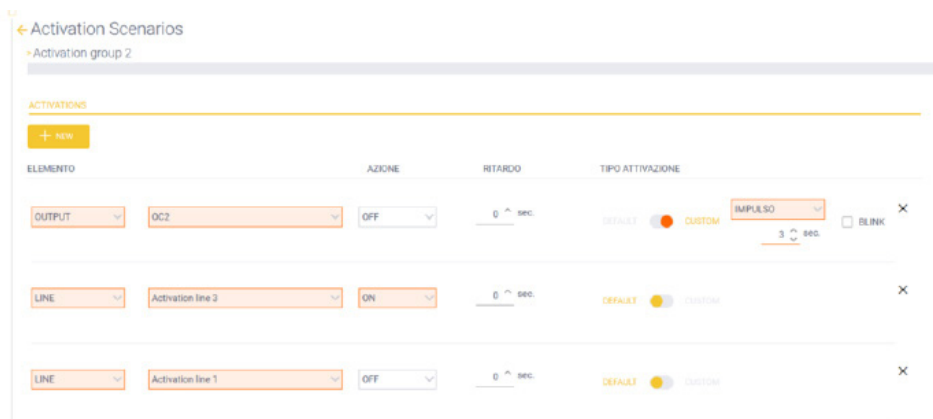
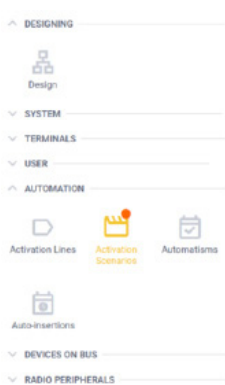
To create a new scenario, click the **+ NUOVA** key and enter the description.

To open the scenario details page, double-click anywhere on the line of the scenario you want, or select it with the check box on the left and click the pencil icon.

Automation

As soon as the new activation scenario has been created, click **+ NUOVA** to add the ACTIVATIONS you want.

You can set the various parameters for each ACTIVATION ELEMENT. If OUTPUT is set, select:



- the output (OC2 in the example)
- the ACTION type: ON, OFF, TOGGLE
- any activation DELAY (in s)
- the ACTIVATION TYPE for the selected output

If LINE is set, select the same parameters described above:

- the line
- the ACTION type: ON, OFF, TOGGLE, SET (for dimmable outputs)
- any activation DELAY (in s)
- the ACTIVATION TYPE for the selected line

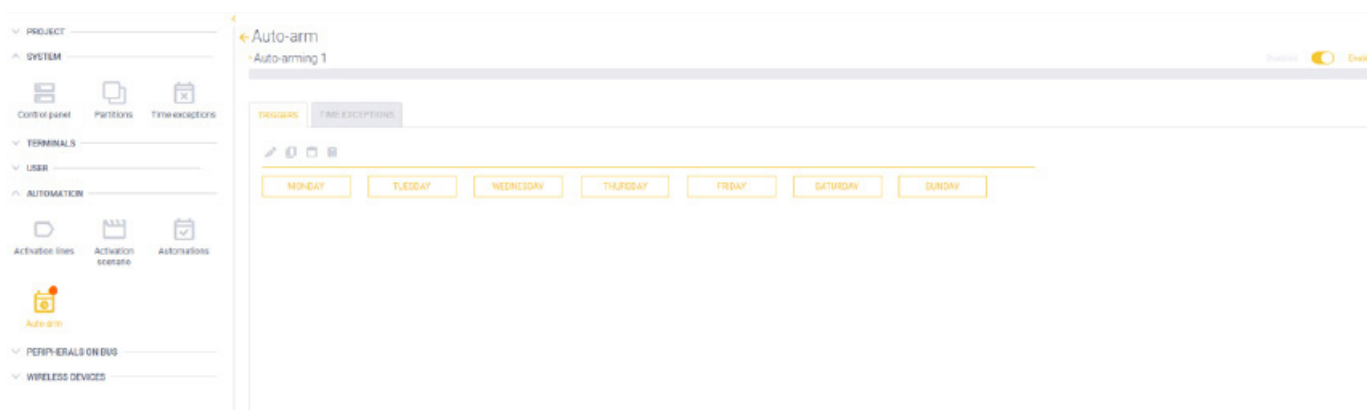
ACTIVATION TYPE serves to:

- activate the outputs using the standard programming method for the individual outputs: **DEFAULT**
- activate the outputs using local programming: **CUSTOM**

11.3 AUTOMATION – Auto-arming (and Automations)

These two sections are very similar and serve to set up automatic system actions following hourly and daily programming within the week.

Automations are generally used to manage automations; **Auto-armings** are expressly for security functions.



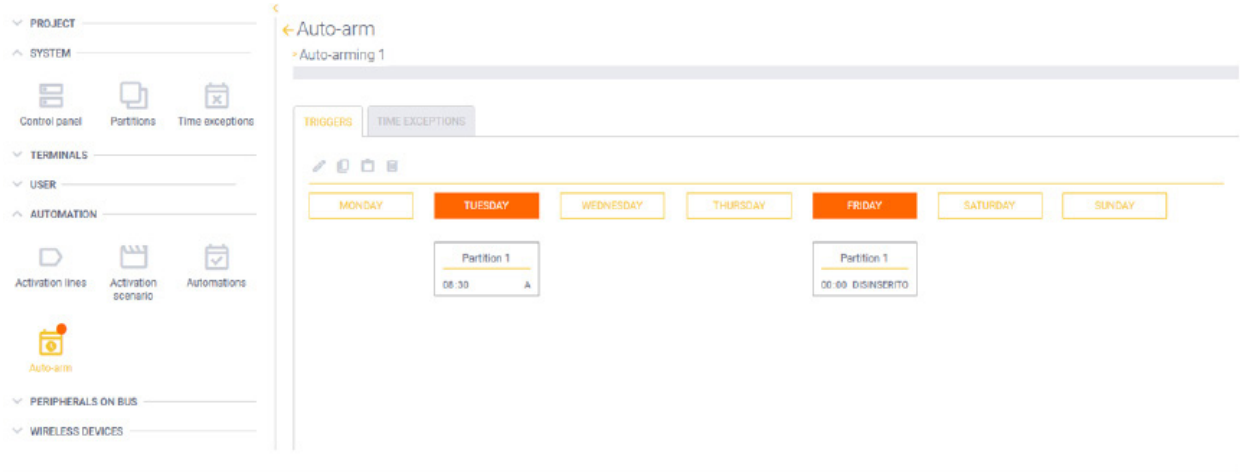
TRIGGERS

The automatic actions to be carried out are set in this tab.

Click on each day of the week to set the time at which the selected partitions will be automatically armed/disarmed.

The example screen below shows a complete list of auto-arming events:

- every Tuesday, Partition 1 will be armed in PARTIAL A mode at 8:30
- every Friday, Partition 1 (and other partitions identified with dots ...) will be disarmed at 00:00.

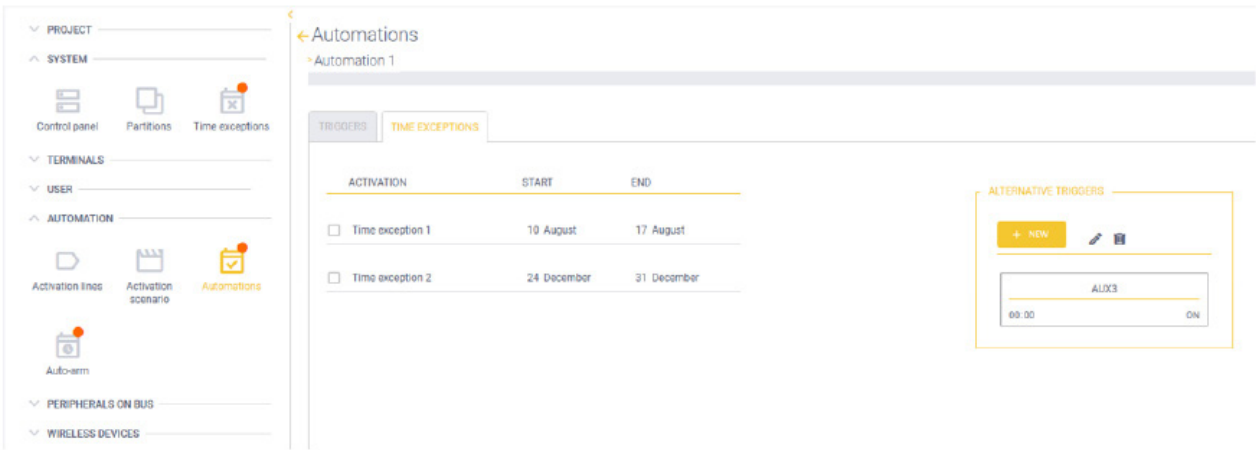


TIME EXCEPTIONS

This tab displays the time exceptions defined during System programming (see para. 8.3 SYSTEM – Time exceptions).

To enable a time exception, it must be selected using the related flag. You can select several time exceptions simultaneously. Time exceptions that are not selected will be ignored.

In the ALTERNATIVE TRIGGERS box, you can define (using the NEW button) certain actuations which will be activated during the period of time covered by the time exceptions enabled. The activation will occur every day at the configured time.



Expansions

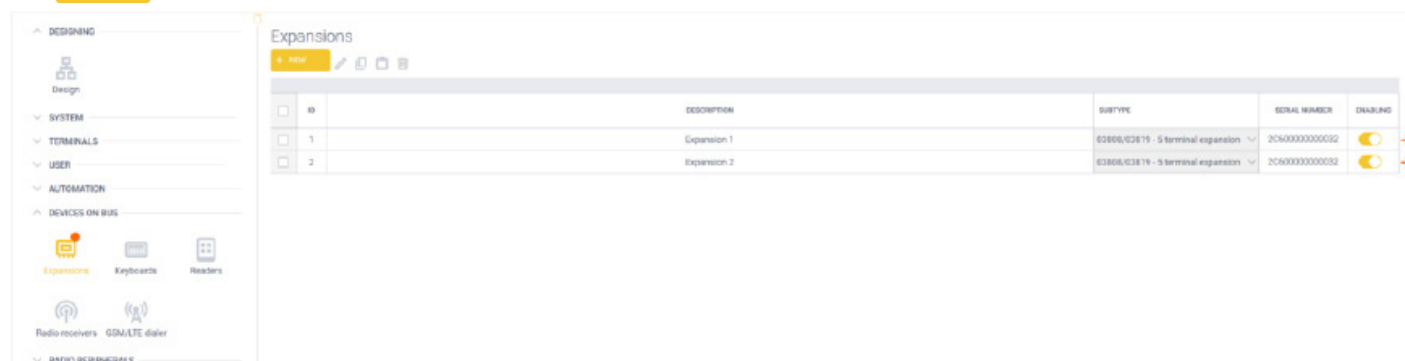
12. EXPANSIONS

This section is related to the expansions that can be connected to the panel; the available parameters and settings depend on the expansion type.

The description can be set for all expansion types.

The figure below shows the expansions page as an example.

Click **+ NUOVA** to add a new expansion.



ENABLING AND DISABLING an expansion (BUS or RADIO)

Each expansion (BUS or RADIO) added is ENABLED by default: It is programmed in the software and operational in the system.

Disabilitato  Abilitato

When an expansion (BUS or RADIO) is DISABLED in the programming, it will continue to exist in the software project and will retain its programming. However, it will NOT be operational and its activities will have no effect on the panel (signalling, notifications, output events, etc.).

Disabilitato  Abilitato

Anything that depends on a disabled expansion will NOT be operational (such as zones and related outputs, or notifications in the case of the dialer). Expansions that allow user interactions will be in the same state as when the expansion is not enrolled, and will not allow any interaction.

12.1 BUS EXPANSIONS – Expansions

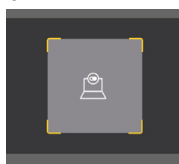
When adding a new expansion, you can specify the **DESCRIPTION** and must specify the **Serial**, "either by entering it on the keypad and by optical acquisition (by clicking on the adjacent symbol)"

Serial is the QR code found on all BUS expansions.

In particular, the software automatically sets some digits of the serial number.

- **2C6** is the expansion type, expansions 03808 and 03819 in this case.
- The installer must enter the 8 digits (in the red box in the figure), which are unique for each expansion.
- The last three digits, **032** in the example, are predefined by the manufacturer.

The  key activates the QRCode scanning using the camera associated with the software (see para. Connection).



New Expansion

ID
3

DESCRIPTION
Expansion 3

Serial
2C6000000000032

Template
03808/03819 - 5 terminal expansion

CANCEL CREATE

After creating the new expansion, you can edit the description and serial, and you can set the ATTRIBUTES option.

ATTRIBUTES – No Sabotage: if enabled, the expansion will NOT detect sabotage (used when, for installation purposes, it does not have to manage sabotage).

12.2 BUS EXPANSIONS – Keyboards

The keyboard summary screen displays a grid in which the SUBTYPE identifies the keyboard type: without reader or terminals (art. 03817) or with inserter and terminals (art. 03818).

In particular, the software automatically sets some digits of the serial number.

← Expansions > Expansion 3

ID
3

Template
03808/03819 - 5 terminal expansion


Serial
2C6000000000032

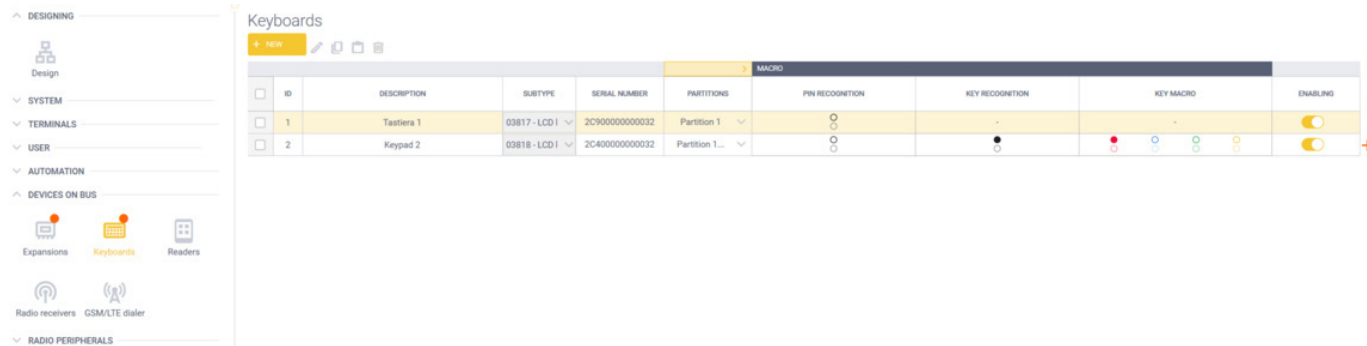
ATTRIBUTES
☐ No Sabotage

Expansions

- **2C9** and **2C4** are the keyboard type without reader or terminals (art. 03817) and with reader and terminals (art. 03818) respectively.
- The installer must enter the 8 digits (in the red box in the figure), which are unique for each keyboard.
- The last three digits, **032** in the example, are predefined by the manufacturer.

The columns in the grid contain some editable data, while other data in the table is display-only (not editable), but is useful for identifying if and what is programmed for the keyboards.

For example, in the figure below you can see that **Keyboard 1** has no reader and nothing is displayed in the KEY RECOGNITION and KEY MACRO columns; **Keyboard 2** has a reader, and the columns contain some data (see ).



ID	DESCRIPTION	SUBTYPE	SERIAL NUMBER	PARTITIONS	PIN RECOGNITION	KEY RECOGNITION	KEY MACRO	ENABLING
1	Tastiera 1	03817 - LCD I	2C900000000032	Partition 1				
2	Keypad 2	03818 - LCD I	2C400000000032	Partition 1...				

Click **+ NUOVA** to create a new keyboard; enter the description and select the template (03817 or 03818).

As for all expansions, the description can be edited.

ID: a numeric index assigned to the keyboard.

Template: the selected mode (03817 or 03818). This section cannot be used to modify the template for a keyboard that has already been added. It has to be removed and a new one added.

Serial: the unique QR code of the keyboard

ATTRIBUTES. This contains some general keyboard options.

Disable keyboard sounds: if enabled, the keyboard will not make any sound (e.g. it will not indicate entry/exit times, which is useful when a keyboard is installed in a bedroom).

Enable proximity reader (option only available on keyboard 03818): if enabled, the reader in the keyboard is used to read transponder keys.

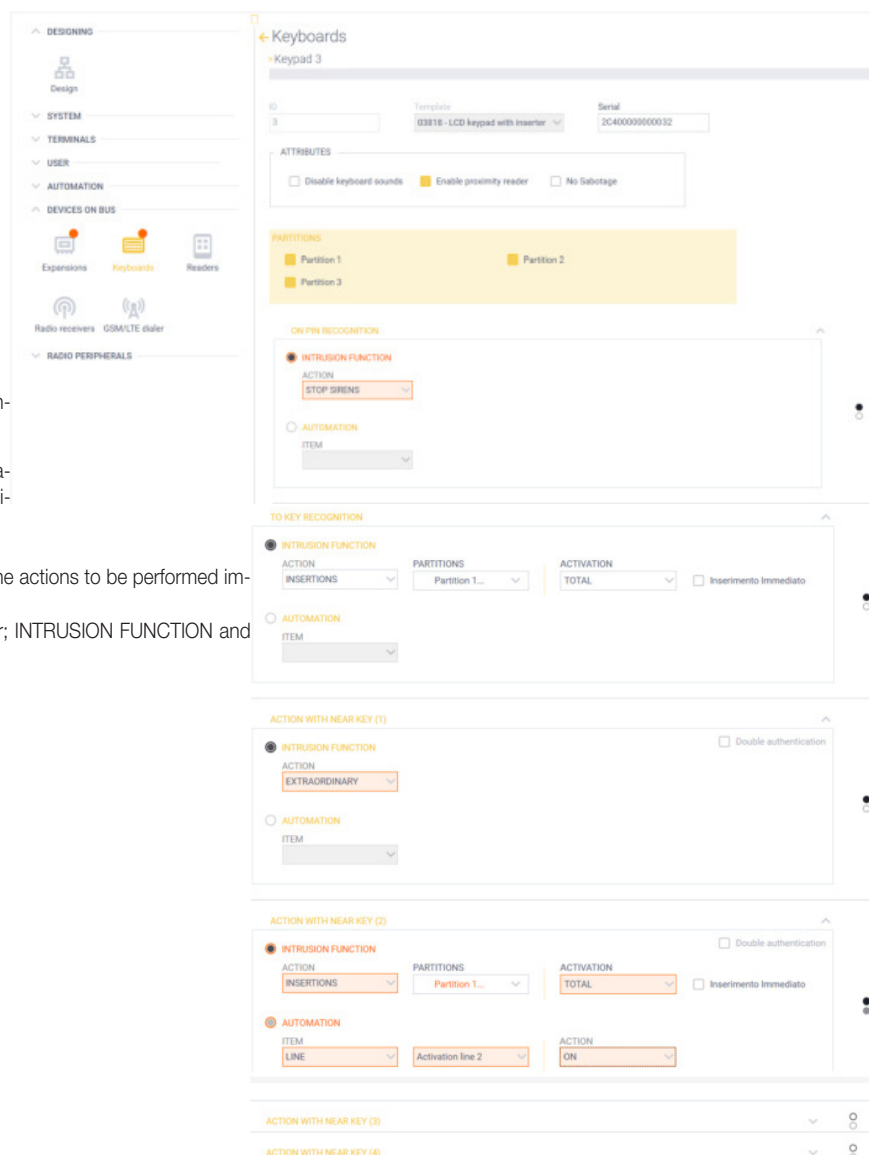
No sabotage: if enabled, the keyboard will not signal expansion sabotage.

PARTITIONS. This section serves to set the partitions enabled on the expansion. N.B. In keypad 03818, these partitions will be enabled on the onboard reader.

ON PIN RECOGNITION. This section serves to program the actions to be performed immediately when the keyboard recognises a valid user PIN.

Two functions can be enabled independently of each other; **INTRUSION FUNCTION** and **AUTOMATION**.

INTRUSION FUNCTION



Keyboards

Keypad 3

ID: 3 Template: 03818 - LCD keypad with Inserter Serial: 2C400000000032

ATTRIBUTES

☐ Disable keyboard sounds ☒ Enable proximity reader ☐ No Sabotage

PARTITIONS

☒ Partition 1 ☒ Partition 2 ☐ Partition 3

ON PIN RECOGNITION

☒ **INTRUSION FUNCTION**

ACTION: STOP SIRENS

☐ **AUTOMATION**

ITEM:

TO KEY RECOGNITION

☒ **INTRUSION FUNCTION**

ACTION: INSERTIONS PARTITIONS: Partition 1... ACTIVATION: TOTAL ☐ Inserimento Immediato

☐ **AUTOMATION**

ITEM:

ACTION WITH NEAR KEY (1)

☒ **INTRUSION FUNCTION** ☐ Double authentication

ACTION: EXTRAORDINARY

☐ **AUTOMATION**

ITEM:

ACTION WITH NEAR KEY (2)

☒ **INTRUSION FUNCTION** ☐ Double authentication

ACTION: INSERTIONS PARTITIONS: Partition 1... ACTIVATION: TOTAL ☐ Inserimento Immediato

☒ **AUTOMATION**

ITEM: LINE Activation line 2 ACTION: ON

ACTION WITH NEAR KEY (3)

ACTION WITH NEAR KEY (4)

Expansions

TO KEY RECOGNITION

INTRUSION FUNCTION

ACTION

INSERTIONS

EXTRAORDINARY

CANCEL AUTOINS.

STOP SIRENS

STOP CALLS

CLEAR MEMORIES

PARTITIONS

Partition 1...

ACTIVATION

TOTAL

☐ Inserimento Immediato

If enabled (see the green box), the ACTION can be selected from the following options:

- **INSERTIONS** – arming/disarming partitions in various modes.
Selecting this action allows you to set which partitions to operate on and in which mode.
- **EXTRAORDINARY** – overtime work request, which postpones the partition auto-arming time by x minutes
This action will be extended to all common partitions common to the profile and keyboard on which the user is operating
- **CANCEL AUTOINS.** – does not perform the next partition auto-arming (from the time at which the ACTION is activated).
This action will be extended to all common partitions common to the profile and keyboard on which the user is operating
- **STOP SIRENS** – deactivates all “siren” outputs
- **STOP CALLS** – stops all ongoing notifications
- **CLEAR MEMORIES** – erases the alarm memories (and sabotage memories if the profile allows).
This action will be extended to all common partitions common to the profile and keyboard on which the user is operating

The Immediate arming option arms the partitions immediately, ignoring all output delay times.

For the following options:

- **TO KEY RECOGNITION**
- **ACTION WITH NEAR KEY (1)**
- **ACTION WITH NEAR KEY (2)**
- **ACTION WITH NEAR KEY (3)**
- **ACTION WITH NEAR KEY (4)**

The same settings as described for **ON PIN RECOGNITION** apply.

ACTION WITH NEAR KEY (x), where x ranges from 1 to 4, are the four actions that can be set on the reader in the keyboard.

AUTOMATION

If enabled, the ACTION can be selected from the following options:

- **OUTPUT** – output activation/deactivation and corresponding output activation mode
- **LINE** – line activation/deactivation and corresponding line activation mode
- **SCENARIO** – activation of an activation scenario

Expansions

12.3 BUS EXPANSIONS – Readers

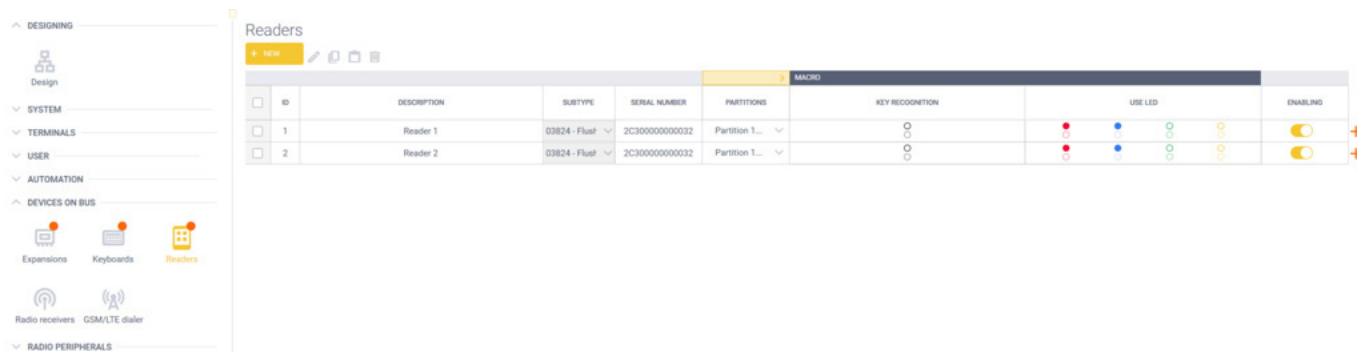
The reader summary screen displays a grid in which the SUBTYPE indicates the reader type, 03824.

In particular, the software automatically sets some digits of the serial number:

- **2C3** is the expansion type, 03824 in this case.
- The installer must enter the 8 digits (in the red box in the figure), which are unique for each reader.
- The last three digits, **032** in the example, are predefined by the manufacturer.

The columns in the grid contain some editable data, while other data in the table is display-only (not editable), but is useful for identifying if and what is programmed for the readers.

For example (in the figure below), note that for **Reader 2**, the KEY RECOGNITION and USE LED columns contain some data (see ).



ID	DESCRIPTION	SUBTYPE	SERIAL NUMBER	PARTITIONS	KEY RECOGNITION	USE LED	ENABLING
1	Reader 1	03824 - Flush	2C300000000032	Partition 1...			
2	Reader 2	03824 - Flush	2C300000000032	Partition 1...			

Click  to create a new reader; enter the description and select the template.

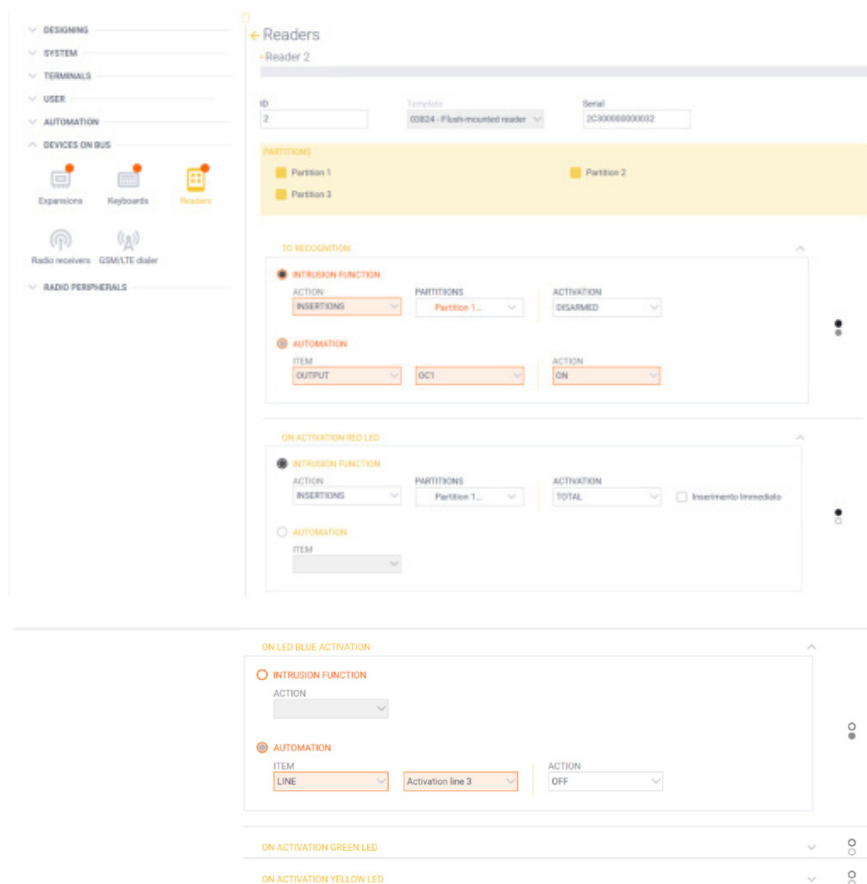
The first box serves to set the description and serial.

PARTITIONS. This section serves to set the partitions enabled on the expansion.

For the following options:

- ON ACTIVATION RED LED
- ON LED BLUE ACTIVATION
- ON ACTIVATION GREEN LED
- ON ACTIVATION YELLOW LED

The same settings as described for **ON PIN RECOGNITION** apply (see the relevant paragraph).



Reader 2

ID: 2 Template: 03824 - Flush-mounted reader Serial: 2C300000000032

PARTITIONS

- Partition 1
- Partition 2
- Partition 3

TO RECOGNITION

INTRUSION FUNCTION

ACTION: INSERTIONS PARTITIONS: Partition 1... ACTIVATION: DISARMED

AUTOMATION

ITEM: OUTPUT OC1 ACTION: ON

ON ACTIVATION RED LED

INTRUSION FUNCTION

ACTION: INSERTIONS PARTITIONS: Partition 1... ACTIVATION: TOTAL ☐ Inseminato Immediato

AUTOMATION

ITEM:

ON LED BLUE ACTIVATION

INTRUSION FUNCTION

ACTION:

AUTOMATION

ITEM: LINE Activation line 3 ACTION: OFF

ON ACTIVATION GREEN LED

ON ACTIVATION YELLOW LED

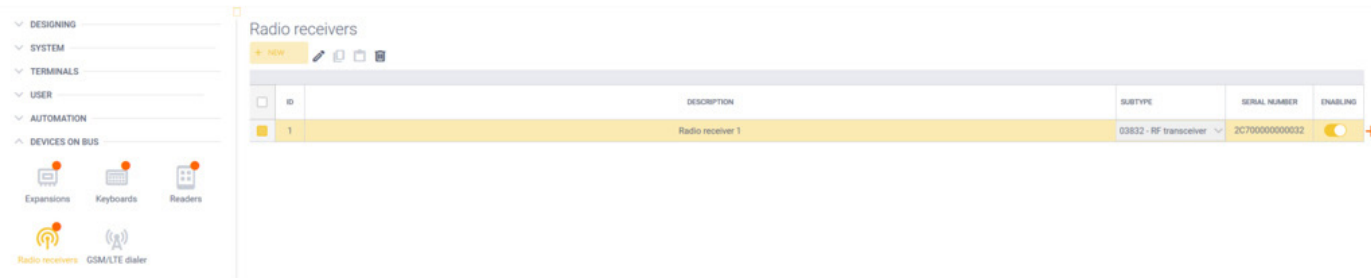
Expansions

12.4 BUS EXPANSIONS – Radio receivers

The radio receiver summary screen displays a grid in which the SUBTYPE indicates the radio frequency interface, 03831, or the signal repeater, 03832.

In particular, the software automatically sets some digits of the serial number:

- **2C7** is the expansion type, transceiver 03831/03832 in this case.
- The installer must enter the 8 digits (in the red box in the figure), which are unique for each transceiver.
- The last three digits, **032** in the example, are predefined by the manufacturer.



Click **+ NUOVA** to create a new radio receiver; enter the description and select the template.

The description and serial can be set.

ID: a numeric index assigned to the receiver.

Serial: the unique QR code of the receiver

ATTRIBUTES

No sabotage: if enabled, receiver sabotage will not be signalled.

← Radio receivers

> Radio receiver 1

ID	Template	Serial
1	03832 - RF transceiver	2C700000000032

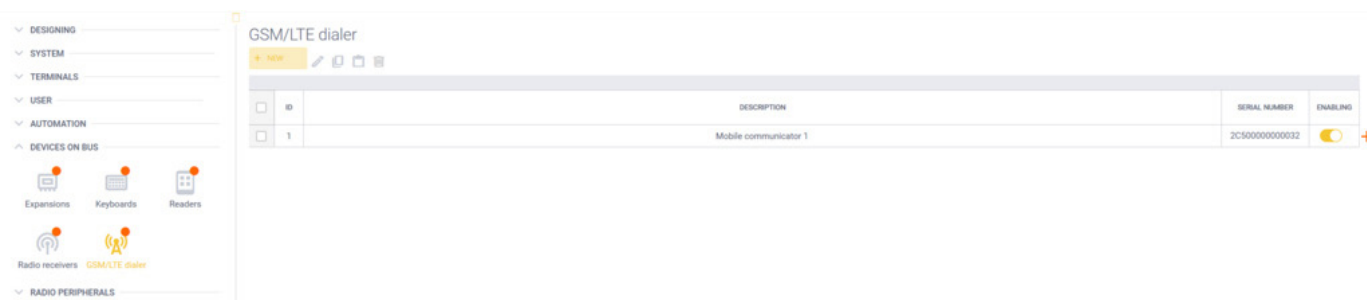
ATTRIBUTES

☐ No Sabotage

Expansions

12.5 BUS EXPANSIONS – (LTE dialer art. 03810/03820)

Only one LTE dialer can be added to the panel.



There is an option to enable/disable the device for maintenance by the installer.

The corresponding parameters are described below.

ATTRIBUTES

No sabotage: if enabled, dialer sabotage will not be signalled.

SMS on 2G network: If enabled, the dialer will send text messages using the 2G network service provided by the operator (standard for SMS) instead of the 4G network service (LTE). **Note:** this option is enabled by default and we do not recommend changing it. Only some operators support the SMS service over 4G; if the option is changed, check that the panel can send text messages.

Emergency action delay: this is the delay time in s before sending a text message in the event of data loss on the dialer BUS line. **NOTE:** If the dialer has a battery and it detects a power failure, the emergency text message is sent after 10 s.

Emergency SMS recipient user: If configured, in the event of data loss on the dialer BUS line, the dialer will receive a text message at the number associated with the user (if programmed). **Note:** programming is limited to INSTALLER and MASTER 1 users (always present in the project).

DATA NETWORK box

APN-NAME, APN-USER, APN-PASSWORD: are parameters provided by the LTE service provider. They are also required for 4G calls (VoLTE), if the operator supports them.

DATA NETWORK: enables/disables use of the data network

AUTOMATIC APN: If enabled, the APN fields will not be editable and the panel and dialer will automatically detect the required configuration (valid with the most common Italian operators)

Note: after configuring the panel and dialer with this option, wait a few minutes to allow self-configuration and check that there are no faults in the dialer (the dialer status can be checked from the MONITOR page or from the installer's diagnostic menu on the keyboard), then read the configuration again with the software, and the acquired APN will be available in the relevant fields (read-only).

VOLUMES box

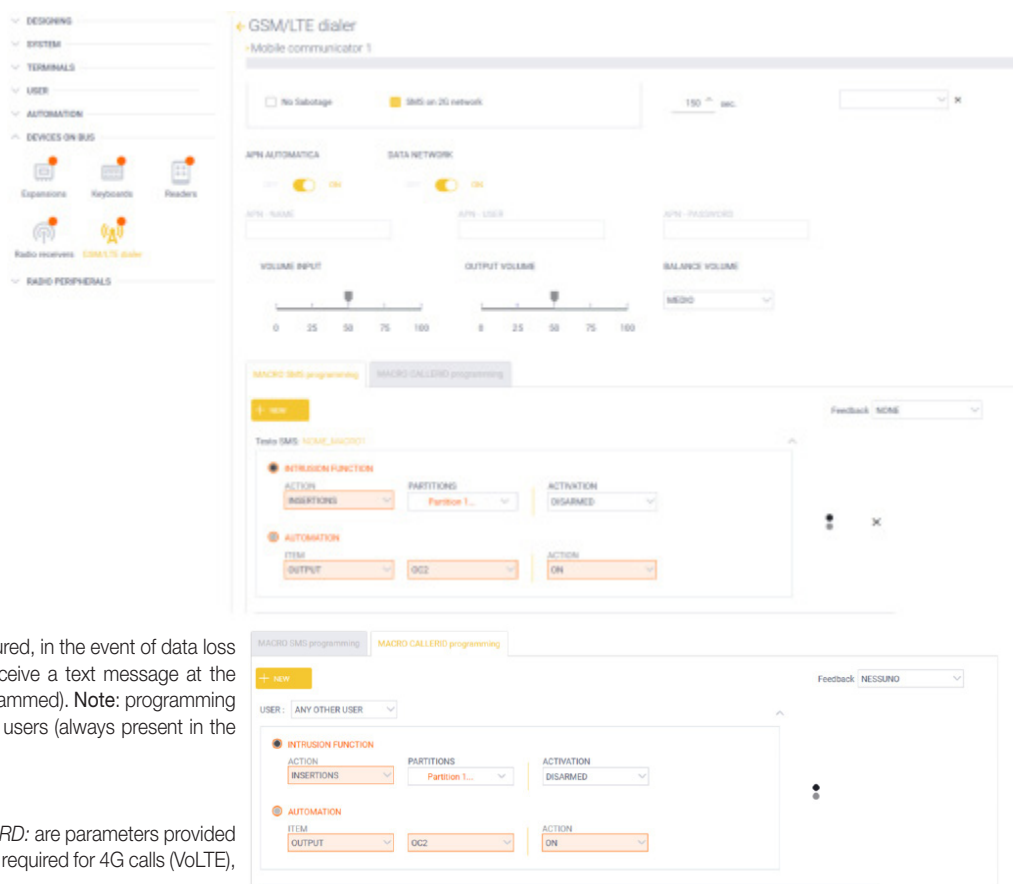
VOLUME INPUT: this adjusts the volume of the analogue input channel to the dialer.

OUTPUT VOLUME: this adjusts the volume of the analogue output channel from the dialer.

BALANCE VOLUME: this adjusts the balance between the input volume and output volume.

MACRO SMS programming and MACRO CALLERID programming

These are programming structures that are identical to the MACROS described previously (see "WILDCARD MACROS" described in para. 10.2 USER – Users).



Expansions

MACRO SMS programming serves to take actions when the dialer receives a text message, the text of which can be programmed in the *SMS text* parameter (INPUT in the example in the figure). The SMS text format is described in the user manual.

MACRO CALLERID programming serves to take actions when the dialer receives a call from a user whose caller ID is intercepted: if the number is from a user configured for a specific callerID action, the corresponding macro runs, otherwise if the number is from a user programmed to the system but not configured for a specific callerID action, the ANY OTHER USER macro runs, if programmed.

Feedback: this parameter serves to alert the user (who sent the command SMS or made the phone call) that the command was successful. The options are:
NONE – no feedback is sent, so the user does not know if the command was successful.

SMS – a result SMS is sent.

RINGBACK – sends a simple ring if successful.

MACRO SMS programming and MACRO CALLERID programming

These are programming structures that are identical to the MACROS described previously (see "WILDCARD MACRO" described in para. 10.2 USER – Users).

MACRO SMS programming serves to take actions when the communicator receives a text message, the text of which can be programmed in the *SMS text* parameter (INPUT in the example in the figure). The SMS text format is described in the user manual.

Other MACRO CALLERID programming serves to take actions when the communicator receives a call from a user whose caller ID is intercepted: if the number is from a user configured for a specific macro callerID, the corresponding macro runs, otherwise if the number is from a user programmed to the system but not configured for a specific macro callerID, the ANY OTHER USER macro runs, if programmed.

Feedback: this parameter serves to alert the user (who sent the command SMS or made the phone call) that the command was successful. The options are:
NONE – no feedback is sent, so the user does not know if the command was successful.

SMS – a result SMS is sent.

RING – sends a simple ring if successful.

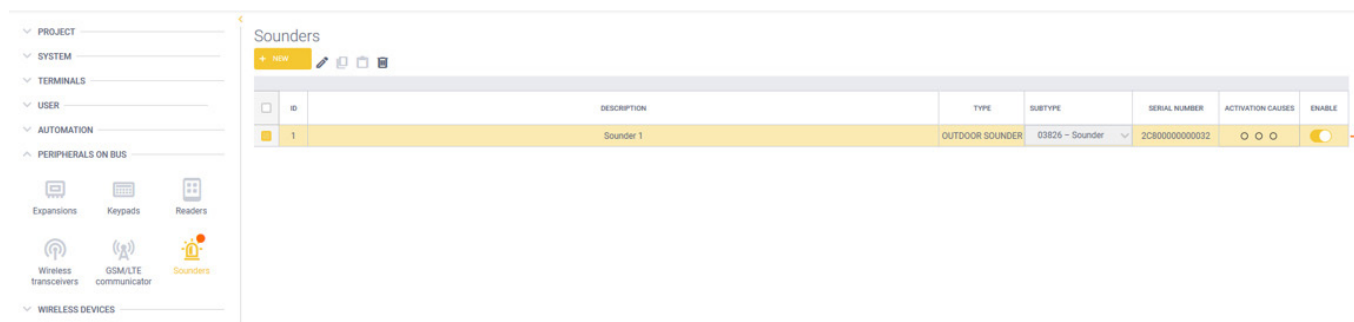
12.6 BUS EXPANSIONS – Sounders

The bus sounder summary screen displays a grid in which the SUBTYPE indicates the sounder type, 03826.

Click on "New" to create a new sounder and set its description.

In particular, the software automatically sets some digits of the serial number:

- **2C8** is the expansion type, Sounder - 03826 in this case.
- The installer must enter the 8 digits (in the red box in the figure), which are unique for each sounder.
- The last three digits, **032** in the example, are predefined by the manufacturer.

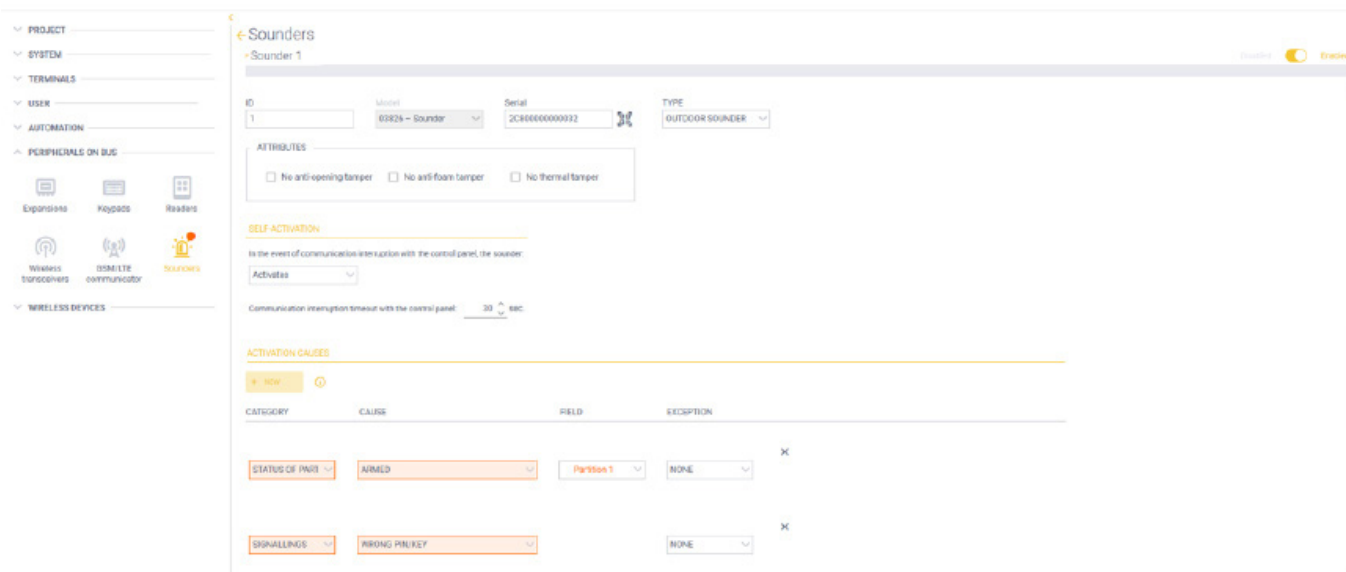


ID	DESCRIPTION	TYPE	SUBTYPE	SERIAL NUMBER	ACTIVATION CAUSES	ENABLE
1	Sounder 1	OUTDOOR SOUNDER	03826 - Sounder	2C800000000032	○ ○ ○	ON

There is an option to enable/disable the device for maintenance by the installer.

Expansions

The corresponding parameters are described below.



TYPE

Allows you to define whether the sounder is an external sounder instead of an internal one.

ATTRIBUTES

Allows you to disable selectively the tampering events generated in the event of opening or tearing ("No anti-opening tamper"), foam attack ("No anti-foam tamper") and oxygen lance or forced freezing attack ("No thermal tamper").

ACTIVATION CAUSES - AUTONOMOUS

Determines the general behaviour of the sounder in the absence of communication, regardless of the activation causes programmed in the subsequent section. This may occur, for instance, in the case of cut BUS cables or a different system failure which prohibits the sending of controls

It includes 3 modes:

- Immediate activation on detection of absence of communication ("Activates")
- Activation only in the event of a sounder tampering ("Activates tamper")
- No activation ("Does not activate")

Communication interruption timeout with the control panel

Allows you to determine after what time interval without valid communication the sounder is considered isolated from the system and therefore operating autonomously. This timeout is ignored if the total absence of power supply provided by the system is detected and so the sounder immediately switches to autonomous operation.

ACTIVATION CAUSES

Up to 3 activation causes per sounder can be configured. The order with which they are defined determines their priority, with the first one from the top deemed to have priority over subsequent ones.

For the choice of activation mode, please refer to the chapter "SYSTEM – Panel – SOUNDERS", in the section about panel configuration.

- Category: allows you to select which category of events the sounder will respond to;
- Cause: Allows you to discriminate, for the selected category, a subset of events for which you want to generate an activation;
- Field: allows you to specify the field of application of the activation (partitions or terminals involved);
- Exception: defines any cases for which the sounder will not perform the activation or will perform it late.

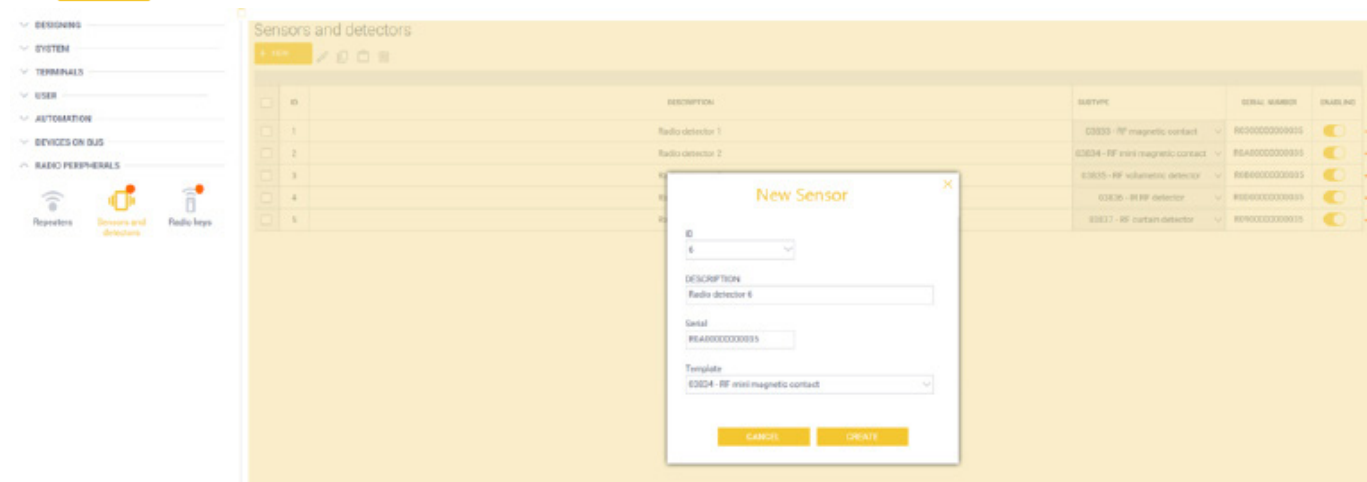
Expansions

12.7 RADIO PERIPHERALS – Sensors and detectors

This section serves to add/delete radio devices and set their parameters in the same way as for BUS devices. For a full description of operation, see the manual for the radio interface 03831.

When adding a new radio device, specify the **Serial** (the QR code on all radio devices) and then you can enter the **DESCRIPTION**.

Click **+ NUOVA** to add a new radio device.



Template serves to select the type of radio device to be added; the list displays the article codes and their descriptions.

After adding the new radio device, you can double-click it to edit the description and set the parameters, which depend on the type of article added.

- **Art. 03833 – Magnetic contact**

ATTRIBUTES - No Sabotage: device sabotage is not detected

ATTRIBUTES - Deactivate light signalling: the LED is not activated to indicate an alarm/sabotage related to the device or its signals

ATTRIBUTES - Detect sabotage from reed: if only one side of the magnet is selected, closing the unused reed will generate a magnetic sabotage condition

ATTRIBUTES - Immediate recovery: if the magnetic signal returns to its standby condition, this is transmitted immediately to the transceiver

ATTRIBUTES - Activate magnetic contact short side: the magnetic reed is on the short side of the device

ATTRIBUTES - Activate magnetic contact long side: the magnetic reed is on the long side of the device

N.B. Both the Activate magnetic contact short side and Activate magnetic contact long side options can be set.

- **Article 03834 – Mini magnetic contact**

ATTRIBUTES - No Sabotage: device sabotage is not detected

ATTRIBUTES - Deactivate light signalling: the LED is not activated to indicate an alarm/sabotage related to the device or its signals

ATTRIBUTES - Detect sabotage from reed: if only one side of the magnet is selected, closing the unused reed will generate a magnetic sabotage condition

ATTRIBUTES - Immediate recovery: if the magnetic signal returns to its standby condition, this is transmitted immediately to the transceiver

- **Article 03835 - Dual technology detector**

- **Article 03836 - Passive infrared detector**

- **Article 03837 - Curtain detector**

ATTRIBUTES - No Sabotage: device sabotage is not detected

ATTRIBUTES - Deactivate light signalling: the LED is not activated to indicate an alarm/sabotage related to the device or its signals

ATTRIBUTES - Disable with partition disarmed: the device disables signal detection and signalling to optimise battery consumption

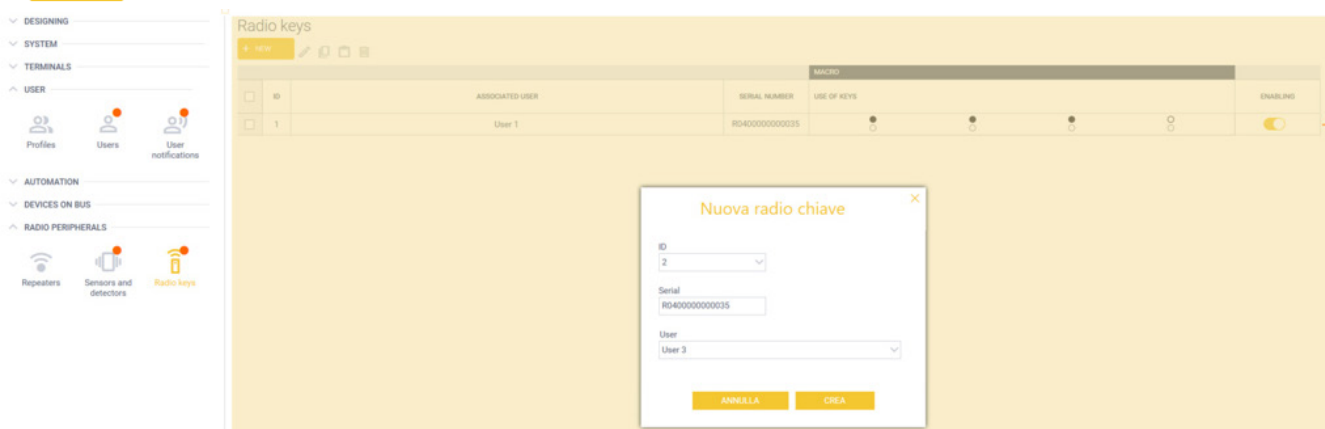
Expansions

12.8 RADIO PERIPHERALS – Radio keys (remote controls)

This section serves to add/delete remote controls and assign them to the users who will use them.

When adding a new radio device (see the figure below), you can enter the **DESCRIPTION** and must specify the **Serial**. Serial is the QR code found on all radio devices.

Click **+ NUOVA** to add a new remote control.



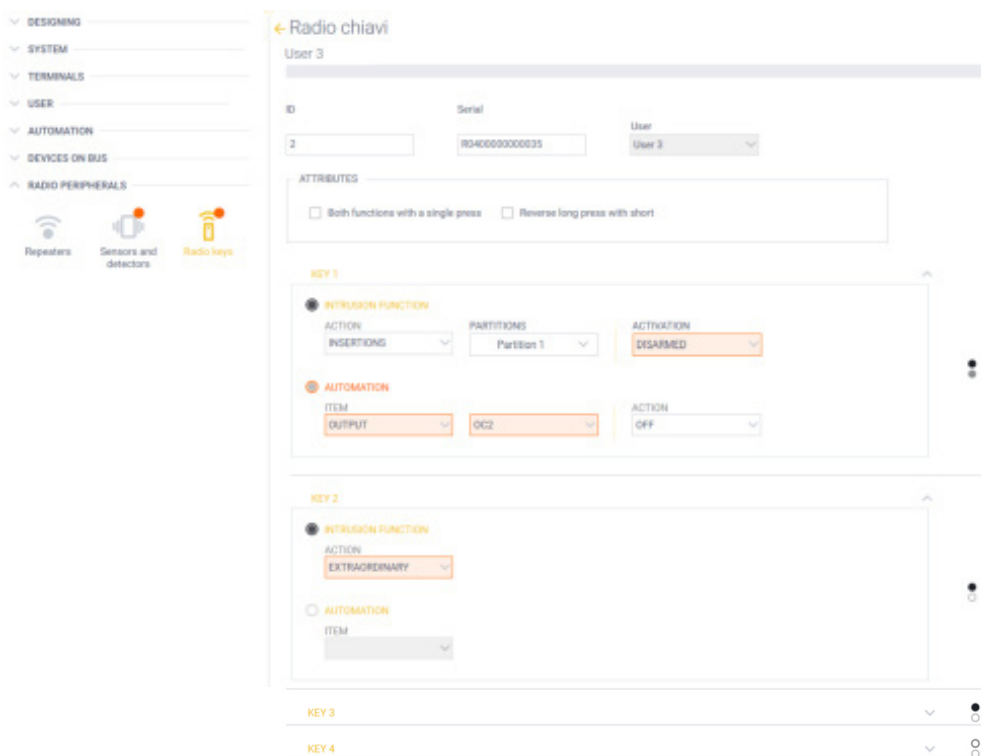
The **User** parameter in the drop-down menu serves to select the user to whom the remote control is to be assigned.

By its nature, the remote control does NOT have its own description since it is associated with a user.

The remote control has 4 keys and each key can be programmed with 2 separate functions defined as **INTRUSION FUNCTION** and **AUTOMATION** (described below);

- to perform the **INTRUSION FUNCTION** programmed for a key, press the key for a short time, ~1 s
- to perform the **AUTOMATION** function programmed for a key, press the key for a long time, >2 s.

The screen below shows the remote control parameters.



The **Enabled/Disabled** option that enables or disables the remote control is at the top right.

ATTRIBUTES – Both functions with a single press: if enabled, a short key press will perform both the **INTRUSION FUNCTION** and **AUTOMATION** function

ATTRIBUTES – Reverse long press with short: if enabled, this swaps the functions activated with a long and short key press (short press=>**AUTOMATION**, long press=>**INTRUSION FUNCTION**).

The **KEY 1**, **KEY 2**, **KEY 3** and **KEY 4** boxes serve to set the **INTRUSION FUNCTION** and **AUTOMATION** in the same way as described in the users, keys, readers, etc. sections.


To activate the remote control, go near the radio receiver and press the F3 and F4 keys at the same time.

Expansions

12.9 RADIO DEVICES – Sirens

In this section, the radio sirens are added/deleted and the related parameters are set.

When adding a new radio siren, specify the **Serial** (the QR code on all radio devices) and then enter the **DESCRIPTION**.

Click on  “NEW” to add a new radio siren.

All the parameters which can be configured for the radio siren are the same as those already described for the bus siren; for full details see para.12.6.

13. SYSTEM MONITOR

This section displays the operating status of all wired and radio devices, zones, outputs, dialer, etc. Alarms, faults, tampering, signal levels, battery levels etc. are displayed, depending on the peripheral type.

In general, the following data is available on the monitor screen:

- **for the panel**

- > partition state
 - armed/disarmed
 - alarm
 - alarm memory
 - sabotage

- > **battery state**

- > voltage and current at the auxiliary power supply terminals
- > faults

- **for wired/BUS peripherals:**

- > on the BUS/disappearance
- > BUS power supply voltage
- > battery state (if any)
- > sabotage

- **for input terminals**

- > operational state
 - standby
 - alarm
 - alarm memory
 - sabotage
 - inhibited/isolated

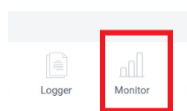
- **for output terminals**

- > activated/deactivated

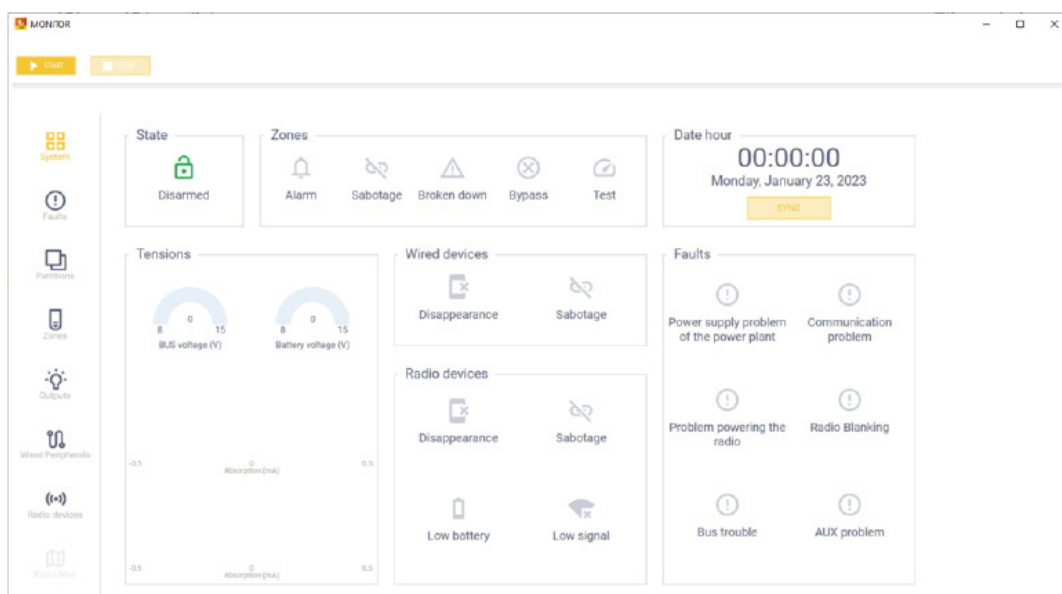
- **for radio devices:**

- > presence/disappearance
- > radio signal level
- > battery level
- > a map with the radio devices configured in the project; the corresponding icon will be disabled if there is no radio receiver in the project.

Click the Monitor icon to start monitoring



When the screen opens, click  .

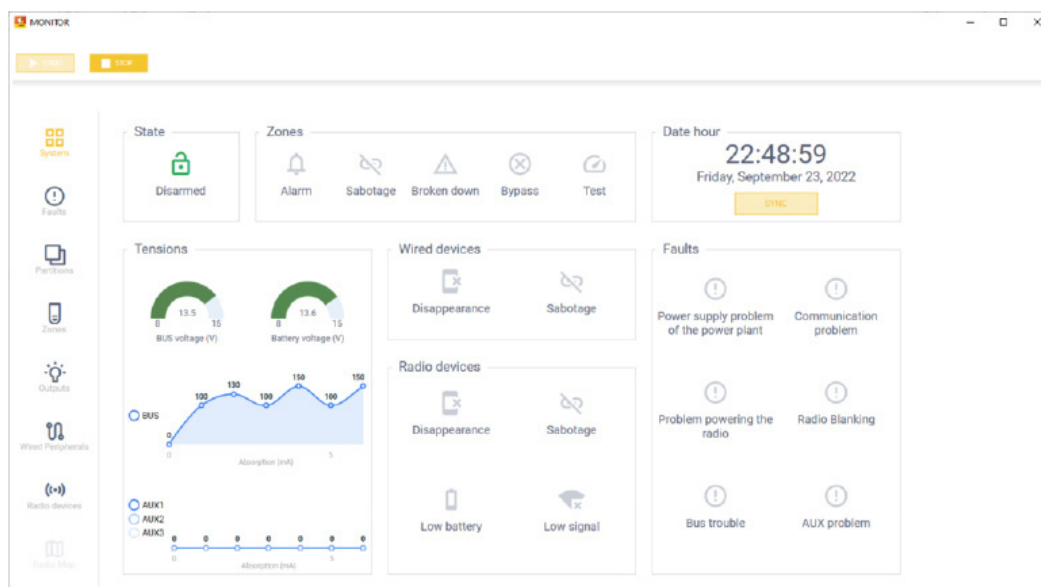


System monitor

The main “Dashboard” page displays the system status in real time, providing a general summary. The “Dashboard” is divided into seven sections:

- State
- Zones
- Date hour
- Tensions
- Wired devices
- Radio devices
- Faults

Dashboard



State: This indicates the armed state of the system partitions.

- In maintenance: when the panel is being serviced
- In programming: when the installer is performing programming
- In alarm
- Armed in total mode
- Armed in partial mode
- Disarmed

Zones: This indicates the state of the zones, i.e. if at least one of the system zones is in one of the following states:




- Alarm
- Sabotage
- Broken down
- Bypass
- Test

Date hour: This displays the time set on the panel and can synchronise it with the time on the PC from which you are monitoring.

Tensions: At intervals of 5 s, this displays the voltages measured on the BUS and battery, and the absorption of the BUS and the three AUX

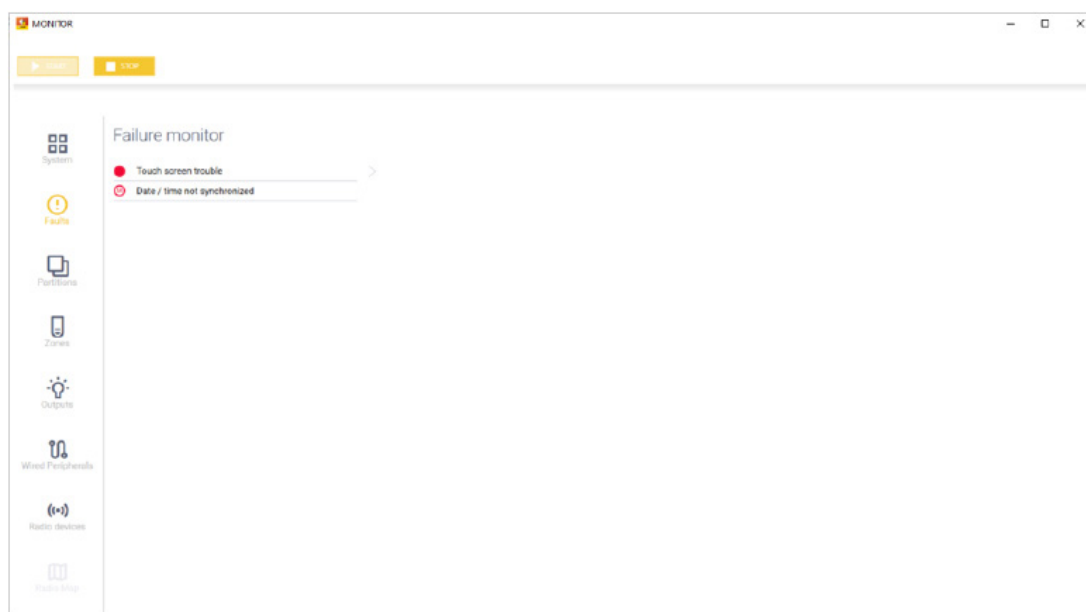
Wired devices: This displays if at least one wired device (keyboards, readers, expansions, etc.) has disappeared or has been sabotaged.

Radio devices: As for wired devices, this displays if at least one of the radio devices has disappeared or has been sabotaged, and indicates if at least one of them has a low battery or low signal.

Failures: This summarises any faults detected by the panel into six macro categories. This box is not interactive. If the  symbol appears for one of the six categories, you can click the  symbol in the left column to view details of the category. This will open the page below containing icons and descriptions of the actual faults detected. If there is a  symbol to the right of the fault, click it to view additional details.

System monitor

Faults



This page lists details of all the faults detected by the panel or from its fault memory.

Some of them have an additional level of detail, which can be reached by clicking the arrow at the end of the general description.

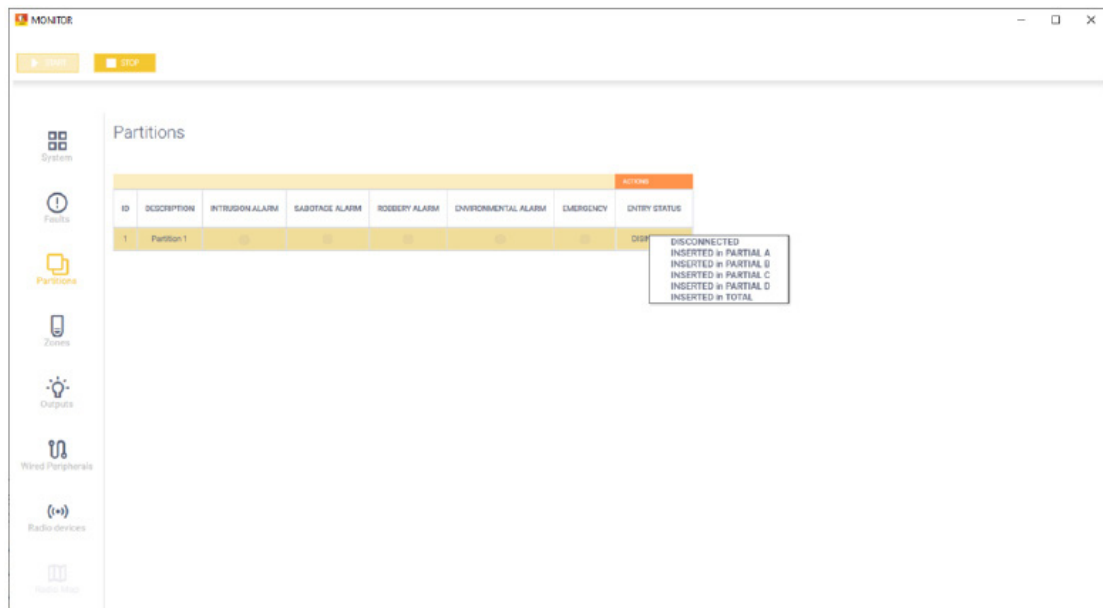
The complete fault list is as follows:

- AC off
- Power-supply unit fault
 - > Overload
 - > Over-temperature
 - > Earth fault
 - > No communication
- Low battery
- Battery fault
 - > Inefficient
 - > Short circuit
 - > Disconnected
- Interconnect BUS fault
 - > Overvoltage
 - > Low voltage
 - > Short circuit
 - > Overcurrent
- Peripheral power supply fault (wired or radio)
 - Disconnected
- Peripheral battery fault (wired or radio)
 - > Disconnected
- Remote fault
 - > Remote fault 1 (Touch screen disconnected)
 - > Remote fault 2 (Alarm not notified)
 - > Remote fault 3
 - > Remote fault 4
- Peripheral disappeared (wired or radio)
- Peripheral low battery (wired or radio)
- Output malfunction
- AUX1 problem
 - > Overvoltage
 - > Low voltage
 - > Short circuit
 - > Overcurrent

System monitor

- AUX2 problem
 - > Overvoltage
 - > Low voltage
 - > Short circuit
 - > Overcurrent
- AUX3 problem
 - > Overvoltage
 - > Low voltage
 - > Short circuit
 - > Overcurrent
- Date/time not synchronised
- Radio jammed
 - > First frequency
 - > Second frequency
 - > Third frequency
 - > Fourth frequency
- PSTN fault
- Mobile DATA channel fault
- Mobile VOICE channel fault
- LAN fault
- Communication fault to the Security Station
 - > Faulty or disappeared
 - > No communication

Partitions

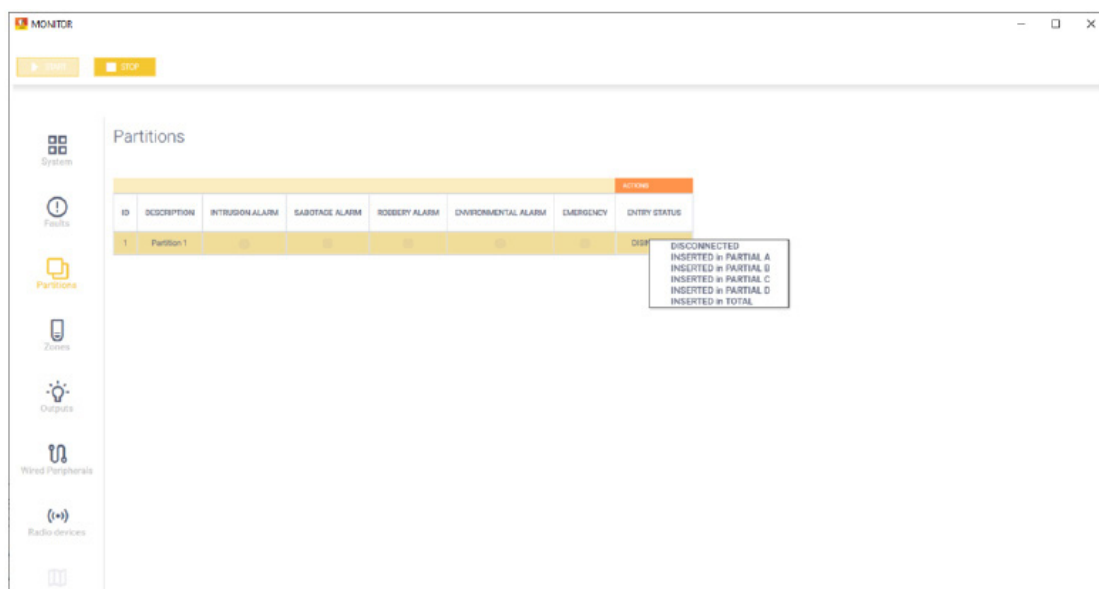


ID	DESCRIPTION	INTRUSION ALARM	SABOTAGE ALARM	ROBBERY ALARM	ENVIRONMENTAL ALARM	EMERGENCY	ENTRY STATUS
1	Partition 1						DISARM

DISCONNECTED
 INSERTED in PARTIAL A
 INSERTED in PARTIAL B
 INSERTED in PARTIAL C
 INSERTED in PARTIAL D
 INSERTED in TOTAL

This page displays the state of the partitions in real time.

- Intrusion alarm
- Sabotage alarm
- Robbery alarm
- Environmental alarm
- Emergency
- Entry status

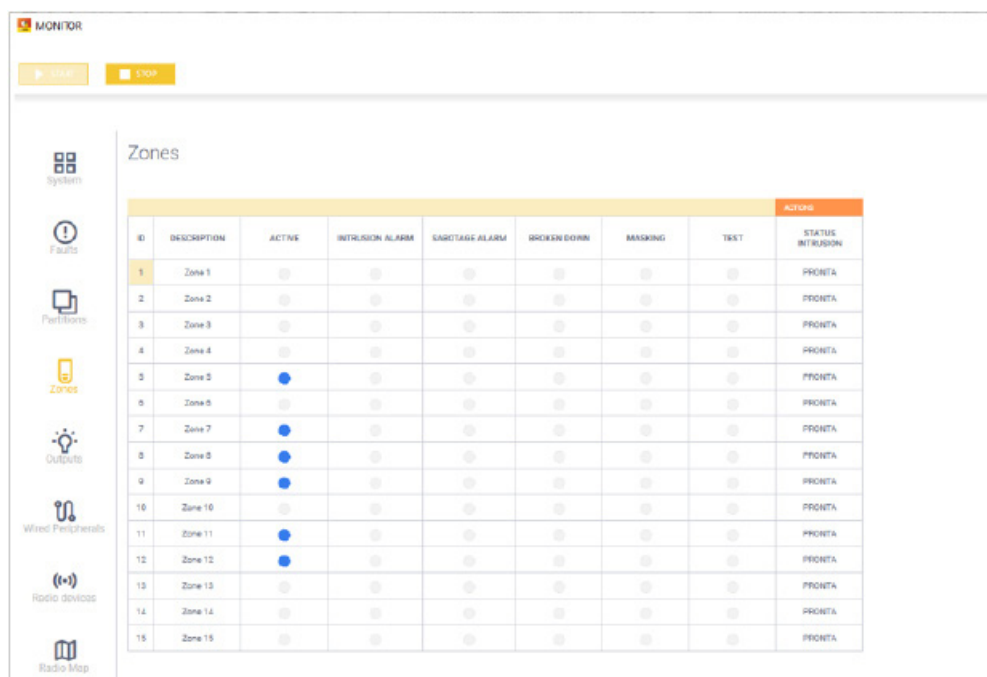


Right-click in the “ACTIONS” column (*) to open the context menu and change the armed status of the selected partition. The following options are available:

- DISCONNECTED
- INSERTED in PARTIAL A
- INSERTED in PARTIAL B
- INSERTED in PARTIAL C
- INSERTED in PARTIAL D
- INSERTED in TOTAL

(*) Actions: The possible commands in the “Actions” column can only be forwarded to the panel if the installer has been enabled by a user. The user can set this enable and the corresponding disable from the keyboard menu User → Permissions → Installer → Use timed user profile. Once enabled, the installer will operate on all partitions belonging to the profile of the user code that authorised them for the specified time.

Zones



This page displays the state of the zone in real time.

- Active
- Intrusion alarm
- Sabotage alarm
- Broken down
- Masking
- Current zone state.

MONITOR

START STOP

Zones

ID	DESCRIPTION	ACTIVE	INTRUSION ALARM	SABOTAGE ALARM	BROKEN DOWN	MASKED	TEST	ACTIONS	
								STATUS	INTRUSION
1	Zone 1							PRONTA	
2	Zone 2							PRONTA	
3	Zone 3							PRONTA	
4	Zone 4							PRONTA	
5	Zone 5							PRONTA	
6	Zone 6							PRONTA	
7	Zone 7							PRONTA	
8	Zone 8							PRONTA	
9	Zone 9							PRONTA	
10	Zone 10							PRONTA	
11	Zone 11							PRONTA	
12	Zone 12							PRONTA	
13	Zone 13							PRONTA	
14	Zone 14							PRONTA	
15	Zone 15							PRONTA	

Include Exclude Inhibit

Right-click in the “ACTIONS” column (*) to perform certain actions on the selected zone. The following options are available:

- Include
- Exclude (permanently disable the zone until the user re-enables it)
- Inhibit (disable that lasts for the duration of the next armed state, and is then re-enabled automatically the next time it is disarmed)

(*) Actions: The possible commands in the “Actions” column can only be forwarded to the panel if the installer has been enabled by a user. The outcome of the action will depend on the type of action required, the REGULATION configured on the panel and the related PERMISSIONS activated from the keyboard. (see the REGULATION paragraph)

If the action is successful, the zone intrusion status will have been changed.

Outputs

MONITOR

START STOP

Outputs

ID	Description	BROKEN DOWN	ACTIONS	
			STATE	
1	SE			
2	OC1			
3	OC2			
4	AUX1			
5	AUX2			
6	AUX3			

Right-click in the “ACTIONS” column (*) to perform certain actions on the selected output. The following options are available:

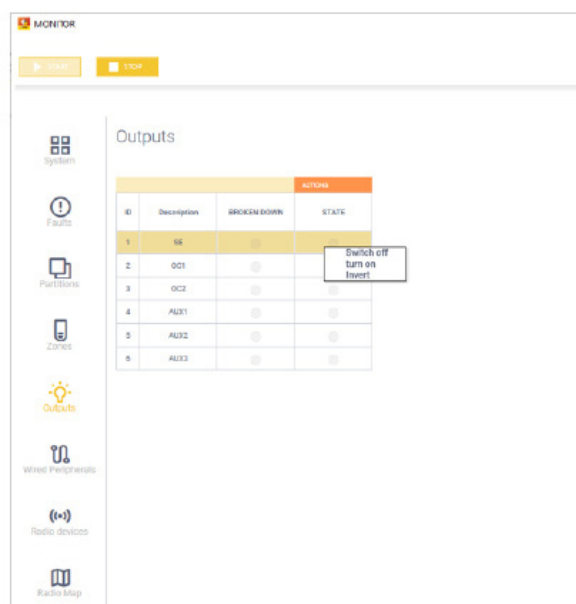
- Switch off
- Turn on
- Invert

The installer can always perform this operation.

System monitor

This page displays the output states.

- Broken down
- State



The screenshot shows the MONITOR interface with a sidebar on the left containing icons for System, Faults, Partitions, Zones, Outputs (highlighted), Wired Peripherals, Radio devices, and Radio Map. The main area is titled 'Outputs' and contains a table with columns: ID, Description, BROKEN DOWN, and STATE. A tooltip 'Switch off turn on Invert' is visible over the STATE column.

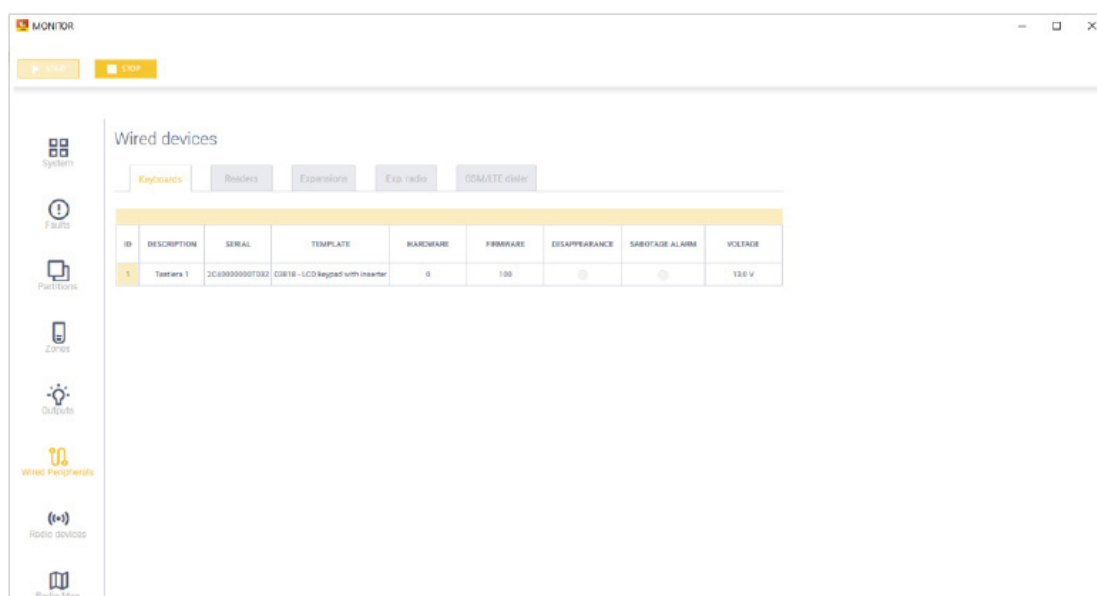
ID	Description	BROKEN DOWN	STATE
1	IS		
2	OC1		
3	OC2		
4	ALX1		
5	ALX2		
6	ALX3		

Right-click in the "ACTIONS" column (*) to change the output state. The following options are available:

- Switch off
- Turn on
- Invert

(*) Actions: The possible commands in the "Actions" column can only be forwarded to the panel if the installer has been enabled by a user. The user can set this enable and the corresponding disable from the keyboard menu User > Permissions > Installer > Use timed user profile. Once enabled, the installer will operate on all partitions belonging to the profile of the user code that authorised them for the specified time.

Wired devices

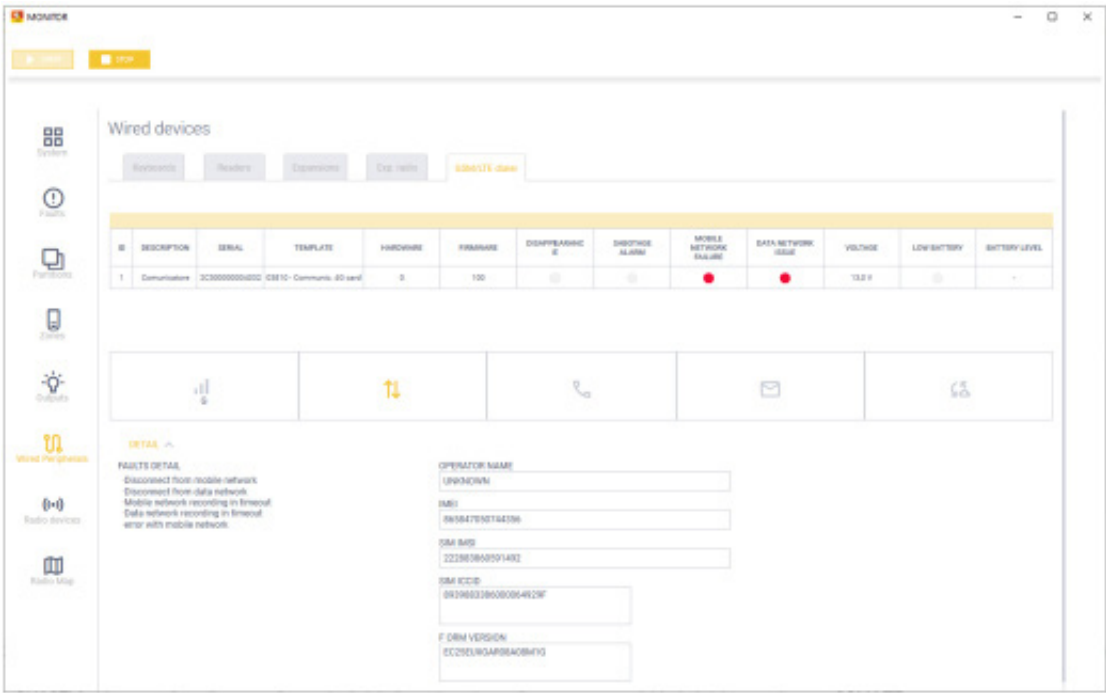


The screenshot shows the MONITOR interface with the 'Wired devices' section selected. The sidebar is the same as in the previous screenshot. The main area has tabs for Keyboards, Readers, Expansions, Exp. radio, and GSM/ETC dialer. Below the tabs is a table with columns: ID, DESCRIPTION, SERIAL, TEMPLATE, HARDWARE, FIRMWARE, DISAPPEARANCE, SABOTAGE ALARM, and VOLTAGE.

ID	DESCRIPTION	SERIAL	TEMPLATE	HARDWARE	FIRMWARE	DISAPPEARANCE	SABOTAGE ALARM	VOLTAGE
1	Testarea 1	2C630000007082	CBS10 - LCD keypad with master	0	1.00			13.0 v

This page displays the list of wired devices enrolled in the panel and their features.

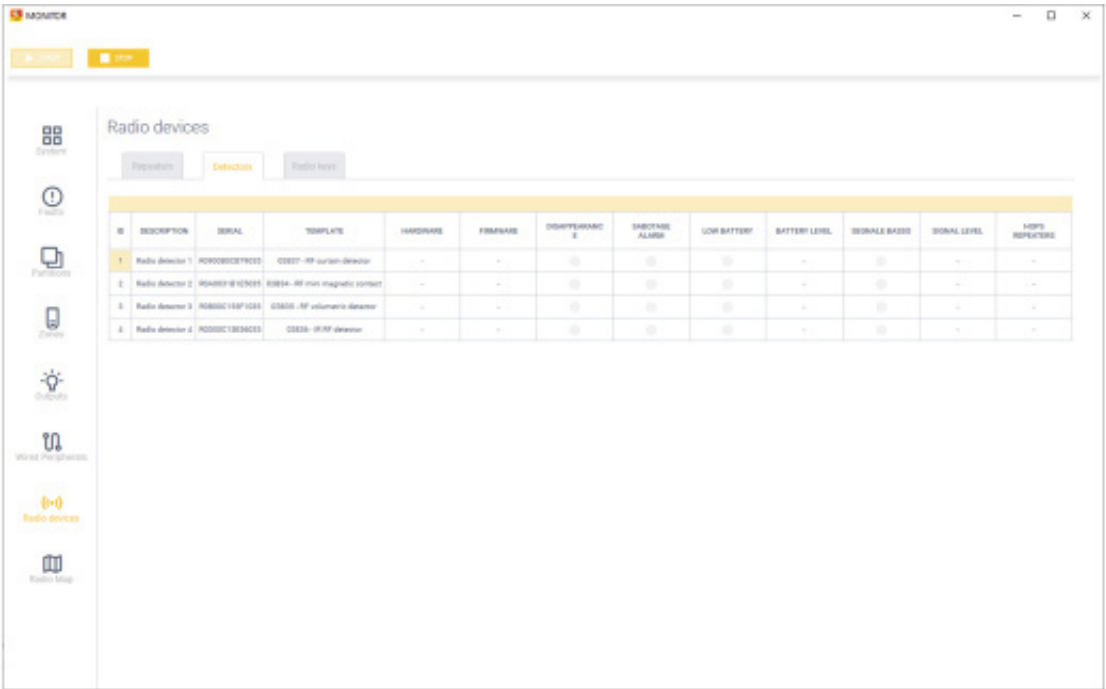
- Description
- Serial
- Template
- Hardware
- Firmware
- Disappearance
- Sabotage alarm
- Voltage
- BUS counter



The five GSM/LTE dialer icons indicate the status of the connected network and signal, the data network and VoLTE availability, the status of any outgoing call in progress, the status of any text message being sent, the status of a data exchange.

FAULTS DETAIL lists any faults related to the GSM/LTE dialer network registration and data connectivity.

Radio devices



This page displays the list of radio devices enrolled in the panel and their features.

- Description
- Serial
- Template
- Hardware
- Firmware
- Disappearance
- Sabotage alarm
- Low battery
- Battery level
- Low signal
- Signal level
- Hops repeaters

System monitor

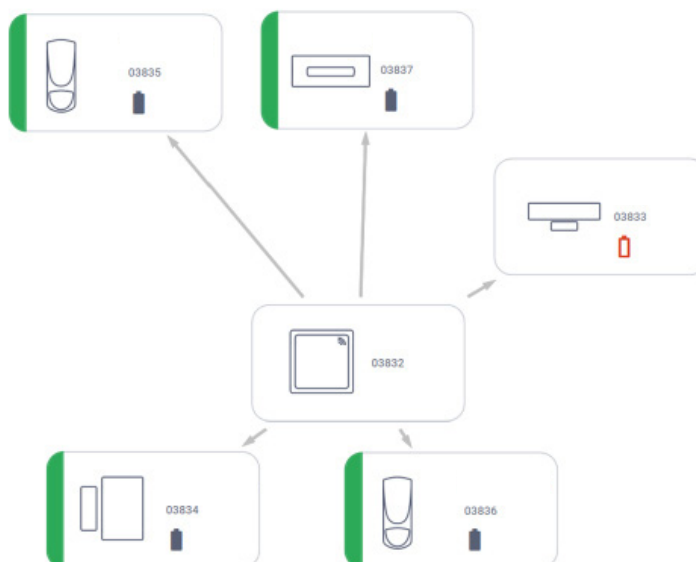
13.1 RADIO MAP

This displays a map of the radio devices configured in the project.

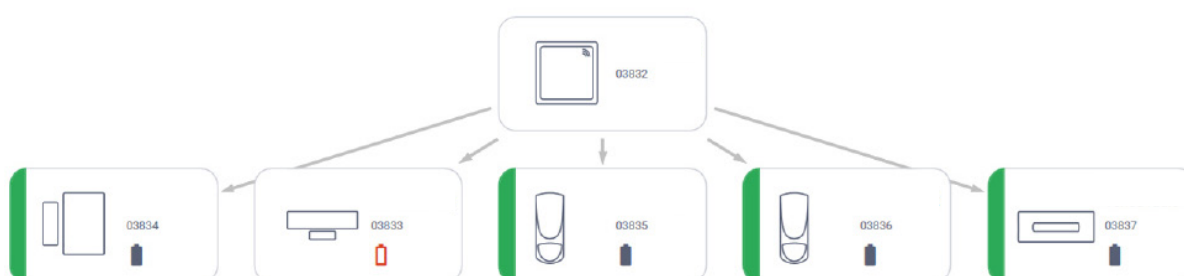
The filter bar **Tutti** **Ricevitori radio** **Ripetitori** **Sensori** serves to choose which device category to view.

• Chart view

Albero Grafo 1:1 Fill Zoom: 134.43% Layout: **Ricarica** Tutti Ricevitori radio Ripetitori Sensori



• Tree view



The battery charge level is shown for each radio device.



The left part of each device icon shows the radio signal level (e.g. green for the Curtain radio detector) and changes colour depending according to the signal detected.

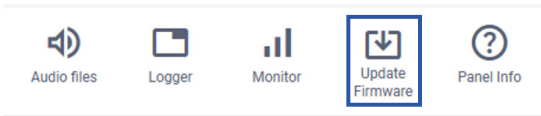


APPENDIX - Updating the panel and device firmware

APPENDIX - Updating the panel and device firmware

There is a wizard in the software to update all system devices with the latest firmware. The wizard can also verify the firmware versions of system devices in relation to an available update package.

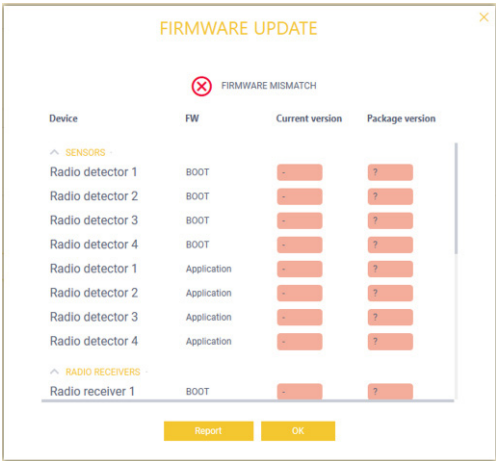
The firmware update (and verification) management wizard is activated with the “Update Firmware” key in the software.



Select a firmware package with a .dat extension from the first window in the wizard.
This file type will normally contain firmware for all BUS and radio devices in the system.



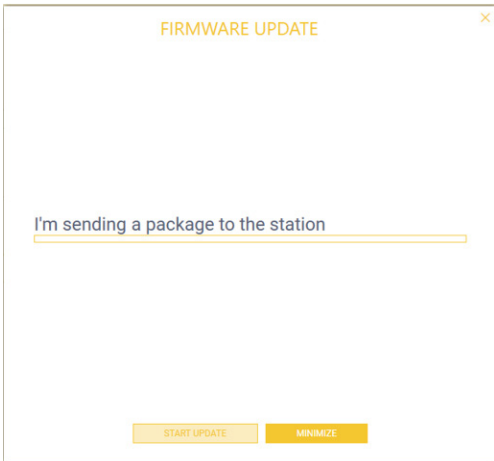
Select “VERIFY” to compare the firmware versions of the devices in the system with those in the .dat file. The report will show if the versions are the same or if there are any devices with a different version.



- NOTES:
- a) The wizard highlights any version mismatches. It is possible that a newly produced device is being compared with an older package; in this case, the current device version is MORE RECENT than the package version.
 - b) The firmware for each device may consist of multiple firmware sub-parts, so the wizard may show version mismatches for each of the sub-parts (example in red in the image above right).
 - c) If the panel cannot communicate with a system device (BUS or RADIO peripheral disappeared or removed), the wizard will still show a version mismatch to indicate that it has failed to make a comparison.
 - d) If you are sure that you have the latest package and there are version mismatches, it is always advisable to perform the upgrade procedure; the end result should be like the report in the image above left (unless point c above occurs).

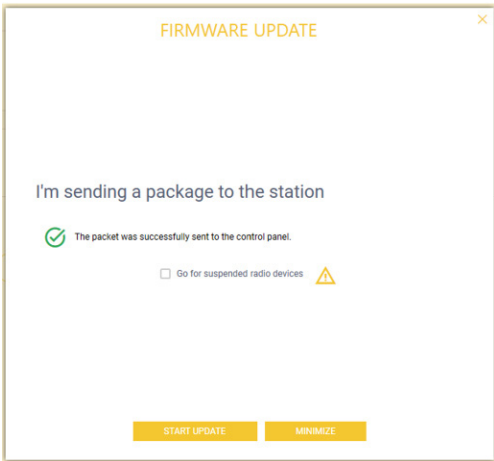
Select "UPDATE" to update the system devices with the firmware from the .dat package; the procedure flow is as follows:

1. The package is sent to the panel



NOTE: The software will display an error message if a user is logged into a keyboard or if the panel is armed.

2. The update procedure starts

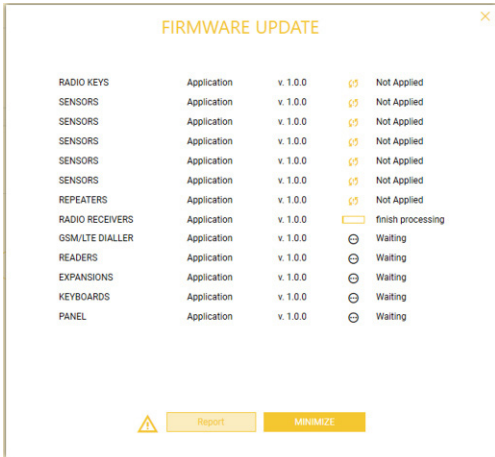


NOTES:

- a) When the panel is configured with regulation grade 2 or grade 3, the software will display an error message if a user has not previously authorised the system update via the PERMISSIONS-USER menu on the keyboard.
- b) If the system contains radio devices that have failed a previous upgrade attempt and/or the radio devices are in the "suspended" state as indicated by a flashing red LED (typically because the battery is too low and must be replaced before repeating the procedure), select the "Force suspended radio devices option.

3. Check the update procedure progress on the SW.

During this step, the current update status is also shown on the keyboard display and the blue LED on the panel.



APPENDIX - Updating the panel and device firmware

NOTES:

- a) The list of current update tasks may show firmware in devices with different hardware versions (e.g. different radio sensor types or wired devices with different hardware over time).
- b) If the system has NO devices of a certain type (e.g. no REPEATERS or no READERS), the panel and software will display the update status as "Not applied" (in which case the update procedure may be shorter).
Other possible states include: "Sent", "Processing", "Waiting", "Updated" (for the panel only), "Failed" (only if there are BUS or RADIO communication problems).

Updating radio keys (remote controls)

If the system has remote controls, their firmware is updated at the beginning of the procedure, in which case the installer must manually press a key on each remote control (as prompted by an indication on the keyboard display) within 2 and a half minutes of starting the procedure. The remote control LED will start flashing green to acknowledge the update; this step may be requested a second time, in which case it will be indicated by the keyboards in the same way. During this procedure, the software will continue to display "Processing" as the firmware update status of the remote controls, after which the panel and software will update the various devices independently, and the software will display feedback on the status of the subsequent steps.

4. At the end of this procedure, you can press the "REPORT key to CHECK the current firmware versions of the newly upgraded devices (as described above)

The panel and software will retrieve the necessary information from the BUS and RADIO devices, and will display the outcome of the update procedure. The report will show if the versions are the same or if there are any devices with a different version.

CAUTION:

The updated information may not be immediately available for radio devices; if there are mismatches, press "REPORT" again after a few tens of seconds. It may be necessary to wait up to 1 minute for systems with a large number of radio devices and/or very long distances and/or environments with high radio interference levels.

If remote controls have been updated, you may have to press the F3 and F4 keys simultaneously on each remote control involved in the procedure before pressing the REPORT key to check the current firmware version.



By-alarm Plus EN 04 2401



VIMAR

Viale Vicenza 14
36063 Marostica VI - Italy
www.vimar.com