



EN 50131-1
EN 50131-3
EN 50131-6
EN 50131-10
EN 50136-1
EN 50136-2
EN 50130-4
EN 50130-5
CEB T031



GameOver



SMARTLIVING
Anti-intrusion control panels and security systems

PROGRAMMING MANUAL

inim

This is a legally binding agreement between the authors of this software (Inim Electronics S.r.l.) and You (You means the licensee or anyone engaged by You or otherwise pertaining to You).

By installing, copying or otherwise using this software, You acknowledge that You have read, understand and agree to be bound by the terms of this agreement (EULA). If You do not agree with any of the terms or conditions of this agreement (EULA), You are not authorised to install or use this software for any purpose whatsoever.

All versions of this software are protected throughout the world by copyright and other intellectual property rights. All rights are property of Inim Electronics S.r.l.. You may not duplicate, sell, distribute or use this software save as provided under this End-User Licence Agreement, unless You obtain written consent from Inim Electronics S.r.l..

Any parties interested in using this software for non-personal purposes must contact Inim Electronics S.r.l..

This license grants the following rights: installation and use. It is allowed to install and use an unlimited number of copies of this product.

This End-User Licence Agreement hereby grants to You the right to reproduce and distribute an unlimited number of copies of this product; each copy must be in whole and accompanied by a copy of this agreement (EULA).

You may not embed this software in another software application or freeware, shareware or commercial product without first obtaining explicit consent from Inim Electronics S.r.l..

You are not permitted to reverse engineer, disassemble, decompile or modify this product or any portion thereof.

This software is Licensed as a single product; You are not permitted to separate and use any portion of it on more than one single workstation.

You are permitted to transfer this product and Your rights under this End-User Licence Agreement on a permanent basis to another person or entity.

Our rights under this agreement (EULA) will terminate immediately if You fail to comply with any of the terms and conditions contained within. If this occurs, You must destroy the Software, and all copies of all and any part of it.

By using this software, You agree to be bound by the terms of this End-User Licence Agreement.

With the exception of any explicit annotations, all rights and the copyright pertaining to the software in its entirety and its parts (including figures, photographs, animation, video, audio, music, text and code) and accompanying documentation are the exclusive property of Inim Electronics S.r.l..

This software is protected by International Copyright Laws and Agreements and must be considered in the same way as all other material which is subject to copyright laws.

Inim Electronics S.r.l. make no warranties of any kind, either statutory or otherwise in relation to this product. The software and all associated material is released without any undertakings of any kind, express or implied. You use this product at your own risk.

In no event shall the authors of this software be liable to You or to those claiming for You for any damage of any kind, whether direct or in direct (including but not limited to, damage or loss of any kind, loss of profits, business interruptions, loss or corruption of data) arising out of or in connection with the use of, or the impossibility to use, this product.

Contact www.inim.it for further details.

SmartLiving control panels, by attributing them to installers and users registered with the Inim Cloud service, can be managed through dedicated web pages and/or apps available to both the installer and the end user.

In order to allow management of the control panel via Inim Cloud an explicit request is required from the users to whom the control panel is to be associated.

End-User Licence Agreement (EULA)

Rights

Reproduction and distribution

Other rights and restrictions

Separation of components

Transfer of the Software

Licence Term

Copyright

Disclaimer of Warranties

Limits of Liability

Processing of personal data

As soon as a control panel is connected to a LAN or a GSM/LTE network, it will be available on the Inim Cloud, however, until the association is explicitly requested by a user the data exchanged are:

- purely technical (in order to allow an association to a user in the future) and do not include any personal data
- always encrypted
- free from any correlation with personal data that may already be present in the Inim Cloud

The control panel events log becomes available only after associating the control panel with the users and can be viewed chronologically from the moment of such an association.

If you do not want to manage the control panel via Inim Cloud and/or do not want to allow any type of connection to Inim Cloud in advance, simply disable the connection with the service via programming (refer to "Enablement for programming").

Table of contents

About this manual	7
0-1 Terminology	7
0-2 Graphic conventions	7
Chapter 1 Programming the control panel	8
1-1 Accessing the Installer menu	8
1-2 Programming via the SmartLeague software	9
1-3 Fast programming from the keypad (Wizard)	9
Chapter 2 The SmartLeague software	10
2-1 Using the software program	10
2-2 Creating a project layout	11
Chapter 3 Inim Cloud	13
3-1 User levels	13
3-2 Web interface	14
3-3 Control panel connection	15
3-4 Control panel registration	16
3-4-1 Control panel registration via keypad for the installer	16
Chapter 4 Programming via keypad	19
4-1 Parameters and control panel options	19
4-2 Terminals	22
4-3 Zones	23
4-4 Outputs	28
4-5 Walk test	29
4-6 Telephone	30
4-7 Events	31
4-8 Timers	37
4-9 Partitions	38
4-10 User Codes	39
4-11 Installer codes	41
4-12 Keys	42
4-13 Arming scenarios	43
4-14 Shortcuts	44
4-15 Expansions	44
4-16 Keypads	45
4-17 Readers	46
4-18 Sounders/Flashers	47
4-19 Language	47
4-20 Messages	47
4-21 Default settings	48
4-22 User functions	49
4-23 Other parameters	50
4-24 Activating outputs without authentication	53
Chapter 5 Programming via the SmartLeague software	54
5-1 Keypads	54
5-2 Proximity readers	56
5-3 Expansions	56
5-4 Sounder/flashers	57
5-5 Nexus	59
5-6 SmartLiving System	64

5-7	Partitions	67
5-8	Terminals	68
5-9	Arming scenarios.	71
5-10	Timers	72
5-11	Codes	72
5-12	Keys	73
5-13	Telephone.	74
5-14	Events	75
5-15	Voice messages.	81
5-16	Icons and shortcuts	82
5-17	SmartLAN.	83
5-18	Wireless transceiver.	86
5-19	Events log	87
Chapter 6	Monitoring the SmartLiving control panel	88
6-1	Remote keypad	88
6-2	Partitions	88
6-3	Zones	89
6-4	Timers	89
6-5	Peripherals	89
6-6	Sounders on BUS	89
6-7	Hedera wireless sounder	90
6-8	BUS isolators	90
6-9	Walk test	90
Chapter 7	Graphic map configuration	91
7-1	Parameters of the icons and objects	92
Chapter 8	Compliance with rules in force	93
Chapter 9	Errors and faults	96
9-1	Faults detected by the control panel	96
9-2	Communication BUS (I-BUS)	97
9-3	Ring Sensitivity	97
Chapter 10	IP and Internet Connectivity	98
10-1	Configuring an IP network	98
10-2	Configuring a router.	99
10-3	Remote access	99
10-4	Connection test.	100
Appendix A	Shortcuts by default	101
Appendix B	Available Icons	102
Appendix C	Voice messages.	103
Appendix D	Screw Terminals	105
Appendix E	Combination of outputs triggered by events	106
Appendix F	SIA Codes	107

ABOUT THIS MANUAL

DCMPINEOSLIVINGE **MANUAL CODE**
7.00 **VERSION**

Terminology

0-1

The main supervisory unit or any constituent parts of the SmartLiving intrusion control system.

CONTROL PANEL, SYSTEM, DEVICE

Directions as seen by the operator when directly in front of the mounted device.

LEFT, RIGHT, BEHIND, ABOVE, BELOW

A device which sends voice calls or digital reports to programmed contact numbers in the event of an alarm.

DIALER

Persons whose training, expertise and knowledge of the products and laws regarding security systems, are able to create, in accordance with the requirements of the purchaser, the most suitable solution for the protected premises.

QUALIFIED PERSONNEL

Click on a specific item on the interface (drop-down menu, options box, graphic object, etc.).

SELECT

Click-on/push a video button/key on a keypad or screen.

PRESS

Graphic conventions

0-2

Following are the graphic conventions used in this manual.

Conventions	Example	Description
Text in italics	Refer to <i>paragraph 0-2 Graphic conventions</i>	Directs you to the title of a chapter, section, paragraph, table or figure in this manual or other published reference.
<text>	# <AccountCode>	Editable field
[Uppercase letter] or [number]	[A] or [1]	Reference relating to a part of the system or video object.
Button		Keypad keys

The "Note" sections contain important information relating to the text.

Note

The "Attention" prompts indicate that total or partial disregard of the procedure could damage the device or its peripherals.

ATTENTION!

Similarly marked dialogue boxes contain recommendations and/or guidelines which the manufacturer wishes to call attention to.



Chapter 1

PROGRAMMING THE CONTROL PANEL

The options, functions and values of the SmartLiving control panel must be programmed by qualified persons only. The SmartLiving control panel is programmed at the factory with almost ready-to-go settings ("default settings") which require only minor changes during the system customization phase.

For example, all the zones, keypads and readers are assigned to (belong to) partition 1, alarm and tamper events related to partition 1 activate the relay output which is monostable set at 3 minutes (Monostable time = 3 minutes), etc.

All the parameters and programming data can be input via keypad or computer (equipped with the SmartLeague software programme) with the following limitations:

- From the keypad you cannot program:
 - Timer exceptions
 - input calibration
 - Sounder/flasher tone
 - BUS speed
 - description of Emergency Keys
 - Parameters relating to the SmartLAN board
 - Parameters relating to the Nexus GSM dialer
 - Parameters relating to the I-BUS Ivy-B
 - Programmable events
 - shortcuts on event
 - output scenarios
 - configuration of cameras
 - Configuration of graphic maps
- Via the SmartLeague software you cannot program:
 - DTMF sensitivity
 - the second Installer code
 - the Installer code PINs
 - the shortcut descriptions

The following chapter describes the programming flow of the system data in the order it appears in the Installer menu on the keypad. The description of both programming methods (from keypad; via PC) are provided.

Accessing the Installer menu

1-1

If you wish to program the system via the installer menu from a keypad and thus upload/download the control panel parameters, you must:

1. Disarm all the control panel partitions.
2. Type-in a valid PIN (installer code) on the keypad then press .

If an Alien keypad is being used, access the "Settings" section by tapping the  button, type in the user code and access the "Installer section", then enter the Installer code.

The PIN is "9999" at default.
3. The system will allow access to installer menu only after the entry of a valid PIN.

Once access to the installer menu is achieved, the system will:

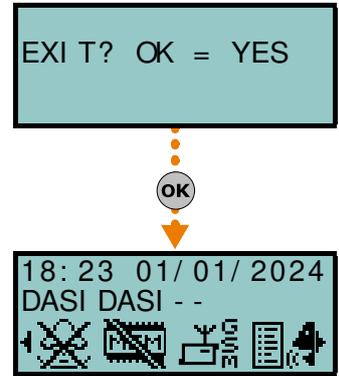
- All the system keypads, except for the one the installer is working on, will be locked.

- Broadcast the "PROGRAMMING" message to all the keypads.
- Force all the system keypads to standby status.
- Bring the call queue and events log to a temporary standstill, thus there will be no events saved to the log, no outputs activated and no outgoing calls.

To exit the installer menu, press **Esc** (o **C**) and when the system asks: "EXIT? OK = YES", press **OK**.

Once you exit the installer menu, the control panel will:

- Reset all functions and apply all the newly changed programming data.
- Restore the I-BUS, reprogramme and make all the peripherals fully operational.
- Restore the call queue, and events log to normal operations.



Programming via the SmartLeague software

1-2

Certain parameters (for example, relating to zones and outputs) can be programmed only after the project layout of the system has been completed (refer to *paragraph 2-2 Creating a project layout*).

1. Go to the "Recent solutions" section and either create a new solution or open an existing solution, or import the programming data of a real control panel by clicking on the key to upload the control panel data.
2. Select the device you wish to configure from the tree menu on the left.
3. Set the parameters in the "Parameters settings" template on the right.
4. To download the data to the control panel, click-on the key.

The limitations described in *paragraph 2-2 Creating a project layout* apply during the uploading and downloading phases.

Note

This manual is limited solely to instructions regarding navigation through the software and where to find the various parameters. For full instructions regarding the complete programming process refer to the SmartLeague Installation and Configuration manual, supplied with the software.

Fast programming from the keypad (Wizard)

1-3

SmartLiving provides you (the installer) with a step-by-step guide to fast system programming via the Installer menu.

The guide consists of a series of questions you (the installer) must answer by means of the keypad keys. The questions must be answered one at a time in order to programme the required settings. This programming process does not cover all the control panel parameters, however, it allows you to program the basic parameters and functions which permit the system to operate at a basic level.

Starting the Wizard (fast programming process) does not delete any previous programming, however, it allows you to overwrite it where necessary.

1. Access the "Wizard" section.

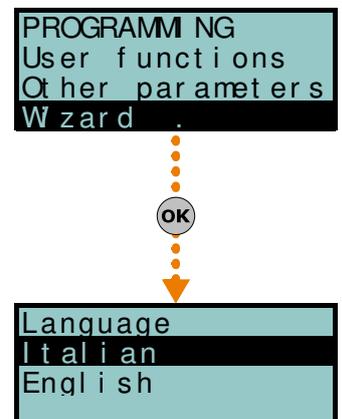
Type in code (Installer) **OK**, PROGRAMMING Wizard **OK**.

2. Answer the questions asked using keys and to select the field you wish to change and the number keys (**1** .., etc.) to edit the number.

or

Use keys and to increase or decrease the number.

3. Press **OK** to save and continue.



Chapter 2

THE SMARTLEAGUE SOFTWARE

The SmartLeague software program allows the installer to prepare the majority of the parameters/settings without actually being connected to the control panel.

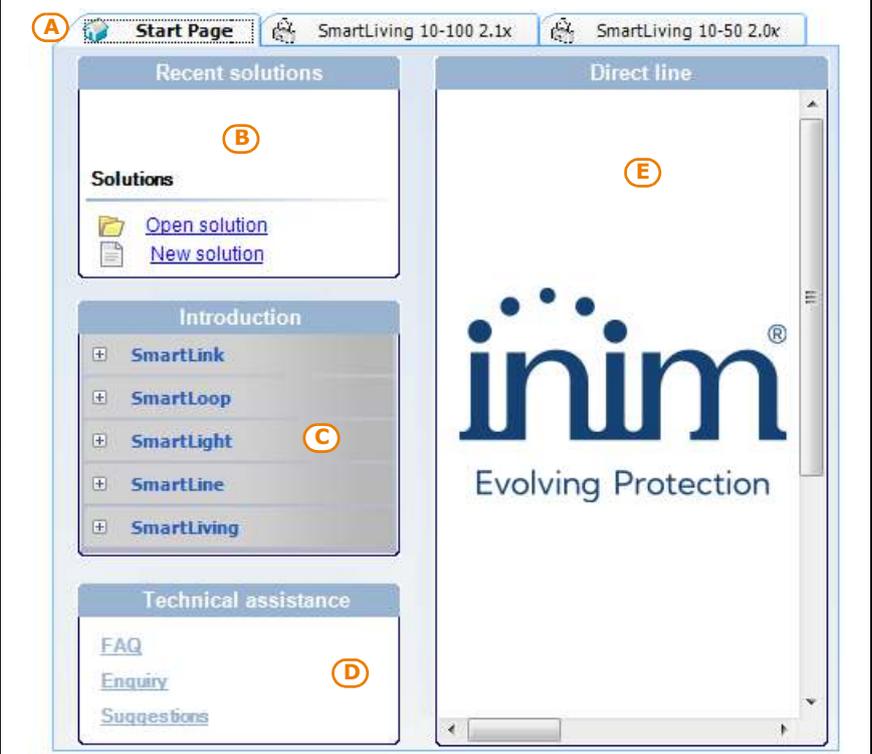
However, connection is required during the upload and download operations. The type of connection depends on the method used for read/write operations to and from the control panel:

- RS232 serial port of the PC
- LAN (combined with the use of a SmartLAN/SI or SmartLAN/G board)
- Modem
- Inim Cloud

The programming parameters of an installation constitute the "solution". The solution can be saved to the memory of the SmartLeague software programme, either for future use or as a "model" for other installations.

The homepage of the SmartLeague software program is common to all the programmable devices and is always active, even during the programming session (in the form of a template):

Table 2-1: SmartLeague - homepage

A	The menu bar, application icons and programming accessories.	
B	List of recent solutions - which will allow you create new solutions or open existing solutions	
C	Documentation installed on the computer.	
D	Help area: via the Internet, it is possible to consult FAQ page, make enquiries and suggestions via e-mail.	
E	Access to the area reserved for registered users of the INIM website. After typing in a Username and Password, you can access the updated versions of the software programme, firmware, technical documentation and service.	

Using the software program

2-1

Each project, from the most uncomplicated to the most complex of systems, is represented by a solution, which contains the programming parameters and installation structure.

A solution is dedicated to a specific type of apparatus and has its own programming interface. You can work on several solutions simultaneously, even if they involve different types of apparatus. Each solution has a template, located next to the

“Homepage”, which can be viewed at all times. In this way it is possible to compare different solutions and even keep two solutions open, one real and one for test purposes (in order to verify the effects of programming).

When a solution opens, the SmartLeague software program presents the following interface:

Table 2-2: SmartLeague - solutions

A	The freshly opened template remains in the forefront whilst the other open template and the Homepage remain in the background.	
B	Installation tree structure.	
C	Project Template where you can select the system peripherals (keypads, readers, expansions, sounder/flashers) and drag and drop them to the tree structure.	
D	Programming template of the component to be programmed (selected from the tree structure).	
E	Keys for data transfer	

A solution can be created or changed even without being connected to the apparatus. For example, without moving from your office, you can plan the layout of an installation or program the options/parameters and download the settings to the system at a later time.

In this case, you must program:

- the Installer PIN - via the “SmartLiving System” from the tree menu on the left. The PIN must be entered in the “Parameters settings - Installer code” section on the right.
- the Type of connection - via the “Settings – Application data” section (if you intend using the serial port or a LAN or GPRS connection); or press the key (if you intend using the SmartModem100).

For the specifications regarding the above-mentioned connections, refer to *paragraph 9-3 Ring Sensitivity*, the *paragraph 5-5-5 GPRS connection* or to the SmartModem100 Installation Manual.

Creating a project layout 2-2

The project layout section, in the SmartLeague software programme, allows you to configure the system (i.e. select the type and number of peripherals present).

You can either create a new solution or change an existing one. The existing solution can be either a project layout created through the SmartLeague application or a solution imported directly from a real system.

1. If you wish to create a new system, go to the “Recent Solutions” section and select “New solution”, then select the type of control panel and firmware version. If you wish to modify an existing system, go to the “Recent solutions” section and select “Open solution”.
or
import the data from a real control panel by clicking on the key, which will upload the control panel data.
2. Select the type of peripheral you wish to configure from the “Project” template, and drag and drop it to the part of the tree menu concerned.
or
Double-click on the peripheral to add it to the configuration.
To remove a component from the structure, select it and press CANC on the computer keyboard.
3. To download the data to the control panel, click-on the key. Downloading operations will:
 - Block all system keypads.
 - Broadcast the “PROGRAMMING” message to all the keypads.
 - Force all the system keypads to standby status.
 - Bring the call queue and events log to a temporary standstill, thus there will be no events saved to the log, no outputs activated and no outgoing calls.

PROGRAMMING
VI A COMPUTER

When the downloading phase terminates, the control panel will complete the operations it usually carries out on exiting the Installer menu.

During the read and write phases, ensure that the control panel partitions are disarmed. This condition is not necessary when you are viewing the events log.

Note

The SmartLeague software programme provides data transfer buttons ( and ) for read/write operations relating to all programming in progress, these buttons are located under the Menu bar. It also provides buttons for read/write operations relating to the project layout or open programming session, these buttons are located in the top left-hand corner of the page concerned.

4. Additionally, the SmartLeague software program provides a button  that allows you to create a file which interfaces with supervisory software such as Inim's SmartLook or WinMag (ask your dealer for details).

Chapter 3

INIM CLOUD



The INIM Electronics Cloud service provides SmartLiving users with a further mode of intrusion panel management via Internet.

The connection of control panels to the Cloud service is achieved via a web interface without any need to configure the network on which the control panel is installed. In particular, it is not necessary to program a router to perform port-forwarding and the like in order to reach the control panel.

Intervention with regard programming relating to network operations is not required on SmartLAN cards, since these cards are programmed by default with DHCP enabled (option to automatically assign an IP address to the devices on the network).

To use the Cloud Service as an installer, you must create your own account at www.inimcloud.com and follow the guided registration procedure.

After correct registration, the installer will receive a confirmation email and an email with an "Installer ID" (Cloud installer 8 digit code), by means of which the installer can carry out operations that will enable Cloud access on already installed systems.

Once logged in, the installer will have access to a customized web interface which has all the tools to:

- register new control panels
- associate or cancel the customer users with the control panels
- supervise the registered control panels
- manage the installer profile

User levels

3-1

The Inim Cloud service provides three different user levels, relating to a single control panel. The ratings may be different in your profile, depending on the control panel:

- **Supervisor**, corresponds to the installer.
- **Admin**, corresponds to the first user who registers the control panel to their cloud profile and who can, through a web interface, supervise the system. And who, by accessing their profile, can delete the control panel from their own account or that of other users. Furthermore, can pass the title of "Admin" to another user.
- **User**, is a user who has registered the control panel to their cloud profile and who can, through a web interface, supervise the system or delete the control panel from their own account.

The "owner" attribute allows a user to delete a control panel from the supervisor's account. It can be assigned both the installer and the end user by the installer during registration of the control panel to cloud.

Therefore, if "owner" is the user, they can enable/disable other users and the installer who supervises the system.

If, instead, "owner" is the installer, they can enable/disable themselves and the "Admin" user.

If an installer "owner" disconnects a control panel, disabling themselves, it will no longer be accessible in the cloud for each user.

OWNERSHIP

Note

Web interface

3-2

Following is the description of the home page; the presence of each of the following elements described depends on the activated functions and the page you are accessing:

Table 3-1: Inim Cloud - home page

A	Buttons for access to the supervision sections	
B	Buttons for quick viewing	
C	Buttons for the management of the supervisor user profile	
D	Text section relating to the button pressed	

Always present in the upper right-hand corner are the buttons for viewing and editing the profile of the user and the control panels registered to the Cloud.

Editing can be done after data has been unlocked by clicking on the respective icon .

Buttons for quick viewing 3-2-1

The Quick View (Table 3-1: Inim Cloud - home page, B) buttons are always present and show (in overlay) the number of ongoing events or for events which viewing has not been confirmed:

- The button opens a window listing the last 4 fault events.
- The button opens a window listing the last 4 alarm or tamper events.
- The button opens a window listing the last 4 control panel and cloud events.
- The button opens a window with a list of the first 4 upcoming maintenance events scheduled in the "Calendar" section. If required this button shows (overlaid) the number of the events that are upcoming on the day in which you consult the cloud.
- The button opens a window listing the control panels registered by the installer to the cloud but not yet assigned to any account. If required this button shows (overlaid) the number of "new" control panels.

Sections for the supervision 3-2-2

The "home page" section is divided in two parts:

- The upper part, with four sections showing the number of events in progress or for which viewing has not been confirmed, grouped in categories:
 - Alarm and tamper events
 - Fault events
 - Generic events of the control panels and cloud

HOME



- Maintenance events
- The lower part, with a list of all the events of all the registered control panels and the cloud.
By clicking on an event you can view more details.
The list can be filtered in accordance with the category of events by clicking on one of the 4 boxes in the upper part.

The "New Installations" sections shows the list of control panels registered by the installer to the cloud service and not yet associated with any customer (*paragraph 3-4 Control panel registration*).

The "Customers" section allows you to manage customers (users) that have been assigned to the registered control panels and also to view the systems.

It displays a list of customers and the respective control panels for each of these.

The list can be filtered in accordance with the category of events by clicking on one of the buttons at the top of the list (  ). The  button allows you to add a new customer by entering the respective data.

It is possible to select a single customer or a single system from the list.

Selecting an customer opens a section with a break-down on the assigned control panel. This section allows you to:

- change the personal details of the customer
- request or transfer the ownership of the control panel
- set the password request (OTP) during user registration
- unregister yourself (as supervisor) or the "Admin" user from the control panel

At the bottom of this section, the  button allows you to add a new control panel.

Selecting a single control panel allows you to view an interface identical to that of the user.

This section allows you to view all the system components but does not allow you to carry out any activations.

The "Calendar" section allows you to manage events such as reminder events ("Maintenance").

The section shows a calendar, viewable in different modes (daily, weekly, monthly, etc.) from which you can select a date/time.

Once selected, a section activates on the right for the programming of the maintenance event schedule and the respective parameters.

Activating the "Notify" option allows you to set the interval that must pass before notification of the event is sent to the addressees (set in the "Notifications section").

The "Notifications" section allows you to set up the recipients of the event notifications relating to the registered control panels.

The events are grouped into 4 categories:

- tamper
- faults
- programming
- maintenance

There is a list of notification recipients for each type of event and it is possible to add others via the  button by specifying:

- name
- phone number for the voice call
- phone number for the SMS message
- email address
- enable the "push" notification for Inim Home users

NEW INSTALLATIONS



CUSTOMERS



Note

CALENDAR



NOTIFICATIONS



Control panel connection

3-3

The connection to the Inim Cloud service is available for all control panels with a firmware version not lower than 6.03.

In order to connect the control panel you must have one of the following devices:

- SmartLAN/G, with a firmware version not lower than 6.08
- SmartLAN/SI, with a firmware version not lower than 5.00
- Nexus/G, with a firmware version not lower than 4.00
- Nexus/4G

If the connection to the Cloud is achieved via Nexus, the use of this will be exclusively for communication with the Cloud and therefore it cannot perform any other operations which are normally available (voice calls, send SMS, respond to commands sent via SMS).

Note

In order to assist the installer when programming a SmartLiving control panel registered to the Inim Cloud service, the SmartLeague software provides an option that, if enabled, performs a preset of some of the control panel parameters that would otherwise have to be programmed individually.

"CLOUD MODE"

Via PC

Start the SmartLeague solution for the control panel, select "SmartLiving System" from the tree menu on the left, then go to the "Programming" template on the right. There you will find the "Cloud Mode" option.

If activated, the software will perform the following default programming:

- The "Inim Cloud" will be assigned to telephone number 12 which will no longer be editable.
- A group of events of various types will be setup and must be communicated to the Cloud when they occur, these events will no longer be editable

Control panel registration

3-4

The registration of a control panel is an operation that allows its accessibility to all Inim Cloud service users.

Therefore, it is necessary that the installer carries out the initial registration, so that the users can add the registered control panel afterwards to their own accounts.

Control panel registration via keypad for the installer

3-4-1

1. Connect the control panel to the Internet.
2. Go to the "Cloud Registrat." section:

Via Keypad

Type in code (Installer) **OK**, PROGRAMMING User functions **OK**, Activations **OK**, Cloud enrollment.

Via Alien keypad

Go to the "Settings" section by pressing the  button, enter the user code and then access the "Installer" section, enter the installer code to access the "User Functions – Activations – Cloud enrollment".

3. Enter the 8-digit installer ID number.
This number is available:
 - in one of the confirmation emails received during registration to the Cloud as an installer
 - in the installer personal profile section of inimcloud.com
 - in the "Programming" section of the Inim Tech Security App
4. The control panel will ask you to specify the owner using the "Inst. Ownership" option
If the option is selected, the control panel is the ownership of the installer, otherwise it is the ownership of the "Admin" user.
5. After setting the above-mentioned option and pressing "OK", the control panel will carry out the registration to Cloud and the keypad will display the string "WAIT".

If the control panel date/time differs by more than 15 minutes from the exact date/time, the registration process may result negative.

Note

6. The keypad will show the result of the procedure by displaying one of the following messages:
 - "Account created!": the control panel has been successfully registered to Cloud
 - "Communicat.Error": generic communication error.
The possible causes may be:
 - no Internet connection
 - date of manufacture of the control panel is earlier than dd/mm/yyyy

- date/time of control panel different, ahead or behind the exact date/time by more than 15 minutes
- "Already enrolled": the control panel is already registered to Cloud
- "Bad ID": the entered Installer ID code is wrong
- "Panel notEnabled": the control panel cannot be registered to Cloud

Registration of the control panel via web and user keypad

3-4-2

The following procedure requires that the user already has a Cloud account and that the control panel to be registered has been previously registered for the service by an installer.

1. Access the service through their user account.
2. Clicking on the button that manages your profile, accesses a page where you can set the parameters of your account and those of registered control panels. In the lower section, below the list of control panels, you have the "New Inim system" section.
3. The **Add** button will allow you start the registration process. The Cloud service will send an OTP (One Time Password) number consisting of 6 digits to the user. This number is also made available in the case of first access to the Cloud service as a user, following an invitation by the installer.



This number has a limited time duration of 15 minutes.

Note

4. Activate the "Cloud enrollment" option:

Via Keypad

Type in code (User) , Activations , Cloud enrollment.

Via Alien keypad

Access the "Menu" section by pressing , then "Activations", and then the "Cloud enrollment" option.

5. Enter the OTP password and wait for the outcome of the registration. The outcome of the procedure will be shown with one of the following messages:
 - "Account created!": the control panel has been successfully registered to Cloud
 - "Communicat.Error": generic communication error. The possible causes may be:
 - no Internet connection
 - date of manufacture of the control panel is earlier than dd/mm/yyyy
 - date/time of control panel different, ahead or behind the exact date/time by more than 15 minutes
 - "Already enrolled": the control panel is already registered to Cloud
 - "Bad/expired OTP": the entered password is incorrect or expired
 - "Panel notEnabled": the control panel cannot be registered to Cloud

Control panel registration via Inim Home App

3-4-3

The following procedure requires that the user already has a Cloud account and that the control panel to be registered has been previously registered for the service by an installer.



MAIN USER

1. Via the Inim Home App the main user receives notification of the ongoing registration carried out by the installer.
2. The user must accept or reject the request within 60 minutes:
 - If the user refuses, the installer can re-propose the invite by accessing the specific section of the installer App.
 - If the user ignores the notification, after the set time has elapsed, the installer can send a new notification.
 - If the user accepts, a page will open on which the user will be asked to enter a control panel user code.
3. The App verifies the entered user code. If the code PIN is at default (from "0001" to "0050") the App will reject it and will repeat the PIN entry request.
4. If the PIN code is valid, the Cloud will forward a request to the control panel.

- If the user is already set in programming by the installer (PIN code and partitions to operate on), the user has immediate access to the operations on the control panel.
- If the PIN is valid but not associated with any user via programming, the system will assign the characteristics of the first available user profile to the user.

From this moment on, the installer will lose the right to invite other users.

At the same time, the newly enrolled user inherits the ability to invite other users for association with the control panel.

The operation can be carried out from the section of the Inim Home App reachable via the "Settings > Configuration" menu, by sharing one of the accessible control panels, and using the e-mail addresses of the accounts of the users to be invited.



1. The main user must make a request to associate a secondary user.
2. Via the Inim Home App the secondary user receives notification of the ongoing registration carried out by the Main User.
3. The secondary user must accept or reject the request within a maximum of 60 minutes:
 - If the secondary user refuses the invite, the main user can propose it again.
 - If the secondary user ignores the invite, after 60 minutes the main user can send them a new request.
 - If the secondary user accepts the invite, the procedure described above for the main user is repeated.
4. The App verifies the entered user code.
If the code PIN is at default (from "0001" to "0050") the App will reject it and will repeat the PIN entry request.
5. If the PIN code is valid, the Cloud will forward a request to the control panel.
 - If the user is already set in programming by the installer (PIN code and partitions to operate on), the user has immediate access to the operations on the control panel.
 - If the PIN is valid but not associated with any user via programming, the system will assign the characteristics of the first available user profile to the user.

SECONDARY USERS

Secondary users do not have the ability to invite additional users.

Chapter 4

PROGRAMMING VIA KEYPAD

Parameters and control panel options 4-1

Table 4-1: Control panel parameters

Parameter	If enabled	If disabled
Dial tone check	The control panel will engage the telephone line and check for the "dial tone", if present, the control panel will start dialing.	The control panel will engage the telephone line, wait two seconds then will start dialing (whether the dial tone is present or not).
Pulse dialing	The control panel will dial using pulse tone.	The control panel will dial using touch tone (DTMF).
DTMF withoutCode	Allows access to the User Menu over-the-phone (during voice calls from the control panel) in accordance with the parameters and enablements of the last user code on the control panel (code 30, 50 or 100).	Allows access to the User Menu over-the-phone during voice calls from the control panel, only after entry of a valid user-code PIN by the recipient.
Line down signal	If a "Tel.Line down" event occurs, the control panel will flash the respective icon  on the keypad displays.	The control panel will detect the "Tel.Line down" event, but it will not be revealed on the keypad displays.
Double call	The control panel will override the answerphone function.	
Call allVoxNums	If several voice calls - generated by the same event - are waiting in the outgoing call queue, the control panel will attempt to call all the expected numbers.	If several voice calls - generated by the same event - are waiting in the outgoing Call Queue, the control panel will send voice calls until just one ends successfully. Any other voice calls relating to the event in question will be cleared (deleted) automatically from the queue.
Call all TLVNums	The same as "Call all VOXNums" but valid for Alarm Receiving Centres.	
RefreshMnstblOut	Each event that triggers an already-activated monostable output will refresh (take back to zero) the programmed Monostable time.	Each event that triggers an already-activated monostable output will not refresh (take back to zero) the programmed Monostable time.
Num15 ForTeleserv	Telephone number 15 in the phonebook is reserved for Teleservice (maintenance over-the-phone). If a user makes a request for Teleservice, the control panel will contact the user's number. Note If you wish the control panel to call an installer company number which uses an INIM modem, you must set "None" in the Telephone Number 15 Type field.	Telephone number 15 in the phonebook can be dedicated to either voice or teleservice.
Install.callback	The control panel will enable the Teleservice function if: <ol style="list-style-type: none"> the installer calls the control panel the control panel detects the ring, picks up, recognizes the installer code and hangs up immediately the control panel calls the Teleservice number and allows access to the system 	
ReaderBuzzer OFF	No reader buzzers will emit audible signals during running entry time, exit time, output time or pre-arm time.	
Keypad lockout	If a wrong code is typed-in at a keypad more than 5 times in succession, the keypad will lock for 10 minutes and show the icon:  Note If you reset the control panel or access programming while the keypad-lockout time is running, it will refresh to zero and start again.	
View open zones	The keypad will show the descriptions of any open zones (zones which are not in standby status) when the partitions disarm. Any auto-bypassable zones will be shown in negative.	

Table 4-1: Control panel parameters

Parameter	If enabled	If disabled
OpenZonesArmLock	The control panel will not arm the partition if it detects any open zones (zones which are not in standby status). If there are zones with the "Auto-bypassable" or "No-Unbypassable" attribute amongst the open-zones (refer to <i>paragraph 4-3 Zones</i>), they will be shown on the keypad as "Not ready". If the user goes ahead with the arming operation, these zones will be bypassed automatically and the partition will arm.	
DTMF sensitivity	The sensitivity of incoming DTMF tones is increased.	
BypassAlsoTamper	If a zone is bypassed (disabled), it will also be unable to generate terminal tamper.	If a zone is bypassed (disabled), it will be able to generate terminal tamper.
BypassVoiceCheck	The control panel will start the voice message 5 seconds after dialing the respective contact number.	The control panel will not start the voice message until it recognizes a voice at the other end of the line.
Confirm with *	The control panel will consider the voice call successful when the call recipient presses "*" on their telephone keypad.	The control panel will consider the voice call successful as soon as it starts the voice message.
NoUserTamp.reset	No user will be allowed to delete of the following events: <ul style="list-style-type: none"> terminal tamper control panel open-tamper control panel dislodgement-tamper peripheral tamper peripheral loss false key 	
Encrypt data	The encryption of data over the Ethernet network will be enabled only for SmartLAN/SI communications. In this case, it is necessary to enable data encryption also when programming the SmartLAN/SI. This programming process is possible only via the SmartLeague software programme.	
Instant restoral	The restoral of the magnetic reed sensor in Air2-MC300 and Air2-MC200 wireless detectors will be signaled instantly.	Reset of the magnetic reed sensor in wireless detectors will be signalled with a delay of up to 10 seconds (maximum).
Teleserv. hidden	The  symbol will not be shown on the keypad display.	If Teleservice is enabled, the  symbol will be shown on the keypad display.
LockInstall.Code	After hard reset (refer to <i>paragraph 4-21 Default settings</i>), all the control panel parameters with the exception of the installer PIN will reset to the factory default settings.	After hard reset (refer to), all the control panel parameters including the installer PIN will reset to the factory default settings (installer PIN default is 9999).
50131ReaderLedOFF	If there are no keys present at the reader, the LEDs of nBy readers will be Off. If a key is waved across the reader, the status will be indicated on the LEDs for 30 seconds before switching Off again. During this 30 second phase, the user can hold the key in the vicinity of the reader and select the desired shortcut indicated by LEDs.	The reader LEDs indicate the related status.
50131StatHidden	The status of the partitions will be hidden. If a valid code is entered at a keypad, the real-time status will be indicated on the keypad concerned for 30 seconds. If the partitions are armed, the status of the system will be hidden from non-authorized users. <ul style="list-style-type: none"> Red keypad LED Off Yellow keypad LED Off Green keypad LED On solid Status icons not present Alarm and Tamper memory hidden If the same event occurs more than five times when the partitions are armed, the event in question will not be signaled further by the control panel. This is due to the fact that each event has a counter which, during armed status, increases by 1 each time it occurs; only when all the partitions disarm will the counter reset. If the partitions are DISARMED: <ul style="list-style-type: none"> the LEDs function normally status icons are present alarm and tamper memories are visible 	The keypad will show the real-time status of the system at all times, regardless of the status of its partitions.
50131IconsHidden	If partitions are armed, the status icons will not be shown on the second line on the keypad, thus non-authorized users will be unable to view the respective conditions on the system. If a valid code is entered at a keypad, the status of the icons will be shown for 30 seconds. The keypad will show the real-time status of the icons when all the keypad partitions are disarmed.	The keypad will show the real-time status of the icons at all times, regardless of the status of its partitions.
50131AlarDelayed	If an instant-zone alarm occurs on a partition while entry time is running, the associated actions (calls, output activation, save to log, etc.) will not be generated until 30 seconds after the expiry of the entry time. If the partition (or partitions) are disarmed during this period, the associated actions will not be generated, however, the keypads will indicate the violation of the instant zone.	If an instant-zone alarm occurs on a partition while entry time is running, the associated actions (calls, output activation, save to log, etc.) will be activated instantly.

Table 4-1: Control panel parameters

Parameter	If enabled	If disabled
50131WarnLedMem	If the control panel detects a fault, the yellow LED on the keypads will go On and will remain On even after the fault clears. To switch the yellow LED Off, clear all activating causes and reset the partition.	If the control panel detects a fault, the yellow LED on the keypads will go On and will go Off automatically when the fault clears.
DayLightSav.time	The control panel clock will go back automatically one hour at 03:00 last Sunday in October, and it will go forwards automatically one hour at 02:00 last Sunday in March.	No automatic clock forward/back operations.
NoStrings SiaProt	The descriptive strings will not be sent in SIA reporting format.	The descriptive strings will be sent in SIA reporting format.
Call all SIA_IP	If several SIA-IP calls - generated by the same event - are waiting in the outgoing call queue, the control panel will attempt to call all the specified numbers.	If several SIA-IP calls - generated by the same event - are waiting in the outgoing Call Queue, the control panel will send voice calls until just one ends successfully.
CONT-IDInversion	Partition arming events using CONTACT-ID reporting format will send the "New event/Event activation" code when the partition is armed and the "Event ended/Event restore" when the partition is disarmed.	Partition arming events using CONTACT-ID reporting format will send the "New event/Event activation" code when the partition is disarmed and the "Event ended/Event restore" when the partition is armed.
Dust event enab.	Enables management of the "Detector dusty" event. The "Output fault" and "Detector dusty" events share the same actions. Therefore, if either of these events occur, the system will send the calls and activate the outputs associated with the "Output fault" event. The events log provides the proper distinction between these two events: <ul style="list-style-type: none"> in the event of an "Output fault", the system will provide the description of the output in fault status in the event of an "Detector dusty", the system will provide the description of the detector that generated the event 	The control panel cannot detect "Detector dusty" status. In the event of an "Output fault", the system will function normally.
Maintenance	You can start the maintenance session from the keypad without opening the control panel or moving the respective jumper. After exiting the Installer menu, you can operate on the system in the same way as when the control panel is placed in maintenance mode by means of the jumper. In order to place the control panel in "RUN" mode, this option must be disabled.	You can also put the control panel in maintenance mode by means of the jumper.
Show scenario	The left side of the second line on the keypad displays shows the description of the active scenario.	The left side of the second line on the keypad displays shows letters relating to the armed/unarmed status of the partitions which the keypad controls.
Tamper siren	The control panel will generate a "Sound.flash.Tamp" event if the passive cone is disconnected from the relay (wire cutting).	
Squawk on arming	This option activates the sounder for a brief period during partition stay/away arming and disarming operations in order to indicate that these operations have been executed successfully.	
50131, Grade 3	The control panel respects Grade 3 EN50131: <ul style="list-style-type: none"> only the installer code can be used to delete fault memories the readers lock for 10 minutes after 5 consecutive attempts to use a false key the keypads lock for 10 minutes after 5 consecutive attempts to key in a false code (valid only when the "Lock keypad" option is enabled) bypassed zones are automatically unbypassed when the system disarms in the presence of ongoing faults and lost peripherals, arming operations will require installer code entry <p>Note</p> <p>In order to comply completely with Grade 3 of Normative 50131, also the other options relative to Grade 2 must be activated (refer to <i>Chapter 8 - Compliance with rules in force</i>).</p>	
Alarm on keypads	All the keypads will emit an audible signal in the event of an alarm or tamper on any of the partitions they are associated with.	In the event of an alarm or tamper the keypads will emit an audible signal.
SingleCallEachEv	At the occurrence of each event, the sequence of phone calls programmed for that specific event stops after the first successful call. Note Any option relating to sending calls to all numbers have the priority over of this option.	Each event generates all the calls set by programming.
Disab.GPRS fault	The control panel will not signal GPRS connection faults or problems.	Each fault or problem with the GPRS service will be signalled.
Disab.Tel.Disarm	The control panel will not carry out the calls programmed for disarm events when there is no active alarm or alarm memory present.	The control panel will carry out the calls programmed for disarm events.
NoStrings SIA-IP	Calls to SIA-IP type numbers will be sent without being combined with description strings (e.g. partition, zone, etc.).	Calls to SIA-IP type numbers will be sent complete with description strings (e.g. partition, zone, etc.).
115200 BPS	Serial port speed at 115200 bps.	Serial port speed at 57600 bps.

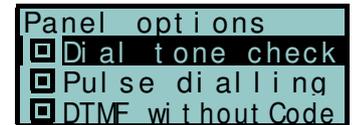
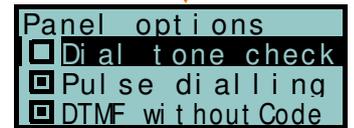
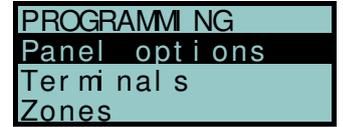
Table 4-1: Control panel parameters

Parameter	If enabled	If disabled
UTC timeOnSIA-IP	Calls to SIA-IP type numbers will contain the date and time in "UTC" format (Coordinated Universal Time).	Calls to SIA-IP type numbers will contain the date and time in local format
No Nexus on Cloud	The Nexus will not be enabled to access Cloud but will continue to perform all its other functions.	The Nexus will be enabled to operate over cloud, but will be unable to carry out its other functions.

1. Access the "Programming Panel options" section.

Type in code (Installer) **OK**, PROGRAMMING Panel options **OK**.

2. Use keys and to select the parameter you wish to enable/disable.
3. Press to enable the selected option, or to disable it.
4. Press **OK** to exit and save the configuration.



Terminals

4-2

This section describes the configuration flexibility of the system terminals. The profile of each terminal can be configured as follows.

- program the type of terminal:
 - Input (I)
 - Output (O)
 - Two way - supervised output (T)
 - Double Zone (D)
 - Unused (-)
- Programme the parameters related to the selected terminal.



For critical events or events of particular importance, it is advisable to use keypad terminals T1 and T2 as the signal outputs. The status of these outputs may switch (On to Off and vice versa) in the event of BUS reset.

ATTENTION!

1. Access the "Programming Terminals" section.

Type in code (Installer) **OK**, PROGRAMMING Terminal s **OK**.

The display will show the:

1st line: the number of terminals

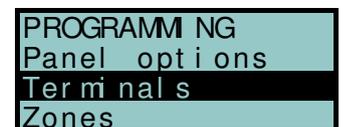
2nd line: the type of terminals and the selected terminal

3rd line: the description of the selected terminal

4th line: the description of the second zone of the selected terminal if it configured as a DOUBLE ZONE.

2. Use keys and to select the device whose terminals you wish to configure. The terminals are arranged as follows:

- terminals from 1 to 5 on the control panel
- terminals from 6 to 10 on the control panel (SmartLiving 1050 and 10100)
- terminals on expansion boards
- terminals on keypads



3. Use and to scroll across the terminals. The selected terminal will blink. The terminal setting is applied by pressing:
 - to configure the terminal as an INPUT ("I")
 - to configure the terminal as an OUTPUT ("O")
 - to configure the terminal as a TWO WAY - SUPERVISED OUTPUT ("T")
 - to configure the terminal as a DOUBLE ZONE ("D")
 - to configure the terminal as UNUSED ("-")
 - to enable/disable the terminal as "Wireless"
4. Once you have configured the terminal, press , , , and to configure its type.

If an UNUSED terminal is configured as **I**, **O**, **T** or **D** and the keypad emits an error "beep", it means that you have exceeded the maximum number of terminals available on the control panel. If you wish to employ the terminal concerned, you must first configure another terminal as UNUSED.

If you are working on an expansion terminal, press key to configure it, and consequently the entire expansion, as wireless. The "Wireless" string will be shown on the bottom line of the display. If you press key again, the operation will undo.

To enable the terminal for a wireless device, it must be configured as:

- INPUT - for single technology Air2 devices
- DOUBLE ZONE - for dual technology Air2 devices

To configure a terminal as a wireless output, proceed as follows:

1. Position the cursor on the terminal concerned.
2. Press to configure the terminal, and consequently the entire expansion, as wireless.
3. Configure the terminal as an "input" ().
4. Press to access the zone parameters programming section.
5. Go to the "Wireless" section.
6. Enroll the terminal as "Terminal T1 CM" or "Terminal T2 CM".
7. Press the "ENROLL" button on the Air2-MC300 device.
8. Enable the "Broadcast RF" option as follows:

Type i n code (Installer) , PROGRAMM NG Zones , select the zone, Opt i ons , Broadcast RF

To configure a wireless terminal as an "output", you must first enroll it as an "input", and then program it as an "output", as described in the instructions (see opposite).

The "Broadcast RF" option must be enabled for each terminal of the Air2-MC300 device concerned.

9. Go back to step 1 and configure the terminal as an output ().
10. Press to access the output parameters programming section (description, options, etc.).

Press in correspondence with any terminal, provided that it is not an UNUSED terminal, to access the parameter programming section of the type of terminal selected, whether it is a zone or an output (refer to *paragraph 4-3 Zones* or *paragraph 4-4 Outputs*).

Zones 4-3

This programming section deals with all the zone parameters.

1. Access the "Programming Zones" section.

Type i n code (Installer) , PROGRAMM NG Zones .

2. Using keys and , select the zone then press .

Description

This is the editable label which identifies the zone. At default all the zones assume the description of the peripheral they refer to, followed by the respective terminal.

- 1st line: default description
- 2nd line: current description
- 3rd line: description being edited
- 4th line: characters available

For example, the default description "Expansion 04 T03 corresponds to the zone located on terminal T3 of Expansion n. The default descriptions "Panel T05" and "Panel T05D" correspond to the two zones located on terminal T5 of the control panel, configured as "Double Zone".

Partitions

These are the partitions the zone belongs to. A zone configured as "Automation" cannot be assigned to any partition.

Use and to enable or disable the selected partition.

Type

Use and to select the type of zone, then press . The available Types are:

- **Instant**
- **Delayed**
- **Delayed unhidden**
- **Route**
- **24 hour**
- **Automation**
- **Armed in Away mode**
- **Disarm**
- **Switch**
- **OnArm/OffDisarm**
- **Patrol**

For "Arm", "Disarm", "Switch", "OnArm/OffDisarm" "Follow" and "Patrol" zones, refer to *Glossary, Command Zones*.

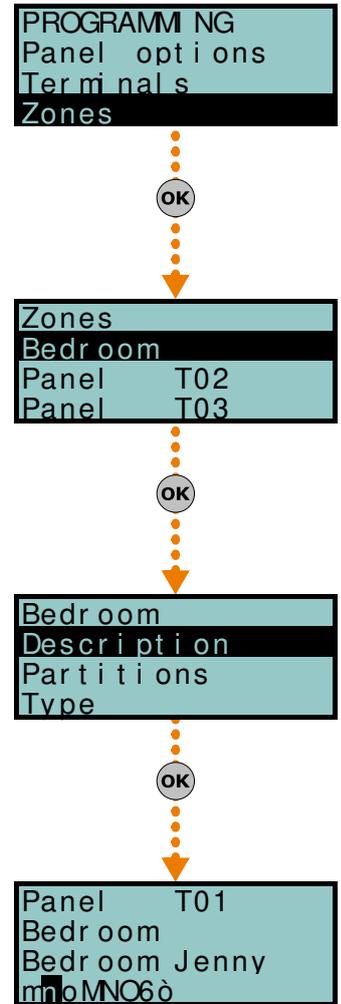
"Delayed" and "Delayed unhidden" zones are delayed during entry and exit phases, in accordance with the respective "Entry Time" and "Exit Time" settings (refer to *paragraph 4-9 Partitions*). A "Delayed unhidden" zone behave as follows:

- if violated when the system is disarmed, it will switch Off the blue LED on the keypad
- if the "View open zones" option is enabled, it will be shown on the keypad
- it will not generate "Partition not ready" events
- On arming from a keypad, the zone will appear as a violated zone but, when the arming operation is confirmed, will behave as a delayed zone and will not generate an alarm.
- if the "OpenZonesArmLock" option is enabled and the zone is violated, it will appear as a violated zone but, when the arming operation is confirmed, will behave as a delayed zone and will not generate an alarm.
- if the "OpenZonesArmLock" option is enabled, the zone is violated and instant arming is required, the zone will appear as a violated zone and when the partition arming operation is confirmed, the partitions the zone belongs to will not be armed.

Options

The available options must be enabled/disabled by keys and :

- **Interior**
- **Auto-bypassable**
- **Unbypassable**
- **Chime**
- **Test**
- **TampReed/FollPir**
- **Broadcast RF**
- **Use sensor LED**



The last three options apply to “Wireless” zones only, a full description of which follows.

Table 4-2: **Wireless zones options**

Option	If enabled	If disabled
TampReed/FoIPir	<ul style="list-style-type: none"> Air2-IR100 - in order to increase battery life, the infrared sensor will deactivate when the partitions it belongs to are disarmed and will only activate when the partitions it belongs to arm. Deactivated detectors do not generate alarms. When the partitions arm, there may be a delay of up to 3 minutes before the detector receives the activation command. Air2-MC300/MC200 - detects magnetic-contact tamper when both reeds are in stand-by status. 	<ul style="list-style-type: none"> Air2-IR100 - the PIR detector will be active at all times. Air2-MC300/MC200 - magnetic-contact tamper will not be detected under any circumstances.
Broadcast RF	This option must be enabled when the zone and one of the Air2-MC300 terminals (“T1” or “T2”) is configured as an “output”. Assures the activation/deactivation of the output within two seconds of the control panel command.	The activation/deactivation of a “wireless” output occurs within 6 minutes of the control panel command.
Use sensor LED	<p>The red LED of Air2-IR100 and Air2-MC300/MC200 devices signal alarm or tamper on the device.</p> <p>Note</p> <p>This option must be enabled on all the terminals of the Air2-MC300.</p>	The red LED of Air2-IR100 and Air2-MC300/MC200 devices is always Off.

- **No-Unbypassable** If this option is enabled, the zone will operate as an “Auto-bypassable” zone, with the difference that it will be automatically unbypassed when the partition next disarms.
- **NoArmIfNotReady**. If this option is enabled, the zone, even if it is a 24H, automation or delayed zone, will not arm when it is not in standby status. This option, for 24H or automation zones, can be used for the management of the “anti-mask” function of detectors which have this feature. Partitions which at the moment of arming have open zones with this option enabled, will not be armed; instead, the system will generate a failed arming even (“Failed to arm”).
- **Delay time 2**. If this option is enabled, delayed zones will activate the second partition entry time. If this option is not enabled, delayed zones will activate the first partition entry time.
- **Last exit zone**. If this option is enabled, and the zone passes from standby status to alarm status while the partition exit time is running, the exit time will be forced to 15 seconds. If the zone passes from alarm status to standby status, the exit time will be forced to 5 seconds.
- **UnbypassOnDisarm**. If this option is enabled, a zone which has been bypassed by a user, will be automatically unbypassed when the partition next disarms.
- **Hold-up**.
- **Fault zone**. If this option is enabled, violation of the zone will generate an Alarm event and contributes to fault signalling (yellow LED on the keypad).
- **Disable tamp. WLS**. If this option is disabled, open/dislodgement tamper on Air2 devices will not generate the respective events.

Activation of this option will void compliance with current regulations.

ATTENTION!

Wireless

Please note that this section will be operative only when the zone you are working on is configured as a wireless zone (refer to *paragraph 4-2 Terminals*).

Note

This section allows you to carry out all the operations relating to the programming of Air2 wireless series devices. The wireless-device programming section is arranged as follows.

- **Enroll device** - allows you to enroll a wireless device not yet enrolled on the terminal concerned.
 - Press **OK** to initialize the enrollment process. Select the type of detector you wish to enroll:
 - **Infrared sensor**, allows you to enroll an Air2-IR100 detector
 - **Magnetic contact**, allows you to enroll Air2-MC300 magnetic reed contact
 - **Terminal T1 M.C.**, allows you to enroll the “T1” terminal of an Air2-MC300
 - **Terminal T2 M.C.**, allows you to enroll the “T2” terminal of an Air2-MC300
 - **Smoke detector**, allows you to enroll an Air2-FD100 smoke detector
 - **Magn.Cont.MC200**, allows you to enroll an Air2-MC200 device.
 - **Curtain sensor**, allows you to enroll an Air2-DT200T curtain detector
 - **Curtain direction**, allows you to set the direction of an Air2-DT200T

- **Double T. sensor**, allows you to enroll an Air2-XDT200W dual technology detector
- **Single T. sensor**, allows you to enroll an Air2-XIR200W passive infrared detector
- **OutdoorDetector**, allows you to enroll an Air2-OTT100W outdoor triple technology detector, an Air2-ODI100W outdoor triple technology detector or an Air2-UT100 universal wireless transceiver

After selecting the desired type, press **OK**. The first line of the keypad will show the "Programming" string.

To enroll the wireless device, press and release its on-board "ENROLL" button. As soon as the enrolling process is complete, the keypad will emit an audible signal (beep) to confirm the operation, and will show (in accordance with the type of device) the following:

- **Delete detector**, allows you to delete (unenroll) an enrolled wireless detector from the terminal concerned
- **Infrared sensor** - allows you to change the parameters of the previously enrolled Air2-IR100 or Air2-FD100 smoke detector. If you press **OK**, it will be possible to adjust the sensitivity of the detector by setting the required number:
 - Air2-IR100: from 1 (least sensitive) to 4 (most sensitive)
 - Air2-FD100: 1=0.08 dB/m (pre-set mode); 2=0.10 dB/m; 3=0.12 dB/m; 4=0.15 dB/m

1. Use keys and to select the field you wish to change, then use the number keys (1, etc.) to edit the number.

or

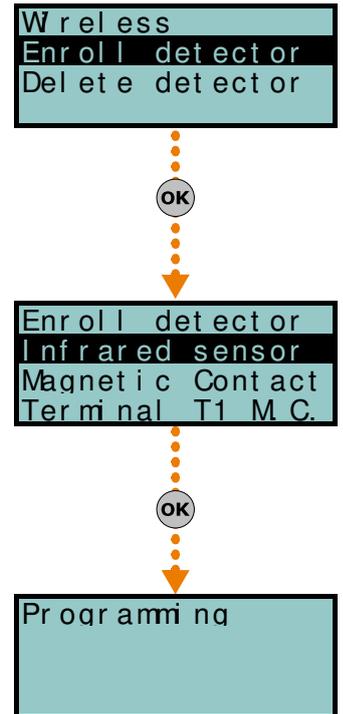
Use keys and to increase or decrease the number.

2. Press **OK** to confirm and exit.

- **Magnetic contact**, allows you to change the parameters of an already enrolled Air2-MC300 magnetic contact. Press **OK**, to access the following options:
 - **LongSide contact**, detection using the long side of the magnetic contact.
 - **ShortSideContact**, detection using the short side of the magnetic contact.
 - **Both contacts**, detection using both sides of the magnetic contact.

If you select the "Both contacts" option, standby status will be detected when either (or both) of the 2 reeds close. If you select either "LongSide contact" or "ShortSideContact", standby status will be detected when the selected reed closes and the other opens. If both reeds close, the system will generate a terminal-tamper event. In fact, the most common method of jamming this type of device is to hold a magnet in the vicinity of the magnetic contact, should this ever occur, both reed relays will close to trigger a tamper event.
 - **Terminal T1 M.C.** and **Terminal T2 M.C.**, to change the parameters of terminal "T1" of an enrolled Air2-MC300. If you press **OK** at this point, the keypad will step back to the Zones menu and you can set up the parameters of the terminal: Balancing, Rollerblind, Times, etc.
Terminals "T1" and/or "T2" of the Air2-MC300 device can be set up in the same way as wired terminals, with the exception that wireless terminals cannot be configured as "double zones".
 - **Magn.Cont. MC200**, allows you to change the parameters of an already enrolled MC200 magnetic contact. Press **OK** to access the following options:
 - **Infrared Shock** - allows you to set the sensitivity of the shock sensor (set "0" to disable, "1" for minimum sensitivity and "63" for the maximum sensitivity).
 - **Tilt** - allows you to set the maximum angle allowed before signalling of tilting occurs.
 - **Tilt duration**, allows you to set the signal delay after the detection of tilting (variation of the angle).

If shock and tilt detection are both enabled, alarm signalling will be generated as soon as one of these conditions exceeds its set value.
 - **Curtain detector**,
 - **Dual T detector**,
 - **Single T detector**,
 - **Outdoor detector**,
- these items display the same menu that appears when **OK** is pressed:
- **Sensitivity** - allows you to set the sensitivity of the PIR detector
 - **Shock Sensit.** - allows you to set the sensitivity of the shock detector
 - **M-wave sensit.**, allows you to set the sensitivity of the microwave sensor
 - **Antimask Sensit.** - allows you to set the sensitivity of the antimasking mechanism



The previously mentioned parameters will be shown in accordance with the specific device type. The values can be "0" for disablement, "1" for minimum value and "15" for maximum value.

Alarm signalling will occur as soon as one of the two sensors exceeds its programmed alarm threshold.

Balancing

The available balancing parameters are:

- Norm. open (NO)
- Norm.closed (NC)
- Single balancing
- Double balancing
- Double Zone (without EOL)
- Double Zone EOL (with EOL)

Alarm cycles

This programmable parameter accepts values between 1 and 15. If you set the value at 15, the zone will operate as a "repetitive zone" (refer to "Alarm cycles").

Detector type

It is possible to configure a zone as:

- Generic zone
- Rollerblind
- Shock

The following Table shows the terminals which accept Generic, Rollerblind and Shock zones, and the respective zone-parameter fields for each type.

Table 4-3: Zone - detector type

	Generic zone	Rollerblind	Shock
Control panel terminals	any	T1, T2	T1, T2
Expansion terminals	any	T1, T2, T3 or T4	T1, T2, T3 or T4
Keypad terminals	any	any	any
Extra Parameters	Al. pulse Duration Multipulse time Alarm pulses	Rollerblind time Rollerbl. pulses	Shock sensit. Shock time Shock pulses

Al. pulse Duration (generic zone)

This is the length of time (after detection of alarm conditions) the zone allows before generating an alarm. Expressed in multiples of 15 milliseconds or 10 seconds.

Multipulse time (generic zone)

This parameter applies only when the "Alarm pulse num." parameter is more than 1.

This is the window during which a number of alarm pulses must be detected (each lasting as long as the programmed "Al.pulse Duration"). The number of alarm pulses must equal or exceed the value programmed for "Alarm pulses", before the system generates an alarm. This window can be expressed in seconds or minutes (see opposite).

Alarm pulse num. (generic zone)

This is the number of pulses (each lasting as long as the programmed "Al.pulse Duration") necessary to generate a zone alarm event. If this value is more than 1, you must also programme the "Multipulse time" parameter.

Rollerblind time (rollerblind zone)

This parameter applies only when the value of the "Rollerbl. pulses" (see below) is more than 1.

This is the time window during which the system must detect a number of pulses equal to or higher than the value programmed for "Rollerbl. pulses" before generating a zone alarm. This window can be expressed in seconds or minutes (see opposite).

Rollerbl. pulses (rollerblind zone)

This is the number of pulses necessary to generate a zone-alarm event. If this value is more than 1, you must also programme the "Rollerblind time" parameter.

Shock sensit. (shock zone)

This is an empirical parameter which regulates the sensitivity of the sensor. Increasing this value decreases detection sensitivity.

Shock time (shock zone)

This parameter applies only when the "Shock pulses" value is more than 1.

If this value is expressed in minutes, there is an error margin of 1 minute (for example, if you set 5 minutes, the period can vary between 4 and 5 minutes).

This is the window during which a number of pulses must be detected the number of alarm pulses must equal or exceed the value programmed for "Shock pulses", before the system generates an alarm. This window can be expressed in seconds or minutes (see opposite).

Shock pulses (shock zone)

This is the number of pulses necessary to generate a zone-alarm event.

If this value is more than 1, you must also programme the "Shock time" parameter.

If this value is 0, the zone alarm will be generated by the "Shock sensit." parameter.

All the above-mentioned values can be programmed as follows:

1. Use and where possible to indicate the time in multiples of 15 milliseconds, seconds or minutes (refer to the note opposite).
2. Use keys and to select the field you wish to change, then use the number keys (1, etc.) to edit the number.
or
Use keys and to increase or decrease the number.
3. Press to confirm and exit.

Outputs 4-4

This programming section describes the programming processes of all the output parameters.

SmartLiving control panels always provide 3 outputs:

- Relay output
- Open collector output (O.C.) 1
- Open collector output (O.C.) 2

The outputs configured on the Flex5 expansion boards are open-collector outputs, with the exception the one configured on terminal T5 that can be configured as an analogue output (industrial standard 0-10V).

The 5 outputs on the Flex5/DAC expansion board can be configured as:

- high-power relay output
- Triac ON/OFF output (default setting)
- Triac dimmer output

The terminal pairs of the Flex5/DAC OUT1-OUT2 and OUT3-OUT4 are provided with the interlock function which is required in applications with, for example, roller blind motors.

Activated via the option, which must be activated for both terminals of the pair, this function has the purpose of inhibiting the simultaneous active status of the associated terminals.

1. Access the "Outputs" section.

Type in code (Installer) , PROGRAMMING Outputs .

2. Use and to select the output then press .

Description

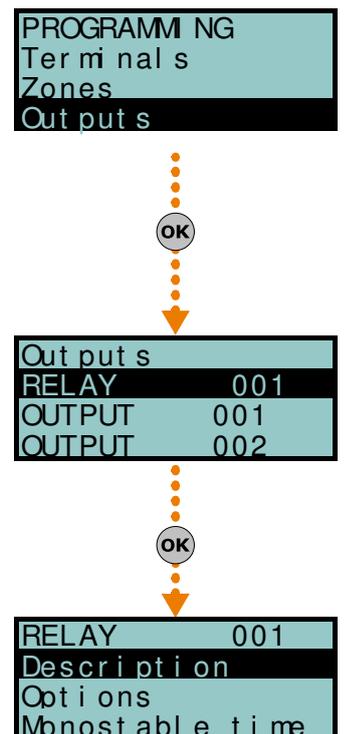
This is the editable output label (device description). By default each output, except for the 3 outputs on the control panel, acquires the description of the device where it is located followed by the relative terminal.

Follow the instructions in *paragraph 4-3 Zones - Descriptions*.

Options

Use and to enable or disable the selected option.

- **Norm. closed:** this will be the output status during standby.
- **Monostable**
- **Buzzer (beeper):** generates a 1Khz signal when the output activates - can be used to drive a buzzer.
- **Blinker:** generates an intermittent signal (0.5 sec ON and 0.5 sec OFF) when the output activates. It can be employed in direct control of a visual signalling device (e.g. flasher).
- **ON after Restoral:** the output does not restore-to-standby (reset) when the trigger-event clears. This option is useful in situations that require a trigger event for output activation and a reset event for its deactivation.



This option applies to "Bistable" outputs only. If it is enabled for a bistable output with reset-event configuration, it will deactivate the output instead of activating it (refer to *paragraph 4-7 Events*).

This option is useful in situations that require the output to reveal event "memory" (event signalling which continues even after the event has cleared). In this case, the output is deactivated by a different event which restores it directly to standby (resets the output).

For example, set:

- O.C. Output 1 is configured as "ON afterRestoral"
- the activation of "Mains failure" event is programmed to trigger O.C. Output 1
- the restoral (reset) of "Valid code" event is programmed to trigger O.C. Output 1

In the event of Mains failure, O.C. Output 1 will activate but will not restore to standby (reset) when the Mains failure condition clears. It will restore to standby (reset) only when "CODE 1" is entered a keypad and generates a "Valid code" for the "CODE 1" event.

- **Switching** - each time you execute an "activate output" command, the output will switch status. Therefore, if it is deactivated it will activate and vice versa.

However, each time you execute a "deactivate output" command, the output will always deactivate.

If you wish to manage this feature through a shortcut, you must use the "Activate outputs" shortcut.

- **Dimmer** - the output is a dimmer output thus the power supplied through the terminals can be adjusted by the end-user
- **Relay Use** - the output is a relay output
- **Home automation** - if the control panel enters programming mode, the activated output will not return to stand-by status.
- **Interlocked** This option enables the interlock function on the pair of terminals which the terminal of the selected Flex5/DAC belongs to (pairs OUT1-OUT2 and OUT3-OUT4).

In order for this to be valid, this option must be enabled for both terminals in the pair.

If the stand-by status of the output is determined by the occurrence of an event, the output will still not return to stand-by status during programming mode.

A declaration as to the type of output which is incoherent with the output itself may cause malfunction.

Note

If this value is expressed in minutes, there is an error margin of 1 minute (for example, if you set 5 minutes, the period can vary between 4 and 5 minutes).

Monostable time

This parameter applies to "Monostable" outputs only. This interval can be expressed in seconds or minutes (see "info" box).

When a "Monostable" output receives an activation signal, it will remain active (On) for the programmed time, regardless of the status of the trigger-event. In some cases, "Monostable" outputs can be forced to standby before the programmed monostable time runs out.

Use keys and and the number keys to set the times.

Walk test

This section provides a quick and easy way of testing all the configured inputs. After initializing the Walk test, all you need to do is walk through the protected partitions and then check the detection capacity of the inputs via the system keypad or SmartLeague software application.

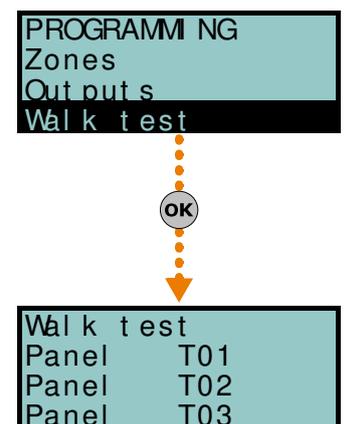
Type in the code (Installer) **OK**, PROGRAMMING Walk test **OK**.

On access this section, the full list of configured zones appears on the screen.

As these input zones are violated by the operator carrying out the walk test, they will be cleared from the list and the keypad will emit a long beep.

You can consider the outcome of test positive when there are no zones left on the list.

4-5



Telephone

4-6

This programming section deals with all the telephone parameters.

The integrated ATS device (alarm transmitting system) provides the following features (in compliance with EN50131 relating to the notification of information).

- Type B notification apparatus (refer to EN50131-1:2008-02, paragraph 8.6 Notification, Table 10, page 46, Grade 2).
- The ATS2 notification apparatus specified in the table, is characterized by:
 - Transmission time - classification D2 (60 seconds)
 - Transmission time - max. values M2 (120 seconds)
 - Classification time - classification T2 (25 hours)
 - Substitution security - S0 (no detection of device substitution)
 - Information security - I0 (no detection of message substitution)

Type in code (Installer) , PROGRAMMING Telephone .

Select number

The Phonebook provides 15 number slots which can be selected by means of keys and . You can program the following fields for each selected number:

- **Number:** edit field for the contact number (maximum 20 digits). Accepts also “,” (= 2 second pause), “*” and “#”.
- **Description:** edit field for the name of the contact person. Follow the instructions in *paragraph 4-3 Zones*.
- **Type:**
 - **None** - the selected number can receive SMS text messages only
 - **Voice** - the selected number can receive voice calls and SMS text messages

If the number refers to the Alarm Receiving Centre, assigns the **ARC** protocol (reporting format):

 - **Ademco 10bps**
 - **Ademco 14bps**
 - **Franklin 20bps**
 - **Radionics 40bps**
 - **Scantronic 10bps**
 - **CONTACT-ID**
 - **SIA** - Level 1 SIA is applied This reporting format (protocol) is capable of sending descriptions of the objects in ASCII characters. if you do not wish to send the descriptions in ASCII characters, select “No SIA strings” (refer to *paragraph 4-1 Parameters and control panel options*). You can set a 4, 5 or 6 digit customer code for this protocol.
 - **Ademco Express**
 - **CESA**
 - **SIA-IP**

Use keys and to select the number type then press .

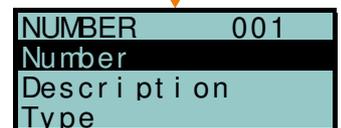
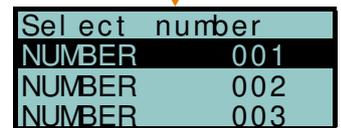
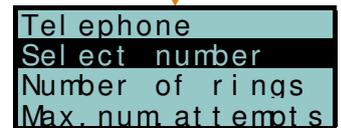
If a telephone number is “SIA-IP” type, the IP address and port of the SIA-IP receiver must be entered in the receiver number field in the “Number” section, using the following format:

xxxxyyzzttt,ppppp

where:

- “xxxxyyzzttt” are the 4 octets of the IP address (standard IPv4), each of which should be written with 3 figures and, if necessary, “0” filler characters and no separation points.
- “ppppp” is the port and should be written with 5 figures and, if necessary, “0” filler characters.

- **Account code:** a 4-character alphanumeric code which identifies the caller in reports to the Alarm Receiving Centre. Some protocols (reporting formats) accept digits only, whilst others accept also “A”, “B”, “C”, “D”, “E” and “F”, available using keys .
- **Partitions:** this option allows you to associate each telephone number with specific partitions. By selecting the partitions, using Keys and , you enable/disable the users (who have at least one of these partitions in common with the telephone number) to modify the number concerned.



- **Options:**
 - **Receive SMS**, this option allows the telephone number to receive an SMS message from the Nexus GSM module, as well as all other event-related communications.
 - **BackupOnOtherCha**, this option, in the event of call failure on a channel, enables the control panel to carry out call attempts on an alternative channel, and then retry on the original channel in order to alternate the set number of attempts.
- **Channel**, this section allows you to select the channel for the priority routing of a call in the event of incoherent programming or in the event of the failed accessibility of the communication device:
 - **PSTN**
 - **Nexus**
 - **SmartLAN**
- **Encryption** - this section allows you to select the encryption type of SIA-IP protocol:
 - **None**
 - **AES 128 bit**
 - **AES 192 bit**
 - **AES 256 bit**

Number of rings

This value determines the number of rings the system allows before picking up an incoming call.

Max.num.attempts

This value determines the number of calls attempts the system will make before deleting the contact number from the call queue.

Message repeats

This value determines the number of times the voice message will be played during the call.

All the above-mentioned values can be programmed as follows:

1. Use keys  and  to select the field you wish to change, then use the number keys (**1**, **.**, etc.) to edit the number.
or
Use keys  and  to increase or decrease the number.
2. Press  to confirm and exit.

Events 4-7

This programming section deals with all the event-generated output actions.

The control panel recognizes all of the events described in this paragraph and is capable of generating pre-programmed actions for each event, both when the event occurs and when it restores/ends.

The actions are:

- activation of outputs
- activation/deactivation of outputs
- event notification via phone call
- send SMS text messages
- event storage
- management of voice messages
- management of the option of each event
- activation of event related shortcuts

Telephone notifications (calls) are queued and sent out in chronological order. However, some events may need to be notified immediately (for example, use of a code under duress), therefore, such events can be given priority by selecting the "Priority" option.

Event notification via e-mail requires the use of a SmartLAN/G board.

Event notification via predefined SMS messages requires the use of a Nexus (refer to *paragraph 5-5-3 Text for SMS messages*).

If a list of telephone calls is programmed for the notification of an event as well as SMS messages, the SMS messages will be sent before the telephone calls.

Note

The following table shows the events the control panel recognizes, the number of events for each type, the trigger and restoral method of each event and the event category (Pulse).

Table 4-4: Event type

Name	Occurs when...	Restores when ...	Number of events	Pulse events	Control panel models
Zone alarm	A zone generates an alarm	A zone restores	One event for each zone	no	all
Terminal tamper	A terminal detects tamper (short-circuit or wire cutting)	A terminal restores	One event for each terminal	no	all
Partition alarm	A 24h zone which belongs to the partition generates an alarm, or a zone which belongs to the partition generates an alarm during Away mode.	All the zones belonging to the partition restore (reset).	One event for each partition	no	all
StayPartit.alarm	A zone which belongs to a partition armed in Stay or Instant mode, generates an alarm.	All the zones belonging to the partition restore (reset).	One event for each partition	no	all
Partition tamper	A zone which belongs to the partition detects tamper (short-circuit or wire cutting).	All the zones belonging to the partition restore (reset).	One event for each partition	no	all
Zone bypass	A zone is inhibited	A zone is enabled (switched On)	One event for each zone	no	all
Real-time zone	The electrical status of a zone switches from standby to alarm.	The electrical status of a zone switches from alarm to standby.	One event for each zone	no	all
	The event is independent of the zone type and the armed/disarmed status of the partitions.				all
Partit.not ready	A zone which belongs to the partition is not in stand-by status.	All the zones belonging to the partition are in standby status.	One event for each partition	no	all
Away arm request	A request is made to arm the interior and perimeter zones of the partition	A request is made to disarm the partition	One event for each partition	Yes	all
Overtime request	A request is made to arm the partition in Stay mode (perimeter zones only) or in Instant mode	A request is made to disarm the partition	One event for each partition	Yes	all
Partit.awayArmed	The partition interior and perimeter zones have been armed effectively	The partition will be disarmed	One event for each partition	no	all
Partit.StayArmed armed	The partition has been armed effectively in Stay or Instant mode	The partition will be disarmed	One event for each partition	no	all
Disarm partition	The partition will be disarmed	The partition will be armed	One event for each partition	no	all
Partition reset	A request is made to reset the partition		One event for each partition	Yes	all
Exit time	The partition exit time starts running	The partition exit time expires	One event for each partition	no	all
Entry time	The partition entry time is running	The partition entry time expires	One event for each partition	no	all
Pre-arm time	The partition Pre-arm time is running	The partition pre-arm time expires	One event for each partition	no	all
Overtime request	A request for overtime relating to the partition is made		One event for each partition	Yes	all
Chime	A chime zone belonging to the partition is violated		One event for each partition	Yes	all
Forced arming	At the time of an arming command, relating to one or more partitions, there are open zones on the partition/partitions involved, or there are other conditions present which lower system security, nonetheless, the user arms the system.		One event for each partition	Yes	all
Failed to arm	The "OpenZonesArmLock" option is enabled at the time of a partition arming command and there is at least one open zone on the partition/s involved. or when one or more of the conditions described in "LossTamp.ongoing" is present (refer to "FaultForNotReady", paragraph 4-23 Other parameters).		One event for each partition	Yes	all
Valid code	A user-code PIN entered at a keypad is recognized as valid		One event for each code	Yes	all
Valid key	A key used at a reader is recognized as valid on the reader		One event for each key	Yes	all

Table 4-4: Event type

Name	Occurs when...	Restores when ...	Number of events	Pulse events	Control panel models
Valid Code AtKeyp.	A user-code PIN entered at a keypad is recognized as valid on the keypad		One event for each keypad	Yes	all
ValidKeyAtReader	A key used at a reader is recognized as valid on the reader		One event for each reader	Yes	all
Partition code	A user-code PIN entered at a keypad is recognized as valid on the partition		One event for each partition	Yes	all
Partition key	A key used at a reader is recognized as valid on the partition		One event for each partition	Yes	all
Failed call	All attempts to call a specific phone number have failed	One call to the phone number has been successful	One event for each contact phone number	no	all
Timer activated	The timer is enabled (On)	The timer is disabled (Off)	One event for each timer	no	all
Thermostat ON	The activation conditions programmed for the keypad thermostat occur.	The deactivation conditions programmed for the keypad thermostat occur.	One event for each keypad	no	all
Scenario ON	The status of all the partitions correspond exactly to the configured scenario.	The status of at least one of the partitions does not correspond to the configured scenario.	One event for each scenario	no	all
ProgrammableEvt	Refer to <i>paragraph 5-14-3 Programmable events</i>			no	all
Emergency key	One of the emergency-buttons is pressed		One event for each emergency-button	Yes	all
Panic Panic	The "Panic" shortcut has been activated.		15	Yes	all
Periodic event	The Periodic Event occurs		4	Yes	all
Control panel open	The control-panel enclosure is removed	The front of the control-panel is replaced	1	no	all
Dislodged panel	The control-panel enclosure is detached from the wall	The control-panel enclosure is reattached to the wall	1	no	all
Zone fuse fault	The zone protection fuse on the control panel is not operational (blown)	The zone protection fuse on the control panel restores	1	no	all
IBUS fuse fault	The I-BUS protection fuse is not operational (blown)	The I-BUS protection fuse restores	1	no	all
Low battery	The backup battery is low (voltage below 10.4V)	The backup battery is charged (voltage above 11.4V)	1	no	all
Mains failure	The primary power supply 230V~ fails	The primary power supply 230V~ is restored	1	no	all
Expansion tamper	An expansion board signals tamper conditions	Tamper conditions clear on all the system expansion boards	1	no	all
Keypad tamper	A keypad signals tamper conditions	Tamper conditions clear on all the system keypads	1	no	all
Reader tamper	A reader signals tamper conditions	Tamper conditions clear on all the system readers	1	no	all
Sound.flash.Tamp	Tamper is detected on a sounder/flasher connected to the BUS	All the sounder/flashers connected to the BUS reset tamper	1	no	all
Nexus tamper	The GSM dialer Nexus signals tamper	Tamper conditions clear on the Nexus	1	no	all
Tamp. LIVPWR100	For future use				
VideoSens.Tamper	For future use				
Expansion loss	An expansion board cannot be found on the BUS	All expansion boards can be found on the BUS	1	no	all
Keypad loss	A keypad cannot be found on the BUS	All keypads can be found on the BUS	1	no	all
Reader loss	A reader cannot be found on the BUS	All readers can be found on the BUS	1	no	all
Sound.flash.Loss	A sounder/flasher device connected to the BUS is not present	All sounder/flasher devices connected to the BUS are present	1	no	all
Nexus loss	The control panel is unable to communicate the Nexus 100	Communication between the control panel and the Nexus restores	1	no	all
Nexus LIVPWR100	The control panel is unable to communicate with the LIVPWR100 board	Communication between the control panel and the LIVPWR100 restores	1	no	SmartLiving G3
VideoSensor loss	For future use				
Jamming	Wireless interference detected	Wireless interference cleared	1	no	all
Low battery WLS	The battery of a least one wireless detector is running low	All the wireless detectors are running with sufficient power	1	no	all

Table 4-4: Event type

Name	Occurs when...	Restores when ...	Number of events	Pulse events	Control panel models
WLS zone loss	Loss of at least one wireless detector has been signalled (supervisory time expired)	All the wireless detector are present	1	no	all
Installer code	An Installer PIN entered at a keypad is recognized as valid		1	Yes	all
Invalid code	An invalid code PIN is entered at a keypad		1	Yes	all
False key	An invalid key is used at a reader		1	Yes	all
Nexus fault	The GSM dialer Nexus signals a fault (see <i>Chapter 9 - Errors and faults</i>)	Fault conditions clear on the Nexus	1	no	all
Tel. line down	The land line is not working	The land line restores	1	no	all
Hard reset	The control panel re-initializes. The system clock may be wrong or not working properly.		1	Yes	all
Call queue full	There are no more slots left in the outgoing call queue		1	Yes	all
Successful call	The call is answered		1	Yes	all
Programming	Access to system programming is authorized	End of system programming	1	no	all
Ongoing call	A call is sent	A call ends	1	no	all
SMSMessageFailed	Nexus failed to send SMS message		1	Yes	all
Output fault	An output fails to switch status as commanded		1	Yes	all
Low credit	The credit remaining on the SIM card inserted in the Nexus is below the minimum credit threshold.	The remaining credit is above the minimum credit threshold.	1	no	all
Time modified	There is a change in the date and time. This event will be recorded together with the date/time before the change.	There is a change in the date and time. This event will be recorded together with the date/time after the change.	1	no	all
Int. Resistance	The internal resistance of the battery has exceeded the $R_{i\ max}$ value.	The internal resistance of the battery returns to below the $R_{i\ max}$ value.	1	no	all
Battery shorted	A short-circuit condition has been detected on the battery connection terminals	The short-circuit condition is no longer present	1	no	SmartLiving G3
Battery disconn.	The backup battery is disconnected	The backup battery is connected	1	no	SmartLiving G3
PwSupplyOverload	Output overload is detected on the power-supply unit	The electrical load returns below the allowed limit	1	no	SmartLiving G3
PwSupply Overheat	The temperature of the power-supply unit has exceeded the allowed limit	The temperature of the power-supply unit is normal	1	no	SmartLiving G3
Ground fault	Leakage to ground is present	The leakage to ground condition is no longer detected	1	no	SmartLiving G3
Overvoltage "x"	A voltage of over 14.5V has been detected on terminal "+AUX" corresponding to number "x" on the LIVPWR100 board.	The normal voltage on the terminal has been restored.	1	no	SmartLiving G3
Overvolt. BUS	A voltage of over 14.5V has been detected on I-BUS terminal "+" on the LIVPWR100 board.	The normal voltage on the terminal has been restored.	1	no	SmartLiving G3
Undervoltage	A voltage below 9.8V has been detected on terminal "+AUX" corresponding to number "x" on the LIVPWR100 board.	The normal voltage on the terminal has been restored.	1	no	SmartLiving G3
Undervoltage BUS	A voltage below 9.8V has been detected on I-BUS terminal "+" on the LIVPWR100 board.	The normal voltage on the terminal has been restored.	1	no	SmartLiving G3
Short circuit "x"	A short-circuit has been detected on terminal "+AUX" corresponding to number "x" on the LIVPWR100 board.	The short-circuit is no longer present.	1	no	SmartLiving G3
Short circuit BUS	A short-circuit has been detected on I-BUS terminal "+" on the LIVPWR100 board.	The short-circuit is no longer present.	1	no	SmartLiving G3
Overload "x"	A load of over 1.5A has been detected on terminal "+AUX" corresponding to number "x" on the LIVPWR100 board.	The terminal restores to normal.	1	no	SmartLiving G3
Overload BUS	A load of over 3.5A has been detected on I-BUS terminal "+" on the LIVPWR100 board.	The terminal restores to normal.	1	no	SmartLiving G3

Table 4-4: Event type

Name	Occurs when...	Restores when ...	Number of events	Pulse events	Control panel models
NoCommunPwSupply	The power supply unit fails to communicate with the control panel	Communication between the power supply unit and the control panel restores.	1	no	SmartLiving G3
Tel. on number 1	A call has been sent to phone number 1	The call has ended (even in the event of negative outcome)	1	no	all
Tel.on number 15	A call has been sent to phone number 15	The call has ended (even in the event of negative outcome)	1	no	all
Sync.data IP2RX	The IP2RX synchronization process has been carried out from a keypad (refer to the User Manual, "Activations")		1	Yes	all
IP conn. lost	The IP connectivity test is enabled and the test result in negative (failed).	A connection attempt has been successful.	1	no	all
IP conn. lost	Nexus has detected GPRS connectivity trouble.	The GPRS connectivity is restored.	1	no	all

Each event can be associated with 3 voice messages, selected from the message list (refer to *Appendix C, Voice messages*).

- Message type
- Message A
- Message B

This feature allows you to create messages which will be played during event-related voice calls to contact numbers, both at the start and end of the event.

The choice of messages and the number of times they are played depends on the "AutomaticDialer" settings.

1. Accessing the "Events" section

Type in code (Installer) **OK**, PROGRAMMING Events **OK**.

2. Use keys and to select the event type (if you are dealing with a group of events, repeat the required operation) and then press **OK**.
3. Select:

- **Activation**, to program the actions to be carried out when the event occurs.
- **Restoral**, to program the actions to be carried out when the event ends.

4. Successively, the parameters to programme are:

TelephoneNumbers

Programme the call recipient numbers.

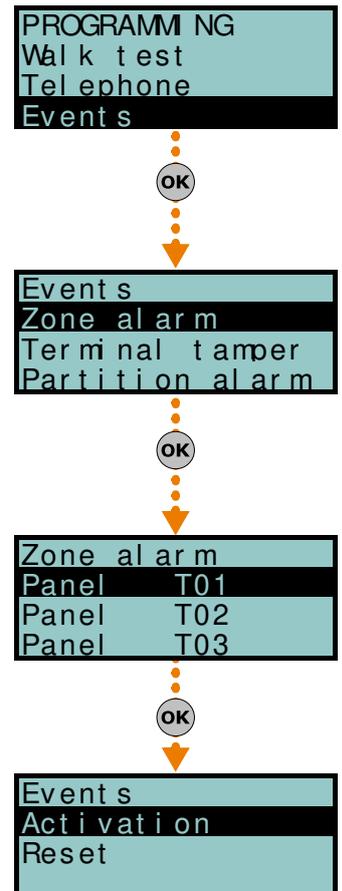
Message type

Message A

Message B

Select the number of the message (see *Table 4-5: Event-related messages* and *Appendix C, Voice messages*):

1. Use keys and to select the field you wish to change, then use the number keys (**1-9**, etc.) to edit the number.
or
Use keys and to increase or decrease the number.
2. Press **OK** to confirm and exit.



The following table shows the voice-message sequence in accordance with the previously mentioned parameters and options.

Table 4-5: Event-related messages

	"Automatic dialer" enabled	"Automatic dialer" disabled
Message type	Plays the message relating to the event type (e.g. "zone alarm", "Mains failure") This message should not be changed.	You can select any message from 1 to 219
Message A	Blank message, editable	
Message B	Contains event details, for events which are not distinctive (e.g. the "zone alarm" event indicates the zone concerned).	
Event Activation Sequence	<ol style="list-style-type: none"> 1. Message type + 260 2. Message A 3. Message B 4. "Location" (244) 	<ol style="list-style-type: none"> 1. Message type 2. Message B 3. "Location" (244)
Sequence in the event of Restoral	<ol style="list-style-type: none"> 1. "Restoral" (97) 2. Message type 3. Message A 4. Message B 5. "Location" (244) 	<ol style="list-style-type: none"> 1. Message A 2. Message B 3. "Location" (244)

If an event is associated with the "Automatic dialer", the "Type Message" option refers to messages 261 to 312, that is to say, the messages containing the event descriptions (event types).

Note

Options

To be activated by keys * and # :

Table 4-6: Event options

Option	If enabled	If disabled
Event ON to log	When the event occurs, it will be saved to the events log.	When the event occurs, it will not be saved to the events log.
Event OFF to log	When the event clears, it will be saved to the events log.	When the event clears, it will not be saved to the events log.
StartPeriodicEv.	When the event occurs, the system will generate Periodic event number 1.	
Silent event	If the event occurs, the system will generate silent calls which will not be signaled on the keypads.	If the event occurs, the system will generate calls which will be signaled on the keypads.
Clear call queue	When the event occurs, the system will cancel the outgoing call queue.	
Send address	In the case of voice calls, the system will include the address of the location alarm (refer to the <i>Table 4-5: Event-related messages</i>)	In the case of voice calls, the system will not include the address of the location alarm (refer to the <i>Table 4-5: Event-related messages</i>)
Local Message ON	When the event occurs, the system will play the event-related voice message on keypad speaker n. 1	
LocalMessage OFF	When the event occurs, the system will not play the event-related voice message on keypad speaker n. 1	
AutomaticDialler	Refer to the <i>Table 4-5: Event-related messages</i>	
Priority	Calls associated with this type of event have priority over all other calls. Therefore, if a priority event occurs, any ongoing calls will be interrupted and the priority-event call will be sent immediately.	
Note This option is applicable only when a Nexus device is installed	ForceAlt.Channel	All the programmed event calls will not be made over the channel indicated by the "Channel" parameter when programming each phone number, but instead will be made over the alternative channel (refer to <i>paragraph 4-6 Telephone</i>).
	Automatic SMS	The dispatched SMS message will consist of the event description in the Events log
	Enable SMS	When the event occurs, the control panel will send an SMS message to all the duly enabled telephone numbers (refer <i>paragraph 4-6 Telephone</i>)
		The SMS text message can be selected from the 50 messages provided by the Nexus device. The SMS text message is identified by the "SMS message number/index", as described below.
		When the event occurs, the control panel will not send an SMS message

Class code

This is the CONTACT-ID reporting format Class-Code which corresponds to the event.

Event code

This is the 2-character alphanumeric code, which corresponds to the event sent the alarm receiving centre (ARC). For zone and terminal events (alarm, tamper, bypass), the "CCC" field of the CONTACT-ID protocol counts the number of hard terminals in accordance with the Hard terminals table (refer to *Appendix D, Screw Terminals*).

Outputs

When programming the Event-Activation section, you must programme the main output which will be activated when the event occurs. When programming the Event-Restoral section, you must program the main output which will be activated when the event ends.

Select the output from the list (which includes the Relay outputs, OC1, OC2 and the terminals configured as outputs and also the sounder/flashers) and press .

If the output has the "ON afterRestoral" option enabled (refer to *paragraph 4-4 Outputs*) and it is programmed on event restoral, the output will deactivate when the event occurs.

Note

For Zone alarm, Terminal tamper, Partition alarm, Stay partition alarm and Partition tamper events, monostable outputs programmed in the "Outputs" section will restore these events when, on expiry of the monostable time, the event concerned has effectively returned to standby status. If the event status restores to standby while the monostable time is running, the event itself will not be restored.

Other outputs

This section allows activation of added outputs (as well as the output programmed in the "Outputs" parameter) when the event occurs or restores.

These added outputs can be selected by means of keys and from a programmable list in the "Added Outputs" section.

OtherOutputsProg

This section allows the creation of the list of outputs (16 for "Activation" or 8 for "Restoral" to be programmed in the "Other outputs" section).

This is the sole list for the entire control panel and is independent of the type of event.

Note

Use keys and to make your selection and then press to confirm.

SIA Codes

If the event is associated with calls using SIA or SIA-IP protocol, this option allows you to program the event code in accordance with SIA Standard, by selecting it from a list.

Use keys and to make your selection and then press to confirm.

An appendix provides an explicative table of all the SIA codes (*Appendix F, SIA Codes*).

Siren sound types

This section allows you to select the audible-visual signals emitted by the sounder/flashers, when these are programmed in the "Outputs" and "Other outputs" section.

Please note that the "Tone Type" is a parameter of the event. Therefore, if several sounders have been programmed in relation to a specific event, they will all emit the programmed tone when the event occurs. If a sounder has been programmed in relation to several events, it will emit the last tone type setting received in order of time.

Use keys and to make your selection and then press to confirm.

For further information regarding the "Outputs", "Other outputs" and "Tone type" parameters of each event, refer to *Appendix E, Combination of outputs triggered by events*.

Timers

4-8

This programming section deals with the 10 system Timers.

Each timer can be programmed to manage:

- the partitions that codes and keypads belong to and have access to the programming process of the timers via the user menu.
- two scheduled activation times ("ON") for each day of the week.
- two scheduled deactivation times ("OFF") for each day of the week.

The SmartLeague software program will allow you program up to 15 exceptions.

A timer can be associated with a:

- a **Partition** - if a partition is associated with a timer which controls automatic-arming operations (refer to *paragraph Activations* in the *User's Manual*), it will arm when the timer switches ON and disarm when the timer switches OFF.
- a **Code** - if the timer is enabled, the code will be authorized to operate on the system only during the period the timer is active (ON).
- a **Key** - if the timer is enabled, the key will be authorized to operate on the system only when the timer is active (ON).

In order to associate timers with any of the above-mentioned objects, it is necessary to access the respective control-panel programming section.

The timers must be enabled/disabled by the user (refer to paragraph Activations in the User's manual).

On exiting the programming session (via keypad, computer or modem) all the timers will be enabled automatically. Therefore, if it will be necessary to disable the timers as required.

1. Accessing the "Timers" section:

Type in code (Installer) **OK**, PROGRAMMING Timers **OK**.

2. Use keys and to select the Timer then press **OK**.

Once the timer has been selected, it will be possible to activate the partitions for access to programming or the activations for every day of the week:

3. Select the "Partitions" option and press **OK**.

4. Select the partitions with access and enable or disable them using and .

5. Press **OK** to confirm and exit.

3. Use and to select the day of the week.

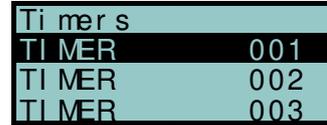
4. Select an activation or a restoral of the timer.

5. Set the selected time (expressed in hours and minutes) by means of keys and then, using keys and select the number.

6. Press **OK** to confirm and exit.

It is also possible to program only activation or only reset of a timer. The field not used for programming purposes must be set as "--:--".

Note



Note



Partitions

4-9

This programming section deals with the system Partitions and the respective options and parameters.

1. Accessing the "Partitions" section:

Type in code (Installer) **OK**, PROGRAMMING Partitions **OK**.

2. Use keys and to select the Partition then press **OK**.

Description

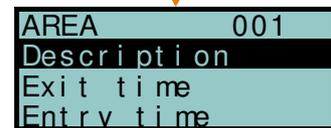
This is the editable partition label (description).

Exit time

A period, expressed in minutes or seconds, during which the user must LEAVE the partition after arming the system (see the "info" box). If you set "0" in this field, there will be no Exit time (delay), therefore, any delayed zones, which belong to the partition, will generate alarms if they are not in standby status when the system arms.

Entry time

A time (expressed in minutes or seconds) the system allows the user to disarm the partition after violation of a delayed zone (for example, after opening the front door). If the system is not disarmed within the set time it will generate an alarm (see "info" box).



If you set "0" in this field, there will be no Entry time (delay), therefore, any delayed zones will generate alarms instantly if they are violated when the system is armed.

Entry time 2

This is the second Entry time (delay).

Pre-arm time

This is the period (expressed in minutes) before an automatic arming operation (see "info" box).

In order to comply with EN50131 instructions, the "Pre-arm" time must be set at a value that is not "0".

Patrol time

An "Inspection" period (expressed in minutes) which allows patrol-key/code holders (security staff, night watchmen, etc.) to check the premises (see "info" box).

All the above-mentioned "times" can be programmed as follows:

1. Use keys and to choose whether to indicate the time in seconds or minutes (see note).
2. Use keys and to select the field you wish to change, then use the number keys (1, ., etc.) to edit the number.
or
Use keys and to increase or decrease the number.
3. Press to confirm and exit.

If this value is expressed in minutes, there is an error margin of 1 minute (for example, if you set 5 minutes, the period can vary between 4 and 5 minutes).

Timers

Select the timer you wish to associate with the "auto-am" operations.

Remember to enable auto-arm partition in the section:

User menu, Act i vat i ons .

Note

Forced auto-arm operations may occur, generated by events active at the time of the auto-arm operation.

Options

- **Auto-resetMemory** - if enabled by means of the key, each partition arming operation will reset the partition alarm/tamper memory automatically.
- **Auto-arm STAYmode** - if enabled by means of the key, the partition will arm in Stay mode at the pre-set auto-arm time. If disabled by means of the key, the partition will arm in Away mode at the pre-set auto-arm time.
- **StopTelOn Disarm** - if enabled, the call queue will clear when the partition disarms.

User Codes

This programming section deals with the user code options/parameters.

The user code PINs must comprise 4, 5 or 6 digits. The PIN of user code n. 1 is "0001" at default. The PINs of the successive user codes are "0002", "0003", etc.

1. Accessing the "Codes" section:

Type i n code (Installer) , PROGRAMM NG Codes .

2. Use keys and to select the code then press .

Description

This is an editable programming field for the code user's name.

Partitions

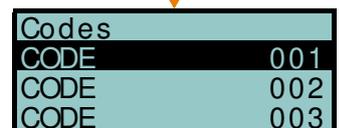
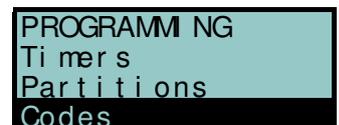
Select the partitions the user code is assigned to. Press , to enable the partition and to disable it.

Options

Use and to enable/disable the code options.

- **Partition filter** - if this option is enabled, the code will be able to change the parameters only of codes with a lower rank in the system hierarchy whose partitions are amongst the partitions assigned to the code being programmed.
For example, a "Master" code with "Partition filter" assigned to partitions 1, 3, 5 and

4-10



7 will be able to enable/disable or change the PIN of any "User" code assigned to partitions 1 and 5 but not the PIN of a "User" code assigned to partitions 1, 2, and 3.

- **Text menu and User menu** - the combination of these two options allows immediate visualization of the menu screens on the keypad displays after acceptance of a valid user PIN. Refer to the following table.

Table 4-7: Combinations "text menu" and "user menu"

Case	Text menu	User menu	Description
A	Disabled	Enabled	Access to the user-menu (shown as a list of operations the user is enabled to perform); at this point the user can scroll the list using and and select the required option.
B	Disabled	Disabled	Visualization of the user-icons associated with function keys F1 , ..., F4 ; at this point the user can press the required function key and activate the associated shortcut.
C	Enabled	Disabled	Shows the descriptions of the personalized user-icons associated with function keys. The descriptions of the shortcuts are shown in place of their associated icons. The user can use and to scroll the list of shortcut descriptions and select the desired shortcut, which can be activated by means of the OK key.
D	Enabled	Enabled	The same as "C"

In all methods of access (A, B and C), the key allows you to access/view the other cases in succession, see figure.

- **AnnounceShortcut** - if enabled on a voice capable keypad, the descriptions of all the shortcuts assigned to the code and associated with the number keys will be announced after acceptance of the entered PIN.
- **Remote access** - if enabled, the code PIN can be used to operate the system from any remote telephone.

If the code PIN is entered on a remote phone keypad, only the shortcuts associated with keys 0 to 9 can be used to:

- Arm/Disarm
- Stop alarms
- Clear call queue
- Delete memory
- Activate Output
- Deactiv. Output
- Listen-in
- Arming status

Any other type of command will have no effect.

- **Patrol** - if enabled, the code will have "Patrol time" attributes.
- **Fixed length** - if enabled, after typing in a PIN and without pressing the **OK** key, the user will be able to activate the shortcut associated with function key "F12", programmed via the "F1/4KeyShortcuts", described later.

If this shortcut is number 1 ("Arm/disarm") and all the partitions assigned to the user code in question are disarmed, the command will arm them, otherwise it will disarm them.

Users code enabled for this option have access to their respective menus only after pressing the **OK** key and entering a valid PIN.

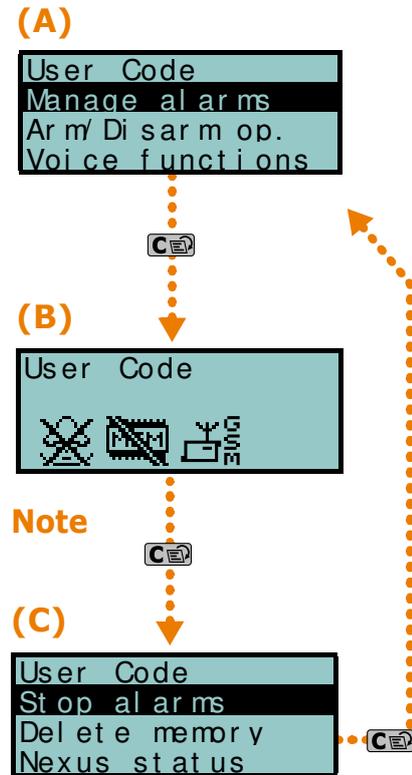
F1/4KeyShortcuts

This section allows you to programme up to 12 shortcuts associated with keys **F1** , ..., **F4** . After valid PIN entry, the keypad will show the icons that correspond to keys **F1** , ..., **F4** and which are associated with these shortcuts. Press the corresponding key to activate the respective shortcut.

0/9 Key shortcuts

This section allows you to program up to 10 shortcuts associated with keys **0** , ..., **9** . After PIN acceptance, the code user can activate the shortcut by pressing the respective number key.

To assign the shortcuts to the function keys, work through the following steps:



1. Use keys and to select the key you wish to associate with the shortcut then press .
2. Press then, using keys and , select the shortcut you wish to associate with the function key from the "Type" list.
3. Press to confirm and exit.
4. If the shortcut is associated with "Arm/Disarm" operations, the application will ask you to select a scenario. If the associated shortcut is "Activate output" or "Deactiv. output", the application will ask you to select the output.

Assigned outputs

This section allows you to enable/disable the outputs the code user can control manually via the:

User menu, Out put s ON/OFF .

1. Use keys and to select the desired output.
2. Use keys and to enable/disable manual control of the output for the code concerned.
3. Press to confirm and exit.

It is possible to program a certain number of outputs which can be activated or deactivated via keypad without entering a user code. For further details refer to *paragraph 4-24 Activating outputs without authentication.*

Timers

This section allows you to assign a timer to the code. The code will be operative only at the pre-set times.

Type

This section allows you to assign a level (rank) in the system hierarchy to the selected code.

The default level of code number 1 is "Master"; the default level of all the other codes is "User".

Note

Enable/disable

This section allows you to enable/disable access to the various sections of the User Menu.

For further details regarding the sections of the User Menu, refer to the User Manual.

The programming steps are identical to those of "Outputs ON/OFF".

Installer codes

4-11

This section allows you to program the functions of the 2 installer codes. The user code PINs must comprise 4, 5 or 6 digits.

Type in Code (Installer) , PROGRAMMING Installer code .

ChangeInst. PIN 1

For security reasons, you must change the PIN of the primary installer code (type-in twice). The PIN is "9999" at default.

ChangeInst. PIN 2

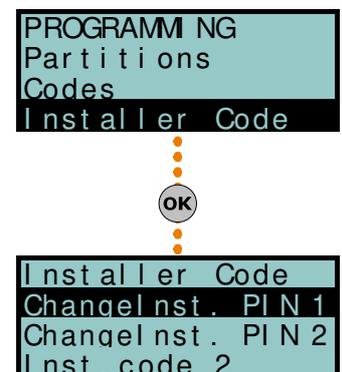
For security reasons, you must change the PIN of the secondary installer code (type-in twice). The PIN is "9998" at default.

Inst.code 2

Use keys and to enable/disable the sections of the installer menu the secondary installer code can access.

In this section, the secondary installer code can access the Installer code PIN 2 section only.

Note



Keys

4-12

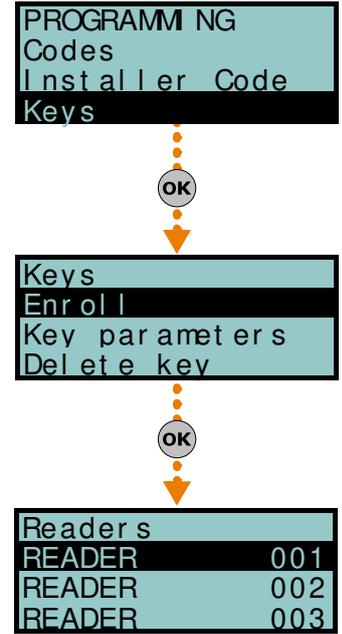
In this section it is possible to set the parameters of the keys and Air2 wireless control devices (for the remote control devices, please refer to the attached manual).

Type in code (Installer) **OK**, PROGRAMMING Keys **OK**.

Enroll

Each digital key and wireless keyfob must be enrolled separately on the system in order to allow it to operate. The enrolling procedure is as follows.

1. View the readers in the control panel configuration. Select the reader you wish to use for the enrollment of the key/s, then press **OK**. If you select a reader simulated by the Air2-BS200, a "W" will be shown at the end of the description.
2. Select the digital key you wish to enroll and press **OK**. If you are using an nBy reader, all the LEDs will begin to blink to indicate that it is ready to enroll the key.
3. The keypad will indicate the current description of the digital key concerned.
4. Hold the digital key in the vicinity of the reader and then move it away. For Air2-KF100 wireless keyfobs, press simultaneously keys 3 and 4.
5. The keypad will emit a beep to confirm that the digital key has been successfully enrolled. If you are using an nBy reader, the red LED will go On. The digital key description on the display will pass to the next key automatically. This method (from step 4.) allows you to enroll as many digital keys as the system requires.
6. Once you have completed the enrolling process, press **Esc** or **C**.



All the enrolled keys will be enabled to operate the system immediately.

Note

Key parameters

This section allows you to programme all the parameters of the selected digital key.

- **Description** - editable field for the name of the digital key user.
- **Partitions** - the partitions the digital key is assigned to and therefore can control.
- **Options** - activated by means of keys **[] *** and **[] #**, are:

Table 4-8: Key options

Option	If enabled	If disabled	
Patrol	The key will be a "Patrol" key.		
Maintenance	The key will be able to block outputs associated with alarm/tamper events for the time that it is held in the vicinity of a reader.		
Use keyShortcuts	If a digital key is held in the vicinity of a reader, only the digital key shortcuts will be indicated, and not the reader shortcuts.	If a digital key is held in the vicinity of a reader, only the reader shortcuts will be indicated and, if configured, the first shortcut programmed on the digital key.	These options do not apply to wireless keyfobs
DisarmNotAllowed	If a digital key is held in the vicinity of a reader when partitions are armed, the Disarm option will be inhibited (all LEDs Off).	If a digital key is held in the vicinity of a reader when partitions are armed, the Disarm option will be allowed (all LEDs Off).	

- **Timers** - this section allows you to associate a timer with the digital key. The key will be able to operate the system only when the associated timer is "On".
- **Shortcuts** - this section allows you to program up to 4 shortcuts (F1, F2, F3, F4) for each key.

The shortcut associated with the key can be one of the following types:

- None
- Arm/disarm
- Stop alarms
- Clear Call Queue
- Delete memory
- Activate Output
- Deactiv. outputs
- Overtime
- Teleservice req.
- Voice guide

If a digital key is held in the vicinity of an nBy reader, the LEDs will run through a series of visual signals with the following meanings:

Table 4-9: Readers - LED visualization

LED On sequence		Option: Use keyShortcuts	
		enabled	disabled
1	Red LED On	Key shortcut F1	shortcut associated with the red LED on the reader
2	Blue LED On	Key shortcut F2	shortcut associated with the blue LED on the reader
3	Green LED On	Key shortcut F3	shortcut associated with the green LED on the reader
4	Yellow LED On	Key shortcut F4	shortcut associated with the yellow LED on the reader
5	All LEDs On	This sequence does not occur	Key shortcut F1
6		Option: DisarmNotAllowed	
		enabled	disabled
		No request to arm all the partitions common to both the key and reader.	Request to disarm all the partitions common to both the key and reader.

Delete key

This section allows you to delete enrolled digital keys from the system configuration. The enrolled digital keys can be found in the list with the symbol.

1. Use keys and to select the enrolled digital keys you wish to delete.
2. Press to delete the selected digital key.
3. Press to confirm and exit.

Enable/disable

This section allows you to enable/disable the digital keys:

1. Use keys and to select the digital key you wish to enable/disable.
2. Use keys and to enable/disable the selected digital key.
3. Press to confirm and exit.

Arming scenarios

4-13

This section allows you to configure up to different 30 arming scenarios.

1. Access "Arming scenarios" section.

Type in code (Installer) , PROGRAMMING Arming scenarios .

2. Use keys and to select the scenario then press .

Description

Editable field for the description of the scenario.

Icon

This section allows you to select the icon you wish to assign to the scenario, simply by indicating the icon number (refer to *Appendix A, Shortcuts by default*):

1. Use keys and to scroll across the digits.
2. Use the number keys (, etc.) to edit the number.
3. Press to confirm and exit.

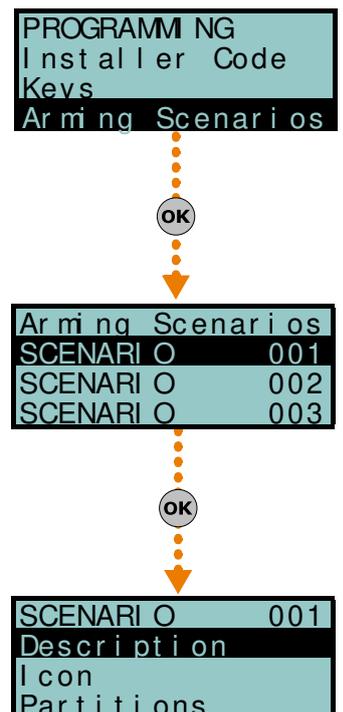
The "Arm" shortcut associated with function key , ... , will visualize the icon selected in this section.

Partitions

This section allows you to configure the scenarios of all the partitions managed by the various models.

1. Use keys and to select the partition, then press .
2. Use keys and to select the operating mode (Away, Stay, Disarm, etc.).

- **None** - the current operating mode of the partition will not be changed.
- **Away** - the partition will arm in Away mode (interior and perimeter).



- **Stay** - the partition will arm in Stay mode (perimeter only).
- **Instant** - the partition will arm in Instant mode (perimeter only with zero delay).
- **Disarm** - the partition will disarm.

Output

Each scenario, when applied, can activate one output (via keypad, at reader, over-the-phone, etc.). Use  and  to select the output then press .

It is possible to use a scenario to activate an output. This can be done through the Scenarios section by simply leaving the respective "Partition" programming fields free (None), thus allowing the association of the Icons with the outputs.

3. Press  to confirm and exit.

Note

Shortcuts

4-14

This section allows you to setup all of the available shortcuts.

1. Accessing the "Shortcuts" section:

Type in code (Installer) , PROGRAMMING Shortcuts .

2. Use keys  and  to select the shortcut then press .

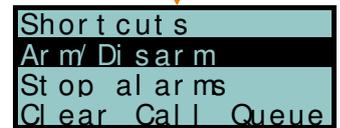
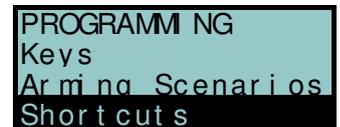
Description

This is the editable label which identifies the shortcut.

Icon

This section allows you to select the icon you wish to represent the scenario, simply by indicating the icon number (refer to *Appendix A, Shortcuts by default*):

1. Use keys  and  to scroll across the digits of the number.
2. Use the number keys (, etc.) to edit the number.
3. Press  to confirm and exit.



Expansions

4-15

This section allows you to programme the parameters of the expansions.

Type in code (Installer) , PROGRAMMING Expansions .

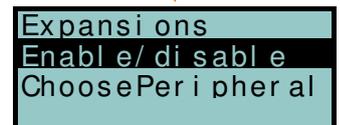
Enable/disable

This section allows you to add/remove expansions from the I-BUS configuration, by means of keys  and .

ChoosePeripheral

This section allows you to select an expansion and program the descriptions and the options:

- **Description** - editable field for the name of the expansion.
- **Options** - keys  and  allow you to enable activation of the expansion buzzer on activation of terminal 1 configured as an output.



Keypads

4-16

This section in the installer menu allows you to program the parameters of the keypads. Not all the keypad parameters can be accessed via the installer menu. Depending on the type of keypad or programming process, it may be necessary to use the SmartLeague software program or, in the case of Alien keypads, access the appropriate section of the keypad functions.

Type in code (Installer) **OK**, PROGRAMMING Keypads **OK**.

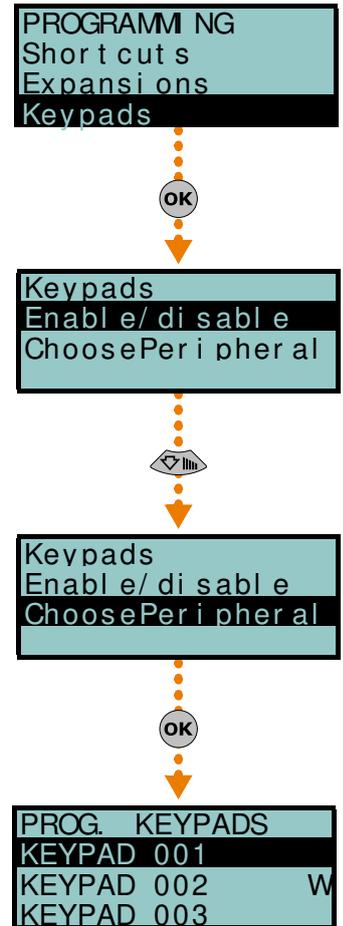
Enable/disable

This section allows you to add/remove expansions from the I-BUS configuration, by means of keys **[*]** and **[#]**.

ChoosePeripheral

This section allows you to program the various options of the selected keypad.

- **Wireless** - This section allows you to start the enrolling process of the wireless keypad (future use)
- **Temp. hysteresis.** - this parameter allows you to enter the hysteresis value for the "Air conditioning" function on the selected keypad (if enabled). The entered value must be expressed in °C decimals (from a minimum of 0 to a maximum of 4).
- **Description** - editable field for the name of the digital key user.
- **Partitions** - use **[*]** and **[#]** to enable/disable the keypad on the system partitions.
- **Options:**
 - **Temperature off** - if this option is enabled, the room temperature will be flashed in alternation on the display. This option is valid for keypads with built-in temperature sensors only.
 - **SilentExitTime** - enables/disables the buzzer during partition Exit Time.
 - **SilentEntryTime** - enables/disables the buzzer during partition Entry time
 - **SignalExitTime** - enables/disables the buzzer when terminal T1 on the keypad is activated as an output.
 - **Disable bell** - enable/disable the buzzer that signals violation of the bell zone relative to the keypad in question.
 - **LED Off in standby** - if enabled, this option switches of the relative LEDs after at least 40 seconds of inactivity on the keypad.
 - **NO Superv. WLS** - If enabled, this option inhibits fault signalling in the event of loss of wireless devices. This option is co-related to the control panel parameter "Wireless Superv." (refer to *paragraph 4-23 Other parameters*).
 - **Disable tamp. WLS** - If this option is disabled, open/dislodgement tamper on Air2 devices will not generate the respective events.
- **F1/4KeyShortcuts** - setting of the shortcuts assigned to keys **[F1 Fn]**, ..., **[F4 P00]**. If you are programming an Alien keypad, this shortcut refers to the position in the list available in the "Scenarios" section of the Alien keypad you are working on. Function keys F1 to F12 must be selected separately and programmed as follows:
 - **Type** - this is the shortcut action which can be selected from those available (refer to *Appendix A, Shortcuts by default*). It is necessary to programme an extra parameter for some shortcuts:
 - "Arm/disarm", this parameter refers to one of the 30 scenarios
 - "Activate outputs", this parameter refers to the output that will be deactivated
 - "Deactiv. outputs", this parameter refers to the output that will be deactivated



The "Listen-in" and "Arming status" will have no effect if the respective command is entered at a keypad. If you are programming an Alien keypad, the only type of shortcut that functions is "Arm/disarm".

Note

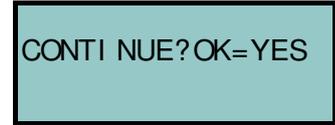
- **Options** - activated by means of keys **[*]** and **[#]**, are:
 - **Requires code** - if enabled, the system will ask for user-code entry before activating the shortcut. If the system recognizes the entered user code, it will activate the shortcut command.
 - **SecurityRiskCode** - if you enable this option, you must also enable the "Requires code" option. When this option is enabled and the selected shortcut involves a scenario that completely disarms a partition, or switches

a partition from Away mode to Stay mode, the security of your system will obviously be at risk, therefore, the system will request code entry.

- **Confirm** - if enabled, the system will ask the user for confirmation (press **OK**) before activating the function-key shortcut. This method draws the users attention to requested operations that do not require codes, and thus avoids accidental arm/disarm operations, etc.

This option is not available for Alien keypads.

It is possible to program a certain number of outputs which can be activated or deactivated via keypad without entering a user code. For further details refer to *paragraph 4-24 Activating outputs without authentication.*



Via Alien keypad

Access the "Settings" section by tapping the button , type-in a valid user code in order to access the "Alien" section.

The complete description of the parameters in this section can be found in the user manual.

Readers

4-17

This section allows you to programme the reader options.

Type in code (Installer) **OK**, PROGRAMMING Readers **OK**.

Enable/disable

This section allows you to add/remove readers to the I-BUS configuration, by means of keys  and .

If it is a reader simulated by the Air2-BS200, a "W" will be shown at the end of the description.

ChoosePeripheral

This section allows you to program the various options of the selected reader.

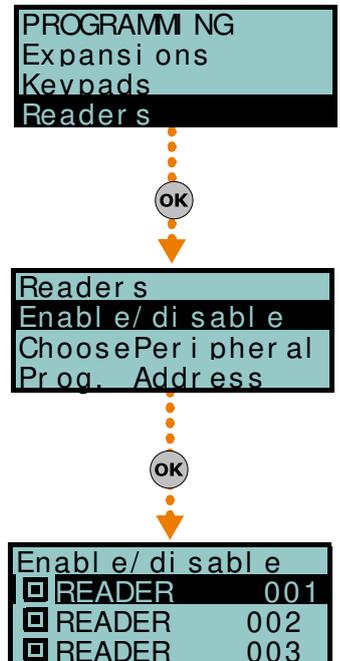
- **Description** - editable field for the name of the digital key user.
- **Partitions** - use  or  to enable/disable the reader on the system partitions.
- **Shortcuts** - this section allows you to programme the shortcuts associated with the 4 differently-coloured LEDs on the reader. In order:
 - Red LED shortcut
 - Blue LED shortcut
 - Green LED shortcut
 - Yellow LED shortcut

The shortcut associated with the LED can be one of the following types:

- None
- Arm/Disarm
- Stop alarms
- Clear call queue
- Delete memory
- Activate Output
- Deactiv. output
- Overtime
- Teleservice req.
- View faults

Prog. Address

This section allows you to activate the address programming phase for the nBy readers.



Sounders/Flashers

4-18

This section allows you to programme the parameters of the sounders connected to the I-BUS and enroll wireless sounderflashes.

Wireless sounders can be programmed via the SmartLeague software programme only.

Type in code (Installer) , PROGRAMMING Sounders .

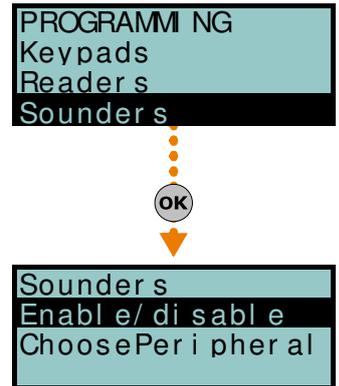
Enable/disable

This section allows you to add/remove sounders from the I-BUS configuration, by means of keys  and .

ChoosePeripheral

This section allows you to programme the various options of the selected sounder.

- **Wireless** - this section allows you to start the enrolling process of the wireless keypad.
- **Description** - editable field for the name of the sounder.

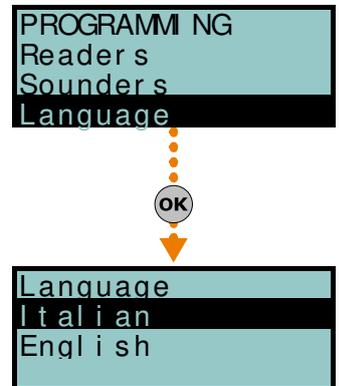


Language

4-19

This option allows you to select the language the system uses in the User and Installer menus for the descriptions of events, faults, etc. However, the edited descriptions of the various system elements such as: zone, partitions, outputs, codes, descriptions will remain unchanged.

Use keys  and  to select the desired language and  to confirm.



Messages

4-20

This section allows you to record (and playback) all the voice messages. The Table in the Appendix shows all the pre-recorded messages provided by the SmartLogos30M voice board.

1. Accessing the "Messages" section:

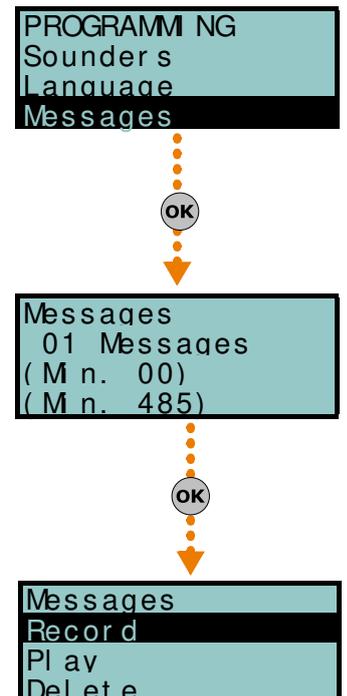
Type in code (Installer) , PROGRAMMING Messages .

2. Use keys  and  to select the field you wish to change, then use the number keys (, etc.) to edit the number.

or

Use keys  and  to increase or decrease the number.

3. Press .
4. Use keys  and  to select the instructions for the selected message then press .



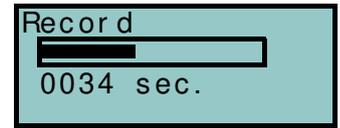
Record

Before recording a voice message, you must first select:

- **No Message** - no recording or playback
- **High quality** - for superior recording/playback quality
- **Average quality** - for good recording/playback quality (similar to phone-line quality).

High quality messages occupy twice the memory space of average quality messages of the same length.

The recording will start when **OK** is pressed, the running recording time (seconds) will be indicated by a second-counter on the keypad display. If you wish to interrupt the record/playback operation manually press **OK**, otherwise, it will end automatically when the pre-set time-out expires.



Play

Message playback section. You can adjust the volume during the playback phase using keys and .

Delete

Delete message section. The control panel will ask for confirmation before deleting the message, by means of the **OK** key.

Default settings

This section allows you to reset to default settings all the control panel parameters, auto-learn zone balancing values, auto-enroll I-BUS peripherals and restore the event codes of CONTACT-ID reporting format.

Reset to factory default can be carried out at a keypad via the installer menu (details follow), or via the control panel PCB, using the following procedure.

1. Disconnect all power to the control panel (mains 230V~ and backup battery).
2. Short-circuit terminals "2" and "3" of the serial cable connector.
3. Power-up the control panel and maintain the short-circuit condition on terminals "2" and "3" for at least 5 seconds.
4. Restore the short-circuit condition.

Within 70 seconds the control panel will reset to default settings, re-enroll all the peripherals currently on the I-BUS and, if a keypad is connected, will ask you to select the Language.

Reset to factory default will not clear the events log.

1. Access the "Default settings" section:

Type in code (Installer) **OK**, PROGRAMMING Default settings **OK**.

2. Use keys and to select the function then press **OK**:

Factory data

If you select this option, the control panel will reset entirely to default settings.

ATTENTION!

Reset of the factory default programming data deletes all the previously programmed parameter settings.

Learn zone bal.

If you select this option, the control panel will learn (save to memory) automatically all the balancing settings of all the zones (**Patent Pending**).

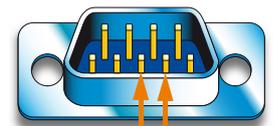
The zone-balancing options are:

- Normally Open
- Normally Closed
- Balancing (Single balancing)
- Double balancing
- Roller blind with EOL

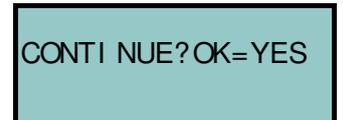
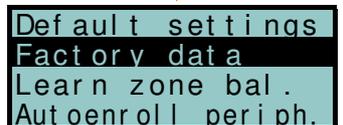
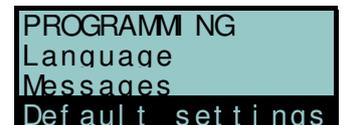
The balancing settings which are not acquired accurately are:

4-21

Serial port



Terminals to be short-circuited



- Roller blind without EOL (which is classified as a normally-closed generic zone)
- Double zone without EOL (which is classified as a normally-closed generic zone)
- Double zone with EOL (which is classified as a generic zone with Double balancing)

In order to allow accurate acquisition of the balancing settings of all the zones, you must:

- Wire and select the balancing settings of all the zones.
- Ensure, as far as possible, that all the zones are in stand-by status
- Activate the "Learn zone bal." option.
- Verify that the operation has been carried properly and that all the settings are accurate (if any zones are not in standby status during this process their settings will not be acquired accurately).
- Set manually any inaccurate zone balancing settings.

Autoenroll periph.

If you select this option, the control panel will enroll automatically all the peripherals it finds on the I-BUS.

CONTACTIDDefault

If you select this option, the control panel will reset to default settings all the event codes used for the CONTACT-ID reporting format.

CONT-ID enumer.

If you select this option, the control panel (after requesting confirmation) will implement incremental numbering (from "1") in the "CCC" field of the CONTACT-ID protocol for the events relative to the zone.

SIA defaults

If you select this option, the control panel (after confirmation) will reset all the factory default settings on SIA parameters of all events.

DeletePrg.events

Press the  key to delete all the events saved to the control panel events log (activation and restoral events):

- all outputs
- all calls
- all options

WLS data reset

Press the  key to delete all the data relating to the Air2-BS200 device.

The data relating to the detectors and wireless keyfobs will not be deleted, nor will the devices simulated by the Air2-BS100 transceiver be deleted from the configuration.

Note

3. The control panel will ask for confirmation of this command (press .

User functions

4-22

This section describes the functions the installer has in common with the user.

1. Access the "User functions" section:

Type in code (Installer) , PROGRAMMING User functions .

2. Use keys  and  to select the function then press .

Activations

This section provides information regarding the "Cloud enrollment" option which allows the SmartLiving panel to access INIM Electronics cloud service.

View

- **Events log** - allows you to view all the events saved to the log.
- **Alarms log** - allows you to view all the events relating to zone/partition alarm and tamper saved to the log.
- **Faults log** - allows you to view all the fault events saved to the log.
- **Arm/Disarm ops.** - allows you to view all the arm/disarm operations saved to the log.

Use key or to scroll the chronological events list. For some events, key allows you to view the partitions details. For example, the details of an "Arm" command will show the code and keypad concerned and, if you press , the list of partitions involved.

- **Nexus status** - allows you to view (on the display) the following parameters of the Nexus device:
 - 1st line: Mobile network provider (on the left side)
 - "--" means that the Nexus is connected to the BUS
 - "C" means that data transfer is in progress
 - data network technology (on the right side)
 - G, GPRS service
 - H, HSPA service
 - 4G, LTE service
 - 2nd line: GSM signal reception (value between 1 and 100)
 - 3rd line: Credit balance, at the last operation (expressed in the local currency)
 - 4th line: Faults present, in this case it is necessary to access the "View-Faults" section for details.
- **System voltage** - allows you to view the voltage the system uses.
- **Zone status** - allows you to view the status of all the zones. Use keys and to scroll the list of accessible zones. The display shows the following zone parameters:
 - 1st line: zone description
 - 2nd line: zone status ("Standby", "Alarm", "Short", "Tamper"), its activation status ("unbypassed" - capable of generating alarms, or "bypassed" - incapable of generating alarms)
 - 3rd line: various indications depending on the device type:
 - wired zone; resistance value reading expressed Ohm
 - wireless zone; wireless signal reception level
 - level of smoke present in the smoke detection chamber of the Air2-FD100 smoke detector, expressed in mdB/m
 - 4th line: level of contamination present in the smoke detection chamber of Air2-FD100 smoke detector (%)

It is advisable to clean the detector when the value exceeds 90%.

- **Faults ongoing** - allows the viewing of any ongoing faults.
- **Panel version** - allows you to view the firmware version and model of the SmartLiving control panel.

Outputs ON/OFF

Allows manual activation/deactivation of the outputs by means of keys and .

Set date/time

Allows you to set the date and time of the control panel.

1. Use key or to select the programming field you wish to change (hour, minutes, etc.).
2. Use keys and to change the selected field.
3. Press to save and exit.

Other parameters

This option allows you to programme the advanced functions of the control panel.

1. Access the "Other parameters" section.

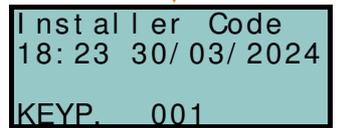
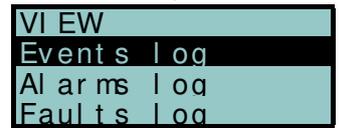
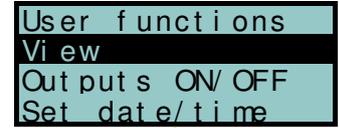
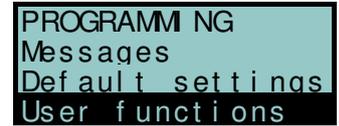
Type in code (Installer) , PROGRAMMING Other parameters .

2. Use keys and to select the parameter then press .

Periodic ev.

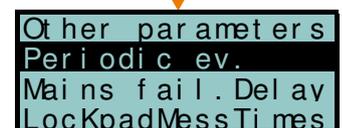
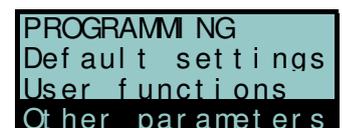
This options allows you to select one of the four periodic events and set the respective parameters.

- **Time per. Event** - this parameter allows you to set the time (hh/mm), day, month and year of the first "Periodic event" (refer to *paragraph 4-7 Events*).



Note

4-23



The time/date setting of this parameter must be later than the control panel clock setting.

Note

- **PeriodicInterval** - this parameter allows you to set the interval between each "Periodic events" (expressed in hours). To disable the "Periodic event", set "0".
- **Options:**
 - **Per.Ev Continuous** - if enabled, the system will generate the corresponding periodic event regardless of its initial date/time. The event will be generated when the programming session is exited, or when the system starts up, and will be generated continuously when the set period expires.
 - **PeriodicEv InMin** - if enabled, the interval (period of time) between two consecutive activations ("Period.Ev.Time") will be established in minutes and not hours.

Mains fail.Delay

This parameter allows you to program the delay, expressed in minutes (see note), between actual mains failure and the "Mains failure" fault event signal.

LockpadMessTimes

The number of times voice messages, relating to events recorded at the keypad, will be played (only for keypads with voice functions).

The playback phase can be stopped by pressing any key. If you set a value of "255" the playback can be stopped by pressing any key, this is the only method of stopping playback.

OverThePhoneVol.

This is the volume of the voice messages over-the-phone.

Ring sensitivity

This value determines the reception sensitivity of incoming call rings. This option is useful in situations of bad reception (break up) or noisy lines.

At default this value is set at 60. Accepted values: 1 to 120.

Wireless superv.

This value determines the wireless-device supervision time. Once the pre-set time expires, the devices which do not respond will be signaled as lost. Accepted values: 12 to 250 minutes (30 minutes at default).

Tel. input gain

This value determines the volume of the incoming call signal. This option is useful in situations which require better comprehension of DTMF tones and improvement of teleservice intervention via modem.

Adj. temperature

This parameter will allow you to enter the effective value of the room temperature read by an external thermometer. This value will replace the keypad temperature reading and thus allow you to correct the temperature sensor on the keypad you are working on (valid for keypads with temperature sensors only).

The entered value must be expressed in °C decimals (for example, type in 252 if the temperature is 25.2 °C).

LowBattery delay

This parameter allows you to programme the delay, expressed in minutes, which will be applied before "LowBattery" events will be signalled.

LinedownDelay

This parameter allows you to programme the delay, expressed in seconds or minutes, which will be applied before "LineDown" events will be signalled.

All the above-mentioned parameters can be programmed as follows.

- Use keys and to select the field you wish to change, then use the number keys (, etc.) to edit the number.

or

Use keys and to increase or decrease the number.

FaultForNotReady

This section allows you to select which events, other than zones in alarm status, will be signaled as system security-risk conditions when the partition arms.

Following are the events which can be enabled/disabled by means of keys and :

#:

- Zone fuse fault
- IBUS fuse fault

If this value is expressed in minutes, there is an error margin of 1 minute (for example, if you set 5 minutes, the period can vary between 4 and 5 minutes).

```

Over ThePhoneVol .
00 Units
(M n. 010)
(Max. 100)
```

```

Tel. input gain
00 Units
(M n. 001)
(Max. 120)
```

If this value is expressed in minutes, there is an error margin of 4 minutes (for example, if you set 7 minutes, the period can vary between 3 and 7 minutes).

- Low battery
- Mains failure
- Tel. line down
- Jamming
- Low battery WLS
- WLS zone loss
- Nexus fault
- Detector dusty
- Faults on zones
- Sounder faults
- Power faults
- Keypad faults
- LossTamp.ongoing

The last item groups the following events:

- Control panel open
- Dislodged panel
- Expansion tamper
- Keypad tamper
- Reader tamper
- Sound.flash.Tamp
- Nexus tamper
- Expansion loss
- Keypad loss
- Reader loss
- Sound.flash.Loss
- Nexus Nexus
- Nexus LIVPWR100
- IP conn. lost

4. Press **OK** to confirm and exit.

Serial number

Section for the visualization of the Control panel serial number.

Telephone line adjustment 4-23-1

The "OverThePhoneVol." and "Tel. input gain" parameters can be used to correct the voice functions of the dialer and the DTMF tones. The values of these parameters affect each other, therefore, and a good result is always a compromise.

If you are not using a GSM interface, you should:

- Adjust one parameter at a time and carry out tests to verify the result.
- Increase/decrease the values in small steps (for example, from 25 to 22 and not from 25 to 15).
- If the DTMF tones are not recognized, or are recognized with difficulty, decrease the value of the "Volume Tel.voice" parameter (in small steps of 2 or 3 units) and verify the effect. If there is no improvement, increase the value of the "VolumeTel. In." parameter until an acceptable level is achieved.
Do not increase the "VolumeTel. In" parameter excessively, as an excessive value may cause incorrect interpretation of DTMF tones.
- If the volume of the telephone messages is low, increase the "Volume Tel.voice" (in small steps of 1 or 2 units) and verify the effect. An excessive value of the "Volume Tel.voice." parameter may cause incorrect interpretation of DTMF tones.

In most cases, the value of the "Volume Tel.voice" parameter is between 15 and 25, whereas, the value of the "VolumeTel. In." parameter is between 20 and 30.

If there is a SmartLinkAdv GSM interface, it is possible to adjust the values of incoming and of the output volume parameters of the SmartLinkAdv.

Any changes to the value of the SmartLinkAdv incoming volume parameter come into effect almost 2 minutes after the setting change, therefore, you must allow this time to pass before verifying the effect.

Note

Activating outputs without authentication

4-24

It is possible to programme a certain number of outputs which can be viewed and activated at the keypad without authentication (i.e. without entering a user code).

Access to these outputs depends on the type of keypad in use:

- for keypads with keys, you must activate the "Output control" shortcut (shortcut n. 21: associated with one of the **F1**, ..., **F4**
- for Alien keypads, you must access the "Commands" section by tapping the button, then the "Domotics" section.

The outputs that can be activated from a keypad with the "NNN" address will be those associated with a specific user code.

The keypad, code and relative outputs must be programmed in accordance with the following procedure:

- Access the section of the Installer menu for the programming of the "NNN" keypad you wish to associate with the outputs:

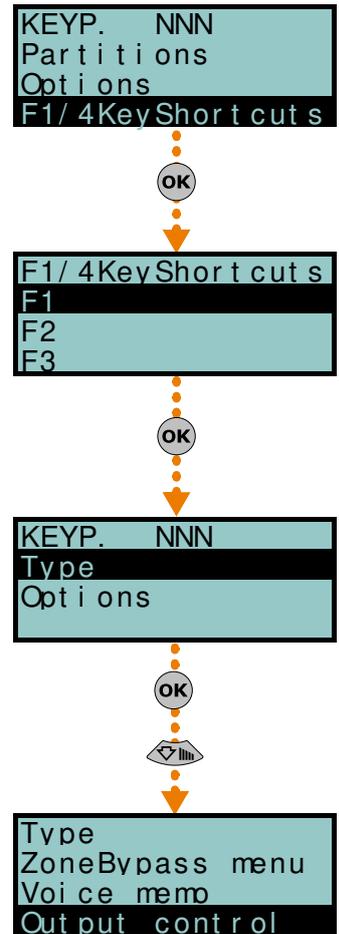
Type in code (Installer) , PROGRAMMING Keypads , ChoosePeripheral , "NNN" Keypad

- Access the "F1/4KeyShortcuts" section and select a function key
- Access the "Type" section and associate the selected function key with the "Output control" shortcut.
- DO NOT ENABLE the "Requires code" option for the shortcut associated with the function key undergoing programming.
- Go back to the installer menu and access the "Codes" section.
- Select the user code shown in the table in accordance with the control panel model undergoing programming:

Table 4-10: User code number

Keypad number	SmartLiving Model		
	505, 515	1050	10100
001	026	041	086
002	027	042	087
003	028	043	088
004	029	044	089
005	030	045	090
006	/	046	091
007	/	047	092
008	/	048	093
009	/	049	094
010	/	050	095
011	/		096
012	/		097
013	/		098
014	/		099
015	/		100

- Access programming of the selected code, at the "Assigned outputs" section.
- Use keys and to select the outputs from those available on the list.



Chapter 5

PROGRAMMING VIA THE SMARTLEAGUE SOFTWARE

Keypads 5-1

Parts of the system	Programming section		
<ul style="list-style-type: none"> + Keypads + Proximity readers + Expansions + Sounders - Nexus - SmartLiving System 	The Keypad option, from the system tree on the left, allows you to configure, via the Programming section, all the parameters which are common to all the keypads.		
	Group	Option	
	Keypad parameters	Wrong PIN keypad lockout	If a wrong code is typed-in at a keypad more than 5 times in succession, the keypad will lock for 10 minutes. The count restarts from 10 minutes in the case of control panel reset or entry into programming.
		View open zones	The keypad will show the descriptions of any zones not in standby status when the partitions disarm. Any auto-bypassable zones will be shown in negative.
		Show scenario	The second line on the keypad display, on the left side, will show the description of the active scenario.
		Message repetitions on voice keypad	Number of playbacks of event voice messages. The playback phase can be stopped by pressing any button.
Press key to end playback		If this option is enabled, message playback can be interrupted solely by pressing any button.	

Click on the node of the **Keypads** option to access a list of all the keypads in the system configuration. Select the required keypad to view and program its parameters.

Node	Group	Option	
<ul style="list-style-type: none"> Keypads (2) <ul style="list-style-type: none"> Keyp. 001 (1) Keyp. 002 (2) 	Description	Description/Name of the keypad (to be customized by the installer).	
	Keypad type	Checkbox for the selection of the keypad type: <ul style="list-style-type: none"> • Keypad with display and keys • Touch-screen keypad • Wireless keypad 	
	General / Partitions	Section for the selection of the partitions the keypad can operate on.	
	General / Details	Shortcut	For each key, from F1 to F12, it is possible to program the type of shortcut selectable from among all the available shortcuts. When programming an Alien keypad, positions F1 - F12 refer to the positions in the list available in the 'Scenarios' section of the Alien keypad you are working on.
		Shortcut parameter	It is necessary to specify a further parameter for each shortcut: <ul style="list-style-type: none"> • Arm/Disarm - this parameter refers to one of the 30 scenarios • Activate output - this parameter involves an output • Deactiv. output - this parameter involves an output • Panic - this parameter will be one of the 15 panic events

General / Details	Options	<ul style="list-style-type: none"> • Requires code - if enabled, the system will ask for user-code entry before activating the shortcut. If the system recognizes the entered user code, it will activate the shortcut command. • Code entry in the event security risk - when this option is enabled and the selected shortcut involves a scenario that completely disarms a partition, or switches a partition from Away mode to Stay mode, the security of your system will obviously be at risk, therefore, the system will request code entry. • Requires confirm - if enabled, the system will ask the user for confirmation (press button) before activating the selected function-key shortcut. This method draws the users attention to requested operations that do not require codes, and thus avoids accidental arm/disarm operations, etc.
	Temperature hysteresis	Programming field for the value of the hysteresis for the "Air conditioning" function of the selected keypad (if enabled). The entered value must be expressed in °C decimals (from a minimum of 0 to a maximum of 4).
	Disable temperature reading	If this option is enabled, the room temperature will not be flashed on the display. This option will take effect if programmed on a keypad with voice functions.
	Disable audible entry-time signal	This option enables/disables the buzzer during partition entry-time
	Disable exit-time signal	This option enables/disables the buzzer during partition exit-time
	Audible signal on terminal T1 output	This option enables/disables the buzzer when the keypad terminal T1 is activated as an output.
	LED OFF in standby	If enabled, in the event of at least 40 seconds inactivity on the keypad, the respective LEDs will switch off.
	Bypass wireless supervision	If enabled, this option inhibits the monitoring function the control panel must perform on the wireless keypad.
	Bypass tamper	If enabled, this option inhibits signalling on the control panel of wireless keypad tamper.
Alien Graphics	This section appears only when "Touch-screen" is selected in the keypad type. In order to program the following parameters, your computer must be connected to the USB port of the keypad.	
	Communication port	This option allows selection of the connection port to the Alien keypad from those found by the PC.
	Refresh	Button for the connection upgrades found by the PC.
	Model	Checkbox for the selection of the Alien keypad.
	Available Skin	Selection of themes available for the Alien graphic interface.
	Background	Button for the visualization of the image background in the Alien user face graphics section.
	All	Button for the visualization of the image background in the Alien user face graphics section complete with buttons.
	Default	Button for the visualization of the selected default skin in the Alien user face graphics section.
	Clean	Button to clear the selected graphics.
	Write skin	Button to set the selected skin on the keypad.
	Write icons	Button to set the icons selected for the buttons on the keypad.
Image	<p>Visualization of the graphics selected for the Alien keypad. You can load an image from the PC by double-clicking on the background or button icons.</p> <p>The image requirements depend on the device model:</p> <ul style="list-style-type: none"> • Alien/S skin: <ul style="list-style-type: none"> - the background file must be a .jpg file with a maximum size of 120 kbytes, 480x272 pixels - each of the 8 main buttons must be a .jpg file with a maximum size of 12 kbytes, 109x88 pixels • Alien/G skin: <ul style="list-style-type: none"> - the background file must be a .jpg file with a maximum size of 120 kbytes, 800x480 pixels - each of the 8 main buttons must be a .jpg file with a maximum size of 12 kbytes, 109x88 pixels 	
Alien Maps	This section appears only when "Touch-screen" is selected in the keypad type. For the programming instructions relating to the graphic maps refer to <i>Chapter 7 - Graphic map configuration</i> .	
Monitoring wireless	This section appears only when "Wireless keypad" is selected in the keypad type. Pressing the Start button starts monitoring on the variation of the signal transmitted by the device and background noise detected over time.	

The process of programming the graphic interface and maps on the Alien keypad must be done through the SmartLeague software program. **ALIEN**

Once you have selected the keypad from the system tree menu on the left, select "Touch keypad" as type of keypad. The "General" section, which is the same for all keypad types, appears with the following sections:

- "Alien graphics", for the graphic interface setup (backgrounds, buttons, icons)
- "Alien maps", for the configuration of the graphic maps accessed by means of the key in the "Maps" section of the "APPs".

In order to configure the modified parameters on the keypad, it is necessary to have a link between the PC to the USB port of the keypad.

Proximity readers 5-2

Parts of the system	Programming section	
	The Proximity readers option, from the system tree on the left, allows you to configure, via the Programming section, all the parameters which are common to all the readers.	
	Group	Option
	Reader parameters	Reader Buzzers OFF No reader buzzers will emit audible signals when the entry time, exit time, output time or pre-arm time is running.
	Proximity reader address configuration	Section for the programming of the proximity reader addresses. Firstly, place the control panel in Service status, click on Proximity reader address configuration option then, holding the nKey device in the vicinity of the reader, select the required address. At the end of the operation, click on the End proximity reader address configuration .
	Address LED codes	Section for the visualization of how the addresses will be reproduced on the LEDs.

Click on the node of the **Proximity readers** option to open a list of all the readers in the system configuration. Select the required reader to view and program its parameters.

Node	Group	Option	
	Description	This is the name used to identify the reader, customizable by the installer.	
	Partitions	Section for the selection of the partitions the reader can operate on.	
	Shortcut	Type	It is possible to assign a shortcut type, selectable from those available, to each of the LEDs
		Option	It is necessary to specify a further parameter for each shortcut: <ul style="list-style-type: none"> • Arm/Disarm - this parameter refers to one of the 30 scenarios • Activate output - this parameter involves an output • Deactiv. output - this parameter involves an output • Panic - this parameter will be one of the 15 panic events

Expansions 5-3

Parts of the system	Programming section	
	Clicking on the node corresponding to the Expansions options a list of all the expansions in the configuration.	
	Description	Edit field for the description of the selected expansion.
	Sound on output	This option that enables/disables the buzzer of the selected expansion when the relevant T1 terminal is activated as an output.

Sounder/flashers 5-4

Parts of the system	Programming section		
<ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions <li style="background-color: #00a0e3; color: white;">⊕ Sounder/flashers ⊕ Nexus ⊕ SmartLiving System 	<p>The Sounder option, from the system tree on the left, allows you to program the patterns in the Programming section.</p> <p>8 modifiable patterns are available. The button allows you to reset the patterns to default.</p>		
	Group	Option	
	Description	<ul style="list-style-type: none"> Burglary Burglary volume low Fire Tamper Pre-alarm Automation Squawk Chime 	Selection menu of the pattern to be programmed.
	Tone	This is the audible signal the sounder will emit. To be selected from the 5 available tones.	
	Time	This is the sounder activation time, expressed in seconds (from 1 to 127) or minutes (from 1 to 127).	
	Volume	Sound level of the sounder/flasher.	
	Flash type	<ul style="list-style-type: none"> 36 flash/min 46 flash/min 56 flash/min ON solid 	Checkbox for the selection of the flash rate (number of flashes per minute).
	Time	This is the flasher activation time, expressed in seconds (from 1 to 127) or minutes (from 1 to 127). If the event that activates the flasher continuously is a zone alarm, terminal tamper, partition alarm or partition tamper, the flasher will also be switched off by memory reset.	
	Activate sounder	Enable/Disable sounder activation	
	Activate flasher	Enable/Disable flasher activation	
	Activate STATUS LED	Enable/Disable activation of the STATUS LED	
	Activate PRG LED	Enable/Disable activation of PRG LED	
	Activate TAMPER output	Enable/Disable activation of TAMPER output	
	Activate FAULT output	Enable/Disable activation of FAULT output	
	Test	Buttons to start and stop a test on the pattern selected via the audio output of the PC in use and the image of the sounder/flasher on the left of the buttons.	
Stop			
Test sounder/flasher pattern	Test	Buttons to start and stop a test on the selected pattern on the sounder/flasher selected from the list provided. This test requires an active connection with the control panel.	
	Stop		

Clicking on the node relating to the **Sounder** option provides a list of all the sounders in the system configuration, both Ivy sounders connected to the control panel via the I-BUS and Hedera wireless sounders. Selection of one of these options will allow you to set up the parameters of the selected sounder.

Node	Group	Option	
<ul style="list-style-type: none"> ⊕ Sounder (2) <ul style="list-style-type: none"> <li style="background-color: #00a0e3; color: white;">Sounder 001 (1) Sounder 002 (2) 	Description	Description string of the sounder/flasher (customizable by the installer).	
	Events	Button to open a window containing a list of the events which activate the sounder.	
	Wireless	Check box for the assignment of the "Wireless" attribute to the selected sounder. If enabled, an Enroll will appear and you will be able to start the procedure for the enrollment of the wireless sounder.	
	Real-time (via cable)	Clicking on the Real-time option displays the following real-time values of the sounder:	
		Battery voltage	Voltage of the internal battery of the sounder/flasher.
		Line voltage	Voltage detected on terminals 1 and 2 of the sounder.
Temperature		Internal temperature of the sounder detected by the thermal probe.	
Foam left/right		Values detected by the anti-foam sensor (left/right).	
Tamper	Value detected by the open-panel tamper sensor.		

Real-time (wireless)	Pressing the Start button initiates a 4 minute countdown during which the values of the following features of the wireless sounder will be shown:	
	Level / foam threshold Level / tamper threshold	From the bars it is possible to read the values (from 1 to 100) detected by the antifoam and tamper sensors. You can adjust the alarm threshold by means of the programming fields at the side. The Default button resets the values to the factory settings.
	Monitoring wireless sounder	This section allows viewing of the sounder/flasher status (<i>paragraph 6-7 Hedera wireless sounder</i>).
Sounder parameters (via cable)	Read sounder	By clicking-on the Read sounder and Write sounder buttons it will be possible to program the sounder parameters.
	Write sounder	
	Default	Button to reset the factory default data
	I-BUS loss signal delay	This is the time the sounder/flasher must wait before signalling the loss of the I-BUS signal (expressed in minutes).
	Version	This is the firmware version of the sounder/flasher board.
	Sounder/Flasher address	Checkbox for the selection of the address of the sounder/flasher on the BUS.
	I-BUS loss Activation of LED input Power failure Open cover signalling Foam tamper signalling Blow-torch tamper signalling Horn fault Battery status	The check boxes in this section allow the association of one or more signals to each of the sounder/flasher events. The available signals are aligned with the wording of each event: <ul style="list-style-type: none"> • FAULT output • TAMPER output • STATUS LED • PRG LED • Flasher • Sounder
	Audible signalling	Selection of the type of sound produced by the magnetodynamic horn.
	Maximum sound (audible signal) time	This is the maximum time the sounder/flasher is allowed to emit the audible signal, however, the visual signals will continue until the device resets.
	STATUS LED ON	If this option is enabled, the STATUS LED will switch On solid.
	Flashes/minute	Selects the flash rate on the flasher.
	Enable flasher LED input	Option to allow blinking on the STATUS LED and PRG LED activated by the LED input.
	Monitor IBUS	If enabled, after each control panel reset, the BUS will be monitored for one minute and its status will be signalled on the PRG LED: <ul style="list-style-type: none"> • On solid - BUS not connected • 1 flash per second - BUS connected but sounder not enrolled • 2 flashes per second - BUS connected and sounder/flasher enrolled
	TAMPER and FAULT outputs	This option allows the selection of the type of contact (normally open or closed) of the outputs during stand-by status.
Sounder parameters (wireless)	Communication loss signalling	By means of a checkbox it is possible to select exactly when the sounder/flasher is to be activated if communication loss with the control panel occurs: <ul style="list-style-type: none"> • never • only when wireless jamming disturbs communication • each time communication is lost In the latter two cases it is necessary to indicate the "Wireless supervision time" , expressed in minutes, after which if communication is still absent the sounder/flasher will activate. The activation type can be defined in the same section (selection of the sound, duration, flash sequence, activation of the STATUS and PRG LEDs).
	Enable foam tamper signalling	If selected, it enables signalling from the anti-foam, open panel, dislodgement and battery inefficient sensors.
	Enable anti-tamper signalling	
	Enable battery inefficient signalling	
PRG/STATUS LED activation	Section where you can indicate the source (control panel or sounder/flasher) of PRG and STATUS LED activation. The selection of one of the two LED activation sources excludes the other.	

Temperature compensation (via cable)	If the internal temperature of the sounder indicated in the Real-time section is incorrect, you can use this section to set the real temperature value and correct the parameter by means of the Compensation button.	
Sounder LED activations	Activation cause	Each sounder LED (PRG or STATUS) has a maximum of 5 list boxes which allow you to select the control panel event which activates the LED.
	Inversion	If the "Inversion" option is not enabled, activation of the LED will occur when the event is active. If the "Inversion" option is enabled, LED activation will occur when the event is not active.
Cause sounder and flasher shutdown	Cause	There are a maximum of 5 check boxes which allow you to select a control panel event for the deactivation of the sounder and flasher.
	Inversion	If the "Inversion" option is not enabled, the sounder and flasher will shutdown on activation of the event. If the "Inversion" option is enabled, the sounder and flasher will shutdown on deactivation of the event.
Monitoring wireless (wireless)	Pressing the Start button starts monitoring on the variation of the signal transmitted by the device and background noise detected over time.	

Nexus 5-5

The Nexus programming phase allows you to select which actions the control panel will implement on receiving a voice call/SMS message (from an authorized user) over the GSM network. Each command comprises a group of fully-programmable parameters.

Each time a user requests an operation - via a correctly formatted SMS message or voice call to the SIM card of the Nexus - the control panel will activate the respective shortcut/event and send confirmation (feedback) of the successfully implemented command.

The following parameters can be programmed solely via the SmartLeague software programme. Select the "Nexus" option from the SmartLiving system tree structure (on the left) and then go to the "Programming" section on the right to program the relative parameters.

INIM does not guarantee the total availability of all the GSM/GPRS functions described in this manual, due to the various combinations of GSM/GPRS service providers, SIM types and telephone models that may be in use.

Note

Parts of the system	Programming section		
	Group	Option	
<ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions ⊕ Sounder/flashers <li style="background-color: #0070C0; color: white;">Nexus ⊖ SmartLiving System 	SMS Commands	This section allows you to view the 30 commands, arranged on lines on a table, which can be activated by SMS messages. Double clicking on the line of a command opens a window where you can program the respective parameters.	
		Action	Identifies the number of the command in the table shown.
		SMS text	This is the identification string to be included in the SMS command.
		Shortcut	This field allows you to select one of the following shortcuts that the control panel can activate: <ul style="list-style-type: none"> • Arm/Disarm • Stop alarms • Clear call queue • Delete memory • Activate output • Deactivate output • Inhibit (bypass) control panel zones • Activate (unbypass) control panel zones • Nexus status • Credit inquiry • GPRS client
		Shortcut parameter	Selection menu for the parameter relating to the shortcut.
		Shortcut 2	Selection menu for the shortcut which is to be activated after the one selected above.
		Shortcut 2 parameter	As per 'Shortcut parameter' but valid for the 'Shortcut 2' command.

<p>SMS Com- mands</p>	<p>Confirm</p>	<p>Identifies the type of command feedback:</p> <ul style="list-style-type: none"> • SMS - feedback will be provided by an SMS text to the phone number of the caller (command dispatcher). • Ring - feedback will be provided on the phone of the caller (command dispatcher). Positive outcome will be indicated by a "ring"; negative outcome by "silence". <p>Confirmation via SMS text or feedback ring will occur only when the phone number that sent the command is not hidden.</p> <ul style="list-style-type: none"> • Buzzer - feedback is provided by an audible signal on the Nexus buzzer. Positive outcome is indicated by three short audible signals; negative outcome is indicated by five long audible signals.
<p>Caller ID Commands</p>	<p>This section will allow you to program up to 200 telephone numbers and the commands associated with each of the numbers. Commands will be carried out when the control panel recognizes the number and the validity of the command. If the telephone number makes a voice call, the command you select from those programmed in the SMS Commands will be activated.</p>	
	<p>N°</p>	<p>Identifies the number of the command in the table shown.</p>
	<p>Name</p>	<p>This is the identification string of the command.</p>
	<p>Telephone num- ber</p>	<p>This is the phone number which, during a call to the Nexus, will activate the command.</p>
	<p>Access Codes</p>	<p>This field associates the user code with the telephone number. The code determines which partitions the telephone-number user can operate on.</p>
	<p>Actions</p>	<p>This is the number that identifies the command option selected from the 30 commands programmed in the SMS Commands section.</p>
	<p>Refuse call</p>	<p>Enabled - when the telephone number calls, the Nexus will not answer the call but will carry out the command associated with the telephone number concerned. Disabled - when the telephone number calls, Nexus will not reject the call but will allow it to proceed normally in such a way that the SmartLiving control panel can activate (if so programmed) the communicator after the programmed number of rings.</p>
<p>Text for SMS messages</p>	<p>Receive diverted SMS</p>	<p>If this option is enabled the selected number will be able to receive SMS messages diverted from the Nexus communicator which do not comply with the command-activation format. SMS "command" messages cannot be diverted.</p>
	<p>This section allows you to edit and program up to 50 SMS messages of up to 80 alphanumeric characters each. These messages can be associated with the events by means of the "SMS number" option described in <i>paragraph 5-14 Events</i>.</p>	
	<p>N°</p>	<p>Identifies the number of the SMS message.</p>
<p>General parameters / Residual credit</p>	<p>Text - Remain- ing characters</p>	<p>Editable field for the SMS text message. The number of characters available are available.</p>
	<p>Enable residual credit check</p>	<p>If this option is enabled, you must also program the method the Nexus will use to make remaining-credit inquiries to the GSM provider.</p> <ul style="list-style-type: none"> • Automatic - the Nexus will make a remaining credit inquiry to the GSM provider (regarding its own SIM) without the need of programming any parameter. • Manual - the interrogation parameters to the provider and reply must be set up manually.
	<p>Manual param- eters - Request</p>	<ul style="list-style-type: none"> • SMS - residual credit request will be made via an SMS text sent by the Nexus to the provider. • Call - the remaining credit inquiry will be made via a call which will be diverted by the Nexus to the provider. • Network command - remaining credit request will be made via a specific command made available by the provider. • Credit request number - this is the phone number or network command (made available by the GSM provider) for remaining credit inquiries. This field must be programmed regardless of the type of manual mode selected (SMS, Call or network command). • Credit request message - this text will be sent to the number in order to obtain information regarding remaining credit.
	<p>Manual param- eter - Answer</p>	<ul style="list-style-type: none"> • SMS - the provider will reply via SMS message. • Call - the provider will reply via call. • Answer number - this is the telephone number (made available by the GSM provider) the residual credit information will come from. This field must be programmed regardless of the selected manual mode (SMS, call or Network command). • Answer message - part of the SMS answer message, to filter the credit information. It is necessary to type in the text which precedes the numeric value of the remaining credit.
	<p>Low credit threshold</p>	<p>The remaining credit limit, expressed in local currency. If credit drops below this limit, the Nexus communicator will signal "Low credit".</p>
<p>Credit request interval</p>	<p>This is the interval, expressed in hours, which must pass between one automatic credit-enquiry and the next.</p>	

General parameters / Volume settings	Balancing	This option allows you to rectify the correlation between input volume/ output volume.
	Input volume	This option allows you to program the volume of the incoming signal to the Nexus and consequently, the volume of the signal received by the control panel.
	Outgoing volume	This option allows you to program the volume of the outgoing signal from the Nexus to recipient phone devices.
General parameters / Other parameters	Disable tamper	If enabled, this option disables tamper signalling on the Nexus communicator.
	Emergency signalling delay	This is the delay, expressed in seconds, that the Nexus device applies before generating the "Nexus lost" event.
	Disable GPRS fault on keypads	If enabled, this option stops the control panel from signalling the occurrence of specific faults or GPRS connection trouble.
GPRS parameters	Access point name (APN)	Editable field for the name of the GPRS provider.
	Advanced	This button opens a window for the user's name and password, sometimes required by the provider. If these details are not required, these fields can be left blank.
	Server address (URL)	This is the IP address of the server (standard IPv4) the Nexus/G device connects to. It is the IP address where the SmartLeague application awaits the incoming GPRS connection for the Nexus/G. You can indicate the address in octets or strings.
	Port	This field is for the server connection port, usually provided by the network administrator.
	Connection name	This is the descriptive string of the connection. This parameter is necessary for Teleservice requests via SMS text message and must have between 4 to 16 characters.

SMS Commands 5-5-1

The "Programming - SMS Commands" section allows you to programme up to 30 SMS-activated commands.

For the description of the programming parameters of each command, refer to the SmartLeague Installation and Configuration Manual.

Users who wish to activate a command via SMS text must enter the command details as follows:

COMMAND USING SMS TEXT

<xxxxxx> <SMS Text>

where:

- <xxxxxx> stands for the PIN of a control panel user
- a blank space must be keyed in after PIN entry
- <SMS Text> which is the command identifier, as previously described

You wish the control panel to activate "Scenario 3", switch On the perimeter lights and confirm the operation via SMS text. Proceed as follows:

EXAMPLE

1. "SMS Text" - choose the desired description, for example "Night mode"
2. "Shortcut" - select the "Arm/Disarm" shortcut
3. "Shortcut option": "Scenario 3"
4. "Shortcut 2" - select the "Activate outputs" shortcut
5. "Shortcut option 2" - the output associated with the perimeter lights
6. "Confirm" - SMS

When a user keys in the following SMS text on a mobile (cellular) phone:

123456 Night mode

where "123456" stands for the User's PIN and this message is sent to the number of the SIM card of the Nexus, the control panel will carry out the requested operations and will send an SMS message of confirmation to the mobile phone of the caller who dispatched the command.

Night mode: command done!

The installer by modify the five predefined default commands:

DEFAULT COMMANDS

- **"CREDIT"** - for balance enquiries relating to the SIM card of the Nexus, the user will receive an SMS text indicating the remaining credit.
- **"STATUS"** - for status enquiries relating to the Nexus, the user will receive an SMS text indicating the:
 - device name and firmware revision

- GSM network provider
- GSM signal reception level
- device tamper status
- BUS status
- Balance (remaining credit)
- scenario active (if present)
- "EXC" (or "ESC"), to inhibit the control panel zones
- "INC", to activate the control panel zones

For the last two commands, the message text must be:

<xxxxxx> EXC <zone description>

where:

- <xxxxxx> is the PIN of a control-panel user coded, followed by a blank space
- "EXC" (or "ESC" or "INC") is the command to be implemented on the zone, followed by a space
- <zone description> is the name zone to be inhibited or activated

Caller ID commands **5-5-2**

The "Programming - Caller ID commands" section allows the programming of up to 200 phone numbers and the commands that will be implemented when the phone number is recognized by the control panel. If a voice call is received from a telephone number, the command you select from those programmed in the "SMS Commands" section will be carried out.

For the description of the programming parameters of each command, refer to the SmartLeague Installation and Configuration Manual.

Text for SMS messages **5-5-3**

The "Parameters settings - Customizable SMS Messages" section will allow you to create up to 50 SMS text messages of 80 alphanumeric characters each. These messages can be associated with the events by means of the "SMS message number/index" option described in *paragraph 4-7 Events*.

General parameters **5-5-4**

The "Programming - General parameters" section will allow you to programme some of the Nexus management functions, such as: low/remaining credit, input and output volume, disablement of tamper protection and the emergency signalling delay.

For the description of the general parameters, refer to the SmartLeague Installation and Configuration Manual.

The remaining credit control feature is subject to temporary or even permanent unavailability caused by changes in the implementation of the methods used by the GSM/GPRS service provider.

INIM provides device programming functions which may be capable of restoring this feature, by means of manual changes to the respective parameter settings.

Note

GPRS connection **5-5-5**

Through the Nexus/G and 4G models it is possible to use the GPRS connection for remote read/write operations on the control panel via SmartLeague.

The "Programming - GPRS Parameters" section allows you to configure the GPRS communication settings of the Nexus device.

For the description of the general parameters, refer to the SmartLeague Installation and Configuration Manual.

Once the parameter settings are complete, you can activate the GPRS connection by means of the following procedure:

1. Start the SmartLeague software application and access "Settings - Application data" menu section.
Select "Connection via GPRS" from the "Communication Type" section, then press "Start".

CONNECTION

2. The "Start" button opens the GPRS connection status window, where you must set the port. The setting must coincide with the "Port" parameter, described above.
3. Press the "Connect" button to activate the server.
4. The connection cannot be established until the teleservice request is received. The teleservice request can be made in different ways, as follows.

Select the "Nexus teleserv." option from the User menu, then press the button to start the teleservice session.

TELESERVICE REQUEST FROM KEYPAD

The Nexus will initialize the connection to the address and port programmed in the "Nexus - Programming - GPRS settings" section of the SmartLeague application. The keypad will show the connection status for about 90 seconds and the following messages may appear:

- **GPRS connected** - this indicates a successful connection; 10 second after the visualization of this message, the keypad will return to standby status and the icon on the second line of the display will blink.
- **Connection Error** - this indicates a failed connection.
- **Error code: xxx** - this indicates that code error is the reason for the failed connection.

Table 5-1: GPRS connection errors

Code	Error
001	GPRS connection error
002	
003	
004	
005	GPRS service not provided by the SIM provider
006	Possible APN error
007	Possible APN error or GPRS not enabled
008	GPRS connection error
015	TCP connection error (wrong URL, wrong port, Nexus server on SmartLeague disconnected or unreachable, etc.)
016	TCP disconnection error
024	GPRS connection error

Code	Error
025	GPRS disconnection error
027	GPRS connection error
028	Command error - connection not supported (the Nexus model in use is not GPRS capable)
029	GPRS multi-connection error
030	Unexpected remote disconnection (sudden shutdown of the Smartleague server)
101	Error during TCP connection
102	
103	
105	Problems with normal control panel operating capacity
106	Generic internal error
107	GPRS disconnection error

The request can be made by means of an SMS text message to the Nexus of the installer company; the message format must be as follows:

TELESERVICE REQUEST VIA SMS

<xxxxxx> CONNECT <Connection Name> <URL>:<Port>

where:

- <xxxxxx> is the installer code PIN, followed by a blank space
- "CONNECT" is the connection command, followed by a space
- <Connection Name> is the description of the connection (previously described), followed by a space
- <URL>: is the IP address of the server you wish to connect to, followed by ":"
- <Port> is the connection port

If you intend using the settings configured in the "Programming - GPRS settings" section (previously described), the last two parameters can be omitted.

After the SMS message has been sent, you must wait until the software indicates that the connection has initialized.

5. Once initialized, you can carry out the desired Upload/Download operations via the SmartLeague software.
6. When the programming session is complete, access "Settings - Application data - GPRS Connection", then select "Disconnect" to end the connection.
If no read/write operations are carried out for 3 consecutive minutes, the GPRS connection will end automatically.

SmartLiving System 5-6

Parts of the system	Programming section				
<ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions ⊕ Sounder/flashers — Nexus ⊖ SmartLiving System 	<p>The SmartLiving System option, from the system tree on the left, allows you to program the basic parameters of the control panel in the Programming section.</p> <p>Click on the corresponding node to access a list of all the individual items relating to the control panel programming process. Select the required item to view and program the respective parameters (refer to the following paragraphs).</p>				
	Group	Option			
	Installer code	This section is for the installer PIN which is required when communicating with the control panel.			
	Control panel description	Edit field for the description of the control panel (max 50 alphanumeric characters).			
	Serial number	Section where, after a reading, it is possible to view the serial number of the control panel.			
	"Cloud Mode"	<p>If enabled, this option will apply a preset of some of the control panel parameters that would otherwise have to be programmed individually for connection to the Inim Cloud service.</p> <p>Refer to <i>paragraph 5-6-1 "Cloud mode" preset</i>.</p>			
	Date/Time	<p>Editable field for the system date and time.</p> <p>You can set the time of the computer in use by means of the Set local date button, then transfer the setting to the control panel by means of the Write on control panel button.</p>			
	Periodic event	<p>Programming field for the date and time of the first "Periodic Event" (refer to <i>paragraph 5-14 Events - Actions</i>).</p> <p>You can transfer the setting to the control panel by means of the Write on control panel button.</p>			
		<table border="1"> <tr> <td data-bbox="509 952 758 1041">PeriodicInterval</td> <td data-bbox="758 952 1527 1041">This parameter allows you to set the interval between "Periodic events" (expressed in minutes or hours). To disable the "Periodic event", set "0".</td> </tr> <tr> <td data-bbox="509 1041 758 1176">Continuous periodic event</td> <td data-bbox="758 1041 1527 1176">If enabled, the system will generate the corresponding periodic event regardless of its initial date/time. The event will be generated when the programming session is exited, or when the system starts up, and will be generated continuously when the set period expires.</td> </tr> </table>	PeriodicInterval	This parameter allows you to set the interval between "Periodic events" (expressed in minutes or hours). To disable the "Periodic event", set "0".	Continuous periodic event
	PeriodicInterval	This parameter allows you to set the interval between "Periodic events" (expressed in minutes or hours). To disable the "Periodic event", set "0".			
Continuous periodic event	If enabled, the system will generate the corresponding periodic event regardless of its initial date/time. The event will be generated when the programming session is exited, or when the system starts up, and will be generated continuously when the set period expires.				
Control panel parameters	Restart monostable outputs	If activated, each event which activates a monostable output refreshes the programmed "Monostable time".			
	Does not arm if any of the zones are not ready	<p>The control panel will not arm the partition if it detects any zones that are not in stand-by status.</p> <p>If, amongst the zones not in standby status, there are zones configured as "Autobypassable" or "No arm if not ready" (refer to <i>paragraph 5-8-1 Zone / Input</i>) they will be indicated on the keypad. If the user still arms the system, these zones will be inhibited automatically and the partitions they belong to will be armed.</p>			
	Bypass tamper in the event of bypassed zones	If a zone is bypassed (disabled), it will also be unable to generate terminal tamper.			
	Prevents the deletion of tamper memory by user code	<p>No user will be allowed to delete of the following events:</p> <ul style="list-style-type: none"> • terminal tamper • control panel open-tamper • control panel dislodgement-tamper • peripheral tamper • peripheral loss • false key 			
	Instant reset of wireless magnetic contact	If this option is enabled, reset of the magnetic reed sensor of wireless detectors will be signalled instantly (otherwise signalling has a maximum delay of 10 seconds).			
	Hide the Teleservice icon on keypad	If this option is enabled, the  symbol which usually appears on the keypad display during teleservice sessions will be hidden.			
	Hold installer code	If this option is enabled, all the control panel parameters with the exception of the installer PIN will reset to the factory default settings after reset.			
	Automatic Daylight Saving Time (DST)	The control panel clock will go back automatically one hour at 03:00 the first Sunday in October, and it will go forward automatically one hour at 02:00 the last Sunday in March.			

Control panel parameters	Use fault output for smoke sensor contamination	<p>Enables management of the "Contaminated smoke detector" event.</p> <p>The "Output fault" and "Detector dusty" events share the same actions. Therefore, if either of these events occur, the system will send the calls and activate the outputs associated with the "Output fault" event.</p> <p>The events log provides the proper distinction between these two events:</p> <ul style="list-style-type: none"> in the event of an "Output fault", the system will provide the description of the output in fault status in the event of an "Detector dusty", the system will provide the description of the detector that generated the event
	Maintenance	<p>The installer can start the maintenance session from the keypad without opening the control panel or moving the jumper. On exiting the Installer menu, it will be possible to operate on the system in the same way as when the control panel is placed in maintenance mode by means of the jumper.</p> <p>In order to place the control panel in "RUN" mode, this option must be disabled.</p>
	Wireless supervision time	<p>Dropdown box for the selection of the supervision time of wireless devices. On expiration of the programmed time, any wireless devices which do not respond will be signalled as lost.</p> <p>Accepted values: 12 to 250 minutes.</p>
	Check horn	<p>The control panel will generate a "Sounder/flasher tamper" event when the passive horn disconnects from the relay (wire cutting tamper).</p>
	Squawk	<p>This option activates the sounder for a brief period during partition stay/away arming and disarming operations. This audible signal indicates that these operations have been executed successfully.</p>
	Sound alarm on keypad	<p>If enabled, all the system keypads will emit an audible signal in the event of an alarm or tamper event on any one of the partitions they belong to.</p>
	Serial speed 115200 bps	<p>If enabled, the bit rate of the serial port will be 115200 bps. if disabled the bit rate will be 57600 bps.</p>
I-BUS parameters	BUS speed	<p>Selection of the BUS communication speed (38.4 / 125 / 250 kbps).</p>
	Mains fault delay	<p>This parameter allows you to program the delay, expressed in minutes, between mains failure and the "Mains failure" fault event signal.</p>
	Low battery delay	<p>This parameter allows you to program the delay, expressed in minutes, which will be applied before "LowBattery" events are signalled.</p>
Telephone options	Telephone-voice volume output	<p>Volume adjustment bar to higher/lower the volume of voice messages during playback over the phone.</p>
	Telephone input volume	<p>Bar for adjustment of the telephone input signal volume. This option is useful in situations which require better comprehension of DTMF tones and improvement of teleservice intervention via modem.</p>
50131 parameters	50131 Grade 3 Compatibility	<p>This option activates a presetting on the control panel which adheres to grade 3 of EN50131.</p>
	Reader LED OFF	<p>If there are no keys present at the reader, the LEDs of nBy readers will be Off. If a key is waved across the reader, the status will be indicated on the LEDs for 30 seconds before switching Off again.</p> <p>During this 30 second phase, the user can hold the key in the vicinity of the reader and select the desired shortcut indicated by LEDs.</p>
	Hide status	<p>The status of the partitions will be hidden. If a valid code is entered at a keypad, the real-time status will be indicated on the keypad concerned for 30 seconds.</p> <p>If partitions are armed, the real-time status of the system will be hidden from non-authorized users.</p> <p>If the partitions are disarmed, the LEDs will function normally, the status icons will be present and the alarm and tamper events will be visible.</p>
	Hide icons	<p>If partitions are armed, the status icons will be hidden from non-authorized users.</p> <p>If a valid code is entered at a keypad, the status of the icons will be shown for 30 seconds.</p> <p>The keypad will show the real-time status of the icons when all the keypad partitions are disarmed.</p>

50131 parameters	Alarm delay	If an instant-zone alarm occurs on a partition while entry time is running, the associated actions (calls, output activation, save to log, etc.) will not be generated until 30 seconds after the expiry of the entry time. If the partition (or partitions) are disarmed during this period, the associated actions will not be generated, however, the keypads will indicate the violation of the instant zone.
	Fault memory LED	If the control panel detects a fault, the yellow LED on the keypads will go On and will remain On even after the fault clears. To switch the yellow LED Off, clear all activating causes and reset the partition.
Forced arming faults	This section allows you to select which events, other than zones in alarm status, will be signalled as system security-risk conditions when the partition arms.	
IP connection test parameters	This section allows you to program the parameters of the IP connection test.	
	IP Address Port	Pv4 Address and port connection attempts are directed to.
	Interval	Time, expressed in seconds, between connection tests. If '0' is set, the connection test will be disabled.
	Number of attempts	Number of connection attempts for each test.

“Cloud mode” preset 5-6-1

In order to assist the installer when programming a SmartLiving control panel registered to the Inim Cloud service, the SmartLeague software provides an option that, if enabled, applies a preset of some of the control panel parameters that would otherwise have to be programmed individually.

If activated, the software will perform the following default programming:

- The “Inim Cloud” will be assigned to telephone number 12 which will no longer be editable.
The only parameter that will remain editable is the **Channel**, i.e. the connection channel (Nexus or SmartLAN).
- A preset of events of various types will be applied and must be communicated to the Cloud when they occur.

Event	Communication to Cloud in case of	
	Activation	Reset
Zone alarm	Yes	Yes
Terminal tamper	Yes	Yes
Zone bypass	Yes	Yes
Effective arming mode on partition	Yes	No
Partition armed in Away mode	Yes	No
Partition disarmed	Yes	No
Overtime request	Yes	No
Partition failed to arm	Yes	No
Thermostat on keypad	Yes	Yes
Activate scenario	Yes	No
Emergency button	Yes	No
Panic	Yes	No
Open-panel tamper	Yes	Yes
Dislodged-panel tamper	Yes	Yes
Zone fuse fault	Yes	Yes
I-BUS fuse fault	Yes	Yes
Battery inefficient	Yes	Yes
Mains failure	Yes	Yes
Expansion tamper	Yes	Yes
Keypad Tamper	Yes	Yes
Reader Tamper	Yes	Yes

Event	Communication to Cloud in case of	
	Activation	Reset
Sounder flasher tamper	Yes	Yes
Nexus tamper	Yes	Yes
LIVPWR100 tamper	Yes	Yes
Video detector tamper	Yes	Yes
Expansion Loss	Yes	Yes
Keypad Loss	Yes	Yes
Reader Loss	Yes	Yes
Sounder/flasher loss	Yes	Yes
Nexus loss	Yes	Yes
LIVPWR100 loss	Yes	Yes
Video detector loss	Yes	Yes
Jamming	Yes	Yes
Low battery wireless zone	Yes	Yes
Wireless zone loss	Yes	Yes
Valid Installer code	Yes	No
Invalid code	Yes	No
False key	Yes	No
GSM trouble	Yes	No
Input undergoing programming	Yes	Yes
Output fault	Yes	No
Low credit	Yes	No

Default settings 5-6-2

The SmartLeague software programme allows you to reset the control panel default values only for the following parameters relative to the programming of events:

- digital dialer parameters
- "CCC" field of CONTACT-ID protocol of the zones
- phone calls on activation and restoral
- outputs on activation or restoral
- message playback on keypads on activation or restoral
- SIA protocol parameters

Table 5-1: **Factory default settings - via SmartLeague software programme**

Option	Part of the system	Template/section
CONTACTIDDefault	SmartLiving System - Events	Programming - Maintenance events
CONT-ID Numbering	SmartLiving System - Terminals	Programming - "Rename the CCC in sequential mode"
DeletePrg.events	SmartLiving System - Events	Programming - Maintenance events

Partitions 5-7

Parts of the system	Programming section		
<div style="font-size: 0.8em;"> <ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions ⊕ Sounder/flashers — Nexus ⊖ SmartLiving System <ul style="list-style-type: none"> ⊕ Partitions </div>	<p>The Partitions option, from the installation tree on the left, accesses a table in the Programming section, where each line corresponds to a partition and each column to a parameter of each partition. Click on the node of the Partitions option to access a list of all the partitions. Select the required item to view and program the respective parameters.</p> <p>The second Entry time is added to this.</p>		
	Group	Option	
	Description	This is the editable partition label (description).	
	Exit time	This is the Exit time window (programmable in seconds or minutes) If you set "0" in this field, there will be no Exit time. Therefore, any delayed zones belonging to the partition will generate alarms instantly if they are not in stand-by status when the partition is armed.	
	Entry Time	This is the Entry time window (programmable in seconds or minutes). If you set "0" in this field, there will be no Entry time. Therefore, any delayed zones belonging to the partition will generate alarms instantly if violated when the partition is armed.	
	Entry Time 2	This is the window for the second Entry time.	
	Details	Pre-arm time	This setting is the delay, expressed in minutes, which precedes automatic-arming on a partition.
		Patrol time	This is the time window for patrol operations (programmable in minutes).
		Timers	Select the timer you want to associate with the automatic-arming operations.
		Autoreset memory on arming	If enabled, the partition alarm and tamper memory will reset automatically when the partition arms.
	Auto-arm in stay mode	If enabled, the partition will arm in "Stay" mode at the programmed time. If disabled, the partition will arm in "Away" mode at the programmed time.	
	Clear call queue on disarm	If enabled, the call queue will clear when the partition disarms.	

Terminals 5-8

Parts of the system	Programming section			
<ul style="list-style-type: none"> + Keypads + Proximity readers + Expansions + Sounder/flashers Nexus SmartLiving System <ul style="list-style-type: none"> + Partitions + Terminals 	<p>The Terminal option, from the system tree on the left, accesses a layout which allows you to configure, via the Programming section, all the terminals and their applications.</p> <p>The terminals of the control panel and devices which are configurable via this section are shown on their respective PCB boards, where their screw terminals are highlighted. The boards can be either in colour or black and white depending on whether they have already been configured via the System Layout section (refer to <i>paragraph 2-2 Creating a project layout</i>).</p> <p>Right clicking on any one of the PCBs allows you to assign a common setting to all the terminals on the selected board. Right clicking on a single terminal allows you to configure it separately.</p> <p>Right clicking on the PCB of an expansion allows you to configure all the board terminals as "Wireless", however, the image will not colour until the respective devices are enrolled.</p> <p>Once a terminal has been assigned a configuration, the "connected" icon will represent the resulting configuration:</p> <ul style="list-style-type: none"> •  Zone or Input •  Output •  Double zone •  I/O or Input/Output <p>Double clicking the icon of a terminal with a configuration opens a window where you can program all the parameters of the selected terminal (refer to <i>paragraph 5-8-1 Zone / Input</i>, <i>paragraph 5-8-2 Output</i> and <i>paragraph 5-8-3 Wireless</i>).</p> <p>Click on the node of the Terminals option to view the sub-options provided by the two sections the terminals can be associated with: Zones and Outputs. Select either of these sections to access the respective table in which each line corresponds to a terminal and each column to a parameter of each terminal.</p> <p>A right click in this section allows you to copy/paste the programming contained in the selected line.</p> <table border="1" data-bbox="311 907 1540 987"> <tr> <td style="text-align: center;"></td> <td style="text-align: center;">Reassign the CCC in sequential mode</td> <td>This button, on the top left of the terminal configuration section, initiates an operation that reassigns the Contact-ID code of each zone in such a way that they are all in sequential order.</td> </tr> </table>		Reassign the CCC in sequential mode	This button, on the top left of the terminal configuration section, initiates an operation that reassigns the Contact-ID code of each zone in such a way that they are all in sequential order.
	Reassign the CCC in sequential mode	This button, on the top left of the terminal configuration section, initiates an operation that reassigns the Contact-ID code of each zone in such a way that they are all in sequential order.		

Zone / Input 5-8-1

Group	Option	
Description	This is the editable label which identifies the zone. By default all the zones assume the description of the peripheral they refer to, followed by the respective terminal.	
Type	Checkbox for the selection of the zone type: Instant, Delayed, Viewable delayed, Route, 24hour, Technological, Arm, Disarm, Switch, Follow, Patrol.	
Balancing	Checkbox for the selection of the balancing type (the options vary in accordance with the zone type). Normally open (NO), Normally closed (NC), Single balancing, Double balancing, Double zone (without EOL), Double zone (with EOL).	
Detector type	Generic zone, Roller blind, Shock	
Alarm cycles	Checkbox for the selection of the number of alarm cycles (between 1 and 14). If you select "Unlimited", the zone will operate as a "repetitive" zone.	
Wiring diagram	Button for to open a window showing the zone connection mode.	
Contact ID	Checkbox to indicate the Contact-ID code associated with the zone for the occurrence or restoral of events such as: <ul style="list-style-type: none"> • Zone alarm • Zone tamper • Zone bypass • Zone real-time 	
"Generic" device parameters	Multi-pulse time	This parameter applies only when the "Alarm pulse num." parameter (see below) is more than 1. This is the window during which a number of alarm pulses must be detected (each lasting as long as the programmed "Al.pulse Duration"). The number of alarm pulses must equal or exceed the value programmed for "Alarm pulses", before the system generates an alarm. This time window can be expressed in seconds or minutes.
	Alarm pulses	This is the number of pulses (each as long as the programmed "Alarm pulse Duration") necessary to generate a zone alarm event. If this value is more than 1, you must also program the "Multi-pulse time" parameter.
	Alarm pulse Duration	This is the length of time (after detection of alarm conditions) the zone allows before generating an alarm. Expressed in multiples of 15 milliseconds or minutes.

Rollerblind device parameters	Rollerblind time	This parameter applies only when the value of the "Roller blind pulses" parameter (see below) is more than 1. This is the time window during which a number of pulses, equal to the value set for "Rollerblind pulses", must be detected before a zone alarm is generated. This time window can be expressed in seconds or minutes.
	Rollerblind pulses	This is the number of pulses necessary to generate a zone-alarm event. If this value is more than 1, you must also program the "Roller blind time" parameter.
Shock device parameters	Shock time	This parameter applies only when the "Shock pulses" (see below) value is more than 1. This is the time window during which the system must detect a number of pulses equal to the value set for "Shock pulses" before generating a zone alarm. This time window can be expressed in seconds or minutes.
	Shock pulses	This is the number of pulses necessary to generate a zone-alarm event. If this value is more than 1, you must also programme the "Shock time" parameter. If this value is 0, the alarm will be generated exclusively in accordance with the "Shock sensitivity" parameter.
	Shock sensitivity	This is an empirical parameter which regulates the sensitivity of the sensor. Increasing this value decreases detection sensitivity.
Real-time	<p>Section for the adjustment of zone detection thresholds. The thresholds can be modified via the number boxes or by using the bar which indicates the levels by means of colours:</p> <ul style="list-style-type: none"> • yellow - tamper/short • green - stand-by • red - alarm • orange - double zone with one zone in alarm status and the other in stand-by status <p>The Real-time button makes a connection with the zone which feeds back information regarding the thresholds. The OK button saves the changes which will be written during the write phase. If the zone is configured as "Wireless", this button will provide information that differs to that indicated; for details refer to <i>paragraph 5-8-3 Wireless</i>.</p>	
Partitions	<p>These are the partitions the zone belongs to. A zone configured as "Automation" cannot be assigned to any partition.</p>	
Options	Interior	A zone that monitors the inside of the protected building. If a partition that a zone belongs to is armed in Stay mode, it will be unable to generate alarms.
	Autobypassable	A zone with this attribute will be bypassed automatically by the control panel if the partition it belongs to arms when the zone is not in standby status. The zone will be unbypassed automatically when it restores to standby or when the partition it belongs to is disarms.
	Unbypassable	A zone with this attribute cannot be bypassed, manually (by the user) or automatically (by the control panel).
	Chime	A zone with this attribute will generate "Chime on partition" events, if violated when the partitions it belongs to are disarmed. Keypads which have partitions in common with the chime zone will emit an audible signal when the "Chime on partition" event occurs. If all the partitions the zone belongs to are armed, the zone will operate as programmed.
	Test	A zone with this attribute cannot generate alarms (activate audible and visual signalling devices). However, any alarm events that occur will be saved to the events memory.
	No-Unbypassable	If this option is enabled, the zone will operate as an "Autobypassable" zone, with the difference that it will be automatically unbypassed when the partition next disarms.
	No arm if not ready	If this option is enabled, the zone, even if it is a 24H, automation or delayed zone, will not arm when it is not in stand-by status. If this option is selected for a 24H or technological zone, it can be used together with the control panel option: "Does not arm if any of the zones are not ready", for the management of the "anti-masking" function on duly capable detectors.
	Activate Entry Time 2	If this option is enabled, delayed zone will activate the second partition entry time. If this option is not enabled, delayed zones will activate the first partition entry time.
	Last exit zone	If this option is enabled and the zone passes from stand-by status to alarm status while the partition exit time is running, the exit time will be forced to 15 seconds. If the zone passes from alarm status to standby status, the exit time will be forced to 5 seconds.
	Unbyp. on disarm	If this option is enabled, a zone which has been bypassed by a user, will be automatically unbypassed when the partition next disarms.
Hold-up	Activation of a zone with this configuration generates an instant alarm even when the partition it belongs to is disarmed. However, audible and/or visual signalling devices will not be activated (silent alarm). Therefore, calls generated by the alarm will not be revealed audibly or visually on the keypad display and LEDs.	
Fault zone	If this option is enabled, violation of the zone will generate a zone alarm event and contribute to fault signalling (yellow LED on the keypad).	

Output 5-8-2

Group	Option	
Description	This is the editable output label (device description). By default each output, except for the 3 outputs on the control panel, acquires the description of the device where it is located followed by the relative terminal.	
Output options	Normally closed	This is the condition of the output during stand-by status.
	Monostable	When a "Monostable" output receives an activation signal, it will remain active (On) for the programmed time, regardless of the status of the event which caused its activation. If this option is enabled, it is possible to set the monostable time in the field below.
	Buzzer - beep 1KHz	When the output is activated, it will generate a 1KHz signal. This can be used to drive a buzzer.
	Flasher - 0.5s ON and 0.5s OFF	When the output is activated, it will generate an intermittent signal (0.5 sec ON and 0.5 sec OFF). This can be used to drive a visual signalling device.
	Do not deactivate on reset	The output will not restore when the activating event ends. This option is useful in situations which require a trigger event for output activation and a reset event for its deactivation. This option applies to bistable outputs only.
	Switch	Each time you perform an "activate output" command, the output will switch status. Therefore, if it is deactivated it will activate and vice versa.
	Dimmer	The dimmer output and the power supply from the terminals can be adjusted by the user.
	Relay use	The output will operate as a relay output.
	Home Automation	If the output is activated when the control panel enters the programming phase, it will not reset to stand-by.
Events	Interlocked	If enabled, this option inhibits the contemporary activation of the associated terminals. It can be enabled only for terminal T01, which will automatically activate the option for the associated T02, and terminal T03, which will automatically activate the option for the associated T04.
	Events	The Events option, from the table available under the Terminal, Outputs option opens a window containing a list of events which can activate the output. You can delete each individual event by clicking on Delete .
Codes	The Codes option, from the table available under the Terminals, Outputs option, opens a window containing a list of user codes which can activate the output.	

Wireless 5-8-3

This section is shown at the bottom of the terminal programming window if the respective expansion is configured as "Wireless". The visualization of the following parameters varies in accordance with the type of wireless device selected in the "Type" check box.

Group	Option
Enroll	Button to start the enrolling a wireless detector which is not yet enrolled (unenrolled) on the terminal concerned.
Remove	Button to delete (unenroll) an enrolled wireless detector from the terminal concerned.
Type	Type of device to be enrolled:
Sensitivity	This selection field allows you to change the sensor sensitivity of Air2 devices.
Infrared Sensitivity	Checkbox for changes to the sensitivity of the infrared sensor of Air2 devices. The sensitivity ranges from 1 (least sensitive) to 15 (most sensitive). The default setting is 10.
Microwave sensitivity	Checkbox for changes to the sensitivity of the microwave sensor of the Air2 device. The sensitivity ranges from 1 (least sensitive) to 15 (most sensitive). The default setting is 10.
Tamper sensitivity	Checkbox for changes to the sensitivity of the anti-tamper sensor of Air2 devices. The sensitivity ranges from 1 (least sensitive) to 15 (most sensitive). The default setting is 5.
Anti-masking sensitivity	Checkbox for changes to the sensitivity of the anti-masking sensor of the Air2 device. The sensitivity ranges from 1 (least sensitive) to 15 (most sensitive). The default setting is 5.
Reed relay type	This selection field allows you to select the Air2 magnetic contact reed: <ul style="list-style-type: none"> • Magnet - long side, for detection using the long side of the magnetic contact. • Magnet short side - for detection using the short side of the magnetic contact. • Both magnets - for detection using both sides of the magnetic contact.
Shock sensor	This check box allows you to select a previously enrolled Air2 magnetic contact and modify the shock-sensor parameters from 1 (least sensitive) to 63 (most sensitive).
Inclination	This number box allows you to set the maximum angle allowed before signalling of tilting occurs, from 1 (minimum tilting) to 15 (90° approx. when compared with the standby position).
Disabled	Check box to disable the corresponding detector

Tilt delay	This parameter allows you to set the delay before signalling of tilting occurs (seconds or milliseconds)	
Options	Tamper on inactive reed relay	Detects tamper on the Air2-MC100 magnetic-contact when both reeds are in stand-by status.
	Disable detector when partition is disarmed	In order to increase battery life, the infrared sensor will deactivate when the partitions it belongs to are disarmed and will only activate when the partitions it belongs to arm. When the detector is deactivated it will not generate alarms. When the partitions arm, there may be a delay of up to 3 minutes before the detector receives the activation command.
	Use detector LED	The red LED on the device provides visual signalling of alarm or tamper conditions on the device itself.
	Broadcast RF	This option assures the activation/deactivation of the output within 2 seconds of the control panel command. Valid only for terminals T1 and T2 of Air2-MC100 configured as outputs.
	Bypass tamper	If this option is disabled, open/dislodgement tamper on Air2 devices will not generate the respective events.
Real-time	Battery level 	Image, that by means of the colour green, represents the battery level of the device.
	Signal reception level 	This is a series of notches that represent the signal reception strength on the device as received by the Air2-BS200 transceiver.
	RF analysis	This button opens a window which allows you to monitor the signal variations transmitted by the device and any detected background noise.

Arming scenarios 5-9

Parts of the system	Programming section		
<ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions ⊕ Sounder/flashers — Nexus ⊖ SmartLiving System <ul style="list-style-type: none"> ⊕ Partitions ⊕ Terminals ⊕ Arming scenarios 	The Arming scenarios option, from the installation tree on the left, accesses a table in the Programming section, in which each line corresponds to a scenario and each column to a parameter of each scenario. Instead, clicking on the node of the Arming scenarios option accesses a list of all the scenarios. Select the required scenario to view and program its parameters.		
	Description	Editable field for the description of the scenario.	
	Partitions	This section allows you to configure the arm/disarm scenarios of all the partitions managed by the control panel. <ul style="list-style-type: none"> • “-” the current operating mode of the partition will not be changed. • Away - the partition will arm in Away mode (interior and perimeter). • Stay - the partition will arm in Stay mode (perimeter only). • Instant - the partition will arm in Instant mode (perimeter only with zero delay). • Disarm - the partition will disarm. 	
	Icon	This section allows you to select the icon you wish to assign to the scenario, by indicating the icon number (refer to <i>paragraph 5-16 Icons and shortcuts</i>): The selected icon will be shown on the right.	
	Output	This dropdown box allows you to select the output that will be activated when the scenario is applied (from keypad, over the phone, from a reader, etc.). It is possible to use a single scenario to activate an output (in this case, actions on partitions must not be programmed), thus allowing display on the keypad of the different icons for the activation of different outputs.	

Timers 5-10

Parts of the system	Programming section	
<ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions ⊕ Sounder/flashers — Nexus ⊖ SmartLiving System <ul style="list-style-type: none"> ⊕ Partitions ⊕ Terminals ⊕ Arming scenarios ⊕ Timers 	Click on the node relating to the Timers option to access a list of all the available timers. Select the required item to view and program the respective parameters in the Programming section.	
	Description	This is an editable field for the description of the timer.
	Monday / ... / Sunday	You can program two "ON" and "OFF" time frames for each day of the week. During the week, the timer will activate in accordance with each "ON" indication and deactivate in accordance with each "OFF" indication, regardless of the number of times "ON" and "OFF" indications occur and also regardless of whether the indications belong to the same day of the week.
	Exceptions	Each exception allows you to define a time frame, expressed in days, within which you can set an "ON" time and an "OFF" (deactivation) time valid for all the days included in the time frame. Exceptions always have priority over the days of the week.
	Partition filter for user-codes	This section indicates the partitions associated with the codes and keypads which have access to timer programming through the user menu.

The SmartLeague software programme allows you to set up 15 setting exceptions for each timer. Each "timer exception" allows you to define different On and Off times for the selected interval (1 or more days, 1 week, etc.). The pre-set times will be applied for the entire interval. The system does not accept intervals which go over the end of the year. Therefore, it is impossible to program an interval such as 12th December to 5th January. In such situations, you must program 2 "timer exceptions", one from 12th to 31st December and the other from the 1st to 5th January, both with the same On and Off settings.

The exceptions have priority over the days of the week. For example, If a "timer exception", lets say 1st May, falls on a Tuesday the settings programmed for 1st May will be applied.

The exceptions cannot be programmed via keypad.

Note

Codes 5-11

Parts of the system	Programming section		
<ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions ⊕ Sounder/flashers — Nexus ⊖ SmartLiving System <ul style="list-style-type: none"> ⊕ Partitions ⊕ Terminals ⊕ Arming scenarios ⊕ Timers ⊕ Users <ul style="list-style-type: none"> ⊕ Codes ⊕ Keys 	Click on the node of the Users option from the system trees to access the Codes and Keys options. The Codes option accesses a table, in the Programming section, where each line corresponds to a code and each column corresponds to a parameter for each code. Click on the node of the Codes option to access a list of all the codes. Select the required code to view and program its parameters.		
	Group	Option	
	Description	This is an editable programming field for the code user's name.	
	Partitions	Section for the selection of the partitions the code is assigned to.	
	Options	Type	Programming field for the assignment of the level in the code hierarchy of the selected user.
		Partition filter	If this option is enabled, the code concerned can change the parameters only of codes of a lower level in the code hierarchy whose partitions are a subset of its own partitions.
		Fixed length code	If this option is enabled, after entering a valid PIN and without pressing "OK", the user of the code concerned can activate the shortcut associated with the "F12" key, programmed through the "F1/F4 key shortcuts", to be described later. If this shortcut is number 1 ("Arm/disarm") and all the partitions assigned to the user code in question are disarmed, the command will arm them, otherwise it will disarm them. If this option is enabled, the user of the code concerned can access their menu only after pressing the "OK" key and typing-in their PIN.
Access to user menu	Selection field to allow menu viewing on the system keypads immediately after user code validation: <ul style="list-style-type: none"> • Icons, function key shortcuts; display of the code icons corresponding to the function keys. At this point, the user can press the function keys and activate the respective shortcut. • Shortcut text - displays the descriptions of the scenarios assigned to the user shortcuts associated with the function keys. The descriptions of the shortcuts will be shown in the place of the respective shortcuts icons. • Standard user menu - opens the user-menu scroll list containing all the operations the user is enabled to perform. 		

Programming section		
Enablement details	This section allows you to enable/disable access to the various sections of the User Menu. For further details regarding the User Menu, refer to <i>Users Manual</i> of the SmartLiving control panel.	
	Enablement of outputs	This section allows you to enable/disable the outputs the code user can control manually (switch ON/OFF) via the user menu.
Shortcut details	F1/F4 key short-cuts	This section allows you to assign a shortcut to each of the function keys F1 to F12 (with the eventual respective parameter) which will activate when the key is pressed.
	0/9 key short-cuts	This section allows you to assign a shortcut to each of the number keys 0 to 9 (with the eventual respective parameter) which will activate when the key is pressed.
Option details	Voice guide	If enabled and if the keypad is equipped with voice functions, after entering the PIN and pressing the OK button the descriptions of the shortcuts relating to the code, set on the numeric keys will be announced.
	Patrol	If enabled, the code will be a "Patrol" code.
	Remote access	If enabled, the code PIN can be used to operate the system over-the-phone. Use of a code over-the-phone allows you to only carry out the shortcuts assigned to the number keys 0 to 9.
	Timers	This section allows you to assign a timer to the code. The code will be operative only at the pre-set times.
Change user PIN	This section allows you to change the PIN to the selected user. Changes will be valid only after the Change PIN button has been pressed.	
	Old PIN	This method allows you to substitute the old code PIN (to be entered in the upper edit field) with a new PIN (to be entered in the lower edit field).
	Master or Manager User PIN	This method, using a Master or Manager user PIN (to be entered in the upper edit field) allows you to substitute the old code PIN with a new one (to be entered in the lower edit field on the right).

Keys 5-12

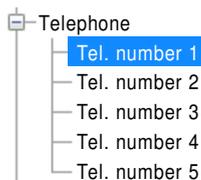
Parts of the system	Programming section		
<ul style="list-style-type: none"> + Keypads + Proximity readers + Expansions + Sounder/flashers Nexus SmartLiving System <ul style="list-style-type: none"> + Partitions + Terminals + Arming scenarios + Timers + Users <ul style="list-style-type: none"> + Codes + Keys 	Click on the node of the Users option from the system trees to access the Codes and Keys options. The Keys option accesses a table, in the Programming section, where each line corresponds to a key and each column corresponds to a parameter of each key. Click on the node of the Keys option to access a list of all the keys. Select the required key to view and program its parameters.		
	Group	Option	
	Description	This is an editable field for the key name/description.	
	Partitions	This section allows the installer to establish which partitions the key can control.	
	Options	Patrol	The key will be a "Patrol" key.
		Maintenance	The key will be able to block outputs associated with alarm/tamper events for the time that it is held in the vicinity of a reader.
		Wireless	This option indicates whether the previously enrolled key is a wireless key or not.
		Use key short-cuts only	If a key is held in the vicinity of a reader, only the key shortcuts will be indicated and not the reader shortcuts.
		Total disarming disabled	If a key is held in the vicinity of a reader when some partitions are armed, the Disarm option will be inhibited (all LEDs Off).
	Timers	This section allows you to associate a timer with the key in order to filter the operability of the key on a time basis.	
Shortcut	This section will allow you to setup the four shortcuts (with the eventual respective parameter) that the key can activate from a proximity reader. Each shortcut is associated with the activation of a LED on the reader (red, blue, green and yellow).		

Telephone 5-13

Parts of the system	Programming section		
<ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions ⊕ Sounder/flashers — Nexus ⊖ SmartLiving System <ul style="list-style-type: none"> ⊕ Partitions ⊕ Terminals ⊕ Arming scenarios ⊕ Timers ⊕ Users <li style="background-color: #00a0e3; color: white;">⊕ Telephone 	<p>Selection of the Telephone option from the installation tree on the left, accesses two subsections in Programming section:</p> <ul style="list-style-type: none"> • Telephone: this is a table where each line corresponds to a telephone number and each column corresponds to a parameter for each number. A right click in this section allows you to copy/paste the activation/restore events contained in the selected line. The Events option, from the table available opens a window containing a list of events which can activate the phone call. You can delete each individual event by clicking on Delete. • Telephone parameters: allows you to program the parameters of the telephone line, telephone diallers and teleservice, as follows. 		
	Group	Option	
	Telephone line parameters	Dial-tone check	The control panel will engage the phone line and check for the "dial tone"; if present, the control panel will start dialing.
		Pulse dialing	The control panel will dial using pulse tone.
		Telephone line fault alert	If a "telephone line fault" event occurs, the control panel will flash the respective icon on the keypad displays.
		Double call	The control panel will override the answerphone function. Option available only for PSTN calls.
		Number of rings for answerphone	This value determines the number of rings the system allows before picking up an incoming call (from 1 to 15).
		Ring sensitivity	This is the numerical value that determines the sensitivity to the recognition of the rings of a phone call to the control panel. This value is set at 60 by default. Accepted values: 1 to 120.
	Telephone communicator parameters	Call all voice/digital/SIA-IP numbers	If several voice calls (digital or SIA-IP) generated by the an event are waiting in the outgoing call queue, the control panel will attempt to send voice calls to all the numbers of this type.
		Access DTMF menu without code	When the control panel makes voice calls, it will allow access to the user menu over-the-phone using the parameters and enablements of the last user code of the control panel model (code 30, 50 or 100).
		Start message after dialling	The control panel will start the voice message 5 seconds after dialling the respective contact number.
		Confirm call with "*"	The control panel will consider the voice call successful when the recipient presses the "*" key on the phone keypad.
		UTC Time on SIA-IP	Calls to SIA-IP type numbers will contain the date and time in "UTC" format (Coordinated Universal Time).
Increase DTMF sensitivity		Option that increase the sensitivity of incoming DTMF tones.	
No SIA/SIA-IP strings		The descriptive strings will not be sent in SIA/SIA-IP protocol.	
Arm/Disarm inverted on C.ID		Partition arming events using CONTACT-ID protocol will send the "New event/Event activation" code when the partition arms, and the "Event ended/Event restore" code when the partition disarms.	
Generates one call only for each event		If this option is enabled, it blocks all the calls programmed for an event after the first successful call. If the options "Call all voice/digital/SIA-IP numbers" are enables, then the latter have priority.	
Stop calls on disarm with no alarms		The control panel will not carry out the calls programmed for disarm events when there is no active alarm or alarm memory present.	
Number of voice mess. repetitions		This value determines the number of times the voice message will be played during the call (from 1 to 15).	
Number of attempts		This value determines the number of calls attempts the system will make before deleting the contact number from the call queue (from 1 to 15).	
Delay on line-down signal	This parameter allows you to program the delay, expressed in seconds or minutes, which will be applied before signaling of "line down" events.		
Teleservice parameters	Telephone number 15 reserved for teleservice	Telephone number 15 in the phonebook is reserved for teleservice (maintenance over-the-phone). If an end-user makes a request for teleservice, the control panel will contact this number.	
	Installer callback	The control panel calls the teleservice number after the installer's call to the control panel	
Cloud Settings	Exclude Nexus from Cloud	If enabled, this option denies access to Cloud through the Nexus. The latter continues to operate normally.	

Click on the node of the **Telephone** option to access a list of all the contact numbers. Select the required number to view and program the respective parameters.

Node	Group	Option
	Description	This is an editable field for the code user's phone number, to be customized by the installer.
	Telephone number	Editable field for the contact number (maximum 20 digits). Accepts also ", " (= 2 second pause), "*" and "#".
	Type	Telephone number type: <ul style="list-style-type: none"> • None - the selected number can receive SMS text messages only • Voice - the selected number can receive voice calls and SMS text messages If the number refers to the Alarm Receiving Centre, assigns the ARC protocol (reporting format): <ul style="list-style-type: none"> • Ademco 10bps, Ademco 14bps, Franklin 20bps, Radionics 40bps, Scantronic 10bps, CONTACT-ID, SIA, Ademco Express, CESA, SIA-IP, Cloud
	Account code	This is the 4-character alphanumeric code which identifies the caller in reports to the Alarm Receiving Centre.
	Channel	Checkbox for the selection of the channel on which the call can be routed: <ul style="list-style-type: none"> • PSTN • Nexus • SmartLAN
	Receive SMS	This option allows the phone number to receive an SMS message from the Nexus GSM module, as well as all other event-related communications.
	Encryption	This field allows you to select the SIA-IP protocol encryption type: <ul style="list-style-type: none"> • None • AES 128 bit • AES 192 bit • AES 256 bit After selecting the type is necessary to indicate the encryption key.
	Toggle channel on call failure	This option, in the event of call failure on a channel, enables the control panel to carry out call attempts on an alternative channel (Nexus) and then retry on the original channel in order to alternate the set number of attempts.
	SIA-IP	If a phone number is configured as "SIA-IP", you must program the IP address and the SIA-IP receiver port in this section.
	Partitions	You can associate each phone number with specific partitions. By selecting the partitions, you can enable/disable users (who have at least one of these partitions in common with the phone number) to modify the number concerned.



Events 5-14

Parts of the system	Programming section		
	The Events option, from the system tree, gives access to the buttons and outputs in the Programming section which allow for the management of the event activation and restore actions.		
	Group	Option	
<pre> graph TD SmartLiving[SmartLiving System] --- Partitions[Partitions] SmartLiving --- Terminals[Terminals] SmartLiving --- Arming[Arming scenarios] SmartLiving --- Timers[Timers] SmartLiving --- Users[Users] SmartLiving --- Telephone[Telephone] SmartLiving --- Events[Events] style Events fill:#add8e6 </pre>	Reset default	Button to reset the default values of the digital communicator for all the events.	
	Event maintenance	Delete activation/restoral outputs	The sections with a Delete button allow you to delete all the outputs associated with the activation/restore actions of each event.
		Delete activation/restoral calls	The sections with a Delete button allow you to delete all the phone calls associated with the activation/restore actions of each event.
		Delete voice message playbacks on activation/reset	The sections with a Delete button allow you to delete all the voice message on keypad playbacks associated with the activation/restore actions of each event.
		Reset default SIA protocols	This section provides a Reset default button that resets the default settings of SIA protocol codes for all the events.
		Delete shortcuts on event	This section provides a Delete Shortcuts button that cancels the "Shortcut on event" parameters on all the events.
Configure other outputs	This section allows you to configure the set of outputs selectable for each individual event in the Other outputs section. 16 outputs are available for the activation of the event and 8 for its restoral, all selectable via boxes between the outputs already configured in the Terminals section.		

Output scenarios	<p>This section provides the list of the 50 available scenarios. Selecting one of them will allow you to use the programming area, alongside the list, to configure each of the 10 outputs available.</p> <p>For each of these it is necessary to indicate the output (from those configured) and the activation type:</p> <ul style="list-style-type: none"> • 0/100, percentage value for the dimmer outputs or analogue outputs of a Flex5 expansion. • ON, command that activates the output or changes the activation status if the output is a "switching" type output. • OFF, command that deactivates the output • Force ON, command that activates the output • Toggle, command that changes the activation status of the output
-------------------------	---

Click on the node of the **Events** option, from the system tree on the left, to access the list of all the event types. The Event Type option accesses a table, in the **Programming** section, in which each line corresponds to an event and each column corresponds to a parameter for each event.

A right click in this section allows you to carry out the following operations on the boxes of the selected column:

- Activate the selection of all boxes
- Deactivate the selection of all boxes
- Invert the selection of all boxes

Click on the node of the Event Type to access a list of all the events. Select the required event to view and program the respective parameters.

Node	Group	Option	
<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <p>Events</p> <ul style="list-style-type: none"> Zone alarm <ul style="list-style-type: none"> PANEL T01 PANEL T02 PANEL T03 PANEL T04 PANEL T05 </div> </div>	Actions	<p>The actions are arranged on lines in a table, each with a check box for the activation of the action when the event occurs and a check box for the activation of the action when the event restoral.</p>	
		Tel. number	This section allows you to select the telephone numbers to call on event activation/restoral.
		Voice message on keyp. 001	Activation of the voice message playback on keypad must be set at address "001" on activation/restoral of each event.
		Output	The output to be activated on activation/restoral of each event can be selected from the check-box list.
		Activate periodic event	When the event occurs, the system will generate the Periodic event.
		Clear call queue	When the event occurs, the system will cancel the outgoing call queue.
		Memory	If this option is enabled, activation/restoral of the event will be saved to the events log.
		Output scenarios	This section provides boxes for the selection of one of the 50 output scenarios, a field for event activation and one for event reset.
Shortcut on event	<p>Programming field for the selection of a control panel operation that will be activated automatically when the event occurs.</p> <p>This field is followed by a further two fields for the definition of the respective parameters.</p>		
Sounder pattern	If a sounder/flasher is included in the outputs, its activation will occur in accordance with the selected pattern.		
Silent event	If the event occurs, the system will generate silent calls which will not be signalled on the keypads.		
Priority event	Calls associated with this type of event have priority over all other calls. Therefore, if a priority event occurs, any ongoing calls will be interrupted and the priority-event call will be sent immediately.		
Force on alternative channel	Calls associated with this type of event will be made via the alternative channel of the channel programmed for each phone number (see Channel on <i>paragraph 5-13 Telephone</i>).		
Voice communicator	<p>This section allows you to program the voice message associated with the activation/restoral of the event.</p> <p>This message is a combination (to be selected by the installer) of the messages that, when necessary, will be played back in the following order:</p> <ol style="list-style-type: none"> 1. "Restoral" - plays when the event restores 2. Type - indicates the event type 3. Message A 4. Message B 5. Send address - plays the message associated with the registered address <p>You can view the sequence of messages in the table on the right of the section, and listen to them by pressing the respective button .</p> <p>You can select individual messages by means of the check boxes on the left.</p>		
Automatic dialer	<p>If this option is enabled, the system will configure an optimal sequence of the messages for the activation/restoral of the event.</p> <p>It is however possible to choose different messages from those available, but the option activated in this way imposes a limited choice depending on the type of event.</p>		

Digital communi- cator	Class code	This is the CONTACT-ID reporting format Class-Code which corresponds to the event.
	Event Code on activation/restoral	This is the 2-character alphanumeric code, which corresponds to the activation/restoral of the event sent the alarm receiving centre (ARC).
	SIA protocol	If the event is associated with calls using SIA protocol or SIA-IP, this parameter allows you to program the event code in accordance with SIA standard by selecting it from the list.
Other outputs	This section allows you to activate additional outputs (besides the one programmed for the "Outputs" parameter) in connection with the verification or restoral of the event. These outputs must be selected from those set up in the Configure other outputs section and are common to all the events.	
Nexus	Enable SMS mess.	When the event occurs, the control panel will send an SMS message to all the duly enabled phone numbers (refer to <i>paragraph 5-13 Telephone</i> , "Receive SMS" parameter).
	Automatic SMS mess.	If enabled, the dispatched SMS message will consist of the event description contained in the Events log.
	SMS number	If the "Automatic SMS" option is not activated, an SMS message from the 50 available on the Nexus will be sent (refer to <i>paragraph 5-5 Nexus</i> , "Receive SMS" parameter).
Programmable event		When you select a programmable event from the SmartLiving system tree on the left, the Programming section on the right will provide the previously-described programming parameters and a button (at the top) which opens a window where you can formulate the event. This window allows you to edit the programmable event as a logical-mathematical formula using events, timers and counters.

Shortcut on event 5-14-1

Exclusively via software, it is possible to program for each event the shortcut that will be activated on the activation of the event itself.

These shortcuts function differently from those which can be activated by the user (refer to *Appendix A, Shortcuts by default*) and allow the control panel to activate automatically determined operations when the event occurs.

The programming phase can be accessed via the SmartLeague, by selecting the event from the system tree menu (on the left) that is to be assigned to the shortcut on the respective "Programming" page (on the right). The "Shortcut functions" section provides check boxes that allow the selection of the shortcut and definition of the relative parameter:

Table 5-1: **Shortcut on event**

Shortcut	Function	Parameter
Activate scenario	Shortcut that activates the scenario selected in the checkbox alongside.	One of the 30 shortcuts available
Activate output	Shortcut that activates/deactivates the output selected in the checkbox alongside.	One of the configured outputs
Deactivate output		
Zone bypass	Shortcut that deactivates/activates the zone selected in the checkbox alongside.	One of the configured zones
Unbypass zone		
Disable code	Shortcut that deactivates/activates the code selected in the checkbox alongside.	One of the available codes
Enable code		
Disable key	Shortcut that deactivates/activates the key selected in the checkbox alongside.	One of the available keys
Enable key		
Activate thermostat	Shortcut that activates the keypad thermostat in the mode selected in the checkbox alongside.	One of the keypads available Thermostat operating mode
Deactivate thermostat	Shortcut that deactivates the keypad thermostat selected in the checkbox alongside.	One of the keypads available
Dimmer up	Shortcut that increases/decreases the set value of the voltage supplied to the dimmer output selected in the check box alongside.	One of the outputs configured as dimmer
Dimmer down		
Delete alarm memory	Shortcut that deactivates the outputs relative to zone/partition alarm and tamper events and deletes the partition and system alarm and tamper memories. This shortcut operates on the partitions selected for the scenario.	One of the 30 shortcuts available

Output scenarios 5-14-2

The assignment of the activation shortcut of an output scenario to the activation and deactivation trigger of each event can be done via the SmartLeague software program only.

The SmartLiving control panel provides 50 output scenarios, each with a maximum of 10 outputs.

Programming occurs in two phases: the first is the definition of the scenarios, the second is the assignment to the activation and restoral of the event.

From the system tree menu on the left, select the "Events" option, the "Output Scenarios" list will appear in the "Programming" section on the right.

There are 50 scenarios available in the list. Selecting one of them will allow you to use the programming area, alongside the list, to configure each of the 10 outputs available.

For each of these it is necessary to indicate the output (from those configured) and the activation type:

- **0/100**, percentage value for the dimmer outputs or analogue outputs of a Flex5 expansion.
- **ON**, command that activates the output or changes the activation status if the output is a "switching" type output.
- **OFF**, command that deactivates the output
- **Force ON**, command that activates the output
- **Toggle**, command that changes the activation status of the output

From the system tree menu on the left, select the event that is to be assigned to the scenarios on the respective "Programming" page on the right.

The "Output scenarios" section provides two programming fields for the selection of the scenarios, one relating to activation of the event and the other to its restoral.

SCENARIO DEFINITIONS

SCENARIOS ON EVENTS

Programmable events 5-14-3

A group of events is available for installer programming. Event activation and restoral depend on a combination of other control panel events based on logical operations, counters and timers.

On account of their enhanced flexibility, special attention is required during the programming and testing phases of the programmable events. The effects of the programmable events must always be rigorously tested.

Each programmable event consists of a structure of mathematical-logical operations, counters and timers. The programming structure consists of:

- 10 programmable events for SmartLiving 505 and 515 control panels, 30 for SmartLiving 1050 and 1050L and 50 for SmartLiving 10100L
- 40 timers
- 10 counters

This programming process can be done only via the SmartLeague software programme. Select a programmable event from "SmartLiving System - Programmable event" from the tree menu on the left, then go to the "Programming" template on the right. The  key (next to the data transfer buttons) opens a window which will allow you the define the event. This window is divided into two sections:

- Equation
- Timers and counter details

Table 5-2: Programmable event

A	Section for the compilation of the logical expression.	
B	Section for the definition of the timers and counters.	
C	Selection field and button for the inclusion of the verified control-panel event to be included in the equation. The restoral of the event is included using the event followed by the "NOT" operator.	
D	Selection field and button for the inclusion of the timer.	
E	Selection field and button for the inclusion of the counter.	
F	Selection field and button for the inclusion of the button.	
G	Button for entering the logical operators in the expression.	
H	Buttons for the deletion of the entire expression or the last element of the expression.	
I	Field for the visualization of the expres- sion.	
J	Button for the commutation of the visual- ization mode of the equation (parameters/ descriptions of parameters).	
K	Field for the addition of eventual notes..	

The logical expression of the event includes various parameters, which may have a "real" value (either "1" or "active" - as in the case of a verified event) or a "false" value (either "0" or "not active" - as in the case of a restored event):

EQUATION

A timer is a logical expression element (it may have an "active" or "non active" value). It is characterized by an interval, therefore, you must specify an interval (in seconds) for each timer you wish to include.

TIMERS

You can select up to four "Start events" (i.e. control panel events which trigger the timer) and up to four "Reset events" (i.e. control panel events which interrupt the timer). You can specify the "Edge" for each of the eight events, that is, the status passage of the selected event ("Activation", "Reset" or "Both").

The last two options allow you to choose when the timer will be "active":

- **Timer active on Start event.** The timer will become "active" on start, that is, when a start event occurs, and will remain "active" for the sat time. The timer will become "non active" when the set time expires or when a reset event occurs.
- **Timer active with delay.** The timer will remain "non active" on start, that is, when a start event occurs and will remain "non active" for the specified time. The timer will become "active" when the specified time expires.

A timer with the "timer active with delay" option enabled will remain "active" until a reset event makes it "non active" again.

Note

A counter is a logical expression element. It is characterized by an increasing value ("Count"). The counter will have a "non active" value until it reaches the set value, which will take the counter to the "active" value.

COUNTERS

You can select up to four "Start events" (i.e. control panel events which increase the counter value) and up to four "Reset events" (i.e. control panel events which annul the counter). You can specify the "Edge" for each of the eight events, that is, the status passage of the selected event ("Activation", "Reset" or "Both").

It is necessary to define an "Autoreset" time that will zero the count when, between two successive increases, a superior time elapses. If you do not desire an "Autoreset" time, you must set the time at "65535" (already set at default), in order to ensure that the count never expires.

You should not set an "Autoreset" value of less than 5 seconds.

Note

Once the event programming process is complete and the event is sent to the control panel, the event programming values will be checked for errors.

If you want to generate an alarm (i.e. activate sounder/flashers and calls) when only two PIRs (DET1 and DET2) go into alarm status within a pre-set time.

EXAMPLES

- T0000; timer 1 will activate when the "Zone alarm DET1" Start event activates for 30 seconds

- T0001; timer 2 will activate when the start event of the "Zone alarm DET2" S activates for 30 seconds
- Both conditions must occur together (AND)
T0000 AND T0001
- Therefore, it is necessary to set the activation of the sounder/flasher and calls on the event configured in this way.
- If the programmable event activates an on-BUS sounder/flasher, associate its deactivation with an event.

If you wish to activate an output for 40 seconds when key 17 is used to arm partition 1, and to disarm and the same output when the partition disarms.

- T0000; associate timer 1 with the activation of the Start event of key 17 recognition
- T0000; timer 1 with a 40 second timeout, "timer active with delay" option enabled
- T0000; associate timer 1 with the restoral of the reset event of partition 1
- Programmable event 1 must be programmed as:
T0000
- Select the output you wish to activate in concurrence with the programmable event
- If the programmable event activates an on-BUS sounder/flasher, associate its deactivation with an event.

If you wish to receive a phone call when a zone q, which belongs to partitions 1 and 2, is violated and one of the two partitions is armed

The automation zone q always generates the zone alarm event (even when the partitions are disarmed). However, the programmable event will occur only when the zone q is in alarm status and at least one of the two partitions is armed.

- Configure zone q as "automation" belonging to partitions 1 and 2
- Remove all the outputs and phone calls associated with the "Alarm zone q" event
- The programmable event must be programmed as "Alarm zone q" AND ("Partition 1 armed in away mode" OR "Partition 2 armed in away mode"):
E0010 AND (E0790 OR E0791)
- Associate the programmable event with the phone call you wish to receive

If you wish to activate a telephone call after 3 consecutive wrong code entries (with a maximum of 120 seconds between each entry).

- C0000; counter 1 will activate on activation of the "False code" Start event, with a count of 3, 120 second autoreset time
- The programmable event must be programmed as:
C0000
- Associate the programmable event with the phone call you wish to receive

If you wish to activate a telephone call and output when at least two detectors out of 5 go into alarm status.

- The programmable event must be programmed as ("Alarm zone 1" + "Alarm zone 2" + "Alarm zone 3" + "Alarm zone 4" + "Alarm zone 5") >= 2
(E0000 + E0001 + E0002 + E0003 + E0004) >= V0002

Associate the programmable event with the phone call you wish to receive and the output you wish to activate.

Voice messages 5-15

The Parameters settings template of the "SmartLiving System - Voice messages" will allow you to:

- upload all the voice messages
- download all the voice messages
- format voice board

Parts of the system	Programming section		
<ul style="list-style-type: none"> + Keypads + Proximity readers + Expansions + Sounder/flashers - Nexus - SmartLiving System <ul style="list-style-type: none"> + Partitions + Terminals + Arming scenarios + Timers + Users + Telephone + Events + Voice messages 	The Voice messages option, from the system tree on the left, accesses the Programming section which provides the voice message read/write buttons and a section for the formatting of the SmartLogos30M voice board.		
	Group	Option	
	Read all messages from the control panel	Button that allows the reading from the control panel of all the messages on the voice board.	
	Write all messages on the control panel	Button that allows the writing on the control panel of all the programmed voice messages.	
	Format SmartLogos board to version ...	This section allows you to format the SmartLogos30M voice board to the version which corresponds to the control panel firmware of the solution you are working on.	
		Check SmartLogos board	Button to start a check on the voice board and obtain information regarding its firmware version.
Format the voice board		Button to start the formatting process of the voice board in order to align the firmware version with that of the control panel. The following formatting options are available: <ul style="list-style-type: none"> • Preserve previously-recorded messages • Format using default messages 	

Click on the node of the **Voice messages** option, from the system tree on the left, to access the list of all the message types. The Message type option accesses a table, in the **Programming** section, in which each line corresponds to an individual message and each column corresponds to a parameter of each message.

Node	Group	Option	
<ul style="list-style-type: none"> - Voice messages <ul style="list-style-type: none"> + Free messages + Arming scenario mes + Shortcut messages + Pre-recorded messag + Zone messages + Partition messages + Code messages + Key messages + Keypad messages + Proximity reader mes 	Buttons		Button to start the text-to speech process of the messages selected in the table. The texts entered in the Text to speech section will be converted into audio files and associated with the selected messages.
			Button to open a window for text-to-speech setting changes.
			Button to invert the selection of the messages listed in the table.
			Button to delete all the selected messages.
			Button to reset to default programming the audio files of the messages selected in the table.
			Button to playback the audio file associated with the message.
		Nr.	Message index inside the voice board memory.
	Options	Description	This is an editable field for the message description.
		Type of coding	Type of coding for the message: <ul style="list-style-type: none"> • No Message, no playback, no recording • High quality, for superior recording/playback quality • Average quality, for recording/playback quality comparable to phone-line quality.
		Quality	Checkbox to indicate the recording quality of the associated audio file.
		Time	This is the duration of the associated audio file (expressed in seconds).
		Text to speech	Text of the associated audio file.

Click on the node of the Message Type option to access a list of all the messages. Select the required message to view and program the respective parameters.

Node	Group	Option	
<ul style="list-style-type: none"> [-] Voice messages <ul style="list-style-type: none"> [-] Free messages <ul style="list-style-type: none"> Message 1 Message 2 Message 3 	Message category	This is the message type the selected message belongs to.	
	Note	This field allows the editing of a text to associate with the message.	
	Recorder	This section provides software for the playback and recording of audio files. This software allows you to edit the audio file associated with the message and: <ul style="list-style-type: none"> • Load an audio file (.wav) • Play the loaded audio file • Record a new audio file • Reset the selected file to default 	
		Good/Average Quality	Button for the selection of the sound quality of the audio file.
	Text to speech	This section allows the editing of the text which will be converted to an audio file and associated with the message. The conversion and association with the message will occur after the execution of text to speech (in this section this can be done using the record button).	

Icons and shortcuts 5-16

Parts of the system	Programming section		
<ul style="list-style-type: none"> [-] Keypads [-] Proximity readers [-] Expansions [-] Sounder/flashers Nexus [-] SmartLiving System <ul style="list-style-type: none"> [-] Partitions [-] Terminals [-] Arming scenarios [-] Timers [-] Users [-] Telephone [-] Events [-] Voice messages [-] Icons [-] Association Shortcut-Icon 	There are two sections in the SmartLeague system tree where you can edit the shortcut icons which appear on the keypad display, in relation to function keys F1 to F12.		
	Group	Option	
	Icons	Click on the node of the Icons option to access a list of the 50 available icons. Select the required icon from the Programming section on the right, to access a page where you can edit the selected icon. In this section you can edit for each icon:	
		Description	This is the descriptive string associated with the icon.
		Draw	You can change the icon by means of digital graphic instruments.
Association Shortcut-Icon	The Shortcut-Icon association option, in the Programming section on the right, accesses a table showing all the shortcuts arranged on lines. Select one of the 50 available icons from the Icon column in order to associate it with selected shortcut. Click on the node of the Shortcut-Icon association option to access a list of the 36 available shortcuts. Select the required shortcut from the Programming section on the right and associate it with an icon by means of a check box then visualize the selected icon.		

SmartLAN 5-17

Parts of the system	Programming section		
<ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions ⊕ Sounder/flashers — Nexus ⊖ SmartLiving System <ul style="list-style-type: none"> ⊕ Partitions ⊕ Terminals ⊕ Arming scenarios ⊕ Timers ⊕ Users ⊕ Telephone ⊕ Events ⊕ Voice messages ⊕ Icons ⊕ Association Shortcut-Icon <li style="background-color: #e0f0ff;">⊕ SmartLAN settings 	<p>The SmartLAN configuration option from the system tree allows you to read and program the parameters of the SmartLAN/G Ethernet interface board.</p> <p>The read programming data comes directly from the SmartLAN board memory, similarly the sent programming data is saved to the memory of the board connected to the control panel and not to the control panel memory.</p>		
	Group	Option	
	LAN board	<p>This section allows you to configure the LAN board inside the network it is connected to.</p>	
		Connection parameters	<ul style="list-style-type: none"> • IP Address • Subnet mask • Gateway • DNS • Obtain IP address automatically - if enabled, the previously-mentioned data will not be required, DHCP will be used. • Communication port • Web server port • SSL port • Timeout (ms) • Enable UPnP - this option enables UPnP protocol which automatically activates "port-forwarding" through the network router of the communication, web and SSL ports (indicated above).
		Account	<ul style="list-style-type: none"> • User name • Password
		E-mail parameters	<ul style="list-style-type: none"> • Subject - this field is for the "Subject" of the e-mails. When the SmartLAN/G board sends an e-mail it will use the description of the event type as the subject. • Sender - this is the e-mail address of the sender. • Mail Server - this is the address of the SMTP server of outgoing post. • Port - this is the out port of the post server (SMTP). • Account - this field is for the selection of a domain for which an automatic configuration of the parameters can be obtained by pressing Preconfigure. • SSL Method • Timeout (s) - selection field for the maximum time (from 60 to 300 seconds) within which the control panel must send an email to the post server. • Authentication request - if the SMTP server requires authentication, enable this option and then set the following: <ul style="list-style-type: none"> • User name • Password
		Dynamic DNS	<p>If a dynamic public IP address is available, you may find it useful to use a domain name which will allow you to trace your SmartLAN device at all times.</p> <p>SmartLeague supports the service offered by:</p> <ul style="list-style-type: none"> • dyndns.org • freedns.afraid.org • no-ip.com • camsec.net • inimdns.it <p>By registering at one of these addresses, you will obtain the access data required in this programming section:</p> <ul style="list-style-type: none"> • Domain • User name • Password • Update every - interval (expressed in seconds) applied by the SmartLAN when upgrading the association of the selected domain with the public IP address. • Test DDNS account - button to start DDNS account verification (for "inimdns.it" service only).
NTP client configuration	<ul style="list-style-type: none"> • Enable NTP synchronization - if enabled, the SmartLiving control panel clock will be synchronized by NTP, therefore, it will be necessary to indicate: • Server • Update every - this is the time, expressed in seconds, that elapses between successive time updates. 		
Modbus	<ul style="list-style-type: none"> • Enable Modbus - if enabled, the Modbus/IP service on SmartLAN/G will be activated; in this case it is necessary to indicate: • Port • Access Codes 		
Contacts	<p>You can save up to 20 e-mail contacts.</p> <p>The contacts can be saved in this page but can also be changed in other parts of the application (instructions follow).</p>		

	This section allows you to configure the parameters for outgoing e-mails generated by the activation or restoral of events with the "Memory" option enabled (refer to <i>paragraph 5-14 Events - Actions - Memory</i>).
Event type	Selection field for the selection of type of events to be programmed. The application will show all the programmable events for the selected type.
Activation / Restoral	The Activation and Restoral sections are the same and are intended, respectively, for the programming of the dispatch of e-mails when the event occurs (Activation) and when the event ends (Restoral).
Sel	If you click on the respective check boxes of events with this option enabled, you can program simultaneously the recipient contacts, text and attachments, as described in the following paragraphs. If you right click on the header on this column, you will be able to carry out selections/deselections which involve all the control panel events or all the events of the same type.
Events log	If this option is enabled, the message text of the event will be saved to the control panel memory. If you right click on the header on this column, you will can carry out selections/deselections which involve all the control panel events or all the events of the same type.
Recipients	Double click on the respective check box to access the e-mail addresses in the contact list. The Contacts window allows you to select and change the e-mail addresses of the recipients. There are 3 buttons: <ul style="list-style-type: none"> • Apply - this option allows you to add or delete the recipients of the selected event only. • Apply to events of the selected group - this option allows you to add or delete the recipients of all events of the same type as the selected event. • Apply to all the selected control panel events - this option allows you to add or delete the recipient contacts for all the selected control panel events.
Text body	This option allows you to edit the text body of the e-mail for each event. Double click on the respective event field to access the message Text body window where you can write a text of up to 512 characters on several lines. You can also add links for direct access to web pages or LAN devices (for example, IP cameras), in this case, you must always include 'http://'. The 3 buttons Apply , Apply to events of the selected group and Apply to all the selected control panel events have the same functions as previously described. If the mouse arrow is positioned on the text body, the contents will be shown as a tooltip.
Attachment	This allows you to attach a document/file to the e-mail for each event. A double click on the checkbox of the selected event accesses the Explore window where you can load or cancel the selected file from the SD-card. The 3 buttons Apply , Apply to events of the selected group and Apply to all the selected control panel events have the same functions as previously described.
Camera	It is possible to associate a camera to each event. A double click on the relative field of the selected event will open the Select Onvif camera window. This window will allow you to select a camera from those configured and select two presets for it. The presets can be selected from those listed after updating the dedicated section (refer to <i>paragraph 5-17-1 ONVIF cameras</i>). The 3 buttons Apply , Apply to events of the selected group and Apply to all the selected control panel events have the same functions as previously described.
Record on SD	If enabled, the recorded frames will be saved to the SD card that is inserted into the SmartLAN board.
Graphic map	This section will allow you to configure the graphic maps which the user has access to through the web interface (refer to <i>Chapter 7 - Graphic map configuration</i>).
ONVIF camera management	This section will allow you to configure the Onvif cameras connected to the SmartLiving system (refer to <i>paragraph 5-17-1 ONVIF cameras</i>).

ONVIF cameras 5-17-1

Remote ZTL control and preset audio/video profiles allow hassle-free user interaction with ONVIF protocol cameras.

The SmartLAN/G board provides support for JPEG and MJPEG streams for surveillance cameras and allows users to retrieve and view video recordings and snapshots. Interaction with ONVIF cameras allows viewing of recorded images (videos and snapshots) previous to and after the occurrence of an event.

The frames are sent as attachments to emails associated with events or are stored for viewing using a web interface or Inim Home App, through the "Camera" section.

To do this it is necessary to:

- program the ONVIF camera (using its own presets), provide it with the ZTL presets necessary for viewing the zone under surveillance and recorded video
- associate a camera with an occurrence (activation or restoral) of an event through the **Email configuration parameters** (see above)
- activate the **Record on SD** option (see above) for the viewing of recorded frames through a web interface
- using the SmartLeague software, configure the ONVIF camera in the SmartLiving system by selecting **SmartLAN configuration** from the tree structure on the left and then going to **Programming - ONVIF camera management** on the right.

This section provides a pane containing the list of the configured cameras. At the side of this is another section containing the parameters relative to the selected camera:

Option	
 	Buttons for the addition of a new camera or for the deletion of a selected camera.
Description	This is the description of the selected camera.
IP Address Port User name Password	Parameter that permits access to the selected camera.
https	If selected, a secure HTTPS connection will be used.
Multimedial profile	Field for the selection of one of the multimedia profiles of the camera. These profiles are listed following a read operation requested by pressing the  button. The  button opens a window showing all the available profiles and where you can edit the "Token" and name of each one. The window provides two buttons: <ul style="list-style-type: none"> •  - for manual entry of a profile in the list •  - for deletion of the selected profile
Pan - Tilt - Zoom	This field indicates whether the selected camera is equipped with PTZ (Pan, Tilt, Zoom) capabilities.
Preset available for the selected profile	This section lists all the presets relating to the profile selected in the previously mentioned programming field. These presets are listed following a read operation requested by pressing the  button. The  button opens a window showing all the available presets and where you can edit the "Token" and name of each one. The window provides two buttons: <ul style="list-style-type: none"> •  - for manual entry of a preset in the list •  - for deletion of the selected preset
URI Snapshot URI Stream	This field allows you to view the addresses (URIs) of frames shots and audio/video streams. These presets are listed following read operation requested by pressing the  button.
Sampling frequency	This is the time that must elapse between two successive frame shots (max. 60 seconds).
Number of frames pre/post event	This is the number of frames (from 0 to 5) which will be saved to the memory before/after the occurrence of the event the camera is associated with.
Images	The image in the lower part of the section reproduces the frame of the camera selected after pressing the  button. Clicking on the image opens window for the viewing of filming in real-time, control of the camera functions and visualization of the available presets.
Include Security Header in messages	This option, if enabled, includes the 'Security Header' in the SOAP messages for the communication with Onvif devices.

Wireless transceiver

5-18

Parts of the system	Programming section	
<ul style="list-style-type: none"> ⊕ Keypads ⊕ Proximity readers ⊕ Expansions ⊕ Sounder/flashers Nexus ⊖ SmartLiving System <ul style="list-style-type: none"> ⊕ Partitions ⊕ Terminals ⊕ Arming scenarios ⊕ Timers ⊕ Users ⊕ Telephone ⊕ Events ⊕ Voice messages ⊕ Icons ⊕ Association Shortcut-Icon <ul style="list-style-type: none"> SmartLAN settings Wireless transceiver 	<p>The Wireless transceiver option from the system tree allows you to read/write the Air2-BS20 transceivers connected to control panel.</p> <p>It provides two sections:</p> <ul style="list-style-type: none"> • Wireless transceivers, for display of the transceivers and their enrolled devices • Sounder and keypad data test, for a configuration test on all the keypads and sounders detected by the system 	
	Wireless transceivers	 <p>The "Read" button accesses the Wireless window where you can select the transceiver (from those in the system configuration) you wish to read.</p> <p>Following, in the Programming section, a number of boards appear, equal to the number of transceivers read; each board shows:</p> <ul style="list-style-type: none"> • the icons of the configured devices and terminals • the serial numbers of all the enrolled devices • the firmware version of the transceiver board <p>Furthermore, it is possible both to read and change:</p> <ul style="list-style-type: none"> • the wireless channel in use • the enablement of the open/dislodgement tamper protection • the enablement of the rolling code <p>The data relating to the wireless transceiver can be saved in the SmartLeague solution. Any changes will become operative only after the "write" phase.</p>
		 <p>The "Read" button accesses the Wireless window where you can select the transceivers (from those configured) that must be programmed.</p> <p>In this way it is possible to replace Air2-BS20 transceivers quickly and without the need to re-enroll all the wireless devices.</p> <p>This procedure can be used only when the transceiver data has been previously read and saved in the SmartLeague solution.</p>
		 <p>Button to start the guided cloning process for the wireless keys enrolled by the transceiver of the selected board.</p> <p>The guide allows the installer to indicate which transceiver, from those selectable, the cloned keys will be assigned to.</p>
Sounder and keypad data test	<p>This section lists the keypads and sounders found or in the configuration with their respective configurations and the results of the consistency check between configurations.</p> <p>Refer to <i>paragraph 5-18-1 Sounder and keypad data test</i>.</p>	

Sounder and keypad data test 5-18-1

Click on the **Check consistency** button to initiate a cross-check between the devices (sounders and keypads) in the control panel configuration, those recognized as wireless and those present on the wireless transceiver.

The outcome of this check will be displayed with a list of devices and their respective configurations:

- **In configuration**, for a device in the control panel configuration.
- **Wireless**, for a device recognized as a wireless device.
- **On transceiver**, for a device in the Air2-BS200 wireless transceiver configuration.

If an inconsistency is highlighted, the process provides a **Fix** button which restores a coherent situation after a request for confirmation.

The following table lists the various configuration conditions of the devices the software detects and, in the case of inconsistent conditions, the correction proposed by the **Fix** button:

Device condition detected	Combination of configurations			Outcome	
	In configuration	Wireless	On transceiver	Test result	Correction
Device is not configured and not detected (potential configuration available)	No	No	No	Fix	Device unenrolled from each configuration
Device enrolled by the transceiver but not in the control panel configuration.	No	No	Yes	Fix	Wireless device both in the control panel and transceiver configurations
Wireless device detected but not in the control panel configuration	No	Yes	No	Fix	Device unenrolled from each configuration
Wireless device detected and enrolled by the wireless transceiver but not in the control panel configuration	No	Yes	Yes	Fix	Wireless device both in the control panel and transceiver configurations
Device wired and in configuration	Yes	No	No	Ok	/
Device in both the control panel and wireless transceiver configurations but not detected	Yes	No	Yes	Fix	Wireless device both in the control panel and transceiver configurations
Wireless device in the control panel configuration only	Yes	Yes	No	Fix	Device unenrolled from each configuration
Wireless device configured correctly	Yes	Yes	Yes	Ok	/

Events log 5-19

Parts of the system	Programming section			
<ul style="list-style-type: none"> + Keypads + Proximity readers + Expansions + Sounder/flashers - Nexus - SmartLiving System <ul style="list-style-type: none"> + Partitions + Terminals + Arming scenarios + Timers + Users + Telephone + Events + Voice messages + Icons + Association Shortcut-Icon - SmartLAN settings - Wireless transceiver <li style="background-color: #0070C0; color: white; padding: 2px;">Events log 	The Programming section of the Events log allows you to view all the events saved to the control panel log. The lines on the table show the individual events and the columns show the following categories.			
	Group	Option		Note
	Num.	Number which indicates the chronological order of the events in the log.	You can group the events into categories by dragging the header of the required category to the grey line above the columns.	
	Date/Time	Event date and time		
	Event	Type of event		
	Filter	Parameters for further event details.		
	Agent			
	Location			
	Category	Logic grouping of events		
	Events log from database		Button to save the contents of the events log to the database.	These buttons are active only when you are working on a solution or a database. In particular, the "Save" button becomes active only after a reading from the control panel.
		Button to load the contents of the events log from the database. A from-to period will be requested, if no particular period is specified the entire contents of the Events Log will be loaded.		
		Button to delete the Events log from the database. A from-to period will be requested, if no particular period is specified the entire contents of the Events Log will be deleted.		

Chapter 6

MONITORING THE SMARTLIVING CONTROL PANEL

The SmartLeague provides a section where, after direct connection to the SmartLiving control panel, it is possible to carry out real-time monitoring on the entire system.

Select the **Check control panel, Monitoring** option from the menu bar.

A window will open with a header showing the control panel model and its firmware version. The window has several sections, selectable by means of the tabs at the top, each relating to different parts of the system.

Remote keypad 6-1

In this section the window is divided in two parts.

The left hand side shows all the keypads available for the system, but only those currently connected to the control panel are highlighted (in colour).

By clicking on one of the keypads in the field on the right, its exact replica will be visualized, it is possible therefore not only to view the display and the status of its LED, but also to issue commands by means of the buttons on the image.

The following buttons are available:

This refreshes the connection with the control panel and thus renew the images in the window.

REFRESH

This accesses a section relating the "thermostat" function.

THERMOSTAT ON KEYPAD

You can program the thermostat and also adjust its temperature setting and operating times.

The manual temperature setting and operating times can be implemented by means of the adjustment bars.

The **Temperature** section indicates the ambient temperature sensed by the thermometer which is reproduced in this section.

Button to open, at the bottom of the window, a section where it is possible to view the real-time status of the control panel.

CONTROL PANEL STATUS

A list of the basic functions of the control panel, the system parts and components will be shown and also information regarding the proper functionality of the system or any ongoing faults.

Partitions 6-2

This section, on the left, shows a list of icons which represent all the partitions the control panel zones are assigned to.

If you click on one of these icons, the right side of the window provides a section where you can view the status of the partition, its arming status and any tamper events.

After entering a valid code, the lower part of the window allows you to change the arming status of the partition and carry out partition reset operations.

Zones 6-3

This section is divided into three parts:

- The part on the left provides a list of all the partitions and the control panel zone groups.
- The part in the centre allows you to view the status of the zones which belong to the selected partition, the arming status of the zones and any tamper events.
The lower part provides a sub-section where, after entering a valid code, you can unbypass or bypass the selected zone.
- The section on the right allows you to view the status of the outputs.
The lower part provides a sub-section where, after entering a valid code, you can activate or deactivate the selected output.

Timers 6-4

This section shows the timer icons.

The status of each icon reflects the status of the respective timer and indicates, in real-time, whether it is enabled or not, or whether it is currently On (operating).

Peripherals 6-5

The SmartLeague provides several sections for peripheral monitoring purposes. selectable by means of the headers on the upper part of the section. In each of these sections the peripherals are represented by icons.

This section shows which keypads, readers and expansion boards, of those available, are included in the configuration and which of these are present or in tamper status.

PERIPHERALS

This section is further divided into several sub-section in accordance with the type of peripheral.

PERIPHERAL DETAILS

The **Update** button (bottom right) provides details of each peripheral:

- tooltips provide information regarding the peripheral model and whether it is present in the configuration or not
- the address, firmware version and operating voltage of each of the peripherals present is shown alongside the icon

Monitoring the IB100 BUS and Nexus communicator requires further selections achieved by ticking the respective check boxes.

Sounders on BUS 6-6

The monitoring phase on the sounders connected to the BUS provides feedback information regarding the sounders and their descriptions.

The information is provided alongside the respective icon: if the sounder is configured, the icon will be clear and accompanied by a description and the fault and tamper status icons, as follows:

Category	Icon	Notification
Alarms		Sounder/flasher loss
		Sounder active
		Flasher active
		STATUS LED On
		PRG LED On
		Sounder flasher tamper
		Foam tamper protection activated
		Wire cutting
		Blow torch protection activated

Category	Icon	Notification
Faults		Sounder broken
		Low battery
		Battery fault
Status		LED input activated
		Output FAULT active
		Output TAMPER active
		Sounder/flasher undergoing programming

Hedera wireless sounder

6-7

The **Real-time** programming section of a wireless sounder allows you to view its status. In this section, the monitoring window lists the parts of the sounder whose status is represented by icons/LED:

Option	LED colour	Status
Tamper	Green	Sounder/flasher not in tamper status
	Red	Sounder/flasher in tamper status (open or dislodged)
Antifoam	Green	Foam level below alarm signalling threshold
	Red	Foam level above alarm signalling threshold
Battery fault	Green	Battery charged
	Red	Battery charge low (below 40%)
Sounder active	Green	Audible signalling Off
	Red	Audible signalling On
Flasher active	Green	Visual signalling Off
	Red	Visual signalling On
STATUS LED ON	Green	STATUS LED off
	Red	STATUS LED On
PRG LED ON	Green	PRG LED off
	Red	PRG LED On

BUS isolators

6-8

This section monitors the functional status of the isolators on the BUS.

Select an isolator from the check box at the top of the section, by means of its address, then press the **Refresh** button, the **Monitor isolator** section will show the real-time value of the voltage and the course of any disturbance on the line.

The course of any disturbance during the time the two sections of the line were divided by the isolator (BUS-A and BUS-B) will be shown on two graphs. An assessment of the functional capacity of the isolator can be achieved by comparing the two graphs.

A **Reset** button is available to clear and restart the graphs.

Walk test

6-9

This section provides a quick and easy way of testing all the configured inputs.

Make the list of zones and the **Start Walk test** button.

Once the test starts, the installer can walk through the protected partitions and verify the proper detection capacity of all the inputs, by means of the information on the keypad display, or by means of the red dots and the time of the violations indicated in this section.

The **Print Walk test** button allows SmartLeague to print the results.

GRAPHIC MAP CONFIGURATION

The SmartLiving supervision functions are based on graphic maps which can accessed by the end-user through an Alien keypad or web interface.

The Alien keypad can manage up to 10 maps (revisions below 2.00 can manage up to 5 maps) and the web interface up to 20 maps. Each map accepts a maximum of 20 objects/buttons represented by icons.

The operability of the graphic maps depends on the use of a micro-SD card. The card must be inserted into the slot on the Alien keypad, for the configuration and access to the Alien keypad maps, or inserted into the slot on the SmartLAN/G Ethernet interface board for the web accessible maps.

Note

Parts of the system	Programming section		
<ul style="list-style-type: none"> [-] Keypads (1) <ul style="list-style-type: none"> Keyp. 001 (1) [-] Proximity readers [-] Expansions [-] Sounder/flashers [-] Nexus [-] SmartLiving System <ul style="list-style-type: none"> [-] Partitions [-] Terminals [-] Arming scenarios [-] Timers [-] Users [-] Telephone [-] Events [-] Voice messages [-] Icons [-] Association Shortcut-Icon SmartLAN settings 	<p>Access to the configuration of the maps is achieved through the sections:</p> <ul style="list-style-type: none"> Alien keypad graphic maps - select the keypad from the tree structure on the left then go to Programming - Alien Maps on the right. Web interface graphic maps - select SmartLAN settings from the tree structure on the left then go to Programming - Graphic Maps on the right. <p>A box, located in the centre of both sections, shows the images of the current map. Above this is a bar with the icons of the objects to be inserted and the buttons to edit the current map.</p> <p>To the left of this you will find the graphic-map tree with the objects inserted.</p>		
	Group	Alien	Web Interface
	Object icons	 <p>The objects are inserted by clicking on the respective icon on the bar and then by clicking on the point on the map where you wish to place it.</p> <p>Left-clicking on any one of the icons positioned on the map will highlight the icon which will then be shown in a frame that will allow you to resize or reposition it.</p> <p>Right-clicking on any one of the icons positioned on the map or map tree on the left allows you to delete the object concerned or change its settings; in this case a window will open showing all the editable settings (refer to <i>paragraph 7-1 Parameters of the icons and objects</i>).</p>	
		Button to show or hide the map tree located to the left of the displayed map.	
		Buttons for the addition of a new map in the last position on the map tree or for the deletion of the last map on the map tree.	
		Button for the insertion or overwriting of the background image of the current map. The name of the current image file is indicated in the lower section.	
		The selection of several icons by means of these buttons will allow you to create their alignment.	
		By selecting several icons, with these buttons it is possible to change their dimensions by assigning them the dimensions of the first icon selected (width, height or both).	
		Not available	The selection of an icon, by means of these buttons, will allow you to resize and reposition the icon so that it occupies a quarter of the image.

	<p>Button to start the procedure which converts the entire graphic map tree to Alien keypad format and web interface format.</p> <p>The conversion process does not delete the configuration of the keypad maps but it overwrites the configuration of the SmartLAN/G maps.</p>	<p>Button to start the procedure which converts the entire graphic map tree to Alien keypad format and web interface format.</p> <p>A window will open which requests the keypad from those configured, and the model.</p> <p>The conversion process does not delete the configuration of the SmartLAN/G maps but it overwrites the configuration of the Alien maps.</p>
	<p>Button to start the procedure which duplicates the configuration of the graphic maps of the current Alien keypad and transfers it to other Alien keypads.</p> <p>A window will open which will request the keypads, from those configured, which the configuration will be transferred to.</p>	<p>Not available</p>

Parameters of the icons and objects 7-1

Group	Option		Note
Size and position	Height, Width, Position X and Y	Number fields for the dimensions of the object icon and its position on the map.	
	String	Field for the string that appears over the icon.	For Alien only
		Button for the definition of the colour of the string.	
Control panel	Selection checkbox for the selection of the part of the anti-intrusion system the icon refers to.		Zone, partition, output, scenario, keypad
Map link	Field for the selection of the map the link refers to. For web interfaces it is possible to indicate the home page.		
Web cam	URL	Configuration parameters for the webcam.	For the web interface only.
	jpeg, m-jpeg		
Images	Section containing the icons which replace the current icons in the event of status change of the represented object. For Alien keypad maps, it is possible to indicate the strings that will appear (when the occurrence requires) below the current string, indicated previously mentioned.		
		Button for the selection of the image that will replace the default image.	
		Button for the cancellation of the selected image.	For the web interface only.
		Button for the definition of the colour of the string.	For Alien only
		Button to reset the factory default images	
Options	Command selection window	If enabled, touching the icon on the map will open a window on the display for command selection.	For Alien only. The commands implement a status change on the object. The type of status depends on the type of object: <ul style="list-style-type: none"> • Arming type - for a 'Partition status' object • Activation/Enablement status - for a 'Zone' object • Activation/Enablement status - for an 'Output' object • Activation/Enablement status - for a 'Scenario' object
	Command with authorization request	If enabled, the keypad will request user-code entry before activating the command associated with the icon.	
	Switch/Invert	If enabled, touching the icon on the map will immediately switch/invert the status of the object it represents. The 'Partition status' object requires further indications relating to the arming type which is to be switched to Away status (totally disarmed).	
	Immediate command	If enabled, touching the icon on the map will almost immediately activate the command. The command can be selected from the drop-down menu which appears.	
	View status	If enabled, this option allows you to visualize the status change on the display by means of an icon change, as selected in the Image section.	
		Button to reset the factory default settings.	

COMPLIANCE WITH RULES IN FORCE

In order to guarantee compliance with the regulations in force, you must adhere to the following guidelines:

- nBy/X readers must be equipped with devices that protect them against forced-opening of their casings (EN50131 grade 2) and dislodgement from their placements (CEI 79-2 level II and EN50131 grade 3).
- The dislodgement protection of the control panel mod. Tamper NO must be mounted (CEI 79-2 level II and EN50131 grade 3).
- JOY, Aria/HG and Concept keypads must be equipped with enabled tamper-protection devices.
- FLEX5/U devices must be mounted inside the enclosure of SmartLiving 1050L, 10100L, 1050L/G3 and 10100L/G3 control panels, or must be equipped with a device that protects them against forced-opening of their casings (EN50131 grade 2) and dislodgement from their placements (CEI 79-2 level II and EN50131 grade 3).
- IB200 devices cannot be used in configurations with security grade 3, unless equipped with a device that protects against dislodgement.
- The lines relating to the intrusion-detection zones must be configured as 'Double balancing' with double EOL resistors, or as Single balancing with single EOL resistor. They must also be equipped with devices which protect them against the forced-opening of their casings.
- Terminal tamper, peripheral tamper and control-panel tamper events must trigger audible signals (sunder signals) for a period of not less than 3 minutes.
- The output activated by the previously mentioned tamper events must be different from the output activated by alarms signals.
- All Code PINs must have 6 digits.
- If a Timer is used for automatic-arming operations, the Pre-arm times must be programmed separately for each partition (the Pre-arm time must not be set at 0).

In particular, in order to guarantee CEI 79-2 compliance of devices, the following options must be programmed as follows:

CEI 79-2 LEVEL II

- The following options must not be activated in the "Panel Options" section:
 - ReaderBuzzer OFF
 - BypassAlsoTamper
 - OpenZonesArmLock
 - 50131ReaderLedOFF
 - 50131StatHidden
 - 50131IconsHidden
 - 50131AlarDelayed
 - 50131WarnLedMem
- Do not enable any of the "FaultsNotReady" options from the "Other parameters" section.
- The "Requires code" option - from the "Keypads - Choose peripheral - Options" section - must be enabled for every keypad and shortcut in use.
- The "Entry Time" parameter of each partition must be no more than 60 seconds.

Compliance with EN50131 Grade 2 is guaranteed by observing the following guidelines.

EN50131, GRADE 2

- In the "Panel options" section, enable:
 - Keypad lockout
 - OpenZonesArmLock
 - NoUserTamp.reset
 - 50131ReaderLedOFF
 - 50131StatHidden
 - 50131IconsHidden
 - 50131AlarDelayed

- 50131WarnLedMem
- The following options must not be activated in the "Panel Options" section:
 - ReaderBuzzer OFF
 - BypassAlsoTamper
- In the section "Other parameters - FaultForNotReady", enable the following options:
 - Zone fuse fault
 - IBUS fuse fault
 - Low battery
 - Mains failure
 - Tel. line down
 - Jamming
 - Low battery WLS
 - WLS zone loss
 - LossTamp.ongoing
- Zones configured as "24H", "Automation" are non-compliant.
- Zones programmed as "Arm", "Disarm", "Switch" or "Follow" comply only when activated by keyswitches with more than 10,000 code combinations.
- An input is set up for system fault management.
- For zones with the "Fault zone" option enabled, it is necessary to eliminate from the relative alarm event the programming of an external sounder/flasher in the "Outputs" parameter. You can program indoor sounder/flashers via the "Other outputs" option.
- The telephone dialer must be enabled.
- The system must include a self-powered outdoor sounder for intrusion-alarm event signalling.
- If a digital telephone dialer is used for transmissions or a voice dialer with a SmartLogos30M board, a channel and a phone number must be reserved for the following events:
 - All events generated by zones with the "Hold-up" attribute.
 - All events generated by "Instant", "Delayed", "Delayed unhidden" and "Route"
 - All events generated by terminal, peripheral and control panel tamper.
 - All faults detected by the control panel.
- The "Alarm Cycles" parameter of each zone must be set between 3 and 10.
- The "Mains fail.Delay" parameter must be set at no more than 1 minute.
- The "Requires code" option on the function-key shortcuts must be enabled for all the assigned shortcuts.
- The "StopTelOn Disarm" partition option must not be enabled.
- The "Entry Time" of each partition must be set at a maximum of 45 seconds.
- You must enable the "Priority" option for any alarm events associated with "Hold-up" zones.
- "Failed to arm" and "Forced arming" events must be saved to the Events log.
- The programmed "LowBattery delay" must not be programmed at more than 5 minutes.

Compliance with EN50131-3 grade 3 is guaranteed by adding to the above-mentioned requirements the following:

EN50131-3, GRADE 3

- In the "Parameters" section, enable option "50131 Grade 3".
- If the installation uses detectors with an anti-mask function, each anti-mask signal must be managed as follows:
 - Prepare an input terminal for the anti-mask signal connection.
 - Programme the following parameters:
 - "Description": assign an explanatory description to the signal
 - "Fault zone": enable this option
 - "NoArmIfNotReady": enable this option
- Use an ATS4 notification appliance:
 - protocol: SIA-IP with encryption
 - interface: SmartLAN/G or SmartLAN/SI

Compliance with EN50131-6 grade 3 is guaranteed for SmartLiving control panel models 1050/G3, 1050L/G3 and 10100L/G3 without additional requirements.

EN50131-6, GRADE 3

Compliance with EN50131-6 grade 3 is guaranteed for SmartLiving control panel models 505/G3, 515, 1050, 1050L and 10100L without additional requirements.

- Remove the power supply/transformer module.
- Install an EN50131-6 Grade 3 certified power supply unit alongside the control panel enclosure. This power supply will output the power for the control panel and the following signals:

- G1 power system fault (overvoltage, overcurrent, short circuit)
- G2 mains power failure fault
- G3 battery fault
- Connect the backup battery to the battery-charge-level control system of the certified power supply unit.
- Power the control panel by means of a continuous current output of the certified power supply, by wiring it through cable J of the connector on the control panel in respect of polarity (BLACK = negative, RED = positive) and, if necessary, by extending the cable.
- Draw the POSITIVE power supply for all the system parts (control panel, peripherals, detectors, etc.) exclusively from the certified power supply unit.
- Prepare 3 input terminals for the fault signal connections (G1, G2, G3, described above) and program the following parameters for each of the 3 terminals:
 - "Description": assign an explanatory description to the signal
 - "Fault zone": enable this option

Chapter 9

ERRORS AND FAULTS

Faults detected by the control panel 9-1

The following table shows the system faults which are signaled on the yellow LED on the keypad  :

FAULT	Message on the User menu, "View/Faults"	Probable cause	Note
Zone fuse blown	Zone fuse fault	Excessive current draw on the "+AUX" terminals of the control panel	
BUS fuse blown	IBUS fuse fault	Excessive current draw on the "+" terminal of the control panel	
Backup battery inefficient or not connected	Low battery	The backup battery of the control panel is almost empty or disconnected.	
Primary power-source loss	Mains failure	The primary power source voltage (230V~) has failed or has been disconnected	
The PSTN landline is unavailable	Tel. line down	Trouble on the PSTN landline	
Interference	Jamming	Wireless transmission is poor	
Wireless detector battery low	Low battery WLS	The battery of at least one wireless detector is running out	To view "Low battery WLS" and "WLS zone loss" signaling, access the user menu, go to "View/Faults", press  to view the list of devices involved
Wireless detector not operative	WLS zone loss	At least one wireless detector is not operating	
Fault on Nexus GSM dialer	Nexus fault / Low signal	The GSM network signal is insufficient	Press  on "Nexus fault" to access the list of current faults.
	Nexus fault / GSM module fault	The GSM module of the Nexus dialer is not operating properly. Call your Installer company	
	Nexus fault / SIM commun. fault	The SIM card does not respond or is not present. The SIM card PIN is not disabled.	
	Nexus fault / Low Credit	The credit left on the SIM card is below the minimum credit threshold.	
	Nexus fault / Provider Unavailable	The GSM network provider of the SIM in use is unavailable.	
	Nexus fault / GPRS conn. lost	NEXUS detects connection problems on GPRS network	
IP connection loss	IP conn. lost	The verification of the IP connection fails.	
Device loss or tamper in progress	LossTamp. ongoing	One of the following events has occurred: <ul style="list-style-type: none"> • Control panel open • Dislodged panel • Expansion tamper • Keypad tamper • Reader tamper • Sound.flash.Tamp • Expansion loss • Keypad loss • Reader loss • Sound.flash.Loss 	

Faults on IVY-BUS sounder	Sounder faults / Horn fault	A defect/damage has been detected on the horn/sounder.	Select "Sounder faults" then click on the OK button to access the list of devices which have at least one fault present. Select the sounder concerned then click on the OK button to access the list of current faults on the device.
	Sounder flasher faults / Low-Batt. Soundfl.	A low-voltage value has been detected on the sounder battery. If the voltage drops below 10V, the device will inhibit the sounder and activate only the flasher (in the event of an alarm). If the voltage drops below 8V, the device will inhibit both the sounder and the flasher.	
	Sounder flasher Faults / Battery resist.	An excessive internal resistance has been detected on the sounder battery. This type of deep fault indicates corrosion inside the battery, therefore, the battery must be replaced.	
Violation of zones with faults	Faults on zones	Violation has occurred on one or more zones with the "Fault zone" option enabled.	Press OK to access the list of zones involved.
Contaminated smoke sensor	Detect or dusty	The smoke chamber of at least one of the Air2-FD100 smoke detectors is contaminated by dirt or dust. Refer to the instructions supplied with the detector for information regarding the respective threshold.	

Communication BUS (I-BUS)

9-2

The control panel monitors the I-BUS continuously.

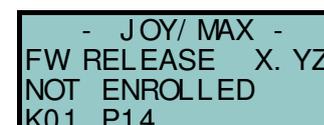
If no signals (control panel and peripheral signals) are detected on the I-BUS for over 40 seconds, the keypad displays will show the warning opposite. The display will show:

1. keypad model
2. keypad firmware version
3. Error type
4. the address of the keypad and the address of the built reader

In this case, the installer must first check that cable "D" of the I-BUS is connected properly. Then check the proper operating capacity of the I-BUS and the general integrity of the entire system.

If the message opposite appears on the keypad display, it means that I-BUS is operating properly but cannot communicate with the keypad in question.

Therefore, the keypad is not present in the system configuration.



One of the two messages shown in the figures may also appear during the control panel firmware updates.

Note

If you are using an Alien user interface, the above-mentioned information will be shown on the bottom bar on the home page.

Ring Sensitivity

9-3

The various configurations of modern telephone lines and the multiplicity of signals that transit along them, require major attention in the design of phone-line interfaces. The optimized phone-line interface on-board SmartLiving control panels has been especially designed to satisfy present day requirements. In addition to the traditional telephone plug for land line (PSTN) connections, there are usually boards for ISDN or ADSL connections.

If there are ADSL filters on the line, it will be necessary to connect the control panel downstream of the filters, to the line dedicated to telephone equipment (this line is clearly indicated on the filters).

Following are two "trouble" conditions which may be caused by ISDN or ADSL connections, etc. , and the "actions" you must take if you encounter such problems.

- The control panel is enabled for "Answerphone" and "Teleservice" functions but fails to pick up incoming calls after the programmed number of rings or picks up after more rings than programmed. If this occurs, increase the value of the "Ring sensitivity" parameter to a suitable level.
- The control panel is enabled for "Answerphone" and "Teleservice" functions but picks up during "through" calls (calls that should not involve the control panel). If this occurs, decrease the value of the "Ring sensitivity" parameter to a suitable level.

Chapter 10

IP AND INTERNET CONNECTIVITY

Configuring an IP network

10-1

Minimum configuration requirements:

- 1 router/modem connected to the Internet. The router/modem must be “port forwarding” capable in order to route external connections.
- 1 SmartLAN connected to the router/modem.

In addition, for programming purposes, a **SmartLeague** equipped PC must be linked to the SmartLAN (point to point connection with crossed Ethernet cable or via router connection).

A good knowledge of networking and TCP/IP protocol is required during the SmartLAN board configuration and the Internet connection phases.

The IP address must uniquely identify each peripheral device connected to a network such as, for example, each computer connected to the company network or directly to the Internet.

The IP address of the SmartLAN is a “static” address and cannot be assigned automatically. You can assign the IP address, set at default as **192.168.1.9**, via the SmartLAN programming page in the SmartLeague software program. The PC used for the initial programming of the SmartLAN must have an IP address of the same address class **192.168.1.xxx** (for example, 192.168.1.123).

Successively, it will be possible to change the IP address of the SmartLAN, therefore, it will be the task of the network administrator to supply one suitable for the requirements and potential of the configured network.

This mask specifies which address class can communicate with the SmartLAN board and, consequently, which peripherals to connect to.

This parameter, which must be requested from the network administrator (**255.255.255.0** at default), allows the SmartLAN to reach all the peripherals with address class **192.168.1.xxx**.

This is the identifier of a service which may have a single peripheral connected to the network. SmartLAN uses two TCP/IP ports:

- The port reserved for access to the web server. Set at **80** at default.
- The Programming port (up/downloading). Set at **5004** at default.

The gateway is the access point which each peripheral connected in the network uses to reach the Internet. In the case of a minimum configuration, the gateway is the router.

The parameter to be configured is the IP address of the gateway and must belong to the IP address class of the internal network (for example, 192.168.1.1).

This is the server used for the resolution of Internet names in IP addresses (for example, it translates www.google.com in 209.85.129.99). The parameter to be configured is the IP address of the DNS server, depends on the network connection provider (Telecom, Vodafone, etc.) and therefore must be requested from the network administrator.

This is a protocol for HTTPS connections. The security of the connection with the computer is guaranteed by integrated cryptography. Secure connection of mobile-devices is guaranteed by SSL protocol

For a secure HTTPS connection, users must connect to the SmartLAN/G using the SSL port (**443** at default) or through the programmed one.

- Default SSL port (443): https://192.168.1.92
- Customized SSL port (xyz): https://192.168.1.92:xyz

IP ADDRESS

SUBNET MASK

TCP/IP PORT

GATEWAY

DNS

SSL

Configuring a router

10-2

Remote access to the SmartLAN requires knowledge of the public IP address of the router, assigned by the provider (Telecom, Vodafone, etc.) for Internet access. This address can be either static or dynamic, thus conditioning remote access to the router:

- **Connection to a dynamic public IP address**
The provider may re-assign a public IP address in either a temporized manner or at each router connection, thus modifying it. This complicates remote access to the router. In order to resolve this problem, many routers have access to a dynamic DNS service for the association of dynamic IP addresses to host names (for example www.dyndns.com). It will be necessary to register a "dynamic DNS host" and set the parameters provided by the ISP (for example, user, password, domain, etc.) on the router. The router will update the dynamic IP address periodically with the registered static hostname (for example, http://casamia.dyndns.org). In this way it will be possible to have remote access to the router by means of a univocal name that is linked to the public IP address.
- **Connection to a static public IP address**
This type of connection links to a public IP address that is always the same. In this case, it is possible either to access the router directly through the fixed IP address, or purchase a domain (for example, www.casamia.com) that is capable of re-routing packets to the fixed IP address assigned by the connection provider. Once remote access to the router has been achieved, it is necessary to route the incoming connections to the SmartLAN. To distinguish these connections, use the previously programmed "IP Address" and "Port" parameters. During this programming phase, it is strongly recommended that you contact the network administrator in order to avoid configuration conflicts.

It is therefore necessary to access the router page reserved for "port forwarding" (sometimes called "virtual server") and set up the route directions of the two services the SmartLAN is enabled on.

- Web server port
 - communication protocol: TCP/IP
 - external port: 8080 (or any other free port provided by the network administrator)
 - internal port: 80 (or the one selected during the programming phase)
 - IP address: IP address of the SmartLAN
- Web server SSL port
 - communication protocol: TCP/IP
 - external port: 443 (or any other free port provided by the network administrator)
 - internal port: 443 (or the one selected during the programming phase)
 - IP address: IP address of the SmartLAN
- Programming port
 - communication protocol: TCP/IP
 - external port: 5004 (or the one selected during the programming phase)
 - internal port: 5004 (or the one selected during the programming phase)
 - IP address: IP address of the SmartLAN

Remote access

10-3

To establish external communication with the SmartLAN/G web server via browser (Firefox, Opera, Internet Explorer, etc.), type in the configured public IP address of the router followed by the number of the external forwarding port, as follows:

- http://www.casamia.com:8080 (in the case of domain associated with static public IP)
- http://casamia.dyndns.org:8080 (in the case of registration with dyndns.org with dynamic public IP)

In order to allow remote communication with the SmartLAN, it is necessary to set the configuration on the SmartLeague (IP address of the router and external rerouting port).

VIA SMARTLEAGUE

For remote access to the SmartLAN/G web server, type on the browser on your mobile phone the public IP address of the configured router followed by the number of the SSL web port, as follows:

VIA MOBILE DEVICES

- http://www.casamia.com:443 (in the case of domain associated with static public IP)
- http://casamia.dyndns.org:443 (in the case of registration with dyndns.org with dynamic public IP)

Connection test

10-4

The SmartLiving control panel can carry out an IP network connection test by making link connection attempts to a precise IP address.

The SmartLeague software programme will allow you to set the test parameters. These parameters can be found in the "Programming - IP connection test parameters" section relating to the "SmartLiving system":

- IP Address, Port - Address IPv4 and port where the connection attempts are to be directed.
- Interval - an intervening period (expressed in seconds) between the test connections. If set at "0" the connection test will be disabled
- Number of attempts - number of connection attempts made during each test

If the connection test is enabled and fails (i.e. the control panel is unable to achieve an IP connection during the programmed number of attempts), the "IP conn. loss" event will be generated.

Appendix A

SHORTCUTS BY DEFAULT

n.	Icon	description	function	parameter
1		Arm/Disarm	Applies a pre-set scenario	which scenario
2		Stop alarms	Immediately deactivates the outputs relative to zone/partition alarm and tamper events and system tamper events.	
3		Clear call queue	Cancels the entire call queue and stops ongoing calls (if any).	
4		Delete memory	Implements a "Stop alarms" operation and at the same time deletes memory of system and partition alarm and tamper events.	
5		Activate Output	Activates one of the programmed outputs.	which output
6		Deactiv. output	Deactivates one of the programmed outputs.	which output
7		Overtime	Delays partition auto-arming time by 30 minutes.	
8		Teleservice req.	Sends a call to the Installer company number (Teleservice number).	
9		Voice menu	Plays a recorded voice message which announces the shortcuts assigned to the number keys.	User code
10		Listen-in	Allows listen-in sessions via phone by means of a microphone on one of the available keypads.	Keypad
11		Intercom Call	Accesses the user menu section: Voice functions/intercom Call	
12		Arm/Disarm menu	Accesses the user menu section: Arm/Disarm	
13		Alarm menu	Accesses the user menu section: Manage alarms	
14		Voice func. menu	Accesses the User Menu section: Voice functions	
15		Activations menu	Accesses the user menu section: Activations	
16		View Nexus status	Accesses the user menu section: View/Nexus status	
17		Arming status	Plays a voice announcement regarding the armed/disarmed status of partitions.	
18		Keypad sett. menu	Accesses the user menu section: Keypad settings	
19		ZoneBypass menu	Accesses the user menu section: Activations/Zones	19

n.	Icon	description	function
20		Voice memo	Accesses the User Menu section: Voice functions
21		Output control	Accesses the user menu section: Outputs ON/OFF
22		Enab.answerphone	Accesses the user menu section: Activations/Answerphone
23		Enab.teleservice	Accesses the user menu section: Activations/Teleservice
24		Enable codes	Accesses the user menu section: Activations/Codes
25		Enable keys	Accesses the user menu section: Activations/Keys
26		Enable timers	Accesses the user menu section: Activations/Timers
27		Enab. auto-arm	Accesses the user menu section: Activations/Auto-arming
28		View events log	Accesses the user menu section: View/Events log
29		View alarm log	Accesses the user menu section: View/Alarms log
30		View faults log	Accesses the user menu section: View/Faults log
31		View arm ops log	Accesses the user menu section: View/Arm/Disarm op.
32		ViewSystemStatus	Accesses the user menu section: View/System status
33		View zone status	Accesses the user menu section: View/Zone status
34		Change PIN	Accesses the user menu section: Change PIN
35		Time/Date	Accesses the user menu section: Time/Date
36		View faults	Accesses the user menu section: View/Faults
37		Thermostat menu	Accesses the user menu section: Thermostat
38		Panic	Activates a "Panic" event

Appendix B

AVAILABLE ICONS

The following Table shows the icons provided at default. The icons can be customized to suit the keypad shortcuts.

Icon number	Icon	Icon number	Icon	Icon number	Icon
1		19		37	
2		20		38	
3		21		39	
4		22		40	
5		23		41	
6		24		42	
7		25		43	
8		26		44	
9		27		45	
10		28		46	
11		29		47	
12		30		48	
13		31		49	
14		32		50	
15		33			
16		34			
17		35			
18		36			

Appendix C

VOICE MESSAGES

The SmartLogos30M voice board is supplied by Inim Electronics with 500 voice message slots, 291 of which are pre-recorded. The messages are arranged in such way as to produce event-related voice calls which clearly describe the related event.

The following Table shows the message numbers and their purpose, together with the respective recording time.

Type	Number	Default message	Message duration (seconds)	
			High quality	Average quality
Available user-messages	1 - 100	''	169 (for all 100 mes-sages)	271 (for all 100 mes-sages)
Not available	101 - 165	''		
Arming scenarios	166	Scenario 1	2.5	4
	167	Scenario 2	2.5	4
	168	Scenario 3	2.5	4
	169	Scenario 4	2.5	4
	170	Scenario 5	2.5	4
	171	Scenario 6	2.5	4
	172	Scenario 7	2.5	4
	173	Scenario 8	2.5	4
	174	Scenario 9	2.5	4
	175	Scenario 10	2.5	4
	176	Scenario 11	2.5	4
	177	Scenario 12	2.5	4
	178	Scenario 13	2.5	4
	179	Scenario 14	2.5	4
	180	Scenario 15	2.5	4
	181	Scenario 16	2.5	4
	182	Scenario 17	2.5	4
	183	Scenario 18	2.5	4
	184	Scenario 19	2.5	4
	185	Scenario 20	2.5	4
	186	Scenario 21	2.5	4
	187	Scenario 22	2.5	4
	188	Scenario 23	2.5	4
	189	Scenario 24	2.5	4
	190	Scenario 25	2.5	4
	191	Scenario 26	2.5	4
	192	Scenario 27	2.5	4
	193	Scenario 28	2.5	4
	194	Scenario 29	2.5	4
	195	Scenario 30	2.5	4
Shortcut	196	Armed in Away mode	2.5	4
	197	Stop alarm	2.5	4
	198	Stop call queue	2.5	4
	199	Delete memory	2.5	4
	200	Activate output	2.5	4
	201	Deactivate output	2.5	4
	202	Overtime request	2.5	4
	203	Request maintenance	2.5	4
	204	StartVoiceNotifier	2.5	4
	205	Listen-in	2.5	4
	206	Intercom Call	2.5	4
	207	Arm/Disarm menu	2.5	4
	208	Alarm management menu	2.5	4
	209	Voice functions	2.5	4
	210	Activations menu	2.5	4
	211	Nexus status	2.5	4
	212	System status	2.5	4
	213	Keypad settings	2.5	4
	214	Zone bypass menu	2.5	4
	215	Voice memo	2.5	4
	216	ON/OFF output menu	2.5	4
	217	Enable/Disable answerphone	2.5	4
	218	Enable teleservice	2.5	4
	219	Enable codes	2.5	4
	220	Enable keys	2.5	4
	221	Enable timers	2.5	4
	222	Enable auto-arming	2.5	4
	223	View events log	2.5	4
	224	View alarms log	2.5	4
	225	View faults log	2.5	4
	226	View arm/disarm operations	2.5	4
	227	View battery status	2.5	4
	228	View zone status	2.5	4
	229	Change PIN	2.5	4

Type	Number	Default message	Message duration (seconds)	
			High quality	Average quality
Zone Terminal	330	Zone 60	3.13	5
	331	Zone 61	3.13	5
	332	Zone 62	3.13	5
	333	Zone 63	3.13	5
	334	Zone 64	3.13	5
	335	Zone 65	3.13	5
	336	Zone 66	3.13	5
	337	Zone 67	3.13	5
	338	Zone 68	3.13	5
	339	Zone 69	3.13	5
	340	Zone 70	3.13	5
	341	Zone 71	3.13	5
	342	Zone 72	3.13	5
	343	Zone 73	3.13	5
	344	Zone 74	3.13	5
	345	Zone 75	3.13	5
	346	Zone 76	3.13	5
	347	Zone 77	3.13	5
	348	Zone 78	3.13	5
	349	Zone 79	3.13	5
	350	Zone 80	3.13	5
	351	Zone 81	3.13	5
	352	Zone 82	3.13	5
	353	Zone 83	3.13	5
	354	Zone 84	3.13	5
	355	Zone 85	3.13	5
	356	Zone 86	3.13	5
	357	Zone 87	3.13	5
	358	Zone 88	3.13	5
	359	Zone 89	3.13	5
	360	Zone 90	3.13	5
	361	Zone 91	3.13	5
	362	Zone 92	3.13	5
	363	Zone 93	3.13	5
	364	Zone 94	3.13	5
	365	Zone 95	3.13	5
	366	Zone 96	3.13	5
	367	Zone 97	3.13	5
	368	Zone 98	3.13	5
369	Zone 99	3.13	5	
370	Zone 100	3.13	5	
Partition	371	Partition 1	3.13	5
	372	Partition 2	3.13	5
	373	Partition 3	3.13	5
	374	Partition 4	3.13	5
	375	Partition 5	3.13	5
	376	Partition 6	3.13	5
	377	Partition 7	3.13	5
	378	Partition 8	3.13	5
	379	Partition 9	3.13	5
	380	Partition 10	3.13	5
	381	Partition 11	3.13	5
	382	Partition 12	3.13	5
	383	Partition 13	3.13	5
	384	Partition 14	3.13	5
	385	Partition 15	3.13	5
Codes	386	Code 1	2.5	4
	387	Code 2	2.5	4
	388	Code 3	2.5	4
	389	Code 4	2.5	4
	390	Code 5	2.5	4
	391	Code 6	2.5	4
	392	Code 7	2.5	4
	393	Code 8	2.5	4
	394	Code 9	2.5	4
	395	Code 10	2.5	4

Type	Number	Default message	Message duration (seconds)	
			High quality	Average quality
Shortcut	230	Date/Time settings	2.5	4
	231	View faults	2.5	4
Not available	232 - 240	∩		
Generic mes-sages	241	Reset	1.25	2
	242	To	0.63	1
	243	Press	1.25	2
	244	Location	6.25	10
	245	Zero	2.5	4
	246	One	2.5	4
	247	Two	2.5	4
	248	Three	2.5	4
	249	Four	2.5	4
	250	Five	2.5	4
	251	Six	2.5	4
	252	Seven	2.5	4
	253	Eight	2.5	4
	254	Nine	2.5	4
Partition status	255	Away mode	3.13	5
	256	Armed in Stay mode	3.13	5
	257	Instant mode	3.13	5
	258	Disarm	3.13	5
Menu	259	To go back to previous menu press *	3.13	5
Activation / Deactivation	260	To activate	1.88	3
	261	To deactivate	1.88	3
Type-in user-code PIN	262	Type-in user-code PIN followed by #	2.5	4
Outputs	263	Relay	2.5	4
	264	Output 1	2.5	4
	265	Output 2	2.5	4
Not available	266 - 270	∩		
Zone Terminal	271	Zone 1	3.13	5
	272	Zone 2	3.13	5
	273	Zone 3	3.13	5
	274	Zone 4	3.13	5
	275	Zone 5	3.13	5
	276	Zone 6	3.13	5
	277	Zone 7	3.13	5
	278	Zone 8	3.13	5
	279	Zone 9	3.13	5
	280	Zone 10	3.13	5
	281	Zone 11	3.13	5
	282	Zone 12	3.13	5
	283	Zone 13	3.13	5
	284	Zone 14	3.13	5
	285	Zone 15	3.13	5
	286	Zone 16	3.13	5
	287	Zone 17	3.13	5
	288	Zone 18	3.13	5
	289	Zone 19	3.13	5
	290	Zone 20	3.13	5
	291	Zone 21	3.13	5
	292	Zone 22	3.13	5
	293	Zone 23	3.13	5
	294	Zone 24	3.13	5
	295	Zone 25	3.13	5
	296	Zone 26	3.13	5
	297	Zone 27	3.13	5
	298	Zone 28	3.13	5
	299	Zone 29	3.13	5
	300	Zone 30	3.13	5
	301	Zone 31	3.13	5
	302	Zone 32	3.13	5
	303	Zone 33	3.13	5
	304	Zone 34	3.13	5
	305	Zone 35	3.13	5
	306	Zone 36	3.13	5
	307	Zone 37	3.13	5
	308	Zone 38	3.13	5
	309	Zone 39	3.13	5
	310	Zone 40	3.13	5
	311	Zone 41	3.13	5
	312	Zone 42	3.13	5
	313	Zone 43	3.13	5
	314	Zone 44	3.13	5
	315	Zone 45	3.13	5
	316	Zone 46	3.13	5
	317	Zone 47	3.13	5
	318	Zone 48	3.13	5
	319	Zone 49	3.13	5
	320	Zone 50	3.13	5
321	Zone 51	3.13	5	
322	Zone 52	3.13	5	
323	Zone 53	3.13	5	
324	Zone 54	3.13	5	
325	Zone 55	3.13	5	
326	Zone 56	3.13	5	
327	Zone 57	3.13	5	
328	Zone 58	3.13	5	
329	Zone 59	3.13	5	
	330	Zone 60	3.13	5

Type	Number	Default message	Message duration (seconds)	
			High quality	Average quality
Keys	396	Key 1	2.5	4
	397	Key 2	2.5	4
	398	Key 3	2.5	4
	399	Key 4	2.5	4
	400	Key 5	2.5	4
	401	Key 6	2.5	4
	402	Key 7	2.5	4
	403	Key 8	2.5	4
	404	Key 9	2.5	4
	405	Key 10	2.5	4
Keypads	406	Keypad 1	2.5	4
	407	Keypad 2	2.5	4
	408	Keypad 3	2.5	4
	409	Keypad 4	2.5	4
	410	Keypad 5	2.5	4
Readers	411	Reader 1	2.5	4
	412	Reader 2	2.5	4
	413	Reader 3	2.5	4
	414	Reader 4	2.5	4
	415	Reader 5	2.5	4
Function keys Emergency	416	Fire	2.5	4
	417	Ambulance	2.5	4
	418	Police	2.5	4
Not available	419	∩		
Event type	420	Zone alarm	2.5	4
	421	Terminal tamper	2.5	4
	422	Partition alarm	2.5	4
	423	Stay alarm	2.5	4
	424	Partition tamper	2.5	4
	425	Zone bypass	2.5	4
	426	Real time zone	2.5	4
	427	Partition not-ready-to-arm	2.5	4
	428	Away arm request	2.5	4
	429	Stay arm request	2.5	4
	430	Armed in Away mode	2.5	4
	431	Armed in Stay mode	2.5	4
	432	Reset partition	2.5	4
	433	Partition armed, leave partition	2.5	4
	434	Disarm partition	2.5	4
	435	Pre-arm alert	2.5	4
	436	Overtime request	2.5	4
	437	Welcome	2.5	4
	438	Forced arming	2.5	4
	439	Failed to arm	2.5	4
	440	Valid user-code	2.5	4
	441	Valid key	2.5	4
	442	Valid code at keypad	2.5	4
	443	Valid key at reader	2.5	4
	444	Valid user-code on partition	2.5	4
	445	Valid key on partition	2.5	4
	446	Failed call	2.5	4
	447	Timer activated	2.5	4
	448	Thermostat	2.5	4
	449	Scenario	2.5	4
	450	Programmable event	2.5	4
	451	Emergency	2.5	4
	452	Open-panel tamper	2.5	4
	453	Dislodged-panel tamper	2.5	4
	454	Zone fuse fault	2.5	4
	455	I-BUS fuse fault	2.5	4
	456	Battery inefficient	2.5	4
	457	Mains failure	2.5	4
	458	Expansion tamper	2.5	4
	459	Keypad Tamper	2.5	4
	460	Reader Tamper	2.5	4
	461	Sounder tamper	2.5	4
	462	Nexus tamper	2.5	4
	463	Expansion Loss	2.5	4
	464	Keypad Loss	2.5	4
	465	Reader Loss	2.5	4
	466	Sounder/flasher loss	2.5	4
	467	Nexus loss	2.5	4
	468	Jamming	2.5	4
	469	Low battery wireless zone	2.5	4
470	Wireless zone loss	2.5	4	
471	Valid Installer code	2.5	4	
472	Invalid code			
473	False key			
474	Nexus fault			
475	Telephone line down			
476	Periodic test event			
477	Hard reset			
478	Call queue full			
479	Successful call			
480	Start programming			
481	Ongoing call			
482	Failed to send message			
483	Output fault			
484	Low GSM credit			
Not available	485	∩		
Voicemail slots	486 - 500	∩	37.5 (for all 15 mes-sages)	60 (for all 15 mes-sages)

Appendix D

SCREW TERMINALS

All the terminals on the SmartLiving control panel and its peripherals (expansions and keypads) are identified by distinctive numbers transcribed in the "CCC" programming field of the "CONTACT-ID" protocol, in order to allow the precise localization of events related to zones or terminals.

In the case of double zones, the second zone will be identified by the number "500 + n." (where "n." stands for the number of the terminal).

n.	SLiving 505	SLiving 515	SLiving 1050	SLiving 10100	n.	SLiving 515	SLiving 1050	SLiving 10100	n.	SLiving 1050	SLiving 10100	n.	SLiving 10100
1	T1 Panel	T1 Panel	T1 Panel	T1 Panel	61	Keyp. 1 T1	Exp. 11 T1	Exp. 11 T1	121	Keyp. 6 T1	Exp. 23 T1	181	Exp. 35 T1
2	T2 Panel	T2 Panel	T2 Panel	T2 Panel	62	Keyp. 1 T2	Exp. 11 T2	Exp. 11 T2	122	Keyp. 6 T2	Exp. 23 T2	182	Exp. 35 T2
3	T3 Panel	T3 Panel	T3 Panel	T3 Panel	63	Keyp. 2 T1	Exp. 11 T3	Exp. 11 T3	123	Keyp. 7 T1	Exp. 23 T3	183	Exp. 35 T3
4	T4 Panel	T4 Panel	T4 Panel	T4 Panel	64	Keyp. 2 T2	Exp. 11 T4	Exp. 11 T4	124	Keyp. 7 T2	Exp. 23 T4	184	Exp. 35 T4
5	T5 Panel	T5 Panel	T5 Panel	T5 Panel	65	Keyp. 3 T1	Exp. 11 T5	Exp. 11 T5	125	Keyp. 8 T1	Exp. 23 T5	185	Exp. 35 T5
6			T6 Panel	T6 Panel	66	Keyp. 3 T2	Exp. 12 T1	Exp. 12 T1	126	Keyp. 8 T2	Exp. 24 T1	186	Exp. 36 T1
7			T7 Panel	T7 Panel	67	Keyp. 4 T1	Exp. 12 T2	Exp. 12 T2	127	Keyp. 9 T1	Exp. 24 T2	187	Exp. 36 T2
8			T8 Panel	T8 Panel	68	Keyp. 4 T2	Exp. 12 T3	Exp. 12 T3	128	Keyp. 9 T2	Exp. 24 T3	188	Exp. 36 T3
9			T9 Panel	T9 Panel	69	Keyp. 5 T1	Exp. 12 T4	Exp. 12 T4	129	Keyp. 10 T1	Exp. 24 T4	189	Exp. 36 T4
10			T10 Panel	T10 Panel	70	Keyp. 5 T2	Exp. 12 T5	Exp. 12 T5	130	Keyp. 10 T2	Exp. 24 T5	190	Exp. 36 T5
11	Exp. 1 T1	Exp. 1 T1	Exp. 1 T1	Exp. 1 T1	71		Exp. 13 T1	Exp. 13 T1	131		Exp. 25 T1	191	Exp. 37 T1
12	Exp. 1 T2	Exp. 1 T2	Exp. 1 T2	Exp. 1 T2	72		Exp. 13 T2	Exp. 13 T2	132		Exp. 25 T2	192	Exp. 37 T2
13	Exp. 1 T3	Exp. 1 T3	Exp. 1 T3	Exp. 1 T3	73		Exp. 13 T3	Exp. 13 T3	133		Exp. 25 T3	193	Exp. 37 T3
14	Exp. 1 T4	Exp. 1 T4	Exp. 1 T4	Exp. 1 T4	74		Exp. 13 T4	Exp. 13 T4	134		Exp. 25 T4	194	Exp. 37 T4
15	Exp. 1 T5	Exp. 1 T5	Exp. 1 T5	Exp. 1 T5	75		Exp. 13 T5	Exp. 13 T5	135		Exp. 25 T5	195	Exp. 37 T5
16	Exp. 2 T1	Exp. 2 T1	Exp. 2 T1	Exp. 2 T1	76		Exp. 14 T1	Exp. 14 T1	136		Exp. 26 T1	196	Exp. 38 T1
17	Exp. 2 T2	Exp. 2 T2	Exp. 2 T2	Exp. 2 T2	77		Exp. 14 T2	Exp. 14 T2	137		Exp. 26 T2	197	Exp. 38 T2
18	Exp. 2 T3	Exp. 2 T3	Exp. 2 T3	Exp. 2 T3	78		Exp. 14 T3	Exp. 14 T3	138		Exp. 26 T3	198	Exp. 38 T3
19	Exp. 2 T4	Exp. 2 T4	Exp. 2 T4	Exp. 2 T4	79		Exp. 14 T4	Exp. 14 T4	139		Exp. 26 T4	199	Exp. 38 T4
20	Exp. 2 T5	Exp. 2 T5	Exp. 2 T5	Exp. 2 T5	80		Exp. 14 T5	Exp. 14 T5	140		Exp. 26 T5	200	Exp. 38 T5
21	Exp. 3 T1	Exp. 3 T1	Exp. 3 T1	Exp. 3 T1	81		Exp. 15 T1	Exp. 15 T1	141		Exp. 27 T1	201	Exp. 39 T1
22	Exp. 3 T2	Exp. 3 T2	Exp. 3 T2	Exp. 3 T2	82		Exp. 15 T2	Exp. 15 T2	142		Exp. 27 T2	202	Exp. 39 T2
23	Exp. 3 T3	Exp. 3 T3	Exp. 3 T3	Exp. 3 T3	83		Exp. 15 T3	Exp. 15 T3	143		Exp. 27 T3	203	Exp. 39 T3
24	Exp. 3 T4	Exp. 3 T4	Exp. 3 T4	Exp. 3 T4	84		Exp. 15 T4	Exp. 15 T4	144		Exp. 27 T4	204	Exp. 39 T4
25	Exp. 3 T5	Exp. 3 T5	Exp. 3 T5	Exp. 3 T5	85		Exp. 15 T5	Exp. 15 T5	145		Exp. 27 T5	205	Exp. 39 T5
26	Exp. 4 T1	Exp. 4 T1	Exp. 4 T1	Exp. 4 T1	86		Exp. 16 T1	Exp. 16 T1	146		Exp. 28 T1	206	Exp. 40 T1
27	Exp. 4 T2	Exp. 4 T2	Exp. 4 T2	Exp. 4 T2	87		Exp. 16 T2	Exp. 16 T2	147		Exp. 28 T2	207	Exp. 40 T2
28	Exp. 4 T3	Exp. 4 T3	Exp. 4 T3	Exp. 4 T3	88		Exp. 16 T3	Exp. 16 T3	148		Exp. 28 T3	208	Exp. 40 T3
29	Exp. 4 T4	Exp. 4 T4	Exp. 4 T4	Exp. 4 T4	89		Exp. 16 T4	Exp. 16 T4	149		Exp. 28 T4	209	Exp. 40 T4
30	Exp. 4 T5	Exp. 4 T5	Exp. 4 T5	Exp. 4 T5	90		Exp. 16 T5	Exp. 16 T5	150		Exp. 28 T5	210	Exp. 40 T5
31	Keyp. 1 T1	Exp. 5 T1	Exp. 5 T1	Exp. 5 T1	91		Exp. 17 T1	Exp. 17 T1	151		Exp. 29 T1	211	Keyp. 1 T1
32	Keyp. 1 T2	Exp. 5 T2	Exp. 5 T2	Exp. 5 T2	92		Exp. 17 T2	Exp. 17 T2	152		Exp. 29 T2	212	Keyp. 1 T2
33	Keyp. 2 T1	Exp. 5 T3	Exp. 5 T3	Exp. 5 T3	93		Exp. 17 T3	Exp. 17 T3	153		Exp. 29 T3	213	Keyp. 2 T1
34	Keyp. 2 T2	Exp. 5 T4	Exp. 5 T4	Exp. 5 T4	94		Exp. 17 T4	Exp. 17 T4	154		Exp. 29 T4	214	Keyp. 2 T2
35	Keyp. 3 T1	Exp. 5 T5	Exp. 5 T5	Exp. 5 T5	95		Exp. 17 T5	Exp. 17 T5	155		Exp. 29 T5	215	Keyp. 3 T1
36	Keyp. 3 T2	Exp. 6 T1	Exp. 6 T1	Exp. 6 T1	96		Exp. 18 T1	Exp. 18 T1	156		Exp. 30 T1	216	Keyp. 3 T2
37	Keyp. 4 T1	Exp. 6 T2	Exp. 6 T2	Exp. 6 T2	97		Exp. 18 T2	Exp. 18 T2	157		Exp. 30 T2	217	Keyp. 4 T1
38	Keyp. 4 T2	Exp. 6 T3	Exp. 6 T3	Exp. 6 T3	98		Exp. 18 T3	Exp. 18 T3	158		Exp. 30 T3	218	Keyp. 4 T2
39	Keyp. 5 T1	Exp. 6 T4	Exp. 6 T4	Exp. 6 T4	99		Exp. 18 T4	Exp. 18 T4	159		Exp. 30 T4	219	Keyp. 5 T1
40	Keyp. 5 T2	Exp. 6 T5	Exp. 6 T5	Exp. 6 T5	100		Exp. 18 T5	Exp. 18 T5	160		Exp. 30 T5	220	Keyp. 5 T2
41		Exp. 7 T1	Exp. 7 T1	Exp. 7 T1	101		Exp. 19 T1	Exp. 19 T1	161		Exp. 31 T1	221	Keyp. 6 T1
42		Exp. 7 T2	Exp. 7 T2	Exp. 7 T2	102		Exp. 19 T2	Exp. 19 T2	162		Exp. 31 T2	222	Keyp. 6 T2
43		Exp. 7 T3	Exp. 7 T3	Exp. 7 T3	103		Exp. 19 T3	Exp. 19 T3	163		Exp. 31 T3	223	Keyp. 7 T1
44		Exp. 7 T4	Exp. 7 T4	Exp. 7 T4	104		Exp. 19 T4	Exp. 19 T4	164		Exp. 31 T4	224	Keyp. 7 T2
45		Exp. 7 T5	Exp. 7 T5	Exp. 7 T5	105		Exp. 19 T5	Exp. 19 T5	165		Exp. 31 T5	225	Keyp. 8 T1
46		Exp. 8 T1	Exp. 8 T1	Exp. 8 T1	106		Exp. 20 T1	Exp. 20 T1	166		Exp. 32 T1	226	Keyp. 8 T2
47		Exp. 8 T2	Exp. 8 T2	Exp. 8 T2	107		Exp. 20 T2	Exp. 20 T2	167		Exp. 32 T2	227	Keyp. 9 T1
48		Exp. 8 T3	Exp. 8 T3	Exp. 8 T3	108		Exp. 20 T3	Exp. 20 T3	168		Exp. 32 T3	228	Keyp. 9 T2
49		Exp. 8 T4	Exp. 8 T4	Exp. 8 T4	109		Exp. 20 T4	Exp. 20 T4	169		Exp. 32 T4	229	Keyp. 10 T1
50		Exp. 8 T5	Exp. 8 T5	Exp. 8 T5	110		Exp. 20 T5	Exp. 20 T5	170		Exp. 32 T5	230	Keyp. 10 T2
51		Exp. 9 T1	Exp. 9 T1	Exp. 9 T1	111		Keyp. 1 T1	Exp. 21 T1	171		Exp. 33 T1	231	Keyp. 11 T1
52		Exp. 9 T2	Exp. 9 T2	Exp. 9 T2	112		Keyp. 1 T2	Exp. 21 T2	172		Exp. 33 T2	232	Keyp. 11 T2
53		Exp. 9 T3	Exp. 9 T3	Exp. 9 T3	113		Keyp. 2 T1	Exp. 21 T3	173		Exp. 33 T3	233	Keyp. 12 T1
54		Exp. 9 T4	Exp. 9 T4	Exp. 9 T4	114		Keyp. 2 T2	Exp. 21 T4	174		Exp. 33 T4	234	Keyp. 12 T2
55		Exp. 9 T5	Exp. 9 T5	Exp. 9 T5	115		Keyp. 3 T1	Exp. 21 T5	175		Exp. 33 T5	235	Keyp. 13 T1
56		Exp. 10 T1	Exp. 10 T1	Exp. 10 T1	116		Keyp. 3 T2	Exp. 22 T1	176		Exp. 34 T1	236	Keyp. 13 T2
57		Exp. 10 T2	Exp. 10 T2	Exp. 10 T2	117		Keyp. 4 T1	Exp. 22 T2	177		Exp. 34 T2	237	Keyp. 14 T1
58		Exp. 10 T3	Exp. 10 T3	Exp. 10 T3	118		Keyp. 4 T2	Exp. 22 T3	178		Exp. 34 T3	238	Keyp. 14 T2
59		Exp. 10 T4	Exp. 10 T4	Exp. 10 T4	119		Keyp. 5 T1	Exp. 22 T4	179		Exp. 34 T4	239	Keyp. 15 T1
60		Exp. 10 T5	Exp. 10 T5	Exp. 10 T5	120		Keyp. 5 T2	Exp. 22 T5	180		Exp. 34 T5	240	Keyp. 15 T2

Appendix E

COMBINATION OF OUTPUTS TRIGGERED BY EVENTS

This appendix shows the event-generated actions (activations/deactivations) of the outputs programmed in the "Outputs" and "Other outputs" sections combined with the "SirenSound types" of the sounders on the BUS.

Table E-1: Output typology

Symbol/Initials	Description
TM	Output on terminal/Relay/OC1/OC2 - monostable
TB	Output on terminal/Relay/OC1/OC2 - bistable
SM	Sounder output with limited flasher time
SB	Sounder output with unlimited flasher time

Table E-2: Functioning and deactivation of the outputs

Symbol/Initials	Description
A	These outputs will deactivate if a Stop alarm, Reset partition or Disarm operation is carried out while the monostable time of the main output is running.
B	These outputs will deactivate only when the event clears after expiry of the monostable time of the main output.
C	These outputs, due to the continuous flasher function, will not deactivate automatically. In order to deactivate the SB flashers of the sounder after expiry of the monostable time applied to the main output, you must: <ul style="list-style-type: none"> • trigger an event which applies a Stop pattern to the SB flashers • reset the partition
D	These outputs will deactivate only when the event clears.
E	These outputs will deactivate if, when an event is active, a Stop alarm operation, reset or disarm partition command operation is carried out.
F	These outputs, due to the continuous flasher function, will not deactivate automatically. In order to deactivate the SB flashers of the device on termination of the event, you must: <ul style="list-style-type: none"> • trigger an event which applies a Stop pattern to the SB flashers • reset the partition
G	These outputs will deactivate when the respective monostable time expires

Table E-3: Output combinations

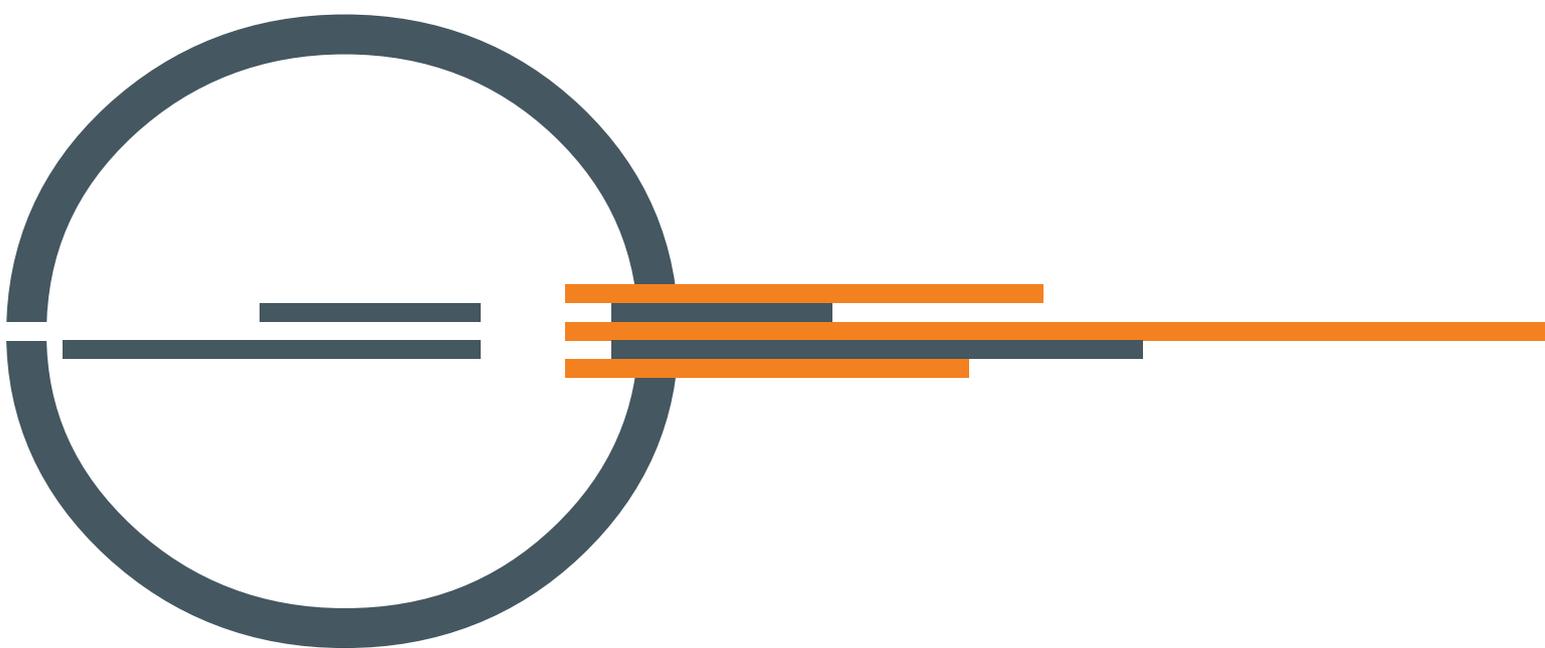
Event groups	Principal output				Other outputs			
	TM	TB	SM	SB	TM	TB	SM	SB
Zone Alarm terminal tamper partition alarm partition tamper	A G				A G	A B	A G	A C
		D E			E G	D G	E G	F
			A G		A G	A B	A G	A C
				F	E G	D G	E G	F
Control panel open Dislodged panel Expansion tamper/loss Keypad tamper/loss Reader tamper/loss Sounder tamper/loss Jamming Wireless zone loss Telephone line down	A G				A G	A D	A G	A C
		D E			E G	D G	E G	C
			A G		A G	A B	A G	A C
				F	E G	D G	E G	C
other events	G				G	B	G	C
		D			G	D	G	F
			G		G	B	G	C
				F	G	C	G	C

Appendix F

SIA CODES

SIA Codes		Event type	
Event activation	Event restoration	English	Italian
BA	BR	Burglary alarm	Violation/Intrusion alarm
BB	BU	Burglary bypass	Intrusion detectors disabled
BT	BR	Burglary trouble	Intrusion detector fault
BV	BR	Burglary verified	Violation/Intrusion confirmed
CA	OA	Automatic closing	Automatic arming
CL	OP	Closing report	Arming notification
CP	OA	Automatic closing	Automatic arming
DO	DR	Access open	Access open
FA	FR	Fire alarm	Fire detector activated
FB	FU	Fire bypass	Fire detector disabled
FI	FK	Fire test begin	Start fire test
FT	FJ	Fire trouble	Fire detector fault
GA	GH	Gas alarm	Gas detected
GB	GU	Gas bypass	Gas detector disabled
GT	GJ	Gas trouble	Gas detector fault
HA	HR	Hold-up alarm	Duress alarm
HB	HU	Hold-up bypass	Duress option disabled
HT	HJ	Hold-up trouble	Duress-signalling device fault
KA	KR	Heat alarm	Heat threshold exceeded
KB	KU	Heat bypass	Heat detector disabled
KT	KJ	Heat trouble	Heat detector fault
LT	LR	Phone line	Telephone line down
MA	MR	Medical alarm	Medical emergency
MB	MU	Medical bypass	Medical assistance option disabled
MT	MJ	Medical trouble	Medical assistance signalling-device fault
NL	OP	Perimeter armed	Stay mode active
OT	OJ	Late to close	Late to close
PA	PR	Panic alarm	Rescue request
PB	PU	Panic bypass	Rescue option disabled
PT	PJ	Panic trouble	Panic trouble
QA	QR	Emergency alarm	Call for help
QB	QU	Emergency bypass	Emergency option disabled
QT	QJ	Emergency trouble	Emergency-signalling device fault
SA	SR	Sprinkler alarm	Sprinkler alarm
SB	SU	Sprinkler bypass	Sprinkler disabled
ST	SJ	Sprinkler trouble	Sprinkler fault

SIA Codes		Event type	
Event activation	Event restoration	English	Italian
TA	TR	Tamper alarm	Tamper alarm
TB	TU	Tamper bypass	Tamper option disabled
UA	UR	Untyped zone alarm	Generic zone alarm
UB	UU	Untyped zone bypass	Generic zone disabled
UT	UR	Untyped zone trouble	Generic zone fault
WB	WU	Water bypass	Water detector disabled
WT	WJ	Water trouble	Water detector fault
ZB	ZU	Freeze bypass	Low-temperature detector disabled
ZT	ZJ	Freeze trouble	Low-temperature detector fault
UX	UX	Undefined	Undefined event
CF	OP	Forced closing	Forced arming
NF	NF	Forced perimeter	Forced perimeter arming
BC	UX	Burglary cancel	Deletion of intrusion memory
CE	UX	Closing extend	Closing extend
JP	UX	User on premises	Recognized access code
YC	YK	Communication fail	Unsuccessful report
MA	MH	Medical alarm	Medical emergency
RB	UX	Remote program begin	Start remote programming
YP	YQ	Power supply trouble	General power-supply fault
YT	YR	System battery trouble	Battery fault
ET	ER	Expansion trouble	I/O expansion fault
XT	XR	TX battery trouble	Low battery on wireless device
LB	LX	Local program	Start local programming
DD	DR	Access denied	Wrong code
RP	UX	Automatic test	Automatic communication test
JL	UX	Log threshold	Events log full
AT	AR	AC trouble	Mains faults
JR	JS	Schedule executed	Schedule executed
YI	YS	Overcurrent trouble	Overvoltage fault
EM	EN	Expansion device missing	I/O expansion loss
YK	UX	Communications restoration	Communications re-established
OU	OV	Output state trouble	Output fault
CI	UX	Fail to close	Unsuccessful arming operation



Evolving Protection

Inim Electronics S.r.l.

Centobuchi, via Dei Laboratori 10
63076 Montepandone (AP), Italy
Tel. +39 0735 705007 _ Fax +39 0735 704912

info@inim.it _ www.inim.it

ISO 9001 Quality Management
certified by BSI with certificate number FM530352



DCMPINE0SLIVINGE-700-20240702