SMARTLIVING

CEI 79-2
EN 50131-3
EN 50131-6
CEB T01

Ness Smart Living

Anti-intrusion Control Panels & Security Systems

INSTALLATION & PROGRAMMING MANUAL

GameOver

Innovative Electronic Solutions

CORPORATION

www.nesscorporation.com

National Customer Service Centre
Ph: 1300 551 991
customerservice@ness.com.au

Quality
ISO 9001
NSW Head Office only

SMARTLIVING

CEI 79-2
EN 50131-3
EN 50131-6
CEB T01

Ness Smartliving
Installation and Programming Manual

Document Part No: 890-443

Table of contents

ABOUT THIS MANUAL

DCMIINE0SLIVINGE **MANUAL CODE**

5.10 **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 a video button, or push a key on the control-panel keypad. **PRESS**

Graphic conventions 0-2

Following are the graphic conventions used in this manual.

Conventions	Example	Description
Text in italics	See *paragraph 0-2 Graphic conventions*	Indicates 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	0 ␣, F1 Fn, OK	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!**

The "DANGER" warnings indicate that total or partial disregard of the procedure could injure the operator or persons in the vicinity. **DANGER!**

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

Chapter 1

GENERAL INFORMATION

Supplier's details 1-1

Supplier:	Ness Corporation
Address:	4/167 Prospect Hwy, Seven Hills, NSW, 2147 Australia
Tel:	+61 2 8825 9222
e-mail:	customerservice@ness.com.au
Web:	www.nesscorporation.com

The persons authorized by the manufacturer to repair or replace the parts of this system, hold authorization to work on Ness Corporation's brand devices only.

Description of the product and various models 1-2

Description:	Intrusion control panel
Models:	SmartLiving 505 SmartLiving 515 SmartLiving 1050 SmartLiving 10100
Applied Normative:	CEI 79-2:1998+Ab:2000, CEI EN 50131-3:2009 and CEI EN 50131-6:2008
Certification agency:	IMQ - Security systems
Security rating:	2

Products certified and conforming to directives 1-3

The SmartLiving intrusion control panel and the devices described in this manual have been certified by the IMQ - Security Systems agency as compliant with CEI 79-2:1998+Ab:2000, CEI EN 50131-3:2009 and CEI EN 50131-6:2008, when duly programmed, as described in *Chapter 7 - Compliancy with the regulations in force*.

The Control panel enclosure houses the following certified devices:

- INIM switching-power supply
- Motherboard (IN082 or IN088)
- SmartLogos30M voice board (accessory item)
- FLEX5/U input/output expansion board (accessory item)
- AUXREL32 relay board (accessory item)
- SmartLAN/SI and SmartLAN/G LAN interface boards (accessory items)
- IB100/RU BUS isolator board (accessory item)
- ProbeTH thermal-probe kit for battery-charge optimization (accessory item)
- TamperNO tamper-protection kit (accessory item)
- Backup battery, 12 V @ 17 Ah
- Motherboard (IN082 and IN088) integrated Type B notification apparatus

The control panel complacency is also guaranteed when connected to the following certified devices:

- FLEX5/P input/output expansion boards
- Joy/MAX, Joy/GR, cCode/G, nCode/G keypads
- nBy/S outdoor-mount proximity readers
- nBy/X universal-mount proximity readers
- IB100/RP BUS isolator
- Self-powered IB100/A BUS isolator
- nCard access-control card for proximity readers
- Tag for nKey or nBoss proximity readers
- Self-powered sounderflashers for outdoor installation: Ivy, Ivy-F, Ivy-M, Ivy-FM, Ivy-B, Ivy-BF, Ivy-BM, Ivy-BFM
- Wireless devices AIR2, AIR2-BS100 (transceivers), Air2-IR100 (PIR detectors), Air2-MC100 (magnetic contacts)

TYPE B NOTIFICATION APPARATUS

ATS2 notification apparatus (refer to EN50131-1:2008-02, paragraph 8.6 Notification, Table 10, page 46, Grade 2 and EN50136) characterized by:

- Transmission time - classification D2 (60 seconds)
- Transmission time - max. values M2 (120 seconds)
- Classification time - classification T2 (25 hours)
- S0 Substitution security (no detection of device substitution)
- I0 Information security (no detection of message substitution)

ATS4 notification apparatus (refer to EN50131-1:2008-02, paragraph 8.6 Notification, Table 10, page 46, Grade 3 and EN50136) features the following parameters (available on SmartLAN/G and SmartLAN/SI only):

- Transmission time - classification D2 (60 seconds)
- Transmission time - max. values M2 (120 seconds)
- Classification time - classification T3 (300 minutes)
- S1 Substitution security (measures aimed at detecting the substitution of the transceiver of the supervised site by means of an identifier code or address in all messages sent over the transmission link).
- I2 Information security (measures aimed at impeding unauthorized changes to transmitted information).

Patents Pending 1-4

The SmartLiving series of control panels employs the following patented technologies.

- **Input/Output Terminals**: each terminal on-board the control panel, keypads and expansion boards can be configured as either an input or output zone.
- **nBy/X proximity reader**: this reader has been especially designed to flush-mount to all models of electrical light-switch backboxes.
- **Learn zone balancing**: this option allows the control panel to save the balancing values of all the system zones automatically, thus eliminating the task of typing them in.

Manuals 1-5

Installation and programming manual (this manual) 1-5-1

This manual (not included in the package) can be purchased from your retailer. You (the installer) should read carefully through it in order to become familiar with all the components and operating procedures of the SmartLiving system.

In order to provide adequate protection, the installer must adhere to all the manufacturer's guidelines relating to the active and passive security devices of this system.

Installation and programming guide 1-5-2

This guide is included in the control panel package and provides all the instructions and illustrations necessary for fast installation and programming of the SmartLiving system. It provides step by step descriptions of the procedures required for the system wiring,

the various connections and first power-up. It also provides a table for the peripheral addressing process and a quick guide indicating default parameters and values and how to programme/change them directly from the keypad.

User's manual 1-5-3

The installer should read carefully through the user's manual (supplied with each control panel). Once the system has been installed, you must ensure that the User's Manual is available to the users for consultation, and that they fully understand how the system works and are aware of all the functions, settings and procedures.

It is the installer's responsibility to inform the system users that, regardless of its capabilities, an intrusion alarm system is not a substitute for the necessary precautions building occupants must take to prevent intrusion.

Operator Qualifications 1-6

Installer 1-6-1

The installer is the person (or group of persons) who sets up and programs the entire security system in accordance with the purchaser's requirements and in respect of the safety and security regulation in force. As the only individual in contact with system users, it is the installer's responsibility to instruct them on how to use the security system properly.

Under normal circumstances, the installer is not allowed to arm/disarm the system without previous authorization from the user. All the system partitions must be disarmed before accessing the parameter programming phase.

The access code of the installer is a level 3 access code.

User 1-6-2

The users are the occupants of the building where this intrusion control panel is installed. Only authorized users can access and operate the system.

Thanks to the extreme flexibility of the system, the most common operations can be carried out without authorization. This operating method must be expressly requested by the main user, as it considerably lowers the security level of the system and may cause false alarms, accidental arm/disarm operations, etc.

A system access code can be associated with each user. The programming process allows you to define the code hierarchy:

- **User**
- **Manager**
- **Master**
  The system codes can carry out, in accordance with their assigned level in the system hierarchy (the "User" being the lowest level), the following operations on all other codes that are inferior hierarchically:
  - enable/disable
  - change PIN
  - change the programming parameters

If the system programming complies with security grade 3 of EN 50131, some partition arming or delete memory operations, requested from a keypad, may be authorized by the entry of a level 3 code (installer code) as well as by a user code.

Access Levels 1-7

The normative defines the following system-access levels, regardless of system-access limitations:

- **Level 1** - access by any person (e.g. passer-by)
- **Level 2** - user access
- **Level 3** - installer or maintenance operator access (authorized by user - level 2)
- **Level 4** - manufacturer access

Conventions – Glossary 1-8

In order to understand the terminology used in this manual and improve your knowledge of this system and its operating procedures, read carefully through the glossary (refer to *Appendix A, Technical terminology and Glossary*).The appendix contains the definitions of technical terms commonly used in the field of security, therefore, relevant to the SmartLiving system.

Chapter 2

THE CONTROL PANEL AND PERIPHERALS

Environmental Conditions 2-1

All control panels from the SmartLiving series are for indoor installation only and operate best under the following conditions:

- **Temperature**: from -10° to +40°C
- **Maximum humidity**:75% (without condensation)
- **Environmental class**:II

The nCode/G, cCode/G, Alien/S, Alien/G, IB100, FLEX5, Nexus and nBy/X peripheral devices are for indoor installation only and operate best under the following environmental conditions:

- **Temperature**: from -10° to +40°C
- **Maximum humidity**:75% (without condensation)
- **Environmental class**:II

The nBy/S reader is suitable for outdoor installation and operates best under the following conditions:

- **Temperature**: from -25° to +70°C
- **Maximum humidity**:93% (without condensation)
- **Protection grade**:IP34
- **Environmental class**:IV

SmartLiving intrusion control panels 2-2

Package contents 2-2-1

Inside the package you will find:

- Metal enclosure containing the wired motherboard and power supply (adapter or switching-power supply)
- User's Manual
- Quick Installation Guide
- Plastic bag:

Table 1: **Package contents**

Control panel models	505	515	1050	1050L	10100L
3k9 Ohm 1/4W resistance	10		20		
Resistance 6k8 Ohm 1/4W	10		20		
Backup-battery wire	1				
Screws to secure the frontplate of the metal enclosure	4				

Items not included in the package:

Thermal probe (battery-charge optimizer which operates in accordance with the battery temperature), backup battery, Dialler Lead, SmartLeague programme CD, Installation Manual. These devices are accessory items which must be purchased separately.

Control panel descriptions 2-2-2

Table 2: **Control panels - electrical and mechanical features**

Control panel models	505	515	1050	1050L	10100L
Power supply voltage	230V ~ -15% +10% 50/60Hz				
Nominal output voltage	13.8V				
Voltage - operating range	9 - 16 V				
Maximum current draw	0.2A		0.4A		0.6A
Current draw of control panel motherboard	110mA @ 22V~		75mA @ 13.8V=		
Maximum distributable current @ 12V	1.2A		3A		5A
Maximum distributable current to open-collector outputs	150mA		500mA		
Maximum power-supply voltage ripple	340mV		70mV		
Max. battery-charge current	1A		2A		
Backup battery	12V 7Ah			12V 17Ah	
	recharged 80% in 24h				
Max. current across +AUX terminals	900mA		4.05A (1.35A for +AUX1, 1.35A for +AUX2, 1.35A for +AUX3)		
Power supply (EN 50131)	Type A				
Enclosure Dimensions (W x H x D)	21.5 x 30.5 x 8.5cm			37.5 x 51 x 8.5cm	
Weight (without battery)	2.5 Kg		2.2 Kg	5.3 Kg	

Compliancy with EN 50131, CEI 79 or CEB T014 requires that the values of the maximum distributable current respect determined limits, as indicated in *paragraph 3-1-3 Maximum current - normative references*.

The control panel label s located inside the enclosure.

The following table shows the maximum number of devices supported by the various control panel models.

Table 3: **Control panel - Main Features**

Control panel models		505	515	1050	1050L	10100L
Total terminals		5	15	50		100
Terminals on panel	**total**	5		10		
	configurable as inputs	5		10		
	configurable as rollerblind/shock	2				
	configurable as outputs	0		5		
Total zones		10	30	100		200
Outputs on control-panel motherboard	**total**	3				
	Relay	1				
	open-collector	2				
Partitions		5		10		15
Keypads (JOY, nCode/G, cCode/G, Alien)		5		10		15
Voice memo slots		5		10		15
FLEX5 expansions		5	10	20		40
nBy Readers		10		20		30
Air2-BS100 Transceivers		10		20		30
Digital keys and keyfobs		50		100		150
Possible key combinations		4294967296				
IB100 isolators		15				
Nexus dialer		1				
Codes		30		50		100
Scenarios		30				
Timer		10				20
Recordable Events		500				1000
Programmable events		10		30		50

Note

SmartLiving control panels are not equipped with built-in dislodgement-tamper microswitches. For the order code of this accessory item, refer to Ness Sales staff.

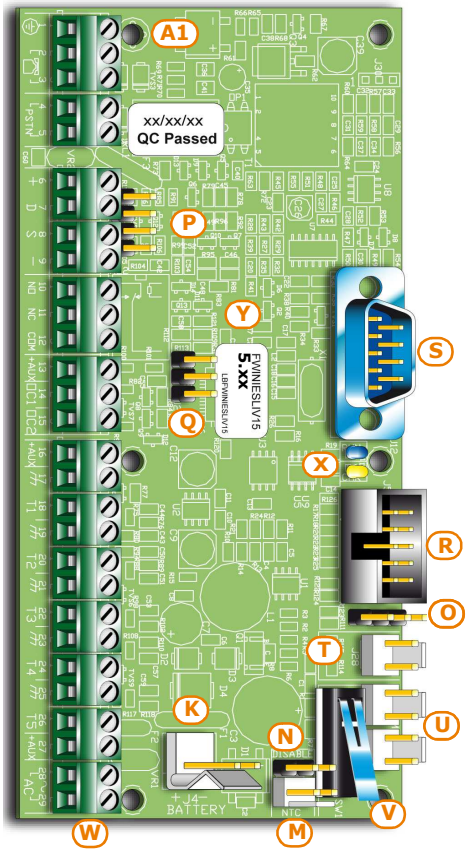
Table 4: **Control panels - description of parts**

Models	505	515	1050	1050L	10100L
A	Power adapter (Transformer)		3A switching power supply		5A switching power supply
B	Mains connection terminal-board (230 Vac) - 50/60 Hz				
C	Power cable - adapter to control panel		Power cable - switching-power supply to panel		
D			Power cable - switching-power supply to panel		
E	Mains cable entry				
F	Metal enclosure				
G	Anchor-screw locations for the metal backbox				
H	Dislodgement-tamper microswitch location				
I	Backup battery				
J	Backup-battery wire				
K	Backup-battery connector				
L	Thermal probe (accessory item)				
M	Thermal probe connector				
N	Thermal probe (enable/disable) jumper				
O	Connectors for the SmartLAN power-supply jumper				
P	Local I-BUS connector				
Q	Maintenance jumper connectors				
R	SmartLogos30M voice-board connector				
S	Control panel to PC serial cable connector				
T	Dislodgement-tamper microswitch connector (accessory item)				
U	Open-panel tamper microswitch connector (accessory item)				
V	Open-panel tamper microswitch				
W	Terminal board				
X	Blue and yellow activity LEDs				
Y	Firmware version label				
Z	Anchor-screw locations for AUXREL32 board				
A1	Ground connection screws				
B1	FLEX5/U expansion board locations				

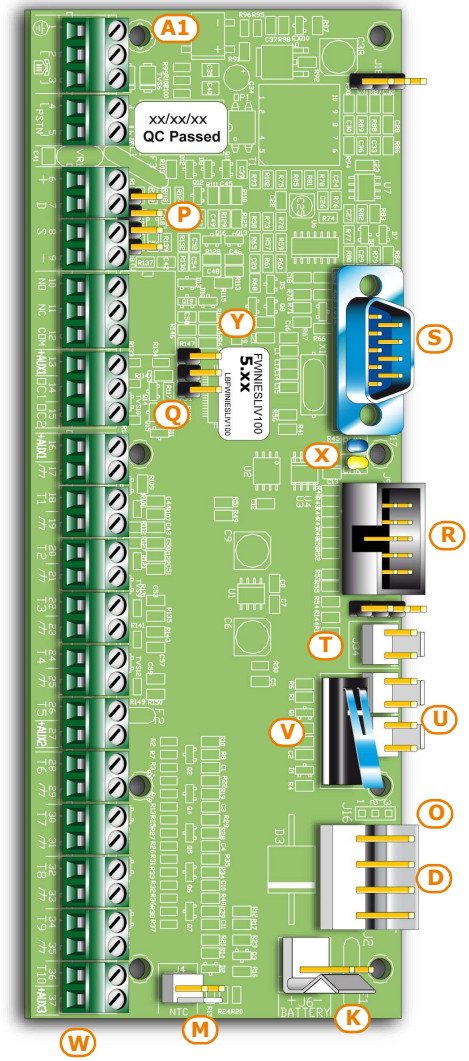
Table 5: **Control panel - terminal board**

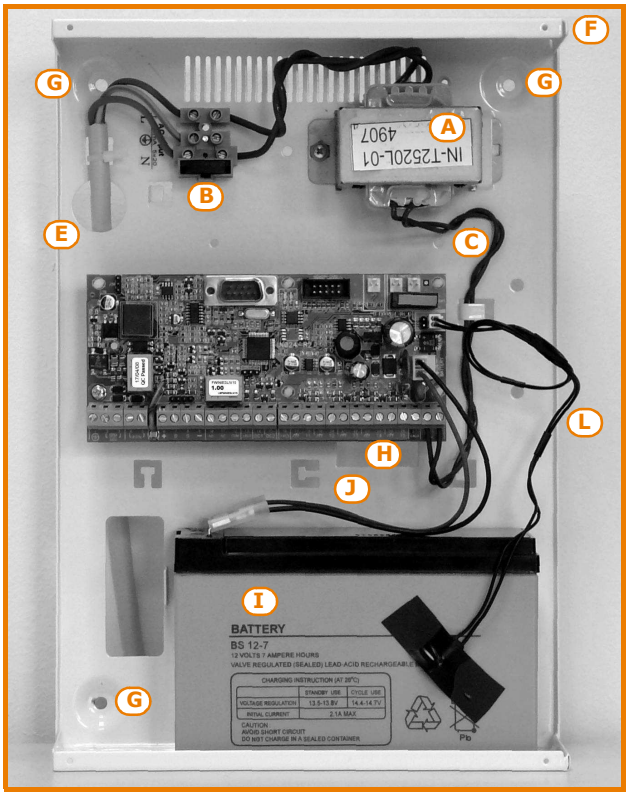
n.	icon/identifier	Model				
		505	515	1050	1050L	10100L
1	⏚	Earth connection				
2-3	☎	Internal telephone-line connection				
4-5	**PSTN**	Land-line connection (PSTN)				
6-7-8-9	**+ D S -**	I-BUS connections				
10-11-12	**NO NC COM**	Voltage-free contacts of the relay output (Typically External Siren)				
13	**+AUX**	12V Ancillary power supply				
14-15	**OC1 OC2**	Open-collector outputs (Typically OC1 Strobe & OC2 Internal Siren)				
16	**+AUX**	+12V Ancillary power supply				
17-19-21-23-25	⏚	Power supply negative (earth or GND)				
18-20-22-24-26	**T1-T2-T3-T4-T5**	Control panel input terminals: T1, T2, T3, T4 and T5				
27	**+AUX**	12V Ancillary power supply				
28-29	**AC**	Power supply input from the transformer				
28-30-32-34-36	**T6-T7-T8-T9-T10**				Terminals: T6, T7, T8, T9 and T10 of the control panel	
29-31-33-35	⏚				Power supply negative (earth or GND)	
37	**+AUX**				12V Ancillary power supply	

SmartLiving 505/515 control-panel motherboard

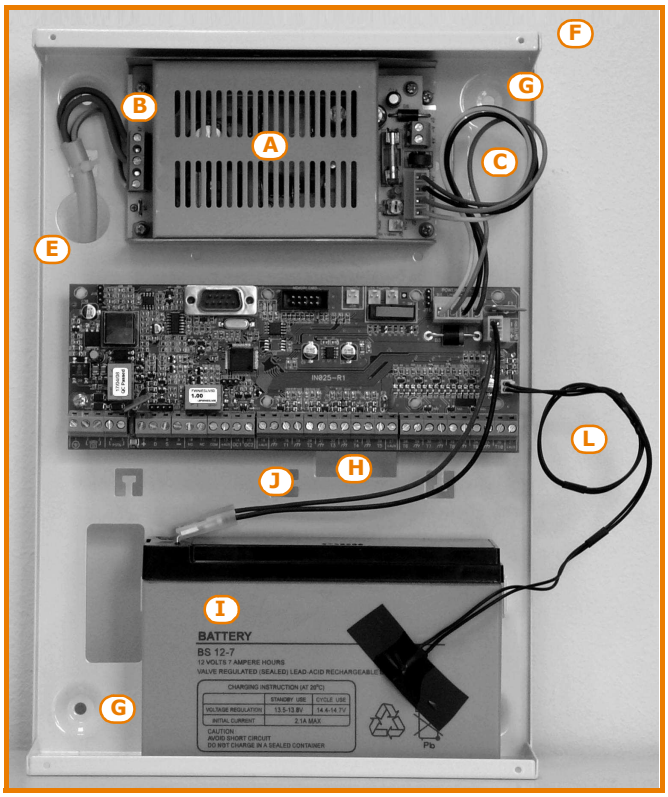


SmartLiving1050/1050L/10100L Control panel motherboard

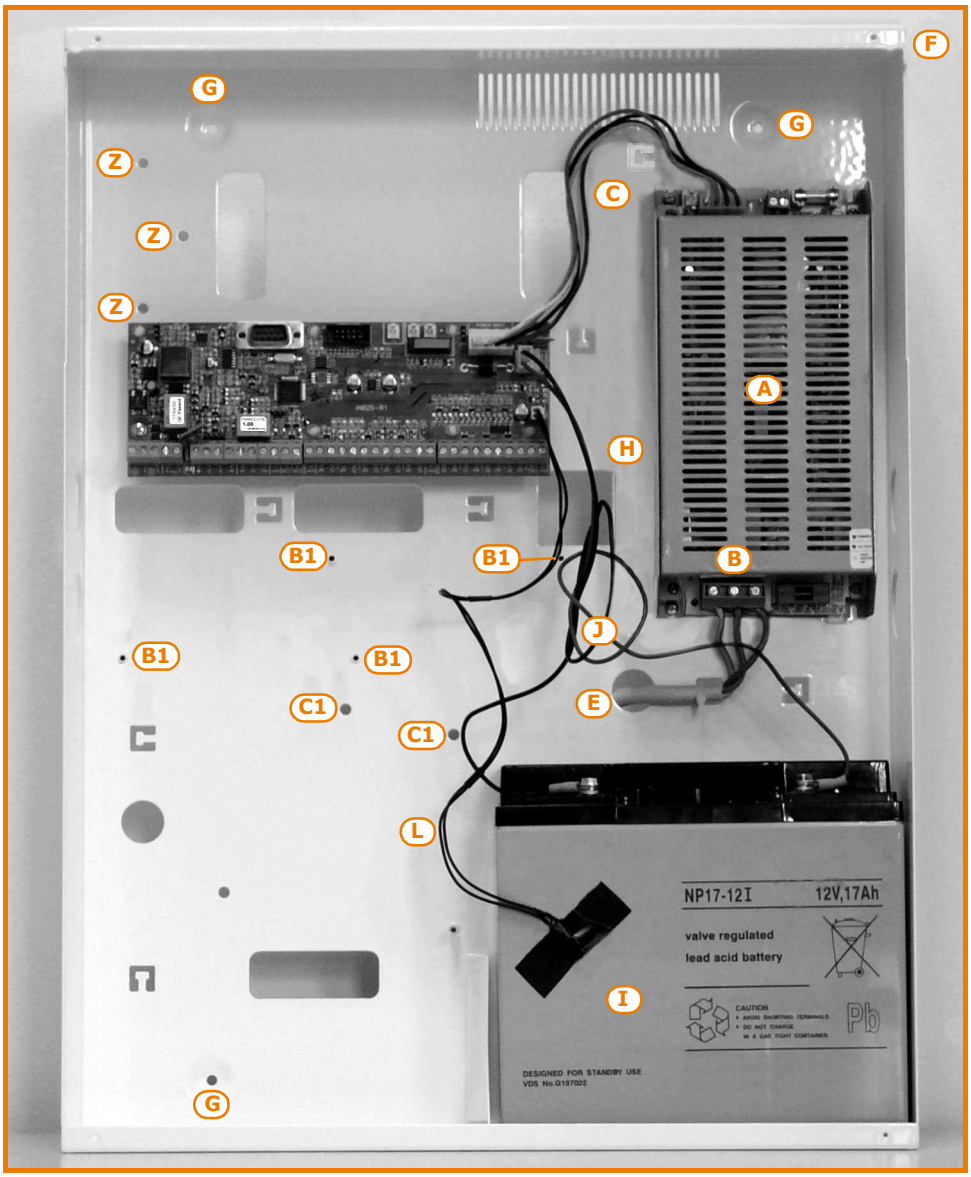




SmartLiving 505/515



SmartLiving 1050



SmartLiving 10100L

Events log memory 2-2-3

The control panel events are saved to a non-volatile semiconductor-memory which retains data without the need of power.

The electrical characteristics of semiconductor devices diminish over time. However, a minimum period of 40 years data retention is guaranteed.

I-BUS interconnections 2-2-4

SmartLiving control panels are equipped with a 4-wire BUS for peripheral interconnections (2 power-supply wire and 2 data exchange wires, refer to *paragraph 3-2-1 The I-BUS line wiring*).

The intellectual property rights regarding the electrical, structural and protocol features of the BUS are the sole property of the manufacturers.

The I-BUS is not a RS485 differential BUS.

Peripherals 2-3

The control panel I-BUS accommodates the following peripherals:

- JOY/GR, JOY/MAX, nCode/G, cCode/G, Alien/G e Alien/S keypads
- Readers (nBy/S and nBy/X)
- Expansions (Flex5)
- Transceivers (Air2-BS100)
- Sounderflashers (Ivy)
- IB100 isolators
- GSM dialer (Nexus)

Joy/GR and Joy/MAX keypads 2-3-1

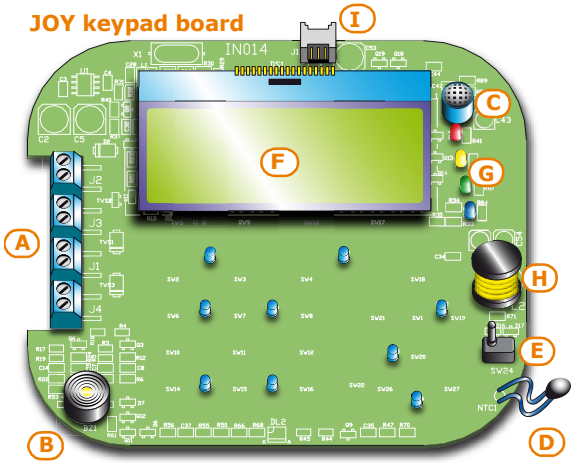
Table 6: **Device specifications**

Joy keypads models	JOY/GR	JOY/MAX
Voltage [V]	9 - 16	
Typical current draw [mA]	70	90
Terminals configurable as OC outputs	2	
Maximum current draw per terminal [mA]	150	
Dimensions (W x H x D) [mm]	142 x 116 x 20	
Weight [g]	160	180

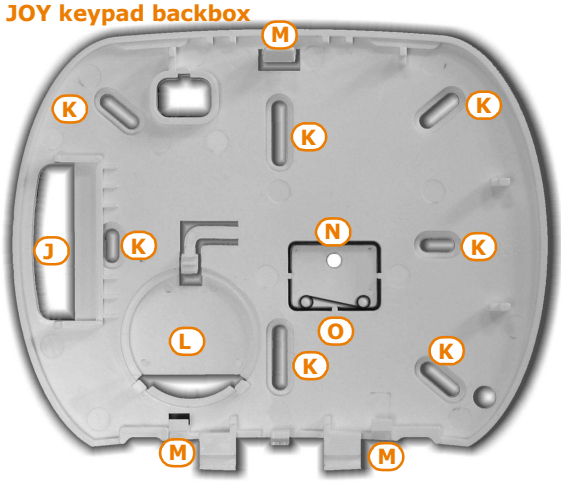
Table 7: **Joy - description of parts**

A	Terminal board
B	Buzzer
C	Microphone (Joy/MAX only)
D	Temperature sensor (Joy/MAX only)
E	Open-tamper microswitch
F	Backlit graphic display
G	Signaling LEDs
H	Antenna (Joy/MAX only)
I	Speaker-wire connector (Joy/MAX only)
J	Wire entry
K	Wall-mount screw locations
L	Speaker housing
M	Board supports
N	Dislodgement-tamper microswitch screw location
O	Dislodgement-tamper microswitch spring

JOY keypad board



JOY keypad backbox



Keypad terminals:

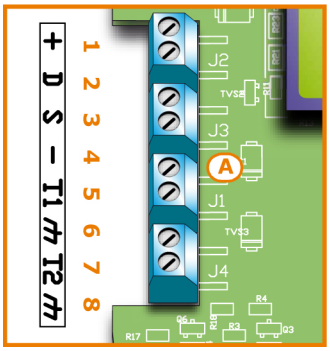
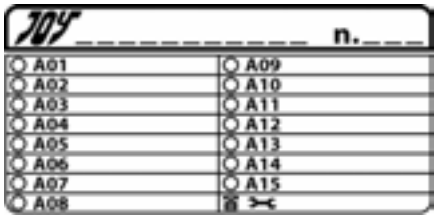


Table 8: **Joy - terminal board**

n.	icon/identifier	description
1	+	Terminal "**+**" for the I-BUS connection
2	D	Terminal "**D**" for the I-BUS connection
3	S	Terminal "**S**" for the I-BUS connection
4	-	Terminal "**-**" for the I-BUS connection
5	T1	Screw terminal of keypad terminal T1
6	⏚	Negative power terminal (Negative or GND)
7	T2	Screw terminal of keypad terminal T2
8	⏚	Negative power terminal (Negative or GND)



Terminals T1 and T2 can be configured as:

- Input (also as Rollerblind or Shock)
- Output
- Double zone
- Supervised Output

The keypad package contains a sticker (to be located under the keypad flip) which can be used to note down the keypad address or label, its location, the partitions it controls and any phone-contact numbers.

nCode/G and cCode/G Keypads 2-3-2

Table 9: **Device specifications**

Keypad models	nCode/G	cCode/G
Voltage [V]	9 - 16	
Typical current draw [mA]	70	80
Terminals configurable as OC outputs	1	
Maximum current draw per terminal [mA]	150	
Dimensions (W x H x D) [mm]	87 x 129 x 18	
Weight [g]	135	155

nCode/G keypad

cCode/G keypad

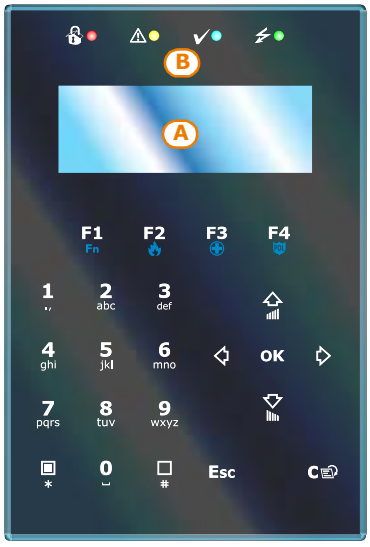
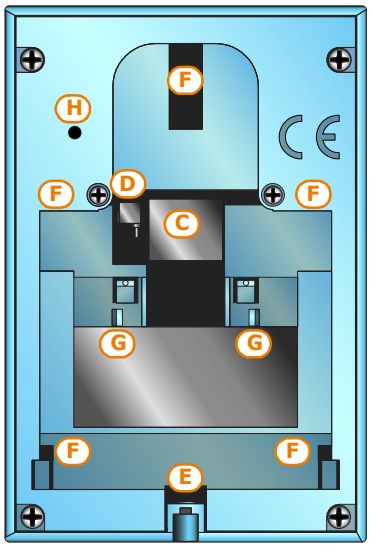


Table 10: **nCode/G and cCode/G - description of parts**

A	Backlit graphic display
B	Signaling LEDs
C	Cable connector
D	Tamper microswitch
E	Screw location
F	Screw location
G	Terminal board guide
H	Buzzer

Retro keypads
nCode/G and cCode/G

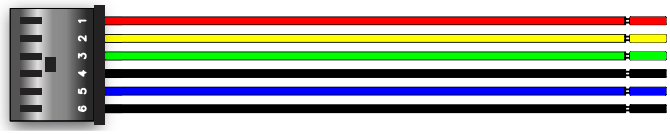


nCode/G and cCode/G keypads are equipped with a buzzer and a T1 terminal which can be configured as:

- Input (also as Rollerblind or Shock)
- Output
- Double zone

You can connect nCode/G and cCode/G keypads using the connector on the back of the device, using either the 6 wire cable (included), or the KB100 terminal board included in the deep-bracket kit (accessory kit).

6 wire cable



KB100 - terminal board

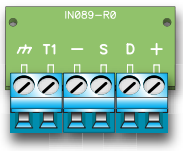


Table 11: **Connection cables - KB100 terminal board**

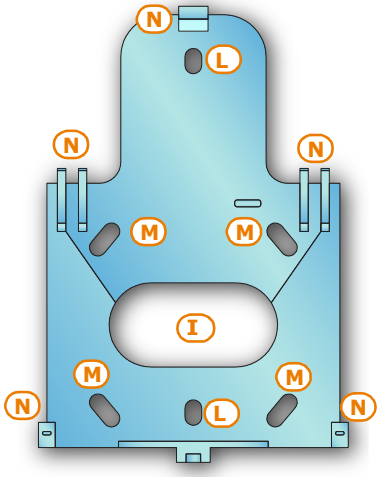
n.	Wire colour	KB100 terminal board	description
1	Red	+	Wire/Terminal "**+**" for the I-BUS connection
2	Yellow	D	Wire/Terminal "**D**" for the I-BUS connection
3	Green	S	Wire/Terminal "**S**" for the I-BUS connection
4	Black	-	Wire/Terminal "**-**" for the I-BUS connection
5	Blue	T1	Wire/terminal of keypad terminal T1
6	Black	⏚	Negative power wire/terminal (Negative or GND)

Table 12: **Brackets - description of parts**

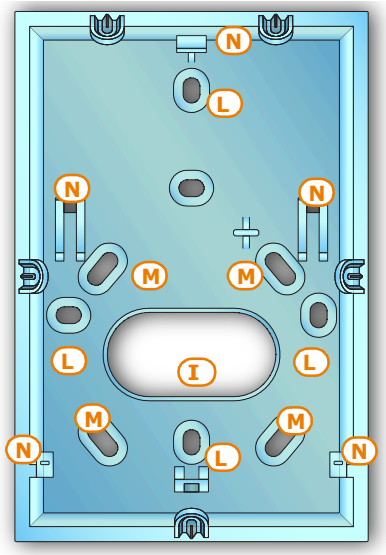
I	Wire entry
L	Wall-mount screw locations
M	Flush-mount screw locations
N	Backlocking grips

Note: Keypads are enabled with Tamper switches, so ensure they are securely mounted before attempting to operate the system.

Mounting bracket



KB100 - deep mounting bracket



Alien/G and Alien/S touch screen keypads 2-3-3

- Touch-screen
- Protection against removal and dislodgement tamper
- Input/Output terminals (Alien/G only)
- Compatible with all SmartLiving 5.0 and higher models
- Thermometer and chronothermostat function
- Microphone and loudspeaker for voice functions
- Built-in proximity reader
- System interface with I-BUS and RS485 BUS
- USB Interface
- SD card interface
- Photoframe function with images on SD card
- Background customization with images on SD Card
- Skin selection
- Black or white

Alien/S - front

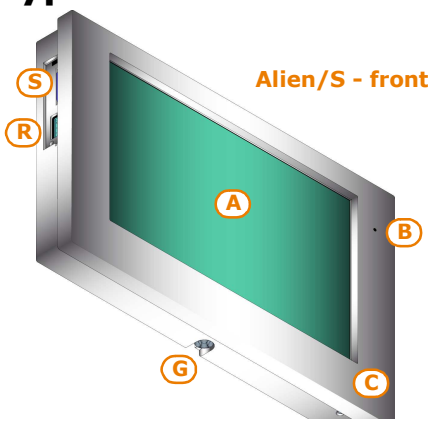
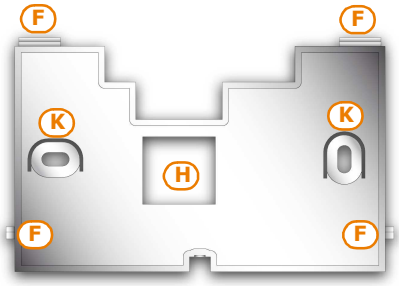
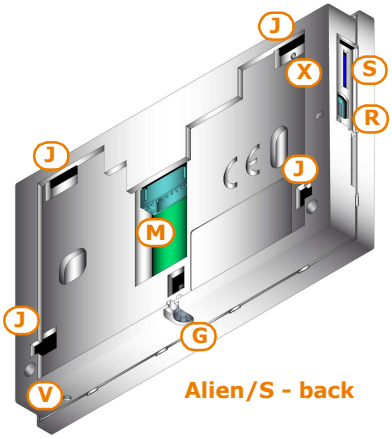


Table 13: **Alien - description of parts**

A	Display
B	Microphone
C	Proximity reader
D	Touch pen holder
E	Closure hooks
F	Backlocking grips
G	Securing screw

Alien/S - mounting bracket





Alien/S - back

Table 13: **Alien - description of parts**

H	Cable entry
I	Screw locations
J	Back-locking grip locations
K	Flush-mount screw locations for "503" box
L	PCB
M	Terminal board/Connector for wires
N	Dislodgement-tamper microswitch
O	Open-tamper microswitch
P	Battery connector
Q	Ethernet connector
R	Mini USB connector
S	Slot for micro-SD card
T	Selection jumper connectors for EOL resistance on RS485
U	LED activity
V	Temperature sensor
W	Reset button
X	Forced calibration button

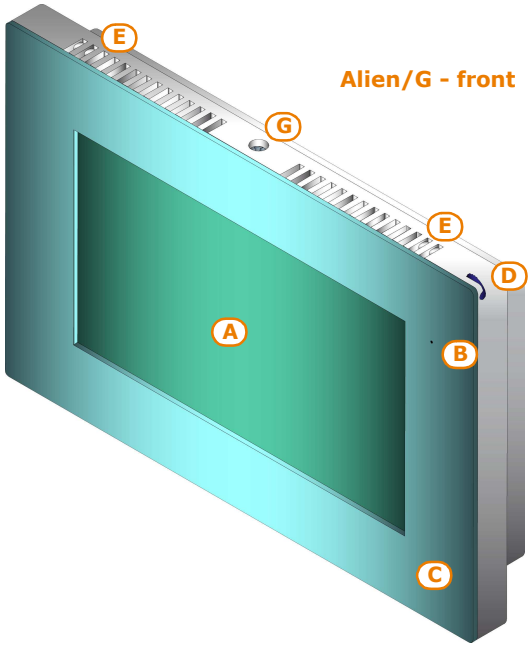
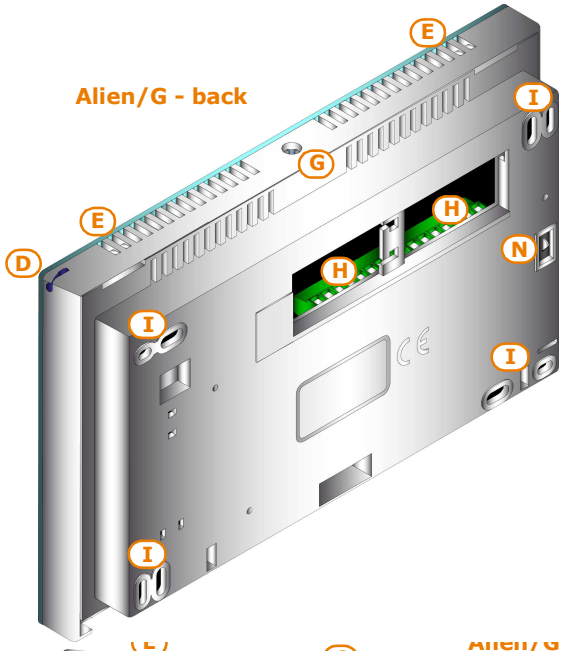
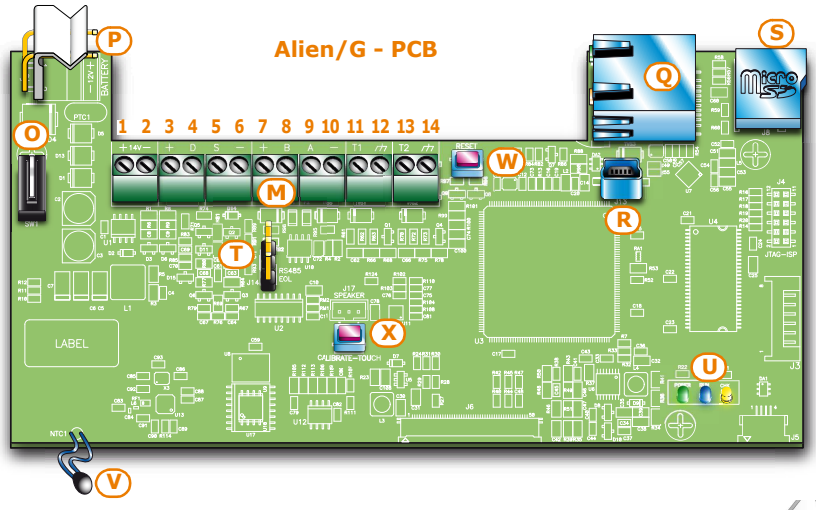
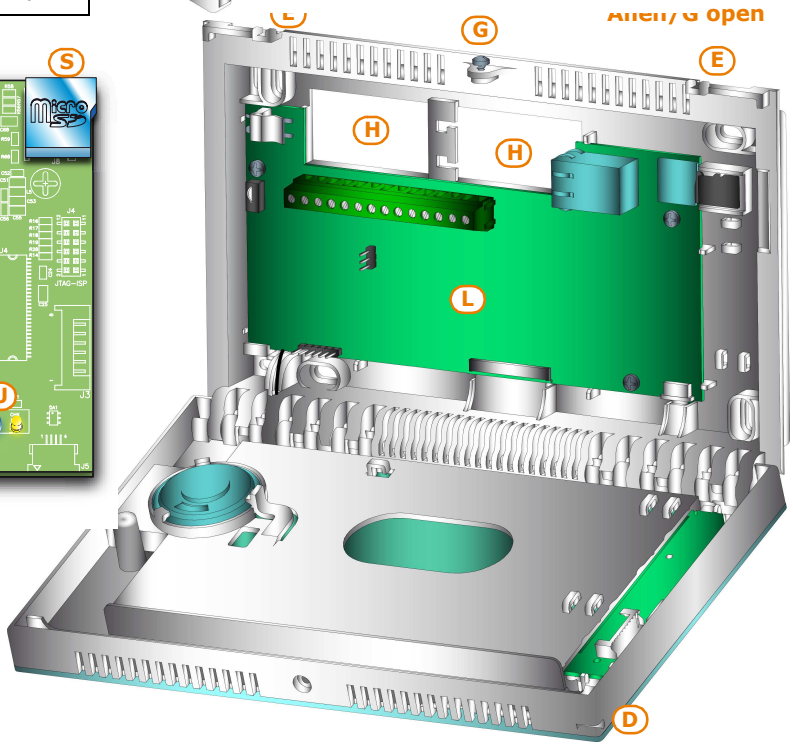


Table 14: **Alien/G - terminal board**

n.	icon/iden-tifier	description
1	**+ 14V**	Positive power terminal
2	**- 14V**	Negative power terminal
3	**+**	Terminal "**+**" for the I-BUS connection
4	**D**	Terminal "**D**" for the I-BUS connection
5	**S**	Terminal "**S**" for the I-BUS connection
6	**-**	Terminal "**-**" for the I-BUS connection
7	**+**	Terminal "**+**" for the RS485 BUS connection
8	**B**	Terminal "**B**" for the RS485 BUS connection
9	**A**	Terminal "**A**" for the RS485 BUS connection
10	**-**	Terminal "**-**" for the RS485 BUS connection
11	**T1**	Screw terminal of keypad terminal T1
13	**T2**	Screw terminal of keypad terminal T2
12 - 14	⏚	Negative power terminal (Negative or GND)







Terminals T1 and T2 can be configured as:

- Input (also as Rollerblind or Shock)
- Output
- Double zone
- Supervised Output

Connection of the Alien/S keypad is achieved through the connector on the back and must done using the 8 wire cable which comes with the keypad.

Alien/S - 8 wire cable

Table 15: **Alien/S - Connection wires**

Wire colour	Alien/S terminal board	description
Red	**+**	Cable/Terminal "**+**" of the I-BUS and RS485 BUS
Yellow	**D**	Cable/Terminal "**D**" for the I-BUS connection
Green	**S**	Cable/Terminal "**S**" for the I-BUS connection
Black	**-**	Cable/Terminal "**-**" of the I-BUS and RS485 BUS
Grey	**B**	Terminal "**B**" for the RS485 BUS connection
Blue	**A**	Terminal "**A**" for the RS485 BUS connection
White	**REOL**	Wire/Terminals to establish the EOL on the RS485

Table 16: **Device specifications**

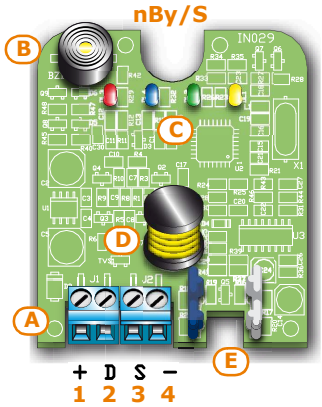
Keypad models	Alien/S	Alien/G
Voltage [V]	9 - 16	
Typical current draw [mA]	150	400
Terminals configurable as OC outputs	-	2
Maximum current draw per terminal [mA]	150	
Input/Output terminals	-	2
Screen dimensions[in]	4.3	7
Number of display colours	65000	
Display resolution	480x272	800x480
SD card capacity [GB]	Max. 16	
Box for flush-mount installation	Bracket for mounting to standard "503" boxes	Flush-mount box supplied (214x129x54 mm)
Dimensions (W x H x D) [mm]	131x81x17	219x143x34 If mounted to flush-mount box: 219x143x17
Weight [g]	160	520

Readers - nBy/S and nBy/X

Table 17: **Device specifications**

Reader models	nBy/S	nBy/X
Voltage [V]	9 - 16	
Typical current draw [mA]	40	35
Dimensions (W x H x D) [mm]	64 x 80 x 17	19 x 50 x 51
Weight [g]	45	25

nBy/S



nBy/X

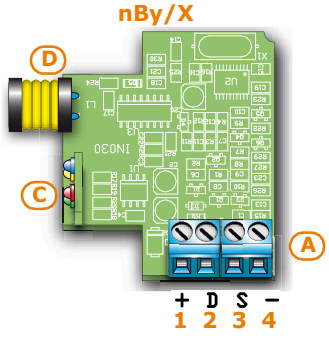


Table 18: **nBy - description of parts**

A	Terminal board
B	Buzzer (nBy/S only)
C	LED
D	Antenna
E	Optical sensors for open-enclosure and dislodgement tamper detection

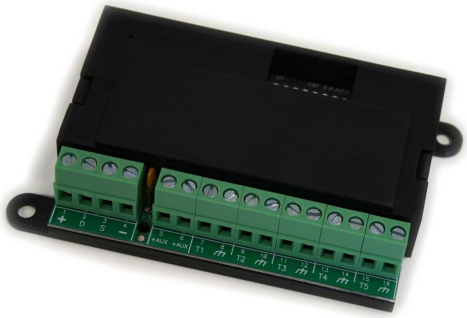
Reader terminals:

Table 19: **nBy - terminal board**

n.	icon/identifier	description
1	**+**	Terminal "**+**" for the I-BUS connection
2	**D**	Terminal "**D**" for the I-BUS connection
3	**S**	Terminal "**S**" for the I-BUS connection
4	**-**	Terminal "**-**" for the I-BUS connection

Patent
Patent

Flex5 expansion boards 2-3-4



Flex5/U

- **Flex5/U** comes in an enclosure with on-view terminals and address DIP-Switch, as shown above. It is evident that this version offers little protection to the terminals and is recommended to be installed in a tamper protected enclosure. The jumper of connector [D] enables/disables the protection against open and dislodgement tamper of the plastic enclosure only.

Table 20: **Device specifications**

Expansion board models		FLEX5/U
Voltage [V]	9 - 16	
Typical current draw [mA]	30	
Max. current across +AUX terminals [mA @13.8V]	300	
Dimensions including enclosure (W x H x D) [mm]		105 x 58 x 18
Weight including enclosure [g]		66

The packages of both versions of the Flex5 expansion board contain:

- Flex5 expansion board in a plastic enclosure
- Dislodgement/Open tamper jumper
- 10 resistors @ 3K9Ohm 1/4W
- 10 resistors @ 6K8Ohm 1/4W

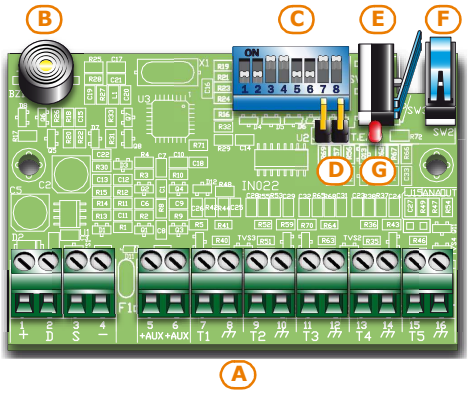


Table 21: **Flex5 - description of parts**

A	Terminal board
B	Buzzer
C	DIP-Switch strip for peripheral device addressing
D	Connector to enable peripheral-tamper detection
E	Dislodgement-tamper microswitch
F	Open-tamper microswitch
G	Peripheral activity LED (where present)

Peripheral activity LED signals are as follows:

- fast blinking - peripheral operative and enrolled (in configuration)
- slow blinking - peripheral operative but not enrolled (not in configuration)

The Flex5 expansion board terminals are as follows:

Table 22: **Expansion terminal board**

n.	icon/ identifier	description
1-2-3-4	**+ D S -**	I-BUS connection terminals
5-6	**+AUX**	12V ancillary power source terminals
7-9-11-13-15	**T1-T2-T3-T4-T5**	Screw terminals for expansion terminals: T1, T2, T3, T4 and T5
8-10-12-14-16	⏚	Negative power terminals (Negative or GND)

Terminals T1, T2, T3, T4 and T5 can be configured as:

- Input (Rollerblind or Shock for terminals T1, T2, T3 and T4 only)
- Output
- Double zone
- Supervised Output

Transceiver for Air2-BS100 2-3-5

The Air2-BS100 two-way wireless system integrates directly with all models of the Ness SmartLiving Series intrusion control panel range.

Description of the Air2 system devices:

- Air2–BS100 transceiver module
- Air2–IR100 passive infrared detector
- Air2–MC100 magnetic contact/rollerblind/exit
- Air2–MC200 magnetic contact/shock and tilt detector
- Air2–KF100 4 button remote-control keyfob
- Air2-FD100 smoke detector

For a complete description of all these devices refer to the Air2-BS100 Installation Guide.

IVY sounder/flasher 2-3-6

The IVY is a High Security Outdoor Siren / Flasher.
The self-powered sounders from the IVY outdoor series are controlled continuously by a microprocessor which monitors all the device parameters to ensure performance and reliability at all times.

For a complete description of all these devices refer to the sounder Installation Guide.

IB100 isolators 2-3-7

Isolators from the IB100 series peripherals can be connected directly to the I-BUS, in order to increase both its length and performance.

Each isolator has 4 input terminals and 4 output terminals for the BUS connection with the following functions:

- Galvanic Isolation, up to 2500V, for the entire BUS between input and output.
- Regeneration of the communication signals.
- Detection of anomalies towards the output section and its consequent isolation.

For a complete description of all these devices refer to the respective Installation Guide.

Nexus dialers 2-3-8

All models of the Nexus dialer are managed by the BUS. The Standard model interfaces SmartLiving control panels with GSM communication channels whereas, the Nexus/G model also interfaces with GPRS channels.

The functions made available to control panels equipped with this device are:

- voice calls via the Nexus using an installed SmartLogos30M voice board
- digital report calls via GSM using CONTACT-ID and ADEMCO 10 bps protocols
- digital report calls via GPRS using SIA-IP (Nexus/G model only)
- SMS messages for each event using either -
  - •• the description provided by the keypad events log
  - •• the customized description (maximum 50 editable SMS texts)
- the control panel carries out commands sent by the user via SMS message
- the control panel carries out commands after recognition of the user's telephone number (CALLER-ID)
- Answerphone

Table 23: **Nexus - electrical and mechanical features**

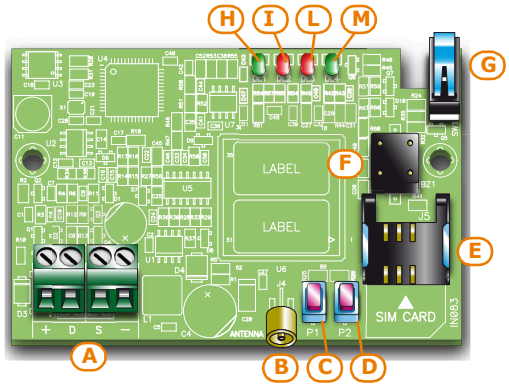
Voltage [V]	9 - 16
Current draw in standby [mA]	90
Maximum current draw [mA]	900
Dimensions including enclosure (W x H x D) [mm]	105 x 58 x 18
Weight including enclosure [g]	66

The Nexus package includes:

- Nexus expansion board in a plastic enclosure
- Remote antenna with 3 meters of cable

Table 24: **Nexus - description of parts**

A	Terminal board
B	Antenna connector
C	P1 button
D	P2 button
E	SIM card housing (SIM non included)
F	Buzzer
G	Open-tamper microswitch
H	Communication LED (green)
I	Emergency LED (red)
L	Fault LED (red)
M	Connection LED (green)



The terminals for the BUS connection are as follows:

Table 25: **Nexus terminal board**

n.	icon/ identifier	description
1	**+**	Terminal "**+**" for the I-BUS connection
2	**D**	Terminal "**D**" for the I-BUS connection
3	**S**	Terminal "**S**" for the I-BUS connection
4	**-**	Terminal "**-**" for the I-BUS connection

Peripheral activity LED signals are as follows:

Table 26: **Nexus LEDs**

LED	Function	ON	OFF
Communication	Indicates communication with the control panel	The LED blinks during ongoing communications	Not communicating
Emergency	Indicates communication failure with the control panel	Blinks in the event of tamper or fault on the BUS	Normal communication with the control panel
Faults	Indicates the presence of faults	Blinks in the event of ongoing faults	No faults present
Connection	Indicates the status of the GSM network	• Slow blinking - Searching for the provider • Fast blinking - Provider found	Device Off

After activation of the Fault LED (indicating a fault is present), you can obtain further information regarding the cause of the fault by simply pressing button P2 [D]. The successive activation of the Emergency and Fault signaling LEDs will signal as follows:

Table 27: **Fault signaling**

LED On	Fault
Communication	No Credit
Emergency	SIM card with PIN request enabled
Faults	Communication problems with the GSM module

You can obtain an indication of the GSM reception level by simply pressing button P1 [C] and observing the number of LEDs which light amongst the Communication, Emergency and the Fault LEDs (viewing lasts 5 seconds):

- 1 LED - weak reception
- 2 LED - good reception
- 3 LED - excellent reception

SmartLAN ethernet interface 2-4

SmartLAN boards (SmartLAN/G and SmartLAN/SI versions) allow the expansion of connectivity of all Ness SmartLiving control panels to the LAN and the Internet.

The operating capacity of the SmartLAN board depends on the proper configuration of the networks it is connected to. Therefore, if you are installing a SmartLAN board, it is necessary to contact the network administrator in order to configure it correctly.

Both boards allow you to programme the control panel parameters via the LAN through the **SmartLeague** software programme.

The SmartLAN/G also allows users to:

- send event-report e-mails and attachments.
- interact, after user authentication, with the control panel through any browser (Explorer, Firefox, Opera, Safari, etc.), providing it has an integrated web-server:
  - •• view the status of zones
  - •• view the status of partitions
  - •• view the status of timers
  - •• view the events log
  - •• access one of the keypads operating within the system which will provide the user with an interface that is recognized by the control panel

Thus the user will be able to arm/disarm partitions, bypass/unbypass zones, activate/deactivate the alarm and tamper memories.

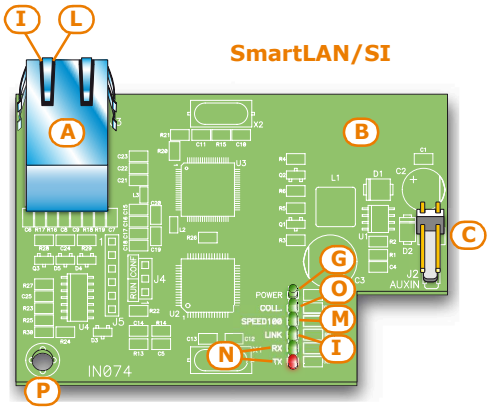
For a more detailed explanation of how to use the Web-server, refer to the User Manual of the control panel in use.

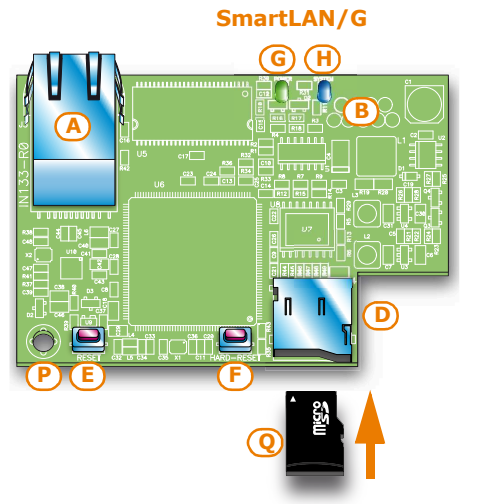
Table 28: **Device specifications**

Expansion board models	SmartLAN/SI	SmartLAN/G
Power supply voltage	12 V	
Maximum current draw	70 mA	90 mA
Operating temperature	-5 / +40 °C	
Dimensions	81 x 54 x 25 mm	
Maximum capacity of the µSD-card		32 Gb
Security protocol	8-bit proprietary encryption	128-bit AES
PCB code	IN074	IN133

Table 29: **SmartLAN - description of parts**

A	RJ45 LAN line jack
B	DB9 serial line jack (on the back)
C	Ancillary power connector (SmartLiving515 only)
D	µSD-card connector
E	RESET button
F	HARD RESET button
G	LED - Board power
H	LED - Control panel to SmartLAN connection
I	LED - Network connection
L	LED - Network activity
M	LED - Connection speed at 100Mbps
N	LED - transmission/reception over BUS RS232
O	LED - Network collision
P	Fixing hole and earthing
Q	SD-card (not included)





AUXREL32 power distribution board

The AUXREL32 power distribution board (accessory item) can be used with SmartLiving 1050L and 10100L models. It provides two relays and allows the system to take full advantage of the current supplied by the switching power supply of the control panel.

Each relay, has a voltage-free contact identified by terminals C1-NO1-NC1 and C2-NO2-NC2. The relays are activated by the OC1 and OC2 outputs on the control panel. The activation of each relay is signaled by the on-board LED ([D] for relay 1 and [E] for relay 2).

The 3 pairs of terminals are available, each protected by a resettable fuse (GND/AUX1 – GND/AUX2 – GND/AUX3), and each capable providing 12V@1A.

Table 30: **Device specifications**

Power supply voltage	12 V
Maximum current	3 A
Operating temperature	-5°C / +40°C
Dimensions	42 x 78 x 20 mm

Table 31: **AUXREL32 - description of parts**

A	Terminal board
B	12V connector
C	OC1/OC2 connector
D	Relay LED 1
E	Relay LED 2
F	12V present LED
G	Screw locations
H	OC1/OC2 connection wire (included)
I	12V power wire (included)

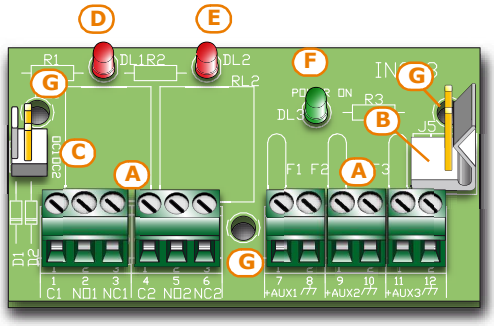
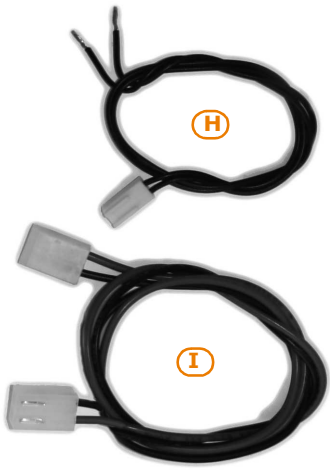


Table 32: **AUXREL32 terminal board**

n.	icon/identifier	description
1-2-3	**C1-NO1-NC1**	Free voltage relay 1
4-5-6	**C2-NO2-NC2**	Free voltage relay 2
7-9-11	**AUX1-AUX2-AUX3**	12V@1A screw terminals
8-10-12	⏚	Negative power terminals (Negative or GND)



Chapter 3

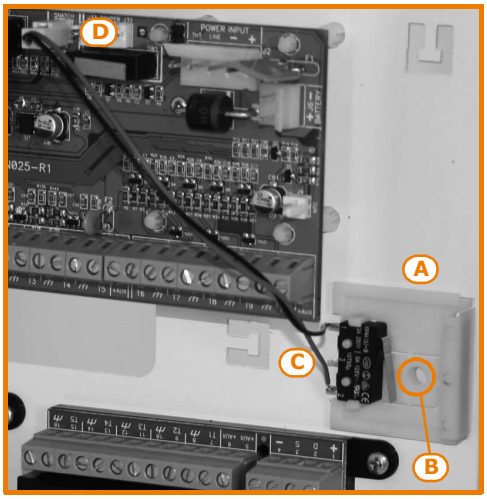
INSTALLATION

Installing the control panel 3-1

Wall-mounting 3-1-1

The control panel should be located in a secure location that can be accessed by authorized building occupants only.

1. Using the backbox (*Table 4: Control panels - description of parts, G*), mark the anchor screw locations on the wall. Be sure not to drill in the vicinity of electrical wiring or plumbing/gas pipes, etc.
2. Insert the screw anchors (recommended size 6mm).
3. Pull the wires through the wire entry.
4. Using the screws, attach the backbox to the wall.
5. Fit the dislodgement-tamper microswitch (provided with SmartLiving 10100L, optional for SmartLiving 505, 515 and 1050, refer to *Appendix H, Order codes, TamperNO*).
   5.1. Insert the dislodgement-tamper bracket [A] into its location on the backbox of the control panel (*Table 4: Control panels - description of parts, H*).
   5.2. Using screw location [B], screw the bracket to the wall.
   5.3. Connect the wire coming from the dislodgement-tamper microswitch [C] to the connector [D] on the board (*Table 4: Control panels - description of parts, T*).



Note

The cable gland must be flame class rating V-1 or higher.

Connecting the Mains power supply 3-1-2

The control panel must be powered through a separate line coming from the Mains box. The line must be protected by a safety-standards compliant circuit breaker (trip switch).

The circuit breaker (trip switch) must be located externally to the apparatus and should be easily accessible. The distance between contacts must be at least 3mm. The manufacturer strongly advises the use of a magnetothermic switch with C intervention curve and nominal (maximum) current - 16A.

The protective earthing system must be compliant with all safety standards and laws in force.

DANGER!

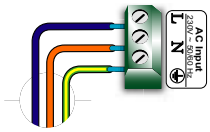
Ensure that the Mains is switched Off during the mains connection phase. Danger of electric shock.

The 505 and 515 models

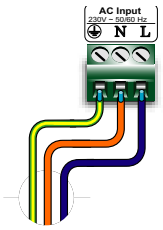
The 505 and 515 models are powered by an external AC power pack.

The 1050 and 10100L models

Pull the cable through the cable entry [E], then connect the mains power to the power-supply terminal board [D], located on the backplate above the motherboard. When connecting the earth wire, follow the indications on the power-supply label [F]. The power-supply provides power to the system and supplies the charge voltage.



SmartLiving 1050



SmartLiving10100L

Maximum current - normative references 3-1-3

Compliance with EN50131, CEI 79 or CEB T014 requires full observation of the rules (relating to the applicable normative and the model of the control panel concerned) presented in the Table below.

The system must be arranged in such a way that the current draw under normal circumstances does not exceed the maximum current allowed and the power source for the battery charge is always available.

Table 33: **Maximum current permitted**

Norm		SmartLiving intrusion control panels			
		505	515	1050	10100L
EN50131-3	Maximum current permitted	1.2A	1.2A	2.6A	3.5A
	Current reserved for the battery charge	1A	1A	2A	2A
CEI 79-2	Maximum current permitted	1.2A	1.2A	2.6A	3.5A
	Current reserved for the battery charge	1A	1A	2A	2A
CEB T014	Maximum current permitted	1.2A	1.2A	2.3A	2.7A
	Current reserved for the battery charge	1A	1A	2A	2A

Connecting the backup battery 3-1-4

The backup battery [A] connection must be completed during the phase described in *Chapter 4 - First power up*.

The SmartLiving 505, 515 and 1050 control panels house one lead battery @12V 7Ah.

The SmartLiving 10100L house two lead batteries, one @12V 17Ah (Max) and the other @12V 1.2Ah.

Note

The battery casing must have HB flame rating or higher.

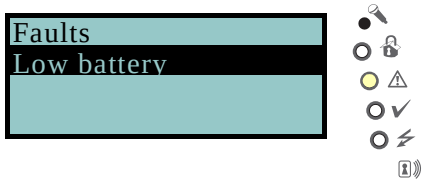
Using the battery wire [B] (included), connect the battery directly to the control panel motherboard.

ATTENTION!

Ensure that battery polarity is correct:
- black wire = negative
- red wire = positive

The backup battery is the secondary power source which powers the system during mains failure (230Vac, 50Hz).

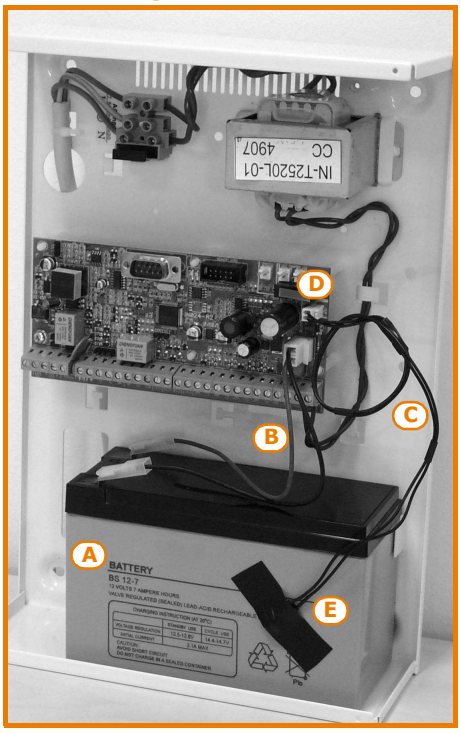
Once powered up, the panel will charge and monitor the battery automatically. The panel tests the efficiency of the battery by simulating load current demand at regular 4 minute intervals. If the control panel detects a voltage inferior to 10.4V (battery inefficient), it will generate a Low battery event that will not clear until the voltage goes back to over 11.4V.



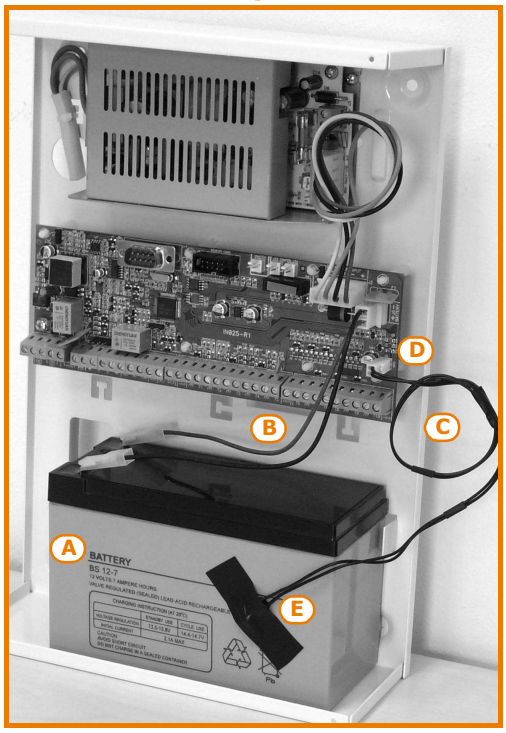
This fault will be signalled on the yellow LED on the keypads. To view the fault event, work through the following steps:

Access User menu, then View (OK), Faults Ongoing (OK).

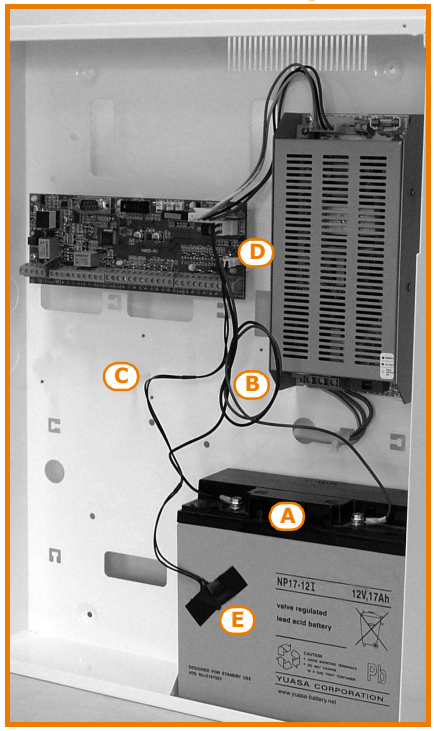
SmartLiving 505/515



SmartLiving 1050



SmartLiving10100L

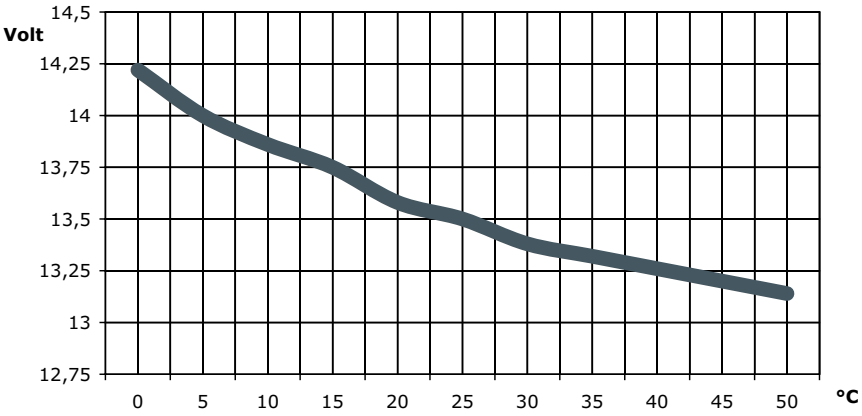


Thermal probe 3-1-5

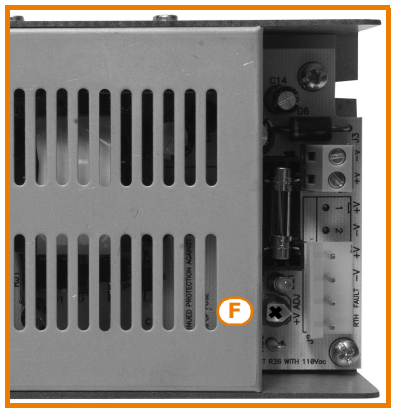
The battery charge process can be optimized by means of a thermal probe [C] (accessory item). This device regulates the charging process in accordance with the battery temperature. The thermal probe protects against battery overheating and consequent permanent damage to the battery.

To connect a thermal probe, work through the following steps.

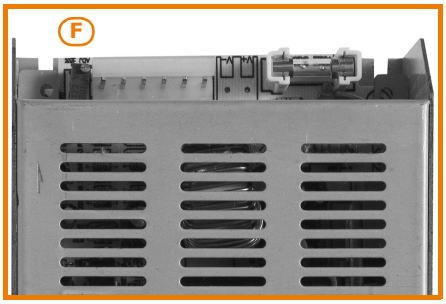
1. Disconnect the battery (if necessary).
2. Connect the thermal probe to the connector on the board [D]. If you are installing a model which is equipped with a switching power supply (SmartLiving 1050, and 10100L), you can connect the thermal probe directly to the power supply connector.
3. If you are installing a SmartLiving505 or 515 model, remove the jumper on the motherboard to enable the thermal probe (refer to *Table 4: Control panels - description of parts, N*).
4. Using adhesive-insulating tape, attach the thermal probe to the battery [E], in such way as to provide optimized heat-transfer measurements.
5. Hold a thermometer against the probe, and measure the probe temperature.
6. Using the following graph, find the value the measurement will be based on.



3A switching power supply



5A switching power supply



7. Using a tester, measure the voltage on the +AUX terminals and adjust the trimmer [F] to the previously measured value.

Opening and closing the control panel 3-1-6

If you wish to remove the metal front plate, work carefully through the following steps.

1. Type-in the installer code on the keypad and press OK. Access to the installer menu inhibits the activation of the output and any report calls associated with the "Open-panel" event.
2. Remove the four screws and the metal-frontplate.
3. Insert the Maintenance jumper (refer to *paragraph 3-1-10 Maintenance status*) and carry out the necessary work.

Once your task is complete, work carefully through the following steps.
Remove the Maintenance jumper., Using the 4 screws, secure the frontplate to the backbox. Exit the Installer menu.

Note

If you exit the Installer menu before replacing the panel frontplate, the system panel will not generate an open-panel event.
However, the system will generate an open-panel event, if the frontplate is not replaced within 15 seconds of closing the open-tamper switch.

Land-line connection (PSTN) 3-1-7

Terminals 4 and 5 on the control panel motherboard (*Table 5: Control panel - terminal board, 4-5*) are for the land-line telephone connection.

In order to protect the control panel against the discharge of atmospheric electricity, (lightning), the manufacture strongly advices the use of the two Gas Arrestors. These Arrestors must be connected to the earth line 1 and terminals 4 and 5 of the landline (PSTN).

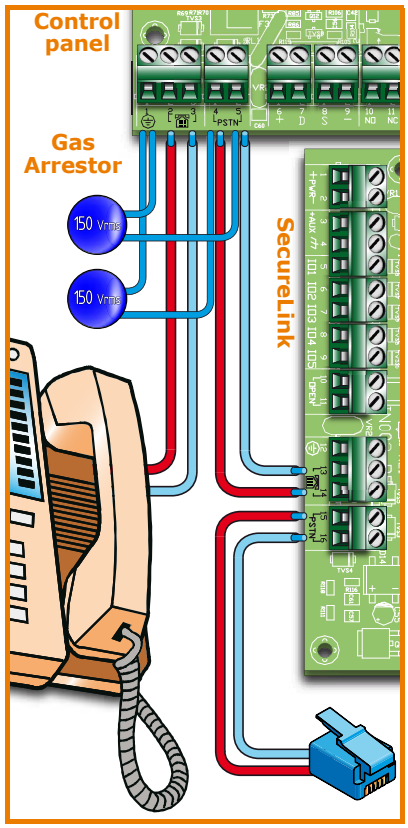
If you are installing the system in a place where the land line (PSTN) service is not available, or if you wish to increase the level of security of the system, these terminals also accept a GSM interface (such as Ness's SecureLink) which simulates the analogue land-line.

Ness provide two versions of the SecureLink GSM interface: SecureLink-G and SecureLink-GP. Both these devices simulate the analogue land line during line-down conditions (line trouble or wire-cutting) and allow the control panel to switch incoming/ outgoing calls to the GSM network.

You can also use the terminals on the SecureLink board to extend the functions provided by the SmartLiving system. The following section describes several methods which will allow you to provide users with advanced functions.

- Arming/Disarming the system over-the-phone using a cost-free call or SMS text
  By connecting one of the "follow zone" configured SmartLiving board terminals to an output on the SecureLink board, it will be possible to arm or disarm the SmartLiving system via SMS.
  In a similar way, using a "switching zone" configured terminal, it will be possible to arm or disarm the SmartLiving system simply by means of a recognized incoming call.
- Alarm warning to users via SMS text
  By connecting one of the alarm outputs of the SmartLiving control panel to an input on the SecureLink board, it will be possible to receive alarm warning via SMS text. The system can be set up to send an editable SMS text to 10 different contact numbers.

All the functions of the SmartLiving system which use the land line (voice dialer, answerphone, report communications and teleservice) can be managed completely over the GSM network by the SecureLink. The SecureLink also allows teleservice maintenance over the GSM network.



Note

If there are ADSL filters on the line, you must connect the control panel downstream of the filters, to the line dedicated to telephone equipment (this line is clearly indicated on the filters). It is recommended all Alarms System be used only where ADSL filters are fitted.

If a SecureLink is not used, connect the incoming PSTN line directly to terminals 4 & 5 of the SmartLiving main board.

Enabling / Disable Phone Line Monitoring

Phone Line Monitoring

Type-in Code (Installer PIN - Default 9999) OK, PROGRAMMING Panel options OK.

Press ▣ * to enable the "Line Down Signal" option, or □ # to disable it.

Press OK to exit and save.

Note: Installation and maintenance to the phone line shall be performed by qualified licensed installers only.

Connecting to a PC 3-1-8

Programming from a PC requires the SmartLeague software programme (refer to *paragraph 6-3 Programming via the SmartLeague programme*) and an RS232 serial cable.

Insert the RS232 serial link (accessory item) into the connector [A], as shown in the figure opposite.

If you wish to purchase an RS232 serial link, refer to the codes in *Appendix H, Order codes*. If your PC is not equipped with an RS232 port, but has a USB instead, you can use Ness's Approved RS232-USB adaptor (accessory item - Ness Part No 101-231).

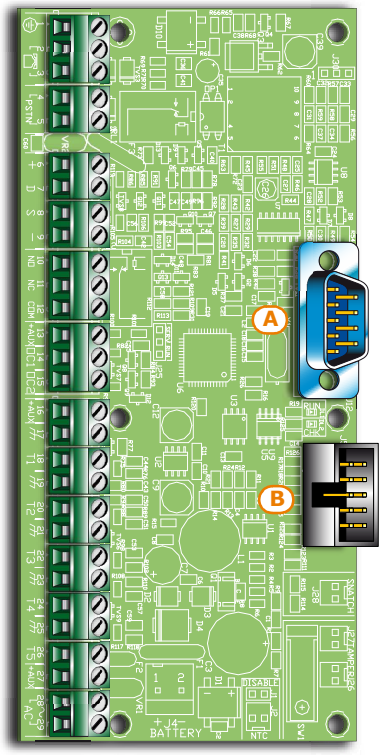
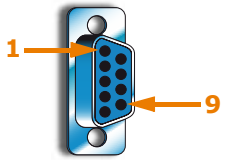
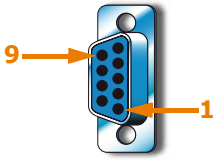
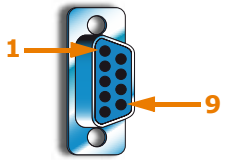
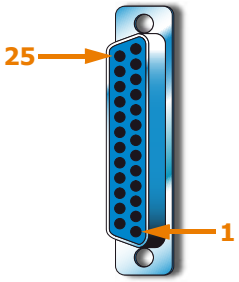


Table 34: **RS232 connector cable**

SmartLiving end DB9F connector		PC end DB9F connector	
	2	3	
	3	2	
	4	4	
	5	5	
	6	6	
	7	7	
	8	8	

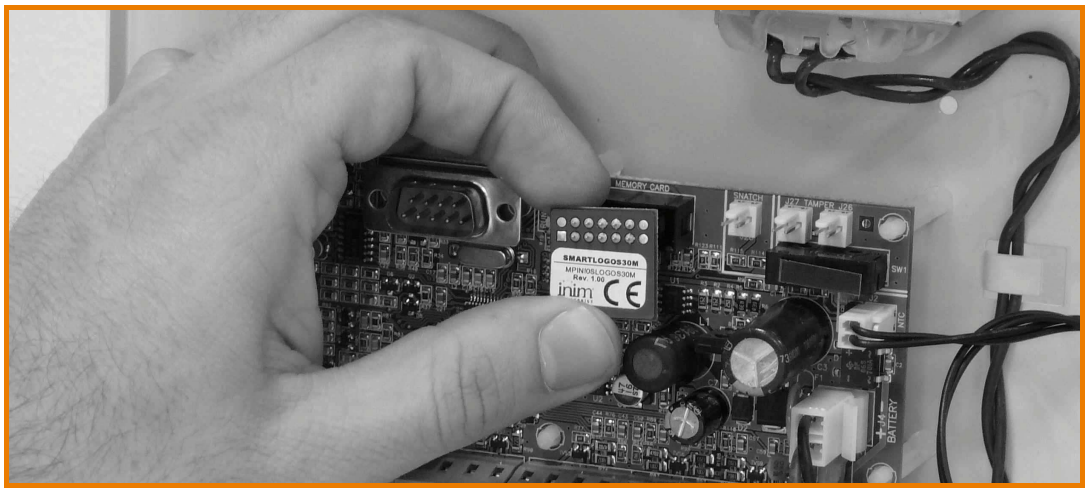
SmartLiving end DB9F connector		PC end DB25F connector	
	2	2	
	3	3	
	4	20	
	5	7	
	6	6	
	7	4	
	8	5	

Connecting the SmartLogos30M voice board (accessory item) 3-1-9

The SmartLogos30M voice board provides the SmartLiving system with an array of useful voice functions.

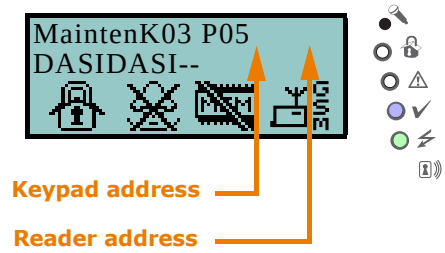
For proper installation of the board, work carefully through the following steps.

1. Disconnect all power sources to the control panel (mains and lead batteries).
2. Connect the board to the respective connector [B].
3. Power up the system from the mains and reconnect the lead batteries.



Maintenance status 3-1-10

The maintenance status is signaled on the keypads by the "Maintenance" message and the address of the keypad. The address of the built-in reader (if enabled) of Alien keypads will also be shown.

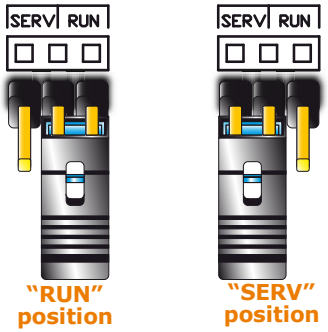


During service/maintenance mode, the control panel:

- Forces the relay output on the motherboard (*Table 5: Control panel - terminal board, 10-11-12*) to standby status.
- Does not activate the outputs (and will force to standby any active outputs) triggered by:
  - •• alarm or zone/partition tamper
  - •• peripheral tamper
  - •• open/dislodged panel tamper
- It allows initialization of the keypad address programming phase.
- It allows initialization of the reader address programming phase.
- It initializes automatically the auto-enrollment of the peripherals connected to the BUS at 10 seconds intervals. It allows assignment of the addresses to the peripherals connected to the BUS and, at 10 second intervals, enrolls the peripherals it finds.
- The control panel will not reset the BUS in an attempt to retrieve peripherals in the event of peripheral loss.
- It will continue to operate as normal, except under the aforesaid circumstances.

During service/maintenance mode, the Alien keypad:

- Does not require user-code entry to access the sections which correspond to the "Settings" key.
- The first parameters shown in the "Settings - Alien" section are the addresses of the Alien keypad and its built-in proximity reader and, only for the Alien/S, the status of tamper enablement on the keypad.
- It is not possible to access the "Clima" section.
- The display shows the address of the Alien keypad and its built-in proximity reader in the top left-hand corner of the home page.
- The display shows the letters relating to the operating status of the partitions in the bottom left-hand corner of the home page.



USING THE MAINTENANCE JUMPER

The control panel can be placed in maintenance mode by:

- Inserting the Maintenance jumper in the "SERV" position.
- Enabling the "Maintenance" option in the 'SmartLeague' Software.

The Maintenance jumper (*Table 4: Control panels - description of parts, Q*) can be inserted in two different positions:

- "RUN" (control panel operating normally)
- "SERV" (control panel ready for maintenance work)

THE "MAINTENANCE" OPTION

The control panel enters "Maintenance" mode when this option is enabled and exits "Maintenance" mode when it is disabled. You can enable/disable this option at the keypad or via computer.

Via Keypad

1. Access the "Programming Panel options" section.

Type-in Code (Installer PIN) OK, PROGRAMMING Panel options OK.

2. Press ▣ * to enable the "Maintenance" option, or □ # to disable it.
3. Press OK to exit and save.

Via PC

Select "SmartLiving System" from the tree menu on the left, then go to the "Programming" template on the right: The "Control panel parameters" section provides the "Maintenance" option, click-on this option to enable/disable it.

Connecting peripherals 3-2

The I-BUS line wiring 3-2-1

The SmartLiving peripherals (keypads, readers, expansions, sounderflashers, transceivers, isolators and GSM communicator) must be connected to the control panel via the I-BUS.

The connection between the control panel and its peripherals is achieved through a 4 wire (or more) cable.

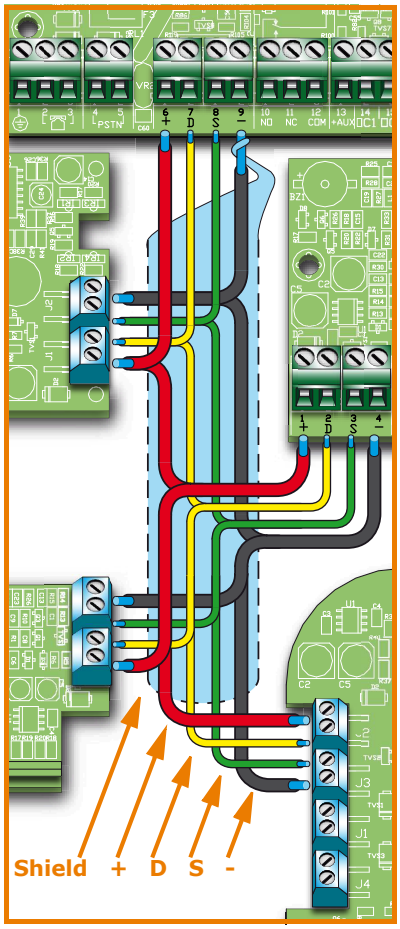
ATTENTION!

If Shielded cable is used, the shield must be connected to one of the ⏚ terminals (Negative or GND) at the control panel end only, and must run along the BUS without being connected to negative or GND at any other point.

The cable specifications depend on the length of the BUS (from the panel terminals to the most distant point), Baud rate and the load current draw.

Table 35: **Recommended cable**

Cable AF CEI 20-22 II	n. wires	Section (mm^2)	I-BUS terminal
4 wire cable + shield	2	0.5	+ -
	2	0.22	D S
6 wire cable + shield	2	0.5	+ -
	2	0.22	D S
	2	0.22	available
6 wire cable + shield	2	0.75	+ -
	2	0.22	D S
	2	0.22	available



The maximum wire length of the I-BUS depends on the deployment of the peripherals connected to the line and their specific current draw (in particular the keypads and expansion boards). The power to peripherals and detectors can be supplied by external power stations or by the line itself.

Furthermore, the speed of the communication BUS (Baud rate) can be modified by means of the SmartLeague programming software. If the BUS is not used to power the peripherals and their loads, the maximum wire length is 300 meters @ 250kbs, regardless of the number of peripherals involved.

An intermediate speed (125kbs) can support a single section of 700 meters.

If you wish to increase the length and performance of the BUS, you can connect IB100 isolators.

If the speed of the communication BUS (Baud rate) is low (38.4 or 125 kbps), you can apply a maximum of 5 isolators in a cascade connection.

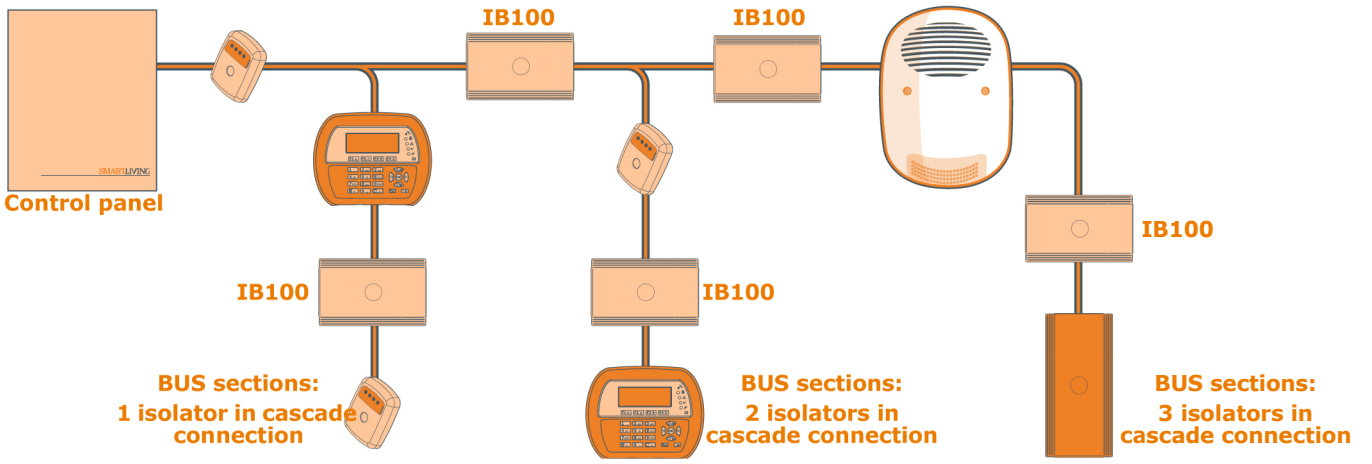
If the speed of the communication BUS (Baud rate) is high (250 or 2 kbps), you can apply a maximum of 2 isolators in a cascade connection.

You can connect up to 15 isolators in all.

ATTENTION!

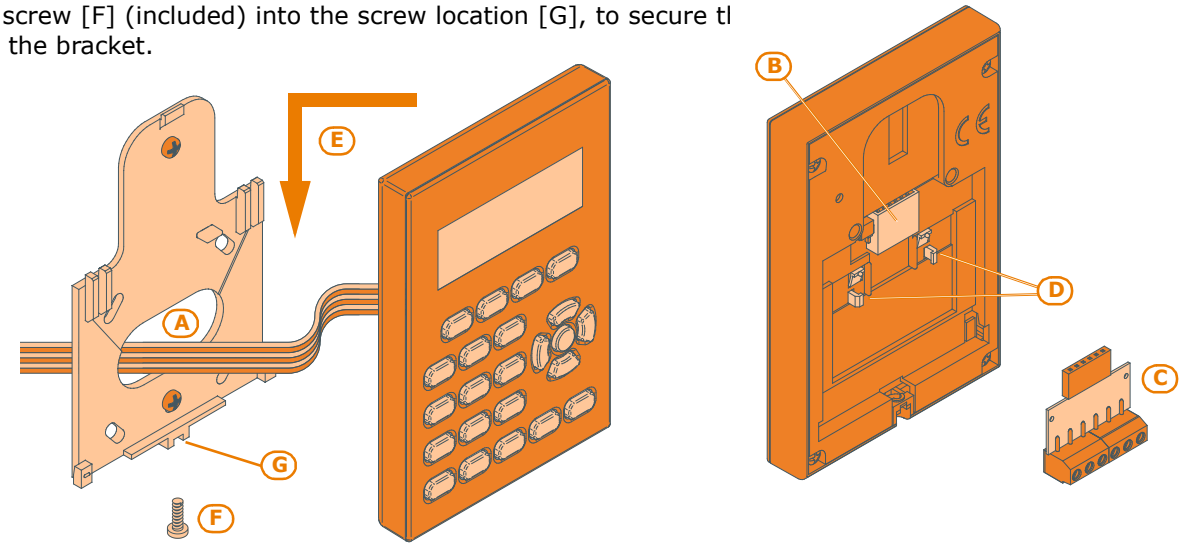
It is extremely important to evaluate correctly the number of isolators connected in cascade to the BUS.

The following example will help you achieve a correct evaluation



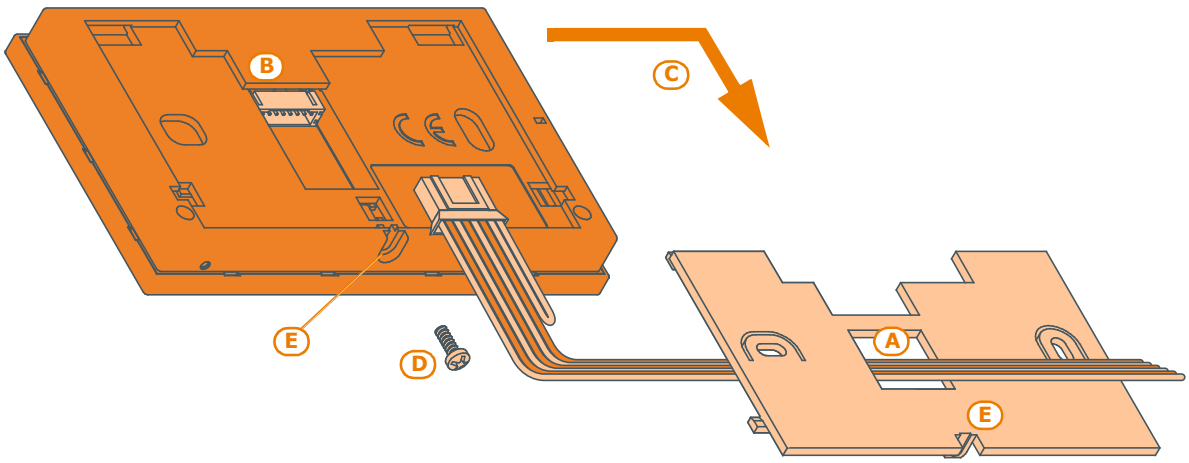
Installing nCode/G and cCode/G keypads 3-2-2

1. Connecting the device to the system
2. Pull the connection wires through the wire entry [A].
3. Connect the cables to the connector on the keypad backplate [B]. If you are using the connector provided with the KB100 kit [C], connect the wires to the terminals, in accordance with the instructions described in *paragraph 2-3-2 nCode/G and cCode/G Keypads*, then insert the connector into the guide [D] until it locks into place.
4. Using at least 2 screws, mount the bracket to the wall.
5. Using the back-locking grips, attach the keypad to the bracket (as shown in figure [E]).
6. Fasten the screw [F] (included) into the screw location [G], to secure tl properly to the bracket.



Installing Alien/S keypads 3-2-3

1. Connecting the device to the system
2. Pull the connection wires through the wire entry [A].
3. Connect the cables to the connector on the keypad backplate [B].
4. Using the respective anchor holes, mount the bracket to the wall or 503 box.
5. Using the back-locking grips, attach the keypad to the bracket (as shown in figure [C]).
6. Fasten the screw [D] (included) into the screw location [E], to secure the keypad properly to the bracket.



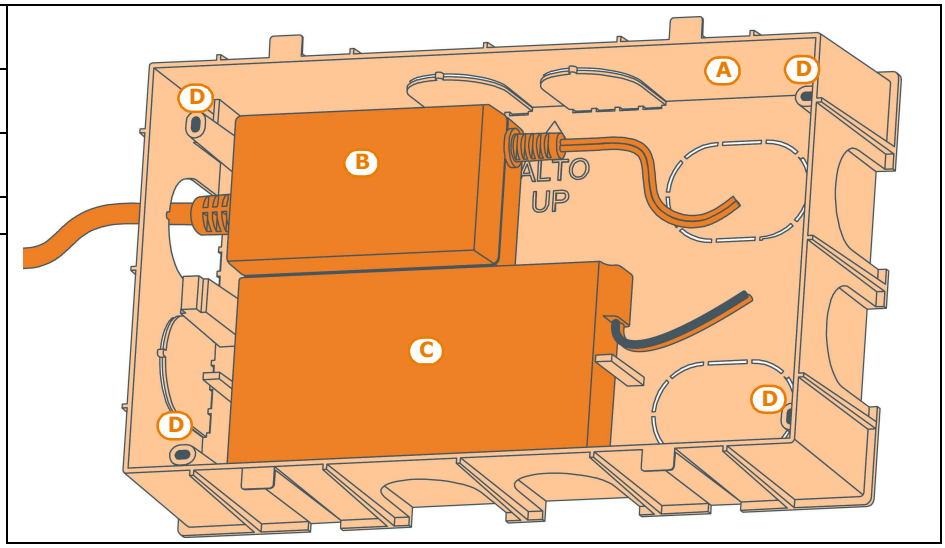
Installing the Alien/G keypad 3-2-4

1. Prepare the placement area on order to flush-mount the device, taking care not to damage any electrical wiring, gas or water papers, etc.
2. Insert the flush-mount box (*Table 36: Alien/G - mounting possibilities, A*) into the placement area and secure it in place.
3. Pull the wires through the most suitable wire entry.

4. Place the backup battery and Alien/G power supply in the most suitable position inside the box.
5. Connect to the mains network.
6. Open the Alien/G casing by first removing the safety screw and then pushing the enclosure clasp open.
7. Pass the wires through the wire entry on the back of the Alien/G.
8. Fit the screws into the screw locations (*Table 36: Alien/G - mounting possibilities, D*) and attach the Alien/G securely to the flush-mount box.
   After securely mounting the Alien/G, make sure that the microswitch is closed.
9. Complete all the connections.
10. Close the Alien/G.

Table 36: **Alien/G - mounting possibilities**

A	Flush-mount box (included)
B	Switching power supply (optional)
C	Backup battery (optional)
D	Screw locations



Alien/G power supply 3-2-5

The Alien/G can be powered via three different sources, which can be used, therefore connected, individually or simultaneously.

MAINS POWER SUPPLY 230VAC 50HZ

The mains supply requires the use of a power supply (*Table 36: Alien/G - mounting possibilities, B*) and a separate line from the mains box. The line must be protected by a safety-standards compliant circuit breaker (trip switch).

The protective earthing system must be compliant with all safety standards and laws in force.

Connect the power supply (already connected to the mains) to terminals "**+ 14 -**" on the PCB, taking care to respect the correct polarity of the wires. The power supply will provide power to the Alien/G and the devices connected terminal to "**+**" of the BUS and also recharge the backup battery.

I-BUS

The I-BUS line for the direct connection to a SmartLiving control panel supplies 12V current through the I-BUS connection terminals "**+**" and "**-**" on the PCB. This current provides power to the Alien/G and the devices connected terminal to "**+**" of the BUS and also recharges the backup battery.

BACKUP BATTERY

The backup battery connection (*Table 36: Alien/G - mounting possibilities, C*) must be achieved through the connecter on the PCB and the specific wire (included) which has a faston terminal at each end.

ATTENTION!

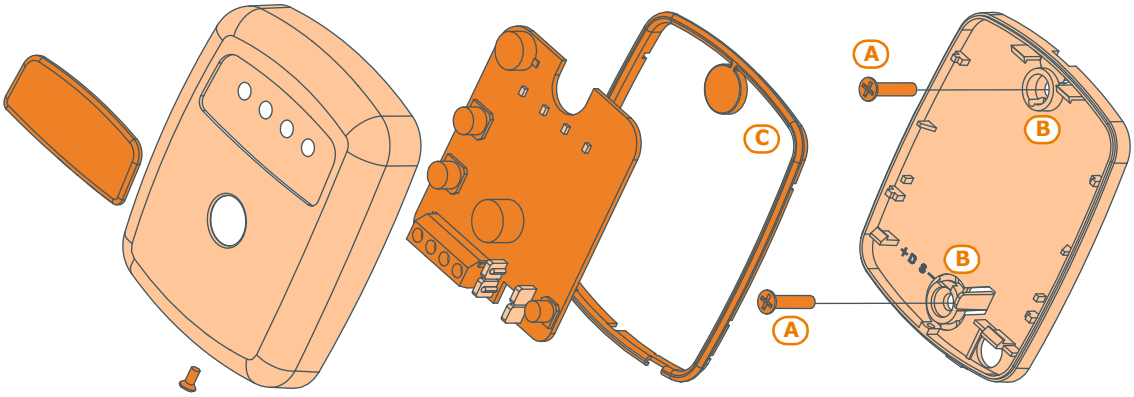
Ensure that battery polarity is correct:
- black wire = negative
- red wire = positive

The lead battery is a secondary power source that provides power to the Alien/G and the devices connected to the BUS, whether it is equipped with a power supply or I-BUS or both.

Installing nBy/S readers 3-2-6

The wall-mount nBy/S reader is suitable for indoor and outdoor installation.

Insert the two anchor screws [A] (included) into the two screw locations [B] on the plastic backplate.



In order to avoid the risk of piercing the silicone seal [C], and thus jeopardizing the waterproofing of the enclosure, insert the screws before fitting the seal.

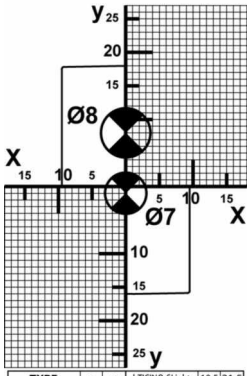
ATTENTION!

Installing nBy/X readers 3-2-7

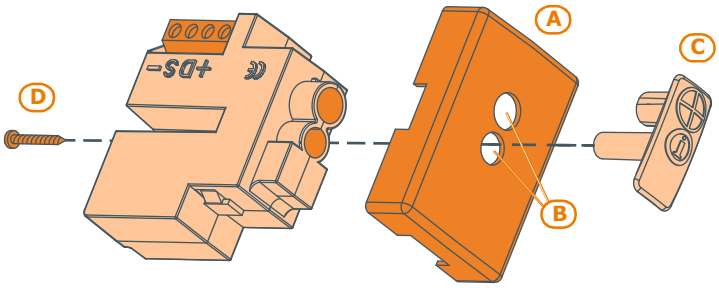
The Universal flush-mount nBy/X (**Patent Pending**) has been especially designed to integrate with all brands of cover plates [A]. Drill two holes [B] for the light guide [C].

Use the adhesive drill-pattern (see opposite) to mark the drilling locations accurately.

1. Ensure that the centre of the cover plate coincides with the crossing of the axes x and y on the drill-pattern. In this way, the two drilling locations (1 x 7mm diameter and 1 x 8mm diameter) will be positioned precisely.
2. Using the screw [D], secure the reader components inside the cover plate.
3. Insert the cover plate (with the reader already assembled) into the light switch box.



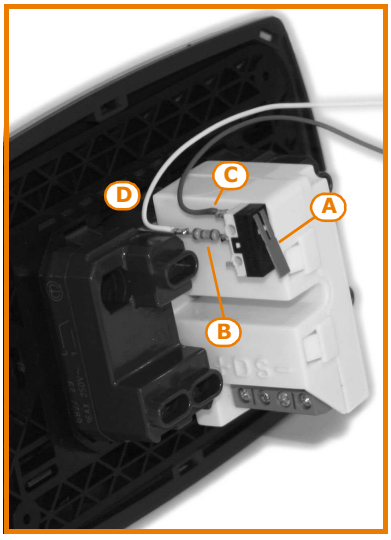
TYPE	x	y	bTICINO-SLight	10.5	21.5
AVE-Sistema45	12.5	22.5	GEWISS-Chorus	11	22
bTICINO-AM500	11.5	21.5	GEWISS-GW20056	11.5	22
bTICINO-Axolute	21	22.5	legrand	10.8	22.2
bTICINO-Magic	8	16	VIMAR-Eikon	11	22
bTICINO-Living	12	19.5	VIMAR-Idea	12	18
bTICINO-SLiving	10.5	21.5	VIMAR-Plana	11	22



The nBy/X reader is not equipped with built-in dislodgement-tamper protection. However, the following section describes how you can protect nBy/X reader against this kind of tamper.

In order to comply with certification (Level 2 - IMQ Security Systems), all the system peripherals must be protected against tamper. Installation of a microswitch will allow the reader to signal tamper events. To obtain this type of protection, work carefully through the following steps.

1. Use a microswitch with at least two normally-open contacts [A]. The one shown in figure 3 has 3 contacts: COM-NO-NC.
2. Configure one of the terminals as follows: Input; 24H; Description = "Tamper reader x"; single balancing with 6K8W [resistance [B]; unlimited alarm cycles. Assign the duly programmed terminal to at least one keypad partition.
3. Using 2 wires, connect the microswitch to the 24H input terminal.
4. On the microswitch:
   4.1. using one of the two wires, connect the common contact (COM) to the GND terminal of the 24H terminal [C].



4.2. Connect the normally-open contact (NO) to one end of the 6k8W resistance [D] (the normally-open contact generates a short-circuit between itself and the COM contact when the microswitch-lever is compressed). Connect the other end of the resistance to the wire which is connected to the 24h input terminal.

5. Install the microswitch as shown in the previous figure, so that the switch lever is compressed. If an unauthorized attempt to dismantle the nBy/X reader occurs, the lever will expand in order to open the contact which triggers instant alarms on the 24H terminal.

Note

This wiring method can be applied in most situations, however, it is only a point of reference. In order to ensure proper protection, you must always take in to account the specific mechanical and electrical conditions of the device you are working on.

ATTENTION!

In order to avoid malfunction, it is advisable not to install nBy/X readers onto metal plates.

Installing the Nexus 3-2-8

In order to allow this device to function properly, you must install it in a safe, dry place which provides the best possible GSM reception.

ATTENTION!

Please ensure the SIM is not PIN enabled. Disable the SIM card PIN before using it in the Nexus Module.

1. Ensure that the Nexus is not powered-up.
2. Insert the SIM card into its housing (refer to *Table 24: Nexus - description of parts, E*).
3. Install the antenna and connect it to the respective input (refer to *Table 24: Nexus - description of parts, B*).
4. Connect the BUS to the terminal board (refer to *Table 24: Nexus - description of parts, A*).

Addressing the peripherals 3-3

In order to allow the control panel to identify the peripherals distinctly, you must assign a different address to each device. However, you can assign the same address to two devices which belong to different categories (e.g. a Flex5 expansion and a JOY keypad) as, in this case, the control panels will see them as two distinct devices.

Table 37: **Peripherals address**

Expansion boards and transceiver address	DIP-switch 12345678
1	00000000
2	00000001
3	00000010
4	00000011
5	00000100
6	00000101
7	00000110
8	00000111
9	00001000
10	00001001
11	00001010
12	00001011
13	00001100
14	00001101
15	00001110
16	00001111
17	00010000
18	00010001
19	00010010
20	00010011
21	00010100
22	00010101
23	00010110
24	00010111
25	00011000
26	00011001
27	00011010
28	00011011
29	00011100
30	00011101
31	00011110
32	00011111
33	00100000
34	00100001
35	00100010
36	00100011
37	00100100
38	00100101
39	00100110
40	00100111

SmartLiving 505 / SmartLiving 515 / SmartLiving 1050 and 1050L / SmartLiving 10100L

Readers address	Red	Blue	Green	Yel-low	nBy/S	nBy/X	Keypads address
1	0	0	0	1	○○○●	⊕	1
2	0	0	1	0	○○●○	⊕	
3	0	0	1	1	○○●●	⊕	2
4	0	1	0	0	○●○○	⊕	
5	0	1	0	1	○●○●	◒	3
6	0	1	1	0	○●●○	◒	
7	0	1	1	1	○●●●	◒	4
8	1	0	0	0	●○○○	⊕	
9	1	0	0	1	●○○●	◒	5
10	1	0	1	0	●○●○	◒	
11	1	0	1	1	●○●●	◒	6
12	1	1	0	0	●●○○	◒	
13	1	1	0	1	●●○●	◒	7
14	1	1	1	0	●●●○	◒	
15	1	1	1	1	●●●●	●	8
16	0	0	0	L	○○○▨	⊕	
17	0	0	L	0	○○▨○	⊕	9
18	0	0	L	L	○○▨▨	⊕	
19	0	L	0	0	○▨○○	⊕	10
20	0	L	0	L	○▨○▨	⊕	
21	0	L	L	0	○▨▨○	⊕	11
22	0	L	L	L	○▨▨▨	⊕	
23	L	0	0	0	▨○○○	⊕	12
24	L	0	0	L	▨○○▨	⊕	
25	L	0	L	0	▨○▨○	⊕	13
26	L	0	L	L	▨○▨▨	⊕	
27	L	L	0	0	▨▨○○	⊕	14
28	L	L	0	L	▨▨○▨	⊕	
29	L	L	L	0	▨▨▨○	⊕	15
30	L	L	L	L	▨▨▨▨	⊕	

0	○	LED Off
1	●	LED On
L	▨	Flashing LED

You must not exceed the maximum number of addresses allowed for each type of peripheral. The above table shows the available peripheral addresses and the maximum number of addresses accepted.

The top left section of the Table shows the maximum number of addresses (5 for the SmartLiving505 model, 10 for the515 model, 20 for the 1050 model and 40 for the 10100 model) and the DIP-switch configuration of the Flex5 expansion board and Air2-

BS100 transceiver (refer to *paragraph 3-3-4 Addressing FLEX5 expansions and the Air2-BS100 transceiver*).

The second section shows the nBy/S and nBy/X reader addresses with the corresponding combination of the reader LEDs (refer to *paragraph 3-3-5 Addressing nBy readers*).

The section on the far right shows the addresses available for the keypads (refer to *paragraph 3-3-2 Addressing the keypads*).

For the Ivy sounderflasher and IB100 isolator addressing procedure, refer to the respective Installation Guides.

It is possible to connect only one Nexus device to the SmartLiving control panels, therefore, there no addressing procedure is required.

Fast addressing of keypads and readers 3-3-1

If, within 4 seconds of inserting the maintenance jumper (*Table 4: Control panels - description of parts, Q*), you press the open-tamper microswitch on the control panel cover (*Table 4: Control panels - description of parts, V*), the SmartLiving system will activate the fast addressing function for the keypads and readers.

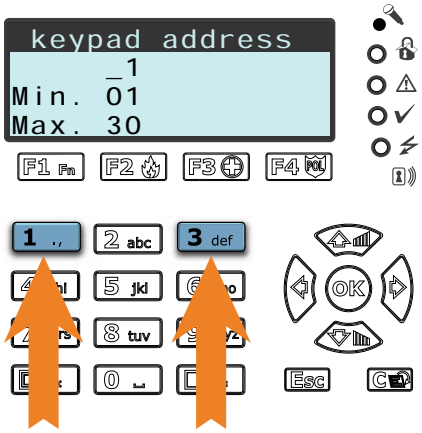
All the keypads and readers connected to the I-BUS will be placed in address programming status and assigned their addresses in sequential order.

At the point, you (the installer) can either change or confirm the assigned addresses

Addressing the keypads 3-3-2

To assign addresses to keypads, follow the procedure described in *paragraph 3-3-1 Fast addressing of keypads and readers* or work through the following steps:

1. Put the control panel in "Maintenance" mode by inserting the respective jumper (*Table 4: Control panels - description of parts, Q*).
2. On the keypad you wish to assign an address to, press **and release keys** 1 ., and 3 def simultaneously; set the address then press OK (if the keypad firmware version is 1.02 or higher, go to point 5).
3. You may also enable or disable the Keypad tamper protection by pressing 1 ., or 2 abc.
4.



For security reasons, if the address is not assigned within 30 minutes of accessing "Maintenance" mode (SERV jumper inserted), the keypad will exit the programming phase automatically.

Addressing the Alien keypad 3-3-3

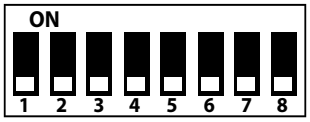
Work carefully through the following steps.

1. Put the control panel in "Maintenance" mode (*paragraph 3-1-10 Maintenance status*).
2. From the Alien keypad, access the "Settings" section by pressing the , and then access the "Alien" section. This section provides a list of the keypad parameters.
3. Set the parameters:
   - PROXY ADDRESS - Alien keypad address
   - PROXY ADDRESS - built-in reader address
   - ALIEN TAMPER - keypad tamper enablement
4. This parameter can be changed by means of keys **+** and **-**.
5. Press **SAVE** to set the addresses and exit.

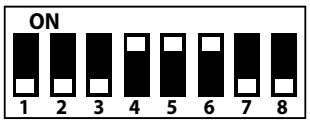
Addressing FLEX5 expansions and the Air2-BS100 transceiver 3-3-4

Using a small screwdriver or similar tool, set the expansion board address on the 8-segment DIP-Switch strip (*Table 21: Flex5 - description of parts, C*). Each segment can be set at "1" (On) or "0" (Off).

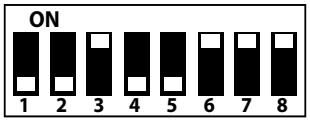
The figure shows some examples.



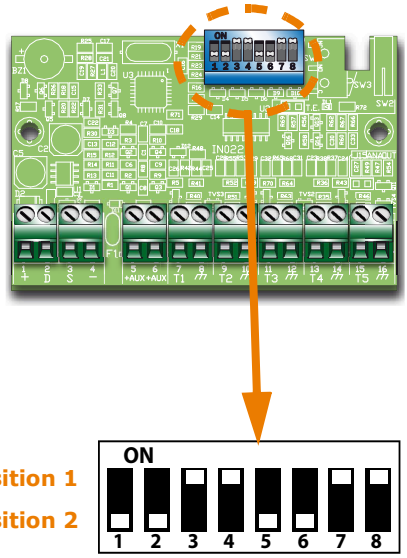
Expansion n. 1



Expansion n.29



Expansion n.40



Addressing nBy readers 3-3-5

To assign addresses to the system readers, follow the instructions described in *paragraph 3-3-5 Addressing nBy readers* or work carefully through the following steps:

1. Put the control panel in "Maintenance" mode (*paragraph 3-1-10 Maintenance status*).
2. Start the "Address Programming" phase using the software or from a keypad:

Type-in Code (Installer PIN) (OK), PROGRAMMING Readers (OK), Prog. address (OK).

or
via the software select "Proximity readers", go to the "Programming" section and then click on "Proximity Reader address configuration".

3. Each reader indicates its own address on its LEDs (refer to the Table in *paragraph 3-3 Addressing the peripherals*).
4. Hold a valid key in the vicinity of the reader. The reader will run through a series of available reader-addresses (an address every 2 seconds). Remove the key when the LEDs indicate the desired address.
5. The reader will hold the addressing phase for a further 10 seconds, in order to allow you to change the address if necessary.
6. The reader will assign the selected address when the 10 second period expires.
7. If you wish to assign an address to another reader, hold a valid key in the vicinity of the reader and work through points 4 to 6.
8. End the reader-address programming phase (exit "Prog. Address" menu via keypad or, if you are using the SmartLeague software, by clicking on "Stop reader address setup".

This procedure does not apply to readers that are built into the keypads.

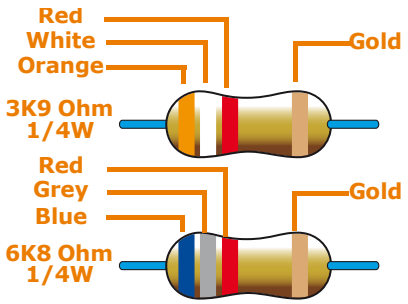
Auto-enrolling peripherals 3-4

The peripherals connected to the BUS are enrolled automatically in the following situations:

- on first startup (refer to *Chapter 4 - First power up*)
- in "Maintenance" mode (refer to *paragraph 3-1-10 Maintenance status*)
- from the Installer menu (refer to *paragraph 6-25 Default settings*)

Type in Code (Installer) (OK), PROGRAMMING Default settings (OK), Auto enroll Periph (OK).

Wiring and balancing alarm detectors 3-5



The wiring and respective balancing method depends on the type of detector you are installing, and the level of protection you wish to achieve. The detectors can be powered through:

- terminals [+AUX/12V] and [-/GND] on the control panel
- terminals [+AUX/12V] and [-/GND] on FLEX5 expansions
- terminal [+/12V] and terminals [-/GND] on keypads
- from any 12V ancillary source on condition that its GND reference is in common with that of the control panel.

The resistors used for balancing are:

- 3K9 Ohm 1/4W
- 6K8 Ohm 1/4W

The following Table indicates the protection level of each detector type and the balancing options provided by the control panel:

Table 38: **Protection level**

BALANCING	N.O.	N.C.	Single	Double	Double zone	Double zone with EOL
Infrared or Double technology	very low	low	medium (*)	high	medium	high
Magnetic contact	very low	low	medium		medium	high

(*) Single balancing provides the same level of protection as Double balancing, when the tamper contact of the detector is connected to a balanced zone on the control panel.

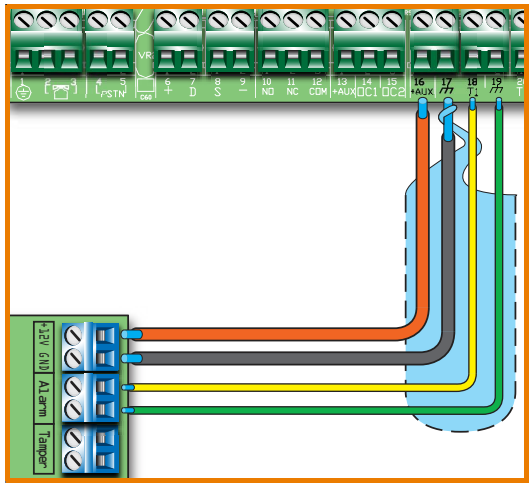
N.C./N.O. Balancing 3-5-1

For N.C. (normally closed) and N.O. balancing (normally open), it is possible to detect two distinct zone conditions:

- standby
- alarm

For each of these, the control panel reads different resistance values on the terminal, expressed below in Ohm.

Ohm	Zone	N.O.
> 2 x 3900 + 6800	alarm	standby
> 2 x 3900 + 6800	alarm	standby
3900 + 6800	alarm	alarm
2 x 3900	alarm	alarm
3900	standby	alarm
0	standby	alarm



If you wish the detector to monitor tamper events, connect the detector "Tamper" terminal to a "24h" zone on the control panel.

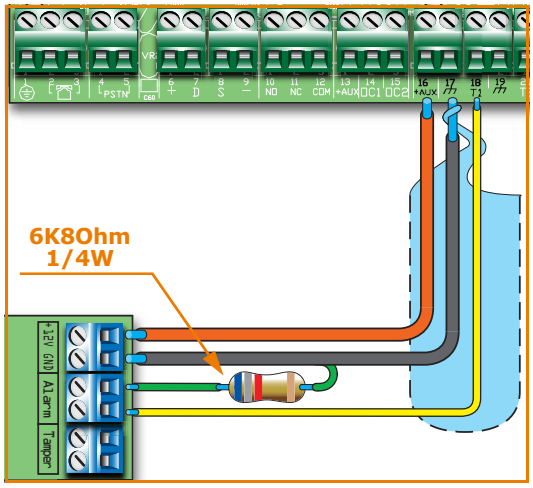
Single (EOL) balancing 3-5-2

Single zones can discriminate 3 conditions on the entire terminal:

- standby
- alarm
- tamper (short-circuit)

For each of these, the control panel reads different resistance values on the terminal, expressed below in Ohm.

Ohm	Zone
> 6800	alarm
6800	standby
0	tamper



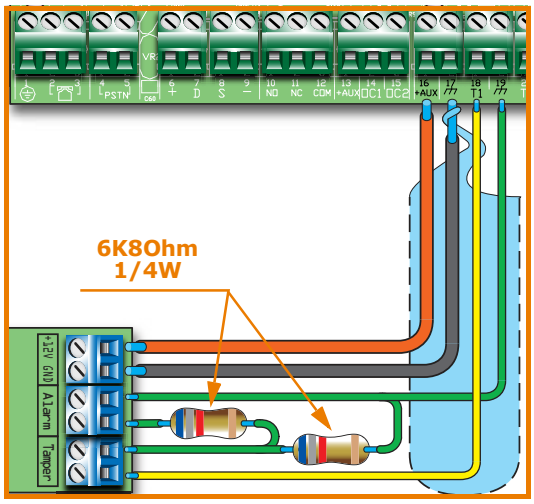
If you wish the detector to monitor tamper events, connect the detector "Tamper" terminal to a "24h" zone on the control panel.

Double (Dual EOL) balancing 3-5-3

Double balancing (also known as 4 State Monitoring) discriminates 4 distinct conditions on the zone terminal:

- standby
- alarm
- tamper (short-circuit)
- tamper (wire cutting)

For each of these, the control panel reads different resistance values on the terminal, expressed below in Ohm.



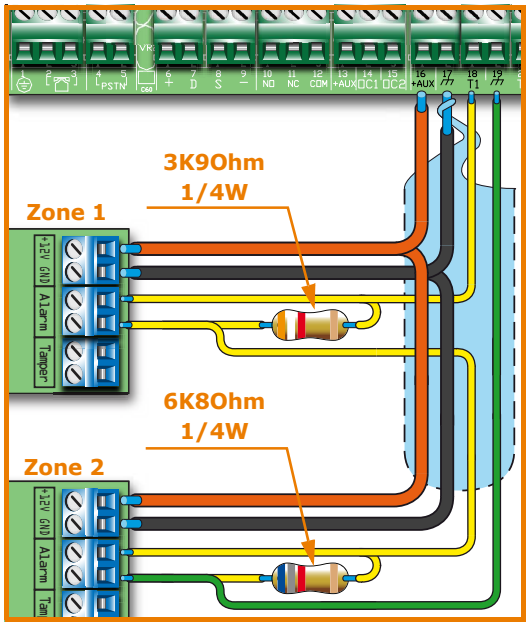
Ohm	Zone
> 6800	tamper (wire cutting)
6800	alarm
6800 / 2	standby
0	tamper (short-circuit)

Double-Zone balancing 3-5-4

Double zones without EOL resistor can discriminate 5 conditions on the entire terminal:

- standby on both zones
- alarm on zone 1 and standby on zone 2
- alarm on zone 2 and standby on zone 1
- alarm on both zones
- tamper (wire cutting)

For each of these, the control panel reads different resistance values on the terminal, expressed below in Ohm.



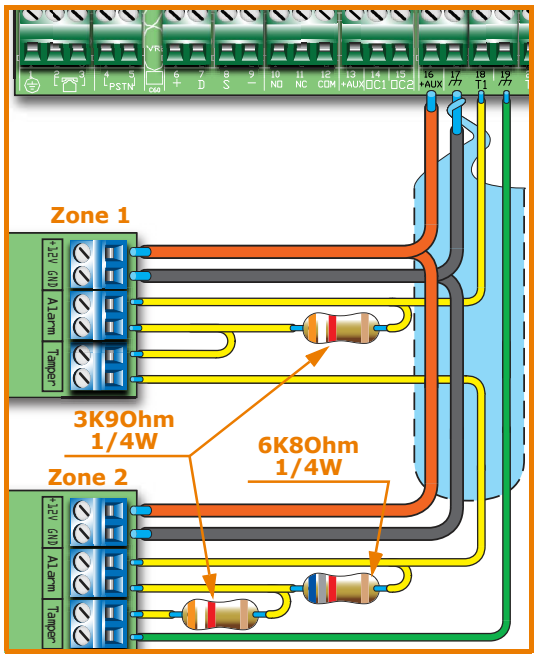
Ohm	Zone 1	Zone 2 (double)
> 3900 + 6800	tamper	
3900 + 6800	alarm	alarm
6800	standby	alarm
3900	alarm	standby
0	standby	standby

Double Zone balancing with EOL 3-5-5

Double zones with EOL resistors can discriminate 6 conditions on the entire terminal:

- standby on both zones
- alarm on zone 1 and standby on zone 2
- alarm on zone 2 and standby on zone 1
- alarm on both zones
- tamper (wire cutting)
- tamper (short-circuit)

For each of these, the control panel reads different resistance values on the terminal, expressed below in Ohm.



Ohm	Zone 1	Zone 2 (double)
> 2 x 3900 + 6800	tamper (wire cutting)	
> 2 x 3900 + 6800	alarm	alarm
3900 + 6800	standby	alarm
2 x 3900	alarm	standby
3900	standby	standby
0	tamper (short-circuit)	

Wiring and balancing rollerblind/shock sensors 3-6

It is possible to choose between two types of balancing for Rollerblind and Shock sensors:

- Normally closed (N.C.)
- Single balancing (NC with EOL)

The following table compares the protection level of rollerblind/shock sensors using the two balancing options provided by the control panel.

Table 39: **Protection level**

BALANCING	N.C.	Single balancing (N.C. with EOL)
Rollerblind or Shock	very low	high

If the rollerblind or shock sensor is connected to a terminal of a wireless device, the connection cable must be less than 2 meters long.

The rollerblind sensor must generate pulses with a length of between 500µsec and 10msec.

Normally closed (N.C.) 3-6-1

In this case, the alarm condition is revealed exclusively by the number of pulses (pulse count) the control panel detects on the terminal.

If this balancing method is applied, the control panel will be unable to detect tamper, wire-cutting or short-circuit.

The discriminated conditions are:

- standby
- alarm

The alarm condition is triggered by the pulse count and sensitivity, in accordance with the programmed parameters (refer to *paragraph 6-7 Zones - Detector type*).

Single balancing (N.C. with EOL) 3-6-2

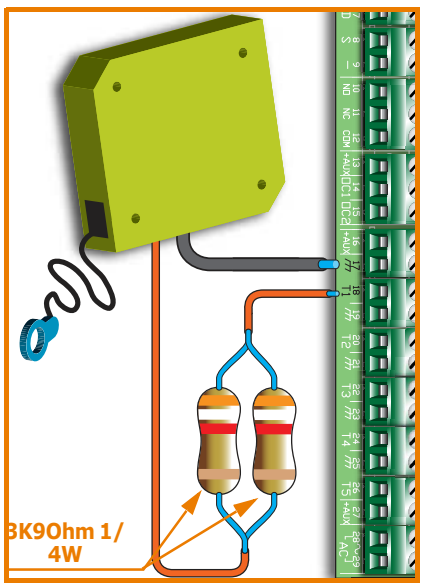
In this case, the discriminated conditions are:

- standby
- alarm
- tamper (wire cutting)
- tamper (short-circuit)

For each of these, the control panel reads different resistance values on the terminal, expressed below in Ohm.

Ohm	Zone
> 3900 / 2	tamper (wire cutting)
3900 / 2	standby
0	tamper (short-circuit)

The alarm condition is triggered by the number of pulses and sensitivity, in accordance with the programmed parameters (refer to *paragraph 6-7 Zones - Rollerblind/Shock*).

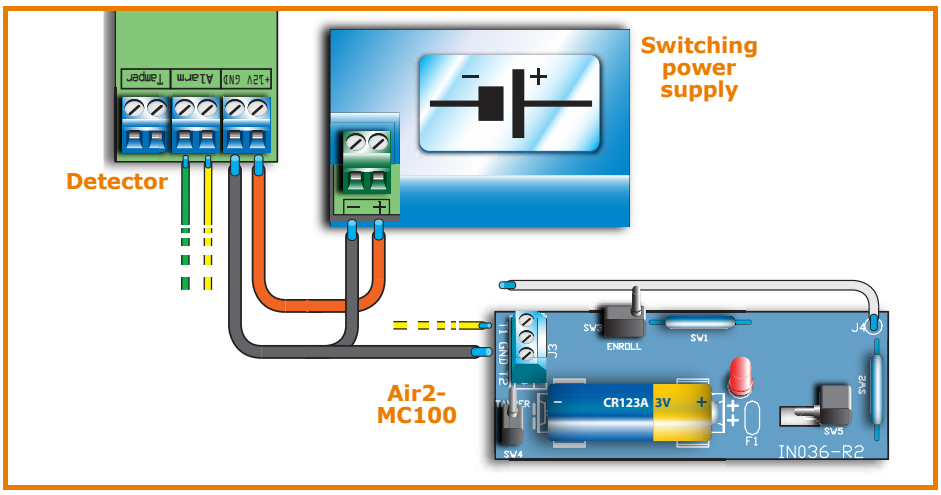


Connecting wireless detectors 3-7

For the connection and deployment of wireless detectors refer to the installation manual of the Air2-BS100 transceiver.

For the connection and balancing of detectors connected to terminals "T1" and "T2" of the Air2-MC100 device, refer to paragraphs *3-5-1*, *3-5-2*, *3-5-3*, *3-6-1* and *3-6-2*.

It is necessary for the "GND" terminal of the Air2-MC100 device to be connected to GND (Negative) of the power source of the detector connected to terminals "T1" or "T2".



Learn zone balancing 3-8

Once you have completed the wiring and configured the balancing of all the zones, you can instruct the control panel to save all the related parameters automatically, by activating the Learn zone bal. option (refer to *paragraph 6-25 Default settings, Learn zone bal.*).

Patent
Patent pending

Connecting the outputs 3-9

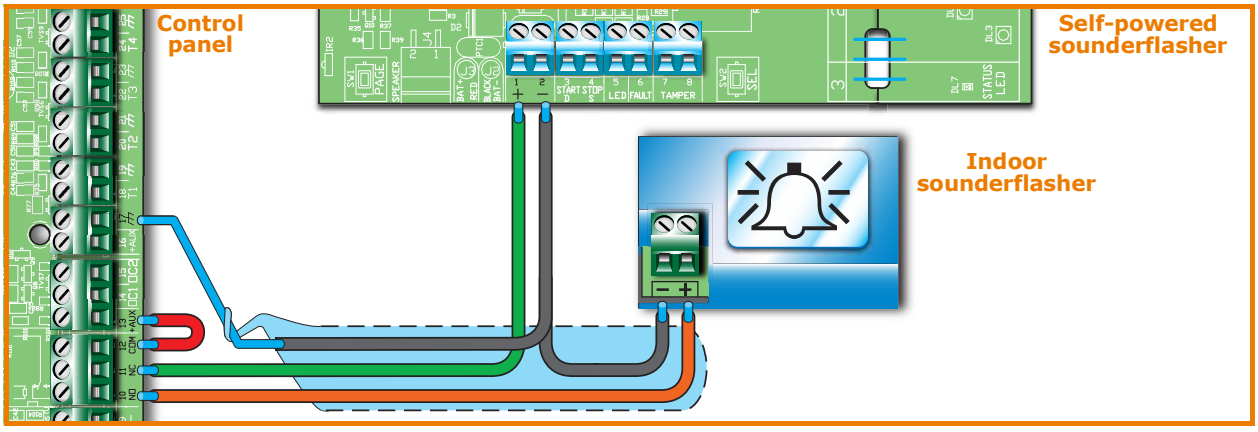
It is possible to set up the outputs to activate in response to the events the control panel manages.

For the connection of the outputs to terminals "T1" and "T2" of the Air2-MC100 device, refer to the Air2-BS100 Installation Guide.

Connecting the sounders 3-9-1

In the event of intrusion alarm, the control panel activates the output/s which are connected to the audible/visual signaling devices. The relay output on the control panel motherboard is the alarm output which is most commonly used to drive a self-powered sounder.

The following wiring diagram shows the connection of a self-powered sounder (IVY as supplied By Ness Corporation) and an indoor sounder.

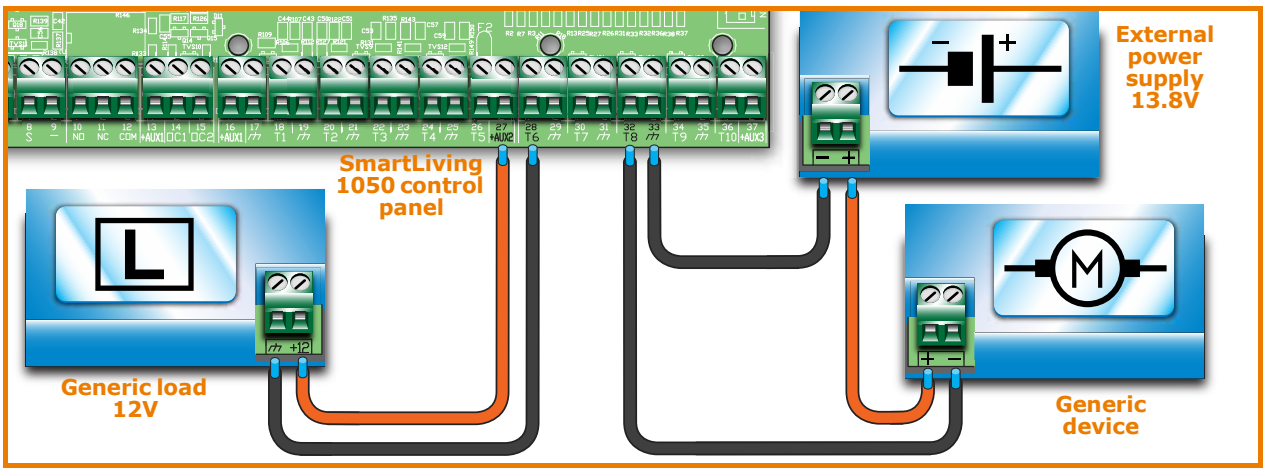


Connecting open-collector outputs 3-9-2

All the system outputs, except for the relay output on the control panel motherboard, are open-collector outputs.

- OC1 and OC2 are open-collector outputs that sink maximum currents in accordance with the *Table 2: Control panels - electrical and mechanical features*.
- All the terminals configurable as outputs are open-collector outputs that sink a maximum current of 150mA.

The wiring diagram below illustrates a series of typical connections which activate the load of a Normally Open output when it closes to GND (⏚).

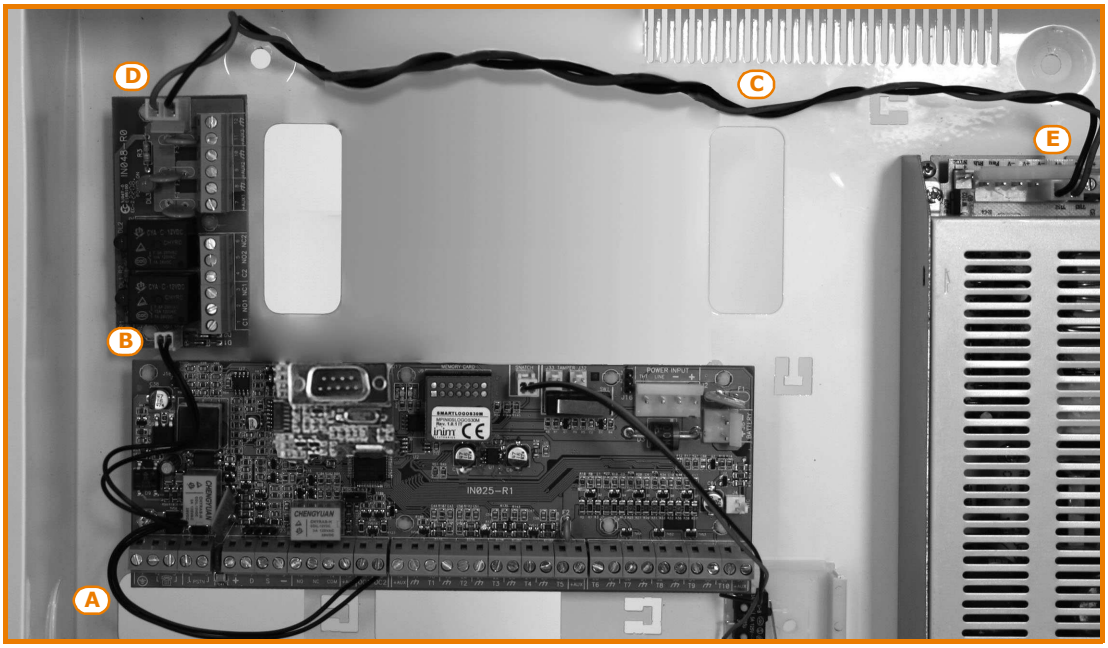


Installing add-on boards 3-10

AUXREL32 3-10-1

If you intend installing this board, work carefully through the following steps.

1. Disconnect all sources of power to the control panel (Mains 230V a.c and battery).
2. Insert the plastic supports into their respective locations (*Table 4: Control panels - description of parts, Z*) on the back of the metal enclosure.
3. Position the board holes on the supports and push the board towards the back of the enclosure until it locks into position.
4. Insert the cable [A] into the connector [B].
5. Connect the two free wires of the cable [A] to terminals 14 (OC1) and 15 (OC2) on the control panel motherboard. Ensure that OC1 and OC2 on the control panel are appropriately connected (*Table 31: AUXREL32 - description of parts, C*).
6. Connect the wire [C] to the connector [D] and to the 2 free pins [E] of the connector on the switching power-supply, as shown in the figure.

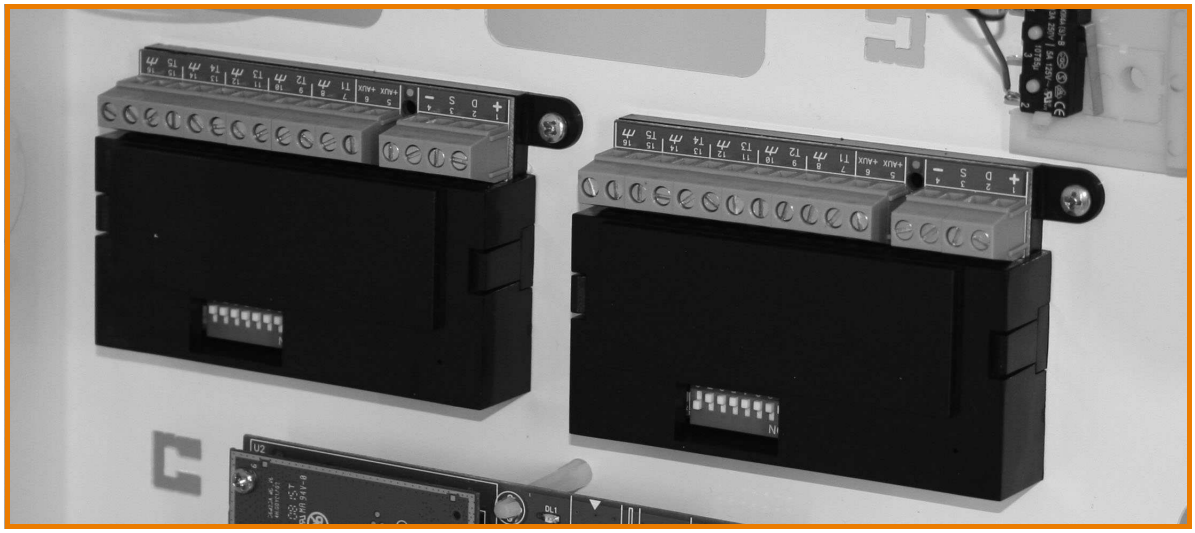


Flex5/U 3-10-2

The metal enclosures of SmartLiving 10100L control panels provide housing for two Flex5/U expansion boards (accessory items). Optional housing are also available to house additional modules mounted away from the SmartLiving Control panel.

If you intend installing this type of board, work carefully through the following steps.

1. Disconnect all sources of power to the control panel (Mains 230V a.c and battery power).
2. Secure the plastic enclosure of the Flex5/U to the backplate of the control panel (*Table 4: Control panels - description of parts, B1*).
3. Connect it to BUS line as described in *paragraph 3-2-1 The I-BUS line wiring*.
4. Address it as described in *paragraph 3-3-4 Addressing FLEX5 expansions and the Air2-BS100 transceiver*.
5. Power up the control panel (reconnect Mains 230V a.c and battery power).

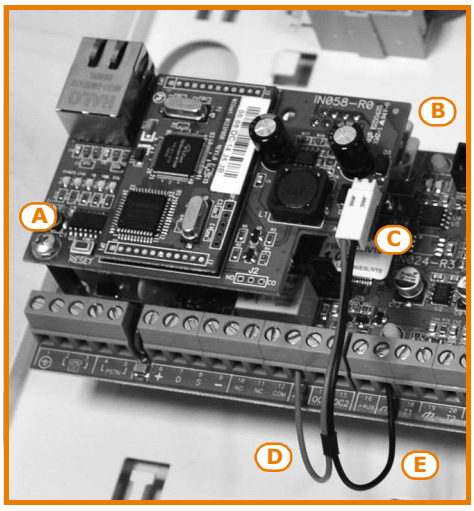


SmartLAN 3-10-3

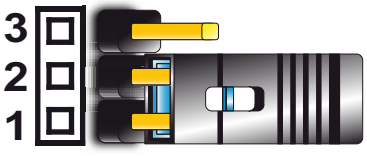
The SmartLAN board, available with SmartLAN/G and SmartLAN/SI versions, allows SmartLiving control panels to extend their connectivity to Ethernet and Internet networks.

The operating capacity of the SmartLAN board depends on the proper configuration of the networks it is connected to. Therefore, if you are installing a SmartLAN board, it is necessary to contact the network administrator in order to configure it correctly.

The figure opposite shows the SmartLAN/SI board mounted inside the box. If you intend installing this board, work carefully through the following steps.



1. Disconnect all sources of power to the control panel (Mains 230V a.c and battery power).
2. Remove the earth connection screw [A] (*Table 4: Control panels - description of parts, A1*) from its location and replace it with the metal spacer (included).
3. Align the screw location on the board with the support and serial connector on the backplate [B], with the connector on the SmartLiving board (*Table 4: Control panels - description of parts, S*).
4. Fasten the screw [A] on the support.
5. **Insert the board power jumper between pins 1 and 2 of the connector** (*Table 4: Control panels - description of parts, O*).
   For SmartLiving 515 model without this connector, use the cable jack and connect it to the connector [C], then connect the free red [D] and black [E] wires respectively to terminals "+" and "-" of the control panel BUS.
6. Power up the control panel (reconnect Mains 230V a.c and battery power).



Note

It is important to note that the e-mail service does not guarantee delivery time of e-mails and their attachments nor even their final delivery.

IP and Internet Connectivity 3-11

Configuring an IP network 3-11-1

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.

IP ADDRESS

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 programme. The PC used for the initial programming of the SmartLAN must have an IP address of the same address class / subnet **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.

SUBNET MASK

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**.

TCP/IP PORT

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.

GATEWAY

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).

DNS

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.

SSL

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

Configuring a router 3-11-2

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 or 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 3-11-3

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)

VIA SMARTLEAGUE

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 MOBILE DEVICES

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:

- 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 3-11-4

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.

FIRST POWER UP

On first power up, the control panel initializes the parameters at default (factory settings).

In addition, the control panel automatically enrolls all the peripherals it "sees" on the I-BUS (automatic addressing phase). The default address of all expansions, keypads and readers is address 1, therefore, if the system is equipped with more than one of each type of device, the automatic enrolling operation will be erroneous. In order to allow the system to perform an accurate auto-enrolling operation on "First power-up", work carefully through the following steps.

Note

The default address of all peripherals (keypads, readers and expansions) is set at address 1.

ATTENTION!

When wiring the system, be careful not to allow any form of power (mains 230V or battery) to reach the control panel or its peripherals.

1. Attach the control panel to the wall.
2. Complete the wiring of the peripherals to the BUS.
3. Connect the BUS wires to the control panel.
4. Complete the wiring and balancing of the system detectors.
5. Connect the detectors to the terminals.
6. Connect the outputs to the control panel and peripheral terminals.
7. Connect the control panel to the telephone line.
8. Connect the SmartLogos30M board to the appropriate connector on the control panel motherboard.
9. Insert the maintenance jumper in the "SERV" position.
10. Connect the primary power source (230V a.c.).
11. Connect the backup battery. The first line of the display of each keypad in the system will show the 'Maintenance' message and the keypad address at default. On first power up (first startup), all the keypads will show "K01" (refer to *paragraph 3-1-10 Maintenance status*).

Note

If several keypads are connected to the I-BUS, their displays may be blank. If this occurs, disregard this aspect and go directly to the next step.

12. Address the peripherals (refer to *paragraph 3-3 Addressing the peripherals*). At least one keypad must be assigned to address 1. Using keypad 1, initialize the addressing phase for nBy/S and nBy/X readers (refer to *paragraph 3-3-5 Addressing nBy readers*).
13. If useful, from the Installer menu, start the step-by-step guided "Fast programming" procedure which allows the programming of all the main parameters of the system (refer to *paragraph 6-4 Fast programming from the keypad (Wizard)*).
    This point skips the successive points and ends at *17*, otherwise, works through the following steps.
14. From the installer menu, start the self-enrolling process of zone balancing (refer to *paragraph 6-25 Default settings*, *SelfEnrol.zone bal*).
15. If necessary, specify the expansion terminals simulated by the Air2-BS100 transceiver (refer to *paragraph 6-6 Terminals*) as "Wireless" terminals.
16. If the installation requires the use of a dialler, programme the telephone numbers relating to the voice and digital dialer functions (refer to *paragraph 6-10 Telephone*).
17. Remove the jumper from the "SERV" position and place it in the "RUN" position.

Chapter 5

INSTALLATION PROJECT VIA THE SMARTLEAGUE

The especially designed SmartLiving system can be programmed from a keypad or via PC. All programming functions can be accessed through the software programme. You will need:

- A computer (to be connected to the control panel)
- The SmartLeague software programme

5-1 The SmartLeague software programme

The SmartLeague software programme 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:

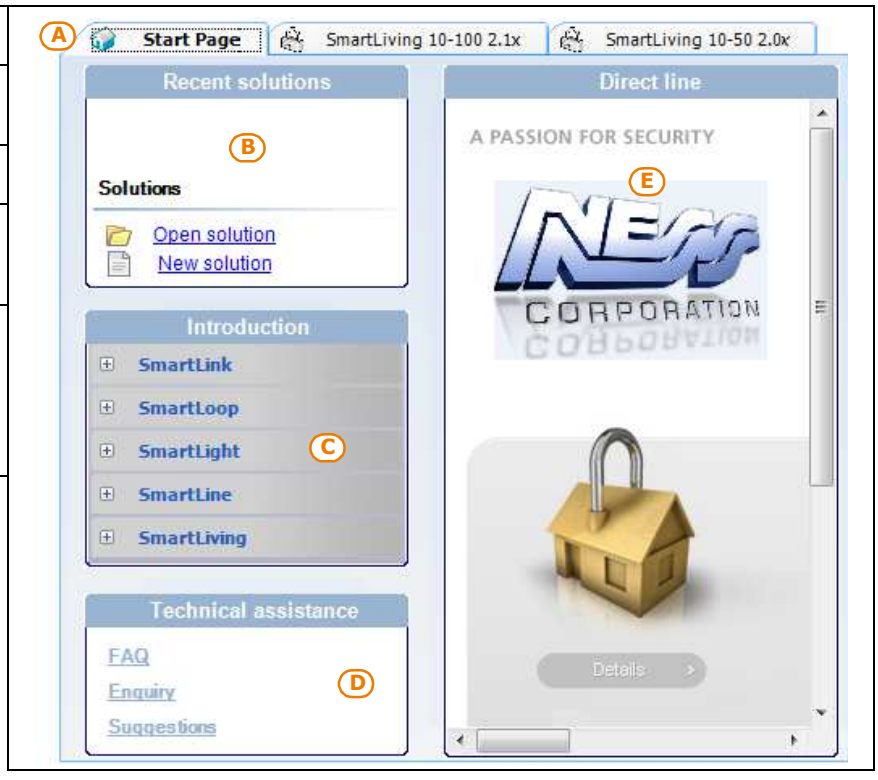
- RS232 serial port of the PC
- LAN (combined with the use of a SmartLAN/SI or SmartLAN/G board)
- Modem

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 programme is common to all the programmable devices and is always active, even during the programming session (in the form of a template):

Table 40: **SmartLeague software programme - 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	Area dedicated to help and service via 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 Ness 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 programme 5-2

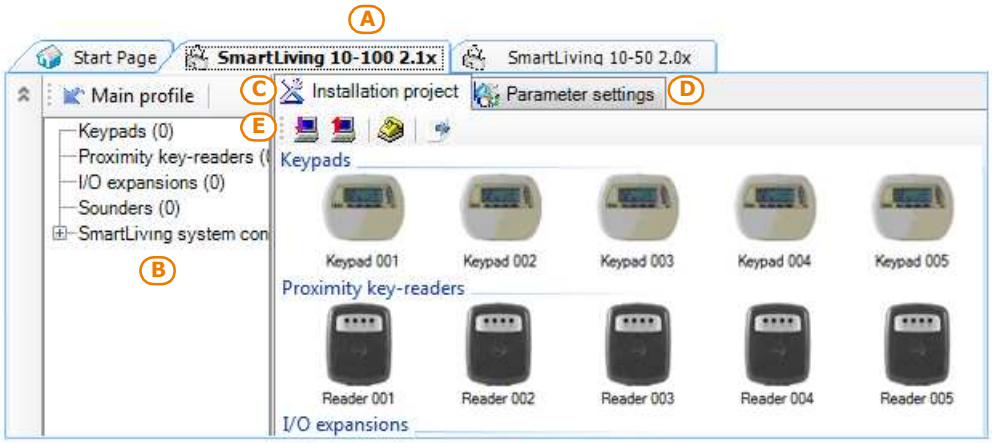
Each project, from the most uncomplicated to the most complex of systems, is represented by a solution, which contains the programming parameters and installation structure.

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 programme presents the following interface:

Table 41: **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, you can plan the layout of an installation or set the options/parameters at your office and download the settings to the system at a later time.

In this case, you must programme:

- 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 full instructions regarding these connections, refer to the SmartLAN board or SmartModem100 Installation Manual.

For details regarding the GPRS connection, refer to *paragraph 6-29-5 GPRS Connections (Nexus/G only)*.

Creating a project layout 5-3

The project layout section, in the SmartLeague software programme, allows you to select the number of peripheral devices you wish to install and thus plan and configure the system.

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 DEL 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.

When the downloading phase terminates, the control panel will complete the operations it usually carries out on exiting the Installer menu, as described in *paragraph 6-2 Accessing the Installer menu*.

PROGRAMMING
FROM COMPUTER

Note

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.

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 programme provides a button that allows you to create a file which interfaces with supervisory software such as Ness's SmartLook or WinMag (ask you dealer for details).

Chapter 6

OPTIONS AND PROGRAMMING METHODS

Introduction 6-1

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 exceptions.

- From the keypad you cannot programme:
  - Timer exceptions
  - Input calibration
  - Sounderflasher tone
  - BUS speed
  - Description of the "Emergency key duos"
  - Parameters relating to the SmartLAN board
  - Parameters relating to the Nexus GSM dialer
  - Parameters relating to the I-BUS Ivy-B
  - Programmable events
- Via the SmartLeague software programme you cannot programme:
  - 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 6-2

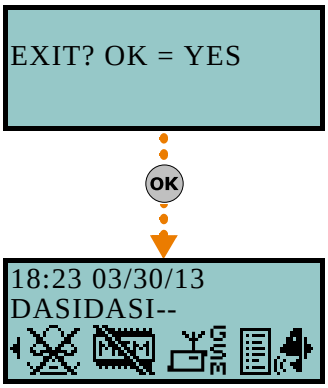
If you wish to programme the system via the installer menu from a keypad and thus upload/download the control panel parameters, you must:

1. Disarm all the control panel partitions.
2. Type-in a valid PIN (installer code) on the keypad then press OK.
   If an Alien keypad is being used, access the "Settings" section by pressing 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:

- Block all system keypads except the one you are using.
- 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:

- Apply all the new settings and values.
- Restore the I-BUS, reprogramme and make all the peripherals fully operational.
- Restore the call queue, and events log to normal operations.

6-3 Programming via the SmartLeague programme

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 5-3 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.

Note

The limitations described in *paragraph 5-3 Creating a project layout* apply during them reading and writing phases.

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.

6-4 Fast programming from the keypad (Wizard)

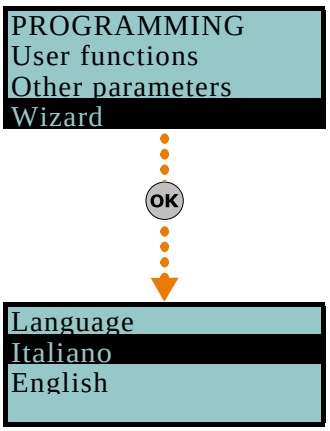
SmartLiving provides you (the installer) with a step-by-step guide to fast system programming via the Installer menu.

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 programme the basic parameters and functions which allow the system to operate properly.

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 the 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.

Panel options 6-5

The following options are provided by the control panel.

Table 42: **Panel options**

Option	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 T 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 send voice calls to all the 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 a Ness 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: 1. the installer calls the control panel 2. the control panel detects the ring, picks up, recognizes the installer code and hangs up immediately 3. 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 autobypassable open-zones will be shown in white on a black background.	
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 *paragraph 6-7 Zones*), 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.

Table 42: **Panel options**

Option	If enabled	If disabled
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: • terminal tamper • control panel open-tamper • control panel dislodgement-tamper • peripheral tamper • peripheral loss • false key	
Encrypt data	The control panel will encrypt data via LAN (for SmartLAN/SI only).	
Instant restoral	The restoral of the magnetic reed sensor in Air2-MC100 and Air2-MC200 wireless detectors will be signaled instantly.	The restoral 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 *paragraph 6-25 Default settings*), 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 on the 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. • Red keypad LED Off • Yellow keypad LED Off • Green keypad LED On solid • Status icons not present • Alarm and Tamper memory hidden • If a particular event occurs more than 5 times when the partitions are armed, it will not be signaled as having occurred more than 5 times. This is due to the limitation placed on the counter of each event. The counters will reset to zero each time all the partitions are disarmed. If the partitions are DISARMED: • The LEDs will function normally. • Status icons present • Alarm and Tamper memory 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.
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 forward 1 hour at 2:00 am on the first Sunday in October and go back 1 hour at 3:00 am on the first Sunday in April	No automatic clock forward/back operations.
NoStringsSiaProt	The descriptive strings will not be sent in SIA reporting format.	The descriptive strings will be sent in SIA reporting format.
AllSiaIP OnPerEv	The control panel will send calls to all SIA-IP numbers programmed for the "Periodic event" (activation and restoral).	
InvertCONTACT-ID	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.

Table 42: **Panel options**

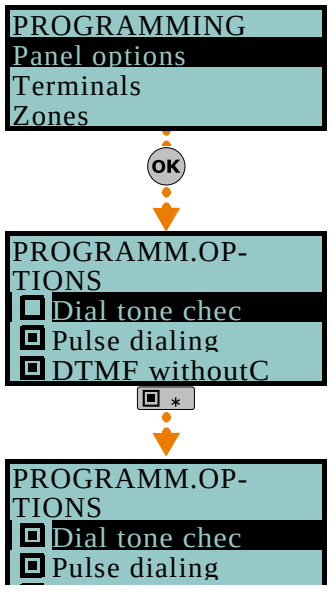
Option	If enabled	If disabled
Dust event enab.	Enables management of the "Detector dusty" event. The "Output fault" and "Detector dusty" events share the same actions. Therefore, if either of these events occur, the system will send the calls and activate the outputs associated with the "Output fault" event. The events log provides the proper distinction between these two events: • 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 jumper (refer to *Table 4: Control panels - description of parts, Q*). 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. **You must disable this option if you wish to put the control panel in "RUN" mode.**	You can also put the control panel in maintenance mode by means of the jumper (refer to *Table 4: Control panels - description of parts, Q*).
View 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: • 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 **Note** In order to comply completely with Grade 3 of Normative 50131, also the other options relative to Grade 2 must be activated (refer to *Chapter 7 - Compliancy with the regulations in force*).	
Al. 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 with 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.

Via Keypad

1. Access the "Programming Panel options" section.

Type-in Code (Installer PIN) (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.



Via PC

Table 43: **Options - via SmartLeague software programme**

Option	Part of the system	Template - section
Dial tone check	SmartLiving System - Telephone	Parameters settings - Telephone line parameters
Pulse dialing		
DTMF withoutCode		Parameters settings - Telephone dialer parameters
Line down signal		Parameters settings - Telephone line parameters
Double call		Parameters settings - Telephone line parameters
Call allVoxNums		Parameters settings - Telephone dialer parameters
Call all TLVNums		Parameters settings - Telephone dialer parameters
RefreshMnstblOut	SmartLiving System	Parameters settings - Control panel parameters
Num15 ForTeleserv	SmartLiving System - Telephone	Parameters settings - Teleservice parameters
Install.callback		
ReaderBuzzer OFF	Proximity readers	Parameters settings - Reader parameters
Keypad lockout	Keypads	Parameters settings - Keypad parameters
View open zones		
OpenZonesArmLock	SmartLiving System	Parameters settings - Control panel parameters
DTMF sensitivity	SmartLiving System - Telephone	Parameters settings - Telephone dialer parameters
BypassAlsoTamper	SmartLiving System	Parameters settings - Control panel parameters
BypassVoiceCheck	SmartLiving System - Telephone	Parameters settings - Telephone dialer parameters
Confirm with *		
NoUserTamp.reset	SmartLiving System	Parameters settings - Control panel parameters
Encrypt data	/	Menu bar - Settings - Application data - Communication type - SmartLAN/SI
Instant restoral	SmartLiving System	Parameters settings - Control panel parameters
Teleserv. hidden		
LockInstall.Code		
50131ReaderLedOFF		Parameters settings - 50131 Parameters
50131StatHidden		
50131IconsHidden		
50131AlarDelayed		
50131WarnLedMem		
DayLightSav.time		Parameters settings - Control panel parameters
NoStringsSiaProt	SmartLiving System - Telephone	Parameters settings - Telephone dialer parameters
AllSiaIP OnPerEv		
InvertCONTACT-ID		
Dust event enab.	SmartLiving System	Parameters settings - Control panel parameters
Maintenance		
View Scenario	Keypads	Parameters settings - Keypad parameters
Tamper siren	SmartLiving System	Parameters settings - Control panel parameters
Squawk on arming		
50131, Grade 3		Parameters settings - 50131 Parameters
Al. on keypads		Parameters settings - Control panel parameters
SingleCallEachEv	SmartLiving System - Telephone	Parameters settings - Telephone dialer parameters

Terminals 6-6

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

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

Patent pending

ATTENTION!

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.

Via Keypad

1. Access the "Programming Terminals" section.

Type-in Code (Installer PIN) OK, PROGRAMMING Terminals OK.

The display will show the:

1° line: the number of terminals

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

3° line: the description of the selected terminal

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

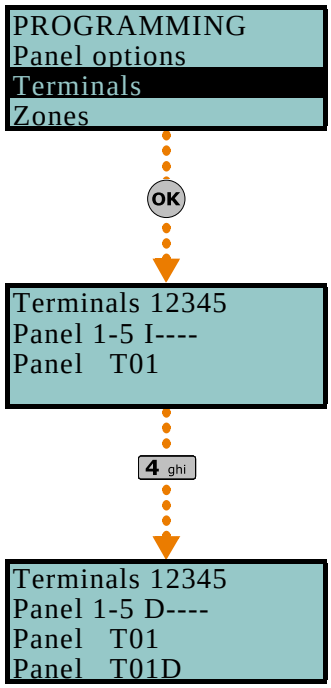
2. Use keys and to select the device whose terminals you wish to configure. The terminals are arranged as follows:

- 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. Configure the terminal by pressing:

- 1 ., to configure the terminal as an INPUT ("**I**")
- 2 abc to configure the terminal as an OUTPUT ("**O**")
- 3 def to configure the terminal as a TWO WAY - SUPERVISED OUTPUT ("**T**")
- 4 ghi to configure the terminal as a DOUBLE ZONE ("**D**")
- 5 jkl to configure the terminal as UNUSED ("**-**")
- 6 mno to enable/disable the terminal as "Wireless"

4. Once you have configured the terminal, press OK, , , 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 a Flex5 expansion terminal, press key 6 mno 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 6 mno again, the operation will undo.

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

- INPUT- for Air2-IR100 and Air2-MC100 devices
- DOUBLE ZONE - for Air2-MC200 devices

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

1. Position the cursor on the terminal concerned.
2. Press 6 mno to configure the terminal, and consequently the entire expansion, as wireless.
3. Configure the terminal as an "input" (1 .,).
4. Press OK 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-MC100 device.
8. Enable the "Broadcast RF" option as follows:

Type in Code (Installer) OK, PROGRAMMING Zones OK, select the zone, Options OK, BroadcastRF. OK

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

Note

The "Broadcast RF" option must be enabled for each terminal of the Air2-MC100 device concerned.

9. Go back to step 1 and configure the terminal as an output (2 abc).
10. Press OK to access the output parameters programming section (description, options, etc.).

Press OK 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 6-7 Zones* or *paragraph 6-8 Outputs*).

Via PC

Select "SmartLiving System - Terminals" from the tree menu on the left, then go to the "Parameters settings" template on the right:

All the terminals will be shown on the respective page. You must configure the terminal graphically using the mouse, as follows:

1. Point to the terminal you require.
2. Right click on the mouse and select the required type.
3. Double click to set the options for the terminal.
4. Position the mouse on the programming field instead of on the specific terminal to configure all the terminals in the same way.

If the terminal is configured as "Zone" (=INPUT) or "Double" (=DOUBLE ZONE), it will appear in the Zone programming section (*paragraph 6-7 Zones*). If the terminal is configured as an "Outputs" (=OUTPUT) or "I/O" (= TWO WAY), it will appear in the Outputs programming section (refer to *paragraph 6-8 Zones*).

Zones 6-7

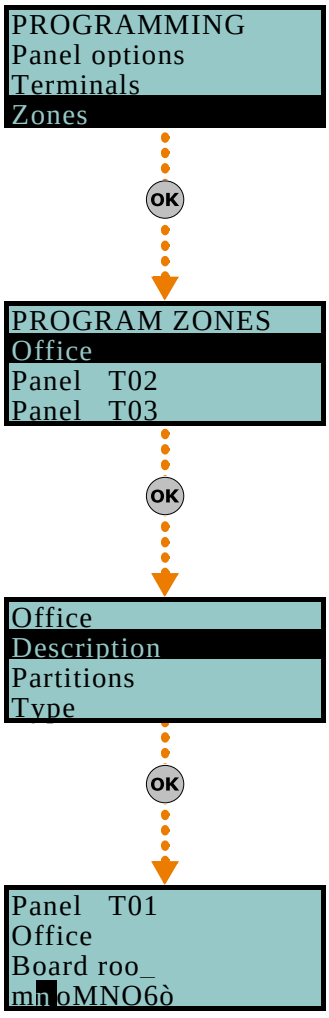
This programming section deals with all the zone parameters.

Via Keypad

1. Access the "Programming Zones" section.

Type-in Code (Installer PIN) OK, PROGRAMMING Zones OK.

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



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.

1° line: default description
2° line: current description
3° line: description being edited
4° 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 OK. The available Types are (refer to *Appendix A, Technical terminology and Glossary*):

- **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 *Appendix A, Technical terminology and 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 6-13 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 (refer to *Appendix A, Technical terminology and Glossary*) 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.

Option	If enabled	If disabled
TampReed/FollPir	• **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. There may be up to a 3 minute delay between the partition arming command and when the detector actually arms. • **Air2-MC100/MC200** - detects magnetic-contact tamper when both reeds are in standby status.	• **Air2-IR100** - the PIR detector will be active at all times. • **Air2-MC100/MC200** - tamper on the magnetic contact will not be detected.
Broadcast RF	This option must be enabled when the zone and one of the terminals of the Air2-MC100 device ("T1" or "T2") is configured as an "output". Assures the activation/deactivation of the output within 2 seconds of the control panel command.	The activation/deactivation of the "wireless" output occurs within 2 minutes of the command from the control panel.
Use sensor LED	The red LED of Air2-IR100 and Air2-MC100/MC200 devices signals alarm and tamper conditions on the device. **Note** This option will be enabled on all the terminals of the Air2-MC100.	The red LED of Air2-IR100 and Air2-MC100/MC200 will be "Off" at all times.

- **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 signaling (yellow LED on the keypad).
- **Disab.tamper WLS** If this option is disabled, open/dislodgement tamper on Air2 detectors will not generate the respective events.

Note

This option applies only to Air2-BS100 transceivers with 1.04 firmware and higher.

ATTENTION!

Activation of this option declines compliance with the directives and regulations in force.

Wireless

Note

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 6-6 Terminals*).

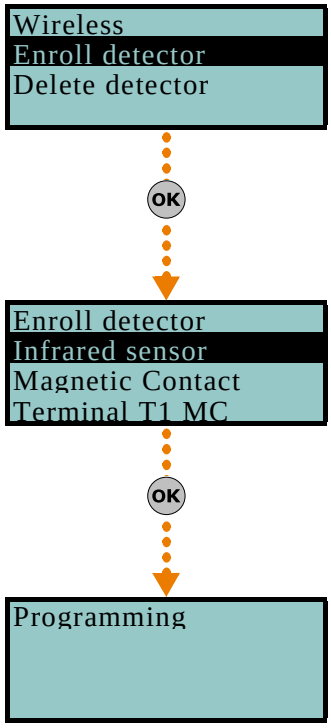
This section allows you to carry out all the operations relating to the programming of Air2 wireless series devices. The wireless-device programming section is arranged as follows.

- **Enroll sensor** - allows you to enroll a wireless detector which has not yet been 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-MC100 magnetic reed contact
  - **Terminal T1 MC -** allows you to enroll the "T1" terminal of an Air2-MC100
  - **Terminal T2 MC -** allows you to enroll the "T2" terminal of an Air2-MC100
  - **Smoke detectors** - allows you to enroll an Air2-FD100 smoke detector
  - **Magn.Cont.MC200** - allows you to enroll an Air2-MC200 device.

  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-MC100 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-MC100. 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-MC100 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.

Balancing

Balancing can be (refer to *Appendix A, Technical terminology and Glossary* and *paragraph 3-5 Wiring and balancing alarm detectors*):

- 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 *Appendix A, Technical terminology and Glossary*, *Alarm cycles)*.

Detector type

It is possible to configure a zone as:

- Generic zone
- Rollerblind
- Shock (Nessensor Vibration Sensors)

The following Table shows the terminals which accept Generic, Rollerblind and Shock zones, and the respective zone-parameter fields for each 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 minutes (see "info" box).

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 Note).

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 Note).

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

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 (Nessensor) zone)

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

Shock time (shock (Nessensor) zone)

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

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 Note).

Shock pulses (shock (Nessensor) 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 millieseconds, 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 OK to confirm and exit.

Via PC

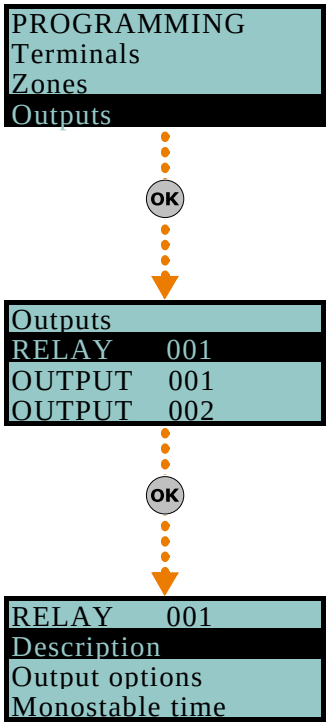
Programming zones via the SmartLeague application is accomplished by the selection and programming of the terminal configured as zone, described in *paragraph 6-6 Terminals*.

Outputs 6-8

This programming section deals with all the output parameters.

SmartLiving control panels provide 3 outputs:

- Relay Output
- O.C. Output 1
- O.C. Output 2



Via Keypad

1. Access the "Outputs" section.

Type-in Code (Installer PIN) OK, PROGRAMMING Outputs OK.

2. Use and to select the output thenpress OK.

Description

This is the editable output label (device description). At default all the outputs, except for the 3 outputs on the control panel motherboard, assume the description of the peripheral they refer to followed by the respective terminal.

Follow the instructions in *paragraph 6-7 Zones - Descriptions*.

Output options

Use * and # to enable or disable the selected option.

- **Norm. closed**: this will be the output status during standby.
- **Monostable** (On for a period of time)
- **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 - can be employed in direct control of a visual signaling device (e.g. flasher).
- **ON afterRestoral**: 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 6-11 Events*).

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

  For example:

  •• 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.

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.

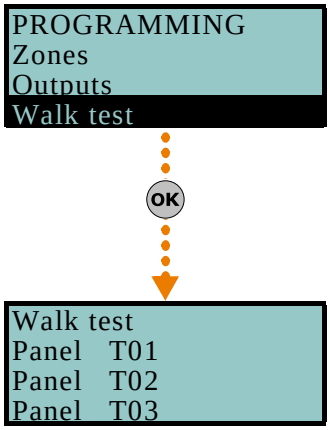
Use keys and and the number keys to set the times.

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).

Via PC

Programming zones via the SmartLeague application is accomplished by the selection and programming of the terminal configured as output, described in *paragraph 6-6 Terminals*.

Walk test 6-9



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.

Via Keypad

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.

Via PC

Select "Check control panel - Monitoring - Walk test" option from the menu bar.

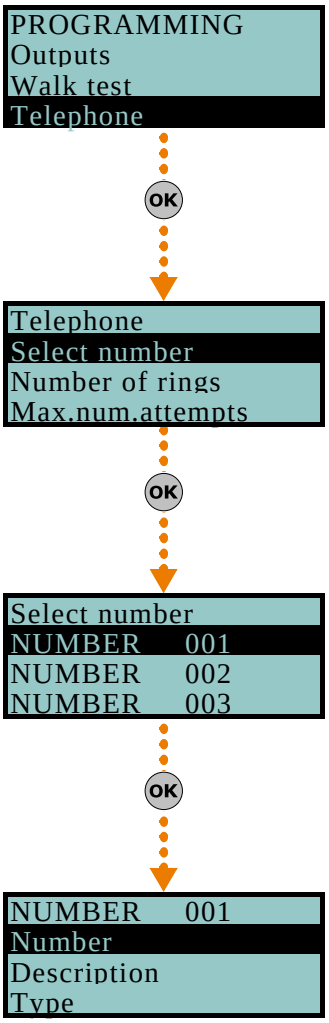
The display will show a list of all the configured zones and the start test button. Once you press the test button, the violated zones will be marked by a red dot.

Telephone 6-10

This programming section deals with all the telephone parameters.

The built-in 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)



Via Keypad

Type-in Code (Installer PIN) OK, PROGRAMMING Telephone OK.

Select number

The Phonebook provides 15 number positions which can be selected by means of keys and . You can programme 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 6-7 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 6-5 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 OK.

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:

xxxyyyzzzttt,ppppp

where:

- "xxxyyyzzzttt" 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 2 abc 3 def.
- **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**

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 [OK] to confirm and exit.

Via PC

Table 44: **Telephone - via SmartLeague software programme**

Option	Part of the system	Template/section
Select number	SmartLiving System - Telephone	Programming
Number of rings		Parameters settings - Telephone line parameters
Max.num.attempts		Parameters settings - Telephone dialer parameters
Message repeats		

Events 6-11

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

The control panel recognizes all of the events described in this paragraph and, for each them, in accordance with programming, can generate actions both when the event occurs and when it restores/ends.

The operations that can be carried out at the control panel are: output activation, notification of events via telephone, notification via SMS messages, event memorization, voice message management, voice message management and management of all the options relating to each event. These actions are triggered as soon as the event occurs (or restores).

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 (refer to *paragraph 3-10-3 SmartLAN*).

Event notification via predefined SMS messages requires the use of a Nexus (refer to *paragraph 6-29-3 Text for SMS messages*).

Note

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.

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 45: **Event type**

Name	Occurs when...	Restores when ...	Number of events	Pulse events
Zone alarm	A zone generates an alarm	A zone restores	One event for each zone	no
Terminal tamper	A terminal detects tamper (short-circuit or wire cutting)	A terminal restores	One event for each terminal	no
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
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
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
Zone bypass	A zone is inhibited	A zone is enabled (switched On)	One event for each zone	no
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
	The event is independent of the zone type and the armed/disarmed status of the partitions.			
Partit.not ready	A zone which belongs to the partition is not in standby status.	All the zones belonging to the partition are in standby status.	One event for each partition	no
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
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
Partit.AwayArmed	The partition interior and perimeter zones have been armed effectively	The partition has been disarmed effectively	One event for each partition	no
Partit.StayArmed armed	The partition has been armed effectively in Stay or Instant mode	The partition has been disarmed effectively	One event for each partition	no
Partition reset	A request is made to reset the partition		One event for each partition	Yes
Exit time	The partition exit time is running	The partition exit time expires	One event for each partition	no
Entry time	The partition entry time is running	The partition entry time expires	One event for each partition	no
Pre-arm time	The partition Pre-arm time is running	The partition Pre-arm time expires	One event for each partition	no
Overtime request	A request for overtime relating to the partition is made		One event for each partition	Yes
Chime	A chime zone belonging to the partition is violated		One event for each partition	Yes
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
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 6-27 Other parameters*).		One event for each partition	Yes
Valid code	A user-code PIN entered at a keypad is recognized as valid		One event for each code	Yes
Valid key	A key used at a reader is recognized as valid on the reader		One event for each key	Yes
Valid Code AtKeyp.	A user-code PIN entered at a keypad is recognized as valid on the keypad		One event for each keypad	Yes

Table 45: **Event type**

Name	Occurs when...	Restores when ...	Number of events	Pulse events
ValidKeyAtReader	A key used at a reader is recognized as valid on the reader		One event for each reader	Yes
Partition code	A user-code PIN entered at a keypad is recognized as valid on the partition		One event for each partition	Yes
Partition key	A key used at a reader is recognized as valid on the partition		One event for each partition	Yes
Failed call	All attempts to call a specific telephone number have failed	One call to the phone number has been successful	One event for each contact telephone number	no
Timer activated	The timer is enabled (On)	The timer is disabled (Off)	One event for each timer	no
Thermostat ON	The activation conditions set for the keypad thermostat occur.	The deactivation conditions set for the keypad thermostat occur.	One event for each keypad	no
Scenario ON	The status of all the partitions corresponds exactly to the pre-set scenario.	The status of all least one of the partitions does not correspond to the pre-set scenario.	One event for each scenario	no
ProgrammableEvt	See *paragraph 6-11-1 Programmable events*			no
Emergency key	One of the emergency-key duos is pressed		One event for each emergency-key duo	Yes
Panic Ev.	The "Panic" shortcut is activated.		15	Yes
Periodic event	The Periodic Event occurs		4	Yes
Panel opened	The control-panel enclosure cover is opened	The control-panel enclosure cover is replaced	1	no
Dislodged panel			1	no
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
IBUS fuse fault	The I-BUS protection fuse is not operational (blown)	The I-BUS protection fuse restores	1	no
Low battery	The backup battery is low (voltage below 10.4V)	The backup battery is charged (voltage above 11.4V)	1	no
Mains failure	The primary 230V a.c. power source is absent (blackout)	The primary 230V a.c. power source restores	1	no
Expansion tamper	An expansion board signals tamper conditions	Tamper conditions clear on all the system expansion boards	1	no
Keypad tamper	A keypad signals tamper conditions	Tamper conditions clear on all the system keypads	1	no
Reader tamper	A reader signals tamper conditions	Tamper conditions clear on all the system readers	1	no
Sound.flash.Tamp	A sounderflasher connected to the BUS signals tamper	All the sounderflashers connected to the BUS reset	1	no
Nexus tamper	The GSM dialer Nexus signals tamper	Tamper conditions clear on the Nexus	1	no
Tamp. V-Monitor	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
Keypad loss	A keypad cannot be found on the BUS	All keypads can be found on the BUS	1	no
Reader loss	A reader cannot be found on the BUS	All readers can be found on the BUS	1	no
Sound.flash.Loss	A sounderflasher cannot be found on the BUS	All sounderflashers can be found on the BUS	1	no
Nexus loss	The control panel is unable to communicate the Nexus 100	Communication between the control panel and the Nexus restores	1	no
Nexus V-Monitor	For future use			
Jamming	Wireless interference detected	Wireless interference cleared	1	no
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
WLS zone loss	Loss of at least one wireless detector has been signaled (supervisory time-out)	All the wireless detector are present	1	no
Installer code	An Installer PIN entered at a keypad is recognized as valid		1	Yes
Invalid code	An invalid code is entered at a keypad		1	Yes
False key	An invalid key is used at a reader		1	Yes
Nexus fault	The GSM dialer Nexus signals a fault (see *Chapter 8 - Errors and faults*)	Fault conditions clear on the Nexus	1	no
Tel. line down	The land line is not working	The land line restores	1	no

Table 45: **Event type**

Name	Occurs when...	Restores when ...	Number of events	Pulse events
Hard reset	The control panel re-initializes. The system clock may be wrong or not working properly.		1	Yes
Call queue full	There are no more slots left in the outgoing call queue		1	Yes
Successful call	The call is answered		1	Yes
Programming	Access to system programming is authorized	End of system programming	1	no
Ongoing call	A call is sent	A call ends	1	no
SMSMessageFailed	Nexus failed to send SMS message		1	Yes
Output fault	An output fails to switch status as commanded		1	Yes
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
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
Int. Resistance	For future use			
Battery shorted				
Battery disconn.				
PwSupplyOverload				
PwSupplyOverheat				
Ground fault				
Overvoltage "x"				
Overvolt. BUS				
Undervoltage				
Undervoltage BUS				
Short circuit "x"				
Short circuit BUS				
Overload "x"				
Overload BUS				
NoCommunPwSupply				
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
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
Sync.data IP2RX	The IP2RX synchronization process has been carried out from a keypad (refer to the User Manual, "Activations")		1	Yes
IP conn. lost	The IP connectivity test is enabled and the test result in negative (failed).	A connection attempt has been successful.	1	no
IP conn. lost	Nexus/G has detected GPRS connectivity trouble.	The GPRS connectivity is restored.	1	no

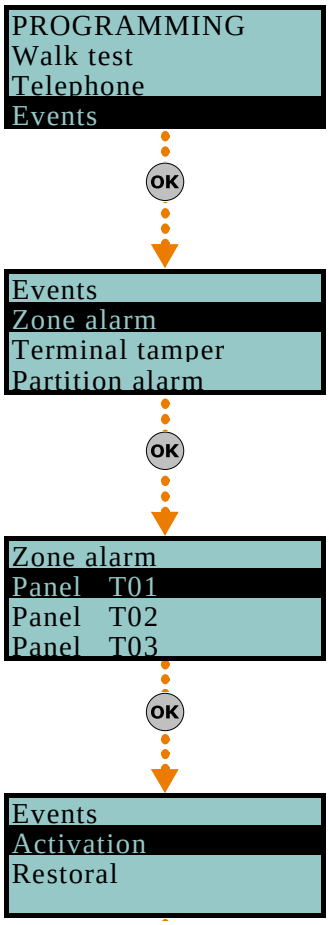
Each event can be associated with 3 voice messages, selected from the message list (refer to *Appendix D, Voice messages*).

- 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.

Via Keypad



1. Accessing the "Events" section

Type-in Code (Installer PIN) 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 programme the actions to be carried out when the event occurs.
- **Restoral** - to programme 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 46: Event-related messages* and *Appendix D, Voice messages*):

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.

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

Table 46: **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	1. Message type + 260 2. Message A 3. Message B 4. "Location" (244)	1. Message type 2. Message B 3. "Location" (244)
Sequence in the event of Restoral	1. "Restoral" (97) 2. Message type 3. Message A 4. Message B 5. "Location" (244)	1. Message A 2. Message B 3. "Location" (244)

Note

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).

Options

To be activated by keys * and #:

Table 47: **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.

Table 47: **Event options**

Option		If enabled	If disabled
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 *Table 46: Event-related messages*)	In the case of voice calls, the system will not include the address of the location alarm (refer to the *Table 46: Event-related messages*)
Local Message ON		When the event occurs, the system will play the event-related voice message on keypad speaker n. 1	
Local MessageOFF		When the event occurs, the system will not play the event-related voice message on keypad speaker n. 1	
Automatic Dialler		Refer to the *Table 46: Event-related messages*	
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 *paragraph 6-10 Telephone*).	
	Automatic SMS message	The dispatched SMS message will consist of the event description in the Events log	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.
	Enable SMS	When the event occurs, the control panel will send an SMS message to all the duly enabled telephone numbers (refer *paragraph 6-10 Telephone*)	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 E, 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 programme 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 sounderflashers) and press OK.

Note

If the output has the "ON afterRestoral" option enabled (refer to *paragraph 6-8 Outputs*) and it is programmed on event restoral, the output will deactivate when the event occurs.

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.

Note

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

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

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

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

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

Siren sound types (Applicable only when using Ness IVY Bus Sirens)

This section allows you to select the audible-visual signals emitted by the sounderflashers, 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 sounderflashers have been programmed in relation to a specific event, they will all emit the programmed tone when the event occurs. If a sounderflasher 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 OK to confirm.

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

Via PC

SMS message number/index

This option can be programmed solely via the SmartLeague software programme. This option is applies only when a Nexus device is installed and the "Automatic SMS" option is disabled. It determines which of the 50 available SMS messages will be sent (refer to *paragraph 6-29-3 Text for SMS messages*) when the event occurs.

Table 48: **Events - via SmartLeague software programme**

Option	Part of the system	Template/section
TelephoneNumbers	SmartLiving System - Events - select a single event	Programming
Message type		
Message A		
Message B		
Options		
Class code		
Event code		
Outputs		
Other outputs		Parameters settings - Other outputs
OtherOutputsProg	SmartLiving System - Events	Parameters settings - Outputs
SIA Codes	SmartLiving System - Events - select the event type	Programming - Digital Dialer
Siren sound types		SmartLiving System - Siren pattern
SMS message number/index		Parameters settings - Nexus

Programmable events 6-11-1

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 temporizers.

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 10100L panels.
- 20 temporizers
- 10 counters

Via PC

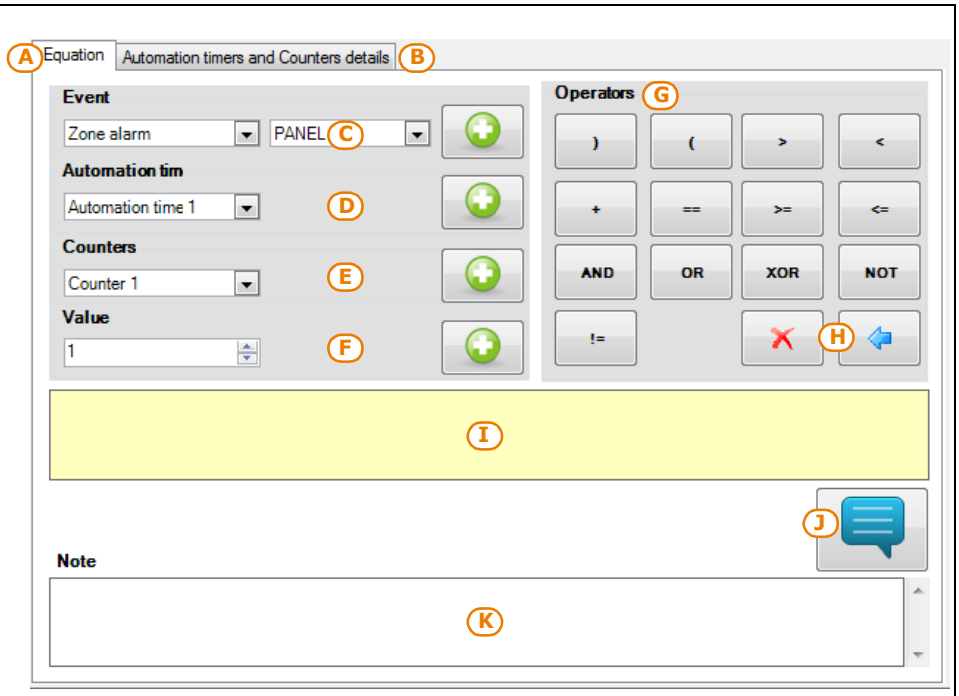
This programming process can be done only via the SmartLeague software programme. Select a programmable event from "SmartLiving System - Programmable event" from the tree menu on the left, then go to the "Parameters settings" template on the right.

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 49: **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	Keys for the inclusion of the logical operators in the expression.
H	Keys for the deletion of the entire expression or the last element of the expression.
I	Field for the visualization of the expression.
J	Key for the commutation of the visualization mode of the equation (parameters/ descriptions of parameters).
K	Field for the addition of eventual notes..



EQUATION

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):

TEMPORIZERS

A temporizer 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 temporizer you wish to include.

You can select up to four "Start events" (i.e. control panel events which trigger the temporizer) and up to four "Reset events" (i.e. control panel events which interrupt the temporizer). 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 temporizer will be "active":

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

Note

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

COUNTERS

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.

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.

Note

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

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.

EXAMPLES

If you wish to generate an alarm (i.e. activate sounderflashers and dialer calls) when only two PIRs (DET1 and DET2) go into alarm status within a pre-set time.
- T0000; temporizer 1 will activate when the "Zone alarm DET1" Start event activates for 30 seconds
- T0001; temporizer 2 will activate when the "Zone alarm DET2" Start event activates for 30 seconds
- Both conditions must occur together (AND)

T0000 AND T0001

- You must set the activation of the sounderflasher and dialer calls on a similarly-configured programmable event.
- If the programmable event activates an on-BUS sounderflasher, 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 temporizer 1 with the activation of the Start event of key 17 recognition
- T0000; temporizer 1 with a 40 second timeout, "temporizer active with delay" option enabled
- T0000; associate temporizer 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 sounderflasher, associate its deactivation with an event.

If you wish to receive a telephone call when a zone x, which belongs to partitions 1 and 2, is violated and one of the two partitions is armed
The automation zone x always generates the zone alarm event (even when the partitions are disarmed). However, the programmable event will occur only when the zone x is in alarm status and at least one of the two partitions is armed.
- Configure zone x as "automation" belonging to partitions 1 and 2
- Remove all the outputs and phone calls associated with the "Alarm zone x" event
- The programmable event must be programmed as "Alarm zone x" 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 telephone 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 telephone 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 telephone call you wish to receive and the output you wish to activate.

Timer 6-12

This programming section deals with the 10 system Timers.

It is possible to programme two "ON" times and two "OFF" times and up to 15 exceptions for each timer of the week.

A timer can be associated with a:
- P**artition** - if a partition is associated with a timer which controls automatic-arming operations (refer to *paragraph 5-4 Activations in the User's Manual)*, it will arm when the timer switches ON and disarm when the timer switches OFF.
- C**ode** - if a code is associated with a timer, it will be enabled to operate the system when the timer switches ON, and disabled when the timer switches OFF.
- K**ey -** if a key is associated with a timer, it will be enabled to operate the system when the timer switches ON, and disabled when the timer switches OFF.

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

Note

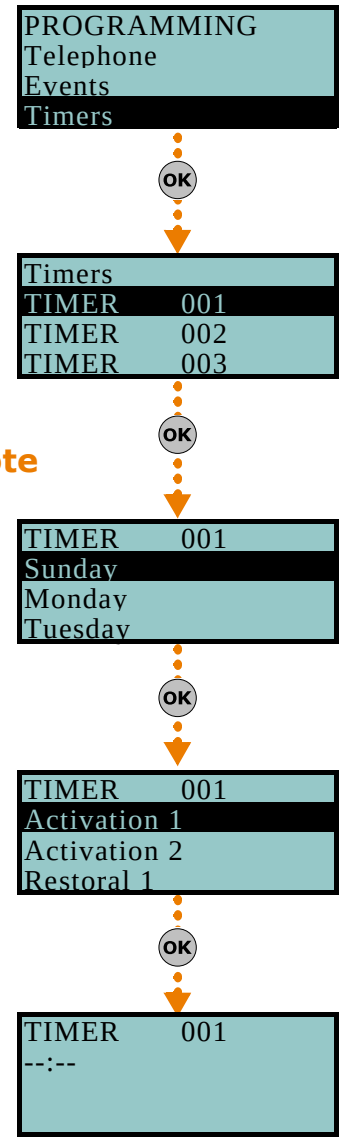
The timers must be enabled/disabled by the user *(refer to paragraph 5-4 Activations in the User's manual*).
On exiting the programming session (via keypad, computer or modem) all the timers will be enabled automatically. Therefore, if it will be necessary to disable the timers as required.

Via Keypad

1. Accessing the "Timers" section:

Type-in Code (Installer PIN) OK, PROGRAMMING Timers OK.

2. Use keys and to select the Timer thenpress OK.
3. Using the same keys, 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.



Note

It is also possible to programme timer activation or restoral only.
If you do not wish to programme the timer activation or restoral setting, enter "--:--" in the field you do not wish to program.

Via PC

Select an item from "SmartLiving System - Timers" from the tree menu on the left, then go to the "Parameters settings" template on the right:

The SmartLeague software programme allows you to set up 15 setting exceptions for each timer (for holiday periods, etc.). 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.

Note

The exceptions cannot be programmed via keypad.

Partitions 6-13

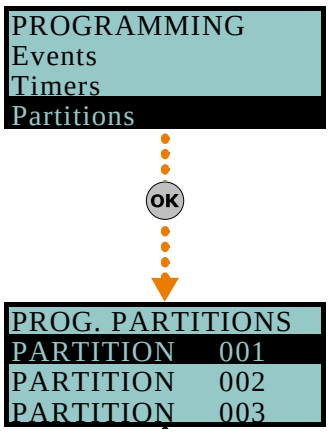
This programming section deals with the system Partitions and the respective options and parameters.

Via Keypad

1. Accessing the "Partitions" section:

Type-in Code (Installer PIN) OK, PROGRAMMING Partitions OK.

2. Use keys and to select the partition thenpress 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 opposite).
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 OK 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.

Note

Remember to enable auto-arm partition in the section:

User menu, Activations OK.

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.

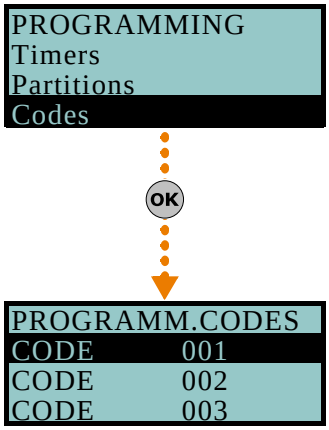
Via PC

Select an item from "SmartLiving System - Partitions" from the tree menu on the left, then go to the "Parameters settings" template on the right.

User Codes 6-14

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.



Via Keypad

1. Accessing the" Codes" section:

Type-in Code (Installer PIN) OK, PROGRAMMING Codes OK.

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

Description

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

Partitions

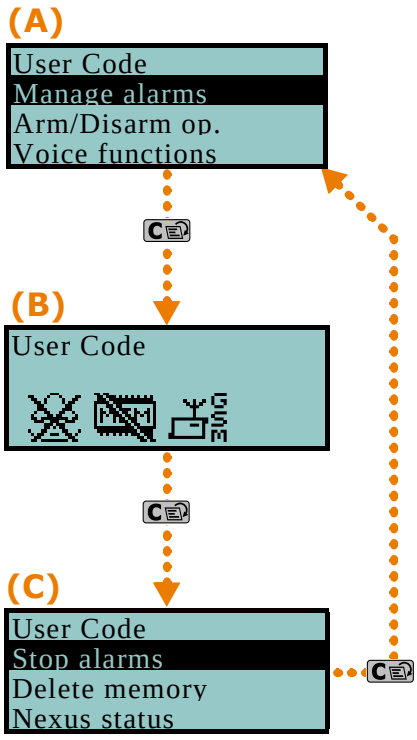
Select the partitions the user code is assigned to. Press , to enable the partition and to disable it.

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, if a code is configured as "Master" with "Partition filter" and is assigned to partitions 1, 3, 5 and 7, it will be able to enable/disable or change the PIN of a "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.

Case	Text menu	User menu	Description
A	Disabled	Enabled	Accesses 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. instead of the shortcut 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**"



Note

In all methods of access (A, B or C), the C key allows you to access/view the other cases via a circular buffer, 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.

Note

Set the "Loc.KpadMess Time" (refer to *paragraph 6-27 Other parameters*) to allow the system to play the messages associated with all the shortcuts assigned to number keys 0 ␣, ..., 9 wxyz.

- **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 telephone keypad, only the shortcuts associated with keys 0 to 9 can be used to:

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

Any other type of command will have no effect.

- **Patrol** - if enabled, the code will be able to disable the system for the pre-set "Patrol time".
- **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.
  A user code with this option enabled has access to its own menu only after pressing the OK key and PIN entry.

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 programme up to 10 shortcuts associated withkeys 0 ␣, ..., 9 wxyz. 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 OK.
2. Press OK then, using keys and , select from the "Type" list the shortcut you wish to associate with the function key.
3. Press OK 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, Outputs ON/OFF OK.

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 OK to confirm and exit.

It is possible to programme a certain number of outputs which can be activated or deactivated via keypad without entering a user code. For further details refer to *paragraph 6-28 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 (refer to *paragraph 1-6-2 User*).

Note

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

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".

Via PC

Select an item from "SmartLiving System - Users - Codes" from the tree menu on the left, then go to the "Parameters settings" template on the right.

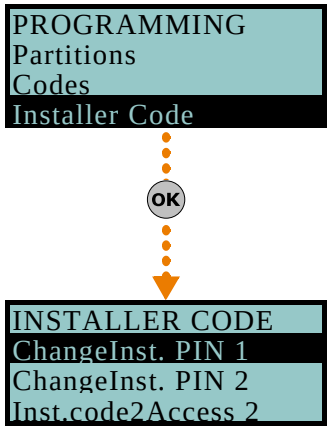
Installer codes

6-15

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

Via Keypad

Type-in a valid code (Installer) OK, PROGRAMMING Installer code OK.



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.code2Access 2

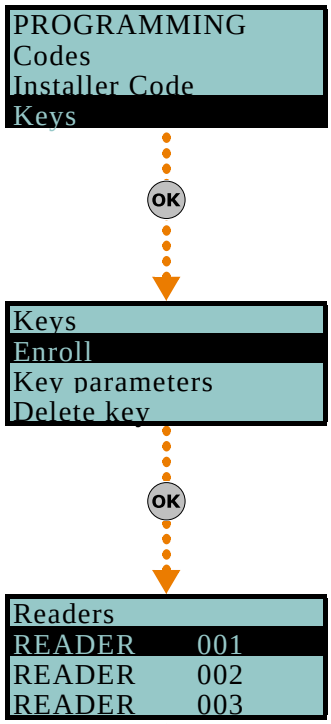
Use keys [*] and [#] to enable/disable the sections of the installer menu the secondary installer code can access.

In this section, the secondary installer code can access Inst.CodePIN2 section only.

Note

Keys 6-16

This section will allow you to programme the parameters of the digital keys and Air2-KF100 wireless keyfobs (for details regarding the wireless keyfobs, refer to the Air2-BS100 Transceiver Installation guide).



Via Keypad

Type-in Code (Installer PIN) [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-BS100, 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/S or nBy/X 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 contemporarily 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/S or nBy/X reader, the red LED will go On. The digital key description will go 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 50: **Key options**

Option	If enabled	If disabled	
Patrol	The digital key will be able to disarm specific partitions for patrol purposes.		
Maintenance	The digital key will be able to block alarm/tamper outputs for the time that it is held in front 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 Air2-KF100 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 programme 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/S or nBy/X reader, the LEDs will run through a series of visual signals with the following meanings:

LED indicator sequence		Option: Use keyShortcuts	
		enabled	**disabled**
1	Red LED On	Digital key shortcut F1	shortcut associated with the red LED on the reader
2	Blue LED On	Digital key shortcut F2	shortcut associated with the blue LED on the reader
3	Green LED On	Digital key shortcut F3	shortcut associated with the green LED on the reader
4	Yellow LED On	Digital key shortcut F4	shortcut associated with the yellow LED on the reader
5	All LEDs On	This sequence does not occur	Digital key shortcut F1
6	All LEDs Off	**Option: DisarmNotAllowed**	
		enabled	**disabled**
		No request to arm ALL the partitions common to both the key and reader.	Request to arm 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 [OK] 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 [OK] to confirm and exit.

Via PC

Select an item from "SmartLiving System - Users - Digital keys" from the tree menu on the left, then go to the "Parameters settings" template on the right.

Arming scenarios 6-17

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

Via Keypad

1. Access "Arming scenarios" section.

Type-in Code (Installer) [OK], PROGRAMMING Arming scenarios [OK].

2. Use keys and to select the scenario thenpress [OK].

Description

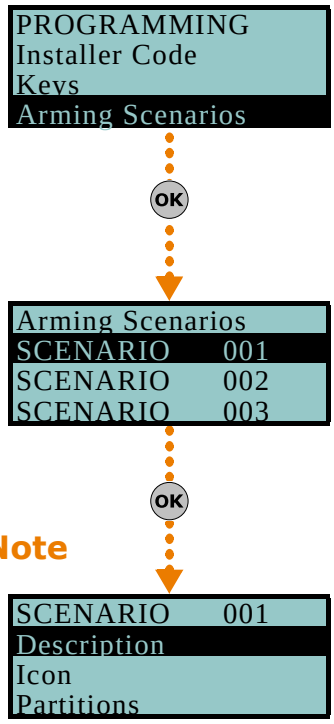
Editable field for the description of the scenario.

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 B, Shortcuts at default*):

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

The "Arm" shortcut associated with function key F1 Fn, ... , F4 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 OK.
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 OK.

Note

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 OK to confirm and exit.

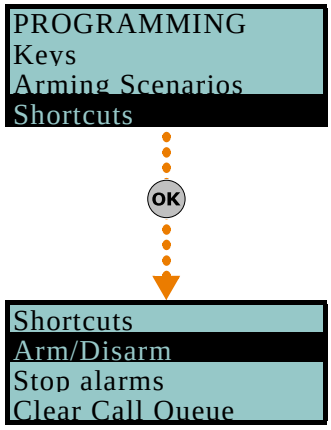
Via PC

Select an item from "SmartLiving System - Scenarios" from the tree menu on the left, then go to the "Parameters settings" template on the right.

Shortcuts 6-18

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

Via Keypad



1. Accessing the "Shortcuts" section:

Type-in Code (Installer PIN) OK, PROGRAMMING Shortcuts OK.

2. Use keys and to select the shortcut thenpress OK.

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 B, Shortcuts at default*):

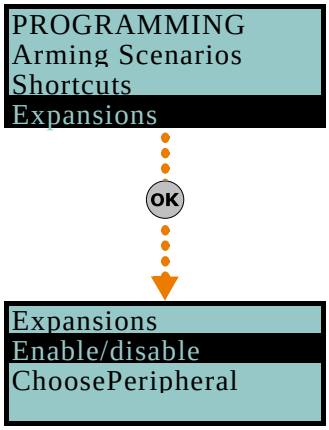
1. Use keys and to scroll across the digits of the number.
2. Use the number keys (1 ., etc.) to edit the number.
3. Press OK to confirm and exit.

Via PC

Select an item from "SmartLiving System - Shortcut icons" from the tree menu on the left, then go to the "Parameters settings" template on the right.

Expansions 6-19

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



Via Keypad

Type-in Code (Installer PIN) OK, PROGRAMMING Expansions 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 edit the description of each expansion board.

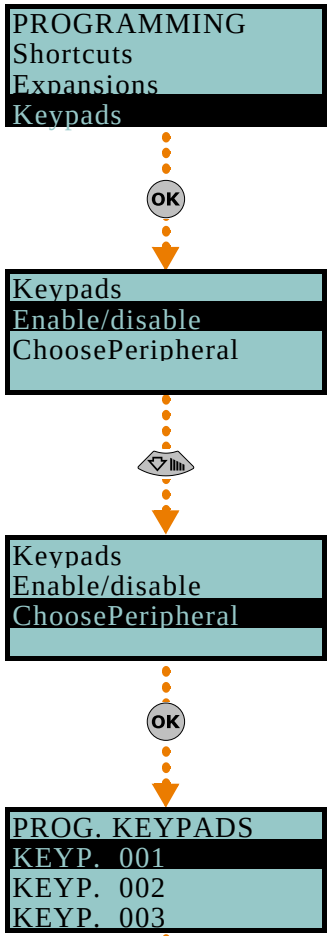
Via PC

Table 51: **Expansions - via SmartLeague software programme**

Option	Part of the system	Template/section
Enable/disable	/	Project
ChoosePeripheral	Expansions - select the expansion	Programming

Keypads 6-20

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



Via Keypad

Type-in Code (Installer PIN) 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 programme the various options of the selected keypad.

- **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** - (Temp available on Alien Keypads only). 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.
- **F1/4KeyShortcuts** - setting of the shortcuts assigned to keys F1 Fn, ..., F4 POU.
  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 B, Shortcuts at 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

Note

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".

  - •• **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 programme a certain number of outputs which can be activated or deactivated via keypad without entering a user code. For further details refer to *paragraph 6-28 Activating outputs without authentication*.

Via PC

Table 52: **Keypads - via SmartLeague software programme**

Option	Part of the system	Template/section
Enable/disable	/	Project
ChoosePeripheral	Keypads - select the keypad	Programming

You can programme the graphic interface of the Alien keypad solely through the SmartLeague software application.

Once you have selected the keypad from the system tree-structure on the left side of the window, you must then access the "Alien graphics" section which will appears only after selecting "Touch-screen keypad" as the type of keypad.

In order to programme the keypad with the configured parameters, you must connect your computer to the USB port of the keypad.

Readers 6-21

This section allows you to programme the reader options.

Via Keypad

Type-in Code (Installer PIN) OK, PROGRAMMING Readers OK.

Enable/disable

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

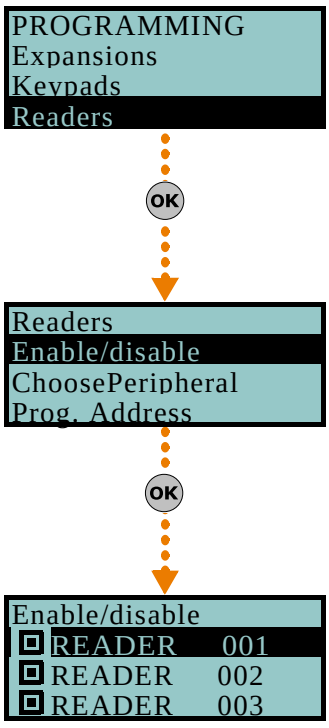
This is a reader simulated by the Air2-BS100, a "W" will be shown at the end of the description.

ChoosePeripheral

This section allows you to programme 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 outputs
  - Deactiv. outputs
  - Overtime
  - Teleservice req.
  - View faults



Prog. Address

This section allows you to activate the enrolling phase and programme the addresses of nBy/S and nBy/X readers.

Follow the instructions for addressing readers in *paragraph 3-3-5 Addressing nBy readers*.

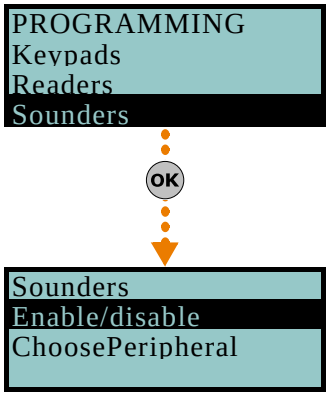
Via PC

Table 53: **Readers - via SmartLeague software programme**

Option	Part of the system	Template/section
Enable/disable	/	Project
ChoosePeripheral	Proximity readers - select the reader	Programming
Prog. Address	Proximity readers	Programming

Sounders 6-22

This section allows you to programme the parameters of the sounderflashers connected to the IBUS.



Via Keypad

Type-in Code (Installer PIN) OK, PROGRAMMING Sounders OK.

Enable/disable

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

ChoosePeripheral

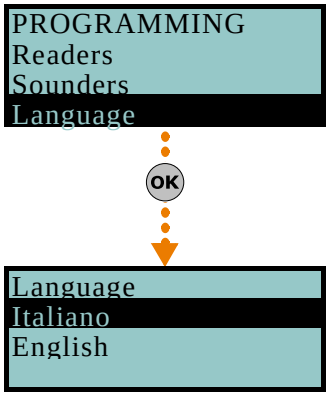
This section allows you to edit the description of each sounderflasher.

Via PC

Table 54: **Sounderflashers - via SmartLeague software programme**

Option	Part of the system	Template/section
Enable/disable	/	Project
ChoosePeripheral	Sounders - select the sounder/ flasher	Programming

Language 6-23



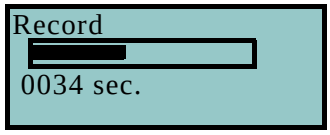
Via Keypad

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 ▲ e ▼ to select the desired language and OK to confirm.

Messages 6-24

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.



Via Keypad

1. Accessing the "Messages" section:

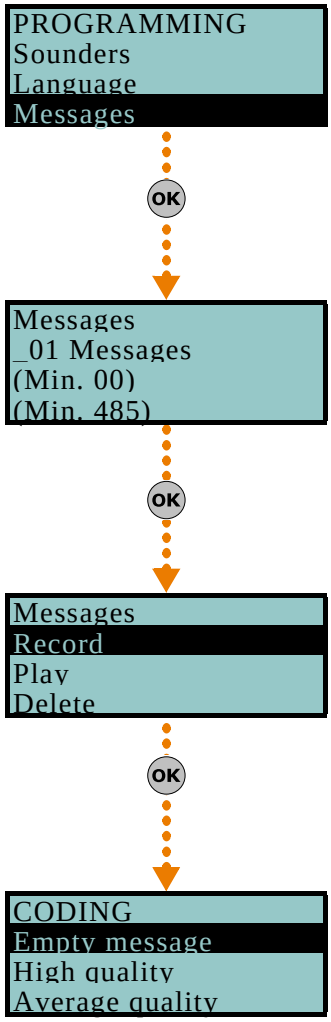
Type-in Code (Installer PIN) OK, PROGRAMMING Messages OK.

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 OK.
4. Use keys and to select the instructions for the selected message thenpress OK.



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.

Via PC

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

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

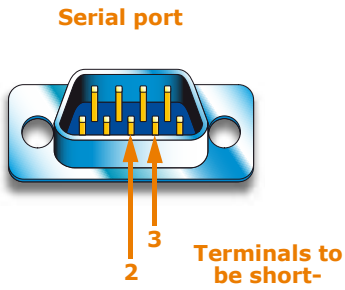
Select an item from "SmartLiving System - Announcements" from the tree menu on the left, then go to the "Parameters settings" template on the right and programme the selected message.

Default settings 6-25

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 and and battery power).
2. Short-circuit terminals "2" and "3" of the serial cable connector (refer to *Table 4: Control panels - description of parts, S*).
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.

Via Keypad

1. Access the "Default settings" section:

Type in Code (Installer) OK, PROGRAMMING Default settings OK.

2. Use keys and to select the function thenpress OK:

Factory data

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

This operations deletes all the previously programmed parameters.

ATTENTION!

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:

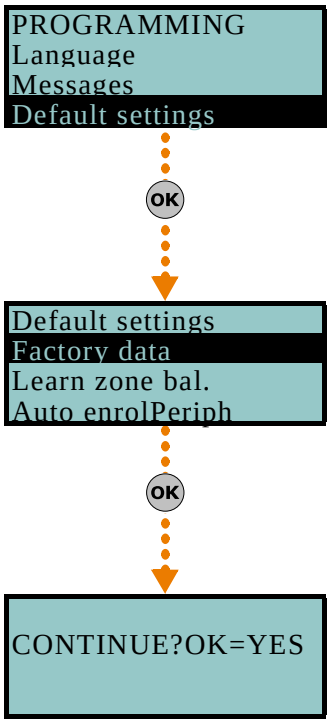
- Normally Open
- Normally Closed
- Balancing (Single balancing)
- Double balancing
- Rollerblind with EOL

The balancing settings which are not acquired accurately are:

- Rollerblind 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 that all the zones are in standby status
- Select 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 settings.



Auto enrol 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 protocol (refer to *Appendix A, Technical terminology and Glossary*).

CONT-ID enumer.

If you select this option, the control panel (after confirmation) will implement incremental numbering (from "1") in the "CCC" field of the CONTACT-ID protocol (refer to *Appendix A, Technical terminology and Glossary*) for the event relating 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 OK 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 OK key to delete all the data relating to the Air2-BS100 device.

Note

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

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

Via PC

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

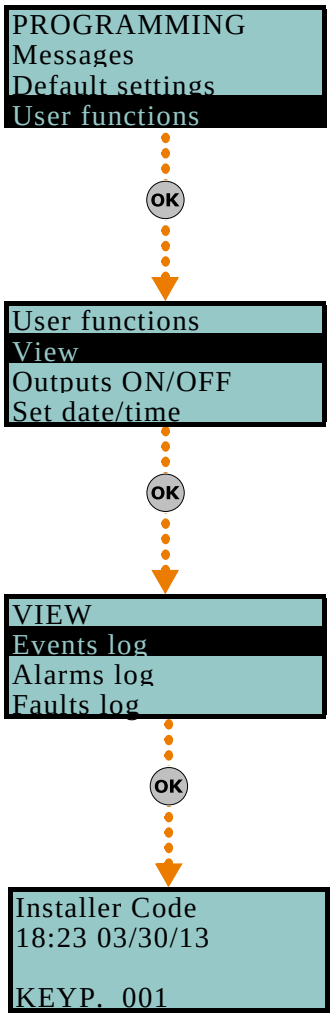
- digital dialer parameters
- "CCC" field of CONTACT-ID protocol of the zones
- phone calls on activation and restoral
- outputs on activation or restoral
- message playback on keypads on activation or restoral
- SIA protocol parameters

Table 55: **Factory default settings - via SmartLeague software programme**

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

User functions 6-26

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



Via Keypad

1. Access the "User functions" section:

Type-in Code (Installer) OK, PROGRAMMING User functions OK.

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

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:

  1° line: GSM network provider (Vodafone, etc.), on the left side and BUS connections on the right side of the string:

  - if nothing appears, it means that the Nexus/G is connected to the BUS
  - if the letter "**G**" appears, it means that the Nexus/G is connected to the BUS and that the GPRS service is available
  - if the letter "**C**" appears, it means that the Nexus/G is connected to the BUS and that a teleservice request (TCP connection) or SIA-IP event report is being sent
  - if "**--**" appears, it means that the Nexus is connected to the BUS

  2° line: GSM signal reception (value between 1 and 100)

  3° line: balance, at the last operation (expressed in the local currency)

  4° line: faults present - 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:

1° line: zone description

2° line: zone status ("Standby", "Alarm", "Short", "Tamper"), its activation status ("unbypassed" - capable of generating alarms, or "bypassed" - incapable of generating alarms)

3° 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

4° line: level of contamination present in the smoke detection chamber of Air2-FD100 smoke detector (%)

Note

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

- **Faults** - allows you to view any current 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 keys and to select the programming field you wish to change (hour, minutes, etc.).
2. Use keys and to make any changes in the selected field.
3. Press [OK] to save and exit.

Via PC

The SmartLeague software programme provides a section which, during a connection to a SmartLiving control panel, allows you to monitor the entire system in real time and access some of the above-mentioned parameters.

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

A window containing various sections will open. The sections can be selected by means of tags, each referring to a different part of the system.

Table 56: **User functions - via SmartLeague software programme**

Option	Part of the system	Section of the monitoring window	Template/section
View/Log	SmartLiving System - Events log		Programming
View/Nexus status		Peripheral details - Sounderflashers, isolators and Nexus	Nexus
View/System status		Remote keypad	Control panel status
		Power	Power supply parameters
View/Zone status		Zones	
View/Faults present		Remote keypad	Control panel status
View/Control panel version		Window heading	
Outputs ON/OFF		Zones	Outputs ON/OFF
Set date/time	SmartLiving System	SmartLiving System	Programming

Other parameters 6-27

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

Via Keypad

1. Access the "Other parameters" section.

Type-in Code (Installer PIN) [OK], PROGRAMMING Other parameters [OK].

2. Use keys and to select the parameter thenpress [OK]:

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 6-11 Events*).

Note

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

- **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 programme the delay, expressed in minutes (see "info" box), between mains failure and the "Mains failure" fault event signal.

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).

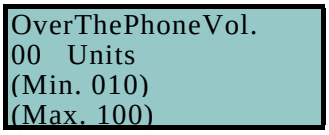
LocKpadMessTimes

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.

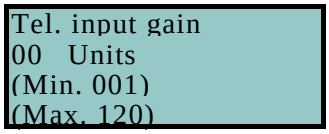
At default this value is set at 60. Accepted values: 1 to 120.

Wireless superv.

This value determines the wireless-detector supervision time. Once the pre-set time expires, the detectors which do not respond will be signaled as lost. Accepted values: 12 to 250 minutes.

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 are signaled.

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).

LinedownDelay

This parameter allows you to programme the delay, expressed in seconds, which will be applied before signaling of "LineDownDelay" events occurs.

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

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

or

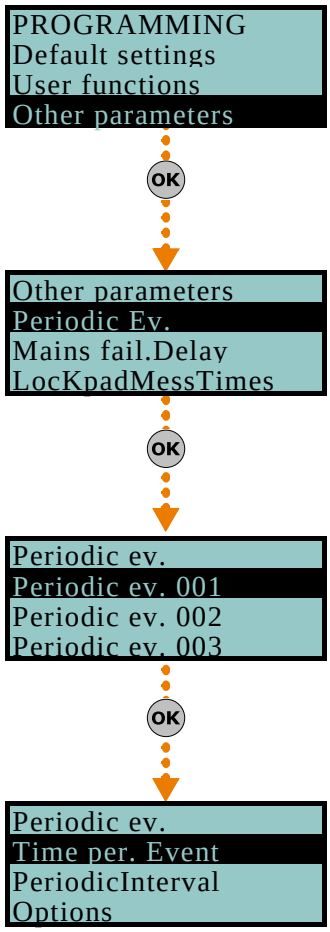
Use keys and to increase or decrease the number.

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
- Low battery
- Mains failure
- Tel. line down
- Jamming
- Low battery WLS
- WLS zone loss
- Nexus fault
- Detector dusty
- Zone faults
- Sounder faults
- Power faults
- LossTamp.ongoing
  The last item groups the following events:
  - Panel opened
  - Dislodged panel
  - Expansion tamper
  - Keypad tamper
  - Reader tamper
  - Sound.flash.Tamp
  - Nexus tamper
  - V-Monitor tamper
  - Expansion loss
  - Keypad loss
  - Reader loss
  - Sound.flash.Loss
  - Nexus loss
  - Scomp. V-Monitor
- IP conn. lost



4. Press [OK] to confirm and exit.

Serial number

Section for the visualization of the Control panel serial number.

Via PC

Table 57: **Other parameters - via SmartLeague software programme**

Option	Part of the system	Template/section
Periodic ev.	SmartLiving System	Parameters settings - periodic event
Mains fail.Delay		Parameters settings - I-BUS parameters
LocKpadMessTimes	Keypads	Parameters settings - Keypad parameters
OverThePhoneVol.	SmartLiving System	Parameters settings - Telephone options
Ring sensitivity	SmartLiving System - Telephone	Parameters settings - Telephone line parameters
Wireless superv.	SmartLiving System	Parameters settings - Control panel parameters
Tel. input gain		Parameters settings - Telephone options
LowBattery delay		Parameters settings - I-BUS parameters
LinedownDelay	SmartLiving System - Telephone	Parameters settings - Telephone dialer parameters
FaultForNotReady	SmartLiving System	Programming - Forced arming faults

Telephone line adjustment 6-27-1

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

- If the DTMF tones are not recognized or are recognized with difficulty, increase the "VolumeTel.In" parameter of the SmartLink by 1 or 2 notches over the medium value "M" then verify the effect. If there is no improvement, decrease the value of the "VolumeTel.In." parameter of the SmartLiving control panel until an acceptable combination is achieved.

Note

Any changes to the value of the SmartLink "VolumeTel.In." parameter come into effect almost 2 minutes after the setting change, therefore, you must allow this time to pass before verifying the effect.

Activating outputs without authentication

6-28

It is possible to programme a certain number of outputs that 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 Fn, ..., F4 BOT
- for Alien keypads, you must access the "Commands" section by pressing 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:

Via Keypad

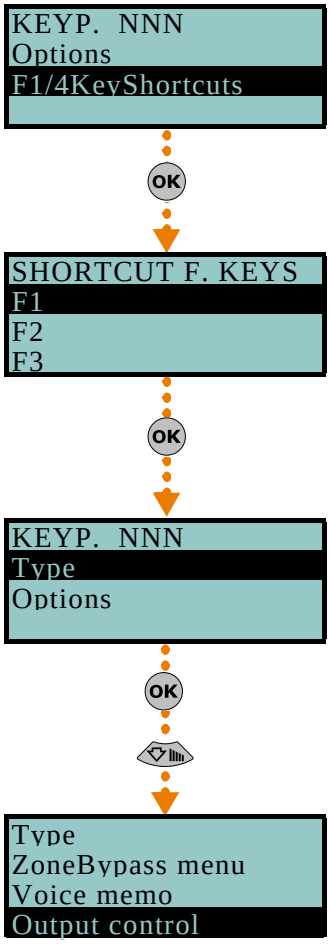
1. Access the section of the Installer menu for the programming of the "NNN" keypad you wish to associate with the outputs :

Type-in Code (Installer) OK, PROGRAMMING Keypads OK.

Select peripheral OK, Keypad "NNN" OK

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

Keypad number	User code number		
	505 / 515	1050 / 1050L	10100L
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



7. Access programming of the selected code, at the "Assigned outputs" section.
8. Use keys [*] and [#] to select the outputs from those available on the list.

Programming the Nexus 6-29

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" item from the SmartLiving system layout (on the left) and then go to the "Programming" section on the right to programme the relative parameters.

Note

Ness 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.

SMS Commands 6-29-1

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.

COMMAND USING SMS TEXT

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

<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

EXAMPLE

You wish the control panel to activate "Scenario 3", switch On the perimeter lights and confirm the operation via SMS text. For an operation of this type, proceed as follows:

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!

DEFAULT COMMANDS

The installer by modify the five predefined default commands:

- "**CREDIT**" for prepaid sims, 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 6-29-2

The "Programming - Caller ID commands" section will allow you to programme up to 200 telephone numbers and the commands which will be implemented when each telephone 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 6-29-3

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 6-11 Events*.

General parameters 6-29-4

In the "Programming - General parameters" section, it is possible to programme some functions relating to the management of the Nexus device, 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.

Note

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

GPRS Connections (Nexus/G only) 6-29-5

The Nexus/G allows you to use the GPRS connection for remote upload/download operations to/from control panels using the SmartLeague software application.

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

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

CONNECTION

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".
2. The "Start" button opens the GPRS connection status window, where you must the set 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.

TELESERVICE REQUEST FROM KEYPAD

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

The Nexus/G 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 58: **Nexus/G - Connection errors**

Access Codes	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

Access Codes	Error
025	GPRS disconnection error
027	GPRS connection error
028	Command error - connection not supported (the Nexus model in use is not GPRS capable)
030	Disconnected from remote
101	Error during TCP connection
102	
103	
104	Probable connection with a server different from the SmartLeague server
105	Problems with normal control panel operating capacity
106	Generic internal error
107	GPRS disconnection error

TELESERVICE REQUEST VIA SMS

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

<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.

Chapter 7

COMPLIANCY WITH THE REGULATIONS IN FORCE

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

- nBy/X readers must be equipped with devices which protect them against the forced-opening and dislodgement of their casings from their locations, in compliance with Level 2, as indicated in *paragraph 3-2-7 Installing nBy/X readers*.
- The Tamper NO dislodgement-tamper-protection device of the control panel must be installed.
- JOY, nCode and cCode keypads must be equipped with enabled tamper-protection devices, as indicated in *paragraph 3-3-2 Addressing the keypads*.
- FLEX5/U expansion boards must be either mounted inside the metal enclosure of the 1050L or 10100L control panel, or equipped with devices which protect them against the forced-opening of their casings and dislodgement from their locations, in compliance with Performance level 2.
- 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 (sounder 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).

CEI 79-2

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

- The following options must not be activated in the "Panel Options" section:
  - ReaderBuzzer OFF
  - BypassAlsoTamper
  - OpenZonesArmLock
  - 50131ReaderLedOFF
  - 50131StatHidden
  - 50131IconsHidden
  - 50131AlarDelayed
  - 50131WarnLedMem
- All of the "FaultsNotReady" options - from the "Other parameters" section - must be disabled.
- 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.

EN50131, GRADE 2

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

- 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.
- You must delete any programming relating to outdoor sounderflashers - from the respective alarm event in the "Outputs" section - for all zones with the "Fault Zone" attribute. You can programme indoor sounderflashers via the "Other outputs" option.
- The telephone dialer must be enabled.
- The system must include a self-powered sounderflasher for intrusion-alarm event signaling
- If you use a digital dialer or voice dialer with SmartLogos30M board for transmissions, a telephone 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.

EN50131-3, GRADE 3

Adhering to the following instructions guarantees compliance with 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
    - "NoArm IfNotReady": enable this option
- Use an ATS4 notification appliance:
  - protocol: SIA-IP with encryption
  - interface: SmartLAN/G or SmartLAN/SI

EN50131-6, GRADE 3

Adhering to the following instructions guarantees compliance with EN50131-6 Grade 3 (Power supplies):

- Remove the power supply unit (*Table 4: Control panels - description of parts, A*).
- Install an EN50131-6 Grade 3 certified power supply unit alongside the control panel enclosure. This power supply unit will provide the following output 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.
- Connect the NEGATIVE/GND pole of the power supply unit to a Negative terminal (Earth or GND, refer to *Table 5: Control panel - terminal board*).
- 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 programme the following parameters for each of the 3 terminals:
  - "Description": assign an explanatory description to the signal
  - "Fault zone": enable this option

ERRORS AND FAULTS

Faults detected by the control panel 8-1

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 (230 Vac) 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 "LowBatt. battery WLS" and "WLS zone loss" signaling, access the user menu, go to "View/Faults", press OK to view the list of devices involved.
Wireless detector not operative	WLS zone loss	At least one wireless detector is not operating	
Nexus GSM dialer faults	Nexus fault / Low signal	The GSM network signal is insufficient	Press OK 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 / ProviderUnavailable	The GSM network provider of the SIM in use is unavailable.	
	Nexus fault /GPRS conn. lost	NEXUS/G detects problems on GPRS network communications	
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: • 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 sounderflasher	Sounder faults / Horn fault	A defect/damage has been detected on the horn/sounder.	Press OK on "Sounder faults" to access the list of devices which have at least one fault present. Press OK on the selected sounderflasher to access the list of current faults on the device concerned.
	Sounderflasher faults / Low-Batt.Soundfl.	A low-voltage value has been detected on the sounderflasher 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.	
	Sounderflasher Faults / Battery resist.	An excessive internal resistance has been detected on the sounderflasher 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	Detector 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) 8-2

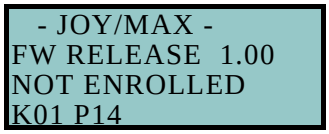
The control panel monitors the I-BUS continuously.

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. Keypad address and built-in reader address (Joy/MAX only)

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.

Note

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

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

LED activity 8-3

The blue and yellow LEDs on the control panel motherboard (refer to *Table 4: Control panels - description of parts, X*) may help in providing information regarding the proper operating capacity of the control panel firmware and I-BUS, as follows.

Blue LED

If the control panel is operating properly, the blue LED on the motherboard will blink rapidly. At the end of a programming session via PC, during restoral of factory default settings and during re-programming operations on the control panel and peripheral firmware, the LED may be either On solid or Off or the entire time. However, once the operation is complete it will start to blink again as previously described.

If the LED is On or Off permanently for no apparent reason (see above), it means that all the system functions are blocked.

Shut the system down and contact your dealer immediately.

Yellow LED

If the control panel is operating properly, the yellow LED on the motherboard should flicker. At the end of a programming session via PC, during restoral of factory default settings and during re-programming operations on the control panel and peripheral firmware, the LED may be either On solid or Off or the entire time. However, once the operation is complete it will start to blink again as previously described.

If the yellow LED is On or Off permanently, it means that there is trouble on the I-BUS.

If the LED is On or Off permanently for no apparent reason (see above), it means that the I-BUS is blocked. This condition is confirmed by the loss of communication with the keypads, readers and expansions.

Check the integrity of the I-BUS line.

Ring Sensitivity 8-4

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.

- Problem - 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. Answer - Increase the value of the "Ring Sensitivity" parameter to a suitable level.
- Problem - The control panel is enabled for "Answerphone" and "Teleservice" functions but picks up during "through" calls (calls that should not involve the control panel). Answer - Decrease the value of the "Ring Sensitivity" parameter to a suitable level.

Calibrating the touch-screen 8-5

If the touch screen of the Alien keypad does not respond to taps, you must carry out the forced calibration process.

You can start this process by pressing and holding for 7 seconds the (*Table 13: Alien - description of parts, X*) button which, for the Alien/G, can be reached on the PCB after opening its casing and, for the Alien/S, can be reached through the relative hole. Once the calibration process starts, simply follow the instructions provided by the keypad.

Appendix A

TECHNICAL TERMINOLOGY AND GLOSSARY

24 HOUR ZONE

Violation of a zone with this attribute will generate an instant alarm even when the partitions it belongs to are disabled. The system will generate the respective alarms which will be shown on the keypad.
These zones usually monitor conditions that are not directly connected to intrusion control. For example, Water tank overflow and flooding detectors are usually configured as 24H zones.
If you are installing a fire detector, please remember that the inputs of SmartLiving control panels are not compliant with EN 50131-1 and EN 50131-3.

ACCESS CODES

These are 4, 5 or 6 digit PINs which allow the building occupants (users) to access the system. Each code can be programmed to control specific functions only, and to operate the system to suit the requirements of the Main user.
Code types
- **Installer code**: used by the installer company technician
- **User code**: assigned to the building occupants

ALARM

Detection of non-authorized entry into the protected building. More specifically, activation of alarm signaling devices (detectors).

ALARM CYCLES

A parameter generally associated with zones. This value determines the number of alarm events a zone can generate before the partitions it belongs to disarm. This value (number of alarm events) resets to zero when the zone partitions re-arm or reset.
If a zone is allowed to generate an unlimited number of alarm events, it is classified as a "repetitive" zone.

ALARM OR TAMPER MEMORY

In the event of:
- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper (keypads, expansions, readers)
- peripheral loss (keypads, expansions, readers)
- false key

The red LEDs on the system keypads and readers go On each time one of the previously-mentioned events occur. This visual warning signal is held even after the event ends (alarm memory), in order to warn you that an event occurred during your absence. This visual warning signal will be held until you clear the event memory (refer to Delete Memory).

ALARM RECEIVING CENTRE (ARC)

This is a private service that monitors premises protected by intrusion control systems equipped with digital or voice dialers.
Alarm Receiving Centres receive alarm reports from monitored systems and take all the necessary actions to protect the occupants of the protected premises.

ANSWERPHONE

The "Answerphone" function, if enabled by the user, allows the control panel to answer incoming calls after a pre-set number of rings. The control panel will pick-up and play the recorded answer message.
During the call, the recipient can type-in a valid PIN (enabled for over-the-phone control) and access the authorized functions.

ARM/DISARM

User operations on one or more partitions. These generally indicate also the status of the partitions. Under normal circumstances, the zones of armed partitions can generate alarms. Under normal circumstances, the zones of disarmed partitions cannot generate alarms. The system generates tamper alarms even when partitions are disarmed.

AUTO-ARM

You can enable/disable the Auto-arm function on each separate partition.
If the auto-arm option is enabled on a timer-controlled partition, the partition will arm/disarm in accordance with the ON/OFF settings of the timer.

AUTO-BYPASSABLE ZONES

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.

AUTOMATION ZONE

These zones operate in the same way as 24h zones, but do not generate partition alarms or visual signals on the system reader and keypad LEDs.
Zones configured in this way can be used for automation applications.

BACKUP BATTERY

This is the secondary power source of the system. If primary (230 Vac) power failure occurs, the battery will take over.
SmartLiving control panels use sealed lead batteries. The battery housing determines the maximum size of the battery and therefore, its power-storage capacity. SmartLiving control panels provide housing for one battery @12V 7Ah. The control panel monitors the battery continuously and keeps it is under constant charge (from Mains).

BALANCING

Connection of a zone to a terminal configured as an input.
It is necessary to programme the balancing of each separate zone and wire the terminal accordingly. The SmartLiving intrusion control panel provides 6 different types of balancing, as follows:

- Normally Open
- Normally Closed
- EOL
- DEOL
- Double zones (only terminals with DOUBLING configuration)
- Double zones with EOL (only for terminals with DOUBLING configuration)

DEOL and customized zones can discriminate 4 conditions:

- Short-circuit
- standby
- alarm
- tamper

If you observe the Events list, you will see that there is an alarm event for each zone and a tamper event for each terminal. This is because a terminal configured as a double zone (or double zone with EOL) must be able to discriminate between alarm and standby conditions on each single zone, whereas tamper and short-circuit conditions involve the entire terminal and not the single zone.

BISTABLE OUTPUT

An output, that once activated, requires an explicit command to deactivate it.
Generally, bistable outputs are used to provide immediate signaling (in real-time) of specific events that occur on the system. For example, if the "Mains Failure" event is associated with a bistable output that is connected to a LED, the LED will signal the event immediately.

BYPASS - ZONE DEACTIVATION

A bypassed (disabled) zone cannot generate alarms. Each zone can be bypassed/unbypassed manually by the system users, or automatically by the control panel. Automatic bypass operations can take place only when the zone is configured as "Auto-bypassable" and the conditions that regulate auto-bypass operations are in effect (refer to Zone Attributes – Auto-bypassable).
Zone deactivation is useful when detectors are not working properly and you wish to avoid false alarms. Under normal circumstances, bypassed (disabled) zones can still generate tamper events. If you do not wish this to occur you must set the "Bypass Tamper" option on the control panel.

CALL QUEUE

A list of outgoing event-associated calls the control panel must send to programmed contact numbers.
Enabled users can clear the call queue manually.

CHIME ZONE

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. This function is widely used in commercial buildings (shops, etc.), and is generally associated with the zone that monitors the entrance to the premises in order to signal the arrival of customers.

COMMAND ZONE

Activation of a zone with this configuration generates the command it is assigned to.
SmartLiving control panels manage the following commands:

- **Disarm zone**: if activated, it will disarm all the partitions it belongs to. Zones configured in this way can be used to disarm partitions by means of a keyswitch.
- **Arm zone**: if activated, it will arm all the partitions it belongs to. For example, keyswitches are usually configured as command zones.
- **OnArm/OffDisarm zone**: if activated, it will generate an arm-partitions command and, the instant it restores to standby, a disarm-partitions command. The command will affect only the partitions the zone belongs to. Zones configured in this way can be used to arm/disarm partitions by means of a keyswitch.
- **Switch zone**: if activated when all the partitions it belongs to are disarmed, it will arm all the partitions. If activated when even one of the partitions it belongs to is armed, it will disarm all of its partitions. The command will affect only the partitions the zone belongs to. Zones configured in this way can be used to arm/disarm partitions by means of a keyswitch.
- **Patrol zone**: if activated, it will have a patrol function in all the partitions it belongs to.

CONTACT-ID

Telephone communication protocol (reporting format) for Alarm Receiving Centres using DTMF tones. Messages transmitted in this protocol contain information regarding the reported events, such as:

- user code ("account code"), the numeric identifier code of the caller
- class code, single digit numeric code that identifies the type of event
- event code, hexadecimal code comprising two characters that identify the event.
- "CCC", a 3 digit numeric code that identifies the device that generated the event

This information is assigned automatically by the control panel or, alternatively, each one can be programmed by the installer.

DEFAULT SETTINGS

A group of operating parameters set at the factory by the manufacturer. The purpose of these settings is to reduce the work of the installer during the installation phase.
The installer can restore the system to "Default Settings" if necessary.

DELAYED ENTRY ZONE

Violation of a zone with this configuration will not generate an alarm but will trigger the associated Timer (Entry time). If the user does not disarm the partition/s within the set "Entry time", the system will generate an alarm.
For example, the zone that monitors the main door of a building is usually configured as a Delayed Entry Zone, in order to give building occupants time to enter the building and disarm the partition without generating an alarm.

DELAYED EXIT ZONE

Violation of a zone with this configuration will not generate an alarm but will trigger the associated Timer (refer to Exit time).
For example, the zone that monitors the main door of a residence or building is usually configured as a delayed exit zone, in order to give occupants time to leave the partition after an arming operation. If the user does not leave the zone within the set "Exit time", the system will generate an alarm.

DELETE ALARM/ TAMPER/FAULT MEMORY

This is an explicit user-command which ends signaling on the red and yellow LEDs of keypad and readers for the following events:
- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper (keypads, expansions, readers)
- peripheral loss (keypads, expansions, readers)
- false key
- ongoing fault
- memory fault

If a user deletes the alarm/tamper memory, the visual signals on the reader/keypad LEDs will clear.
If the settings for norm. 50131 compliancy are active, the keypads may, in addition, require entry of a level 3 access code code (installer code) for the deletion of fault memories.

DIGITAL DIALER

This device allows the control panel to send report calls to Alarm Receiving centres (ARC).
SmartLiving control panels provide a built-in digital dialer which supports all the most widely used protocols.

DOUBLE ZONE

An electrical input point used for the management/supervision of signals coming from 2 intrusion detection devices.
The terminal the zone is connected to must be configured as a "double input zone". Terminals with this configuration allow the system to distinguish between two distinct alarms coming from the two different zones it is connected to.

ENTRY TIME (OR ENTRY DELAY)

The time (expressed in minutes or seconds) that the system allows the user to disarm the partition after zone violation. It the system is not disarmed within the set time it will generate an alarm.
Each partition can be programmed with its own Entry time.

EVENT

An operative status recognized by the system.
For example: detector alarm, mains failure, blown fuse, user-code recognition, etc., are all events recognized by the control panel.
Each event (e.g. mains failure) can be associated with an activation event (when the event occurs) and a restoral event (when the event ends).
Each event can be programmed to generate the following actions:
- activation of one or more outputs
- transmission of one or more e-mails
- send one or more SMS messages
- activation of one or more voice calls
- activation of one or more digital calls

For example, it is possible to activate output 3 when the event starts and to activate output 5 when it restores.

EVENTS LOG (OR EVENTS MEMORY)

This is the non-volatile portion of the memory the panels saves events to. The events are saved in chronological order with the following details:
- event description - with details regarding new events and restorals
- information regarding the user or the cause of event
- event location
- event date and time

The events log can be viewed by the system users and the installer.
Partition events (zone alarms, partition alarms, arm/disarm operations, recognized codes and keys, etc.) can be viewed by users with at least one partition in common with the event element.
For example, if a user arms several partitions from a keypad, the events log will show:
- description of the event - "Arm request"
- description of the code and partitions involved
- description (label) of the keypad involved
- date and time of the request

EXIT TIME (OR EXIT DELAY)

A short period (expressed in minutes or seconds) during which the user must disarm the partition after violation (for example, after opening the front door) otherwise the system will generate an alarm.
Each partition can be programmed with its own Exit time.

EXPANSION BOARDS

These boards can be used to increase the number of terminals (zones or outputs) and/or the size of the system (in order to extend it over a larger area). Expansion boards can be connected to the system via the I-BUS.

FAULT

A condition which indicates that a system component is not working properly.
Some faults can jeopardize the performance of the entire system. Mains failure (230V a.c.), telephone line-down and low battery are typical faults.

GENERIC ZONE

This type of zone usually comprises a motion detector which senses for the presence of movement in the protected partition. For example, PIRs, Double technology detectors, magnetic contacts on doors and windows.

GSM DIALER

A device which allows the control panel to make telephone calls over the GSM network and also allows users to interact with the control panel over-the-phone or by means of SMS text messages.

HOLD-UP ZONE (OR PANIC ZONE OR SILENT ZONE)

Activation of a zone with this configuration generates an immediate alarm even when the partition it belongs to is disarmed. The outputs and programmed calls will be activated, but the alarm will not be signaled on the red LEDs on the keypads and readers or on the keypad displays.
Under normal circumstances zones with this attribute are activated manually (using hidden buttons or similar devices) in situations of duress (armed robbery, etc.).

I-BUS

This is the two-way communication line (4 wires only) which connects the peripheral devices (keypads, readers, expansions, etc.) to the control panel.
The 4 easily identifiable wires, on the control panel motherboard and on the expansions, are:

- **"+"** power 12 Volt
- **"D"** data
- **"S"** data
- **"-"** Ground

I/O TERMINAL

A terminal configured as a Controlled Output (I/O, input-output) is capable of reading the status of the output.
This configuration can be used for creating automations, for example the condition of an alarm condition on "AND" zones:

- the single alarm events of two zones activate respectively an output terminal and an I/O terminal
- both the outputs are monostable, for example at 30 seconds
- the terminals are shorted

The input section of I/O terminals triggers the alarm actions (calls and sounderflashers), only when the two zones are both violated (AND) within the monostable time of the outputs.

INSTALLER CODE (ACCESS LEVEL 3)

The Installer code is generally a 4, 5 or 6 digit PIN that allows the installer to access the system Programming Menu either from a keypad or via the respective software programme, on condition that all the system partitions are disarmed.
In accordance with EN 50131 grade 3 security, the installer code is a level 3 access code.

INSTALLER MENU

List of system functions and respective parameters accessed via keypad.
This menu allows the installer to program, check and change nearly all of the system parameters. The installer menu can be accessed from any keypad after entry of a valid installer PIN, and on condition that all the system partitions are disarmed, or can be accessed via a computer equipped with the SmartLeague software.

INSTANT ZONE

Violation of a zone with this attribute will generate an immediate alarm (no delay).

INTERIOR ZONE

A zone that monitors the inside of the protected building.
For example, the interior zones of an office building are the zones that monitor offices and entrance points.
If a partition that a zone belongs to is armed in Stay mode, it will be unable to generate alarms.

KEY

A portable control device (card or keyfob) which allows the authorized user to access the system.
The key must be held in the vicinity of the reader in such a way to allow the system to read it and permit access to authorized operations.
Each key is programmed with:

- A random code selected from over 4 billion possible combinations.
- A label (usually the name of the user).
- The partitions it controls (arms, disarms, etc.).
- A group of pre-set parameters which allow the key user to operate the system in accordance with the authorized access level (for example, a key can be programmed to arm or disarm the system only at certain times of the day).

KEYPAD

This device allows users to access and control the system. Keypads can be connected to the system via the I-BUS.
The keypad allows users to access and control the partitions which are common to both the code and keypad in use. The user can arm/disarm partitions, view the status of the zones, stop visual and audible signaling devices.

MAGNETIC CONTACT

A generic magnetic-contact is a detector/sensor based on an magnet which, when placed near the sensor, provokes the mechanical closure of an electrical contact.

MAINTENANCE

If you wish to carry out maintenance work on the control without generating false alarms (tamper and intrusion), you must put the control panel in "Maintenance" mode. The control panel in must also be in "Maintenance" mode during the keypad and reader addressing process. The other functions of the control panel are still available (arm/disarm operations, events, calls, etc.).

MONOSTABLE OUTPUT

An output, that once activated, does not require an explicit command to deactivate it. This output must be programmed with a timeout (Monostable time expressed in seconds or minutes). Once activated, this output will remain active until the pre-set Monostable time expires.
Generally, monostable outputs are used to provide continuous signaling of the events they are associated with. For example, if the "Alarm Partition 1" event is associated with a monostable output with a 2 minute timeout, the output (sounder) will signal the event for 2 minutes then will deactivate automatically.

ONE-WAY WIRELESS SYSTEM

An advanced wireless-technology system in which the control panel and its devices are equipped with a transceiver module. If a detector senses an alarm condition, it will generate a number of event transmissions which under the right circumstances should reach the control panel.

OUTPUT

An electrical output point connected to a signaling or control device activated/deactivated by the control panel in response to programmed events.
The terminal the device is connected to must be configured as an "output".
Outputs are usually connected to audible or visual signaling devices but can be used for other purposes such as: switching on lights or opening doors/gates.

PANIC

Signaling that may be associated with a state of emergency perceived by the user and signaled to the intrusion control panel by means of a button or the activation of a shortcut.
This type of signaling generates an event which activates the programmed outputs and calls. This type of signaling does not activate the red LEDs on the keypads and readers nor is it visualized on the keypad displays.

PARTITION

A group of zones.
A partition identifies a group of zones that belong to a spatial or logical portion of the protected premises. For example, a partition may comprise all the zones that protect the downstairs partition of a house (spatial partition), or all the entrances of an office building (logical partition).

PARTITION ARM/ DISARM OPERATIONS

This refers to the status of a partition as requested by the user.
The user can carry out the following operations.

- **Disarm** - this operation disables the partition completely. In this way, none of the zones belonging to the partition can generate alarms.
- **Away mode** - this operation enables the interior and perimeter zones of the partition. In this way, all of the zones of the partition can generate alarms.
- **Stay mode -** this operation enables only the perimeter zones of the partition. In this way, only the perimeter zones of the partition can generate alarms.
- **Instant mode** - this operation enables the partition perimeter zones only and annuls delays. In this way, violation of the perimeter zones of the partition will generate instant alarms.
- **Hold** - this operation forces the partition to hold its current status.

PATROL

A periodic inspection of the protected premises carried out by authorized security staff.
Patrol staff can disarm each partition for the pre-set time only (programmable separately for each partition). The partitions concerned will rearm-as-before automatically when the pre-set time expires. Persons involved in periodic security inspections require codes with the "Patrol" attribute.
If the system receives a partition disarm command (generated by a code or key) while the patrol time is running, the "Patrol" function will be interrupted immediately. In this case, when the patrol time expires the partition will not be re-armed automatically and therefore will be disarmed.

PERIMETER ZONE

A zone that monitors the entrance points of the protected building.
Perimeter zones are usually direct entrance points such as doors and windows. For example, the front door of an apartment and windows that allow access from outside.

PERIODIC EVENT

Event whose activation occurs in accordance with a set time and date established during the event programming phase, are repeated with the programmed periodicity.
Several periodic events are available for use, of which the first can be activated forcibly by other events.

PERIPHERALS

Devices connected to the control panel via the I-BUS.
SmartLiving control panels manage the following peripherals:

- Keypads (Joy, nCode, cCode, Alien)
- Proximity Readers (nBy)
- Expansions (Flex5)
- Transceiver (Air2-BS100)
- Sounderflashers (Ivy)
- Isolators (IB100)
- GSM dialer (Nexus)

PRE-ARM TIME

The period (expressed in minutes) before an automatic arming operation.
For example, if a partition is set to arm automatically at 10:30 with a Pre-arm time of 5 minutes, all the partition keypads and readers will initiate an audible countdown at 10:25 in order to warn users of the forthcoming arming operation.
Each partition can be programmed with its own Pre-arm time.

PREMISES

The installation site.
Identifies the building or part protected by the intrusion control system, generally, a house or office.

PRIMARY POWER SOURCE

Under normal circumstances, the mains power supply (230Vac) 50 Hz (110V a.c. 60Hz in some countries).
Usually connected to a switching power supply or transformer (depending on the model) that provides the stabilized voltage to the system and the charge source to the batteries.

PROGRAMMABLE EVENT

Pulse events are events which are a combination of other control panel events based on logical operations, counters and temporizers.
For example, when it is necessary for more that one PIR detector to signal violation within a pre-set time in order to generate an alarm.

PULSE EVENTS

Spot events are events which restore automatically immediately after their activation. Some of the previously mentioned events are spot events.
For example, the "valid code" event activates as soon as the code is entered at the keypad, therefore, it is impossible to determine its restoral as it starts and ends instantly.
Pulse events (Spot events) can be programmed to activate:
- an output and calls when the event occurs
- an output when the event restores (only if the output has the option "ON afterRestoral" activated)

Under normal circumstances, spot events are assigned to monostable outputs (Refer to Monostable Outputs).

READER

This device allows users to access and control the system. The system readers are connected to the control panel via the I-BUS.
By means of the readers, each user can arm/disarm the partitions which are common to both the key and reader in use and can activate shortcuts (refer to Shortcuts) . The key (TAG) must be held in the vicinity of the reader in such a way to allow the system to read it and permit access to authorized operations. Although readers provide a more limited access to the system, they are easiest way of carrying out day-to-day operations (arm, disarm, etc.).

ROLLERBLIND ZONE

This type of zone comprises a sensor that detects any movement of the protected rollerblind.

ROUTE ZONE

Violation of a zone with this configuration will not generate an alarm during the pre-set Entry time (refer to Entry time).
For example, the zones that monitor the way to a command device (Keypad/Reader) are usually configured as Path Zones, in order to give building occupants time to enter the building, reach the command device (Keypad/Reader) and disarm the partition without generating an alarm.
Violation of a zone with this configuration will generate an instant alarm if the Entry time (Entry delay) has been revoked (as per Stay Mode).

RS485 BUS

4 wire two-way high-speed digital communication line with 4 pole twisted shielded cable.
The 4 wires, clearly identified on the terminals are:
"+" power 12 Volt
"**B**" data
"**A**" data
"-" Ground

SCENARIO

A pre-set arming configuration which applies various operating modes to the system partitions.
Following is an example of a pre-set scenario:
- Partition 1Disarm
- Partition 2Away arm
- Partition 3Stay arm
- Partition 4Hold
- Partition 5Disarm

SmartLiving control panels can be programmed (by the installer) with as many as 30 scenarios in accordance with user requirements.
The "Arm/disarm" shortcut must always be associated with one of the 30 available scenarios. When the system applies the selected scenario, the partitions will arm accordingly.

SHOCK ZONE

This type of zone usually comprises a shock detector (e.g Glassbreak detector) which senses for shock waves (vibration caused by hard blows).

SHORTCUTS

The shortcuts allow direct access to the user menu sections and various operations which normally require several steps inside the user menu.
For example, to activate/deactivate an output manually, you must:
- type in a user code
- access the User Menu
- access the option in the appropriate section (activate outputs)
- select the output
- activate/deactivate the selected output as required

Instead, the "Activate Output" and "Deactiv. Output" shortcuts allow you to activate/deactivate an output by simply pressing a single key or, if required for security reasons, after entering a user code.
The shortcuts can assigned to:
- keypads
- codes (entered at the keypad or via remote telephone)
- readers
- keys

Some shortcuts (for example, "Activate Outputs") require details before the system can implement them. These details (parameter, value, etc.) depend on the source of the shortcut command (keypad, code, reader, keys).
Refer to the details in the *Appendix B, Shortcuts at default* shortcuts list.

SMOKE DETECTORS

Optical smoke detectors are equipped with sampling chambers (based on light scattering mass - Tyndall effect). They are capable of sensing the presence of smoke particles and thus detecting a fire in its early stages.
These detectors have low power absorption during standby. The current absorption increases during alarm status and thus signals the danger of fire to the control panel.

SUPERVISED OUTPUT

An output that is monitored and therefore allows verification of its improper operating capacity (unsuccessful activation/deactivation).

SUPERVISION

The "supervision time" is the interval during which the wireless-system devices (in general wireless detectors in permanent placements) must signal to the control panel that they are operating in the network. If a wireless device fails to signal before the "supervision time" expires, it will be classified as "Lost" and the control panel will trigger a "peripheral-loss" fault event.

TAMPER

Detection of a serious condition that jeopardizes the operating capacity of the device concerned and thus puts the system at risk.
Tamper conditions are detected by tamper switches connected to the system zones, keypads, readers, expansions and control panel. Generally, these events are triggered by system violation such as unauthorized opening of a keypad cover.

TELEPHONE ACTIONS

These are calls sent to programmed contact numbers when specific events start and end (restoral).

TELESERVICE

This is a service provided by the installer company with the user's collaboration. The installer connects to the control panel over-the-phone or via a GPRS or Internet connection and, in this way, can check and/or change the control panel programming data.

TERMINAL

A screw terminal for the connection of zones (detection devices) and/or outputs (command/signaling devices).
The terminals (with some exceptions) of the control panel, keypads and expansion boards can be configured as:

- Input zone
- Double zone (ZONE DOUBLING)
- Output
- Supervised output
- Unused terminal

TEST ZONE

A zone with this attribute cannot generate alarms (activate audible and visual signaling devices). However, any alarm events that occur will be saved to the events memory.
The installer usually assigns the “test” attribute when the system is undergoing tests, in order to avoid false alarms. In this way, the installer can see if a zone is operating properly by simply referring to the events log.

TIMER

A logical entity for automatic time-management of programmed peripherals or elements.
SmartLiving control panels provide 10 timers.
Each timer can be programmed to manage:

- An activation time (ON Time) and a deactivation time (OFF Time) on preset days of the week and specific dates.
- 5 timer-slot exceptions. Each "exception" refers to a specific interval of one or more days, which can be programmed with an ON and OFF Time.

The timers can be used for different purposes:

- If a timer is associated with a partition, the system will arm and disarm the partition automatically in accordance with the On/Off settings of the timer.
- If a timer is associated with a code, the latter will be allowed to access the system only when the timer is On.
- If a timer is associated with a key, the latter will be allowed to access the system only when the timer is On.
- If the “Timer xxx” event is assigned to an output, the latter will activate/deactivate the connected device in accordance with the On/Off settings of the timer.

No matter how they are employed, the timers must always be enabled by the user.

TRANSCEIVER

Transceiver-equipped devices
In two-way wireless systems, all the devices are equipped with transceivers. In one-way wireless systems, the main unit is equipped with a receiver module whereas the peripheral devices are equipped with transmitters.

TWO-WAY WIRELESS SYSTEM

A wireless-technology system in which the control panel and its devices are equipped with a transmitter module and a receiver module.
These systems are more reliable than one-way wireless systems as each device transmission is validated by a reverse transmission.

UNBYPASSABLE ZONE

A zone with this attribute cannot be bypassed, manually (by the user) or automatically (by the control panel).
This attribute is usually assigned to high-security zones.

UNUSED TERMINAL

If a terminal is configured as an "unused" terminal, it will not be included in the terminal configuration (total sum of control panel terminals).
This ensures that any "Unused" terminals on the expansion boards and keypads are still available for use.

USER CODE

Each code is programmed with:

- A 4, 5 or 6 digit PIN which allows access the system.
- A label which identifies the user (usually the user's name).
- The group of partitions it controls (arms, disarms, etc.).
- A group of pre-set parameters which allow the operator to work on the system in accordance with its authorized access level (for example, a code can be enabled to consult the events log but not to change the date and time).
- A hierarchical level, that may allow the user to change to parameters of codes on a lower level in the system hierarchy.
  - User (the lowest level)
  - Manager
  - Master

USER MENU

List of functions available to the user after entry of a valid code at the keypad.

VIEWABLE DELAYED ZONE

This is a delayed entry and exit zone and does not generate alarms when violation occurs during the running entry/exit time, however, the violation will be signaled on the keypad.

VOICE DIALER

This device allows the control panel to send voice calls to programmed contact numbers.
In SmartLiving control panels the voice dialer function is provided by the SmartLogos30M board (accessory item).

VOICE MEMO

If the system is equipped with a SmartLogos30M voice board, all keypads with voice functions present in the system configuration will allow users to record memos. Messages can be recorded, played and deleted as required.

WIRELESS

An intrusion control system whose devices (detectors, keypads, keyfobs) communicate with the control panel over radio waves.
Usually, only the control panel of wireless-systems is mains powered (220Va.c.) while, the wireless devices are battery powered. The battery life is of utmost importance in the design layout and operational capacity of these systems.

ZONE

An electrical input point used for the management/supervision of signals coming from an intrusion detection device. The terminal the zone is connected to must be configured as an "input" zone.
Zones are usually connected to a single device, however, it is possible (if the zone is duly wired and configured) to connect more than one device. If a zone is connected to more than one device it is impossible to identify the alarm-trigger device in the event of an alarm.

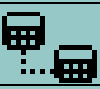
ZONE ALARM

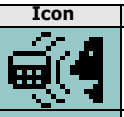
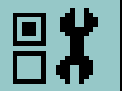
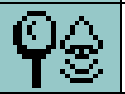
The conditions which generate a zone alarm, on the understanding that the zone belongs to several partitions, are as follows: the zone must detect violation and all the partitions it belongs to must be armed.
Zone alarms provoke activation of audible and visual signaling devices (sounders, flashers, reader/keypad LEDs, etc.) and generate voice and digital calls. Zone alarm events automatically generate partition alarm events on all the partitions the zone belongs to.
A violated zone will not generate alarms if:

- it belongs to several partitions and one of them is disarmed
- it is inhibited
- it is in test status (the event will be saved to the events log only)
- it an "interior" zone, and one of the partitions it belongs to is armed in Stay or Instant mode

Appendix B

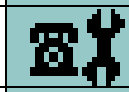
SHORTCUTS AT DEFAULT

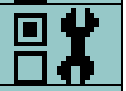
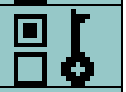
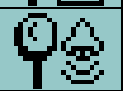
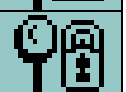
n.	Icon	description	function	parameter
1		**Arm/Disarm**	Applies a pre-set scenario	which scenario
2		**Stop alarms**	Immediately deactivates the outputs relative to zone/partition alarm and tamper events and system tamper events.	
3		**Clear call queue**	Cancels the entire call queue and stops ongoing calls (if any).	
4		**Delete memory**	Carries out a "Stop alarms" operation and, at the same time, deletes memory of system and partition alarm and tamper events.	
5		**Activate outputs**	Activates one of the programmed outputs.	Output
6		**Deactiv. outputs**	Deactivates one of the programmed outputs.	Output
7		**Overtime**	Delays auto-arming time of partitions 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 eavesdropping over-the-phone by means of a microphone located on suitably placed keypad.	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**	Provides voice information regarding the armed/disarmed status of the 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.answer-phone**	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

AVAILABLE ICONS

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

Icon number	Icon
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	

Icon number	Icon
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	

Icon number	Icon
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	

Appendix D

VOICE MESSAGES

The SmartLogos30M voice board provides 500 voice message slots, 291 of which are pre-recorded at factory. 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 messages)	271 (for all 100 messages)
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
Shortcuts	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
Shortcuts	230	Date/Time settings	2.5	4
	231	View faults	2.5	4
Not available	232 - 240	"		
Generic messages	241	Restoral	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
None 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 user-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 fault	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 flasher 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	Initialize programming		
	481	Ongoing call		
	482	Failed to send message		
	483	Output fault		
	484	Low GSM credit		
Not available	485	"		
Voice memo slots	486 – 500	"	37.5 (for all 15 messages)	60 (for all 15 messages)

Appendix E

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
1	Panel T1	Panel T1	Panel T1	Panel T1
2	Panel T2	Panel T2	Panel T2	Panel T2
3	Panel T3	Panel T3	Panel T3	Panel T3
4	Panel T4	Panel T4	Panel T4	Panel T4
5	Panel T5	Panel T5	Panel T5	Panel T5
6			Panel T6	Panel T6
7			Panel T7	Panel T7
8			Panel T8	Panel T8
9			Panel T9	Panel T9
10			Panel T10	Panel T10
11	Exp. 1 T1	Exp. 1 T1	Exp. 1 T1	Exp. 1 T1
12	Exp. 1 T2	Exp. 1 T2	Exp. 1 T2	Exp. 1 T2
13	Exp. 1 T3	Exp. 1 T3	Exp. 1 T3	Exp. 1 T3
14	Exp. 1 T4	Exp. 1 T4	Exp. 1 T4	Exp. 1 T4
15	Exp. 1 T5	Exp. 1 T5	Exp. 1 T5	Exp. 1 T5
16	Exp. 2 T1	Exp. 2 T1	Exp. 2 T1	Exp. 2 T1
17	Exp. 2 T2	Exp. 2 T2	Exp. 2 T2	Exp. 2 T2
18	Exp. 2 T3	Exp. 2 T3	Exp. 2 T3	Exp. 2 T3
19	Exp. 2 T4	Exp. 2 T4	Exp. 2 T4	Exp. 2 T4
20	Exp. 2 T5	Exp. 2 T5	Exp. 2 T5	Exp. 2 T5
21	Exp. 3 T1	Exp. 3 T1	Exp. 3 T1	Exp. 3 T1
22	Exp. 3 T2	Exp. 3 T2	Exp. 3 T2	Exp. 3 T2
23	Exp. 3 T3	Exp. 3 T3	Exp. 3 T3	Exp. 3 T3
24	Exp. 3 T4	Exp. 3 T4	Exp. 3 T4	Exp. 3 T4
25	Exp. 3 T5	Exp. 3 T5	Exp. 3 T5	Exp. 3 T5
26	Exp. 4 T1	Exp. 4 T1	Exp. 4 T1	Exp. 4 T1
27	Exp. 4 T2	Exp. 4 T2	Exp. 4 T2	Exp. 4 T2
28	Exp. 4 T3	Exp. 4 T3	Exp. 4 T3	Exp. 4 T3
29	Exp. 4 T4	Exp. 4 T4	Exp. 4 T4	Exp. 4 T4
30	Exp. 4 T5	Exp. 4 T5	Exp. 4 T5	Exp. 4 T5
31	Keyp. 1 T1	Exp. 5 T1	Exp. 5 T1	Exp. 5 T1
32	Keyp. 1 T2	Exp. 5 T2	Exp. 5 T2	Exp. 5 T2
33	Keyp. 2 T1	Exp. 5 T3	Exp. 5 T3	Exp. 5 T3
34	Keyp. 2 T2	Exp. 5 T4	Exp. 5 T4	Exp. 5 T4
35	Keyp. 3 T1	Exp. 5 T5	Exp. 5 T5	Exp. 5 T5
36	Keyp. 3 T2	Exp. 6 T1	Exp. 6 T1	Exp. 6 T1
37	Keyp. 4 T1	Exp. 6 T2	Exp. 6 T2	Exp. 6 T2
38	Keyp. 4 T2	Exp. 6 T3	Exp. 6 T3	Exp. 6 T3
39	Keyp. 5 T1	Exp. 6 T4	Exp. 6 T4	Exp. 6 T4
40	Keyp. 5 T2	Exp. 6 T5	Exp. 6 T5	Exp. 6 T5
41		Exp. 7 T1	Exp. 7 T1	Exp. 7 T1
42		Exp. 7 T2	Exp. 7 T2	Exp. 7 T2
43		Exp. 7 T3	Exp. 7 T3	Exp. 7 T3
44		Exp. 7 T4	Exp. 7 T4	Exp. 7 T4
45		Exp. 7 T5	Exp. 7 T5	Exp. 7 T5
46		Exp. 8 T1	Exp. 8 T1	Exp. 8 T1
47		Exp. 8 T2	Exp. 8 T2	Exp. 8 T2
48		Exp. 8 T3	Exp. 8 T3	Exp. 8 T3
49		Exp. 8 T4	Exp. 8 T4	Exp. 8 T4
50		Exp. 8 T5	Exp. 8 T5	Exp. 8 T5
51		Exp. 9 T1	Exp. 9 T1	Exp. 9 T1
52		Exp. 9 T2	Exp. 9 T2	Exp. 9 T2
53		Exp. 9 T3	Exp. 9 T3	Exp. 9 T3
54		Exp. 9 T4	Exp. 9 T4	Exp. 9 T4
55		Exp. 9 T5	Exp. 9 T5	Exp. 9 T5
56		Exp. 10 T1	Exp. 10 T1	Exp. 10 T1
57		Exp. 10 T2	Exp. 10 T2	Exp. 10 T2
58		Exp. 10 T3	Exp. 10 T3	Exp. 10 T3
59		Exp. 10 T4	Exp. 10 T4	Exp. 10 T4
60		Exp. 10 T5	Exp. 10 T5	Exp. 10 T5

n.	SLiving 515	SLiving 1050	SLiving 10100
61	Keyp. 1 T1	Exp. 11 T1	Exp. 11 T1
62	Keyp. 1 T2	Exp. 11 T2	Exp. 11 T2
63	Keyp. 2 T1	Exp. 11 T3	Exp. 11 T3
64	Keyp. 2 T2	Exp. 11 T4	Exp. 11 T4
65	Keyp. 3 T1	Exp. 11 T5	Exp. 11 T5
66	Keyp. 3 T2	Exp. 12 T1	Exp. 12 T1
67	Keyp. 4 T1	Exp. 12 T2	Exp. 12 T2
68	Keyp. 4 T2	Exp. 12 T3	Exp. 12 T3
69	Keyp. 5 T1	Exp. 12 T4	Exp. 12 T4
70	Keyp. 5 T2	Exp. 12 T5	Exp. 12 T5
71		Exp. 13 T1	Exp. 13 T1
72		Exp. 13 T2	Exp. 13 T2
73		Exp. 13 T3	Exp. 13 T3
74		Exp. 13 T4	Exp. 13 T4
75		Exp. 13 T5	Exp. 13 T5
76		Exp. 14 T1	Exp. 14 T1
77		Exp. 14 T2	Exp. 14 T2
78		Exp. 14 T3	Exp. 14 T3
79		Exp. 14 T4	Exp. 14 T4
80		Exp. 14 T5	Exp. 14 T5
81		Exp. 15 T1	Exp. 15 T1
82		Exp. 15 T2	Exp. 15 T2
83		Exp. 15 T3	Exp. 15 T3
84		Exp. 15 T4	Exp. 15 T4
85		Exp. 15 T5	Exp. 15 T5
86		Exp. 16 T1	Exp. 16 T1
87		Exp. 16 T2	Exp. 16 T2
88		Exp. 16 T3	Exp. 16 T3
89		Exp. 16 T4	Exp. 16 T4
90		Exp. 16 T5	Exp. 16 T5
91		Exp. 17 T1	Exp. 17 T1
92		Exp. 17 T2	Exp. 17 T2
93		Exp. 17 T3	Exp. 17 T3
94		Exp. 17 T4	Exp. 17 T4
95		Exp. 17 T5	Exp. 17 T5
96		Exp. 18 T1	Exp. 18 T1
97		Exp. 18 T2	Exp. 18 T2
98		Exp. 18 T3	Exp. 18 T3
99		Exp. 18 T4	Exp. 18 T4
100		Exp. 18 T5	Exp. 18 T5
101		Exp. 19 T1	Exp. 19 T1
102		Exp. 19 T2	Exp. 19 T2
103		Exp. 19 T3	Exp. 19 T3
104		Exp. 19 T4	Exp. 19 T4
105		Exp. 19 T5	Exp. 19 T5
106		Exp. 20 T1	Exp. 20 T1
107		Exp. 20 T2	Exp. 20 T2
108		Exp. 20 T3	Exp. 20 T3
109		Exp. 20 T4	Exp. 20 T4
110		Exp. 20 T5	Exp. 20 T5
111		Keyp. 1 T1	Exp. 21 T1
112		Keyp. 1 T2	Exp. 21 T2
113		Keyp. 2 T1	Exp. 21 T3
114		Keyp. 2 T2	Exp. 21 T4
115		Keyp. 3 T1	Exp. 21 T5
116		Keyp. 3 T2	Exp. 22 T1
117		Keyp. 4 T1	Exp. 22 T2
118		Keyp. 4 T2	Exp. 22 T3
119		Keyp. 5 T1	Exp. 22 T4
120		Keyp. 5 T2	Exp. 22 T5

n.	SLiving 1050	SLiving 10100
121	Keyp. 6 T1	Exp. 23 T1
122	Keyp. 6 T2	Exp. 23 T2
123	Keyp. 7 T1	Exp. 23 T3
124	Keyp. 7 T2	Exp. 23 T4
125	Keyp. 8 T1	Exp. 23 T5
126	Keyp. 8 T2	Exp. 24 T1
127	Keyp. 9 T1	Exp. 24 T2
128	Keyp. 9 T2	Exp. 24 T3
129	Keyp. 10 T1	Exp. 24 T4
130	Keyp. 10 T2	Exp. 24 T5
131		Exp. 25 T1
132		Exp. 25 T2
133		Exp. 25 T3
134		Exp. 25 T4
135		Exp. 25 T5
136		Exp. 26 T1
137		Exp. 26 T2
138		Exp. 26 T3
139		Exp. 26 T4
140		Exp. 26 T5
141		Exp. 27 T1
142		Exp. 27 T2
143		Exp. 27 T3
144		Exp. 27 T4
145		Exp. 27 T5
146		Exp. 28 T1
147		Exp. 28 T2
148		Exp. 28 T3
149		Exp. 28 T4
150		Exp. 28 T5
151		Exp. 29 T1
152		Exp. 29 T2
153		Exp. 29 T3
154		Exp. 29 T4
155		Exp. 29 T5
156		Exp. 30 T1
157		Exp. 30 T2
158		Exp. 30 T3
159		Exp. 30 T4
160		Exp. 30 T5
161		Exp. 31 T1
162		Exp. 31 T2
163		Exp. 31 T3
164		Exp. 31 T4
165		Exp. 31 T5
166		Exp. 32 T1
167		Exp. 32 T2
168		Exp. 32 T3
169		Exp. 32 T4
170		Exp. 32 T5
171		Exp. 33 T1
172		Exp. 33 T2
173		Exp. 33 T3
174		Exp. 33 T4
175		Exp. 33 T5
176		Exp. 34 T1
177		Exp. 34 T2
178		Exp. 34 T3
179		Exp. 34 T4
180		Exp. 34 T5

n.	SLiving 10100
181	Exp. 35 T1
182	Exp. 35 T2
183	Exp. 35 T3
184	Exp. 35 T4
185	Exp. 35 T5
186	Exp. 36 T1
187	Exp. 36 T2
188	Exp. 36 T3
189	Exp. 36 T4
190	Exp. 36 T5
191	Exp. 37 T1
192	Exp. 37 T2
193	Exp. 37 T3
194	Exp. 37 T4
195	Exp. 37 T5
196	Exp. 38 T1
197	Exp. 38 T2
198	Exp. 38 T3
199	Exp. 38 T4
200	Exp. 38 T5
201	Exp. 39 T1
202	Exp. 39 T2
203	Exp. 39 T3
204	Exp. 39 T4
205	Exp. 39 T5
206	Exp. 40 T1
207	Exp. 40 T2
208	Exp. 40 T3
209	Exp. 40 T4
210	Exp. 40 T5
211	Keyp. 1 T1
212	Keyp. 1 T2
213	Keyp. 2 T1
214	Keyp. 2 T2
215	Keyp. 3 T1
216	Keyp. 3 T2
217	Keyp. 4 T1
218	Keyp. 4 T2
219	Keyp. 5 T1
220	Keyp. 5 T2
221	Keyp. 6 T1
222	Keyp. 6 T2
223	Keyp. 7 T1
224	Keyp. 7 T2
225	Keyp. 8 T1
226	Keyp. 8 T2
227	Keyp. 9 T1
228	Keyp. 9 T2
229	Keyp. 10 T1
230	Keyp. 10 T2
231	Keyp. 11 T1
232	Keyp. 11 T2
233	Keyp. 12 T1
234	Keyp. 12 T2
235	Keyp. 13 T1
236	Keyp. 13 T2
237	Keyp. 14 T1
238	Keyp. 14 T2
239	Keyp. 15 T1
240	Keyp. 15 T2

Appendix F

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 sounderflashers on the BUS.

Table 59: **Output typology**

Symbol/Initials	Description
TM	Output on terminal/Relay/OC1/OC2 - monostable
TB	Output on terminal/Relay/OC1/OC2 - bistable
SM	Sounderflasher output with limited flasher time
SB	Sounderflasher output with unlimited flasher time

Table 60: **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 sounderflasher after expiry of the monostable time applied to the main output, you must: • 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: • 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 61: **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 Sounderflasher 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 G

SIA CODES

SIA Codes		Event type
Event activation	Event restoral	
BA	**BR**	Burglary alarm
BB	**BU**	Burglary bypass
BT	**BR**	Burglary trouble
BV	**BR**	Burglary verified
CA	**OA**	Automatic closing
CL	**OP**	Closing report
CP	**OA**	Automatic closing
DO	**DR**	Access open
FA	**FR**	Fire alarm
FB	**FU**	Fire bypass
FI	**FK**	Fire test begin
FT	**FJ**	Fire trouble
GA	**GH**	Gas alarm
GB	**GU**	Gas bypass
GT	**GJ**	Gas trouble
HA	**HR**	Hold-up alarm
HB	**HU**	Hold-up bypass
HT	**HJ**	Hold-up trouble
KA	**KR**	Heat alarm
KB	**KU**	Heat bypass
KT	**KJ**	Heat trouble
LT	**LR**	Phone line
MA	**MR**	Medical alarm
MB	**MU**	Medical bypass
MT	**MJ**	Medical trouble
NL	**OP**	Perimeter armed
OT	**OJ**	Late to close
PA	**PR**	Panic alarm
PB	**PU**	Panic bypass
PT	**PJ**	Panic trouble
QA	**QR**	Emergency alarm
QB	**QU**	Emergency bypass
QT	**QJ**	Emergency trouble
SA	**SR**	Sprinkler alarm
SB	**SU**	Sprinkler bypass
ST	**SJ**	Sprinkler trouble

SIA Codes		Event type
Event activation	Event restoral	
TA	**TR**	Tamper alarm
TB	**TU**	Tamper bypass
UA	**UR**	Untyped zone alarm
UB	**UU**	Untyped zone bypass
UT	**UR**	Untyped zone trouble
WB	**WU**	Water bypass
WT	**WJ**	Water trouble
ZB	**ZU**	Freeze bypass
ZT	**ZJ**	Freeze trouble
UX	**UX**	Undefined
CF	**OP**	Forced closing
NF	**NF**	Forced perimeter
BC	**UX**	Burglary cancel
CE	**UX**	Closing extend
JP	**UX**	User on premises
YC	**YK**	Communication fail
MA	**MH**	Medical alarm
RB	**UX**	Remote program begin
YP	**YQ**	Power supply trouble
YT	**YR**	System battery trouble
ET	**ER**	Expansion trouble
XT	**XR**	TX battery trouble
LB	**LX**	Local program
DD	**DR**	Access denied
RP	**UX**	Automatic test
JL	**UX**	Log threshold
AT	**AR**	AC trouble
JR	**JS**	Schedule executed
YI	**YS**	Overcurrent trouble
EM	**EN**	Expansion device missing
YK	**UX**	Communications restoral
OU	**OV**	Output state trouble
CI	**UX**	Fail to close