



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



sol

Anti-intrusion control panels and security systems



GameOver

User's manual

inim
ELECTRONICS

Warranty

INIM Electronics s.r.l. (Seller, Our, Us) warrants the original purchaser that this product shall be free from defects in materials and workmanship under normal use for a period of 24 months. As INIM Electronics s.r.l. does not install this product directly, and due to the possibility that it may be used with other equipment not approved by Us; INIM Electronics s.r.l. does not warrant against loss of quality, degradation of performance of this product or actual damage that results from the use of products, parts or other replaceable items (such as consumables) that are neither made nor recommended by INIM Electronics. Seller obligation and liability under this warranty is expressly limited to repairing or replacing, at Seller's option, any product not meeting the specifications. In no event shall INIM Electronics s.r.l. be liable to the purchaser or any other person for any loss or damage whether direct or indirect or consequential or incidental, including without limitation, any damages for lost profits, stolen goods, or claims by any other party caused by defective products or otherwise arising from the incorrect or otherwise improper installation or use of this product.

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover damage arising from improper maintenance or negligence, damage caused by fire, flood, wind or lightning, vandalism, fair wear and tear.

INIM Electronics s.r.l. shall, at its option, repair or replace any defective products. Improper use, that is, use for purposes other than those mentioned in this manual will void the warranty. Contact Our authorized dealer, or visit our website for further information regarding this warranty.

Limited warranty

INIM Electronics s.r.l. shall not be liable to the purchaser or any other person for damage arising from improper storage, handling or use of this product.

Installation of this Product must be carried out by qualified persons appointed by INIM Electronics. Installation of this Product must be carried out in accordance with Our instructions in the product manual.

Directive 2014/53/EU

Hereby, INIM Electronics s.r.l., declares that the following devices are in compliance with the essential requirements and other relevant provisions of Directive 2014/53/UE:

Sol030S, Sol030G, Sol030P, all Air2 devices and variants

All the devices mentioned here above can be used in all EU countries without restrictions.

Documents for the users

Declarations of Performance, Declarations of Conformity and Certificates concerning to INIM Electronics S.r.l. products may be downloaded free of charge from the web address www.inim.biz, getting access to Extended Access and then selecting "Certifications" or requested to the e-mail address info@inim.biz or requested by ordinary mail to the address shown in this manual.

Manuals may be downloaded free of charge from the web address www.inim.biz, getting access to Extended Access and then selecting "Manuals".

Leading-edge systems (DM37/08)

The devices described in this manual, depending on the settings selected during the installation phase and the implementation of the concepts illustrated in this guide, allow you to create an Intrusion Detection and Hold-up Alarm System (I & HAS) compliant with EN 50131-1:2006 + A1: 2009, safety grade 3 (at highest) and an alarm transmission system (ATS) compliant with EN 50136-1: 2012 in category ATS6 (at highest SP6 or DP4).

The devices described are compliant with European standards EN 50131-3: 2009 (in reference to control and indicating equipment - CIE), EN 50131-6: 2008 + A1: 2014 (in reference to power supplies - PS), EN 50131- 10: 2014 and EN 50136-2: 2013 (in reference to transceivers on supervised sites - SPT).

As a support to the design, planning, operation, installation, commissioning and maintenance of intrusion alarm systems installed in buildings, the following regulatory documents should be consulted: CEI 79-3 and CEI CLC / TS 50131-7.

Depending on the State where the components described are installed, certified compliance with local laws and regulations may be required.

Copyright

The information contained in this document is the sole property of INIM Electronics s.r.l. No part may be copied without written authorization from INIM Electronics s.r.l.

All rights reserved.

Table of contents

Warranty	2
Limited warranty	2
Directive 2014/53/EU	2
Documents for the users	2
Leading-edge systems (DM37/08)	2
Copyright.	2
Table of contents	3
About this manual.	5
0-1 Terminology	5
0-2 Graphic conventions.	5
Chapter 1 General information	6
1-1 Manufacturer's details	6
1-2 Description of products.	6
Chapter 2 The Sol system.	7
2	7
2-1 Telephone functions.	8
2-2 Voice functions	8
2-3 AlienMobile Application	8
2-4 Inim Cloud	9
2-5 Versatility of the Sol system	9
Chapter 3 Sol User	10
3-1 User Codes	10
3-2 Access to user menu	10
3-3 Multi-system access.	11
Chapter 4 Shortcuts.	12
4-1 Keypad shortcuts.	14
4-2 Shortcut with code.	15
4-3 Key and Reader shortcuts	15
4-4 Shortcut on event	16
Chapter 5 Control panel signalling	17
5-1 LED signalling	17
5-2 Signalling on the Buzzer	18
Chapter 6 Using the Sol system	19
6-1 Managing alarms	19
6-2 Arming and disarming partitions	20
6-3 Arming scenarios.	21
6-4 Voice memo	21
6-5 Activations	21
6-6 Outputs management.	22
6-7 Change code PIN	22
6-8 Change telephone numbers.	22
6-9 Connection to a LAN/Wi-Fi network	23

6-10	Overtime request	23
6-11	Listen-in	23
6-12	Partition status enquiry	23
Chapter 7	Using the keypads	24
7-1	Keypad displays	26
7-2	Using the keys	28
7-3	Operations from LCD keypads	29
7-4	Operations via touch-screen keypad	36
7-5	Alarm clock and memo	41
Chapter 8	Readers and Keys	42
8-1	Proximity readers	42
8-2	Keys	43
8-3	Reader and key operations	44
Chapter 9	Commands over-the-phone	46
9-1	Use of telephone calls	46
9-2	Use of SMS text messages	46
9-3	Operations via telephone	47
Chapter 10	Graphic maps	49
Appendix A	Glossary	51
Appendix B	Fault signals	57
	WEEE	59

About this manual

DCMUINEOSOLE **MANUAL CODE**
 1.00 **REVISION**
USER'S MANUAL

This manual contains instructions relating to the user interface of the Sol control panel, its functions and use.

This manual is supplied with every control panel and must be given to the end-user for consultation. It is the duty of the installer to ensure that the end-user fully understands how the system works and is aware of the configuration set by the installer.

Terminology

0-1

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

**CONTROL PANEL,
SYSTEM, DEVICE**

Refer to the directions as perceived by the operator when directly in front of the mounted device or computer screen.

**LEFT, RIGHT,
BEHIND, ABOVE,
BELOW**

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

The following images represent the display of a control panel with an LCD screen and relative signalling. For other types of displays, it is necessary to refer exclusively to the notifications which are shown and not to the image shown:



The detached notes contain important information about the text.

Note

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

ATTENTION!

Chapter 1

General information

1-1

Manufacturer's details

Manufacturer: INIM ELECTRONICS s.r.l
 Production plant: Centobuchi, via Dei Lavoratori 10
 63076, Montepandone (AP), Italy
 Tel.: +39 0735 705007
 Fax: +39 0735 704912
 e-mail: info@inim.biz
 Web: www.inim.biz

The persons authorized by the manufacturer to repair or replace the parts of this system have authorization to work on INIM Electronics brand devices only.

1-2

Description of products

DESCRIPTION

anti-intrusion control panel

MODELS AND FUNCTIONS

Table 1-1: Sole control panels - functions

Control panels	Sol-S	Sol-G	Sol-P
Graphic display	/	Built-in LCD (192x64)	Built-in touchscreen (4.3", 480x272, 65.000 colours)
Keypad	/	Built-in, touch keys	/
Proximity reader	Yes	Yes	Yes
Signalling LEDs	7	4	4
Microphone	No	Yes	Yes
Buzzer/Speaker	No	Yes	Yes
Sounder-flasher	Yes	Yes	Yes
Brightness sensor	No	Yes	Yes
Tamper protection	Yes	Yes	Yes
Wireless management (Air2)	Yes	Yes	Yes
Voice functions	Optional (with Smartlogos30M board)		
Telephone functions	Optional (with Sol-PSTN module)		
Connectivity via LAN	Optional (with Sol-LAN module)		
Wireless Connectivity	Optional (with Sol-WIFI board)		
GSM Connectivity	Optional (with Sol-3G module)		

APPLICABLE STANDARDS

EN 50131-1:2006 + A1:2009,
 EN 50131-3:2009,
 EN 50131-6:2008 + A1:2014,
 EN 50131-10:2014,
 EN 50136-1:2012,
 EN 50136-2:2013,
 EN 50130-4:2011 + A1:2014,
 EN 50130-5:2011,
 CEB T031:2014-12 (ed.1)

SECURITY RATING

2

ATS CATEGORIES

up to SP6 or DP4 (in accordance with configurations)

The Sol system

Chapter 2

A typical Sol system comprises:

- a Sol control panel
- wireless intrusion-detection devices (PIR or microwave detectors, magnetic contacts, linear beam detectors, etc.)
- system control peripherals: proximity readers, wireless keypads
- alarm signalling devices and, generally, the events detected by the system (wireless sounders, visual-audible signalling devices, etc.)

Some Sol control panel models are equipped with an integrated keypad or graphic display on the frontplate:

- Sol-G models have a touch-screen keypad and an LCD screen
- Sol-P models have a 4.3" colour touch-screen display

Besides the keypad and display, the system can also be managed by proximity readers which provide a fast, easy-to-use interface for the most frequently used daily operations, such as arming/disarming operations. Authorized electronic key users can operate the system in accordance with the functions they are enabled to control by holding the key in front of the proximity key reader.

Table 2-1: Control panels - description of parts

A	Graphic display
B	Keypad
C	Signalling LEDs
D	Microphone
E	Proximity reader
F	Buzzer/ Speaker
G	Sounder-flasher
H	Brightness sensor

The diagram illustrates three models of the Sol control panel: Sol-P (top), Sol-P (bottom left), and Sol-S (bottom right). Each panel is annotated with callouts A through H, corresponding to the legend table. Sol-P panels feature a large green graphic display (A) and a keypad (B). Sol-S panels feature a proximity reader (E) and a buzzer/speaker (F). All panels include signalling LEDs (C), a microphone (D), and a sounder-flasher (G). A brightness sensor (H) is also present on the Sol-P models.

All models of the control panel manage a wireless system for the deployment of wireless and remote-control devices.

Sol control panels are capable of managing numerous events (not only alarms, but also faults, tamper, code/key identification, arm/disarm events) in response to which it is possible to activate audible/visual signalling or messages (voice, phone calls, SMS text or e-mail messages with attachments or push notifications).

The Sol also provides home-automation functions, such as programmed arm/disarm operations, access control, output activation/deactivation.

2-1 Telephone functions

For each of the events recognized by the Sol control panel, it is possible to activate report calls to Alarm receiving Centres (via digital dialer), as well as voice calls and SMS messages to specific contact numbers.

By calling the Sol control panel or on receiving a call from it (via voice dialer), it is possible to enter a valid code PIN and activate shortcut commands and customized automatic functions.

The shortcuts can be activated via keys "0" to "9" on the telephone keypad after recognition of the code PIN. Each code can be programmed with customized shortcuts, such as: arm, disarm, activate/deactivate outputs, delete alarm memory, etc.

If the system is equipped with a SmartLogos30M voice board, the code shortcuts assigned to keys "0" to "9" will be announced over-the-phone, in order to facilitate operations.

Additionally, it is possible to activate the Listen-in function that will allow you to listen to the sounds picked up by the control panel microphone.

When a user requests an operation, via a correctly formatted SMS message or voice call to the SIM card of the GSM communicator, the control panel will activate the respective shortcut and send confirmation (feedback) of the successfully implemented command.

2-2 Voice functions

If the Sol control panel is equipped with a SmartLogos30M voice board, you will be able to take advantage of all the voice functions provided by the control panel and telephone.

Your installer will program the voice messages you require:

- for event-associated calls
- on the control panel in correspondence to events

Additionally, every control panel with voice functions has its own voice memo-box for the recording and playback of a message by users. This handy function allows you to leave messages for other users who have access to the keypad; refer to *paragraph 6-4 Voice memo*. You can record, play and delete messages at your own discretion.

The presence of a new memo in the memo-box will be indicated on the blue LED on the keypad, as described in *Table 5-1: Frontplate LEDs*.

The SmartLogos30M voice board provides a total of 60 seconds for voice messages.

2-3 AlienMobile Application



INIM Electronics now offers Sol control panel users the Alien Mobile application for Smartphones and Android or Apple tablets, in two different versions:

- **AlienMobile** - free App with basic functions
- **AlienMobile+** - purchasable App with advanced functions

The application can be downloaded from an on-line application store (Play store or Apple app store).

The user, via Smartphone or tablet, can monitor Sol panels by means of an interface similar to the one described in this manual for the touch-screen keypad.

It is the installer's task to prepare the control panel for direct connection to the devices which use the AlienMobile application and to configure the application for use with the system to be monitored and, finally, to provide end-users with all the necessary access data.

For instructions regarding use and access to the system via AlienMobile, refer to the application manual.

Inim Cloud

2-4

The INIM Electronics Cloud service provides Sol system users with a further method of intrusion panel management via Internet.

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

Programming operations relating to network are not required on Sol control panels, as they are programmed at default with the DHCP enabled (option that permits the automatic assignment of IP addresses to the devices in the network).

In order to allow use of the Cloud service, the user must have their own account at www.inimcloud.com, registered as "user".

After login, the user will have access to a customized web interface which provides all the tools required for supervision of all the control panels registered by the user.

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



Table 2-2: Inim cloud - home page

A	Button for the selection of one of the registered control panels and description of the selected control panel.	
B	Buttons for access to the sections relating to the selected control panel	
C	Description of the main user and supervisor. The symbol indicates Cloud ownership.	
D	Buttons for quick viewing	
E	Buttons for user profile management	
F	Section for the display of all the ongoing alarms and alarm memories	
G	Text section relating to the button pressed	

Present at all times in the upper right corner are the buttons for viewing and editing the profile of the user and control panel registered to the cloud. The upgrading of the status of each control panel can be achieved by clicking-on and unblocking the relative icon.

In order to use the Inim Cloud services, registration must be carried out also by the user.

For registration of an installation and use of the Cloud service refer to the Inim Cloud user manual.

Versatility of the Sol system

2-5

Sol control panels, in addition to the typical functions offered by anti-intrusion systems, also provide users with accessory functions which do not necessarily involve the purpose of anti-intrusion, such functions provide for the use of devices alternative to those available.

For instance, it is possible to schedule the ON/Off times of lights; access control functions; Arm and Disarm operations via buttons and also program actions that follow a logical sequence of events/situations and much more.

Therefore, the manufacturer suggests that you contact your installer and request the possibility to evaluate the feasibility of these options

Chapter 3

Sol User

3-1 User Codes

Each User Code comprises a PIN for identification purposes and a group of parameters which determine its rank in the system code hierarchy and the operations the user is entitled to perform.

The PIN is made up of 4, 5 or 6 digits that the user must enter in order to allow identification.

The PIN of the user code enabled at default is "0001". The PINs of the successive user codes are "0002", "0003" etc., up to "0050".

Note

For security reasons all the system default codes must be changed. The installer must provide each of the system users with a code PIN that must be changed immediately to a code PIN of their choice.

Each user code has the following parameters, to be programmed by the installer or by other user codes of hierarchically superior level.

- **Partitions** - user codes can control only the partitions they are assigned to. If a user code is entered at a keypad, the user can control only the partitions which are common to both the code and keypad concerned. For example, if a code enabled on partitions 1, 2 and 3 is entered at a keypad which enabled on partitions 2, 3 and 4, it will be able to operate on partitions 2 and 3 only.
- **User type**
Each code can be assigned a specific level in the system hierarchy:
 - User
 - Manager
 - Master

Each code, in accordance with its assigned level in the system-hierarchy (the "User" being the lowest level), is capable of carrying out the following operations on all other codes that are hierarchically inferior:

 - enable/disable
 - change PIN
 - change several programming parameters
- **The commands over the phone.**
This option enables access to the system via remote telephone. If this option is enabled, the User can send commands to the control panel over-the-phone. Commands can be sent during calls to/from the control panel. After a valid PIN entry on the telephone keypad the user can activate specific shortcuts (refer to *paragraph 4-2 Shortcut with code*). This method of entering commands will affect the code partitions only.
- **Timer restriction on codes**
If a code is associated with one of the timers, it will be able to operate the system only when the timer is On.
- **Group of outputs which can be activated/deactivated manually**
After accessing the Outputs ON/OFF section (user menu) you can activate/deactivate the duly programmed outputs.

3-2 Access to user menu

In order for code users to access their user menus, they must first validate their codes. This can be done by typing-in the code PIN and pressing the **OK** button.





If the installer has enabled the "Fixed length" option on a user code, the user must first press the **OK** button and then type-in their PIN. **FIXED LENGTH**

At this point, there are 3 different methods that allow first access to the user menu, depending on how the system has been programmed, as follows:

The user accesses the user menu directly:

- Alarm management
- Arm/Disarm operations
- Voice functions
- Activations
- View
- Outputs ON/OFF
- Set date/time
- Keypad settings
- Change PIN
- TelephoneNumbers
- Settings
- Overtime request
- Codes
- Timers

The user can select the desired option from the menu by means of buttons  and  and by pressing the **OK** button.

Multi-system access

3-3

Users can access several systems using the same code/key/remote-control device. The user code, key or remote-control device must be enrolled separately on the control panels concerned, and can be programmed with different attributes and functions in accordance with the requirements of each specific system.

The keys and codes provide the systems with random codes (for keys) or PINs (for codes) which the system associates with the respective attributes and functions programmed by the installer. For example, a user key/code may be enabled on partitions 1 and 2 on system A, on partitions 3, 4 and 5 on system B and on partitions 4 and 5 on system C.

This operating method is possible for all keys and codes.

Chapter 4

Shortcuts

The shortcuts are control panel functions which, in a single operation, provide a fast way of carrying out specific operations which would normally require a series of activations.




















They can be divided into three categories:

- immediate command shortcuts, which activate functions instantly
- service shortcuts, that provide direct access to Sol system data
- direct access shortcuts, that provide direct access to sections of the user menu on the keypad

They can be activated by the user or by the occurrence (activation) of an event.

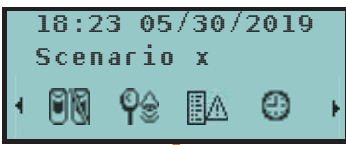
The method of activation of a shortcut depends on the device being used (keypad with LCD display, code typed-in at a keypad or remotely via telephone, reader, key or wireless key) and the category it belongs to.

Shortcut			on keypad			on code		on reader	on keys	on event
description	function	parameter	n.	Icon	String	via keypad	over-the-phone			
Arm/Disarm	Applies a pre-set scenario	which scenario	1		Arm/Disarm	Available	Available	Available	Available	Available Activate scenario
Stop alarms	Shortcut that deactivates instantly the outputs relative to alarm and tamper events and deletes the partition and system alarm and tamper memories.		2		Stop alarms	Available	Available	Available	Available	Not available
Clear call queue	Cancels the entire call queue and stops ongoing calls (if any).		3		Clear call queue	Available	Available	Available	Available	Not available
Delete memory	Deletes memory of system and partition alarm and tamper events.		4		Delete memory	Available	Available	Available	Available	Available
Activate output	Activates one of the programmed outputs.	which output	5		Activ. output	Available	Available	Available	Available	Available
Deactivate output	Deactivates one of the programmed outputs.	which output	6		Deactiv. output	Available	Available	Available	Available	Available
Overtime	Delays auto-arming time of partitions by 30 minutes.		7		Overtime	Available	Available	Available	Available	Not available
Listen-in	Allows listen-in over-the-phone by means of a keypad microphone.	Keypad	10		Listen-in	Not available	Available	Not available	Not available	Not available
Arm/Disarm menu	Accesses the user menu section: Arm/Disarm op.		12		Arm/disarm menu	Available	Not available	Not available	Not available	Not available
Alarm management menu	Accesses the user menu section: Alarm management		13		Alarm menu	Available	Not available	Not available	Not available	Not available
Voice functions menu	Accesses the user menu section: Voice functions		14		Voice func. menu	Available	Not available	Not available	Not available	Not available
Activations menu	Accesses the user menu section: Activations		15		Activations menu	Available	Not available	Not available	Not available	Not available
View Sol-3G status	Accesses the user menu section: View / Sol-3G status		16		View Sol-3G status	Available	Not available	Not available	Not available	Not available
Arming status	Provides voice information regarding the armed/disarmed status of the partitions.		17		Arming status	Available	Available	Not available	Not available	Not available

Shortcut			on keypad		on code		on reader	on keys	on event	
description	function	parameter	n.	Icon	String	via keypad				over-the-phone
Keypad settings	Accesses the user menu section: Keypad settings		18		Keypad sett.menu	Available	Not available	Not available	Not available	Not available
Zone activations menu	Accesses the user menu section: Activations / Zones		19		ZoneBypass menu	Available	Not available	Not available	Not available	Not available
Voice memo	Accesses the user menu section: Voice functions		20		Voice memo	Available	Not available	Not available	Not available	Not available
ON/OFF output menu	Accesses the user menu section: Outputs ON/OFF		21		Output control	Available	Not available	Not available	Not available	Not available
Enable/Disable answerphone	Accesses the user menu section: Activations / Answerphone		22		Enab. answerphone	Available	Not available	Not available	Not available	Not available
Enable codes	Accesses the user menu section: Activations / Codes		24		Enable codes	Available	Not available	Not available	Not available	Not available
Enable keys	Accesses the user menu section: Activations / Keys		25		Enable keys	Available	Not available	Not available	Not available	Not available
Enable timers	Accesses the user menu section: Activations / Timers		26		Enable timers	Available	Not available	Not available	Not available	Not available
Enable auto-arming	Accesses the user menu section: Activations / Auto-arming		27		Enab. auto-arm	Available	Not available	Not available	Not available	Not available
View events log	Accesses the user menu section: View / Events log		28		View events log	Available	Not available	Not available	Not available	Not available
View alarms log	Accesses the user menu section: View / Alarms log		29		View alarm log	Available	Not available	Not available	Not available	Not available
View faults log	Accesses the user menu section: View / Faults log		30		View faults log	Available	Not available	Not available	Not available	Not available
View arm/disarm operations	Accesses the user menu section: View / Arm/Disarm op.		31		View arm ops log	Available	Not available	Not available	Not available	Not available
View system status	Accesses the user menu section: View / System status		32		ViewSystem-Status	Available	Not available	Not available	Not available	Not available
View zone status	Accesses the user menu section: View / Zone status		33		View zone status	Available	Not available	Not available	Not available	Not available
Change PIN code	Accesses the user menu section: Change PIN		34		Change PIN	Available	Not available	Not available	Not available	Not available
Time/Date	Accesses the user menu section: Set date/time		35		Time/Date	Available	Not available	Not available	Not available	Not available
View faults	Accesses the user menu section: View/Faults present		36		View faults	Available	Not available	Not available	Not available	Not available
Panic	Activates a "Panic" event	which panic event	38		Panic	Available	Available	Available	Available	Not available
Zone bypass	Bypasses one of the configured zones	which zone			Not available	Not available	Not available	Not available	Not available	Available
Unbypass zone	Unbypasses one of the configured zones	which zone			Not available	Not available	Not available	Not available	Not available	Available
Disable code	Disables one of the configured codes	which code			Not available	Not available	Not available	Not available	Not available	Available
Enable code	Enables one of the configured codes	which code			Not available	Not available	Not available	Not available	Not available	Available
Disable key	Disables one of the configured keys	which key			Not available	Not available	Not available	Not available	Not available	Available
Enable key	Enables one of the configured keys	which key			Not available	Not available	Not available	Not available	Not available	Available

4-1

Keypad shortcuts



The installer can program each LCD keypad with up to 12 shortcuts associated with 4 function keys **F1_{Fn}**, **F2_🔥**, **F3₊**, **F4_🔒**. The shortcuts are identified by icons which appear on the lower part of the display. The presence of arrows to the far right and left of the icons indicate that by pressing keys **←**, **→**, the user can access other shortcuts in cases where there are more than 4 on the keypad.

The 12 keypad shortcuts can be activated in 4 different ways, as follows.

A- By ALL.

Pressing the respective key **F1_{Fn}**, ..., **F4_🔒** will activate the shortcut instantly without code entry. The shortcut will affect all the keypad partitions.

B- By code users only.

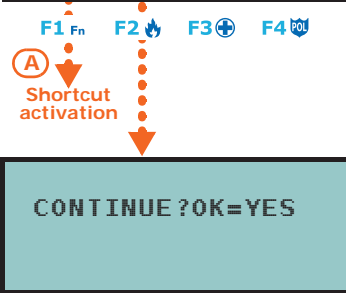
Press the respective key **F1_{Fn}**, ..., **F4_🔒**, then enter a valid code, the shortcut will activate after code recognition. The shortcut will affect the partitions common to both the keypad and code.

C- By code users only when activation of the shortcut lowers system security.
 ("Requires authorization in the event of lowered security").

If a shortcut involves a scenario that completely disarms a partition, or switches a partition from Away mode to Stay mode, the security of the system will obviously be lowered, therefore, the system will request code entry. The shortcut will affect the partitions common to both the keypad and code.

D- By ALL with confirmation request.

Pressing the respective key **F1_{Fn}**, ..., **F4_🔒** will prompt the system to ask you if you want to continue or not. If you press **OK** the shortcut will activate instantly, if you press **C** or **Esc** the operation will be abandoned. This method protects against accidental operations. The shortcut will affect all the keypad partitions.



To activate the desired shortcut, press the button **F1_{Fn}**, ..., **F4_🔒** that corresponds to the icon that identifies the shortcut. The system will activate the shortcut instantly (case A), or will request explicit confirmation (case D), or will request code entry (cases B and C).

Control panels with touch-screen keypads do not have function keys **F1_{Fn}**, **F2_🔥**, **F3₊**, **F4_🔒**, nor do they provide access to certain functions via shortcuts. However, they provide buttons on the display which, with a single tap, activate functions and applications. For further details refer to *paragraph 7-4 Operations via touch-screen keypad*.

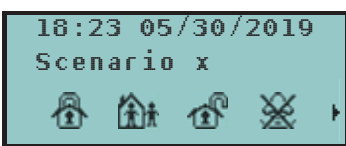






Table 4-1: Default shortcuts from the keypad

Shortcut	Icon	Description	Operation	Confirm
Arm in Away mode	n.1	AWAY	Arms all the system partitions.	No confirmation or valid code entry required.
Arm in Stay mode	n.39	STAY	Arms some of the system partitions.	No confirmation or valid code entry required.
Disarm the system	n.37	DISARM	Disarms all the system partitions.	Valid code entry required.
Stop alarms	n.2	Stop alarms	Deactivates instantly the outputs activated by alarm and tamper events	Valid code entry required.
Zone activations menu	n.19	ZoneBypass menu	Accesses the user menu section: Activations / Zones	Valid code entry required.
View alarms log	n.29	View alarm log	Accesses the user menu section: View / Alarms log	No confirmation or valid code entry required.
View faults	n.36	View faults	Accesses the user menu section: View/ Faults present	No confirmation or valid code entry required.
Time/Date	n.35	Time/Date	Accesses the user menu section: Set date/time	Valid code entry required.
Voice functions menu	n.14	Voice func. menu	Accesses the user menu section: Voice functions	No confirmation or valid code entry required.
Keypad settings	n.18	Keypad sett. menu	Accesses the user menu section: Keypad settings	No confirmation or valid code entry required.

Shortcut with code

4-2

Besides the keypad shortcuts available to all on keys **F1**  **F2**  **F3**  **F4**  , each user code can have as many as 10 customized shortcuts activable via the telephone or the panel keypad keys.

1. Establish communication with the control panel.
2. Type in your code followed by "#".
3. Listen to the voice prompts regarding the available shortcuts.
4. Press the number key which corresponds to the required shortcut.

Over-the-phone

Key and Reader shortcuts

4-3

Shortcuts on nBy/S, nBy/X readers and integrated in Sol-S control panels

4-3-1

The procedure for the activation of shortcuts by a user with an electronic key (or tag) changes in accordance with the enablements of the LEDs on the proximity reader or on the frontplate of the Sol-S control panel.

The user must hold the electronic key in the vicinity of the reader, as soon as the reader recognizes the key, the relevant LEDs will light to indicate the various shortcuts.

LEDS ENABLED

When the required shortcut is indicated, the user must move the key away from the reader to activate the required shortcut.

The lighted sequence on the Reader LEDs is as follows (refer to *Table 8-2: Reader LEDs with key at reader*).

1. **Red LED on for 3 seconds** - shortcut associated with the red LED of the reader or first shortcut of the key
2. **Blue LED on for 3 seconds** - shortcut associated with the blue LED of the reader or second shortcut of the key
3. **Green LED on for 3 seconds** - shortcut associated with the green LED of the reader or third shortcut of the key
4. **Yellow LED on for 3 seconds** - shortcut associated with the yellow LED of the reader or fourth shortcut of the key
5. **All LEDs on for 3 seconds** - first shortcut associated with the user key
6. **All LEDs off for 3 seconds** - disarm all the partitions.
7. If the key is not removed, the reader will run through the entire sequence again starting from the red LED. Selection of the desired shortcut (indicated by a specific LED) will not occur until the key is removed.

If, during this phase, any of the partitions are armed, the LED sequence will start at point 6.


LEDS NOT
ENABLED

If the installer has enabled option "50131ReadLedOFF", the reader LEDs will be off, therefore, to select and activate a shortcut, it is necessary to:

1. Wave the key across the sensitive area of the reader: the LEDs will signal the respective status for 30 seconds.
2. During this 30 second period, the user must hold a valid key in the vicinity of the reader in order to generate the shortcut, as previously described.

Shortcuts on readers integrated into Sol-G and Sol-P control panels

4-3-2

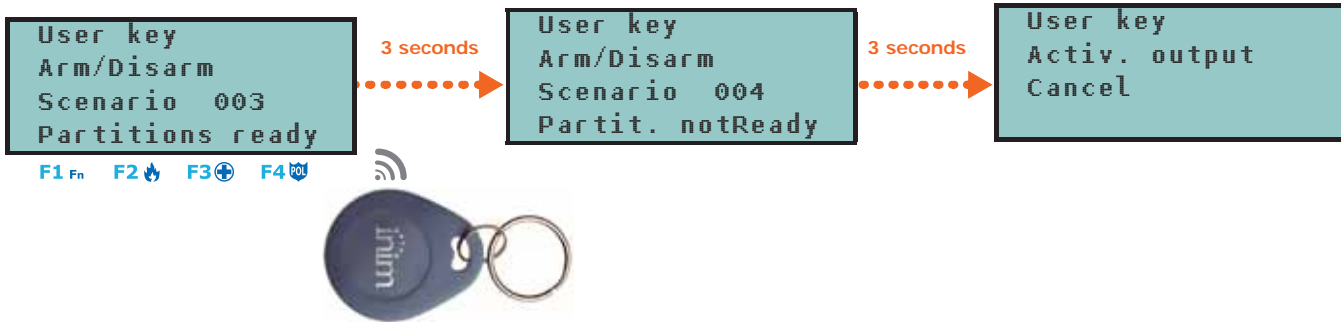
The user must hold a valid key in the vicinity of the integrated reader (the position of the reader is indicated by the  symbol).

As soon as the key is recognized, the reader display will show, one-by-one at 3 second intervals, the shortcuts available on the reader and on the key. When the required shortcut is indicated, the user must move the key away from the reader to activate the required shortcut.

The shortcuts appear on the display in the following order:

1. Description of the first reader shortcut for 3 seconds
2. Description of the second reader shortcut for 3 seconds
3. Description of the third reader shortcut for 3 seconds
4. Description of the fourth reader shortcut for 3 seconds
5. Description of the fourth reader shortcut for 3 seconds
6. The "Disarm" option, to disarm all the partitions
7. Then, starting at point 1., the system will run through the sequence again until the user moves the key away in order to select the shortcut indicated at the time.

If, during this phase, any of the partitions are armed, the LED sequence will start at point 6.



4-3-3

Remote-control shortcuts

To activate the shortcuts programmed by the installer on the 4 remote-control buttons, the user simply needs to press the button which corresponds to the desired shortcut. The successful outcome of the operation will be signalled by the buzzer and LEDs on the remote control itself (refer to *Table 8-3: Feedback signals provided by wireless keys*).

4-4

Shortcut on event

The shortcuts on events are control panel functions which are triggered (activated) by the occurrence of an event.

The definition of these functions and their activations are possible only by means of the appropriate programming of the Sol control panel and cannot be carried out by the user.

Control panel signalling

Chapter 5

The frontplates of Sol control panels are capable of emitting signals discernible by the user, other than those on the display (if present) and sounder-flasher.





These are visual and audible signals emitted by a buzzer/speaker and the LEDs on the frontplate, if present, in response to the occurrence of specific events in accordance with programming.

LED signalling

5-1




The following table shows the signalling on the 4 LEDs common to the control panel frontplates, Aria/W keypads and the icons on the touch-screen display that represent them.

Table 5-1: Frontplate LEDs


LED/Icon activation	Red 	Yellow 	Blue 	Green 
OFF Icon not present	All the partitions of the control panel/keypad are disarmed.	No faults present.	Open zones on the control panel/keypad partitions.	Primary power failure (230V a.c.)
ON Icon on solid	At least one of the control panel/keypad partitions is armed.	At least one fault is present.	All the zones on the keypad partitions are in standby status: Ready to arm.	Primary power (230V a.c.) is present
Slow blinking (ON: 0.5sec OFF 0.5sec)	All the partitions of the control panel/keypad are disarmed. Memory of alarm/tamper on at least one partition or memory of a system alarm is present.	No faults present. At least one zone belonging to the control panel/keypad partitions that is either disabled (inhibited) or is in Test status. PSTN or GSM communicator is disabled.	All the zones belonging to the control panel/keypad partitions are in standby status. An unplayed voice message is present in the memo box.	
Fast blinking (ON: 0.15sec OFF 0.15sec)	At least one of the control panel/keypad partitions is armed. Memory of alarm/tamper on at least one partition or memory of a system alarm is present.	At least one fault is active and at least one zone belonging to the control panel/keypad partitions is either inhibited (disabled) or is in Test status.	Open zones on the control panel/keypad partitions. An unplayed voice message is present in the memo box.	

The frontplate of the Sol-S control panel provides a further three LEDs:

Table 5-2: Accessory LEDs on the Sol-S frontplate

LED activation	Yellow 	Yellow 	Yellow 
OFF	No zones bypassed	All wireless devices present	The battery charge on all wireless devices is sufficient.
ON	At least one zone is bypassed	Loss of at least one wireless device.	The battery charge of at least one wireless devices is low.

The list of faults signalled by the yellow fault LED  can be found on the table in *Appendix B, Fault signals*.

Following is the list of events which cause the Red System Alarm LED  to blink:

- Open panel tamper
- Dislodged panel tamper
- Keypad Tamper
- Reader Tamper

- Keypad Loss
- Reader Loss
- False key

FALSE KEY

If the “False key” event is configured as a “Silent event”, the red LED will not blink.

HIDE STATUS

If the installer has enabled the “Hide status” option (or “50131StatHidden” on keypad), the status of the partitions will not be shown. If a valid code is entered, the real-time status of the system will be shown for 30 seconds.

Additionally:

- If the partitions are armed, the status of the system will be hidden from non-authorized users.
 - Red LED Off
 - Yellow LED Off
 - Green LED On
 - 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

5-2

Signalling on the Buzzer

The buzzers on Sol control panels and Aria/W keypads provide users with audible signals, as long as the volume is turned up.

The buzzer signals the running entry, exit and pre-arm times of enabled partitions. The activation these signals can be set up by means of the keypad options described in *paragraph 7-3-8 Keypad and display settings*.

Table 5-3: Signalling and types of signal

Signalling	Type of signal
Button pressed	Single pulse (beep)
Entry time running	8 pulses + 5 second pause
Exit time running	3 pulses + 5 second pause; 4 short pulses + 5 second pause during the final 20 seconds of the exit Time
Pre-arm time running	1 pulse + 5 second pause
Alarm	Fast pulses

Using the Sol system

Chapter 6

The Sol system can be accessed and operated in the following ways:

- Via **keypad with LCD screen** (integrated into **Sol-G** control panel models and **Aria/W** wireless keypads)
in which case the user can operate the system in two ways:
 - by means of shortcuts (refer to *paragraph 4-1 Keypad shortcuts*);
 - by entering a valid code that accesses the respective user menu (refer to *paragraph 3-2 Access to user menu*)

Refer to *paragraph 7-3 Operations from LCD keypads*.

- Via **display touch-screen** (integrated into **Sol-P** control panel models)
in this case, users are provided with buttons, displayed on the screen, that with a single tap activate functions and applications. For further details refer to *paragraph 7-4 Operations via touch-screen keypad*.
- Via **proximity reader (nBy/S, nBy/X reader integrated into the control panels)**
In this case a valid key is required and the access procedure is that described in *paragraph 8-3 Reader and key operations*.
- Via **telephone**
during a call from/to the control panel itself or via an SMS message and valid code entry (PIN).
Refer to *paragraph 9-3 Operations via telephone*.
- Via **remote-control device**
by pressing the keys, as described in *paragraph 8-2-1 Wireless keys (remote-control keys)*.
- Via **AlienMobile Application**
in this case, users are provided with buttons, on the screen of their Smartphones, which activate functions and applications from remote locations.
- Via **Inim Cloud**
by means of a browser, the user can access a customized web interface which provides all the registered control panels.

Managing alarms

6-1

The Sol control panel signals alarm status when one of the following events occurs:

- Zone alarm, when violation of a zone is detected.
- Zone tamper, when tamper (opening, dislodgement or delinquency) is detected on a device that is connected to the terminals
- Peripheral tamper, when tamper (opening, dislodgement or act of delinquency) is detected on one of the devices connected to the BUS (reader, wireless receiver)
- Peripheral loss, when sudden loss of one of the devices connected to the BUS occurs
- Control panel tamper, when tamper (opening, dislodgement or delinquency) is detected on the control panel itself

In each of the following cases, the control panel will start the programmed alarm signalling such as the activation of outputs, sounders, the sending of messages (SMS, email, push notifications) or telephone calls.

These events will be saved to the events log.

The typical operations the user must perform in the event of alarms and/or tamper conditions are:

- Stop the ongoing alarms by deactivating the outputs related to the system alarm and tamper events.
- Cancel the entire call queue and stop ongoing calls (if any).
- Delete the alarm and tamper memories.

These operations can be carried out through:

- LCD display keypad (*paragraph 7-3-1 Alarm management*)
- Touchscreen display (*paragraph 7-4-2 Alarm management*)
- Proximity readers (*paragraph 8-3-1 Alarm management*)
- Keyfobs (*paragraph 8-3-1 Alarm management*)
- Telephone (*paragraph 9-3-1 Alarm management*)
- AlienMobile Application
- InimCloud

6-2

Arming and disarming partitions

The operating status of partitions can be changed by users who are authorized to access them.

Through the appropriate user access sections for Sol system management, it is possible to request the following commands:

- **Disarm** - this command disables the partition completely. During this status, none of the zones belonging to the partition can generate alarms.
- **Away mode** - this command enables "Away mode" operating status on the partition. During this status, all of the zones belonging to the partition can generate alarms.
- **Stay mode** - this command enables "Stay mode" operating status on the partition. In this way, only the perimeter zones of the partition can generate alarms.
- **Instant mode** - this command enables "Instant mode" operating status on the partition. During this status, all the zones belonging to the partition, with the exception of the interior zones, can generate instant alarms with no entry-time delay.
- **Hold** - this command forces the partition to hold its current status.

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.

Note

When arming partitions, all the zones must be in stand-by status (not violated) and no faults must be present.

Arming the system when zones are violated or faults are present will generate a "Forced arming on partition" event. This event highlights the fact that partitions were armed when conditions which lowered the security of the system were present (for example, "Low battery" or "Mains failure").

Appropriate programming of the control panel can however prevent the arming of partitions in the presence of causes of reduced security.

These operations can be carried out through:

- LCD display keypad (*paragraph 7-3-2 Arming commands and scenarios*)
- Touchscreen display (*paragraph 7-4-3 Arming commands and scenarios*)
- Proximity readers (*paragraph 8-3-2 Arming commands and scenarios*)
- Keyfobs (*paragraph 8-3-2 Arming commands and scenarios*)
- Telephone (*paragraph 9-3-2 Arming commands and scenarios*)
- Auto-arm
- Violation of a command zone
- AlienMobile Application
- InimCloud

Via Auto-arm operations

If a partition is associated with a timer which controls automatic-arming operations, it will arm when the timer switches ON and disarm when the timer switches OFF (refer to *paragraph 6-5 Activations*). Users who are authorized to control Auto-arm operations must:

- activate the timer associated with the Auto-arm operations
- enable the Auto-arm option for the partitions concerned

Arming scenarios

6-3

A scenario is a preset arming configuration which applies various operating modes to the Sol security system partitions (the scenarios are programmed by the installer in accordance with user requirements).

Following the activation of a scenario it possible to change the status of several outputs simultaneously.

The installer will set up the system and make available the scenarios which best suit user requirements.

The user can activate the scenarios via:

- LCD display keypad (*paragraph 7-3-2 Arming commands and scenarios*)
- Touchscreen display (*paragraph 7-4-3 Arming commands and scenarios*)
- Proximity readers (*paragraph 8-3-2 Arming commands and scenarios*)
- Keyfobs (*paragraph 8-3-2 Arming commands and scenarios*)
- Telephone (*paragraph 9-3-2 Arming commands and scenarios*)
- AlienMobile Application
- InimCloud

Voice memo

6-4

The voice functions are available exclusively on control panel models with integrated keypads (Sol-G and Sol-P).

The functions are:

- Record message in the voice memo box
- Playback message in the voice memo box
- Delete message in the voice memo box

The operation time-out (expressed in seconds) will be signalled by a counter and a progress bar on the display. To stop the record/playback session manually, press **OK**, otherwise, the session will end automatically when the pre-set time-out expires.

This operation must be confirmed by pressing **OK**.

**RECORD/
PLAYBACK**

DELETE

These operations can be carried out through:

- LCD display keypad (*paragraph 7-3-3 Voice memo*)
- Touchscreen display (*paragraph 7-4-4 Voice memo*)

Activations

6-5

The activation (and deactivation) of the various elements of the Sol system allows them to operate normally in accordance with their programming (= activation) or disable their functions completely (= deactivation).

The user can activate or deactivate the following elements:

- **Zone** - deactivated (disabled) zones cannot generate alarms (bypassed).
- **Auto-arm operations** - can be activated/deactivated on each individual partition. If this option is enabled on a partition, it will arm and disarm in accordance with the On/Off settings of the respective timer.
- **Codes** - deactivated (disabled) codes cannot access the system. Activation/Deactivation can be achieved only on hierarchically inferior codes (refer to *paragraph 3-1 User Codes*).
- **Keys** - deactivated (disabled) keys cannot access the system.
- **Keypads** - deactivated (disabled) keypads do not permit code entry (or access to the menu), therefore, they cannot manage shortcuts. However, the LEDs and display will be refreshed.
- **Readers** - deactivated (disabled) readers cannot recognize keys. However, the LEDs will indicate the current status of the system.
- **Timers** - activated timers (On) manage their associated elements (partitions, codes, keys) in accordance with their settings. Deactivated timers cannot time-manage their associated elements, therefore, they will function in accordance with Timer Off status.

Note

On exiting the programming session, all the timers will be activated automatically. It is the task of the user to deactivate timers which are not used for system control purposes.

- **Dialer** - a deactivated (disabled) dialer cannot send voice or digital calls. However, if appropriately programmed, it will be capable of managing incoming calls.
- **PSTN/GSM Answerphone** - if activated (enabled), the control panel will answer incoming calls (on the PSTN landline and GSM network) with the prerecorded "Answerphone" message.
- - If activated (enabled), the Installer PIN will be accepted by the system and the installer will have access to the Installer menu. If deactivated (disabled), entry of the installer PIN will generate an "Invalid Code" event and the installer will be denied access to the respective menu.
- **Sync IP2RX** - if activated (enabled), the control panel will send a specific string to the IP2RX software in order to allow its identification.
- **Registration to Inim Cloud** - this section allows the Sol control panel to access INIM Electronics cloud service.

The activations of the elements can be carried out from:

- LCD display keypad (*paragraph 7-3-4 Activations*)
- Touchscreen display (*paragraph 7-4-5 Activations*)
- AlienMobile Application
- InimCloud

6-6 Outputs management

The user can activate/deactivate manually the outputs the user code in question is authorized to work on.

It is possible to activate/deactivate low-power open-collector or relay outputs and view their status by means of the respective icons.

The activations of the outputs can be implemented via:

- LCD display keypad (*paragraph 7-3-6 Outputs management*)
- Touchscreen display (*paragraph 7-4-7 Outputs management*)
- Proximity readers (*paragraph 8-3-3 Outputs management*)
- Keyfobs (*paragraph 8-3-3 Outputs management*)
- Telephone (*paragraph 9-3-3 Activation of outputs*)
- AlienMobile Application
- InimCloud

6-7 Change code PIN

This section allows the user to change the code PIN used for accessing the system and also the PINs of other users with a lower rank in the system hierarchy (refer to *paragraph 3-1 User Codes*).

In order to be EN50131 compliant, all PINs must have 6 figures.

This operation can be done through:

- LCD display keypad (*paragraph 7-3-9 Change code PIN*)
- Touchscreen display (*paragraph 7-4-10 Change PIN*)

6-8 Change telephone numbers

Users can change the contact numbers used by the telephone dialer of the Sol control panel.

Only contact voice-contact numbers with at least one partition in common with the entered user code and keypad in use will be shown.

This operation can be done through:

- LCD display keypad (*paragraph 7-3-10 Edit telephone numbers*)
- Touchscreen display (*paragraph 7-4-11 Edit telephone numbers*)

Connection to a LAN/Wi-Fi network

6-9

The Sol control panel can connect to a LAN network, whether cabled via the Ethernet port of the optional Sol-LAN module, or Wi-Fi via the optional Sol-WIFI module, and therefore have access to a local or Internet network.

The connectivity to the Sol control panel LAN is subject to the configuration of the network itself. The manufacturer strongly recommends that the user contacts the network administrator for the correct configuration.

The connection of the control panel and configuration of its settings can be carried out by the user from the user menu, which can be accessed via:

- LCD display keypad (*paragraph 7-3-11 Connection to a network*)
- Touch-screen, after accessing the "Settings - Alphanumeric display" section from the home page (*Table 7-15: Touch-screen keypad menu*) that operates as an LCD keypad.

Overtime request

6-10

This operation can be carried out under the following conditions only.

- The partition concerned must be timer-controlled.
- The Auto-arm partition option must be enabled (refer to *paragraph 6-5 Activations*).

Each overtime request postpones the auto-arming operation by 30 minutes.

This operation can be done through:

- LCD display keypad (*paragraph 7-3-12 Overtime request*)
- Touchscreen display (*paragraph 7-4-12 Overtime request*)
- Proximity readers (*paragraph 8-3-4 Overtime request*)
- Keyfobs (*paragraph 8-3-4 Overtime request*)
- Telephone (*paragraph 9-3-4 Overtime request*)

Listen-in

6-11

During a telephone communication with the control panel, the user can activate the Listen-in function and listen to sounds coming from premises with control panels that have at least one partition in common with the code used over-the phone (for Sol-G and Sol-P control panel models).

Shortcut n.10 must be assigned (by the installer) to one of the number keys relating to the code that will generate this operation (refer to *paragraph 9-3-5 Listen-in*).

This function can be activated over-the-phone only.

Partition status enquiry

6-12

During a telephone communication with the control panel, the user, after entering a valid code, can access a control panel with voice functions and enquire about the armed/disarmed status of the partitions.

The control panel will announce the armed/disarmed status of the partitions the entered PIN is assigned to.

This operation can be implemented through:

- LCD display keypad (*paragraph 7-3-15 Partition status enquiry*)
- Telephone (*paragraph 9-3-6 Partition status enquiry*)

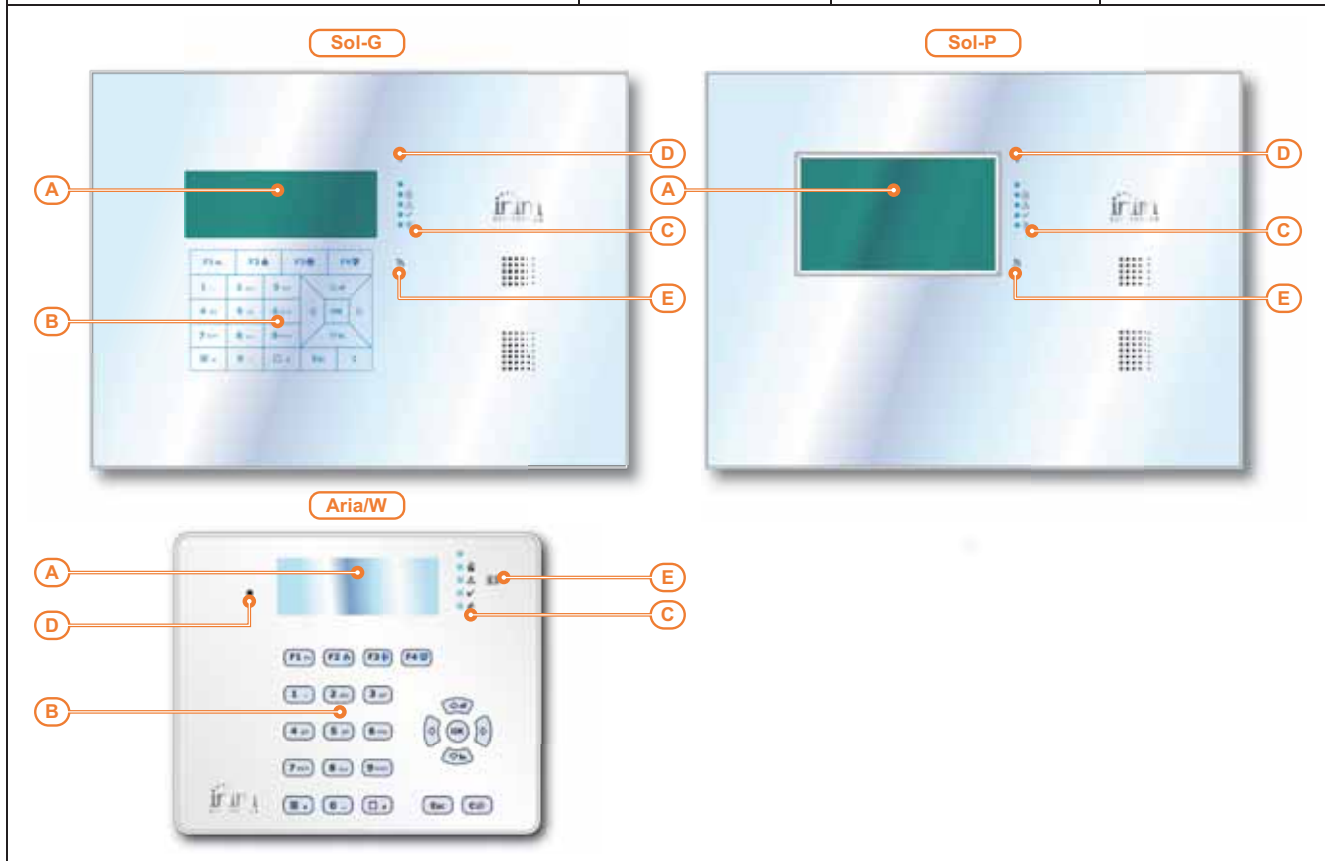
Chapter 7

Using the keypads

The keypads available are those integrated into the frontplate of Sol-G and Sol-P control panel models and the Aria/W wireless keypad. They provide the features shown in the following table:

Table 7-1: Keypads - functions

Models	Integrated into the control panel		Peripherals	
	Sol-G	Sol-P	Aria/W	
A	Graphic display	LCD 192x64	65536 colour touch screen 4.3 inches 480x272	LCD 96x32
B	Keys	23 (touch)	No	23 (in soft rubber)
C	Signalling LEDs	4	4	4
D	Microphone	Yes	Yes	No
E	Built-in proximity reader	Yes	Yes	No
	Buzzer	Yes	Yes	Yes
	Brightness sensor	Yes	Yes	Yes
	Tamper protection	Yes	Yes	Yes
	Wireless	No	No	Yes
	Keypad lock-out	No	Yes	No



The keypad is the most complete and versatile device for system management.

The installer assigns the partitions and portions/sections of the system that users with codes have access to via the keypad in use.

The graphic display shows the necessary information and provides a user-interface based on a user menu and icons for the operations to be performed.





Each user, in possession of a code PIN entered at a keypad and recognized by the control panel, can be enabled to operate on the system or on part of it.

In order for code users to access their user menus, they must first validate their codes. This can be done by typing-in the code PIN and pressing the **OK** button.



ACCESSING THE KEYPAD

It is possible to extend the use of some of the system shortcuts to users without assigned codes.

LCD keypads allow use of shortcut functions associated with the keys **F1**  **F2**  **F3**  **F4**  , these operations are usually reserved for authorized users (users with assigned codes).

Also touch-screen keypads provide shortcuts, such as the activation of scenarios and applications, such as the setting-up of the keypad itself, which can be activated without code entry by the buttons displayed on the screen.

SHORTCUT

The Aria/W wireless keypad provides all the functions for the control and management of the Sol control panel via the Air2 system, which it interfaces with through the transceiver integrated into the control panel or through an optional Air2-BS200 transceiver.

It is equipped with an accelerometer which provides both anti-tamper and “wake-up” from stand-by functions, whereas the brightness sensor controls the display and key brightness optimally with respect to the surrounding environment. Moreover, it has an automatic shutdown function in the event of loss of wireless connection.

WIRELESS TERMINALS

Keypads with LCD screens (integrated into the Sol-G control panel and Aria/W wireless keypad) allow the user to set the keypad backlight to suit the measured ambient lighting conditions. The keypad manages two different brightness settings:

- Day
- Night

These settings can be programmed via the “Keypad settings” section in the user menu.

BACKLIGHTING

The Sol-P control panel provides a touchscreen user-interface with a 4.3 inch colour display. Access to the keypad functions is achieved by tapping on the respective buttons displayed on the screen.

Graphics management provides ample room for customization, with skin and background selection and image rotation. The user can also control the screen brightness, contrast and image transparency.

The keypad provides the following user applications:

- graphic maps for the supervision of the entire system monitored by the Sol control panel through a graphic layout containing images, icons and buttons on the display
- the alarm clock and memo functions which generate audible signals and display pop ups are programmable directly by the user

TOUCH-SCREEN KEYPADS

7-1

Keypad displays

7-1-1










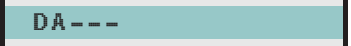
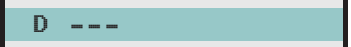

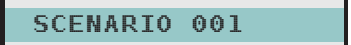


LCD screen

The graphic LCD screen is backlit, it is possible to adjust the screen brightness and contrast via the respective options on the user menu (refer to *paragraph 7-3-8 Keypad and display settings*).

The following table describes the messages which are shown on the keypad display, in accordance with the actual status of the control panel:

- **Stand-by** - indicates the control panel is functioning normally and there are no alarm, tamper or fault events present on the system.
- **Alarm or Zone tamper** - indicates that the control panel has detected trouble on a zone, such as zone violation (intrusion) or detection of a lost device
- **Maintenance** - indicates that the control panel is in maintenance mode for repair or programming purposes

Table 7-2: Display visualization

Line	Control panel status		
	Stand-by	Alarm or tamper	Maintenance
1	 <p>The first line of the display shows the date and time.</p>	 <p>If at least one of the keypad partitions has saved an alarm or tamper event to the memory, the first line of the screen will flash the descriptions of the zones concerned every 3 seconds.</p> <p>Note</p> <p>Open zones are signalled by blinking on the red LED . </p>	 <p>If the control panel is in Maintenance status, the "Maintenance" string will be shown.</p>
	 <p>If the "View open zones" control-panel option is enabled, approximately every 3 seconds the descriptions of zones that are not in standby status will be shown in sequential order when the keypad partitions are disarmed.</p>  <p>Any auto-bypassable zones will be shown in white on black background.</p>	  <p>If the control panel is in Maintenance mode and at least one of the keypad partitions has saved an alarm or tamper event to the memory, the above-described strings will alternate on the display.</p>	
2 left	 <p>The left side of the second line shows the characters that indicate the current status of the partitions the keypad is assigned to:</p> <ul style="list-style-type: none"> • D = partition disarmed • A = partition armed in Away mode (interior and perimeter zones armed) • S = partition armed in Stay mode (perimeter zones armed) • I = partition armed in Instant mode (perimeter zones armed with no delay) • - = partition does not belong to the control panel/keypad 	  <p>In the event of a partition alarm or tamper memory, the red LED on the keypad and the characters corresponding to the partitions concerned will blink. </p>	<p>The line is the same as when the control panel is in standby condition.</p>
	 <p>If the "View scenario" control-panel option is enabled (enabled at default), the left side of the second line on the keypad display will show the description of the active scenario.</p>		
2 right	 <p>The right side of the second line may show several icons which provide visual information regarding the system. For a detailed description of these icons refer to <i>Table 7-4: Information icons</i>.</p>		
3 4	 <p>Lines three and four on the display are occupied by the icons which correspond to the shortcuts assigned to the function keys F1 Fn , ..., F4 .</p> <p>If no shortcuts are programmed on the keypad function keys, the respective spaces on the display will remain empty.</p>		

What appears on the display of Air/W keypads as the flashing of the characters that indicate the operating statuses of the partitions, is not actually true flashing but is in fact the solid negative image of the characters themselves.

Note

Touchscreen display

7-1-2

Following is the description of the screen layout of a Sol-P control panel; the presence of each one of the elements described depends on the activated functions and the page being accessed:

Table 7-3: Sol-P - display

A	Data and Time of the Sol control panel. If the control panel is in Maintenance status, this field will show "Maintenance" string.	
B	Keypad LED icons (<i>Table 5-1: Frontplate LEDs</i>).	
C	Icon which indicates the presence of an SD card in the card slot. After entering a valid user code, the Logout button that appears in this field will allow the user to close the session.	
D	Section for active functions, with the buttons for access to the control panel, its applications and the Sol system. The home page (shown in the figure) shows the function buttons indicated in <i>Table 7-15: Touch-screen keypad menu</i> .	
E	String showing the arming status of the control panel, in accordance with the active scenario or status of the partitions. If a keypad partition changes its status in relation to the active scenario, or when the control panel is placed in Maintenance mode, this string will show the characters which indicate the real status of the partitions, as described in <i>Table 7-2: Display visualization</i> .	
F	Tapping this section on the display opens (for 3 seconds) a window containing a list of the active scenarios. If required by programming (<i>paragraph 7-3 Operations from LCD keypads</i>), it may request entry of a valid code.	
G	System information icons, as described in <i>Table 7-4: Information icons</i> .	
H	If the user is working inside a section, this field will show the following buttons which may cover the information icons: <ul style="list-style-type: none"> • Back This key allows the user to step back to the previously active function. • Home page Button which allows the user to go directly to the home page. 	

Further viewing on the display depends on the section/page being accessed by means of the buttons. The layout of such pages depends on the functions and buttons available and how they are used (*paragraph 7-4-1 Function buttons*).

There are also alerts which the control panel activates automatically and that appear as pop-ups during the following events:

POP-UP

- **Zone alarm or tamper**
If any of the keypad partitions has alarm or tamper event memory, a pop-up window will appear showing:
 - an "ALARM" warning and the description of the zone which generated the alarm or tamper signal
 - the **Disarm** button, to disarm all the armed partitions that the code has access to
 - the **Stop alarms** button, to deactivate the outputs activated by the alarm signal
 - **Clear call queue** button, to cancel the calls in the outgoing call queue
 - the **Home** button to access the home page directly
- Activation of the **entry time**
- Activation of the **exit time**
If an entry or exit time is activated, a pop-up will appear showing:
 - a string indicating the remaining seconds of the running entry/exit time
 - the **Disarm** button, to disarm all the armed partitions that the code has access to
 - the **Scenarios** button, to access the section containing the list of scenarios available for activation
 - the **Home** button to access the home page directly
- **Keypad locked**, this icon appears when the user taps the display and the keypad is locked due to 5 consecutive invalid code entries.
- **Reader locked**, this icon appears when the user holds a key in the vicinity of a reader which has been locked due to 5 consecutive attempts to use an invalid key.



CLEANING THE DISPLAY

Pressing the "Settings" button on the home page for at least 7 seconds disables the sensitivity of the display for 20 seconds. During this interval, the "CLEAN SCREEN" message is shown to indicate that it is possible to clean the screen.

Pressing any part of the screen for 50 seconds will reboot the keypad.

































REBOOTING

7-1-3

Status icons on display

The icons that appear on the second line, on the right side of the LCD screen or on the top and bottom bars of the display, provide system information, therefore, their appearance or status (fixed or flashing) depends on the status they are reporting:

Table 7-4: Information icons

Icon	Signalling	Sol-G	Aria/W	Sol-P
Telephone line	Telephone line busy	 Solid		 Solid
	Telephone line down	 Blinking		 Blinking
Lost	At least one wireless peripheral or device is not responding	 Solid		 Solid
	All the peripherals in the system configuration are responding properly, however, loss of a peripheral has been detected and cleared (Peripheral Loss memory).	 Animated	 Solid	 Blinking
Answerphone	Answerphone function enabled	 Solid		 Solid
Key	False key	 Blinking	 Solid	 Blinking
Peripheral tamper	At least one peripheral (keypad, reader, expansion) is in tamper status (enclosure open or dislodged)	 Solid		 Solid
	All peripherals are appropriately placed and all enclosure covers are closed, however, tamper was previously detected and cleared (Tamper memory).	 Animated	 Solid	 Blinking
Control panel Tamper	The Control panel is in tamper status (enclosure open or device dislodged).	 Solid		 Solid
	The Control panel is appropriately placed and the enclosure is closed, however, panel tamper has been detected and cleared (Panel tamper memory).	 Animated	 Solid	 Blinking
Call on GSM	A phone call is in progress on the GSM communicator	 Solid		 Solid
Sending SMS	An SMS text message is being sent through the GSM communicator	 Solid		 Solid
LAN	A SIA-IP event report is being sent through the LAN	 Solid		 Solid
SIA-IP over GSM	A SIA-IP event report is being sent through the GSM communicator	 Solid		 Solid

7-2

Using the keys

The following section describes the typical usage of the keys. Some of the keys may have specific functions which will be indicated when necessary.

Table 7-5: The keypad keys





Keys	Name	Typical application
1 ., 2 abc 3 def 4 ghi 5 jkl 6 mno 7 pqrs 8 tuv 9 wxyz 0 _	Number keys	These keys are used to input data into the system.
OK	OK	This key confirms the selection made.
 	UP, DOWN	These keys scroll the menu lists and/or adjust graphically displayed options (for example, keypad or volume adjustment).
 	LEFT, RIGHT	These keys scroll through the options or data being viewed (for example, when viewing partitions in the events log or when selecting partitions in the arm/disarm menu).
C	C	This key steps back on the open menu without confirming the selected options or, after entering a user PIN and pressing OK, to pass through the 3 possible visualizations of the user-menu (refer to <i>paragraph 3-1 User Codes</i>).

Table 7-5: The keypad keys

Keys	Name	Typical application
Esc	ESC	This key exits the user menu definitely without confirming options
*	ENABLE	This key enables options (refer to <i>paragraph 7-3-4 Activations</i>).
#	DISABLE	This key disables options.
F1 Fn F2 F3 F4	F1, F2, F3, F4 or function keys	These keys activate the shortcuts which correspond to the associated icons. They can also be used as Emergency keys (refer to <i>paragraph 7-2-1 Emergency functions</i>).

Emergency functions

7-2-1

The control panel provides 3 special functions which can be activated from the keypad:

- Fire Emergency
- Ambulance Emergency
- Police Emergency

Activation of these keys will generate the associated events and actions (e.g. activation of outputs and calls).

To activate an emergency request, press and hold for 3 seconds the required key combination and wait for the confirmation beep, as follows:

Table 7-6: Emergency keys

Emergency	Key combinations	Touch-screen buttons
Fire	F1 Fn + F2	
Ambulance	F1 Fn + F3	
Police	F1 Fn + F4	

If any two function keys are pressed at the same time, the functions relating to the icons associated with the keys will not be activated.

Note

Operations from LCD keypads

7-3

Alarm management

7-3-1

The actions that can be performed from the keypad in the event of alarm and tamper events are:

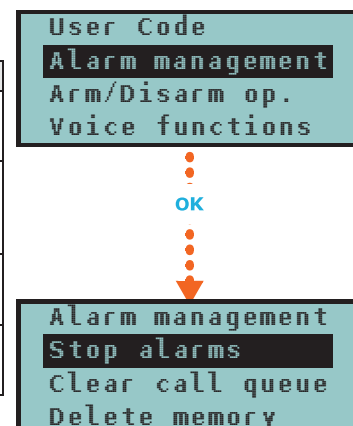
- Stop alarms
- Clear call queue
- Delete memory

The user can operate via the keypad in two ways:

- activate the shortcuts associated with keys F1 Fn , ..., F4 (shown on the display) with or without code entry
- access the "Alarm management" section of the user menu by typing in a valid code PIN.

Table 7-7: Shortcut for the management of alarms from a keypad

Shortcut	User menu section	Operation
Alarm management menu n.13	Alarm management,	Access the section with the list of available operations.
Stop alarms n.2	Stop alarms	Deactivates instantly the outputs relative to zone/partition alarm and tamper events and deletes the partition and system alarm and tamper memories.
Clear call queue n.3	Clear call queue	Cancels the entire call queue and stops ongoing calls (if any).
Delete memory n.4	Delete memory	Deletes memory of system and partition alarm and tamper events.



7-3-2

Arming commands and scenarios

```
Zone not ready
Control panel 01
```

If the arming of one or more partitions is requested from a keypad and some of the zones involved are not in standby status (thus causing command execution to generate an instant alarm), the keypad will provide a list of the zones that are not in standby status.

The user can scroll the list and check the zones which are not in standby status. If you wish to implement the command, the visualized zones will generate an instant alarm.

If you request an arm-partition command at a keypad (for one or more partitions) and conditions (programmed by the installer) which lower the security of the system are present, the keypad will provide a list of the conditions concerned, as shown in the figure opposite.

The user can scroll through the list to see the causes of reduced security, then decide whether or not to force the arming command.

The user can operate via the keypad in two ways:

- activate the shortcuts associated with keys **F1 Fn** , ..., **F4** (shown on the display (with or without code entry) of the “Arm/Disarm” type (shortcut no. 1) that will apply the programmed scenario.

If the shortcut is activated by the entry of a code PIN with the “Fixed Length” attribute, and if all the partitions the user controls are disarmed, they will switch status and arm; likewise, if all the partitions the user controls are armed they will switch status and disarm.

- Access the “Arm/Disarm” section in the user menu. In this section it is possible to select the arm or disarm mode for each partition individually:

1. Select the desired partition, using keys **◀** and **▶**.
2. Select the required operating mode for the selected partition, using keys **▲** and **▼**.

- “D”, to disarm.
- “A”, to arm in Away mode (entire system armed)
- “S”, to arm in Stay mode (system partially armed).
- “I”, to arm in Instant mode (no delays)
- “N”, not to change the operating status.

3. Once the arming modes are set on all the partitions, press **OK**.

```
Ongoing faults
Low battery
Tel. line down
```

```
User Code
Alarm management
Arm/Disarm op.
Voice functions
```

OK

```
Arm/Disarm op.
PARTITION 001
Away
TD---
```

ENTRY TIME WINDOW

If during the entry time a code is entered, and if the code is authorized to access the “Arm/Disarm” section of the user menu, the partitions common to the code and keypad will disarm immediately.

Table 7-8: Shortcut for Arm/Disarm partition operations from a keypad

Shortcut	User menu section	Operation
Arm/Disarm	n.1	Activate the scenario selected from those available.
Arm/disarm menu	n.12	Accesses the section containing the list of partitions which the user can access and change the operating status.

SHOW SCENARIO

If the “View scenario” control-panel option is enabled (or “View scenario” on keypad, enabled at default), the left side of the second line on the keypad display will show the description of the active scenario.

7-3-3

Voice memo

The voice functions available at the Sol-G control panel with SmartLogos30M voiceboard are:

- Record message in the voice memo box
- Playback message in the voice memo box
- Delete message in the voice memo box

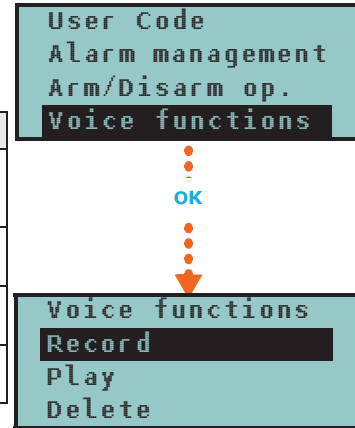
The user can operate via the keypad in two ways:

- activate the shortcuts associated with keys **F1 Fn** , ..., **F4** (shown on the display) with or without code entry
- access the “Voice functions” section of the user menu by entering a valid PIN code (section not available if the voiceboard is not installed)

During the playback phase the volume can be adjusted using keys and .

Table 7-9: Shortcut for voice function from a keypad

Shortcut	User menu section	Operation
Voice functions menu n.14	Voice functions	Access the section with the list of available operations.
	Record	Record message in the voice memo box
	Play	Playback message in the voice memo box
	Delete	Delete message in the voice memo box



7-3-4

Activations

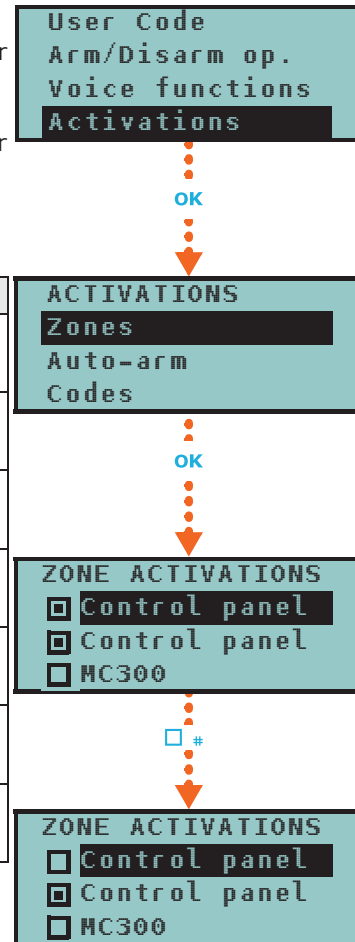
The user can implement activations via the keypad in two ways:

- activate the shortcuts associated with keys **F1** , ..., **F4** (shown on the display) with or without code entry
- access the "Activations" section of the user menu by entering a valid code PIN.

In this section it is possible to activate the selected element by means of the * button or deactivate it by means of the # button.

Table 7-10: Shortcut for activations from a keypad

Shortcut	User menu section	Operation
Activations menu n.15	Activations	Access the section with the list of available elements.
Zone activations menu n.19	Zones	List of zones
Enable/Disable answerphone n.22	Answerphone	"Answerphone" function
Enable codes n.24	Codes	List of codes
Enable keys n.25	Keys	List of keys
Enable timers n.26	Timers	List of timers
Enable auto-arming n.27	Auto-arm	Auto-arm single partition



7-3-5

View

From the keypad, the user can view the current status of some of the system elements:

- the events log (alarms, faults, arm/disarm operations, etc.), which shows the chronology with which the events occurred and were restored
- the status of the GSM communicator (Sol-3G)
- the control panel power-supply voltage, its firmware version and model
- the electrical status of the zones (stand-by, alarm, short-circuit, tamper) and their bypassed status
- activation status of the timers
- any faults present (refer to *Appendix B, Fault signals*)

To view these statuses:

- activate the shortcuts associated with keys **F1** , ..., **F4** (shown on the display) with or without code entry;
- access the "View" section of the User menu by entering a valid PIN.

User Code
Voice functions
Activations
View

OK

VIEW
Events log
Alarms log
Faults log

OK

Valid code
User Code
Local keypad
18:23 5/31/2019

OK

Event ID 1234
Event Num.: 5678

User access to the information in the “Logs” section is filtered. For example, a user can only view the zone alarms relating to the partitions the entered user code and keypad concerned have in common.

Press keys and to scroll the chronological events list.

For some events, pressing the button will allow the user to view the respective details.

Table 7-11: Shortcut for viewing from a keypad

Shortcut			User menu section	Operation
			View	Access the section with the list of items that can be viewed.
View events log	n.28		Events log	Events log
View alarms log	n.29		Alarms log	Alarms log
View faults log	n.30		Faults log	Faults log
View arm/disarm operations	n.31		Arm/Disarm ops.	Arm/Disarm log
GSM Menu status	n.16		Sol-3G status	Status of GSM communicator
View system status	n.32		System status,	
			Batt	the voltage measured on the battery
			Pow.	the control panel power supply voltage
			Aux	the voltage measured on terminal “AUX”
			I-BUS	the voltage measured on terminal “+” of the I-BUS
View zone status	n.33		Zone status	Zone status
View faults	n.36		Ongoing faults	Ongoing fault
			PanelVersion	the firmware version and the control panel model

GSM STATUS

Table 7-12: View GSM status from keypad

Line	Display	View
1		<ul style="list-style-type: none"> Mobile network provider (on the left side) “--” indicates that the GSM card is present in the control panel “C” means that data transfer is in progress data network technology (on the right side) <ul style="list-style-type: none"> G, GPRS service 3G, UMTS service H, HSPA service
2		GSM signal reception (value between 1 and 100)
3		balance, at the last operation (expressed in the local currency)
4		Faults present, in this case it is necessary to access the “View-Faults” section for details.

ZONE STATUS

Table 7-13: View zone status from keypad

Line	Display	View
1		Zone description
2		Zone status (“Standby”, “Alarm”, “Short-circuit”, “Tamper”) and its activation status (“unbypassed” - capable of generating alarms, or “bypassed” - incapable of generating alarms)
3		Indications that vary depending on the device type: <ul style="list-style-type: none"> wireless zone; level of wireless signal reception (from 0 to 7) Air2-FD100 smoke detector; level of wireless signal and level of smoke present in the sensing chamber, expressed in mdB/m
4		Level of contamination present in the smoke detection chamber of Air2-FD100 smoke detector (%)

Outputs management

This section allows the user to activate/deactivate manually the outputs the code is enabled to work on.

The user can implement output activations via the keypad in two ways:

- activate the shortcuts associated with keys **F1 Fn** , ... , **F4 POL** (shown on the display) with or without code entry
- access the "Outputs ON/OFF" section of the user menu by entering a valid PIN.

Once the output has been selected, it can be activated by the **□ *** key and deactivated by the **□ #** key.

Table 7-14: Shortcut for output activations from a keypad

Shortcut		User menu section	Operation
ON/OFF output menu	n.21	Outputs ON/OFF	Access the section with the list of available outputs
Activate output	n.5		Activates the output programmed for the shortcut
Deactivate output	n.6		Deactivates the output programmed for the shortcut

Change date and time

The keypads provide a section for the control panel date and time setting and its format.

The user can operate via the keypad in two ways:

- activate the "Date/Time" shortcut (shortcut n.35), associated with one of the keys **F1 Fn** , ... , **F4 POL** shown on the display, with or without code entry
- access the "Set date/time" section of the User menu by entering a valid PIN.
 1. Use keys **◀** and **▶** to select the programming field to be changed (hour, minutes, etc.).
 2. Use keys **▲** and **▼** to change the selected field.
 3. Press **OK** to save the setting.

Keypad and display settings

The keypads provide a section for the settings of the keypad display and buzzer and also for the buzzer of the control panel.

The parameters which are available depend on the type of keypad.

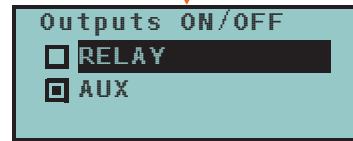
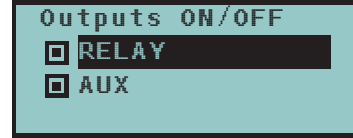
- **Brightness/Day** - for the adjustment of the backlight brightness of the display and key LEDs, when any key is pressed and for the following 20 seconds, in "Day" mode.
- **BrighStdby/Night** - for the adjustment of the backlight brightness of the display and key LEDs, when the keypad is in Standby and in "Night" mode.
- **Contrast** - for the adjustment of the black/white contrast.
- **Volume** - intensity of buzzer loudness.
- **Keypad options:**
 - **NoExitTimeSignal** - if enabled, the buzzer will not emit audible signals during partition Exit time.
 - **NOEntryTimeSignal** - if enabled, the buzzer will not emit audible signals during partition Entry time.
 - **Beep on output** - if enabled, the buzzer will emit an audible signal during activation of terminal T1, when it is programmed as an output.
 - **Chime** - if enabled, the buzzer will not emit audible signals when a chime zone is violated.
 - **LED Off in standby** - if enabled, this option switches of the relative LEDS after at least 40 seconds of inactivity on the keypad.

These settings apply only to the keypad in use and will be saved even in the event of panel shutdown.

The user can operate via the keypad in two ways:

- by activating the "Date/Time" shortcut (shortcut n.18), associated with one of the keys **F1 Fn** , ... , **F4 POL** shown on the display, with or without code entry
- access the "Keypad settings" section of the User menu by entering a valid PIN.

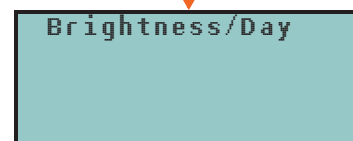
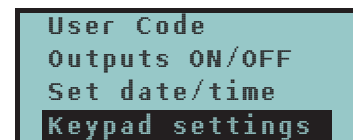
7-3-6









7-3-7



7-3-8





1. Use  and , followed by **OK** to select the parameters to be programmed.
2. Use keys  and  to increase or decrease the value of the selected parameter. To activate the selected option press  * , to deactivate it press  # .
3. Press **OK** to save.

7-3-9

Change code PIN

To change the PINs of user codes via keypad, the user can operate in two ways:

- activate the "Change PIN" shortcut (shortcut n.34), associated with one of the keys **F1 Fn** , ..., **F4 Fn** shown on the display, with or without code entry
- access the "Change PIN" section of the user menu by typing-in the current code PIN.
 1. Use keys  and  followed by **OK** to select the code to be changed.
 2. Type-in the new PIN (4, 5 or 6 digits) using keys **0** , ..., **9** then press **OK**.
 3. Type-in the new PIN again using keys **0** , ..., **9** and press **OK** to save.





***3

7-3-10

Edit telephone numbers

To edit telephone numbers from the keypad, it is necessary to access the user menu in the "Telephone Numbers" section (entry of code PIN required).

Access the phonebook:

1. Use keys  and  to select the required phone number then press **OK**; each programming field accepts a 20 digit phone number.
2. Use keys  and  to select the field to be edited, then use the number keys (**1** , ..., etc.) to edit the number. The following characters are also accepted: "," (= 2 second pause), "*" and "#".
3. Press **OK** to confirm and exit.



7-3-11





Connection to a network

The connection of the control panel and the configuration of the parameter settings can be done through the User menu. It is necessary to enter the user code PIN, access the "Settings" section, then the "IP Par.and Wi-Fi" section.

This section provides the following sub-sections:

- **Wi-Fi Networks** - by pressing the **OK** button the control panel will start scanning for available networks, those found will be listed in order in accordance with their signal strength. At this point the user can select a network and make the connection using the **OK** button, after entering the respective password, if required.
- **Options:**
 - **Enable DHCP** - if enabled, the IP connection parameters will be obtained automatically, in accordance with DHCP protocol.
 - **Enable Wi-Fi** - if enabled, the Sol-WIFI module will activate for the Wi-Fi connection.
 - **Test Internet** - if enabled, the control panel will automatically carry out an Internet connection test every 5 minutes, if failed, the system will force the restart of the Wi-Fi connection.

Once the option has been selected, it is enabled using the  * button and disabled using  # . The **OK** button confirms any changes to the options.

- **IP Parameters** - this section is for the network parameter settings (IP address, subnet mask, gateway, DNS, communication port).
 1. Use keys  and  to select the Timer then press **OK**.
 2. Use keys  and  to select the field to be edited, then use the number keys (**1** , ..., etc.) to edit the number. Insert the octets inclusive of zeros (e.g.: 192168001010 per 192.168.1.10).
 3. Press **OK** to confirm and exit.



Overtime request

7-3-12

The overtime request via keypad can be activated in two ways:

- activate the "Overtime" shortcut (shortcut n.7), associated with one of the keys **F1.Fn** , ..., **F4.Fn** shown on the display, with or without code entry
- access the "Overtime req." section of the user menu by typing in a valid code PIN.











Code Management

7-3-13

The user menu provides a section for the programming of the parameters of hierarchically-lower user codes (refer to *paragraph 3-1 User Codes*).





The parameters which can be changed in this section are also available in other sub-sections.

Access the "Timers" section of the user menu by typing-in a valid code PIN.

1. Use keys  and  followed by **OK** to select the code to be changed.
 2. Use keys  and  followed by **OK** to select the parameter to be changed.
 3. Change the parameter then press **OK** to save the changes.
- **Description:** edit field for the code description.
 - **Partitions** - select the partitions the user code is assigned to. Press  , to enable the partition and  to disable it.
 - **Options** - use keys  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, and 5, 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.
 - **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 code.
 - **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 output
 - Deactivate output
 - Listen-in
 - Arming status
 - **Patrol** - if enabled, the code will have the attributes of a "Patrol" code.
 - **Fixed length** - if enabled, the user will be able to arm and disarm the control panel simply by typing in their PIN without need of pressing the **OK** button. If all the partitions the user controls are disarmed, it will arm them, otherwise it will disarm them. If this option is enabled, the user of the code concerned can access their menu only after pressing **OK** and typing-in their PIN.
 - **Key shortcuts** - this section allows the user to configure up to 10 shortcuts to be associated with the phone number keys. After PIN acceptance, the code user can activate the shortcut by pressing the respective number key.

CODE PARAMETERS

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

1. Use keys  and  to select the key to be associated with the shortcut then press **OK**.
 2. Press **OK** then, using keys  and  , select from the "Type" list the shortcut to be associated with the function key.
 3. Press **OK** to confirm and exit.
 4. If the shortcut is associated with "Arm/Disarm" operations, the system will ask the user to select a scenario. If the associated shortcut is "Activate output" or "Deactiv. output", the system will ask the user to select an output.
- **ActivatableOutputs** - this section allows the user to enable/disable the outputs the code is allowed to control manually:

User menu, **Outputs ON/OFF**

1. Use keys and to select the desired output.
 2. Use keys and to enable/disable manual control of the output for the code concerned.
 3. Press **OK** to confirm and exit.
- **Timers** - this section allows the user to assign a timer to the code. The code will be operative only at the pre-set times.
 - **Type** - this section allows the user to assign a level (rank) in the system hierarchy to the selected code.
 - **Enablements** - this section allows the user to enable/disable access to the various sections of the user menu. The programming steps are identical to those of "Outputs ON/OFF".

7-3-14

Timer programming

This section allows the programming of all the timers the user has access to.

The user can program two "ON" times and two "OFF" times for each day of the week.

A timer can be associated with:

- a **Partition** - if the timer is enabled and the partition is enabled for automatic-arming operations (refer to *paragraph 7-3 Operations from LCD keypads*), the partition will arm when the timer is active (ON) and will disarm when the timer switches OFF.
- a **Code** - if the timer is enabled, the code will be authorized to operate on the system only during the period the timer is active (ON).
- a **Key** - if the timer is enabled, the key will be authorized to operate on the system only during the period the timer is active (ON).

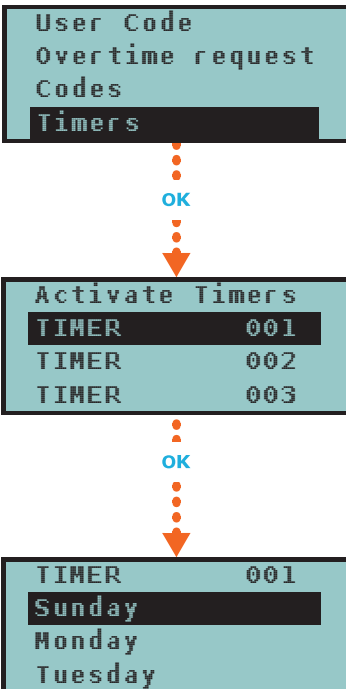
To associate a timer with a partition or a code, it is necessary to access the respective section in the user menu. The association of timers with keys must be done by the installer during the programming phase.

Access the "Timers" section of the user menu by typing-in a valid code PIN.

1. Use keys and to select the Timer then press **OK**.
2. Using the same keys, select the day of the week.
3. Select an activation or a restoral of the timer.
4. Set the selected time (expressed in hours and minutes) by means of keys and then, using keys and select the number.
5. Press **OK** to confirm and exit.

It is also possible to program only activation or only reset of the timer.

The field that does not require programming must be set as "--".



7-3-15

Partition status enquiry



This function will allow the control panel to announce in sequential order the descriptions of the partitions and their respective armed/disarmed operating status.

The user code must be enabled (by the installer) to activate shortcut n.17 via keys **F1 Fn**, ..., **F4 Fn** or the number keys.

After entering a valid user-code, press the key which is assigned to the shortcut.

The control panel will announce the status only of the partitions associated with the code.

Note

7-4

Operations via touch-screen keypad

7-4-1








Function buttons

The keypad user-interface is shown as a menu of function keys. The keys are visualized as icons which activate the respective functions when tapped on the touch screen.

The following table provides a description of the function keys displayed on the home page. The home page coincides with the page that is displayed when the user has not activated any function or application, or has simply not touched the display for at least 45 seconds.

Some of these keys activate their assigned functions after entry of a user code that opens a session, which is closed by tapping "Logout" button on the top right of the Home page or after 45 seconds inactivity on the keypad.

Table 7-15: Touch-screen keypad menu

Icon/key	Function	Code required
	SCENARIOS Accesses the section containing the list of programmed scenarios which can be activated. Refer to <i>paragraph 7-4-3 Arming commands and scenarios</i> .	No code required for access. Depending on programming, the activation of scenarios may require code entry.
	COMMANDS Accesses a section containing the list of outputs which can be activated. Refer to <i>paragraph 7-4-7 Outputs management</i> . The outputs are divided in two sections: <ul style="list-style-type: none"> • "Domotics", outputs for the management of home automation • "Intrusion" outputs programmed through the intrusion-control system 	<ul style="list-style-type: none"> • "Domotics", no code required • "Intrusion", code required.
	INTRUSION This accesses a section where the user can view and change the status of parts of the intrusion-control system: <ul style="list-style-type: none"> • "Partitions" - section where the user can view and change the status of the partitions. • "Zones" - section where the user can view and change the status of the zones. • "Events Log" - section where the user can view the events log. Refer to paragraphs <i>7-4-2</i> , <i>7-4-3</i> and <i>7-4-6</i> .	User code required.
	MENU Accesses two sections: <ul style="list-style-type: none"> • "Actions" - which lists the control panel commands in the event of alarm, tamper or overtime requests. Refer to paragraphs <i>7-4-2</i> and <i>7-4-12</i>. • "Activations" - where it is possible to view and enable the activations described in <i>paragraph 7-4-5 Activations</i>. 	User code required.
	SETTINGS Accesses the sections for the settings of the keypad and the Sol control panel: <ul style="list-style-type: none"> • "Display settings" - provides information regarding the settings of the keypad the user is working on. It shows the model, firmware revision and the address of the keypad and built-in reader. Furthermore, it allows the user to modify the viewing mode of the display by changing the available screen options by means of the + and - keys. Refer to <i>paragraph 7-4-9 Keypad settings</i>. • "Date/Time", "Change PIN", "Tel.Numbers" - these sections allow the user to change the date and time on the control panel clock, the user PINs and the contact phone numbers saved to the memory. Refer to paragraphs <i>7-4-8</i>, <i>7-4-10</i> and <i>7-4-11</i>. • "Installer" - this section allows access to the installer menu after entry of a valid installer PIN, thus putting the control panel in programming mode. • "Alphanumeric keypad" - this section allows the user to work on the touch-screen keypad as if it were an LCD keypad. Tap the HOME button to step back to the standard mode. 	User code required. Installer code required for the "Installer".
	SYSTEM Accesses a section where it is possible to view the system parts: <ul style="list-style-type: none"> • List of ongoing faults • Power-supply voltage of the control panel • Information on the GSM communications module Refer to <i>paragraph 7-4-6 View</i> .	User code required.
	APPS Accesses the keypad applications: <ul style="list-style-type: none"> • "Voice functions" - accesses a section where the user can activate the control panel voice board functions. Refer to <i>paragraph 7-4-4 Voice memo</i>. • "Maps" - accesses the system by means of the graphic maps (refer to <i>Capitolo 10</i>, <i>Graphic maps</i>). • "Alarm clock" • "Memo" - application for the programming and activation of audible signalling and pop ups (refer to <i>paragraph 7-5 Alarm clock and memo</i>). 	No code requested

Alarm management

7-4-2

The typical operations the user must perform in the event of alarms and/or tamper conditions are:

- Stop the ongoing alarms by deactivating the outputs related to the system alarm and tamper events.
- Cancel the entire call queue and stop ongoing calls (if any).
- Delete the alarm and tamper memories.

To perform these operations, it is necessary to access the "Menu" section, enter the user code and then access the "Actions" section.

This section contains a list of control panel commands which can be activated by means of the **ACTIVATE** button.



7-4-3

Arming commands and scenarios

The touch-screen keypad allows users to activate the programmed scenarios and also set up the arming mode of the partitions the users control (have access to):

In the case of arming requests in conditions of reduced security (partitions not ready or faults present) the keypad will show the list of causes of reduced security.

SCENARIOS



- Access "Scenarios" section This section provides a list of the scenarios which can be activated by means of the **ACTIVATE** button.

Tapping the bottom bar on the home page will open (for 3 seconds) a window containing a list of the active scenarios. If required by programming, the system may request entry of a valid user code ("Show scenario with code", *paragraph 7-4-9 Keypad settings*).

PARTITIONS



- Access the "Intrusion" section, type-in the user code and then access the "Partitions" section.

This section displays the partitions separately. The user can scroll and select a partition by means of the right/left scroll buttons and then select the arming mode by means if up/down buttons.

- "D", to disarm.
- "A", to arm in Away mode (entire system armed)
- "S", to arm in Stay mode (system partially armed).
- "I", to arm in Instant mode (no delays)
- "N", not to change the operating status.

To apply the selected arming mode, press the **OK** button.

7-4-4

Voice memo



To access the voice functions via the touch screen keypad, you must first access the "Apps" section and then the "Voice functions" section.

Following is a list of the sections relating to each function which can be accessed by tapping the relative **ON** button:

- Record message in the voice memo box
- Playback message in the voice memo box
- Delete message in the voice memo box

These sections reproduce the same voice functions as those previously described for LCD keypads.

7-4-5

Activations



To activate (and deactivate) the elements of the Sol system via the touch-screen keypad, access the "Menu" section, enter the user code and then access the "Activations" section.

Following is a list of the sections relating to the elements the user can activate by pressing the **ACTIVATE** button.

Each section presents its own elements arranged in list form. Each element is associated with two buttons - **ON** for activation and **OFF** for inhibition, and an icon which changes in accordance with the status:

- - activated/enabled
- - deactivated/disabled

7-4-6

View

The touch-screen keypad provides sections for the visualization of the current status of all system elements.

The "Activations" (*paragraph 7-4-5 Activations*) and "Commands" (*paragraph 7-4-7 Outputs management*) sections allow status viewing of the activatable elements and outputs. It is possible to add other elements to these which can be reached through other sections:

- the events log (alarms, faults, arm/disarm operations, etc.), which shows the chronology with which the events occurred and were restored
- the status of the GSM communicator
- the control panel power-supply voltage, its firmware version and model
- the electrical status of the zones (stand-by, alarm, short-circuit, tamper) and their bypassed status
- any faults present (refer to *Appendix B, Fault signals*)

Access the "Intrusion" section and enter the user code. The following sections will be available:



- In the "Partitions" section, the partitions are listed and show their arming status, which can be changed, as described in *paragraph 7-4 Operations via touch-screen keypad*.

PARTITIONS

The "View partition status" option (refer to *paragraph 7-4-9 Keypad settings*) will allow the user to select the visualization mode of the operating status on the bottom bar of the screen:

- "Single partition" - the characters relating to the operating status of the partitions will be shown, as described in *Table 7-2: Display visualization*
- "Single scenario" - the description of the active scenario will be shown

- In the "Zones" section, the zones are listed in this and show their status icons (positioned to the left of each zone description):

ZONES

- , green spot - stand-by status
- , red spot - alarm status
- , yellow triangle - fault/tamper

Each zone is associated with two buttons, **ON** for activation and **OFF** for inhibition, and an icon which changes in accordance with the status:

- , activated/enabled
- , deactivated/disabled

- In the "Events Log" section, all the events saved to the log are displayed one at a time, however, the up/down buttons will allow the user to scroll the entire list of events. Each event shows the relative details and, where possible, allows the user to view the partitions involved by means of the **PARTITIONS** button.

EVENTS LOG



Access the "System" section and enter the user code. The following sections will be available:

- The "Faults" section allows the user to view all the faults present on the system and, where possible, the fault details by means of the **DETAILS** button.
- The "Voltage" section allows the user to view the control panel power-supply voltage.
- The "Sol-3G info" section allows the user to view the parameters of the GSM communicator.

ONGOING FAULT

VOLTAGE

GSM

Table 7-16: View GSM Status

Line	View
1	<ul style="list-style-type: none"> • Mobile network provider (on the left side) • "--" indicates that the GSM card is present in the control panel • "C" means that data transfer is in progress • data network technology (on the right side) <ul style="list-style-type: none"> G, GPRS service 3G, UMTS service H, HSPA service
2	GSM signal reception (value between 1 and 100)
3	balance, at the last operation (expressed in the local currency)
4	Presence of ongoing faults

Status viewing and monitoring of the Sol system elements is also possible via the graphic maps, accessible through the "Maps" section in the "Apps" section.

Via Graphic maps

Refer to *Capitolo 10 , Graphic maps*.



Outputs management

7-4-7

From a touch-screen keypad it is possible to activate/deactivate manually the outputs the code is enabled to work on.



Access the "Commands" section, where the following sections are available:

- "Home automation" - allows access to the outputs of the home-automation system, code entry not required.
- "Intrusion", for access to the outputs of the intrusion control system, code entry required.

The available outputs are listed in both sections.



The activatable outputs are associated with two buttons, **ON** for activation and **OFF** for deactivation, and an icon which changes accordingly:

-  - output activated
-  - output deactivated

7-4-8

Change date and time

The touch-screen keypad has a section where the user can set the date and time of the control panel and the required date/time format.

Access the "Settings" section, type-in a valid user code then access the "Date/Time - Change PIN - Change tel. num."

Changes can be made using the left/right and up/down scroll keys and confirmed by the **OK** key.



7-4-9

Keypad settings

Access the "Settings" section, type-in a valid user code and then access the "Display settings" section.

This section allows the user to view the firmware version of the control panel and change the parameter settings of the keypad in use.

The settings will be saved even in the event of control-panel shutdown.

- **Transparency** - intensity of the transparency effect
- **Brightness** - intensity of the screen brightness when the screen is touched and for the following 45 seconds
- **Stand-by brightness** - intensity of screen brightness when the keypad is in stand-by status
- **Buzzer volume** - buzzer loudness
- **Voice volume** - speaker loudness
- **Skin** - for the selection of one of the skins for the touch-screen
- **Language** - for selection of the language used by the control panel
- **View partitions** - for the viewing mode of the operating status of the partitions on the bottom bar of the display
- **Exit time** - enables/disables the audible signal during exit time
- **Entry time** - enables/disables the audible signal during entry time
- **Chime** - enables/disables the audible signal for the bell function
- **Brightness adjustment** - enables/disable the brightness sensor
- **Maps** - enables/disables the automatic start up of the graphic maps application when the keypad is in stand-by status
- **Show scenario with code** - enables/disables the request for user-code entry when the user taps the lower bar on the home page to view the active scenarios.
- **Emergency lights** - if enabled, the keypad brightness will increase to the maximum level during mains power-cut events and will remain so until the mains power restores to normal

Select the parameter using the up/down scroll keys and change it by means of the "+" and "-" keys. To confirm changes and exit the section press **SAVE**.

7-4-10

Change PIN

To change user code PINs via the touch-screen keypad, access the "Settings" section, enter a valid user code, then go to the "Date/Time - Change PIN - Change tel. num." section, then to the "Change PIN" section.

In this section it is necessary first to select the required code from those available on the list. The next step is to change the code by means of the buttons on the screen and confirm changes by pressing the **OK** button.



7-4-11

Edit telephone numbers

To edit telephone numbers via the the touch-screen keypad, access the "Settings" section, enter a valid user code, then go to the "Date/Time - Change PIN - Change tel. num." section, then to the "Change tel num" section.

In this section it is necessary first to select the required telephone number from those available on the list. The next step is to edit the number using the screen buttons and confirm changes by pressing the **OK** button.



Overtime request

7-4-12

Overtime requests via the touch-screen keypad can be activated by accessing the "Menu" section, entering a valid user code and then accessing the "Actions" section.

The section contains a list of control panel commands which can be activated by simply tapping **ON**, amongst which the "Overtime request".



Alarm clock and memo

7-5

The touch-screen keypad provides applications which allow the user to manage events which, as required, will activate a pop-up notification (audible and visual) on the display.

Programming and/or activation of alarm and memo events have no effect on the programming or regular functioning of the Sol control panel and its peripherals.

Note

The "Alarm clock" and "Memo" functions in the "Apps" section access lists that provide all the events and, for each, provide buttons for activation (**ON**, **OFF**) and programming (**SET**).

Each event can be programmed with:

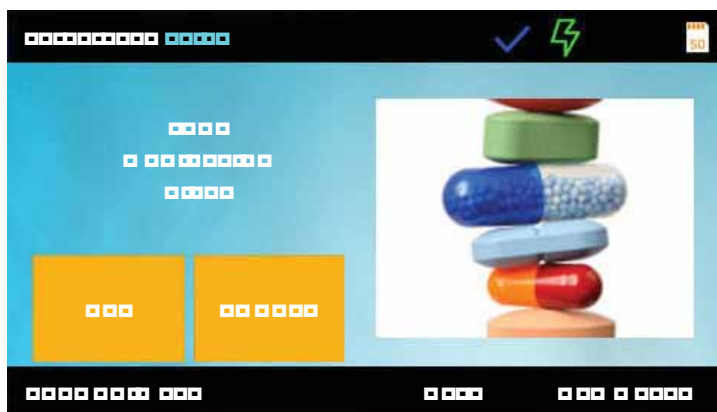
- description
- day the week, by selecting the respective button in the upper part of the "When?" section
- time, by changing the field selected with the arrows

For "Memo" events only, the user can also program:

- additional text
- day of the week or alternatively a specific date in the lower part of the "When?" section
- a second time, in the "When" section, by selecting **Time 1**
- if a specific date is programmed, the user will be able to set a regular interval (periodicity) in the lower part of the "When?" section and a time pattern (cadence) by tapping on the **OFF** button until the desired value is obtained.
- audible signals and images that correspond to the memo

Touching the "Alarm clock" or "Memo" button for at least 5 seconds will delete all the programming in the section concerned.

When activation of the appropriately programmed event occurs, a window will appear similar to the one shown here. The **OFF** button deactivates signalling, whereas the **SNOOZE** button defers it for 5 minutes.



Chapter 8

Readers and Keys

8-1 Proximity readers

Sol control panels can also manage an By/S or nBy/X reader integrated into the control panel frontplate.

Readers (also referred to as proximity readers) have 4 LEDs:

- **F1:** Red
- **F2:** Blue
- **F3:** Green
- **F4:** Yellow

Each reader is enabled to operate on specific partitions, whereas each key is enabled to operate only on the partitions the user is allowed to control. Therefore, if a key is held in the vicinity of a reader, it will be possible to control only the partitions which the two devices have in common.

Each reader can be programmed with up to 4 shortcuts (one per LED).

If the keypad is equipped with a buzzer, the latter will signal the running entry, exit and pre-arm times on the enabled reader partitions (refer to *paragraph 5-2 Signalling on the Buzzer*).

8-1-1 Signalling on reader LEDs

The LEDs have two distinct operating modes:

- When no key is present at the reader (refer to *Table 8-1: Reader LEDs with no key at reader*), the LEDs will indicate the current status of the associated shortcut.
- When a key is present at the reader (refer to *Table 8-2: Reader LEDs with key at reader*), the LEDs will indicate, in rapid succession, the available shortcuts.

Table 8-1: Reader LEDs with no key at reader

LED	Red	Blue	Green	Yellow
OFF (All LEDs Off)	All the reader partitions are disarmed. No alarm/tamper memory on the reader partitions or system tamper memory.			
ON / OFF (in accordance with the associated shortcut)	The scenario associated with the arming-shortcut of the red LED is active/inactive. The output associated with the output-activation shortcut of the red LED is active/inactive. Faults are present/not present.	The scenario associated with the arming-shortcut of the blue LED is active/inactive. The output associated with the output-activation shortcut of the blue LED is active/inactive. Faults are present/not present.	The scenario associated with the arming-shortcut of the green LED is active/inactive. The output associated with the output-activation shortcut of the green LED is active/inactive. Faults are present/not present.	The scenario associated with the arming-shortcut of the yellow LED is active/inactive. The output associated with the output-activation shortcut of the yellow LED is active/inactive. Faults are present/not present.
Intermittent blinking (ON: 2.3sec OFF 0.1sec)	At least one Reader-partition is armed.			
Slow blinking (ON: 0.5sec OFF 0.5sec)	The reader partitions are disarmed. Alarm/tamper memory on at least one of the reader partitions, or system tamper memory.	The scenario associated with the last key used is active.		
Fast blinking (ON: 0.15sec OFF 0.15sec)	At least one Reader-partition is armed. Alarm/tamper memory on at least one of the reader partitions, or system tamper memory.			

Table 8-2: Reader LEDs with key at reader

LED	Red	Blue	Green	Yellow
OFF (no light)	Request to arm ALL the partitions common to both the key and reader.			
ON (only one LED On)	Request to activate the shortcut associated with the red LED on the reader or the first shortcut of the key	Request to activate the shortcut associated with the blue LED on the reader or the second shortcut of the key	Request to activate the shortcut associated with the green LED on the reader or the third shortcut of the key	Request to activate the shortcut associated with the yellow LED on the reader or the fourth shortcut of the key
ON (All the LEDs On)	Request to activate the shortcut associated with the key.			
Fast blinking (ON: 0.15sec OFF 0.15sec one LED only)	If the shortcut associated with the red LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.	If the shortcut associated with the blue LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.	If the shortcut associated with the green LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.	If the shortcut associated with the yellow LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.
Fast blinking (ON: 0.15sec OFF 0.15sec ALL LEDs)	If the shortcut associated with the key is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.			

If a key is present, all operations (arm, disarm, etc.) will apply only to the partitions common to both the key and reader.

Note

If the installer has enabled the "LED Off reader" option (or "50131LedOFFLett." on keypads option), the reader LEDs will remain Off when there is no key in the vicinity of the reader (in order to hide the armed status of the partitions).

READER LED OFF

Keys

8-2

The Sol system is capable of managing contact-free electronic keys, which INIM electronics offers in various versions:

- tags for proximity readers
- cards for proximity readers
- keyfobs (remote-control keys)

Each key is unique and is identified by a random code selected from over 4 billion code combinations. During the system programming phase, the installer enrolls each key on the control panel in order to allow the system to recognize it when it is used.

Each key is characterized by the following parameters (programmed by the installer) in accordance with the requirements of the key user.

- The **Partitions** it is enabled to control. If a key is used at a reader, it can operate only on the partitions the two devices have in common. For example, if the key controls partitions 1, 3, and 5 and the reader controls partitions 1, 2 and 6, the key can operate on partition 1 only, as it is the only partition the key and reader have in common. If a button on the remote-control is pressed, the user will be allowed access only to the partitions the device is assigned to.
- Up to 4 **Shortcuts**.
- A **Timer** can be set up to restrict the use of a key. The system will allow the key to operate the system only when the Timer is active. In this way, the user will be unable to access the system at all other times.
- **Patrol** attribute - this option is usually enabled on keys used by security personnel or night watchmen for patrol purposes. This type of key does not allow the user to select the "Arm Type". When a key with this attribute is recognized, the system will perform the following operations:
 - Disarm the partitions common to the key and reader concerned.
 - Activate the respective Patrol Time for the partitions concerned.
 - Re-arm the partitions (as before) when the Patrol Time expires.

If the patrol key is held in the vicinity of the reader while the Patrol Time is still running (for example, if the inspection ends ahead of time), the Patrol Time will end immediately and the partitions will arm as before.
- The **Maintenance** option allows keys to deactivate instantly any outputs associated with zone and partition alarm/tamper events (on the Partitions the key and reader have in common). This type of key can select the reader shortcuts and its customized (personal) shortcuts.






8-2-1

Wireless keys (remote-control keys)

The wireless keys have 4 buttons which can each be programmed with a shortcut. It is possible to choose between two different graphics symbols for the buttons.

Remote-controls have 5 LEDs, 4 of which are associated with buttons and the other is a confirmation LED. Thanks to two-way communication (transceiver), the LEDs and buzzer on the remote-control keys provide users with feedback signals that notify them of the successful outcome or failure of the requested operation:

Table 8-3: Feedback signals provided by wireless keys

Button	Icon	LED 1	LED 2	LED 3	LED 4	Buzzer signal	Operation
F1		1 flash				beep	Activates shortcut 1
F2			1 flash			beep	Activates shortcut 2
F3				1 flash		beep	Activates shortcut 3
F4					1 flash	beep	Activates shortcut 4
F2 + F3			1 flash	1 flash		beep	Block/Unblock remote-control device
Any				4 flashes	4 flashes		Remote-control device blocked

Note

If an operation is successful, but the corresponding LED fails to light, it is an indication that the battery is low.

The battery must be replaced before it runs out completely.

Table 8-4: Control panel signals over wireless keyfob

Feedback from panel	Confirmation LED - green	Confirmation LED - red	Buzzer signal
Command not received		1 flash	
Operation not done		4 flashes	bop
Operation done	3 flashes		long beep

8-3

Reader and key operations

8-3-1

Alarm management

The operations that users can perform via proximity readers or keys, in relation to alarm and/or tamper events, depend on the programming of the associated shortcuts.

Via Reader

Hold a valid key in the vicinity of the reader until the reader LEDs or display indicates "Stop alarms" (shortcut n.2), "Clear call queue" (shortcut n.3), "Delete call memory" (shortcut n.4).

Via Wireless key

Push the respective button on the wireless key and verify the outcome of the requested operation, as described in *paragraph 8-2-1 Wireless keys (remote-control keys)*.

8-3-2

Arming commands and scenarios

Via a reader or key it is possible to activate the programmed scenarios for the associated shortcuts:

Via Reader

Hold a valid key in the vicinity of the reader and remove it when "Arm/Disarm" (shortcut n.1) is indicated on the LEDs (the system will apply the preset scenario).

Via Wireless key

Push the respective button on the wireless key and verify the outcome of the requested operation, as described in *paragraph 8-2-1 Wireless keys (remote-control keys)*.

8-3-3

Outputs management

The activations and deactivations that users can perform via proximity readers or keys depend on the programming of the associated shortcuts.

Hold a valid key in the vicinity of the reader until the reader LEDs or display indicates "Activate output" (shortcut n.5), "Deactivate output" (shortcut n.6).

Via Reader

Push the respective button on the wireless key and verify the outcome of the requested operation, as described in *paragraph 8-2-1 Wireless keys (remote-control keys)*.

Via Wireless key

Overtime request

8-3-4

The overtime request via proximity reader or key is possible through one of the appropriately programmed associated shortcuts.

Hold a valid key in the vicinity of the reader until the reader LEDs or display indicates "Overtime" (shortcut n.7).

Via Reader

Push the respective button on the wireless key and verify the outcome of the requested operation, as described in *paragraph 8-2-1 Wireless keys (remote-control keys)*.

Via Wireless key

Chapter 9

Commands over-the-phone

9-1 Use of telephone calls

9-1-1 Panel to user calls

The installer will instruct the user as to which events generate voice calls. Event report calls will be sent to the selected contact numbers as the event occurs and, in most cases, also when it ends.

During the call, the call recipient can:

- press "*" on the phone keypad, go to the next message in the queue or, if there is only one message, end the successful call.
- type-in their code PIN on the phone keypad followed by "#" and access the customized shortcuts assigned to the code. The control panel will activate the voice guide which will announce the available shortcuts and the number keys to press. The respective shortcut will activate when the key indicated by the voice guide is pressed.

9-1-2 User to control panel calls

If the "Answerphone" function (refer to *paragraph 6-5 Activations*) is enabled, the user can call the control panel from any remote phone and send commands to the system (refer to *paragraph 4-2 Shortcut with code*) and/or activate Listen-in sessions (refer to *paragraph 6-11 Listen-in*).

1. Dial the control panel telephone number.
2. The control panel will answer after the programmed number of rings and will play message n.262: "Enter valid code followed by #".
3. Type in the user code PIN followed by "#".
4. The control panel will activate the voice function which will announce the available shortcuts and the number keys to press.
5. As soon as the selected number is pressed on the telephone keypad, the control panel will activate the corresponding shortcut.

If the system is equipped with a GSM communicator, the user can send commands to the control panel also by phoning the number of the SIM card inside the device. If appropriately configured (by the installer), the user will receive an SMS text message or a feedback ring from the GSM communicator confirming the successful outcome the command.

9-2 Use of SMS text messages

9-2-1 SMS text from control panel to user

If the Sol control panel is equipped with a GSM communicator, users can receive SMS text notification of events.

If an event (appropriately programmed by the installer) occurs or restores, the control panel will send an SMS text notification to the programmed contact numbers.

9-2-2 SMS text from user to control panel

If the Sol control panel is equipped with a GSM communicator, users can send commands to the control panel via SMS text messages to the number of the SIM card inserted in the device.

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> this is the command identifier, this parameter must be provided by the installer.

If appropriately configured (by the installer), the user will receive an SMS text message or a feedback ring from the GSM communicator confirming the successful outcome the command.

By default, commands are predefined and can be modified by the installer:

- **"CREDIT"** - for balance enquiries relating to the SIM card of the GSM communicator, the user will receive an SMS text indicating the remaining credit.
- **"STATUS"** - for status enquiries relating to the GSM communicator, the user will receive an SMS text containing 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

Operations via telephone

9-3

Alarm management

9-3-1

The operations that can be performed via the keypad in the event of alarm or tamper are:

- Stop alarms
- Clear call queue
- Delete memory

Type-in the PIN of an authorized user followed by **"#"** on the telephone keypad, then press the key (from **"0"** to **"9"**) which the installer has programmed to "Stop alarms" (Shortcut n.2), "Clear call queue" (Shortcut n.3), "Delete memory" (macro n.4).

Arming commands and scenarios

9-3-2

Type in an enabled code PIN followed by **"#"**. Press the number key (from **"0"** to **"9"**) associated with the "Arm/Disarm" shortcut (shortcut n.1) in order to apply the pre-set scenario.

Activation of outputs

9-3-3

Type-in the PIN of an authorized user code followed by **"#"** on the telephone keypad, then press the key (from **"0"** to **"9"**) which the installer has programmed to activate "Activate output" (Shortcut n.5) or "Deactivate output" (Shortcut n.6).

Overtime request

9-3-4

Type-in the PIN of an authorized user code followed by **"#"** on the telephone keypad, then press the key (from **"0"** to **"9"**) which the installer has programmed to activate "Overtime" (shortcut n.7).

9-3-5

Listen-in



Type-in the PIN of an authorized user code followed by “#” on the telephone keypad, then press the key (from “0” to “9”) which the installer has programmed to activate “Listen-in” (shortcut n.10).

The control panel will open a Listen-in channel between the user on the phone and the control panel itself.

Press “*”, to end the Listen-in phase and step back to the voice-announced Shortcut menu.

9-3-6

Partition status enquiry

Type-in the PIN of an authorized user code followed by “#” on the telephone keypad, then press the key (from “0” to “9”) which the installer has programmed to activate “Arming status” (shortcut n.17).

The control panel will announce (in order) the descriptions of the partitions the entered PIN is assigned to and their current armed/disarmed status.

Press “*”, to step back to the main menu to listen to all the voice announcements relating to the entered PIN.

Graphic maps

Chapter 10

The Sol control panel provides monitoring functions are based on graphic maps which the user can access through a touch-screen keypad.

The graphic maps are linked together in a tree structure that allows the user to view the status of every part of the security system and interact with it through the icons shown.

The touch-screen keypad can manage up to 10 maps and the Web interface up to 20 maps. Each map supports up to 20 objects/buttons represented by icons.

The type of icon used and its function as a default button is described in the following table. It is possible to change these functions during the programming phase and associate each icon with a descriptive string or even make use of customized icons.

The Graphic map function requires installation of a micro-SD board. If this board is not installed the **MAPS** button will show the message "no SD-card" and the application will not start.

Note

Via touch-screen keypad

















Access the "Apps" section, then the "Maps" section.

Table 10-1: Graphic map icons at default

Subject	Icon	Button
Link		Link to the home page of the touch-screen keypad
		Map link
Partition		Partition armed in Away mode
		Partition armed in Away mode
		Partition armed in Instant mode
		Partition disarmed
		Partition alarm/tamper memory
		After a valid code entry a window will open where the user can select the required arming mode.

Table 10-1: Graphic map icons at default

Subject	Icon		Button
Zone		Zone shorted/tamper Zone alarm/tamper memory	After a valid code entry the zone will change its activation status
		Zone in stand-by status	
		Zone in alarm status	
		Zone disabled/bypassed	
Output		Output activated	Output switches status
		Output deactivated	
Scenario		Scenario active	/
		Scenario inactive	After a valid code entry the user can activate the scenario
Ongoing fault		Scenario active	Accesses the faults viewing section
		Scenario inactive	
Reset partitions			After a valid code entry the user can deactivate instantly the outputs relative to alarm and tamper events and clear the alarm and tamper memory
Clear call queue			After a valid code entry the user can clear the call queue completely and interrupt any ongoing call.
Stop alarms			After a valid code entry the user can deactivate instantly the outputs activated by zone/partition alarm and tamper events and system tamper events.
View events log			After a valid code entry the user can access the events log

Glossary

Appendix A

Detection of non-authorized entry into the protected building. Generally the activation of a detector.

ALARM

In the event of:

- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper
- peripheral loss
- false key

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

ALARM OR TAMPER MEMORY

This is a private service that monitors premises protected by intrusion control systems equipped with digital communicators 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.

ALARM RECEIVING CENTRE (ARC)

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.

ANSWERPHONE

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.

ARM/DISARM

The user 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-ARM

This is the secondary power source of the system. If primary (230 Vac) power failure occurs, the battery will take over.

This is a 7V sealed battery that is kept constantly charged and efficient by the control panel and by the primary power source.

BACKUP BATTERY

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).

BYPASS - ZONE DEACTIVATION

A list of outgoing event-associated calls the control panel must send to programmed contact numbers.

Enabled users can clear the call queue manually.

CALL QUEUE

The Cloud is a web service that provides data storage space ("cloud storage") that, by means of any Internet connection, is accessible at any time and from any place. The data are then shared over the network, along with the resources to process them ("cloud computing") with all users who have a valid access.

The Cloud provider guarantees therefore that the user has both the resources for the processing and editing of data, and data synchronization that can be accessed and modified by multiple users without the risk of being lost.

CLOUD

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:** assigned to the installer of the security system
- **User code:** assigned to the end-user of the security system

CODE

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.

DEFAULT SETTINGS

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.

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.

This is an explicit user-command which ends signalling on the red and yellow LEDs on keypad and readers for the following events:

- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper
- peripheral loss
- false key
- ongoing fault
- memory fault

If a user deletes the alarm/tamper memory, the visual signals on the reader/keypad LEDs will clear.

This device allows the control panel to send report calls to Alarm Receiving centres (ARC). In Sol control panels the digital communicator is optional.

The time (expressed in minutes or seconds) that the system allows the user to disarm the partition after zone violation. If the system is not disarmed within the set time it will generate an alarm.

Each partition can be programmed with its own Entry time.

An operative status recognized by the system.

For example: detector alarm, mains failure (230V~), blown fuse, user-code recognition, etc., are all events recognized by the control panel.

Each event is 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
- activation of an output scenario
- 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
- activation of shortcut functions

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

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.

A condition which indicates that a system component is not working properly.

Some faults can jeopardize the performance of the entire system. Typical faults are Mains failure (230V~), telephone line-down and low battery.

DELAYED ENTRY ZONE

DELAYED EXIT ZONE

DELETE ALARM/ TAMPER/FAULT MEMORY

DIGITAL TELEPHONE DIALER

ENTRY TIME (OR ENTRY DELAY)

EVENT

EVENTS LOG (OR EVENTS MEMORY)

EXIT TIME (OR EXIT DELAY)

FAULT

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.

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.

This is an explicit user-command which ends signalling on the red and yellow LEDs on keypad and readers for the following events:

- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper
- peripheral loss
- false key
- ongoing fault
- memory fault

If a user deletes the alarm/tamper memory, the visual signals on the reader/keypad LEDs will clear.

This device allows the control panel to send report calls to Alarm Receiving centres (ARC).

In Sol control panels the digital communicator is optional.

The time (expressed in minutes or seconds) that the system allows the user to disarm the partition after zone violation. If the system is not disarmed within the set time it will generate an alarm.

Each partition can be programmed with its own Entry time.

An operative status recognized by the system.

For example: detector alarm, mains failure (230V~), blown fuse, user-code recognition, etc., are all events recognized by the control panel.

Each event is 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
- activation of an output scenario
- 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
- activation of shortcut functions

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

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.

A condition which indicates that a system component is not working properly.

Some faults can jeopardize the performance of the entire system. Typical faults are Mains failure (230V~), telephone line-down and low battery.

DELAYED ENTRY ZONE

DELAYED EXIT ZONE

DELETE ALARM/ TAMPER/FAULT MEMORY

DIGITAL TELEPHONE DIALER

ENTRY TIME (OR ENTRY DELAY)

EVENT

EVENTS LOG (OR EVENTS MEMORY)

EXIT TIME (OR EXIT DELAY)

FAULT

A map is an graphic representation of part of the area supervised by the security system and identified by an image file. The entire system can be represented by maps which can be linked together.

Each map can contain objects represented by icons. These icons are capable of changing status in accordance with the objects they represent and can operate as activation buttons for specific functions.

The user, by means of access to a graphic map, can view the supervised area and also access the security system functions.

An object can be:

- Partition
- Zone
- Output
- Map link
- Button

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.

A proprietary 4-conductor bidirectional digital high-speed communication line used to connect its peripherals to the control panel.

The 4 easily identifiable wires, on the control panel motherboard and on the expansions, are:

- “+” 12 Volt power supply
- “D” data
- “S” data
- “-” Ground

The installer code is generally characterized by a PIN (4, 5 or 6 digits) through which the installer, by entering it on a keypad or using in the software program (provided that all the system partitions are disarmed) has access to the programming menu and can check and change all the system parameters.

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 PC equipped with Sol software.

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.

A camera is an electronic instrument that records two-dimensional image sequences. It is part of a telesurveillance system monitored by an intrusion-control panel.

The IP camera (or “webcam”) transmits video images to an URL address, for direct viewing or for storage of the recorded material.

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).

This device allows users to access and control the system.

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 signalling devices, etc.

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.

The control panel must always be placed in “Maintenance” mode before the installer starts work on the system, otherwise the system will generate false alarms (tamper and intrusion). The other functions of the control panel are still available (arm/disarm operations, events, calls, etc.).

An electrical output point connected to a signalling or control device activated/deactivated by the control panel in response to programmed events.

The terminal of the device is connected to must be configured as an “output”.

Outputs are usually connected to audible or visual signalling devices but can be used for other purposes such as: switching on lights or opening doors/gates.

This is the configuration of the activation mode of several outputs at the same time.

For each output it is possible to set the digital status (On - Off).

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

Signalling that can be associated with a state of emergency perceived by the user and signalled to the intrusion control panel by means of a button or the activation of a shortcut.

This type of signalling generates an event which activates the programmed outputs and calls. This type of signalling does not activate the red LEDs on keypads and readers nor is it visualized on the displays.

GRAPHIC MAP

GSM DIALER

I-BUS

INSTALLER CODE

INSTALLER MENU

INTERIOR ZONE

IP CAMERA

KEY

KEYPAD

MAGNETIC CONTACT

MAINTENANCE

OUTPUT

OUTPUT SCENARIOS

PANIC

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).

This refers to the status of a partition as requested by the user.

The user can carry out the following operations.

- **Disarm** - this command disables the partition completely. During this status, none of the zones belonging to the partition can generate alarms.
- **Away mode** - this command enables "Away mode" operating status on the partition. During this status, all of the zones belonging to the partition can generate alarms.
- **Stay mode** - this command enables "Stay mode" operating status on the partition. During this status, all the zones belonging to the partition, with the exception of interior zones, can generate alarms.
- **Instant mode** - this command enables "Instant mode" operating status on the partition. During this status, all the zones belonging to the partition, with the exception of the interior zones, can generate instant alarms with no entry-time delay.
- **Hold** - this command forces the partition to hold its current status.

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.

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.

Device for management and use of the system, external to the control panel.

These are devices connectible to the control panel by I-BUS as well as wireless devices.

Sol control panels manage the following peripherals on the IBUS:

- Proximity Readers (nBy)
- Transceiver (Air2-BS200)

The following wireless devices can be added, and are recognized by the control panel as peripheral devices:

- Keypads (Air2-Aria/W)
- Sounders (Air2-Hedera)

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.

The installation site.

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

The primary source of electrical power to the system and, typically, is a network voltage @ 230V~ 50 Hz (115V60Hz in some states).

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.

This device allows users to access and control the system.

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.).

Configuration of the arming mode requested for each of the system partitions.

The shortcuts are control panel functions which, in a single operation, provide a fast way of carrying out specific operations which would normally require a series of activations.

They can be activated by the end-user (at keypads, on codes typed in at keypads or on remote telephones, at readers or on keys) or on the occurrence (activation) of an event.

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.

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.

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 sensors connected to the system zones, keypads, readers and control panel. Generally they are unauthorized access events on devices.

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

PARTITION

PARTITION ARM/ DISARM OPERATIONS

PATROL

PERIMETER ZONE

PERIPHERALS

PRE-ARM TIME

PREMISES

PRIMARY POWER SOURCE

READER

SCENARIO

SHORTCUT

SMOKE DETECTORS

SUPERVISION

TAMPER (OR ACT OF DELINQUENCY)

TELEPHONE ACTIONS

Screw terminal for the connection of zones (detection devices) or outputs (command/ signalling devices).

TERMINAL

A logical entity for automatic time-management of programmed peripherals or elements.

TIMER

Sol control panels manage 20 timers.

Each timer can be programmed to manage:

- Two activation times (ON) and two deactivation times (OFF) on preset days of the week.
- 15 timer-slot exceptions. Each "exception" refers to a specific interval of one or more days, for which it is possible to specify the time of activation (ON) and the time of deactivation (OFF).

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 times set for the day concerned.
- 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-equipped devices

TRANSCEIVER

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.

Each code is programmed with:

USER CODE

- 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

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

USER MENU

This device allows the control panel to send voice calls to programmed contact numbers.

VOICE DIALER

In Sol control panels the telephone dialer is provided by the SmartLogos30M board (to be installed on the control panel).

If the system is equipped with a SmartLogos30M board, it is possible to record a voice message for each control panel with voice functions present in the system configuration. Messages can be recorded, played and deleted as required.

VOICE MEMO

Software application that allows the user to view web contents over the Internet.

WEB BROWSER

Software application that processes web page requests from a web browser.

WEB SERVER

An intrusion control system whose devices (detectors, keypads, keyfobs) communicate with the control panel over radio waves.

WIRELESS

Usually, in wireless systems, only the control panel is mains powered (230V~), whereas the system peripherals are battery powered. The battery life is of utmost importance in the design layout and operational capacity of these systems.

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.

ZONE

A zone usually has only one device connected to it, however, it is possible (if the zone is appropriately wired and configured) to connect more than one device. If more than one device is connected, it will be impossible to identify precisely which device triggers the alarm.

Fault signals

Appendix B

The faults listed below are the faults that may be shown when accessing the user menu:

View, Faults ongoing, Faults log

Fault	Signalling on keypad	Occurs when...	Restores when ...	Control panel event
Battery fault	Low battery	The backup battery is low	The backup battery is charged	Yes
AC Mains failure	Mains failure	The primary power supply 230V~ fails	The primary power supply 230V~ is restored	Yes
Telephone line down	Tel. line down	The land line is not working	The land line restores	Yes
Jamming	Jamming	Wireless interference detected	Wireless interference cleared	Yes
Low battery on wireless zone	Low battery WLS	The battery of a least one wireless detector must be replaced	All the wireless detectors are running with sufficient power	Yes
Wireless zone loss	WLS zone loss			
GSM communicator faults	GSM fault	One of the faults below is present	None of the faults below are present	No
Insufficient cover	No signal			
GSM module communication fault	GSM module fault	The GSM module of the GSM communicator is not operating properly.	/	No
SIM communication fault	SIM commun. fault	The SIM card does not respond or is not present. The SIM card PIN is not disabled.	/	No
Low credit	Low credit	The credit left on the SIM card is below the minimum credit threshold.	/	Yes
Provider unavailable	ProviderUnavail.	The GSM network provider of the SIM in use is unavailable.	/	No
GPRS connection lost	IP conn. lost	The communicator detects connection problems on GPRS network	/	No
Contaminated smoke sensor	Detector dusty	The smoke chamber of at least one of the Air2-FD100 smoke detectors is contaminated by dirt or dust.	The contamination level of all detectors is below the programmed threshold	Yes
Violation of zones with faults	Faults on zones			
Internal resistance of battery too high	Int. Resistance	The internal resistance of the battery has exceeded the $R_{i\max}$ value.	The internal resistance of the battery returned to below the $R_{i\max}$ value.	Yes
Battery disconnected	Battery disconn.	The buffer battery is disconnected	The buffer battery is connected	Yes
Overvoltage on Aux	Overvoltage AUX	A voltage of over 14.5V detected on "+AUX" terminal	The normal voltage on the terminal has been restored.	Yes
Overvoltage on BUS power supply	Overvolt. BUS	A voltage of over 14.5V detected on the "+" terminal of the I-BUS	The normal voltage on the terminal has been restored.	Yes
Low voltage on Aux	Low voltage AUX	A voltage below 9.8V detected on the "+AUX" terminal	The normal voltage on the terminal has been restored.	Yes
Undervoltage on BUS	Undervoltage BUS	A voltage below 9.8V detected on the "+" terminal of the I-BUS	The normal voltage on the terminal has been restored.	Yes
Short-circuit on Aux	Short circuit AUX	Short-circuit detected on the "+AUX" terminal	The short-circuit is no longer present.	Yes
Short-circuit on BUS power supply	Short circuit BUS	A short-circuit has been detected on the "+" terminal of the I-BUS	The short-circuit is no longer present.	Yes
Overload on Aux	Overload AUX	A load of over 100mA detected on the "+AUX" terminal	The terminal restores to normal.	Yes
Overload on BUS power supply	Overload BUS	A load of over 200mA has been detected on the "+" terminal of the I-BUS	The terminal restores to normal.	Yes
Low battery on wireless keypad	Low battery WLS	The battery of a least one wireless keypad must be replaced	All the wireless keypads are running with sufficient power	No
Open/Dislodged-panel tamper	Control panel open			

Fault	Signalling on keypad	Occurs when...	Restores when ...	Control panel event
Keypad Tamper	Keypad tamper	A keypad signals tamper conditions	Tamper conditions clear on all the system keypads	Yes
Reader Tamper	Reader tamper	A reader signals tamper conditions	Tamper conditions clear on all the system readers	Yes
Keypad Loss	Keypad loss	A keypad cannot be found on the BUS	All keypads can be found on the BUS	Yes
Reader Loss	Reader loss	A reader cannot be found on the BUS	All readers can be found on the BUS	Yes
Internet connection loss	IP conn. lost	The IP connectivity test is enabled and the test result is negative (failed).	A connection attempt has been successful.	Yes

- a. Press the **OK** button to access the list of devices affected by the fault.
- b. Press the **OK** button to access the list of the ongoing faults.

Informative notice regarding the disposal of electrical and electronic equipment (applicable in countries with differentiated waste collection systems)

WEEE

The crossed-out bin symbol on the equipment or on its packaging indicates that the product must be disposed of correctly at the end of its working life and should never be disposed of together with general household waste.

The user, therefore, must take the equipment that has reached the end of its working life to the appropriate civic amenities site designated to the differentiated collection of electrical and electronic waste.

As an alternative to the autonomous-management of electrical and electronic waste, you can hand over the equipment you wish to dispose of to a dealer when purchasing new equipment of the same type.

You are also entitled to convey for disposal small electronic waste products with dimensions of less than 25cm to the premises of electronic retail outlets with sales areas of at least 400m², free of charge and without any obligation to buy.

Appropriate differentiated waste collection for the subsequent recycling of the discarded equipment, its treatment and its environmentally compatible disposal helps to avoid possible negative effects on the environment and on health and favours the re-use and/or recycling of the materials it is made of.

**Information about disposal of batteries and accumulators (applicable in Countries with separate collection systems)**

This marking on batteries and/or their manual and/or their packaging, indicates that batteries of these products, at the end of their working life, should not be disposed of as unsorted municipal waste, but must be object of a separate collection. Where marked, the chemical symbols Hg, Cd o Pb indicate that the battery contains mercury, cadmium or lead above the reference levels of the directive 2006/66/EC. If batteries are not properly disposed of, these substances, together with other ones contained, can cause harm to human health and to the environment.

To protect human health and the environment, to facilitate treatment and recycling of materials, separate batteries from other kind of waste and use the collection scheme stated in your area, in accordance to current laws.

Before disposing of the batteries, it's appropriate to remove them from their holders avoiding to damage them or causing short circuits.





ISO 9001 Quality Management
certified by BSI with certificate number FM530352

Centobuchi, via Dei Laboratori 10
63076 Montepandone (AP), Italy
Tel. +39 0735 705007 _ Fax +39 0735 704912

info@inim.biz _ www.inim.biz



DCMUINE0SOLE-100-20190805