

USER'S MANUAL



The producer 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 the producer does not install this product directly, and due to the possibility that it may be used with other equipment not approved by Us; the producer 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 the producer. 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 the producer 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

The producer 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

The producer 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 the producer. Installation of this Product must be carried out in accordance with Our instructions in the product manual.

The information contained in this document is the sole property of the producer. No part may be copied without written authorization from the producer.

All rights reserved.

Hereby the producer declares that the Ability control panels are in compliance with the essential requirements and other relevant provisions of Directive 1999/5/CE (R&TTE).

The full declarations of conformity of the above-mentioned devices are available at URL: www.abilityprotection.biz

Warranty

Limited Warranty

Copyright

Directive 1999/5/CE compliance

Table of contents

Warranty	2
Limited Warranty	2
Copyright	2
Directive 1999/5/CE compliance.	2
Table of contents	3
Chapter 1 General information.	5
1-1 Description of the product and various models	5
1-2 Manuals	6
1-3 Operator Qualifications.	6
1-4 Technical Terminology – Glossary	6
Chapter 2 The Ability system.	7
2-1 Introduction	7
2-2 The Technologies.	8
2-3 nCode/S keypad	8
2-4 Reader - nBy.	11
2-5 User Codes	13
2-6 Keys	14
2-7 Multi-system access.	15
2-8 Telephone and voice functions.	15
2-9 Arming Scenarios.	15
Chapter 3 Shortcuts	16
3-1 Keypad shortcuts.	16
3-2 Shortcut with code.	17
3-3 Keys and readers shortcuts.	17
3-4 Shortcut list	17
Chapter 4 Using the system	18
4-1 Managing alarms	19
4-2 Arming and disarming partitions	19
4-3 Activations	20
4-4 View.	21
4-5 Activating/Deactivating outputs.	23
4-6 Change date and time	23
4-7 Keypad settings.	24
4-8 Change PIN.	24
4-9 Teleservice request	25
4-10 Overtime request.	25
4-11 Commands over-the-phone.	25
Appendix A Technical terminology and Glossary.	26
Appendix B Shortcuts at default	30
Appendix C Fault signals	31

Chapter 1

GENERAL INFORMATION

Description of the product and various models

1-1

Description: Intrusion control panel

Models: Ability 510M
Ability 510B
Ability 510V
Ability 1030M
Ability 1030B
Ability 1030V

Applicable Normative: CEI 79-2:1998+Ab:2000

Performance level: II

The following table describes the main features of the 6 control panel models:

Table 1: **Control panel - Main Features**

	Ability control panels					
	510M	510B	510V	1030M	1030B	1030V
Total terminals	10			30		
Terminals on panel	5			10		
Terminals on panel configurable as inputs	5			10		
Terminals on panel configurable as Rollerblind/ Shock	2					
Terminals on panel configurable as outputs	0			5		
Total zones	20			60		
Relay outputs on panel motherboard	1					
Open-collector outputs on panel motherboard	2 (150mA)			2 (500mA)		
Partitions	5					
nCode/S keypads	5			10		
FLEX5 Expansions	10			20		
nBy Readers	10			20		
Transceiver (Air2-BS100)	1					
Codes	10			20		
Scenarios	15					
Digital keys and keyfobs	20			50		
Timer	2					
Recordable Events	250					
Recording time for voice messages	/	30 sec.	60 sec.	/	30 sec.	60 sec.

Manuals 1-2

Installation Manual 1-2-1

The Installation Manual is not included in the package, however, it can be purchased directly from your retailer. It is the installer's duty to read all the Installation Manual thoroughly, in order to become familiar with all the components and operating procedures of the Ability system. In order to provide adequate protection, you (the installer) must adhere to all the manufacturer's guidelines relating to the active and passive security devices of this system. It is the installer's responsibility to inform the system users that, regardless of its capabilities, an intrusion alarm system is not a substitute for the necessary precautions building occupants must take to prevent intrusion.

User's Manual (this manual) 1-2-2

DCMUINE0ABILITY **MANUAL CODE**

1.60 **VERSION**

The User Manual is included in the package. You (the installer) should read carefully through it. Once the system has been installed, the installer must ensure that the User's Manual is available to the users for consultation, and that they fully understand how the system works and are aware of all the functions, settings and procedures.

Operator Qualifications 1-3

Installer 1-3-1

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

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

User 1-3-2

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

The most common operations can be carried out without code/key verification. This method must be expressly requested by the main user, as it considerably lowers the security level of the system and may cause false alarms, accidental arm/disarm operations, etc.

Technical Terminology – Glossary 1-4

In order to help you understand the terminology used in this manual and improve your knowledge of this system and its operating procedures, read carefully through the Technical Terminology – Glossary (refer to *Appendix A, Technical terminology and Glossary*).

The appendix contains the definitions of technical terms commonly used in the field of security, therefore, relevant to the Ability system.

Chapter 2

THE ABILITY SYSTEM

Introduction

2-1

The manufacturer wishes to thank you for choosing this Ability intrusion control system. Its advanced technology and user-friendly operations provide an extremely high level of protection combined with ease-of use.

The manufacturer recommends that all parts of this manual be read thoroughly before starting up Ability system. The user must be familiar with all the operating procedures of the Ability system and must follow the installer's instructions carefully. Once you have become accustomed to the day-to-day operations, your installer will explain and, if required, programme the advanced functions of the system.

A typical system comprises:

- Ability control panel
- intrusion detection devices (PIR or microwave detectors, magnetic contacts, linear beam detectors, etc.)
- system management peripherals (nBy proximity readers, nCode/S keypads)
- alarm signalling devices which generally signal the events detected by the system (sounders, flashers, etc.)

The keypad (nCode/S) is an extremely flexible peripheral device which allows you to manage the system with ease. The large graphic display provides all the information necessary for fast understanding of the system status and the steps to take in the event of an alarm. All users have secret codes (PINs) which allow them to access and control the system in accordance with their permitted access level.

The customizable voice technology of the Ability 510B/V and 1030B/V provides users with system status information over-the-phone.

nBy readers (2 versions available: nBy/S wall-mount and By/X flush-mount) allow you to access and control the system. Although these devices are not as flexible as keypads, they provide a quick and easy way of carrying out day-to-day operations such as arming and disarming the system. Authorized digital-key users can operate the system in accordance with their programmed access level (enabled functions, etc.) by holding the key in front of the proximity key reader.

All Ability control panels are capable of managing the "Air2" two-way wireless system. This system integrates wireless devices (detectors, keyfobs, etc.) into the hardwired environment.

The Ability intrusion control panel recognizes a large number of events (such as: alarm conditions, faults, tamper, key/code recognition, arm/disarm operations), and in response activates audible/visual signals and calls. The calls can be:

1. report calls to alarm receiving centres - via the most widely used reporting protocols.
2. voice calls (to contact numbers) which provide users with clear information regarding the system status and the events which have occurred on the protected premises (for Ability510B/V and 1030B/V only).

The Ability intrusion control panel also provides automatic facilities, such as:

- arm and disarm operations set up on a weekly basis
- simple yet useful access-control functions which allow the system to deny access to specific keys/codes at certain times
- pre-set activation/deactivation of household devices (building automation) such as courtesy lights
- other similar automatic facilities.



The Technologies

2-2

Expertise in the arena of total security and a commitment to precision and high quality allow our R & D professionals to deliver excellence in design technology and dependability through time.

EASY4U

2-2-1

This user-friendly tool provides an interesting array of graphic features and functions. Ability intrusion control panels are compatible with nCode/S keypads (equipped with 96x32 pixel graphic displays) only. The four-line alphanumeric display screen (16 characters per line) can be edited or used for customized user-operations. The keypad shortcuts allow time-consuming sequences to be transformed into simple keystroke actions. In this way, frequently-used or repetitive sequences of keystrokes can be eliminated. The shortcuts can be used for a variety of tasks and make operations less tedious and less error-prone. The use of customizable graphic-objects, which indicate the system status, helps users to understand the current situation.

Besides accepting various commands (Arm, Disarm, etc.), the nBy reader also allows users to manage the "shortcuts" programmed on the keypad.

nCode/S keypad

2-3

The Ability control panels manages nCode/S keypad. The keypads allow users to manage all aspects of the security system.

The nCode/S is equipped with:

- graphic display
- 23 keys
- 4 LEDs
- buzzer

The keypad is the device that allows authorized code users to control the entire system or specific partitions. However, system control can be extended to other building occupants who do not hold a valid code. The Ability intrusion control panel offers an array of innovative features. In addition to the traditional User menu (accessed by means of user-code entry), this system provides a series of shortcuts" (refer to "Shortcuts" in Appendix) associated with keys **F1 Fn**, **F2**, **F3**, **F4 POL**. Generally, intrusion control panels do not allow access to the system via keypad without code entry. However, by means of the customized (personal) shortcuts **F1 Fn** to **F4 POL**, it is possible to enable building occupants to access and operate the system without code entry.

Your installer will program the shortcuts to suit your requirements and explain how they are used. For example, it may be useful to allow all the building occupants to arm the system without code entry, as this operation increases the level of system security. However, operations which lower the level of system security should be reserved for code users only. Under normal circumstances, operations which increase system security can be allowed without valid-code entry whereas, operations which lower system security (Disarm, Delete Alarm/Tamper memory, Deactivate Alarm/Tamper outputs) should be allowed only after valid-code entry.

Each keypad is assigned (by the installer) to the partitions it controls.



Display - description

2-3-1

The brightness and contrast of the backlit-graphic LCD (96 x 32 pixel) can be adjusted by way of the respective options on the User Menu (refer to paragraph 4-7 *Keypad settings*).

The first line of the display shows the date and time.

The left side of the second line shows the characters that indicate the current status of the partitions the keypad is assigned to:

- 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 keypad










```
18:23 20/08/2011
DTPID
No alarms
No faults
```


If a partition has memory of an alarm or tamper condition, the character that represents the partition concerned will blink.

The right side of the second line shows several icons which provide visual information regarding the system. Their meanings are described in the following table.

Table 2: **The icons (shown on the second line of the display)**

Icon	Name	Not present	On solid	Blinking or interchanging icons
	Telephone line		Telephone line busy	(Icon blinking) Telephone line down
	Peripheral tamper	All peripherals are properly placed and all enclosures are closed.	At least one peripheral (keypad, reader, expansion) is in tamper status (enclosure open or device dislodged).	(Interchanging icon) All peripherals are properly placed and all enclosure covers are closed, however, tamper has been detected and cleared (Tamper memory).
	Peripheral Loss	All the peripherals in the system configuration are responding properly (Present).	At least one peripheral (keypad, reader, expansion) is not responding properly.	(Interchanging icon) All the peripherals in the system configuration are responding properly, however, loss of a peripheral has been detected and cleared (Peripheral Loss memory).
	Teleservice	Teleservice disabled	Teleservice enabled	
	Key			(Icon blinking) False key
	Control panel Tamper	The Control panel is properly placed and the enclosure is closed.	The Control panel is in tamper status (enclosure open or device dislodged).	(Interchanging icon) The Control panel is properly placed and the enclosure is closed, however, panel tamper has been detected and cleared (Panel tamper memory).

If duly programmed by the installer, the  icon will not be shown on the display when Teleservice is enabled.

Nota Bene

The third line shows zone alarms and zone tamper status.

The fourth line shows the faults status.

Display - standby status

2-3-2

- A)** If the control panel is in Maintenance status, the first line on the screen will show the string indicated in the figure. The characters "K03" indicate the address of the keypad itself (in the example, the keypad is at address 3).



```
MaintenK03
DTPID
No alarms
No faults
```

- B)** If a keypad partitions has Alarm or Tamper memory, the third line of the screen will flash the descriptions of the zones concerned every 3 seconds. In the event of partition alarm or tamper memory, the red LED on the keypad and the characters corresponding to the partitions concerned will blink.



```
18:23 20/08/2011
DTPID T
Panel T03
No faults
```

- C)** If the "View open zones of disarmed partitions" option is enabled, the third line on the screen will flash (approximately every 3 seconds) the descriptions of any zones which are not-in-standby status when the keypad partitions disarm. Any auto-bypassable zones will be shown in white on black background.

Case C is discernible from case B in the fact that in case B, the red LED on the keypad blinks.

Case C is shown only if case B is not present.

Nota Bene

Using the keypad 2-3-3

The following section describes how the keys are usually employed. Some of the keys may have specific functions which will be indicated when necessary.

Table 3: The keys

Keys	Name	Typical application
 	Number keys	Used to type in User PINs
	OK	Confirms the selected item (parameter, etc.)
	UP, DOWN	Navigate through the menu lists or adjust keypad volume
	LEFT, RIGHT	Scroll along the data rows (for example, partitions in the events log, etc.).
	C	Steps back on the open menu without changing the selected item (parameter, etc.).
	ESC	Exits the User menu without changing the selected item (parameter, etc.).
	ENABLE	Enables options (refer to paragraph 4-3 Activations)
	DISABLE	Disables options
	F1, F2, F3, F4 or function keys	Activate the associated shortcuts. Can be used also as Emergency keys (refer to paragraph 2-3-4 Emergency keys).

Emergency keys

This control panel provides 3 "key-duos" for Emergency Calls which can be activated by pressing the respective keys on any of the system keypads:

1. + = Fire Emergency
2. + = Ambulance Emergency
3. + = Police Emergency

Utilization of any of the "key-duos" will generate the respective events and actions (e.g. activation of outputs and calls).

To activate an emergency call, press simultaneously and hold keys + , or + , or + for at least 3 seconds until the selected emergency call is confirmed by a beep.

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

2-3-4

18: 23 20/08/2011
DTPID
No alarms
No faults

Press simultaneously


Nota Bene


Visual signals on the keypad LEDs 2-3-5

The following table describes the visual signals on the keypad LEDs.

Table 4: Keypad LEDs

LED	Red	Yellow	Blue	Green
OFF (no light)	All the keypad partitions are disarmed.	No faults present.	Open zones on the keypad partitions.	Primary power failure (230V a.c.)
ON (Solid)	At least one of the keypad partitions is armed.	At least one fault has been detected.	All the zones on the keypad partitions are in standby status: Ready to arm.	Primary power OK (230V a.c.)
Slow blinking (ON: 0.5sec OFF: 0.5sec)	All the keypad partitions are disarmed. Memory of alarm/tamper on at least one of the keypad partitions or memory of a system alarm.	No faults present. At least one of the zones on the keypad partitions is bypassed (OFF).		
Fast blinking (ON: 0.15sec OFF: 0.15sec)	At least one keypad-partition is armed. Memory of alarm/tamper on at least one of the keypad partitions or memory of a system alarm.	At least one fault has been detected and at least one of the zones belonging to the keypad partitions is bypassed (OFF).		

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

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

- Open panel tamper
- Dislodged panel tamper
- Expansion tamper
- Keypad Tamper
- Reader Tamper
- Expansion Loss
- Keypad Loss
- Reader Loss
- False key

Signalling on the Buzzer

The buzzer signals the running entry, exit and pre-arm time (refer to *Appendix A, Technical terminology and Glossary*) of enabled partitions.

Buzzer signal	Description
8 pulses with 5 second pause	Entry time
3 pulses with 5 second pause; 4 short pulses with 5 second pause during the final 20 seconds of the Exit Time	Exit time
1 pulse with 5 second pause	Pre-arm time

Emergency status

In the event of keypad configuration error or communication error between the system peripherals, the display will show one of the screens opposite. If this occurs, you must contact your installer immediately and get the fault cleared.

2-3-6

- nCode S -
FW RELEASE 1.00
NO COMMUNICATION
KO1

- nCode S -
FW RELEASE 1.00
NOT ENROLLED
KO1

2-3-7

Reader - nBy

The Ability intrusion control panels manage nBy/S and nBy/X readers. The proximity reader is the easiest way for users to interact with the Ability intrusion control system. The nBy/S model has been especially designed to mount to all types of surface by means of just two screws. It is also IP34 rated (heavy duty) and therefore suitable for outdoor use. It is equipped with a buzzer and 4 LEDs:

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

The Universal flush-mount nBy/X (**Patent Pending**) has been especially designed to integrate with all brands of cover plates. It is equipped with 4 LEDs (red, blue, green and yellow). Readers do not provide the same extent of system control as keypads, however, these devices are quick and easy-to-use and are extremely useful when carrying out day-to-day operations (arm/disarm partitions, etc.). Readers are usually located near the main entry/exit points of the protected building. These devices allow system access to valid keys only. The system readers are capable of recognizing the customized (personal) parameters of each individual user key. Each reader is enabled to operate on specific partitions, whereas each key is enabled to operate only on the

2-4



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 and each key can be programmed with up to 4 shortcuts. The user or the installer can choose, for each key, which shortcut to activate between the key or the reader shortcut.

Unlike most traditional readers (which generally carry out arm/disarm operations only), ABy readers also manage a series of useful shortcut commands. For example, it is possible to associate two shortcuts with the red and blue LEDs for arm and disarm operations, and a shortcut to the green LED for gate control, and yet another to the yellow LED for "Clear call queue" operations.

The buzzer signals the running entry, exit and pre-arm time of the reader partitions (refer to paragraph 2-3-6 *Signalling on the Buzzer*).



Signalling on the Reader LEDs 2-4-1

The LEDs have two distinct operating in modes:

1. If no key is present at the reader (refer to *Table 5: Reader LEDs with no key at reader*), the LEDs will show the current operating status of the reader partitions.
2. If a key is present at the reader (refer to *Table 6: Reader LEDs with key at reader*), the LEDs will indicate (in rapid succession) the shortcuts available for selection.

Table 5: Reader LEDs with no key at reader

LED	Red	Blue	Green	Yellow
OFF (no light)	All the reader partitions are disarmed. No alarm/tamper memory on the reader partitions or system tamper memory.			
ON (Solid)	The scenario associated with the arming shortcut assigned to the red LED is active.	The scenario associated with the arming shortcut assigned to the blue LED is active.	The scenario associated with the arming shortcut assigned to the green LED is active.	The scenario associated with the arming shortcut assigned to the yellow LED is active.
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 shortcut of the last key used at the reader 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 6: 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 reader/key shortcut associated with the red LED	Request to activate the reader/key shortcut associated with the blue LED	Request to activate the reader/key shortcut associated with the green LED	Request to activate the reader/key shortcut associated with the yellow LED
ON (All LEDs On).	Request to activate the customized 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.

Nota Bene

User Codes

2-5

Each User Code comprises a PIN for identification purposes, and a group of parameters which determines 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 only user code enabled at default is 0001. The PINs of the successive codes are 0002, 0003, etc.

The installer is not allowed to change User code PINs. The installer provides the system users with default user PINs which they must change immediately to PIN codes of their choice.



Each user code is characterized by the following parameters, programmed by the installer in accordance with specific user rank.

- **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 the code is enabled on partitions 1, 2, 3, 4 and 5 and the keypad is enabled on partitions 4 and 5, the user operations will affect partitions 4 and 5 only.
- **User Code Types (rank)** - There are two user code types (ranks), "Main User" and "User". "Main User" codes can disable ordinary "User" codes and change their PINs. However, a "Main User" code cannot be used to disable another "Main User" code or change its PIN. "User" codes can change their own PINs only.
- **Timer Restriction** - If a code is associated with one of the 2 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) the user can activate/deactivate the duly programmed outputs.
- **Menu sections** the user can access (refer to paragraph 2-5-1 Accessing the User Menu, point 1.).
- **Customized Shortcuts** - Each code can be programmed to manage:
 - up to 4 customized (personal) shortcuts assigned to keys **F1** **Fn** to **F4** **POL**
 - up to 10 customized (personal) shortcuts assigned to keys **0** **↵** to **9** **wxyz**

These shortcuts are available only after accessing the User Menu.

Accessing the User Menu

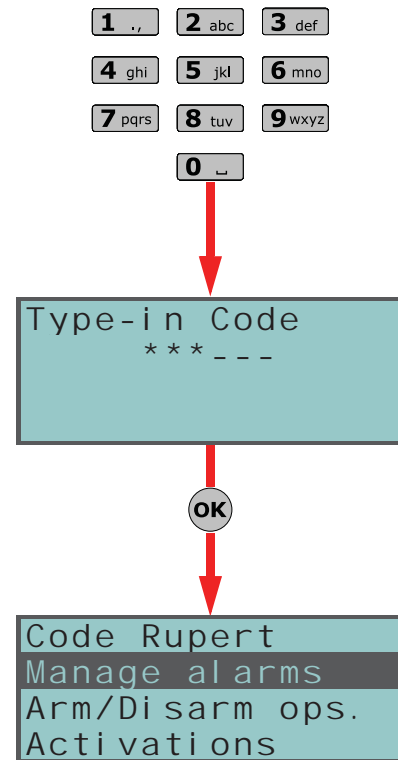
In order to access your customized (personal) menu, you must type in your PIN then press **OK**. At this point (see figure opposite) select with the keys

 and  the menu you require then press **OK** to open it. Following is a the list of available User-Menu sections:

- Manage alarms
- Arm/Disarm ops.
- Activations
- View
- Outputs ON/OFF
- Set date/time
- Set Keypad
- Change PIN
- Teleservice req.
- Overtime

The user can press the keys **F1** **Fn** to **F4** **POL** and **0** **↵** to **9** **wxyz** if these keys are associated with shortcuts.

Nota Bene



2-5-1

Keys 2-6

The Ability system is capable of managing contact-free digital-keys, which are available in three versions:

- **AbKey** - proximity tag
- **AbCard** - proximity card
- **Air2-KF100** - wireless keyfob

Each key is unique and is identified by a random code selected from over 4 billion code combinations. During the installation phase, each key is enrolled on the system in order to allow it to operate.

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

- **Partitions** - User codes can control only the partitions they are assigned to. 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 keyfob button is pressed, the user will be allowed access only to the partitions the wireless keyfob 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 who must patrol the protected premises at regular intervals. This type of key does not allow the user to select the "Arm Type". On acceptance of a Patrol key, the system will carry out the following actions:
 1. disarm the partitions common to the key and reader concerned
 2. activate the respective Patrol Time for the partitions concerned;
 3. 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.
- **Service** option - On acceptance of a key with this attribute, the system will deactivate any outputs associated with Zone alarm/tamper 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.



Air2-KF100 Wireless keyfobs

The KF100 keyfob has 4 remote-control buttons which can each be programmed with a shortcut (ask your installer for details). The graphic-choice feature allows you to identify the buttons by numbers or icons.

The keyfob also provides 4 button-associated LEDs and a confirmation LED. As a result of two-way communications with the BS100 transceiver, the KF100 keyfob imparts audible and visual feedback signals (beep and LED signals) which notify the user of the outcome of requested operations.

2-6-1

Technical specifications KF100	Value
Battery	3V CR2032 Lithium battery (included)
Buzzer	Multitone
Rubber pushbutton version	- with icons - with numbers

Table 7: **Feedback signals provided by KF100 wireless keyfob**

Push button	Icon	LED 1	LED 2	LED 3	LED 4	Buzzer signal	Operation
F1		1 flash				beep	Shortcut activation 1
F2			1 flash			beep	Shortcut activation 2
F3				1 flash		beep	Shortcut activation 3
F4					1 flash	beep	Shortcut activation 4
F2 + F3			1 flash	1 flash		beep	Block wireless keyfob
any			4 flashes	4 flashes			Keyfob blocked

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.

Nota Bene

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

Multi-system access 2-7

Users can access several systems using the same code/key/keyfob. The user code, key or keyfob 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 and 4 on system B and on partitions 4 and 5 on system C.

This operating method is possible for all keys and codes.

Telephone and voice functions 2-8

Each Ability control panel events can be associated with report calls to an Alarm Receiving Centre (via a digital dialer) and to contact numbers (via a voice dialer).

The installer can associate a voice message with an event; each message is customizable for the user.

Arming Scenarios 2-9

A scenario is a configuration (programmed by the installer in accordance with the user's needs) which arms/disarms the various partitions of the Ability security system and activates one or more outputs.

For instance, if all the building occupants leave the premises, they apply the Away arming mode. Therefore, they arm all the partitions and activate all the outputs which close the rollerblinds and switch off the lights. However, if people remain on the premises, they need to apply an arming configuration which allows them to move freely in parts of the premises (e.g. upstairs) and activate the outputs which switch on the night lights, etc.

The installer will programme the system in accordance with these needs and create suitable arming configurations (scenarios). These scenarios can be activated by the users via keypads, readers, remote controls and over-the phone by means of arming shortcuts (refer to *Chapter 3 - Shortcuts*).

Chapter 3

SHORTCUTS

Keypad shortcuts

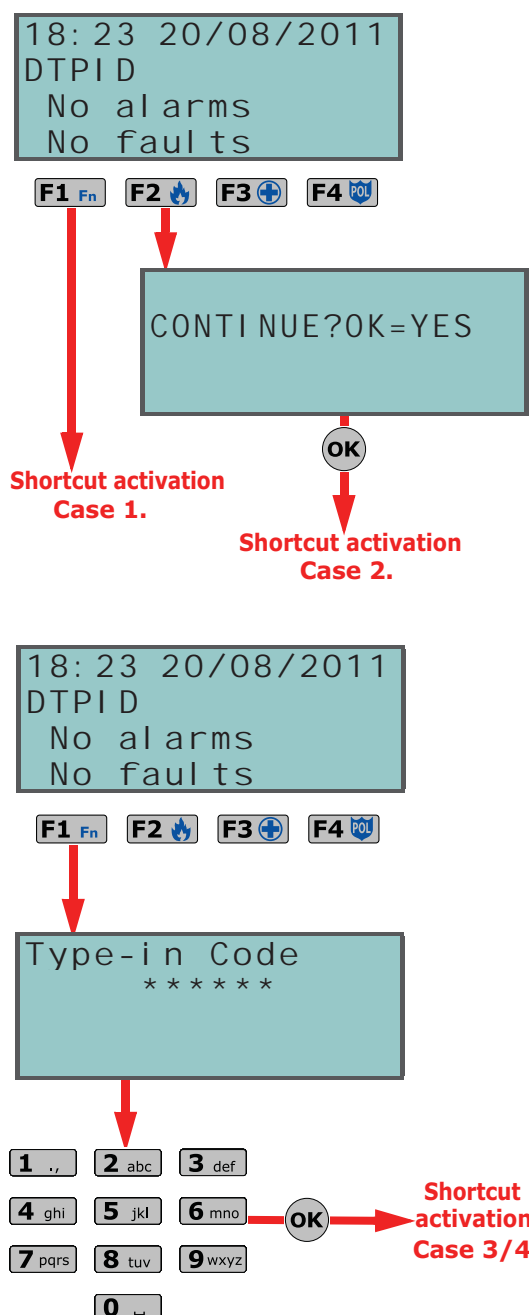
Each keypad can be programmed with up to 4 shortcuts associated with 4 function keys **F1** **F2** **F3** **F4**.

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

1. **By ALL** - press the respective key **F1** to **F4**, to activate the shortcut instantly without code entry. The shortcut will affect all the keypad partitions.
2. **By ALL with confirmation request** - press the respective key from **F1** to **F4** and confirm the operation. If you press **OK** the shortcut will activate instantly, if you press **Cancel** or **Esc** the operation will be abandoned. This method protects against accidental operations. The shortcut will affect all the keypad partitions.
3. **Code users only** - press the respective key from **F1** to **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.
4. **Code users only when activation of the shortcut lowers system 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 your system will obviously be at risk, therefore, the system will request code entry. The shortcut will affect the partitions common to both the keypad and code.

To activate a shortcut, press the key from **F1** to **F4** which corresponds to the shortcut. The system will either activate the shortcut instantly (case 1.) or will request confirmation (case 2.) or code entry (cases 3. and 4.) before carrying out the operation.

3-1



Shortcut with code 3-2

Besides the keypad shortcuts provided by keys **F1** **F2** **F3** **F4**, each user code can have as many as 14 customized (personal) shortcuts.

Users can access their code-shortcuts by entering their PINs and pressing **OK** (refer to paragraph 2-5-1 *Accessing the User Menu*). Each code can be programmed to manage:

- Up to 4 shortcuts activated by keys **F1** to **F4**
- Up to 10 shortcuts activated by keys to **0** to **9**

To activate a shortcut at a keypad, work through the following steps.

1. type in your code then press **OK**
2. press the key from **F1** to **F4** or **0** to **9** associated with the shortcut

Keys and readers shortcuts 3-3

nBy/S and nBy/X reader shortcuts 3-3-1

Hold a valid key in the vicinity of the reader, a series of visual signals on the reader LEDs will indicate the various shortcuts.

When the required shortcut is indicated, remove the key to activate the corresponding shortcut action.

The visual signals on the Reader LEDs are as follows (refer to *Table 6: Reader LEDs with key at reader*).

1. **Red LED on for 3 seconds** - shortcut associated with the red LED of the reader or of the key
2. **Blue LED on for 3 seconds** - shortcut associated with the blue LED of the reader or of the key
3. **Green LED on for 3 seconds** - shortcut associated with the green LED of the reader or of the key
4. **Yellow LED on for 3 seconds** - shortcut associated with the yellow LED of the reader or of the key
5. **All LEDs on for 3 seconds** - 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. Selection of the desired shortcut will not occur until the key is removed.

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

Keyfob shortcuts 3-3-2

To activate the keyfob shortcuts (programmed by your installer) assigned to keys **F1** to **F4**, simply push the button which corresponds to the desired command. The successful outcome of the operation will be signaled by the buzzer and feedback LEDs on the keyfob (refer to *Table 7: Feedback signals provided by KF100 wireless keyfob*).

Shortcut list 3-4

For the complete list of shortcuts refer to the table in *Appendix B, Shortcuts at default*.

Shortcuts 1 to 8, shown in the table, carry out the specified actions instantly.

All other shortcuts (from 9 to 29) provide direct access to specified sections in the User Menu, therefore, can be activated at keypads only.

Chapter 4

USING THE SYSTEM

This chapter describes all the operations users can carry out with or without authorization (user PIN entry). The tools and methods which allow access the system operations are as follows.

The system can be accessed:

- Via **Keypad** nCode/S
The keypad allows users to operate the system:
 1. by means of shortcuts (refer to paragraph *3-1 Keypad shortcuts*);
 2. by means of access codes via the User Menu (refer to paragraph *2-5 User Codes* and paragraph *3-2 Shortcut with code*). This chapter describes the procedure via menu as described at paragraph *2-5-1 Accessing the User Menu*.
- From **Reader** (nBy/X and nBy/S)
This proximity-key reader provides users with only one way of accessing the system, as described in paragraph *3-3 Keys and readers shortcuts*.
- Via **Command Zone**
After violation of a duly-programmed zone which sends a command to the control panel.
- via **Wireless keyfob**
by means of keys **F1** to **F4** as described in paragraph *2-6-1 Air2-KF100 Wireless keyfobs*.

Managing alarms

4-1



This paragraph describes the actions users can take during typical alarm and tamper conditions:

- **Stop alarms** - deactivates instantly the outputs activated by zone/partition alarm and tamper events and system tamper events.
- The system tamper events are:
 - Open panel
 - Dislodged panel
 - Peripheral tamper (expansion, keypad, reader)
 - Peripheral loss (expansion, keypad, reader)
- **Clear call queue** - clears the outgoing call queue and stops any ongoing calls.
- **Delete memory** - implements a "Stop alarms" operation and, at the same time, deletes memory of system and partition alarm and tamper events.

Via Keypad

Method 1

Activate the shortcuts associated with keys **F1** Fn to **F4** POL with or without code entry.

- The shortcut which is assigned to "Alarm menu" operations (shortcut n.10) allows you to view the respective section (User Menu) where, by means of keys  and , you can select and activate one of the following option using the **OK** key.
 - **Stop alarms**
 - **Clear call queue**
 - **Delete memory**
- The following shortcuts activate the associated commands:
 - Shortcut n.2: "Stop alarms"
 - Shortcut n.3: "Clear call queue"
 - Shortcut n.4: "Delete memory"

Method 2

Access the "Alarm management" section (User Menu) by means of a valid PIN.

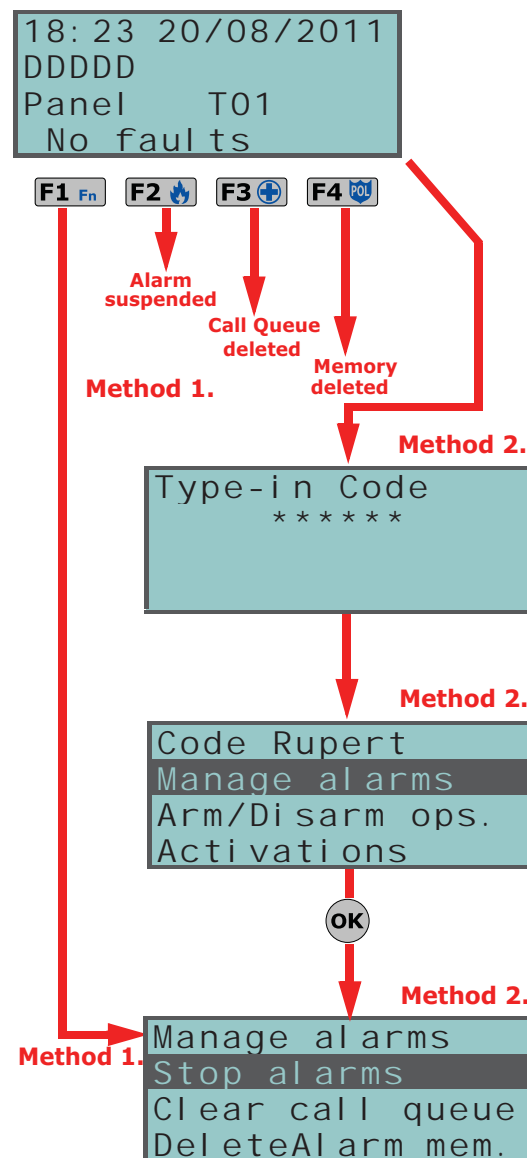
Follow the instructions described in **Method 1**.

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) or "DeleteAlarm mem." (shortcut n.4).

Via Wireless keyfob

Push the respective button on the keyfob and verify the outcome of the requested operation, as described in paragraph 2-6-1 *Air2-KF100 Wireless keyfobs*.



Arming and disarming partitions

4-2






Via Keypad

Method 1

Activate the shortcuts associated with keys **F1** Fn to **F4** POL with or without code entry.

- The shortcut which is assigned to "Arm/Disarm" operations (shortcut n.1) applies the pre-set scenario.

- The shortcut assigned to "Arm/Disarm menu" (shortcut n.9), allows you to view the respective section and arm (in Stay or Away mode) or disarm each partition separately.

- Use keys  and  to select the required partition.
- Use keys  and  to select the required operating mode (Stay, Away, Instant, Disarm, Hold).
- Once the required operation has been selected, press .

Method 2

Access the "Arm/Disarm" section of the User menu by means of a valid PIN.

Follow the instructions described in **Method 1**.

Via Reader

Hold a valid key in the vicinity of the reader and select the LED or description relating to an "Arm/Disarm" shortcut (shortcut n.1). The system will apply the programmed scenario

Via Command Zone

Under normal circumstances, a command zone comprises a mechanical key-lock or callpoint which activates an electrical contact wired to the command zone. In accordance with how the command zone is configured, it is possible to:

- arm the partitions the zone belongs to
- disarm the partitions the zone belongs to
- switch the status of the partitions (arm any disarmed partitions and disarm any armed partitions, refer to "Switch Zone" in *Appendix A, Technical terminology and Glossary*)
- arm the partitions the zone belongs to when the command zone is violated, and disarm the partitions the zone belongs to when it restores to standby

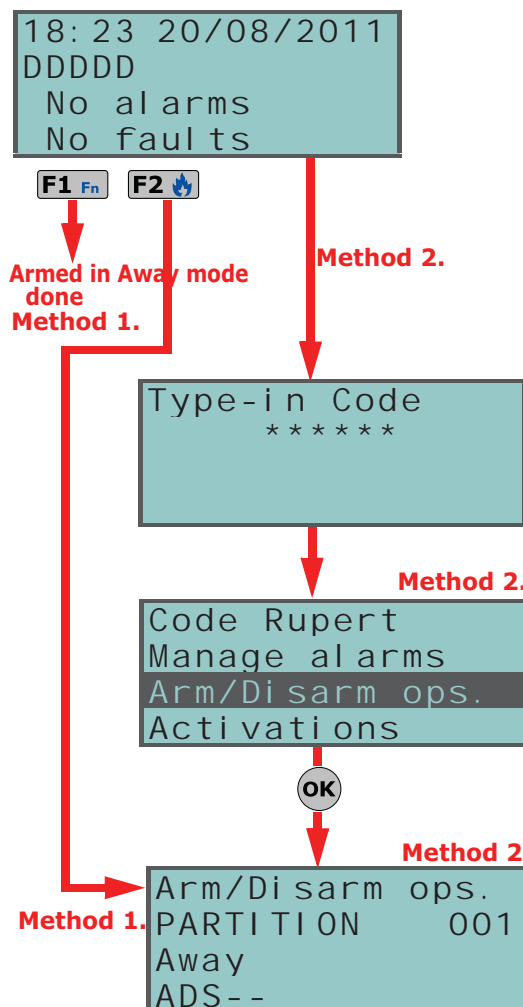
Via Wireless keyfob

Push the respective button on the keyfob and verify the outcome of the requested operation, as described in paragraph 2-6-1 *Air2-KF100 Wireless keyfobs*.

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. Users who are enabled to control Auto-arm operations (refer to paragraph 4-3 *Activations*) must:

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



Activations

4-3

The activation/deactivation of the Ability system peripherals and elements (described in the following section) enables them to operate in accordance with their settings (activation) or disables their functions completely (deactivation). The user has full control over activation/deactivation of the Ability system peripherals and elements.

The following section describes the consequences of activation/deactivation.

- Zone** - a deactivated zone (bypassed zone) cannot generate alarms.
- Auto-arm operations** - can be activated/deactivated separately on each single 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.
- Keys** - deactivated (disabled) keys cannot access the system.
- Keypads** - deactivated (disabled) keypads cannot provide access to the system, therefore, cannot generate commands or shortcuts. The signals on the LEDs and display will be updated.

- **Readers** - deactivated (disabled) readers cannot provide access to the system, therefore, cannot accept keys or generate commands. The signals on the LEDs will be updated.
- **Timers** - activated timers (On) manage their associated elements (partitions, codes, keys) in accordance with their settings. Deactivated timers cannot time-manage their associated elements (partitions, codes, keys), therefore, they will function in accordance with Timer Off status.

All the timers will be activated automatically when you exit the programming session. You must deactivate timers which are not used for system control purposes.

- **Dialer** - a deactivated (disabled) dialer cannot send voice or digital calls. However, if duly programmed, it will be able to manage incoming calls.
- **Teleservice** - if activated (enabled), the installer will be able to access the system via modem. The Teleservice call allows the installer to work on the control panel parameters. Teleservice operations involve a request from you and the installers acceptance, therefore, this option needs to be enabled only when required.

Via Keypad

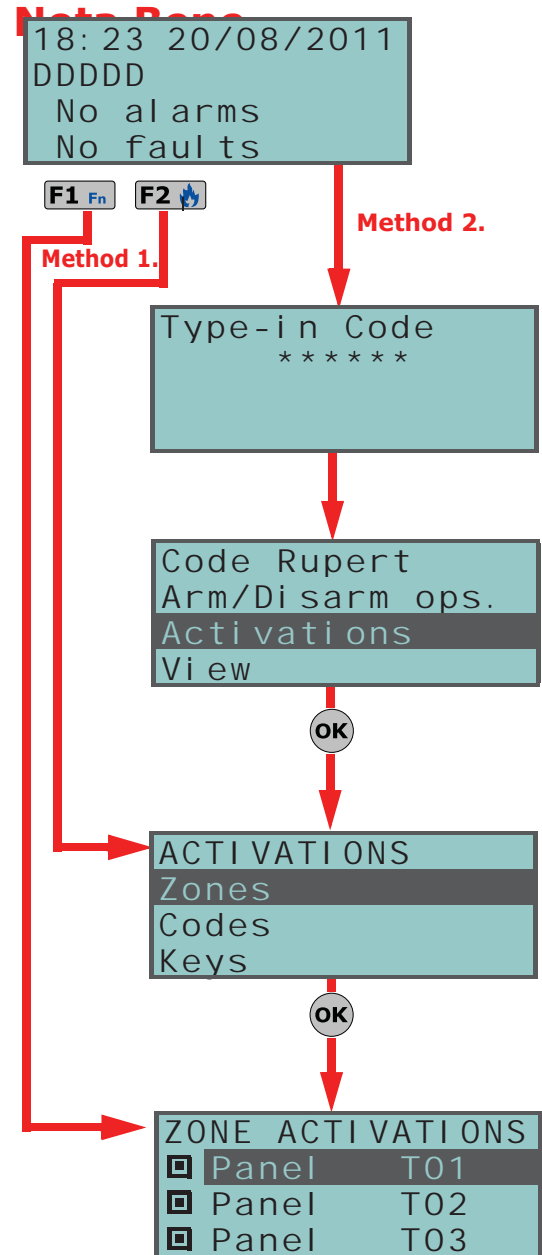
Method 1

Activate the shortcuts associated with keys **F1** **Fn** to **F4** **POL** with or without code entry.

- The shortcut assigned to the "Activations menu" (shortcut n.11), allows you to view the respective section in the User Menu.
 1. Use keys and followed by **OK**, to select the category of elements (zones, codes, etc.) you wish to activate/deactivate.
 2. Use keys and followed by **OK**, to select the single element.
 3. Use to activate the selected element or to deactivate it.
- Other shortcuts which provide direct access to sub-sections of the "Activations" section are:
 - Shortcut n.14 accesses "Activations/Zones"
 - Shortcut n.16 accesses "Activations/Teleservice"
 - Shortcut n.17 accesses "Activations/Codes"
 - Shortcut n.18 accesses "Activations/Keys"
 - Shortcut n.19 accesses "Activations/Timers"
 - Shortcut n.20 accesses "Activations/Auto-arm"

Method 2

Access the "Activations" section of the User menu by means of a valid PIN. Follow the instructions described in **Method 1**.



View

4-4

This section allows you to view the events log and the current status of some of the system peripherals and elements.

The "Events log", "Alarms log", "Faults log" and "Arm/Disarm ops." allow you to view the start and end of the corresponding events in chronological order.

The "System voltage" section allows you to view the respective voltage panel.

The "Zone status" section allows you to view the status of the zone (**Standby**, **Alarm**, **Short-circuit**, **Tamper**) and operating mode (**Unbypassed**, therefore, able to generate alarms, or **Bypassed**, therefore, unable to generate alarms).

The "Faults" section allows you to view current faults only (refer to *Appendix C, Fault signals*).

Zone status
Zone n. 77
Standby Unbypassed

The "Panel version" section allows you to view the firmware version and model of your Ability control panel.

When viewing the wireless zones, the last line on the display indicates the level of signal strength on a scale of 0 to 7; the higher the value the better the signal.




Via Keypad

Method 1

Activate the shortcuts associated with keys **F1 Fn** to **F4 POL** (shown on the display) with or without code entry.



- The shortcut assigned to "View menu" (shortcut n.12), allows you to access the respective section in the User Menu and view the contents of the:

- **Events log**
- **Alarms log**
- **Faults log**
- **Arm/Disarm ops.**

User access to the information in the "Logs" is filtered. For example, a user can view only the zone alarms relating to the partitions the code and keypad concerned have in common. Press keys  and  to scroll the chronological events list. For some events, key  allows you to view the partitions details. For example, the details of an "Arm" command will show the code and keypad concerned and, if you press

, the list of partitions involved.

- **System voltage**

- **Zone status** - allows you to view only the zones associated with the partitions the code and keypad concerned have in common. Use keys  and  to scroll the list of zones.

- **Faults**

- **PanelVersion**

- Other shortcuts which provide direct access to sub-sections of the "View" section are:

- Shortcut n.21 accesses "View/Events log"
- Shortcut n.22 accesses "View/Alarms log"
- Shortcut n.23 accesses "View/Faults log"
- Shortcut n.24 accesses "View/Arm/Disarm ops."
- Shortcut n.25 accesses "View/System voltage"
- Shortcut n.26 accesses "View/Zone status"
- Shortcut n.29 accesses "View/Faults"

Method 2

Access the "View" section of the User menu by means of a valid PIN.

Follow the instructions described in **Method 1**.

Panel Version
2.00 1030B ABIL

18:23 20/08/2011
DDDDD
No alarms
Tel. line down

F1 Fn **F2 POL**

Method 1.

Method 2.

Type-in Code

Code Rupert
Arm/Disarm ops.
Activations
View

OK

VIEW
Events log
Alarms log
Faults log

OK

Valid code
18:23 20/08/2011
Code Rupert
KEYP. 001



Valid Code
18:23 20/08/2011
PARTITION 001

Activating/Deactivating outputs

This section allows you to activate/deactivate manually the outputs the code controls.

Via Keypad

Method 1

Activate the shortcuts associated with keys **F1 Fn** to **F4 POL** with or without code entry.

- The shortcut assigned to "Output control" (shortcut n.15), allows you to view the "Outputs ON/OFF" section of the User Menu where you can:
 - Use keys and to select the output you wish to activate/deactivate.
 - Press to activate the selected output or to deactivate it.
- The shortcut assigned to the "Activate outputs" operation (shortcut n.5) will activate the output when the respective button is pressed.
- The shortcut assigned to the "Deactiv. outputs" (macro n.6) will deactivate the output when the respective button is pressed.

Method 2

Access the "Outputs ON/OFF" section of the User Menu by means of a valid PIN. Follow the instructions described in **Method 1**.

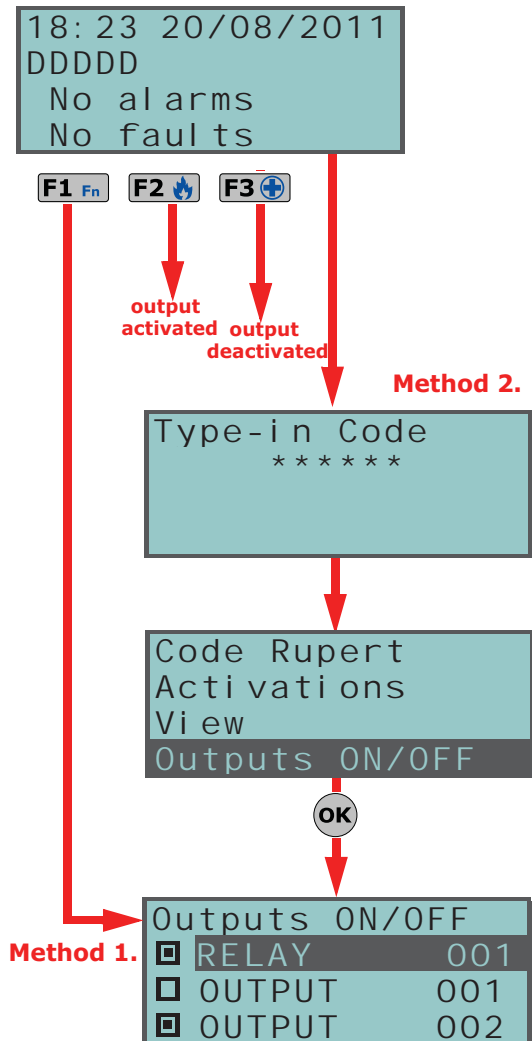
Via Reader

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

Via Wireless keyfob

Push the respective button on the keyfob and verify the outcome of the requested operation, as described in paragraph 2-6-1 *Air2-KF100 Wireless keyfobs*.

4-5



Change date and time

This option allows you to set the date and time in accordance with the selected format.

Via Keypad

Method 1

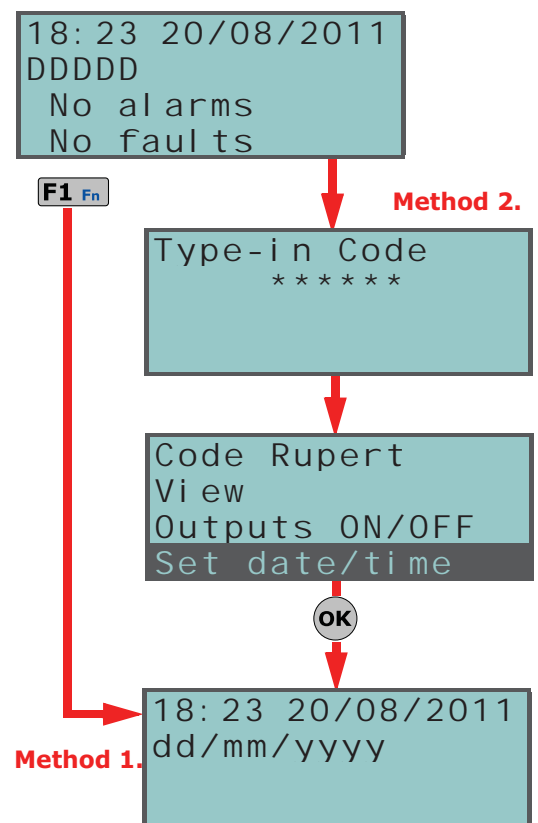
Activate the "Set date/time" shortcut (shortcut n.28) associated with one of the following keys **F1 Fn** to **F4 POL**, to shown on the display, with or without code entry, to access the User Menu at the "Set date/time" section.

- Use keys and to select the programming field (hour, minutes, etc.).
- Use keys and to change the value in the selected field.
- Press to save the setting.

Method 2

Access the "Keypad date/time" section by means of a valid PIN. Follow the instructions described in **Method 1**.

4-6



Keypad settings

This option allows you to program the display and buzzer settings.

- **Brightness** - the level of brightness of the display and key LEDs, when a key is pressed and held for 20 seconds.
- **Standby brightness** - the level of brightness of the display and key LEDs during standby status.
- **Contrast** - allows you to adjust the black/white contrast.
- **Volume** - allows you to adjust the buzzer volume (3 levels available).
 - Off
 - Low volume
 - High volume

These settings apply only to the keypad you are working on, and will be saved even in the event of panel shutdown.

Via Keypad

Method 1

Activate the shortcut assigned to the "Keypad sett.menu" (shortcut n.13) and associated with one of the following keys **F1 Fn** to **F4 POL** (shown on the display) with or without code entry, to access the "Keypad settings" section of the User Menu.

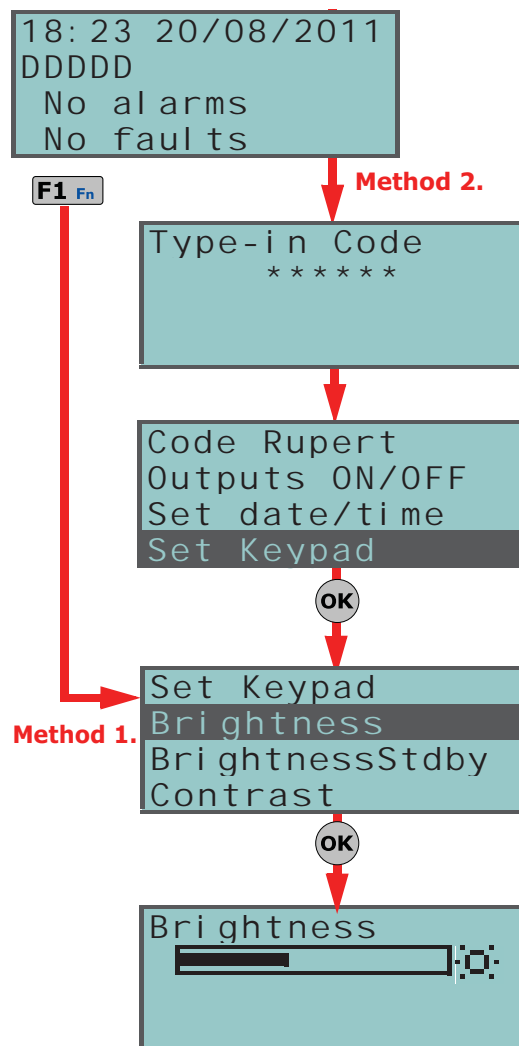
1. Use keys and followed by **OK** to select the required parameters.
2. Use keys and to increase or decrease the value of the selected parameter.
3. Press **OK** to save.

Method 2

Access the "Keypad Settings" section of the User Menu by means of a valid PIN.

Follow the instructions described in **Method 1**.

4-7



Change PIN

This section allows you to change your User Code PIN. If your code has "Main User" status, it will also allow you to change the PINs of other users but not of other "Main Users".

Via Keypad

Method 1

Activate the shortcut assigned to the "Change PIN" (shortcut n.27) and associated with one of the following keys **F1 Fn** to **F4 POL** (shown on the display), with or without code entry, to access the "Change PIN" section of the User Menu.

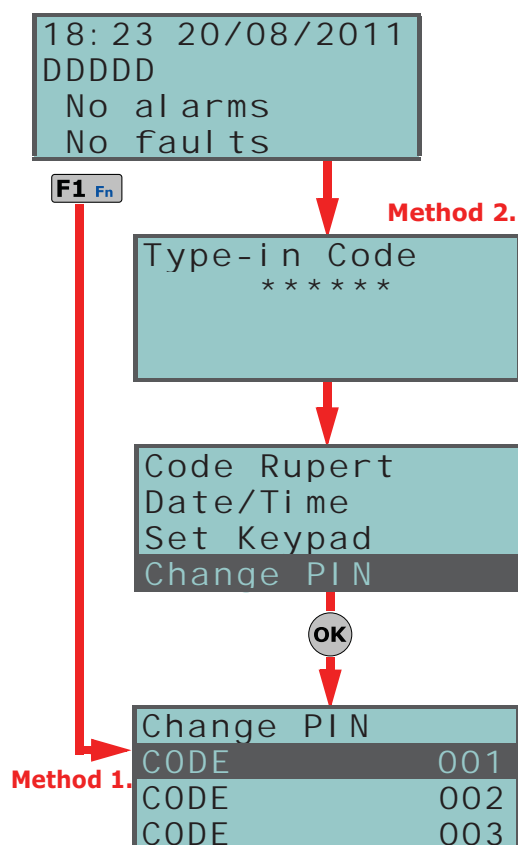
1. Use keys and followed by **OK** to select the user code you wish to change.
2. Type-in the new PIN (4, 5 or 6 digits) using keys **0** to **9 wxyz** then press **OK**.
3. Type-in the new PIN again using keys **0** to **9 wxyz** then press **OK** to save.

Method 2

Access the "Keypad Settings" section of the User Menu by means of a valid PIN.

Follow the instructions described in **Method 1**.

4-8



Teleservice request

4-9

This command sends a call to the installer company.

Your installer must enable control panel option "Num5 ForTeleserv", otherwise this function will not be available.

Via Keypad

Method 1

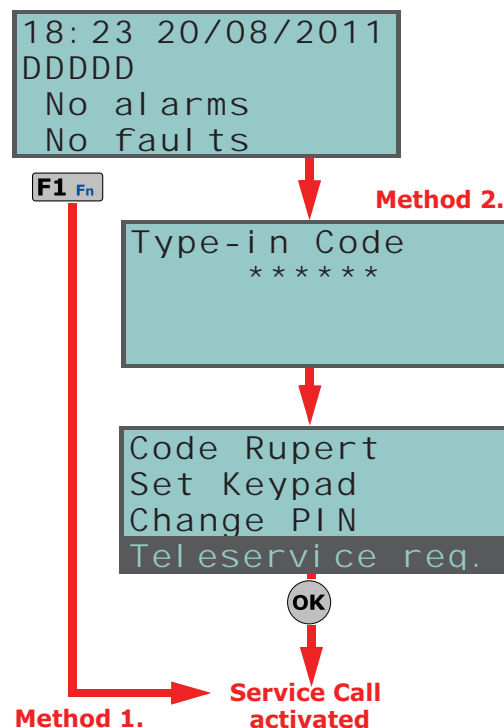
Activate the shortcut assigned to the "Teleservice req." (shortcut n.8).

Method 2

Access the "Teleservice" section of the User menu by means of a valid PIN.

Via Reader

Hold a valid digital key in the vicinity of the reader and select the LED or description relating to "Teleservice req." (shortcut n.8).



Overtime request

4-10

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

- The partition concerned must be timer-controlled.
- The auto-arm option must be enabled (refer paragraph 4-3 *Activations*).

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

Via Keypad

Method 1

Activate the shortcut assigned to the "Overtime" (shortcut n.7).

Method 2

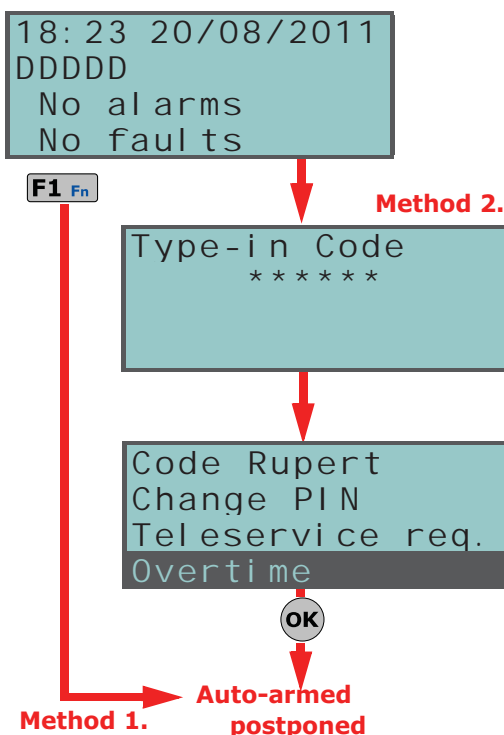
Access the "Overtime req." section of the User Menu by means of a valid PIN.

Via Reader

Hold a valid digital key in the vicinity of the reader and select the LED or description relating to "Overtime" (shortcut n.7).

Via Wireless keyfob

Push the respective button on the keyfob and verify the outcome of the requested operation, as described in paragraph 2-6-1 *Air2-KF100 Wireless keyfobs*.



Commands over-the-phone (for Ability 510B/V and 1030 B/V only)

4-11

Your installer will instruct you as to which events generate voice calls. Event report calls will be sent to the programmed contact numbers of your choice when the event occurs and, in most cases, also when it ends.

During playback, you can press "*" to go to the next message or, if there is only one message, end the successful call.

Appendix A

TECHNICAL TERMINOLOGY AND GLOSSARY

These are 4, 5 or 6 digit PINs which allow the building occupants (users) to access the system.

Each code can be programmed to control specific functions only, and to operate the system to suit the requirements of the Main User.

Code types

- **Installer code:** used by the installer company technician
- **User code:** assigned to the building occupants

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

In the event of:

- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper (keypads, expansions, readers)
- peripheral loss (keypads, expansions, readers)
- false key

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

This is a private company that monitors premises protected by intrusion control systems equipped with Digital or Voice dialers (refer to Digital dialer and Voice dialer).

Alarm Receiving Centres receive alarm reports from monitored systems and take all the necessary actions to protect the occupants of the protected premises.

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.

You can enable/disable the Auto-arm function on each separate partition.

If the auto-arm option is enabled on a timer-controlled partition, the partition will arm/disarm in accordance with the ON/OFF settings of the timer.

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

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

Enabled users can clear the call queue manually.

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 stops all signaling on the red keypad/reader LEDs and the following events:

- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper (keypads, expansions, readers)
- peripheral loss (keypads, expansions, readers)
- false key

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

ACCESS CODES

ALARM

ALARM OR TAMPER MEMORY

ALARM RECEIVING CENTRE (ARC)

ARM/DISARM

AUTO-ARM

BACKUP BATTERY

CALL QUEUE

DELAYED ENTRY ZONE

DELAYED EXIT ZONE

DELETE ALARM/TAMPER MEMORY

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

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, user-code recognition, etc.

Each event (e.g. mains failure) can be associated with an activation event (when the event occurs) and a restoral event (when the event ends).

Each event can be programmed to generate the following actions:

- activation of one or more outputs
- transmission of one or more e-mails
- activation of one or more voice calls
- activation of one or more digital calls

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.

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

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

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

This device allows the system to send calls over the GSM network.

The SmartLink is a custom GSM interface. This device is capable of providing the control panel with a telephone line even in the event of telephone line tamper (line cutting). This function increases the level of security considerably.

This is the two-way communication line (4 wires only) which connects the peripheral devices (keypads, readers, expansions, etc.) to the control panel.

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

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

The Installer code is identified by a 4, 5 or 6 digit PIN. This PIN allows the installer to access the system Programming Menu either from a keypad or via the respective software application, on condition that all the system partitions are disarmed.

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 by typing in the installer PIN, under the condition that all the system partitions are disarmed, or from a computer via the Ability Suite software application.

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.

DIGITAL DIALER

ENTRY TIME (OR ENTRY DELAY)

EVENT

EVENTS LOG (OR EVENTS MEMORY)

EXIT TIME (OR EXIT DELAY)

EXPANSION BOARDS (FLEX5)

FAULT

GSM INTERFACE

I-BUS

INSTALLER CODE

INSTALLER MENU

INTERIOR ZONE

A 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. Keypads can be connected to the system via the I-BUS.

The keypad allows users to access and control the partitions which are common to both the code and keypad in use. The user can arm/disarm partitions, view the status of the zones, stop visual and audible signaling devices.

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.

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

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

A periodic inspection of the protected premises carried out by authorized security staff.

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.

Devices connected to the control panel via the I-BUS.

Ability control panels manage the following peripherals:

- nCode/S keypads
- Proximity Readers (nBy)
- Expansions (Flex5)
- Transceiver (Air2-BS100)
- Sounder (Ivy)

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.

Under normal circumstances, the mains power supply (230Vac) 50 Hz (110V a.c. 60Hz in some countries).

Usually connected to a switching power supply or transformer (depending on the model) that provides the stabilized voltage to the system and the charge source to the batteries.

This device allows users to access and control the system. The system readers are connected to the control panel via the I-BUS.

The key (TAG) allows the user to activate shortcuts (refer to Shortcuts) and arm/disarm the partitions which are common to both the key (TAG) and reader in use. 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.).

A pre-set arming configuration which applies various operating modes to the system partitions.

KEY

KEYPAD (NCODE/S)

MAGNETIC CONTACT (AIR2-MC100)

OUTPUT

PARTITION

PARTITION ARM/DISARM OPERATIONS

PATROL

PERIMETER ZONE

PERIPHERALS

PRE-ARM TIME

PREMISES

PRIMARY POWER SOURCE

READER (NBY)

SCENARIO

The shortcuts allow quick access to User Menu options which normally require several step-by-step operations.

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 switches connected to the system zones, keypads, readers, expansions and control panel. Generally, these events are triggered by system violation such as unauthorized opening of a keypad cover.

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

This is a service provided by the installer company. The installer company requires your collaboration and authorization before opening a teleservice session and working on the system via telephone line.

A zone with this attribute cannot generate alarms (activate audible and visual signalling devices). However, any alarm events that occur will be saved to the events memory.

Event memory

If zones are not operating properly, the "Test" option will allow the installer to check them without the risk of generating false alarms

A logical entity for automatic time-management of programmed peripherals or elements. Ability control panels provide 2 timers.

Transceiver-equipped devices

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

Each code is programmed with:

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

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

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

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

Usually, only the control panel of wireless-systems is mains powered (220Va.c.) while, the wireless devices are battery powered. The battery life is of utmost importance in the design layout and operational capacity of these systems.

An electrical input point used for the management/supervision of signals coming from an intrusion detection device.

A bypassed zone (disabled zone) cannot generate alarms. Activation/Deactivation of zones can be carried out manually by users or, under certain circumstances, automatically by the control panel.

SHORTCUTS

SUPERVISION

TAMPER

TELEPHONE ACTIONS

TELESERVICE

TEST ZONE

TIMER

TRANSCIVER

USER CODE

USER MENU

VOICE DIALER

WIRELESS

ZONE

ZONE BYPASS/UNBYPASS

Appendix B


SHORTCUTS AT DEFAULT

n.	description	function	parameter
1	Arm/disarm	Applies a pre-set scenario	Scenario
2	Stop alarms	Immediately deactivates the outputs relative to zone/partition alarm and tamper events and system tamper events.	
3	Clear call queue	Cancels the call queue and stops ongoing calls (if any).	
4	Delete memory	Carries out a "Stop alarms" operation and, at the same time, deletes memory of system and partition alarm and tamper events.	
5	Activate outputs	Activates one of the programmed outputs.	Output
6	Deactiv. outputs	Deactivates one of the programmed outputs.	Output
7	Overtime	Delays auto-arming time of partitions by 30 minutes.	
8	Teleservice req.	Sends a call to the Installer company number (Teleservice number).	
9	Arm/disarm menu	Accesses the User Menu section: Arm/Disarm	
10	Alarm menu	Accesses the User Menu section: Manage alarms	
11	Activations menu	Accesses the User Menu section: Activations	
12	View menu	Accesses the User Menu section: View	
13	Keypad sett.menu	Accesses the User Menu section: Keypad Keypad	
14	ZoneBypass menu	Accesses the User Menu section: Activations/Zones	
15	Output control	Accesses the User Menu section: Outputs ON/OFF	
16	Enab.teleservice	Accesses the User Menu section: Activations/Teleservice	
17	Enable codes	Accesses the User Menu section: Activations/Codes	
18	Enable keys	Accesses the User Menu section: Activations/Keys	
19	Enable timers	Accesses the User Menu section: Activations/Timers	
20	Enab. auto-arm	Accesses the User Menu section: Activations/Auto-arm	
21	View events log	Accesses the User Menu section: View/Events log	
22	View alarm log	Accesses the User Menu section: View/Alarms log	
23	View faults log	Accesses the User Menu section: View/Faults log	
24	View arm ops log	Accesses the User Menu section: View/Arm/Disarm ops.	
25	ViewSystemStatus	Accesses the User Menu section: View/System Voltage	
26	View zone status	Accesses the User Menu section: View/Zone status	
27	Change PIN	Accesses the User Menu section: Change PIN	
28	Time/date setup	Accesses the User Menu section: Time/Date	
29	View faults	Accesses the User Menu section: View/Faults	

Appendix C

FAULT SIGNALS

The following table shows how system faults, indicated by the yellow LED, are signaled clearly on the keypad  :

FAULT	User menu string: "View/ Faults"	Probable cause	Note
Zone fuse blown	Zone fuse fault	Excessive current draw on the "+AUX" terminals on the control panel	
BUS fuse blown	IBUS fuse fault	Excessive current draw on the "+" terminal on the control panel	
Backup battery low or disconnected	Low battery	The control panel backup-battery is running low or is not connected properly	
Mains failure	Mains failure	The primary power source (230 Vac) has failed (blackout) or is not connected properly	
Telephone line down	Tel. line down	The telephone line is not working	
Wireless noise	Jamming	Rogue wireless signal	
Low wireless-detector battery	Low battery WLS	The battery of at least one wireless detector is running out	To view the details of "Low battery WLS" and "WLS zone loss" events, select "View/Faults" from the user menu, then press the  button to access the list of devices involved in the fault event.
Wireless detector loss	WLS zone loss	At least one wireless detector is not responding (lost)	



Ability

