integra

Alarm control panel

INTEGRA

Firmware version 1.25

EN



USER MANUAL

integra_u_en 08/26

Satel®

SATEL sp. z o.o. • ul. Budowlanych 66 • 80-298 Gdańsk • POLAND
tel. +48 58 320 94 00
www.satel.pl

IMPORTANT

Before you start using the control panel, please read carefully this manual in order to avoid mistakes that can lead to malfunction or even damage to the equipment.

Changes, modifications or repairs not authorized by the manufacturer shall void your rights under the warranty.

The INTEGRA control panels should only be connected to the **analog subscriber lines**. In case of changing the analog line to the digital one, it is necessary to contact the alarm system installer.

Pay special attention if the telephone line used by the control panel is frequently busy and/or failures are reported, concerning the line and/or monitoring. Report such situations to the alarm system installer immediately.

To ensure adequate protection, the alarm security system must be in good working order, therefore SATEL recommends that it be regularly tested. The control panel is equipped with a number of self-diagnostic functions which, when properly configured by the installer, ensure control over correct functioning of the system.

The alarm system cannot prevent burglary, hold-up or fire from happening, but in emergency situation it will allow you to take steps to minimize the potential damage (by triggering optical or acoustic alarm signal, notifying appropriate authorities of the alarm etc.). Thus, it can deter any would-be intruders.

SATEL aims to continually improve the quality of its products, which may result in changes in their technical specifications and software. Current information about the changes being introduced is available on our website.
Please visit us at:
https://support.satel.pl

The declaration of conformity may be consulted at www.satel.pl/ce

Factory default codes:

Service code: 12345

Object 1 master user (administrator) code: 1111

Signs in this manual

Caution – information on the safety of users, devices, etc.

Note – suggestion or additional information.

CONTENTS

1. Introduction 4
2. Technical reliability of the alarm system 4
3. Alarm system operating costs 4
4. Authorization of users 5
   4.1 Authorization using two identifiers 5
   4.2 Factory default codes: 5
   4.3 Operation under duress 6
5. Operating the alarm system from keypad 6
   5.1 Keypads description 7
      5.1.1 LCD display 7
      5.1.2 LED indicators 9
      5.1.3 Keys 10
      5.1.4 Built-in proximity card reader 10
      5.1.5 Sound signaling 10
   5.2 [Code]# – arming / disarming menu 11
      5.2.1 Arming menu 12
      5.2.2 Disarming menu 12
   5.3 [Code]* – user menu 12
      5.3.1 Functions list 12
      5.3.2 Navigating through the menu and running functions 16
      5.3.3 Menu shortcuts 17
      5.3.4 Data editing 17
      5.3.5 Description of user functions 19
   5.4 Arming 25
      5.4.1 Full arming without partition selection 25
      5.4.2 Full arming the selected partitions 25
      5.4.3 Arming in the selected mode 26
      5.4.4 Quick arming 26
      5.4.5 Denial of arming 26
      5.4.6 Failure of arming procedure 27
      5.4.7 Shortening the exit delay time 27
   5.5 Disarming and alarm clearing 27
      5.5.1 Disarming all partitions 27
      5.5.2 Disarming selected partitions 27
      5.5.3 Alarm clearing without disarming 28
   5.6 Two-code arming / disarming 28
   5.7 Triggering the alarm from the keypad 28
   5.8 Users 28
      5.8.1 User types 30
      5.8.2 Adding new user 31
      5.8.3 Edit user 31
      5.8.4 Removing a user 31
      5.8.5 Adding proximity card / DALLAS iButton 32
      5.8.6 Adding keyfob 32
      5.8.7 Editing keyfob settings 33
      5.8.8 Removing keyfob 33
   5.9 Master users (administrators) 34

5.10 Zone bypassing 34
5.10.1 Zone inhibiting 34
5.10.2 Zone isolating 35
5.10.3 Unbypassing 35
5.11 Viewing the event log 35
5.11.1 Viewing all events 35
5.11.2 Viewing the events required for Grade 2 35
5.11.3 Viewing the selected events 35
5.11.4 Way of presenting events 36
5.12 Replacing batteries in wireless keypad 36
5.13 Programming the thermostatic output settings 37
5.13.1 Programming temperature 1 (economic temperature) 37
5.13.2 Programming temperature 2 (comfortable temperature) 37
5.13.3 Programming hysteresis 37
5.13.4 Enabling / disabling the COOLING option 38
5.13.5 Rules for programming the thermostatic output settings 38
5.14 Programming the partition timer 38
5.15 Zone testing 39
5.16 Outputs control 40
5.16.1 Controlling the MONO SWITCH type of output 40
5.16.2 Controlling the BI SWITCH type of output 41
5.16.3 Controlling the REMOTE SWITCH type of outputs 41
5.16.4 Controlling the roller shutter outputs 41
6. Using the partition keypad 41
6.1 Description of partition keypads 42
6.1.1 LED indicators 42
6.1.2 Keys 43
6.1.3 Built-in proximity card reader 43
6.1.4 Sound signaling 43
6.2 Functions available from the partition keypad 44
6.2.1 [Code]✱ / presenting the card 44
6.2.2 [Code]# / holding the card 44
6.2.3 Quick arming 45
6.2.4 Triggering the alarm from the keypad 45
6.2.5 Silencing the alarm sound at the keypad 45
6.2.6 Code changing 45
7. Using the entry keypad 45
7.1 Description of the entry keypad 46
7.1.1 LED indicators 46
7.1.2 Keys 46
7.1.3 Built-in proximity card reader 46
7.1.4 Sound signaling 46
7.2 Functions available from the entry keypad 46
8. Using the code lock 47
8.1 Description of code locks 48
8.1.1 LED indicators 48
8.1.2 Keys 48
8.1.3 Sound signaling 48
8.2 Functions available from code lock 48

8.2.1 [Code]✱ / [Code]# 48
8.2.2 Generating alarm from the keypad 49
8.2.3 Code changing 49
9. Confirming voice messaging 49
10. Call answering and telephone control 49
10.1 Answering phone calls 50
10.2 Telephone control 50
10.3 Audio alarm verification 51
11. SMS control 51
12. Operating the alarm system using keyfob 52
13. Manual update history 53
14. Brief description of operating the system from keypad 56

1. Introduction

Thank you for choosing the product offered by the SATEL Company. Wishing you full satisfaction with the choice you made, we are always ready to provide you with professional assistance and information on our products.

The SATEL Company is manufacturer of a broad range of devices dedicated for use in security alarm systems. Further information is available on our website **www.satel.pl** or at the points of sale offering our products.

It is recommended that that the installers prepare their own user manual for the alarm system installed by them. The manual must include all changes and modifications made in relation to the factory default settings.

The installer should train the users in the rules of operating the alarm system.

The performance of extra features such as SMS, CLIP or push notifications depends on external networks and third-party services – including telecommunications providers – which are beyond our control. These services may occasionally experience disruptions that affect the delivery of notifications. The proper functioning of these features may also depend on the settings of your devices. While we do our best to minimize the risk of such issues, we cannot accept responsibility for the uninterrupted and error-free operation of features that rely on third-party services, particularly telecommunications networks or from the actions of device manufacturers.

2. Technical reliability of the alarm system

A failure of any component of the alarm system will result in deterioration of the level of protection. Unfortunately, the devices which are installed outside (e.g. the outdoor sirens) are exposed to the adverse effects of weather. During storms, the devices connected to the electrical system or telephone line are vulnerable to damage as a result of atmospheric discharge.

The control panel is provided with a number of safeguards and automatic diagnostic features to test the system performance. Detection of irregularities is signaled e.g. by the indicator on the keypad. **You should immediately respond to such a signal, and, if necessary, consult the installer**.

In addition, some features designed for testing the alarm system are available in the control panel. They make it possible to check the detectors, sirens, telephone communicators, etc. for correct functioning. **Only regular testing and inspection of the alarm system will allow you to keep a high level of protection against intrusion.**

It is recommended that the installer, at the request of the user, carry out periodic maintenance of the alarm system.

It is in the interest of the user to anticipate and plan in advance the procedures in case an alarm is set off by the control panel. It is important to be able to verify the alarm, determine its source and take appropriate actions (e.g. evacuation in the event of a fire alarm).

3. Alarm system operating costs

The control panel can inform the users and the monitoring station about the status of protected facility. Implementation of these tasks means financial costs. The amount of the costs incurred depends on the amount of information sent. A failure, as well as an incorrect

programming of the control panel, may result in increased costs (due to making of excessive number of calls).

Please inform the installer, which is a priority: to deliver information at any cost, or to prevent excessive costs. For example, after an event code has failed to be sent successfully to the monitoring station, the control panel may repeat attempts every few minutes to send the code or to cease the attempts to send the code until a next event occurs.

4. Authorization of users

Operation of the alarm system is possible after the user authorization, which allows the control panel to verify that the user is authorized to perform the given operation. The authorization can be done on the basis of:

- code,
- a proximity card (passive transponder, which may be in the form of a card, tag, etc.),
- DALLAS iButton (chip),
- keyfob.

You cannot assign the same identifier (code, proximity card, DALLAS iButton or keyfob) to two users.

For safety reasons, different people should not use the same identifier.

The installer can configure the panel so that it will not accept codes that contain less than three digits (e.g. 1111 or 1212) or consist of consecutive digits (3456).

The installer may permit the use of certain functions without the need for user authorization.

Using an invalid code, proximity card or DALLAS iButton three times may:

- *trigger an alarm,*
- *block the keypad / reader for 90 seconds.*

4.1 Authorization using two identifiers

Some LCD keypads (e.g. INT-KLCDR, INT-KLFR, INT-KWRL, INT-KWRL2, etc.) and some keypads (e.g. INT-SCR, CR-MF5 and SO-MF5) have a built-in proximity card reader. The installer can configure these devices so that the user has to use two identifiers for authorization: the code and the card. The function to be executed after the authorization depends on the second identifier:

- code – whether it will be confirmed by using the # key or the * key,
- card – whether it will be presented only or held.

4.2 Factory default codes:

By default, the following codes are preprogrammed in the control panel:

service code: 12345

object 1 master user (administrator) code: 1111

The factory default codes make it possible to assign individual codes to consecutive persons who are to use the alarm system (see: “Users” p. 28).

The factory default codes should be changed before you start using your alarm system (CHANGE OWN CODE function available in the user menu).

The control panel can inform the user that the code change is necessary, if the code is known to other users.

The master code should not be used on a daily basis because of the risk of its being captured. It is recommended that the administrator enter for himself an ordinary user's code.

4.3 Operation under duress

When acting under duress, the DURESS type code must be used instead of the normal user code (see “User types” p. 30).

5. Operating the alarm system from keypad

SATEL offers the following keypads for INTEGRA control panels:

INT-TSG – touchscreen keypad,

INT-TSG2 – touchscreen keypad,

INT-TSG2R – touchscreen keypad with built-in 13.56 MHz MIFARE proximity card reader,

INT-TSH – touchscreen keypad,

INT-TSH2 – touchscreen keypad,

INT-TSH2R – touchscreen keypad with built-in 13.56 MHz MIFARE proximity card reader,

INT-TSH210 – touchscreen keypad,

INT-TSI – touchscreen keypad,

INT-KSG – LCD keypad with touch keys,

INT-KSG2R – LCD keypad with touch keys and built-in 13.56 MHz MIFARE proximity card reader,

INT-KLCD – LCD keypad with mechanical keys,

INT-KLCDR – LCD keypad with mechanical keys and built-in 125 kHz EM-Marin proximity card reader,

INT-KLCDK – LCD keypad with mechanical keys,

INT-KLCDL – LCD keypad with mechanical keys,

INT-KLCDS – LCD keypad with mechanical keys,

INT-KLFR – LCD keypad with mechanical keys and built-in 125 kHz EM-Marin proximity card reader.

INT-KWRL – wireless LCD keypad with mechanical keys and built-in 125 kHz EM-Marin proximity card reader.

INT-KWRL2 – wireless LCD keypad with mechanical keys and built-in 125 kHz EM-Marin proximity card reader.

The keypads are available in a variety of color options for the enclosure, display and key backlight. The color variant is indicated by the additional designation in the keypad name (e.g. INT-KLCD-GR – green display and key backlight; INT-KLCD-BL – blue display and key backlight).

This manual includes information on the following keypads:

- wired: INT-KLCD, INT-KLCDR, INT-KLCDK, INT-KLCDL, INT-KLCDS and INT-KLFR,
- wireless: INT-KWRL and INT-KWRL2.

For information on other keypads, please refer to the manuals of these keypads.

The wired keypad is faster to react to user actions than the wireless keypad. The wireless keypad powered by an external power supply (connected to the APS-055 power supply) works similarly to the wired keypad. In the wireless keypad powered by the battery, the sleep mode is started after 20 seconds of inactivity. When the wireless keypad is in the sleep mode, the display is off and the LED indicators, sound signaling, backlight (of display and keys) and proximity card reader are disabled. To wake up the keypad, press e.g. *.

5.1 Keypads description

5.1.1 LCD display

In wireless keypads, the display is disabled when the keypad is in the sleep mode.

The display provides information on the system state and allows you to operate and program the alarm system. The installer defines the display backlight settings.

The display can operate in one of the following modes:

- standby mode,
- partition state preview mode.

The installer decides if the partition state preview mode is available.

The messages about events that occurred in the alarm system (e.g. arming or disarming, countdown of auto-arming delay, countdown of entry or exit delay, alarm, etc.) are displayed regardless of the operating mode.

Enter the code and press the # key to open the arming / disarming menu (p. 11).

Enter the code and press the * key to open the user menu (p. 12).

Standby mode

The following items are displayed in the upper line: date and time in format selected by the installer.

The keypad name or the status of selected partitions (determined by the installer) may be displayed in the bottom line.

Press the 9 key for 3 seconds to switch the display to the partition state preview mode.

Partition state preview mode

The symbols show the status of partitions operated by the keypad (including those from which alarm is signaled by the keypad).

Press the 9 key for 3 seconds to switch the display to the standby mode.

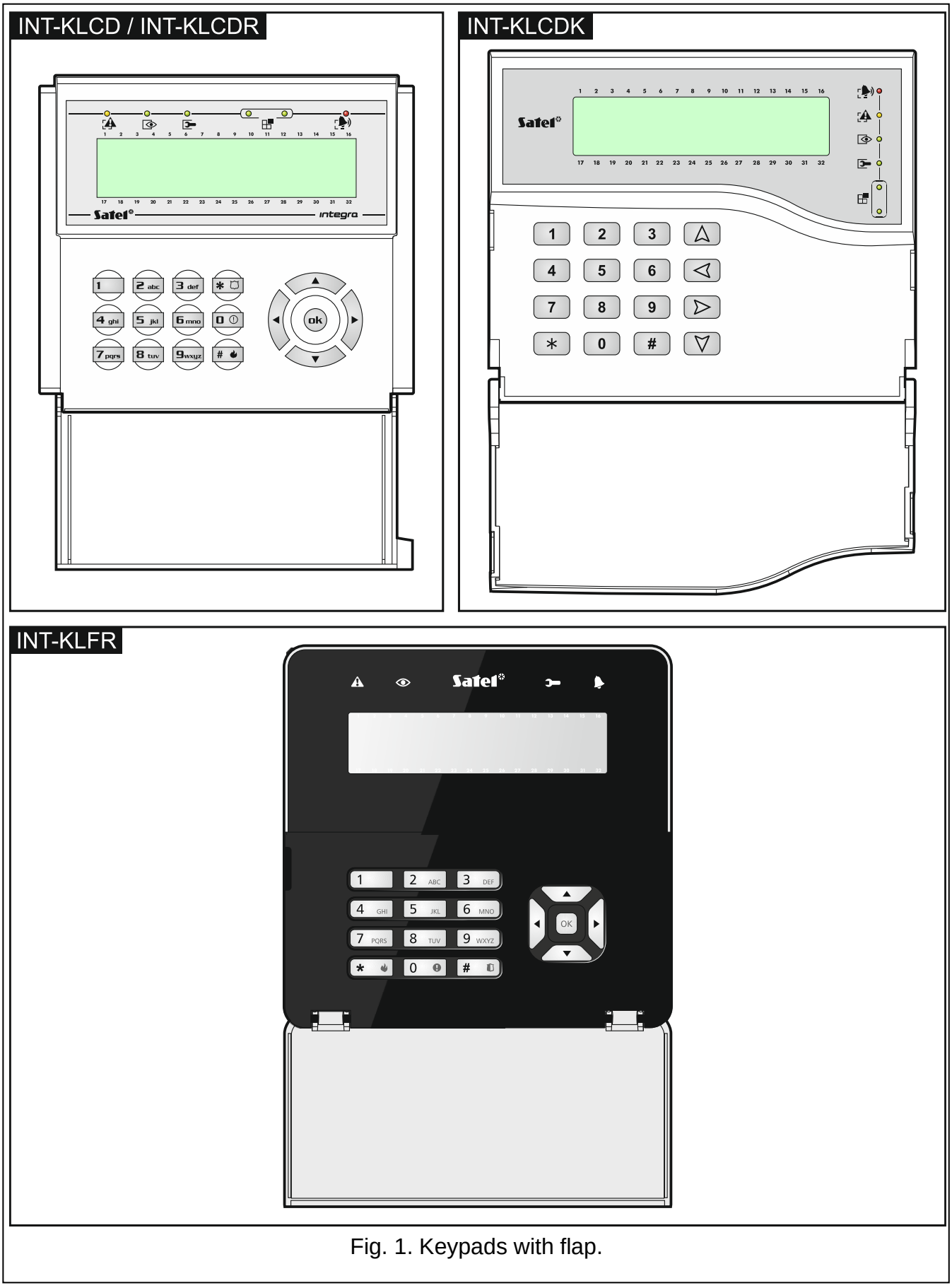


Fig. 1. Keypads with flap.

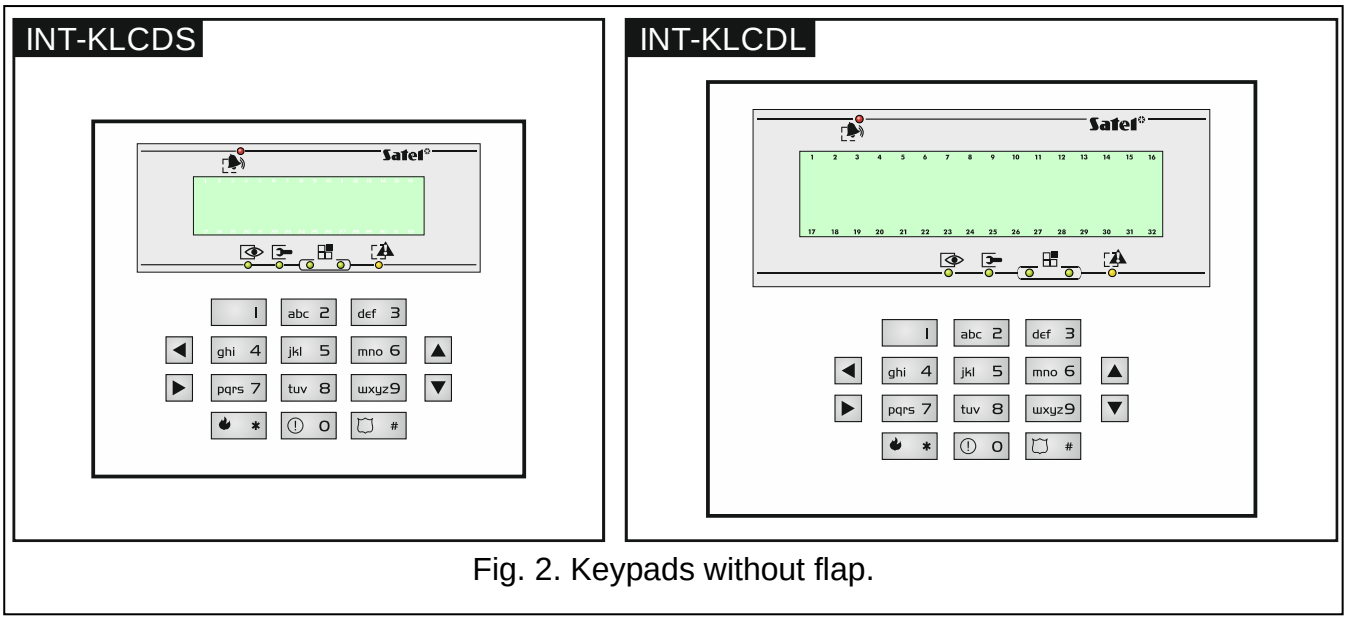


Fig. 2. Keypads without flap.

5.1.2 LED indicators

In wireless keypads, the LED indicators are disabled when the keypad is in the sleep mode.

LED	Color	Description
	green	**ON** – all keypad operated partitions are armed **flashing** – some keypad operated partitions are armed or exit delay countdown is running
	red	**ON** or **flashing** – alarm or alarm memory
	yellow	**flashing** – trouble or trouble memory
	green	**flashing** – service mode started
	green	if zone status is being presented or the keypad is switched to graphic programming mode (see: „Selection from the multiple-choice list” s. 18), two indicators show which data set is being displayed (see: table 2)

Table 1. Description of keypad LED indicators.

Data type	Indicator		Information
	left side/upper	right side/lower	
Zones/Outputs	OFF	OFF	numbers 1-32
	OFF	ON	numbers 33-64
	ON	OFF	numbers 65-96
	ON	ON	numbers 97-128
Expanders	OFF	OFF	system addresses 0-31 (00-1F HEX)
	OFF	ON	system addresses 32-63 (20-3F HEX)

Table 2. Information presented by the indicators.

Information about the armed state can be extinguished after a time period defined by the installer.

If the installer has enabled the GRADE 2 option:

- *the indicator provides information about alarms only after the code has been entered and confirmed with the ✱ key,*
- *flashing of the indicator means that there is a trouble in the system, some zones are bypassed, or that there was an alarm.*

5.1.3 Keys

The keys designated with digits and letters enable entering the code and data, when using the functions available in the menu. Additionally, if you press and hold down the selected digit keys for approx. 3 seconds, you can (if the keypad has been so configured by the installer):

1 - check the state of zones,
4 - check the state of partitions,
5 - view the alarm log (based on the event log),
6 - view the trouble log (based on the event log),
7 - view the troubles,
8 - turn on/off CHIME in the keypad,
9 - toggle the display between the standby mode and partition state preview mode.

The other keys enable you to:

✱ - enter the user menu (after entering the code),
- cancel the started operation.

or **ok** - arm / disarm and clear alarm (after entering the code),
- start the selected function,
- confirm the entered data.

◄ ▲ ▼ ► - navigate through the display (scroll through the displayed messages, functions and options, and move the cursor),
- run the installer selected functions (after entering the code).

- trigger the fire alarm.

- trigger the medical (auxiliary) alarm.

- trigger the panic alarm.

5.1.4 Built-in proximity card reader

Some keypads (e.g. INT-KLCDR, INT-KLFR, INT-KWRL, INT-KWRL2, etc.) allow you to operate the system using proximity cards (proximity tags or other passive transponders). The installer defines which functions can be executed after presenting or holding the card.

In wireless keypads, the proximity card reader is disabled when the keypad is in the sleep mode.

5.1.5 Sound signaling

Beeps generated when operating

The installer can disable the sound signaling.

1 short beep – pressing any number key.

2 short beeps – confirmation of command execution, signaling of entering the user menu, submenu or function.

3 short beeps – signaling of:

- starting the procedure of arming (there is exit delay in the partition) or arming (there is no exit delay in the partition),
- disarming and/or alarm clearing,
- turning output off,
- turning off the CHIME in the keypad by pressing the 8 key,
- toggling the display between the standby mode and the partition state preview mode by pressing the 9 key.
- exiting the function and returning to the menu after confirmation of the data entered.

4 short beeps and 1 long beep – signaling of:

- turning output on,
- turning on the CHIME in the keypad by pressing the 8 key,
- ending the function and exiting the user menu after confirmation of the data entered.

1 long beep – signaling of:

- violated/ bypassed zones when arming,
- fault of the vibration detector (10. 24H VIBRATION type zone was not violated during the vibration detector test run upon starting the arming procedure).

2 long beeps – invalid code/card, function not available or exiting the function without confirmation of the data entered (e.g. by using the ✱ key).

3 long beeps – unavailable function.

Events signaled by sounds

Only installer selected events are signaled.

Alarms are signaled for the time programmed by the installer.

In wireless keypads, the audible signaling is disabled when the keypad is in the sleep mode (except for the CHIME signal).

5 short beeps – zone violation (CHIME).

Long beep every 3 seconds, followed by a series of short beeps for 10 seconds and 1 long beep – countdown of exit delay (if the time is shorter than 10 seconds, only the final sequence of short beeps will be generated).

A sequence of 7 beeps of diminishing duration, repeated every few seconds – countdown of auto-arming delay.

2 short beeps every seconds – countdown of entry delay.

2 short beeps every 3 seconds – signaling a new trouble.

Continuous beep – alarm.

Long beep every second – fire alarm.

5.2 [Code]# – arming / disarming menu

Information given in the section below do not apply to users having the SIMPLE USER right (see p. 29).

After you enter the code and confirm it with the # key:

- a message on the need to change the code or a service note may be displayed,
- alarm will be cleared – if the user is authorized to clear the alarm and there is an alarm in the system,
- one partition will be disarmed – if the user is authorized to disarm the partition, has access to only one partition operated from the keypad and that partition is armed, or has access to many partitions, but only one partition is armed,
- one partition will be armed – if the user is authorized to arm the partition, has access to only one partition operated from the keypad and that partition is disarmed,
- the arming/disarming menu will be displayed.

5.2.1 Arming menu

The arming menu will be displayed if:

- the user is authorized to arm the partition,
- the user has access to a number of partitions operated from the keypad,
- none of the partitions accessible to the user is armed,
- there is no alarm.

Two functions are available in the menu:

Arm all	*arming all partitions*
Arm selected	*arming selected partitions*

5.2.2 Disarming menu

The disarming menu will be displayed if:

- the user is authorized to disarm the partition,
- the user has access to a number of partitions operated from the keypad,
- at least two partitions accessible to the user are armed.

Two functions are available in the menu:

Disarm all	*disarming all partitions*
Disarm selected	*disarming selected partitions*

5.3 [Code]✻ – user menu

After you enter the code and confirm using the ✻ key, the user menu will be displayed. The list of available functions depends on the user authority level, as well as the system status and configuration. In order to exit the user menu, press the ✻ key. The keypad will quit the menu automatically, if 2 minutes have elapsed since the last keypress.

Upon entering the code and confirming with the ✻ key, a message about the need to change the code or a service note may be displayed.

5.3.1 Functions list

The functions available after entering the service code have been highlighted with white text against black background. Highlighted with a frame are functions available to the administrators.

View clear. al.	*view cleared alarms from selected partition zones*
System reset	*restore system after verified alarm*
Disarm	*disarm selected partitions*

Clear alarm — *clear alarm*
Clear other al. — *clear alarm in other objects*
Abort voice m. — *cancel telephone messaging*
Arm — *arm selected partitions*
Arm (2 codes) — *start two code arming*
Disarm (2codes) — *start two code disarming*
Defer auto-arm — *postpone the auto-arming*
Set auto-arm d. — *set auto-arming postpone time*
Arming mode — *select arming mode*
Cancel 1st code — *cancel consent to two code arming/disarming*
Change own code — *change own code*
Change tel.code — *change own telephone code*
Change prefix
- Prefix normal — *set normally used prefix*
- Prefix duress — *set duress prefix*
- Recall time — *set time to remind of the need to change prefix*

Users
- **New user** — *add new user*
  - Code — *set code*
  - Telephone code — *set telephone code*
  - Partitions — *assign partitions available to the user*
  - Type — *select type of code*
  - Schedule — *select time schedule*
  - Existence time — *set code validity time*
  - Bypass time — *set bypass time*
  - Rights — *assign rights*
  - Keypads etc. — *assign modules available to the user*
  - New prox. card — *add proximity card*
  - Rem. prox. card — *remove proximity card*
  - New DALLAS — *add DALLAS iButton*
  - Remove DALLAS — *remove DALLAS iButton*
  - New RX key fob — *add 433 MHz keyfob*
  - Rem. RX keyfob — *remove 433 MHz keyfob*
  - Button 1 — *assign function to keyfob button 1*
  - Button 2 — *assign function to keyfob button 2*
  - Button 3 — *assign function to keyfob button 3*
  - Button 4 — *assign function to keyfob button 4*
  - Button 1 and 2 — *assign function to combination of keyfob buttons 1 & 2*
  - Button 1 and 3 — *assign function to combination of keyfob buttons 1 & 3*
  - Events (RX) — *set event generating rules*
  - New ABAX keyfob — *add keyfob supported by ABAX 2 / ABAX system*
  - Rem.ABAX keyfob — *remove keyfob supported by ABAX 2 / ABAX system*
  - Button 1 — *assign function to keyfob button 1*
  - Button 2 — *assign function to keyfob button 2*

Button 3 *assign function to keyfob button 3*
Button 4 *assign function to keyfob button 4*
Button 5 *assign function to keyfob button 5*
Button 1 and 5 *assign function to combination of keyfob buttons 1 & 5*
Events (ABAX) *set event generating rules*
Confirm. (ABAX) *set confirmation rules*
Name *program user name*

Edit user *edit existing user*

[select user]

[list of parameters identical as in case of a new user]

Remove user *remove user*

Masters

New master *add new master*

Code *set code*
Rights *assign rights*
Keypads etc. *assign modules available to the master*
New prox. card *add proximity card*
Rem. prox. card *remove proximity card*
New DALLAS *add DALLAS iButton*
Remove DALLAS *remove DALLAS iButton*
New RX key fob *add 433 MHz keyfob*
Rem. RX keyfob *remove 433 MHz keyfob*
Button 1 *assign function to keyfob button 1*
Button 2 *assign function to keyfob button 2*
Button 3 *assign function to keyfob button 3*
Button 4 *assign function to keyfob button 4*
Button 1 and 2 *assign function to combination of keyfob buttons 1 & 2*
Button 1 and 3 *assign function to combination of keyfob buttons 1 & 3*
Events (RX) *set event generating rules*
New ABAX keyfob *add keyfob supported by ABAX 2 / ABAX system*
Rem.ABAX keyfob *remove keyfob supported by ABAX 2 / ABAX system*
Button 1 *assign function to keyfob button 1*
Button 2 *assign function to keyfob button 2*
Button 3 *assign function to keyfob button 3*
Button 4 *assign function to keyfob button 4*
Button 5 *assign function to keyfob button 5*
Button 1 and 5 *assign function to combination of keyfob buttons 1 & 5*
Events (ABAX) *set event generating rules*
Confirm. (ABAX) *set confirmation rules*
Name *set master name*

Edit master *edit existing master*

[select master]

[list of parameters identical as in case of a new master]

Remove master *remove master*

Zone bypasses
- Inhibit — *temporary zone bypass*
- Isolate — *permanent zone bypass*

Set time — *set control panel clock*

System state — *check troubles / check system state*

Events
- **Selected**
  - Select events — *select type of events to be viewed*
  - Select part. — *select partitions from which events are to be viewed*
  - View — *view selected events*
  - View Grade2 — *view events required for Grade 2*
- All — *view all events*
- Grade2 — *view events required for Grade 2*

Reset zones — *reset 43. RESETABLE POWER SUPPLY type outputs*

Clr.latch.outs — *clear latched outputs*

Fin.f.door open — *end door fire opening*

Change options
- Replace battery — *enabling batteries replacement in wireless keypad*
- Keypad chime — *turn on/off CHIME in keypad*
- Outputs chime — *block zone violation signal. on 11. CHIME type outputs*
- Timers — *edit timers*
- Temperatures — *edit the 120. THERMOSTAT output settings*
- Part. timers — *program partition timers*
- No exp.tamp.al. — *block expander tampers*
- Perm.serv.accs. — *enable/disable permanent installer access*
- Serv. can edit — *make user editing available to installer*
- Serv. ArmDis... — *make system control available to installer*
- Perm.DLOADX acc — *enable/disable permanent DLOADX / INTEGRA Soft access*
- DLOADX IP — *set address of computer with DLOADX / INTEGRA Soft program*
- GUARDX IP — *set address of computer with GUARDX program*
- Erase s.message — *erase service note*

Tests
- Partitions — *check current state of partitions*
- Zones — *check current state of zones*
- Supply voltages — *check module supply voltage*
- Radio devices — *check radio signal level for wireless devices*
- Temperatures — *check temperatures (wireless devices with temp. sensor)*
- **Zones test**
  - **New**
    - Burglary zones — *start new test for burglary zones*
    - Fire/tech.zones — *start new test for fire and technical zones*
    - One zone — *start new test for single zone*
  - View results — *view test results*
  - Finish test — *abort test*

Clear results	*clear test results*
Battery test	*test battery and 60. TECHN. - BATTERY LOW zones*
Manual tr. test	*start manual test transmission*
Station 1A test	*start test transmission to station 1 – main phone number*
Station 1B test	*start test transmission to station 1 – backup phone number*
Station 2A test	*start test transmission to station 2 – main phone number*
Station 2B test	*start test transmission to station 2 – backup phone number*
GPRS monit.test	*send test transmission via GPRS [only INTEGRA 128-WRL]*
Messaging test	*start messaging test*
Answering test	*display information on answered tel. call*
Prox. card test	*check proximity card number*
CA-64 PTSA test	*start mimic board test*
View masters	*view master users*
Keypad name	*display keypad name*
File in DLOADX	*display inf. on DLOADX program file with control panel data*
Panel version	*display information on control panel firmware version*
STM prg.version	*display inf. on ABAX syst. firmware [only INTEGRA 128-WRL]*
GSM IMEI/v/sig.	*display information on GSM telephone [only INTEGRA 128-WRL]*
IP/MAC/IMEI/ID	*disp. inf. on ETHM-1 / ETHM-1 Plus / INT-GSM / INT-GSM LTE*
Modules version	*display information on module firmware version*
Time synchron.	*start time synchronization*
Service access	*set installer access time*
Open door	*open selected door controlled by system*
Outs control	*control outputs*
Service mode	*start service mode*
Take SM over	*take over service mode*
Downloading	
Start DWNL-RS	*start local programming*
Finish DWNL-RS	*finish local programming*
Start DWNL-MOD.	*start communication via external modem*
Start DWNL-TEL	*start communication via 300 bps modem*
Start DWNL-CSD	*start CSD communication [only INTEGRA 128-WRL]*
Start DWNL-GPRS	*start GPRS communication [only INTEGRA 128-WRL]*
ETHM-1 →DLOADX	*start comm. with DLOADX / INTEGRA Soft via ETHM-1 Plus*
ETHM-1 →GUARDX	*start communication with GUARDX via ETHM-1 Plus*
INT-GSM →DLOADX	*start comm. with DLOADX / INTEGRA Soft via INT-GSM LTE*
INT-GSM →GUARDX	*start communication with GUARDX via INT-GSM / INT-GSM LTE*

5.3.2 Navigating through the menu and running functions

1. Use the ▼ or ▲ key to find the required submenu or function. The ➢ cursor indicates the submenu that you can enter / function that you can run.
2. Press the ▶ or # key to enter the submenu (the ◀ key allows to exit the submenu) or start the function.

5.3.3 Menu shortcuts

Support for the user menu shortcuts can be disabled by the installer.

You can use shortcuts for quick access to some menu elements (submenus, functions). Press the suitable digit key (or combination of keys) to enter a submenu or start a function. Below is the list of shortcuts. They are shown in square brackets.

[1] Change own code
[2] Users
  [21] New user
  [22] Edit user
  [23] Remove user

If the installer is not authorized to edit the users, the shortcuts beginning with the digit 2 run functions from the MASTERS submenu.

[4] Zone bypasses
  [41] Inhibit
  [42] Isolate
[5] Events
  [51] Selected events
  [52] All events
[6] Set time
[7] System state
[8] Outputs control
[9] Service mode
[0] Downloading
  [01] Start DWNL-RS
  [02] Finish DWNL-RS
  [03] Start DWNL-MOD.
  [04] Start DWNL-TEL
  [05] Start DWNL-CSD [only INTEGRA 128-WRL]
  [06] Start DWNL-GPRS [only INTEGRA 128-WRL]
  [07] ETHM-1 →DLOADX
  [08] ETHM-1 →GUARDX
  [09] INT-GSM →DLOADX
  [00] INT-GSM →GUARDX

5.3.4 Data editing

The editing method depends on the type of data. Having completed the editing, press **#** or **ok** to save the changes. If you want to exit the function without saving the changes, press **✱**.

Described below are general rules for entering data, however they may be different as regards some functions.

Selection from the single-choice list

Shown in the upper line of display is description of the function, and in the lower one – the currently selected item. Press the ▼ or ▲ key to scroll through the list of items. The ▶ and ◀ keys are not used.

Selection from the multiple-choice list

The functions that allow you to make multiple choice can be identified by an additional symbol situated at the right-hand side of the display:

– displayed item is selected / option is enabled,

· – displayed item is not selected / option is disabled.

Press any number key (for some functions, this does not apply to the 0 key) to change the currently displayed symbol to the other one. Press the ▼ or ▲ key to scroll through the list of items. For some functions, pressing the key 0 will allow you to enter the number of item to be edited (e.g. number of zone to be bypassed / unbypassed). This will speed up the search.

For some functions, pressing the ▶ or ◀ key will switch the keypad into the **graphic programming mode**. The and · symbols show the status of up to 32 items (these can be e.g. zones, partitions, etc.). Additionally, in case of zone bypassing, the symbol is used. The ▶ key moves the cursor to the right, and the ◀ key to the left. If the list of items is longer than 32, pressing the ▶ key when the cursor is placed over the last item will display the next list, and pressing the ◀ key when the cursor is placed over the first item will display the previous list ((see also description of the indicators, p. 9). Pressing the key 0, 1 or 2 three times in the graphic mode within 3 seconds will have the following effect:

000 - the · symbol will be displayed at all available items,

111 - the symbol will be displayed at all available items,

222 - reversal of the selection made: the · symbol will be displayed at all items where the symbol was displayed, and the symbol where the · symbol was displayed.

On pressing the ▼ or ▲ key, the keypad will return to the text mode.

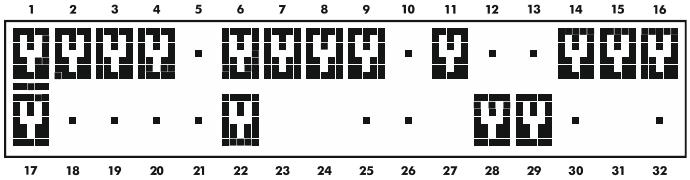


Fig. 3. Example of how information is presented in the graphic programming mode. The blank fields are not available for editing.

Entering decimal and hexadecimal values

To enter digits, use the number keys. To enter characters from A to F, use the 2 and 3 keys. Keep pressing the keys until the required character appears.

Entering names

The characters that can be entered by using the keys are presented in Table 3. Keep pressing the key until the required character appears. Hold down the key to display the digit assigned to the key.

Shown on the left side in the upper line of the display is information about the letter case: [ABC] or [abc] (it will be displayed after pressing any key and will be visible for a few seconds after the last keystroke).

The ▶ key moves the cursor to the right, and the ◀ key to the left. The ▲ key deletes the character on the left side of the cursor.

Key	Characters available after next keystroke																	
1	!	?	'	`	↵	"	{	}	$	%	&	@	\	^	|	⌫	#	1
2	a	b	c	2														
3	d	e	f	3														
4	g	h	i	4														
5	j	k	l	5														
6	m	n	o	6														
7	p	q	r	s	7													
8	t	u	v	·	●	■	▼	↑	←	→	↓	8						
9	w	x	y	z	9													
0		.	,	:	;	+	-	*	/	=	_	<	>	(	)	[	]	0

Table 3. Characters available when entering names. The upper case letters are available under the same keys (to change the letter case, press ▼ key.

5.3.5 Description of user functions

View cleared alarms – available, if the user did not view the violated zones after alarm clearing. It allows to check which zones triggered the alarm. After completion of the viewing, the function is no longer available.

System reset – available to the installer, if the option REQUIRED SYSTEM RESET AFTER VERIFIED ALARM is enabled, and a verified alarm took place. After occurrence of the verified alarm, it is necessary to reset the system using this function, in order to make re-arming possible.

Disarm – allows to disarm the partitions accessible to the user from the given keypad.

Clear alarm – allows to silence the alarm.

Clear other alarms – allows to silence the alarms from other objects, to which the user has normally no access.

Abort voice messaging – terminates the telephone messaging.

The messaging can be cancelled automatically together with alarm clearing. The messaging cancellation rules are defined by the installer.

Arm – allows to arm the partitions accessible to the user from the given keypad.

Arm (2 codes) – allows to initiate arming of the partitions which require entering 2 codes.

Disarm (2codes) – allows to initiate disarming of the partitions which require entering 2 codes.

Defer auto-arming – available when auto-arming delay countdown is running. It allows to postpone by a programmed time period the auto-arming of the partition in which the auto-arming delay countdown is running. Entering just zeros will block the auto-arming function (until the next auto-arming time).

Set auto-arming delay – available when the auto-arming delay is programmed for at least one partition and the auto-arming delay countdown is not currently running in that partition. It allows to postpone by a programmed time period the auto-arming of the partition.

Arming mode – allows to select the arming mode which is to be used (the shortcut key is shown in square brackets):

[0] **full arming** (to be used after everybody has left the protected area),

[1] **full arming + bypasses** (allows the users to stay in the protected area) – the zones for which the BYPASSED IF NO EXIT option is enabled by the installer will be bypassed,

[2] **arming without interior** (allows the users to stay in the protected area):
- interior zones (3. INTERIOR DELAYED zone type) will be disarmed,
- violating the exterior zone (8. EXTERIOR zone type) will trigger a silent alarm,
- violating another alarm zone will trigger a loud alarm.

[3] **arming without interior and without entry delay** (allows the users to stay in the protected area – to be used when nobody else is to enter the protected area) – this arming mode is similar to the previous one, but the delayed zones operate as the instant ones (no entry delay).

Cancel 1st code – if the partition is armed/disarmed using two codes and the first code has already been entered, the user can still cancel the consent to arming/disarming.

Change own code – allows the user to change his/her own code.

Change telephone code – allows the user to change his/her own telephone code.

Change prefix – available to the administrator, if the use of prefixes in the system has been made available by the installer (the prefix length has been defined). It enables to program the prefixes and the time to remind about the need to change the prefix. Each code will have to be preceded by a prefix:

normal – for everyday use. By default, it consists of a suitable number of digits 0 (e.g. if the determined prefix length is 4, the default prefix is 0000),

DURESS – for use, when the user has been forced to enter the code. Using the code will trigger a silent alarm. By default, it consists of a suitable number of digits 4 (e.g. if the determined prefix length is 3, the default prefix is 444).

Users – the following functions are available in the submenu:

New user – allows to create a new user (see: “Adding new user” p. 31).

Edit user – allows to edit the existing users (see: “Edit user” p. 31).

Remove user – allows to remove the existing users (see: “Removing a user” p. 31).

The administrator defines whether the installer is to have access to the USERS submenu (SERV. CAN EDIT option in the CHANGE OPTIONS submenu).

Masters – the submenu provides the following functions available to the installer:

New master – allows to create a new administrator.

Edit master – allows to edit the existing administrators.

Remove master – allows to remove the existing administrators.

Zone bypasses – the following functions are available in the submenu:

Inhibit – allows to temporarily bypass the zones (see: “Zone inhibiting” p. 34).

Isolate – allows to permanently bypass the zones (see: “Zone isolating” p. 35).

Set time – allows to program the control panel clock. The data are entered in the following format:
time – hour:minute:second,
date – day:month:year.

System state – allows to view the troubles and, if the GRADE 2 global option has been enabled by the installer, also the alarms and bypassed zones, as well as to check the partition status.

Events – the submenu contains functions which allow to view the events saved to the control panel memory (see: “Viewing the event log” p. 35).

The content of received SMS messages is also saved to the events log of the INTEGRA 128-WRL control panel.

Reset zones – running the function will result in a temporary deactivation of the 43. RESETABLE POWER SUPPLY type outputs, thus making it possible to reset the alarm memory for detectors supplied from those outputs (e.g. fire detectors).

Clear latched outputs – allows to turn off some of the control panel outputs for which the LATCH option is enabled, as well as the 9. DAY ALARM, 12. SILENT ALARM and 116. INTERNAL SIREN type outputs.

Fin.f.door open – restores the normal operating mode in all modules executing the access control functions (in case of fire, the doors controlled by these modules may be automatically unlocked).

Change options – the following functions are available in the submenu:

Replace battery – allows to disable the tamper protection in the selected wireless keypad for 3 minutes. During this time you can open the keypad enclosure and replace the battery. The function is available if a wireless keypad is installed in the alarm system. The function is supported by ACU-120 / ACU-270 controller with firmware version 5.03 and ACU-220 / ACU-280 controller.

Keypad chime – allows to turn on/off the CHIME in the keypad. The CHIME is five short sounds by means of which the keypad indicates e.g. opening of a door / window when the system is disarmed. The installer defines which zones of the alarm system can trigger the CHIME.

Outputs chime – allows to block the chime signal from selected partitions on the 11. CHIME type output.

Timers – allows to program parameters of the timers, the editing of which is permitted by the installer.

Temperatures – allows to edit the 120. THERMOSTAT output settings (see “Programming the thermostatic output settings” p. 37).

Partition timers – allows to program the partition timers (see: “Programming the partition timer” p. 38).

No expanders tamper alarms – allows to temporarily disable the expansion module tamper supervision. In case of any problems with the expansion modules, report the fact to the installer.

Permanent service access – the option is available to the master user (administrator). If enabled, the installer has permanent access to the alarm system, which, among other things, enables the control panel to be programmed from the keypad or in the DLOADX / INTEGRA Soft program.

Enabling PERMANENT SERVICE ACCESS option will clear the installer access time programmed with the SERVICE ACCESS function. On the other hand, programming the installer access time will disable the PERMANENT SERVICE ACCESS option.

Service can edit – the option is available to the master user (administrator). If it is enabled, the installer can add, edit and delete users in the administrator's object.

Service arm/disarm/clear/bypass – the option is available to the master user (administrator). If it is enabled, the installer can arm/disarm the system, clear alarms and bypass zones in the administrator object.

Permanent DLOADX access – the option is available to the master user (administrator). If it is enabled, the control panel can be programmed in the DLOADX / INTEGRA Soft program, irrespective of whether or not the installer has access to the alarm system.

DLOADX IP – enables programming the address of the computer, on which the DLOADX / INTEGRA Soft program is installed. If the address is programmed, the control panel users can start from the keypad the communication with the DLOADX / INTEGRA Soft program via ETHM-1 Plus / ETHM-1 / INT-GSM / INT-GSM LTE module (see

description of the ETHM-1 →DLOADX and INT-GSM →DLOADX functions, available in the DOWNLOADING submenu). You can enter an IP address or domain name.

GUARDX IP – enables programming the address of the computer, on which the GUARDX program is installed. If the address is programmed, the control panel users can start from the keypad the communication with the GUARDX program via ETHM-1 Plus / ETHM-1 / INT-GSM / INT-GSM LTE module (see description of the ETHM-1 →GUARDX and INT-GSM →GUARDX functions, available in the DOWNLOADING submenu). You can enter an IP address or domain name.

Erase service message – allows the user to delete the service message.

Tests – the following functions are available in the submenu:

Partitions – allows to check the status of partitions accessible to the user and operated from the keypad. The partition status is shown by a symbol. The numbers placed on the glass allow you to identify the partition numbers. By factory default, the partition status is shown by the following symbols (which can be changed by the installer):

b - temporary blocked,
? - entry delay,
E - exit delay (less than 10 seconds),
e - exit delay (more than 10 seconds),
P - fire alarm,
A - alarm,
p - fire alarm memory,
a - alarm memory,
a - armed,
■ - disarmed, not ready to be armed (violated zones),
· - disarmed, ready to be armed.

Zones – allows to check the status of zones in the partitions accessible to the user and operated from the keypad. The zone status is shown by a symbol. The numbers placed on the glass allow you to identify the zone numbers. On starting the function, the status of zones 1-32 is displayed. Use the ▶ and ◀ keys to display the status of other zones (see also description of the ⊞ LEDs, p. 9). By factory default, the zone status is shown by the following symbols (which can be changed by the installer):

b - zone bypass,
l - trouble “long violation”,
f - trouble “no violation”,
T - tamper alarm,
A - alarm,
▉ - zone tamper,
■ - zone violation,
t - tamper alarm memory,
a - alarm memory,
· - zone OK.

Supply voltages – available to the installer. Enables checking of the supply voltage for individual expansion modules.

Temperatures – allows the user to check the temperature. The temperature information is provided by wireless temperature detectors or ABAX 2 wireless devices equipped with a temperature sensor.

Radio devices – allows to check the radio signal level for ABAX 2 / ABAX system wireless devices supported by the control panel.

Zone Test – the submenu contains functions which allow to test the detectors connected to the zones (see: “Zone testing” p. 39).

Battery test – available to the installer. Upon starting the function, the control panel will generate events to inform about the status of batteries of the control panel and hardwired expansion modules with power supply. Additionally, the status of 60. TECH.-BATTERY LOW type zones will be analyzed.

Manual transmission test – generates an event, which starts the procedure of event transmission to the monitoring station (a code sent with the system identifier).

Monitoring station test (1A, 1B, 2A, 2B) – allows to send a test transmission to the monitoring station (separate functions for each of the telephone numbers). When sending the transmission, messages are displayed to inform about the currently performed operation. The function is useful when starting the reporting or in case of any reporting trouble.

GPRS monit.test – sends a test transmission to the monitoring station via cellular data network (GPRS). When sending the transmission, messages on the display provide information on the currently performed operation. **only INTEGRA 128-WRL**

Messaging test – allows to test the messaging function. Upon starting the function:

1. Enter the number of the telephone (consecutive number on the telephone list).
2. Press the ▼ key.
3. Enter the number of voice message.
4. Press the **#** key. The control panel will call the indicated number and play back the message.

Answering test – if this function is started, information on the number of rings and going off-hook is displayed when answering the telephone call.

Proximity card test – allows to check the number of proximity card and establish to whom it belongs (if the card belongs to a user of the system).

CA-64 PTSA test – allows to test the mimic board.

View masters – available to the administrator. It makes it possible to check in which objects the master users are created.

Keypad name – allows to check the given keypad name.

File in DLOADX – displays the date and time of writing the data to the control panel in the DLOADX program and the name of file with control panel data.

Panel version – displays information on the control panel firmware version.

STM program version – displays information on the program version of the processor used to operate ABAX system and control panel zones. **only INTEGRA 128-WRL**

GSM IMEI/v/sig. – allows to check the level of signal received by the GSM telephone antenna, individual identification number of the telephone, and the telephone version. The ▲ and ▼ keys are to be used for scrolling through the displayed information. **only INTEGRA 128-WRL**

IP/MAC/IMEI/ID – displays the information related to the ETHM-1 Plus / ETHM-1 / INT-GSM / INT-GSM LTE modules installed in the system. In the case of the ETHM-1 Plus / ETHM-1 module, the information includes:

- local IP address,
- MAC number,
- public IP address,

– individual identification number assigned to the ETHM-1 Plus module by the SATEL server [ID].

In the case of the INT-GSM / INT-GSM LTE module, the information includes:

– IMEI number,

– individual identification number assigned to the INT-GSM / INT-GSM LTE module by the SATEL server [ID],

– cellular signal strength for SIM1 / SIM2 cards,

– operator of the network into which the SIM1 / SIM2 card is logged,

– SIM1 / SIM2 card account balance (press **#** to check the balance).

Use the ▶ and ◀ keys to scroll the information. If several modules are connected to the control panel, use the ▼ and ▲ keys to scroll the list of modules.

If the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module, information about both modules is displayed, except that the IMEI number of INT-GSM / INT-GSM LTE module is not shown.

Modules versions – allows to check the firmware versions for devices connected to the control panel communication buses.

Time synchronization – allows to manually start synchronization of the control panel clock and the time server. It applies to the control panel to which the ETHM-1 / ETHM-1 Plus / INT-GSM / INT-GSM LTE module is connected. The address of time synchronization server must be programmed in the control panel.

The function is unavailable, if the time synchronization is running. Automatic time synchronization takes place every day at 05:30 and after the control panel restart.

Service access – available to the master user (administrator). Allows to program the time period of installer access to the alarm system. The time is programmed in hours. Programming the value 0 means the installer will have no access.

Open door – allows to unlock the door controlled by the alarm system (modules executing the access control functions) or activate the 101. CARD READ – EXPANDER type outputs.

Outputs control – allow to control the devices connected to the MONO SWITCH, BI SWITCH, REMOTE SWITCH, SHUTTER UP and SHUTTER DOWN type outputs (see: “Outputs control” p. 40).

Service mode – available to the installer. Initiates the service mode.

Take SM over – available to the installer. If the service mode has been initiated from another keypad, it can be “taken over”, i.e. the service menu can be displayed on the keypad, on which the TAKE SM over function has been started.

Downloading – the following functions are available in the submenu:

Start DWNL-RS – available to the installer. Enables communication with the DLOADX / INTEGRA Soft program through the RS-232 port of the control panel (local programming).

Finish DWNL-RS – available to the installer. Disables the local programming of control panel.

Start DWNL-MOD. – enables communication with the DLOADX program via the external modem (analog, GSM or ISDN).

Start DWNL-TEL – enables communication with the DLOADX program via the 300 bps modem.

Start DWNL-CSD – enables CSD communication with the DLOADX program through the built-in GSM communicator. **only INTEGRA 128-WRL**

Start DWNL-GPRS – enables GPRS communication with the DLOADX program through the built-in GSM communicator. **only INTEGRA 128-WRL**

ETHM-1 →DLOADX – enables communication with the DLOADX / INTEGRA Soft program using the ETHM-1 (firmware version 1.03 or newer) / ETHM-1 Plus module. The communication takes place over Ethernet. If the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module and an attempt to establish communication via Ethernet fails, an attempt will be made to establish communication via the cellular data network.

ETHM-1 →GUARDX – enables communication with the GUARDX program using the ETHM-1 (firmware version 1.03 or newer) / ETHM-1 Plus module. The communication takes place over Ethernet. If the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module and an attempt to establish communication via Ethernet fails, an attempt will be made to establish communication via the cellular data network.

INT-GSM →DLOADX – enables communication with the DLOADX / INTEGRA Soft program using the INT-GSM / INT-GSM LTE module. The communication takes place via the cellular data network.

INT-GSM →GUARDX – enables communication with the GUARDX program using the INT-GSM / INT-GSM LTE module. The communication takes place via the cellular data network.

5.4 Arming

This section describes how to initiate the arming procedure. The procedure ends when the exit delay countdown is over (if the procedure is ended successfully, the system becomes armed – see also “Failure of arming procedure” p. 27). If the exit delay time is 0, the system becomes armed instantly.

The installer can configure the alarm system so that the arming functions will not be available after tamper. A message on the display will indicate that the user must call for service. The arming functions will not be available until the service code is entered and confirmed with the # key.

5.4.1 Full arming without partition selection

The arming without partition selection is possible when none of the partitions to which you have access is armed and the keypad is not signaling any alarm.

1. Enter the code and press the # key.
2. When the ARM ALL function is displayed, press the # key. The arming procedure will be initiated in all partitions that you have access to and that are operated by the keypad.

If you can only arm one partition, the arming procedure will be initiated in this partition after you enter the code and press the # key.

5.4.2 Full arming the selected partitions

Arming from the arming / disarming menu

1. Enter the code and press the # key.
2. Keep pressing the ▼ key until the cursor indicates the ARM SELECTED function.
3. Press the # key. A list of partitions which can be armed will be displayed.
4. Use the ▼ or ▲ key to find the partition you want to arm (or press 0 key and enter the partition number).

5. Press any key from 1 to 9. The ▪ symbol in the upper right-hand corner will be replaced by the ✚ symbol (see also “Selection from the multiple-choice list” p. 18).
6. Repeat the steps 4 and 5 for the next partitions you want to arm.
7. Having selected the partitions you want to arm, press the # key.

Arming from the user menu

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Keep pressing the ▼ key until the cursor indicates the ARM function.
3. Press the # key. A list of partitions which can be armed will be displayed.
4. Use the ▼ or ▲ key to find the partition you want to arm (or press 0 key and enter the partition number).
5. Press any key from 1 to 9. The ▪ symbol in the upper right-hand corner will be replaced by the ✚ symbol (see also “Selection from the multiple-choice list” p. 18).
6. Repeat the steps 4 and 5 for the next partitions you want to arm.
7. Having selected the partitions you want to arm, press the # key.

5.4.3 Arming in the selected mode

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Keep pressing the ▼ key until the cursor indicates the ARMING MODE function.
3. Press the # key. A list of arming modes will be displayed (see: description of the ARMING MODE function, p. 19).
4. Use the ▼ or ▲ key to find the arming mode you want to use, and then press the # key.
5. When the ARM function is displayed, press the # key. Proceed in the same way, as for the full arming of selected partitions (steps 4-7).

5.4.4 Quick arming

The installer may permit arming without using the code / card. The partitions indicated by the installer will be armed.

1. Select the arming mode (press one of the keys: 0 – full arming; 1 – full arming + bypasses; 2 – arming without interior; 3 – arming without interior and without entry delay).
2. Press the # key. The arming procedure will begin.

5.4.5 Denial of arming

The installer can program the control panel so that the arming procedure could not be started, if:

– a zone is violated in the partition,
– there is a trouble in the system (including tamper),
– there was a verified alarm.

A message will be displayed in the keypad specifying the cause of refusal.

If after a verified alarm the arming is impossible, the installer must be called. The arming will only be possible after the installer intervention (see: description of the SYSTEM RESET function, p. 19).

Bypassing violated zones when arming

If the arming procedure could not be started, and a message on the display informs you that there are violated zones, you can review the list of such zones upon pressing the 2 key. To scroll through the list, use the ▼ and ▲ keys. If you want to bypass a violated zone, press

the 4 key. A message on the display will prompt you to press the 1 key to confirm that the zone is to be bypassed.

Forced arming

If the arming procedure could not be started, the displayed message can allow of the forced arming (1=Arm). On pressing the 1 key, the system will be armed despite a violated zone or a trouble.

5.4.6 Failure of arming procedure

If the installer has enabled the GRADE 2 option, the arming procedure may end in failure. The system will not be armed, if at the end of the exit delay countdown:

– there is a violated zone in partition which was not violated when the arming procedure was started,
– there is a trouble which did not exist when the arming procedure was started.

5.4.7 Shortening the exit delay time

If such an option is permitted by the installer, the partition exit delay time may be shortened upon pressing in turn the 9 and # keys. In order to shorten the exit delay time you should use the same keypad which was used for arming.

5.5 Disarming and alarm clearing

5.5.1 Disarming all partitions

1. Enter the code and press the # key.
2. When the DISARM ALL function is displayed, press the # key. All partitions that you have access to and that are operated by the keypad will be disarmed.

If you can only disarm one partition, the partition will be disarmed after you enter the code and press the # key.

5.5.2 Disarming selected partitions

Disarming from the arming / disarming menu

1. Enter the code and press the # key.
2. Keep pressing the ▼ key until the cursor indicates the DISARM SELECTED function.
3. Press the # key. A list of partitions which can be disarmed will be displayed.
4. Use the ▼ or ▲ key to find the partition you want to disarm (or press 0 key and enter the partition number).
5. Press any key from 1 to 9. The · symbol in the upper right-hand corner will be replaced by the ■ symbol (see also “Selection from the multiple-choice list” p. 18).
6. Repeat the steps 4 and 5 for the next partitions you want to disarm.
7. Having selected the partitions you want to disarm, press the # key.

Disarming from the user menu

1. Enter the code and press the * key. The user menu will be displayed.
2. When the DISARM function is displayed, press the # key. A list of partitions which can be disarmed will be displayed.
3. Use the ▼ or ▲ key to find the partition you want to disarm (or press 0 key and enter the partition number).

4. Press any key from 1 to 9. The · symbol in the upper right-hand corner will be replaced by the ■ symbol (see also “Selection from the multiple-choice list” p. 18).
5. Repeat the steps 3 and 4 for the next partitions you want to disarm.
6. Having selected the partitions you want to disarm, press the # key.

5.5.3 Alarm clearing without disarming

1. Enter the code and press the * key. The user menu will be displayed.
2. Use the ▼ key to find the CLEAR ALARM function.
3. Press the # key.

5.6 Two-code arming / disarming

1. Enter the code and press the * key. The user menu will be displayed.
2. Keep pressing the ▼ key until the cursor indicates the ARM (2 CODES) / DISARM (2CODES) function.
3. Press the # key. Proceed in the same way, as for the full arming of selected partitions (steps 3-7).
4. If the installer has not set the code validity specify the code validity and press the # key.

Prior to expiration of the code validity, the user entering the second code must arm / disarm the partition using the:

- LCD keypad (see: “Arming” or “Disarming and alarm clearing”),
- partition keypad ([*code*]#),
- reader (read-in of proximity card or DALLAS iButton).

The installer can configure the alarm system so that the second code will have to be entered on another LCD keypad, partition keypad, etc.

5.7 Triggering the alarm from the keypad

The installer can permit triggering alarms from the keypad. To trigger an alarm, do the following:

fire alarm – press the key for approx. 3 seconds,

medical (auxiliary) alarm – press the key for approx. 3 seconds,

panic alarm – press the key for approx. 3 seconds. The installer defines whether the loud panic alarm (setting off the loud alarm signal) or the silent panic alarm (without the loud signal) will be triggered.

5.8 Users

The users can be added, edited and removed by:

- master user (administrator),
- installer (if the SERV. CAN EDIT option is enabled by the administrator),
- user (if granted the USERS EDITING right).

The following data can be defined for the user:

Code – a sequence of digits for user authentication when using keypads and code locks. The control panel supports codes consisting of 4 to 8 characters, however the installer can define the minimum length of the code.

Telephone code – a sequence of digits for user authentication when using the functions of telephone call answering and telephone control (see: “Call answering and telephone control” p. 49).

Partitions – partitions to which the user has access (i.e. he is authorized to arm or disarm them, clear alarms etc.).

Type – see: “User types” p. 30.

User schedule – parameter for the SCHEDULED type code (see: “User types” p. 30.

Validity time – parameter for the RENEWABLE, TEMPORARY or SCHEMATIC type codes (see: “User types” p. 30.

Blocking time – parameter for the BLOCKING PARTITION type code (see: “User types” p. 30.

Rights – define which functions can be used by the user. The following rights (permissions) are available:

- Arming
- Disarming
- Disarm, when other user arm [Can alw.disarm] – if the user does not have this right, he/she can only disarm the system if it was armed by him/her
- Partition alarm clearing [Alarm clearing]
- Object alarm clearing [Object al.clr.]
- Other objects alarm clearing [Other al.clr.]
- Telephone messaging canceling [V.msg.clearing]
- Auto-arming defer [Arm deferring]
- First code for two codes partition [Enter.1st code]
- Second code for two codes partition [Enter.2nd code]
- Access temporary blocked partitions [Block p.access]
- Change own code
- Users editing
- Zone bypasses
- Zone isolation [Zones isolate]
- Clock setting
- Trouble state checking [Troubles view.]
- Event log reviewing [Events viewing]
- Detectors resetting [Zones resett.]
- Options programming [Options chang.]
- Access to menu TEST [Tests]
- Downloading starting [Downloading]
- Access to BI & MONO outputs [Outs control]
- System state review in GUARDX [GUARDX using]
- Resetting outputs [Clr.latch.outs]
- Simple user – having entered the code, confirmed with the **#** key, the user never selects the partitions which are to be armed / disarmed. All partitions the user has access to will be armed / disarmed.
- Administrator – the user has access to the menu functions which are reserved for the administrator

Keypads etc. – additional modules from which the user will be able to operate the system (proximity card arm/disarm devices, partition keypads, code locks, reader expanders).

Proximity cards / DALLAS chips – if the proximity card / DALLAS iButton reader is used in the system, a proximity card / DALLAS iButton can be assigned to the user, which will allow the user to operate the system using the readers.

Keyfobs – in case of the INTEGRA 128-WRL control panel or any other control panel to which a module with keyfob support is connected (ACU-220, ACU-280, ACU-120, ACU-270, ACU-100, ACU-250, INT-RX or INT-RX-S), a keyfob can be assigned to the user, which will allow to operate the system remotely. The user may have up to 2 keyfobs: the APT-200 / APT-210 (supported by the ABAX 2 / ABAX system) or the APT-100 (supported by the ABAX system) and the 433 MHz (supported by the INT-RX or INT-RX-S modules).

Buttons – the button functions are available, if a keyfob has been assigned to the user. It is possible to assign a zone to a keyfob button or combination of buttons. The zone will be violated upon pressing the button / combination of buttons. The assigned zone should not exist physically.

Events (RX) / **Events (ABAX)** – if a keyfob has been assigned to the user, it is possible to define whether pressing the appropriate keyfob button will result in logging an event which informs that the keyfob has been used.

ABAX confirmation – if an ABAX 2 / ABAX system keyfob has been assigned to the user, it is possible to determine the status of which outputs will be shown by the keyfob LEDs on pressing any button.

Name – individual user name.

5.8.1 User types

The name as used in the keypad is shown in the square brackets. The description includes only the codes, but the information provided below applies to all identifiers assigned to the user.

Normal – basic type of user.

One-time [Single] – the user will get one-time access.

Renewable [Time renewable] – the user has access to the system for a defined period of time. The user validity time should be defined. Before the validity time expires, the control panel will prompt the user to change the code. After the code has been changed, the validity time will run from the beginning.

Temporary [Time not renew.] – the user has access to the system for a defined period of time. The user validity time should be defined. After the validity time expires, the user will have no access to the system.

Duress – code to be used in hold-up and duress situations. Use it to trigger a silent alarm and send the event code to the monitoring station.

"Mono" output operating [Mono outputs] – code for control of the MONO SWITCH type outputs.

"Bi" output operating [Bi outputs] – code for control of the BI SWITCH type outputs.

Blocking partition [Part.temp.block.] – the code enables access to the armed partitions. Using the code will block the armed partition(s) (the partition zones will not trigger the burglary alarm). The blocking time is defined individually for each user within the range from 1 to 109 minutes. If, however, the time of blocking for guard round is defined for the partition and its duration is longer, the blocking will last longer.

Cash machine zones bypassing [Acces.to cash m.] – the code to be used to unblock access to the cash dispenser (the 24H CASH MACHINE type zones will be temporarily bypassed in the partition).

Guard – using this code means having made the round (additionally, it can result in the partition being temporarily bypassed for the duration of guard round). The installer defines

the modules which are used to confirm making the round and determines the time interval between successive rounds. If such a user is granted access to the partition, he/she will have the same possibilities as the NORMAL type user.

Scheduled – the user has access to the system as per the time schedule for a specified period of time. It is necessary to select the schedule (the schedule is programmed by the installer) and define the user validity period.

5.8.2 Adding new user

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Press in turn the 2 and 1 keys. The list of functions to define the user parameters will be displayed.

If the service code has been entered, before the list of functions is displayed, it is necessary to specify the object in which the new user is to be created (the service code enables access to all objects).

3. Using the appropriate functions, define the user's parameters.

At least one identifier, i.e. code, proximity card, DALLAS iButton or keyfob, must be assigned to the user.

The new user may not be granted a higher authority level than the person who is adding that user to the system.

4. Press the ✻ key.
5. When a prompt is displayed asking if you want to save the changes, press the 1 key.
6. A message will inform you that a new user has been created. Press the ✻ key to return to the USERS submenu.

5.8.3 Edit user

The user can edit the users in relation to which he/she is the superior. For example, if the user A has created the user B, and the user B has created the user C, then the user A can edit the users B and C.

The user being edited may not be granted a higher authority level than the person who is editing such a user.

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Press the 2 key twice. The list of users will be displayed.
3. Use the ▼ or ▲ key to find the user who is to be edited.
4. Press the # key. The list of functions to define the user parameters will be displayed.
5. Using the appropriate functions, modify the user's parameters.
6. Press the ✻ key.
7. When a prompt is displayed asking if you want to save the changes, press the 1 key.
8. A message will inform you that the user has been modified. Press the ✻ key to return to the list of users.

5.8.4 Removing a user

The user can remove the users in relation to which he/she is the superior. For example, if the user A has created the user B, and the user B has created the user C, then the user A can remove the users B and C.

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Press in turn the 2 and 3 keys. The list of users will be displayed.
3. Use the ▼ or ▲ key to find the user who is to be removed.
4. Press the # key. A message will inform you that the user has been removed.
5. Press the ✻ key to return to the list of users.

5.8.5 Adding proximity card / DALLAS iButton

1. When adding or editing a user / administrator, run the NEW PROX. CARD / NEW DALLAS FUNCTION.
2. Use the ▼ or ▲ key to indicate the device with a reader that you will use to read the proximity card / DALLAS iButton number, or select ENTER MANUALLY.
3. Press the # key.

Adding card / iButton using the reader

1. Present the card / iButton to the reader twice (the messages on the display will guide you).
2. When the card / iButton number is displayed, press the # key. The list of functions for editing settings will be displayed.
3. Press the ✻ key.
4. When a prompt is displayed asking if you want to save the changes, press the 1 key.

Entering card / iButton number manually

1. Enter the card number (see “Entering decimal and hexadecimal values” p. 18).
2. Press the # key. The list of functions for editing settings will be displayed.
3. Press the ✻ key.
4. When a prompt is displayed asking if you want to save the changes, press the 1 key.

5.8.6 Adding keyfob

If you want to add an APT-200 / APT-210 keyfob that was previously used in another system, you must restart the keyfob:
APT-200: press and hold the ○ and ● buttons for 10 seconds,
APT-210: press and hold the ^ and v buttons for 10 seconds,
APT-200 / APT-210: remove the battery for 10 seconds.

1. When adding or editing a user / administrator, run the NEW RX KEYFOB / NEW ABAX KEYFOB function (depending on which keyfob is to be added).
2. Use the ▼ or ▲ key to indicate the module that you will use to add the keyfob, or select ENTER MANUALLY.
3. Press the # key.

Adding keyfob using the module

1. Press a keyfob button twice (the messages on the display will guide you).
2. When the keyfob number is displayed, press the # key. The list of functions for editing settings will be displayed. The list will include functions for editing keyfob settings.
3. Program the keyfob settings (see “Editing keyfob settings” p. 33).
4. Press the ✻ key.
5. When a prompt is displayed asking if you want to save the changes, press the 1 key.

Entering keyfob number manually

1. Enter the keyfob number (see “Entering decimal and hexadecimal values” p. 18).
2. Press the # key. The list of functions for editing settings will be displayed. The list will include functions for editing keyfob settings.
3. Program the keyfob settings (see “Editing keyfob settings” p. 33).
4. Press the ✱ key.
5. When a prompt is displayed asking if you want to save the changes, press the 1 key.

5.8.7 Editing keyfob settings

Prior to assigning the zones to buttons / combinations of buttons, consult the installer.

Numeration of the keyfob buttons and LEDs is described in section “Operating the alarm system using keyfob” (s. 52).

1. When adding or editing a user / administrator, run the BUTTON 1 function.
2. Use the ▼ or ▲ key to select the zone that is to be violated when the 1 keyfob button is pressed. You can also enter the zone number from the keypad.
3. Press the # key. The list of functions for editing settings will be displayed.
4. Configure settings of the other keyfob buttons / button combinations in the same way.
5. Run the EVENTS (RX) / EVENTS (ABAX) function. The list of buttons / button combinations will be displayed. In the upper right-hand corner of the display, an additional symbol is located:
   - – pressing the button / button combination is saved in the event log (default setting),
   - · – pressing the button / button combination is not saved in the event log.
6. Specify whether pressing the button / button combination should be saved in the event log (see “Selection from the multiple-choice list” p. 18) then press the # key.
7. For the APT-200 / APT-210 (ABAX 2 / ABAX) / APT-100 (ABAX) keyfobs, run the ABAX CONFIRMAT. function. A list will be displayed showing the outputs that have been assigned by the installer for confirmation (maximum 8). Select up to 3 of them (see: “Selection from the multiple-choice list” p. 18). Upon pressing any keyfob button, the status of selected outputs will be shown by the keyfob LEDs for a few seconds. Thus you can get confirmation that the function has been executed or information on the current status of the system.

The installer can define the list of outputs from the keypad (ABAX CONFIRMAT. function [SERVICE MODE ▶STRUCTURE ▶HARDWARE ▶EXPANDERS ▶ABAX CONFIRMAT.] or a computer with the DLOADX program (“Keyfobs ABAX” window) / INTEGRA Soft program (“ABAX2 keyfobs” tab).

8. Press the # key. The list of functions for editing settings will be displayed.
9. Press the ✱ key.
10. When a prompt is displayed asking if you want to save the changes, press the 1 key.

5.8.8 Removing keyfob

1. When adding or editing a user / administrator, run the REM. RX KEY FOB / REM.ABAX KEYFOB function (depending on which keyfob is to be removed). This function is available when the user / administrator has a keyfob.
2. When the keyfob number and a prompt asking if you want to remove the keyfob are displayed, press the 1 key. The list of functions for editing settings will be displayed.
3. Press the ✱ key.

4. When a prompt is displayed asking if you want to save the changes, press the 1 key.

Removal of a keyfob will not erase its settings (dependences between the buttons and zones, confirmation rules, etc.). When added to the user / administrator, the new keyfob will have the same settings as the deleted one.

The installer can remove all keyfobs, including their settings, using the functions available in the service mode (▶STRUCTURE ▶HARDWARE ▶EXPANDERS ▶REM.RX KEY FOBS / REM.ABAX KEYFOB).

5.9 Master users (administrators)

The master users (administrators) can be added, edited and removed by the installer. There can be 1 administrator in each object. The administrator has access to all partitions in the object and also specifies how the system can be accessed by using the service code. Most of the parameters which are defined for the ordinary user can be defined for the administrator (see “Users” p. 28).

5.10 Zone bypassing

If a zone is not to trigger alarm, you can bypass it, when the partition to which the zone belongs is disarmed. Zone bypassing is useful e.g. when you want to leave a window open when the system is armed or when a detector connected to the zone is out of order and sets off false alarms.

Zone bypassing reduces the level of protection. If a zone is bypassed while the system is armed, an intruder can exploit this vulnerability.

If a zone is bypassed because of its malfunctioning, call in the installer (service technician) immediately to repair the defect.

For security considerations, the installer may reduce the number of zones that the user will be allowed to bypass.

For the zone bypassing function you can use the graphic mode (see “Selection from the multiple-choice list” p. 18).

5.10.1 Zone inhibiting

Required right: ZONE BYPASSES. The inhibited zone will be bypassed until the partition to which the zone belongs is disarmed, or until the zone is unbypassed by the user.

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Press in turn the 4 and 1 keys to run the INHIBIT function. The list of zones will be displayed (you will see the status of the first of the zones that you can bypass/unbypass). The symbol in the upper right corner of the display indicates:
   - ・ – the zone is not bypassed,
   - ⊟ – the zone is inhibited,
   - ■ – the zone is isolated.
3. Use the ▼ or ▲ key to find the zone you want to inhibit. You can also press the 0 key and enter the zone number.
4. Keep pressing any key from 1 to 9 until the ⊟ symbol is displayed.
5. Press the # key to inhibit the zone and exit the function.

5.10.2 Zone isolating

Required rights: ZONES BYPASSING and ZONE ISOLATION. The isolated zone will remain bypassed until unbypassed by the user.

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Press in turn the 4 and 2 keys to run the ISOLATE function. The list of zones will be displayed (you will see the status of the first of the zones that you can bypass/unbypass). The symbol in the upper right corner of the display indicates:
   · – the zone is not bypassed,
   – the zone is inhibited,
   – the zone is isolated.
3. Use the ▼ or ▲ key to find the zone you want to isolate. You can also press the 0 key and enter the zone number.
4. Keep pressing any key from 1 to 9 until the symbol is displayed.
5. Press the # key to isolate the zones and exit the function.

5.10.3 Unbypassing

Required right: ZONES BYPASSING. To unbypass the zone, you can use the INHIBIT or ISOLATE function. Proceed in the same way as when bypassing zones, but keep pressing any key from 1 to 9 until the · symbol is displayed in the upper right-hand corner.

5.11 Viewing the event log

The events viewing function, when started by the administrator or the ordinary user, provides no information about:

- *panic alarms,*
- *alarms triggered using the DURESS type code.*

5.11.1 Viewing all events

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Press in turn the 5 and 2 keys. The last event which occurred in the system will be displayed.
3. Keep pressing the ▲ key to view previous events.

5.11.2 Viewing the events required for Grade 2

If the GRADE 2 option is enabled in the system, the function allowing the installer and administrators to view events required by EN 50131 for Grade 2 is available.

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Press the 5 key. Functions available in the EVENTS submenu will be displayed.
3. Keep pressing the ▼ key until the cursor indicates the GRADE2 function.
4. Press the # key. The last Grade 2 required event which occurred in the system will be displayed.
5. Keep pressing the ▲ key to view previous events.

5.11.3 Viewing the selected events

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Press in turn the 5 and 1 keys.

3. When the SELECT EVENTS function is displayed, press the # key. The list of event types will be displayed.
4. Select which event types are to be displayed (see “Selection from the multiple-choice list” p. 18).
5. Press the # key. This will bring you back to the SELECTED submenu.
6. Keep pressing the ▼ key until the cursor indicates the VIEW function.
7. Press the # key. The last one of the selected events which occurred in the system will be displayed.
8. Keep pressing the ▲ key to view previous events.

In addition to defining the event types to be displayed, the SELECT PART. function can also be used to indicate the partitions to which the events are to refer.

If the GRADE 2 option is enabled in the system, the installer or administrator can use the VIEW GRADE2 function instead of the VIEW function. In such a case, the events selected among those required by the EN 50131 standard for Grade 2 will be displayed.

5.11.4 Way of presenting events

The following information is shown in the display upper line:

– date and time of event occurrence,
– additional information on the events in shortened form, e.g. number of partition, zone, user, timer, expander, keypad, etc.

Event description is displayed in the lower line.

If no key is pressed for a few seconds, additional information on the event will be displayed, e.g. name of partition, zone, user, timer, expander, keypad, etc. After a few seconds, the event description will be displayed again, and so on.

Press the ▶ key to display additional information on the event.

Press the ◀ key when the event description is displayed to see further additional information on the event, shown in a shortened form.

Using the ◀ or ▶ key will block the automatic toggling between description of the event and additional information on the event.

After the list of events has been scrolled through using the ▲ or ▼ key, the automatic toggling between description of the event and additional information on the event will be restored.

5.12 Replacing batteries in wireless keypad

If the battery in the INT-KWRL2 / INT-KWRL wireless keypad is low, it should be replaced. You must run the REPLACE BATTERY function before you open the keypad enclosure.

1. Enter the code and press the * key. The user menu will be displayed.
2. Keep pressing the ▼ key until the cursor indicates the CHANGE OPTIONS function.
3. Press the # key.
4. Keep pressing the ▼ key until the cursor indicates the REPLACE BATTERY function.
5. Press the # key.
6. Keep pressing the ▼ key until you find the wireless keypad in which you want to replace the battery.
7. Press the # key. The status of tamper switch in the keypad will not be checked for 3 minutes, which allows you to replace the battery.

5.13 Programming the thermostatic output settings

The user can edit the following settings of the thermostatic output (the 120. THERMOSTAT type output):

- temperature 1 (economic temperature),
- temperature 2 (comfortable temperature),
- hysteresis,
- COOLING option.

Ask the installer to find out what each thermostatic output is used for.

Thermostatic output settings are used to adjust the operating parameters of the ART-200 / ART-210 wireless radiator thermostats.

1. Enter the code and press the ✻ key. The user menu will be displayed.
2. Keep pressing the ▼ key until the cursor indicates the CHANGE OPTIONS submenu.
3. Press the # key.
4. Keep pressing the ▼ key until the cursor indicates the TEMPERATURES function.
5. Press the # key. The list of the 120. THERMOSTAT type outputs will be displayed.
6. Keep pressing the ▼ or ▲ key until the cursor indicates the thermostatic output whose settings you want to edit.
7. Press the # key. The functions used to edit the thermostatic output settings will be displayed.

5.13.1 Programming temperature 1 (economic temperature)

Temperature 1 (economic temperature) is the first temperature threshold. If the first temperature threshold is active:

- heating: the output will be turned on when the temperature drops below temperature T1,
- cooling: the output will be turned on when the temperature rises above temperature T1.

Ask the installer to find out when the first temperature threshold is active.

1. Start the TEMPERATURE 1 function. The temperature will be displayed.
2. Enter the new temperature (see “Temperature programming rules”).
3. Press the # key to confirm the changes.

5.13.2 Programming temperature 2 (comfortable temperature)

Temperature 2 (comfortable temperature) is the second temperature threshold. If the second temperature threshold is active:

- heating: the output will be turned on when the temperature drops below temperature T2,
- cooling: the output will be turned on when the temperature rises above temperature T2.

Ask the installer to find out when the second temperature threshold is active.

1. Start the TEMPERATURE 2 function. The temperature will be displayed.
2. Enter the new temperature (see “Temperature programming rules”).
3. Press the # key to confirm the changes.

5.13.3 Programming hysteresis

Hysteresis is the temperature difference between turning the thermostatic output on and off. The output will be turned on when temperature drops below the threshold (heating) / rises above the threshold (cooling) by a value higher than the hysteresis. The output will be turned

off when the temperature reaches the threshold. Hysteresis is used to prevent the output from being repeatedly turned on and off when the temperature fluctuates.

1. Start the HYSTERESIS function. The hysteresis will be displayed.
2. Enter the new hysteresis (see: “Hysteresis programming rules”).
3. Press the # key to confirm the changes.

5.13.4 Enabling / disabling the COOLING option

If this option is enabled, the output is turned on when the temperature rises above the set value (the output controls the cooling). If this option is disabled, the output is turned on when the temperature drops below the set value (the output controls the heating).

To enable / disable the option, press the ▶ key. When the option is enabled, the ■ symbol is displayed. When the option is disabled, the · symbol is displayed.

5.13.5 Rules for programming the thermostatic output settings

Temperature programming rules

You can enter a value from -30°C to 70°C (with accuracy to 0.5°). To enter a negative value, press the 3 key when the cursor is on the first position. To clear the currently set value, press the 2 key when the cursor is on the first position.

The ART-200 / ART-210 wireless radiator thermostat regulates temperature in the range from 5°C to 30°C.

Hysteresis programming rules

You can enter a value from 0°C to 7.5°C (with accuracy to 0.5°). If you program 0°C, a hysteresis of 0.5°C will be set.

5.14 Programming the partition timer

The partition timer automatically arms / disarms the partition.

1. Enter the code and press the * key. The user menu will be displayed.
2. Keep pressing the ▼ key until the cursor indicates the CHANGE OPTIONS submenu.
3. Press the # key.
4. Keep pressing the ▼ key until the cursor indicates the PART. TIMERS function.
5. Press the # key. The list of partitions will be displayed.
6. Use the ▼ or ▲ key to find in the list the partition for which you want to program the timer.
7. Press the # key.
8. When the ACTIVE option is displayed, make sure it is enabled (the 4 symbol is displayed next to the option). If it is not enabled (the · symbol is displayed next to the option), press any digit key.
9. Keep pressing the ▼ key until the cursor indicates the TYPE function.
10. Press the # key.
11. Use the ▼ or ▲ key to select the timer type:
    everyday – if the partition is to be armed / disarmed at the same time every day,
    weekly – if the partition is to be armed / disarmed at different times on different days of the week.
12. Press the # key.

13. If you have selected the daily variant, the function will allow you at once to program the arming time, and upon pressing the ▲ or ▼ key – the disarming time. Upon confirmation with the # key, you will be brought back to the list of options and functions.
14. If you have selected the weekly variant, you will be brought back to the list of options and functions, where functions will appear to enable programming of the arming / disarming time for each day of the week (in the same way as for daily timer).

i *Programming the value 99:99 means that the partition will not be armed / disarmed.*

15. After the arming time has been programmed, an additional function will be displayed, which allows you to define which arming mode will be activated by the given timer. By default, the timer activates the full arming mode. If another arming mode is to be activated, run this function (for the daily timer or individually for each day of the week) and, use the ▲ or ▼ key to select another arming mode and press the # key.
16. Having programmed all parameters, press the * key.
17. When a prompt is displayed asking if you want to save the changes, press the 1 key.

5.15 Zone testing

Within periodic inspections of the security alarm system, the detectors must be checked for proper functioning. The zone testing function will allow you to do it without triggering the reaction normally expected on violation, which is of particular importance in case of permanently armed zones.

1. Enter the code and press the * key. The user menu will be displayed.
2. Keep pressing the ▼ key until the cursor indicates the TESTS submenu.
3. Press the # key.
4. Keep pressing the ▼ key until the cursor indicates the ZONE TEST submenu.
5. Press the # key.
6. When the NEW function is displayed, press the # key.
7. Select whether burglary zones or fire and technical zones, or single zone, will be tested, and then press the # key.
8. Select the partitions in which zones will be tested (see: “Selection from the multiple-choice list” p. 18).
9. Specify the test duration (maximum 50 minutes) and press the # key.
10. Define, whether violation of a zone is to trigger CHIME in the keypad (if yes, press any numeric key – the ▣ symbol will be displayed).
11. Press the # key. The zone test will start.

i *Beginning of the zone test in any partition will start the test mode in all ABAX 2 / ABAX system wireless devices which are used together with the control panel (LED indicators of the wireless detectors will signal violations).*

If any detectors with remote LED indicator ON/OFF function are connected to the control panel, you can switch on the LED indicators in them for the test duration (the installer can configure the control panel so that this will take place automatically at the beginning of the test).

You can terminate the zone test before expiration of the programmed time, using the FINISH test function (▶TESTS ▶ZONE TEST ▶FINISH TEST). Up to 6 seconds can elapse between starting the function to the actual end of the test (during this the FINISH TEST function will be still available).

12. Depending on the type of tested detector:
    - magnetic contact – open and close the door or window protected by the magnetic contact,
    - motion detectors – pass in front of the detector,
    - other detectors – follow the manufacturer's directions for the detector testing.
13. Look through the test results. To do so, enter again the ZONES TEST submenu (see: steps 1-5) and start the VIEW RESULTS function. You can scroll through the list of results, using the ▲ and ▼ keys. Press the ▶ or ◀ key to switch over the display to the graphic mode, in which the results are shown as symbols:
    - ▪ - zone was not violated,
    - ■ - zone was violated.

    Pressing the ▶ or ◀ key in the graphic mode will display information on another set of zones (see also description of the ⊞ LED indicators, p. 9).

The test results can be cleared using the CLEAR RESULTS function (▶TESTS ▶ZONES TEST ▶CLEAR RESULTS).

5.16 Outputs control

Using the keypad, you can control the operation of devices connected to the outputs (e.g. open/close roller blinds/shutters, turn on/off lighting or heating, etc.). The installer defines how the outputs should work (whether the output will be activated for a defined time or it will remain active until deactivated by the user, timer, etc.).

If permitted by the installer, the control function can be started without using the code, upon pressing in turn the 8 and # keys.

1. Enter the code and press the ✱ key. The user menu will be displayed.
2. Press the 8 key. Depending on the output settings, the following will be displayed:
    - list of output groups – use the ▼ or ▲ key to find the group with the output, then press the # key to display the list of controllable outputs,
    - the list of controllable outputs.
3. Use the ▼ or ▲ key to find the output you want to control. The output status is shown by a symbol. For the MONO SWITCH, BI SWITCH and REMOTE SWITCH outputs the following symbols are used:
    - ▪ - output inactive (turned off),
    - ■ - output active (turned on)

The output status can be presented according to the zone status. The displayed symbols should then be interpreted as follows:

- ▪ - *zone not violated (the device controlled by output is inactive),*
- ■ - *zone violated (the device controlled by output is active).*

The way of presenting the status of roller shutter outputs differs from how the status of other outputs is presented (see "Controlling the roller shutter outputs").

5.16.1 Controlling the MONO SWITCH type of output

When the output is turned off:

- press the ▶ key to turn on the output for the time programmed by the installer,

- press the # key to program the time for which the output is to be turned on, and after programming the time, press the # key again.

When the output is turned on, press any number key to turn it off.

5.16.2 Controlling the BI SWITCH type of output

Press the # or ▶ key to switch the output status.

When the output is turned on, press any number key to turn it off.

5.16.3 Controlling the REMOTE SWITCH type of outputs

Depending on the output settings, press the # or ▶ key to turn on the output for the time programmed by the installer or switch the output status.

When the output is turned on, press any number key to turn it off.

5.16.4 Controlling the roller shutter outputs

A pair of outputs programmed as SHUTTER UP and SHUTTER DOWN is used for controlling the roller shutter. Displayed on the list of outputs is only the name of output programmed as SHUTTER UP. The roller shutter (output) status is shown by symbols:

· - roller shutter not moving (both outputs are turned off),

↑ - roller shutter moving up (SHUTTER UP output is turned on),

↓ - roller shutter moving down (SHUTTER DOWN output is turned on).

If you want to control the roller shutter, press the # or ▶ key. A cursor in the form of a horizontal line will be displayed under the symbol showing the roller shutter status.

If the roller shutter is not moving:

- press the ▲ key to move the roller shutter up (turn on the SHUTTER UP output),
- press the ▼ key to move the roller shutter down (turn on the SHUTTER DOWN output).

If the roller shutter is moving up, press the ▼ key or any number key to stop the roller shutter (turn off the SHUTTER UP output).

If the roller shutter is moving down, press the ▲ key or any number key to stop the roller shutter (turn off the SHUTTER DOWN output).

If you want to stop controlling the roller shutter, press the # or ◀ key. The cursor under the symbol showing the roller shutter status will disappear.

6. Using the partition keypad

The main task of the partition keypad is to arm/disarm one partition. Additionally, it offers a number of other functions, including e.g. the access control (supervision of a single door).

SATEL offers the following partition keypads:

INT-S,

INT-SK,

INT-SCR (can operate as the INT-SCR partition keypad with proximity card reader or the INT-S/SK partition keypad),

CR-MF5 (can operate as the INT-SCR partition keypad with proximity card reader),

SO-MF5 (can operate as the INT-SCR partition keypad with proximity card reader).

This manual includes information on the INT-S, INT-SK, INT-SCR keypads. For information on other keypads, please refer to the manuals of these keypads.

The keypads are available with keys backlight in various color versions. The color version is indicated by an additional letter symbol included in the keypad designation (e.g. INT-S-GR – green backlight; INT-S-BL – blue backlight).

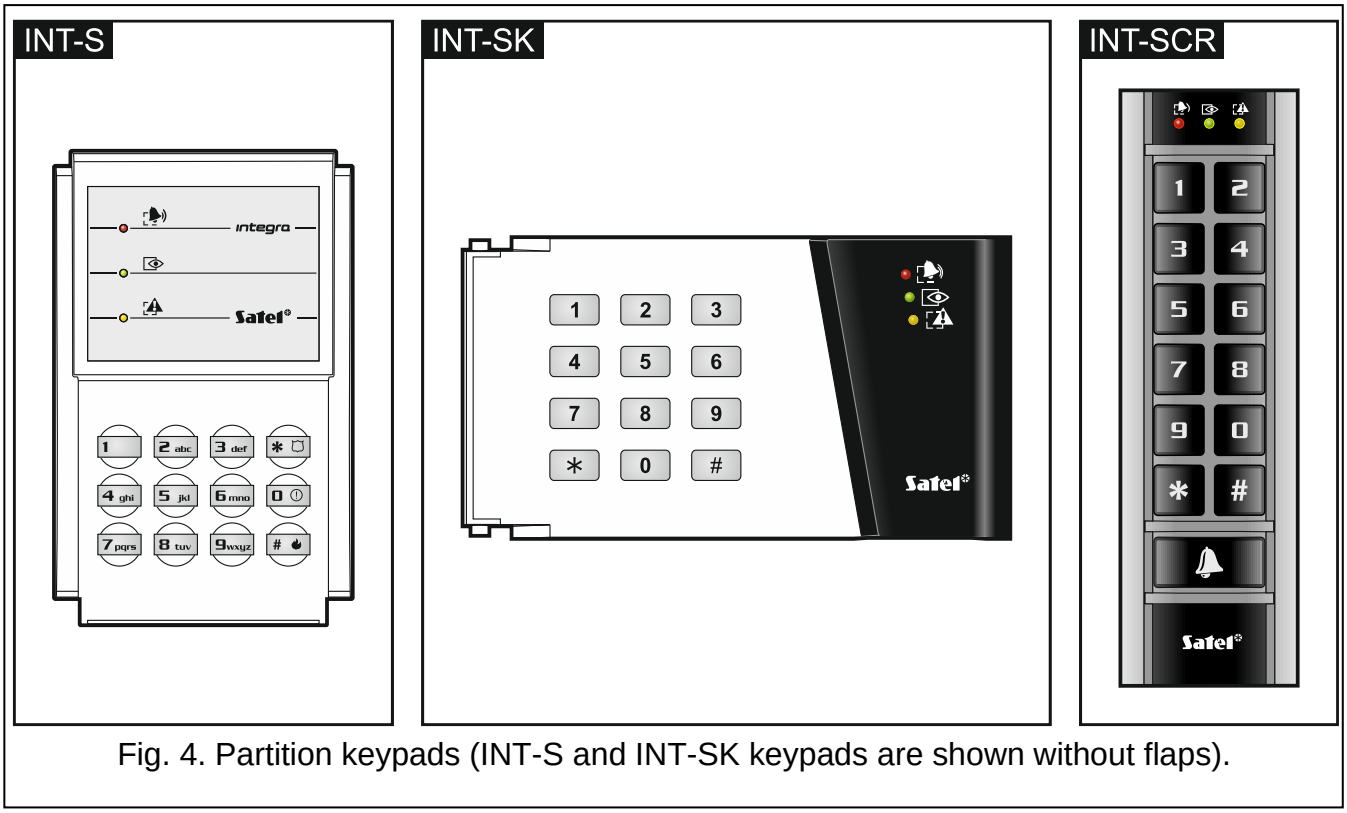


Fig. 4. Partition keypads (INT-S and INT-SK keypads are shown without flaps).

6.1 Description of partition keypads

6.1.1 LED indicators

LED	Color	Description
	green	**ON** – partition armed **flashing** – exit delay countdown is running in partition
	red	**ON** or **flashing** – alarm or alarm memory
	yellow	**flashing** – trouble or trouble memory (LED is turned off when the partition is armed)

Table 4. Description of LED indicators in partition keypads.

Information about the armed state can be extinguished after a time period defined by the installer.

If the installer has enabled the GRADE 2 option:

- *the indicator will not inform about the alarms,*
- *flashing of the indicator means that there is a trouble in the system, some zones are bypassed, or that there was an alarm.*

The and indicators flashing alternately indicate that the system is waiting for the second code during the two code arming / disarming.

All indicators flashing in turn indicate that there is no communication with the control panel.

6.1.2 Keys

The keys are used to enter the code and run functions available from the partition keypad.

In the INT-SCR keypad, the [🔔] key is additionally available. It controls the keypad OC type output (the output is active, when the key is pressed).

6.1.3 Built-in proximity card reader

The INT-SCR keypad has a built-in proximity card reader (proximity tags or other 125 kHz passive transponders). Presenting the card is interpreted in the same way as entering the code and confirming with the ✱ key. Holding the card (for approx. 3 seconds) is interpreted in the same way as entering the code and confirming with the # key.

6.1.4 Sound signaling

Beeps generated when operating

The installer can disable the sound signaling or replace it with flashing of the keys backlight.

1 short beep – a number key was pressed or a code / card was used.

2 short beeps – the first code / card is accepted during two-code arming / disarming.

3 short beeps – signaling of:

- starting the procedure of arming (there is exit delay in the partition) or arming (there is no exit delay in the partition),
- disarming and/or alarm clearing.

4 short and 1 long beeps – confirmation that the function has been executed.

3 pairs of short beeps – code change is required.

1 long beep – refusal to arm (there are violated zones in the partition or there is a trouble).

2 long beeps – wrong code / card.

3 long beeps – unavailable function.

Events signaled by sounds

Only installer selected events are signaled.

Alarms are signaled for the time programmed by the installer.

5 short beeps – zone violation (CHIME).

Long beep every 3 seconds, followed by a series of short beeps for 10 seconds and 1 long beep – countdown of exit delay (if the time is shorter than 10 seconds, only the final sequence of short beeps will be generated).

A sequence of 7 beeps of diminishing duration, repeated every few seconds – countdown of auto-arming delay.

2 short beeps every second – countdown of entry delay.

Continuous beep – alarm.

Long beeps every 2 seconds – alarm memory.

Long beep every second – fire alarm.

Short beeps every 2 seconds – fire alarm memory.

Very short beeps – door open too long.

6.2 Functions available from the partition keypad

The availability of the functions depends on:

- user type and rights,
- keypad settings,
- partition status.

6.2.1 [Code]✱ / presenting the card

Enter the code and press ✱ / present the card to:

- disarm the partition,
- clear the alarm,
- get access (turn on the output controlling the electric strike, electromagnetic lock or other door actuator),
- switch the status of 25. BI SWITCH outputs,
- turn on the 24. MONO SWITCH outputs,
- confirm the guard round,
- temporarily block the partition.

Several functions can be run simultaneously (e.g. disarming, clearing the alarm and getting access).

If the and LEDs are flashing alternately after you used a code or a card, it means that using both code and card is required to run a function.

If the and LEDs are flashing alternately after you used a code/card to disarm the partition, it means that the keypad is waiting for the second user code/card (two-code disarming).

6.2.2 [Code]# / holding the card

Enter the code and press # / hold the card to:

- start the partition arming procedure / arm the partition,
- disarm the partition,
- clear the alarm,
- get access (turn on the output controlling the electric strike, electromagnetic lock or other door actuator),
- switch the status of 25. BI SWITCH outputs,
- turn on the 24. MONO SWITCH outputs,
- confirm the guard round,
- temporarily block the partition,
- unblock cash machine access.

Several functions can be run simultaneously (e.g. disarming, clearing the alarm and getting access).

If the and LEDs are flashing alternately after you used a code or a card, it means that using both code and card is required to run a function.

If the and LEDs are flashing alternately after you used a code/card to arm / disarm the partition, it means that the keypad is waiting for the second user code/card (two-code arming / disarming).

6.2.3 Quick arming

The installer can permit the arming without user authorization.

1. Select the arming mode by pressing one of the keys:
   0 - full arming,
   1 - full arming + bypasses,
   2 - arming without interior,
   3 - arming without interior and without entry delay.
2. Press the **#** key. The arming procedure will begin (if the exit delay is 0, the partition will be armed immediately).

6.2.4 Triggering the alarm from the keypad

The installer can permit triggering alarms from the keypad. To trigger an alarm:

fire alarm – press the # (INT-S) / * (INT-SK) / # (INT-SCR) key for approx. 3 seconds,

medical (auxiliary) alarm – press the 0 key for approx. 3 seconds,

panic alarm – press the * (INT-S) / # (INT-SK) / * (INT-SCR) key for approx. 3 seconds, The installer defines whether the loud panic alarm (setting off the loud alarm signal) or the silent panic alarm (without the loud signal) will be triggered.

6.2.5 Silencing the alarm sound at the keypad

Press any number key to silence the alarm signaling in the keypad for about 40 seconds.

6.2.6 Code changing

You can change your code if the keypad settings allow it.

1. Press and hold the 1 key for 3 seconds.
2. When the and indicators start flashing alternately, enter the old code and press the **#** key.
3. When the and indicators start flashing alternately, enter the new code and press the **#** key.

7. Using the entry keypad

The INT-SCR multifunction keypad can work in the entry keypad mode (INT-ENT). The main task of the zone keypad is activation of the delay for the 3. INTERIOR DELAYED type zones. The time period during which these zones will act as delayed ones is programmable for the keypad. If more than one zone keypads are assigned to the partition, a different delay activation time can be programmed for each of them. After expiry of the programmed time, the interior delayed zones will again operate as instant ones.

7.1 Description of the entry keypad

7.1.1 LED indicators

LED	Color	Description
	green	**flashing** – delay activation time is running

The indicators flashing in turn from left to right indicate that there is no communication with the control panel.

7.1.2 Keys

The keys are used to enter the code and run functions available from the keypad.

The [🔔] key controls the keypad OC output (the output is turned on when the key is pressed).

7.1.3 Built-in proximity card reader

The keypad has a built-in proximity card reader (proximity tags or other 125 kHz passive transponders). Presenting the card is interpreted in the same way as entering the code and confirming with the [*] key. Holding the card (for approx. 3 seconds) is interpreted in the same way as entering the code and confirming with the [#] key.

7.1.4 Sound signaling

Beeps generated when operating

The installer can disable the sound signaling or replace it with flashing of the keys backlight.

1 short beep – a number key was pressed or a code / card was used.

3 short beeps – confirmation of delay activation.

4 short and 1 long beeps – confirmation that the function has been executed.

3 pairs of short beeps – code change is required.

2 long beeps – wrong code / card.

3 long beeps – delay activation is impossible (the partition is disarmed or the delay has already been started) or the function is unavailable.

Event signaling

The installer decides whether events are signaled by sounds.

Short beep every 3 seconds – countdown of delay activation time.

7.2 Functions available from the entry keypad

The availability of the functions depends on:

- user type and rights,
- keypad settings,
- partition status.

Enter the code and press the * or # key / present or hold the card to:

- activate delay for the 3. INTERIOR DELAYED zones,
- switch the status of 25. BI SWITCH outputs,
- turn on the 24. MONO SWITCH outputs,
- confirm the guard round.

8. Using the code lock

The basic task of the code lock is to execute the access control function (supervise a single door).

SATEL offers the following code locks:

INT-SZ,

INT-SZK.

The code locks are available with keys backlight in various color versions. The color version is indicated by an additional letter symbol included in the code lock designation (e.g. INT-SZ-GR – green backlight; INT-SZ-BL – blue backlight).

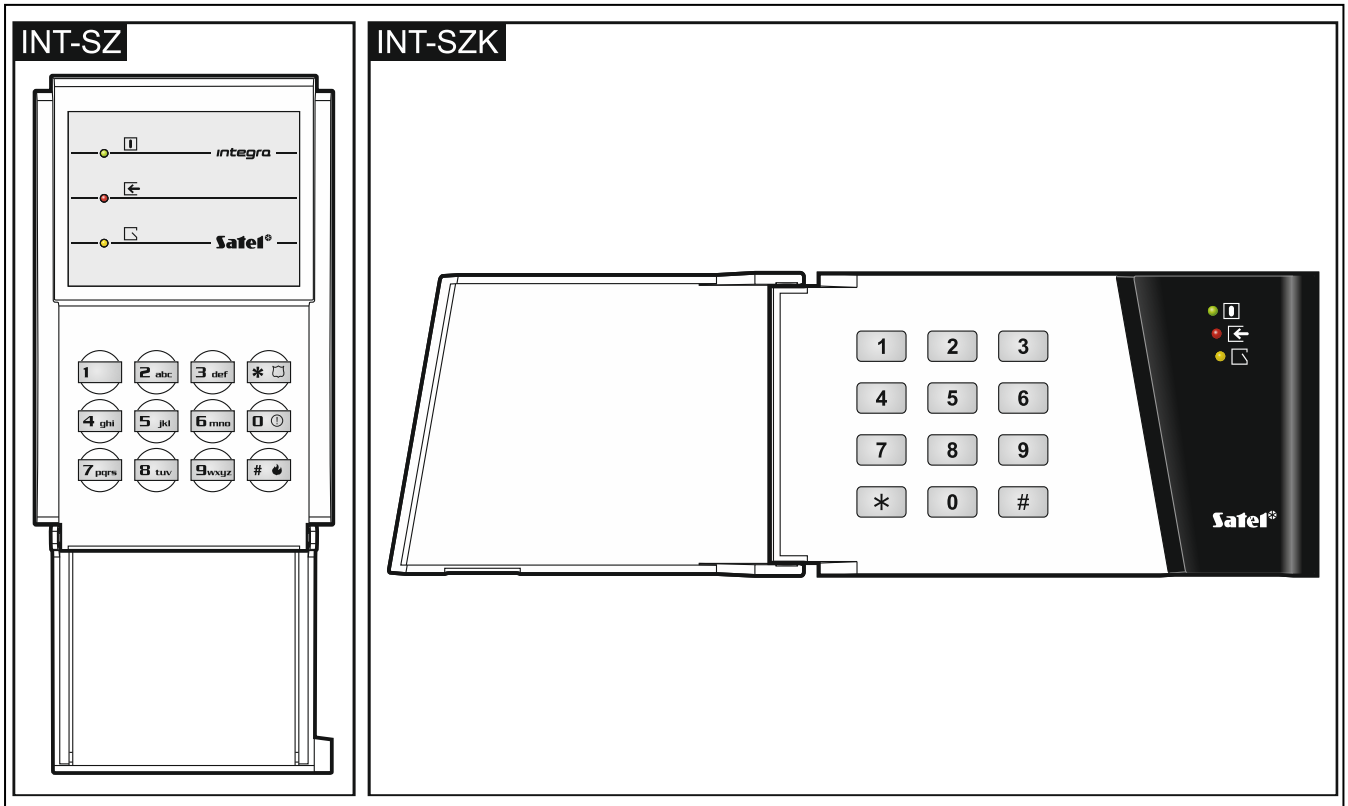


Fig. 5. Code locks.

8.1 Description of code locks

8.1.1 LED indicators

LED	Color	Description
	green	**ON** – code lock is operated by the control panel
	red	**ON** – door unlocked
	yellow	**flashing** – door open

Table 5. Description of the code lock LED indicators.

All indicators flashing in turn indicate that there is no communication with the control panel.

8.1.2 Keys

The keys are used to enter the code and run functions available from the code lock.

8.1.3 Sound signaling

Beeps generated when operating

The installer can disable the sound signaling or replace it with flashing of the keys backlight.

1 short beep – a number key was pressed or a code was used.
4 short and 1 long beeps – confirmation of door unlocking or execution of another function.
3 pairs of short beeps – code change is required.
2 long beeps – wrong code.
3 long beeps – unavailable function.

Events signaled by sounds

Only installer selected events are signaled.

5 short beeps – zone violation (CHIME).
Very short beeps – door open too long.

8.2 Functions available from code lock

The availability of the functions depends on:

- user type and rights,
- code lock settings,
- partition status.

8.2.1 [Code]✻ / [Code]#

Enter the code and press the ✻ or # key to:

- get access (turn on the lock relay output),
- switch the status of 25. BI SWITCH outputs,
- turn on the 24. MONO SWITCH outputs,

- confirm the guard round,
- temporarily block the partition.

8.2.2 Generating alarm from the keypad

The installer can permit generating alarms from the keypad. To generate an alarm:

fire alarm – press the [# 🔥] (INT-SZ) / [*] (INT-SZK) key for approx. 3 seconds,

medical (auxiliary) alarm – press the 0 key for approx. 3 seconds,

panic alarm – press the [* 🔔] (INT-SZ) / [#] (INT-SZK) key for approx. 3 seconds. The installer defines whether the generated alarm will be loud (setting off the loud alarm signaling) or silent (without loud signaling).

8.2.3 Code changing

You can change your code if the lock settings allow it.

1. Press the 1 key for approx. 3 seconds.
2. When the [1] and [←] indicators start flashing alternately, enter the old code and press the # key.
3. When the [1] and [↘] indicators start flashing alternately, enter the new code and press the # key.

9. Confirming voice messaging

The installer can configure the control panel so that confirmation of listening to the voice message be required. If there is no confirmation, the control panel can connect many times for playback of the message. Having listened to the message can be confirmed from the keypad of DTMF dialing telephone. The installer defines whether any 4-digit sequence is sufficient to confirm receipt of a voice message, or it must be a specific code. After entering of the code, the control panel indicates with sounds:

1 short beep repeated every 3 seconds – the message has been confirmed, wait for playback of the next voice message,

4 short and 1 long beeps – the message has been confirmed, there are no more voice messages,

2 long beeps – an invalid code has been entered (the message has not been confirmed).

If the control panel is sending messages about several events and confirmation of the voice messages is required, each message should be confirmed. The first message must be confirmed before the second message can be played back, and so on.

The installer can configure the control panel so that acknowledgement of receiving the message by the user will:

- *clear messaging other users,*
- *allow to get access to the INT-VG module voice menu.*

10. Call answering and telephone control

The information below does not apply to the control panels to which the INT-VG module is connected.

The call answering and telephone control functions are available to the users who have the **telephone code**. These functions require that the DTMF dialing phone be used. The call

answering function allows to get information on the partition status (armed, disarmed). Owing to the telephone control function, it is possible to control the REMOTE SWITCH type outputs using the telephone.

10.1 Answering phone calls

1. Establish connection with the control panel, using one of the following methods (consult the installer to learn which method is supported by the control panel):

   single call – call the telephone number of control panel. The control panel will answer the call after the number of rings programmed by the installer.

   double call – call the telephone number of control panel. Hang up after the number of rings programmed by the installer. Call again within three minutes. The call will be answered by the control panel immediately.

   Establishing connection will be signaled by three short beeps.
2. Enter the telephone code on the telephone keypad. 4 short beeps and 1 long beep will confirm that you have got access to the call answering function. If the entered code is invalid, this will be signaled by the control panel by two long beeps.

If you make a mistake when entering the code, enter the 4 digits anyway, and when the control panel signals that the code is wrong, enter the correct code.

After entering three wrong codes, the control panel will hang up.

In case of a single call, if:

- *no code has been entered and the connection is terminated,*
- *an invalid code has been entered and the connection is terminated,*

the control panel will answer no calls for the next few minutes. It enables e.g. a fax to be connected after the control panel.

3. Within up to 15 seconds, enter the 2-digit partition number (e.g. 01, 07 or 15). The control panel will inform you about the partition status by means of sounds:

   3 short beeps – partition disarmed,

   4 short and 1 long beeps – partition armed.

   If you do not press any key for 15 seconds, the control panel will hang up.
4. Press in turn the 0 and # keys. The control panel will hang up.

10.2 Telephone control

1. Get access to the phone call answering function (steps 1-2 in section “Answering phone calls””).
2. Within up to 15 seconds, press in turn the 2 and # keys on the telephone keypad. 4 short beeps and 1 long beep will confirm that you have got access to the telephone control function.
3. Within up to 15 seconds, enter the 2-digit number of the remote switch (e.g. 01, 07 or 15). The control panel will indicate the remote switch status change with sounds:

   3 short beeps – the switch has been turned off,

   4 short and 1 long beeps – the switch has been turned on.

The operating mode of the REMOTE SWITCH type output depends on how the output has been configured by the installer.

4. Press in turn the 0 and # keys (the control panel will hang up) or 1 and # (return to the phone call answering function).

10.3 Audio alarm verification

Remote audio alarm verification is possible when the INT-AV module is connected to the control panel.

1. Get access to the phone call answering function (steps 1-2 in section “Answering phone calls”).
2. Within up to 15 seconds, press in turn the 3 and # keys on the telephone keypad. 4 short beeps and 1 long beep will confirm that you have got access to the function of audible alarm verification. The DTMF commands you can use after starting the listen-in / talk session are described in the INT-AV module manual.

11. SMS control

In the case of INTEGRA 128-WRL control panel or any control panel to which the INT-GSM / INT-GSM LTE module is connected, you can control the alarm system using SMS messages. The SMS message must be sent to the control panel / module (to the number of the SIM card installed). Include the control command in the SMS body. Agree with the installer on:

- content of the control commands.
- the functions to be run by these commands. The following functions are available:
  - zone violation,
  - zone inhibiting
  - unbypassing
  - arming
  - disarming,
  - alarm clearing
  - activating the output,
  - deactivating the output,
  - toggling the output,
  - checking partition status,
  - sending USSD code to the operator of SIM card (e.g. to check the card balance or to top it up). The reply received from the operator will be sent as an SMS message to the phone number from which the control command was sent.
- other SMS control requirements (e.g. phone numbers from which it will be possible to send control commands).

You can insert several control commands in one SMS message.

When sending the USSD codes, the SMS message must have the following form:

xxxx=yyyy=

where “xxxx” is the control command and “yyyy” is the USSD code supported by the cellular network operator.

In the case of INT-GSM / INT-GSM LTE module you can use a command controlling the sending of USSD codes to send an SMS message. The SMS message must have the following form:

xxxx=tttt:cccc=

where “xxxx” is the control command, “tttt” is the phone number to which the SMS message is to be send, and “cccc” is the content of SMS message to be sent.

12. Operating the alarm system using keyfob

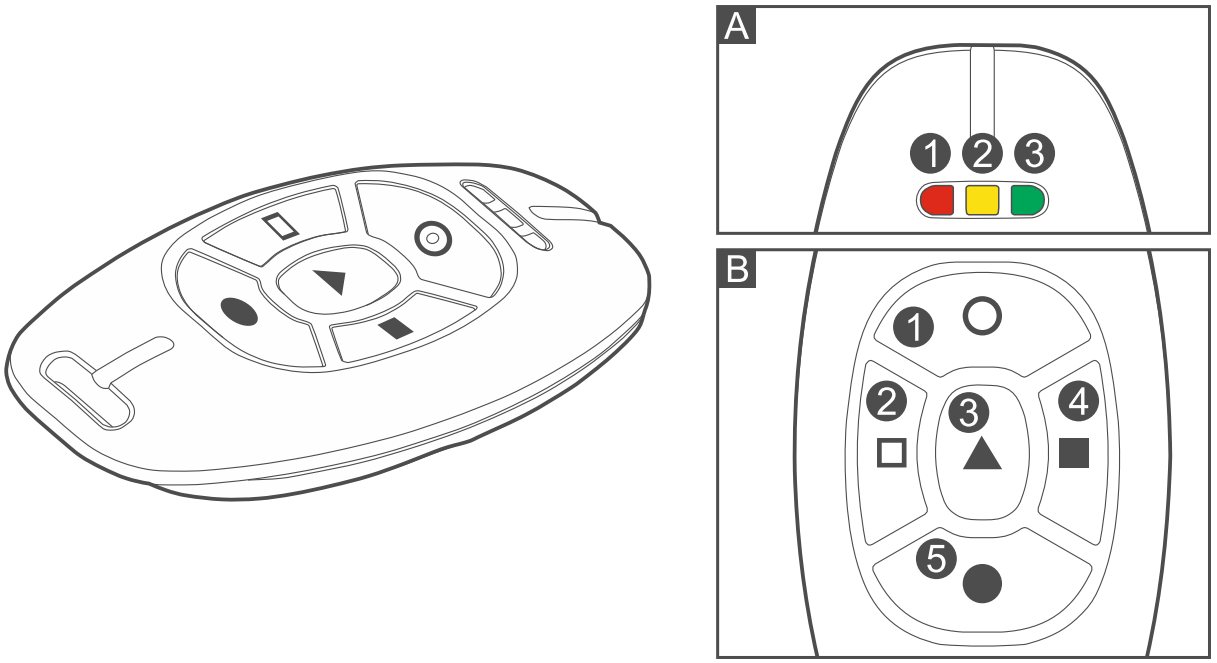


Fig. 6. APT-200 [light gray enclosure] / APT-100 [dark gray enclosure] keyfob. A – numeration of LEDs. B – numeration of keyfob buttons.

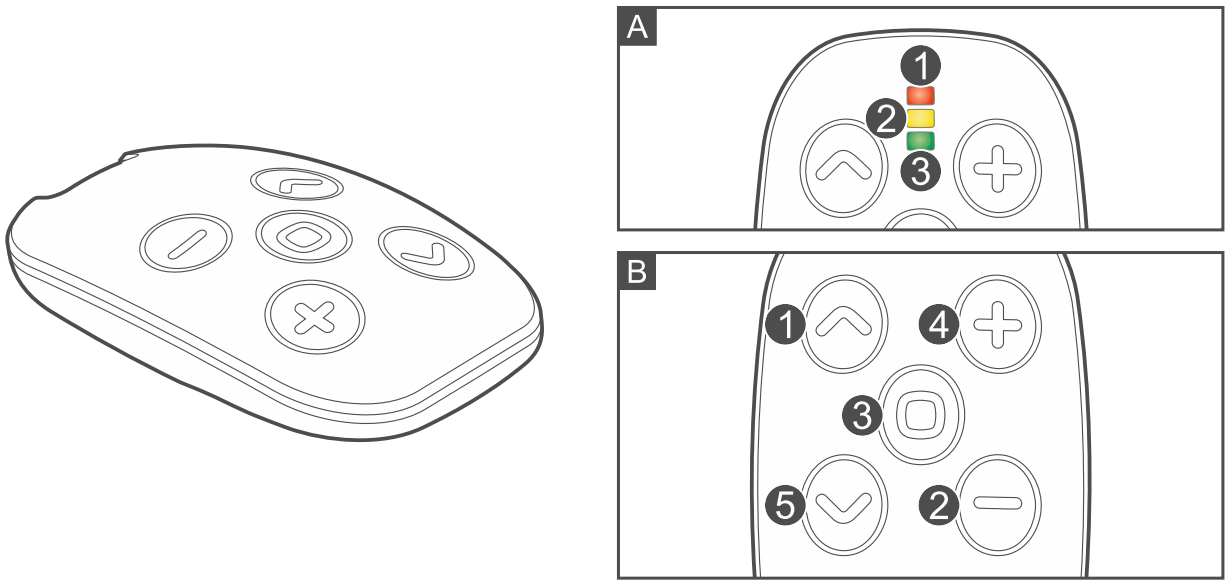


Fig. 7. APT-210 keyfob. A – numeration of LEDs. B – numeration of keyfob buttons.

The users can control the alarm system using a keyfob in case of:

- INTEGRA 128-WRL control panel (ABAX).

- any control panel to which connected is:
  - ABAX 2 (ACU-220 / ACU-280) / ABAX (ACU-120 / ACU-270 / ACU-100 (firmware version 2.00 or newer) / ACU-250) controller,
  - INT-RX-S / INT-RX module.

The user can have 2 keyfobs:

- bidirectional keyfob: APT-200 / APT-210 (supported by the ABAX 2 and ABAX system) or APT-100 (supported by the ABAX system).
- 433 MHz keyfob (supported by the INT RX and INT-RX-S modules).

The keyfob can start up to 6 functions. Consult the person who has configured the keyfob settings to find out:

- what functions are run by keyfob buttons / button combinations,
- what is shown by the keyfob LEDs (APT-200 / APT-210 / APT-100 keyfobs).

See also “Adding keyfob” s. 32.

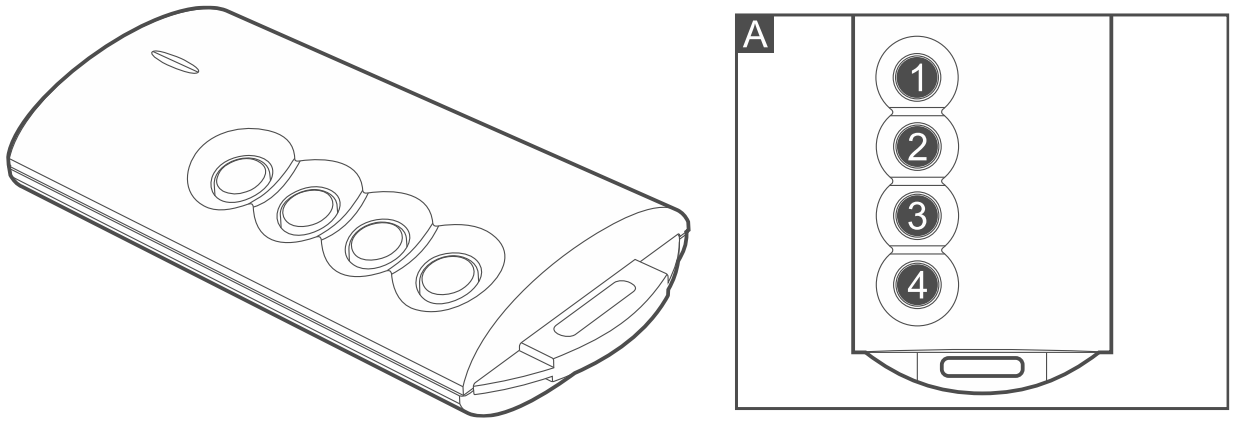


Fig. 8. T-4 keyfob (433 MHz keyfob). A – numeration of keyfob buttons.

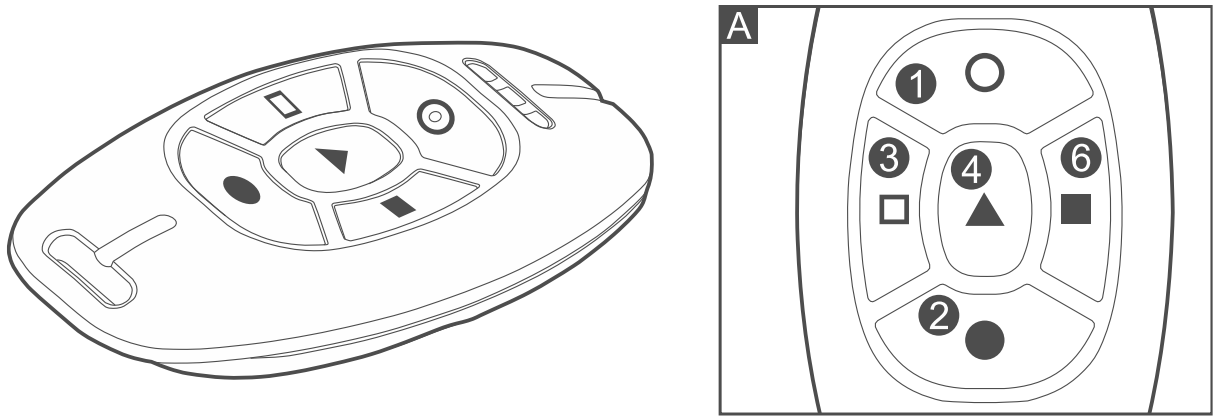


Fig. 9. MPT-300 [black enclosure] / MPT-350 [light gray enclosure] keyfob (433 MHz keyfob). A – numeration of keyfob buttons. The button designated with digit 6 corresponds to the combination of buttons 1 and 3 in other 433 MHz keyfobs.

13. Manual update history

Date	Firmware version	Introduced changes
2013-08	1.12	• Information on INT-TSG keypad has been added (p. 6).

		• Note about the user having SIMPLE USER right has been added (p. 11). • List of user functions has been supplemented (p. 12). • Description of CHANGE TELEPHONE CODE user function has been added (p. 20). • Description of SIMPLE USER right has been added (p. 29). • Description of ADMINISTRATOR right has been added (p. 29). • Information on maximum duration of zone testing has been modified (p. 39). • Section “Audio alarm verification” has been added (p. 51).
2013-12	1.12	• Information on the INT-KLFR (p. 5, 6 and 10) and INT-TSI (p. 6) keypads has been added. • Description of IP/MAC ETHM-1 user function has been modified (p. 23).
2014-10	1.13	• Information on the ETHM-1 Plus module has been added. • List of user functions has been supplemented (p. 12). • Note on the possibility to disable user menu shortcuts by the installer has been added (p. 17). • Information on new functionality of the key 0 when editing the multiple-selection list in text mode has been added (p. 18, 25, 34 and 35). • Description of GPRS MONIT.TEST user function has been added (p. 23).
2015-10	1.14	• Notes have been added to the effect that the installer should provide information on how to operate the alarm system (p. 4). • Section on technical reliability of the alarm system has been modified (p. 4). • Information on INT-TSH keypad has been added (p. 6). • Information on single zone testing ability has been added (p. 15 and p. 39). • Description of KEYPAD CHIME function has been modified (p. 21). • Description of IP/MAC ETHM-1 function has been updated (p. 23). • Information on automatic synchronization of control panel clock with time server after control panel restart has been added (p. 27). • Information on shortening the exit delay time from the keypad has been supplemented (p. 27). • Section on zone bypassing has been modified (p. 34).
2018-06	1.18	• List of user functions has been supplemented (p. 12). • List of user functions that can be run using shortcuts has been supplemented (p. 17). • Description of DLOADX IP function has been updated (p. 21). • Description of GUARDX IP function has been updated (p. 22). • Name of IP/MAC ETHM-1 function has been changed to IP/MAC/IMEI/ID and function description has been modified (p. 23). • Description of functions available in DOWNLOADING submenu has been modified (p. 24). • Description of INT-GSM →DLOADX function has been added (p. 25). • Description of INT-GSM →GUARDX function has been added (p. 25). • Section “SMS control” has been modified (p. 51).
2018-10	1.18	• Information on REPLACE BATTERY function has been added (p. 15, 21 and 36).
2019-05	1.19	• Information about wireless keypads has been added. • Information about ABAX 2 system devices has been added. • Description of functions started by long press of a numeric key on the keypad has been modified (p. 10). • Description of TEMPERATURES function has been modified (p. 22). • Section “Operating the alarm system using keyfob” has been modified (p. 52).
2021-08	1.20	• Information on the INT-GSM LTE module has been added. • Information on the INT-TSG2 and INT-TSH2 keypads has been added.
2022-11	1.21	• List of user functions has been supplemented (p. 12).

		• Description of TEMPERATURES has been added, a new function available in the CHANGE OPTIONS submenu (p. 21). • Section “Programming the thermostatic output settings” has been added (p. 37).
2026-08	1.25	• Information on the INT-TSG2R, INT-TSH2R, INT-TSH210 and INT-KSG2R keypads has been added. • Information on the CR-MF5 and SO-MF5 keypads has been added. • Information on the INTEGRA Soft program has been added. • Note on the availability of some functions has been added (p. 4). • Section “Keypads description” has been updated (p. 7). • List of user functions has been updated (p. 12). • Section “Arming” has been modified (p. 25). • Section “Disarming and alarm clearing” has been modified (p. 27). • Section “Adding keyfob” has been modified (p. 32). • Note on the APT-200 / APT-210 keyfob registered in another system has been added (p. 32). • Section “Editing keyfob settings” has been added (p. 33). • Section “Zone bypassing” has been modified (p. 34). • Section “Programming the thermostatic output settings” has been updated (p. 37). • Section “Outputs control” has been updated (p. 40). • Section “Using the partition keypad” has been updated (p. 41). • Section “Using the entry keypad” has been updated (p. 45). • Section “Using the code lock” has been updated (p. 47). • Section “Operating the alarm system using keyfob” has been updated (p. 52).

14. Brief description of operating the system from keypad

flashing – trouble or trouble memory / Grade 2: trouble or trouble memory, bypassed zones or alarm

ON – all partitions operated by the keypad are armed
flashing – some partitions are armed

ON or **flashing** – alarm or alarm memory

[CODE]# – arming / disarming / alarm clearing

Quick arming:
0# - full arming
1# - full arming + bypasses
2# - arming without interior
3# - arming without interior and without entry delay

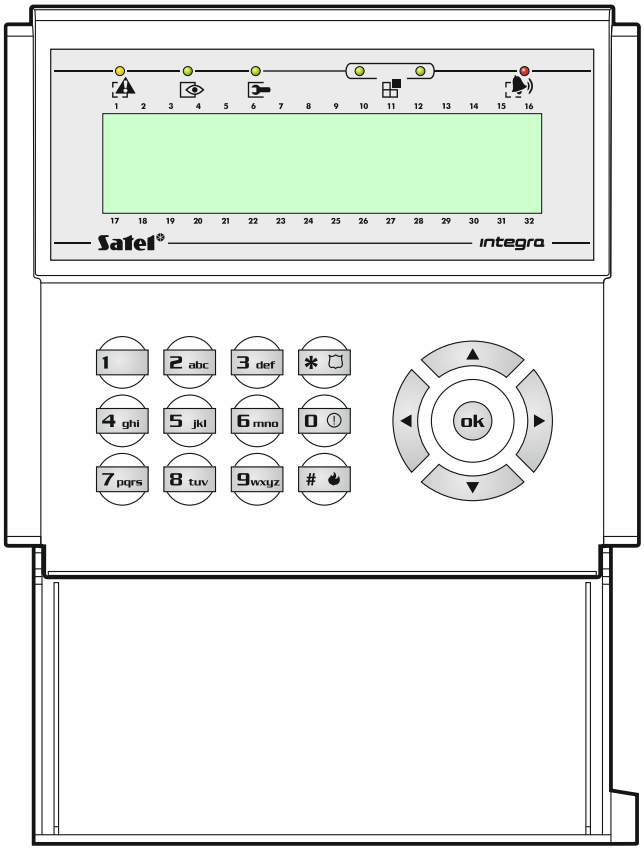
9# – end of exit delay countdown

8# – quick control of outputs

[CODE]✻ – enter the user menu
User menu shortcuts:
1 Change own code
2 Users [Masters]
21 New user [New master]
22 Edit user [Edit master]
23 Remove user [Remove master]
4 Zone bypasses
41 Inhibit
42 Isolate
5 Events
51 Selected events
52 All events
6 Set time
7 System state
8 Outputs control
9 Service mode
0 Downloading
01 Start DWNL-RS
02 Finish DWNL-RS
03 Start DWNL-MOD.
04 Start DWNL-TEL
05 Start DWNL-CSD [INTEGRA 128-WRL]
06 Start DWNL-GPRS [INTEGRA 128-WRL]
07 ETHM-1 →DLOADX
08 ETHM-1 →GUARDX
09 INT-GSM →DLOADX
00 INT-GSM →GUARDX

○ ○ – 1. group (numbers: 1-32 / addresses 00-1F)
○ ● – 2. group (numbers: 33-64 / addresses 20-3F)
● ○ – 3. group (numbers: 65-96)
● ● – 4. group (numbers: 97-128)
(○ – LED OFF; ● – LED ON

flashing – service mode started



Shortcut keys (press for approx. 3 seconds):
1 – check zone status
4 – check partition status
5 – view alarms in event log
6 – view troubles in event log
7 – view troubles
8 – CHIME signal ON/OFF
9 – toggle display between standby mode and partition status mode
(!) – trigger medical (aux) alarm
– trigger fire alarm
– trigger panic alarm