perfecta

Alarm control panel

PERFECTA 64 M

EN

Firmware version 2.04

CE

USER MANUAL

perfecta_64_M_u_en 06/25

Satel®

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

IMPORTANT

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

To ensure adequate protection, the alarm security system must be in good working order, therefore SATEL recommends that it be regularly tested.

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

Hereby, SATEL sp. z o.o. declares that the radio equipment type PERFECTA 64 M is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.satel.pl/ce

Factory default codes:
Service code: 12345
User 62 code: 1111

Signs in this manual

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

 Note – suggestion or additional information.

CONTENTS

1. Introduction

Thank you for choosing this product by SATEL. Read this manual before you start using the alarm system.

It is recommended that the installer prepare and deliver to the users a customized alarm system user manual. The manual must include all changes and modifications 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 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 in the keypad by an indicator. **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, control panel cellular communicator, 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. Realization of these features 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. Glossary

Alarm – warning that an intruder or other hazard (e.g. glass pane break, gas detection, etc.) has been detected in the protected area by the detectors. The alarm can be signaled in keypads or by sirens (during a defined time or until cleared). Additionally, information on the alarm can be sent to the monitoring station or the user.

Alarm zone – the zone whose violation can result in the alarm being triggered. The alarm zones can be either **instant** (violation will trigger the alarm at once) or **delayed** (violation will only trigger the alarm after a defined period of time has elapsed, e.g. the entry delay).

Armed mode – the status of alarm system in which zone violation will trigger the alarm.

Code – a sequence of digits used for user authentication. It allows the user to operate the alarm system by using keypad.

Day armed mode – the status in which only some zones in the partition are armed, as selected by the installer. The indicated zones will be armed during the day, when the user(s) stay in the protected area, but there is no risk of the zones being violated by the user(s). If no such zones are indicated by the installer, this arming mode is unavailable.

Detector – the basic component of alarm system, which analyzes the environment and, if a situation recognized as a threat occurs, transmits appropriate information to the control panel (e.g. motion detectors on detecting motion, magnetic contacts on opening the door/window, glass-break detectors on breaking glass pane, gas detectors on sensing gas, etc.).

Entry delay – time counted from entering into the protected area, which makes it possible to disarm the partition before the alarm is triggered.

Entry route – the route which the user must have to follow after entry into the protected area before being able to disarm the system. It is usually the same as the exit route.

Exit delay – time counted from starting the arming procedure in the partition, which makes it possible to leave the protected area before the alarm is triggered.

Exit route – the route which the user must have to take after arming before he leaves the protected area. It is usually the same as the entry route.

Fire alarm – alarm triggered by fire detectors, or from the keypad, in the event of fire.

Full armed mode – the status in which all zones belonging to the partition are armed.

Installer – the person who has installed and configured the alarm system.

Medical (auxiliary) alarm – alarm triggered by means of a button, or from the keypad, if it is necessary to call the medical assistance.

Night armed mode – the status in which only some zones in the partition are armed, as selected by the installer. The indicated zones will be armed at night, when the user(s) stay in the protected area, but there is no risk of the zones being violated by the user(s). If no such zones are indicated by the installer, this arming mode is unavailable.

Panic alarm – alarm triggered by means of the panic button, or from the keypad, in case of a hold-up.

Partition – a part of the protected area, composed of a number of zones. The division into partitions makes it possible to limit the access to part of the premises to some selected users, and to arm/disarm the system only in part of the protected area.

Protected area – the area supervised by detectors being part of the alarm system.

Proximity card – a passive transponder that can be used for user authentication if a device that has a proximity card reader is installed in the alarm system. The transponder can be a card, a tag, etc.

Reporting – reporting events that occurred in the alarm system to the monitoring station. The information about occurrence of an event can be transmitted via cellular network or

Ethernet. The companies offering the alarm system monitoring service undertake to intervene if specific events occur (e.g. alarms, troubles, etc.).

Service code – a code that allows access to the service mode, as well as some functions in the user menu.

Service technician – the person whose function is to control operability of the installed alarm system and its components, as well as to eliminate possible problems. These duties can be fulfilled by the installer or a person assigned by him.

Siren/beacon – a device providing information about alarms or other events in the alarm system by means of acoustic or optical signaling.

Tamper alarm – reaction of the alarm system to opening the housing of a device which is part of the alarm system, tearing off the device from the wall, cutting through the alarm system cables, etc. Actions taken by the alarm system may be similar as in the event of alarm, however, if the tamper alarm occurs, it is advisable to call in the installer so that he can make a checkup.

User – a person which can operate the alarm system, using a code or remote control keyfob.

Warning alarm – in some situations, when the alarm criteria are met, the alarm system does not take up immediately all the actions provided for in the event of alarm. These actions are postponed, reaction of the system being limited to signaling warning alarm in keypads or on indoor sirens/beacons. Thus, the user who has made a mistake entering the protected area (without disarming the system first), has some extra time to disarm the system. Contact your installer to obtain detailed information on the situations when the alarm will be preceded by warning alarm.

Zone – **1.** a separated portion of the protected area that can supervised by a detector. A single zone can be a corridor, window or door. **2.** the terminals on control panel/expander electronics board to which you can connect a detector or another device whose state is to be supervised (panic button, siren tamper contact, power supply output indicating loss of 230 VAC supply, etc.).

Zone bypassing (inhibiting / isolating) – procedure preventing the alarm from being triggered by the selected zone when it is in the armed mode. Violations of the zone will be ignored by the control panel.

Zone violation – a change of the zone status to another, different from that defined for the normal state (e.g. as a result of motion being sensed by the motion detector, gas being sensed by the gas detector, etc.).

5. EN 50131 standard for Grade 2 consequences

If the installer has configured the control panel in compliance with the EN 50131 standard requirements for Grade 2:

1. The user codes should be composed of at least 5 characters.
2. The amount of information provided in the keypads by means of the indicators, display and sound signaling is limited.
3. The quick arming from keypad (without entering the code) is not available.
4. Arming may be impossible, if one of the situations provided for in the standard occurs (zone violation, trouble).

How requirements of the standard affect the use of the control panel is described in detail hereunder.

6. Keypads

SATEL offers the following keypads for the PERFECTA 64 M alarm control panel:

PRF-LCD – hardwired keypad with mechanical keys,

INT-KSG2R – hardwired keypad with touch keys,

INT-TSG2 – hardwired touchscreen keypad,

INT-TSG2R – hardwired touchscreen keypad,

INT-TSH2 – hardwired touchscreen keypad,

INT-TSH2R – hardwired touchscreen keypad,

INT-TSH210 – hardwired touchscreen keypad,

PRF-LCD-A2 – wireless keypad with mechanical keys and built-in proximity card reader (ACU-220 / ACU-280 module must be connected),

PRF-LCD-WRL – wireless keypad with mechanical keys (PERFECTA-RF module must be connected).

The alarm system should include at least one keypad.

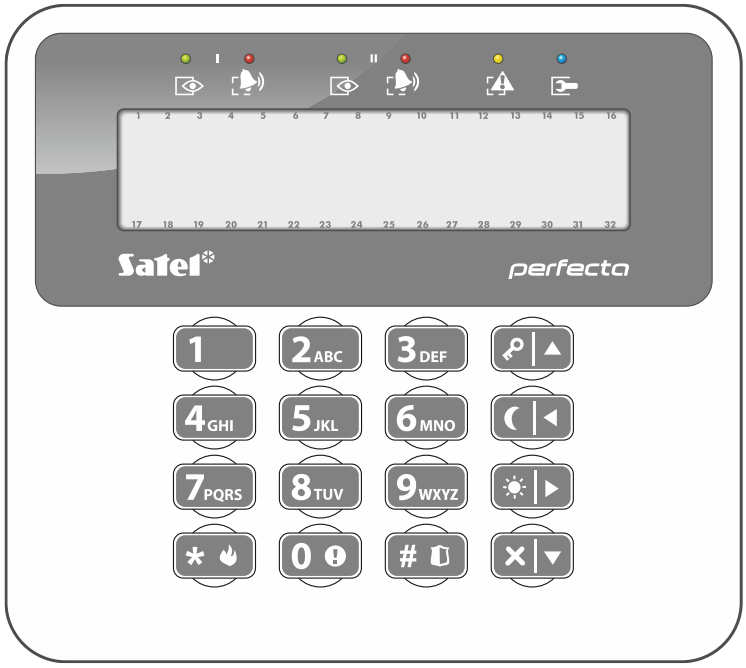


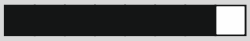
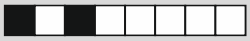
Fig. 1. PRF-LCD / PRF-LCD-WRL keypad.

The following manual includes instructions on how to use the wired PRF-LCD keypad and the wireless PRD-LCD-WRL / PRF-LCD-A2 keypad. For instruction on how to use the INT-KSG2R, INT-TSG2, INT-TSG2R, INT-TSH2, INT-TSH2R and INT-TSH210 keypads, please refer to the manuals provided with 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 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. [*].

6.1 Keypads description

6.1.1 LED indicators

LED	Color	Description
	green	two LEDs (marked I and II) – ask the installer which LED indicates the state of which partition **ON** – at least 1 partition is armed **flashing** – exit delay countdown in at least 1 partition
	red	two LEDs (marked I and II) – ask the installer which LED indicates the state of which partition **ON** or **flashing** – alarm or alarm memory in at least 1 partition The way of presenting the information is shown graphically below. The information is presented for 2 seconds and repeated (□ – LED is OFF; ■ – LED is ON). The higher position in the list means the higher priority of the presented status:  – fire alarm,  – burglary / panic alarm,  – warning alarm,  – tamper alarm,  – fire alarm memory,  – burglary / panic alarm memory,  – warning alarm memory,  – tamper alarm memory.
	yellow	**flashing** – trouble or trouble memory
	blue	**ON** – service mode is active and service menu is displayed **flashing** – service mode is active but service menu is hidden or displayed in another keypad

Information about the armed state can be hidden after a time period defined by the installer. After you enter the code and press the ✱ *key, the indicators operate as shown in the table.*

The trouble information is hidden after arming. The installer defines if the trouble information is hidden after just one of the partitions is armed in any mode or after all partitions are armed in full mode.

If the Grade 2 *option is enabled by installer:*

- *the*  *LEDs indicate alarms only after entering the code and pressing* ✱*,*
- *flashing of the*  *LED means that there is a trouble in the system, some zones are bypassed, or that there was an alarm.*

6.1.2 Display

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:

- normal mode,
- system preview mode.

The installer decides if the system preview mode is available.

The messages about events that occurred in the alarm system are displayed regardless of the operating mode.

Enter the code and press * to open the user menu (p. 16).

Normal mode

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

Press and hold 9 WXYZ for 3 seconds to switch the display to the system preview mode.

System preview mode

The installer defines the items to be displayed in the system preview mode. This can be:

- text,
- symbol that represents the partition state:
  F – fire alarm,
  A – alarm,
  W – warning alarm,
  T – tamper alarm,
  C – full arm,
  N – night arm,
  D – day arm,
  ? – entry delay,
  E – exit delay (less than 10 seconds),
  e – exit delay (more than 10 seconds),
  f – fire alarm memory,
  a – alarm memory,
  w – warning alarm memory,
  t – tamper alarm memory,
  · – not armed.
- symbol that represents the zone state:
  b – inhibited (not displayed when armed),
  I – isolated (not displayed when armed),
  ! – first alarm,
  F – fire alarm,
  A – alarm,
  T – tamper alarm,
  ▮ – tamper (Double EOL zone),
  ● – violated,
  f – fire alarm memory,
  a – alarm memory,
  t – tamper alarm memory,
  · – normal state.

- symbol that represents the output state:
  · – deactivated,
  ■ – activated.
- information on temperature from an ABAX 2 wireless device,
- date,
- time,
- keypad name,
- information on the power consumption of the appliance connected to the ASW-200 smart plug.

Press and hold 9 WXYZ for 3 seconds to switch the display to the normal mode.

Messages

The keypad displays the following messages (the higher position on the list, the higher the priority):

- alarm,
- countdown of entry delay,
- countdown of exit delay,
- alarm memory.

Messages about alarm and alarm memory will not be displayed, if the GRADE 2 option is enabled by the installer.

6.1.3 Keys

Functions of keys	
1 ... 0	press to enter digits (code, partition number, etc.)
7 PQRS	press and hold for 3 seconds to view the troubles
8 TUV	press and hold for 3 seconds to turn on/off the keypad CHIME
9 WXYZ	press and hold for 3 seconds to switch the display between the normal mode and the system preview mode
0	press and hold for 3 seconds to trigger the medical alarm
#	enter the code and press # to arm the system in full mode [if the system is disarmed and there is no alarm] or disarm the system and clear the alarm [if the system is armed and/or there is an alarm] press and hold for 3 seconds to trigger the panic alarm
*	enter the code and press * to enter the user menu press and hold for 3 seconds to trigger the fire alarm
	used for full arming (see: “Arming”)
	used for night arming (see: “Arming”)
	used for day arming (see: “Arming”)

[×|▼]	used to disarm the system and clear the alarm (see: “Disarming and alarm clearing”)

Availability of the functions depends on the keypad settings.

The functions of keys in the user menu are described in the “User menu” section (p. 16).

6.1.4 Sound signaling

The installer can disable the sound signaling.

Beeps generated when operating

1 short beep – pressing any number key.

3 short beeps – confirmation of:

- starting the arming procedure (there is exit delay in the partition) or arming (there is no exit delay in the partition),
- disarming and/or alarm clearing,
- selecting the partition which is to be armed or disarmed, or where alarm is to be cleared – in such a case the keypad is waiting for the code to be entered,
- turning output off,
- turning off the CHIME in the keypad, using the [8 TUV] key,
- switching over the display from the normal mode to the system preview mode, and vice versa, by means of the [9 WXYZ] key.

4 short beeps and 1 long beep – confirmation of:

- turning output on,
- turning on the CHIME in the keypad, using the [8 TUV] key.

2 long beeps – incorrect code or pressing the [*] key, if not preceded by entering code or selecting a partition.

3 long beeps – refusal to carry out a command (the user does not have the required authority level or the function is not available).

Beeps generated during programming

1 short beep – pressing any number key.

2 short beeps – entering the user menu, submenu or starting a function.

3 short beeps – exiting the service function on pressing the [#] key.

4 short beeps and 1 long beep – termination of the user function on pressing the [#] key, or quitting the service mode.

2 long beeps – exiting the function on pressing the [*] key, or an unavailable function.

Event signaling

Only installer selected events are signaled.

Duration of the alarm signaling is to be defined by the installer.

If the Grade 2 *option is enabled by installer, the keypad will not signal by sounds any troubles and alarms.*

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).

2 short beeps every seconds – countdown of entry delay.

2 short beeps every 3 seconds – trouble / trouble memory. The installer defines whether the signaling is to last until trouble restore, or until trouble review / trouble memory clearing. When one or both partitions are armed, trouble / trouble memory is not audibly indicated by the keypad.

Short beep every 0.5 seconds – warning alarm.

Continuous beep – alarm.

Long beep every second – fire alarm.

6.2 Codes

The code is used for user authentication. The user needs to enter the code to access the functions that enable operating the alarm system.

The installer may permit starting some of the functions without using the code.

Do not make your code available to other people.

Using an incorrect code three times may block the keypad for 90 seconds. As long as the keypad is blocked, entering the correct code is treated as entering an incorrect code ("Wrong code" message is displayed).

6.2.1 Factory default codes

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

user 62 code: 1111

service code: 12345

The factory default codes should be changed before you start using your alarm system (see: "Changing code").

6.3 Proximity cards

The PRF-LCD-A2 keypad has a built-in proximity card reader. Using the proximity card, the user can:

- arm the system,
- disarm the system and/or clear alarm,
- control devices connected to the alarm system outputs.

*When the PRF-LCD-A2 keypad is powered by the battery, the reader works only if the keypad is woken up (when the keypad is in the sleep mode, press e.g. * to wake it up).*

6.4 Arming

Completion of the steps below will start the arming procedure. The procedure ends when the exit delay countdown is over (if the procedure is completed successfully, the system becomes armed – see also "Failure of arming procedure"). If the exit delay time is 0, the system becomes armed instantly.

The day/night arming modes are available if the installer has defined which zones are to be active in this armed mode.

During the exit delay countdown, you can leave the partition through an exit route mapped out by the installer without triggering alarm.

6.4.1 Arming with code

Arming without partition selection

Enter the code, and then press:

[*|▲] - to arm the system in full mode,

[☀|▶] - to arm the system in day mode,

[☾|◀] - to arm the system in night mode.

In the partitions you have access to, the arming procedure will begin.

Arming the selected partition

1. Select the partition which is to be armed (press one of the keys: [1] - partition 1; [2 ABC] - partition 2; [3 DEF] - partition 3; [4 GHI] - partition 4).
2. Select the arming mode (press one of the keys: [*|▲] - full arming; [☀|▶] - day arming; [☾|◀] - night arming). Backlight of the keys will start flashing, which indicates that the code must be entered.
3. Enter the code.
4. Press [# ◧] or press again the key corresponding to the selected arming mode. In the selected partition, the arming procedure will begin.

When the quick arming is available, the steps 3 and 4 are skipped.

6.4.2 Arming with proximity card

Decide with the installer which of the following arming methods to use:

- card read (bring the card close to the keys and move it away),
- card hold-down (bring the card close to the keys and hold for about 3 seconds).

All partitions to which you have access will be armed in full mode.

If you arm and disarm the system by bringing the card close to the keypad, disarming has the priority. This means that if some of the partitions are armed and some are not, when you bring the card close to the keypad, the partitions will be disarmed.

6.4.3 Quick arming

The installer may permit arming without using the code / proximity card.

1. Indicate the partition(s) to be armed (press one of the keys: [1] - partition 1; [2 ABC] - partition 2; [3 DEF] - partition 3; [4 GHI] - partition 4; [0 ⓿] - all partitions).
2. Select the arming mode (press one of the keys: [*|▲] - full arming; [☀|▶] - day arming; [☾|◀] - night arming). In the partition(s), the arming procedure will begin.

6.4.4 Arming without delay

If there is nobody in the partition or nobody is leaving the partition which is to be set to the day / night armed mode, you can arm the partition without exit delay (there will be no exit delay signaling). When arming the system, press and hold for 3 seconds one of the keys used to select the arming mode: [*|▲], [☀|▶] or [☾|◀] (when arming with code, do it after you enter the code). The exit delay countdown will not run.

6.4.5 Terminating the exit delay countdown

When the exit delay countdown is running, you can terminate it, thus shortening the exit delay time. Press and hold [🔑|▲], [☀|▶] or [☾|◀] for about 3 seconds (it is of no consequence which key you will press).

6.4.6 Service mode and arming

If you try to arm the system when the service mode is active, you will be informed about it by a message displayed on the keypad. Press [1] if you want to arm the system.

6.4.7 System problems and arming failure

The installer may configure the system so that it is tested for any problems by the control panel during arming. The possible problems that prevent arming are given below:

- at least one zone that must not be violated during arming (the *Priority* option has been enabled for the zone by the installer) is violated in the partition,
- at least one alarm zone is violated beyond the exit route in the partition,
- a zone is bypassed in the partition,
- there is tamper in the partition,
- there is trouble in the system.

The check can be performed twice:

- before starting the arming procedure,
- after the exit delay countdown expires.

System not ready and forced arming

If you are trying to arm a partition, but the arming procedure fails to start and the "System not ready" message is displayed instead, there are some problems in the system that prevent it from being armed.

When the **"System not ready 1=Arm 2=Check"** message is displayed, you can:

- press [*🔥] to cancel the arming,
- press [1] to force the arming,
- press [2ABC] to check what has prevented the arming procedure from starting.

When the **"System not ready 2= Check"** message is displayed, you can:

- press [*🔥] to cancel the arming,
- press [2ABC] to check what has prevented the arming procedure from starting.

If forced arming is not available, you will be able to arm the system only after the causes that made starting of the arming procedure impossible are eliminated.

List of problems

If, after pressing [2ABC], it turns out there are several causes that prevent arming, you can scroll the list using the [✕|▼] or [🔑|▲] keys.

If you want to bypass a violated zone or unbypass a bypassed zone, press [4GHI] (you need to have the *Zone inhibition* right). A prompt will appear asking you whether to execute the function. Press [1] to confirm or [*🔥] to deny.

Having reviewed the list of problems, press [*🔥] to go back to the "System not ready" message.

Failure of arming procedure

If the system is not armed after the exit delay countdown is over, it means that the control panel detected a problem that was not there when the exit delay countdown started. The installer may configure the control panel this way, e.g. to meet the EN 50131 standard for Grade 2.

Ask the installer how you will be informed of the arming failure.

6.5 Disarming and alarm clearing

If you disarm a partition in which there is an alarm, the alarm will be cleared.

Alarm clearing results in canceling the voice messaging about alarm (unless the control panel has already managed to notify the users about the alarm).

6.5.1 Disarming and clearing alarm with code

Disarming and alarm clearing without partition selection

Enter the code and then press [✕|▼]. Disarming / alarm clearing will take place in the partitions to which you have access.

Disarming and alarm clearing in selected partition

1. Select the partition which is to be disarmed and/or where alarm is to be cleared (press one of the keys: [1] - partition 1; [2 ABC] - partition 2; [3 DEF] - partition 3; [4 GHI] - partition 4).
2. Press [✕|▼]. Backlight of the keys will start flashing, which indicates that the code must be entered.
3. Enter the code.
4. Press [✕|▼] or [# ◧]. Selected partition will be disarmed / alarm will be cleared.

6.5.2 Disarming and clearing alarm with proximity card

Bring the card close to the keys and move it away. All partitions to which you have access will be disarmed / alarm will be cleared in them.

6.5.3 Alarm clearing without disarming

If the partition is armed and you want to clear the alarm without disarming the partition, enter the code and then press [🔧|▲], [☀|▶] or [☾|◀] (it is of no consequence which key you will press). In the partitions you have access to, the alarm will be cleared.

You cannot clear the warning alarm without disarming the system first.

6.6 Triggering the alarm from keypad

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

fire alarm – press and hold [* 🔥] for about 3 seconds,

medical (auxiliary) alarm – press and hold [0 🚨] for about 3 seconds,

panic alarm – press and hold [# ◧] for about 3 seconds. The installer defines whether the loud panic alarm (indicated by the keypads) or the silent panic alarm (not indicated by the keypads) will be triggered.

6.7 Turning the CHIME on /off

The CHIME is five short sounds by means of which the keypad will inform you e.g. that a door / window is open. The installer defines which zones of the alarm system can trigger the CHIME and whether it can be turned on/off by the users.

Press and hold 8 TUV for about 3 seconds to turn on or off the CHIME signaling.

6.8 User menu

Enter the code and press * to get access to the user menu. The functions you can run will be displayed. The list of available functions depends on your rights, as well as on the state and configuration of the system.

In order to quit the function and/or user menu, press *. The keypad will quit the menu automatically, if 2 minutes have elapsed since the last keypress.

Functions of keys in the user menu	
1 ... 0	enter digits, letters and other characters enable / disable an option check / uncheck an item
#	start a function save changes and quit the function
*	exit the user menu quit the function (usually without saving changes)
▲	scroll up the list move the cursor left clear the character to the left of the cursor (edit numbers and names) exit the graphic mode (see: “Graphic mode”)
◄	exit the submenu move the cursor left enter the graphic mode (see: “Graphic mode”)
►	enter the submenu start a function move the cursor right enter the graphic mode (see: “Graphic mode”)
▼	scroll down the list change the letter case (edit names) exit the graphic mode (see: “Graphic mode”)

6.8.1 Navigating through the menu and running functions

To navigate throughout the menu, you can use the arrow keys or number shortcuts. You can also combine the two methods. The cursor → shows the submenu you can enter / function you can run.

Using the arrow keys

1. Use the ▼ or ▲ key to find the required submenu or function.

2. Press [☀|▶] or [# ◧] to open a submenu (use the [☾|◀] key to exit the submenu) or run a function.

Using the number shortcuts

Most submenus and functions are designated by numbers. To find these numbers, refer to section “User functions list”. Using the number keys, enter the number of submenu / function to enter the submenu / run the function. You can enter at once several digits (corresponding to successive numbers of submenus and functions) to quickly run the selected function.

For example, to start the zone inhibiting function, enter the user menu and then press [4 GHI] [1], where:

[4 GHI] - entering the 4.ZONE BYPASSES submenu,

[1] - running the 1.INHIBIT function.

i *Remember that the sequence of digits which starts a function e.g. from the main menu level will not start the same function from the submenu level.*

6.8.2 Data editing

The editing method depends on the type of data. Having completed the editing, press [# ◧] to save the changes. If you want to exit the function without saving the changes, press [* 🔥].

Selection from the single-choice list

In the lower line of the display, the currently selected item is presented. You can scroll the list using the [✕|▼] and [🔑|▲] keys.

Selection from the multiple-choice list

In the lower line of the display, one of the items you can choose from is presented. You can scroll the list using the [✕|▼] and [🔑|▲] keys. The following symbol is situated in the upper right corner of the display:

▣ – displayed item is selected / option is enabled,

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

Press any number key to change the currently shown symbol for another one.

Press [☀|▶] or [☾|◀] to enter the graphic mode.

Graphic mode

In the graphic mode you can see on the display the state of up to 32 items simultaneously. These can be zones, outputs, options, etc. The state is represented by the same symbols as in the basic mode. No symbol means that this item is unavailable and cannot be edited. The numbers around the display will help you identify the item. For items 33-64, the cursor is the flashing ■ symbol. This makes it easier to recognize which items are displayed.

Use the [☀|▶] or [☾|◀] key to move the cursor. When the cursor is over the item you want to edit, press any number key. A different symbol will be displayed.

In the graphic mode you can quickly change the status of all available items:

- if you press [0] 3 times within 3 seconds, the · symbol will be displayed for all items,
- if you press [1] 3 times within 3 seconds, the ▣ symbol will be displayed for all items,
- if you press [2 ABC] 3 times within 3 seconds, you will switch all the items to the opposite state (all the · symbols will switch to ▣, and the ▣ symbols will switch to ·).

If you press [☀|▶] when the cursor is on the last available item, the state of the next 32 items will be displayed. If you press [☾|◀] when the cursor is on the first available item, the state of the previous 32 items will be displayed.

Press [✕|▼] or [🔧|▲] to exit the graphic mode and return to the basic mode.

Entering decimal values

To enter digits, use the number keys. Use the [☀|▶] and [☾|◀] keys to move the cursor. In some functions, the [🔧|▲] key deletes the character on the left side of the cursor.

Entering hexadecimal values

To enter digits, use the number keys. To enter the A, B and C characters, use the [2 ABC] key, and to enter D, E and F, use the [3 DEF] key (keep pressing the key until the required character appears). Use the [☀|▶] and [☾|◀] keys to move the cursor. The [🔧|▲] key deletes the character on the left side of the cursor.

Entering names

The characters that can be entered by using the keys are presented in Table 1. Keep pressing the key until the required character appears. Long press the key to display the digit assigned to it.

Shown on the right 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).

Use the [☀|▶] and [☾|◀] keys to move the cursor. The [🔧|▲] key deletes the character on the left side of the cursor.

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

Table 1. Characters available when entering names. The upper case letters are available under the same keys (to change the letter case, press [✕|▼]).

6.8.3 User functions list

Presented below are all items of the user menu. The menu displayed on the keypad contains only the items to which you have access, because of the rights granted to you or status of the system.

Shown in square brackets are key sequences that enable calling the given submenu or starting the given function from the main menu level.

1.Change code *change own code*

2.Users

[21] 1.New user *add new user*

[211] 1.Code *enter code*

[212] 2.Schedule *select user schedule*
[213] 3.Partitions *select supported partitions*
[214] 4.Add key fob *add keyfob*
[215] 5.Remov.key fob *remove keyfob*
Button ○/↑ *select function to run with button ○ / ↑*
Button □/- *select function to run with button □ / -*
Button ▲/□ *select function to run with button ▲ / □*
Button ■/+ *select function to run with button ■ / +*
Button ●/↓ *select function to run with button ● / ↓*
Button ○+●/↑↓ *select function to run with buttons ○+● / ↑+↓*
LED 1 *select operating mode of red LED [APT-200/APT-210]*
LED 2 *select operating mode of yellow LED [APT-200/APT-210]*
LED 3 *select operating mode of green LED [APT-200/APT-210]*
Key fob event *do you want to write keyfob use to event log*
[216] 6.Add card *add proximity card*
[2161] 1.Enter number *enter card number manually*
[2162] 2.Select reader *read card number using reader*
[217] 7.Delete card *remove proximity card*
[218] 8.Name *enter the user name*
[22] 2.Edit user *edit a user*
[selecting user]
1.Code *edit code*
2.Schedule *change user schedule*
3.Partitions *select supported partitions*
4.Add key fob *add keyfob*
5.Remov.key fob *remove keyfob*
Button ○/↑ *select function to run with button ○ / ↑*
Button □/- *select function to run with button □ / -*
Button ▲/□ *select function to run with button ▲ / □*
Button ■/+ *select function to run with button ■ / +*
Button ●/↓ *select function to run with button ● / ↓*
Button ○+●/↑↓ *select function to run with buttons ○+● / ↑+↓*
LED 1 *select operating mode of red LED [APT-200/APT-210]*
LED 2 *select operating mode of yellow LED [APT-200/APT-210]*
LED 3 *select operating mode of green LED [APT-200/APT-210]*
Key fob event *do you want to write keyfob use to event log*
6.Add card *add proximity card*
1.Enter number *enter card number manually*
2.Select reader *read card number using reader*
7.Delete card *remove proximity card*

- 8.Name — *edit user name*
- [23] 3.Remove user — *remove a user*

3.Outputs reset — *deactivate outputs / activate* 21. Detectors reset *output*

4.Zone bypasses

- [41] 1.Inhibit — *inhibit zones*
- [42] 2.Isolate — *isolate zones*

5.Event log — *view events*

6.Settings

- [61] 1.Set time — *set the clock*
- [62] 2.Timers — *program timer settings*
  - [621] 1.Settings — *set start / stop time of timers*
    - [6211] 1.Monday — *set start / stop time for Monday*
      - [62111] 1.Timer 1 — *start / stop time of timer 1 on Monday*
      - [62112] 2.Timer 2 — *start / stop time of timer 2 on Monday*
      - [62113] 3.Timer 3 — *start / stop time of timer 3 on Monday*
      - [62114] 4.Timer 4 — *start / stop time of timer 4 on Monday*
      - [62115] 5.Timer 5 — *start / stop time of timer 5 on Monday*
      - [62116] 6.Timer 6 — *start / stop time of timer 6 on Monday*
      - [62117] 7.Timer 7 — *start / stop time of timer 7 on Monday*
      - [62118] 8.Timer 8 — *start / stop time of timer 8 on Monday*
    - [6212] 2.Tuesday — *set start / stop time for Tuesday*
      - [62121] 1.Timer 1 — *start / stop time of timer 1 on Tuesday*
      - [62122] 2.Timer 2 — *start / stop time of timer 2 on Tuesday*
      - [62123] 3.Timer 3 — *start / stop time of timer 3 on Tuesday*
      - [62124] 4.Timer 4 — *start / stop time of timer 4 on Tuesday*
      - [62125] 5.Timer 5 — *start / stop time of timer 5 on Tuesday*
      - [62126] 6.Timer 6 — *start / stop time of timer 6 on Tuesday*
      - [62127] 7.Timer 7 — *start / stop time of timer 7 on Tuesday*
      - [62128] 8.Timer 8 — *start / stop time of timer 8 on Tuesday*
    - [6213] 3.Wednesday — *set start / stop time for Wednesday*
      - [62131] 1.Timer 1 — *start / stop time of timer 1 on Wednesday*
      - [62132] 2.Timer 2 — *start / stop time of timer 2 on Wednesday*
      - [62133] 3.Timer 3 — *start / stop time of timer 3 on Wednesday*
      - [62134] 4.Timer 4 — *start / stop time of timer 4 on Wednesday*
      - [62135] 5.Timer 5 — *start / stop time of timer 5 on Wednesday*
      - [62136] 6.Timer 6 — *start / stop time of timer 6 on Wednesday*
      - [62137] 7.Timer 7 — *start / stop time of timer 7 on Wednesday*
      - [62138] 8.Timer 8 — *start / stop time of timer 8 on Wednesday*
    - [6214] 4.Thursday — *set start / stop time for Thursday*
      - [62141] 1.Timer 1 — *start / stop time of timer 1 on Thursday*
      - [62142] 2.Timer 2 — *start / stop time of timer 2 on Thursday*
      - [62143] 3.Timer 3 — *start / stop time of timer 3 on Thursday*

[62144] 4.Timer 4 *start / stop time of timer 4 on Thursday*
[62145] 5.Timer 5 *start / stop time of timer 5 on Thursday*
[62146] 6.Timer 6 *start / stop time of timer 6 on Thursday*
[62147] 7.Timer 7 *start / stop time of timer 7 on Thursday*
[62148] 8.Timer 8 *start / stop time of timer 8 on Thursday*
[6215] 5.Friday *set start / stop time for Friday*
[62151] 1.Timer 1 *start / stop time of timer 1 on Friday*
[62152] 2.Timer 2 *start / stop time of timer 2 on Friday*
[62153] 3.Timer 3 *start / stop time of timer 3 on Friday*
[62154] 4.Timer 4 *start / stop time of timer 4 on Friday*
[62155] 5.Timer 5 *start / stop time of timer 5 on Friday*
[62156] 6.Timer 6 *start / stop time of timer 6 on Friday*
[62157] 7.Timer 7 *start / stop time of timer 7 on Friday*
[62158] 8.Timer 8 *start / stop time of timer 8 on Friday*
[6216] 6.Saturday *set start / stop time for Saturday*
[62161] 1.Timer 1 *start / stop time of timer 1 on Saturday*
[62162] 2.Timer 2 *start / stop time of timer 2 on Saturday*
[62163] 3.Timer 3 *start / stop time of timer 3 on Saturday*
[62164] 4.Timer 4 *start / stop time of timer 4 on Saturday*
[62165] 5.Timer 5 *start / stop time of timer 5 on Saturday*
[62166] 6.Timer 6 *start / stop time of timer 6 on Saturday*
[62167] 7.Timer 7 *start / stop time of timer 7 on Saturday*
[62168] 8.Timer 8 *start / stop time of timer 8 on Saturday*
[6217] 7.Sunday *set start / stop time for Sunday*
[62171] 1.Timer 1 *start / stop time of timer 1 on Sunday*
[62172] 2.Timer 2 *start / stop time of timer 2 on Sunday*
[62173] 3.Timer 3 *start / stop time of timer 3 on Sunday*
[62174] 4.Timer 4 *start / stop time of timer 4 on Sunday*
[62175] 5.Timer 5 *start / stop time of timer 5 on Sunday*
[62176] 6.Timer 6 *start / stop time of timer 6 on Sunday*
[62177] 7.Timer 7 *start / stop time of timer 7 on Sunday*
[62178] 8.Timer 8 *start / stop time of timer 8 on Sunday*
[6218] 8.Everyday *set everyday start / stop time*
[62181] 1.Timer 1 *start / stop time of timer 1 every day*
[62182] 2.Timer 2 *start / stop time of timer 2 every day*
[62183] 3.Timer 3 *start / stop time of timer 3 every day*
[62184] 4.Timer 4 *start / stop time of timer 4 every day*
[62185] 5.Timer 5 *start / stop time of timer 5 every day*
[62186] 6.Timer 6 *start / stop time of timer 6 every day*
[62187] 7.Timer 7 *start / stop time of timer 7 every day*
[62188] 8.Timer 8 *start / stop time of timer 8 every day*

[6219] 9.Exceptions *set start / stop time for exceptions*
[62191] 1.Except. 1 *set start / stop time for exception 1*
[621911] 1.Timer 1 *start / stop time of timer 1 for exception 1*
[621912] 2.Timer 2 *start / stop time of timer 2 for exception 1*
[621913] 3.Timer 3 *start / stop time of timer 3 for exception 1*
[621914] 4.Timer 4 *start / stop time of timer 4 for exception 1*
[621915] 5.Timer 5 *start / stop time of timer 5 for exception 1*
[621916] 6.Timer 6 *start / stop time of timer 6 for exception 1*
[621917] 7.Timer 7 *start / stop time of timer 7 for exception 1*
[621918] 8.Timer 8 *start / stop time of timer 8 for exception 1*
[62192] 2.Except. 2 *set start / stop time for exception 2*
[621921] 1.Timer 1 *start / stop time of timer 1 for exception 2*
[621922] 2.Timer 2 *start / stop time of timer 2 for exception 2*
[621923] 3.Timer 3 *start / stop time of timer 3 for exception 2*
[621924] 4.Timer 4 *start / stop time of timer 4 for exception 2*
[621925] 5.Timer 5 *start / stop time of timer 5 for exception 2*
[621926] 6.Timer 6 *start / stop time of timer 6 for exception 2*
[621927] 7.Timer 7 *start / stop time of timer 7 for exception 2*
[621928] 8.Timer 8 *start / stop time of timer 8 for exception 2*
[62193] 3.Except. 3 *set start / stop time for exception 3*
[621931] 1.Timer 1 *start / stop time of timer 1 for exception 3*
[621932] 2.Timer 2 *start / stop time of timer 2 for exception 3*
[621933] 3.Timer 3 *start / stop time of timer 3 for exception 3*
[621934] 4.Timer 4 *start / stop time of timer 4 for exception 3*
[621935] 5.Timer 5 *start / stop time of timer 5 for exception 3*
[621936] 6.Timer 6 *start / stop time of timer 6 for exception 3*
[621937] 7.Timer 7 *start / stop time of timer 7 for exception 3*
[621938] 8.Timer 8 *start / stop time of timer 8 for exception 3*
[62194] 4.Except. 4 *set start / stop time for exception 4*
[621941] 1.Timer 1 *start / stop time of timer 1 for exception 4*
[621942] 2.Timer 2 *start / stop time of timer 2 for exception 4*
[621943] 3.Timer 3 *start / stop time of timer 3 for exception 4*
[621944] 4.Timer 4 *start / stop time of timer 4 for exception 4*
[621945] 5.Timer 5 *start / stop time of timer 5 for exception 4*
[621946] 6.Timer 6 *start / stop time of timer 6 for exception 4*
[621947] 7.Timer 7 *start / stop time of timer 7 for exception 4*
[621948] 8.Timer 8 *start / stop time of timer 8 for exception 4*
[622] 2.From *set start date for exceptions*
[6221] 1.Except. 1 *set start date for exception 1*
[62211] 1.Timer 1 *start date of exception 1 for timer 1*
[62212] 2.Timer 2 *start date of exception 1 for timer 2*

[62213] 3.Timer 3 *start date of exception 1 for timer 3*
[62214] 4.Timer 4 *start date of exception 1 for timer 4*
[62215] 5.Timer 5 *start date of exception 1 for timer 5*
[62216] 6.Timer 6 *start date of exception 1 for timer 6*
[62217] 7.Timer 7 *start date of exception 1 for timer 7*
[62218] 8.Timer 8 *start date of exception 1 for timer 8*
[6222] 2.Except. 2 *set start date for exception 2*
[62221] 1.Timer 1 *start date of exception 2 for timer 1*
[62222] 2.Timer 2 *start date of exception 2 for timer 2*
[62223] 3.Timer 3 *start date of exception 2 for timer 3*
[62224] 4.Timer 4 *start date of exception 2 for timer 4*
[62225] 5.Timer 5 *start date of exception 2 for timer 5*
[62226] 6.Timer 6 *start date of exception 2 for timer 6*
[62227] 7.Timer 7 *start date of exception 2 for timer 7*
[62228] 8.Timer 8 *start date of exception 2 for timer 8*
[6223] 3.Except. 3 *set start date for exception 3*
[62231] 1.Timer 1 *start date of exception 3 for timer 1*
[62232] 2.Timer 2 *start date of exception 3 for timer 2*
[62233] 3.Timer 3 *start date of exception 3 for timer 3*
[62234] 4.Timer 4 *start date of exception 3 for timer 4*
[62235] 5.Timer 5 *start date of exception 3 for timer 5*
[62236] 6.Timer 6 *start date of exception 3 for timer 6*
[62237] 7.Timer 7 *start date of exception 3 for timer 7*
[62238] 8.Timer 8 *start date of exception 3 for timer 8*
[6224] 4.Except. 4 *set start date for exception 4*
[62241] 1.Timer 1 *start date of exception 4 for timer 1*
[62242] 2.Timer 2 *start date of exception 4 for timer 2*
[62243] 3.Timer 3 *start date of exception 4 for timer 3*
[62244] 4.Timer 4 *start date of exception 4 for timer 4*
[62245] 5.Timer 5 *start date of exception 4 for timer 5*
[62246] 6.Timer 6 *start date of exception 4 for timer 6*
[62247] 7.Timer 7 *start date of exception 4 for timer 7*
[62248] 8.Timer 8 *start date of exception 4 for timer 8*
[623] 3.Till *set end date for exceptions*
[6231] 1.Except. 1 *set end date for exception 1*
[62311] 1.Timer 1 *end date of exception 1 for timer 1*
[62312] 2.Timer 2 *end date of exception 1 for timer 2*
[62313] 3.Timer 3 *end date of exception 1 for timer 3*
[62314] 4.Timer 4 *end date of exception 1 for timer 4*
[62315] 5.Timer 5 *end date of exception 1 for timer 5*
[62316] 6.Timer 6 *end date of exception 1 for timer 6*

[62317] 7.Timer 7 *end date of exception 1 for timer 7*
[62318] 8.Timer 8 *end date of exception 1 for timer 8*
[6232] 2.Except. 2 *set end date for exception 2*
[62321] 1.Timer 1 *end date of exception 2 for timer 1*
[62322] 2.Timer 2 *end date of exception 2 for timer 2*
[62323] 3.Timer 3 *end date of exception 2 for timer 3*
[62324] 4.Timer 4 *end date of exception 2 for timer 4*
[62325] 5.Timer 5 *end date of exception 2 for timer 5*
[62326] 6.Timer 6 *end date of exception 2 for timer 6*
[62327] 7.Timer 7 *end date of exception 2 for timer 7*
[62328] 8.Timer 8 *end date of exception 2 for timer 8*
[6233] 3.Except. 3 *set end date for exception 3*
[62331] 1.Timer 1 *end date of exception 3 for timer 1*
[62332] 2.Timer 2 *end date of exception 3 for timer 2*
[62333] 3.Timer 3 *end date of exception 3 for timer 3*
[62334] 4.Timer 4 *end date of exception 3 for timer 4*
[62335] 5.Timer 5 *end date of exception 3 for timer 5*
[62336] 6.Timer 6 *end date of exception 3 for timer 6*
[62337] 7.Timer 7 *end date of exception 3 for timer 7*
[62338] 8.Timer 8 *end date of exception 3 for timer 8*
[6234] 4.Except. 4 *set end date for exception 4*
[62341] 1.Timer 1 *end date of exception 4 for timer 1*
[62342] 2.Timer 2 *end date of exception 4 for timer 2*
[62343] 3.Timer 3 *end date of exception 4 for timer 3*
[62344] 4.Timer 4 *end date of exception 4 for timer 4*
[62345] 5.Timer 5 *end date of exception 4 for timer 5*
[62346] 6.Timer 6 *end date of exception 4 for timer 6*
[62347] 7.Timer 7 *end date of exception 4 for timer 7*
[62348] 8.Timer 8 *end date of exception 4 for timer 8*
[624] 4.Active *activate / deactivate timer*
[63] 3.Thermostats *program thermostat settings*
[631] 1.Temp. T1 *set economy temperature*
[6311] 1.Thermost. 1 *economy temperature of thermostat 1*
[6312] 2.Thermost. 2 *economy temperature of thermostat 2*
[6313] 3.Thermost. 3 *economy temperature of thermostat 3*
[6314] 4.Thermost. 4 *economy temperature of thermostat 4*
[6315] 5.Thermost. 5 *economy temperature of thermostat 5*
[6316] 6.Thermost. 6 *economy temperature of thermostat 6*
[6317] 7.Thermost. 7 *economy temperature of thermostat 7*
[6318] 8.Thermost. 8 *economy temperature of thermostat 8*
[632] 2.Temp. T2 *set comfort temperature*

- [6321] 1.Thermost. 1 — *comfort temperature of thermostat 1*
- [6322] 2.Thermost. 2 — *comfort temperature of thermostat 2*
- [6323] 3.Thermost. 3 — *comfort temperature of thermostat 3*
- [6324] 4.Thermost. 4 — *comfort temperature of thermostat 4*
- [6325] 5.Thermost. 5 — *comfort temperature of thermostat 5*
- [6326] 6.Thermost. 6 — *comfort temperature of thermostat 6*
- [6327] 7.Thermost. 7 — *comfort temperature of thermostat 7*
- [6328] 8.Thermost. 8 — *comfort temperature of thermostat 8*

- [633] 3.Hysteresis — *set hysteresis*
  - [6331] 1.Thermost. 1 — *hysteresis of thermostat 1*
  - [6332] 2.Thermost. 2 — *hysteresis of thermostat 2*
  - [6333] 3.Thermost. 3 — *hysteresis of thermostat 3*
  - [6334] 4.Thermost. 4 — *hysteresis of thermostat 4*
  - [6335] 5.Thermost. 5 — *hysteresis of thermostat 5*
  - [6336] 6.Thermost. 6 — *hysteresis of thermostat 6*
  - [6337] 7.Thermost. 7 — *hysteresis of thermostat 7*
  - [6338] 8.Thermost. 8 — *hysteresis of thermostat 8*
- [634] 4.Active — *activate / deactivate thermostat*

7.Troubles / 7.System state — *check troubles / checking system status*

8.Outputs ctrl. — *control the outputs*

9.Tests

- [91] 1.Zones test — *start zone test*
- [92] 2.Outputs test — *start output test*
- [93] 3.Signal level — *check cellular / radio signal level*
- [94] 4.Test event — *start manual test transmission*
- [95] 5.Others
  - [951] 1.Zones — *check zone status*
  - [952] 2.Card test — *check proximity card number*
- [96] 6.ID change — *change existing ID*
- [97] 7.IMEI/ID / 7.IMEI/ID/MAC.. — *check the IMEI number / ID number / MAC address / IP address*
- [98] 8.FW versions — *check firmware version of devices*
- [99] 9.Measurement — *check measurement results*
  - [991] 1.Temperature — *check temperature (ABAX 2 devices with temp. sensor)*
  - [992] 2.Power consum. — *check power consumption (ASW-200 smart plug)*
- [90] 0.FW update — *start remote update of the control panel firmware*

0.SIM cards

- [01] 1.SIM1 credit — *SIM1 card account status*
- [02] 2.SIM2 credit — *SIM2 card account status*
- [03] 3.Top up SIM1 — *top up SIM1 card account*
- [04] 4.Top up SIM2 — *top up SIM2 card account*
- [05] 5.SIM1 PUK code — *enter PUK code SIM1 card*
- [06] 6.SIM2 PUK code — *enter PUK code SIM2 card*

Replace battery	*enable battery replacement in wireless keypad*
Service access	*define service access rules*
PERFECTA Soft	*start remote communication with PERFECTA Soft*
Service mode	*start service mode*

6.9 Changing code

1. Enter the user menu and press 1 to run 1.CHANGE CODE function.
2. Enter the new code.
3. Press # to save new code.

6.10 Users

There can be up to 62 users in the system.

6.10.1 Adding a user

1. Enter the user menu and press in turn 2 ABC 1 1 to run 1.CODE function.
2. Enter the new user's code.
3. Press # to save the code. Functions that allow entering the user data will be displayed.
4. Press 2 ABC to run 2.SCHEDULE function.
5. Use the ✕ | ▼ or 🔑 | ▲ key to select from the list the user schedule. Five installer defined schedules are available. The schedule defines the rights the user will have and the default way of keyfob operation (you can add the keyfob later on).

	Schedule name and number				
	Normal	Simple	Arms only	Duress	Master
Right	**1**	**2**	**3**	**4**	**5**
Arming	✓	✓	✓	✓	✓
Disarming	✓	✓		✓	✓
Alarm clearing	✓	✓		✓	✓
DURESS				✓	
Zone inhibition	✓				✓
Zone isolation					✓
Change access code	✓	✓	✓		✓
Users editing	✓				✓
Control	✓	✓			✓
Tests	✓				✓
Service access					✓
Changing panel ID					✓

Table 2. Factory default settings of the user schedules. The installer can change the names of schedules and assign other rights to them.

Using the DURESS *right code will trigger a silent alarm, which is not signaled in any way, but the alarm code will be sent to the monitoring station.*

6. Press [# ◧] to confirm schedule selection. Functions that allow entering the user data will be displayed.
7. Press [3 DEF] to run 3.PARTITIONS function.
8. Assign partition(s) to which the user is to have access. The user should have access to at least one partition.
9. Press [# ◧] to confirm partition selection. Functions that allow entering the user data will be displayed.
10. Press [8 TUV] to run 8.NAME function.
11. Enter the user name.
12. Press [# ◧] to save the name. Functions that allow entering the user data will be displayed.
13. Press [* 🔥] to finish adding the user. Prompt for saving the changes will be displayed.
14. Press [1] to save changes.

6.10.2 Editing a user

1. Enter the user menu and press in turn [2 ABC] [2 ABC] to run 2.EDIT USER function.
2. Use the [✕ | ▼] or [🔑 | ▲] key to select from the list the user you want to edit (if you know the user number, you can enter it).
3. Press [# ◧] to start editing the selected user. Functions that allow editing the user data will be displayed.
4. Use available functions to modify the user data (proceed in the same way as when adding a user).
5. Having made all changes, press [* 🔥] to finish editing the user.

6.10.3 Removing a user

1. Enter the user menu and press in turn [2 ABC] [3 DEF] to run 3.REMOVE USER function.
2. Use the [✕ | ▼] or [🔑 | ▲] key to select from the list the user you want to remove (if you know the user number, you can enter it).
3. Press [# ◧] to remove selected user.

6.10.4 Adding keyfob

You can add a keyfob when adding or editing a user.

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 ● for 10 seconds,
APT-210: press and hold the ^ and v for 10 seconds,
APT-200 / APT-210: remove the battery for 10 seconds).

If the MPB-300 panic button operates as the MPT-350 keyfob, follow the instructions below to add it.

1. Press [4 GHI] to run 4.ADD KEY FOB function.
2. Press twice any button of the keyfob (messages on the display will prompt you for what to do next). Type and serial number of the keyfob being added will be displayed.
3. Press [1] to add the keyfob.

6.10.5 Configuring keyfob settings

You can configure a keyfob when adding or editing a user.

Symbols from the APT-200 / MPT-350 and APT-210 keyfob buttons are used in the menu. Refer to Table 3 to find out how to interpret the symbols if you use the T-4 keyfob.

Symbols used in the menu							
	APT-200 / MPT-350	○	□	▲	■	●	○+●
	APT-210	↑	-	□	+	↓	↑↓
Number of T-4 keyfob button (see: Fig. 4)		1	3	4	1+3	2	1+2

Table 3. Menu symbols corresponding to particular T-4 keyfob buttons.

1. Run BUTTON ○/↑ function.
2. Use the [✕|▼] or [🔑|▲] key to select from the list the operation that control panel is to perform after the button ○ [APT-200 / MPT-350] / ^ [APT-210] is pressed on the keyfob.

i *For information on zone types and output functions, please consult the installer.*

3. Press [# ◧] to confirm the selection. Functions that allow entering / editing the user data will be displayed.
4. Configure settings of the other keyfob buttons in the same way.
5. For the APT-200 / APT-210 keyfob, configure how the LEDs will operate when a keyfob button is pressed (even when the button does not start any function).
   5.1. Use the [✕|▼] key to find the LED 1 function.
   5.2. Press [# ◧] to start the function.
   5.3. Use the [✕|▼] or [🔑|▲] key to select from the list the operating mode of the red keyfob LED.
   5.4. Press [# ◧] to confirm the selection.
   5.5. Repeat this procedure to configure the settings for the rest of the keyfob LEDs.
6. Use the [✕|▼] key to find the KEY FOB EVENT option.
7. Use the [☀|▶] key to define whether the use of the keyfob is to be saved to the event log (💾 - yes, · - no).

6.10.6 Removing keyfob

You can remove a keyfob when adding or editing a user.

1. Press [5 JKL] to run 5.REMOV.KEY FOB function. Type and serial number of the keyfob being removed will be displayed.
2. Press [1] to remove the keyfob.

6.10.7 Adding proximity card

You can add a proximity card when adding or editing a user.

1. Press [6 MNO] to start the 6.ADD CARD function.
2. Press:
   [1] - if you want to enter the card number manually,
   [2 ABC] - if you want to use a device with the proximity card reader to add the card.

Entering card number manually

1. Enter the card number (see: “Entering hexadecimal values” p. 18).

2. Press [# ◧] to confirm the card number.

Reading card number using the reader

1. Use the [✕|▼] or [🔑|▲] key to select from the list a reader device that you want to use to add the card.
2. Press [# ◧] to confirm the selection.
3. Bring the card close to the reader two times (the messages on the display will guide you).

The proximity card/disarm device will send the card number only after you move the card away from the reader.

6.10.8 Removing proximity card

You can remove a proximity card when adding or editing a user.

1. Press [7 PQRS] to start the 7.DELETE CARD function.
2. The number of the card to be removed will be displayed.
3. Press [1] to remove the card.

6.11 Outputs reset

Using 3.OUTPUTS RESET function you can:

- deactivate *1. External siren*, *2. Internal siren*, *3. Burglary*, *4. Fire alarm*, *5. DURESS alarm*, *6. Panic alarm*, *7. AUX. alarm*, *8. Alarm – not verified*, *9. Alarm - verified*, *10. Tamper alarm*, *13. Zone violation, 4. Chime* and *27. Latch* function outputs,
- deactivate for 16 seconds the *11. Fire detectors power supply* function output (to clear the alarm memory of fire detectors),
- activate the *21. Detectors reset* function output.

Enter the user menu and press [3 DEF] to run 3.OUTPUTS RESET function.

6.12 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, for example, 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 service technician immediately to repair the defect.

For security considerations, the installer may only permit bypassing of some of the zones.

The zone bypassing functions can also be used to unbypass the zones (the zone inhibiting function makes it also possible to unbypass an isolated zone, while the zone isolating function makes it also possible to unbypass an inhibited zone).

6.12.1 Zone inhibiting

The inhibited zone will remain bypassed until disarming the partition it belongs to, or until unbypassing the zone by the user.

If the zone belongs to several partitions and is only armed when all partitions are armed, it will be unbypassed after disarming one of the partitions.

1. Enter the user menu and press in turn 4GHI 1 to run 1.INHIBIT function.
2. The list of zones will be displayed (you will see the status of the first of the zones that you can bypass/unbypass). You can scroll up and down the list using the ✕|▼ and 🔑|▲ keys. The symbol in the upper right corner of the display indicates:
   · – zone is not bypassed,
   ▣ – zone is inhibited,
   ■ – zone is isolated.
3. Press any number key to change the displayed symbol to one of the following symbols:
   ▣ – the zone is to be inhibited,
   · – the zone is to be unbypassed.
4. Press ☀|▶ or ☾|◀ to enter the graphic mode (see: “Graphic mode” p. 17). To exit the graphic mode and return to the basic mode, press ✕|▼ or 🔑|▲.
5. Press #◧ to inhibit/unbypass zones.

6.12.2 Zone isolating

The isolated zone will remain bypassed until it is unbypassed by the user.

Enter the user menu and press in turn 4GHI 2ABC to run 2.ISOLATE function. The way of indicating the zone state and the procedure are identical to those used for inhibiting the zones, but pressing any number key will change the displayed symbol to one of the following symbols:

■ – the zone is to be isolated,

· – the zone is to be unbypassed.

6.13 Viewing the event log

Enter the user menu and press 5JKL to run 5.EVENT LOG function. The last event that occurred in the system will be displayed. In the upper line of the display, the event occurrence time is presented, and in the lower line – the event description. Press ☀|▶ to see some additional information related to the event in the lower line (e.g. the partition in which the event occurred, the zone that caused the event etc.). Press ☾|◀ to see the information related to reporting the event in the upper line. The following characters are presented in square brackets:

space – event is not reported,

e – event sent via Ethernet (ETHM-1 Plus module),

g – event sent via cellular data network, SIM1 card,

G – event sent via cellular data network, SIM2 card,

s – event sent via SMS, SIM1 card,

S – event sent via SMS, SIM2 card,

a – event sent via GSM voice channel, SIM1 card,

A – event sent via GSM voice channel, SIM2 card,

+ – test event sent via all defined transmission paths,

? – test event not sent via all defined transmission paths.

You can use the 🔑|▲ and ✕|▼ keys to scroll the event log.

6.14 Settings

6.14.1 Setting the clock

1. Enter the user menu and press 6 MNO 1 to start the 1.SET TIME function. Time according to the control panel clock will be displayed.
2. Enter the new time.
3. Press # to save new time. Date according to the control panel clock will be displayed.
4. Enter the new date.
5. Press # to save new date.

6.14.2 Programming the timer settings

The timers are used, among others, to arm / disarm partitions or to control the *15. Controlled* type outputs (the devices connected to those outputs) and the thermostats. Ask the installer to find out what each timer is used for.

Setting the timer start / stop time

1. Enter the user menu and press 6 MNO 2 ABC 1 to start the 2.SETTINGS function.
2. Use the ✕ | ▼ or 🔑 | ▲ key to select from the list a day of the week (timers used on the selected day) or 8.EVERYDAY (timers used on those days of the week for which no timers are configured).
3. Press # to confirm the selection. The list of editable timers will be displayed.
4. Press ✕ | ▼ or 🔑 | ▲ to select from the list a timer.
5. Press # to confirm the selection. The timer start and stop time will be displayed (if no times are configured, you will see empty fields).
6. Enter a new timer start / stop time (hour:minutes). See: “Time setting rules”.
7. Press # to confirm the changes.

Setting an exception

Setting the exception time period

1. Enter the user menu and press 6 MNO 2 ABC 2 ABC to start the 2.FROM function.
2. Use the ✕ | ▼ or 🔑 | ▲ key to select from the list an exception.
3. Press # to confirm the selection. The list of editable timers will be displayed.
4. Use the ✕ | ▼ or 🔑 | ▲ key to select from the list a timer.
5. Press # to confirm the selection. The exception start date will be displayed (if no date is configured, you will see an empty field).
6. Enter a new date (year-month-day). See: “Date setting rules”.
7. Press # to confirm the changes.
8. Press ☾ | ◄ ☾ | ◄ 3 DEF to start the 3.TILL function.
9. Use the ✕ | ▼ or 🔑 | ▲ key to select from the list an exception.
10. Press # to confirm the selection. The list of editable timers will be displayed.
11. Use the ✕ | ▼ or 🔑 | ▲ key to select from the list a timer.
12. Press # to confirm the selection. The exception end date will be displayed (if no date is configured, you will see an empty field).
13. Enter a new date (year-month-day). See: “Date setting rules”.
14. Press # to confirm the changes.

Setting the timer start / stop time for the exception

1. Enter the user menu and press 6MNO 2ABC 1 9WXYZ to start the 9.EXCEPTIONS function.
2. Use the ✕|▼ or 🔑|▲ key to select from the list an exception.
3. Press #◧ to confirm the selection. The list of editable timers will be displayed.
4. Use the ✕|▼ or 🔑|▲ key to select from the list a timer.
5. Press #◧ to confirm the selection. The timer start / stop time for when the exception is in effect will be displayed (if no times are configured, you will see empty fields).
6. Enter a new timer start / stop time (hour:minutes). See: “Time setting rules”.
7. Press #◧ to confirm the changes.

Timer activation / deactivation

1. Enter the user menu and press 6MNO 2ABC 4GHI to start the 4.ACTIVE function.
2. The list of timers will be displayed (you will see the status of the first of the editable timers). You can scroll up and down the list using the ✕|▼ and 🔑|▲ keys. The symbol in the upper right corner of the display indicates:
   - · – inactive timer (it is not started / stopped),
   - ⏱ – active timer (it is started / stopped at a set time).
3. Press any number key to change the currently shown symbol for another one.
4. Press ☀|▶ or ☾|◀ to start the graphic mode (see: “Graphic mode” p. 17). To exit the graphic mode and return to the basic mode, press ✕|▼ or 🔑|▲.
5. Press #◧ to confirm the changes.

Rules for programming the timer settings

Time setting rules

You can only set the timer start time or the stop time. The hour or minutes may remain undefined (e.g. if you enter a value from beyond the range, i.e. more than 23 for the hour or 59 for the minutes, it will be changed to xx). For example:

xx:45 – the timer will be started / stopped every hour throughout the day (at 0:45, 1:45 etc.),

11:xx – the timer will be started / stopped every minute between 11.00 and 11:59.

Date setting rules

i *You must program both the start and end date for the time period during which the exception is in effect.*

One or two of the three date components may remain undefined (e.g. if you enter a value from beyond the range, i.e. more than 2099 for the year, 12 for the month or 31 for the day, it will be changed to letters x). For example:

xxxx-12-25 – the exception will be valid from / to 25 Dec. each year,

xxxx-xx-12 – the exception will be valid from / to 12th day of each month each year,

xxxx-03-xx – the exception will be valid from the beginning of March each year (same as xxxx-03-01) / to the end of March each year (same as xxxx-03-31),

2025-xx-05 – the exception will be valid from / to 5th day of each month in 2025,

2025-xx-xx – the exception will be valid from the beginning of 2025 (same as 2025-01-01) / to the end of 2025 (same as 2025-12-31),

2025-06-xx – the exception will be valid from the 1st of June 2025 (same as 2025-06-01) / to the 30th of June 2025 (same as 2025-06-30).

As you can see from the above examples, how you interpret the dates depends on whether the unidentified value is the start or end of the exception.

6.14.3 Programming the thermostat settings

The thermostats are used to control the *24.Thermostat* type outputs (the devices connected to those outputs). Ask the installer to find out what each thermostat is used for.

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

Programming temperature T1 (economy temperature)

The temperature T1 (economy temperature) is the first temperature threshold. If the first temperature threshold is active, the thermostat will be turned on when the temperature drops below temperature T1 (economy temperature). Ask the installer to find out when the first temperature threshold is active.

1. Enter the user menu and press 6 MNO 3 DEF 1 to start the 1.TEMP. T1 function.
2. Use the ✕|▼ or 🔑|▲ key to select from the list a thermostat.
3. Press # to confirm the selection. The temperature will be displayed (if no temperature is configured, you will see empty fields).
4. Enter a new temperature. See: “Temperature programming rules”.
5. Press # to confirm the changes.

Programming temperature T2 (comfort temperature)

The temperature T2 (comfort temperature) is the second temperature threshold. If the second temperature threshold is active, the thermostat will be turned on when the temperature drops below temperature 2 (comfort temperature). Ask the installer to find out when the second temperature threshold is active.

1. Enter the user menu and press 6 MNO 3 DEF 2 ABC to start the 1.TEMP. T2 function.
2. Use the ✕|▼ or 🔑|▲ key to select from the list a thermostat.
3. Press # to confirm the selection. The temperature will be displayed (if no temperature is configured, you will see empty fields).
4. Enter a new temperature. See: “Temperature programming rules”.
5. Press # to confirm the changes.

Programming hysteresis

Hysteresis is the temperature difference between turning the thermostat on and off. The thermostat will be turned on when the temperature drops below the threshold by a value higher than the hysteresis. The thermostat will be turned off when the temperature reaches the threshold. Hysteresis is used to prevent the thermostat from being repeatedly turned on and off when the temperature fluctuates.

1. Enter the user menu and press 6 MNO 3 DEF 3 DEF to start the 3.HYSTERESIS function.
2. Use the ✕|▼ or 🔑|▲ key to select from the list a thermostat.
3. Press # to confirm the selection. The hysteresis will be displayed (if no hysteresis is configured, you will see empty fields).
4. Enter a new hysteresis. See: “Hysteresis programming rules”.
5. Press # to confirm the changes.

Thermostat activation / deactivation

1. Enter the user menu and press 6 MNO 3 DEF 4 GHI, to start the 4.ACTIVE function.

2. The list of thermostats will be displayed (you will see the status of the first of the editable thermostats). You can scroll up and down the list using the ✕|▼ and 🔧|▲ keys. The symbol in the upper right corner of the display indicates:
   · - inactive thermostat (it is not turned on / off),
   - active thermostat (it is turned on / off based on the temperature measurements).
3. Press any number key to change the currently shown symbol for another one.
4. Press ☀|► or ☾|◄ to enter the graphic mode (see: "Graphic mode" p. 17). To exit the graphic menu and return to the basic menu, press ✕|▼ or 🔧|▲.
5. Press # to confirm the changes.

Rules for programming the thermostat settings

Temperature programming rules

You can enter a value from -30°C to 70°C (with accuracy to 0,5°). To enter a minus sign, press 3 DEF when the cursor is on the first position. To clear the currently programmed value, press 2 ABC 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, the thermostat will be turned on when the temperature drops below the threshold by 0,5°C.

6.15 Checking the troubles / system state

When the ⚠ LED is flashing, check what is the cause of this signaling. Enter the user menu and press 7 PQRS. To scroll the list, use the ✕|▼ and 🔧|▲ keys.

6.15.1 Information on system state

If the *Grade 2* option is enabled by the installer, the 7.SYSTEM STATE function, instead of the 7.TROUBLES function, is available in the user menu. When the function is running, the following information is displayed:

- alarms,
- bypassed zones,
- troubles,
- partition status (disarmed or arming type).

6.15.2 What to do in the event of trouble

Each trouble poses a danger to proper functioning of the alarm system and should be repaired as soon as possible. If necessary, consult the installer.

6.15.3 Trouble memory and clearing the trouble memory

The installer defines whether only the current troubles are to be presented, or also those which have already ended. The flashing letter "M" in the upper right corner of the display means that the trouble has already ended. You can clear the trouble memory after quitting the function.

1. Press * 🔥 to quit the function. The "Clear trouble memory? 1=Yes" message will appear on the display.
2. Press 1 to clear the trouble memory (press * 🔥, if you don't want to clear the trouble memory).

6.16 Output control

Using the keypad, you can control the operation of devices connected to the outputs (e.g. to raise/lower 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.).

6.16.1 Quick control of outputs

Consult the installer whether the quick control of outputs is available (it is required to assign the outputs to keys designated with digits, which can only be done by the installer). If the quick control is available, you can turn ON/OFF devices connected to the outputs without entering the code.

Quick activation of output

Press the key to which the controllable output is assigned, and then [#].

Quick deactivation of output

Press the key to which the controllable output is assigned, and then [*].

6.16.2 Controlling the outputs by means of function

1. Enter the user menu and press [8 TUV] to run 8.OUTPUTS CTRL. function.
2. Symbols illustrating the status of outputs you can control will be presented in the upper line of the display:
   · – output is deactivated,
   ■ – output is activated.
   The name of the output indicated by the cursor is presented in the lower line of the display.
3. Use the [▶] or [◀] key to move the cursor to the output you want to control.
4. Press [#] to activate the output or [0] to deactivate the output.

6.16.3 Controlling the outputs by means of proximity card

Ask the installer if the function to control the outputs with proximity card is available and which outputs can be controlled this way.

Bring the card close to the keys and hold for 3 seconds to change the output state:

- deactivated outputs will be activated,
- activated outputs will be deactivated.

6.17 Tests

6.17.1 Zone test

The 1.ZONES TEST function allows you to test the system zones and detectors.

You can test the zones for which the installer has programmed other wiring type than No detector*.*

Zone violation during the test will not trigger the control panel reaction, as preprogrammed for the zone.

When testing the zones, the keypad does not present the current zone state, but only indicates whether or not the zone was violated during the test.

1. Enter the user menu and press in turn [9 WXYZ] [1] to run 1.ZONES TEST function.

2. Define the test duration (from 1 to 99 minutes).
3. Press [# ◧] to start test.
4. The zones that you can test will be presented on the display by the symbol · (no symbol means that the zone cannot be tested). The numbers around the display will help you identify the zones. For zones 1-32, the cursor is displayed in the upper line. For zones 33-64, the cursor is displayed in the lower line. Use the [☀|▶] or [☾|◀] key to display the next/previous zones.
5. Violate the zone (e.g. walking through the area supervised by the motion detector or opening the window supervised by the magnetic contact).
6. The keypad should inform you that the zone has been violated (the zone symbol changes to ■). Information on the violation will be presented until the zone test is terminated.
7. The test will be terminated automatically after the defined time has elapsed. You can terminate it earlier by pressing [* 🔥].

6.17.2 Output test

The 2.OUTPUTS TEST function makes it possible to test the system outputs and sirens or other devices connected to the outputs.

1. Enter the user menu and press in turn [9 WXYZ] [2 ABC] to run 2.OUTPUTS TEST function.
2. Symbols illustrating the status of outputs you can test will be presented in the upper line of the display · (no symbol means that the output cannot be tested):
   · – output inactive,
   ■ – output active.
3. Use the [☀|▶] or [☾|◀] key to hover the cursor over the output you want to test. The name of the output will be presented in the lower line of the display.
4. Press [# ◧] to activate the output or [0 ⓘ] to deactivate the output.

6.17.3 Checking the level of cellular / radio signal

Using the 3.SIGNAL LEVEL function you can check:

- the level of signal received by the cellular antenna,
- noise level in the 433 MHz frequency band [if the PERFECTA-RF module is connected to the control panel],
- the level of radio signal received by the control panel from MICRA wireless devices [if the PERFECTA-RF module is connected to the control panel].

Enter the user menu and press in turn [9 WXYZ] [3 DEF] to run 3.SIGNAL LEVEL function. The signal level information will be presented as a percentage. You can scroll the list using the [✕|▼] and [🔑|▲] keys.

6.17.4 Starting the test transmission

The 4.TEST EVENT function makes it possible to test the communication with monitoring stations. Enter the user menu and press in turn [9 WXYZ] [4 GHI] to run 4.TEST EVENT function. A “Manual transmission test” event will be saved to the control panel memory. The event code will be sent to the monitoring station.

i *The test transmission is sent via all transmission paths which are used for reporting.*

6.17.5 Checking the zone status

If you want to check the zone status, enter the user menu and press in turn [9 WXYZ] [5 JKL] [1] to run 1.ZONES function. The zone status is presented by the same symbols as in the system status preview mode (see p. 9). The numbers around the display will help you identify the

zones. For zones 1-32, the cursor is displayed in the upper line. For zones 33-64, the cursor is displayed in the lower line. Use any arrow key to view next/previous zones. If the zone is not used, its status is not displayed.

6.17.6 Checking the proximity card number

If you want to check the proximity card number and find out who the card belongs to, use the 2.CARD TEST function.

1. Enter the user menu and press in turn 9WXYZ 5JKL 2ABC to run 2.CARD TEST function.
2. Use the ✕|▼ or 🔑|▲ key to select a device with a reader, and then press # ◧.
3. Present the card to the reader in the selected device.
4. The display will show the user name in the upper line and the card number in the lower line. If the card does not belong to the system user, you will see the message "Unassigned" in the upper line.

6.17.7 ID change

The 6.ID CHANGE function makes it possible to change the individual identification number assigned for the needs of communication via the SATEL server.

1. Enter the user menu and press in turn 9WXYZ 6MNO to run 6.ID CHANGE function. The “Change the panel ID ? 1=Yes” message will be displayed.
2. Press 1. The existing ID number will be deleted and the SATEL server will assign a new ID number.

The ID number will not be changed until the control panel is connected to the SATEL server.

If you change the ID number, the PERFECTA CONTROL application users will have to configure the alarm system settings again (the applications using the old ID number will not be able to connect to the control panel).

6.17.8 Checking the IMEI number / ID number / MAC address / IP address

Using the 7.IMEI/ID function you can check:

- IMEI – individual identification number of the control panel cellular communicator,
- ID – individual identification number for the purpose of communication via the SATEL server (assigned automatically by the SATEL server).

These parameters are required when configuring the PERFECTA CONTROL application.

If the ETHM-1 Plus module is connected to the control panel, the 7.IMEI/ID/MAC.. function is available instead of 7.IMEI/ID. The function is used to check the IMEI number, the ID number and:

- MAC – hardware address of the ETHM-1 Plus module.
- Internal IP – local IP address of the ETHM-1 Plus module.
- External IP – public IP address of the ETHM-1 Plus module.

Enter the user menu and press in turn 9WXYZ 7PQRS to run 7.IMEI/ID / 7.IMEI/ID/MAC.. function. To scroll through the information, use the ✕|▼ and 🔑|▲ keys.

6.17.9 Checking the firmware version of devices in system

Using the 8.FW VERSIONS function, you can check the firmware version of devices included in the alarm system:

- control panel,
- modules connected to the control panel,

- MICRA wireless devices [if the PERFECTA-RF module is connected to the control panel].

Enter the user menu and press in turn 9WXYZ 8TUV to run 8.FW VERSIONS function. Information on the control panel firmware version will be displayed. To scroll the list of devices, use the ✕|▼ and 🔑|▲ keys.

6.17.10 Starting remote update of the control panel firmware

1. Enter the user menu and press in turn 9WXYZ 0 to run 0.FW UPDATE function.
2. New firmware download will start (if a new firmware version is available on UPSERV update server). After the firmware download is completed, the update will start. If you want to stop the procedure, press *.

6.18 SIM cards

6.18.1 Checking the balance of SIM card

If the control panel is properly configured by the installer, you can use a keypad to check the balance of SIM card.

1. Enter the user menu and press in turn:
   0 1 to run 1.SIM1 CREDIT function and check the balance of SIM 1 card,
   0 2ABC to run 2.SIM2 CREDIT function and check the balance of SIM 2 card,
2. The information received from the SIM card operator will be presented on the display. To scroll through the information, use the ✕|▼ and 🔑|▲ keys.

6.18.2 Topping up the SIM card

If the control panel is properly configured by the installer, you can use a keypad to top up the SIM card.

1. Enter the user menu and press in turn:
   0 3DEF to run 3.TOP UP SIM1 function and top up the SIM 1 card,
   0 4GHI to run 4.TOP UP SIM2 function and top up the SIM 2 card.
2. Enter the top-up code (e.g. from the scratch-card).
3. Press #. The top-up information received from the SIM card operator will be presented on the display.

6.18.3 Unblocking the SIM card

If the SIM card has been blocked (after entering an invalid PIN code three times), you can unblock it by entering the PUK code.

1. Enter the user menu and press in turn:
   0 5JKL to run 5.SIM1 PUK CODE function and enter PUK code for SIM 1 card,
   0 6MNO to run 6.SIM2 PUK CODE function and enter PUK code for SIM 2 card.
2. Enter the 8-digit PUK code.
3. Press #. The SIM card will be unblocked (the PIN code preprogrammed in the control panel will be written to the card).

6.19 Replacing battery in wireless keypad

If you want to replace the battery in wireless keypad, run the REPLACE BATTERY function first. This will prevent the tamper alarm from being triggered when you open the keypad enclosure.

1. Enter the user menu.

2. Keep pressing the (🔑|▲) key until the cursor → indicates the REPLACE BATTERY function.
3. Press (# ◧).
4. After the "SELECT..." message appears, use the (✕|▼) or (🔑|▲) key to find on the list the wireless keypad in which you want to replace the battery.
5. Press (# ◧). Tamper alarms from the selected keypad will be blocked for 3 minutes. During that time you can replace the battery.

6.20 Service access

If the alarm system is to comply with the EN 50131 standard requirements for Grade 2, the service access should be limited.

The SERVICE ACCESS function allows you to define the rules of access to the system by the person using the service code (installer/service technician). These rules apply to all methods of getting access to the alarm system, i.e. by using keypad, PERFECTA SOFT program and PERFECTA CONTROL application.

Starting the function will display the list of options. To scroll the list, use the (✕|▼) and (🔑|▲) keys.

Active – if this option is enabled, the installer/service technician has access to the alarm system i.e.:
- after entering the service code, it is possible to enter the service mode and run some functions available in the user menu,
- it is possible to configure the alarm system in the PERFECTA SOFT program.

Partition 1 – if this option is enabled, the installer/service technician can operate the partition 1 (arm / disarm it, clear alarm, bypass / unbypass zones) and edit the users (grant them access to the partition 1). The option is available, if you have access to the partition 1.

Partition 2 – if this option is enabled, the installer/service technician can operate the partition 2 (arm / disarm it, clear alarm, bypass / unbypass zones) and edit the users (grant them access to the partition 2). The option is available, if you have access to the partition 2.

Partition 3 – if this option is enabled, the installer/service technician can operate the partition 3 (arm / disarm it, clear alarm, bypass / unbypass zones) and edit the users (grant them access to the partition 3). The option is available, if you have access to the partition 3.

Partition 4 – if this option is enabled, the installer/service technician can operate the partition 4 (arm / disarm it, clear alarm, bypass / unbypass zones) and edit the users (grant them access to the partition 4). The option is available, if you have access to the partition 4.

If there is no user in the alarm system having the SERVICE ACCESS right, the installer/service technician has access to the alarm system (also in the PERFECTA SOFT program and the PERFECTA CONTROL application), can operate the partitions and edit the users.

6.21 Starting remote communication with PERFECTA SOFT

The PERFECTA SOFT function is used to start remote communication with the PERFECTA SOFT program for the purpose of programming the alarm system. The communication is carried out via Ethernet (if the ETHM-1 Plus module is connected to the control panel) or via cellular data network.

For more information on the remote programming of the alarm control panel, please refer to the alarm control panel programming manual.

6.22 Establishing communication with PERFECTA SOFT via GPRS/LTE

The PERFECTA SOFT function makes it possible to start communication with the PERFECTA SOFT program via cellular network (data transmission) to allow remote programming of the control panel. This is one of the methods for establishing communication between the PERFECTA SOFT program and the alarm control panel. For more information, please refer to the control panel programming manual.

6.23 Service mode

The SERVICE MODE function is only available after entering the service code. It allows you to enter the service mode. After entering the service mode, the functions that allow you to configure the alarm system will be displayed. For more information, please refer to the control panel programming manual.

7. Listening in

If a microphone is connected to the alarm control panel, the installer can make the listen-in function available to the users. This function allows you to listen in remotely, on a telephone, to what is going on in the protected facilities, e.g. to verify the alarm. You can use the listening in functionality by:

- calling the control panel phone number (consult the installer to learn the phone number you must call),
- after having listened to the voice message by which the control panel will notify you about a new event in the alarm system.

Consult the installer to determine whether both ways of using the function are available, or just one of them.

8. Keyfobs

You can operate the alarm system by using a keyfob if one of the modules is connected to the control panel:

- ACU-220 / ACU-280 – you can use the ABAX 2 system keyfob: APT-200 / APT-210,
- PERFECTA-RF – you can use the MICRA system keyfob: MPT-350,
- INT-RX-S – you can use a 433 MHz keyfob: MPT-350, T-4, T-2 or T-1.

The keyfob can start up to 6 functions. For information about functions assigned to individual buttons / button combinations, please consult the person who has configured the keyfob settings. If you have the APT-200 / APT-210 keyfob, ask the person about the keyfob LEDs. They can indicate the system state.

If the MPB-300 panic button operates as the MPT-350 keyfob:

- pressing the button is treated as pressing the ○ button on the keyfob,
- opening the tamper switch is treated as pressing the ● button on the keyfob.

The alarm system may be configured so that, in some circumstances, arming the system by using the keyfob will fail (see "System problems and arming failure"). Consult the installer to learn how you are to be effectively notified of the system arming failure.

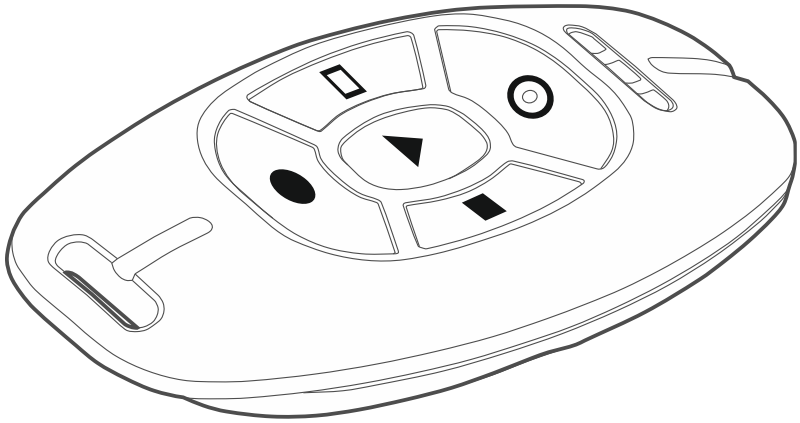


Fig. 2. APT-200 / MPT-350 keyfob.

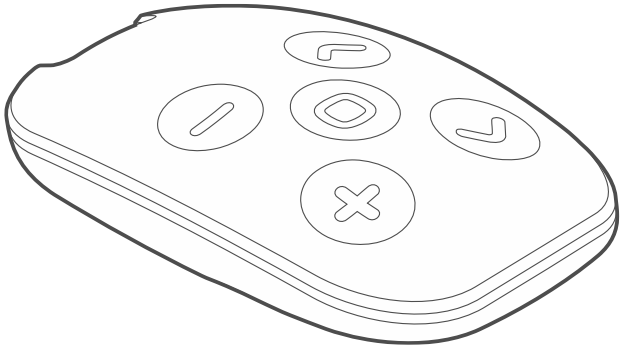


Fig. 3. APT-210 keyfob.

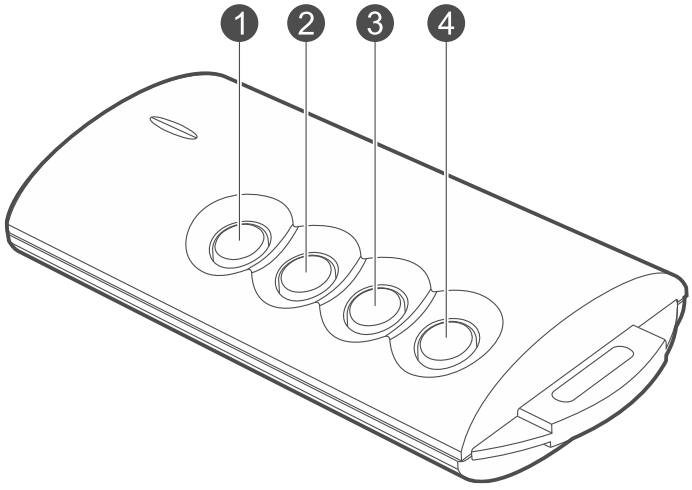


Fig. 4. T-4 keyfob and button numbers.

9. SMS control

You can control your alarm system by using SMS messages containing appropriate control commands. The SMS message must be sent to the control panel phone number (number of the currently used SIM card). Agree with the installer on:

- content of the control commands.

- functions that are to be run by these commands. The following functions are available:
  - zone violation,
  - arming,
  - disarming and alarm clearing,
  - triggering panic, fire or medical alarm,
  - activation / deactivation / switchover of *15. Controlled* type of output,
  - checking partition status,
  - sending USSD code to the operator of SIM card installed in the control panel (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.
- 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.

Using the command that controls sending of the USSD codes, you can send an SMS message via the control panel. The form of SMS message you will send to the control panel must be as below:

xxxx=tttt:cccc=

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

The control panel is case sensitive.

The alarm system may be configured so that, in some circumstances, arming the system by using the SMS message will fail (see “System problems and arming failure”). Consult the installer to learn how you are to be effectively notified of the system arming failure.

10. PERFECTA CONTROL application

The PERFECTA CONTROL is a mobile application for remote operation of the alarm system. You can use the app to:

- check the status of partitions, zones and outputs,
- arm / disarm the system or clear alarm,
- bypass / unbypass the zones,
- control the outputs,
- view the troubles,
- view the event log.

Additionally, the application can provide information on the alarm system events by using push notifications.

If no keypad is connected to the control panel, some functions are not available.

If the IP cameras are installed in the protected premises, you can watch video from these cameras in the application.

Communication between the application and the control panel is encrypted.

You can download the application from the internet stores: “Google play” (Android system devices) or “App Store” (iOS system devices).

To add a new alarm system that you want to control from the application, you will need:

- control panel IMEI number and ID number. You can:
  - obtain them in the form of a QR code from the installer or a user who has already entered the control panel data to application,
  - access them in the keypad ([code] * 9WXYZ 7PQRS).
- your user code.

The IMEI number is used to establish connection both via cellular data network and via Ethernet. The MAC address of the ETHM-1 Plus module is not used to establish connection.

10.1 First start of PERFECTA CONTROL (Android)

1. Decide if you want the access to the application to be password-protected. You will proceed to the next step.
2. The tutorial will be displayed. Tap “Skip” to skip it.
3. The screen for adding a new alarm system will be displayed (Fig. 5).

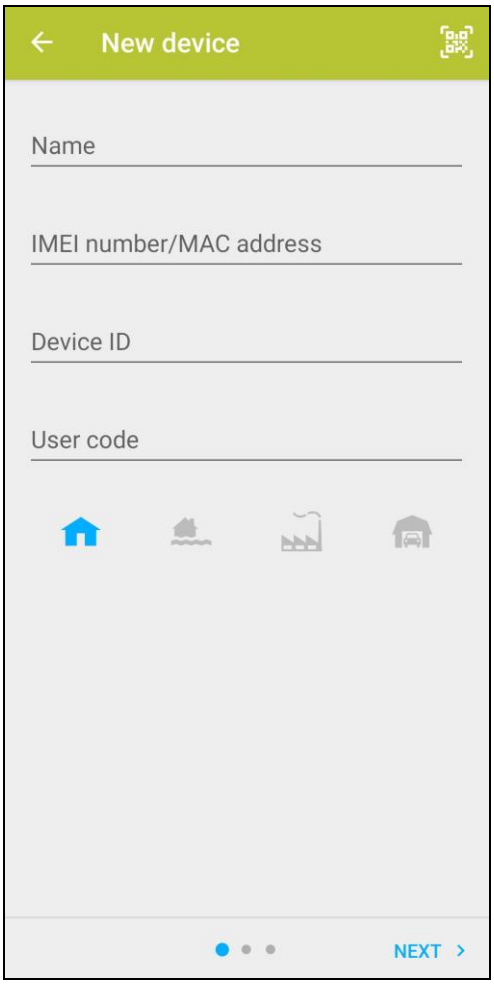


Fig. 5. PERFECTA CONTROL application (Android): the screen for adding a new alarm system.

10.1.1 Adding a new alarm system by using the QR code (Android)

1. Tap  .
2. Tap “Scan QR code” (use the camera to read the code – allow the application to access the camera) or “Select an image” (the QR will be read from an image file – indicate where the file is saved on your phone).
3. Enter the password protecting the QR code and tap “OK”. The name of the system and the control panel’s IMEI number and ID number will be entered.
4. Enter your user code.
5. Select the icon that will be displayed next to the name on the list of alarm systems.
6. Tap “Next”.
7. Enable / disable the push notifications of the alarm system events. If you enable the push notifications, select the events about which you want to be informed.
8. If you want to watch video from IP cameras in the application, configure the camera settings. If you do not want to use the application to watch video from IP cameras, tap “Done”.

10.1.2 Adding a new alarm system without using the QR code (Android)

1. Enter the name (it will help you identify the alarm system while using the application).
2. Enter the control panel’s IMEI number.
3. Enter the control panel’s ID number (the individual identification number for the purpose of communication via the SATEL server).
4. Enter your user code.
5. Select the icon that will be displayed next to the name on the list of alarm systems.
6. Tap “Next”.
7. Enable / disable the push notifications of the alarm system events. If you enable the push notifications, select the events about which you want to be informed.
8. If you want to watch video from IP cameras in the application, configure the camera settings. If you do not want to use the application to watch video from IP cameras, tap “Done”.

10.2 First start of PERFECTA CONTROL (iOS)

1. Decide if you want the application to send notifications. You will proceed to the next step.
2. Decide if you want the access to the application to be password-protected. You will proceed to the next step.
3. The tutorial will be displayed. Tap “Skip” to skip it.
4. The screen for adding a new alarm system will be displayed (Fig. 6).

10.2.1 Adding a new alarm system by using the QR code (iOS)

1. Tap  .
2. Allow the application to access the camera.
3. Scan the QR code.
4. Enter the password protecting the QR code and tap “OK”. The name of the system and the control panel’s IMEI number and ID number will be entered.
5. Enter your user code.
6. Select the icon that will be displayed next to the name on the list of alarm systems.
7. Tap “Next”.

8. Enable / disable the push notifications of the alarm system events. If you enable the push notifications, select the events about which you want to be informed.
9. If you want to watch video from IP cameras in the application, configure the camera settings. If you do not want to use the application to watch video from IP cameras, tap “Done”.

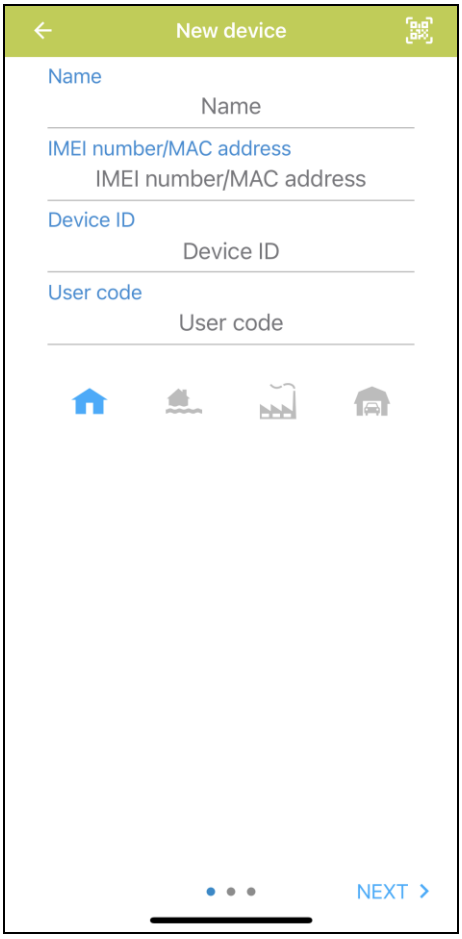


Fig. 6. PERFECTA CONTROL application (iOS): the screen for adding a new alarm system.

10.2.2 Adding a new alarm system without using the QR code (iOS)

1. Enter the name (it will help you to identify the alarm system while using the application).
2. Enter the control panel’s IMEI number.
3. Enter the control panel’s ID number (the individual identification number for the purpose of communication via the SATEL server).
4. Enter your user code.
5. Select the icon that will be displayed next to the name on the list of alarm systems.
6. Tap “Next”.
7. Enable / disable the push notifications of the alarm system events. If you enable the push notifications, select the events about which you want to be informed.
8. If you want to watch video from IP cameras in the application, configure the camera settings. If you do not want to use the application to watch video from IP cameras, tap “Done”.

11. Sirens

The main task of the siren is to provide information about emergency situations by means of sound or light signals. The installer can configure the alarm system so that the siren will additionally signal the following:

1 sound / flash – starting the arming procedure (if the exit delay time is 0, the system is armed immediately),

2 sounds / flashes – disarming,

4 sounds / flashes – clearing alarm,

7 sounds / flashes – arming with keyfob is impossible or the arming procedure has failed.

The signaling can be triggered in all cases or only after a keyfob or a zone is used to arm / disarm the system or clear alarm. Discuss with the installer which option you prefer.

12. Manual update history

Manual version	Introduced changes
06/23	• List of user functions has been supplemented (p. 18). • Note on the APT-200 keyfob previously registered to another system has been added (p. 27). • Chapter “Quick control of outputs” has been updated (p. 35). • Chapter “Checking the zone status” has been added (p. 36). • Chapter “Checking the proximity card number” has been added (p. 37).
12/24	• Information on the INT-TSG2R and INT-TSH2R keypads has been added in the “Keypads” section (p. 7). • List of user functions has been updated (p. 18). • Note on the ABAX2 keyfob previously registered to another system has been modified (p. 27). • Information on the APT-210 keyfob has been added in the “Configuring keyfob settings” (p. 28). • The “Viewing the event log” section has been updated (p. 30). • Information on the ART-210 radiator thermostat has been added in the “Programming the thermostat settings” section (p. 33). • The “Checking the IMEI number / ID number / MAC address / IP address” section has been updated (p. 37). • The “Starting remote communication with PERFECTA Soft” section has been updated (p. 39). • Information on the APT-210 keyfob has been added in the “Keyfobs” section (p. 40). • Note on using the IMEI number to establish connection between the mobile app and the control panel has been added (p. 43).
06/25	• Information on the INT-TSH210 keypad has been added in the “Keypads” section (p. 7). • List of user functions has been updated (p. 18). • Note on the MPB-300 button operating as the MPT-350 keyfob has been added (p. 27). • Section „Outputs reset” has been updated (p. 29). • Section „Starting remote update of the control panel firmware” has been added (p. 38). • Information on the MPB-300 button operating as the MPT-350 keyfob has been added in the „Keyfobs” section (p. 40). • Section „Sirens” has been updated (p. 46).