



**EBS**

CREATING A SENSE OF SECURITY  
SINCE 1989

# **ALARM CONTROL PANEL**

## **CPX230NWB**

User manual

Firmware version: 2.10.0

GPRS transmitter configurator version: 1.4.85.3

OSM server version: 1.3.71.036

## DECLARATION OF COMPLIANCE



We, EBS Sp. z o.o., declare with full responsibility that the present product meets all requirements provided for in the Directive 1999/5/EC of European Parliament and Council dated 9 March 1999. The copy of the "Declaration of Compliance" can be found at <http://www.ebs.pl/en/certificates/>.

### IMPORTANT INFORMATION



Crossed symbol of a trash bin means that at the territory of European Union, the product, after finishing its useful life, shall be disposed of in a separate, specially dedicated collection point. It refers to the equipment itself and its accessories marked with that symbol. The products shall not be disposed of together with non-sortable municipal waste.

The content of the document is presented "as is". The present document shall not be deemed to be providing any warranties, either express or implicit, including but not limited to, any implied warranties of merchantability or fitness for a particular purpose, unless it is required by relevant law. The manufacturer reserves the right to amend the present document or withdraw it any time, without notice.

The manufacturer of the equipment promotes the sustainable development policy. It reserves the right to modify and improve any functions of the product described in the present document without previous notice.

The availability of particular functionalities will depend on the software version of the equipment. Details can be found at the nearest dealer of the equipment.

In no event, the Manufacturer shall be held liable for any loss of data or loss of profits or any specific, incidental, consequential or indirect damages caused in any way.

## MANUFACTURER

EBS Sp. z o.o.  
59 Bronisława Czecha St.  
04-555 Warsaw, POLAND  
E-mail : [sales@ebs.pl](mailto:sales@ebs.pl)  
Technical support: [support@ebs.pl](mailto:support@ebs.pl)  
Webpage : [www.ebs.pl](http://www.ebs.pl)



CREATING A SENSE OF SECURITY  
SINCE 1989

## **CONTENT:**

|  |           |
|--|-----------|
| <b>1. INTRODUCTION.....</b>  | <b>5</b>  |
| <b>2. CONTROL UNIT FUNCTIONS.....</b>  | <b>6</b>  |
| 2.1. FUNCTIONAL CHARACTERISTIC.....  | 6         |
| 2.2. SPECIFICATIONS.....   | 7         |
| <b>3. KEYPAD KP32 SPECIFICATION.....</b>   | <b>8</b>  |
| <b>4. WIRELESS KEYPAD KP2W .....</b>   | <b>12</b> |
| 4.1. TRANSMISSION.....   | 12        |
| 4.2. LED SIGNALLING.....   | 12        |
| 4.3. DESCRIPTION OF KEYPAD ELEMENTS .....  | 13        |
| 4.4. KEYPAD SPECIFICATION.....   | 14        |
| <b>5. REMOTE CONTROL SPECIFICATION.....</b>  | <b>15</b> |
| <b>6. USER CATEGORIES .....</b>  | <b>15</b> |
| <b>7. ARMING THE SYSTEM.....</b>   | <b>16</b> |
| 7.1. ARMING MODES.....   | 16        |
| 7.2. ARMING METHODS.....   | 16        |
| 7.3. ARMING INDICATION ON THE KP32 KEYPAD.....                                       | 16        |
| 7.4. ARMING THE SYSTEM USING THE STANDARD METHOD, WITH MODE AND PARTITION SELECTION. | 16        |
| 7.4.1. ARMING USING A KP32 KEYPAD .....  | 16        |
| 7.4.2. ARMING USING A KP2W KEYPAD .....  | 18        |
| 7.4.3. ARMING FROM THE REMOTE .....  | 18        |
| 7.5. QUICK ARMING WITH MODE AND PARTITION SELECTION.....                             | 18        |
| 7.5.1. ARMING USING A KP32 KEYPAD .....  | 19        |
| 7.5.2. ARMING USING A KP2W KEYPAD .....  | 20        |
| 7.5.3. QUICK SWITCHING OF ARMING MODES WITHOUT CODES FOR KP31 AND KP2W.....          | 20        |
| 7.6. ARMING THE SYSTEM WITH FAULT .....  | 20        |
| <b>8. DISARMING THE SYSTEM.....</b>  | <b>21</b> |
| 8.1. DISARMING THE SYSTEM .....  | 21        |
| 8.1.1. DISARMING USING A KP32 KEYPAD .....   | 21        |
| 8.1.2. DISARMING USING A KP2W KEYPAD .....   | 22        |
| 8.1.3. DISARMING USING THE REMOTE.....   | 22        |
| 8.2. ALARM DISPLAY.....  | 22        |
| 8.3. ALARM MUTE .....  | 23        |
| <b>9. USER FUNCTIONS.....</b>  | <b>24</b> |
| 9.1. ALARMS MEMORY .....   | 25        |
| 9.1.1. HISTORY OF ALARMS FROM TRIGGERED INPUTS .....                                 | 25        |
| 9.1.2. OTHER ALARM HISTORY .....   | 25        |
| 9.2. FAULTS MEMORY .....   | 26        |
| 9.3. BLOCKING INPUTS.....  | 27        |
| 9.4. CURRENT INPUT STATUS .....  | 28        |
| 9.5. FUNCTION CHIME .....  | 28        |
| 9.6. ADDING NEW USERS.....   | 28        |
| 9.7. ARMING ONLY USER (CAN'T DISARM THE SYSTEM).....                                 | 29        |
| 9.8. DELETING USERS.....   | 29        |
| 9.9. CHANGE OF USER CODE.....  | 30        |

|            |                             |           |
|------------|-----------------------------|-----------|
| 9.10.      | PROGRAMMING TIME .....      | 30        |
| 9.11.      | PROGRAMMING DATE .....      | 31        |
| 9.12.      | TESTING THE ZONES .....     | 31        |
| 9.13.      | TESTING THE OUTPUTS .....   | 31        |
| 9.14.      | DURESS CODE .....           | 32        |
| 9.15.      | EMERGENCY BUTTONS.....      | 32        |
| 9.16.      | TEXT MESSAGES .....         | 32        |
| <b>10.</b> | <b>CHANGE HISTORY .....</b> | <b>42</b> |

# 1. INTRODUCTION

Thank you for choosing EBS alarm control panel.

CPX230NWB is a simple, functional alarm control panel integrated with GSM/GPRS/SMS transmitter, intended for small- and medium- sized facilities. The control panel is equipped with 3 outputs and 7 wired (for TEOL configuration up to 14) and up to 32 wireless zones with the possibility to be divided into 2 partitions. Dedicated KP32 LED keypad was designed in a modern, discreet style. Portable size, large, comfortable buttons and simple installation contribute to indisputable advantage of our system.

## 2. CONTROL UNIT FUNCTIONS

### 2.1. FUNCTIONAL CHARACTERISTIC

#### ZONES

- 7 wired zones with the NC / NO / EOL-NC / EOL-NO / DEOL-NC / DEOL-NO / TEOL configuration possibility
- Up to 32 wireless zones
- Detection lines – instant, delayed, 24h burglary, arming/disarming by violation, 24h tamper, interior delay, 24h burglary silent, 24h fire, perimeter, perimeter exit, 24h gas, 24h water leakage, night (bypassed), night with prealarm, arming/disarming by state change

#### PROGRAMMABLE OUTPUTS

- 1 monitored alarm output, high-current (max. current 1.1A)
- 2 monitored alarm outputs, low-current (max. current 50mA)

#### FEEDING OUTPUTS

- 1 signalling device output (max. current 350mA)
- 1 detector output (max. current 350mA)
- 1 keypad output (max. current 100mA)

#### PARTITIONS

- 2 partitions with the possibility to assign any number of zones to each of them

#### KEYPAD

- cooperation with LED KEYPAD KP32
- ability to connect up to three keypads
- cooperation with KEYPAD KP2W
- ability to program up to 32 KP2W keypads (every keypad occupies one of the available wireless zone)

#### REMOTE CONTROL

- cooperation with remote control RC-10
- ability to program up to 32 remote control

#### TRANSMISSION

- Transmission of signals through GPRS/SMS module.
- Encryption of data transfer using AES standard
- Communication with monitoring station using dedicated OSM.Server server that ensures the reliability of data transfer thanks to a redundancy function.
- Control of GSM/GPRS connection – automatic restoration of connection with monitoring station or switching to secondary server

#### CONFIGURATION

- Local, using KP32 keypad or a computer
- Remote through GPRS, SMS or CSD

## USERS

- 1 service code (ATS – Alarm Transmission System is a special type of user, meaning the monitoring station, that is authorized by the main access code to the device)
- 1 installer code
- 1 admin code (main)
- 31 user codes
- Possibility to restrict the scope of authorization to a few codes only

## SYSTEM OPTIONS

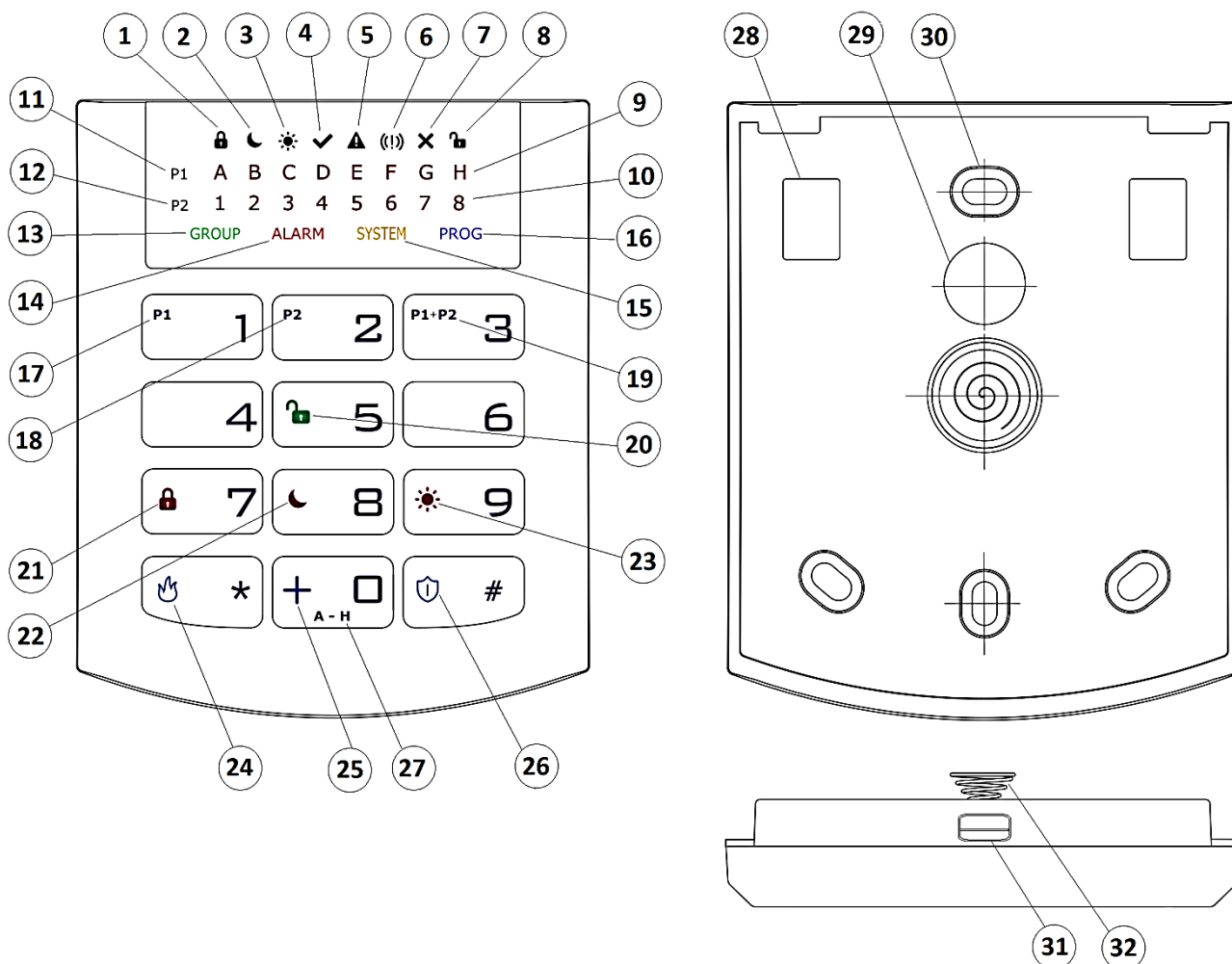
- Automatic diagnosis of basic system components
- Possibility to review faults, alarm memories, event log
- System/technical event history – min. 5000 events

### 2.2. SPECIFICATIONS

|  |   |
|--|---|
| Supply voltage:  | 18VAC (16-20VAC)  |
| Required transformer Power:  | min. 20VA max 60VA  |
| Supported modems:  | * <b>model CPX230NWB-5xx</b> : Cinterion BGS2-W (GSM: 850, 900, 1800, 1900 MHz)<br><br>* <b>model CPX230NWB-6xx</b> : Cinterion EHS6 (UMTS: 800, 850, 900, 1900, 2100 MHz; GSM: 850, 900, 1800, 1900 MHz) |
| Current consumption average/max:<br>(average measured: fully charged battery, established connection with server, connected keypad, no sensors connected)                | 120mA / 180mA @18VAC<br>* Measured with <u>BGS2-W Cinterion</u><br><br>95mA / 170mA @18VAC<br>* Measured with <u>EHS6 Cinterion</u>   |
| Average current consumption; lack of external supply (without keypad/ with keypad):<br>(fully charged battery, established connection with server, no sensors connected) | 60mA / 85mA @13VDC<br>* Measured with <u>BGS2-W Cinterion</u><br><br>35mA / 65mA @13VDC<br>* Measured with <u>EHS6 Cinterion</u>  |
| Charging current:<br>(measured with totalny discharged battrey)  | max. 350mA  |
| Charging voltage:  | 13.8V   |
| Supported bartery type:  | Lead-acid 12V   |
| Low voltage – event treshold:  | 11V   |
| Voltage battery cut off level:   | below 9V  |
| Working temperature:   | -10°C to +55°C  |
| Working humidity:  | 5% to 93%   |
| PCB dimensions:  | 152mm x 78mm x 30mm   |

### 3. KEYPAD KP32 SPECIFICATION

|                              |   |
|------------------------------|---|
| <b>Communication:</b>        | wire  |
| <b>Power supply voltage:</b> | 10 – 13.8 VDC   |
| <b>Power consumption:</b>    | typ. 20 mA, max. 80 mA  |
| <b>Keypad weight:</b>        | 70 g  |
| <b>Size of casing:</b>       | 99 x 82 x 19 mm   |
| <b>Keypad type:</b>          | LED, 16 status LEDs, 4 mode LEDs (GROUP, ALARM, SYSTEM, PROG) |
| <b>Button layout:</b>        | Standard telephone keypad 3 x 4 buttons                       |



Drawing 1. KP32 Keypad

#### 1. **FULLY ARMED mode arming symbol** – indicated with diodes A (partition P1) and 1 (partition P2)








Blinks slowly: exit time countdown

Blinks quickly: entry time countdown

Lit continuously: partition armed in full mode,

Not lit: partition not armed in full mode.



2. **SLEEP Night mode arming symbol**  – indicated with diodes B (partition P1) and 2 (partition P2)
- Blinks slowly: exit time countdown,  
Blinks quickly: entry time countdown,  
Lit continuously: partition armed in sleep mode,  
Not lit: partition not armed in sleep mode.
3. **STAY Day mode arming symbol**  – indicated with diodes C (partition P1) and 3 (partition P2)
- Blinks slowly: exit time countdown,  
Blinks quickly: entry time countdown,  
Lit continuously: partition armed in stay mode,  
Not lit: partition not armed in stay mode.
4. **READY symbol**  – indicated with diodes D (partition P1) and 4 (partition P2)
- Lit when all lines (without the “ignore when arming” option selected) are in nominal condition (not triggered).
5. **Partition input or output sabotage/failure symbol**  – indicated with diodes E (partition P1) and 5 (partition P2)
- Blinks quickly: no longer present, but there were failures/sabotage of inputs or outputs assigned to the partition,  
Lit continuously: there are failures/sabotage of inputs or outputs assigned to the partition.
6. **Partition alarm/alarm memory symbol**  – indicated with diodes F (partition P1) and 6 (partition P2)
- Blinks quickly: no longer present, but there were alerts from lines assigned to the partition,  
Lit continuously: there is an alarm from a line assigned to the partition.
7. **Line bypass symbol**  – indicated with diodes G (partition P1) and 7 (partition P2)
- Lit when at least one line belonging to the partition is locked out (bypassed) by the user.
8. **DISARM Partition disarming symbol**  – indicated with diodes H (partition P1) and 8 (partition P2)
- Lit when the given partition is disarmed, e.g. in DISARM mode.
9. **Diodes A-H (white)**

A row of diodes used to indicate the status of partition P1 (example: when lit, "B" diode means partition P1 is armed in sleep mode).

**10. Diodes 1-8 (white)**

A row of diodes used to indicate the status of partition P2 (example: when lit, "3" diode means partition P2 is armed in stay mode).

**11. Partition 1 ("P1")**

The P1 symbol means partition 1, to which diodes from A to H are assigned.

**12. Partition 2 ("P2")**

The P2 symbol means partition 2, to which diodes from 1 to 8 are assigned.

**13. "GROUP" diode**

When this diode is blinking quickly, it means entering the user function in which either lines or users are shown.

**14. "ALARM" diode**

When this diode is lit, it means a general system alarm (e.g. keypad sabotage, ALARM button on the remote), where:

Blinks: alarm triggered in the past,

Lit continuously: current alarm.

**15. "SYSTEM" diode**

When this diode is lit, it means a system failure, e.g.: power failure, battery failure, ATS connection failure, power output failure, clock loss, keypad sabotage.

Blinks – it means that control panel memory stores failures that have passed,

Lit continuously – there is a failure in the system that has not been repaired,

Not lit – there are no failures in the system.

**16. "PROG" diode**

Blinks slowly – the service function is enabled (a user function),

Blinks – data will be entered,

Lit continuously – installation engineer's service mode is enabled.

**17. Button 1 "P1"**

A function button that supports the arming of partition P1.

**18. Button 2 "P2"**

A function button that supports the arming of partition P2.

**19. Button 3 "P1+P2"**

A function button that supports simultaneous arming of partitions P1 and P2.

**20. Button 5 (open padlock)**

A function button that supports disarming.

**21. Button 7** (locked padlock)

A function button that supports the arming in full mode.

**22. Button 8** (moon)

A function button that supports the arming in sleep mode.

**23. Button 9** (sun)

A function button that supports the arming in stay mode.

**24. Button "\*" (flame)**

FIRE function button - pressing for about 3 sec generate a fire alarm.

**25. Button 0 "+"**

HELP function button - pressing for about 3 sec generate a medic alarm.

**26. Button "#"** (shield)

BURGLARY function button - pressing for about 3 sec generate a panic alarm.

**27. Button 0 (A - H)**

A function button which enables switching between groups.

**28. Screw connectors**

Connectors for connecting cables leading from keypads to the alarm control.

**29. Cable entry hole**

A place for inserting connection cables.

**30. Installation holes**

The keypad has four oval installation holes for proper mounting of the keypad.

**31. Casing opening latch**

It is recommended to use a 2.5 - 5 mm flat screwdriver for opening the casing. Slide it lightly into the indicated hole and make a slight leverage movement towards the back of the casing.

**32. Sabotage switch**




After installing the keypad, the contact of this switch is closed. Unauthorized keypad removal will result in sending a signal to the alarm control. A spring is mounted on the switch lever to compensate for uneven surfaces.

## 4. WIRELESS KEYPAD KP2W

The wireless keypad KP2W is intended as a secondary keypad. It allows only to:

- arm/disarm the system in a full and circuital mode
- activation of attack, fire and medical alarm analogically as for main keypad operation.

Keep in mind, that the wireless keypad KP2W uses one-way transmission and cannot receive communication from the control panel.



The keypad KP2W is equipped with keys marked with numbers **0** to **9** and function keys  and  and .

After pressing any key, the keypad is backlit.

### 4.1. TRANSMISSION

The transmission is signaled by blinking of the blue transmission LED located in the lower right corner of the display. This means that the information is send to the alarm control panel.

The keypad transmits the entered characters as soon as any of the following conditions is met:

- a) key  or  is pressed
- b) 8 keys are pressed
- c) after 3 seconds of pressing the last key

### 4.2. LED SIGNALLING

The keypad KP2W is equipped with two LEDs that inform about low battery and sending a radio transmission.

The low battery is signalled by showing a red battery symbol in the upper left corner of the display:



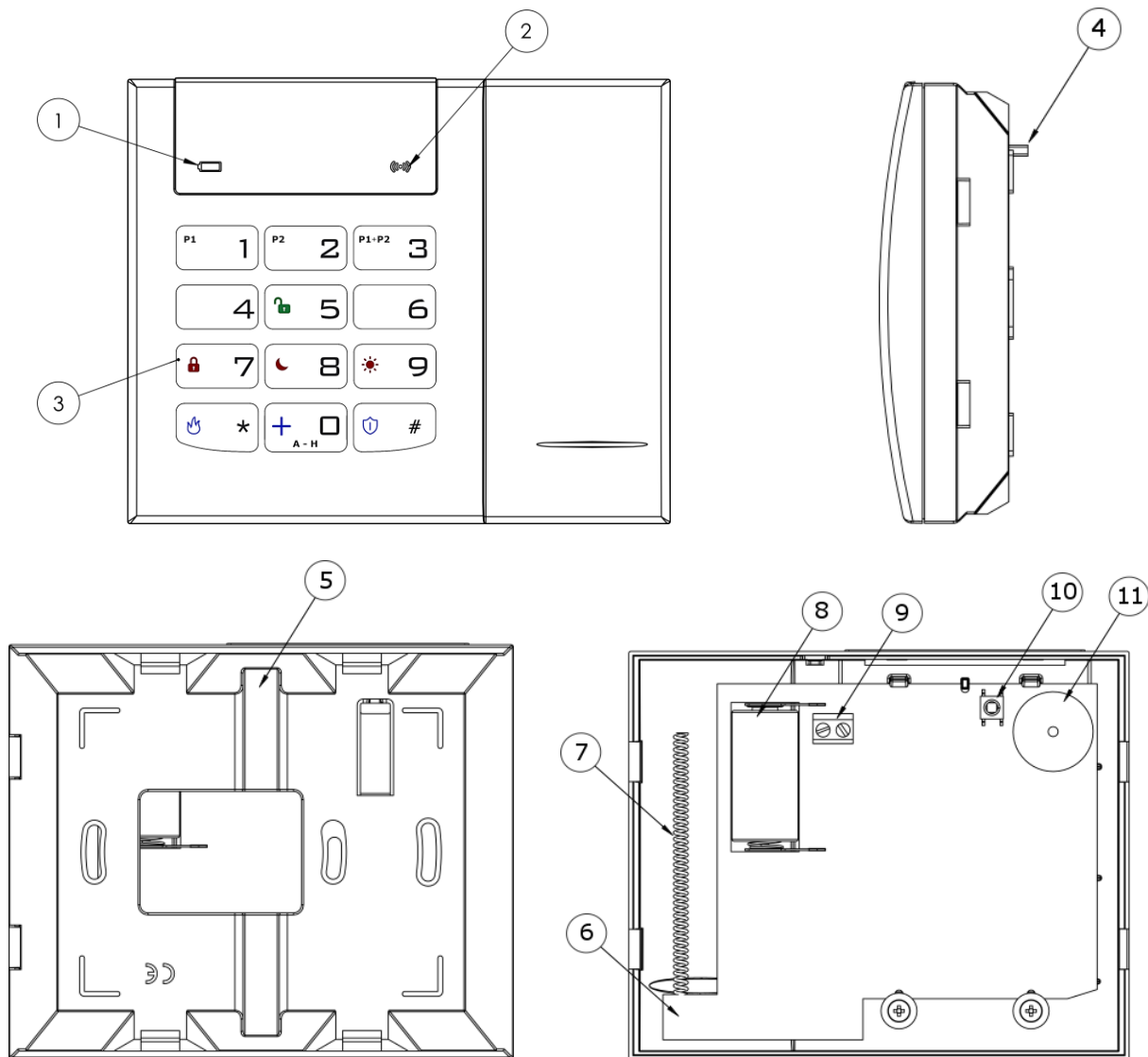
After such icon appears, the battery should be replaced as soon as possible.

Each user-called keypad transmission to the system is signalled by the LED in the lower right corner of the keypad display:



Displaying this symbol during operation means sending data to the alarm control panel and is a normal and desired device operation.

### 4.3. DESCRIPTION OF KEYPAD ELEMENTS



**Drawing 1. KP2W Keypad**

#### **1. Low battery LED (RED)**

On – battery is low,

Off – battery O.K.

#### **2. Data transmission LED (BLUE)**

Blinks – data transmission in progress

Off – no data transmission

#### **3. Keypad buttons**

Buttons on the KP2W keypad function the same as on the KP32 keypad (see section 3 KEYPAD KP32 SPECIFICATION - points 17 to 27). After first pressing any button, the keypad is backlit. After a few-second idle time, backlight gets automatically dimmed.

#### **4. Anti-sabotage switch**

After the keypad is assembled the switch contact is closed. Unauthorized disassembly of the keypad will send the message to the alarm control panel.

**5. Canal for wires**

**6. Mainboard**

**7. Antenna**

**8. Battery**

Lithium Battery CR123A 3V.

**9. Screw Connector**

Connector for wired magnet contact – open door switch. Keep closed if not used.

**10. Sabotage sensor (tamper)**

**11. Buzzer**

|                                  |
|----------------------------------|
| <b>4.4. KEYPAD SPECIFICATION</b> |
|----------------------------------|





|                                    |                       |
|------------------------------------|-----------------------|
| <b>Power supply:</b>               | 1 battery CR123A 3V   |
| <b>Working time:</b>               | 3 years*              |
| <b>Frequency of operation</b>      | 433,92 MHz            |
| <b>Communication range</b>         | up to 500m (open air) |
| <b>Communication</b>               | one way               |
| <b>Average current consumption</b> | 30 µA                 |
| <b>Operation temperature</b>       | -10 °C +55 °C         |
| <b>Alarm inputs</b>                | 1, NC type            |
| <b>Dimensions</b>                  | 125 x 102 x 33 mm     |
| <b>Wight without battery</b>       | 150 g                 |

\*Working conditions: test transmission every 15 minutes, keypad use (arming/disarming) 2 times a day, open door switch closed, working temperature 20°C

## 5. REMOTE CONTROL SPECIFICATION

|                           |                            |
|---------------------------|----------------------------|
| <b>Frequency:</b>         | 433,92MHz                  |
| <b>Coding:</b>            | Code hopping               |
| <b>Number of buttons:</b> | 4                          |
| <b>Batteries:</b>         | 2 x lithium 3V type CR2016 |



-  – ARM button
-  – DISARM button
-  – SILENT ALARM button
-  – ALARM button

**Note! The above shows the recommended settings for remote buttons. During the control panel configuration stage, it is possible to freely assign functions to individual buttons!**

## 6. USER CATEGORIES

Due to the different level of access to the functionality of the system, there are three user categories:

1. Administrator – the user with the highest access level. They can both arm, and disarm the system, as well as access and make changes in all user functions presented in chapter 9 User's Functions and its subsections. The Admin is an A1 user and their rights can't be changed.
2. Regular user – a user who can arm and disarm the system and has access to the history of alarms and failures, the status of inputs, and can block inputs, change their code, test inputs and outputs.
3. Arming only – a user who can only arm the system. They do not have access to functions that require a code. If the option "Access to history requires authorisation" has not been enabled during the set-up, this user can enter the functions to which this option applies (see chapter 9).

## 7. ARMING THE SYSTEM

### 7.1. ARMING MODES

Each partition can be armed in one of the following modes:

- Stay - arming partitions in this mode results in only perimeter and perimeter output lines reacting to triggering.
- Sleep - arming partitions in this mode means that night lines do not activate alarms when triggered.
- Fully armed – partition is armed and violation of any zone will cause an alarm.

The user can select the arming mode or allow the system to make this decision independently.






**Note: If no zone and/or output is assigned to the partition, the partition will not be armed.**

### 7.2. ARMING METHODS

- standard – requiring authorisation with the user's code, which is active always, without the need for additional configuration when setting up the control panel,
- quick (so called *quick arming*) – arming the system or its part without the need for code authorisation, which can be additionally defined when configuring the control panel,
- immediately – **applies only to arming by the remote control**. If during the configuration of the remote control, the "arm immediately" function was assigned to the any button, pressing this button will fully arm immediately (omitting time for exit).

### 7.3. ARMING INDICATION ON THE KP32 KEYPAD

System arming is indicated by lighting up appropriate diodes below the arming mode symbols. Diodes being lit below the  symbol means full arming, the  symbol means sleep arming, and the  symbol means stay arming. Diodes in the first row (A-H) indicate the status of partition P1, diodes in the second row (1-8) indicate the status of partition P2.


### 7.4. ARMING THE SYSTEM USING THE STANDARD METHOD, WITH MODE AND PARTITION SELECTION

#### 7.4.1. Arming using a KP32 keypad

##### 7.4.1.1. Fully armed mode



**Note: When the correct code and appropriate button sequence are entered, the keypad will always generate a triple tone.**

**When an incorrect code is entered, the keypad will generate a long continuous sound. Press \*, and then enter the correct code.**

**If the keypad rejects the correct code (continuous long sound), also**



press , to delete previously entered data, and then re-enter the correct code.

In order to arm the system in fully armed mode, enter one of the following sequences:

1. Arming all partitions:

   # <user code> or      # <user code> or

<user code> <-here, the system will be armed in full mode in two cases:

- a) If perimeter output lines are assigned and they are triggered during the exit time countdown.
- b) If no perimeter output lines are assigned.

2. Arming only the first partition P1:

     # <user code>

3. Arming only the second partition P2:

     # <user code>

When the correct code is entered the keypad will generate a triple tone and then the system will be armed at once or after the exit time passes.

#### 7.4.1.2. Sleep mode

Arming partitions in sleep mode is sensible when the partition has at least one night line assigned (whether switched off during the night or delayed). In order to arm a partition in sleep mode, enter one of the following sequences:

1. Arming all partitions:

   # <user code> or      # <user code>

2. Arming only the first partition P1:

     # <user code>

3. Arming only the second partition P2:

     # <user code>

#### 7.4.1.3. Stay mode

Arming partitions in stay mode is possible only when they have perimeter lines assigned. If not, the system will reject arming attempts, which will be indicated by the keypad with a continuous, several seconds-long sound.

The system will be armed in stay mode when one of the following sequences is entered:

1. Arming all partitions:

9 # <user code> or 3 9 # <user code> or

<user code> <- in this case, partitions will be armed in stay mode only if the partitions has at least one perimeter exit assigned to them and it is not triggered during exit time countdown (if a trigger occurs, the system will switch to full mode).

Arming only the first partition P1:

1 9 # <user code>

2. Arming only the second partition P2:

2 9 # <user code>

### 7.4.2. Arming using a KP2W keypad

**Arming with KP2W keypads is done exactly the same way as with KP32, but pressing # after entering the code speeds up sending the information to the control panel by about 2 - 3 seconds.**



**Note:** The KP2W keypad has no ability of indicating arming, disarming or entering an incorrect code by sound. Arming and disarming of the system may be indicated by main signaller chirp (if active). Armed – once, disarmed – twice. Full system status indication is available with KP32 keypads.

### 7.4.3. Arming from the remote control

Press the remote button marked with the locked padlock symbol , assigned to the system arming function (**NOTE: it is assumed that during configuration of the remote control, arming was assigned to the locked padlock button, as the central enables assigning remote buttons to various functions; it is possible to configure arming with a different button.**). If exit time has been selected, the keypad will confirm arming by blinking diodes A (partition P1) and/or 1 (partition P2) below the locked padlock symbol on the glass. Diodes lit permanently mean the system is armed in full mode.

Arming using the remote always arms partitions in full mode, even if a partition has perimeter lines assigned.

## 7.5. QUICK ARMING WITH MODE AND PARTITION SELECTION

If the installation engineer enabled the "Allow quick arming without user authorisation" option during configuration, then so called quick arming is available, which does not require entering the access code.

## 7.5.1. Arming using a KP32 keypad

### 7.5.1.1. Quick arming of all partitions

To arm all partitions without entering the code, three button combinations can be used. The table below shows methods for quick arming of all partitions, including modes in which the control panel is to be armed.

|  |  |   |
|--|--|---|
| <ul style="list-style-type: none"> <li>• <b>FULLY ARMED MODE</b><br/> </li> <li>• <b>SLEEP MODE</b><br/> </li> <li>• <b>STAY MODE</b><br/> </li> </ul> | <ul style="list-style-type: none"> <li>• <b>FULLY ARMED MODE</b><br/> </li> <li>• <b>SLEEP MODE</b><br/> </li> <li>• <b>STAY MODE</b><br/> </li> </ul> | <ul style="list-style-type: none"> <li>• <b>FULL MODE</b><br/> </li> <li>• <b>SLEEP MODE</b><br/> </li> <li>• <b>STAY MODE</b><br/> </li> </ul> |
|--|--|---|

### 7.5.1.2. Quick arming with partition selection

To arm the selected partitions without entering the code, three button combinations can be used. The table below shows methods for quick arming of selected partitions, including modes in which the control panel is to be armed.

| <u>Quick arming of partition P1, with mode selection</u>   |  | <u>Quick arming of partition P2, with mode selection</u>   |  |
|--|--|--|--|
| <ul style="list-style-type: none"> <li>• <b>FULLY ARMED MODE</b><br/> </li> <li>• <b>SLEEP MODE</b><br/> </li> <li>• <b>STAY MODE</b><br/> </li> </ul> | <ul style="list-style-type: none"> <li>• <b>FULLY ARMED MODE</b><br/> </li> <li>• <b>SLEEP MODE</b><br/> </li> <li>• <b>STAY MODE</b><br/> </li> </ul> | <ul style="list-style-type: none"> <li>• <b>FULLY ARMED MODE</b><br/> </li> <li>• <b>SLEEP MODE</b><br/> </li> <li>• <b>STAY MODE</b><br/> </li> </ul> | <ul style="list-style-type: none"> <li>• <b>FULLY ARMED MODE</b><br/> </li> <li>• <b>SLEEP MODE</b><br/> </li> <li>• <b>STAY MODE</b><br/> </li> </ul> |

## 7.5.2. Arming using a KP2W keypad

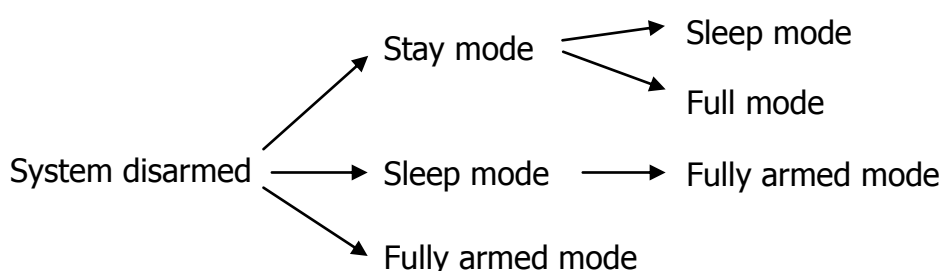
**Arming with KP2W keypads is done exactly the same way as with KP32!**



**Note:** The KP2W keypad has no ability of indicating arming, disarming or entering an incorrect code by sound. Arming and disarming of the system may be indicated by main signaller chirp (if active). Armed – once, disarmed – twice. Full system status indication is available with KP32 keypads.



## 7.5.3. Quick switching of arming modes without codes for KP31 and KP2W

It is possible to change the system arming mode without entering the code and disarming first, in the following order:



**Note:** This only works in the order shown, never in reverse! Partial or complete disarming of any part of the system is only possible using the sequence where the code is entered.

## 7.6. ARMING THE SYSTEM WITH FAULT

If the installation engineer enabled the *"Request arming confirmation (by pressing #) in case of a failure"* option, and failures occur during any arming (regardless of the method or mode), the KP32 keypad will indicate this fact by blinking the ALARM and SYSTEM diodes and a long sound signal. Additionally, lit diodes 1 to 8 will indicate system errors. This condition will last for 10 seconds. If failures cannot be repaired quickly, press  to arm the system. Pressing  will cancel arming.



**Note:** Remove the causes of faults as soon as possible.

### Error codes:

- 1 – Damage or disruption of detector
- 2 – Damage of signalling device or signalling device active
- 3 – Damage of internal connection or sabotage
- 4 – AC power supply damage
- 5 – Battery damage

- 6 – ATS damage
- 8 – Other damages






**Note! Faults in the system do not prevent arming via remote control, KP2W keypad and via text messages (SMS).**

## 8. DISARMING THE SYSTEM

Disarming the system can be carried out by those users, whose rights have not been restricted (administrator, regular user – see chapter 6 User Categories). The so-called unauthorised users can only arm the system.






### 8.1. DISARMING THE SYSTEM


#### 8.1.1. Disarming using a KP32 keypad

Diodes being lit below the  symbol means full arming, the  symbol means sleep arming, and the  symbol means stay arming. Diodes in the first row (A-H) indicate partition P1, diodes in the second row (1-8) indicate partition P2. When a detector at an input to the building is triggered, the keypad will emit an interrupted sound – the entry delay time. Additionally, the corresponding diode will begin to blink, depending on which partition the triggered spot was assigned to, and which mode the system armed in (e.g. blinking of diode 2 means that a detector assigned to partition two was triggered, and the system is armed in sleep mode). Disarm the system during the entry countdown time in order not to trigger an alarm.

##### 8.1.1.1. Disarming all partitions

In order to disarm all partitions, the given user needs to have access to them. Otherwise, only the partition which the user has access to will be disarmed. Below are shown three button combinations enabling the entire system to be disarmed:





1. <user code>
2.  5  # <user code>
3.  3  5  # <user code>

The keypad will generate a 3-tone sound to confirm the correct code. If chirps are active, disarming will also be confirmed by two chirps of the indicator. When the system is disarmed, alarm is also muted (disabled), and diodes H and 8 on the keypad below the  symbol are lit.

##### 8.1.1.2. Disarming with partition selection


In order to disarm the given partition, the given user needs to have access to it:


1.  1  5  # <user code> <- disarming first partition P1

2.     <user code> <- disarming second partition P2


The keypad will generate a 3-tone sound to confirm the correct code. If chirps are active, disarming will also be confirmed by two chirps of the indicator.  
When the system is disarmed, alarm is also muted (disabled).



**Note: If an incorrect code is entered, the keypad will generate a long continuous sound. Press , and then enter the correct code. When the correct code and appropriate button sequence are entered, the keypad will always generate a triple tone.**

If the keypad rejects the correct code (continuous long sound), also press , to delete previously entered data, and then re-enter the correct code.


### 8.1.2. Disarming using a KP2W keypad

**Disarming with KP2W keypads is done exactly the same way as with KP32, but pressing  after entering the code speeds up sending the information to the control panel by about 2 - 3 seconds.**




**Note: the keypad does not indicate entering correct or incorrect codes**

### 8.1.3. Disarming using the remote


Press the remote button marked with the open padlock symbol , assigned to the system disarming function (**NOTE: it is assumed that during configuration of the remote, disarming was assigned to the open padlock button, as the central enables assigning remote buttons to various functions; it is possible to configure disarming with a different button.**)

The keypad will confirm system disarming by switching off diodes A (if only partition P1 was armed) or 1 (if only partition P2 was armed), or both at once (if both partitions were armed) below the locked padlock symbol on the glass. In turn, diodes H and 8 below the open padlock symbol will light. If chirps are active, disarming will also be confirmed by two chirps of the indicator.

## 8.2. ALARM DISPLAY

Blinking of diodes F and/or 6 below the symbol  (and/or diode ALARM if the alarm was triggered in the system by another source than input line e.g keypad sabotage, trigger from remotes) means that an alarm was triggered while you were absent. If diodes F and/or 6 (or ALARM, see above bracket) are lit continuously, it means that the system is still in alarm condition. Tread carefully! If you suspect an intruder is still on site, leave immediately and call security.



### 8.3. ALARM MUTE

1. To mute (deactivate) the alarm, enter the code and press  3 beeps will confirm the code. Also, the system will be disarmed.
2. In order to identify the alarm type, please refer to 9.1 Alarms memory chapter of the present manual.

## 9. USER FUNCTIONS



**Note: The following operations can be performed only using the main keypad KP32.**

If the option "Access to alarm and fault memory requires authorisation" is not enabled during configuration, then you access the functions showing the alarm and failure history and current input status without entering the user code. If the option is enabled, then after , enter the code and confirm by pressing  when accessing alarm and failure history.

Additionally, if the option "After disarming disable alarm history notification" is enabled and is defined the delay time turning off present historical alarm, then after disarming the system (partition), past alarms from zones assigned to partition (F diode blinking - partition 1, 6 diode - partition 2), after assigned delay time, will cease to be shown on the keypad (diodes will turn off). The user will retain access to state of the alarm memory from inputs, by entering the 3# function, until he chooses to delete it. If the system is armed, and the alarm caused by any 24-hour zone will occur, then the fault memory can be turned off by arming and disarming the system (if this option is checked) or by entering the 3# keypad function and deleting the memory.

The CPX230NWB has a group display feature - A, B, C, D for input lines (detectors):

- display of triggered inputs,
- display of faults memory,
- blocking inputs
- testing inputs,
- enabled/disabled function chime

and users:

- adding/deleting users.

There are 8 numbers in every group - 32 in total. Table below shows circuit names inputs/users and their corresponding numbers:


| Name | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | D1 | D2 | D3 | D4 | D5 | D6 | D7 | D8 |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| No.  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |





## 9.1. ALARMS MEMORY

### 9.1.1. History of alarms from triggered inputs


  - Show triggered inputs



This function shows the history of alarms that were triggered in the armed system. After activating the function, diodes GROUP and PROG blink slowly, and alarms since the last arming are shown. Blinking of group A diodes means that it is currently being shown. Continuously lit diodes of the other groups (B, C and/or D) mean that inputs assigned to them were triggered. Diodes switched off means that no triggering has occurred in the given group. Switch between groups using the  button.

The bottom row (diodes 1 to 8) shows information on which inputs specifically triggered the alarms (diodes continuously lit) and which did not (diodes off). Pressing  deletes the alarm memory. Pressing  exits without deleting the alarm memory.

### 9.1.2. Other alarm history

If no diode is lit in the alarm history, but the ALARM diode continues to blink, it means that an alarm was triggered in the system by another source than an entry line. You can access the *Other alarm* history by entering from the main menu:

   - Show other alarms

When the function is activated, diodes ALARM and PROG blink slowly, while LEDs 1 to 8 show the type of the alarm source. Pressing the button corresponding to the blinking/continuously lit LED provides information on the alarm source within the group. Pressing  returns you to the main menu without deleting the alarm memory, while  exits and deletes the memory.

**If:**

**Diode 2 is lit** – keypads were sabotaged. After pressing button 2, diodes will be lit to indicate which keypads were sabotaged:

- 1 – Keypad tamper 1
- 2 – Keypad tamper 2
- 3 – Keypad tamper 3

**Diode 3 is lit** – an alarm button was used. After pressing button 3, diodes will be lit to indicate which button was used:


- 1 – Fire alarm activated
- 2 – Help alarm activated



**Diode 4 is lit** – trigger from remotes



**Note: Alarm history is also deleted when the system is armed.**


## 9.2. FAULTS MEMORY


 - Show faults memory


The function shows failures that are present in the system. When it is activated, diodes SYSTEM and PROG blink slowly. LEDs 1 to 8 show failures that occurred but are no longer present, which is indicated by diode blinking, or which are currently present in the system, and in this case the diodes are continuously lit. Pressing  deletes the failure memory. Pressing  exits without deleting the failure memory.

### Faults description:

#### 1 – Sabotage of zones

Pressing the  button shows the numbers of inputs with active sabotage.

Blinking of group A diodes means that it is currently being shown. Continuously lit diodes of the other groups (B, C and/or D) mean that inputs assigned to them are sabotaged. Diodes switched off means there is no sabotage in the given group. Switch between groups using the  button.

To return to the main failure branch, press .


#### 2 – Fault of outputs 1 - 3

To display more detailed information about fault of outputs, press  button.


1 – Fault of output 1

2 – Fault of output 2

3 – Fault of output 3

To return to the main fault menu, press .


#### 3 – Fault of feeding outputs

To display more detailed information about fault of feeding outputs, press  button.

1 – Fault of feeding output + KP

2 – Fault of feeding output +AUX1

3 – Fault of feeding output +AUX2


To return to the main fault menu, press .

#### 4 – AC fault

#### 5 – Battery fault

#### 6 – ATS fault

#### 7 – Other damages

Pressing  button shows other damage that has occurred:



1 – Clock fault

2 – Fault of control panel settings



3 – *Keypads tamper*

Pressing the  button shows information on the numbers of wired keypads with active sabotage.

#### 4 – Low battery level in wireless detectors

Pressing the  button shows the numbers of wireless detectors that indicate low battery levels. Blinking of group A diodes means that it is currently being shown. Continuously lit diodes of the other groups (B, C and/or D) mean that detectors assigned to them have low battery levels. Diodes switched off mean that all detectors in the given group have sufficient battery levels. Switch between groups using the  button.

#### 5 – Wireless detector signal lost





Pressing the  button shows the numbers of wireless detectors which have lost contact with the central. Blinking of group A diodes means that it is currently being shown. Continuously lit diodes of the other groups (B, C and/or D) mean that detectors assigned to them have lost contact with the central. Diodes switched off mean that no detector in the group has problems with communication. Switch between groups using the  button.

To return to the main failure branch, press .

### 9.3. BLOCKING INPUTS




The zone blocking function allows de-activating stand-by mode of any zones or bypassing any damaged lines. Also, zones which are not in stand-by mode and which the user has access to can be blocked. Zones remain blocked until de-arming. System informs the user about that fact with quickly flashing LED marked with the number of the blocked zone.


#### Zone blocking:

1. Enter the function number   and confirm with . Next, enter the user code and press . A correct code will be confirmed with a 3-tone sound signal.




**Note: When an incorrect code is entered, the keypad will generate a long continuous sound. Enter the correct code again.**

2. When function activation is confirmed, diodes GROUP and PROG, and the diode assigned to group A will blink. Select the inputs to be blocked using buttons 1 to 8, switch to other groups (B, C or D - 8 inputs in each) using . Pressing number buttons changes input block status (diodes with the numbers of their corresponding inputs will switch on/off). Confirm blocking the selected inputs with the  button. The change will be confirmed with a triple tone. In order to cancel the change, press the  button.



After this procedure, the G and/or 7 LEDs below the symbol  will light up, depending on partition which the blocked zones are assigned.

## 9.4. CURRENT INPUT STATUS

If the user notices that diodes D and/or 4 below the indicator  are switched off, then the function showing the actual status of inputs can be used to see which detectors are triggered or sabotaged.





– Showing the actual status of inputs

Blinking of diodes belonging to a group means that it is currently being shown. Continuously lit diodes of other groups mean that detectors assigned to them have been triggered or sabotaged. Diodes switched off mean that no detector in the group has been triggered or sabotaged. Switch between groups using the  button. Pressing  exits the function.

## 9.5. FUNCTION CHIME

The function "Chime" allows to inform the person in the room about violation of the input zones (e.g. opening or closing the entrance door). When the system is disarmed and 'chime zone' is violated, all wired keypads make a beep sound. No report is sent to the monitoring station. It can be enabled/disabled by enter:



Blinking of diode belonging to a group (from A to D) means that it is currently being shown. To enable/disable the chime for the selected line, press the appropriated key (numbers from 1 to 8). Enable this function will be signalled by the lit chosen number, disable by switched off diode. Switch between groups using the  button. Pressing  exits the function.

Time of saving parameters depends on the number of lines that have been changed. More changes means longer save.





## 9.6. ADDING NEW USERS







The function adds the code of a new user. The code can only be added by the administrator. Default administrator code: 1111.



**Note: The individual code must not be identical. If one code duplicates another or is a code under duress by another user (the last digit of the code increases, i.e. for the code 2345, for example, a code under duress is 2346), it will not be saved, which the keypad will indicate with a continuous, several-second sound.**

**To add a new user:**


1. Enter the function    <administrator code> . A correctly entered code will be confirmed with a triple tone.

2. Added users will be shown (diodes from A to D - groups to which the numbers from 1 to 8 are assigned). The currently shown group will be indicated by blinking of the corresponding diode (A-D). A continuously lit number within a group means that the given user already exists. Other groups where users are assigned will be continuously lit. An unlit group means that there are no users assigned there. Switch between groups using the  button.
3. Select a user number in the group you have selected (group A, B, C or D, numbers from 1 to 8), different than one that has already been added. The selected number will start blinking, press  to confirm.
4. Partition numbers to which the new user can have access to are indicated. Pressing 1 or 2 turns the diode of the corresponding partition on or off. Once access is configured,  to confirm. All diodes should be off now.
5. Enter the code of the newly added user (from 4 to 7 digits, depending on the defined length) and confirm with .
6. Re-enter the code of the newly added user and press  to complete adding, or  to exit without saving changes.
7. If the user has been added correctly, you will hear a triple confirmation tone, otherwise you will hear a continuous signal.

## 9.7. ARMING ONLY USER (CAN'T DISARM THE SYSTEM)

This function disables the ability of selected users to disarm the system. After enabling this option, users will be able to arm the control panel only. You have to enter:

   **<administrator code>** 

Users whose rights to disarm have been removed will be displayed (diodes from A to D – groups to which the numbers from 1 to 8 are assigned). The currently shown group will be indicated by blinking of the corresponding diode (A, B, C or D). A continuously lit number (1–8) within a group means that a user without the right to disarm already exists. Other groups with users of this type will be continuously lit. An unlit group means that there are no users without the right to disarm. Pressing button 1–8 on the keypad activates (diode goes on) or disables (diode goes off) option for the existing user. For a non-existent user, pressing the button will not switch on the diode. Switch between groups using the  button.

**Note: The function can be enabled/disabled for existing users in the system.**








## 9.8. DELETING USERS

The function deletes user codes. Codes can only be deleted by the administrator. A correctly entered function will be confirmed with a triple tone. Default administrator code: 1111.



**Note: The Administrator account (user A1) may not be deleted.**

### To delete a user:

1. Enter the function    # <administrator code>  #. A correctly entered code will be confirmed with a triple tone.
2. Added users will be shown (diodes from A to D - groups to which the numbers from 1 to 8 are assigned). The currently shown group will be indicated by blinking of the corresponding diode (A-D). A continuously lit number within a group means that the given user exists. Other groups where users are assigned will be continuously lit. An unlit group means that there are no users assigned there. Switch between groups using the  button.
3. Enter the number of the user to be deleted within your selected group (group A, B, C or D, numbers from 1 to 8; the number will start blinking) and press  # to confirm or  \* to exit without saving changes.
4. If the user has been deleted correctly, you will hear a triple confirmation tone, otherwise you will hear a continuous signal.

## 9.9. CHANGE OF USER CODE

The user can change its code here. 3 beeps will confirm the successfully entered function.

 7   # <User code>  # <Code>  # <Code>  #

where:

**User code** – Code of a user changing the password

**Code** – New access code (from 4 to 7 digits)

In any moment you can press  # to exit without saving changes.

## 9.10. PROGRAMMING TIME

You can change system time here. Time can be changed by the administrator only. 3 beeps will confirm the successfully entered function. Default admin code: 1111.

 6   # <Administrator code>  # <hh> <mm>  #

where:

**hh** – Hours

**mm** – Minutes

In any moment you can press  \* to exit without saving changes.

## 9.11. PROGRAMMING DATE

You can change system date here. Date can be changed by the administrator only. 3 beeps will confirm the successfully entered function. Default admin code: 1111.

    <Administrator code>  <YY> <MM> DD &img alt="Keypad button # with lock icon" data-bbox="796 138 850 158"/>

where:

**YY** – Year






**MM** – Month

**DD** – Day


In any moment you can press  to exit without saving changes.

## 9.12. TESTING THE ZONES

The function allow user to test zones and detectors connected to zones input.

   <User code>  <Duration of test> 

*Duration of test* is the time in minutes after which the test will be finished and the system will return to the main menu. The default time is 10 minutes and so it will be set if the user skips entering the time from the keypad or enters 0.





When this function is activated, diodes of groups A, B, C and D will be lit on the keypad, together with their corresponding inputs (1 to 8). A blinking diode by the given group indicates that inputs belonging to this group are shown, although these are the inputs assigned to the partition which the user who entered the code has access to. Diodes switch off when the corresponding detector is triggered. By pressing the  button, the user can switch between groups and check which inputs from the given group have been triggered.

Example of use: the tester sets the time that is sufficient to walk around the protected building. Then, by walking around they trigger the detectors (when detector is triggered, the diode on the keypad with the number assigned to the detector should go on). After returning to the wired keypad, it is visible, which detectors have worked correctly – diodes that are off (activated B5 detector – diode 5 in the B group should be off); and which are damaged (or they have not been activated properly) – diodes that are on

To exit the testing function press  or .

## 9.13. TESTING THE OUTPUTS

The function allow user to test outputs and alarm siren connected to the outputs.

   < User code > 

After activation this function, LEDs 1 - 3 display the outputs used in the system. Only outputs defined as "alarm" type and belong to the user's partitions are presented. Pressing the key (1-3) activates relevant output (like an alarm), but not reporting the event to the

monitoring station. Thus the siren or other signalling devices can be checked. Repeated pressing the key, disables the output.

To exit the testing function press  or  .

## 9.14. DURESS CODE

Duress code is used to inform the monitoring station about a distress event. Each user has his own duress code. User's duress code is his standard code with last digit increased by one. If the last digit is 9 it should be changed to 0. Example:

User's code is 3446, his duress code is 3447

User's code is 3449, his duress code is 3440

Whenever duress code is input, distress event will be sent. It can be used in every command that requires user authorization, i.e. arming/disarming and every system option that requires user code, like partition state checking.

Duress code is disabled by default. It can be enabled by the installer or by the configuration program.

## 9.15. EMERGENCY BUTTONS

The keypad of CPX230NWB has 3 function keys. Pressing and holding for 3 seconds one of these keys will generate an alarm corresponding to the key:



– Fire alarm, activating the fire alarm



– Help alarm, activating the medical alarm



– Panic alarm, activating the break-in alarm

**Note** – for the emergency buttons to work, it is necessary to be in arm/disarm ready mode and wait at least 10 seconds since last 0-9 key press. You can also press '\*' key to clear keypad buffer and use emergency button after that without any delay.

**Fire alarm** – when activated it is signalled on a keypad with all digits blinking slow (first row) and fast (second row). Enter and confirm any user code to deactivate it.

**Help alarm** – when activated it is signal on a keypad with the ALARM led blinking.

**Panic alarm** – not signaled on a keypad.

Every emergency alarm generates an event that can be send to the monitoring station. Events configuration is set by the installer.

## 9.16. TEXT MESSAGES

CPX230NWB Alarm Control Panel can be managed by text messages. User can use a variety of texts that can be send to the device in order to configure it or poll its status. For SMS to be accepted, the phone number from which the text is being send, has to be enlisted on the allowed numbers list. CPX230NWB can store up to 10 phone numbers and up to 32 text messages. If, for any reason, the SMS can not be send at the moment, it will be send as soon as the connection with the GSM network is re-established but not later than 1 day after the occurrence of the event triggering SMS send request (text messages get expired



and are deleted). Message should contain only characters from English alphabet. Furthermore, if the text contains any spaces, content of the message, starting from the equation mark (=) till the end of the message, should be enclosed in quotes (" ").

**Descriptions of messages handled by the unit are listed below.**

**Note:** Some components of commands are given in square brackets [...]. This means that they are optional fields.

| <b>Acquiring the state of partitions</b> |  |
|--|--|
| Command syntax                           | XXXX GETARMED  |
| Command description                      | <p>Acquiring the information which partitions are armed/disarmed</p> <p>XXXX – admin code</p> <p><i>Example: 1234 GETARMED</i></p>   |
| Feedback message description             | <p>PARTITION1:X, PARTITION2:Y - Information about partitions arm/disarm state.</p> <p>PARTITION1,PARTITION2 – default partitions names, they can be changed with the SETNAME command</p> <p>X,Y – partition states, possible values:</p> <p>0 – disarmed</p> <p>1 – armed</p> <p>GETARMED:ERROR – command rejected by the system</p> |

| <b>Setting the name of partition, zone, outputs, users and system</b> |   |
|---|---|
| Command syntax  | XXXX SETNAME=ELEMENT,[NR],VALUE_without_spaces<br>XXXX SETNAME="ELEMENT,[NR],VALUE_with_spaces"   |
| Command description   | <p>Setting the name (position VALUE) for the item (a value items below) number nr.</p> <p>XXXX – admin code</p> <p>Possible values position ELEMENT:</p> <p>PARTITION - Setting the name of partition; numbers 1 and 2</p> <p>ZONE - Setting the name of input line unit corresponding to the indicated number; the numbers from 1 to 32</p> <p>OUTPUT - Setting the name of output corresponding to the indicated number; the numbers from 1 to 3</p> <p>USER - Setting the name of user with the specified number; the numbers from 1 to 32</p> <p>SYSTEM - Setting the name of object which panel and alarm system were installed. Note: here position "nr" does not exist.</p> <p><i>Example 1:</i></p> <p><i>1234 SETNAME=PARTITION,1,Cellar</i></p> <p><i>Example 2:</i></p> <p><i>1234 SETNAME="PARTITION,2,Kids Room"</i></p> |
| Feedback message description  | <p>SETNAME:OK – command accepted</p> <p>SETNAME:ERROR-PERMISSION - you do not have permission to execute this command</p> <p>SETNAME:ERROR-FORMAT - incorrect format command</p> <p>SETNAME:ERROR-VALUE - incorrectly stated value</p> <p>SETNAME:ERROR-PERMISSION - command rejected; other errors</p>   |

| <b>Getting the name of partition, zone, outputs, users and system</b> |   |
|---|---|
| Command syntax  | XXXX GETNAME=ELEMENT,[NR]   |
| Command description   | <p>Acquiring the name of the element with the specified number nr. This command is complementary to SETNAME - there are describes the permissible values of individual fields, see the table "Setting the name of the partition, inputs, outputs, users and system.</p> <p>XXXX – admin code</p> <p>Possible values position ELEMENT:</p> <p>PARTITION - Acquiring the name of partition; numbers 1 and 2</p> <p>ZONE - Acquiring the name of input line unit corresponding to the indicated number; the numbers from 1 to 32</p> <p>OUTPUT - Acquiring the name of output corresponding to the indicated number; the numbers from 1 to 3</p> <p>USER - Acquiring the name of user with the specified number; the numbers from 1 to 32</p> <p>SYSTEM - Acquiring the name of object which panel and alarm system were installed. Note: here position "nr" does not exist.</p> <p>XXXX – user code</p> <p><i>Example: 1234 GETNAME=PARTITION,1</i></p> |
| Feedback message description  | <p>GETNAME=ELEMENT,[NR],VALUE - command executed correctly, the name of element</p> <p>(NOTE: If the name has not been changed (remains the default), it will not be given in the reply)</p> <p>GETNAME:ERROR-PERMISSION - you do not have permission to execute this command</p> <p>GETNAME:ERROR-FORMAT - wrong format command</p> <p>GETNAME:ERROR-VALUE – wrong value</p> <p>GETNAME:ERROR-PERMISSION - command rejected; other errors</p>  |

| <b>Setting the phone number</b> |   |
|---------------------------------|---|
| Command syntax                  | XXXX SETTELNUM=ID,NUMBER  |
| Command description             | <p>Setting the phone number for pointed index on the phone number list</p> <p>XXXX – admin code</p> <p>ID – index of phone number on the list, possible values: 1 to 10</p> <p>NUMBER – phone number, on which the texts will be send</p> <p><i>Example: 1234 SETTELNUM=3,800123456</i></p> |
| Feedback message description    | <p>SETTELNUM:OK – command accepted</p> <p>SETTELNUM:ERROR – command rejected by the system</p>  |

| <b>Getting the phone number</b> |   |
|---------------------------------|---|
| Command syntax                  | XXXX GETTELNUM=ID   |
| Command description             | <p>Getting the phone number for pointed index on the phone number list</p> <p>XXXX – admin code</p> <p>ID – index of phone number on the list, possible values: 1 to 10</p> <p><i>Example: 1234 GETTELNUM=2</i></p> |
| Feedback message description    | <p>GETTELNUM=ID,NUMBER – information about phone number</p> <p>GETTELNUM:ERROR – command rejected by the system</p>   |

| <b>Setting the content of text message</b> |  |
|--|--|
| Command syntax                             | XXXX SETMESSAGE=ID,MESSAGE_without_spaces<br>XXXX SETMESSAGE="ID,MESSAGE_with_spaces"  |
| Command description                        | Setting the content of text message under the pointed index<br>XXXX – admin code<br>ID – index of text, possible values: 1 to 32<br>MESSAGE – content of the text message<br><i>Example: 1234 SETMESSAGE=4,Robbery</i> |
| Feedback message description               | SETMESSAGE:OK – command accepted<br>SETMESSAGE:ERROR – command rejected by the system  |

| <b>Getting the content of text message</b> |  |
|--|--|
| Command syntax                             | XXXX GETMESSAGE=ID   |
| Command description                        | Getting the content of text message under the pointed index<br>XXXX – admin code<br>ID – index of text, possible values: 1 to 32<br><i>Example: 1234 GETMESSAGE=30</i> |
| Feedback message description               | GETMESSAGE=ID,MESSAGE – information about the contents of text message<br>GETMESSAGE:ERROR – command rejected by the system  |

| <b>Assigning a text message and a phone number to the event</b> |   |
|---|---|
| Command syntax  | XXXX SETUSERSMS=EVENT,TELNUM,MSG_ID   |
| Command description   | <p>Assigning a text message and a phone number to the event. The text will be send to the phone number when this event occurs.</p> <p>XXXX – user code</p> <p>EVENT – a short name of the event, possible event names are listed at the end of this chapter</p> <p>TELNUM – ten-digit chain of zeroes and ones. Each digit (counting from the left) represents an index of the phone number – first digit for the first phone number, second digit for the second number, and so on.</p> <p>0 – message will not be send to this number</p> <p>1 – message will be send to this number</p> <p><i>Example:</i></p> <p>1234 SETUSERSMS=ARM1,1000000110,6</p> <p>Means, that when ARM1 event occurs (partition 1 armed), text message number 6 will be sent to phone numbers with indexes 1,8 and 9.</p> |
| Feedback message description                                    | <p>SETUSERSMS=EVENT,TELNUM,MSG_ID:OK – command accepted</p> <p>SETUSERSMS=EVENT,TELNUM,MSG_ID:ERROR – command rejected by the system</p>  |

| <b>Getting a text message content and a phone number assigned to the event</b> |   |
|--|---|
| Command syntax   | XXXX GETUSERSMS=EVENT   |
| Command description  | <p>Getting the content of a text message and a phone number assigned to the specified event.</p> <p>XXXX – user code</p> <p>EVENT – a short name of the event, possible event names are listed at the end of this chapter</p> <p><i>Example:</i> 1234 GETUSERSMS=ARM1</p> |
| Feedback message description   | <p>GETUSERSMS=EVENT:TELNUM,MSG_ID – information about text message and phone number assigned to the event</p> <p>GETUSERSMS=EVENT:ERROR – command rejected by the system</p>  |

| <b>Getting delay between disarming and turning off historical alarms notification</b> |  |
|---|--|
| Command syntax  | XXXX CPGETALARMSHOWTIME  |
| Command description   | <p>This command is used to get delay between disarming and turning off historical alarms notification. This feature can also be disabled altogether.</p> <p>XXXX – user code</p> |
| Feedback message description  | <p>CPGETALARMSHOWTIME:delay – when feature is enabled, delay is in seconds</p> <p>CPGETALARMSHOWTIME:OFF – when feature is disabled</p>  |

| <b>List of events handled by the SETUSERSMS and GETUSERSMS commands</b> |                                     |
|---|-------------------------------------|
| Alias name  | Description                         |
| ARM1  | Partition 1 armed                   |
| ARMSTAY1  | Partition 1 armed in perimeter mode |
| ARM2  | Partition 2 armed                   |
| ARMSTAY2  | Partition 2 armed in perimeter mode |
| DISARM1   | Partition 1 disarmed                |
| DISARM2   | Partition 2 disarmed                |
| INPUT1<br>(to INPUT32)  | Violation of zones 1...32           |
| INPUT1-OFF<br>(to INPUT32-OFF)  | Violation of zones 1...32 ended     |
| INPUT1-TAMPER<br>(to INPUT32-TAMPER)                                    | Sabotage of zones 1...32            |
| INPUT1-TAMPEREND<br>(to INPUT32-TAMPEREND)                              | Sabotage of zones 1...32 ended      |
| INPUT1-LOCK<br>(to INPUT32-LOCK)  | Bypass of zones 1...32              |
| INPUT1-UNLOCK<br>(to INPUT32-UNLOCK)                                    | Bypass of zones 1...32 ended        |
| OUTPUT1-ON<br>(to OUTPUT3-ON)   | Zones 1...3 triggered               |
| OUTPUT1-OFF<br>(to OUTPUT3-OFF)   | Zones 1...3 trigger ended           |
| OUTPUT1-TAMPER<br>(to OUTPUT3-TAMPER)                                   | Fault of zones 1...3                |
| OUTPUT1-TAMPEREND<br>(to OUTPUT3-TAMPEREND)                             | Fault of zones 1...3 ended          |
| POWER-FAIL  | Power failure                       |
| POWER-OK  | Power failure ended                 |
| BATTERY-FAIL  | Battery failure                     |
| BATTERY-OK  | Battery failure ended               |
| AUX1-FAIL   | Failure of auxiliary output 1       |
| AUX2-FAIL   | Failure of auxiliary output 2       |
| AUX1-OK   | Failure of auxiliary output 1 ended |
| AUX2-OK   | Failure of auxiliary output 2 ended |



|   |                                  |
|---|----------------------------------|
| KEYPAD1-LOST<br>(to KEYPAD3-LOST)           | Failure of keypad 1...3          |
| KEYPAD1-OK<br>(to KEYPAD3-OK)               | Failure of keypad 1...3 ended    |
| KEYPAD1-TAMPER<br>(to KEYPAD3-TAMPER)       | Sabotage of keypad 1...3         |
| KEYPAD1-TAMPEREND<br>(to KEYPAD3-TAMPEREND) | Sabotage of keypad 1...3 ended   |
| KEYPAD-FIRE-BEGIN                           | 'Fire' alarm started             |
| KEYPAD-HELP-BEGIN                           | 'Help' alarm started             |
| KEYPAD-SILENTALARM-BEGIN                    | 'Panic' alarm started            |
| KEYPAD-FIRE-END                             | 'Fire' alarm ended               |
| JAMMING-BEGIN                               | GSM jamming                      |
| JAMMING-END                                 | GSM jamming ended                |
| DETECTOR1-LOST<br>(to DETECTOR32-LOST)      | Detector 1...32 signal lost      |
| DETECTOR1-OK<br>(to DETECTOR32-OK)          | Detector 1...32 signal restored  |
| DETECTOR1-PWR<br>(to DETECTOR32-PWR)        | Detector 1...32 battery low      |
| DETECTOR1-PWROK<br>(to DETECTOR32-PWROK)    | Detector 1...32 battery restored |

| <b>List of errors sent as feedback messages</b> |  |
|---|--|
| Alias name                                      | Description                                      |
| ERROR-PERMISSION                                | Permission to issue this command was not granted |
| ERROR-FORMAT                                    | Wrong command syntax                             |
| ERROR-VALUE                                     | Wrong parameter value                            |
| ERROR-EMPTY                                     | Parameter value missing                          |
| ERROR   | Other error                                      |

## 10. CHANGE HISTORY

| Date / Version / Firmware | Description   |
|---------------------------|---|
| 2017.09.20/ v1.0 / 2.8.6  | First version of the manual   |
| 2018.02.20/ v1.2 / 2.9.1  | Added chapters: User categories, Arming only user   |
| 2018.07.26/ v1.3 / 2.10.0 | Added a new response type and information about a new arming method by using the remote control |