ALARM CONTROL UNIT

CPX220NWB

User manual

Version of the manual:	v1.1
Date of issue:	2016.10.21
Firmware version:	2.6.2
GPRS transmitter configurator version:	1.3.64.3
OSM server version:	1.3.60.4

EN

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 Bronislawa Czecha St.
04-555 Warsaw, POLAND
E-mail : sales@ebs.pl
Technical support: support@ebs.pl
Webpage : www.ebs.pl

CREATING A SENSE OF SECURITY
SINCE 1989

CONTENT:

1. INTRODUCTION

Thank you for choosing EBS alarm control unit.

CPX200NWB is a simple, functional alarm control unit integrated with GSM/GPRS/SMS transmitter, intended for small- and medium- sized facilities. The central unit is equipped with 3 outputs and 7 wired and 9 wireless zones with the possibility to be divided into 2 partitions. Dedicated KP16 LED keypad was designed in a modern, discreet style. Portable size, large, comfortable buttons and simple installation contribute to indisputable advantage of our system.

The product was designed in accordance with the requirements of PN-EN 50131 standards, grade 2, Environmental class II.

2. CONTROL UNIT FUNCTIONS

2.1. FUNCTIONAL CHARACTERISTIC

ZONES

- 7 zones with the NC / NO / EOL-NC / EOL-NO / DEOL-NC / DEOL-NO configuration possibility
- Up to 16 wireless zones
- Detection lines – instant, delayed, 24h burglary, arming/disarming, 24h tamper, interior delay, 24h fire

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 KP16
- ability to connect up to three keypads

TRANSMISSION

- Transmission of signals through GPRS/SMS module.
- Encryption of data transfer using AES standard
- Communication with monitoring station using dedicated OSM.2007 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 KP16 keypad or a computer
- Remote through GPRS, SMS or CSD

USERS

- 1 admin code (main)
- 1 service code
- 8 user codes
- Possibility to restrict the scope of authorization to a few codes only

SYSTEM OPTIONS

- Automatic diagnosis of basic system components

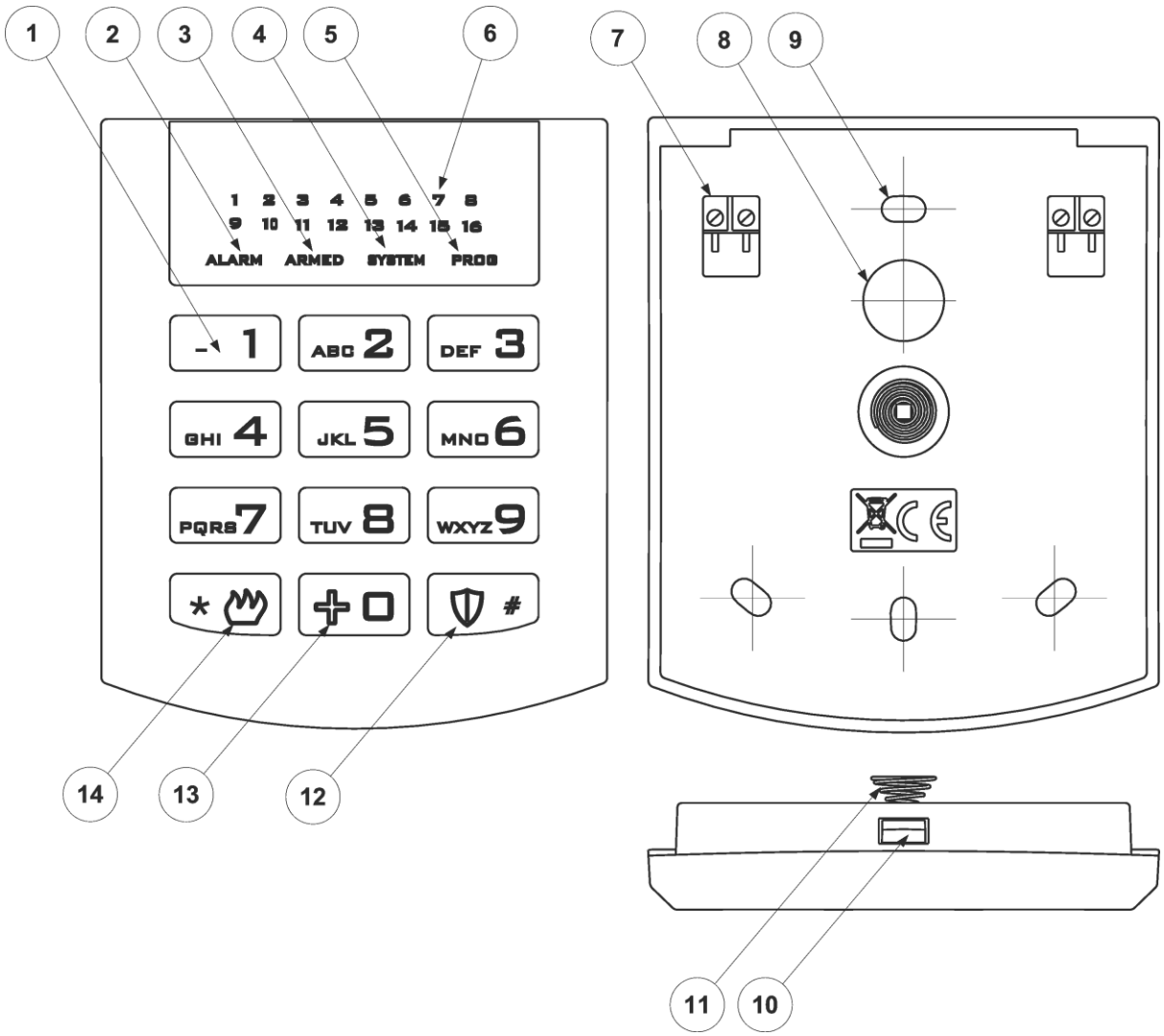
- Possibility to review faults, alarm memories, event log
- System/technical event history – min. 5000 events

2.2. SPECIFICATIONS

Supply voltage:	18VAC (16-20VAC)
Required transformer Power:	min. 20VA
Current consumption average/max: (average measured@: fully charged battery, established connection with server, connected keypad, no sensors connected)	120mA / 1100mA @18VAC
Average current consumption; lack of external supply (without keypad/ with keypad): (fully charged battery, no sensors connected, established connection with server)	60mA / 80mA
Charging current: (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:	-10ºC to +55ºC
Working humidity:	5% to 93%
PCB dimensions:	152mm x 78mm x 30mm

3. KEYPAD SPECIFICATION

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



Drawing 1. KP16 Keypad

1. **Keypad buttons**

   0-9 buttons and ***** as well as **#** are intended for the keypad and alarm control unit operation. After first pressing any button, the keypad is backlit. After a few-second idle time, backlight gets automatically dimmed. In order to make codes easier to remember, buttons are marked with the alphabet.

2. **ALARM LED (red):**

   Flashing light – means that alarms occurred in the system (alarms memory).

   Constant light – means that system is in alarm state.

   Off – system is operating correctly.

3. **ARMED LED (red):**

   Flashing light – means that time for leaving any of the partitions is counted.

   Constant light – at least one partition is armed

   Off – partitions disarmed.

4. **SYSTEM LED (yellow):**

   Flashing light – means that in the control unit's memory there are faults that has already ceased (there was power loss, but it has already restored).

   Constant light – there is a fault in the system that was not removed.

   Off – no fault in the system.

5. **PROG LED (blue):**

   Flashing slowly – service function is activated and it is one of the user functions.

   Flashing – data will be entered.

   Constant light – installer service function is activated.

6. **1 – 16 LEDs (red)**

   When LED goes on during normal operation, it means the line it is assigned to was disrupted. Flashing LED means the zone was interlocked. After activating service functions, LEDs display data.

7. **Screwed Connectors**

   Connectors for connecting cables joining the keypad with the alarm control unit.

8. **Cable Entry**

   It is a place for entering the connection cables.

9. **Assembly Holes**

   The keypad was equipped with four round assembly holes for proper fastening the keypad.

10. Casing Opening Latch

To open the casing it is recommended to use flat 2.5-5mm screwdriver. Insert it slightly in indicated hole and perform slight lever movement toward the rear side of the casing.

11. 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 unit. In order to eliminate surface unevenness, a spring is located on the switch lever.

12. - 14. Emergency Buttons

 – Fire alarm

 – Medical alarm

 – Burglary alarm

See item 9.12. Emergency buttons.

4. WIRELESS KEYPAD KP1W

The wireless keypad KP1W 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.

4.1. KEYS OF THE KEYPAD

The keypad KP1W is equipped with keys marked with numbers **0** to **9** and function keys * and #.

After pressing any key, the keypad is backlit.

4.2. 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 central 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

4.3. LED SIGNALLING

The keypad KP1W is equipped with two LEDs that inform about low battery and sending a radio transmission.

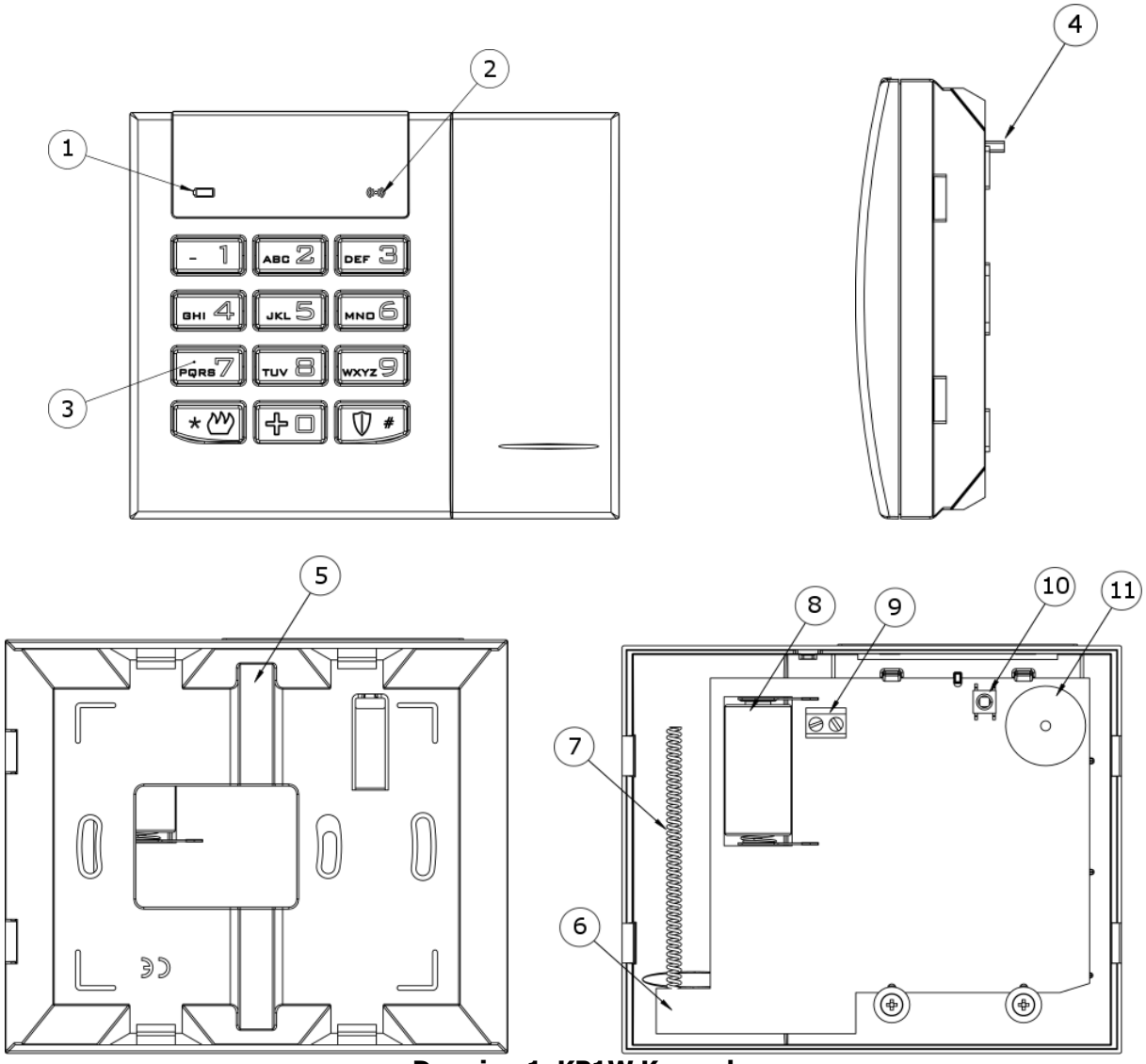
The low battery is signaled by showing a red battery symbol in the upper left corner of the display:

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

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

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

4.4. DESCRIPTION OF KEYPAD ELEMENTS



Drawing 1. KP1W Keypad

1. **<u>Low battery LED (RED)</u>**
   On – battery is low,
   Off – battery O.K.
2. **<u>Data transmission LED (BLUE)</u>**
   Blinks – data transmission in progress
   Off – no data transmission
3. **<u>Keypad buttons</u>**
   0-9 buttons and ***** as well as **#** are intended for keypad and control unit operation. After first pressing any button, the keypad is backlit. After a few-second idle time, backlight gets automatically dimmed. In order to make codes easier to remember, buttons are marked with the alphabet.
4. **<u>and 10. Anti-sabotage switch</u>**

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

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.

11. **Buzzer**

4.5. KEYPAD SPECIFICATION

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

Frequency:	433,92MHz
Coding:	Code hopping
Number of buttons:	4
Battery:	Varta Li-Mn 3V type CR2032

– ARM button

– DISARM button

– SILENT ALARM button

– ALARM button

6. ARMING THE SYSTEM

6.1. ARMING MODES

Each partition can be armed in one of the following modes

- Stay (perimeter) – partition is armed, but only perimeter and perimeter exit zones violation will cause an alarm
- Away (full) – partition is armed and violation of any zone will cause an alarm
User can choose the arming mode or let the system do it for himself.

6.2. ARMING THE SYSTEM

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

6.2.1. ARMING FROM THE MAIN KEYPAD KP16

Note: If incorrect code is entered the keypad will emit long constant sound. Repeat the arming process by entering the correct code.

Stay mode is in fact a part of the Away mode. Every time a correct code is given, the system will **immediately** arm in the stay mode (provided it has perimeter zones). Afterwards, the system can automatically arm in the away mode, if proper conditions were met.

6.2.1.1. Stay mode

Arming the partition in stay mode is possibile only if it has perimeter zones assigned to it.

Partition will arm in the stay mode in following cases:

1. Input the user code, press and hold the [#] button for 3 seconds.
2. Input the user cold and press the [#] button. If the perimeter exit zones is violated during the exit time countdown, partition will arm in away mode. If perimeter zone is not violated during the exit time countdown, partition will remain armed in the stay mode.

6.2.1.2. Away mode

In order to arm the partition in the away mode, user has to input his code and press the [#] button. Exit time countdown will start. Partition will arm in the stay mode in the following cases:

1. Partition has perimeter exit zones and at least one of them is violated during the exit time countdown.
2. Partition does not have any perimeter exit zones.

Correct code will be confirmed by the keypad by 3 beeps.
Leave the facility before the time for leaving expires. That state is indicated by intermittent sound and quick flashing the ARMED LED on the keypad until the system gets fully armed. If the chirps are activated the arming will be confirmed by one chirp of siren.

6.2.2. ARMING FROM THE AUXILIARY KEYPAD KP1W

Note: The keypad KP1W has no ability of sound signaling of arming, disarming or entering an incorrect code. Arming and disarming of the system may signaled by main signaler chirp (if active). Armed – once, disarmed – twice. The full signalization of system status is available with keypads KP16.

6.2.2.1. Stay mode

Arming the partition in stay mode is possibile only if it has perimeter zones assigned to it.

Partition will arm in the stay mode in following cases:

1. Input the user code, press and hold the [#] button for 3 seconds.
2. Input the user cold and press the [#] button. If the perimeter exit zones is violated during the exit time countdown, partition will arm in away mode. If perimeter zone is not violated during the exit time countdown, partition will remain armed in the stay mode.

6.2.2.2. Away mode

In order to arm the partition in the away mode, user has to input his code and press the [#] button. Exit time countdown will start. Partition will arm in the stay mode in the following cases:

1. Partition has perimeter exit zones and at least one of them is violated during the exit time countdown.
2. Partition does not have any perimeter exit zones.

Leave the facility before the time for leaving expires. If the code was correct system gets armed. If the chirps are activated the arming will be confirmed by one chirp of siren.

6.2.3. ARMING FROM THE REMOTE CONTROL

Press the remote control button indicated by the closed padlock symbol, assigned to the arming function. Keypad confirms arming by lighting ARMED LED. If the chirps are activated, the arming will be confirmed by one chirp of siren.
Arming from the remote control always arming partition in Away mode, even if partition includes a perimeter zones.
Note! The control panel allows you to assign remote control buttons to various functions. It is possibile to configure different arming button.

6.3. ARMING THE SYSTEM WITH FAULT

If during the arming any faults are present in the system, the keypad will indicate it with flashing ARMED and SYSTEM LEDs and long constant audio signal. LEDs 1 to 8 will indicate which system errors are present. That state will maintain for 10 seconds. If there is no possibility to quickly remove faults, press [#] to arm the system. Pressing [*] will cancel the arming process.

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, KP1W keypad and via text messages (SMS).

7. DISARMING THE SYSTEM

7.1. DISARMING THE SYSTEM

7.1.1. DISARMING FROM THE KEYPAD KP16

1. Enter the facility through the entrance door. Intermittent sound and slow flashing of ARMED LED on the keypad will remind of the need to disarm the system before the delay time for entrance expires.
2. Enter the code and press [#]. 3-tone beep of the keypad will confirm the correct code input. The partition the user has access to will be disarmed. If the chirps are activated the disarming will be confirmed by two chirps of siren. If the user has access to all partitions, all of them will be disarmed. If there is no armed partitions in the system, ARMED LED will be deactivated.
3. The system can be also disarmed in different way- by changing the partition state. See chapter 8. PARTITION HANDLING.
4. When system is disarmed, alarm will be muted (deactivated).

Note: Incorrect code will be indicated with a long constant sound. Enter the correct code immediately and press [#].

7.1.2. DISARMING FROM THE KEYPAD KP1W

1. Enter the code and press [#]. If the code was correct the partition the user has access to will be disarmed. If the chirps are activated the disarming will be confirmed by two chirps of siren. If the user has access to all partitions, all of them will be disarmed. If there is no armed partitions in the system, ARMED LED will be deactivated.
2. When system is disarmed, alarm will be muted (deactivated).

Note: KEYPAD KP1W does NOT signal any code entrance - correct or not.

7.1.3. DISARMING FROM THE REMOTE CONTROL

Press the remote control button indicated by the open padlock, assigned to the disarming function. keypad confirms disarming by blanking ARMED LED. If the chirps are activated the disarming will be confirmed by two chirps of siren.
Note! The control panel allows you to assign remote control buttons to various functions. It is possibile to configure different disarming button.

7.2. ALARM DISPLAY

If red ALARM LED flashes when the system is armed, it means that while you were absent some alarms occurred (numbers of lines that initiated them will be displayed as well) which have already ceased. But, if ALARM LED emits constant light, it means that system still is in alarm state. Exercise caution! If you suspect any intruder to be present in the facility, leave the facility immediately and call security guards.

7.3. 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 ALARMS MEMORY chapter of the present manual.

8. PARTITION HANDLING

8.1. ARMING / DISARMING WITH SELECTING PARTITIONS WITH KEYPAD KP16

1. Enter the number of the function [+0] and confirm using [#]. Then enter the user code and press [#]. 3-tone beep will confirm the correct code input.

Note: If incorrect code is entered the keypad will emit long constant sound. Enter the correct code once again.

2. LEDs 1 and 2 will display the current partition state. LED on – partition armed, LED off - partition disarmed. Only LEDs indicating the partitions the user has access to will be on.
3. To change the partition state press buttons with partition numbers (LEDs with relevant partition number will go on/off). Confirm the change of partition state using [#] button. 3 beeps will confirm the change. To cancel the entered changes, press [*].
4. If partition arming was selected, the keypad will indicate counting the time for leaving the facility. Leave the facility before the time for leaving expires. After it is armed the ARMED LED will be constantly on.
5. If partition disarming is selected, the relevant partition will be immediately disarmed.

8.2. QUICK ARMING / DISARMING PARTITIONS WITH KEYPAD KP16

1. Enter the number of the function ([+0] [1] for partition one or [+0] [2] for partition two) and confirm using [#]. Then enter the user code and press [#]. 3-tone beep will confirm the correct code input.

Note: If incorrect code is entered the keypad will emit long constant sound. Enter the correct code once again.

2. If partition arming was selected, the keypad will indicate counting the time for leaving the facility. Leave the facility before the time for leaving expires. After it is armed the ARMED LED will be constantly on.
3. If partition disarming is selected, the relevant partition will be immediately disarmed.

8.3. QUICK ARMING / DISARMING PARTITIONS WITH KEYPAD KP1W

1. Enter the number of the function ([0] [1] for partition one or [0] [2] for partition two) and confirm using [#]. Then enter the user code and press [#].

Note: the keypad does not confirm entering the code.
If configured, the arming will be signaled with single chirp, disarming – double chirp.

2. If partition arming was selected, leave the facility before the time for leaving expires.
3. If partition disarming is selected, the relevant partition will be immediately disarmed.

9. USER FUNCTIONS

Note: The following operations can be performed only using the main keypad KP16.

9.1. ALARMS MEMORY

[DEF 3] [# ⏻] - Display of alarms memory

The function displays the history of alarms that occurred in the system. When the function is activated, ALARM and PROG LEDs are flashing slowly and all alarms that occurred since last arming are displayed. LEDs 1 - 16 display the information from which zones the alarm was activated. To clear the alarms memory, press [# ⏻]. To exit without clearing the alarms memory, press [* ⏻].

Alarm source types:

Diodes 1 to 16 – Sabotage of lines 1 to 16

If no diodes are on and the ALARM led is blinking, then there alarms that were triggered by the source other than input lines. *Other alarms* history can be accessed by selecting following code from the main menu: [DEF 3] [- 1] [# ⏻].

After pressing the button corresponding to active LED, the detailed information about the alarm source within selected type is displayed.

Pressing [* ⏻] will result in return to the main menu.

Other alarm source types:

2 – Keypads tamper

3 – Emergency button used

4 – Remote control alarm

Other alarm source types -> Keypads tamper:

1 – Keypad tamper 1

2 – Keypad tamper 2

3 – Keypad tamper 3

Other alarm source types -> Emergency button used:

1 – Fire alarm activated

2 – Help alarm activated

Other alarm source types -> Remote control alarm:

5 – Remote control alarm

Note: Alarms memory is cleared after the system is armed.

9.2. FAULTS MEMORY

[4 GHI] [# ⛉] - Display of faults memory

The function displays the faults that are present in the system. When the function is activated, SYSTEM and PROG LEDs are flashing slowly and all faults that are currently present in the system are displayed. Led 1 – 8 display information on the cause of fault. To clear the faults memory, press [# ⛉]. To exit without clearing the faults memory, press [* ✍].

Faults description:

1 – *Sabotage of zones*

To display more detailed information about sabotage of zones, press [1 -] button.
1 – Sabotage of zone 1
2 – Sabotage of zone 2
⋮
16 – Sabotage of zone 16
To return to the main fault menu, press [* ✍].

2 – *Fault of outputs 1 - 3*

To display more detailed information about fault of outputs, press [2 ABC] 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 [3 DEF] 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*

No more detailed information.

5 – *Battery fault*

No more detailed information.

6 – *ATS fault*

No more detailed information.

7 – Other damages

To display more detailed information about other damages, press [PQRS 7] button.

1 – Clock fault

2 – Fault of central unit settings

3 – *Keypads tamper*

To display more detailed information about keypads tamper, press [DEF 3] button.

1 – Keypad tamper 1

2 – Keypad tamper 2

3 – Keypad tamper 3

To return to the ***Other damages***, press [*] button.

4 – Low battery of the wireless detectors (zones 8-16)

To display numbers of detectors with low battery level press [GHI 4] key.

To return to the main fault menu, press [*].

5 – Loss of connection with the wireless detectors

To display numbers of detectors with connection loss status press [JKL 5] key.

To return to the main fault menu, press [*].

9.3. ZONE BLOCKING

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 number of the function [JKL 5][0] and confirm with [#]. Enter the user code and press [#]. 3-tone beep will confirm the correct code input.

Note: If incorrect code is entered the KEYPAD will emit long constant sound. Enter the correct code once again.

2. Use buttons numbered 1 to 9 to select zones you want to block. Selecting zone 10 to 16 can be achieved by pressing and holding for 2 seconds the buttons 0 to 6 (0 for 10, 1 for 11, 2 for 12, etc.).
3. Change the zones blocking status by pressing numbered buttons (LEDs with relevant zone number will go on/off). Press [#] to confirm blocking of selected zones. 3 beeps will confirm the change. To cancel the entered changes, press [*].

9.4. ADDING A NEW USER

You can add a new user code here. New codes can be added by the administrator only. 3 beeps will confirm the successfully entered function. Default admin code: 1111.

Note: Individual code cannot be the same; if any code is the same as another one, it will not be recorded.

To add a new user:

1. Enter the function code [8 TUV] [1 -] and press [#] to confirm.
2. Enter the admin code and confirm it with [#]. 3 beeps will confirm the correct code input.
3. Numbers of already existing users will be displayed.
4. Enter the ID of newly added user (1 to 8), other than already added ID numbers, and press [#] to confirm. Numbers of partitions a new user can have access to will be displayed.
5. To activate/deactivate LED of an appropriate partition, press 1 or 2. When the access is set, press [#] to confirm. All LEDs shall be off now.
6. Enter the code of a newly added user (4 to 7 digits) and press [#] to confirm.
7. Enter the code of a newly added user again and press [#] to finish adding or [*] to exit without saving changes.
8. Successful adding a new user will be confirmed with 3 beeps, otherwise a constant sound will be emitted.

9.5. USER DELETE

You can delete a user here. Codes can be deleted by the administrator only. 3 beeps will confirm the successfully entered function. Default admin code: 1111.

Note: You cannot delete Admin account (user no. 0) and Installer account (user no. 9)

To delete a user:

1. Enter the function code [TUV 8] [+ 0] and press [# ⛉] to confirm.
2. Enter the admin code and confirm it with [# ⛉]. 3 beeps will confirm the correct code input.
3. Numbers of already existing users will be displayed.
4. Enter the ID code (1- 8) of a user to be deleted and press [# ⛉] to confirm or [* ♨] to exit without saving changes.
5. Successful deletion of a user will be confirmed with 3 beeps, otherwise a constant sound will be emitted.

9.6. CHANGE OF USER CODE

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

[PQRS 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.

9.7. 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.

[MNO 6] [+ 0] [# ⛉] **< Administrator code >** [# ⛉] **<hh> <mm>** [# ⛉]

where:

Administrator code – Administrator code
hh – Hours
mm – Minutes

In any moment you can press [* ♨] to exit without saving changes.

9.8. 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.

[MNO 6] [- 1] [#] **< Administrator code >** [#] **<YY> <MM> DD>** [#]

where:

Administrator code – Administrator Code
YY – Year
MM – Month
DD – Day

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

9.9. TESTING THE ZONES

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

[JKL 5] [JKL 5] [#] **<User code>** [#] **<Duration of test>** [#]

Duration of test is the time in seconds after which the test will be finished and the system will return to the main menu.

After activation this function, LEDs 1 - 16 display the zones used in the system. Only zones belong to the user's partitions are presented. Relevant LED goes off after violation of the zone. Example of use: walk around the protected object and activate detectors. After activate detectors, relevant LEDs will go off. LEDs that are still on, indicate inactive or broken detectors.

To exit the testing function press [*] or [#] .

9.10. TESTING THE OUTPUTS

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

[JKL 5] [MNO 6] [#] **< 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 [#] .

9.11. 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 and confirmed by [#] button, 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.

9.12. EMERGENCY BUTTONS

The keypad of CPX200NWB has 3 function keys. Pressing and holding for 3 seconds one of these keys will generate an alarm corresponding to the key:

[*] – Fire alarm

[+] – Medical alarm

[#] – Burglary 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 signaled on a keypad with all digits blinking slow (first row) and fast (second row). Enter and confirm any user code to deactivate it.

Medical 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.

9.13. ALARM FROM REMOTE CONTROL

The remote control has 2 alarm button.

Press the remote control button indicated by symbol ((( ))) to trigger an alarm with audible signal.

Press the remote control button indicated by symbol ⊙ to initiate a silent alarm without audible signal.

Alarms from remote control can be generated regardless of whether or not the partition is armed.

For normal and silent alarm can be sent a message to the monitoring station, depending on the configuration of the control panel.

Note! The control panel allows you to assign remote control buttons to various functions. It is possibile to configure different alarm button.

9.14.TEXT MESSAGES

CPX200NWB Alarm Control Unit 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. CPX200NWB 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:

Acquiring the state of partitions	
Command syntax	XXXX GETARMED
Command description	Acquiring the information which partitions are armed/disarmed XXXX – user code *Example: 1234 GETARMED*
Feedback message	PARTITION1:X, PARTITION2:Y or GETARMED:ERROR

Feedback message description	PARTITION1:X, PARTITION2:Y - Information about partitions arm/disarm state. PARTITION1,PARTITION2 – default partitions names, they can be changed with the SETNAME command X,Y – partition states, possibile values: 0 – disarmed 1 – armed GETARMED:ERROR – command rejected by the system

Setting the name of partition	
Command syntax	XXXX SETNAME=PARTITION,NR,VALUE
Command description	Setting the name of the partition. XXXX – user code NR – number of the partition, possibile values: 1 or 2 VALUE – new name of the partition *Example 1:* *1234 SETNAME=PARTITION,1,Cellar* *Example 2:* *1234 SETNAME="PARTITION,2,Kids Room"*
Feedback message	SETNAME::OK or SETNAME:ERROR
Feedback message description	SETNAME::OK – command accepted SETNAME:ERROR – command rejected by the system

Getting the name of partition	
Command syntax	XXXX GETNAME=PARTITION,NR
Command description	Acquiring the name of the partition XXXX – user code NR – number of the partition, possibile values: 1 or 2 *Example: 1234 GETNAME=PARTITION,1*
Feedback message	GETNAME=PARTITION,NR,VALUE or GETNAME:ERROR
Feedback message description	GETNAME=PARTITION,NR,VALUE – partition name GETNAME:ERROR – command rejected by the system

Setting the phone number	
Command syntax	XXXX SETTELNUM=ID,NUMBER
Command description	Setting the phone number for pointed index on the phone number list XXXX – user code ID – index of phone number on the list, possible values: 1 to 10 NUMBER – phone number, on which the texts will be send *Example: 1234 SETTELNUM=3,800123456*
Feedback message	SETTELNUM:OK or SETTELNUM:ERROR
Feedback message description	SETTELNUM:OK – command accepted SETTELNUM:ERROR – command rejected by the system

Getting the phone number	
Command syntax	XXXX GETTELNUM=ID
Command description	Getting the phone number for pointed index on the phone number list XXXX – user code ID – index of phone number on the list, possible values: 1 to 10 *Example: 1234 GETTELNUM=2*
Feedback message	GETTELNUM=ID,NUMBER or GETTELNUM:ERROR
Feedback message description	GETTELNUM=ID,NUMBER – information about phone number GETTELNUM:ERROR – command rejected by the system

Setting the content of text message	
Command syntax	XXXX SETMESSAGE=ID,MESSAGE
Command description	Setting the content of text message under the pointed index XXXX – user code ID – index of text, possible values: 1 to 32 MESSAGE – content of the text message *Example: 1234 SETMESSAGE=4,Robbery*
Feedback message	SETMESSAGE:OK or SETMESSAGE:ERROR
Feedback message description	SETMESSAGE:OK – command accepted SETMESSAGE:ERROR – command rejected by the system

Getting the content of text message	
Command syntax	XXXX GETMESSAGE=ID
Command description	Getting the content of text message under the pointed index XXXX – user code ID – index of text, possible values: 1 to 32 *Example: 1234 GETMESSAGE=30*
Feedback message	GETMESSAGE=ID,MESSAGE or GETMESSAGE:ERROR
Feedback message description	GETMESSAGE=ID,MESSAGE – information about the contents of text message GETMESSAGE:ERROR – command rejected by the system

Assigning a text message and a phone number to the event	
Command syntax	XXXX SETUSERSMS=EVENT,TELNUM,MSG_ID
Command description	Assigning a text message and a phone number to the event. The text will be send to the phone number when this event occurs. XXXX – user code EVENT – a short name of the event, possible event names are listed at the end of this chapter 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. 0 – message will not be send to this number 1 – message will be send to this number *Example:* 1234 SETUSERSMS=ARM1,1000000110,6 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.
Feedback message	SETUSERSMS=EVENT,TELNUM,MSG_ID:OK or SETUSERSMS=EVENT,TELNUM,MSG_ID:ERROR
Feedback message description	SETUSERSMS=EVENT,TELNUM,MSG_ID:OK – command accepted SETUSERSMS=EVENT,TELNUM,MSG_ID:ERROR – command rejected by the system

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

List of events handled by the SETUSERSMS and GETUSERSMS commands	
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 (to INPUT16)	Violation of zones 1…16
INPUT1-OFF (to INPUT16-OFF)	Violation of zones 1…16 ended
INPUT1-TAMPER (to INPUT16-TAMPER)	Sabotage of zones 1…16
INPUT1-TAMPEREND (to INPUT16-TAMPEREND)	Sabotage of zones 1…16 ended
INPUT1-LOCK (to INPUT16-LOCK)	Bypass of zones 1…16
INPUT1-UNLOCK (to INPUT16-UNLOCK)	Bypass of zones 1…16 ended
OUTPUT1-ON (to OUTPUT3-ON)	Zones 1…3 triggered
OUTPUT1-OFF (to OUTPUT3-OFF)	Zones 1…3 trigger ended
OUTPUT1-TAMPER (to OUTPUT3-TAMPER)	Fault of zones 1…3
OUTPUT1-TAMPEREND (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 (to KEYPAD3-LOST)	Failure of keypad 1...3
KEYPAD1-OK (to KEYPAD3-OK)	Failure of keypad 1...3 ended
KEYPAD1-TAMPER (to KEYPAD3-TAMPER)	Sabotage of keypad 1…3
KEYPAD1-TAMPEREND (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 (to DETECTOR16-LOST)	Detector 1…16 signal lost
DETECTOR1-OK (to DETECTOR16-OK)	Detector 1…16 signal restored
DETECTOR1-PWR (to DETECTOR16-PWR)	Detector 1…16 battery low
DETECTOR1-PWROK (to DETECTOR16-PWROK)	Detector 1…16 battery restored

List of errors sent as feedback messages	
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. THE BEHAVIOR OF THE SYSTEM IN COMPATIBILITY MODE FOR GRADE 2

The system operates in accordance with the EN 50131 standard requirements for Grade 2, i.e.:

- zones status is available only after user code has been entered
- information about alarms is available only after user code has been entered
- information about alarms memory is available only after user code has been entered
- information about failures is available only after user code has been entered
- information about failures memory is available only after user code has been entered
- arming requires authorization
- prior to arming, the control panel checks circumstances that may prevent arming
- the codes in the system must be at least 5 characters
- after entering an invalid code three times, all keypads in the system will be blocked for 90 seconds.

11. CHANGE HISTORY

Date / Version / Firmware	Description
2016.08.29 / i1.0 / 2.5.2	First version of the manual
2016.10.21 / i1.1 / 2.6.2	Minor fixes