Version of the manual: v1.3
Date of issue: 27.07.2018

CREATING A SENSE OF SECURITY
SINCE 1989

ALARM CONTROL PANEL

CPX230NWB

Installation and programming 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 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 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, 7 wired (for TEOL configuration up to 14 wired) 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 PANEL 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 14 wired zones for the TEOL configuration possibility
- Up to 32 wireless zones
- Detection zones – 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 signaling 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 wired LED keypad KP32
- ability to connect up to three keypads
- cooperation with wireless keypad KP2W
- ability to connect up to 32 keypads KP2W (every keypad occupies one of the available wireless zones)

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

2.3. ACCESSORIES AND SOFTWARE APPLICATIONS

Keypads	Description
KP32-0 (black), KP32-9 (white)	LED wired keypad
KP2W-9 (white)	Wireless keypad
RC-10	Remote controller, 4 buttons

Sensors	Description
MC-10	Wireless Magnetic Contact
PIR-10	Wireless Motion Detector
PIR-11	Wireless Motion Detector (PET)
SD-20	Wireless Smoke Detector
MC-11	Wireless Magnetic Contact with additional input
FL-10	Wireless Flood Detector
GS-21	Wireless Carbon Monoxide and Natural Gas Detector
GS-22	Wireless Carbon Monoxide and Propane-butane Detector

Programmers	Description
GD-PROG	CPX Control Panel Programmer
SP-PROG	Universal Programmer
SP-PROG-BT	Universal Programmer with Bluetooth module
MINI-PROG-BT	CPX Mini Programmer Bluetooth module CPX

Application software	Description
GPRS Transmitter Configurator	Configuration App of GPRS Transmitters (PC, Windows)
OSM	Communication Server for Alarm Receiving Center
AVA INSTALL	Installers smartphone application for configuration and monitoring of the control panel (Android)
AVA	Mobile Monitoring application for control and monitoring of control panel. (Android, iOS). For Users.

3. INSTALLATION AND WIRING

3.1. SEQUENCE OF INSTALLATION

1. Develop installation diagram accounting for the location of control panel, keypad, detectors and other system components.
2. Install the control panel in hardly accessible place with uninterrupted power supply ensured.
3. Install the keypad in a location convenient for a user and connect it with the control panel. For description of keypad installation, please refer to chapter 3.6.3 Keypad installation.

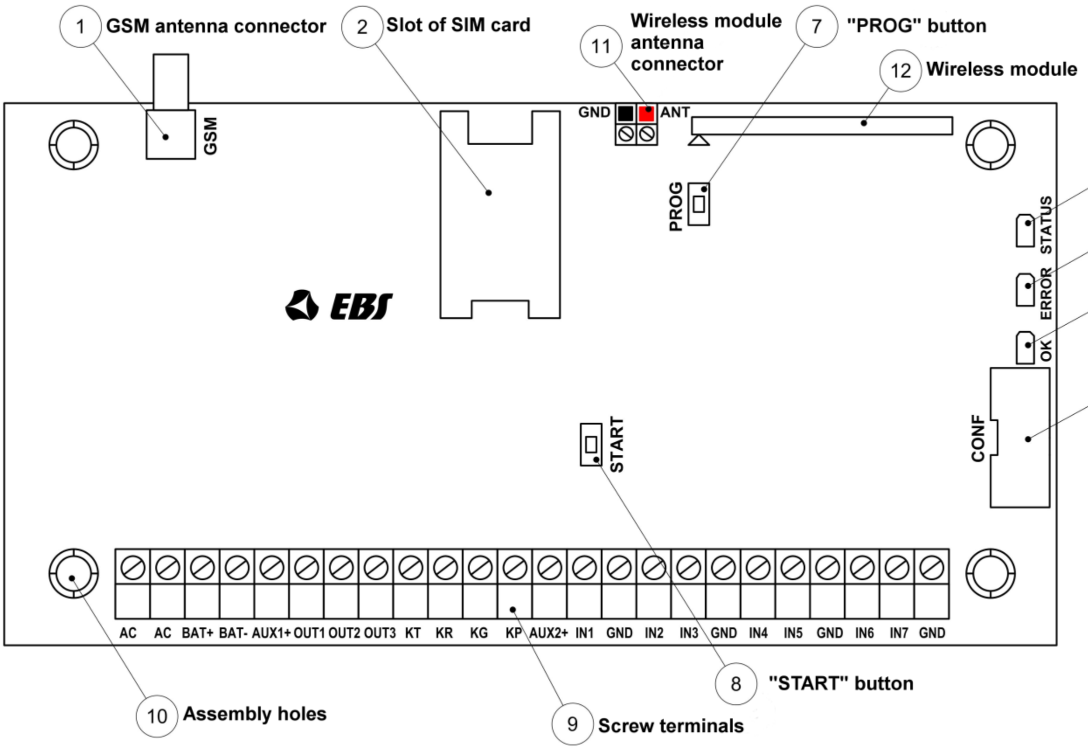
⚠ **NOTE: Maximum length of cables connecting the control panel with the keypad, at the core diameter 0.5mm^2 cannot exceed 200m.**

4. Install detectors and door and window reed relays. Connect the installed elements with control panel. For sample configuration of zones, please refer to chapter 3.4 Configuration of wired input zones.
5. Install and connect signaling devices with the control panel. For sample signaling devices connection diagrams, please refer to chapter 3.5 Sample connection of signaling device.
6. Complete the remaining cable connections.
7. Connect the battery to the screw terminals BAT +, BAT- and external power 16-20VAC to screw terminals AC, AC.
8. Program the functions of the control panel. Programming procedure was described in the chapters below.

⚠ **NOTE: If you use more than one keyboard in the system, be sure to address each assignment of the keyboard (see chapter 3.6.4.).**

9. Verify the operation of the system and all its components.

3.2. DESCRIPTION OF PCB ELEMENTS



Drawing 1. Description of PCB elements

1. GSM antenna connector (female SMA)

GSM antenna is delivered separately as one of the optional system components. It is recommended to use antenna with cable that allows finding adequate position ensuring optimal GSM range. The control panel is compatible with GSM antenna with male SMA connector.

This type of antenna (photo on the left) should be install (self-adhesive tape) on nonmetallic surface (plastic, glass etc.) in vertical position. The high placement position , free of nearby objects will give You the best possible GSM signal. Antenna shouldn't be placed in close range to metal objects (especially wires). Don't put antennas into cases (above all in metal cases). Antenna wire shouldn't be flexed or rucked. There is not recommend to extend antenna wire.

NOTE: Antenna shouldn't be installed on alarm central case or in close range to wireless receivers. It could decrease the signal range.

2. Slot of SIM card

The control panel is equipped with integrated GSM/GPRS/SMS transmitter. SIM card with active GPRS transmission is necessary to communicate with the server. The card shall be installed in the slot indicated in the drawing.

NOTE: Before you insert the card, make sure that PIN code authorization is deactivated, or PIN code is compliant with the code programmed in the control panel. Default factory PIN code of the control panel is 1111.

3. “STATUS” LED

Yellow LED diode. For the detailed description please refer to chapter 7.

4. “ERROR” LED

Red LED diode. For the detailed description please refer to chapter 7.

5. “OK” LED

Green LED diode. For the detailed description please refer to chapter 7.

6. “CONF” programming connector

“CONF” IDC10 connector allows the control panel configuration using dedicated programming devices such as **GD-PROG, MINI-PROG-BT, SP-PROG-BT** and any computer equipped with RS232 port (GD-PROG) or USB port (MINI-PROG-BT, SP-PROG-BT) or Bluetooth (MINI-PROG-BT, SP-PROG-BT).

7. “PROG” button for default settings restoration

Pressing the button for 10s during connecting the control panel with power supply will delete all users and restore the default admin and installer code. Default admin code is 1111, default installer code is 2222.

8. “START” button for battery activation of control panel without the mains power supply

If the control panel is activated in the situation of power supply fault, press the button after connecting the unit to the battery.

9. Screw terminals of the control panel

For detailed information on feeding, input and output connectors, please refer to chapter 3.3.

10. Assembly holes of the control panel (132x61mm hole span)

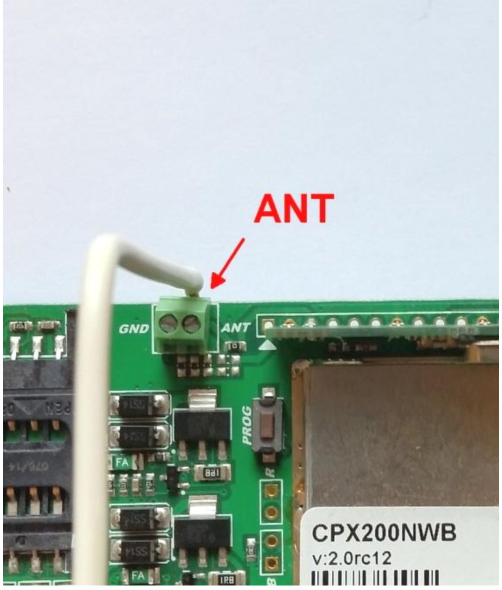
The above holes are intended for the control panel to be assembled in any type of casing. In option a dedicated plastic **OBDNA** casing can be ordered (the casing includes appropriate 230VAC/18VAC transformer).

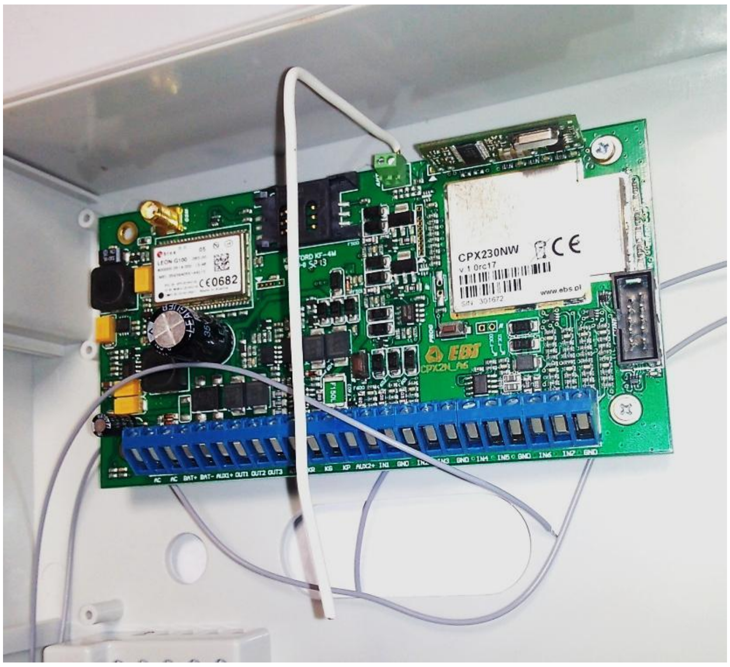
11. Wireless module antenna connector

CPX230NWB included two types of antennas: internal and external dipole type.

433MHz internal antenna

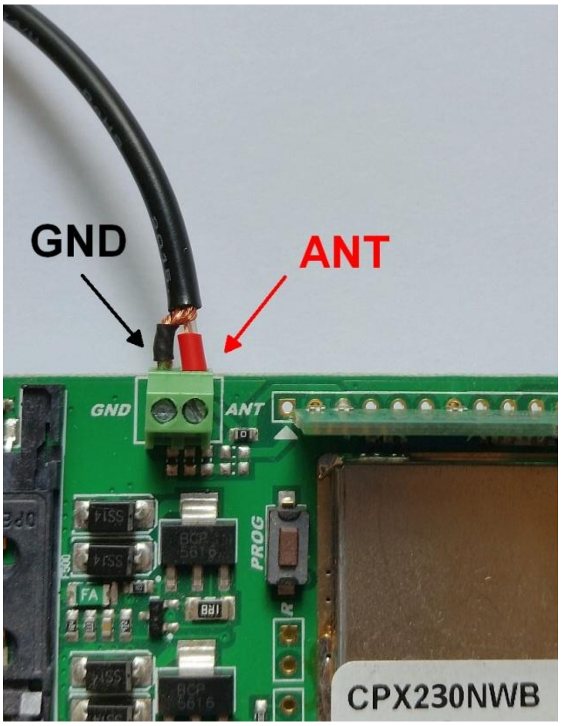
Internal antenna (photo on the left) can be used wherever required compact size and antenna provides appropriate coverage level detectors. Ending of the internal antenna without isolation should be mounted in hot pole of the socket described as ANT (correct pole is marked red on Drawing 1 and on photo below). Cold pole has been filled with plastic element (marked as a black spot). Correct antenna install position in the photo attached below.





433MHz external antenna dipol type

NOTE: In order to improve the signal coverage in harsh environments, you can use an external antenna dipole type. Antenna should be connected to GND and ANT connector regarding to the color on the endings of the wires. Before screw the antenna, remove plastic element from GND socket. Correct install position for dipole antenna in the attached photo below.

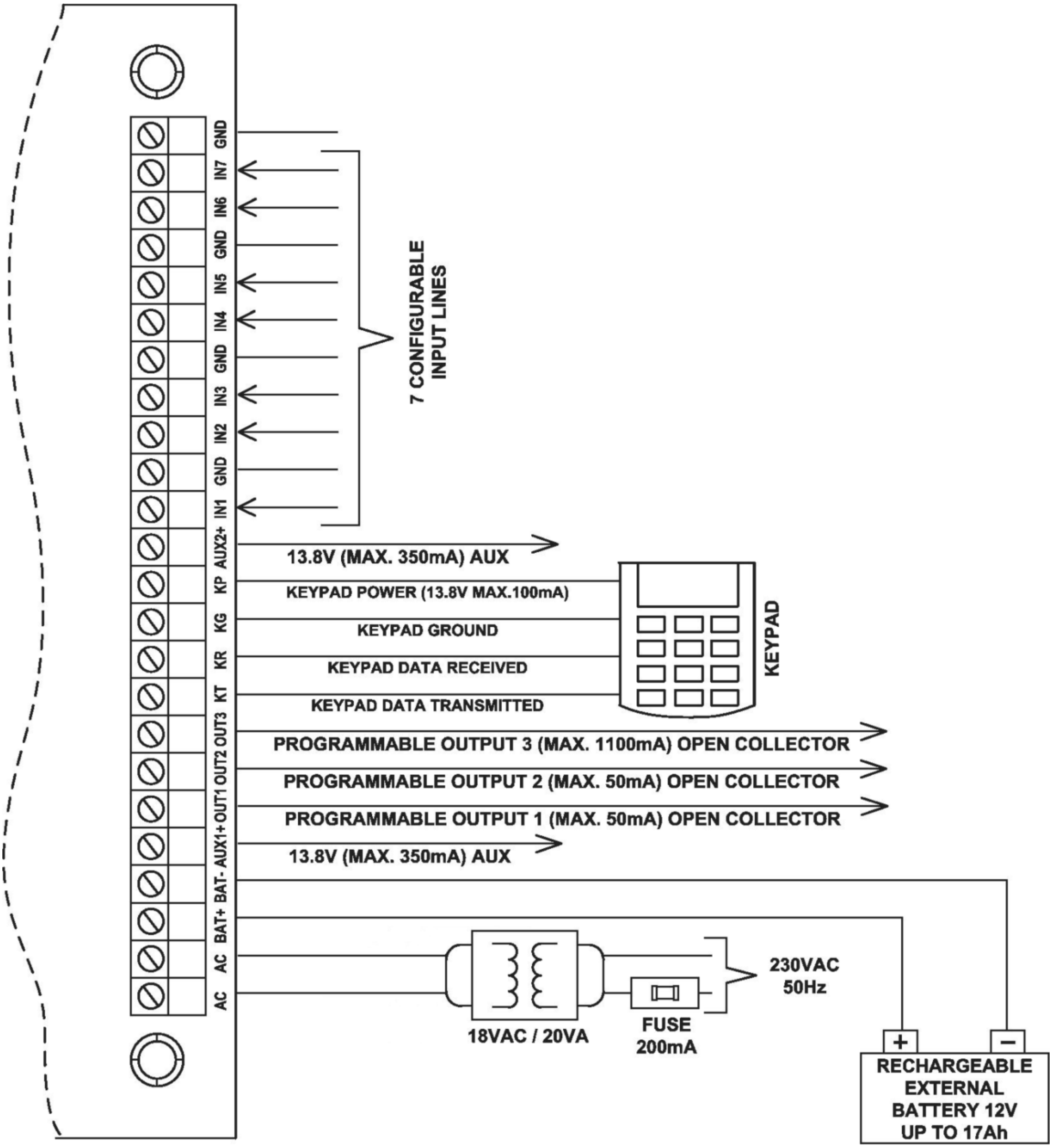


12. Wireless module

The wireless module is used to receive signals from remote controls and wireless detectors.

3.3. DESCRIPTION OF SCREW TERMINALS OF THE CONTROL PANEL

NOTE: Any assembly and installation works shall be carried out with power supply off and battery disconnected.

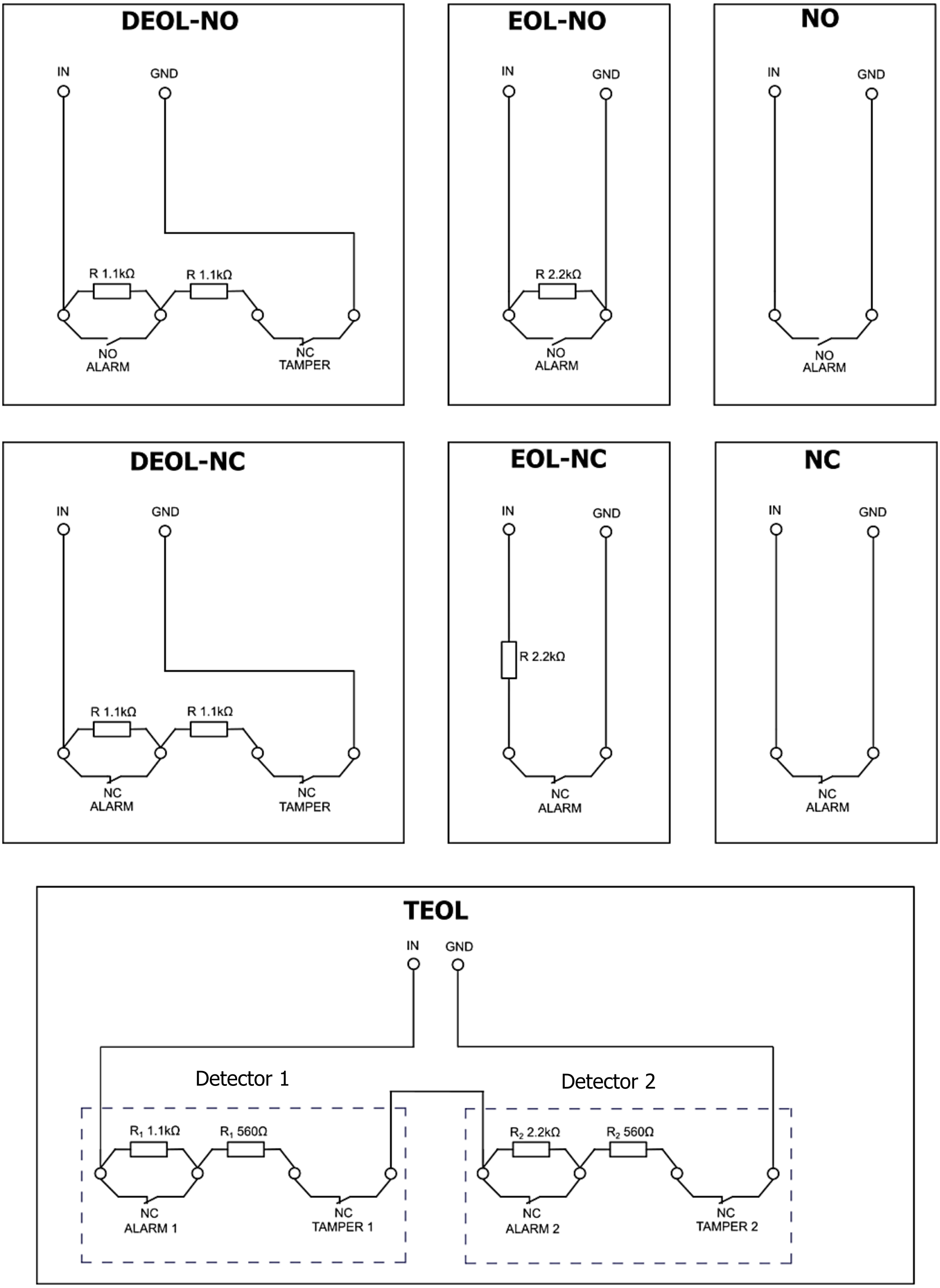

GND
IN7
IN6
GND
IN5
IN4
GND
IN3
IN2
GND
IN1
AUX2+
KP
KG
KR
KT
OUT3
OUT2
OUT1
AUX1+
BAT-
BAT+
AC
AC
7 CONFIGURABLE INPUT LINES
13.8V (MAX. 350mA) AUX
KEYPAD POWER (13.8V MAX.100mA)
KEYPAD GROUND
KEYPAD DATA RECEIVED
KEYPAD DATA TRANSMITTED
KEYPAD
PROGRAMMABLE OUTPUT 3 (MAX. 1100mA) OPEN COLLECTOR
PROGRAMMABLE OUTPUT 2 (MAX. 50mA) OPEN COLLECTOR
PROGRAMMABLE OUTPUT 1 (MAX. 50mA) OPEN COLLECTOR
13.8V (MAX. 350mA) AUX
230VAC 50Hz
18VAC / 20VA
FUSE 200mA
+
−
RECHARGEABLE EXTERNAL BATTERY 12V UP TO 17Ah

Drawing 2. Description of screw terminals of the control panel

3.4. CONFIGURATION OF WIRED INPUT ZONES

All wired input zones are fully configurable and can operate as normally closed (NC)) or normally open (NO) as well as with assigned parameters (EOL-NO or EOL-NC) using 2.2kΩ resistors or with assigned double parameters (DEOL-NO or DEOL-NC) using 1.1kΩ resistors. The TEOL configuration is used to double an alarm zone, i.e. connect two wire detectors to one clamp at the central, and it is possible to detect alarms from detector 1 and detector 2 (see drawing 3), while signaling sabotage switch (tamper) open will be common for both detectors.

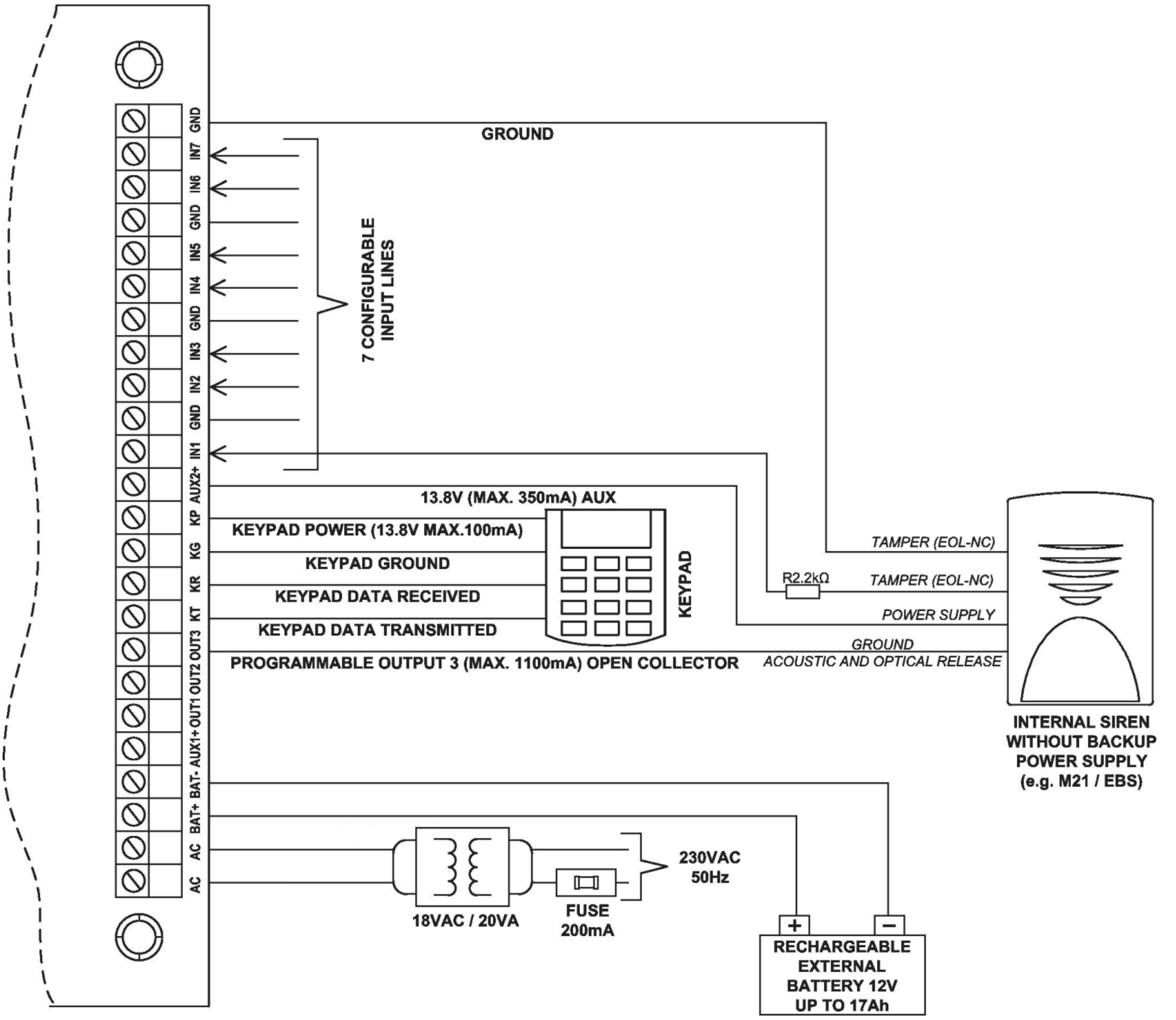
Both resistor types are included in the delivery of the control panel. Various configurations of input zones are presented in the drawing 3.



Drawing 3. Configuration of input zones

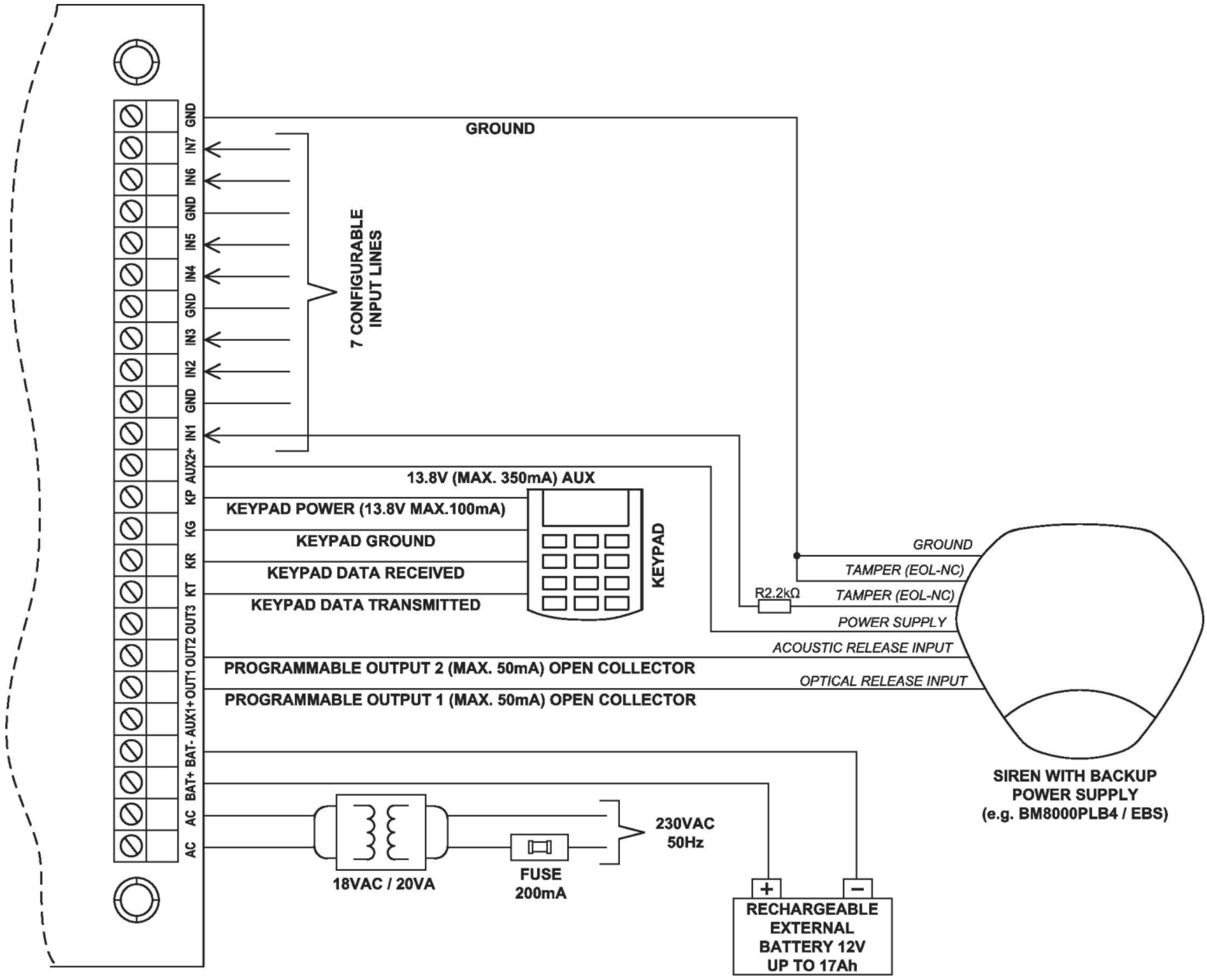
3.5. SAMPLE CONNECTION OF SIGNALING DEVICE

3.5.1. Internal signaling device without independent source of power supply



Drawing 4. Sample connection of internal signaling device without independent source of power supply

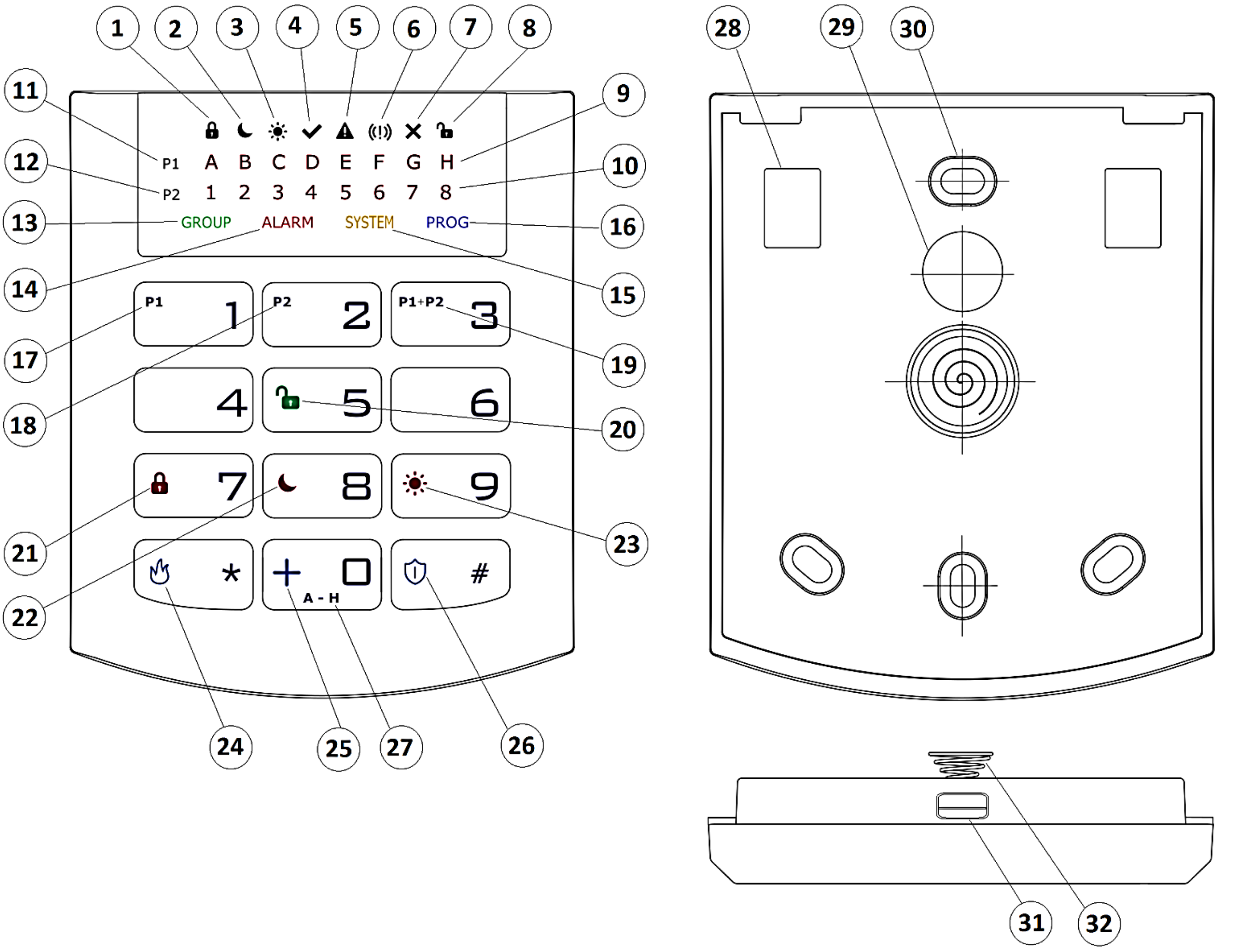
3.5.2. External signaling device with independent source of power supply



Drawing 5. Sample connection of external signaling device with independent source of power supply

3.6. KP32 KEYPAD

3.6.1. Description of keypad elements



Drawing 6. KP32 Keypad

1. **<u>FULLY ARMED mode arming symbol 🔒 – indicated with diodes A (partition P1) and 1 (partition P2)</u>**

   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. **<u>SLEEP Night mode arming symbol ☾ – indicated with diodes B (partition P1) and 2 (partition P2)</u>**

   Blinks slowly: exit time countdown,

   Blinks quickly: entry time countdown,

   Lit continuously: partition armed in night mode, Not lit: partition not armed in night 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 day mode,

   Not lit: partition not armed in day mode.

4. **READY symbol ✓– indicated with diodes D (partition P1) and 4 (partition P2)**

   Lit when all zones (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 zones assigned to the partition,

   Lit continuously: there is an alarm from a zone assigned to the partition.

7. **Line bypass symbol ✕ – indicated with diodes G (partition P1) and 7 (partition P2)**

   Lit when at least one zone belonging to the partition is locked out (bypassed).

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 night 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 day 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 zones 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 night mode (SLEEP).

23. Button 9 (sun)

A function button that supports the arming in day mode (STAY).

24. Button “*” (flame)

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

25. **Button 0 "+"**

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

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

    PANIC function button - press for about 3 sec to 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 central.

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 central. A spring is mounted on the switch lever to compensate for uneven surfaces.

3.6.2. Keypad specification

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

3.6.3. Keypad installation

1. KP32 keypad is intended for inside installation, on dry and even surface. Usually, it is installed on wall, near the entrance door, 120 -140 cm high from the ground.
2. To open the keypad casing – insert a flat screwdriver in the bottom part of the casing and press the latch. Then carefully take both parts of the casing apart, starting from the casing's bottom.
3. Mark and drill holes in the wall to install the rear part of the casing.

4. Screw the rear part of the casing to the wall. The attached 4 screws with dowels are designed for concrete base. For other substrates should choose the appropriate screws individually.
5. Connect cables joining the keypad with the alarm control panel. Keypad terminals marked: KT, KR, KP, KG shall be connected with KT, KR, KP, KG terminals in the alarm control panel (see drawing 2.).
6. Assembly the rear part of the casing with the front one starting from the casing's top. Make sure that the keypad is well assembled and sabotage switch is pressed in.

3.6.4. Addressing devices connected to the keypad bus

Each keypad to be connected to the bus must have its own individual address from the 1 to 3 range. Addresses must not repeat (the control panel does not support devices having identical addresses). It is recommended that consecutive addresses be assigned starting from 1. In keypads, the address is set by software means. By default, address 1 is set.

Programing keypad address:

1. Remove the keypad from the wall (tamper switch should be open).
2. Press and hold buttons 🔓 5 and P1 1 or P2 2 or P1+P2 3 at the same time until the corresponding diode turns on (A for address no. 1, B for no. 2, and C for no. 3).
3. After a few dozen seconds programmed keypad will be worked properly with the new addresses.

3.7. WIRELESS KEYPAD KP2W

The wireless keypad KP2W was designed to work with the hybrid control panel CPX230NWB. There is a possibility to add up to 32 of these keypads, however each of them occupies one of 32 input zones. For instance, if you add 5 keypads KP2W, there leave 27 input zones which can be used for other devices (e.g. detectors).

The transmission between the keypad and the control panel is protected with changing code and encrypted. The device sends to the control panel a cyclic test transmission and lack of it will be signaled in the system as a breach of the zone, to which the keypad is assigned to. The keypad detects and alerts low battery voltage, as well as opening of the case or its removal from the surface.

The keypad has also an NC input for connecting additional door opening detector.

Keep in mind, that the wireless keypad KP2W uses one-way transmission and cannot receive communication from the control panel. Therefore, we suggest to set one of the control panel outputs in arming/disarming signalization (so-called chirp) and to connect an acoustic signaler to this output. This will facilitate use of the panel.

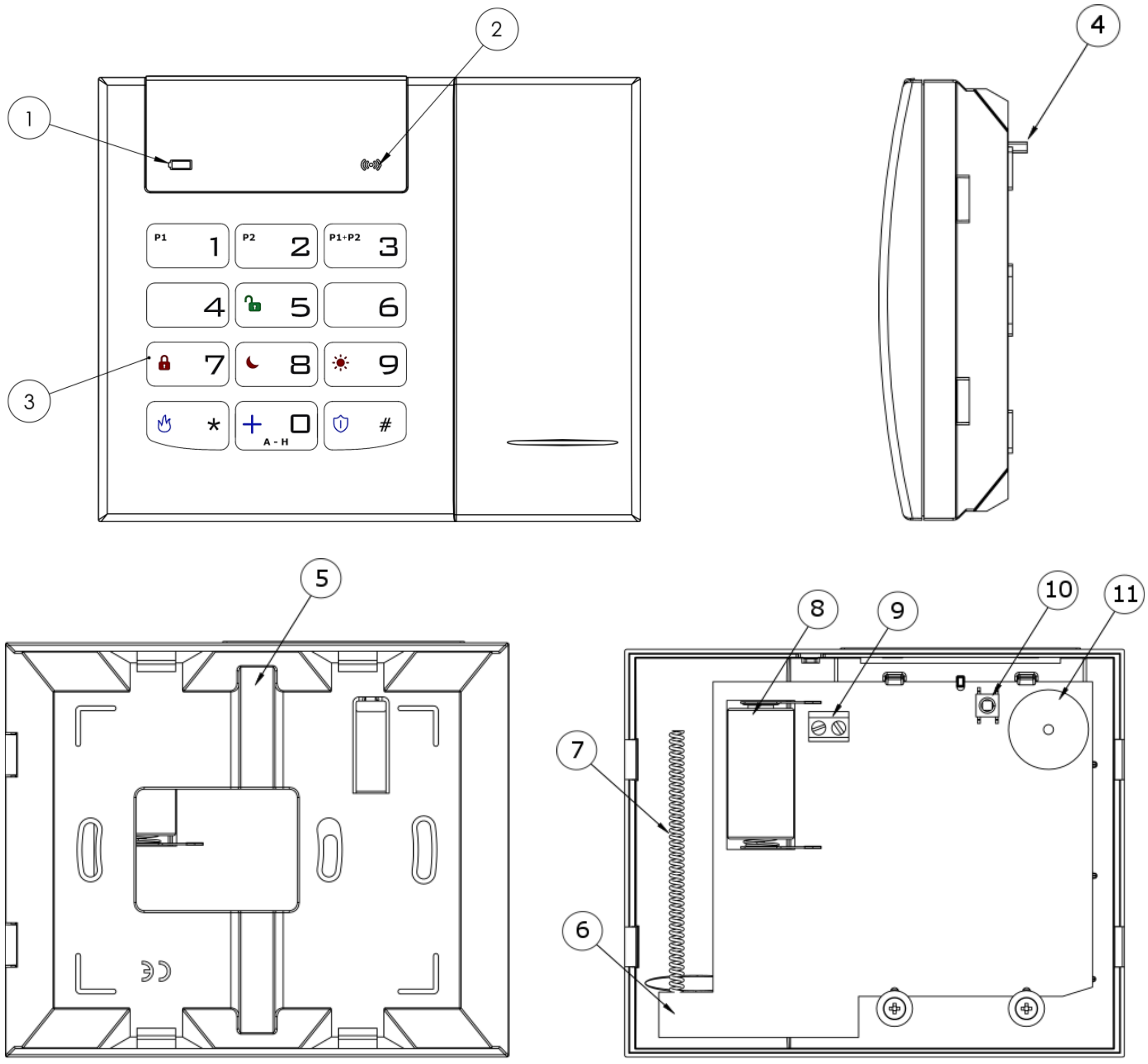
We recommend to have at least one wire keypad KP32 installed in the alarm system in order to set parameters of the control panel, display system status and change user codes. We also recommend to use AVA application with the control panel CPX230NWB to facilitate controlling operation of our alarm control panels.

3.7.1. Adding KP2W to the system

The wireless keypad KP2W can be introduced to the alarm system memory in a manner similar to wireless sensors. There are two methods available:

- Using KP32 keypad, see chapter 4.3.16.1. Wireless sensors configuration.
- Using software "GPRS Transmitter configurator", see chapter 6.3.2. Wireless zones.

3.7.2. Description of keypad elements



Drawing 7. KP2W 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>**

Buttons on the KP2W keypad function the same as on the KP32 keypad (see section 3.6.1 Description of keypad elements - 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 anti-sabotage switch is closed. Unauthorized disassembly of the keypad will send the message to the alarm control panel.

5. **Canal for wires**
6. **Mainboard**
7. **Antenna 433,92MHz**
8. **Battery**

   Lithium Battery CR123A 3V.

9. **Screw Connector**

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

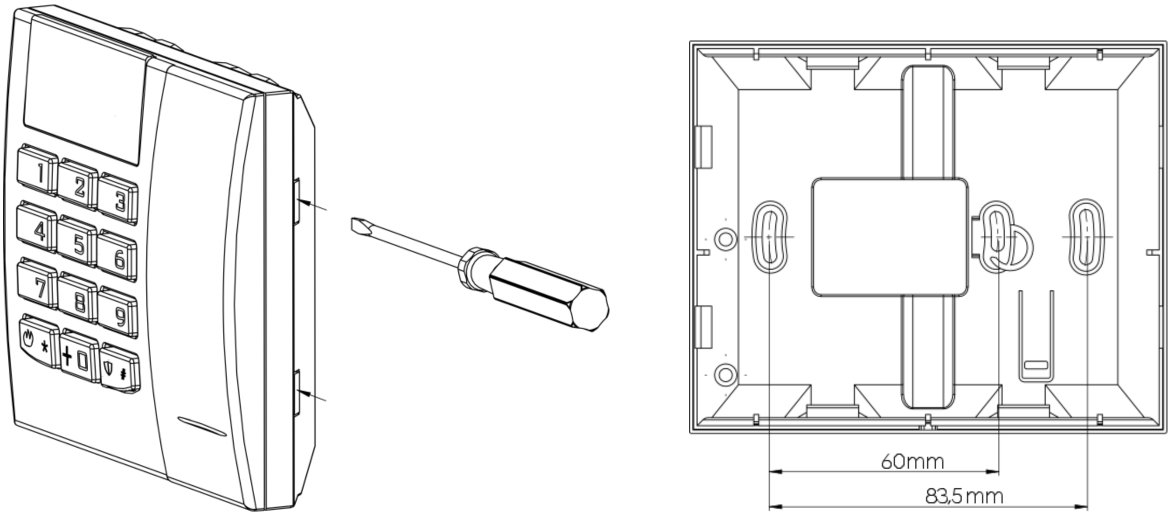
10. **Sabotage sensor (tamper)**
11. **Buzzer**

3.7.3. 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, keyboard use (arming/disarming) 2 times a day, open door switch closed, working temperature 20°C

3.7.4. Keypad installation



Drawing 8. Case opening latches and mounting holes

The keyboard KP2W is intended for indoors installation on dry and smooth surface. Usually it is located on the wall, by the front doors, 120-140 cm above the ground.

1. Open the keypad case – insert a flat-head screwdriver in the hole in the bottom part of the case and press the latch. Then, press the other latch and carefully draw aside both parts of the case, starting from the bottom one.
2. Mark and drill holes in the wall for assembly of the back part of the case.
3. Screw down the back part of the case.
4. Put in a CR123A battery as per markings on the plate. The incorrect placement of the battery will result in the failure to start the device. As soon as the battery is inside, two LEDs (for battery – red one, for transmission – blue one) and keys backlight will light up temporarily.
5. Put together the front part of the case with the back one starting from the top of the case. Make sure that the keypad is properly assembled and the tamper switch is pressed down.

3.7.5. Door opening sensor

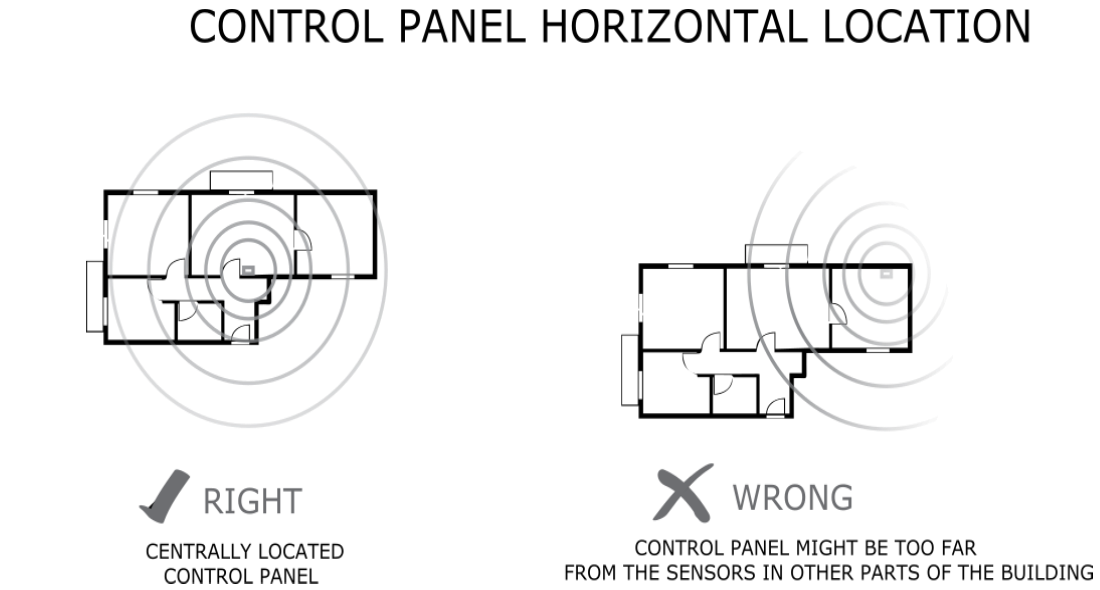
The keyboard KP2W is equipped with a feature enabling connection of opening sensor (reed relay), which can be used as a door opening sensor.

The NC connector (normally closed) used in this case should be shorted, if the possibility to connect the sensor is not used. The connector can be found on the keypad board and labelled 9 in Drawing 7.

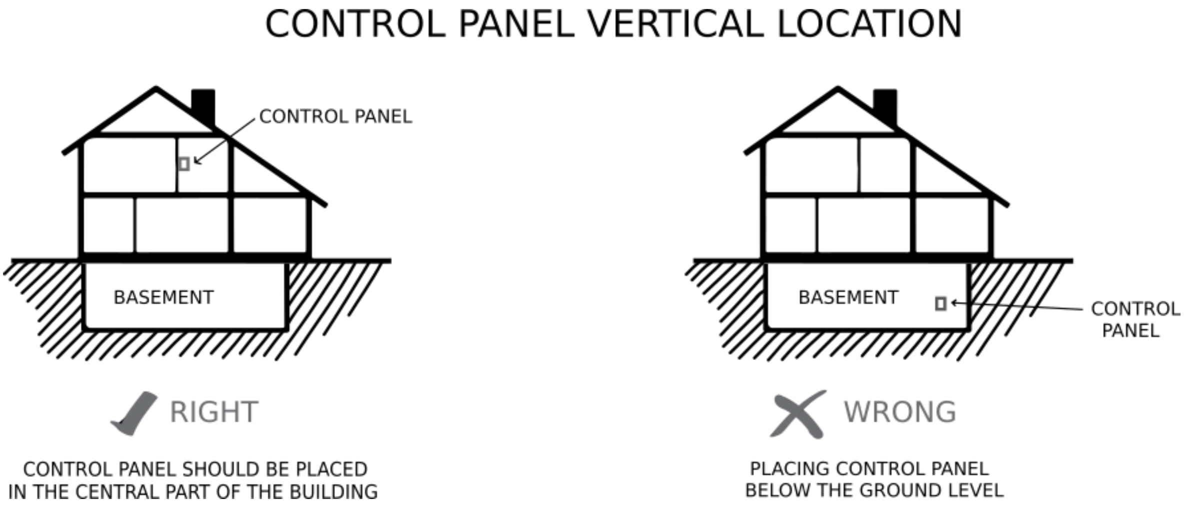
This sensor in the alarm system CPX230NWB will have assigned the same zone number as the keypad.

3.8. CONTROL PANEL LOCATION

The control panel should be located in the control panel part of the object. The central location of the control panel usually provides good communication with all wireless detectors. See drawings 9 and 10.

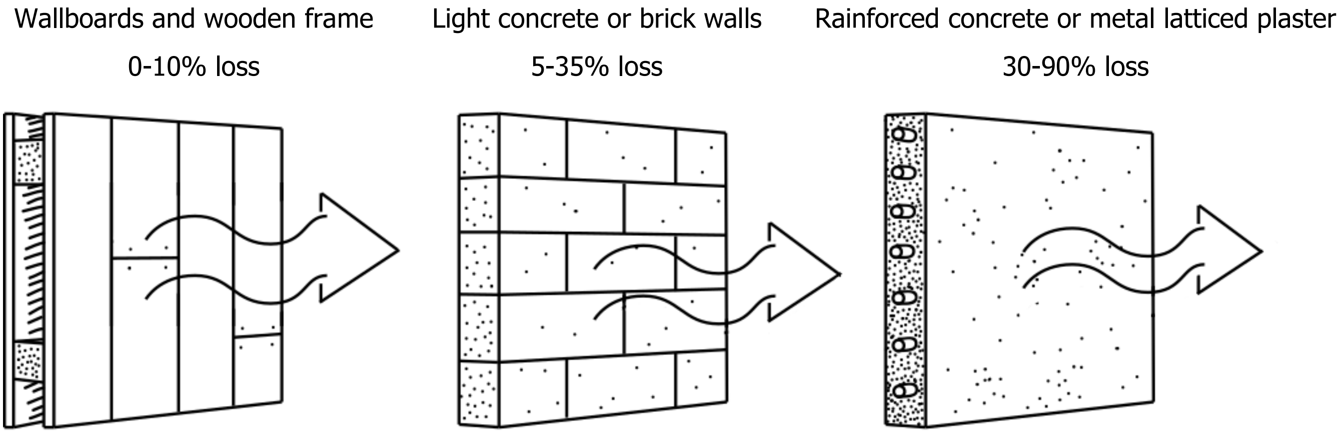

CONTROL PANEL HORIZONTAL LOCATION
RIGHT
CENTRALLY LOCATED CONTROL PANEL
WRONG
CONTROL PANEL MIGHT BE TOO FAR FROM THE SENSORS IN OTHER PARTS OF THE BUILDING

Drawing 9. Control panel horizontal location


CONTROL PANEL VERTICAL LOCATION
CONTROL PANEL
BASEMENT
RIGHT
CONTROL PANEL SHOULD BE PLACED IN THE CENTRAL PART OF THE BUILDING
BASEMENT
CONTROL PANEL
WRONG
PLACING CONTROL PANEL BELOW THE GROUND LEVEL

Drawing 10. Control panel vertical location

The radio waves are attenuated by walls and other obstacles. Lowest attenuation have wallboards and wooden frame. Medium attenuation have light concrete and brick walls. Reinforced concrete and metal latticed plaster have the greatest attenuation. The drawing 11 shows the signal loss through various different types of materials. (**NOTE:** the figure is simplified, only for illustration – remember that radio waves propagate multidirectionally).

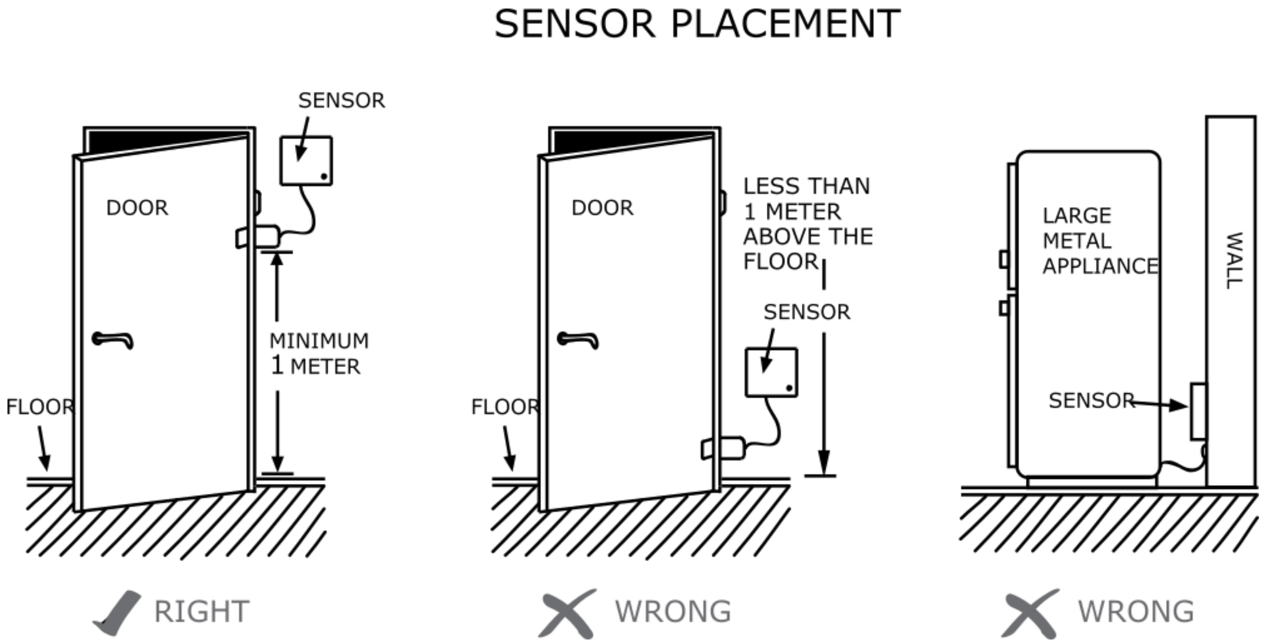

Wallboards and wooden frame
0-10% loss
Light concrete or brick walls
5-35% loss
Rainforced concrete or metal latticed plaster
30-90% loss

Drawing 11. Signal loss through construction materials

3.9. WIRELESS DETECTORS INSTALLATION RECOMMENDATIONS

The wireless detectors should be located relative to the panel in such a way as to be on the same side of the control panel as the radio antenna and electronic components. In this way you get the best radio coverage.

Additional installation tips describes the drawing 12.



Drawing 12. Sensor placement

4. SERVICE MODE

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

Service mode is intended for configuration of basic parameters related to zones, outputs and partitions. It allows to manually, using a keypad, program all correlations necessary for correct system operation.
After the service mode is initiated a number of service functions are available. To configure the system, enter the number of function and its arguments, related to the function, as following:

<Number of function> # **<Argument>** #

where:

Number of function – a number of one of available service functions,
Argument – the argument of a given service function (of BIN or DEC type).

Each service function has one of two argument types: binary (BIN) or decimal (DEC) . Handling each of the two types of arguments is presented below:

Binary type (BIN)
When the binary argument type function is entered, the current option status is displayed with LEDs relevant to a given option of the function on/off. Press 1 to 9 buttons to change the status of LED and the option it corresponds to. Options 10 – 16 may be changed by long press (for 2 sec) the buttons 0 – 6. The installer can change the option status as many times as they want. When the desired status is set, press # to confirm or * to exit without saving changes.

Decimal type (DEC)
Service function that accepts decimal type arguments can also accept any length strings of decimal numbers, not exceeding the maximum length pre-defined for the function. When a character is entered, a cursor gets automatically ready for entering the next character. Press # to save currently entered changes and exit the service function, press * to cancel entered changes and exit the service function. Before you press any key on a keypad, the currently programmed parameter value is displayed. It is presented by displaying subsequent digits of the parameter with a short pause in between. When all digits of the parameter are displayed, the pause is longer.
After pressing the numerical button, the lately entered digit is displayed on a keypad. The way the digits are displayed on a keypad is presented in the table below:

Number entered	LEDs on
0	**1 2 3 4 5 6 7 8**
1	**1** 2 3 4 5 6 7 8
2	1 **2** 3 4 5 6 7 8
3	1 2 **3** 4 5 6 7 8
4	1 2 3 **4** 5 6 7 8
5	1 2 3 4 **5** 6 7 8
6	1 2 3 4 5 **6** 7 8
7	1 2 3 4 5 6 **7** 8
8	1 2 3 4 5 6 7 **8**
9	**1** 2 3 4 5 6 7 **8**
10	1 **2** 3 4 5 6 7 **8**
11	1 2 **3** 4 5 6 7 **8**
12	1 2 3 **4** 5 6 7 **8**
13	1 2 3 4 **5** 6 7 **8**
14	1 2 3 4 5 **6** 7 **8**
15	1 2 3 4 5 6 **7 8**

4.1. ACTIVATION OF SERVICE MODE

To activate the service mode the installer code authorization is required.

[☀ 9] [☀ 9] [⛉ #] **<Installer code>** [⛉ #]

3 beeps will confirm the correct input of the code and function number. PROG LED on will inform that currently, the user is in service mode. When any service function is entered, PROG LED will be blinking. After exit from the function, PROG LED will be lit constantly again, informing that the user is in the main service mode menu.

4.2. EXIT FROM SERVICE MODE

To exit the service mode press [+ A-H □] and confirm with [⛉ #]. Using that function will trigger the control panel's reset using configured parameters.

The device will exit test mode automatically after 5 minutes without pressing the buttons and system will restart.

4.3. INSTALLER MENU

After enter the service mode You get permission to configure alarm central. By this commands You can get into some menu sections (more information about procedures You will get in chapters bellow):

[P1 1] [⛉ #]	Installer code change
[P2 2] [⛉ #]	Power loss time report

3 #	Reset to default settings
4 #	System options
5 #	Users remote manager
6 #	Expanded system options
7 # **<code length>** #	Access code length
8 # **<time[sec]>** #	Alarm history notification disabling delay
9 # **<time[h]>** #	Time to detect loss of wireless detectors
9 0 # **<1/2/3><number** #	Entering and changing ACN numbers
9 1 # **<1/2/3>** #	Deleting ACN numbers and set-up
1 0 # 1 #	Switch off periodic repeating of wireless detectors loss events
1 1 # **<time[h]>** #	Periodic repeating of wireless detectors loss events
1 **<XX> <Y>** # **<Z>** #	Zones configuration
2 **<XX> <Y>** # **<Z>** #	Outputs configuration
3 **<XX> <Y>** # **<Z>** #	Partitions configuration
4 **<XX> <Y>** #	Wireless zones configuration
5 **<XX> <Y>** #	Remote controllers configuration
6 **<XX> <Y>** #	Emergency buttons

4.3.1. Installer code

The installer code can be changed here. 3 beeps will confirm the successfully entered function.

1 # **<Installer code>** # **<Installer code>** #

where:

Installer code – new installer code (from 4 to 7 digits)

You can press * any time to exit without saving changes.

4.3.2. Power loss

The function determines time in seconds after which failure is to be reported. The function's argument is of decimal type. 3 beeps will confirm the successfully entered function.

To change /configure the time:

P2 2 ⓘ # **<Time>** ⓘ #

where:

Time – time in seconds

You can press ✋ * any time to exit without saving changes.

4.3.3. Reset to default settings

That function resets the settings to their default configuration, accessible from the service mode level. Additionally, the function sets the default output options and default installer code. The wireless detectors and remote controls are not deleted.

In order to protect the settings against accidental modification, the function is to be confirmed with installer code. 3 beeps will confirm the successfully entered function. Using that function will trigger the control panel's reset using default parameters.

P1+P2 3 ⓘ # **<Installer code>** ⓘ #

You can press ✋ * any time to exit without saving changes.

4.3.4. System options

That function allow to switch on and switch off additional options of the system. The argument of the function is BIN type. By pressing 1, 2, 3, 4, 5, 6, 7 and 8 keys, you can switch on/off proper option. 3 beeps will confirm the successfully entered function.

4 ⓘ # **<Options>** ⓘ #

Where:

Options – number of option (BIN type parameter):

- **1** – Enable faults memory indication – when is switched off, LED SYSTEM does not show by blinking the faults that are not active; you can display inactive faults by choosing "faults memory" user function.
- **2** – Disable ATS monitoring. If this option is enabled, ATS failure isn't signaled to the user in any way on the keypad and it doesn't cause arm prevention.
- **3** – Request arming confirmation (by pressing #) in case of failure. If this option is enabled, the user is additionally notified of system failures when arming the system. The wired keypad produces a continuous sound, the ALARM and SYSTEM diodes start flashing slowly and error codes are displayed on diodes 1–8 (see User's Manual, section 7.6 Arming the system with a fault). To arm the system press # button. Information on failures and triggering are available after entering with the use of the wired keypad the user's function: failure memory and current state of inputs. In the case of a system failure, if the option is disabled, the arming lock will be automatically omitted.
- **4** – Access to alarm and fault memory requires authorization. If this option is enabled, checking alarm memory and fault memory is available only after a user code is entered. This option must be enabled in order to comply with EN 50131 standard requirements for Grade 2.

- **5** – Alarms and inputs interlocking states are not displayed. If this option is enabled, alarms and zone state are not displayed on the keypad. This option must be enabled in order to comply with EN 50131 standard requirements for Grade 2.
- **6** – Temporary keyboard lock after three access failures. If this option is enabled, the keypad will be blocked for 90 seconds, after entering an invalid code three times. After this period, another lock will occur after entering a wrong code three times. The counter of invalid codes will be reset after a correct code is entered (e.g. after entering invalid code two times). This option must be enabled in order to comply with EN 50131 standard requirements for Grade 2.
- **7** – Use duress code. Duress code is used to inform the monitoring station about a distress event. Each user has his own duress code.

You can press * any time to exit without saving changes.

4.3.5. Users remote management

That function allow to switch on or switch off remote users management. The argument of the function is BIN type. By pressing key 1, you can switch on/off option. 3 beeps will confirm the successfully entered function.

5 # **<Options>** #

Where:

Options – number of option (BIN type parameter):

- **1** – enable/disable users remote management.

You can press * any time to exit without saving changes.

4.3.6. Expanded system options

An additional system function used to turn individual options on or off. The argument of this function is of the BIN type. 3 beeps will confirm the successfully entered function.

6 # **<Options>** #

Options – option number:

- **1 –** Premises lock. This function turns off the ability to arm the control panel. When this function is turned on, the user will not be able to arm the site by any way (i.e. SMS/GPRS, remote, arming inputs, schedules, wired keypad, wireless keypad). Disarming the system is possible, however. Attempts to arm will be rejected by the control panel.
- **2 –** Defaults restoral lock. This function allows the user to turn off the ability to restore the factory-default installation engineer code. However, when restoring default settings using the Configuration, when the "Restore device’s default settings" option is selected, a window with a request to enter the installer code or service code (ATS) will appear.

  When this function is turned on, the Manufacturer recommends that installer code and service code (ATS) code are changed.

NOTE: If newly set codes are lost, it will be necessary to send the blocked devices to the EBS technical service.

- **3** – Allow quick arming without user authorization. When this function is turned on, it is possible to quickly arm the system using a keypad, without the need to enter the user authorisation code.
- **4** – After disarming disable alarm history notification. With this option checked, 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, (refer to chapter 4.3.8) 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.
- **5** – Prevent arming using wired keypad when inputs are triggered or sabotaged. If this option is selected, you can't arm the system with KP32 if the detectors have been triggered or tampered with. Triggering/tampering with any detector assigned to the system is signalled by the diodes READY – D going off – in the case of a detector assigned to Partition 1; 4 in the case of a detector from Partition 2. If the system has been broken into two partitions, you can't arm the control panel even, if the detector has been triggered/tampered within only one of them. When attempting to arm the system, the wired keypad emits a high one-second sound and, at the same time, the diodes GROUP, ALARM, SYSTEM and PROG will go on for about 4 seconds. System failures do not affect this option.
NOTE: This option is available since the firmware version 2.8.8.

You can press * any time to exit without saving changes.

4.3.7. Access code length

The function enables setting the length of the administrator and user codes (the change applies to all users). The code range is from 4 to 7 digits. By default, this value is set to 4.

7 # **<code length>** #

Where:

code length – code length code from the range of 4 to 7.

Reducing the code length is possible only if the shortened user codes do not conflict with each other.

Example:
There are 5-digit codes in the CPX database – 44440, 44444, and 44449. It will not be possible to shorten the code to 4 digits due to the conflict of identical resulting codes. The change will not be accepted, which the keypad will signal with a several seconds long continuous sound. In such a case, one solution is to delete a user or users who have similar codes.

1. **If the user code in the CPX database is shorter than the defined value, then '0' will be added to the codes at their ends:**
   <u>Example:</u> If the code 1234 exists in the database, then after code length is changed to 6 digits, the code will appear as 123400.
2. **If a user code in the CPX database is longer than the defined value, then the access code will be the "n" first digits, according to the value set.**
   <u>Example:</u> If the code 1234567 exists in the database, then after code length is changed to 5 digits, the code will appear as 12345.
3. **For codes under duress:**
   - **If the code 12345 exists in the database, then after code length is changed to 7 digits, the code will appear as 1234500, so the code under duress will be 1234501.**
   - **If the code 12345 exists in the database, then after code length is changed to 4 digits, the code will appear as 1234, so the code under duress will be 1235.**

4.3.8. Alarm history notification disabling delay

8 # **<time[sec]>** #

This function is only available after checking "After disarming disable alarm history notification" option. It sets the delay time in seconds, after which the alarm memory will no longer be shown on the keypad. It means, that when the system is armed, and there will be violation of input zones shown by the F and 6 diodes blinking, then after disarming and previously defined time the diodes will turn off. The alarm memory will still be accessible with 3# function, until the user decides to delete it.

4.3.9. Time to detect loss of wireless detectors

This function allows you to set the time after which a notification is sent to the monitoring station about the loss of the wireless detector.

9 # <time [h]> #

The time is expressed in hours. The default value is 6 hours, the minimum is 2 and the maximum is 24.

NOTE: This option is available since the firmware version 2.8.8

4.3.10. Switch off periodic repeating of wireless detectors loss events

This function allows you to switch off only the option periodic repeating to the monitoring station events about loss of the wireless detector.

1 0 # 1 #

NOTE: This option is available since the firmware version 2.10.0

4.3.11. Periodic repeating of wireless detectors loss events

This function allows you to switch on periodic repeating of wireless detector loss events to the monitoring station (starting from the first loss).

1 1 # **<time [h]>** #

The time is expressed in hours. The default value is 6 hours, the minimum is 2 and the maximum is 24.

NOTE: This option is available since the firmware version 2.10.0.

4.3.12. ACN numbers for communication in the Contact ID format

When transmitting data in the Contact ID format, you can set up individual numbers for system account identification – ACN0, and its subsystems accounts, partition 1 – ACN1 and partition 2 – ACN2. This allows you to determine, which part of the system the signal from.
NOTE: This option is available since the firmware version 2.9.0

4.3.12.1. Entering and modification of ACN Numbers

If ACN0 number is entered, it is attached to each system event sent to the monitoring station. System events are those that provide information about the entire system, i.e. power failure, modem reset, clock loss.

If numbers ACN1 and ACN2 are entered, the ACN1 is attached to each non-system event (with partition ID 1 and/or 2) with information about partition 1, and to events with information about partition 2 – the ACN2. Non-system events are those with information about particular partitions, i.e. about arming/disarming partitions 1 and/or 2, alarms activated by triggering the detectors assigned to partitions.

In order to define numbers, press the keypad:

9 1 # **<button 1/2/3> <number>** #

Where:

button 1 – setting or changing the ACN1 number of the partition 1 account

button 2 – setting or changing the ACN2 number of the partition 2 account

button 3 – setting or changing the ACN0 number of the system account

number – ACN number – any four hexadecimal characters

If diodes 1, 2 and 3 are turned off, it means the ACNs have not been set up. The ACN0 number is set by pressing button 3, keying in four hexadecimal characters and pressing the confirmation button ⛉#. The ACN1 and ACN2 numbers are set in the same way. If the diodes are turned on, pressing buttons 1, 2, 3 allows you to see the assigned numbers and to change them if necessary.

⚠ **NOTE: If you have assigned an account number only to one of the partitions, the same number will be automatically assigned to the other partition and to the system.**

4.3.12.2. Delating the ACN numbers and changing option settings

To delete numbers or set up system event messages, press:

✱9 +0 ⛉# **<Button 1/2/3>** ⛉#

Where:

button 1 – means <u>deleting</u> the ACN0 number sent to the system account

button 2 – means <u>deleting</u> the ACN1 and ACN2 numbers sent to the partition 1 and 2 accounts

button 3 – set-up how system events are to be sent, where:

- diode 3 is off – system events are sent only to the system account
- diode 3 is on – system events are sent to all accounts

⚠ **NOTE: If you have deleted the ACN0 number, the ACN1 and ACN2 numbers will be also deleted.**

4.3.13. Zones configuration

Wired and wireless zones can be configured using complex service functions, after activation of which, all the parameters related to the relevant zone can be given subsequently or in a form of series of service functions that configure one zone-related parameter. Additional configuration of wireless zones is described in item 4.3.16.

Codes of zone configuration functions are defined as per the following pattern:

P1 1 **<XX> <Y>** ⛉# **<Z>** ⛉#

where:

XX – zone number from **01** to **32**, the table below shows zones names 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
Number	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

Entering number **00** will change the parameters for all zones in the system,

Y – number of parameter related to a given zone,

Z - number (or value) of the next parameter.

- **For Y=0** – complex function, the initiation of which configures the parameters listed below as another set of parameters;

Example:

a) change of many parameters at the time for zone A1 using complex functions – zone A1 is to be set as immediate circuit, in NC mode, to be blocked after 8 violations and generate alarm when violated after arming, with the 500ms sensitivity:

P1 1 +A-H 0 P1 1 +A-H 0 # +A-H 0 # # P1 1 # 8 # P2 2
5 +A-H 0 +A-H 0

⚠ **Note: In case of complex function (programming many parameters at the time) after the parameter is entered and confirmed wit #, the parameter is saved in the configuration memory and the system waits for entering another parameter, and so on, until all parameters of the complex service function are entered. Press * to cancel changes entered in currently configured parameter only and exit service function – previously entered parameters, confirmed with #, will not be cancelled.**

- **For Y=1** – type of zone response (DEC type parameter). Options from 10 to 13 are selected for longer (about 2 seconds) pressing the key from 0 to 3; possible values for the parameter **Z**:
  - 0 – instant
  - 1 – delay
  - 2 – 24h burglary
  - 3 – arming/disarming by violation
  - 4 – 24h tamper
  - 5 – interior delayed
  - 6 – 24h burglary silent
  - 7 – 24h fire
  - 8 – perimeter
  - 9 – perimeter exit
  - 10 – 24h gas
  - 11 – 24h water leakage
  - 12 – night (bypassed)
  - 13 – night with prealarm
  - 14 - arming/disarming by state change (available since the firmware version 2.10.0)
- **For Y=2** – delay **Z** in seconds for the zone of selected "delay" response type (DEC type parameter). For other response types the parameter is irrelevant.
- **For Y=3** – operation mode (DEC type parameter), possible values for the parameter **Z**:
  - 0 – unused zone

- 1 – NC mode
- 2 – NO mode
- 3 – EOL/NC mode
- 4 – EOL/NO mode
- 5 – DEOL/NC mode
- 6 – DEOL/NO mode
- 7 – Wireless mode
- 8 – TEOL mode

Example:

b) change of a single parameter – operation mode of number 2 zone into NO operation mode:

1 0 2 3 # 2 #

- **For Y=4** – number of alarms **Z** after which the zone will be automatically blocked until re-arming (DEC type parameter). If 0, zone will not be blocked**.**
- **For Y=5** – zone options (BIN type parameter), possible values for the parameter **Z**:
    - 1 – zone ignored during arming – i.e. can be violated during partition arming (e.g. delay zone shall be set to that option)
    - 2 – generates alarm when violated after arming
    - 3 – interlocking the zone (bypassing zone) if the zone violated when arming (parameter "After time for exit")
    - 4 – enable/disable the function "Chime". 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.
- **For Y=6** – sensitivity **Z** in milliseconds, i.e. after what time the zones is considered to change its status – default value for **Z** 400ms.

Example:

c) change of sensitivity of all zones into 200 milliseconds:

1 0 0 6 # 2 0 0 #

⚠ **Note: For wireless zones 8 – 32 complex function 1XX0 should not include option (function) 6 – sensitivity. Function 1XX3 (operation mode) displays the value 7 for wireless zones 8 – 32, and the value can not be changed.**

4.3.14. Outputs configuration

Outputs, similar as zones, can be configured using complex service functions after activation of which, all the parameters related to the relevant output can be given subsequently or in a form of series of service functions that configure one output-related parameter. Codes of output configuration functions are defined as per the following pattern:

2 **<XX> <Y>** # **<Z>** #

where:

***XX* –** determines the number of output from **01** to **03**; entering number **00** will change the parameters for all outputs in the system,

***Y* –** number of parameter related to a given output,

Z - number (or value) of the next parameter;

- **For Y=0 –** complex function, the initiation of which configures the parameters listed below as another set of parameters;

Example: Change of many parameters at the time for output 1 using complex function – output 1 is to be set as alarm signaling with activation time 120 seconds:

2 0 1 0 # 1 # 1 2 0 #

Note: In case of complex function (programming many parameters at the time) after the parameter is entered and confirmed with # the parameter is saved in the configuration memory and the system waits for entering another parameter, and so on, until all parameters of the complex service function are entered. Press * to cancel changes entered in currently configured parameter only and exit service function – previously entered parameters, confirmed with #, will not be cancelled.

- **For Y=1 –** type of output (DEC type parameter), possible values for the parameter **Z**:
  - 0 – not used,
  - 1 – signaling alarm,
  - 2 – armed status,
  - 3 – power failure,
  - 4 – ATS failure – no communication with receiving server.
  - 5 – GSM signal jamming indicator
  - 6 – chirp on arm/disarm
  - 7 – chirp on arm/disarm and signaling alarm

Example: Change of 3 output type into triggered by power failure:

2 0 3 1 # 3 #

- **For Y=2 –** time of output activation **Z** in seconds (DEC type parameter), ; if 0 is set, output will operate in bi-stable mode.

Example: Change of a single parameter – operation mode of number 2 output into bi-stable operation mode:

2 0 2 2 # 0 #

It is possible to configure the chirp options using following patterns:

- **For Y=3 –** chirp signal duration **Z** in milliseconds;

Example: change of chirp signal duration of all zones into 600 milliseconds

2 0 0 3 # 6 0 0 #

- **For Y=4 –** interval duration between two following chirps **Z** in milliseconds;

Example: change of interval duration between two following chirps of all zones into 500 milliseconds:

2 0 0 4 # 5 0 0 #

Note: Chirp settings are common to all outputs.

The factory values for both parameters are 250 ms

4.3.15. Partitions configuration

Partition configuration can be configured similarly as zones and outputs, using complex service functions after activation of which, all the parameters related to the relevant partition can be given subsequently or in a form of series of service functions that configure one partition-related parameter. Codes of partition configuration functions are defined as per the following pattern:

3 **<XX> <Y>** # **<Z>** #

where:

XX – determines the number of partition from **01** to **02**; entering number **00** will change the parameters for both partitions,

Y – number of parameter related to a selected partition,

Z - number (or value) of the next parameter;

- **For Y=0 –** complex function, the initiation of which configures the parameters listed below as another set of parameters;
- **For Y=1 –** zones belonging to a partition (BIN parameter). A blinking group diode (from A to D) means that the group is currently being shown. If other groups are continuously lit, it means they contain zones assigned to the selected partition. Diodes switched off means that no zones in the given group are assigned to the defined partition. By pressing buttons from 1 to 8, the user can assign zones from the given group to the selected partition. Switching between groups is possible using the 0 button. No Z parameter; no Z parameter,
- **For Y=2 –** outputs belonging to partition (BIN type parameter), no Z parameter**,**
- **For Y=3 –** time for leaving the partition **Z** in seconds (DEC type parameter),
- **For Y=4 –** alarm time in the partition **Z** in seconds (DEC type parameter),
- **For Y=5 –** partition options (BIN type parameter), possible values **Z**:
  - 1 – Quiet signaling of time for entering (during counting the time for leaving, the buzzer in a keypad is not active)
  - 2 – Quiet signaling of time for leaving (during counting the time for leaving, the buzzer in a keypad is not active)

- **For Y=6** – auto-arming time **Z** for the partition (DEC type parameter, time of day written in the 24-hour notation in the form HHMM),
- **For Y=7** – auto-arming option (BIN type parameter), possible values for the parameter **Z**:
  - 1 – auto-arming activation/deactivation
- **For Y=8** – auto-disarming time **Z** for the partition (DEC type parameter, time of day written in the 24-hour notation in the form HHMM),
- **For Y=9** – auto-disarming option (BIN type parameter), possible values for the parameter **Z**:
  - 1 – auto-disarming activation/deactivation

Notes:

Execution of complex function 3006 (auto-arming time for all partitions) will copy activation/deactivation option from the first partition to the second partition.

Execution of complex function 3007 (auto-arming activation/deactivation for all partitions) will copy auto-arming time from the first partition to the second partition.

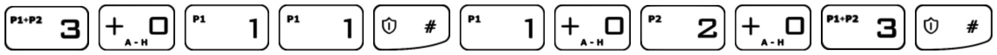
Execution of complex function 3008 (auto-disarming time for all partitions) will copy activation/deactivation option from the first partition to the second partition.

Execution of complex function 3009 (auto-disarming activation/deactivation for all partitions) will copy auto-disarming time from the first partition to the second partition.

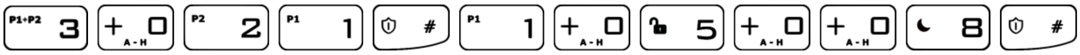
If the time in the device is set forward (eg. when the time is changed to Daylight saving time), and arming or disarming time is in the period which has been omitted, then the hour will be not used. Eg. If the auto-arming time is set to 2:30, and time was changed forward from 2:00 to 3:00, the control panel will not arm.

Examples:

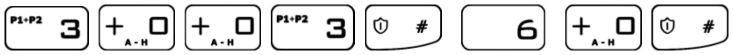
a) change of a single parameter – assigning A1, B2, C3 zones to the first partition:



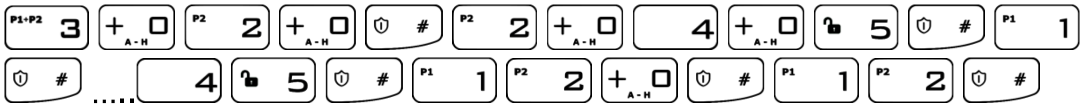
b) change of a single parameter – assigning A1, B5, D8 zones to the second partition:



c) change of time for leaving both partitions into 60 seconds:



d) change of many parameters at the time for partition 2 using complex function – zones A2, B4, C5 and output 1 to belong to partition 2, time for leaving the one to be 45 seconds, alarm time in partition 2 to be 120s and signaling of time for entering and leaving was quiet:



⚠ **Note: In case of complex function (programming many parameters at the time) after the parameter is entered and confirmed with #, the parameter is saved in the configuration memory and the system waits for entering another parameter, and so on, until all parameters of the complex service function are entered. Press * to cancel changes entered in currently configured parameter only and exit service function – previously entered parameters, confirmed with #, will not be cancelled.**

4.3.16. Wireless zones configuration

4.3.16.1. Wireless sensors configuration

Wireless zones can be configured using complex service functions, after activation of which, all the parameters related to the relevant zone can be given subsequently or in a form of series of service functions that configure one zone-related parameter. Codes of zone configuration functions are defined as per the following pattern:

4 **<XX> <Y>** #

Where:

XX – zone number from **01** to **32**, the table below shows zones names 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
Number	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

entering number **00** will change the parameters for all zones in the system,

Y – number of parameter related to a given zone:

For Y=0 – complex function, the initiation of which configures the parameters listed below as another set of parameters:

For Y=1 – Delete a sensor. After selecting this option, you can confirm deleting by pressing # key, or you can cancel function by pressing * key.

Example:

a) delete a wireless sensor B2 (number 10, see the table above):

4 1 0 1 # #

For Y=2 – Add a sensor. After selecting this option, the sabotage button on the sensor has to be pressed. Once the transmission with the sensor is established, its serial number will be displayed on the keypad (hexadecimal value). If accepted, the sensor will be saved.

Example:

a) add a wireless sensor B3 (number 11, see the table above):

4 1 1 2 # (press the sabotage button) #

For Y=3 – Type of a wireless sensor (read only):

0 – no sensor
1 – PIR-10 sensor
2 – MC-10 sensor
4 – SD-10 sensor
5 – PIR-11 sensor
6 – SD-20 sensor
7 – KP2W keypad
8 – MC-11 sensor
9 – FL-10 sensor
12 – GS-21sensor
13 – GS-22 sensor

For Y=4 – Signal strength of wireless detectors. The function allows to check signal strength of wireless detectors. LEDs 1 – 8 will display signal strength from selected wireless detectors. No lighted LEDs indicates no signal.

1 LED – 12% signal strength
2 LEDs – 25% signal strength
3 LEDs – 37% signal strength
4 LEDs – 50% signal strength
5 LEDs – 62% signal strength
6 LEDs – 75% signal strength
7 LEDs – 88% signal strength
8 LEDs – 100% signal strength

At the same time, the keypad indicate the signal strength by a sound. 1 beep means 25% signal strength, 2 beeps means 50% signal strength, 3 beeps means 75% signal strength, 4 beeps means 100% signal strength.

To exit the function press * (or #, if no key has been selected).

Note: During the adding a new wireless detector (function 2), the front cover of the detector should be removed. It is recommended to add wireless sensors individually. To prevent the accidental transmissions from other detectors, only one detector cover should be removed during the procedure of adding a new detector.

4.3.16.2. Delete all wireless sensors

To remove all wireless sensors from the system, enter the following function:

4 0 0 1 #

After entering the function PROG LED is blinking, the other LEDs are off. Pressing # key deletes all wireless sensors, generating 3 beeps and exit the function. If you press * key will exit the function and detectors will not be erased.

4.3.17. Remote controllers configuration

4.3.17.1. Remote controllers configuration

Remote controllers can be configured using complex service functions, after activation of which, all the parameters related to the relevant remote control can be given subsequently or in a form of series of service functions that configure one remote control related parameter. Codes of the remote control configuration functions are defined as per the following pattern:

🔓 5 **<XX> <Y>** # **<Z>** #

Where:

XX – determines the number of remote control for **01** to **32**, the table below shows remote control names 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
Number	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

Y – number of parameter related to a given remote control

Z - number (or value) of the next parameter;

For Y=0 – complex function, the initiation of which configures the parameters listed below as set of parameters.

For Y=1 – Delete a remote control. After selecting this option, you can confirm deleting by pressing # key, or you can cancel function by pressing * key; no **Z** parameter.

For Y=2 – Add a remote control. After selecting this option, any key on the remote control has to be pressed. Once the transmission with the remote control is established serial number will be displayed on the keypad (hexadecimal value). If accepted, the remote control will be saved; no **Z** parameter.

For Y=3 – type of the remote control (read only); no **Z** parameter.
0 – no remote control
2 – RC-10 remote control

For Y=4 – The user to which the remote control is assigned

For Y=5, 6, 7, 8 – Functions for the remote's buttons, where 5 means button 🔒, 6 – 🔓, 7 – ⊙, 8 – ((O)); possible values for **Z**:

0 – no function
1 – arm (fully armed)
2 – disarm
3 – alarm
4 – silent alarm
5 – enable output 1
6 – enable output 2
7 – enable output 3
8 – disable output 1

9 – disable output 2
10 – disable output 3
11 – ambulance (available since Firmware above ver. 2.8.8)
12 – arm immediately (available since Firmware above ver. 2.10.0)

Note:

„Alarm” function is triggering an alarm with audible signal.

„Silent alarm” function is triggering an alarm without audible signal.

Switch on/off output 1, 2 and 3 functions allow control of any external devices.

„Ambulance” function works the same way as „HELP” button on the keypad, ie generates a medical alarm.

“Arm immediately” function allows fully arming the system without counting down time for exit (if is set).

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.

Example:

a) delete a remote control no. 1:

5 0 1 1 #

b) add a remote control no. 1:

5 0 1 2 # (press any key on the remote control) #

4.3.17.2. Delete all remote controllers

To remove all remote controllers from the system, enter the following function:

5 0 0 1 #

After entering the function PROG LED is blinking, the other LEDs are off. Pressing # key deletes all remote controllers, generating 3 beeps and exit the function. If you press * key will exit the function and remote controllers will not be erased.

4.3.18. Emergency buttons

To configure emergency buttons, use the following pattern:

6 **<XX> <Y>** # **<Z>** #

where:

XX – defines the alarm button according to the coding:

- **00** – a change of settings of all alarm buttons
- **01** – FIRE button, activating the fire alarm
- **02** – HELP button, activating the medical alarm
- **03** – PANIC button, activating the break-in alarm

Y – number of parameter related to a given emergency button;

Z - number (or value) of the next parameter;

- **For Y = 0** – complex function, the initiation of which configures the parameters listed below as set of parameters.
- **For Y = 1** – Configuration emergency button, possible values for the parameter **Z**:
  - 1 – enable/disable emergency button:
  - 2 – output 1
  - 3 – output 2
  - 4 – output 3

After confirming the desired option, the output numbers assigned to the given alarm button are displayed. By using buttons 2–4, you can change the status of outputs that are activated if the alarm is triggered off by the function key that is being set up. For functions that enable or disable all buttons, their outputs will remain unchanged.

Functions which configure all three buttons, will not change the outputs setting.

Example:

a) enabling all emergency buttons:

6 0 0 1 # 1 #

b) enabling "panic" (burglary) function (# held) and changing output 2 and output 3 state:

6 0 3 1 # 1 3 4 #

4.4. TEXT MESSAGES

In order for installer to be able to configure text messages, administrator has to grant him necessary permission first. This can be achieved by typing in following code:

5 2 # **<admin code>** #

Next, installer's access to text messages can be changed by pressing the 1 key. This will toggle LED 1. When the LED is active, installer is granted the access, when led is inactive, installer is refused access to text messages. Choice of installer's permissions can be accepted by pressing the # button.

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 (" ").

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

Using following commands, the installer can set up text messages and get the information about it.

Setting the phone number	
Format	XXXX SETTELNUM=ID,NUMBER
Command description	Setting the phone number for pointed index on the phone number list XXXX – service code (ATS) or admin code or installer code (administrator has to grant him necessary permission first) 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 description	SETTELNUM:OK – command accepted SETTELNUM:ERROR – command rejected by the system

Getting the phone number	
Format	XXXX GETTELNUM=ID
Command description	Getting the phone number for pointed index on the phone number list XXXX – service code (ATS) or admin code or installer code (administrator has to grant him necessary permission first) ID – index of phone number on the list, possible values: 1 to 10 *Example: 1234 GETTELNUM=2*
Feedback message description	GETTELNUM=ID,NUMBER – information about phone number GETTELNUM:ERROR – command rejected by the system

Setting the content of text message	
Format	XXXX SETMESSAGE=ID,MESSAGE_without_spaces XXXX SETMESSAGE=”ID,MESSAGE_with_spaces”
Command description	Setting the content of text message under the pointed index XXXX – service code (ATS) or admin code or installer code (administrator has to grant him necessary permission first) ID – index of text, possible values: 1 to 32 MESSAGE – content of the text message *Example: 1234 SETMESSAGE=4,Robbery*
Feedback message description	SETMESSAGE:OK – command accepted SETMESSAGE:ERROR – command rejected by the system

Getting the content of text message	
Format	XXXX GETMESSAGE=ID
Command description	Getting the content of text message under the pointed index XXXX – service code (ATS) or admin code or installer code (administrator has to grant him necessary permission first) ID – index of text, possible values: 1 to 32 *Example: 1234 GETMESSAGE=30*
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	
Format	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 – service code (ATS) or admin code or installer code (administrator has to grant him necessary permission first) 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 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	
Format	XXXX GETUSERSMS=EVENT
Command description	Getting the content of a text message and a phone number assigned to the specified event. XXXX – service code (ATS) or admin code or installer code (administrator has to grant him necessary permission first) EVENT – a short name of the event, possible event names are listed at the end of this chapter *Example:* 1234 GETUSERSMS=ARM1
Feedback message description	GETUSERSMS=EVENT:TELNUM,MSG_ID – information about text message and phone number assigned to the event GETUSERSMS=EVENT:ERROR – command rejected by the system

Acquiring the state of partitions	
Format	XXXX GETARMED
Command description	Acquiring the information which partitions are armed/disarmed XXXX – service code (ATS) or admin code or installer code (administrator has to grant him necessary permission first) *Example: 1234 GETARMED*
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, possible values: 0 – disarmed 1 – armed GETARMED:ERROR – command rejected by the system

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

Getting the name of partition, zone, outputs, users and system	
Format	XXXX GETNAME=ELEMENT,[NR]
Command description	Acquiring the name ofthe 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. XXXX – service code (ATS) or admin code or installer code (administrator has to grant him necessary permission first) Possible values position ELEMENT: PARTITION - Acquiring the name of partition; numbers 1 and 2 ZONE - Acquiring the name of input zone unit corresponding to the indicated number; the numbers from 1 to 32 OUTPUT - Acquiring the name of output corresponding to the indicated number; the numbers from 1 to 3 USER - Acquiring the name of user with the specified number; the numbers from 1 to 32 SYSTEM - Acquiring the name of object which panel and alarm system were installed. Note: here position "nr" does not exist. *Example: 1234 GETNAME=PARTITION,1*
Feedback message description	GETNAME=ELEMENT,[NR],VALUE - command executed correctly, the name of element (NOTE: If the name has not been changed (remains the default), it will not be given in the reply). GETNAME:ERROR-PERMISSION - you do not have permission to execute this command GETNAME:ERROR-FORMAT - wrong format command GETNAME:ERROR-VALUE – wrong value GETNAME:ERROR-PERMISSION - command rejected; other errors

List of events handled by the SETUSERSMS and GETUSERSMS commands	
Alias name	Description
ARM1	Partition 1 fully armed
ARMSTAY1	Partition 1 armed in perimeter mode
ARM2	Partition 2 fully armed
ARMSTAY2	Partition 2 armed in perimeter mode
DISARM1	Partition 1 disarmed
DISARM2	Partition 2 disarmed
INPUT1 (to INPUT32)	Violation of zones 1…32
INPUT1-OFF (to INPUT32-OFF)	Violation of zones 1…32 ended
INPUT1-TAMPER (to INPUT32-TAMPER)	Sabotage of zones 1…32
INPUT1-TAMPEREND (to INPUT32-TAMPEREND)	Sabotage of zones 1…32 ended
INPUT1-LOCK (to INPUT32-LOCK)	Bypass of zones 1…32
INPUT1-UNLOCK (to INPUT32-UNLOCK)	Bypass of zones 1…32 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 DETECTOR32-LOST)	Detector 1…32 signal lost
DETECTOR1-OK (to DETECTOR32-OK)	Detector 1…32 signal restored
DETECTOR1-PWR (to DETECTOR32-PWR)	Detector 1…32 battery low
DETECTOR1-PWROK (to DETECTOR32-PWROK)	Detector 1…32 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

5. CONFIGURATION WIZARD

5.1. PRELIMINARY NOTES

The **Configuration wizard of GPRS transmitters** can be downloaded from www.ebs.pl (login: ebs, password: ebs). Activate the option of installation wizard which leads through the program installation process. By default it will be installed in C:\Program Files\EBS\ directory. The installation wizard can also create shortcuts to the program on the desktop and in the Windows menu.

If it is the first use of the equipment, SIM card shall not be inserted into the slot until the equipment is programmed using the above software. Otherwise, SIM card can be blocked during the attempts of giving an incorrect PIN code. Alternatively, you can use SIM card with PIN code authorization deactivated.

In case of remote programming, SIM card must be inserted before the configuration settings transmission is initiated. In this case use either SIM cards with PIN code authorization deactivated or change the PIN code using a mobile phone before the card is inserted into the equipment.

5.2. COMPUTER – REQUIREMENTS

The minimum requirements for PC computer on which the configuration wizard is to be installed are the following:

Hardware:

- Processor 1GHz, 32-bit (x86) or 64-bit (x64)
- 1 GB RAM (for 32-bit) or 2 GB RAM (for 64-bit)
- 4,5 GB HDD,

Software:

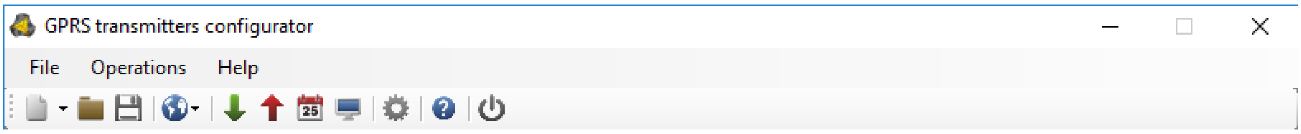
- Operating system: Windows 7 or newer
- .NET Framework 4.5 software or newer.

5.3. PROGRAM FUNCTONS

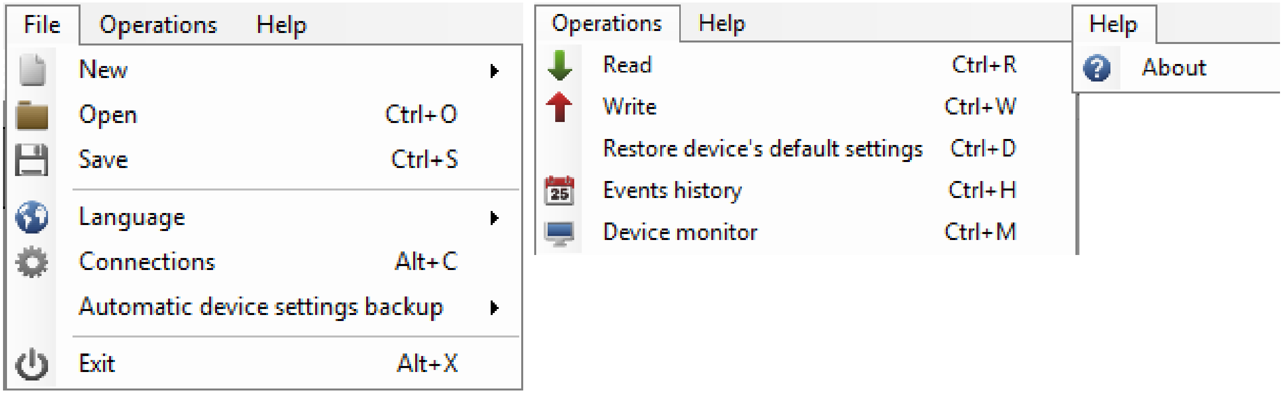
After the program is installed and started, the main window will be displayed on the screen. From that level you can access both, program functions and programmable parameters (see chapter 6.).

The main program window was divided into a few areas.

Main menu: located in the top section of the window, contains control and program configuration functions.



The main menu is composed of the following:

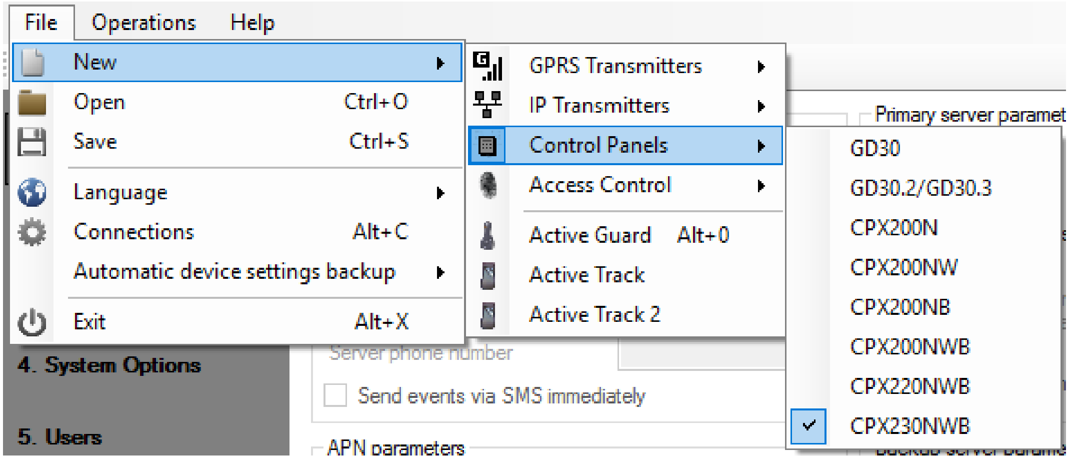


Main menu is also reflected in the visual form of icons on a taskbar:

5.3.1. Menu -> File

5.3.1.1. Menu -> New

Opens a new set of parameters. In this option configuration parameters of the equipment can be edited.



Select a relevant type of the equipment: CPX230NWB

5.3.1.2. File -> Open

If you have a file with recorded settings you can use it for programming another equipment. First, indicate a directory where the file was saved, then give the file name. User can modify the received data. In order to be effective the implemented changes must be sent to the equipment.

5.3.1.3. File -> Save

If you program many pieces of equipment in various configurations, you do not need to remember each configuration. You can save all settings on your hard drive under a specific name and read it later on. The function records all information from the configuration wizard's windows on a hard drive. After calling the function, a window asking for file name is displayed. By default, data is saved in files with **.cmi** extension.

5.3.1.4. Menu -> Language

This option allows selecting one of available languages (defined in enclosed external language files).

5.3.1.5. File -> Connections

Before you start the equipment programming, define the type of connection to be used.

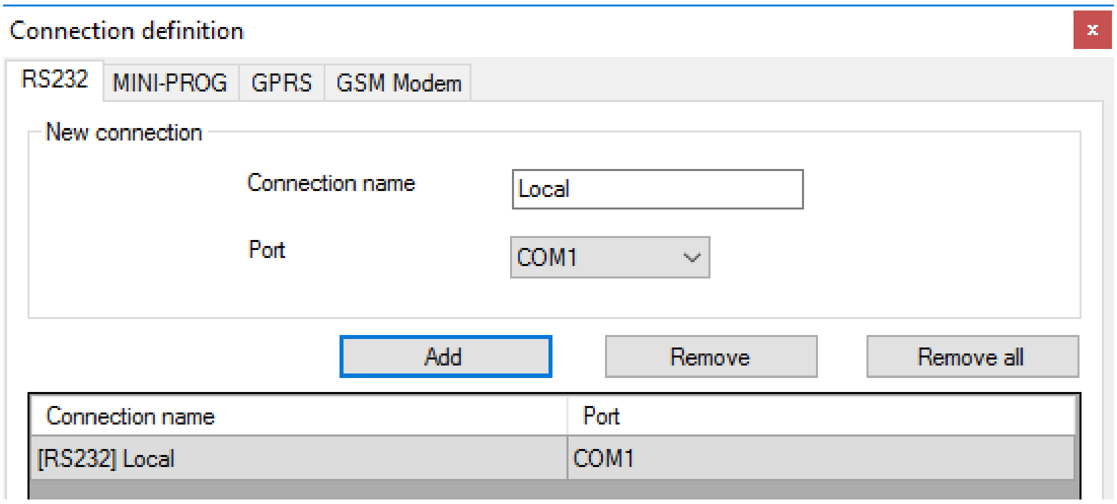
There are two programming methods available: local and remote.

5.3.1.5.1. Local connection

Local connection means that configuration wizard (or, in fact, a computer, on which it is installed) is directly connected to a relevant connector of the alarm control panel via dedicated programming cable using RS-232 serial port (GD-PROG) or USB port or Bluetooth (MINI-PROG-BT, SP-PROG-BT). All channel connection (also USB and Bluetooth) "open" virtual COM serial ports used in communication control panel-Configurator.

To program the equipment or perform other activities (i.e. read the settings from the equipment, change the firmware, etc.) you have to define the connection parameters.

For the above purpose you shall use the following window, available after activating File option from the Main Menu and selecting Connection function or after clicking ⚙ icon on a taskbar and opening RS232 tab.



Connection name: Local

Port: COM1

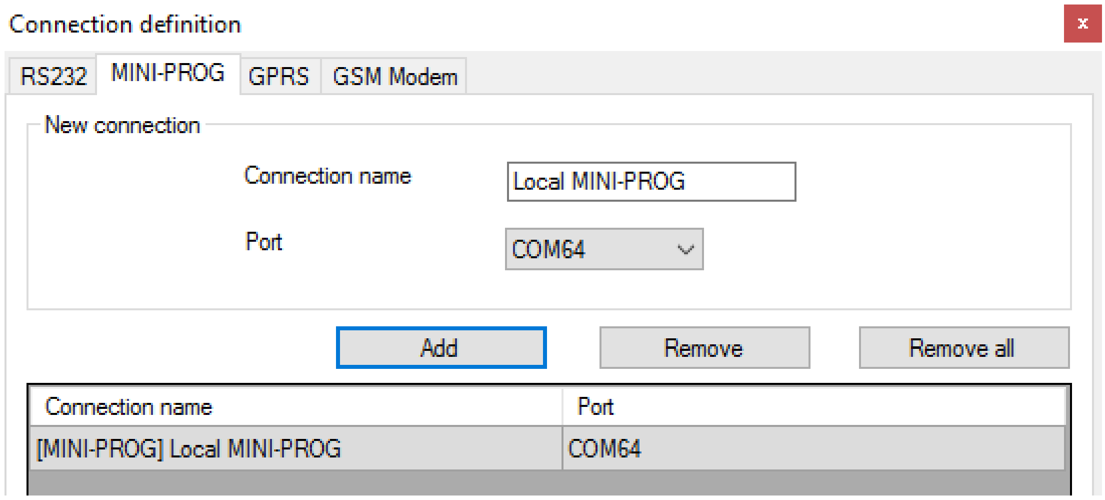
Connection name	Port
[RS232] Local	COM1

Define:

- Connection name, e.g. Local
- Select serial port, e.g. COM1

Click [Add] button to confirm the setting. The connection is saved (and moved to the table). From that moment the program will enable a wire connection with the equipment and allows reading and recording the parameters in the equipment's memory.

In the next tab labelled "MINI-PROG" (the name is derived from programmer) you have to also define the connection parameters.



Connection name: Local MINI-PROG

Port: COM64

Connection name	Port
[MINI-PROG] Local MINI-PROG	COM64

Operations are identical to the one for the "RS232" tab. Specify the name, the appropriate COM port, and add the connection.

MINI-PROG-BT and SP-PROG-BT programmers have microUSB slots, which can be used to connect to a PC/laptop using the USB port, but they also have Bluetooth integrated for communication.

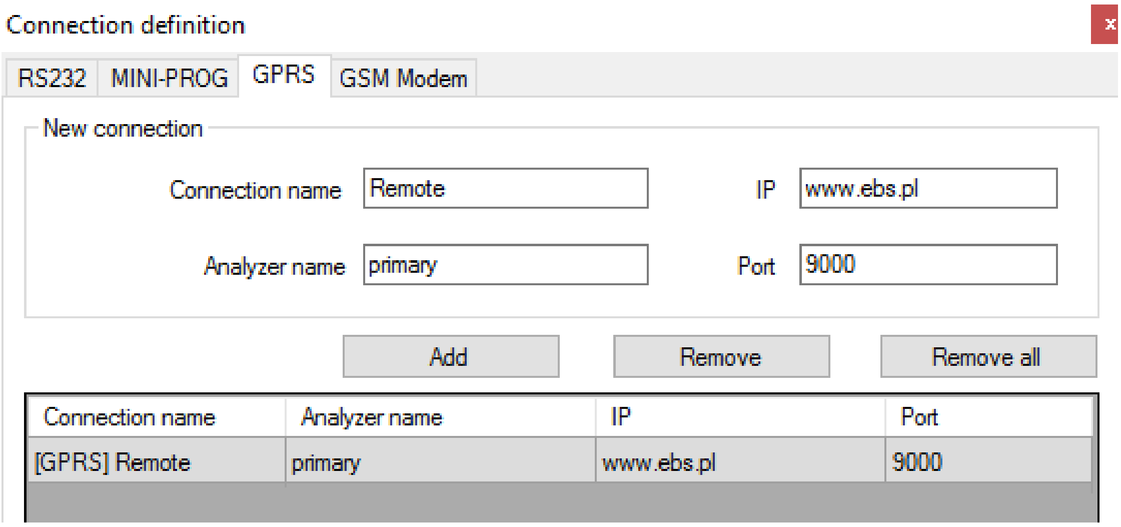
After connecting (whether using USB or Bluetooth), find the appropriate COM port for the given device and select it.

5.3.1.5.2. Remote connection

As explained above the equipment and software allows full configuration using GPRS connection or CSD channel. For such programming mode the connection parameters shall be adequately defined.

GPRS connection

The configuration of that mode requires the activation of File option from Main Menu, and selecting Connection function (or clicking ⚙ icon on a taskbar) and opening GPRS tab. The following window will be displayed on the screen.



Connection name: Remote

IP: www.ebs.pl

Analyzer name: primary

Port: 9000

Connection name	Analyzer name	IP	Port
[GPRS] Remote	primary	www.ebs.pl	9000

Define:

- Connection name, e.g. Remote
- Select analyzer name, e.g. primary
- Enter analyzer name, e.g. www.ebs.pl
- Enter the port on which analyzer will listen to instructions, e.g. 9000

Click [Add] button to confirm the setting. The connection is saved (and moved to the table). From that moment the program will enable a remote connection with the equipment and allows reading and saving the parameters in the equipment's memory.

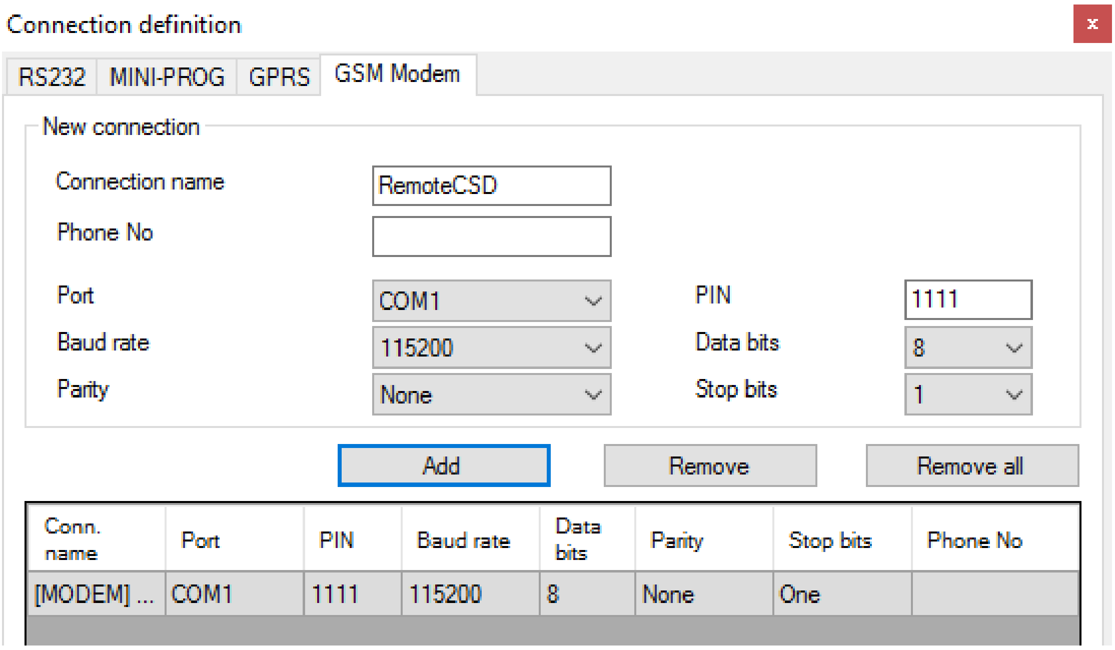
⚠ **NOTE: Such parameters as: analyser's name, analyser's address, port refer to the settings of the OSM.Server monitoring system receiver. Remote programming is available only in case the above mentioned equipment (software) is used.**

CSD connection

The configuration of that mode requires activation of File option from Main Menu, and selecting Connection function (or clicking ⚙ icon on a taskbar) and opening GSM Modem tab.

The window will be displayed on the screen where you define:

- Connection name, e.g. RemoteCSD
- Serial port to which the GSM modem is connected to (e.g. COM1)
- PIN code of SIM card installed in the GSM modem, e.g. 1111
- Serial port parameters: Number of bits per second (e.g. 115200), Data Bits (8), Parity (none), Stop Bits (1).



Connection name: RemoteCSD
Phone No:
Port: COM1
Baud rate: 115200
Parity: None
PIN: 1111
Data bits: 8
Stop bits: 1

Conn. name	Port	PIN	Baud rate	Data bits	Parity	Stop bits	Phone No
[MODEM] ...	COM1	1111	115200	8	None	One	

Click [Add] button to confirm the setting. The connection is saved (and moved to the table). From that moment the program will enable a remote connection with the equipment and allows reading and saving the parameters in the equipment's memory.

⚠ **NOTE: Remote configuration via CSD channel is available only in case the CSD data transfer is active for both SIM card inserted in the equipment and SIM card installed in GSM modem. Additionally, the control panel must accept CSD connections – see item 6.7.1.2. Authorized GSM Modems Numbers.**

Programming through CSD connection is possible also when OSM.Server system is installed, with at least one GSM modem connected. If the device is registered for the server (serial number and SIM card number – see OSM.Server Manual) you can use the connection via OSM. Provided that no GPRS connection is established. Programming attempt (via GPRS connection – see the above) will end with a question whether you want to use a modem connected to the server. If the answer is yes, the procedure will continue as in case of other programming channels.

5.3.1.6. File -> Automatic device settings backup

All configuration wizard's settings, both these read from devices and these saved in the equipment are automatically recorded on a hard drive. If, during configuration wizard's installation no directories were changed, the files can be found in e.g.:

C:\Program Files\EBS\KonfiguratorLX\configs\CPX230NWB_20000\

CPX230NWB_20000 directory contains all files related to programming the CPX230NWB type device of the serial number 20000. Files names contain date and time of the operation and its type (recording/reading). The files are recorded with .cmi extension.

5.3.1.7. File -> Exit

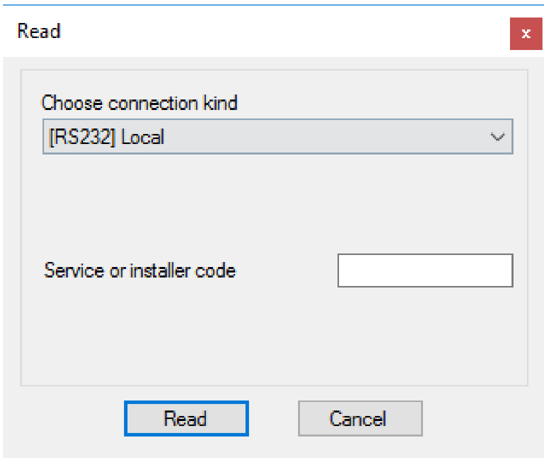
Ends the program operation.

5.3.2. Menu -> Operations

5.3.2.1. Operations -> Read

The function reads the data saved in the memory of GPRS module. Data is exchanged through the port selected in the section "Select connection type" (see the description of "Configuration" option below). A correct readout is confirmed with relevant message. You can save the data downloaded from the equipment in a file (see item 5.3.1.3.), and then use it for other devices.

You can use that function after you define a type and parameters of the connection. E.g. for local connection the following window is displayed:



Read

Choose connection kind

[RS232] Local

Service or installer code

where:

Connection – type of connection to the device.

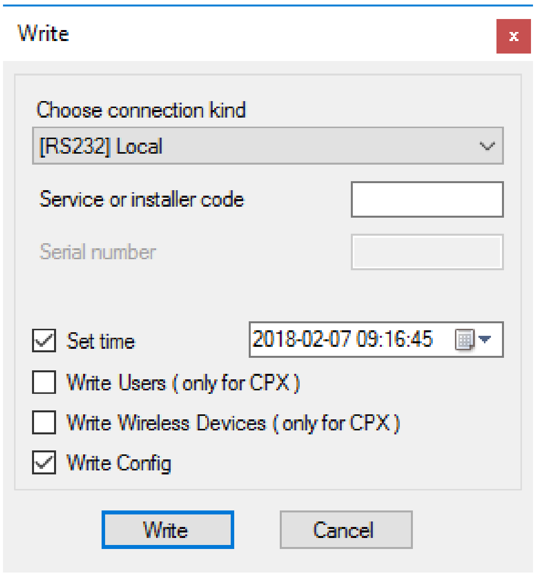
Service or installer code – access code of the equipment.

For detailed description of connection configuration, please refer to item 5.3.1.5.

5.3.2.2. Operations -> Write

The function is similar to the above, but it allows recording data to the memory of the device. It is also possible to set internal timer of the device. For the above you have to check the box “Set the time” and enter a respective date and time. A correct entry is confirmed with a relevant message.

For all the changes which you made in the Configurator and added new users and wireless devices are stored by the control panel, you should send it using this function.



Write

Choose connection kind

[RS232] Local

Service or installer code

Serial number

☑ Set time 2018-02-07 09:16:45

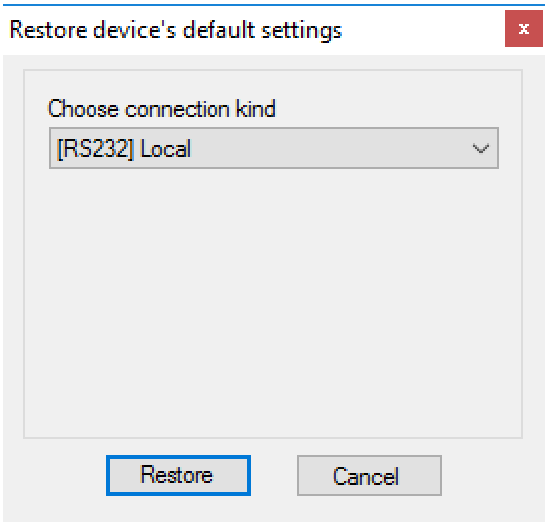
☐ Write Users (only for CPX)

☐ Write Wireless Devices (only for CPX)

☑ Write Config

5.3.2.3. Operations -> Restore device’s default settings

In case the “Read” operation results in an error message (e.g. when access code is not known) you can return to default settings. For the above select that function. The screen displays the message “Do you really want to overwrite current configuration with default values?” Upon confirmation the connection definition window will be displayed:



The operation is possible using local connection only. After the operation is completed the equipment parameters will return to default factory settings.

5.3.2.4. Operations -> Events history

The function enables to read out the events lately recorded in the memory of the equipment. Please refer to chapter 6.12.

5.3.2.5. Operations -> Equipment monitoring

The function allows the on-going monitoring of the equipment condition. Please refer to chapter 6.11.

5.3.3. Menu -> Help

Select this function for additional information about the program.

5.4. DEVICE PROGRAMMING

In order to program the equipment, first you have to establish a connection with the equipment. Depending on the connection mode two programming methods are available.

5.4.1. Local programming

For local programming of the equipment, you should:

- In PROG mode connect e.g. GD-PROG, SP-PROG-BT, or MINI-PROG-BT service cable between CONF connector (on device's PCB) and computer's COM port, defined in Connections -> RS-232 option or MINI-PROG (from the name programmer).
- Connect the power supply to the alarm control panel. Upon connecting the power supply and detecting the programming cable, the module will indicate it with LEDs: the green one will go on and the red one will flash quickly.
- Start the configuration wizard and define the options of the equipment (please refer to chapter 6).

NOTE: Enter correct PIN code for used SIM card.

- Select Send function. The window will appear where you have to select the previously defined local connection (chapter 5.3.1.5.1.). Copy the settings into the memory of the equipment.
- Switch the power off and disconnect the programming cable or switch the programming device into DEBUG (or MONITOR) mode to monitor the operation.
- Insert SIM card.
- Re-connect the power supply.
- The equipment is ready for operation.

5.4.2. Remote programming

Remote programming of the equipment is possible in two cases:

- User has a configuration wizard of GPRS transmitters and computer-connected GSM modem.
- User works based on the receiver of OSM.Server monitoring system.

In the first case remote programming is carried out via CSD channel and the procedure is the same as for local programming, with the only difference that in the options of a connection the "GSM modem" shall be selected (please refer to chapter 5.3.1.5.2. – CSD connection.

NOTE: Remote configuration via CSD channel is available only in case the CSD data transfer is active for both SIM card inserted in the equipment and SIM card installed in GSM modem.

In the second case, in accordance with chapter 5.3.1.5.2. – GPRS connection, you shall define remote connection based on OSM.Server parameters. Since OSM.Server receives (and sends) information only from equipment that is registered in its database, the first operation you have to do for remote programming it to properly register the equipment. The procedure is described in OSM.Server user manual.

5.4.2.1. First programming of the equipment

As no access parameters to GPRS network and OSM.Server are defined in the equipment, you shall start the programming with defining the parameters. Irrespectively of the input method, first you have to register the equipment in the OSM.Server database.

Before starting the remote programming, you have to make sure that the SIM card was inserted (subject to conditions defined in chapter 6.1.5.3.) and the equipment was connected to power supply. The user must know the serial number of the equipment and SIM card telephone number.

The programming procedure is the following:

- Using the pad of OSM.Server device, indicate with the cursor the correct equipment in 'Equipment' tab.
- Click "Config" option and then indicate "Set configuration" function. A list of parameters will be displayed.

- Enter server address, server port and APN. When clicking OK, the system will send entered parameters to the equipment (SMS).
- Wait until the equipment reports to the server (in Equipment tab, it will be marked green).
- Start the software and define the options of the equipment (for description, please refer to chapter 7).
- Select Send function. The window will appear where you have to select the previously defined remote connection (chapter 5.3.1.5.2.). Copy the settings into the memory of the equipment.
- Close the configuration wizard's window after you finish the data input.
- The equipment is ready for data transmission.

5.4.2.2. Reprogramming of equipment

As access parameters to GPRS network and OSM.Server are defined in the equipment, you can proceed with programming any time.

If the equipment is installed in a secured facility, i.e. it has a SIM card inserted and it is connected to power supply, the programming procedure in the following:

- Start the configuration wizard software and define the options of the equipment (for description, please refer to chapter 6.).
- Select Send function. The window will appear where you have to select the previously defined remote connection (chapter 5.3.1.5.2.). Copy the settings into the memory of the equipment.
- Close the configuration wizard's window after you finish the data input.
- The equipment is ready for data transmission in accordance with new settings.

6. PROGRAMMABLE PARAMETERS

Parameters available in configuration wizard were divided into groups: Access, Transmission, Inputs/Outputs, System Options, Users, Monitoring, Restrictions, SMS Notifications, Link Control, Firmware. Each of the groups will be described in detail further on.

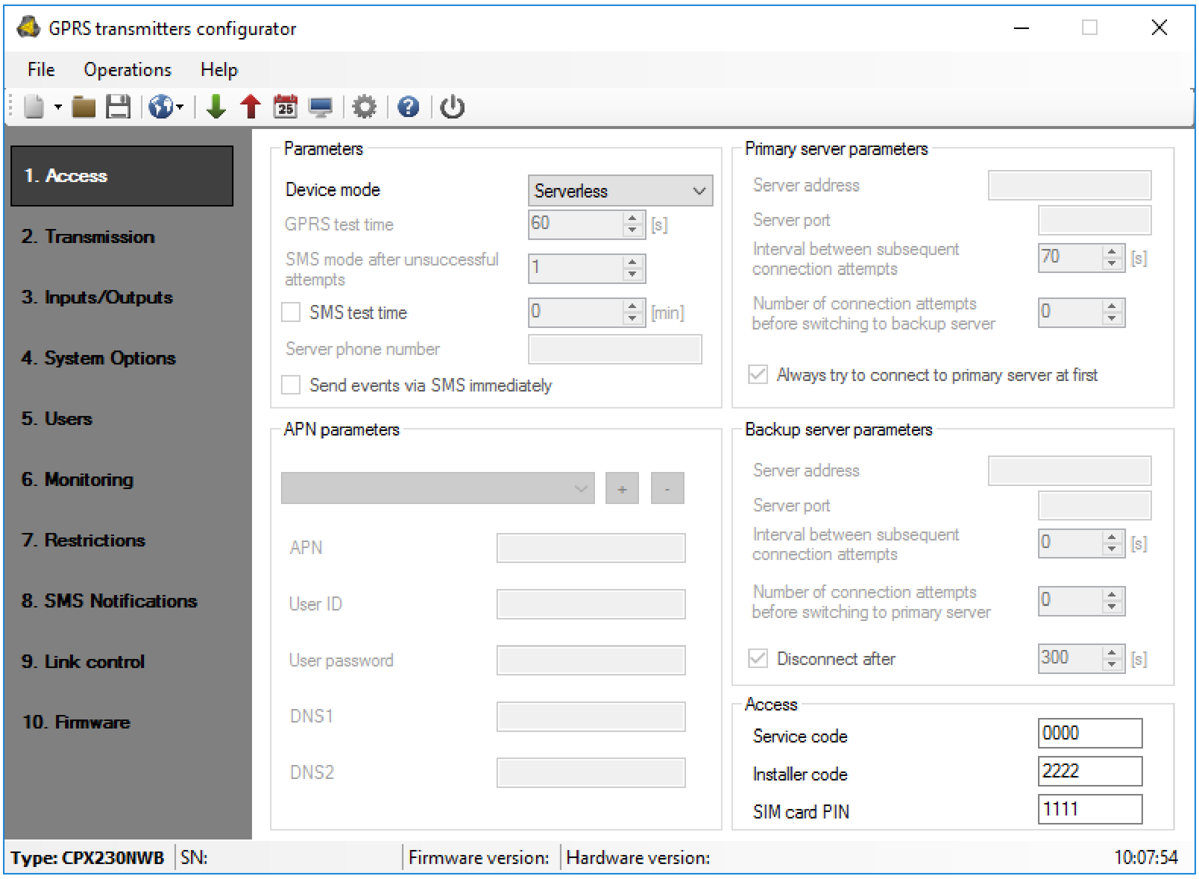
6.1. ACCESS

6.1.1. Parameters

6.1.1.1. Equipment operation mode

Depending on user's preferences, the equipment can operate in one of 4 modes (to be selected from a drop list):

- GPRS & SMS: GPRS transmission (TCP/IP protocol) in standard and in case of problems with that connection, automatic switch into SMS mode
- SMS: Transmission only in SMS mode without the attempt of establishing a GPRS connection
- GPRS: GPRS transmission (TCP/IP protocol) in standard. In case of any problems with that connection, no remote connection is possible
- No server connection: no transmission with server, remote communication with a user is possible only via SMS messages



Parameters

Device mode: Serverless
GPRS test time: 60 [s]
SMS mode after unsuccessful attempts: 1
□ SMS test time: 0 [min]
Server phone number:
□ Send events via SMS immediately

APN parameters

APN:
User ID:
User password:
DNS1:
DNS2:

Primary server parameters

Server address:
Server port:
Interval between subsequent connection attempts: 70 [s]
Number of connection attempts before switching to backup server: 0
☑ Always try to connect to primary server at first

Backup server parameters

Server address:
Server port:
Interval between subsequent connection attempts: 0 [s]
Number of connection attempts before switching to primary server: 0
☑ Disconnect after: 300 [s]

Access

Service code: 0000
Installer code: 2222
SIM card PIN: 1111

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 10:07:54

6.1.1.2. GPRS test period

At a pre-defined interval the equipment sends "Test" signal that informs the monitoring station that the device is operating. In that box, you can determine at what interval defined in seconds the message will be sent.

6.1.1.3. SMS mode after a number of unsuccessful attempts

Here you define the number of attempts to connect with the server. If during the attempts no connection is established, after they terminate, the device will switch into SMS mode. In this mode the equipment still attempts to connect with the server, at an interval defined in item 6.1.3.3.

6.1.1.4. SMS test period

The function is the same as for GPRS. It refers to the situation of any problems with GPRS transmission, when the equipment automatically switches into SMS mode (it also refers to the operation mode via SMS only). Sending a test SMS message as often as in case of GPRS transmission is usually undesirable. That parameter allows significant extension of interval between tests (time in minutes) or disabling that option.

6.1.1.5. Telephone number of a server

If to the server application (e.g. OSM.Server) a GSM modem is connected, here you have to enter its number. SMS messages will be sent to this number in case the equipment encounters problems with GPRS transmission.

In case the box remains empty or one digit is entered only (including 0), the device will not switch into SMS mode – it will operate in GPRS mode only.

⚠ **NOTE: This box will be inactive in case the GPRS operation mode of the equipment was defined.**

6.1.1.6. Send SMS events immediately

In case the GPRS connection is lost, information on upcoming events will be sent by SMS immediately, even in case the equipment has not switched to SMS mode yet.

6.1.2. Access Point Parameters

6.1.2.1. APN

The parameter depends on GSM network operator whose GPRS service will be used. It defines the name of access point to GPRS network. There is a possibility to obtain a private access point. In this case its name will be given by a particular GSM network operator.

6.1.2.2. User ID

Most often it is not required while using public APN. For private APN, you should obtain that parameter from the operator (without it no access to GPRS network can be granted).

6.1.2.3. User password

Most often it is not required while using public APN. For private APN, you should obtain that parameter from the operator (without it no access to GPRS network can be granted).

⚠ **NOTE: Using private APN increases the system security.**

6.1.2.4. DNS1 and DNS2

It defines the address of primary and secondary DNS (Domain Name System). If server address was entered as a domain name at least one DNS address must be entered.

6.1.3. Primary Server Parameters

6.1.3.1. Server IP Address

It is the IP address of a monitoring system receiver (OSM.Server) or a computer on which "Communication server" software is installed, e.g. 89.123.115.8. The address can be given as a server's domain name, e.g. modul.gprs.com. In such a case at least one DNS server address is required.

6.1.3.2. Server port

It defines a port which was dedicated in the server for the receipt of data from the equipment.

6.1.3.3. Interval between subsequent attempts

The programmed equipment with SIM card inserted will automatically attempt to establish connection with a server. Here you can define an interval (in seconds) after which the equipment will retry to connect with a server, in case the previous attempt was unsuccessful.

6.1.3.4. Number of attempts of establishing connection with a server

You can define how many times the equipment will try to connect with the server in case of subsequent faults. After a defined number of attempts, the equipment will initiate the procedure of connecting with secondary server. The option is active only in case the secondary server parameters were defined.

6.1.3.5. Sequence of connections with servers

If you check this box, the equipment will try to establish a connection with primary server, irrespectively of the secondary server parameters set (in particular, the number of connection attempts).

6.1.4. Secondary Server Parameters

6.1.4.1. Server IP Address

It is the IP address of a secondary (redundant) monitoring system receiver (OSM.Server) or a computer on which "Communication server" software is installed, e.g. 89.130.125.82. The address can be given as a server's domain name, e.g. monitor.gprs.com. In such a case at least one DNS server address is required.

6.1.4.2. Server port

It defines a port which was dedicated in the server for the receipt of data from the equipment.

6.1.4.3. Interval between subsequent attempts

If the equipment cannot connect with primary server, after the defined number of attempts it will initiate the procedure of connecting with a secondary server. Here you can define an interval (in seconds) after which the equipment will retry to connect with a server, in case the previous attempt was unsuccessful.

6.1.4.4. Number of attempts of establishing connection with a server

You can define how many times the equipment will try to connect with a secondary server. In case of subsequent unsuccessful attempts, after the defined number of attempts is executed, the equipment will return to the procedure of connecting to primary server.

6.1.4.5. Time for disconnection

If you check this box, the equipment will disconnect the secondary server after a defined time. The following operation depends on the Connection sequence parameter (refer to 7.1.3.5). If the option is active the equipment will try to connect to primary server. In case the option is inactive, the equipment will complete the procedure of connecting to secondary server first, and in case it is unsuccessful, it will move on to attempting the connection with primary server.

6.1.5. Access

6.1.5.1. Service code

It secures the equipment against unauthorized access. It is used for both, equipment programming and for its remote control (in TCP/IP or SMS mode). Default factory setting is 0000. It should be changed at first equipment start-up (programming). The code can be composed of from four to seven digits.

6.1.5.2. Installer code

Installer's code is used for equipment programming process using KP32 keypad. Default factory setting is 2222. It should be changed at first equipment start-up (programming). The code can be composed of from four to seven digits.

Installer's code could be read and change remotely via OSM.Server Console or by sending SMS message. In case of reading Installer's code via OSM.Server Console, please send following Custom command:

```
GETPARAM=3,1
```

The answer with current Installer's code appears in the bottom part of the Console window.

Installer's code could be changed via OSM.Server Console. In such case, please send following Custom command:

```
SETPARAM=3,1,new_code
```

where new_code should contain from 4 up to 7 digits.

6.1.5.3. SIM Card PIN code

Since the equipment uses GSM network for its operation, it is necessary to obtain a SIM card from a mobile network operator. You have to set a PIN code of a SIM card dedicated for operation in particular equipment before its first use. It is necessary for automatic start up of the system. In case you have a card without the PIN code, you can enter any value in that box, e.g. 0000.

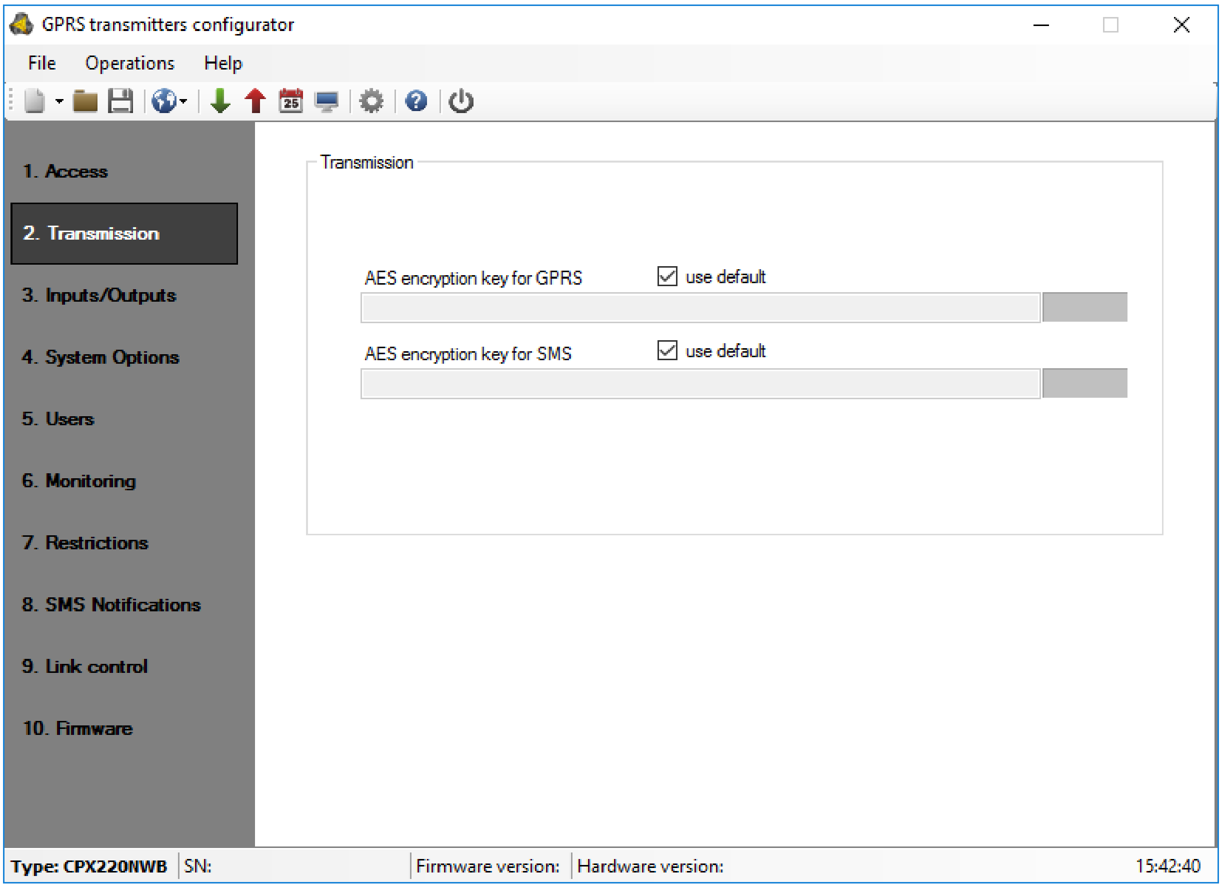
If you enter incorrect PIN code, the system will not start after inserting the card and switching the power supply on and you will not be able to use the card until you enter the PUK code (using any GSM phone).

Default factory PIN code entered in the equipment is: 1111.

6.2. TRANSMISSION

For the maximum transmission security the data transmitted are encrypted using AES. The option can be used for both, GPRS and SMS transmissions.

In case encrypted transmission was selected, you can enter own data encryption key (DEK) (256 bits - 0-9 and A-F characters) or use default setting.



AES encryption key for GPRS ☑ use default

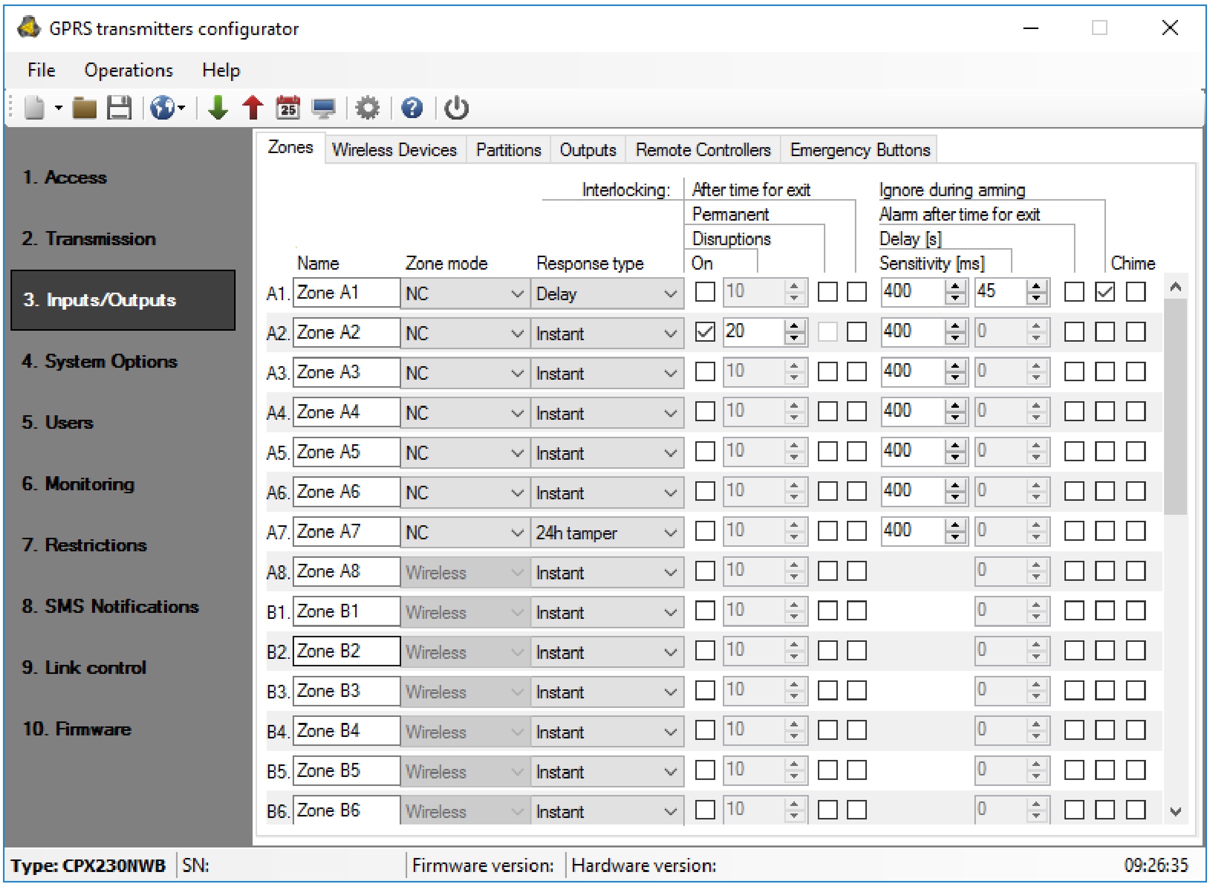
AES encryption key for SMS ☑ use default

Type: CPX220NWB | SN: | Firmware version: | Hardware version: | 15:42:40

6.3. INPUTS / OUTPUTS

The alarm control panel has 32 configurable zones and 3 software controlled outputs. Zones can be freely divided into two partitions. Each of zones and outputs has a number of programmable parameters defined below.

6.3.1. Zones (inputs)



				Interlocking:								
	Name	Zone mode	Response type	On	Disruptions	Permanent	After time for exit	Sensitivity [ms]	Delay [s]	Alarm after time for exit	Ignore during aming	Chime
A1.	Zone A1	NC	Delay	□	10	□	□	400	45	□	☑	□
A2.	Zone A2	NC	Instant	☑	20	□	□	400	0	□	□	□
A3.	Zone A3	NC	Instant	□	10	□	□	400	0	□	□	□
A4.	Zone A4	NC	Instant	□	10	□	□	400	0	□	□	□
A5.	Zone A5	NC	Instant	□	10	□	□	400	0	□	□	□
A6.	Zone A6	NC	Instant	□	10	□	□	400	0	□	□	□
A7.	Zone A7	NC	24h tamper	□	10	□	□	400	0	□	□	□
A8.	Zone A8	Wireless	Instant	□	10	□	□		0	□	□	□
B1.	Zone B1	Wireless	Instant	□	10	□	□		0	□	□	□
B2.	Zone B2	Wireless	Instant	□	10	□	□		0	□	□	□
B3.	Zone B3	Wireless	Instant	□	10	□	□		0	□	□	□
B4.	Zone B4	Wireless	Instant	□	10	□	□		0	□	□	□
B5.	Zone B5	Wireless	Instant	□	10	□	□		0	□	□	□
B6.	Zone B6	Wireless	Instant	□	10	□	□		0	□	□	□

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 09:26:35

6.3.1.1. Zone mode

The parameter allows for determining the stable input zone state. Any change of that state causes alarm message to be sent. Wired input can be NO or NC type. The following configuration types are available: NO / NC / EOL-NO / EOL-NC / DEOL-NO / DEOL-NC / Wireless / TEOL. NC type input must be closed for the whole time. Zone interruption causes its induction. NO type input remains open. It activates when closed. EOL and DEOL (with parameters or double parameters assigned) differ in the number of resistors allowing to distinguish alarm from sabotage. The TEOL configuration is used to double an alarm zone, i.e. connect two wire detectors to one clamp at the central, and it is possible to detect alarms from detector 1 and detector 2 (see drawing 3), while signaling sabotage switch (tamper) open will be common for both detectors.

Electric diagrams for all configuration types were described in chapter 3.4 Configuration of wired input zones.

6.3.1.2. Response type

- **Instant** – disruption of the zone causes immediate alarm, if the system is armed.
- **Delay** – that type of zone is usually used for detectors operation at the facility entries. The zone switches into alarm state after the expiration of programmed time for entry. If the system is armed, the zone activation initiates counting the time for entry to a particular partition. The system should be disarmed before the expiration of programmed time in order not to trigger the alarm.
- **24h burglary** – that zone causes immediate alarm irrespectively of whether the system is armed or not.
- **Arming/disarming by violation** – the zone can be used for arming or disarming the system. In case the zone is activated with the system disarmed, the partition assigned to the zone is armed. In case the zone is activated with the system armed, the partition assigned to the zone is disarmed.
  Note: For wired zones, it is recommended to configure them as NC or NO for this response type.
- **24h tamper** – the zone can be used for connecting tamper/sabotage circuits. In case of trigger when partition is disarmed, it generates "violation of the zone" event without the alarm. In case of trigger when partition is armed, it generates "violation of the zone" event and raises the alarm.
- **Interior delay** – the zone can be used when keypad is not in the first partition which could be triggered during access to the keypad. In case of the interior delay partition is triggered, system checks if time for enter is counting. If yes, the zone is treated as delay zone. If not, the lien is treated as instant zone.
- **24h burglary silent** – sends a report to the central station but provides no keypad display or sounding.
- **24h fire** – works like 24h burglary.
- **Perimeter** – This zone will be armed immediately after arm command. Detectors protecting the entrance to the building (doors and windows) are defined like this. Violation of this zone will raise the alarm, even during the exit time countdown.
- **Perimeter exit** – If the system is armed only by using a code, without selecting the arming mode, violating this zones during exit time countdown will arm the system in the fully armed mode. If this is not violated during exit time countdown, partition will be armed in the stay mode. If the system is armed and a mode is selected, then triggering this zone during the exit time countdown will be ignored, and the system will be armed in the selected mode. If the system is armed, this zone behaves like the delayed zone.
- **24h gas –** works like 24h burglary.
- **24h water leakage –** works like 24h burglary.
- **Night (bypassed) –** this zone is used for detectors located in places where humans move around during the night. Violation of this zone will not trigger an alarm when the system is armed in sleep mode. When the system is armed in full mode, the zone will behave like an instant.

- **Night with prealarm –** When the system is armed in sleep mode violation of this zone will start the exit time countdown. The system should be disarmed before the expiration of programmed time, in order for the system not to trigger an alarm (or arm it in daily mode if there are people in the building). If the system is armed in full mode, then a night delayed zones will behave like an instant, while in perimeter mode, triggers on this zone will be ignored.
- **Arming/disarming by state change** - Violation of the zone will arm the partition to which the zone is assigned. End of violation will disarm the partition. In case the system is armed and the zone violation occurs, the partition to which the zone is assigned will start to arm again (signaling the countdown of the configured time for exit). End of violation will result in disarming the partition.
  Note: For wired zones, it is recommended to configure them as NC or NO for this response type.

  Arming/disarming by state change is available since the firmware version 2.10.0.

6.3.1.3. Interlocking

The option allows interlocking any input zone, which means that any changes of state at this input are ignored and not reported to monitoring station.

You can set the set permanently blocking input ("Permanent"), or turn on the blocking after a given number of input violations.

If you select "After time for exit", the input zone will be blocked if the zone was violated when arming. In this case, an event about blocked zone will be generated, which allows to inform the monitoring station about the problem with the zone. This lock will last until disarming. If the input is selected as the "Alarm after time for exit", then "Interlocking after time for exit" has priority - the zone will be blocked and will not generate an alarm.

If the zone is set to "After time for exit" and is violated or sabotaged after the time for exit, then is automatically blocked (bypass is activated). Automatically blocked zones (block "After time for exit"" or automatic blockout after "n" disruptions) are automatically unlocked after disarming partitions to which they belong

6.3.1.4. Sensitivity

That parameter defines a minimum time the change must maintain at the particular zone, to be detected by a transmitter. Default factory setting of the parameter is 400 ms.

6.3.1.5. Delay

The parameter is active for delayed and perimeter exit zones only. It defines a time from the zone disruption was detected after which an alarm is generated.

6.3.1.6. Alarm after time for exit

When selected, the alarm will be generated if the zone remains violated when the time to exit is up.

When deselected, alarm will NOT be generated in above case.

First alarm will be generated after the zone is returned and violated again.

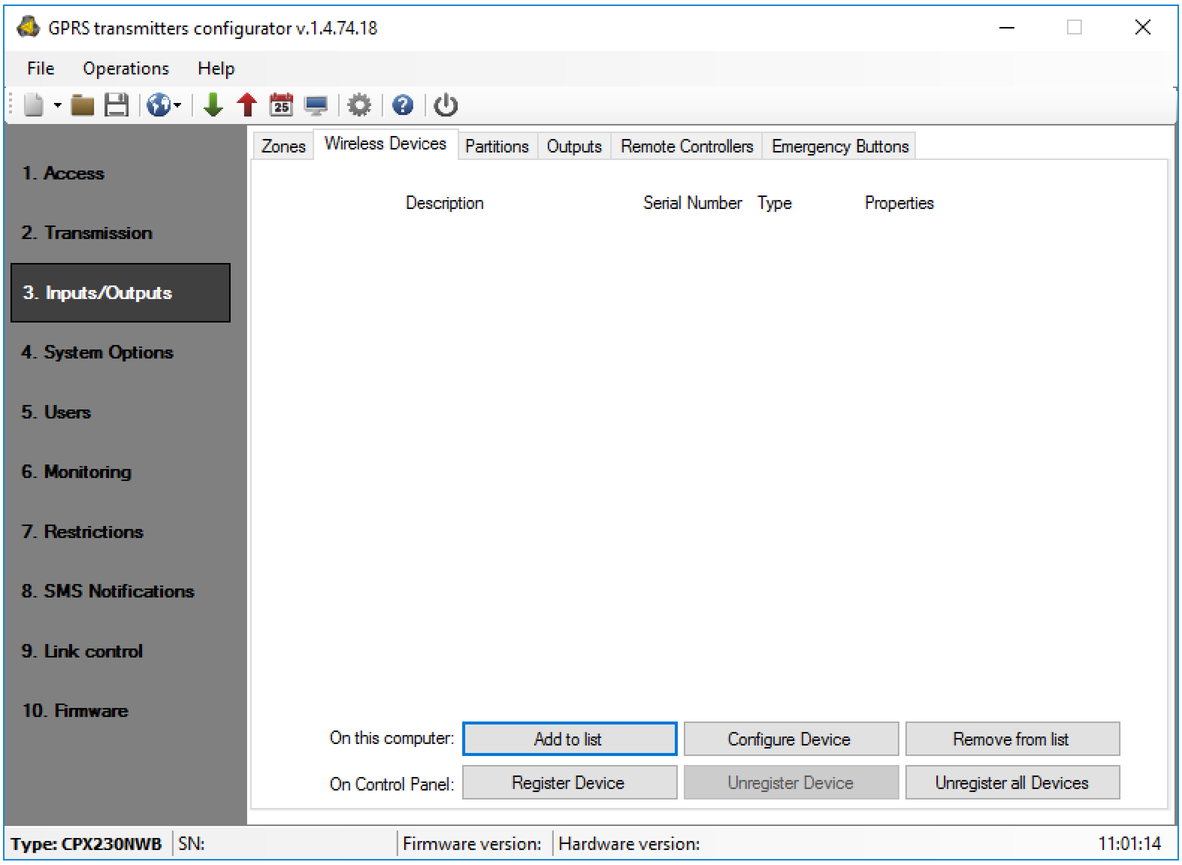
6.3.1.7. Ignore during arming

Zone can be violated during partition arming (e.g. delay zone shall be set to that option).

6.3.1.8. 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

6.3.2. Wireless zones (devices)

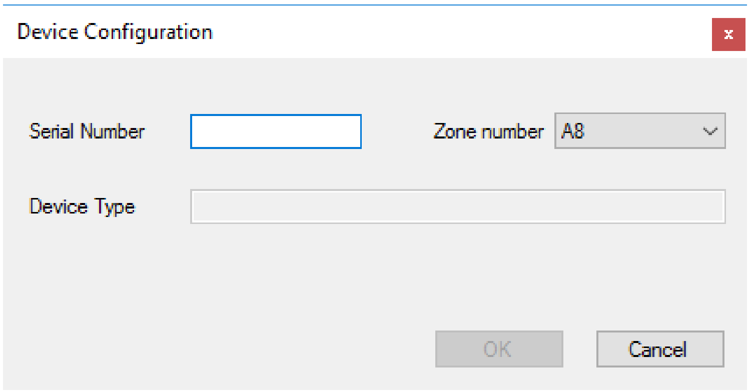


CPX230NWB is capable of storing information up to about 32 wireless inputs: A1 to A8, B1 to B8, C1 to C8, D1 to D8.

There are two ways to add detectors (described below).

The first way is to add the device to the list on the computer (by entering the serial number) on which the Configurator is installed, and then to send all newly added devices to the control panel.

When you press "Add to list" the following window appears:



Device Configuration

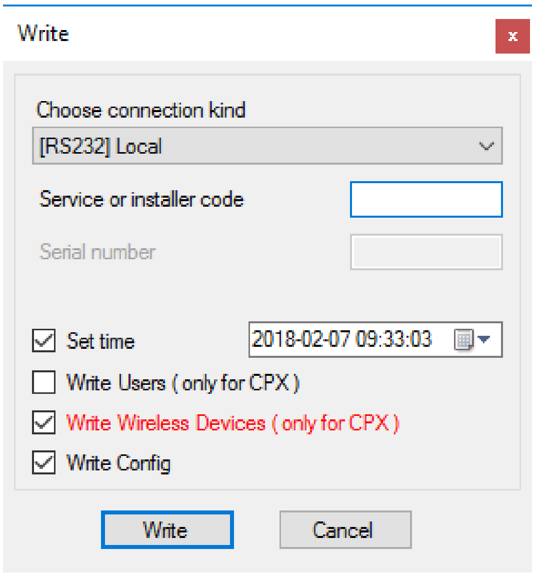
Serial Number

Zone number A8

Device Type

Enter the serial number S/N located on the label of the detector. The next box refers to the zone (input) number, which can be assigned. The device type will appear automatically when the first two digits are entered. After filling this field, press the “OK” button.

Now for the detector to be seen by the panel, this information must be sent by pressing *Write* ⬆ on Quick Access bar (or Operations -> Write). A window will pop up:



Write

Choose connection kind

[RS232] Local

Service or installer code

Serial number

☑ Set time 2018-02-07 09:33:03

□ Write Users (only for CPX)

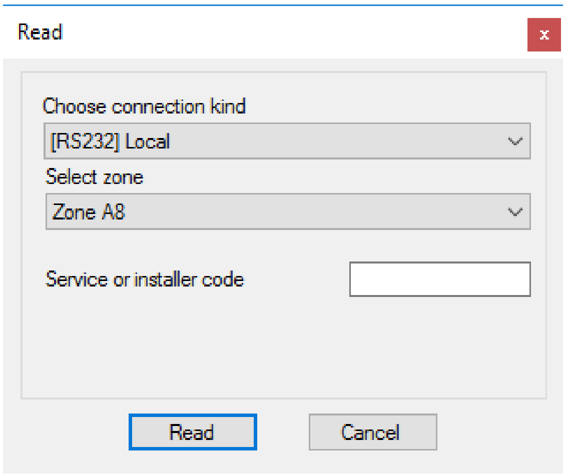
☑ Write Wireless Devices (only for CPX)

☑ Write Config

where one have to mark the third checkbox "Write Wireless Devices (only for CPX)” and press ”Write”. From now on, the detector and the control panel will communicate with each other correctly.

⚠ **NOTE: To receive the control panel signals from the detector it is necessary to enter the correct serial number.**

The second way is to directly register the detector in the control panel.
To add a wireless detector press the "Register Device" button.



Read

Choose connection kind

[RS232] Local

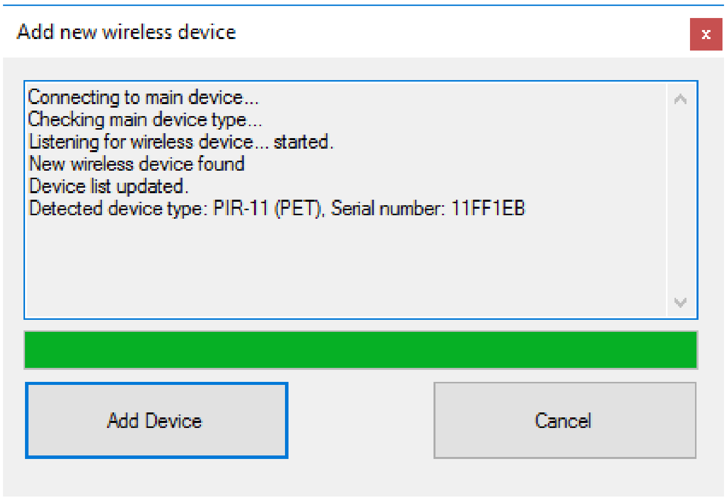
Select zone

Zone A8

Service or installer code

In the new window, select proper connection (serial port number to which CPX230NWB is connected) and zone number for new device. Then enter service code and press "Read" button. A new window pops up with an information about the control panel starting listening for wireless devices.

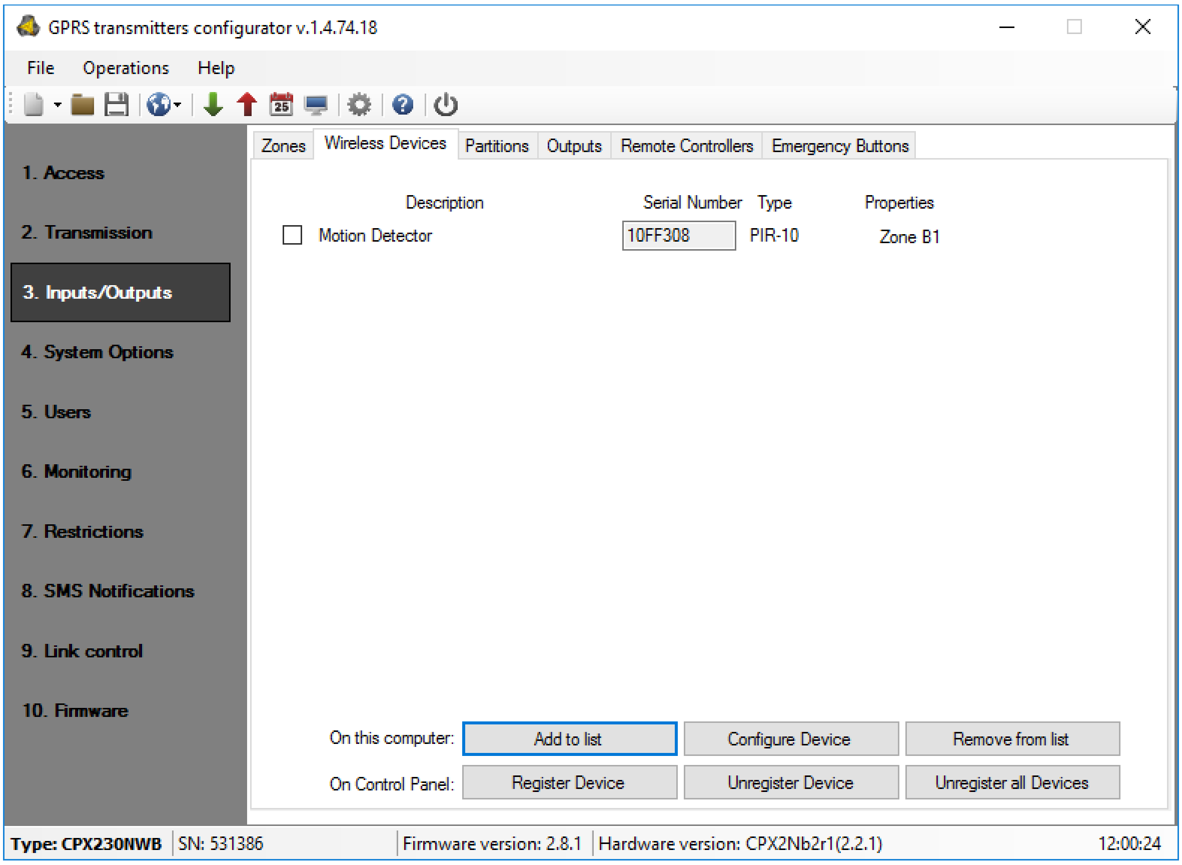
Configurator will be waiting for a wireless signal. User has to press the tamper button on the sensor for a while. CPX230NWB will detect the transmission and print sensor's type and ID. It is recommended to add wireless sensors individually. To prevent the accidental transmissions from other detectors, only one detector cover should be removed during the procedure of adding a new detector. The control panel detects the communication, and informs the user about the type and serial number of the device.



Add new wireless device

```
Connecting to main device...
Checking main device type...
Listening for wireless device... started.
New wireless device found
Device list updated.
Detected device type: PIR-11 (PET), Serial number: 11FF1EB
```

To bind this sensor with the Alarm Control panel, press "Add Device". New sensor will appear in the previously selected Zone row:

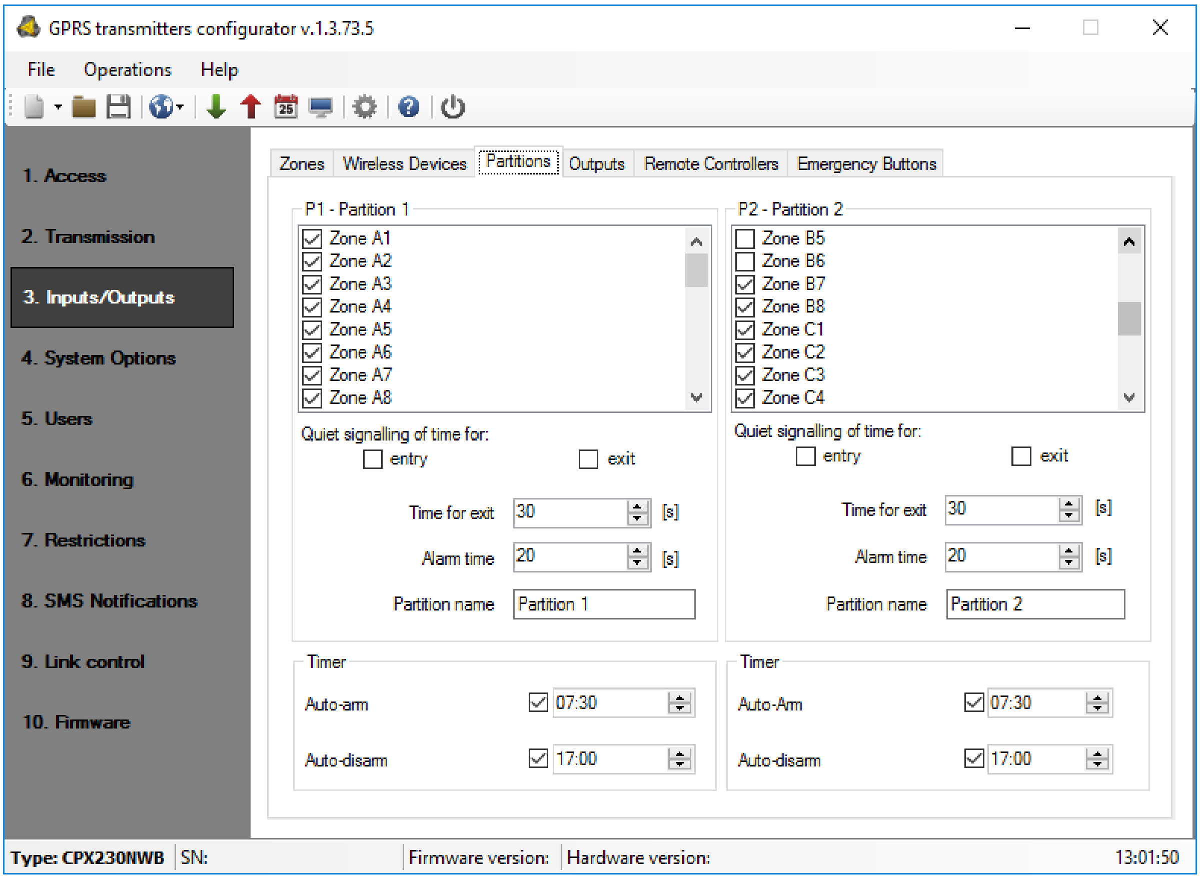


Description	Serial Number	Type	Properties
□ Motion Detector	10FF308	PIR-10	Zone B1

Type: CPX230NWB | SN: 531386 | Firmware version: 2.8.1 | Hardware version: CPX2Nb2r1(2.2.1) | 12:00:24

Now, each detector can be attributed to the type of reaction and assigned with other parameters (in the "Zones" tab), except for sensitivity.

6.3.3. Partitions



P1 - Partition 1

☑ Zone A1
☑ Zone A2
☑ Zone A3
☑ Zone A4
☑ Zone A5
☑ Zone A6
☑ Zone A7
☑ Zone A8

Quiet signalling of time for: □ entry □ exit

Time for exit: 30 [s]

Alarm time: 20 [s]

Partition name: Partition 1

Timer

Auto-arm ☑ 07:30

Auto-disarm ☑ 17:00

P2 - Partition 2

□ Zone B5
□ Zone B6
☑ Zone B7
☑ Zone B8
☑ Zone C1
☑ Zone C2
☑ Zone C3
☑ Zone C4

Quiet signalling of time for: □ entry □ exit

Time for exit: 30 [s]

Alarm time: 20 [s]

Partition name: Partition 2

Timer

Auto-Arm ☑ 07:30

Auto-disarm ☑ 17:00

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 13:01:50

6.3.3.1. P1 - Partittion 1, P2 – Partition 2

In that tab you can assign the zones from group A, B, C and D to the specific monitoring partitions. If the zone is not assigned to any of the partitions (and it is not of 24h type), all events received from that zone (disruption/return) will be ignored.

6.3.3.2. Entry / Exit

The parameter allows switching off the indication of time for entry/ exit displayed by KP32 keypad.

6.3.3.3. Time for exit

It is time for leaving the partition. Assigned zones will be active (monitored) after the expiration of pre-defined time, counting from the time the arming zone was disrupted.

6.3.3.4. Alarm time

The parameter defines the time the alarm will be indicated by KP32 keypad.

6.3.3.5. Partition name

The parameter allows you to give any name for the partition.

6.3.3.6. Timer

In this section, you can set the parameters of automatic arming and disarming the partition.

You can set the time for arming/disarming and you can independently turn on and off each time. By clicking the check box, located on the left side of the time field, you can activate/deactivate the time. If auto-arming/disarming is off, the time field is grayed out.

When the partition is automatically armed / disarmed, to the monitoring station is sent a report that was done by the user with the number 253.

At the time of auto-arming, exit time is starting. During the exit time, the user may at any time to stop arming with the code. Then the system will not be armed.

If there is a fault in the system, they not prevent arming (like remote control and remote command).

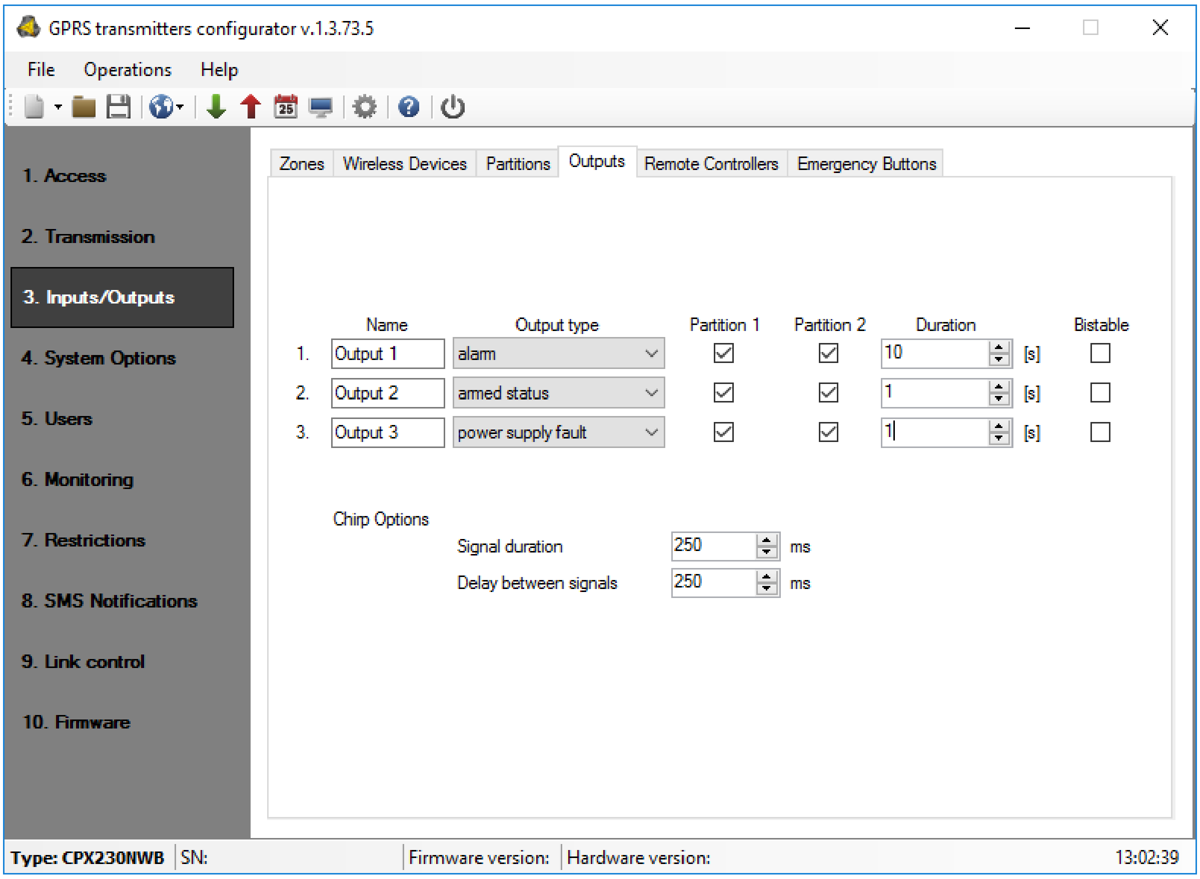
For each input zone is available „Interlocking after time for exit” option. If this option is active, in the case of arming with violated zone, after time for exit, will be generated event about blocked zone. Zone blocking will continue until partition disarming (see item 6.3.1.3. Interlocking).

When set to the same time arming and disarming, the system will first be disarmed and then immediately armed.

If the time in the device is set forward (eg. when the time is changed to Daylight saving time), and arming or disarming time is in the period which has been ommited, then the hour will be not used. Eg. If the auto-arming time is set to 2:30, and time was changed forward from 2:00 to 3:00, the control panel will not arm.

Times of arming and disarming can also configure by remote command via GPRS or SMS.

6.3.4. Outputs



	Name	Output type	Partition 1	Partition 2	Duration		Bistable
1.	Output 1	alarm	☑	☑	10	[s]	□
2.	Output 2	armed status	☑	☑	1	[s]	□
3.	Output 3	power supply fault	☑	☑	1	[s]	□

Chirp Options

Signal duration 250 ms

Delay between signals 250 ms

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 13:02:39

6.3.4.1. Outputs 1 / 2 / 3

Types of outputs:

- **Unused** – Output is inactive.
- **Alarm** – Output is activated when alarm is detected.
- **Armed status** – Output is activated when any of the assigned partitions is armed in any mode (stay, sleep, fully armed).
- **Power supply fault** – Output is activated when power supply fault is detected.
- **Communication loss** – Output is activated when information transmission to server is not possible.
- **GSM jamming indicator** – Output is activated when jamming GSM.
- **Chirp** – The output is activated when arming (1 chirp) or disarming (2 chirps). The minimum duration of the chirp signal possible to set from the configurator is 40ms. In the case of set time for exit chirp is generated after arming, similarly in the case of the time for entry chirp is generated after disarming.
- **Alarm & chirp** – The output is activated when alarm is detected or when arming/disarming.

6.3.4.2. Partition 1 (P1) / 2 (P2)

The parameter allows assigning particular monitoring partitions to outputs.

6.3.4.3. Activation time

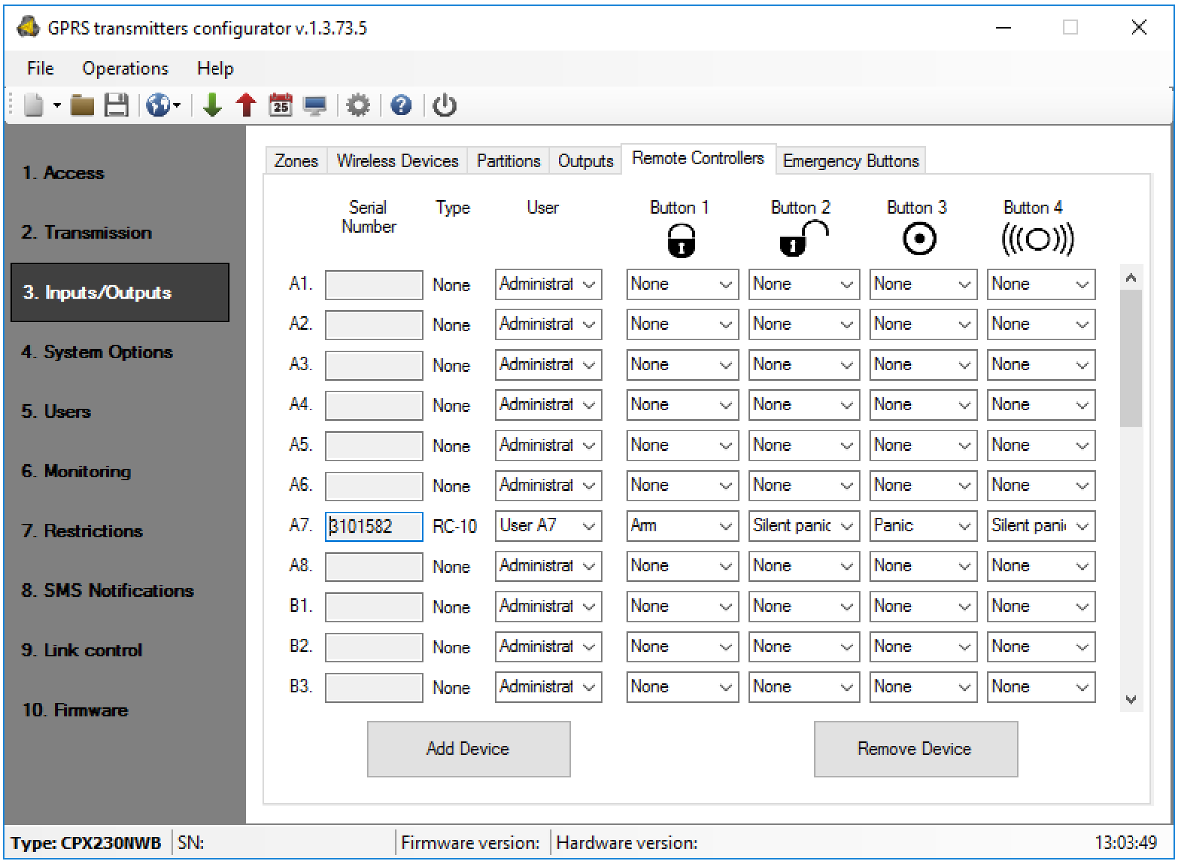
The parameter defines the time the output is to be active.

6.3.4.4. Bistable

The parameter allows set bistable mode of the output. In this mode, the output will be switched on for the duration of the state specified in the "Output Type".

If you set the output type as "unused", the output state can be changed only with remote command.

6.3.5. Remote controllers



	Serial Number	Type	User	Button 1	Button 2	Button 3	Button 4
A1.		None	Administrat	None	None	None	None
A2.		None	Administrat	None	None	None	None
A3.		None	Administrat	None	None	None	None
A4.		None	Administrat	None	None	None	None
A5.		None	Administrat	None	None	None	None
A6.		None	Administrat	None	None	None	None
A7.	3101582	RC-10	User A7	Arm	Silent panic	Panic	Silent pani
A8.		None	Administrat	None	None	None	None
B1.		None	Administrat	None	None	None	None
B2.		None	Administrat	None	None	None	None
B3.		None	Administrat	None	None	None	None

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 13:03:49

Configurator allows adding and configuring remote controllers in the same way as it was done in the Wireless Inputs configuration. In order to add a remote controller, User has to select a row corresponding to desired remote controller and press the *Add Device* button. New window will appear, where necessary serial port configuration and service code parameters have to be filled in. Pressing OK will invoke new window indicating, that control panel is waiting for incoming transmission from the remote controller. User has to press one of the controller button, in order to bind it with the Alarm Control panel. Device's ID and serial number will appear. To accept, press *Add Device.* New remote controller has been added in the previously selected row.

User can configure remote controllers, to suit his needs. Remote controller has to be assigned to one of the previously added users (or administrator) – *User* column. Controller’s buttons can be assigned to the actions of the Alarm Control panel. In order to assign a button to the action, one has to select the desired action from the drop-down menu in the corresponding *Button* column – columns from *Button 1* to *Button 4*. Remote controller can have less then 4 buttons, in that case, additional *Button* columns should be left with the None option selected.

NOTE: The selected user number must be activated by the Administrator. For this user number should be generated an access code.

“Arm” function is fully arming the system.

“Disarm” function is disarming the system.

„Alarm” function is triggering an alarm with audible signal.

„Silent alarm” function is triggering an alarm without audible signal.

Switch on/off output 1, 2 and 3 functions allow control of any external devices.

„Ambulance” function works the same way as „HELP” button on the keypad, ie generates a medical alarm.

“Arm immediately” function allows fully arming the system without counting down time for exit (if is set).

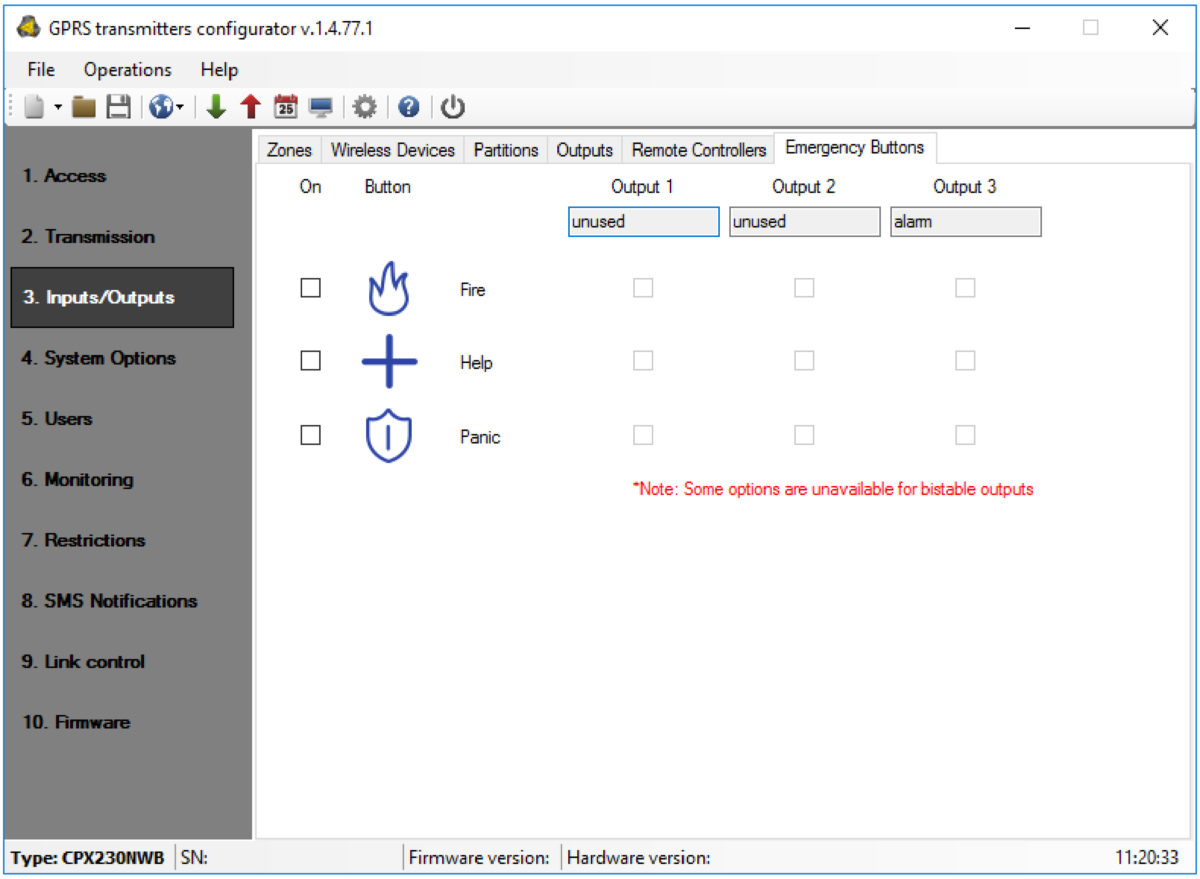
Alarms from remote control can be generated regardless of whether or not the partition is armed.

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

The control panel allows you to assign remote control buttons to various functions. It is possible to configure different alarm button but the manufacturer recommends assigning a button ((○)) to normal alarm, and ⊙ to silent alarm

Configuration for pilots should be automatically write to the control panel. Nevertheless the Manufacturer recommends that after adding and configuring the pilot/s information has been sent by pressing the red arrow "Write" from the Quick Access bar (or "Operations" -> "Write"). A window will appear, as in the chapter on wireless detectors. You have to select third checkbox “Write Wireless Devices (only for CPX)” ", enter the service code and press “Write”.

6.3.6. Emergency Buttons


GPRS transmitters configurator v.1.4.77.1

File Operations Help

1. Access
2. Transmission
3. Inputs/Outputs
4. System Options
5. Users
6. Monitoring
7. Restrictions
8. SMS Notifications
9. Link control
10. Firmware

Zones | Wireless Devices | Partitions | Outputs | Remote Controllers | Emergency Buttons

On	Button		Output 1	Output 2	Output 3
			unused	unused	alarm
□	🔥	Fire	□	□	□
□	+	Help	□	□	□
□	🛡	Panic	□	□	□

*Note: Some options are unavailable for bistable outputs

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 11:20:33

6.3.6.1. Icons

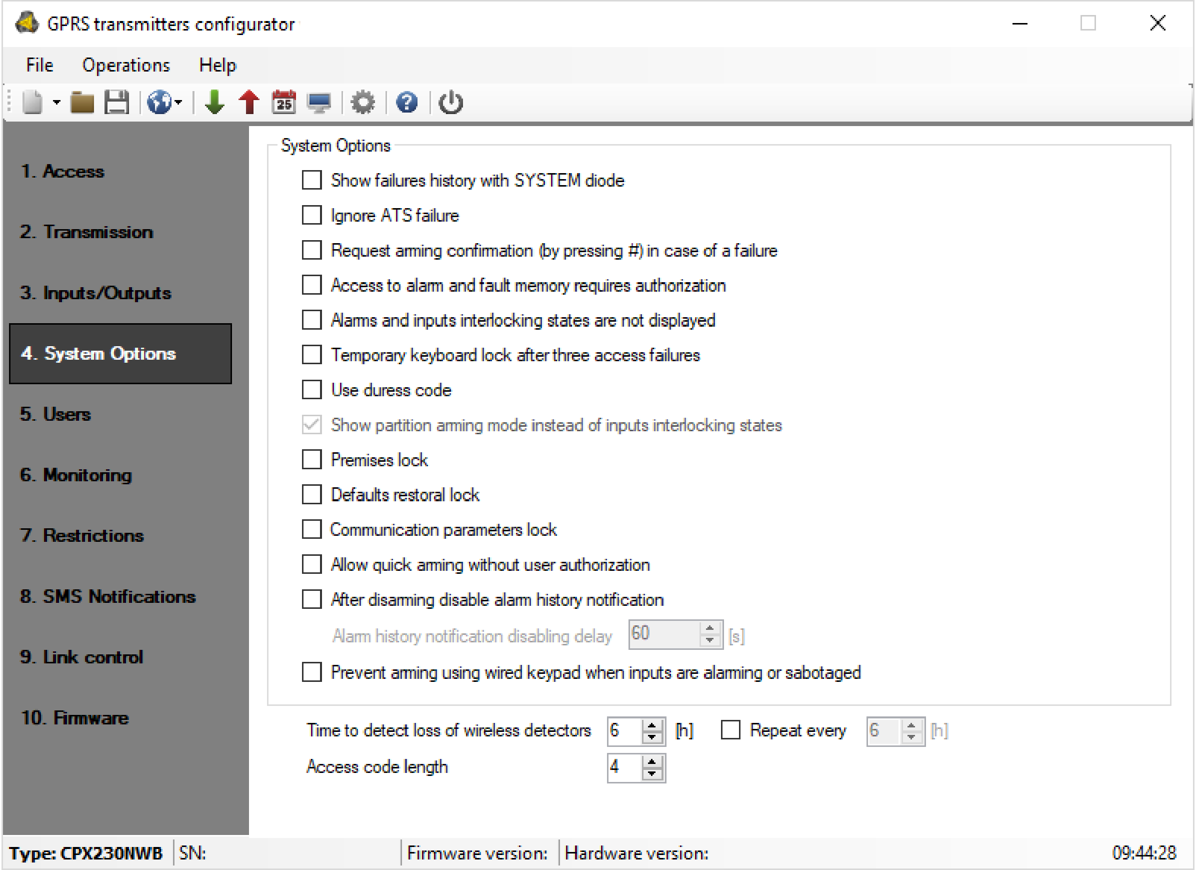
🔥 + 🛡 symbols match the [🔥 *] [+ A-H ▢] [🛡 #] function keys on the keypad. The "On" checkbox has to be checked in order to enable the function key support. Events associated with emergency buttons will be transmitted to monitoring station only if they are enabled in the "Monitoring" tab (see item 6.6.).

6.3.6.2. Outputs

User can choose which outputs should be turned on in case of the emergency button activation (pressing and holding a button for 3 seconds).

Each of the outputs has the reminder of it's function chosen in the "Outputs" tab.

6.4. SYSTEM OPTIONS



System Options

□ Show failures history with SYSTEM diode
□ Ignore ATS failure
□ Request arming confirmation (by pressing #) in case of a failure
□ Access to alarm and fault memory requires authorization
□ Alarms and inputs interlocking states are not displayed
□ Temporary keyboard lock after three access failures
□ Use duress code
☑ Show partition arming mode instead of inputs interlocking states
□ Premises lock
□ Defaults restoral lock
□ Communication parameters lock
□ Allow quick arming without user authorization
□ After disarming disable alarm history notification
Alarm history notification disabling delay 60 [s]
□ Prevent arming using wired keypad when inputs are alarming or sabotaged

Time to detect loss of wireless detectors 6 [h] □ Repeat every 6 [h]
Access code length 4

Type: CPX230NWB | SN: | Firmware version: | Hardware version: 09:44:28

6.4.1. Show failures history with SYSTEM diode

Selecting this option will result in notifying about the occurrence and ending of failures in the system by blinking the SYSTEM diode on KP32 keypads until the failure memory is deleted.

6.4.2. Ignore ATS failure

Selecting this option turns off signaling a loss of communication with the server on KP32 keypad.

6.4.3. Request arming confirmation (by pressing #) in case of failure

If this option is enabled, the user is additionally notified of system failures when arming the system. The wired keypad produces a continuous sound, the ALARM and SYSTEM diodes start flashing slowly and error codes are displayed on diodes 1–8 (see User's Manual, section 6.6 Arming the system with a malfunction). To arm the system press # button. Information on failures and triggering are available after entering with the use of the wired keypad the user's function: *faults memory* and *current input status*.

6.4.4. Access to alarm and fault memory requires authorization

Selecting this option enables limitation to access to alarm memory and fault memory. Checking alarm memory and fault memory will be available only after entering user code. This option must be enabled in order to comply with EN 50131 standard requirements for Grade 2.

6.4.5. Alarms and inputs interlocking states are not displayed

Selecting this option disables display alarms and inputs interlocking states. This option must be enabled in order to comply with EN 50131 standard requirements for Grade 2.

6.4.6. Temporary keyboard lock after three access failures

Selecting this option enables keypad blocking after entering invalid codes. The keypad will be blocked for 90 seconds, after entering an invalid code three times. After this period, another lock will occur after entering a wrong code three times. The counter of invalid codes will be reset after a correct code is entered (e.g. after entering invalid code two times). This option must be enabled in order to comply with EN 50131 standard requirements for Grade 2.

6.4.7. Use duress code

Duress code is used to inform the monitoring station about a distress event without an audible alarm. Each user has his own duress code.

6.4.8. Show partition arming mode instead of inputs interlocking states

Option not available for CPX230NWB

6.4.9. Premises lock

This function turns off the ability to arm the control panel. When this function is turned on, the user will not be able to arm the site by any way (i.e. SMS/GPRS, remote, arming input, schedules, keypad, wireless keypad). Disarming the system is possible, however.

Attempts to arm will be rejected by the control panel - the wired keypad emits a 4 times sound and at the same time, the diodes GROUP, ALARM, SYSTEM and PROG will light up for 4 times. System failures do not affect this option The Configurator log will then register that the system was not armed due to the Premises lock function being on (log entry only when arming from a keypad).

6.4.10. Defaults restoral lock

The function “Defaults restoral lock” allows the user to turn off the ability to restore the factory-default installer’s code. However, when restoring default settings using the Configuration, when the "Restore device’s default settings" option is selected, a window with a request to enter the installer’s code or service code (ATS) will appear.

When this function is turned on, the Manufacturer recommends the installer’s code and service code (ATS) are changed.

NOTE: If newly set codes are lost, it will be necessary to send the blocked devices to the EBS technical service.

6.4.11. Communication parameters lock

After checking that option changing:

- service code (ATS)
- turning on/off "Communication settings lock" option
- server phone number
- APN, user ID, user password
- primary server port
- secondary server port
- SMS encryption key
- GPRS encryption key
- DNS server addresses
- phone numbers, to which SMS messages will be forwarded

will require service code (ATS) knowledge! As a result, it will be impossible to register control panel in other monitoring station without authorization.

After activating this option, resetting to default settings via Configurator, will also require service code (ATS).

On the other hand, installer will be able to:

- change transmission parameters, e.g. GPRS and SMS test periods, SMS limits,
- send it to control panel (with the exception of communication parameters written above, which will be blocked),
- read settings saved on the device,
- save control panel settings to .emi file.

Default service code (ATS) is 0000 – it is recommended to change it to unique, preferably 7-digit code. In case of losing this code it will be necessary to send the device to EBS office.

6.4.12. Allow quick arming without user authorization

When this function is selected, it is possible to quickly arm the system using a keypad, without the need to enter the user authorisation code. Partial or complete disarming of any part of the system will only possible using the sequence where the code is entered.

6.4.13. After disarming disable alarm history notification

When this function is selected, 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, (refer to chapter 6.4.14) 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, untill 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.

6.4.14. Alarm history notification disabling delay

This function is only availible after checking "After disarming disable alarm history notification" option. It sets the delay time in seconds, after which the alarm memory will no longer be shown on the keypad. It means, that when the system is armed, and there will be violation of input zones shown by the F and 6 diodes blinking, then after disarming and previously defined time the diodes will turn off. The alarm memory will still be accessible with 3# function, until the user decides to delete it.

6.4.15. Prevent arming using wired keypad when inputs are triggered or sabotaged

If this option is selected, you can't arm the system with KP32 if the detectors have been triggered or tampered with. Triggering/tampering with any detector assigned to the system is signalled by the diodes READY – D going off – in the case of a detector assigned to Partition 1; 4 in the case of a detector from Partition 2. If the system has been broken into two partitions, you can't arm the control panel even, if the detector has been triggered/tampered within only one of them. When attempting to arm the system, the wired keypad emits a high one-second sound and, at the same time, the diodes GROUP, ALARM, SYSTEM and PROG will go on for about 4 seconds. System failures do not affect this option.
NOTE: This option is available since the firmware version 2.8.8.

6.4.16. Time to detect loss of wireless detector

This function allows you to set the time after which a notification is sent to the monitoring station about the loss of the wireless detector.

The time is expressed in hours. The default value is 6 hours, the minimum is 2 and the maximum is 24.
NOTE: This option is available since the firmware version 2.8.8.

6.4.17. Repeat every

This function allows you to switch on periodic repeating of wireless detector loss events to the monitoring station (starting from the first loss).

The time is expressed in hours. The default value is 6 hours, the minimum is 2 and the maximum is 24.
NOTE: This option is available since the firmware version 2.10.0.

6.4.18. Access code length

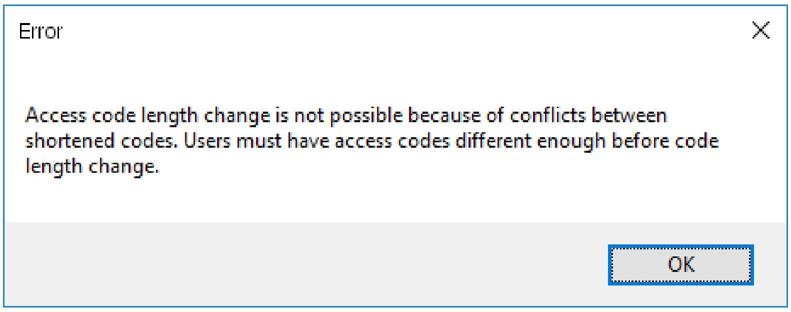
The function enables setting the length of the administrator and user codes (the change applies to all users). The code range is from 4 to 7 digits. By default, this value is set to 4.

⚠ **Reducing the code length is possible only if the shortened user codes do not conflict with each other.**

During shortening the access code length is recommended to remove old and upload a new users to avoid conflicts.

Example:

There are 5-digit codes in the CPX database – 44440, 44444, and 44449. It will not be possible to shorten the code to 4 digits due to the conflict of identical resulting codes. The change will not be accepted, which the keypad will signal with a several seconds long continuous sound and a message window will be displayed):



Access code length change is not possible because of conflicts between shortened codes. Users must have access codes different enough before code length change.

In such a case, one solution is to delete a user or users who have similar codes.

1. **If the user code in the CPX database is shorter than the defined value, then '0' will be added to the codes at their ends:**

   Example: If the code 1234 exists in the database, then after code length is changed to 6 digits, the code will appear as 123400.

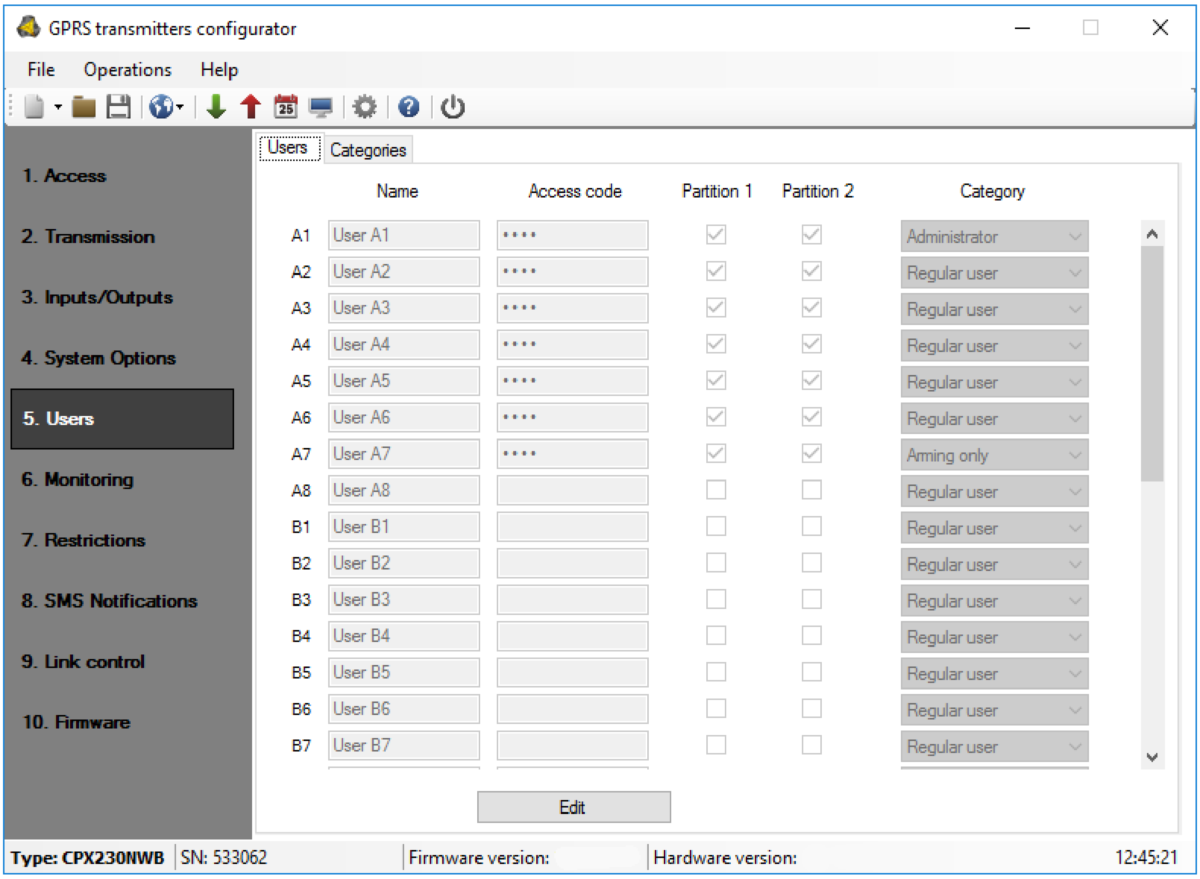
2. **If a user code in the CPX database is longer than the defined value, then the access code will be the "n" first digits, according to the value set.**

   ⚠ **Example: If the code 1234567 exists in the database, then after code length is changed to 5 digits, the code will appear as 12345.**

3. **For codes under duress:**
   - **If the code 12345 exists in the database, then after code length is changed to 7 digits, the code will appear as 1234500, so the code under duress will be 1234501.**
   - **If the code 12345 exists in the database, then after code length is changed to 4 digits, the code will appear as 1234, so the code under duress will be 1235.**

6.5. USERS

6.5.1. Users

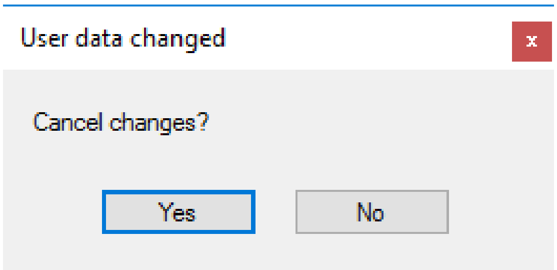


	Name	Access code	Partition 1	Partition 2	Category
A1	User A1	••••	☑	☑	Administrator
A2	User A2	••••	☑	☑	Regular user
A3	User A3	••••	☑	☑	Regular user
A4	User A4	••••	☑	☑	Regular user
A5	User A5	••••	☑	☑	Regular user
A6	User A6	••••	☑	☑	Regular user
A7	User A7	••••	☑	☑	Arming only
A8	User A8		□	□	Regular user
B1	User B1		□	□	Regular user
B2	User B2		□	□	Regular user
B3	User B3		□	□	Regular user
B4	User B4		□	□	Regular user
B5	User B5		□	□	Regular user
B6	User B6		□	□	Regular user
B7	User B7		□	□	Regular user

Type: CPX230NWB | SN: 533062 | Firmware version: | Hardware version: | 12:45:21

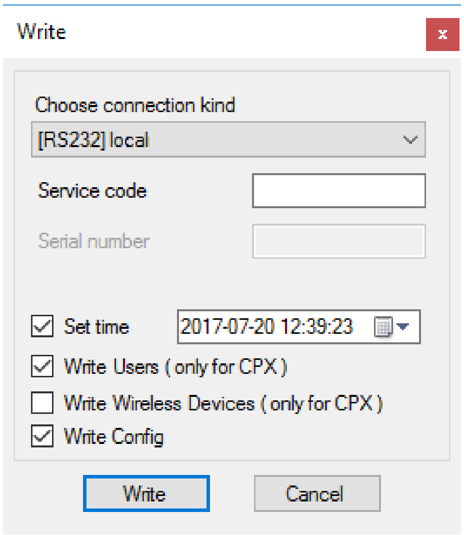
This option allows user managing. To be able to manager the users one has to press the 'Edit' button first and the input the correct administrator code. Granted the authorization, it will be possible to edit the users' passwords, partition privileges and category choose (regular user, arming only).

After editing press the 'Accept changes' button to save the configuration in the program, or press the "Cancel" button to withdraw the entered data. Then a question box will appear:


User data changed

Cancel changes?

After accepting changes please remember to upload the configuration to the device. When uploading a configuration, "Write users" option must be selected in the writing options (second box):



Write

Choose connection kind: [RS232] local

Service code

Serial number

☑ Set time 2017-07-20 12:39:23

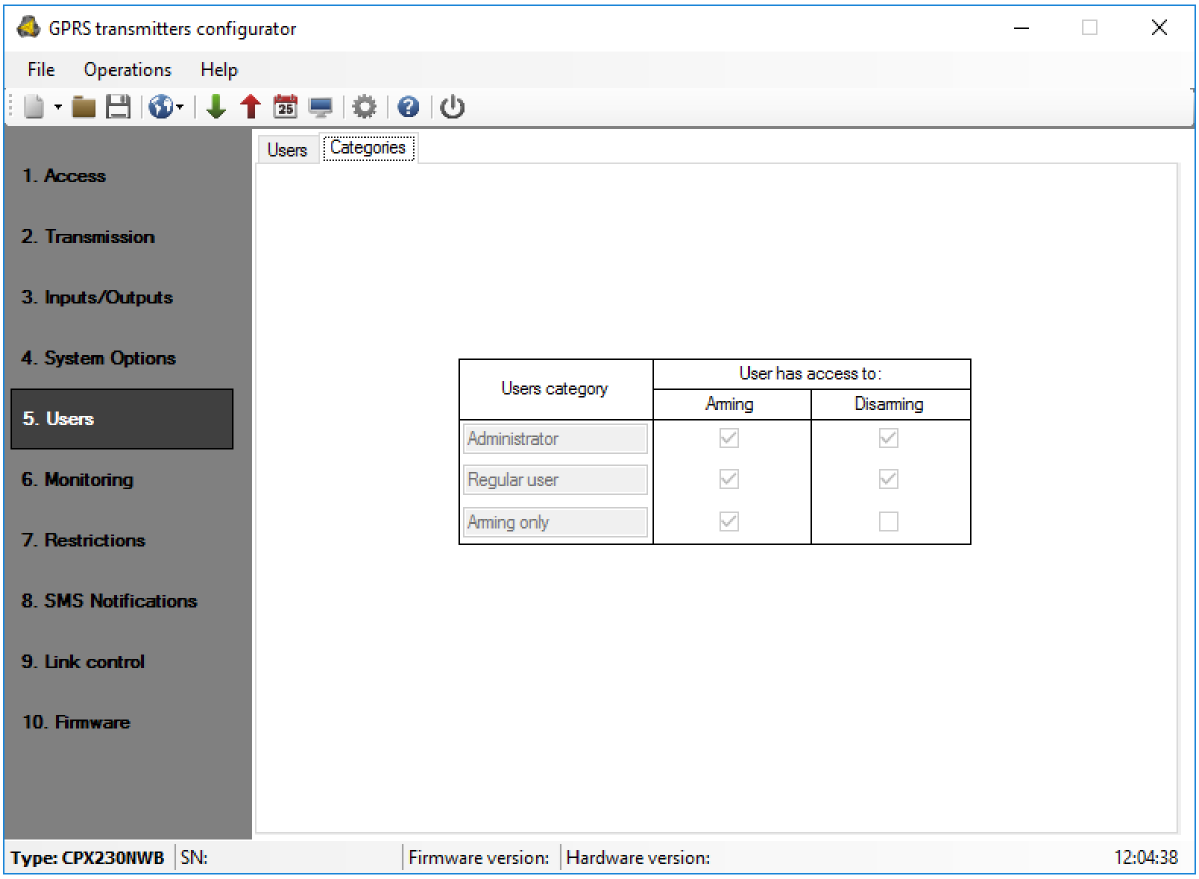
☑ Write Users (only for CPX)

☐ Write Wireless Devices (only for CPX)

☑ Write Config

Users' configuration changes can be made only via programming cable. Users update is not possible remotely via GPRS.

6.5.2. User categories



Users category	User has access to:	
	Arming	Disarming
Administrator	☑	☑
Regular user	☑	☑
Arming only	☑	☐

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 12:04:38

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.

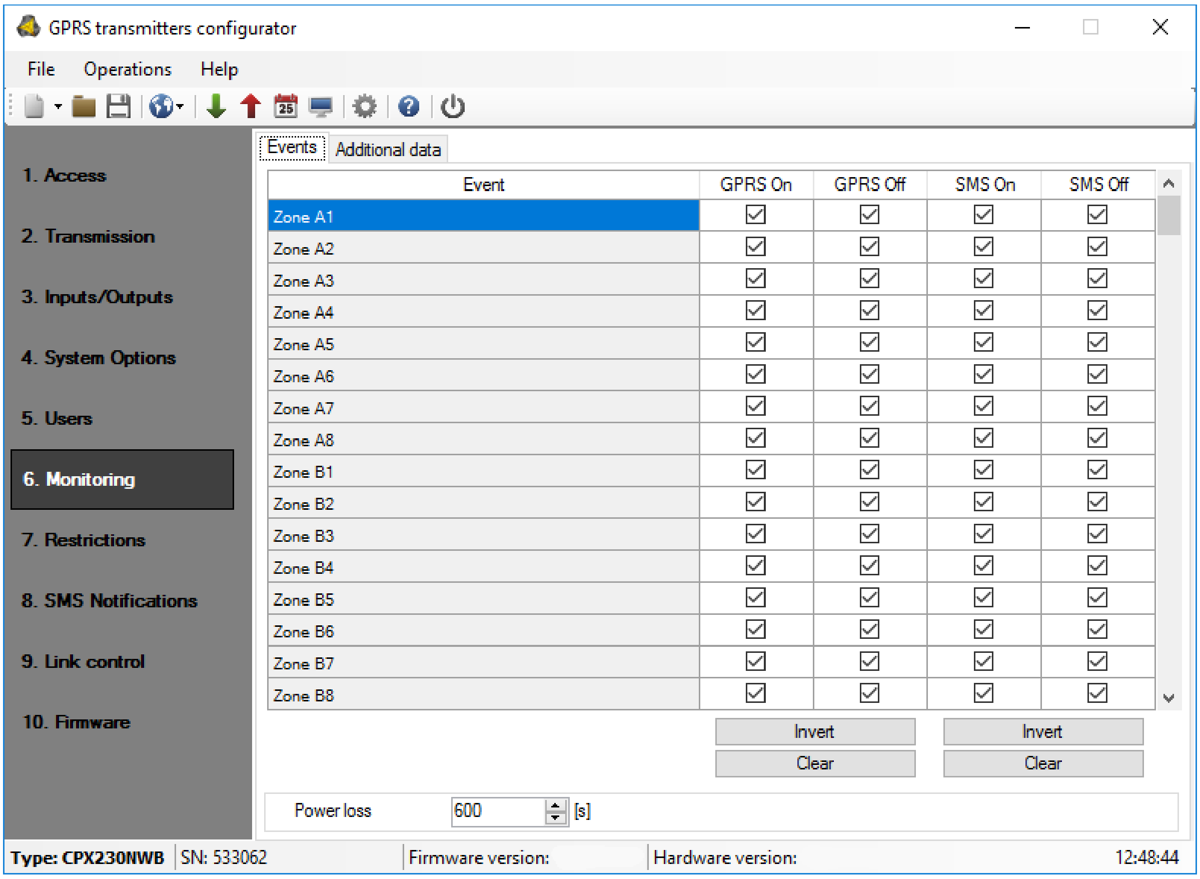
2. Regular user – a user who can arm and disarm the system and has access to the history of alarms and failures, the status of inputs, and can block inputs, change their code, test inputs and outputs.
3. Arming only – a user who can only arm the system. They do not have access to functions that require a code. If the option "Access to alarm and fault memory requires authorisation" has not been enabled during the set-up, this user can enter the functions to which this option applies (see chapter 9).

6.6. MONITORING

That option allows determining which of available signals generated by the equipment will be transmitted to the monitoring station.

NOTE: The "Configuration change" event refers to configuration change via SMS or via GPRS instructions only.

6.6.1. Events



Event	GPRS On	GPRS Off	SMS On	SMS Off
Zone A1	☑	☑	☑	☑
Zone A2	☑	☑	☑	☑
Zone A3	☑	☑	☑	☑
Zone A4	☑	☑	☑	☑
Zone A5	☑	☑	☑	☑
Zone A6	☑	☑	☑	☑
Zone A7	☑	☑	☑	☑
Zone A8	☑	☑	☑	☑
Zone B1	☑	☑	☑	☑
Zone B2	☑	☑	☑	☑
Zone B3	☑	☑	☑	☑
Zone B4	☑	☑	☑	☑
Zone B5	☑	☑	☑	☑
Zone B6	☑	☑	☑	☑
Zone B7	☑	☑	☑	☑
Zone B8	☑	☑	☑	☑

Power loss 600 [s]

Type: CPX230NWB SN: 533062 Firmware version: Hardware version: 12:48:44

6.6.1.1. GPRS ON/OFF

In these columns you can check which signals are to be reported to the monitoring station via GPRS transmission. You have the option to send information on both, alarms (change of zone state from idle into active) and returns of zones states from active into idle (normalisation). In order to transmit a particular signal you have to check it (by clicking a relevant check box on the right hand side).

Press [Clear] button to remove all checked signals.

Press [Reverse] to reverse the check into the opposite ones.

6.6.1.2. SMS ON/OFF

In these columns you can check which signals are to be reported to the monitoring station via SMS message – when the equipment is not connected with server via GPRS connection. You have the option to send information on both, alarms (change of input state from idle into active) and returns of zone states from active into idle (normalisation). In order to transmit a particular signal you have to check it (by clicking a relevant check box on the right hand side).

Press [Clear] button to remove all checked signals.

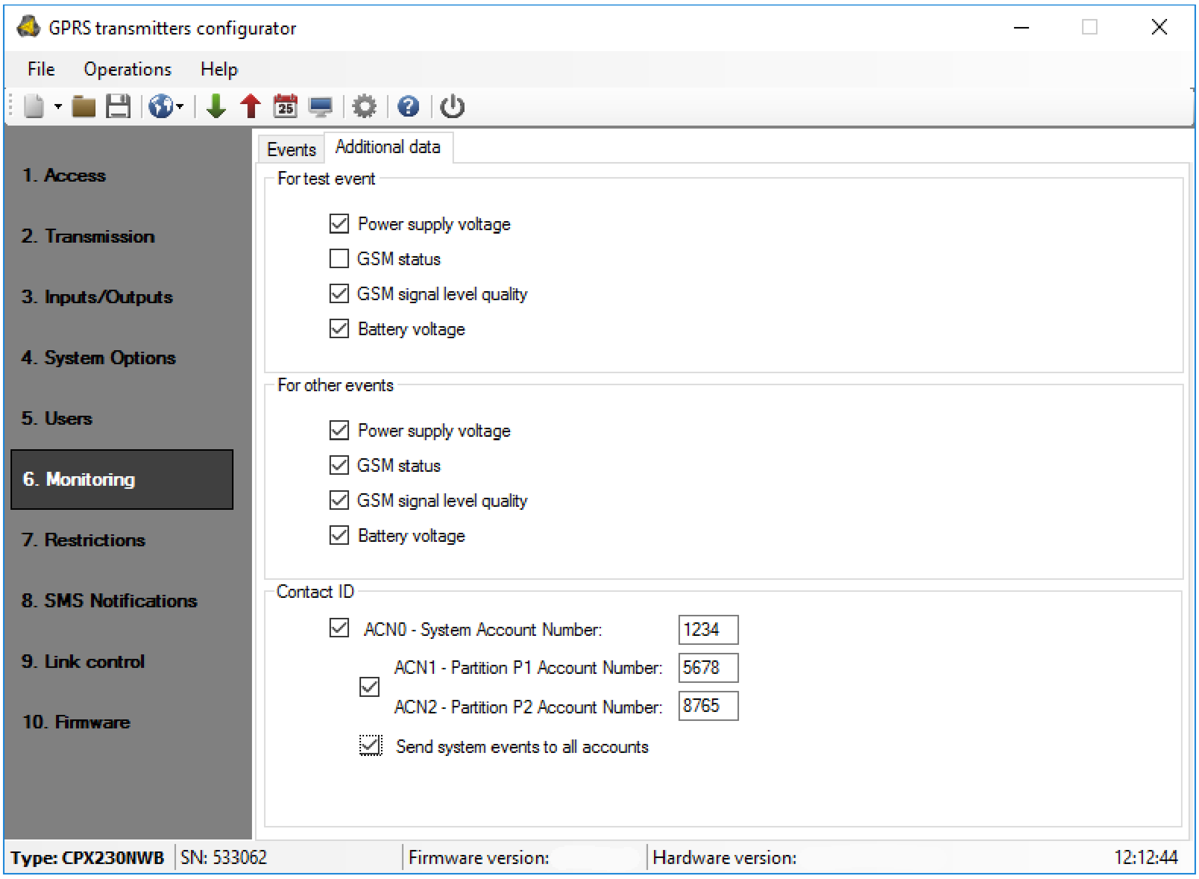
Press [Reverse] to reverse the check into the opposite ones.

6.6.1.3. Power loss

One of the additional options of the equipment is the control of supplying voltage. As transient power losses can occur in some facilities, you can avoid reporting them by entering the time after which the information will be sent. The value of the parameter means that power loss must last for that pre-defined time for the equipment to recognize it a factual power loss and to send a relevant message.

6.6.2. Additional data

The Additional data functionality allows for defining kinds of additional data which will be transmitted together with events to monitoring station via GPRS/SMS. The data may become valuable information about device's work conditions though it may increase amount of bytes sent through GSM network.



For test event

- ☑ Power supply voltage
- □ GSM status
- ☑ GSM signal level quality
- ☑ Battery voltage

For other events

- ☑ Power supply voltage
- ☑ GSM status
- ☑ GSM signal level quality
- ☑ Battery voltage

Contact ID

☑ ACN0 - System Account Number: 1234

☑ ACN1 - Partition P1 Account Number: 5678

ACN2 - Partition P2 Account Number: 8765

☑ Send system events to all accounts

Type: CPX230NWB SN: 533062 Firmware version: Hardware version: 12:12:44

6.6.2.1. For test and other events

It is possible to define two separate sets of additional data kinds: for test events (sent periodically according to setting on Access tab) and for other events. Put a mark next to the name of data kind to turn on transmission of this data kind to monitoring station. Empty field means that this kind of data will be not transmitted.

The adjustable parameters are:

- Power status – information about connected charger and battery charging
- GSM status – status about connection to GSM network, type of connection to server (GPRS/SMS), information about ongoing phone calls
- GSM signal level quality – quality of connection to GSM network (CSQ and BER parameters)
- Battery voltage – voltage of battery in millivolt unit

6.6.2.2. Contact ID

When transmitting data in the Contact ID format, in this section you can define individual numbers for system account identification – ACN0, and its subsystems accounts, partition 1 – ACN1 and partition 2 – ACN2. This allows you to determine, which part of the system the signal from.

NOTE: This option is available since the firmware version 2.9.0.

⚠ **NOTE: Numbers ACN0, ACN1 and ACN2 consist of four hexadecimal characters.**

6.6.2.2.1. System Account Number – ACN0

If ACN0 number is set, it is attached to each system event sent to the monitoring station. System events are those that provide information about the entire system, i.e. power failure, modem reset, clock loss.

6.6.2.2.2. Partition Account Number – ACN1 (partition 1),ACN2 (partition 2)

If numbers ACN1 and ACN2 are set, the ACN1 is attached to each non-system event (with Partition ID 1 and/or 2) with information about partition 1, and to events with information about Partition 2 – the ACN2. Non-system events are those with information about particular partitions, i.e. about arming/disarming Partitions 1 and/or 2, alarms activated by triggering the detectors assigned to partitions.

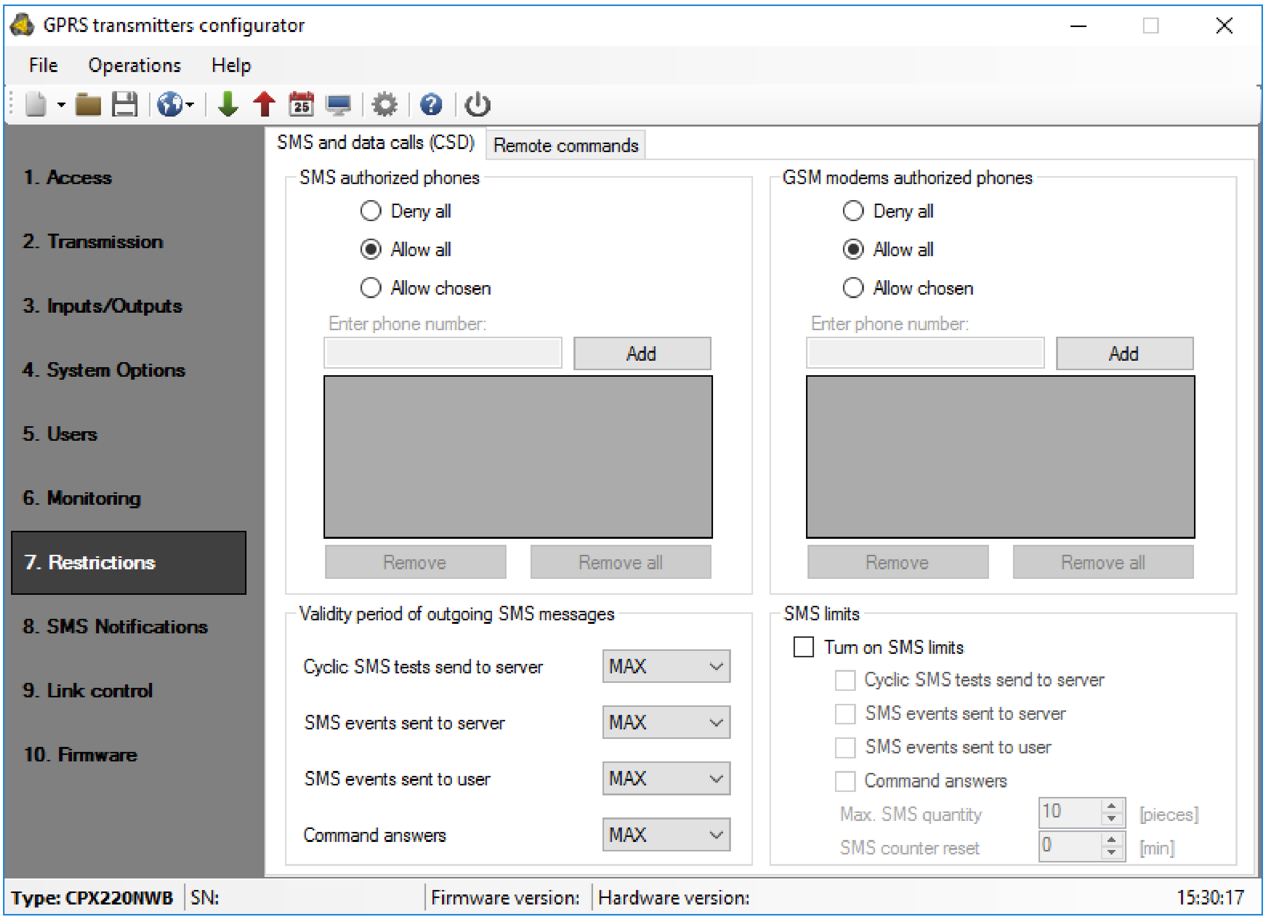
⚠ **If you enter an account number only for one of the partitions, you will not be able to send settings to the control panel. Both ACN1, and ACN2 must be provided.**

6.6.2.2.3. Send system events to all accounts

Selecting this option will send system events to all accounts, i.e. the system account, partition 1 account and partition 2 account.

6.7. RESTRICTIONS

6.7.1. SMS and data calls (CSD)



SMS authorized phones
○ Deny all
● Allow all
○ Allow chosen
Enter phone number:

GSM modems authorized phones
○ Deny all
● Allow all
○ Allow chosen
Enter phone number:

Validity period of outgoing SMS messages
Cyclic SMS tests send to server: MAX
SMS events sent to server: MAX
SMS events sent to user: MAX
Command answers: MAX

SMS limits
□ Turn on SMS limits
□ Cyclic SMS tests send to server
□ SMS events sent to server
□ SMS events sent to user
□ Command answers
Max. SMS quantity: 10 [pieces]
SMS counter reset: 0 [min]

Type: CPX220NWB | SN: | Firmware version: | Hardware version: | 15:30:17

6.7.1.1. Authorized SMS Telephone Numbers

The user can restrict a remote access to the equipment (via SMS) from pre-defined telephone numbers. Created list of telephone numbers (up to 5) means that the equipment can be controlled from these telephone numbers only.

Available options are:

- Restrict all: Means no possibility of communication.
- Allow all: Means that communication is allowed from any telephone number.
- Allow selected: Means that communication is allowed only from these listed telephone numbers. You can define up to 5 telephone numbers.

When 'Allow selected' box is selected you receive access to an edit box. Enter the subsequent numbers in the box and click [Add] button to move the number to the table below. To remove the number from the table, place the cursor in a particular number zone and click [Remove].

"Remove all" option will clear all the numbers from the table.

⚠ **NOTE: Incoming SMSs are authorized by comparing the number from which the SMS arrived with the ones that are entered in the table. It is allowed to enter only a part of the number in the table e.g. 1234. Then, all numbers containing the stipulated sequence, e.g. 600123456 or 601234567 will be accepted.**

⚠ **NOTE: If modem connected to OSM.Server server will be used for sending SMS, its telephone number must be added to the above list**.

6.7.1.2. Authorized GSM Modems Numbers

For connections in CSD channel the user can restrict a remote access to the equipment via GSM modems. Created list of numbers (up to 5) means that the equipment can communicate with these numbers only.

Available options are:

- Restrict all: Means no possibility of communication.
- Allow all: Means that communication is allowed from any telephone number.
- Allow selected: Means that communication is allowed only from these listed telephone numbers. You can define up to 5 numbers.

When 'Allow selected' box is checked, you receive access to an edit box. Enter the subsequent numbers in the box and click [Add] button to move the number to the table below. To remove the number from the table, place the cursor in a particular number zone and click [Remove].

"Remove all" option will clear all the numbers from the table.

⚠ NOTE: Incoming CSD connection is authorized by comparing the number from which it arrived with the ones that are entered in the table. It is allowed to enter only a part of the number in the table e.g. 1234. Then, all numbers containing the stipulated sequence, e.g. 600123456 or 601234567 will be accepted.

⚠ NOTE: If modem connected to OSM.Server server will be used for incoming CSD connection, its telephone number must be added to the above list.

6.7.1.3. Validity Period of Outgoing SMS

The user can define time for the equipment to transfer information via SMS. Validity period is defined separately for the following groups of information:

- SMS tests to server
- SMS events sent to server
- SMS events sent to the user
- Replies to commands

You have an option to select among the values on a drop list by clicking the arrow next to the check box. Available options are: 5, 10, 15, 30 minutes; 1, 2, 6, 12 hours; 1, 7 days; MAX (no validity period set).

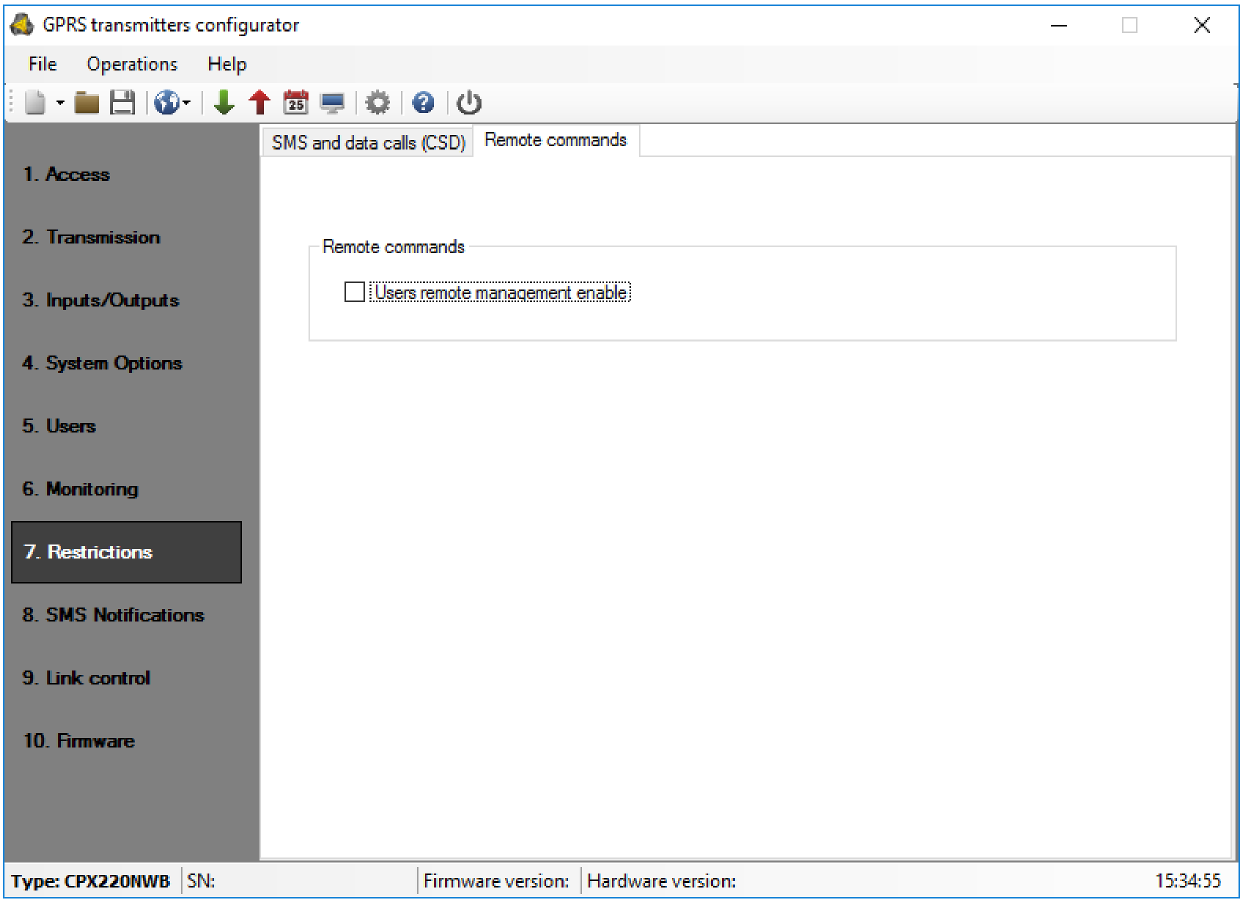
Outgoing SMS

The user can restrict the number of SMS to be sent by the equipment. As GPRS shall be the primary transmission mode, this restriction is important mainly for economic reasons.

Check the [Activate SMS restrictions] check box to activate the access to information groups subject to restrictions:

- SMS tests to server
- SMS events sent to server
- SMS events sent to the user
- Replies to commands
- Restrictions are defined by specifying two values:
- Max number of SMS: Defines a maximum number of SMS sent in a time unit (please refer to 'Counter reset' parameter). This option protects the user against sending too large volume of SMS, e.g. in case of a fault.
- Counter reset: That parameter defines time (in minutes) after which the counter of SMS sent is to be reset.

6.7.2. Remote commands



Remote commands

□ Users remote management enable

Type: CPX220NWB | SN: | Firmware version: | Hardware version: | 15:34:55

6.7.2.1. Users remote management enable

Selecting this option allows you to remotely configure user accounts.

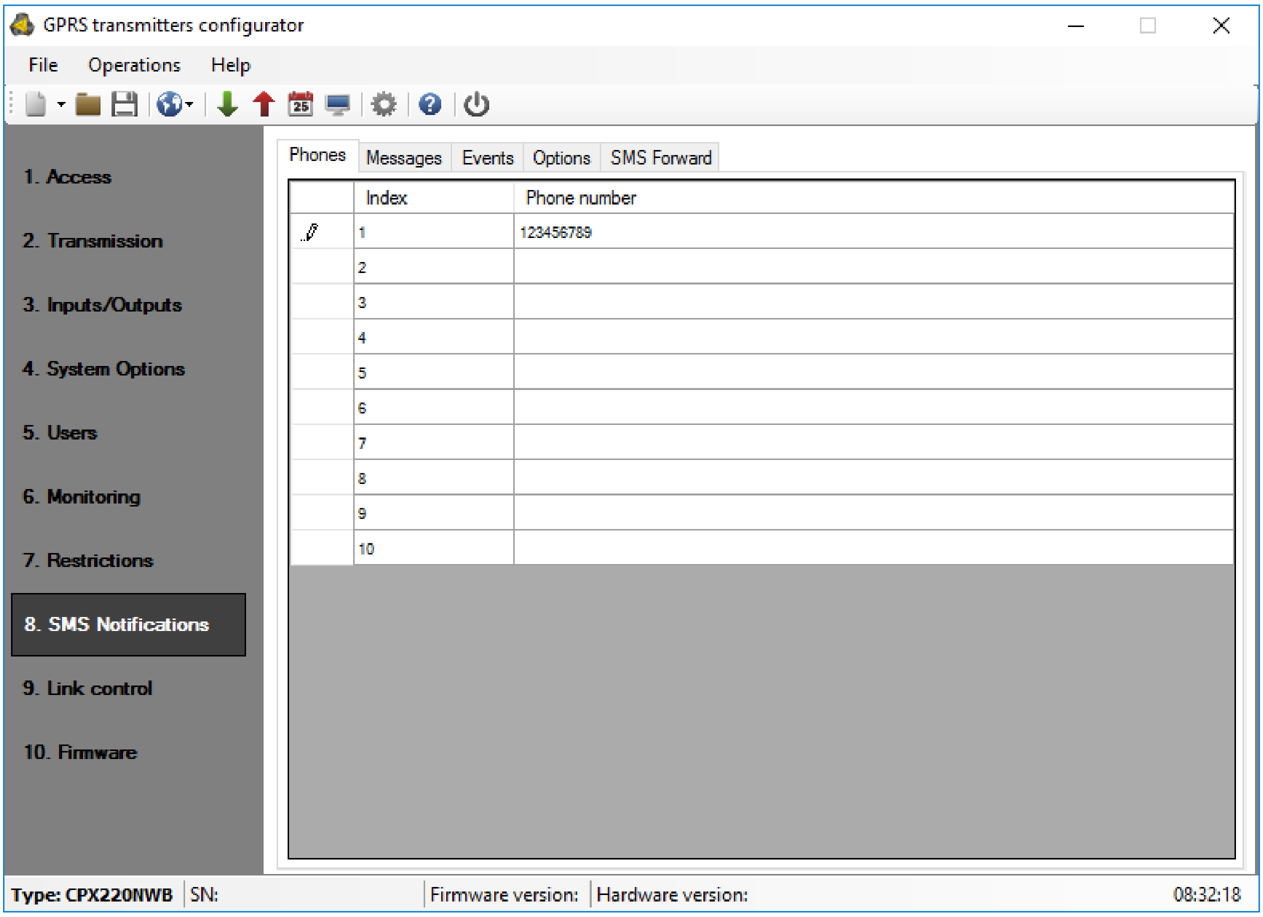
NOTE: If the user will use mobile application AVA the option “Users remote management enable” have to be turn on.

6.8. SMS NOTIFICATIONS

6.8.1. Phones

CPX230NWB can notify users about occurrence of certain events by text message. Before sending the message, may occur an additional attempt a voice call (see item 6.8.4. Options).

In order to add user’s number to the notification list, one has to type in the number next to the number index. Device can handle up to 10 phone numbers.



Index	Phone number
1	123456789
2	
3	
4	
5	
6	
7	
8	
9	
10	

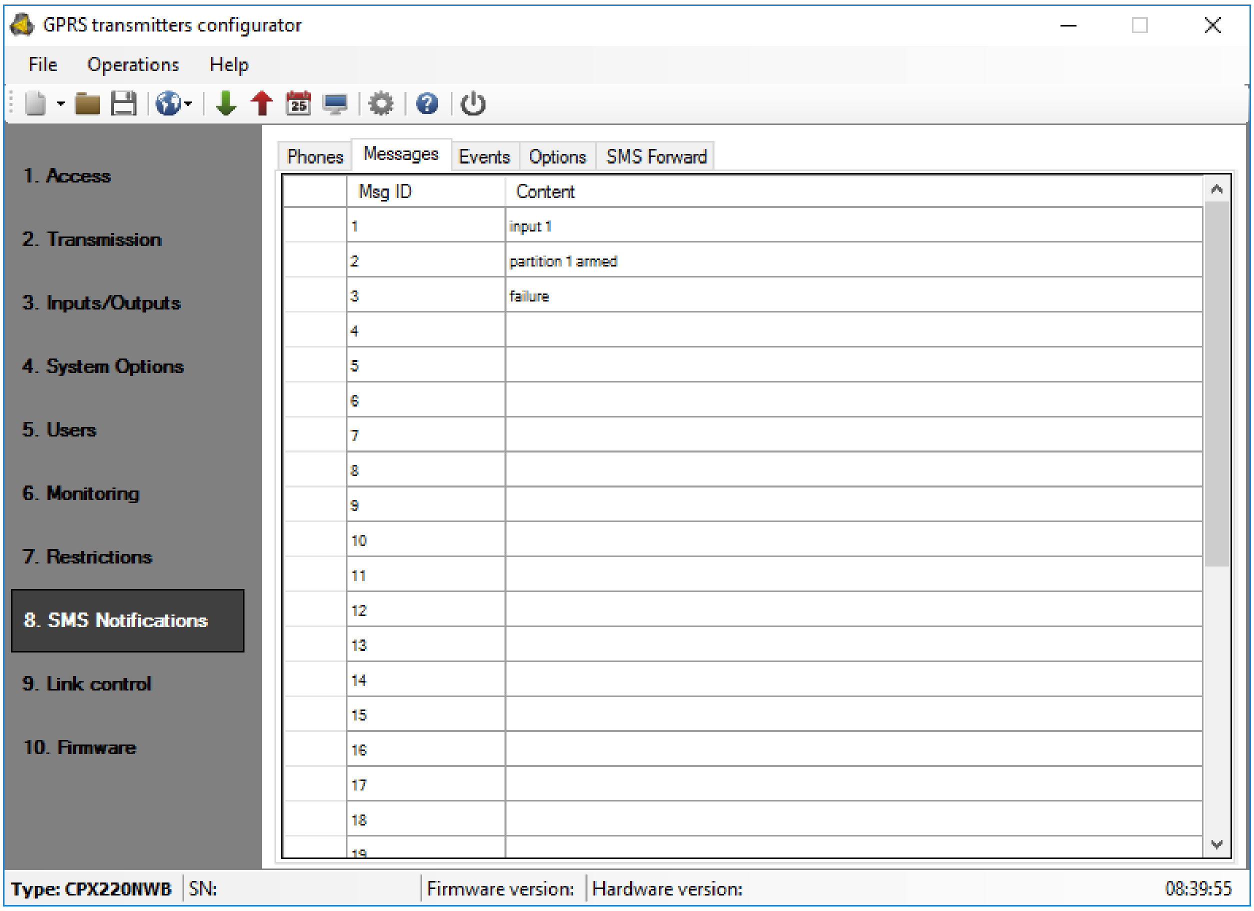
Type: CPX220NWB | SN: | Firmware version: | Hardware version: | 08:32:18

6.8.2. Messages

Text for each message has to typed in the Messages tab. These messages can be later assigned to specific events in the Events tab. Before sending the message, may occur an additional attempt a voice call (see item 6.8.4. Options).

NOTE

In text messages can be used only alphanumeric characters, as well as: ! @ # $ % " < > & * ( ) + : ? ` ; ' = , . / and space.

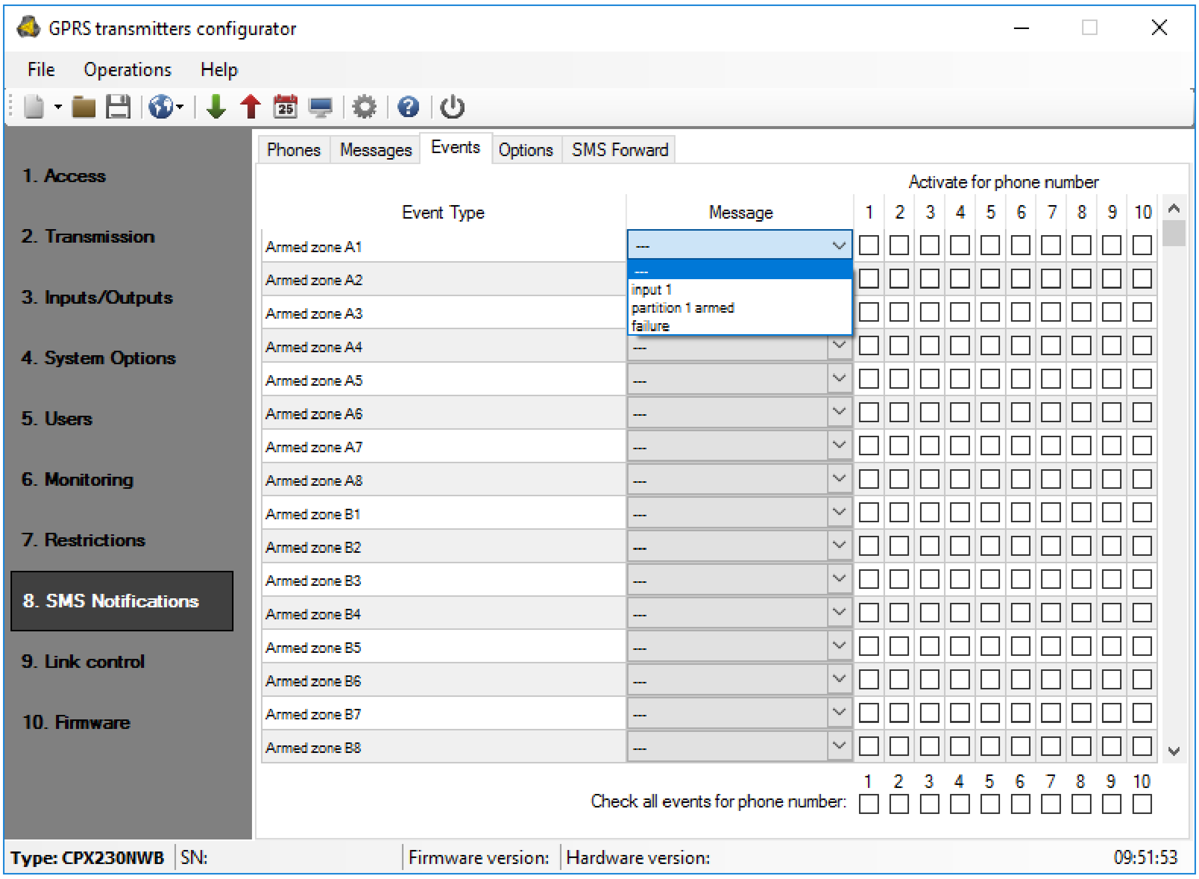


Msg ID	Content
1	input 1
2	partition 1 armed
3	failure
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	

Type: CPX220NWB | SN: | Firmware version: | Hardware version: | 08:39:55

6.8.3. Events

In order to assign a message to an event, one has to select Event Type, and for that Event Type in the Message column, select one of the messages defined before. To assign a number to an event, a corresponding column from Num 1 to Num 10 has to be checked. From now on, whenever this event occurs, a text containing selected message will be send to the selected phone numbers. Before sending the message, may occur an additional attempt a voice call (see item 6.8.4. Options).



Activate for phone number

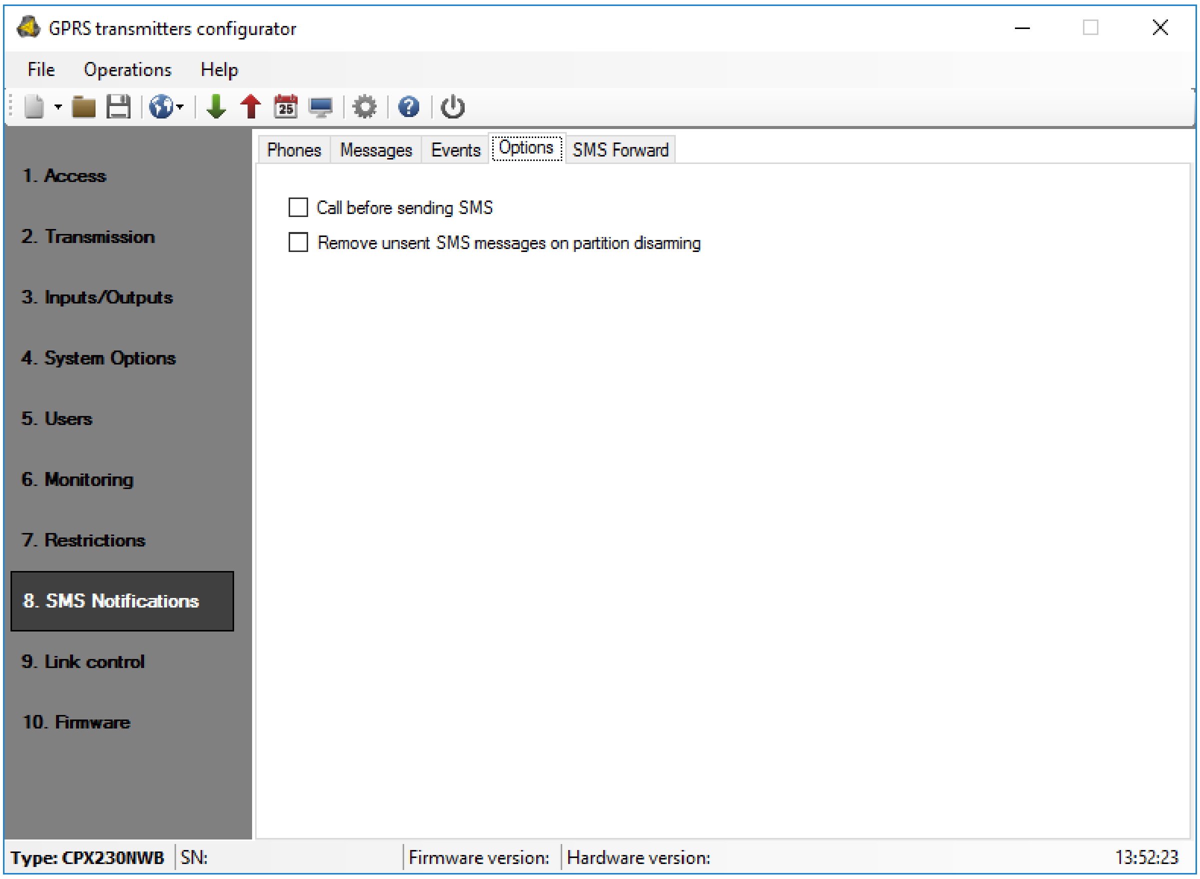
Event Type	Message	1	2	3	4	5	6	7	8	9	10
Armed zone A1	---	□	□	□	□	□	□	□	□	□	□
Armed zone A2		□	□	□	□	□	□	□	□	□	□
Armed zone A3		□	□	□	□	□	□	□	□	□	□
Armed zone A4	---	□	□	□	□	□	□	□	□	□	□
Armed zone A5	---	□	□	□	□	□	□	□	□	□	□
Armed zone A6	---	□	□	□	□	□	□	□	□	□	□
Armed zone A7	---	□	□	□	□	□	□	□	□	□	□
Armed zone A8	---	□	□	□	□	□	□	□	□	□	□
Armed zone B1	---	□	□	□	□	□	□	□	□	□	□
Armed zone B2	---	□	□	□	□	□	□	□	□	□	□
Armed zone B3	---	□	□	□	□	□	□	□	□	□	□
Armed zone B4	---	□	□	□	□	□	□	□	□	□	□
Armed zone B5	---	□	□	□	□	□	□	□	□	□	□
Armed zone B6	---	□	□	□	□	□	□	□	□	□	□
Armed zone B7	---	□	□	□	□	□	□	□	□	□	□
Armed zone B8	---	□	□	□	□	□	□	□	□	□	□

	1	2	3	4	5	6	7	8	9	10
Check all events for phone number:	□	□	□	□	□	□	□	□	□	□

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 09:51:53

6.8.4. Options

In this section you can enable additional options for sending SMS messages.



□ Call before sending SMS

□ Remove unsent SMS messages on partition disarming

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 13:52:23

6.8.4.1. Call before sending SMS

“Call before sending SMS” option should be selected if you need additional information about the incoming SMS message. If this option is activated, before sending an SMS the device “rings” the user to inform about the incoming SMS.

The connection attempt takes several seconds. The user can reject or accept the call. If a user receives a call, the unit will disconnect the call. After trying to call, the device sends an SMS message.

Sending a message to the first user (the first defined phone number), is followed by an attempt to call the next user and send a message. And so on.

A voice call to a single user occurs no more than once every 15 minutes.

6.8.4.2. Remove unsent SMS messages on partition disarming

If option is enabled, disarming the partition removes all waiting SMS, except the SMS messages related to partition is still armed.

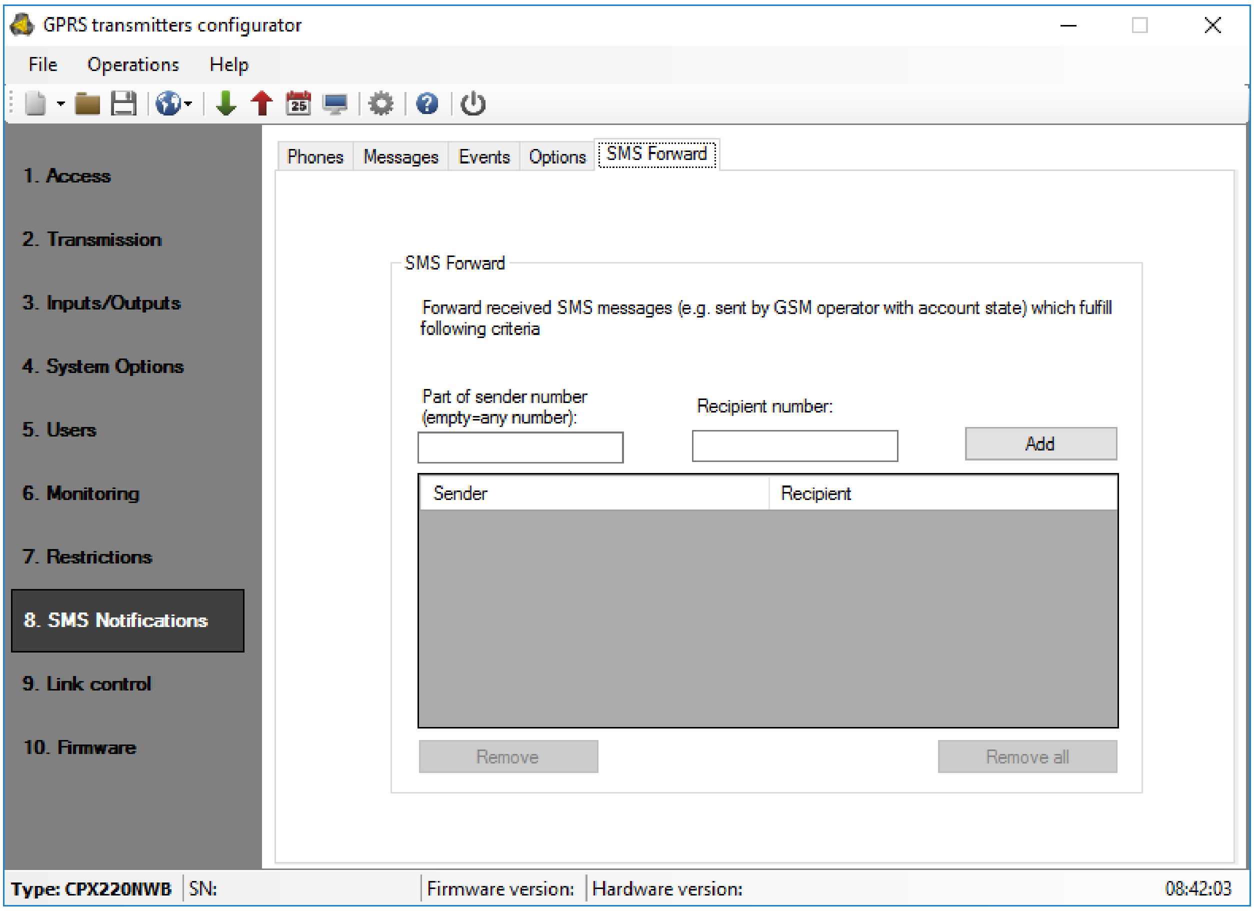
In other words, waiting (unsent) SMS messages related to disarmed partition and related to the alarm system will be removed and will not be sent.

If the user disarm both partitions, all waiting SMS messages will be removed.

All SMS messages related to new events occurs after disarming, will be saved in memory and sent as soon as possible.

Note: The producer does not recommend using this option because it reduces security of the system. The option for use only by advanced users.

6.8.5. SMS Forward



SMS Forward

Forward received SMS messages (e.g. sent by GSM operator with account state) which fulfill following criteria

Part of sender number (empty=any number):

Recipient number:

Sender	Recipient

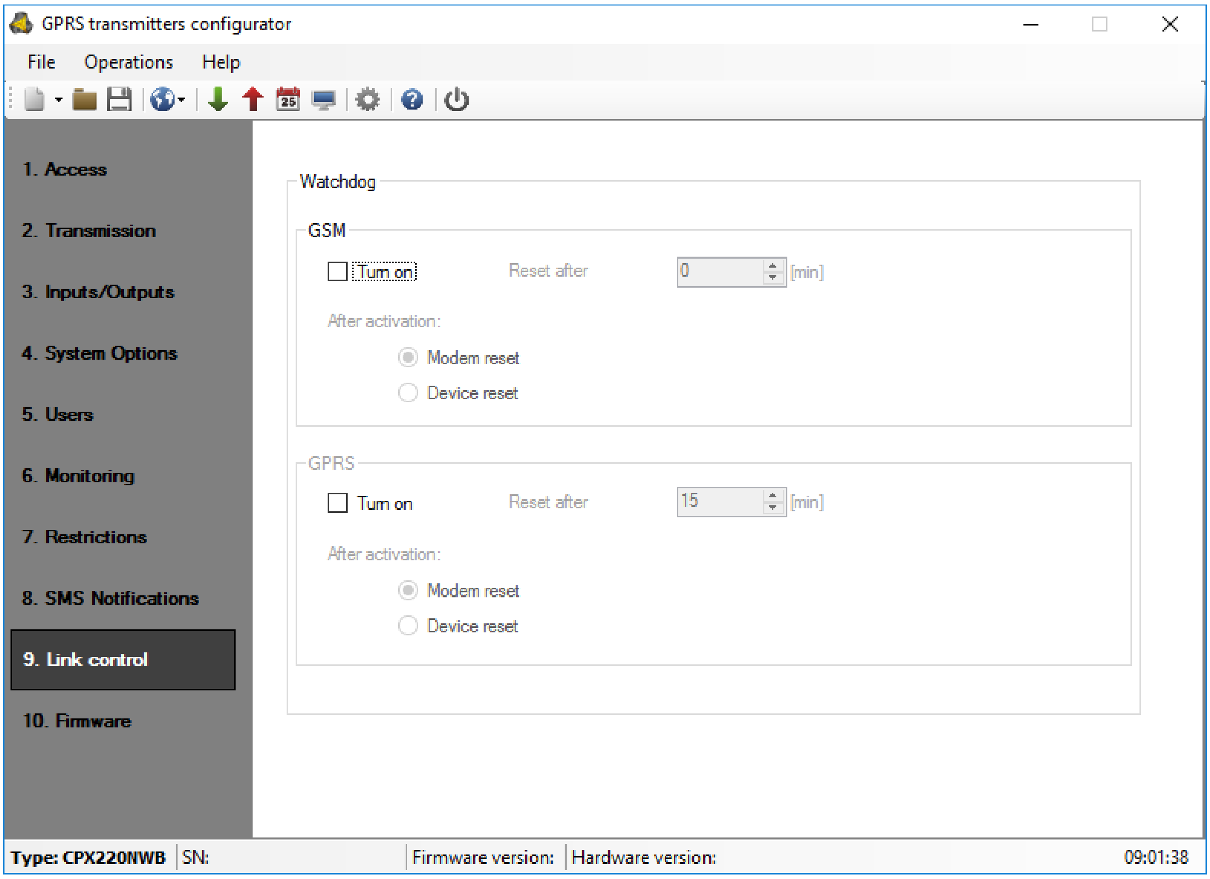
The equipment is able to transfer the received SMS messages to pre-defined telephone numbers in accordance with pre-defined rules. The function may prove necessary in case of account info sent via SMS. In this box you can enter up to 2 rules intended for transfer of SMS messages.

Each rule is composed of a set: a fragment of a sender's telephone number and correct telephone number of a recipient. In extreme situation a fragment of sender's telephone number can be composed of an empty sequence, which means it is applicable to any telephone number. Rules are processed in accordance with a pre-defined sequence from the beginning to the end, i.e. the result of processing of a given rule does not influence the processing of the subsequent rules. It also means that a given SMS message can be sent to a few telephone numbers or that the same SMS can be sent a few times to the same telephone number. Such a case occurs when the condition that refers to a sender's telephone number is met for at least two rules having the same recipient's number.

⚠ **NOTE: The user is responsible for correct entering the telephone numbers that prevents any turmoil in sending SMS messages.**

6.9. LINK CONTROL

These options allow automatic equipment's response in case the connection with the monitoring station is lost. It refers to situations when the equipment lost the connection with GSM network or GPRS transmission is not possible.



Watchdog

GSM

□ Turn on   Reset after 0 [min]

After activation:

● Modem reset

○ Device reset

GPRS

□ Turn on   Reset after 15 [min]

After activation:

● Modem reset

○ Device reset

Type: CPX220NWB | SN: | Firmware version: | Hardware version: | 09:01:38

6.9.1. GSM

Activating that function (checking the [Activate] box) allows the access to parameters defining the equipment's response after leaving GSM network.

You can define after what time from the moment the connection was lost the equipment shall initiate activities aiming at its restoration. The time is selected in a [Reset after] box and is defined in minutes.

Then, define what activity shall be initiated by the equipment. Select by checking an appropriate box at the response description:

- Modem reset
- Device reset

In case the equipment lost the GSM connection, it shall wait for a defined period of time after the fact was ascertained and then it shall perform stipulated tasks.

6.9.2. GPRS

Activating that function (checking the [Activate] box) allows the access to parameters defining the equipment's response after losing connection with a server.

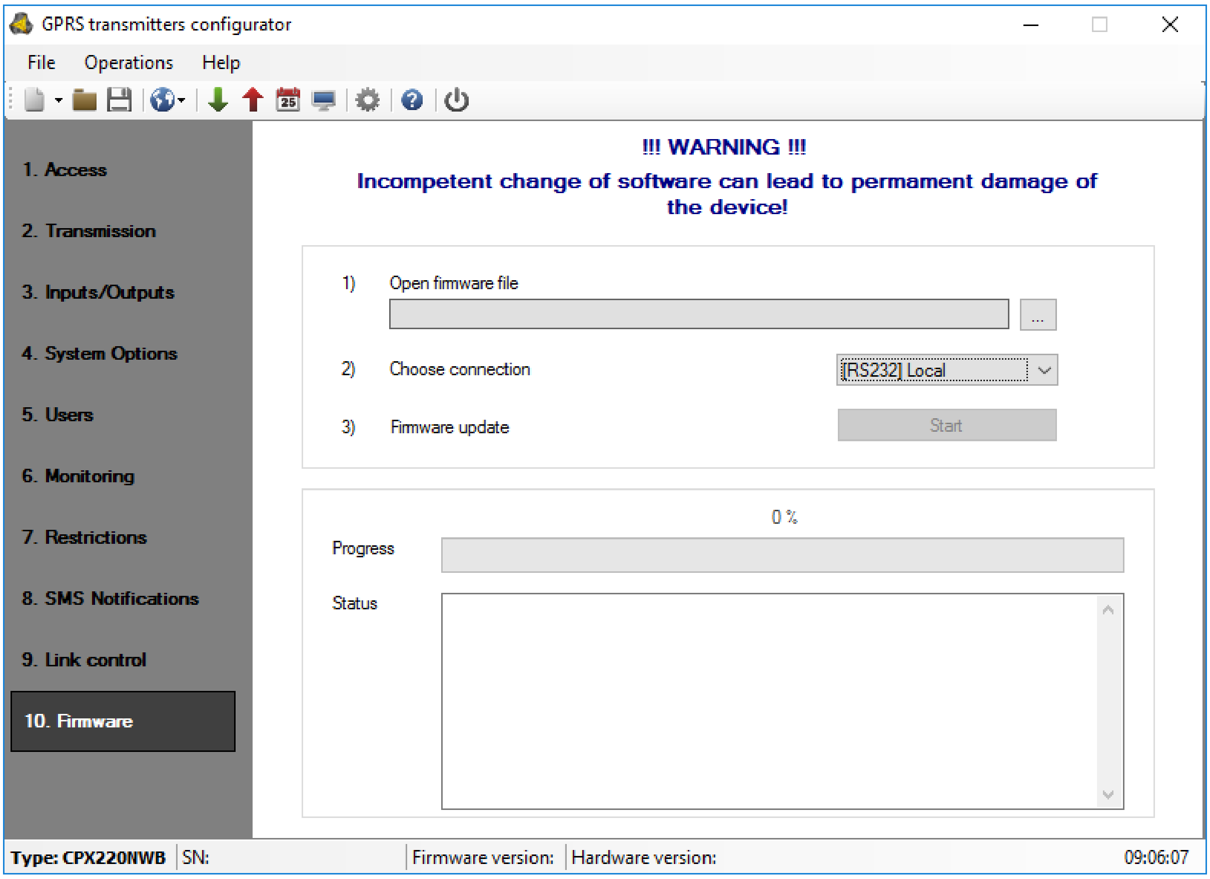
You can define after what time from the moment the connection was lost the equipment shall initiate activities aiming at its restoration. The time is selected in a [Reset after] box and is defined in minutes.

Then, define what activity shall be initiated by the equipment. Select by checking an appropriate box at the response description:

- Modem reset
- Device reset

In case the equipment lost the GPRS connection, it shall wait for a defined period of time after the fact was ascertained and then it shall perform stipulated tasks.

6.10.FIRMWARE



!!! WARNING !!!

Incompetent change of software can lead to permament damage of the device!

1) Open firmware file

2) Choose connection [RS232] Local

3) Firmware update

0 %

Progress

Status

Type: CPX220NWB | SN: | Firmware version: | Hardware version: | 09:06:07

The equipment has integrated bootloader that enables module software update. During the programming all that process information is displayed.

The following activities shall be performed:

- Start configuration wizard,
- Go to wizard's "Firmware" option,
- Open a file with a new firmware (click [Open] to indicate a location of an appropriate file),
- Select the file transmission method: local.
- Click [Start] button. The software replacement procedure will be initiated.

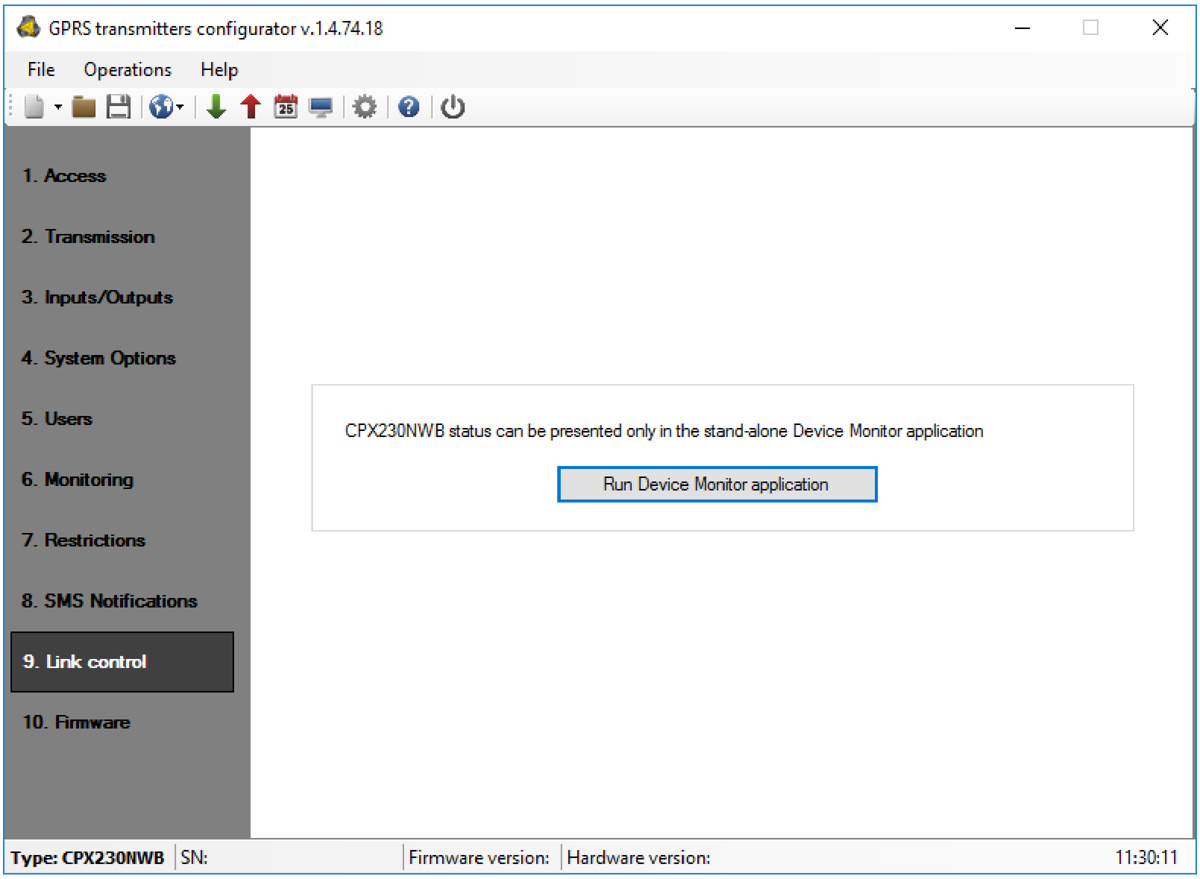
- The course of recording is displayed in special software's window.
- Close the configuration wizard after you finish the recording.
- Wait a few couple of seconds for the equipment to re-start.

Since now the equipment will operate under the control of a new firmware.

NOTE: The firmware update procedure shall be carried out with special care as improperly performed operation can prevent the correct operation of the equipment.

6.11.DEVICE MONITORING

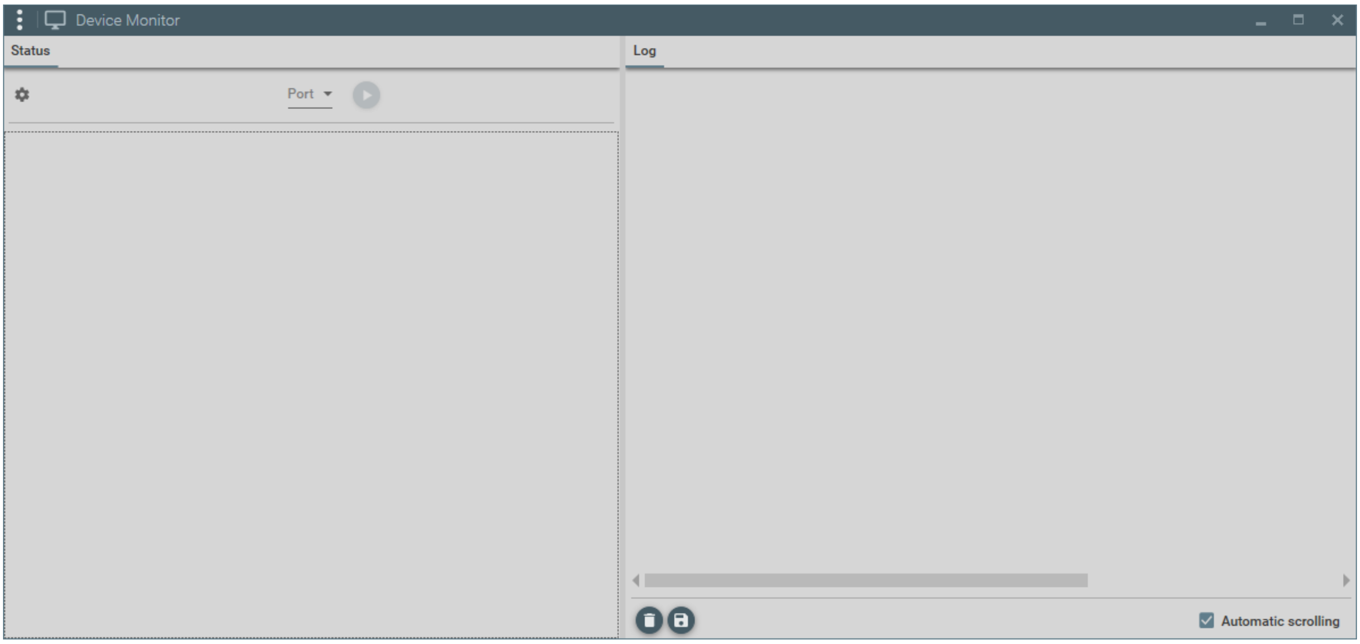
The feature of monitoring the device is accessible from the main menu level - tab Operations -> Device Monitor, or from the quick access menu - monitor icon. After choosing this option, there appears a pop-up window with an information about the necessity of turning on an external application Device Monitor.



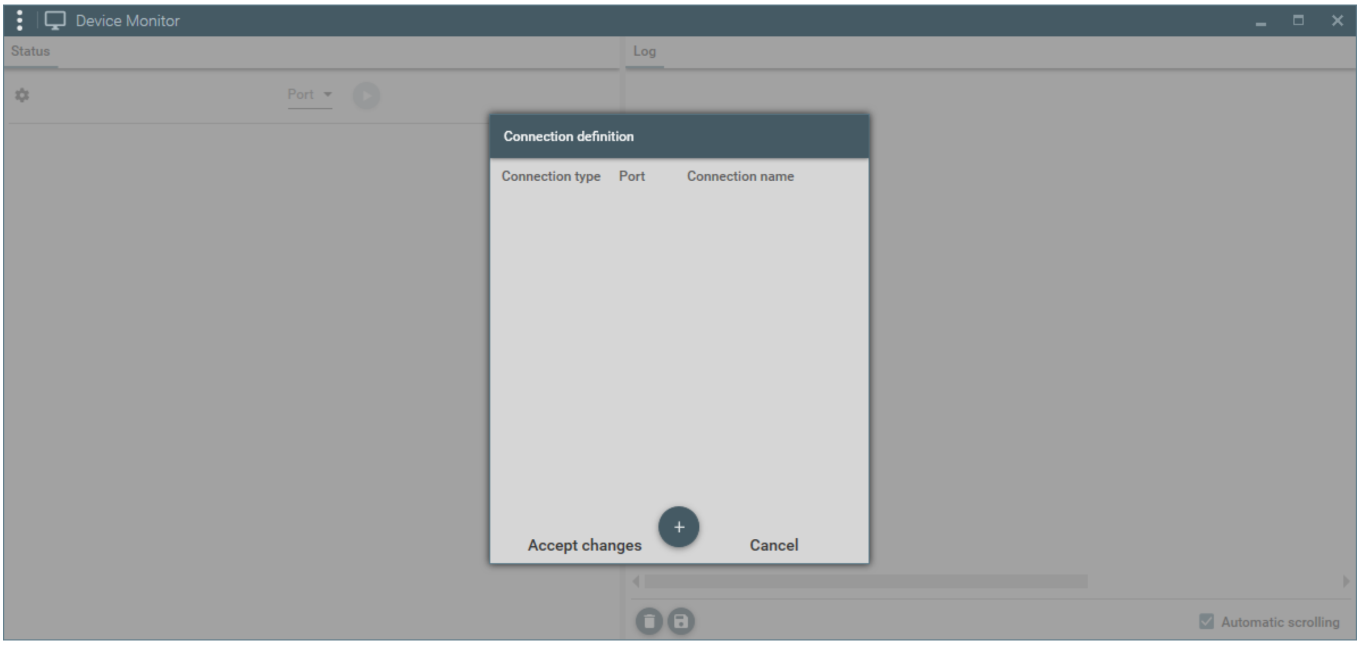
CPX230NWB status can be presented only in the stand-alone Device Monitor application

Type: CPX230NWB | SN: | Firmware version: | Hardware version: | 11:30:11

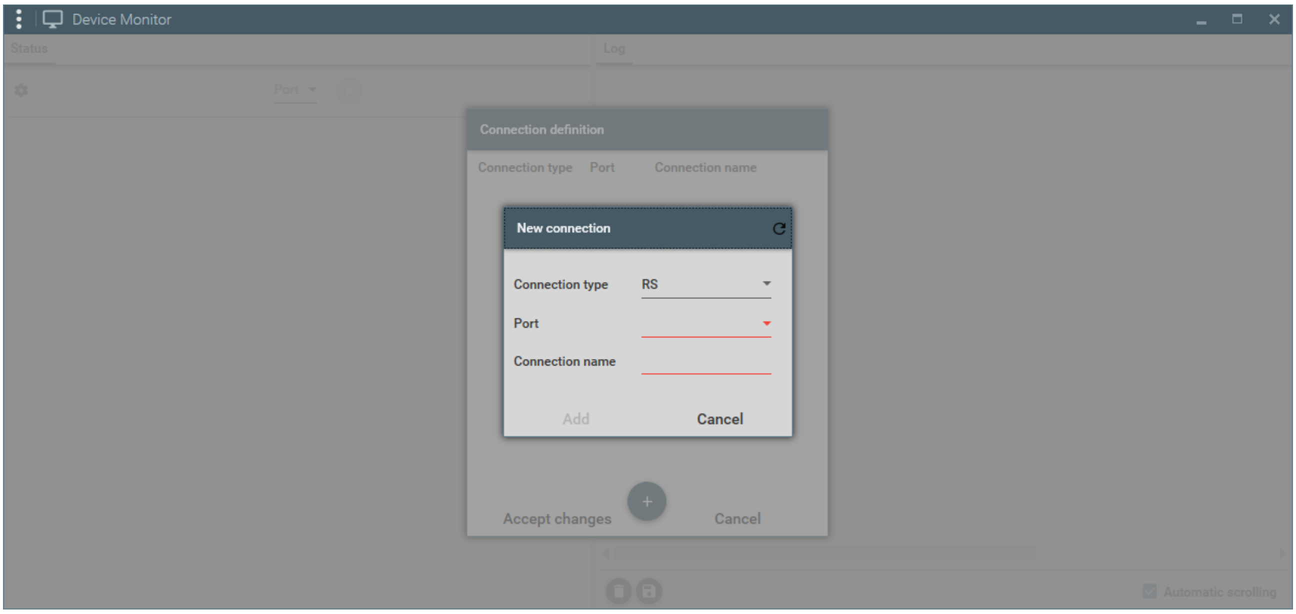
This application is installed with the GPRS transmitters configurator by default.



To use this app, the alarm control panel have to be connected to the PC/laptop via GD-PROG cable, SP-PROG/SP-PROG-BT, or MINI-PROG-BT in DEBUG(MONITOR) mode. Then click ⚙ on the top left corner. A window will appear:

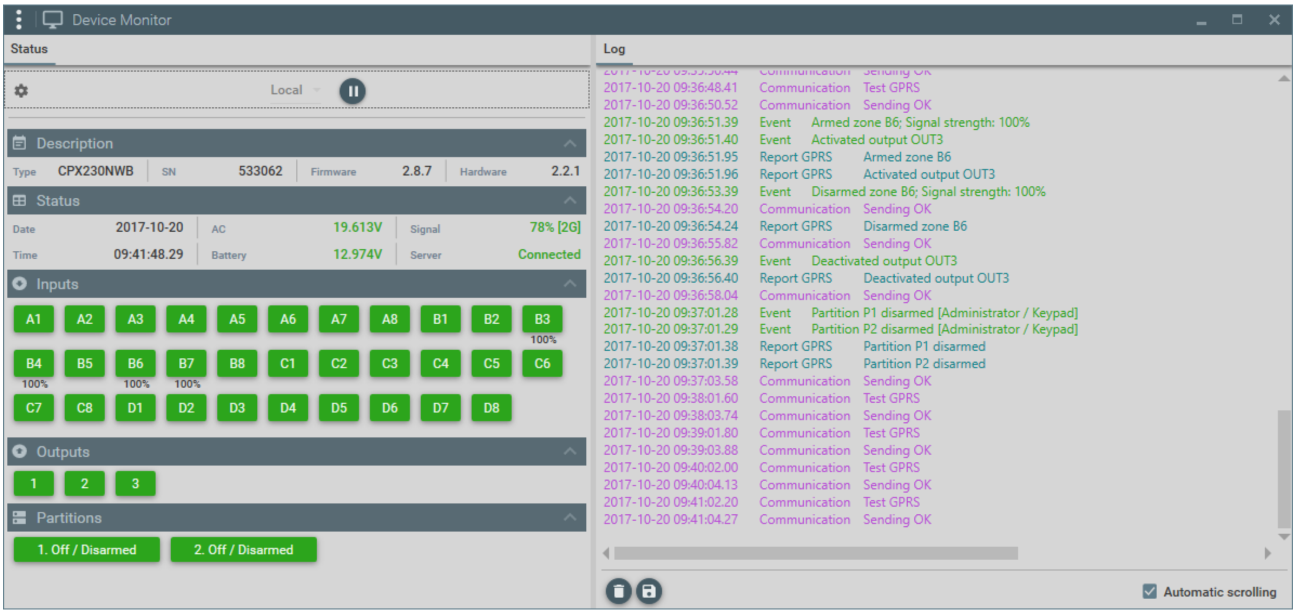


after pressed „+" and type, port and name connection defined a new connection can be add.



Connection type: RS
Port:
Connection name:

A new connection appear in the "Port" field after accept changes. Select them and click “Play” button. On the monitor, there are shown information about device type, serial number, firmware and PCB version, and time set on the CPX device.



Type CPX230NWB | SN 533062 | Firmware 2.8.7 | Hardware 2.2.1

Date 2017-10-20 | AC 19.613V | Signal 78% [2G]

Time 09:41:48.29 | Battery 12.974V | Server Connected

1. Off / Disarmed
2. Off / Disarmed

```
2017-10-20 09:36:48.41   Communication   Test GPRS
2017-10-20 09:36:50.52   Communication   Sending OK
2017-10-20 09:36:51.39   Event   Armed zone B6; Signal strength: 100%
2017-10-20 09:36:51.40   Event   Activated output OUT3
2017-10-20 09:36:51.95   Report GPRS   Armed zone B6
2017-10-20 09:36:51.96   Report GPRS   Activated output OUT3
2017-10-20 09:36:53.39   Event   Disarmed zone B6; Signal strength: 100%
2017-10-20 09:36:54.20   Communication   Sending OK
2017-10-20 09:36:54.24   Report GPRS   Disarmed zone B6
2017-10-20 09:36:55.82   Communication   Sending OK
2017-10-20 09:36:56.39   Event   Deactivated output OUT3
2017-10-20 09:36:56.40   Report GPRS   Deactivated output OUT3
2017-10-20 09:36:58.04   Communication   Sending OK
2017-10-20 09:37:01.28   Event   Partition P1 disarmed [Administrator / Keypad]
2017-10-20 09:37:01.29   Event   Partition P2 disarmed [Administrator / Keypad]
2017-10-20 09:37:01.38   Report GPRS   Partition P1 disarmed
2017-10-20 09:37:01.39   Report GPRS   Partition P2 disarmed
2017-10-20 09:37:03.58   Communication   Sending OK
2017-10-20 09:38:01.60   Communication   Test GPRS
2017-10-20 09:38:03.74   Communication   Sending OK
2017-10-20 09:39:01.80   Communication   Test GPRS
2017-10-20 09:39:03.88   Communication   Sending OK
2017-10-20 09:40:02.00   Communication   Test GPRS
2017-10-20 09:40:04.13   Communication   Sending OK
2017-10-20 09:41:02.20   Communication   Test GPRS
2017-10-20 09:41:04.27   Communication   Sending OK
```

☑ Automatic scrolling

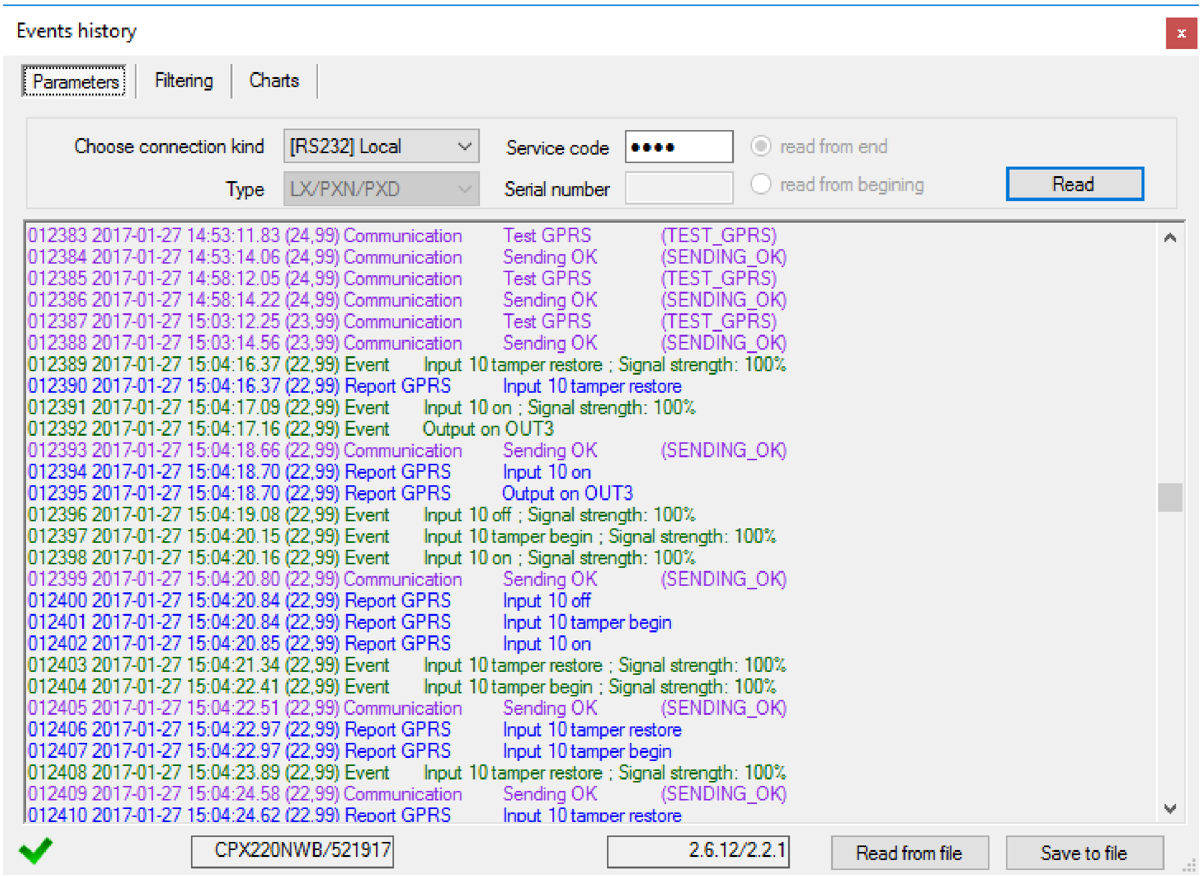
Device Monitor additionally provides the feature of overseeing the following parameters:

- AC voltage,
- GSM signal strenght
- connection with OSM.Server (monitoring station)
- tatus of the wired and wireless lines (inputs) – when you move the cursor on the line, additional information will come up, such as:
  - Input type, for example wired (NO)
  - Serial number
  - Reaction type, e.g. immediate, 24h tampering
  - Signal level
  - status – intact, alarm, tampering or unused (when the detector is not assigned to any partition)

- outputs state
- partitions state (armament)

Changes of all parameters are also displayed in a text form in 'Log' box.

6.12. EVENTS HISTORY



Choose connection kind: [RS232] Local

Type: LX/PXN/PXD

Service code: ••••

Serial number:

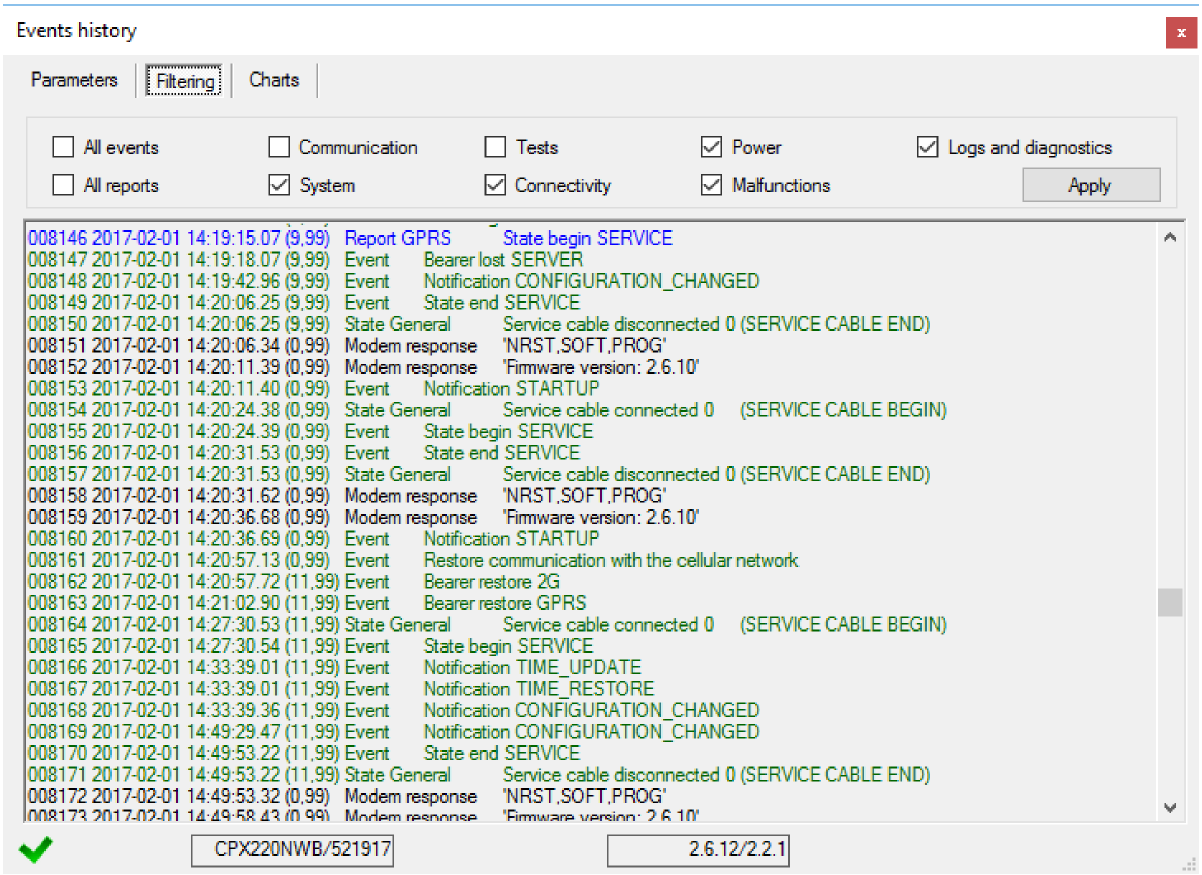
○ read from end

○ read from begining

```
012383 2017-01-27 14:53:11.83 (24,99) Communication      Test GPRS          (TEST_GPRS)
012384 2017-01-27 14:53:14.06 (24,99) Communication      Sending OK         (SENDING_OK)
012385 2017-01-27 14:58:12.05 (24,99) Communication      Test GPRS          (TEST_GPRS)
012386 2017-01-27 14:58:14.22 (24,99) Communication      Sending OK         (SENDING_OK)
012387 2017-01-27 15:03:12.25 (23,99) Communication      Test GPRS          (TEST_GPRS)
012388 2017-01-27 15:03:14.56 (23,99) Communication      Sending OK         (SENDING_OK)
012389 2017-01-27 15:04:16.37 (22,99) Event      Input 10 tamper restore ; Signal strength: 100%
012390 2017-01-27 15:04:16.37 (22,99) Report GPRS        Input 10 tamper restore
012391 2017-01-27 15:04:17.09 (22,99) Event      Input 10 on ; Signal strength: 100%
012392 2017-01-27 15:04:17.16 (22,99) Event      Output on OUT3
012393 2017-01-27 15:04:18.66 (22,99) Communication      Sending OK         (SENDING_OK)
012394 2017-01-27 15:04:18.70 (22,99) Report GPRS        Input 10 on
012395 2017-01-27 15:04:18.70 (22,99) Report GPRS        Output on OUT3
012396 2017-01-27 15:04:19.08 (22,99) Event      Input 10 off ; Signal strength: 100%
012397 2017-01-27 15:04:20.15 (22,99) Event      Input 10 tamper begin ; Signal strength: 100%
012398 2017-01-27 15:04:20.16 (22,99) Event      Input 10 on ; Signal strength: 100%
012399 2017-01-27 15:04:20.80 (22,99) Communication      Sending OK         (SENDING_OK)
012400 2017-01-27 15:04:20.84 (22,99) Report GPRS        Input 10 off
012401 2017-01-27 15:04:20.84 (22,99) Report GPRS        Input 10 tamper begin
012402 2017-01-27 15:04:20.85 (22,99) Report GPRS        Input 10 on
012403 2017-01-27 15:04:21.34 (22,99) Event      Input 10 tamper restore ; Signal strength: 100%
012404 2017-01-27 15:04:22.41 (22,99) Event      Input 10 tamper begin ; Signal strength: 100%
012405 2017-01-27 15:04:22.51 (22,99) Communication      Sending OK         (SENDING_OK)
012406 2017-01-27 15:04:22.97 (22,99) Report GPRS        Input 10 tamper restore
012407 2017-01-27 15:04:22.97 (22,99) Report GPRS        Input 10 tamper begin
012408 2017-01-27 15:04:23.89 (22,99) Event      Input 10 tamper restore ; Signal strength: 100%
012409 2017-01-27 15:04:24.58 (22,99) Communication      Sending OK         (SENDING_OK)
012410 2017-01-27 15:04:24.62 (22.99) Report GPRS        Input 10 tamper restore
```

✓ CPX220NWB/521917 2.6.12/2.2.1

The function enables to read out the events lately recorded in the memory of the equipment. The control panel has an event log memory where about 5 thousand technical events can be recorded. You can review the events history via GPRS and RS232 connection. In the second situation, first you have to connect the equipment to a PC computer via GD-PROG cable. Then, in the "Event History" box select an appropriate RS232 port or GPRS connection, enter access code and click "Read" button. After correct reading you will get the access to "Filtering" and "Graphs" functions which allow you a quick diagnosis of the equipment.



Events history

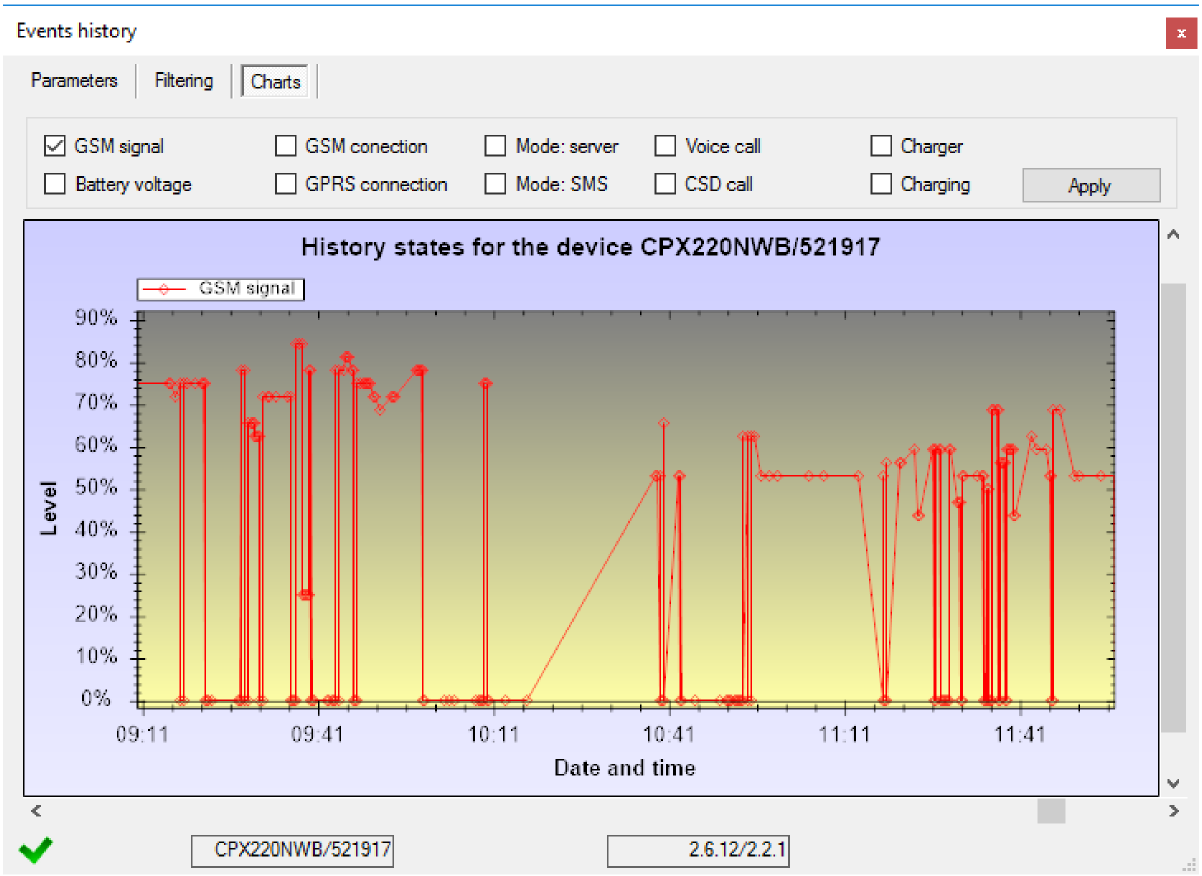
Parameters | Filtering | Charts

□ All events □ Communication □ Tests ☑ Power ☑ Logs and diagnostics

□ All reports ☑ System ☑ Connectivity ☑ Malfunctions

```
008146 2017-02-01 14:19:15.07 (9,99)  Report GPRS       State begin SERVICE
008147 2017-02-01 14:19:18.07 (9,99)  Event        Bearer lost SERVER
008148 2017-02-01 14:19:42.96 (9,99)  Event        Notification CONFIGURATION_CHANGED
008149 2017-02-01 14:20:06.25 (9,99)  Event        State end SERVICE
008150 2017-02-01 14:20:06.25 (9,99)  State General     Service cable disconnected 0 (SERVICE CABLE END)
008151 2017-02-01 14:20:06.34 (0,99)  Modem response    'NRST,SOFT,PROG'
008152 2017-02-01 14:20:11.39 (0,99)  Modem response    'Firmware version: 2.6.10'
008153 2017-02-01 14:20:11.40 (0,99)  Event        Notification STARTUP
008154 2017-02-01 14:20:24.38 (0,99)  State General     Service cable connected 0    (SERVICE CABLE BEGIN)
008155 2017-02-01 14:20:24.39 (0,99)  Event        State begin SERVICE
008156 2017-02-01 14:20:31.53 (0,99)  Event        State end SERVICE
008157 2017-02-01 14:20:31.53 (0,99)  State General     Service cable disconnected 0 (SERVICE CABLE END)
008158 2017-02-01 14:20:31.62 (0,99)  Modem response    'NRST,SOFT,PROG'
008159 2017-02-01 14:20:36.68 (0,99)  Modem response    'Firmware version: 2.6.10'
008160 2017-02-01 14:20:36.69 (0,99)  Event        Notification STARTUP
008161 2017-02-01 14:20:57.13 (0,99)  Event        Restore communication with the cellular network
008162 2017-02-01 14:20:57.72 (11,99) Event        Bearer restore 2G
008163 2017-02-01 14:21:02.90 (11,99) Event        Bearer restore GPRS
008164 2017-02-01 14:27:30.53 (11,99) State General     Service cable connected 0    (SERVICE CABLE BEGIN)
008165 2017-02-01 14:27:30.54 (11,99) Event        State begin SERVICE
008166 2017-02-01 14:33:39.01 (11,99) Event        Notification TIME_UPDATE
008167 2017-02-01 14:33:39.01 (11,99) Event        Notification TIME_RESTORE
008168 2017-02-01 14:33:39.36 (11,99) Event        Notification CONFIGURATION_CHANGED
008169 2017-02-01 14:49:29.47 (11,99) Event        Notification CONFIGURATION_CHANGED
008170 2017-02-01 14:49:53.22 (11,99) Event        State end SERVICE
008171 2017-02-01 14:49:53.22 (11,99) State General     Service cable disconnected 0 (SERVICE CABLE END)
008172 2017-02-01 14:49:53.32 (0,99)  Modem response    'NRST,SOFT,PROG'
008173 2017-02-01 14:49:58.43 (0,99)  Modem response    'Firmware version: 2.6.10'
```

CPX220NWB/521917 2.6.12/2.2.1



Events history

Parameters | Filtering | Charts

☑ GSM signal □ GSM conection □ Mode: server □ Voice call □ Charger

□ Battery voltage □ GPRS connection □ Mode: SMS □ CSD call □ Charging

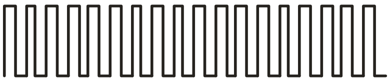
CPX220NWB/521917 2.6.12/2.2.1

7. LED INDICATION

The equipment indicates its current state using 3 LEDs, installed directly on PCB.

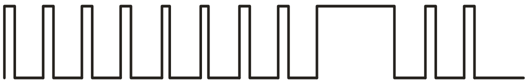
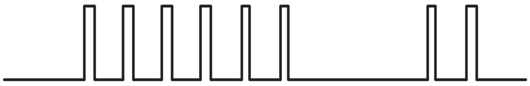
7.1. NETWORK LOG-IN

After SIM card is inserted and power supply connected to the equipment, the GSM network log-in attempt is undertaken.

Description	**LEDs**		
	OK (green)	**ERROR (red)**	**STATUS (yellow)**
GSM network log-in attempt		—	—

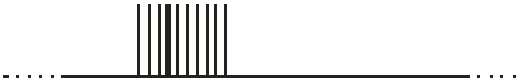
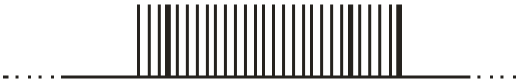
7.2. GSM RANGE

GSM signal strength is indicated by flashing green LED (1-8 blinks). The operation mode of the equipment is indicated by green LED which goes on for 2 seconds after the range is indicated. In case the LED does not go on for 2 seconds after the range is indicated, it means SMS mode of equipment operation. Range indication is interrupted during data transmission, after which the GSM range is displayed.

Description	**LEDs**		
	OK (green)	**ERROR (red)**	**STATUS (yellow)**
GSM range = 8 **GPRS mode**		—	—
GSM range = 6 **SMS mode**		—	—

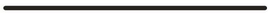
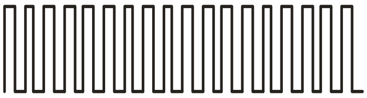
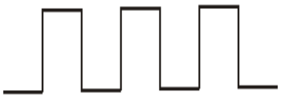
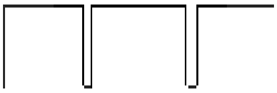
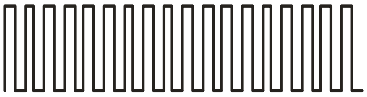
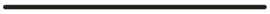
7.3. TRANSMISSION

During data transmission green LED indicates the data sending.

Description	**LEDs**		
	OK (green)	**ERROR (red)**	**STATUS (yellow)**
GPRS transmission		—	—
SMS transmission		—	—

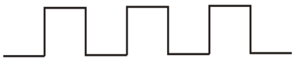
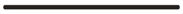
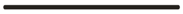
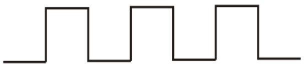
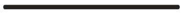
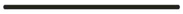
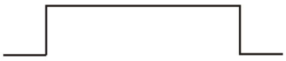
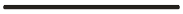
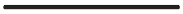
7.4. PROGRAMMING

After the programming mode is detected, LEDs start indicating the programming state.

Description	LEDs		
	OK (green)	ERROR (red)	STATUS (yellow)
Service cable connected			
Programming in CSD mode			

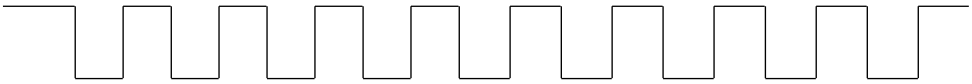
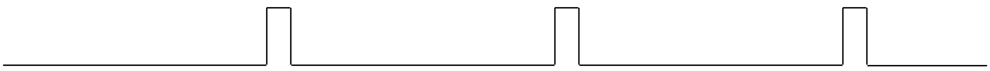
7.5. FIRMWARE UPDATE

During programming the bootloader activity is indicated. In case of error during updating process, bootloader remains in the equipment and repeated equipment programming is possible.

Description	LEDs		
	OK (green)	ERROR (red)	STATUS (yellow)
No software in the equipment	 1/sek		
Software update			
Decryption of firmware received	 10 sek		

7.6. NO SIM CARD OR SIM CARD DAMAGED

In case of any problems with SIM card the equipment indicates it with a red ERROR LED and green OK LED.

LED	Indication
OK (green)	
ERROR (red)	

7.7. SYSTEM ERROR

During the equipment's operation errors can occur. Error is indicated by constant light of red LED and most often it means a communication problem with a modem or SIM card.

8. GRADE 2 SETTINGS

8.1. GRADE 2 SETTINGS

To meet the requirements of EN 50131 standard for Grade 2, do the following:

- Set the entry time to be no longer than 45 seconds.
- The alarm outputs should be configured as follows: operation time of acoustic sirens should be not shorter than 90 second and no longer than 15 minutes.
- Set the zones sensitivity less than 400 ms.
- Set interlocking input zones to value from 3 to 10
- Set the power loss time to be no longer than 60 minutes (see item 4.3.2. and see item 6.6.1.3.).
- Use user codes with a length of at least 5 characters.
- As an emergency power source use 12V lead-acid sealed battery connected to the control panel. The battery capacity should be sufficient to operate the system without a power supply for 12 hours.
- In the GPRS Transmitters Configurator (see item 6.4.) or in the installer menu (see item 4.3.4.) set the System Options:

  - enable option "Show failures history with SYSTEM diode"
  - disable option "Ignore ATS failure"
  - enable option "Confirm arming in case of a failure (by pressing #)"
  - enable option "Access to alarm and fault memory requires authorization"
  - enable option "Alarms and inputs interlocking states are not displayed"
  - enable option "Temporary keyboard lock after three access failures"
- In the GPRS Transmitters Configurator, in option "Monitoring" (see item 6.6.1.) enable monitoring of the following events (select the columns: GPRS On, GPRS Off, SMS On, SMS Off):

  - Input A1 – D8
  - Input A1 – D8 tamper
  - Output 1 – 3 tamper
  - Power
  - Battery
  - Jamming
  - Keypad output failure
  - Output AUX1 failure
  - Output AUX2 failure
  - Keypad communication lost
  - Keypad tamper
  - Keypad power failure
  - Clock loss

8.2. 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.

9. EXTRAS

9.1. REMOTE COMMANDS AND CONFIGURABLE PARAMETERS

The control panel receives SMS in a specially designed form. If SMS that was received by the equipment is not correct, it gets automatically deleted and the equipment does not initiate any activity. The following format of the message is accepted, and it allows sending a few commands in one SMS message, while each of them must be separated with a SPACE:

ACCESS CODE▨COMMAND/PARAM▨COMMAND/PARAM▨………

where:

ACCESS CODE - access code of the equipment, may be either a service code, user code or administrator code. In case the command requires authorization by administrator code (e.g. CPGETUSERS), this code should be passed to the command only once, either as access code or as a parameter passed along with the command. In other words, whenever access code is not an administrator code and the command has to be authorized by the administrator code, it has to be passed as a command’s parameter.

▨ - space

COMMAND/PARAM - instruction (see the tables below)

The newly configured parameter will be taken into account when the device will need to use it, there is no need to restart the unit. However, there are parameters, changes to which will be detected only in special circumstances, for example – the server address. If it is changed when the device is online, a restart is needed. When CPX230NWB boots up, it will connect to the newly configured address.

In order to delete a parameter, the message has to contain the name of the parameter followed by the equation mark (=). For example, to delete the number to which text messages are sent, one has to send a following text: “XXXX SMS=”, where XXXX is the access code.

ATS – (Alarm Transmission System) – is a special type of user, meaning the monitoring station. The user is authorized by the main access code to the device (the code to read the configuration via a cable). ATS is also authorized by encryption keys. If the command is sent through an encrypted transmission, code is not required.

User – regular user with the ability to arm and disarm the partition to which they have rights, and other rights described in the user manual. Several regular users may be in the system.

Administrator – a special user who has privileges to add and delete other users.

9.1.1. Configuration parameters

9.1.1.1. APN

Format:	APN=apn_name
Limitations:	Data length to 31 characters, can be changed by ATS only
Description	Configures the APN through which data will be sent by GPRS

9.1.1.2. UN

Format:	UN=username
Limitations:	Data length to 31 characters, can be changed by ATS only
Description	Sets the user name for APN

9.1.1.3. PW

Format:	PW=password
Limitations:	Data length to 31 characters, can be changed by ATS only
Description	Sets the password for APN

9.1.1.4. SERVER

Format:	SERVER=server_address
Limitations:	Data length to 31 characters, can be changed by ATS only
Description	Sets the OSM server address with which the device exchanges data. Server_address can be given in the domain format, eg.device.mycompany.com domain or IP address, such as 213.216.102.98

9.1.1.5. PORT

Format:	PORT=port
Limitations:	A number between 1-65535, can be changed by ATS only
Description	Sets the OSM server address with which the device exchanges data

9.1.1.6. DNS1

Format:	DNS1=dns1
Limitations:	Valid IPv4 address in numerical form (up to 15 characters), possible to change by ATS only

Description	It defines the address of primary DNS (Domain Name System). If server address was entered as a domain name at least one DNS address must be entered.

9.1.1.7. DNS2

Format:	DNS1=dns2
Limitations:	Valid IPv4 address in numerical form (up to 15 characters), possible to change by ATS only
Description	It defines the address of backup DNS (Domain Name System). If server address was entered as a domain name at least one DNS address must be entered.

9.1.1.8. SMS

Format:	SMS=phone_number
Limitations:	Data length to 15 characters, can be changed by ATS only
Description	Sets the phone number for sending SMS with the events in the absence of GPRS communication. If the number is not configured sending SMS messages will not be available. Phone_number may contain a prefix of the country.

9.1.1.9. SMSPERIOD

Format:	SMSPERIOD=time_in_minutes
Limitations:	String representig a number, can be changed by ATS only
Description	Sets the SMS test period, the time is given in minutes.

9.1.1.10. RLIMIT

Format:	RLIMIT
Limitations:	can be executed by ATS only.
Description:	Removes automatic temporary blockade from all inputs.
Format:	RLIMIT=input_mask
Limitations:	can be executed by ATS only.
Description:	Releases the selected temporary automatic locks. The parameter is a decimal number made from a 9-bit word: A9 … A2, A1, where A2 input 1 and A3 input 2. EXAMPLE: RLIMIT=6 releases locks from the inputs IN1, IN2 RLIMIT=2 releases locks from the input IN1

9.1.1.11. DT

Format:	DT=YY/MM/DD,hh:mm
Limitations:	Data length of 14 characters, can be changed only by ATS or Administrator
Description	Sets date and hour

9.1.1.12. SETMASK

Format:	SETMASK=id_typu,indeks,maska
Ograniczenia:	type_id must be 0, 1 or 2, command can be issued by ATS only
Opis	This is a low-level command which operates directly on the device configuration memory. Sets mask bits in parameter *type_id,index*. This command does not generate any events in addition to the information that the configuration has been changed. FOR: SETMASK=0,65,0x01 Enable function **Premises lock**. This function turns off the ability to arm the control panel. When this function is turned on, the user will not be able to arm the site by any way (i.e. SMS/GPRS, remote, arming input, schedules, keypad, wireless keypad). Disarming the system is possible, however. Arming attempts will be rejected by the control panel. SETMASK=2,19,0x100 Enable function **Defaults restoral lock**. This function allows the user to turn off the ability to restore the factory-default installer's code. However, when restoring default settings using the Configuration, when the "Restore device's default settings" option is selected, a window with a request to enter the installer's code or service code (ATS) will appear. **NOTE: If you lose the newly set codes, you will need to send blocked devices to EBS technical service.** SETMASK=2,19,0x400 Turning off the **Allow quick arming without user authorisation** function. After turning this function off, the system can only be armed if an access code is entered.

9.1.1.13. CLEARMASK

Format:	CLERMASK=id_typu,indeks,maska
Ograniczenia:	type_id must be 0, 1 or 2, command can be issued by ATS only

Opis	This is a low-level command which operates directly on the device configuration memory. Sets mask bits in parameter *type_id,index*. This command does not generate any events in addition to the information that the configuration has been changed. FOR: CLEARMASK=0,65,0x01 Disable function **Premises lock**. When this function is turned off, the user can arm and disarm the control panel again. CLEARMASK=2,19,0x100 Disable function **Defaults restoral lock**. When this function is turned off, it will be possible to restore the default installation engineer code using the "PROG" button, located on the central, and from the Configurator. CLEARMASK=2,19,0 x 400 Turning off the **Allow quick arming without user authorisation** function. After turning this function off, the system can only be armed if an access code is entered.

9.1.2. General commands

They provide the execution of various tasks remotely, or the querying of certain parameters. If the command is sent via SMS , the response is sent back to the telephone number from which the command came. Do not send several commands in one SMS message or one frame, since only one command will be executed , and it will not necessarily be the first command in the list.

9.1.2.1. DISC

Format:	DISC
Limitations:	Can be executed by ATS only
Description	Disconnects TCP connection with OSM server

9.1.2.2. KILL

Format:	KILL
Limitations:	Can be executed by ATS only
Description	Restarts the GSM modem in the device. This results in breaking a GPRS session and deregistration from the GSM network and re-registration to GSM and GPRS network when you restart the modem.

9.1.2.3. RESET

Format:	RESET
Limitations:	Can be executed by ATS only
Description	Restarts the whole device. This results in breaking a GPRS session and deregistration from the GSM network and re-registering to GSM and GPRS network when you restart the device and modem.

9.1.2.4. DESC

Format:	DESC
Limitations:	Can be executed by ATS only
Description	Returns a string with a description of the device containing firmware version and serial number

9.1.2.5. GETCFG

Format:	GETCFG
Limitations:	Returns max. 160 characters, can be executed by ATS only
Description	Gets the current, basic configuration of the device. The parameters are returned in the following order: SERVER:PORT, _APN_UN_PW,_DNS0 Where: _ Space character (asci 0x20) SERVER – OSM server address PORT – OSM server port APN – APN name by means of which the GPRS session is compiled UN – APN user name PW –APN password DNS0 –DNS server address

9.1.2.6. OUT

Format:	OUT=o,s,[time]
Limitations:	Can be executed only by ATS or administrator

Description	Set the state ‘s’ on the output ‘o’. o – output selection (1–3) s – final output state (1 – on, 0 – off) time – in case when output is switching on, duration can be described in seconds. 0 means bistable state. If this parameter is not typed then output will switch on for duration set during configuration. Output can be switched off by remote command in any time regardless from output set type and work mode. Examples: OUT=2,1 – switch on output 2 for time set during configuration OUT=2,0 – switch off output 2 OUT=1,1,0 – switch on output 1 in bistable state OUT=3,1,10 – switch on output 3 for 10 seconds

9.1.2.7. FLUSH

Format:	FLUSH=x
Limitations:	x is equal to 0 or 1, possible to execution only by ATS
Description	For x = 0 it clears the queue of outstanding events to be sent to the OSM server. This results in the loss of outstanding events – the device generates then an event indicating the fact. For x = 1 it clears the event log of the device.

9.1.2.8. SENDSMS

Format:	SENDSMS=phone_no,text_without_spaces
	SENDSMS=”phone_no,text_with_spaces”

Limitations:	This command does not work when sent via SMS; possible to execution only by ATS
Description	Allows you to send the SMS to the specified phone number (phone_no) with the specified content. This command is a tool with which you can get information about the phone number of the SIM card installed in the device when connected to the OSM server using GPRS.

9.1.2.9. GETSTATUS

Format:	GETSTATUS
Limitations:	Can be executed by ATS, administrator or user.
Description	Gets the current status of the device. The returned data are in the following format: zones,partitions,outputs,battery_voltage,voltage_AC,0x0,0x0, blocked_zones where: *zones* – means the current zone status. It is a bit-vector, where bit 1

	(counting from 0) means the zone 1 , bit 2 the zone 2, etc. If the zone is impaired, the bit is set. *Partitions* – means the current partition status. It is a bit-vector, where bit 0 means the partition 1 and bit 1 the partition 2 (otherwise than for the zone and outputs where bit 1 means the zone /output 1). If the partition is armed or counts down the time to output the corresponding bit is set. *Outputs* – means the current status of outputs. It is a bit-vector, where bit 1 (counting from 0) means the output 1, bit 2 the output 2 and bit 3 the output 3. If the output is enabled the bit is set. *Battery_voltage* – battery voltage in mV (12000 = 12V). If the battery is not connected, the readings may be incorrect, and be around 9V (9000) *voltage_AC* – AC voltage at the AC terminals of CPX230NWB (downstream the transformer) in mV (18000 = 18V) *blocked_zones* – means the current status of the zone blockade. It is a bit-vector, where bit 1 (counting from 0) means the zone A1, bit 2 the zone A2 itd. If the zone is blocked, the bit is set.

9.1.2.10. GETPARAM

Format:	GETPARAM=parameter
Limitations:	Parameter is equal to APN or UN or PW or Server or PORT or SMS or SMSPERIOD or as *id_typu , index*, possible to execution only by ATS
Description	Allows you to retrieve the value of a proper configuration parameter. The configuration parameters are described in the section on parameters. It is a twin command with SETPARAM.

9.1.2.11. CPGETALARMSHOWTIME

Format:	CPGETALARMSHOWTIME
Limitations:	Can be changed by ATS, the admin and the user
Description	The command is used to retrieve the time settings after which the signalling of historical alarms is switched off. The time is counted down from the moment the partition is disarmed. The command returns: CPGETALARMSHOWTIME: delay – if the function "After disarming disable the historical alarm signalling" is active, *delay* is the time expressed in seconds CPGETALARMSHOWTIME: OFF – if the function "After disarming disable the historical alarm signalling" is not active

9.1.2.12. CPSETALARMSHOWTIME

Format:	CPSETALARMSHOWTIME=delay
Limitations:	It can be carried out by the ATS, the admin or the installer if they have been authorised to perform maintenance services
Description	The command is used to set the time settings after which the signalling of historical alarms is switched off. The time is counted down from the moment the partition is disarmed. This functionality can also be disabled. The *delay* parameter is the delay value in seconds (0–9999999) or the text message "OFF" in order to disable the functionality (the signalling is not turned off). If the value is zero, the alarm signalling turns off when the system is disarmed. The command returns: CPSETALARMSHOWTIME:EOK – correct execution CPSETALARMSHOWTIME:EEFORMAT – incorrect command format or *delay* range Example: CPSETALARMSHOWTIME=20 – 20-second delay time CPSETALARMSHOWTIME= OFF – if the function "After disarming disable the historical alarm signalling" is not active

9.1.2.13. CPGETACN

Format:	CPGETACN
Available since:	2.8.8
Limitations:	It can be carried out by the ATS or the installer if they have been authorised to perform maintenance services
Description	The command is used to retrieve the settings of account numbers for Contact ID. The command returns: CPGETACN:EOK,system[,acn_id:acn_value]… Where: *system* – has the ALL value (for system events going to all accounts) or ACN0 (system events sent only to the ACN0 system account) *acn_id* – it is an ACN account identifier, 0 for ACN0, 1 for ACN1, 2 for ACN2. *acn_value* – account number expressed in hexadecimal format There can be 3 pairs (acn_id: acn_value) – one for each account. Examples of returned values: CPGETACN:EOK:ALL,0:0x1234,1:0x1235,2:0x1236

9.1.2.14. CPSETACN

Format:	CPSETACN=system[,acn_id:acn_value]…
Available since:	2.8.8
Limitations:	It can be carried out by the ATS or the installer if they have been authorised to perform maintenance services
Description	The command is used to change the settings of account numbers for Contact ID. It sets or deletes all ACNs. *system* – has the ALL value (for system events going to all accounts) or ACN0 (system events sent only to the ACN0 system account) *acn_id* – it is an ACN account identifier, 0 for ACN0, 1 for ACN1, 2 for ACN2 *acn_value* – a two-byte account number (preferably in hexadecimal format: 0xFFFF) There can be 3 pairs (acn_id: acn_value) – one for each account. **NOTE:** • If only ACN0 has been specified, the ACN1 and ACN2 numbers are deleted. • The values of account numbers can be repeated, for example the ACN2 can be the same as the ACN1 and the ACN0. • It is recommended to enter all three ACNs. Otherwise, they can adopt the values of other account numbers that were provided in the parameters. • The control panel accepts the following three situations, where one of them is accepted on the basis of the command arguments: o No account numbers o Only main account (ACN0) o All account numbers (ACN0, ACN1, ACN2) The command returns: CPSETACN:EOK – correct execution CPSETACN: EFORMAT – incorrect command format CPSETACN: ERROR-VALUE – invalid acn_value range CPSETACN: EID – incorrect range of acn_id Example: CPSETACN=ALL,0:0x1234,1:0x1235,2:0x1236 CPSETACN=ACN0,0:1237

9.1.3. Commands for managing the users

9.1.3.1. CPGETUSERS

Format:	CPGETUSERS[= adminPassword]
Limitations:	This command only works when sent through an encrypted way, you must know the administrator password (the user id = 0). The command needs the option "Allow remote user management" to be set active in the Configurator. Can be executed only by ATS or administrator. If the command is executed by the ATS, give *adminPassword*.
Description	Gets a list of users defined in the device. *adminPassword* is the system administrator password. The command returns: CPGETUSERS:id:name:partitions,… Where *id* is the user number, *name* is the text user name (which may be empty), *partitions* is the bit-vector specifying the partitions to which the user is authorized – bit 0 corresponds to the partition 1 , bit 1 to the partition 2. The user with id = 0 is the administrator CPGETUSERS:EPERMISIONS If the administrator password specified is incorrect CPGETUSERS:ENOT_ALLOWED If the command is sent via open SMS or the configuration does not allow remote management of users CPGETUSERS:EFORMAT If the format of the sent command is incorrect

9.1.3.2. CPGETUSERID

Format:	CPGETUSERID=password
Limitations:	This command only works when sent through an encrypted way and the option "Allow remote user management" is set to active in the Configurator. Possible to execution only by ATS.

Description	Verifies the user code specified as an argument of the command – checks whether a user with the specified code exists. *Password* is the password of the user, *id* is the user number, *partitions* are the partitions to which the user is authorized – bit 0 corresponds to the partition 1 , bit 1 to the patition 2. The command returns: CPGETUSERID:EOK,id,partitions If the user with the specified code exists CPGETUSERID:EPERMISIONS If the specified password is incorrect CPGETUSERID:ENOT_ALLOWED If the command is sent via open SMS or the configuration does not allow remote management of users CPGETUSERID:EFORMAT If the format of the sent command is incorrect

9.1.3.3. CPSETUSERPARTITIONS

Format:	CPSETUSERPARTITIONS=id,partitions[,adminPassword]
Limitations:	This command only works when sent through an encrypted way, you must know the administrator password (the user id = 0), id ranging from 1 to 31 inclusive. The command needs the option "Allow remote user management" to be set active in the Configurator. Can be executed only by ATS or administrator. If the command is executed by ATS, specify a*dminPassword*.
Description	Sets the user authorization to the partition. Id is the number of the user whose authorizations are changed, the *partitions* is the bit-vector with the partitions to which the user should have the authorization – bit 0 corresponds to the partition 1, bit 1 to the partition 2, *adminPassword* is the system administrator password. The command returns: CPSETUSERPARTITIONS:EOK,id,partitions If the change of the partition assignment was successful CPSETUSERPARTITIONS:ENOT_EXISTS,id,partitions If the specified user does not exist CPSETUSERPARTITIONS:EPERMISIONS,id,partitions If the administrator password specified is incorrect CPSETUSERPARTITIONS:ENOT_ALLOWED If the command is sent via open SMS or the configuration does not allow remote management of users CPSETUSERPARTITIONS:EFORMAT If the format of the sent command is incorrect

9.1.3.4. CPSETUSERPASSWORD

Format:	CPSETUSERPASSWORD=id,password[,adminPassword]
Limitations:	This command only works when sent through an encrypted way, you must know the administrator password (the user id = 0), id ranging from 1 to 31 inclusive. The command needs the option "Allow remote user management" to be set active in the Configurator. Can be executed only by ATS or administrator. If the command is executed by ATS, specify *asminPassword*
Description	Changes the user's password. *Id* is the user identifier whose password is changed, the password is his new password and the *adminPassword* is the system administrator password. The command returns: CPSETUSERPASSWORD:EOK,id It the command is completed 128dministrato CPSETUSERPASSWORD:ENOT_EXISTS,id If the specified user does not exist CPSETUSERPASSWORD:EPERMISIONS,id If the administrator password specified is incorrect CPSETUSERPASSWORD:ELENGTH,id If the new password is too short or too long or does not consist of digits CPSETUSERPASSWORD:ENOT_ALLOWED If the command is sent via open SMS or the configuration does not allow remote management of users CPSETUSERPASSWORD:EFORMAT If the format of the sent command is incorrect

9.1.3.5. CPADDUSER

Format:	CPADDUSER=id,partitions,password[,category][,adminPassword]
Limitations:	This command only works when sent through an encrypted way, you must know the administrator password (the user id = 0), id ranging from 1 to 31 inclusive. The command needs the option "Allow remote user management" to be set to active in the Configurator. Can be executed only by ATS or administrator. If the command is executed by ATS, specify *adminPassword*

Description	Adds a new user. *Id* is the user number, *partitions* are the partitions to which the user will have the authorization – bit 0 corresponds to the partition 1, bit 1 to the partition 2 , *password* is the password of newly created user, *category* – if set to *NODISARM* value, the user will not be able to disarm partitions (available since Firmware above ver. 2.8.8), *adminPassword* is the the system administrator password. The command returns: CPADDUSER:EOK,id,partitions When a user is added CPADDUSER:EALREADY_EXISTS,id,partitions If the specified user already exists CPADDUSER:EID,id,partitions If the specified user ID is incorrect CPADDUSER:EPERMISIONS,id,partitions If you can not create a user because the password is incorrect (administrator or user) CPADDUSER:ELENGTH,id If the new password is too short or too long or does not consist of digits CPADDUSER:ENOT_ALLOWED If the command is sent via open SMS or the configuration does not allow remote management of users CPADDUSER:EFORMAT If the format of the sent command is incorrect

9.1.3.6. CPDELUSER

Format:	CPDELUSER=id[,adminPassword]
Limitations:	This command only works when sent through an encrypted way, you must know the administrator password (the user id = 0), id ranging from 1 to 31 inclusive. The command needs the option “Allow remote user management” to be set active in the Configurator. Can be executed only by ATS or administrator. If the command is executed by ATS, specify *adminPassword*

Description	Delete the user. *Id* is the user number, a*dminPassword* is the system administrator password. The command returns: CPDELUSER:EOK,id If the user is deleted CPDELUSER:ENOT_EXISTS,id If the specified user does not exist or after attempt to delete administrator or installer CPDELUSER:EPERMISIONS,id If you can not delete a user because the administrator password is incorrect CPDELUSER:ENOT_ALLOWED If the command is sent via open SMS or the configuration does not allow remote management of users CPDELUSER:EFORMAT If the format of the sent command is incorrect

9.1.3.7. CPSETADMINPASSWORD

Format:	CPSETADMINPASSWORD=newPassword
Limitations:	This command only works when sent through an encrypted way, you do not need to know the administrator password (the user id = 0). The command needs the option "Allow remote user management" to be set active in the Configurator. Can be executed only by ATS or administrator.
Description	Changes the main user password – the system administrator. The command is designed to give the ability to remotely restore the password (by monitoring station employees) if it is forgotten. *NewPassword* is the new password of the main user. The command returns: CPSETADMINPASSWORD:EOK CPSETADMINPASSWORD:ENOT_ALLOWED If the command is sent via open SMS or the configuration does not allow remote management of users CPSETADMINPASSWORD:ELENGTH If the new password is too short or too long or does not consist of digits CPSETADMINPASSWORD: EPERMISIONS If the password can not be changed because it is already used by another user. If you type the current administrator password, the command returns EOK.

9.1.3.8. CPGETUSERRIGHTS

Format:	CPGETUSERRIGHTS=id[,adminPassword]
Limitations:	This command is available since Firmware above ver. 2.8.8. Only works when sent through an encrypted way, you must know the administrator password (the user id = 0), id starts from 1 for the first regular user. The command needs the option ”Allow remote user management” to be set active in the Configurator.
Description	Get user access rights. *Id* is the user number. The command returns: CPGETUSERRIGHTS:EOK,id,category[,…] User exists. Category can be: *USER* for regular users, *NODISARM* for users which cannot disarm partitions CPGETUSERRIGHTS:ENOT_EXISTS,id If the specified user does not exist CPGETUSERRIGHTS:EPERMISIONS,id If administrator password is incorrect CPGETUSERRIGHTS:ENOT_ALLOWED If the command is sent via open SMS or the configuration does not allow remote management of users CPGETUSERRIGHTS:EFORMAT If the format of the sent command is incorrect

9.1.4. Commands for managing the partitions, zones and outputs

9.1.4.1. CPGETSTATUS

Format:	CPGETSTATUS[=password]
Limitations:	You must know the administrator or user password. Can be executed by ATS, administrator or user. If the command comes from ATS and was not authorized with a code, enter the *password*.
Description	password is the system administrator or user password. The command returns: CPGETSTATUS:Ready,CurrentPartitionAlarms,alarmHistory, otherAlarmHistory,zoneTampers,keypadTampers,zones,zonesLock, partitions,outputs,batteryVoltage,powerSupplyVoltage,silentAlarms, zonesComFailures,zonesPowerFailures,partitionsStayAway,partitionsNight Where: *Ready* takes the value 1 if the system is ready for arming , 0 if it is not ready. *CurrentPartitionAlarms* is a bit-vector determining whether the current partitions are in alarm condition. Bit 0 corresponds to the first partition, bit 1 corresponds to the second partition. *alarmHistory* a bit-vector indicating the alarm memory from the last arming. Bit 1 (counting from 0), corresponding to the zone A1,… bit 32 corresponds to the zone D8. *otherAlarmHistory* a bit-vector indicating the additional alarm memory from the last arming. Bit 1 (counting from 0), corresponding to the tamper keypad 1, bit 2 corresponds to the tamper keypad 2, bit 3 corresponds to the tamper keypad 3, bit 7 corresponds to the alarm from remote controls. *zoneTampers* is a bit-vector indicating the zone tampering. Bit 1 (counting from 0) means the zone A1. *keypadTampers* is the alarm from the keypads tampering. Bit 0 means the keypad 1. *Zones* – means the current status of the zones. It is a bit-vector, where the bit 1 (counting from 0) means the zone A1, bit 2 means the zone A2, etc. If the zone is impaired, the bit is set. *zonesLock* – means the current status of the zone blockade. It is a bit-vector, where bit 1 (counting from 0) means the zone A1, bit 2 means the zone A2, etc. If the zone is blocked, the bit is set. *Partitions* – means the current status of the partitions. It is a bit-vector, where bit 0 means the partition 1, the bit 1 the partition 2 (otherwise than for the zones and outputs where bit 1 means the zone/output 1). If the partition is armed or counts down, the time to output the corresponding bit is set. *Outputs* – means the current status of outputs. It is a bit-vector, where bit 1 (counting from 0) means the output 1, bit 2 means the output 2 and bit 3 means the output 3. If the output is enabled, the bit is set. *batteryVoltage* – battery voltage in mV (12000 = 12V). If the battery is

	not connected, the readings may be incorrect, and be around 9V (9000) *powerSupplyVoltage* – AC voltage at AC terminals of CPX230NWB (downstream the transformer) in mV (18000 = 18V). *silentAlarms* is a bit-vector indicating the quiet alarm memory since the last arming (arming cancels the alarm memory). Bit 1 (counting from 0), corresponds to the zone 1, … bit 7 corresponds to the zone A7. *zonesComFailures* – is a bit-vector indicating the communication failures between wireless detectors and control panel. Bit 1 (counting from 0), corresponds to the zone A1, … bit 32 corresponds to the zone D8. *zonesPowerFailures* – is a bit-vector indicating detectors power failures in wireless detectors (means low battery in wireless detectors). Bit 1 (counting from 0), corresponds to the zone A1, … bit 32 corresponds to the zone D8. *partitionsStay* – is a bit vector where 1 means perimeter mode and 0 means one of the other possible arming modes. Bit 0 corresponds to partition 1. Bit 1 corresponds to partition 2 *partitionsNight* – is a bit vector where 1 means partition armed in sleep mode and 0 means partition in one of the other possible arming modes. Bit 0 corresponds to partition 1. Bit 1 corresponds to partition 2. CPGETSTATUS:EPERMISIONS If the specified password is incorrect CPGETSTATUS:ENOT_ALLOWED If the command was sent via open SMS CPDELUSER:EFORMAT If the format of the sent command is incorrect

9.1.4.2. CPGETFAILURES

Format:	CPGETFAILURES[= password]
Limitations:	You must know the administrator or user password. Can be executed by ATS, administrator or user. If the command comes from ATS and was not authorized with a code, enter the *password*.
Description	*password* is the system administrator or user password The command returns: CPGETFAILURES:outFailures,powerOutFailures,powerInFailures,keypadCommFailures,keypadPowerFailures,otherFailures Where: *outFailures* is a bit-vector informing about the failures of outputs. Bit 1 (counting from 0) means the output 1. *powerOutFailures* is a bit-vector informing about the failures of power supply outputs. Bit 0 means the output KPOUT, bit 1 means the output AUX1, bit 2 means the output AUX2. *powerInFailures* is a bit-vector informing about the failures of power

	supply. Bit 0 means the supply network failures, bit 1 means the battery failure. *keypadCommFailures* is a bit-vector informing about the failures of communication with keypads. Bit 0 means the keypad 1. *keypadPowerFailures* is a bit-vector informing about the power supply failures reported by keypads. Bit 0 means the keypad 1. *otherFailures* is a bit-vector determining the current system failures. The meaning of bits is as follows: bit 0 – loss of clock bit 1 – configuration memory failure CPGETFAILURES:EPERMISIONS If the specified password is incorrect CPGETFAILURES:ENOT_ALLOWED If the command was sent via open SMS CPDELUSER:EFORMAT If the format of the sent command is incorrect

9.1.4.3. CPSETPARTITIONS

Format:	CPSETPARTITIONS=[STAY/SLEEP]partitions[,delay][,password]
Limitations:	You must know the administrator or user password. Can be executed by ATS, administrator or user. If the command comes from ATS and was not authorized with a code, enter the *password*.
Description	Arms the specified partitions. Partitions a bit-vector indicating which partition one wants to arm. Bit 0 is the partition 1 , bit 1 is the partition 2. Bit setting means that one wants to arm the partition. Sending a command with the *partitions* argument equal to zero, has no sense, since it does not change anything – if the partitions is 0, the user's password is not checked and the status returned by the command is equal to EOK. Delay can take on value: *NOW* – arms immediately the defined partition without counting down the time for exit, *DEFAULT* – arms the partition with default time for exit. Password is the code of the user who performs arming. The specified partitions will be armed from the user's id to which the code belongs. *STAY* and *SLEEP* statement before the partitions vector is optional. *STAY* means that selected partitions will be armed in stay mode, while *SLEEP* - in sleep mode. It is possible to change arm mode but it is not possible to arm in stay mode the partition that has no perimeter zones assigned. The command returns: CPSETPARTITIONS=[STAY,SLEEP]partitionList: EOK If the command is sent with NOW and executed CPSETPARTITIONS=[STAY,SLEEP]partitionList: EOK,x,y If the command is sent with DEFAULT and executed; x,y – time for exit (in seconds)for the partition 1 (x) and 2 (y) *partitionList* is the list of partitions which has been armed (note that *partitionList* may be different from partitions, if the user does not have permissions to desired partitions). If you send a command to arm both partitions (CPSETPARTITIONS=3), regardless of whether or not a partition (or partitions) is armed, you will receive a message about arming both partitions (CPSETPARTITIONS=3:EOK - only if a command sent by a user who has permissions to both partitions). CPSETPARTITIONS=[STAY,]partitions:ENOT_ALLOWED If at least one of the partitions does not have any perimeter zones assigned to it or if an attempt to arm during the alarm. CPSETPARTITIONS=[STAY/SLEEP]partitions,password:EFORMAT If the data format is incorrect (partitions,password are the command arguments) CPSETPARTITIONS=[STAY/SLEEP]partitions:EPERMISIONS If the user with the specified password does not exist

9.1.4.4. CPUNSETPARTITIONS

Format:	CPUNSETPARTITIONS=partitions[,password]
Limitations:	You must know the administrator or user password. Can be executed by ATS, administrator or user. If the command comes from ATS and was not authorized with a code, enter the *password*.
Description	Disarms the specified partitions. *Partitions* is a bit-vector specifying which partitions you want to disarm. Bit 0 is the partition 1, bit 1 is the partition 2. Setting the bit means that one wants to disarm the partition. Sending a command with the *partitions* argument equal to zero, has no sense, since it does not change anything – if the *partitions* is 0, the user's password is not checked and the status returned by the command is equal to EOK. *Password* is the code of the user, who performs disarming. The specified partitions will be armed from the user's id to whom the code belongs. The command returns: CPUNSETPARTITIONS=partitionList:EOK If the command is executed. *partitionList* is the list of partitions which has been disarmed (note that *partitionList* may be different from *partitions*, if the user does not have permissions to desired partitions). If you send a command to disarm both partitions (CPSETPARTITIONS=3), regardless of whether or not a partition (or partitions) is disarmed, you will receive a message about disarming both partitions (CPUNSETPARTITIONS=3:EOK - only if a command sent by a user who has permissions to both partitions). CPUNSETPARTITIONS=partitions:ENOT_ALLOWED If an attempt to disarm the armed control panel with the enabled alarm (the alarm is deactivated). CPUNSETPARTITIONS=partitions,password:EFORMAT If the data format is incorrect (*partitions,password* are the command arguments) CPUNSETPARTITIONS=partitions:EPERMISIONS If the user with the specified password does not exist

9.1.4.5. CPZONESLOCK

Format:	CPZONESLOCK=zones[,password]
Limitations:	You must know the administrator or user password. Can be executed by ATS, administrator or user. If the command comes from ATS and was not authorized with a code, enter the *password*.
Description	Blocks permanently the given zones. It generates the events *INPUTx_LOCK*. Zones is a bit-vector indicating the zones, which one wants to block. Bit 1 (counting from 0) means the zone 1. Sending a command with the argument of *zones* equal to 0, has no sense, since it does not change anything. *Password* is the system administrator or user password, who has authorizations to the partition containing the blocked zones. The command returns: CPZONESLOCK:EOK,zones If the command is executed CPZONESLOCK:ENOT_ALLOWED If the command was sent via open SMS CPZONESLOCK:EFORMAT If the format of the sent command is incorrect CPZONESLOCK:EPERMISIONS If the user has not authorization to the proper partition CPZONESLOCK:ENOT_EXISTS If the user with the specified password does not exist

9.1.4.6. CPZONESUNLOCK

Format:	CPZONESUNLOCK=zones[,password]
Limitations:	You must know the administrator or user password. Can be executed by ATS, administrator or user. If the command comes from ATS and was not authorized with a code, enter the *password*.
Description	Removes permanent and temporary blockade from the given zones. It generates the events *INPUTx_UNLOCK*. *Zones* is a bit-vector indicating the zones, which one wants to unblock. Bit 1 (counting from 0) means the zone 1. Sending the commands with the argument of *zones* equal to 0, has no sense, since it does not change anything. *Password* is the system administrator or user password. The command returns: CPZONESUNLOCK:EOK,zones If the command is executed CPZONESUNLOCK:ENOT_ALLOWED If the command was sent via open SMS CPZONESUNLOCK:EFORMAT If the format of the sent command is incorrect CPZONESUNLOCK:EPERMISIONS If the user has not authorization to the proper partition CPZONESUNLOCK:ENOT_EXISTS If the user with the specified password does not exist

9.1.4.7. CPPARTITIONSGETZONES

Format:	CPPARTITIONSGETZONES[= password]
Limitations:	You must know the administrator or user password. Can be executed by ATS, administrator or user. If the command comes from ATS and was not authorized with a code, enter the *password*.
Description	*password* is the system administrator or user password Returns a list of zones assigned to the partition in the format CPPARTITIONSGETZONES:P1Zones,P2Zones Where: *P1Zones*, *P2Zones* are the bit-vectors indicating which zones are assigned to the first and second partition respectively. Bit 1 (counting from 0) means the zone A1. CPPARTITIONSGETZONES:EPERMISIONS If the specified password is incorrect CPPARTITIONSGETZONES:ENOT_ALLOWED If the command was sent via open SMS CPPARTITIONSGETZONES:EFORMAT If the format of the sent command is incorrect

9.1.4.8. CPPARTITIONSGETOUTPUTS

Format:	CPPARTITIONSGETOUTPUTS[= password]
Limitations:	You must know the administrator or user password. Can be executed by ATS, administrator or user. If the command comes from ATS and was not authorized with a code, enter the *password.*
Description	*password* is the system administrator or user password Returns a list of outputs assigned to the partition in the format CPPARTITIONSGETOUTPUTS:P1Outputs,P2Outputs Where *P1Outputs,P2Outputs* are the bit-vectors indicating which outputs are assigned to the first and second partition respectively. Bit 1. (counting from 0) means the output 1. CPPARTITIONSGETOUTPUTS:EPERMISIONS If the specified password is incorrect CPPARTITIONSGETOUTPUTS:ENOT_ALLOWED If the command was sent via open SMS CPPARTITIONSGETOUTPUTS:EFORMAT If the format of the sent command is incorrect

9.1.5. Commands for managing the wireless devices

9.1.5.1. CPGETKEYFOBS/CPGETDETECTORS

Format:	CPGETKEYFOBS CPGETDETECTORS
Limitations:	Can be executed by ATS
Description:	This command returns a list of all programmed wireless devices: key fobs (CPGETKEYFOBS command) or wireless detectors (CPGETDETECTORS command). The command returns: CMD:id:SERIALNO[,id:SERIALNO,...] Where *id* is the device number, starting from 0. For remotes, it is the remote number – 1 (i.e. id=0 corresponds to remote no. 1, id=1 corresponds to remote no. 2, etc.), for wireless detectors it is the zone number – 1 (id=0 corresponds to detector no. 1, id=1 corresponds to detector no. 2, etc.), *SERIALNO* is a 7-digit serial number of the device in hexadecimal format (0–9 and A-F characters). CMD:EEMPTY If the database contains no devices of the specified type -EBADSOURCE and NAK on protocol level, If the command was sent by an unauthorised user

9.1.5.2. CPDETECTORLOST

Format:	CPDETECTORLOST=?
	CPDETECTORLOST=hours

Available since:	2.8.8
Limitations:	It can be carried out by the ATS and the installer if they have been authorised to perform maintenance services

Description	The command returns or sets the time (in hours) after which the loss of wireless devices is reported. *hours* is a set or desired number of hours until the reporting of the loss. The minimum value is 2 hours, the maximum is 24, by default it is set to 6 h. The command returns: CPDETECTORLOST=minutes – for the command CPDETECTORLOST=? it returns the time set in the control panel CPDETECTORLOST =: EOK – if the command is executed correctly CPDETECTORLOST =: EPERMISIONS – no authorisation or wrong code CPDETECTORLOST =: EID – when the data range is incorrect CPDETECTORLOST =: EFORMAT – when the format of the command is incorrect

9.1.6. Commands for managing the security settings

9.1.6.1. SETATSPWD

Format:	SETATSPWD=oldpwd,newpwd
Limitations:	Can be executed by ATS
Descriptrion	This command changes ATS password from *oldpwd* to *newpwd*. The command returns: SETATSPWD:EOK – if the password has been changed successfully SETATSPWD:EPERMISSIONS – if sent with permissions other than ATS, or the old ATS password entered incorrectly SETATSPWD:ELENGTH – if length of the new password is incorrect – longer than 7 characters, shorter than 4, or contains restricted characters (e.g. space, #, etc.) SETATSPWD:EFORMAT – if the format of the sent command is incorrect

9.1.6.2. SETCOMMLOCK

Format:	SETCOMMLOCK=state,ats_password
Limitations:	State can be only 0 or 1 value; can be executed by ATS
Descriptrion	This command turns on (if state is equal to 1) or turns off (if state is equal to 0) 'communication settings lock' option. For this command to work, there must be entered the correct service code (ATS) as the *ats_password argument*. The command returns: SETCOMMLOCK:state,EOK – if the lock has been turned on or off (the state argument informs about specific action) SETCOMMLOCK:EPERMISSIONS - if sent with permissions other than ATS, or the ATS password entered incorrectly SETCOMMLOCK:EFORMAT - if the format of the sent command is incorrect

9.1.6.3. GETCOMMLOCK

Format:	GETCOMMLOCK
Limitations:	Can be executed by ATS
Descriptrion	This command get the state of "Communication parameters lock" option The command returns: GETCOMMLOCK:0 – the lock is on GETCOMMLOCK:1 – the lock is off GETCOMMLOCK:EPERMISSIONS – if sent with permissions other than ATS

9.2. DICTIONARY OF THE TERMS

ATS (Alarm Transmission System) – A special type of user account which is a monitoring station authorized with the device main access code.

P1, P2 – denote Partition 1 and Partition 2, respectively, which are the areas monitored by their assigned zones (detectors).

AES (Advanced Encryption Standard) – An advanced symmetric key encryption block cipher, currently among the most popular encryption methods. AES was published in 1997 by Vincent Rijmen and Joan Daemen and accepted as an encryption standard by the U.S. government in 2002.

NO – A configuration type of the input zone which enables detection of two states: normal (standby), in which the NO relay is open, and alarm (breach), in which the NO relay is closed.

NC – A configuration type of the input zone which enables detection of two states: normal (standby), in which the NC relay is closed, and alarm (breach), in which the NC relay is open.

EOL – A parametric configuration type of the input zone which enables detection of three operating states with a 2.2 kΩ parametric resistor: normal (standby), alarm (breach), and failure.

DEOL – A two-parametric configuration type of the input zone which enables detection of four operating states with two 1.1 kΩ parametric resistors: normal (standby), alarm (breach), tampering, and zone failure (e.g. by shorting of wiring).

TEOL – A configuration type which doubles the input zone by enabling connection of two zone detectors to a single input terminal of an alarm control panel. In this configuration, the source detector of an alarm signal is identified; the tamper input is common for both detectors. Each detector in this configuration requires two resistors.

Chirp – A short sound output by an alarm siren connected to one of the OUT terminals of an alarm control panel. There can be one chirp or a series of chirps.

RS-232 – A serial data communication standard. It is used for data exchange between hardware units over COM ports.

TAMPER – An anti-tamper switch, the tripping of which indicates an intentional disruption of operation of an alarm system, e.g. by opening the cover of a detector.

Clock loss – An event which indicates that the RTC has been reset. It is generated when an alarm system is powered on after a power cycle.

Alarm history – A list of all past and currently inactive alarms logged in an alarm system.

Watchdog – A feature which enables an automatic reaction of an alarm device when its connection to a monitoring station is lost.

10. CHANGE HISTORY

Date / Version / Firmware	Description
2017.09.22/ v1.0 / 2.8.7	First version of the manual
2017.10.20/ v1.1 / 2.8.7	Update information about Device Monitor and CPSETPARTITIONS command
2018.02.12/1.2/2.9.1	Added information about the new function for remote controls; updating information regarding the addressing of devices; update of the CPADDUSER command; adding the information about user categories related remote command CPGETUSERRIGHT; addition of the "Time to detect loss of wireless detectors" function and the related remote CPDETECTORLOST command; addition of the possibility of defining ACN numbers for accounts with the Contact ID protocol and related CPSETACN and CPGETACN remoted commands; expanding system options;
2018.07.27/ v1.3 / 2.10.0	Added a new response type to the zone, information about a new arming method by using the remote control and the option periodic repeating of wireless detector loss events