ALARM CONTROL UNIT

CPX220NWB

Installation and programming manual

Version of the manual:	v1.2
Date of issue:	2016.10.27
Firmware version:	2.6.3
GPRS transmitter configurator version:	1.3.64.3
OSM server version:	1.3.60.4

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:

LIST OF DRAWINGS AND DIAGRAMS

1. INTRODUCTION

Thank you for choosing EBS alarm control unit.

CPX220NWB is a simple, functional alarm control unit integrated with GSM/GPRS/SMS transmitter, intended for small- and medium- sized facilities. The central unit is equipped with 3 outputs and 16 zones with the possibility to be divided into 2 partitions. Dedicated KP16 LED keypad was designed in a modern, discreet style. Portable size, large, comfortable buttons and simple installation contribute to indisputable advantage of our system.

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

2. CONTROL UNIT FUNCTIONS

2.1. FUNCTIONAL CHARACTERISTIC

ZONES

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

PROGRAMMABLE OUTPUTS

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

FEEDING OUTPUTS

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

PARTITIONS

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

KEYBOARD

- cooperation with LED keyboard KP16
- ability to connect up to three keypads

TRANSMISSION

- Transmission of signals through GPRS/SMS module
- Encryption of data transfer using AES standard
- Communication with monitoring station using dedicated OSM.2007 server that ensures the reliability of data transfer thanks to a redundancy function
- Control of GSM/GPRS connection – automatic restoration of connection with monitoring station or switching to secondary server

CONFIGURATION

- Local, using KP16 keypad or a computer
- Remote through GPRS, SMS or CSD

USERS

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

SYSTEM OPTIONS

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

2.2. SPECIFICATIONS

Supply voltage:	18VAC (16-20VAC)
Required transformer Power:	must use transformer with power from 20VA to 60VA
Current consumption average/max: (average measured@: fully charged battery, established connection with server, connected keypad, no sensors connected)	120mA / 1100mA @18VAC
Average current consumption; lack of external supply (without keypad/ with keypad): (fully charged battery, no sensors connected, established connection with server)	60mA / 80mA
Charging current: (measured with totalny discharged battrey)	max. 350mA
Charging voltage:	13.8V
Supported bartery type:	Lead-acid 12V
Low voltage – event treshold:	11V
Voltage battery cut off level:	below 9V
Working temperature:	-10ºC to +55ºC
Working humidity:	5% to 93%
PCB dimensions:	152 x 78 x 30mm

2.1. ACCESSORIES AND SOFTWARE APPLICATIONS

Keypads	Description
KP16-0 (black), KP16-9 (white)	LED wired keypad
KP1W-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

Programmers	Description
GD-PROG	CPX Controll 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	Mobile Configuration App of GPRS Transmitters. For Installers (Android)
AVA	Mobile Monitoring application for controll and monitoring of controll panel. (Android, iOS). For Users.

3. INSTALLATION AND WIRING

3.1. SEQUENCE OF INSTALLATION

1. Develop installation diagram accounting for the location of control unit, keypad, detectors and other system components.

2. Install the control unit 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 unit. For description of keypad installation, please refer to chapter 0.

⚠ **NOTE: Maximum length of cables connecting the control unit with the keypad, at the core diameter 0.5mm2 cannot exceed 200m.**

4. Install detectors and door and window reed relays. Connect the installed elements with control unit. For sample configuration of zones, please refer to chapter 3.4.

5. Install and connect signalling devices with the control unit. For sample signalling devices connection diagrams, please refer to chapter 3.5.

6. Complete the remaining cable connections.

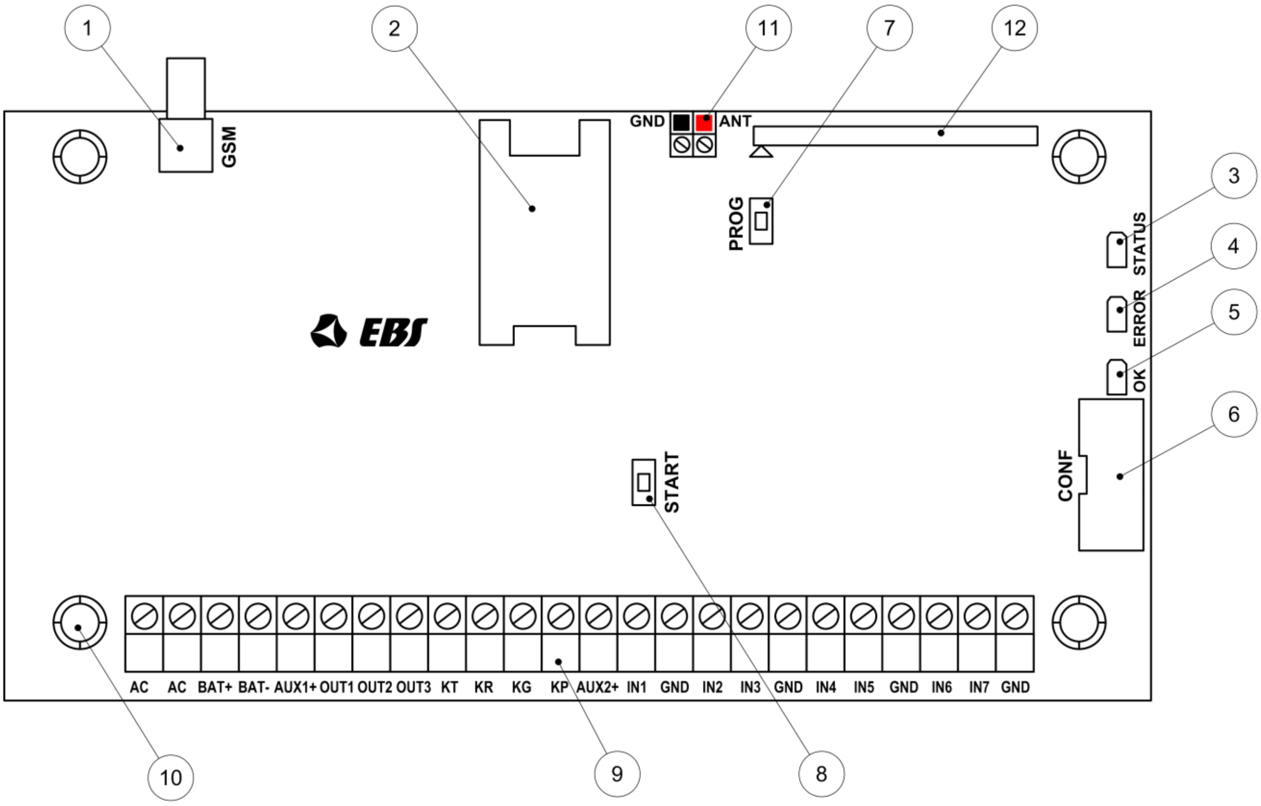
7. Connect power supply and a battery with the control unit.

8. Program the functions of the control unit. 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 unit is compatible with GSM antenna with male SMA connector.

This type of antenna should be install (sellotape) on nonmetalic surface (plastic, glass etc.) in vertical position (foto attached below). The hight 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 (especcialy 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 instaled on alarm central case or in close range to wireless recivers. It could decrease the signal range.

2. Slot of SIM card

The control unit 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 unit. Default factory PIN code of the control unit is 1111.

3. "STATUS" LED

Yellow LED diode. For the detailed description of "STATUS" LED operation, please refer to chapter 7.

4. "ERROR" LED

Red LED diode. For the detailed description of "ERROR" LED operation, please refer to chapter 7.

5. "OK" LED

Green LED diode. For the detailed description of "OK" LED operation, please refer to chapter 7.

6. "CONF" programming connector

"CONF" IDC10 connector allows the control unit configuration using dedicated **GD-PROG** programming device and any computer equipped with RS232 port.

7. "PROG" Button for default settings restoration

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

8. "START" button for battery activation of control unit without the mains power supply

If the control unit 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 unit

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

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

The above holes are intended for the control unit 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).

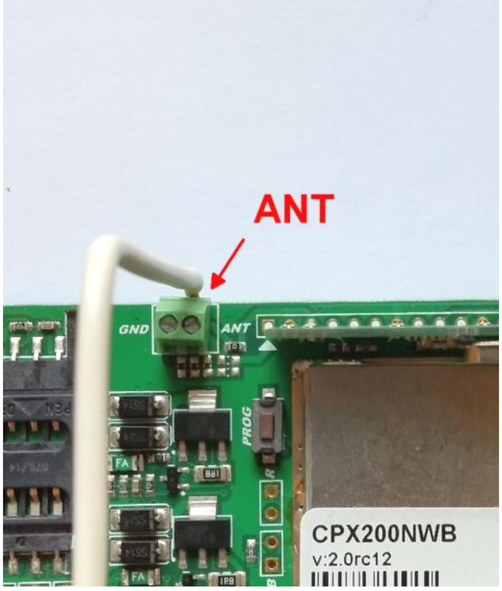
11. Wireless module antenna connector

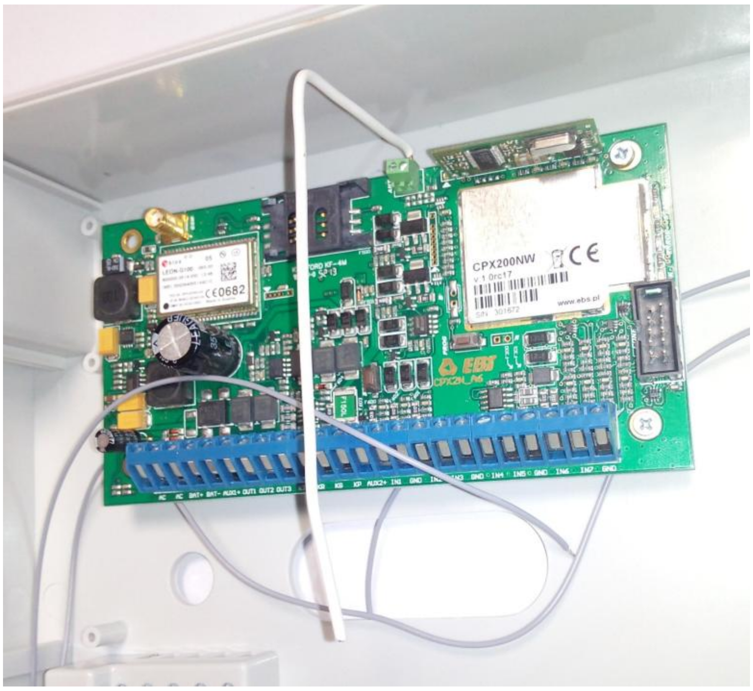
CPX220NWB included two types of antennas: internal and external dipole type.

433MHz internal antenna

Internal antenna 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). Cold pole has been filled with plastic element (marked as a black spot). Correct antenna install position in the photo attached below.

⚠

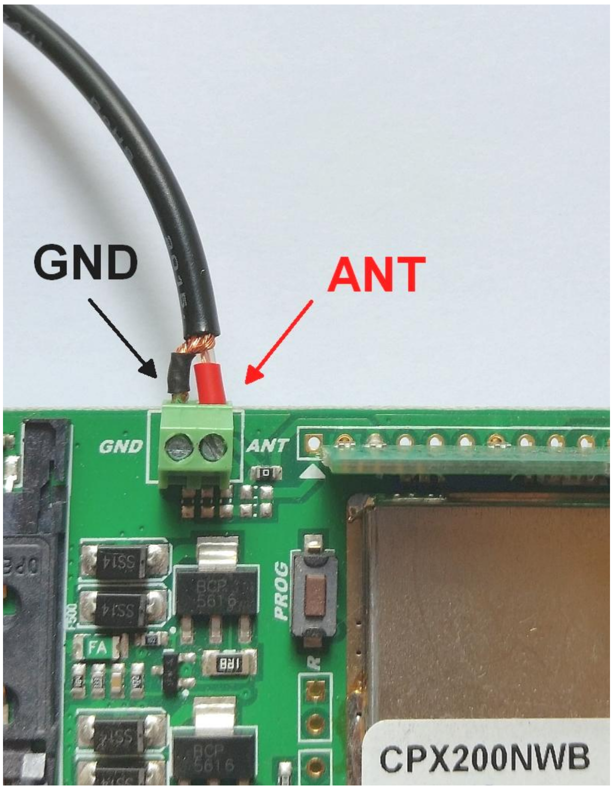


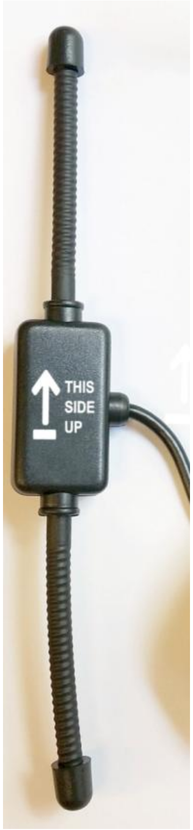


433MHz external antenna dipol type

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

⚠



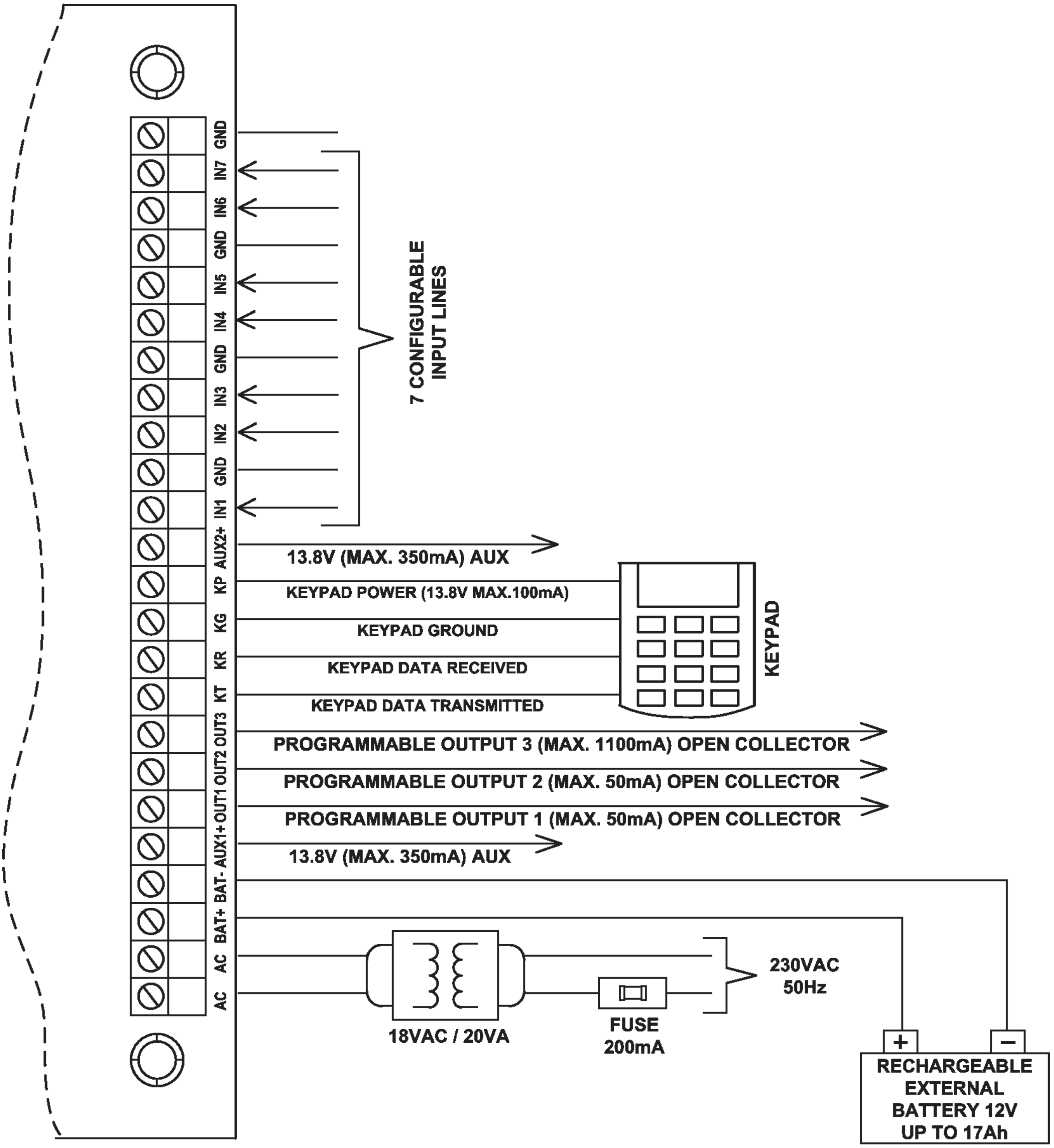


12. **Wireless module**

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

3.3. DESCRIPTION OF SCREW TERMINALS OF THE CONTROL UNIT

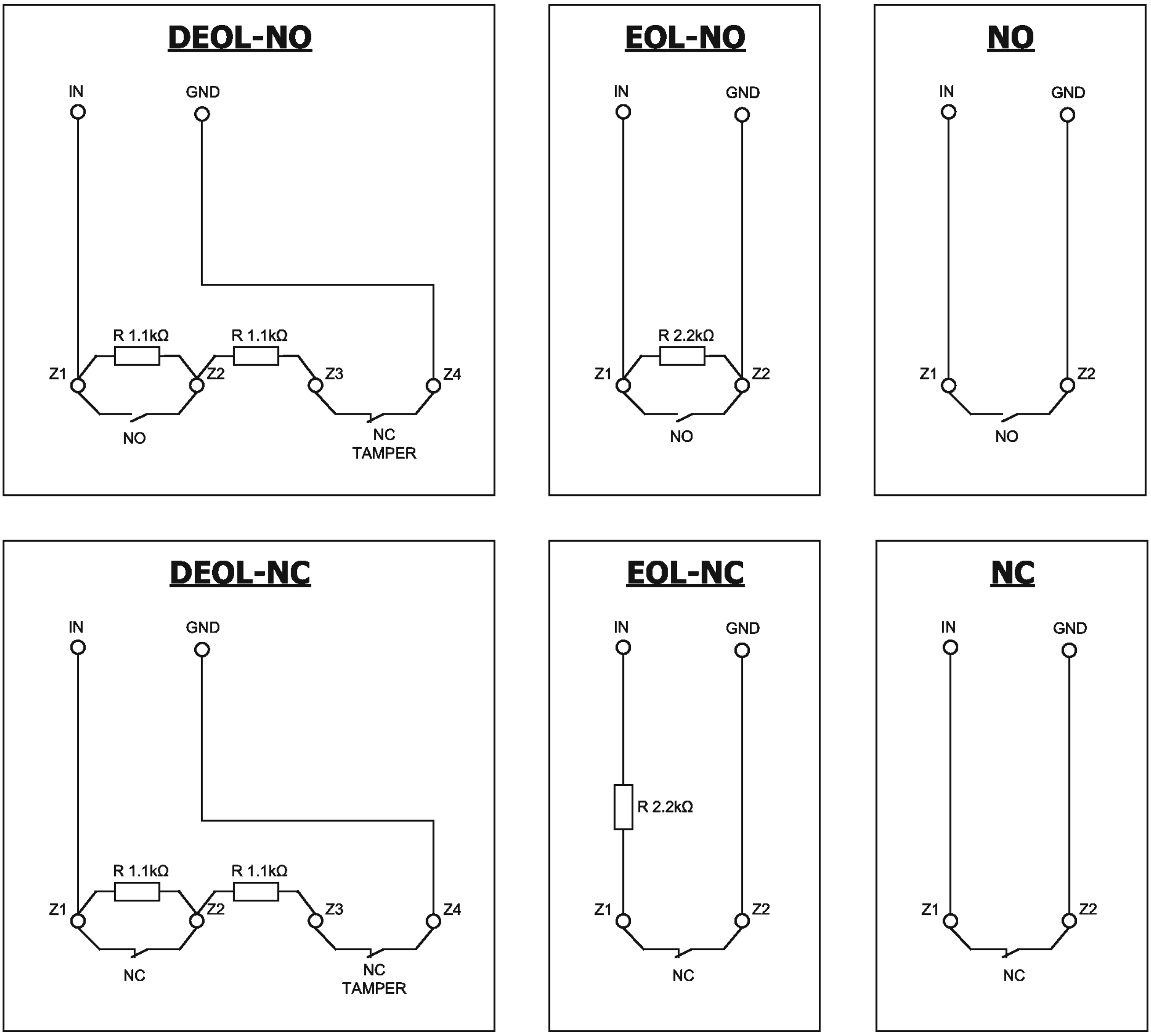
NOTE: Any assembly and installation works shall be carried out with power supply off and battery disconnected.



Drawing 2. Description of screw terminals of the control unit

3.4. CONFIGURATION OF WIRED INPUT LINES

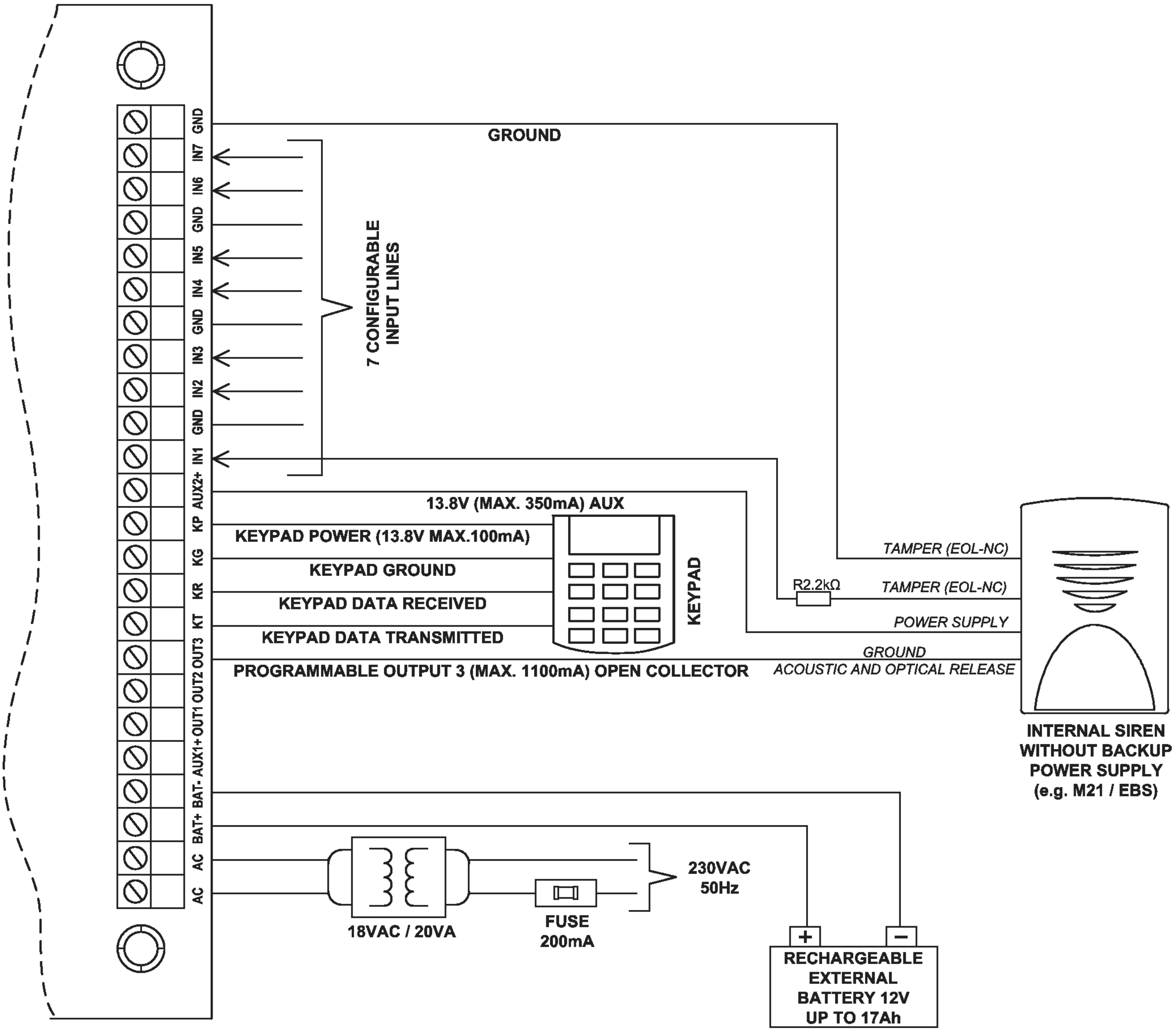
All wired input lines are fully configurable and can operate as normally closed (NC)) or normally open (NO) as well as with assigned parameters (EOL-NO or EOL-NC) using 2.2kΩ resistors or with assigned double parameters (DEOL-NO or DEOL-NC) using 1.1kΩ resistors. Both resistor types are included in the delivery of the control unit. Various configurations of input lines are presented in the drawing 3.



Drawing 3. Configuration of input lines

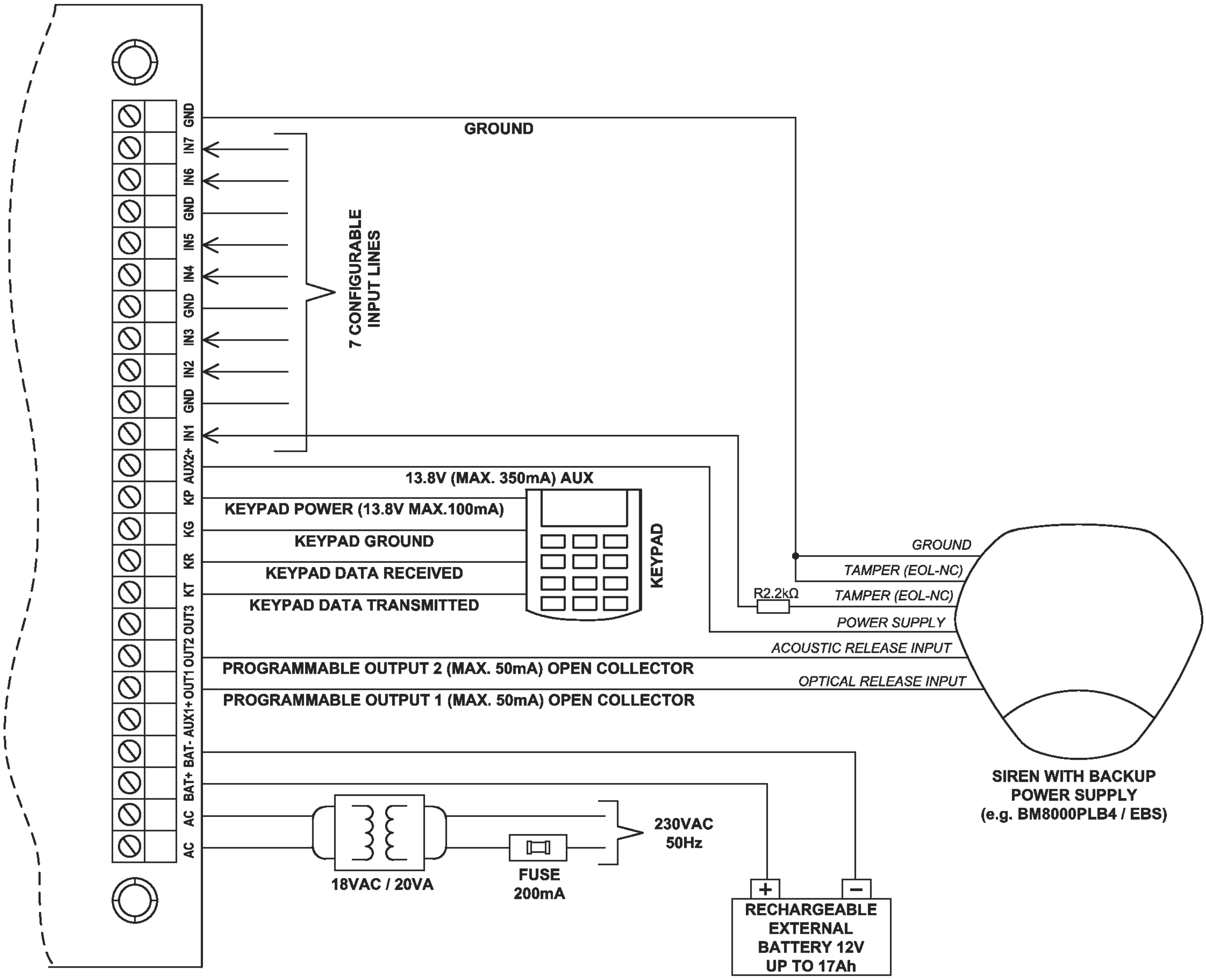
3.5. SAMPLE CONNECTION OF SIGNALLING DEVICE

3.5.1. Internal signalling device without independent source of power supply



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

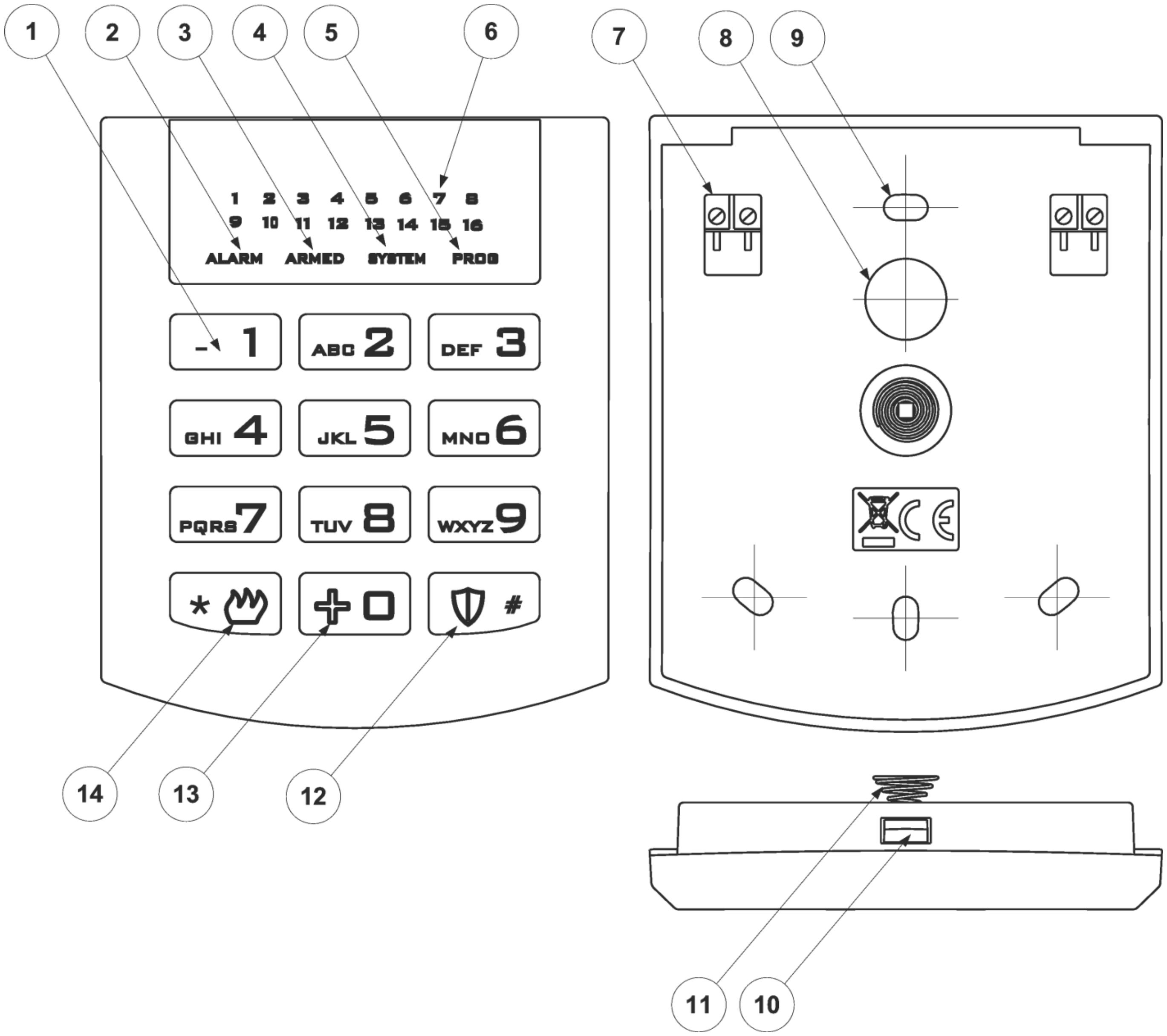
3.5.2. External signalling device with independent source of power supply



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

3.6. KP16 KEYPAD

3.6.1. Description of keypad elements



Drawing 6. KP16 Keypad

1. Keypad buttons

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

2. ALARM LED (red):

Flashing light – means that alarms were present in the system (alarm memory).

Constant light – means that system is in alarm state.

Off – system is operating correctly.

3. ARMED LED (red):

Flashing light – means that time for exit in any of partitions is counted.

Constant light – at least one partition is armed

Off – partitions disarmed.

4. SYSTEM LED (yellow):

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

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

Off – no fault in the system.

5. PROG LED (blue):

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

Flashing – data will be entered.

Constant light – installer service function is activated.

6. 1 - 16 LEDs (red)

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

7. Screw terminals

The connectors for connecting cables joining the keypad with the alarm control unit.

8. Cable entry

It is a place for entering the connection cables.

9. Assembly holes

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

10. Casing opening latch

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

11. Anti-sabotage switch

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

12. - 14. Emergency buttons

See item 4.3.11. Emergency buttons and 6.3.6. Emergency Buttons.

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 (ALARM, ARMED, SYSTEM, PROG)
Button layout:	Standard telephone keypad 3 x 4 buttons

3.6.3. Keypad installation

1. KP16 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 indywidually.

5. Connect cables joining the keypad with the alarm control unit. Keypad terminals marked: KT, KR, KP, KG shall be connected with KT, KR, KP, KG terminals in the alarm control unit (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 suport 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. At the same time, press and hold the JKL 5 and - 1, ABC 2 or DEF 3, which means a new keypad address.

3. After about 5 seconds the keypad will display the programmed keypad address.

4. After programming the keypad address, reset the control panel CPX220NWB.

3.7. WIRELESS KEYPAD KP1W

The wireless keypad KP1W was designed to work with the hybrid central panel CPX220NWB. There is a possibility to add three of these keypads, however each of them occupies one of 16 input lines.

The transmission between the keypad and the central panel is protected with changing code and encrypted. The device sends to the central panel a cyclic test transmission and lack of it will be signaled in the system as a breach of the line, 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.

The wireless keypad KP1W uses one-way transmission and cannot receive communication from the control panel. Therefore, we suggest to set one of the central 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.

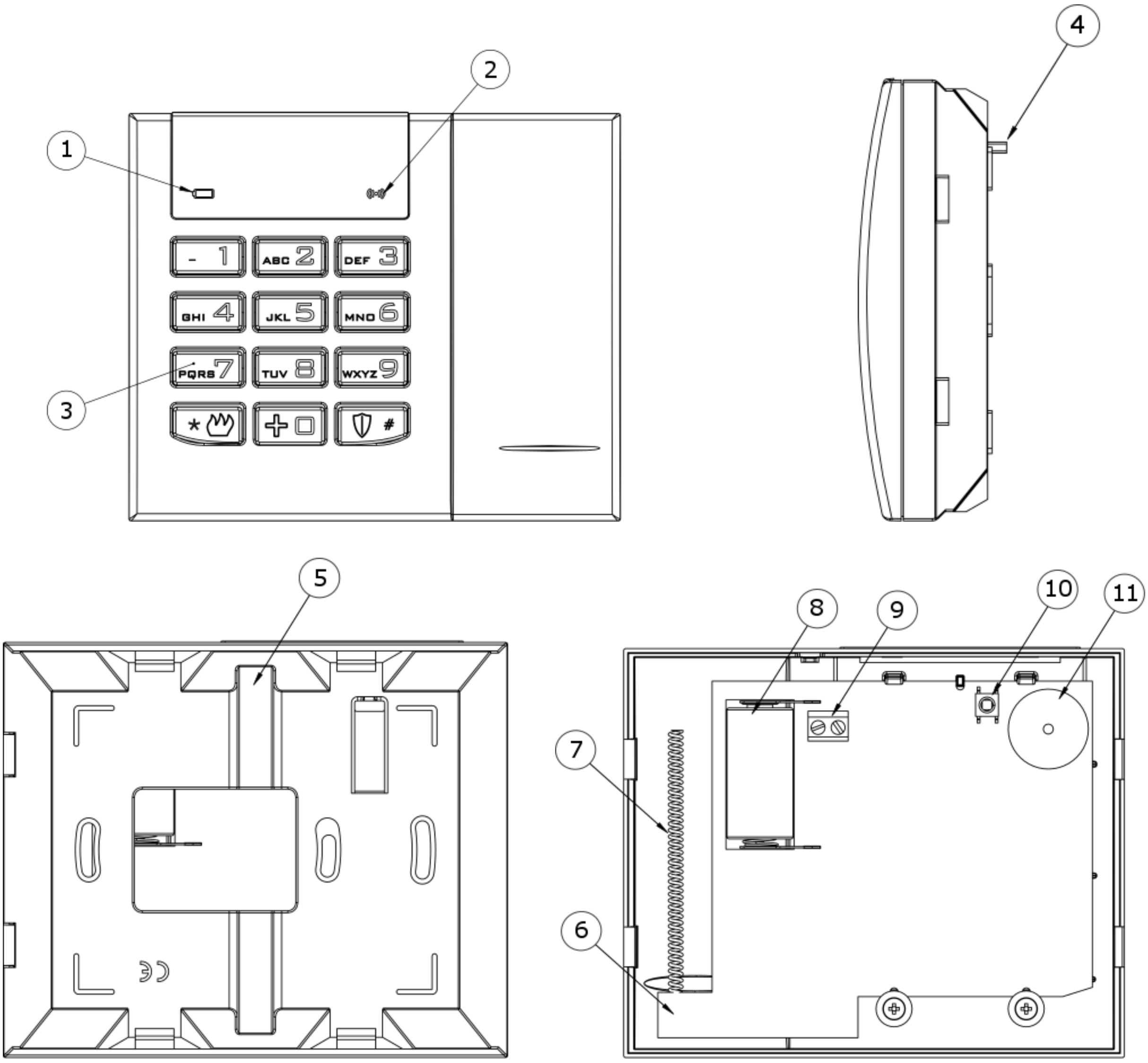
We recommend to have at least one wire keypad KP16 installed in the alarm system in order to set parameters of the control panel, display system status and change user codes. We also recommend to use AVA application with the control panel CPX220NWB to facilitate controlling operation of our alarm control panels.

3.7.1. Adding KP1W to the system

The wireless keypad KP1W can be introduced to the alarm system memory in a manner similar to wireless sensors. There are two methods available:

- Using KP16 keypad, see chapter 4.3.9.1. Wireless sensors configuration.
- Using software “GPRS Transmitter configurator”, see chapter 6.3.2. Wireless zones.

3.7.2. Description of keypad elements



Drawing 7. KP1W Keypad

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

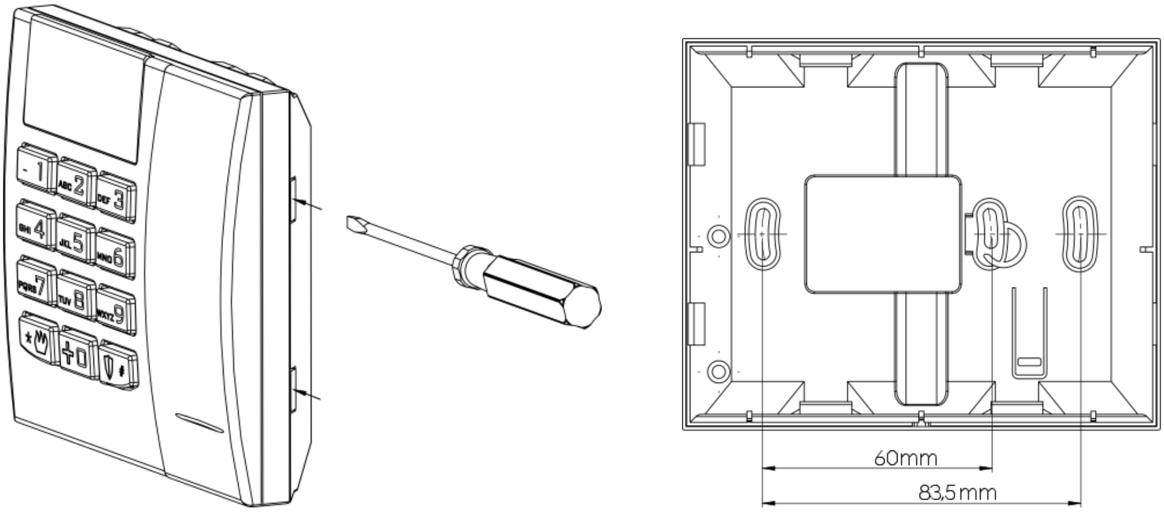
10. **Buzzer**

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 KP1W 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

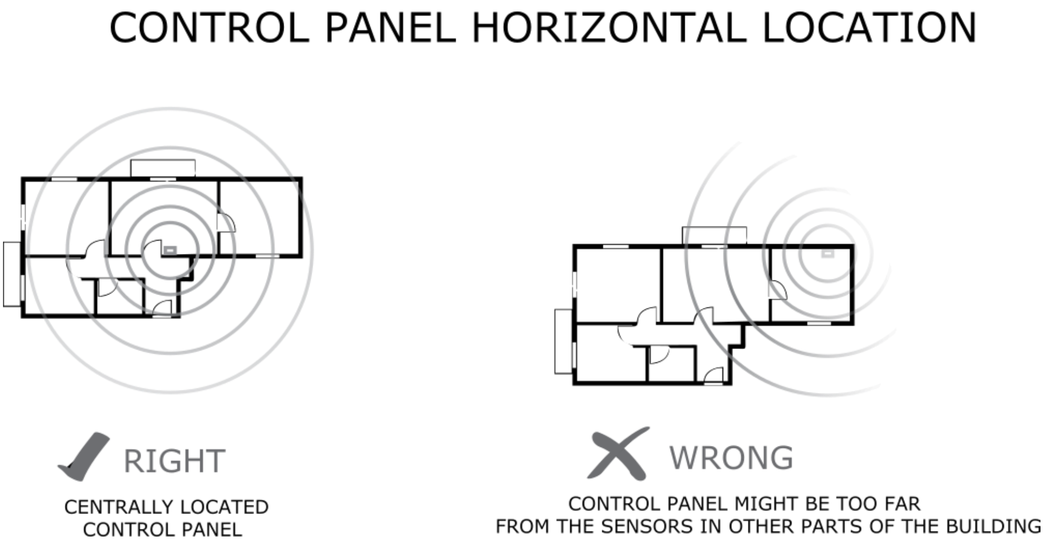
The keyboard KP1W is equipped with a feature enabling connection of opening sensor (reed relay), which can be used as a door opening sensor.

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 Figure 7.

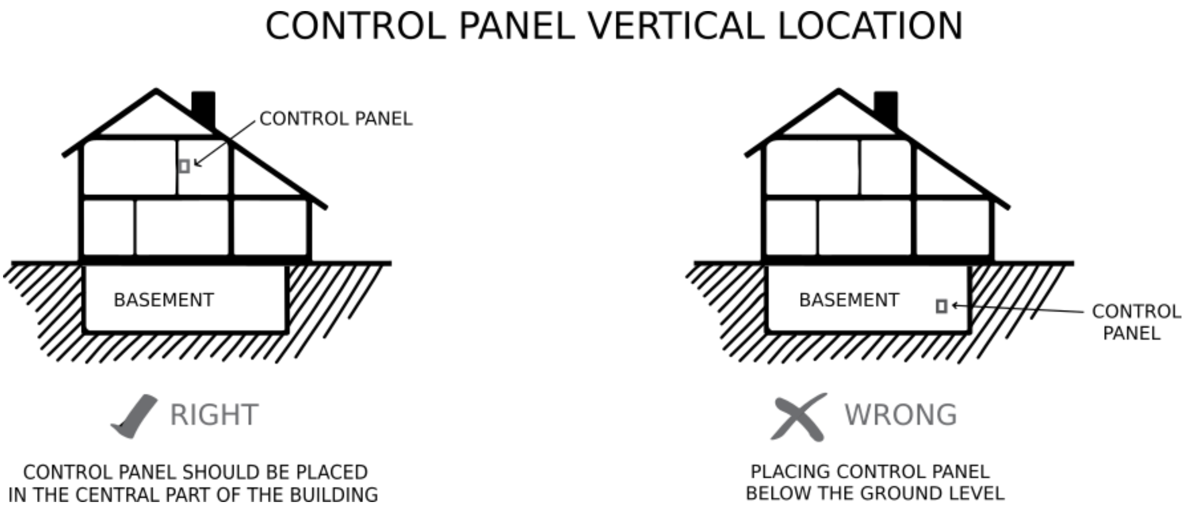
This sensor in the alarm system CPX220NWB will have assigned the same line number as the keypad.

3.8. CONTROL PANEL LOCATION

The control panel should be located in the central part of the object. The central location of the panel usually provides good communication with all wireless detectors. See drawings 8 and 10.

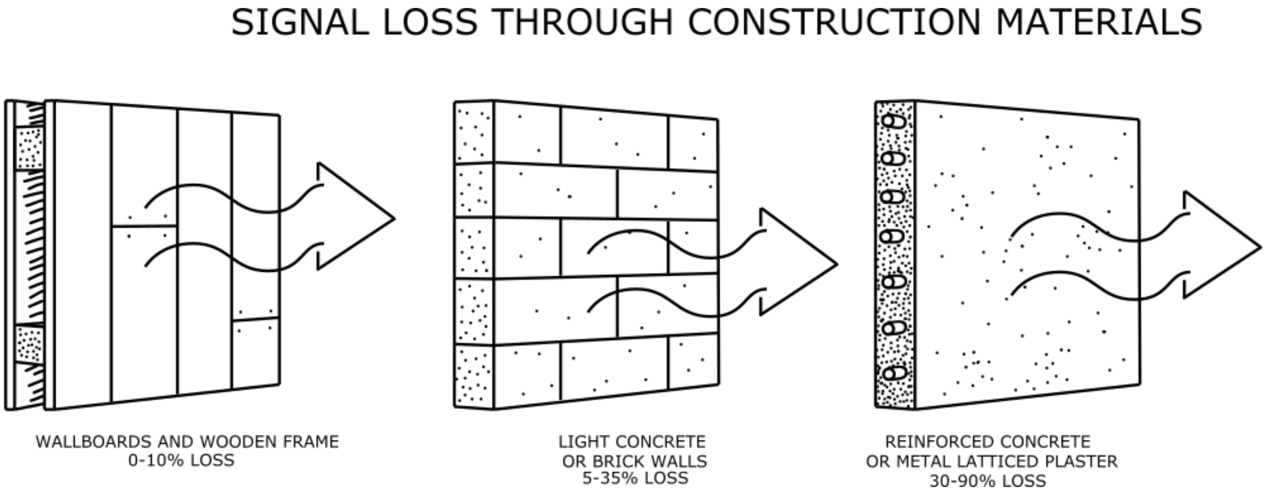

CONTROL PANEL HORIZONTAL LOCATION
RIGHT
CENTRALLY LOCATED
CONTROL PANEL
WRONG
CONTROL PANEL MIGHT BE TOO FAR
FROM THE SENSORS IN OTHER PARTS OF THE BUILDING

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.

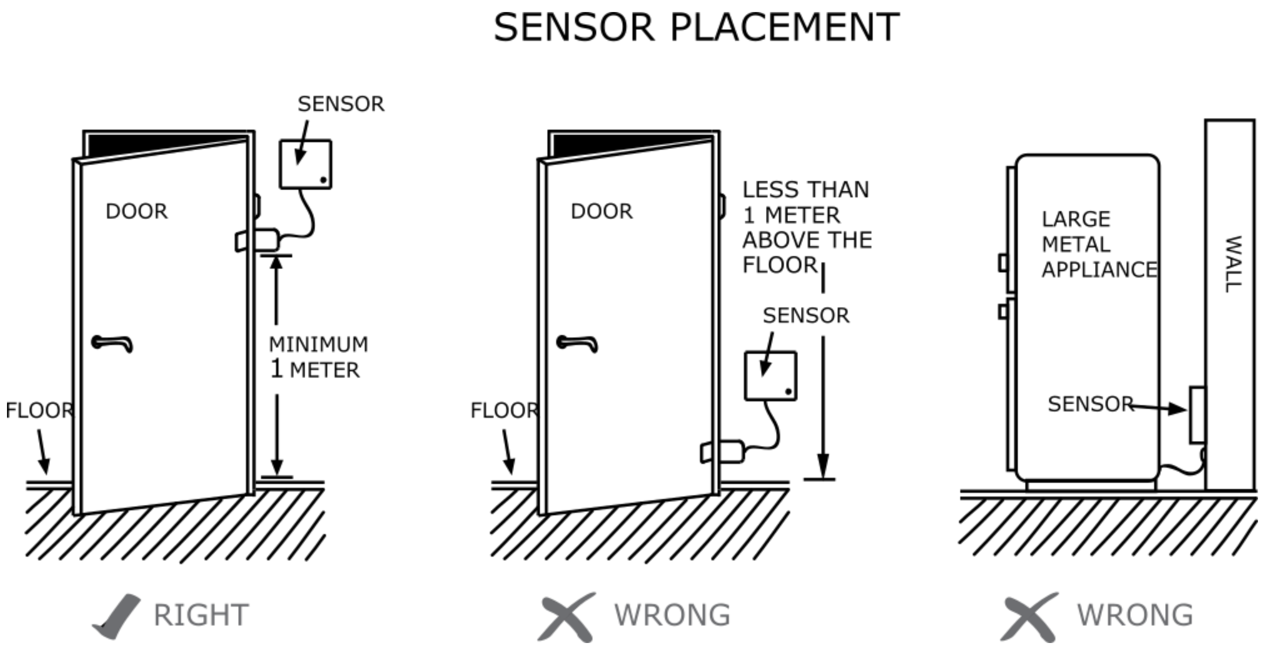

SIGNAL LOSS THROUGH CONSTRUCTION MATERIALS
WALLBOARDS AND WOODEN FRAME
0-10% LOSS
LIGHT CONCRETE
OR BRICK WALLS
5-35% LOSS
REINFORCED CONCRETE
OR METAL LATTICED PLASTER
30-90% LOSS

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 KP16.**

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 BIT or DEC type).

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

Binary type (BIT)
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 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:

Entered digit	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**

4.1. ACTIVATION OF SERVICE MODE

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

WXYZ9 WXYZ9 🛡# **<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 +0 and confirm with 🛡#. Using that function will trigger the control unit'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 permision to configure alarm central. By this commands You can get into some menu sections (more information about procedures You will get in chapters bellow):

-1 🛡#	Instaler code change
ABC2 🛡#	Power loss time raport
DEF3 🛡#	Reset to default settings
GHI4 🛡#	System options
JKL5 🛡#	Users remote manager
-1 **<XX> <Y>** 🛡#	Zones configuration
ABC2 **<XX> <Y>** 🛡#	Outputs configuration
DEF3 **<XX> <Y>** 🛡#	Partitions configuration
GHI4 **<XX> <Y>** 🛡#	Wireless zones configuration

JKL5 **<XX> <Y>** #	Remote controllers configuration
MNO6 **<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:

ABC2 # **<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 unit's reset using default parameters.

DEF3 # **<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 BIT type. By pressing 1, 2, 3, 4, 5 and 6 keys, you can switch on/off proper option. 3 beeps will confirm the successfully entered function.

GHI4 # **<Options>** #

Where:

Options – number of option (BIT 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 his 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** – Disable automatic arm prevention overriding when fault. If this option is disabled and at least on fault is active in the system, arm prevention isn't signaled to the user during partition arming. Instead arm prevention is automatically overridden. If option is enabled, faults causes arm prevention which can be overridden by user.
- **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 line 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.

NOTE: Firmware versions older than 2.1.0 do not support the duress code. Upgrading the Firmware to version 2.1.0 or newer one has to make sure that there are no conflicts between existing users and their duress codes.

- **8** – Show partition arming mode instead of inputs interlocking states. By default systerm will show violated and interlocked zones on diodes 1-8. Setting this option will tell the system to show partitoin armind mode on diodes 1-2. Zones states will no longer be available.

  Display scheme:

  Led off – partition disarmed

  Led on – partition armed in away mode

  Led blinking – partition armed in stay mode

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 BIT 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 (BIT type parameter):

- **1** – Users remote management enable – when is swiched on

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

4.3.6. 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 4.3.9.

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

-1 **<XX> <Y>** #

where:

XX – determines the number of zone from **01** to **16**; entering number **00** will change the parameters for all zones in the system,

Y – number of parameter related to a given zone:

- **0** – complex function, the initiation of which configures the parameters listed below as another set of parameters;
- **1** – type of zone response (DEC type parameter):
  - 0 – instant
  - 1 – delay
  - 2 – 24h burglary
  - 3 – arming/disarming
  - 4 – 24h tamper
  - 5 – interior delayed
  - 6 – 24h burglary silent
  - 7 – 24h fire
  - 8 – perimeter
  - 9 – perimeter exit
- **2** – delay in seconds for the circuit of selected "delay" response type (DEC type parameter). For other response types the parameter is irrelevant.
- **3** – operation mode (DEC type parameter):
  - 0 – unused circuit
  - 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
- **4** – number of alarms after which the zone will be automatically blocked until re-arming (DEC type parameter). If 0, zone will not be blocked.
- **5** – zone options (BIT type parameter):

  - 1 – circuit ignored during arming – i.e. can be violated during partition arming (e.g. delay circuits 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")
- **6** – sensitivity in milliseconds, i.e. after what time the input is considered to change its status – default value; 400ms

Note: For wireless zones 8 – 16 complex function 1XX0 should not include option (function) 6 – sensitivity. Function 1XX3 (operation mode) displays the value 7 for wireless zones 8 – 16, and the value can not be changed.

Examples:

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

1 0 2 3 # 2 #

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

1 0 0 6 # 2 0 0 #

c) change of many parameters at the time for zone 1 using complex functions – zone 1 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:

1 0 1 0 # 0 # # 1 # 8… …#
2 # 5 0 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.**

4.3.7. 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>** #

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:

- **0 –** complex function, the initiation of which configures the parameters listed below as another set of parameters;
- **1 –** type of output (DEC type parameter):
  - 0 – not used,
  - 1 – signalling alarm,
  - 2 – stand-by indicator,
  - 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 signalling alarm
- **2 –** time of output activation in seconds (DEC type parameter); if 0 is set, output will operate in bi-stable mode.

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

a. chirp signal duration:

ABC 2 +0 +0 DEF 3 # **<X>** #, where <X> is the time in miliseconds

b. interval duration between two following chirps:

ABC 2 +0 +0 GHI 4 # **<X>** #, where <X> is the time in miliseconds

NOTE: Chirp configuration is common for all outputs

Example:

a) change of a single parameter – operation mode of number 2 output into bi-stable operation mode:

ABC 2 +0 ABC 2 ABC 2 # +0 #

b) change of 3 output type into triggered by power failure:

ABC 2 +0 DEF 3 - 1 # DEF 3 #

c) change of many parameters at the time for output 1 using complex function – output 1 is to be set as alarm signalling with activation time 120 seconds:

ABC 2 +0 - 1 +0 # - 1 # - 1 ABC 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.**

4.3.8. 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:

DEF 3 **<XX> <Y>** #

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:

- **0 –** complex function, the initiation of which configures the parameters listed below as another set of parameters;
- **1** – zones belonging to partition (BIT type parameter, zones 10 – 16 may be set by long press the keys 0 – 6),
- **2 –** outputs belonging to partition (BIT type parameter),
- **3 –** time for leaving the partition in seconds (DEC type parameter),
- **4 –** alarm time in the partition in seconds (DEC type parameter),
- **5 –** partition options (BIT type parameter):
  - 1 – Quiet signalling of time for entering (during counting the time for leaving, the buzzer in a keypad is not active)
  - 2 – Quiet signalling of time for leaving (during counting the time for leaving, the buzzer in a keypad is not active)
- **6** – auto-arming time (DEC type parameter, time of day written in the 24-hour notation in the form HHMM),
- **7** – auto-arming option (BIT type parameter):
  - 1 – auto-arming activation/deactivation
- **8** – auto-disarming time (DEC type parameter, time of day written in the 24-hour notation in the form HHMM),
- **9** – auto-disarming option (BIT type parameter):
  - 1 – auto-disarming activation/deactivation

Notes:

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

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

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

Execution of complex function 3009 (auto-disarming activation/deactivation for all paritions) 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 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.

Examples:

a) change of a single parameter – assigning 1, 2, 3 zones to the first partition:

DEF 3 +0 -1 -1 # -1 ABC 2 DEF 3 #

b) change of a single parameter – assigning 1, 10, 11 zones to the second partition:

DEF 3 +0 ABC 2 -1 # -1 +0 (long press) -1 (long press) #

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

DEF 3 +0 +0 DEF 3 # MNO 6 +0 #

d) change of many parameters at the time for partition 2 using complex function – zones 2, 4, 5 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 signalling of time for entering and leaving was quiet:

DEF 3 +0 ABC 2 +0 # ABC 2 GHI 4 JKL 5 # -1 # … … GHI 4 JKL 5 # -1 ABC 2 +0 # -1 ABC 2 #

⚠ **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.**

4.3.9. Wireless zones configuration

4.3.9.1. 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:

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

Where:

XX – determines the number of wireless zone from **01** to **16**; entering number **00** will change the parameters for all zones in the system,

Y – number of parameter related to a given zone:

- **0** – complex function, the initiation of which configures the parameters listed below as another set of parameters:
- **1** – Delete a sensor. After selecting this option, you can confirm deleting by pressing # key, or you can cancel function by pressing * key.
- **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.
- **3** – Type of a wireless sensor (read only):
  - 0 – no sensor
  - 1 – PIR-10 sensor
  - 2 – MC-10 sensor
  - 3 – GS-10 sensor
  - 4 – SD-10 sensor
  - 5 – PIR-11 sensor
  - 6 – SD-20 sensor
  - 7 – KP1W keypad
  - 8 – MC-11 sensor
  - 9 – FL-10 sensor

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.

Example:

a) delete a wireless sensor no. 10:

GHI 4 - 1 + 0 - 1 #

b) add a wireless sensor no. 11:

GHI 4 - 1 - 1 ABC 2 # #

4.3.9.2. Signal strength of wireless detectors

The function allows to check signal strength of wireless detectrors.

GHI 4 ✢0 ✢0 WXYZ 9 🛡#

LEDs 1 – 16 indicate line with wireless detectors.

Enter the line number and press 🛡# to confirm. 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 return to line selecting menu press *🔥 or 🛡# .

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

4.3.9.3. Delete all wireless sensors

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

GHI 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.

4.3.10. Remote controllers configuration

4.3.10.1. 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:

JKL 5 **<XX> <Y>** 🛡#

Where:

XX – determines the number of remote control

Y – number of parameter related to a given remote control:

- **0** – complex function, the initiation of which configures the parameters listed below as set of parameters:
- **1** – Delete a remote control. After selecting this option, you can confirm deleting by pressing # key, or you can cancel function by pressing * key.
- **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.
- **3** – type of the remote control (read only)
  - 0 – no remote control
  - 1 – P300 remote control
  - 2 – RC-10 remote control
- **4** – The use to which the remote control is assigned
- **5, 6, 7, 8** – buttons functions:
  - 0 – no fuction
  - 1 – arm
  - 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

Note:

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

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

Alarms from remote control can be generated regardless of whether or not the partition is armed. For normal and silent alarm can be sent a message to the monitoring station, depending on the configuration of the control panel.

Example:

a) delete a remote control no. 1:

JKL 5 +0 - 1 - 1 #

b) add a remote control no. 1:

JKL 5 +0 - 1 ABC 2 # #

4.3.10.2. Delete all remote controllers

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

JKL5 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.

4.3.11. Emergency buttons

To configure emergency buttons, use the following pattern:

MNO6 **<XX> <Y>** #

where:

XX – emergency button:

- **01** – fire
- **02** – help
- **03** – panic
- **00** – all buttons above

Y – enable/disable emergency button:

- **0** – disable emergency button
- **1** – enable emergency button:
  - 1 – output 1
  - 2 – output 2
  - 3 – output 3

After service command confirmation, there will be digits displayed which represent outputs activated by emergency button. Use digits 1-3 to change this setting.

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

Example:

a) enabling all emergency buttons:

MNO6 0 0 1 # #

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

MNO6 0 DEF3 1 # ABC2 DEF3 #

4.4. TEXT MESSAGES CONFIGURATION

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: JKL5 ABC2 # **<administrator 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.

CPX220NWB 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 (" ").

Installer can configure the text messages using following commands:

Acquiring the state of partitions	
Command syntax	XXXX GETARMED
Command description	Acquiring the information which partitions are armed/disarmed XXXX – user code *Example: 1234 GETARMED*
Feedback message	PARTITION1:X, PARTITION2:Y or GETARMED:ERROR
Feedback message description	PARTITION1:X, PARTITION2:Y – Information about partitions arm/disarm state. PARTITION1,PARTITION2 – default partitions names, they can be changed with the SETNAME command X,Y – partition states, possibile values: 0 – disarmed 1 – armed GETARMED:ERROR – command rejected by the system

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

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

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

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

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

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

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

Feedback message	SETUSERSMS=EVENT,TELNUM,MSG_ID:OK
	or
	SETUSERSMS=EVENT,TELNUM,MSG_ID:ERROR

Feedback message description	SETUSERSMS=EVENT,TELNUM,MSG_ID:OK – command accepted SETUSERSMS=EVENT,TELNUM,MSG_ID:ERROR – command rejected by the system

Getting a text message content and a phone number assigned to the event	
Command syntax	XXXX GETUSERSMS=EVENT
Command description	Getting the content of a text message and a phone number assigned to the specified event. XXXX – user code EVENT – a short name of the event, possible event names are listed at the end of this chapter *Example:* 1234 GETUSERSMS=ARM1

Feedback message	GETUSERSMS=EVENT:TELNUM,MSG_ID
	or
	GETUSERSMS=EVENT:ERROR

Feedback message description	GETUSERSMS=EVENT:TELNUM,MSG_ID – information about text message and phone number assinged to the event GETUSERSMS=EVENT:ERROR – command rejected by the system

List of events handled by the SETUSERSMS and GETUSERSMS commands	
Alias name	Description
ARM1	Partition 1 armed
ARMSTAY1	Partition 1 armed in perimeter mode
ARM2	Partition 2 armed
ARMSTAY2	Partition 2 armed in perimeter mode
DISARM1	Partition 1 disarmed
DISARM2	Partition 2 disarmed
INPUT1 (to INPUT16)	Violation of zones 1…16
INPUT1-OFF (to INPUT16-OFF)	Violation of zones 1…16 ended
INPUT1-TAMPER (to INPUT16-TAMPER)	Sabotage of zones 1…16
INPUT1-TAMPEREND (to INPUT16-TAMPEREND)	Sabotage of zones 1…16 ended
INPUT1-LOCK (to INPUT16-LOCK)	Bypass of zones 1…16
INPUT1-UNLOCK (to INPUT16-UNLOCK)	Bypass of zones 1…16 ended
OUTPUT1-ON (to OUTPUT3-ON)	Zones 1…3 triggered
OUTPUT1-OFF (to OUTPUT3-OFF)	Zones 1…3 trigger ended
OUTPUT1-TAMPER (to OUTPUT3-TAMPER)	Fault of zones 1…3
OUTPUT1-TAMPEREND (to OUTPUT3-TAMPEREND)	Fault of zones 1…3 ended
POWER-FAIL	Power failure
POWER-OK	Power failure ended
BATTERY-FAIL	Battery failure
BATTERY-OK	Battery failure ended
AUX1-FAIL	Failure of auxiliary output 1

AUX2-FAIL	Failure of auxiliary output 2
AUX1-OK	Failure of auxiliary output 1 ended
AUX2-OK	Failure of auxiliary output 2 ended
KEYPAD1-LOST (to KEYPAD3-LOST)	Failure of keypad 1...3
KEYPAD1-OK (to KEYPAD3-OK)	Failure of keypad 1...3 ended
KEYPAD1-TAMPER (to KEYPAD3-TAMPER)	Sabotage of keypad 1…3
KEYPAD1-TAMPEREND (to KEYPAD3-TAMPEREND)	Sabotage of keypad 1…3 ended
KEYPAD-FIRE-BEGIN	'Fire' alarm started
KEYPAD-HELP-BEGIN	'Help' alarm started
KEYPAD-SILENTALARM-BEGIN	'Panic' alarm started
KEYPAD-FIRE-END	'Fire' alarm ended
JAMMING-BEGIN	GSM jamming
JAMMING-END	GSM jamming ended
DETECTOR1-LOST (to DETECTOR16-LOST)	Detector 1…16 signal lost
DETECTOR1-OK (to DETECTOR16-OK)	Detector 1…16 signal restored
DETECTOR1-PWR (to DETECTOR16-PWR)	Detector 1…16 battery low
DETECTOR1-PWROK (to DETECTOR16-PWROK)	Detector 1…16 battery restored

List of errors sent as feedback messages

Alias name	Description
ERROR-PERMISSION	Permission to issue this command was not granted
ERROR-FORMAT	Wrong command syntax
ERROR-VALUE	Wrong parameter value
ERROR-EMPTY	Parameter value missing
ERROR	Other error

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 Pentium II 400MHz,
- 64 MB RAM,
- 1GB HDD,
- RS-232 serial port,
- Colour screen (min. 15”, resolution min. 800x600),
- Keypad,
- Mouse.

Software:

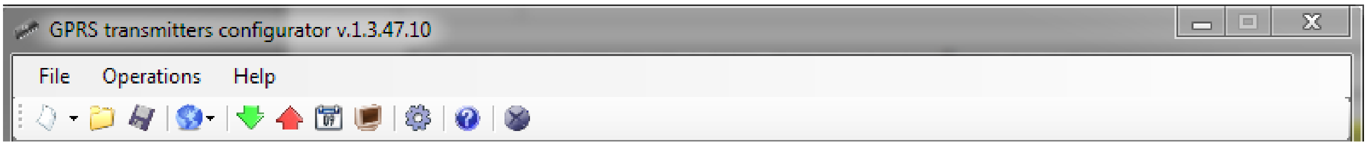
- Operating system: Windows 2000, Windows XP, Windows Vista or Windows 7,
- .NET Framework 2.0 software (delivered with a configuration installation wizard).

5.3. PROGRAM FUNCTONS

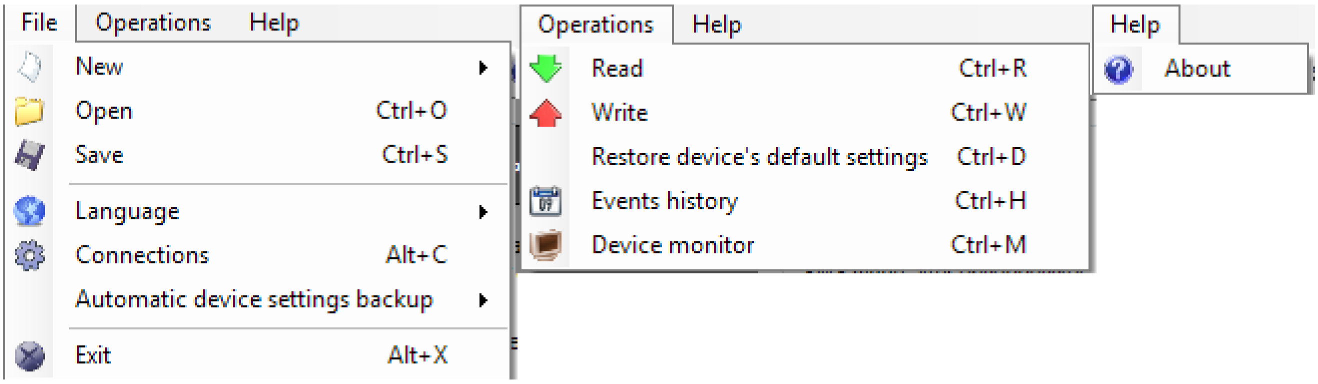
After the program is installed and started, the main window will be displayed on the screen. From that level you can access both, program functions and programmable parameters (see chapter 6.).

The main program window was divided into a few areas.

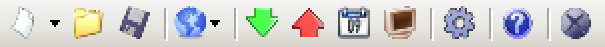
Main menu: located in the top section of the window, contains control and program configuration functions.



The main menu is composed of the following:



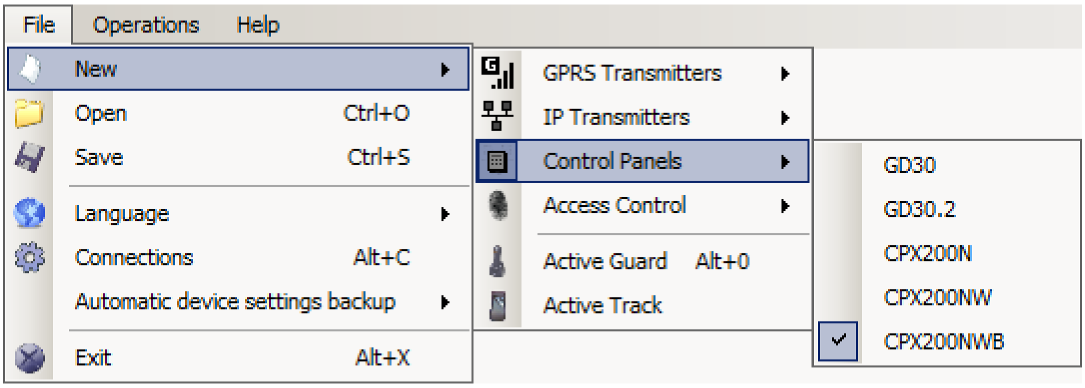
Main menu is also reflected in the visual form of icons on a taskbar:



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: CPX220NWB

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

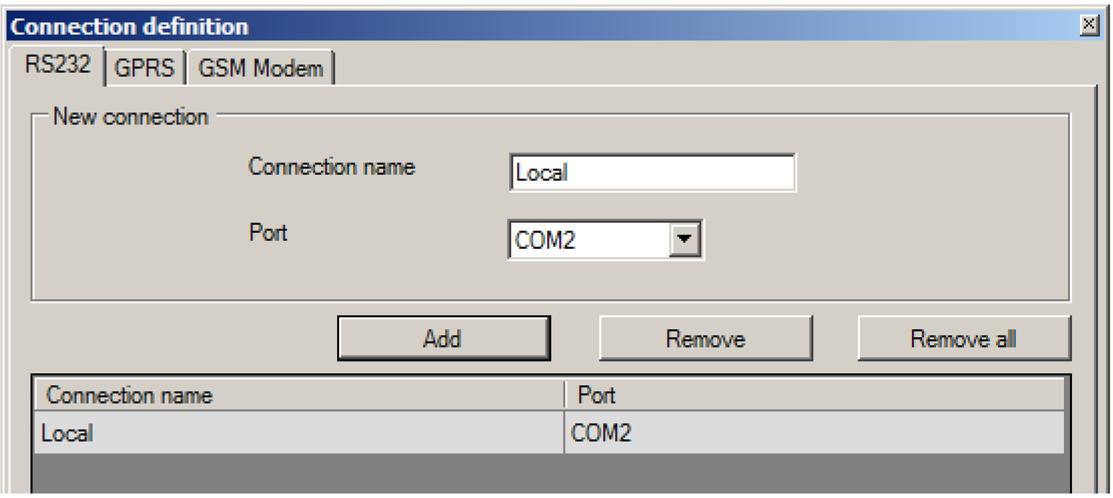
Before you start the equipment programming, define the type of connection to be used.

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 unit. The connection is executed through a dedicated programming cable using RS-232 serial port.

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.



New connection

Connection name: Local

Port: COM2

Connection name	Port
Local	COM2

For the above purpose you shall use the above window, available after activating File option from the Main Menu and selecting Connection function or after clicking ⚙ icon on a taskbar and opening RS-232 tab.

Define:

- Connection name, e.g. Local
- Select serial port, e.g. COM2

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.

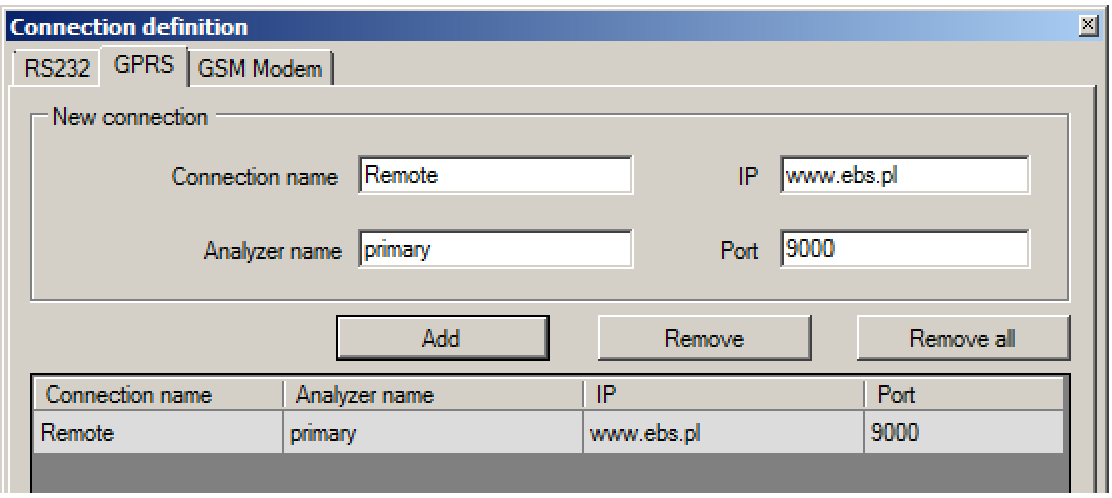
5.3.1.5.2. Remote connection

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
Remote	primary	www.ebs.pl	9000

Define:

- Connection name, e.g. Remote
- Select analyser name, e.g. primary
- Enter analyser name, e.g. www.ebs.pl
- Enter the port on which analyser 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.

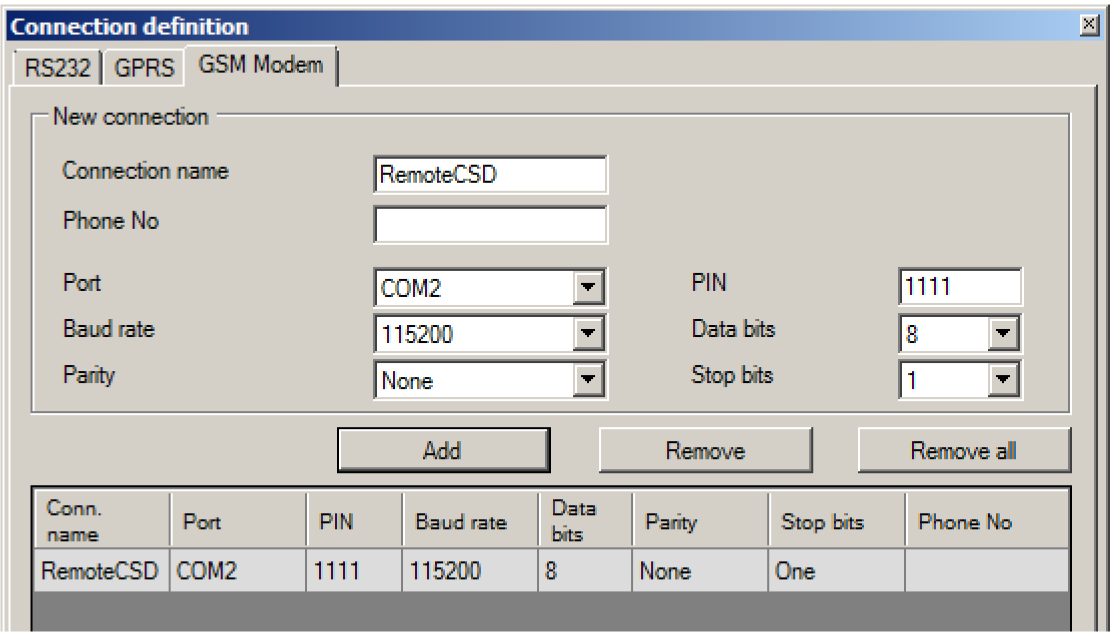
⚠ **NOTE: Such parameters as analyser's name, analyser's address, port refer to the settings of the OSM.2007 monitoring system receiver. Remote programming is available only in case the above mentioned equipment (software) is used.**

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. COM2)
- 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: COM2
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
RemoteCSD	COM2	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 unit must accept CSD connections – see item 6.7.1.2. Authorized GSM Modems Numbers.

Programming through CSD connection is possible also when OSM.2007 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.2007 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\CPX220NWB_20000\

CPX220NWB_20000 directory contains all files related to programming the CPX220NWB 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

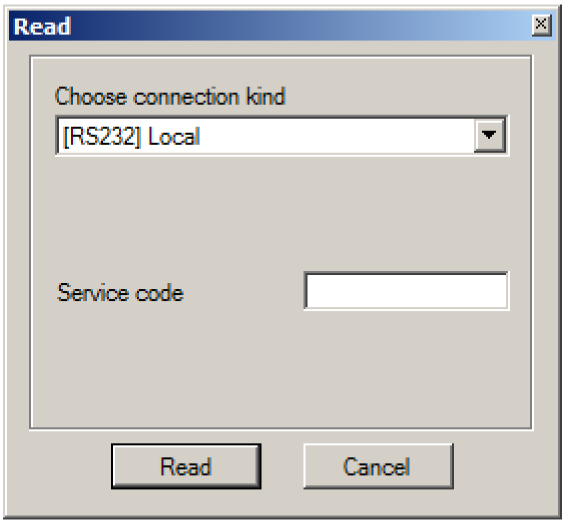
Ends the program operation.

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:



Choose connection kind
[RS232] Local

where:

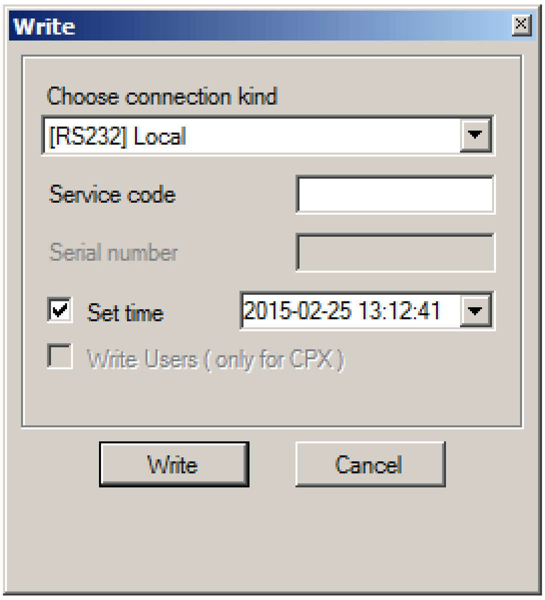
Connection – type of connection to the device.

Service 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.


Write

Choose connection kind: [RS232] Local

Service code:

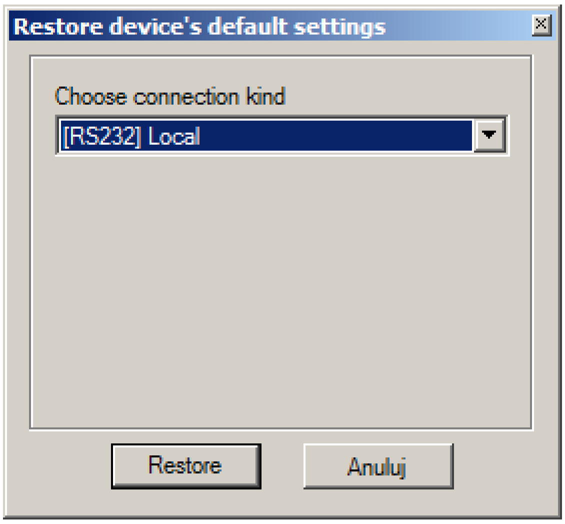
Serial number:

☑ Set time: 2015-02-25 13:12:41

□ Write Users (only for CPX)

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:


Restore device's default settings

Choose connection kind: [RS232] Local

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 GD-PROG service cable between CONF connector (on device's PCB) and computer's COM port, defined in Connections -> RS-232 option.
- Connect the power supply to the alarm control unit. 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 8).

⚠ **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 mode.
- 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.2007 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.2007 parameters. Since OSM.2007 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.2007 user manual.

5.4.2.1. First programming of the equipment

As no access parameters to GPRS network and OSM.2007 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.2007 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.2007 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.2007 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.

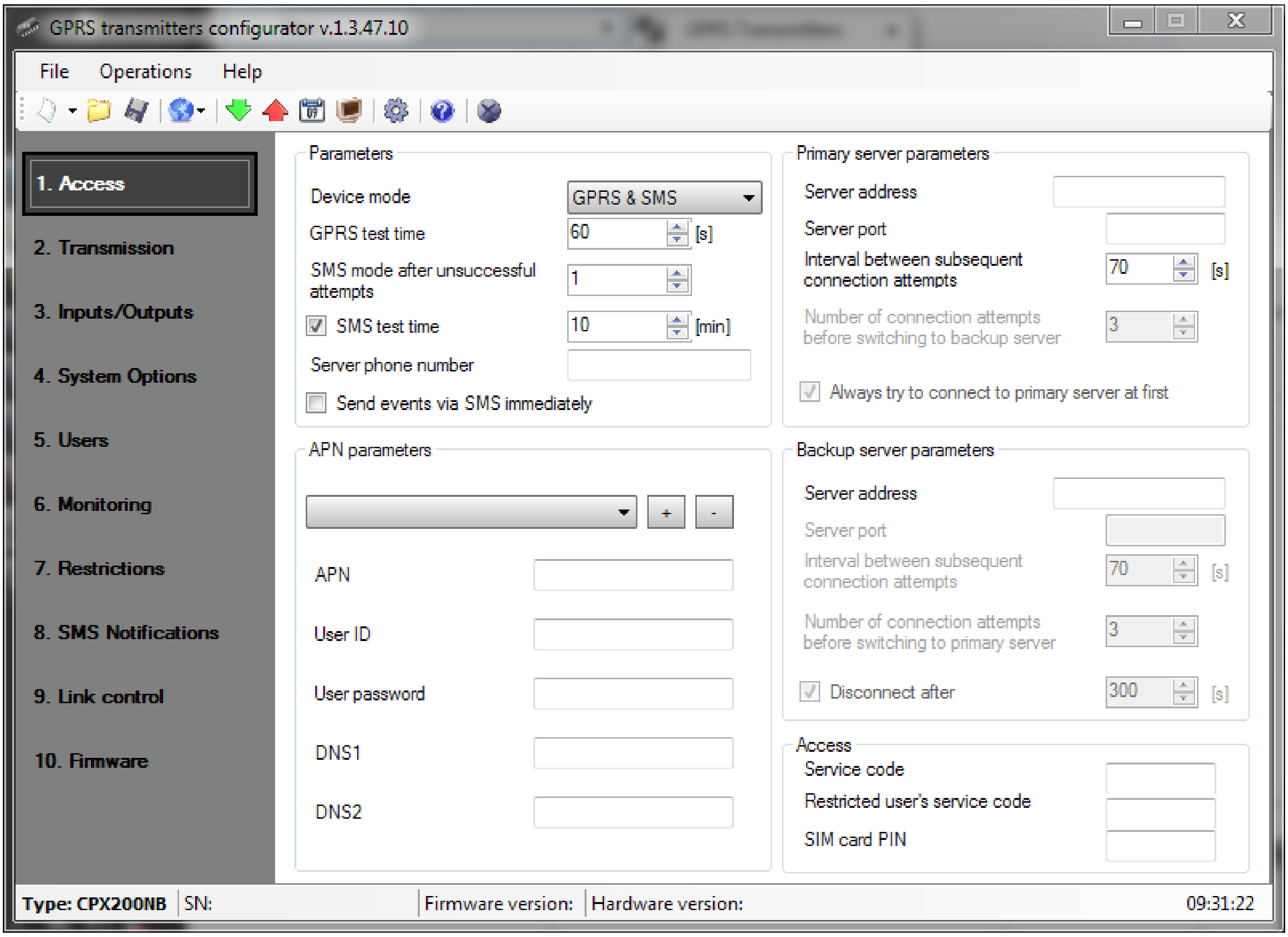
6.1. ACCESS

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: GPRS & SMS

GPRS test time: 60 [s]

SMS mode after unsuccessful attempts: 1

☑ SMS test time: 10 [min]

Server phone number:

□ Send events via SMS immediately

Primary server parameters

Server address:

Server port:

Interval between subsequent connection attempts: 70 [s]

Number of connection attempts before switching to backup server: 3

☑ Always try to connect to primary server at first

APN parameters

APN:

User ID:

User password:

DNS1:

DNS2:

Backup server parameters

Server address:

Server port:

Interval between subsequent connection attempts: 70 [s]

Number of connection attempts before switching to primary server: 3

☑ Disconnect after: 300 [s]

Access

Service code:

Restricted user's service code:

SIM card PIN:

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:31:22

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.2007) 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 0 is entered, the equipment 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 Name

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.2007) 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.2007) 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’s code

Installer’s code is used for equipment programming process using KP16 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.2007 Console or by sending SMS message. In case of reading Installer’s code via OSM.2007 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.2007 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.

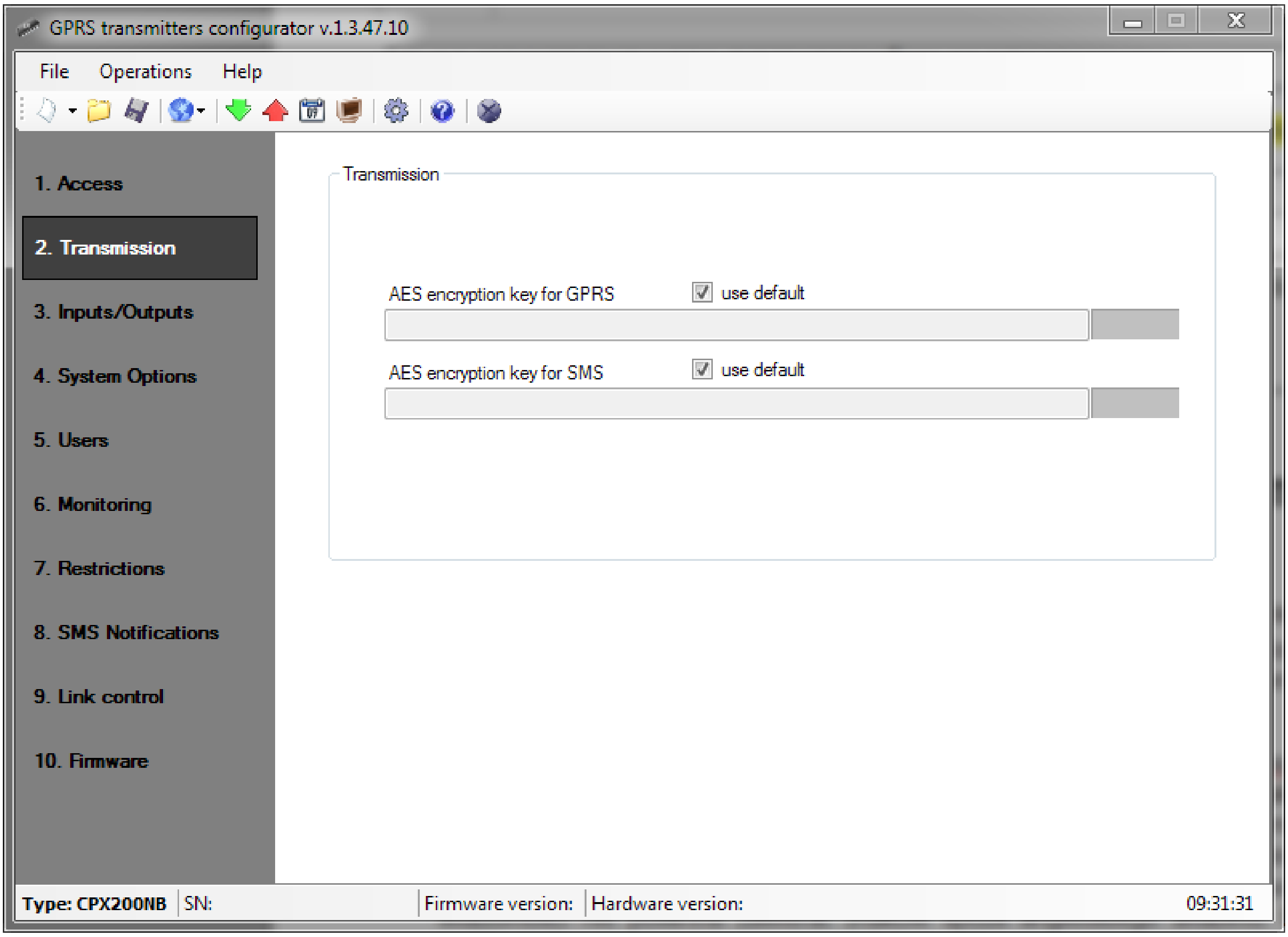
If you enter incorrect PIN code, the system will not start after inserting the card and switching the power supply on and you will not be able to use the card until you enter the PUK code (using any GSM phone).

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

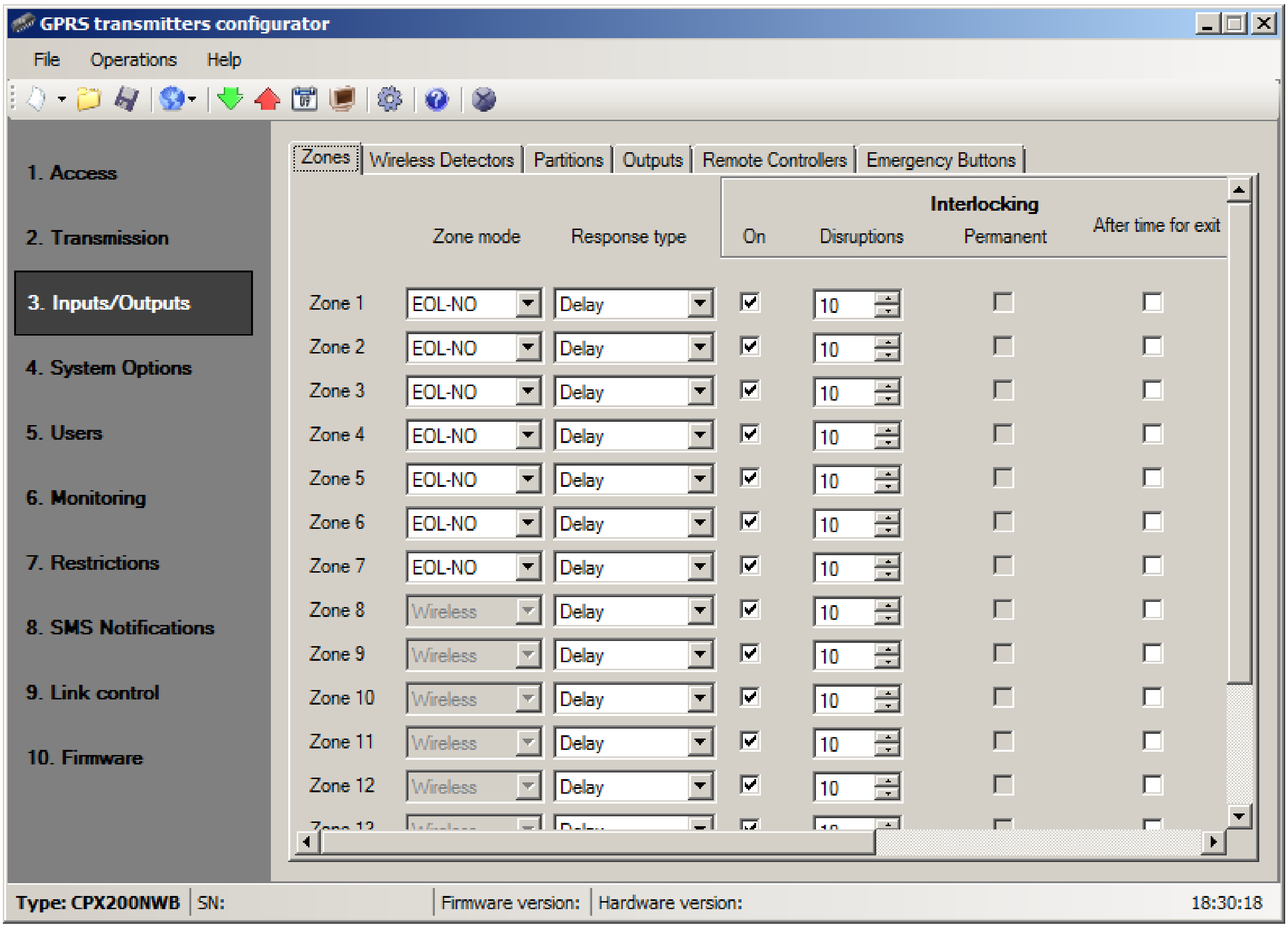
AES encryption key for SMS ☑ use default

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:31:31

6.3. INPUTS / OUTPUTS

The alarm control unit has 16 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



	Zone mode	Response type	Interlocking			After time for exit
			On	Disruptions	Permanent	
Zone 1	EOL-NO	Delay	☑	10	□	□
Zone 2	EOL-NO	Delay	☑	10	□	□
Zone 3	EOL-NO	Delay	☑	10	□	□
Zone 4	EOL-NO	Delay	☑	10	□	□
Zone 5	EOL-NO	Delay	☑	10	□	□
Zone 6	EOL-NO	Delay	☑	10	□	□
Zone 7	EOL-NO	Delay	☑	10	□	□
Zone 8	Wireless	Delay	☑	10	□	□
Zone 9	Wireless	Delay	☑	10	□	□
Zone 10	Wireless	Delay	☑	10	□	□
Zone 11	Wireless	Delay	☑	10	□	□
Zone 12	Wireless	Delay	☑	10	□	□

Type: CPX200NWB | SN: | Firmware version: | Hardware version: | 18:30:18

6.3.1.1. Zone mode

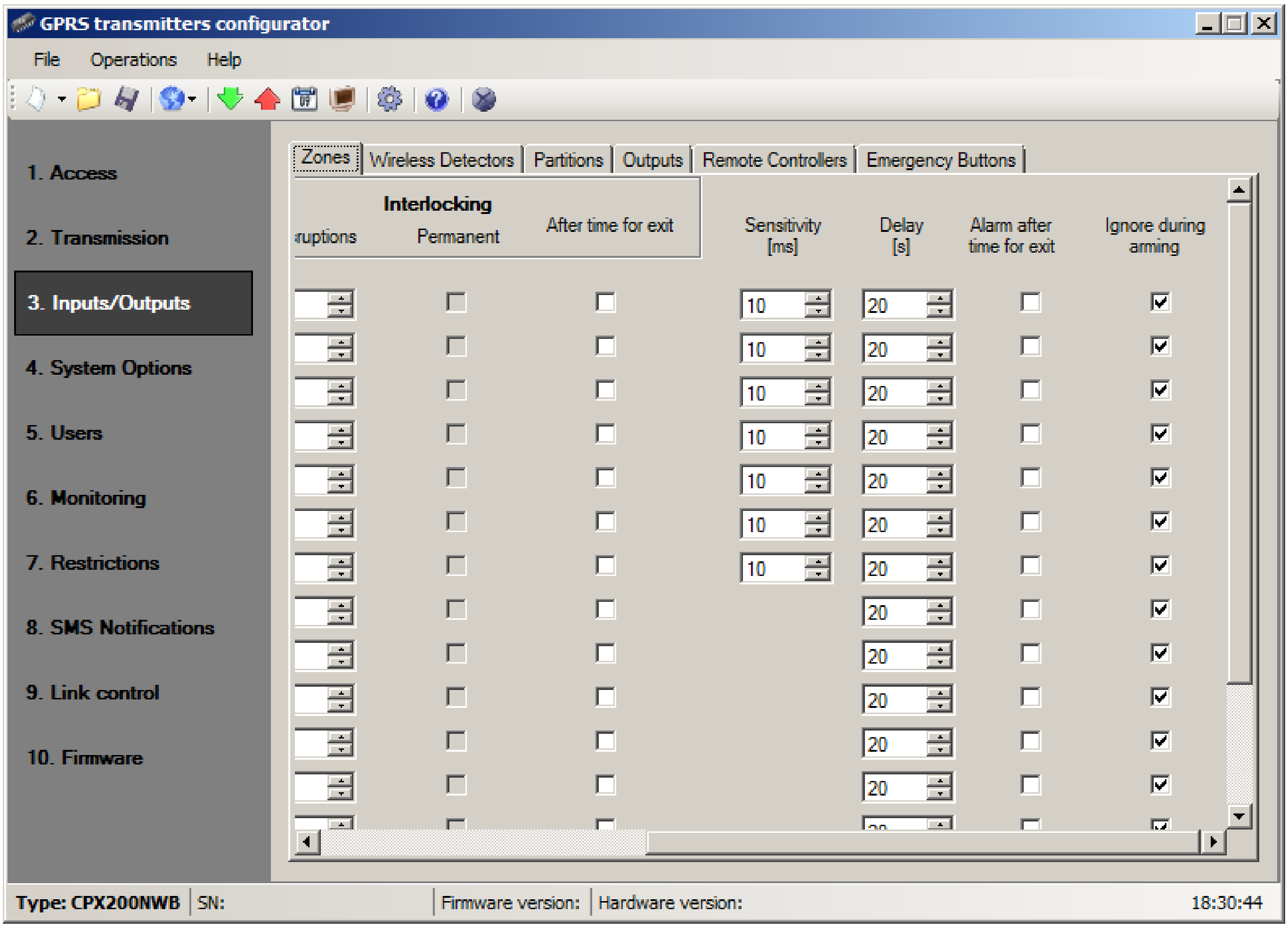
The parameter allows for determining the stable input line state. Any change of that state causes alarm message to be sent. Wired input can be NO or NC type. The following configuration types are available: NO / NC / EOL-NO / EOL-NC / DEOL-NO / DEOL-NC / Wireless. NC type input must be closed for the whole time. Line 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. Electric diagrams for all configuration types were described in chapter 3.4.

6.3.1.2. Response type

- **Instant** – disruption of the line causes immediate alarm, if the system is armed.
- **Delay** – that type of line is usually used for detectors operation at the facility entries. The line switches into alarm state after the expiration of programmed

time for entry. If the system is armed, the line 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 line causes immediate alarm irrespectively of whether the system is armed or not.
- **Arming/disarming** – the line can be used for arming or disarming the system. In case the line is activated with the system disarmed, the partition assigned to the line is armed. In case the line is activated with the system armed, the partition assigned to the line is disarmed.
- **24h tamper** – the line 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 line 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 line is treated as delay line. If not, the lien is treated as instant line.
- **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 immidiately after arm command. Violation of this zone will raise the alarm, even during the exit time countdown.
- **Perimeter exit** – Violating this zones during exit time countdown will arm the system in the away mode. If this is not violated during exit time countdown, partition will be armed in the stay mode. If the system is armed, this zone behaves like the delayed zone.



	Interlocking					
ruptions	Permanent	After time for exit	Sensitivity [ms]	Delay [s]	Alarm after time for exit	Ignore during arming
	☐	☐	10	20	☐	☑
	☐	☐	10	20	☐	☑
	☐	☐	10	20	☐	☑
	☐	☐	10	20	☐	☑
	☐	☐	10	20	☐	☑
	☐	☐	10	20	☐	☑
	☐	☐	10	20	☐	☑
	☐	☐		20	☐	☑
	☐	☐		20	☐	☑
	☐	☐		20	☐	☑
	☐	☐		20	☐	☑
	☐	☐		20	☐	☑

Type: CPX200NWB | SN: | Firmware version: | Hardware version: | 18:30:44

6.3.1.3. Interlocking

The option allows interlocking any input line, 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 line will be blocked if the line was violated when arming. In this case, an event about blocked line will be generated, which allows to inform the monitoring station about the problem with the line. 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 line is set to "After time for exit" and is violated or sabotaged after the time for exit, then is automatically blocked (bypass is activated). User can unlock the input by use the function 50 # (block inputs).

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 line remains violated when the time to exit is up.

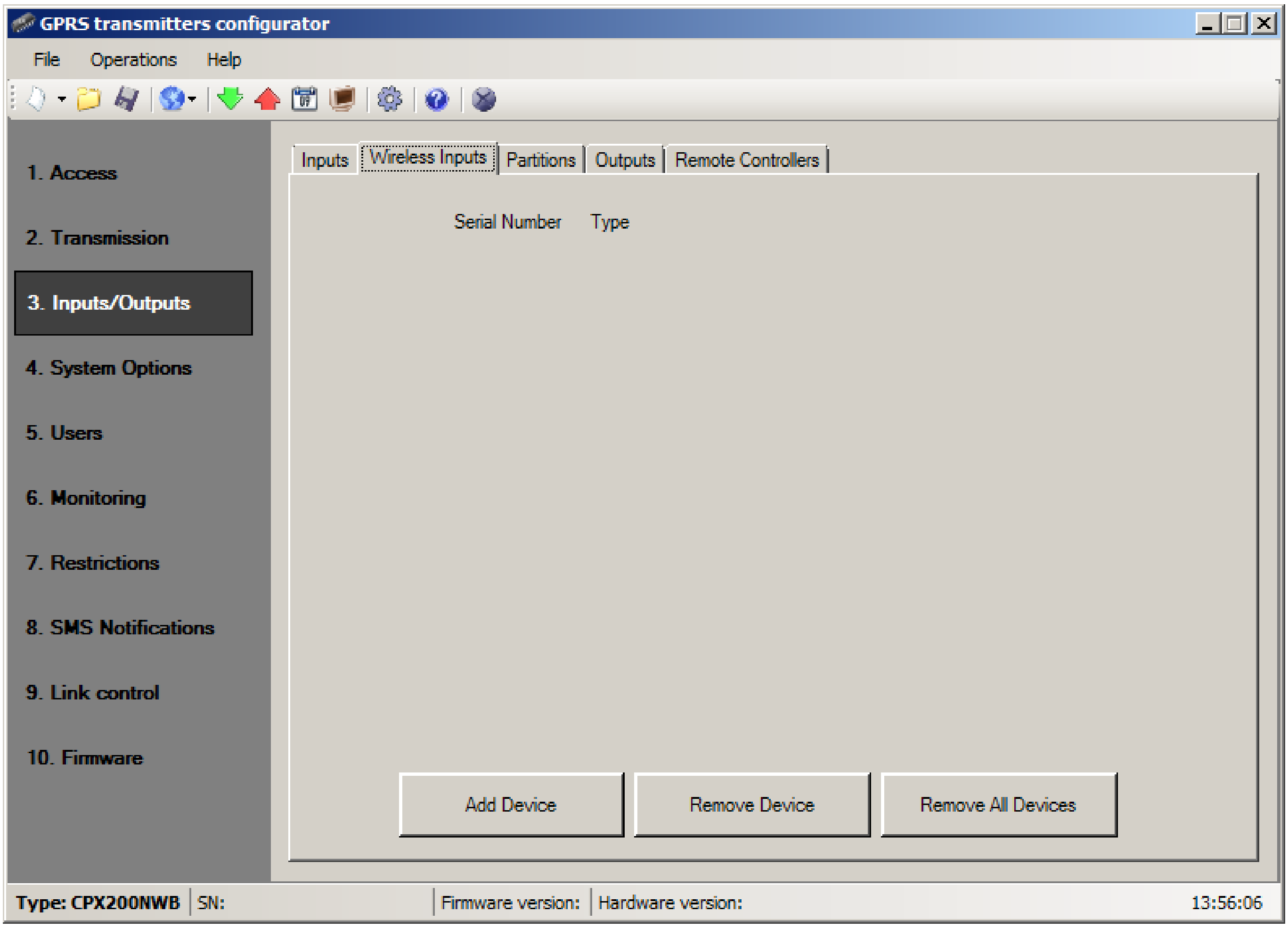
When deselected, alarm will NOT be generated in above case.

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

6.3.1.7. Ignore during arming

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

6.3.2. Wireless zones

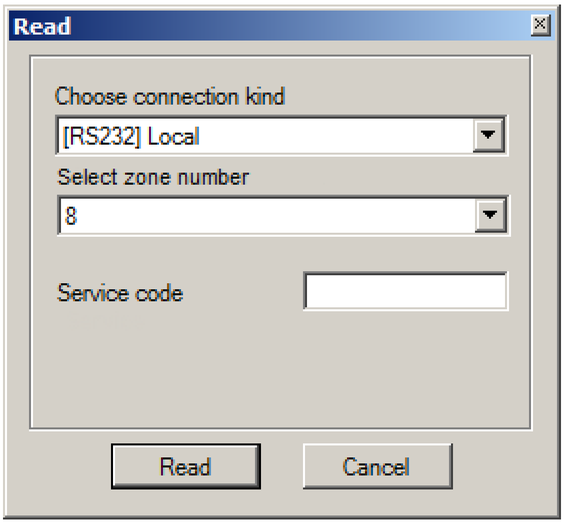


CPX220NWB is capable of storing information about up to 16 wirelles inputs number from 1 to 16.

Remove the front cover of the detector that you want to enroll to the control panel. 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.

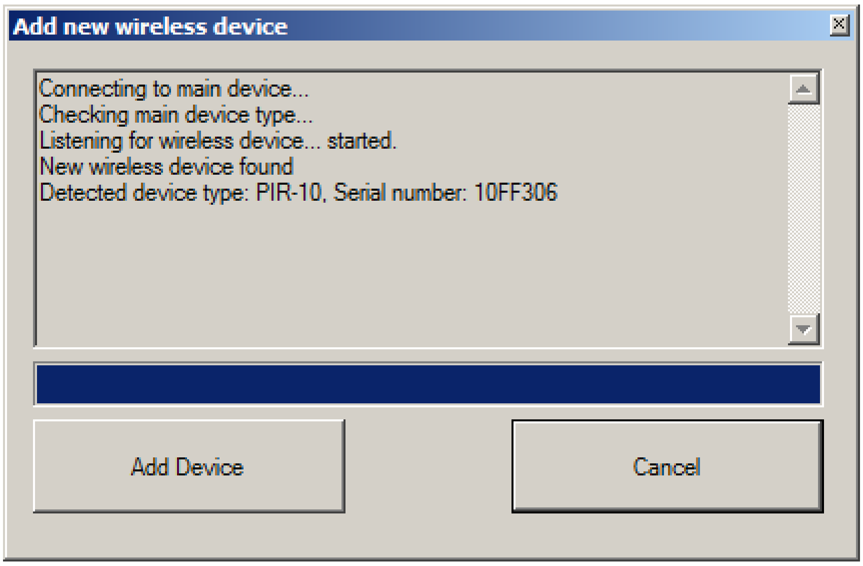
In order to add a wireless input, click *Add Device*. New window will appear, where proper connection has to be chosen (serial port number to which CPX220NWB is connected to) and service code has be typed in.

In new window, choose proper connection (serial port number to which CPX220NWB is connected to) and zone number for new device. Then enter service code and press Read button.



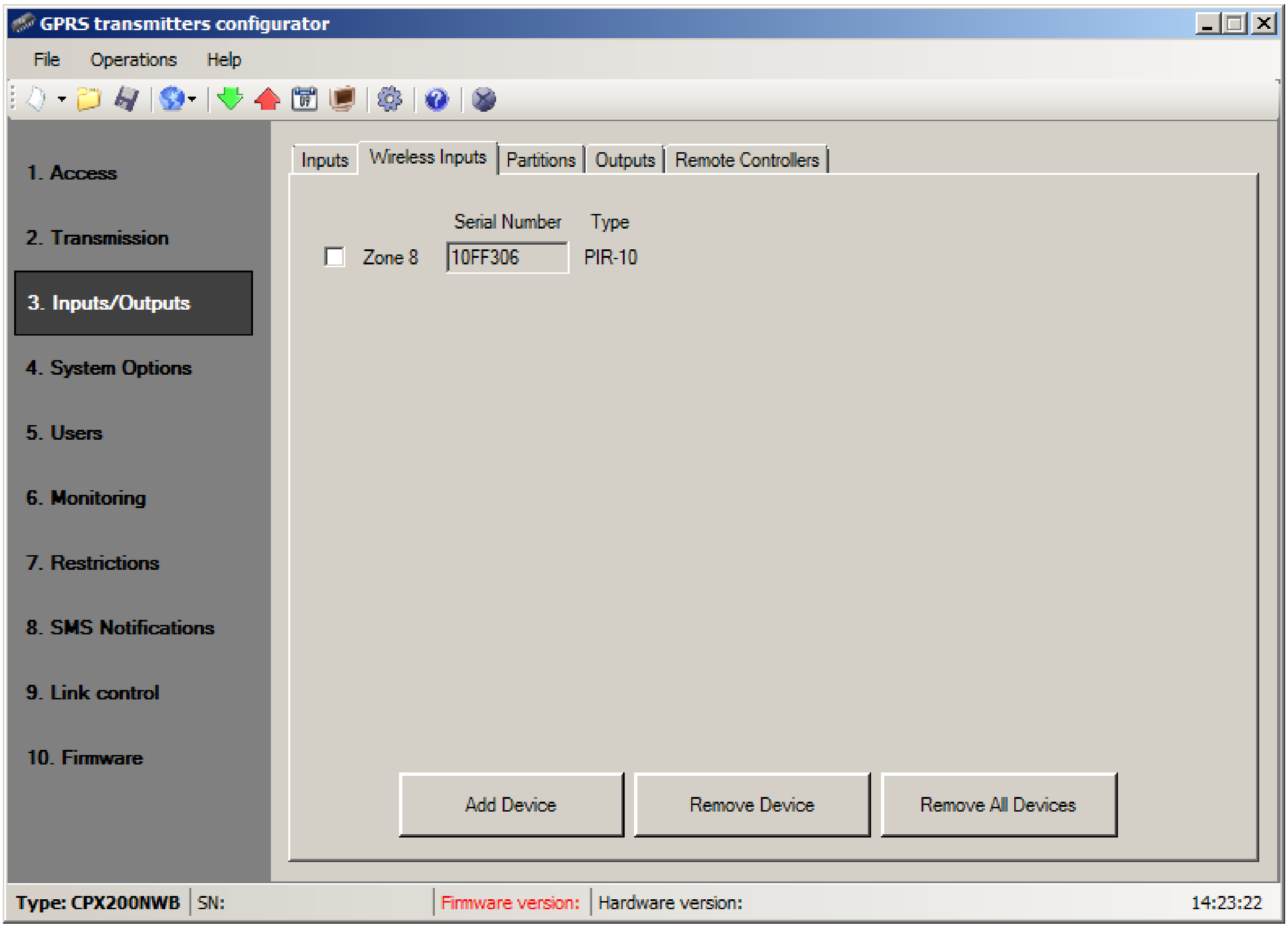
A new window appears.

Configurator will be waiting for a wirells signal to come. User has to press for a while the tamper switch on the sensor. CPX220NWB will detect the transmission and print sensor's type and ID.



```
Connecting to main device...
Checking main device type...
Listening for wireless device... started.
New wireless device found
Detected device type: PIR-10, Serial number: 10FF306
```

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

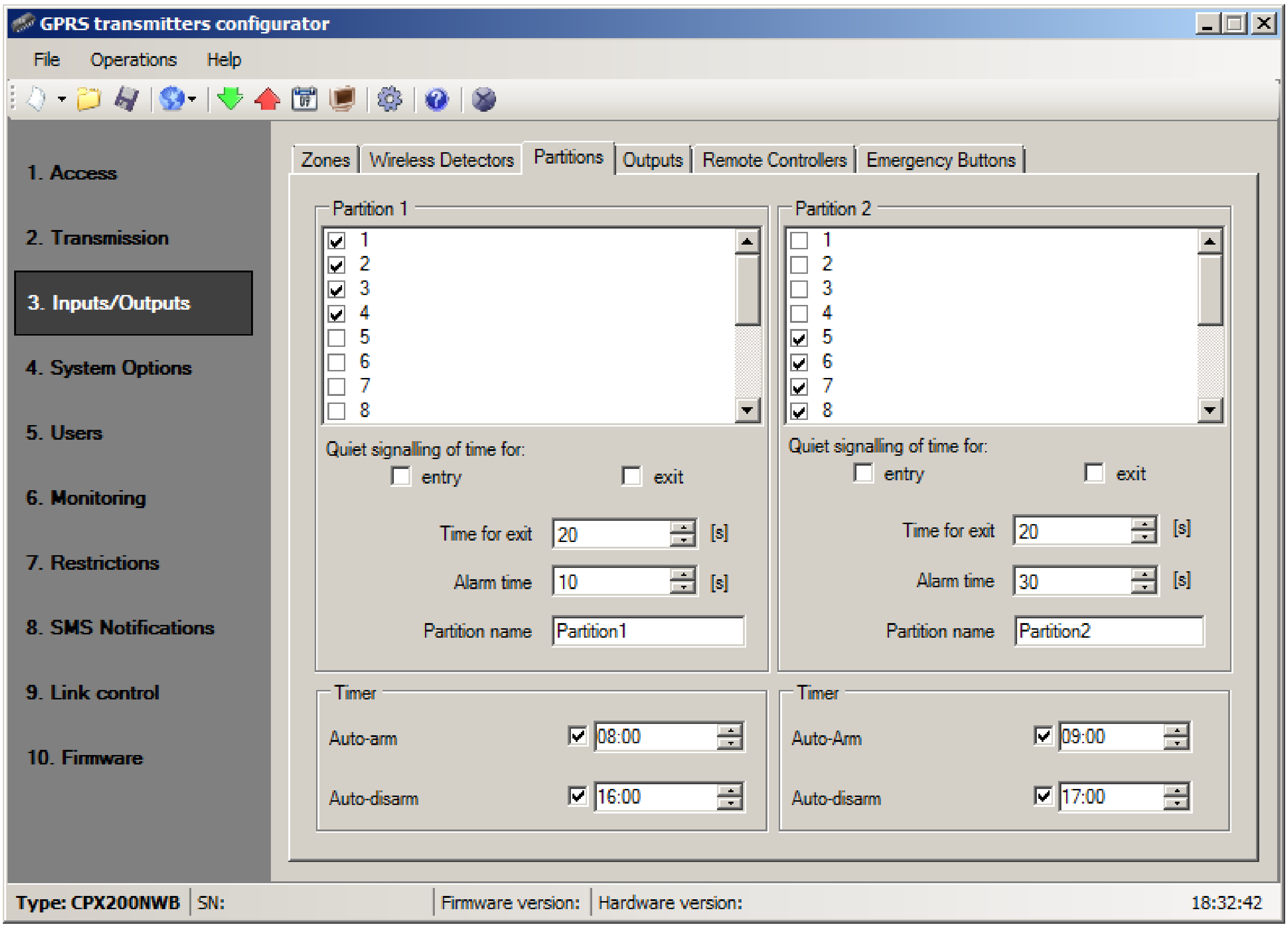


		Serial Number	Type
□	Zone 8	10FF306	PIR-10

Type: CPX200NWB | SN: | Firmware version: | Hardware version: | 14:23:22

Sensor preferences can be set now in the Inputs tab. You can choose the same options as for wired zones excluding sensitivity.

6.3.3. Partitions



Partition 1

☑ 1
☑ 2
☑ 3
☑ 4
□ 5
□ 6
□ 7
□ 8

Quiet signalling of time for:
□ entry □ exit

Time for exit 20 [s]

Alarm time 10 [s]

Partition name Partition1

Partition 2

□ 1
□ 2
□ 3
□ 4
☑ 5
☑ 6
☑ 7
☑ 8

Quiet signalling of time for:
□ entry □ exit

Time for exit 20 [s]

Alarm time 30 [s]

Partition name Partition2

Timer

Auto-arm ☑ 08:00

Auto-disarm ☑ 16:00

Timer

Auto-Arm ☑ 09:00

Auto-disarm ☑ 17:00

Type: CPX200NWB | SN: | Firmware version: | Hardware version: | 18:32:42

6.3.3.1. Partittion 1 / 2

In that tab you can assign the zones from 1 to 16 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 KP16 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 KP16 keypad.

6.3.3.5. Partition name

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

6.3.3.6. Alarm time

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 line 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).

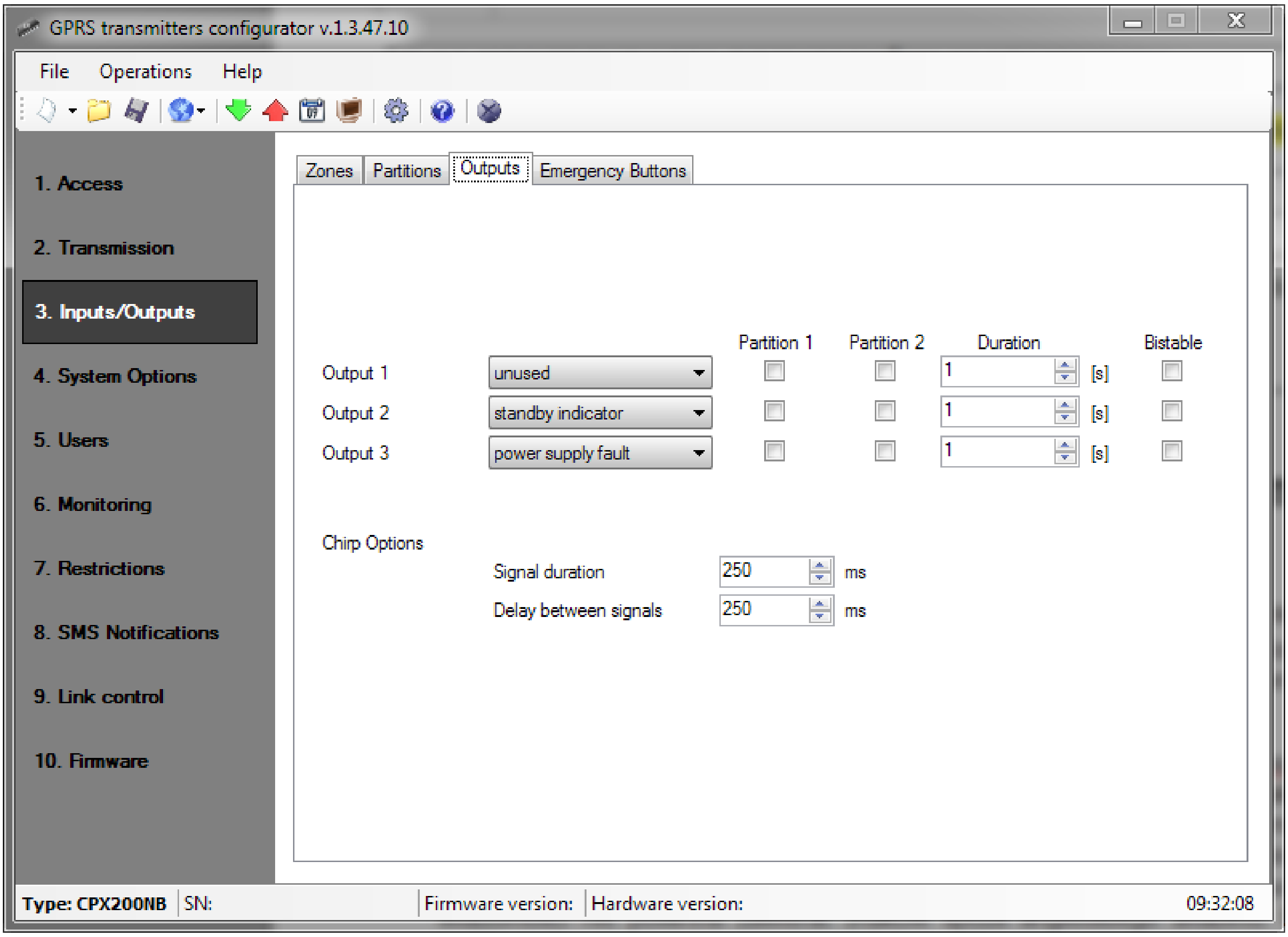
When set to the same time arming and disarming, the system will first be disarmed and then immediately armed.

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.

NOTE: To use the auto-arming/disarming function, you should do a firmware upgrade to version 2.4.7 or higher, then read and write the configuration of the device using "GPRS transmitters configurator" program in version 1.3.57.3 or higher.

6.3.4. Outputs



		Partition 1	Partition 2	Duration		Bistable
Output 1	unused	□	□	1	[s]	□
Output 2	standby indicator	□	□	1	[s]	□
Output 3	power supply fault	□	□	1	[s]	□

Chirp Options

Signal duration 250 ms

Delay between signals 250 ms

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:32:08

6.3.4.1. Outputs 1 / 2 / 3

Types of outputs:

- **Unused** – Output is inactive.
- **Alarm** – Output is activated when alarm is detected.
- **Standby indicator** – Output is activated when any of the assigned partitions is 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 / 2

The parameter allows assigning particular monitoring partitions to outputs.

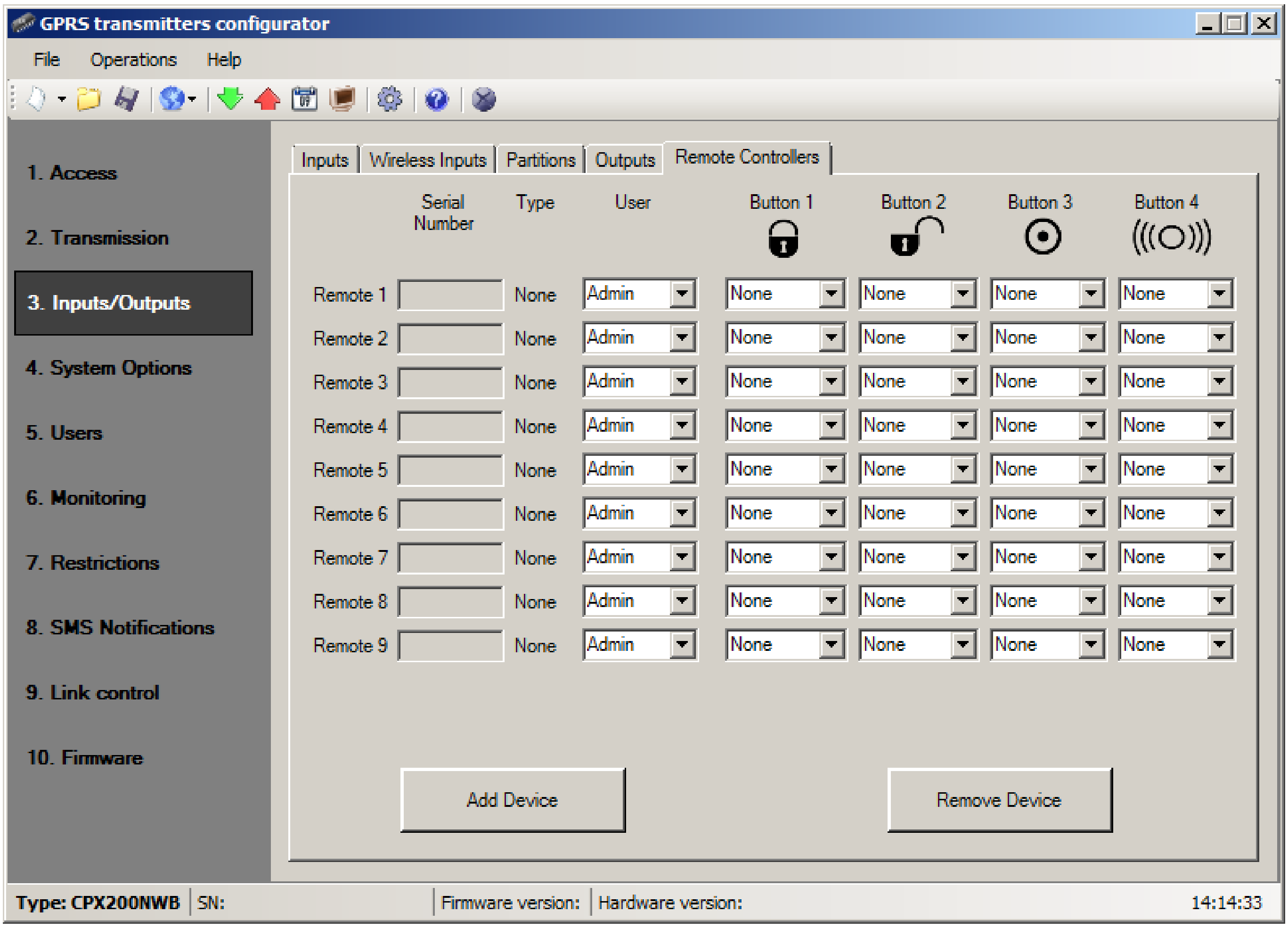
6.3.4.3. Activation time

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
Remote 1		None	Admin	None	None	None	None
Remote 2		None	Admin	None	None	None	None
Remote 3		None	Admin	None	None	None	None
Remote 4		None	Admin	None	None	None	None
Remote 5		None	Admin	None	None	None	None
Remote 6		None	Admin	None	None	None	None
Remote 7		None	Admin	None	None	None	None
Remote 8		None	Admin	None	None	None	None
Remote 9		None	Admin	None	None	None	None

Type: CPX200NWB | SN: | Firmware version: | Hardware version: | 14:14:33

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 controler, User has to select a row coressponding to desired remote controller and press the *Add Device* button. New window will appear, where necessary serial port configuration and service code parameteres have to be filled in. Pressing OK will invoke new window indicating, that CPX220NWB is waiting for incoming tranmisson from the remote controller. User has to press one of the controller button, in order to bind it with the Alarm Control Unit. 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 assinged to one of the previously added users (or administrator) – *User* column. Controller's buttons can be assigned to the actions of the Alarm Control Unit. 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* colums 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.

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

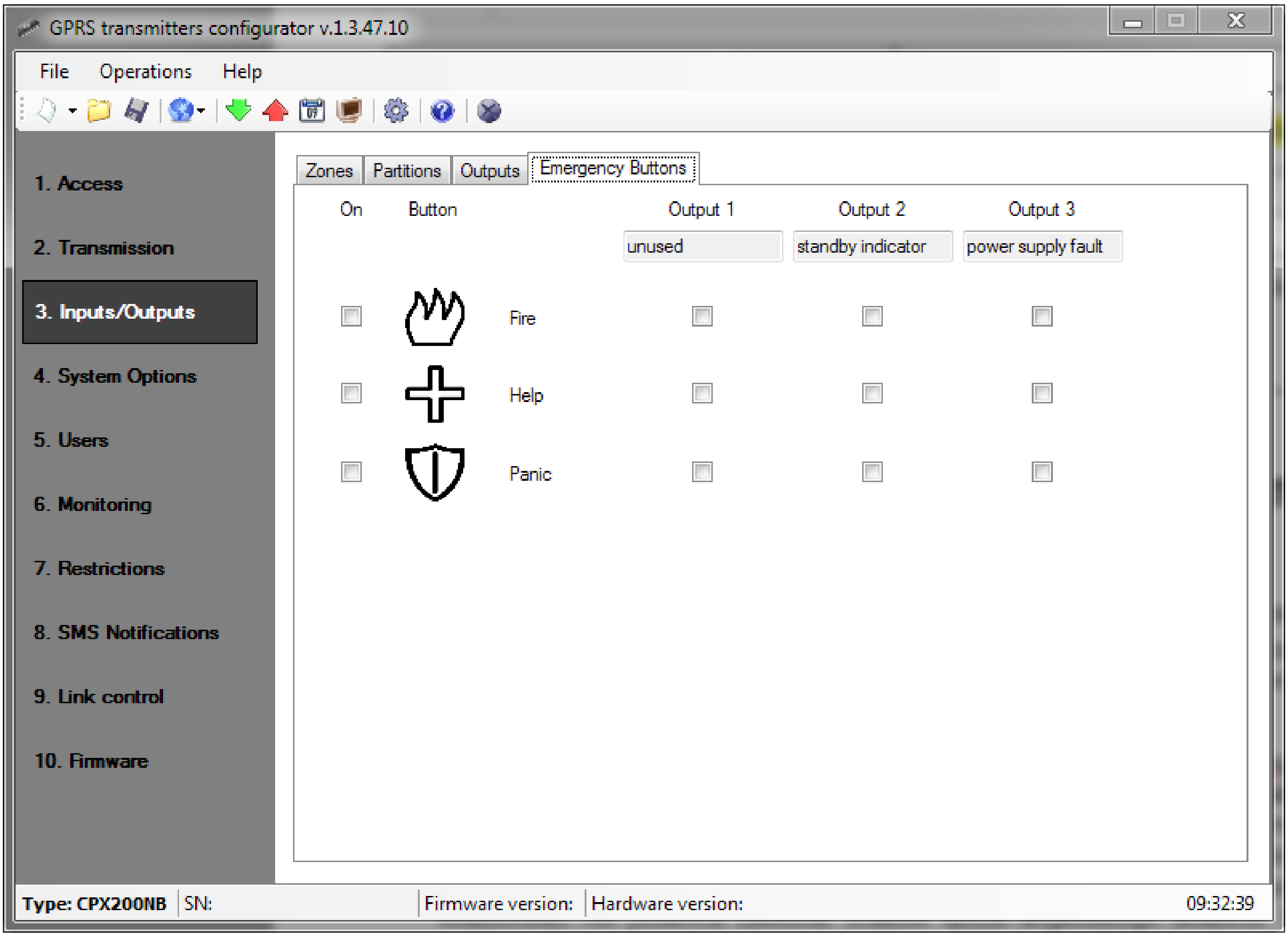
„Silent alarm" function is triggering an alarm without audible signal.

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

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

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

6.3.6. Emergency Buttons



On	Button		Output 1	Output 2	Output 3
			unused	standby indicator	power supply fault
□	🔥	Fire	□	□	□
□	✚	Help	□	□	□
□	🛡	Panic	□	□	□

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:32:39

6.3.6.1. Icons

🔥 ✚ 🛡 symbols match the [* 🔥] [✚ □] [🛡 #] function keys on the keypad. The "On" checkbox has to be checked in orded to enable the function key support.

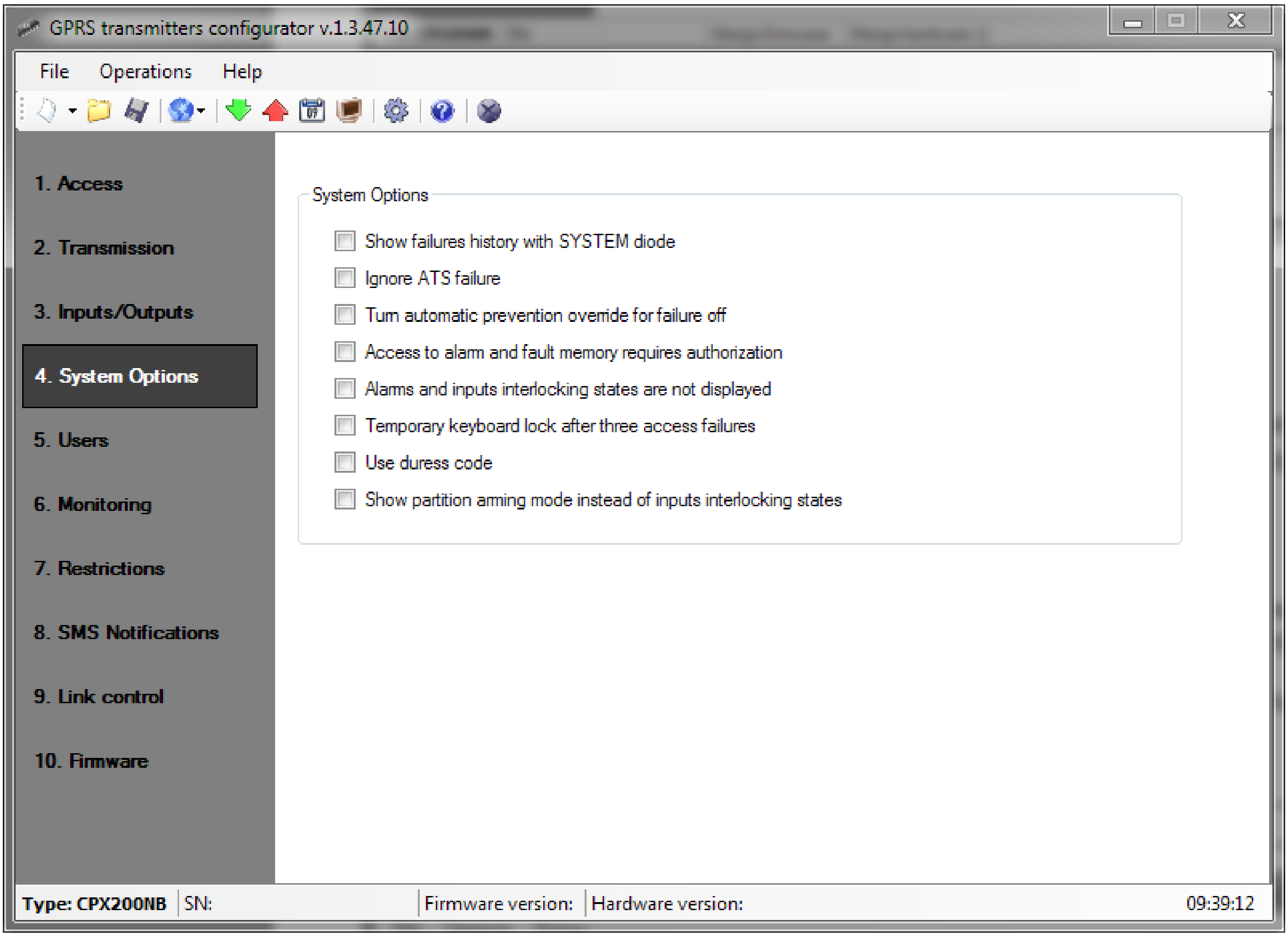
Events associated with emergency buttons will be transmitted to monitoring station only if they are enabled in the "Monitoring" tab (see item 6.6.).

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 outpus 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
- □ Turn automatic prevention override for failure off
- □ 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

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:39:12

6.4.1. Show failures history with SYSTEM diode

Selecting this option indicates that a fault occurred in the system and be completed. This condition will be indicated by flashing SYSTEM LED on the keyboard KP16 until cleared the fault memory.

6.4.2. Ignore ATS failure

Selecting this option turns off signaling a loss of communication with the server on KP16 keypad.

6.4.3. Turn automatic override for failure off

Selecting this option enables the system fault signal when arming.

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. Each user has his own duress code.

⚠ **NOTE: Firmware versions older than 2.1.0 do not support the duress code. Upgrading the Firmware to version 2.or newer one has to make sure that there are no conflicts between existing users and their duress codes.**

6.4.8. Show partition arming mode instead of inputs interlocking states

Show partition arming mode instead of inputs interlocking states. By default systerm will show violated and interlocked zones on diodes 1-16. Setting this option will tell the system to show partitoin armind mode on diodes 1-2. Zones states will no longer be available.

Display scheme:

Led off – partition disarmed

Led on – partition armed in away mode

Led blinking – partition armed in stay mode

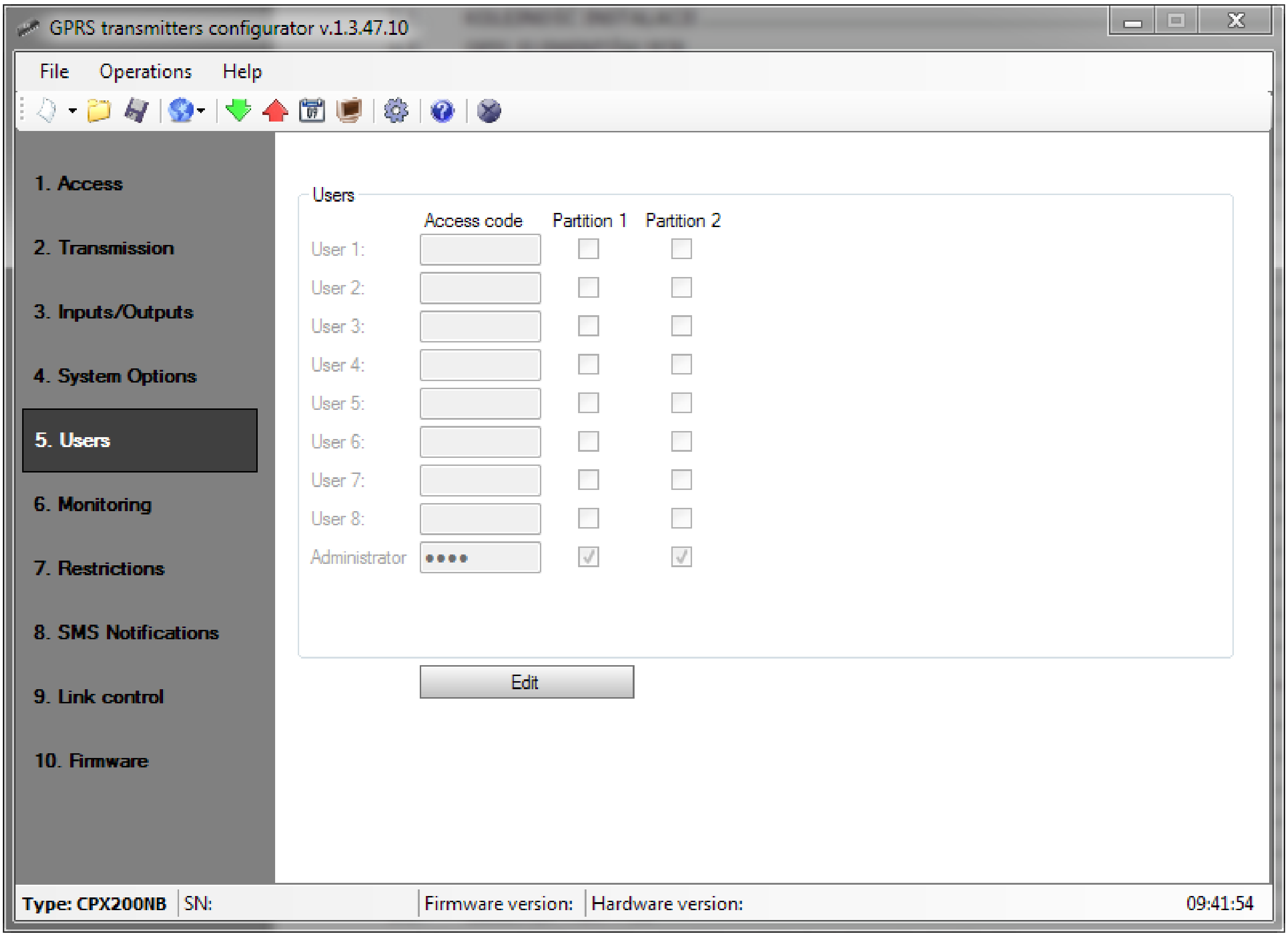
NOTE: this option is available only when "Alarms and inputs interlocking states are not displayed" option is inactive.

6.5. USERS

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 and partition priviliages.

After editing press the ‘Accept changes’ button, and then upload the configuration to the device. When uploading a configuration, "Write users" option must be selected in the writing options.

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



Users

	Access code	Partition 1	Partition 2
User 1:		□	□
User 2:		□	□
User 3:		□	□
User 4:		□	□
User 5:		□	□
User 6:		□	□
User 7:		□	□
User 8:		□	□
Administrator	••••	☑	☑

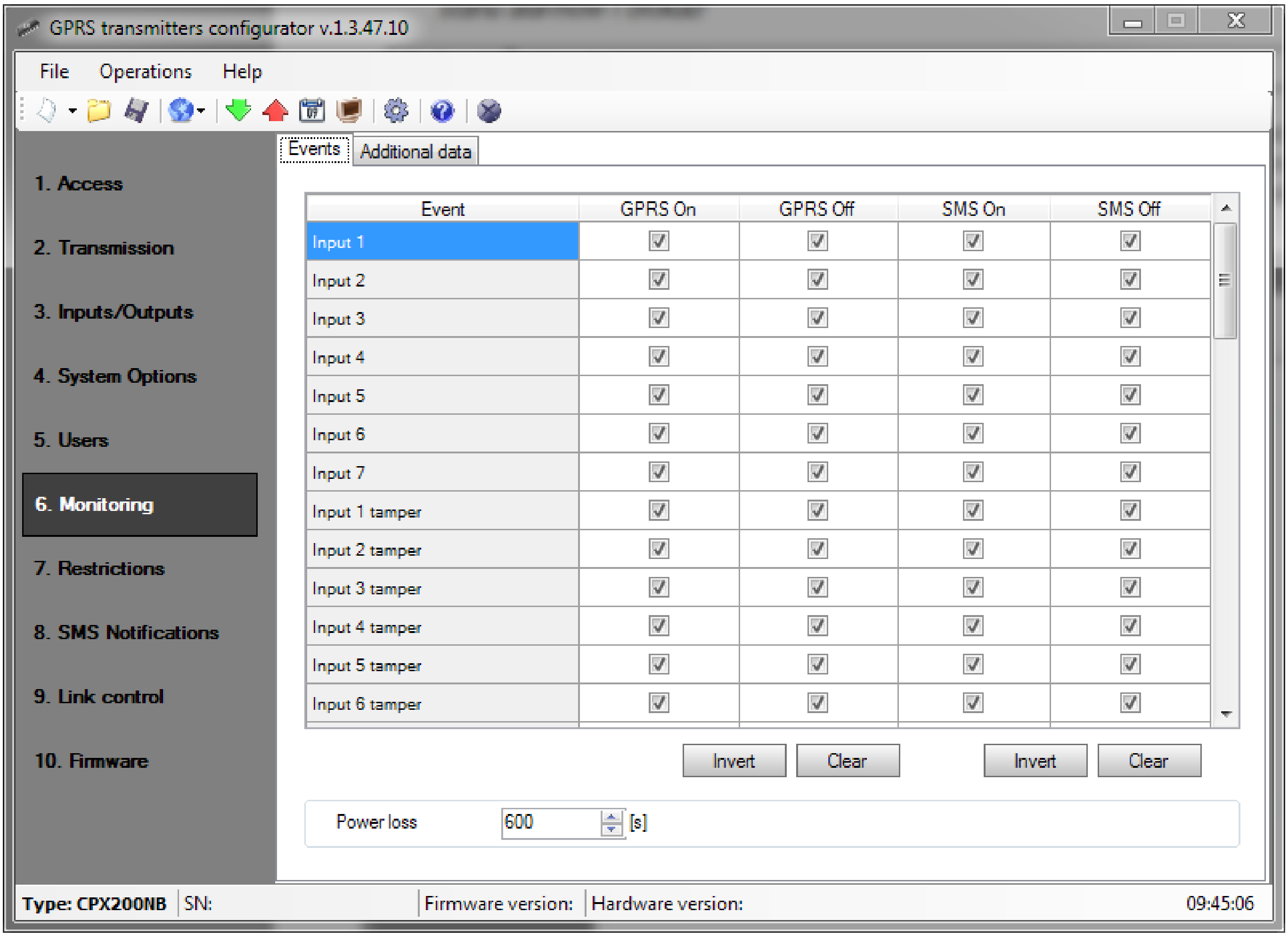
Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:41:54

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
Input 1	☑	☑	☑	☑
Input 2	☑	☑	☑	☑
Input 3	☑	☑	☑	☑
Input 4	☑	☑	☑	☑
Input 5	☑	☑	☑	☑
Input 6	☑	☑	☑	☑
Input 7	☑	☑	☑	☑
Input 1 tamper	☑	☑	☑	☑
Input 2 tamper	☑	☑	☑	☑
Input 3 tamper	☑	☑	☑	☑
Input 4 tamper	☑	☑	☑	☑
Input 5 tamper	☑	☑	☑	☑
Input 6 tamper	☑	☑	☑	☑

Power loss 600 [s]

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:45:06

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.

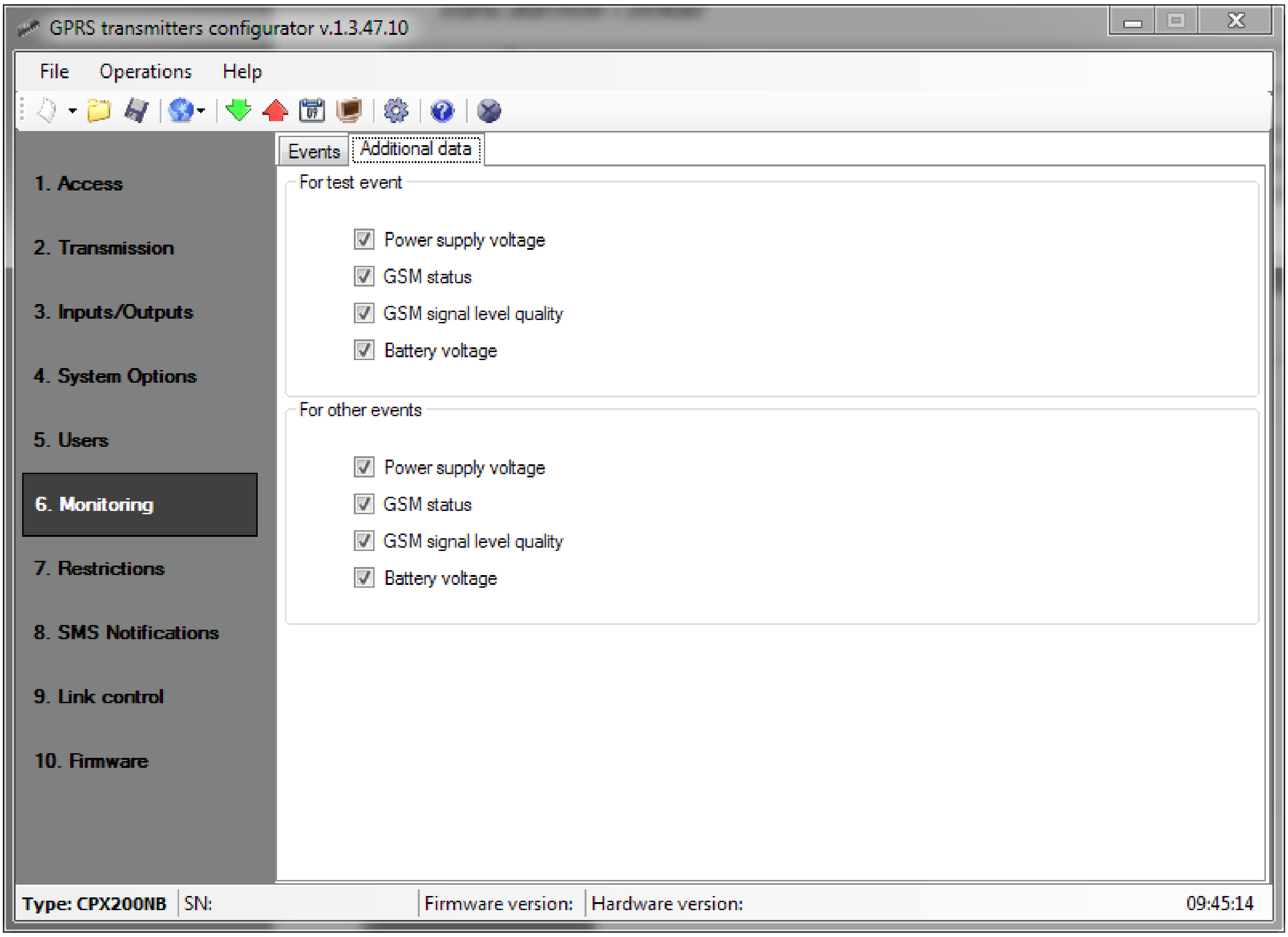
Press [Reverse] to reverse the check into the opposite ones.

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. 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.



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

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:45:14

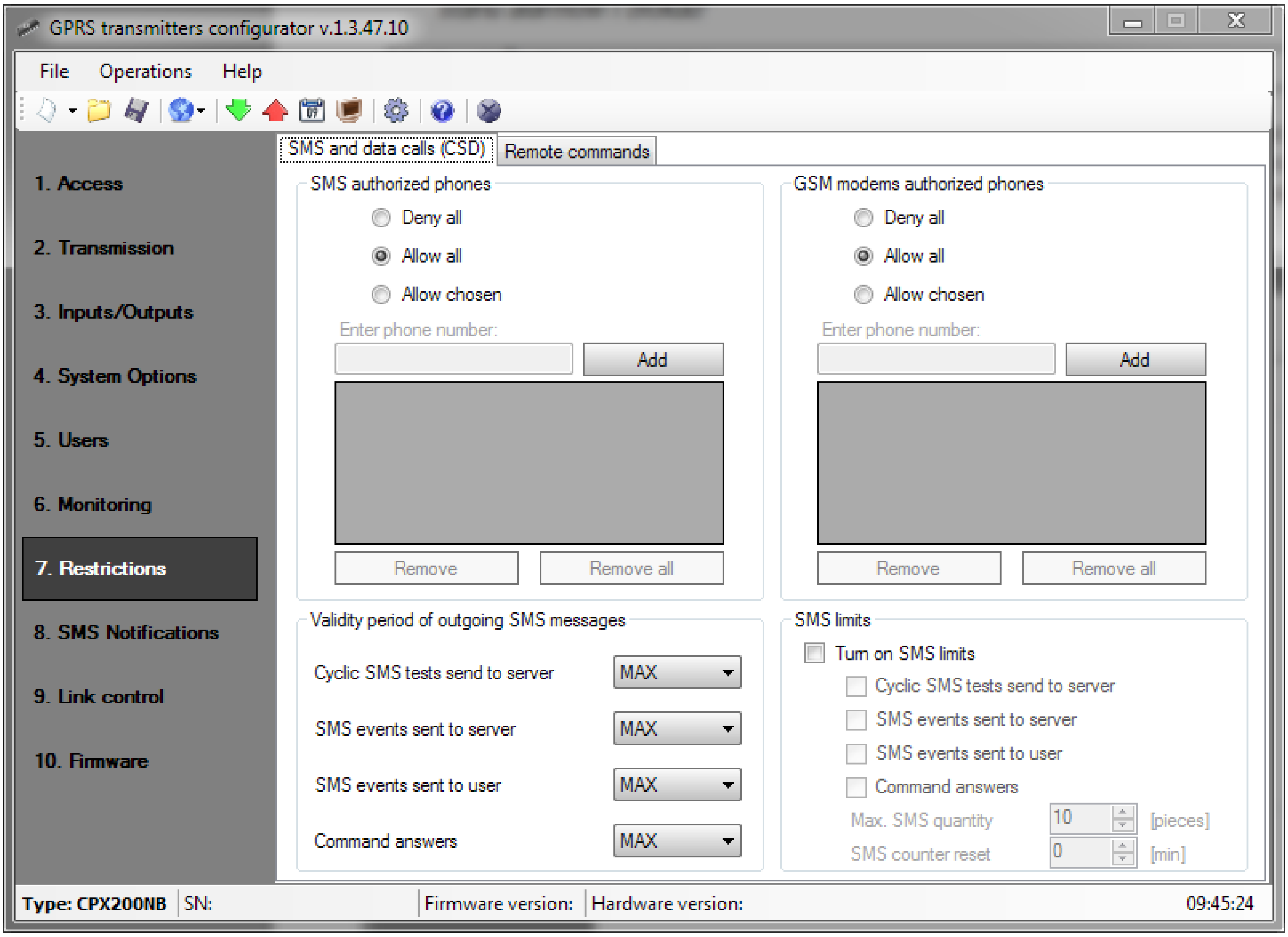
The adjustable parameters are:

- 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

6.7. 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: CPX200NB | SN: | Firmware version: | Hardware version: | 09:45:24

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 line 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. 600**1234**56 **or** 60**1234**567 **will be accepted.**

NOTE: If modem connected to OSM.2007 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 line 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. 600**1234**56 or 60**1234**567 **will be accepted**.

NOTE: If modem connected to OSM.2007 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).

6.7.1.4. 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.

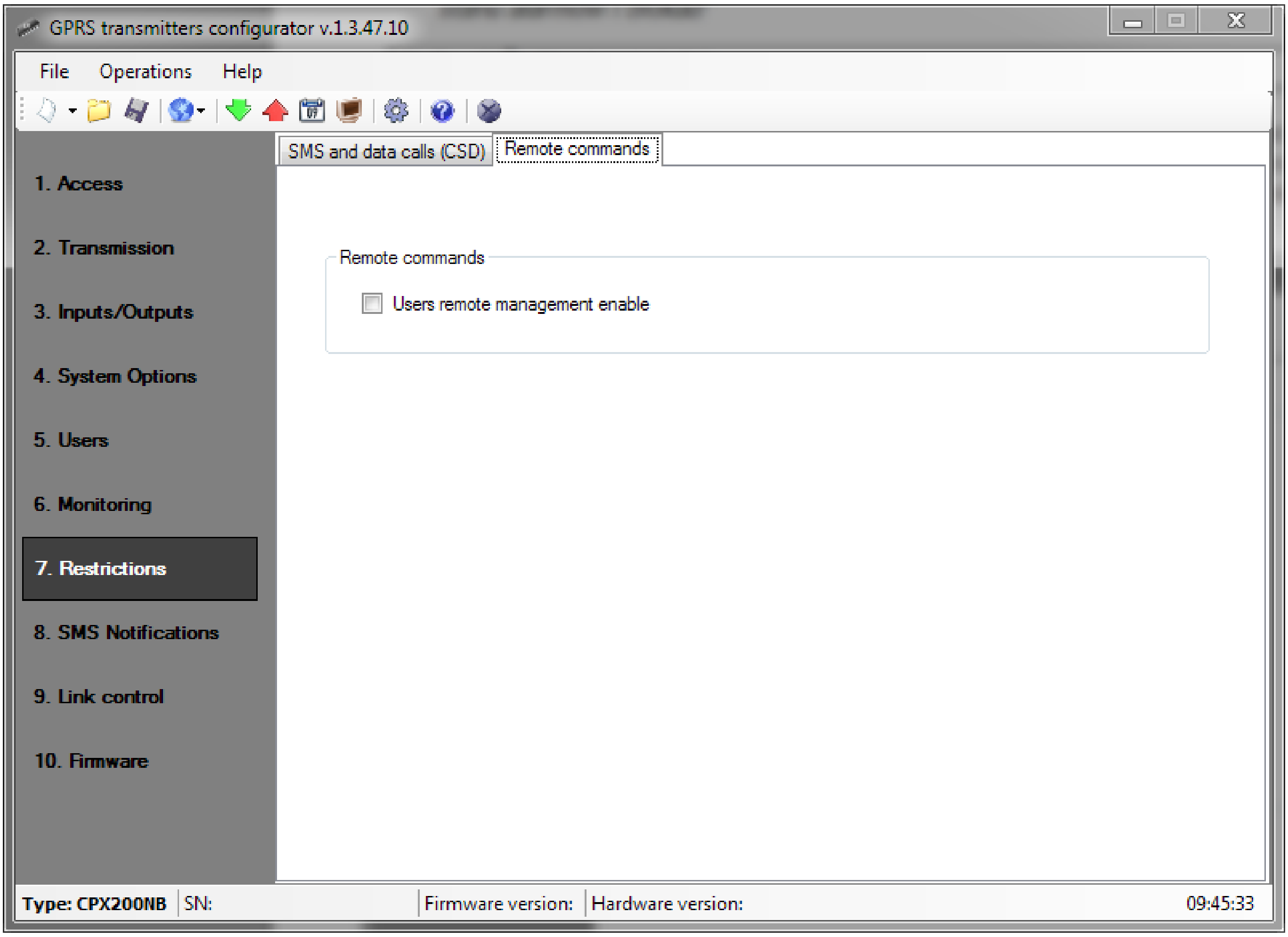
Check the [Activate SMS restrictions] check box to activate the access to information groups subject to restrictions:

- 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

6.7.2.1. Users remote management enable

Selecting this option allows you to remotely configure user accounts.



Remote commands

□ Users remote management enable

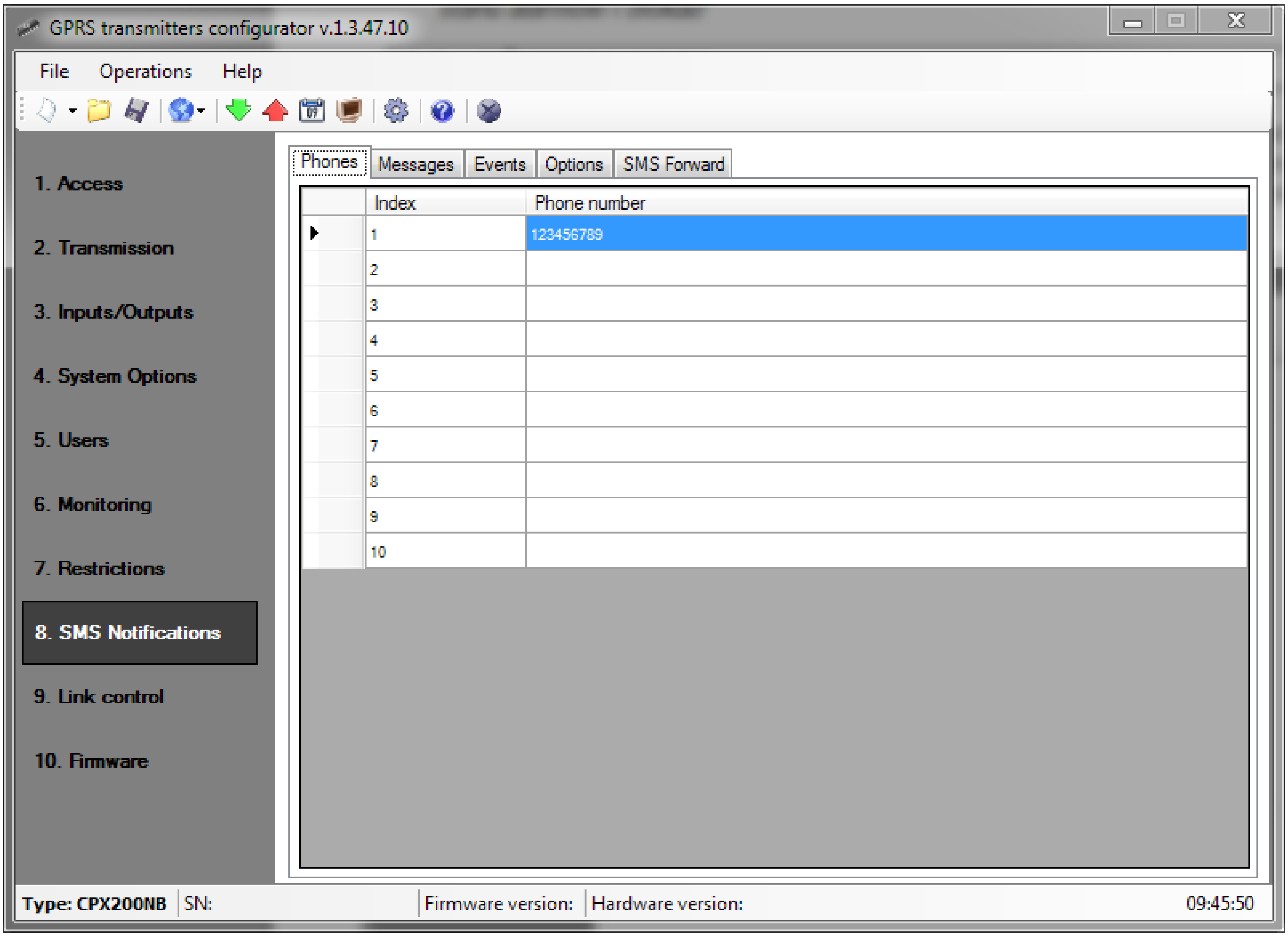
Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:45:33

6.8. SMS NOTIFICATIONS

6.8.1. Phones

CPX220NWB 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	

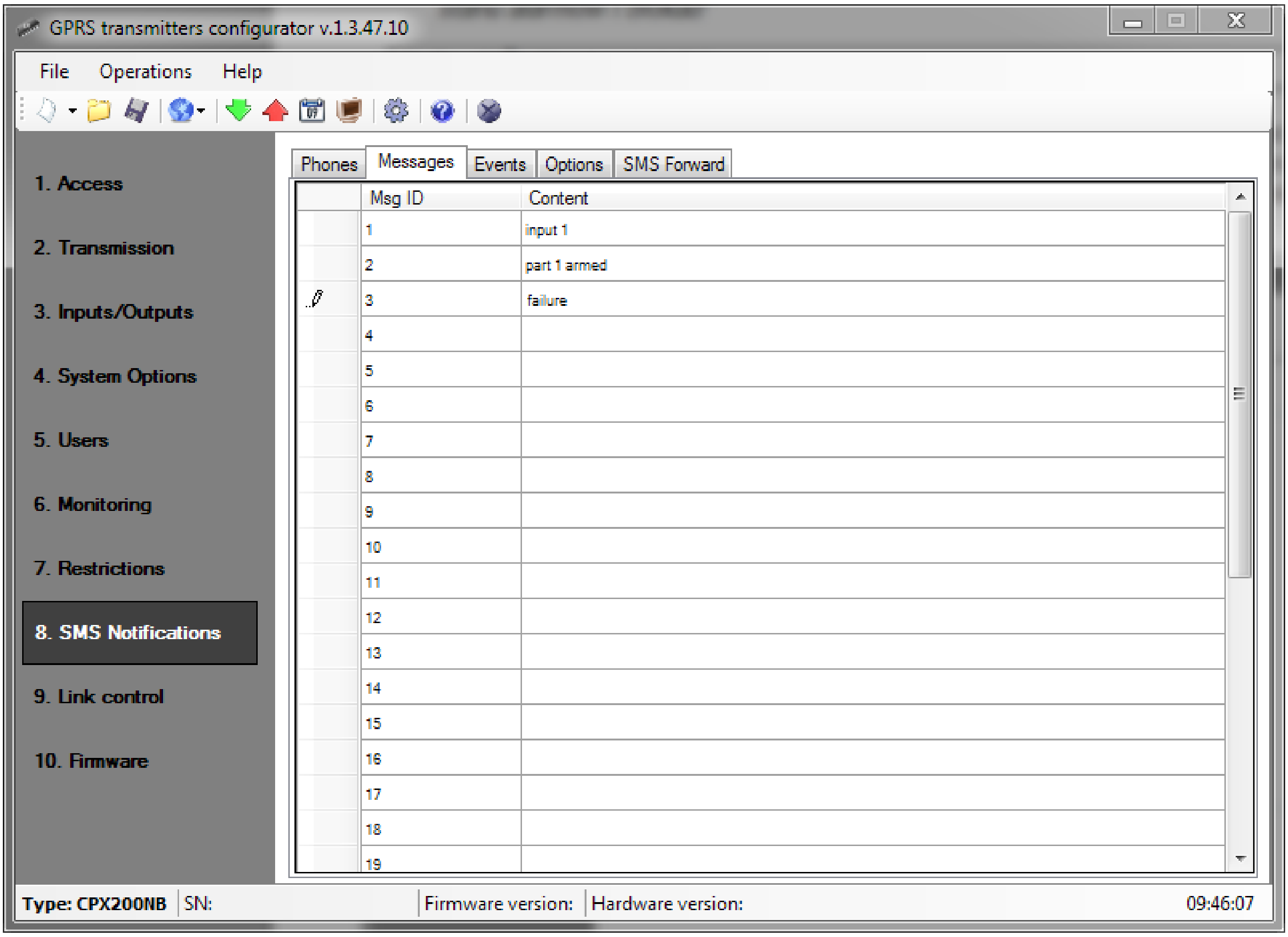
Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:45:50

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.

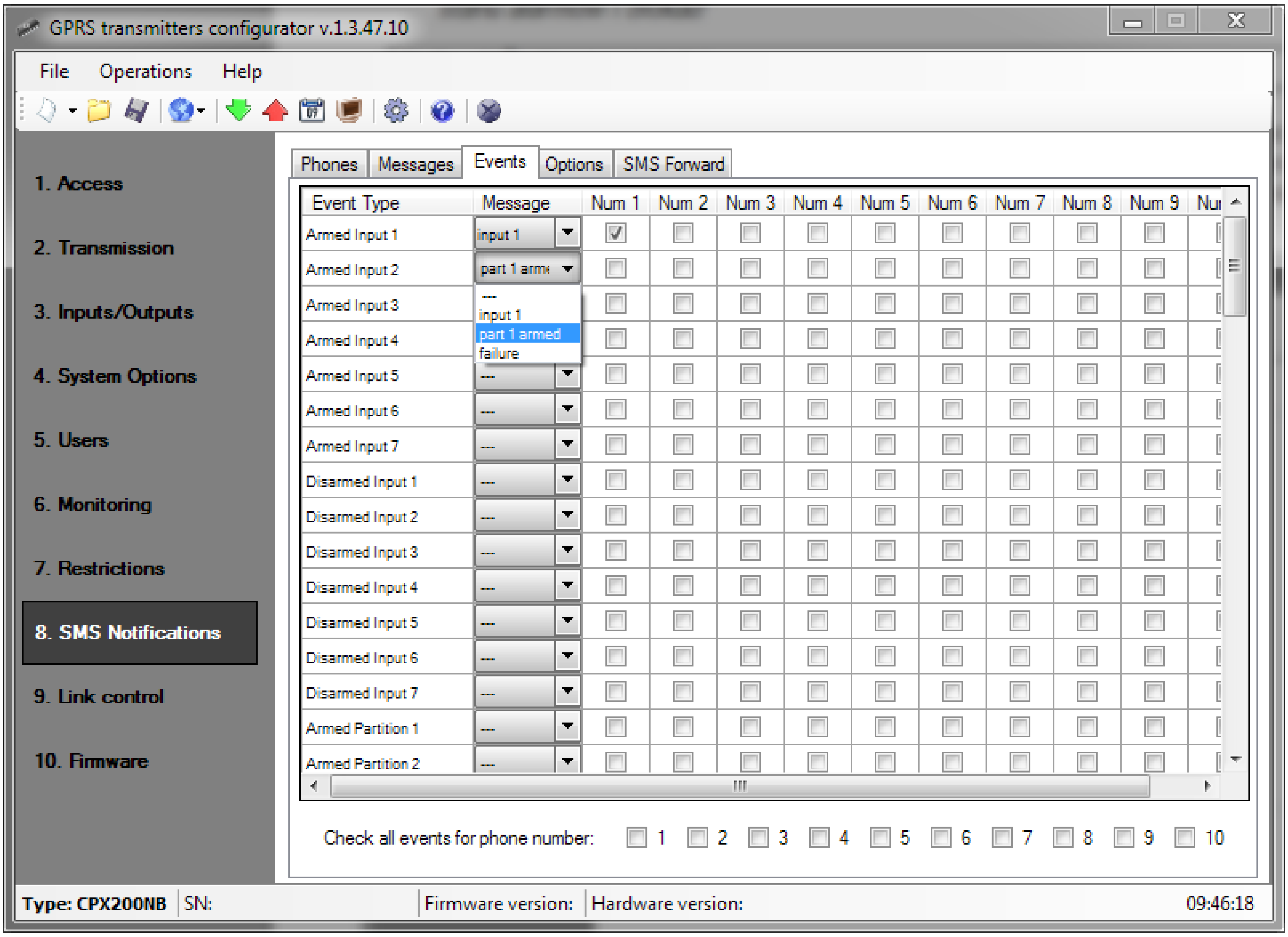


Msg ID	Content
1	input 1
2	part 1 armed
3	failure
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	

Type: CPX200NB | SN:

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).



Event Type	Message	Num 1	Num 2	Num 3	Num 4	Num 5	Num 6	Num 7	Num 8	Num 9	Nu
Armed Input 1	input 1	☑	□	□	□	□	□	□	□	□	□
Armed Input 2	part 1 arme --- input 1 part 1 armed failure	□	□	□	□	□	□	□	□	□	□
Armed Input 3		□	□	□	□	□	□	□	□	□	□
Armed Input 4		□	□	□	□	□	□	□	□	□	□
Armed Input 5	---	□	□	□	□	□	□	□	□	□	□
Armed Input 6	---	□	□	□	□	□	□	□	□	□	□
Armed Input 7	---	□	□	□	□	□	□	□	□	□	□
Disarmed Input 1	---	□	□	□	□	□	□	□	□	□	□
Disarmed Input 2	---	□	□	□	□	□	□	□	□	□	□
Disarmed Input 3	---	□	□	□	□	□	□	□	□	□	□
Disarmed Input 4	---	□	□	□	□	□	□	□	□	□	□
Disarmed Input 5	---	□	□	□	□	□	□	□	□	□	□
Disarmed Input 6	---	□	□	□	□	□	□	□	□	□	□
Disarmed Input 7	---	□	□	□	□	□	□	□	□	□	□
Armed Partition 1	---	□	□	□	□	□	□	□	□	□	□
Armed Partition 2	---	□	□	□	□	□	□	□	□	□	□

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

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:46:18

6.8.4. Options

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

6.8.4.1. Cooperation with the smartphone

This option should be selected if a smartphone application will be used for remote operation of the control panel.

6.8.4.2. 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.

6.8.4.3. Remove unsent SMS messages on partition disarming

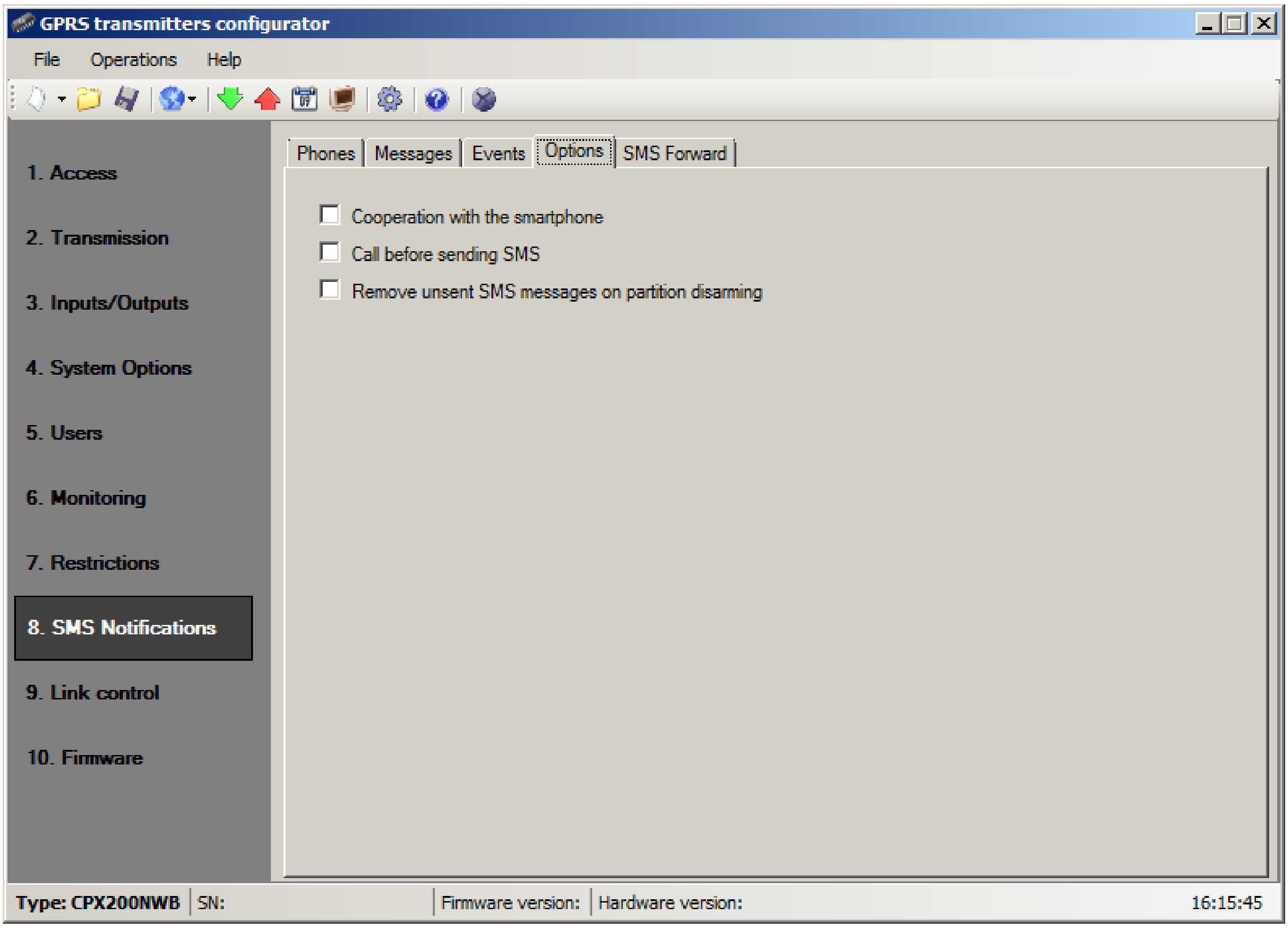
If option is enabled, disarming the partition removes all waiting SMS, except the SMS messages related to partition is still armed.

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.



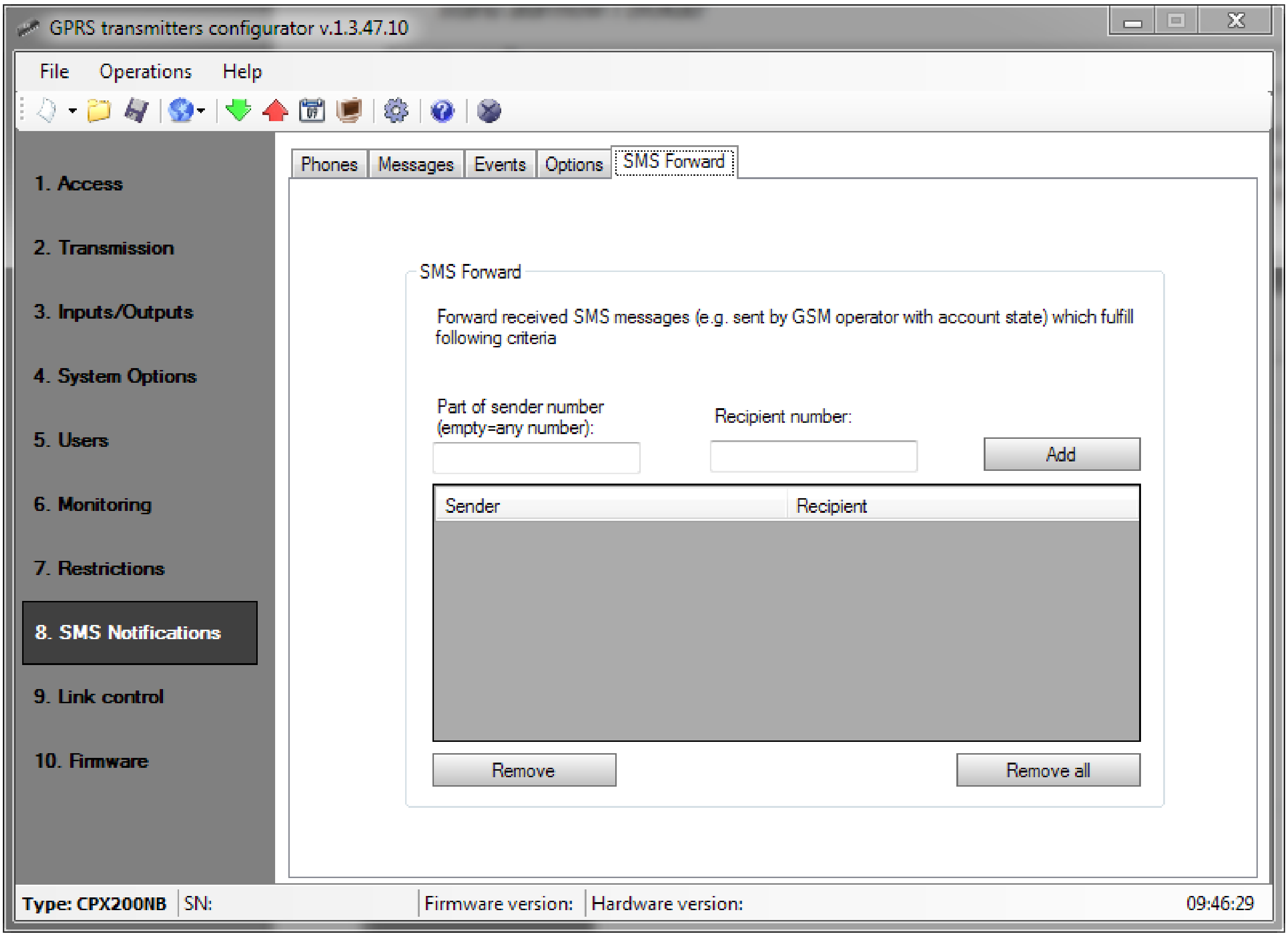
□ Cooperation with the smartphone

□ Call before sending SMS

□ Remove unsent SMS messages on partition disarming

Type: CPX200NWB | SN: | Firmware version: | Hardware version: | 16:15:45

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

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:46:29

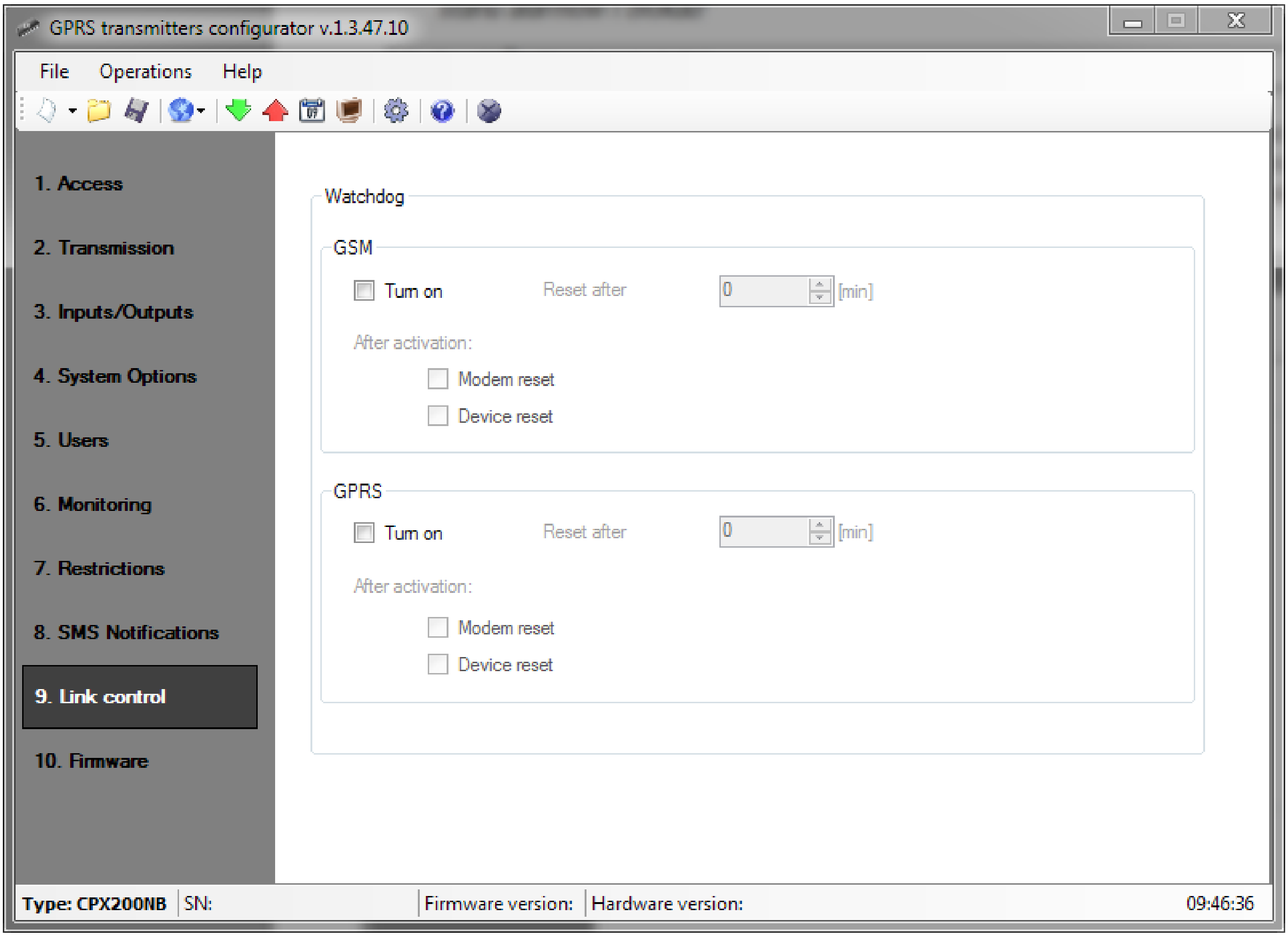
The equipment is able to transfer the received SMS messages to pre-defined telephone numbers in accordance with pre-defined rules. The function may prove necessary in case of account info sent via SMS. In this box you can enter up to 5 rules intended for transfer of SMS messages.

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 0 [min]

After activation:

□ Modem reset

□ Device reset

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:46:36

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.

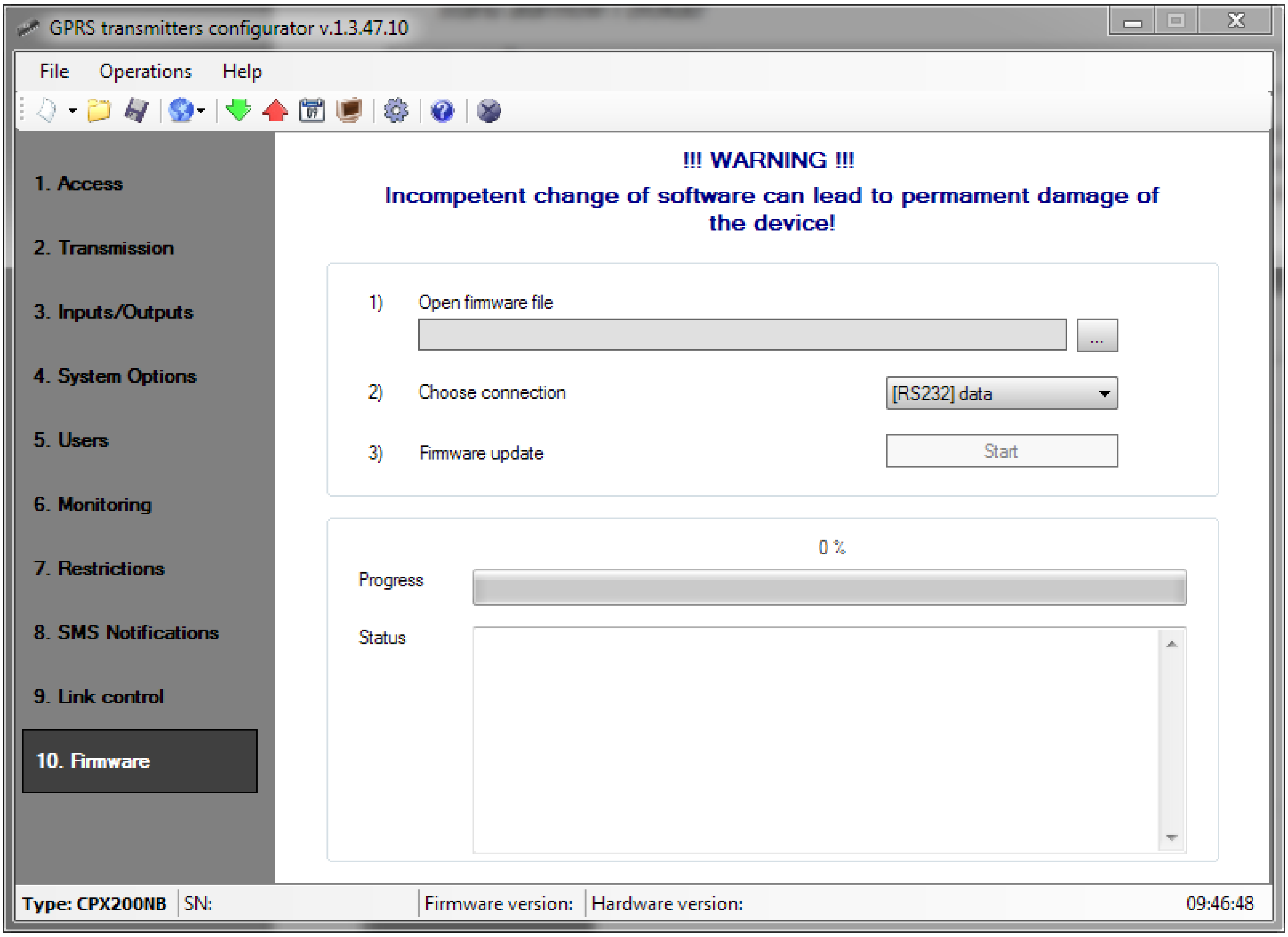
You can define after what time from the moment the connection was lost the equipment shall initiate activities aiming at its restoration. The time is selected in a [Reset after] box and is defined in minutes.

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] data

3) Firmware update

Progress 0 %

Status

Type: CPX200NB | SN: | Firmware version: | Hardware version: 09:46:48

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:

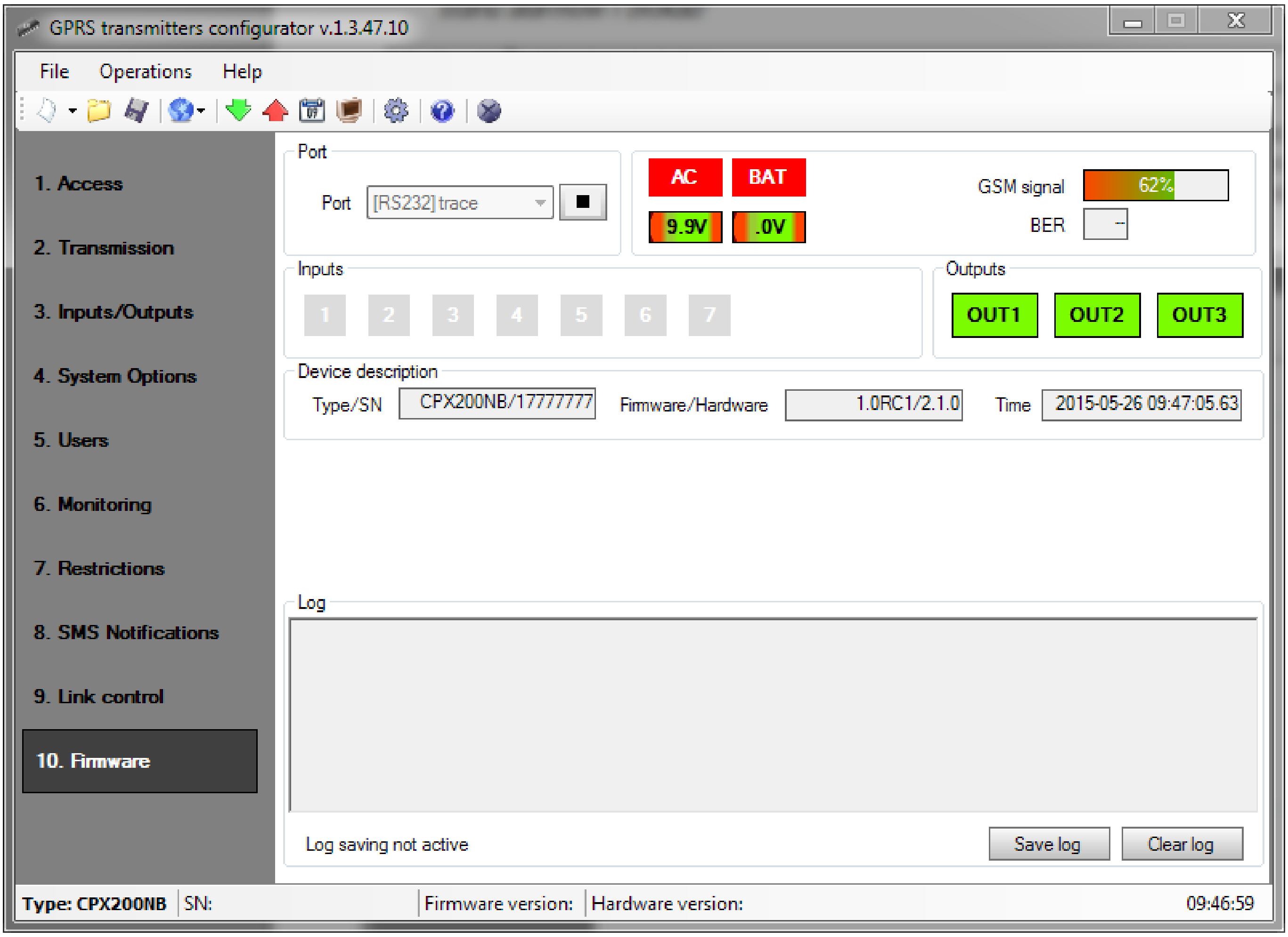
- Start configuration wizard,
- Go to wizard's "Firmware" option,

- 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


GPRS transmitters configurator v.1.3.47.10

Port: [RS232] trace

AC BAT 9.9V .0V

GSM signal: 62%

BER: -

Device description

Type/SN: CPX200NB/17777777

Firmware/Hardware: 1.0RC1/2.1.0

Time: 2015-05-26 09:47:05.63

Log saving not active

Type: CPX200NB | SN: | Firmware version: | Hardware version: | 09:46:59

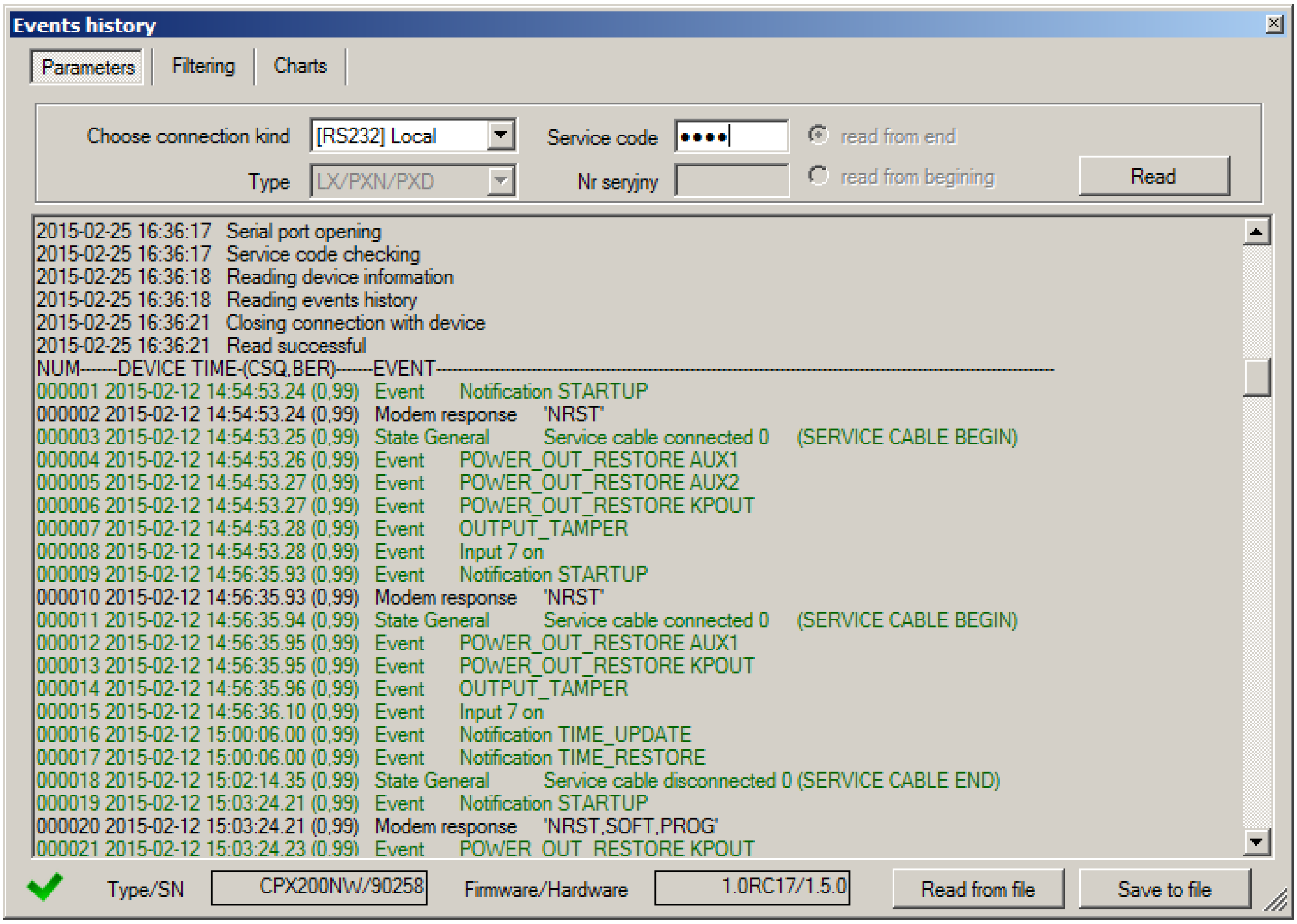
The function "Device Monitoring" allows the on-going monitoring of the control unit's condition. In order to use that functionality, connect the alarm control unit to a PC computer via GD-PROG cable in DEBUG mode and then, in "Port" box select an appropriate RS232 port. Monitor allows the control of the following parameters:

- Condition of mains power supply
- GSM network signal strength and bit error ratio (BER)

- Condition of zones
- Condition of outputs
- Equipment type/ serial number
- PCB version
- Equipment time

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

6.12.EVENTS HISTORY



Choose connection kind: [RS232] Local

Service code: ••••

● read from end

○ read from begining

Type: LX/PXN/PXD

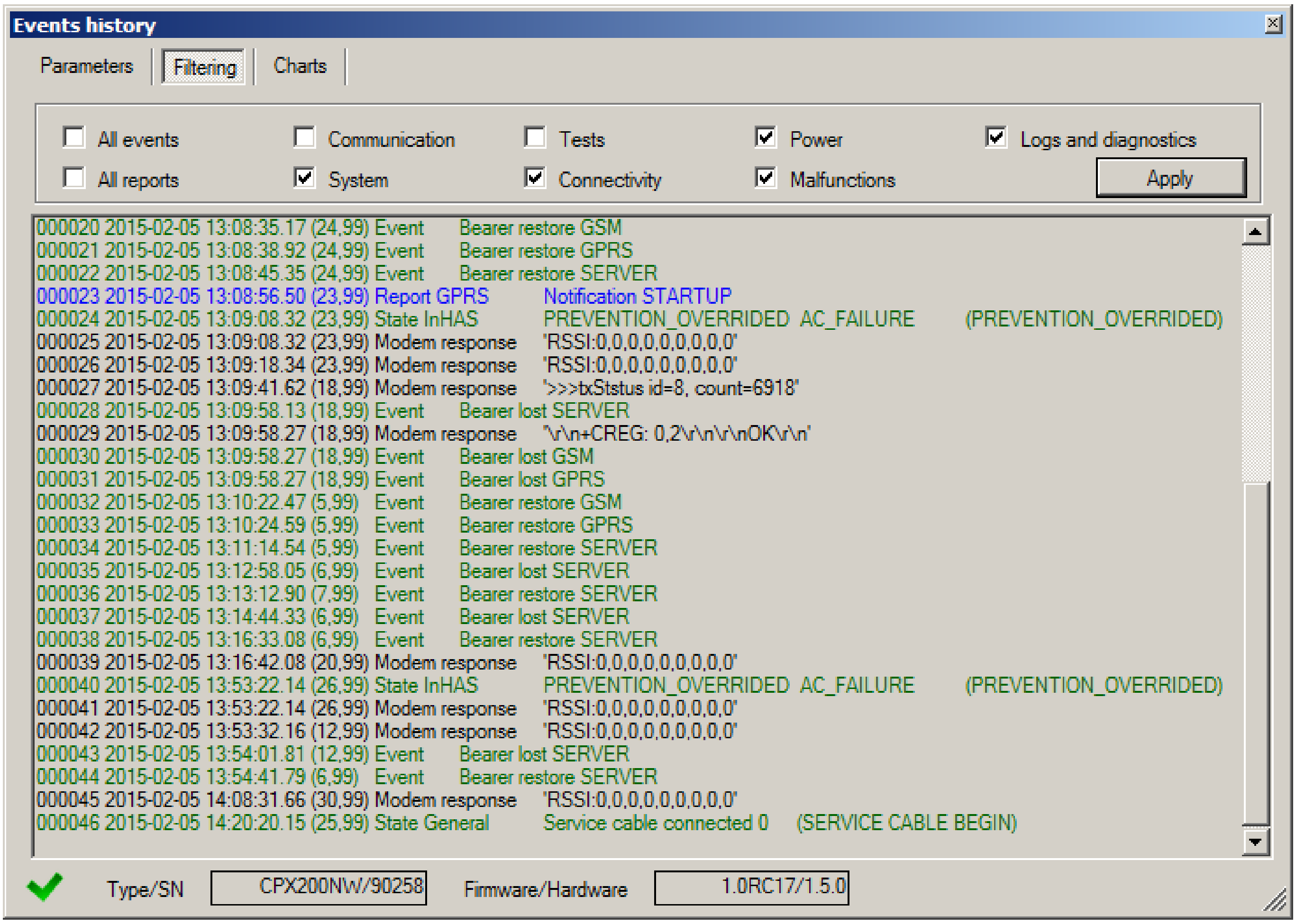
Nr seryjny:

```
2015-02-25 16:36:17  Serial port opening
2015-02-25 16:36:17  Service code checking
2015-02-25 16:36:18  Reading device information
2015-02-25 16:36:18  Reading events history
2015-02-25 16:36:21  Closing connection with device
2015-02-25 16:36:21  Read successful
NUM------DEVICE TIME-(CSQ,BER)------EVENT------------------------------------------------------------------------
000001 2015-02-12 14:54:53.24 (0,99)  Event      Notification STARTUP
000002 2015-02-12 14:54:53.24 (0,99)  Modem response    'NRST'
000003 2015-02-12 14:54:53.25 (0,99)  State General        Service cable connected 0     (SERVICE CABLE BEGIN)
000004 2015-02-12 14:54:53.26 (0,99)  Event      POWER_OUT_RESTORE AUX1
000005 2015-02-12 14:54:53.27 (0,99)  Event      POWER_OUT_RESTORE AUX2
000006 2015-02-12 14:54:53.27 (0,99)  Event      POWER_OUT_RESTORE KPOUT
000007 2015-02-12 14:54:53.28 (0,99)  Event      OUTPUT_TAMPER
000008 2015-02-12 14:54:53.28 (0,99)  Event      Input 7 on
000009 2015-02-12 14:56:35.93 (0,99)  Event      Notification STARTUP
000010 2015-02-12 14:56:35.93 (0,99)  Modem response    'NRST'
000011 2015-02-12 14:56:35.94 (0,99)  State General        Service cable connected 0     (SERVICE CABLE BEGIN)
000012 2015-02-12 14:56:35.95 (0,99)  Event      POWER_OUT_RESTORE AUX1
000013 2015-02-12 14:56:35.95 (0,99)  Event      POWER_OUT_RESTORE KPOUT
000014 2015-02-12 14:56:35.96 (0,99)  Event      OUTPUT_TAMPER
000015 2015-02-12 14:56:36.10 (0,99)  Event      Input 7 on
000016 2015-02-12 15:00:06.00 (0,99)  Event      Notification TIME_UPDATE
000017 2015-02-12 15:00:06.00 (0,99)  Event      Notification TIME_RESTORE
000018 2015-02-12 15:02:14.35 (0,99)  State General        Service cable disconnected 0 (SERVICE CABLE END)
000019 2015-02-12 15:03:24.21 (0,99)  Event      Notification STARTUP
000020 2015-02-12 15:03:24.21 (0,99)  Modem response    'NRST,SOFT,PROG'
000021 2015-02-12 15:03:24.23 (0,99)  Event      POWER_OUT_RESTORE KPOUT
```

✓ Type/SN: CPX200NW/90258

Firmware/Hardware: 1.0RC17/1.5.0

The function enables to read out the events lately recorded in the memory of the equipment. The control unit 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.

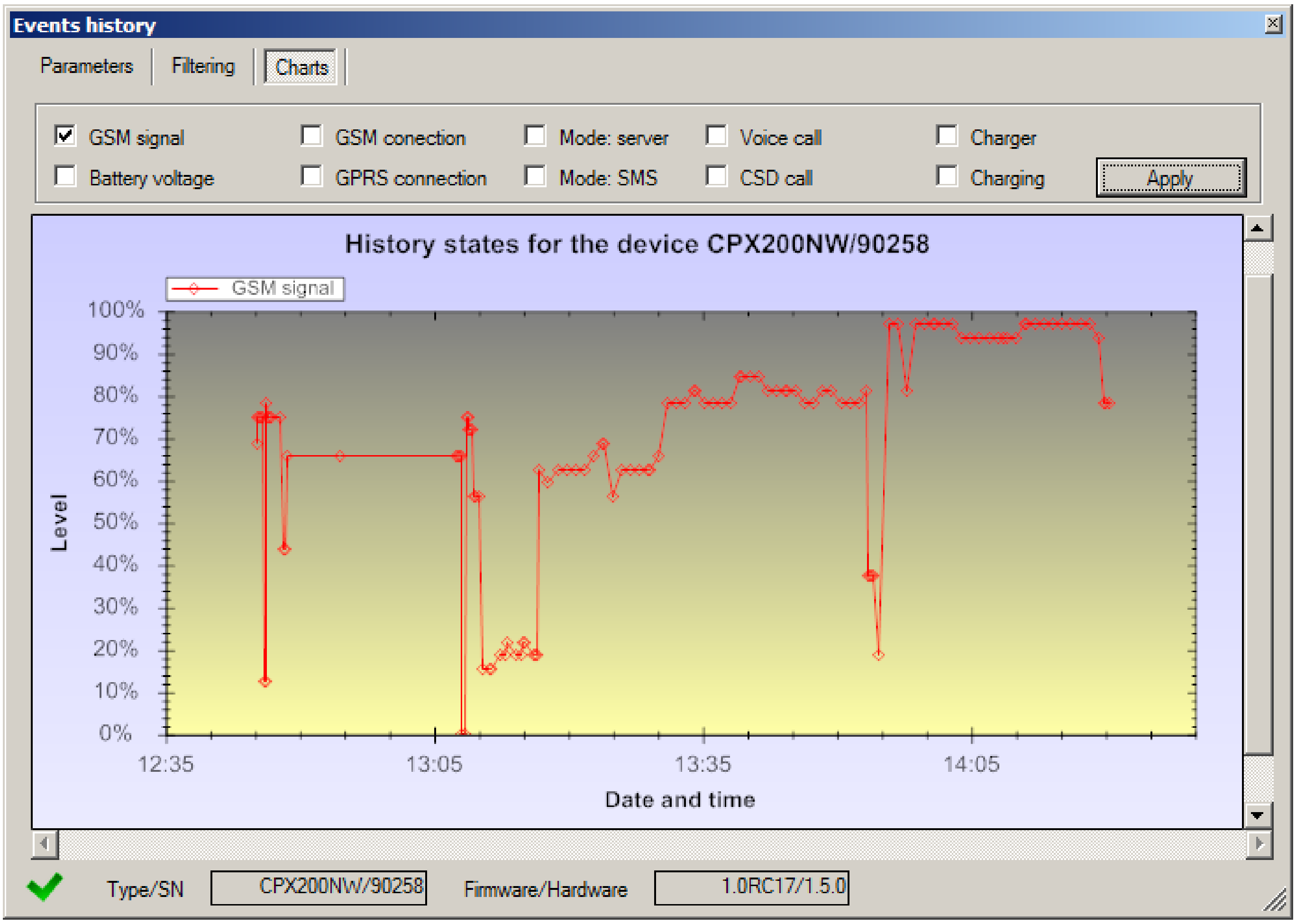


☐ All events ☐ Communication ☐ Tests ☑ Power ☑ Logs and diagnostics

☐ All reports ☑ System ☑ Connectivity ☑ Malfunctions

```
000020 2015-02-05 13:08:35.17 (24,99) Event       Bearer restore GSM
000021 2015-02-05 13:08:38.92 (24,99) Event       Bearer restore GPRS
000022 2015-02-05 13:08:45.35 (24,99) Event       Bearer restore SERVER
000023 2015-02-05 13:08:56.50 (23,99) Report GPRS        Notification STARTUP
000024 2015-02-05 13:09:08.32 (23,99) State InHAS        PREVENTION_OVERRIDED  AC_FAILURE       (PREVENTION_OVERRIDED)
000025 2015-02-05 13:09:08.32 (23,99) Modem response     'RSSI:0,0,0,0,0,0,0,0,0'
000026 2015-02-05 13:09:18.34 (23,99) Modem response     'RSSI:0,0,0,0,0,0,0,0,0'
000027 2015-02-05 13:09:41.62 (18,99) Modem response     '>>>txStstus id=8, count=6918'
000028 2015-02-05 13:09:58.13 (18,99) Event       Bearer lost SERVER
000029 2015-02-05 13:09:58.27 (18,99) Modem response     '\r\n+CREG: 0,2\r\n\r\nOK\r\n'
000030 2015-02-05 13:09:58.27 (18,99) Event       Bearer lost GSM
000031 2015-02-05 13:09:58.27 (18,99) Event       Bearer lost GPRS
000032 2015-02-05 13:10:22.47 (5,99)  Event       Bearer restore GSM
000033 2015-02-05 13:10:24.59 (5,99)  Event       Bearer restore GPRS
000034 2015-02-05 13:11:14.54 (5,99)  Event       Bearer restore SERVER
000035 2015-02-05 13:12:58.05 (6,99)  Event       Bearer lost SERVER
000036 2015-02-05 13:13:12.90 (7,99)  Event       Bearer restore SERVER
000037 2015-02-05 13:14:44.33 (6,99)  Event       Bearer lost SERVER
000038 2015-02-05 13:16:33.08 (6,99)  Event       Bearer restore SERVER
000039 2015-02-05 13:16:42.08 (20,99) Modem response     'RSSI:0,0,0,0,0,0,0,0,0'
000040 2015-02-05 13:53:22.14 (26,99) State InHAS        PREVENTION_OVERRIDED  AC_FAILURE       (PREVENTION_OVERRIDED)
000041 2015-02-05 13:53:22.14 (26,99) Modem response     'RSSI:0,0,0,0,0,0,0,0,0'
000042 2015-02-05 13:53:32.16 (12,99) Modem response     'RSSI:0,0,0,0,0,0,0,0,0'
000043 2015-02-05 13:54:01.81 (12,99) Event       Bearer lost SERVER
000044 2015-02-05 13:54:41.79 (6,99)  Event       Bearer restore SERVER
000045 2015-02-05 14:08:31.66 (30,99) Modem response     'RSSI:0,0,0,0,0,0,0,0,0'
000046 2015-02-05 14:20:20.15 (25,99) State General      Service cable connected 0     (SERVICE CABLE BEGIN)
```

Type/SN: CPX200NW/90258 Firmware/Hardware: 1.0RC17/1.5.0



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

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

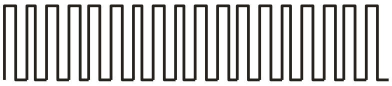
Type/SN: CPX200NW/90258 Firmware/Hardware: 1.0RC17/1.5.0

7. LED INDICATION

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

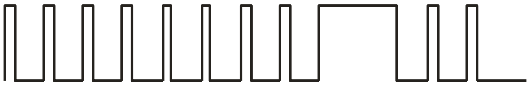
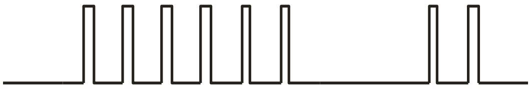
7.1. NETWORK LOG-IN

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		—	—

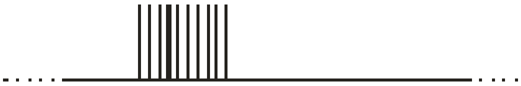
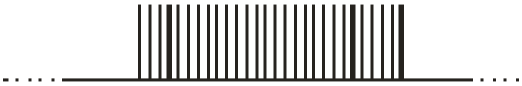
7.2. GSM RANGE

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**		—	—

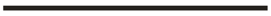
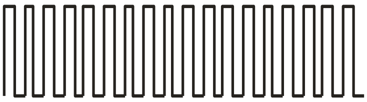
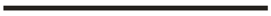
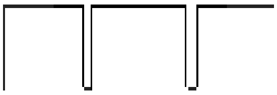
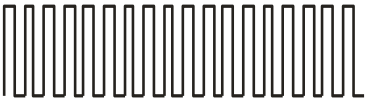
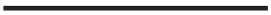
7.3. TRANSMISSION

During data transmission green LED indicates the data sending.

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

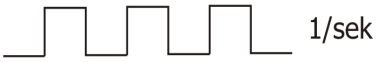
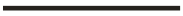
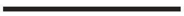
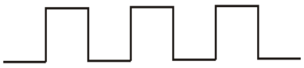
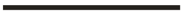
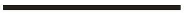
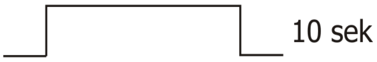
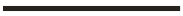
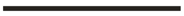
7.4. PROGRAMMING

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			

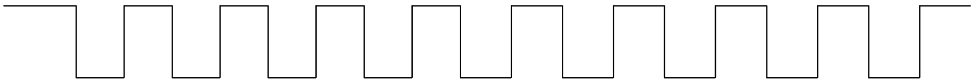
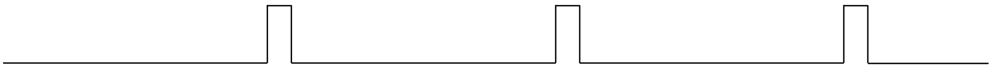
7.5. FIRMWARE UPDATE

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	 		
Software update			
Decryption of firmware received	 		

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 lines 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 “Turn automatic prevention override for failure off”

  - 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 1 – 16

  - Input 1 – 16 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
- Time lost

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 unit 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 CPX220NWB 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. 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.

9.1.1.7. 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.

9.1.1.8. 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:	Removes temporary automatic blockade from the given zones given by mask. Input_mask is decimal number made from 17 bit vector where bit 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. Examples: RLIMIT= 6 Removes blocade from zone 1 and zone 2 RLIMIT= 2 Removes blocade from zone 1

9.1.1.9. 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

9.1.2. 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_wihout_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 CPX220NWB (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 1, bit 2 the zone 2 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.

9.1.3. Commands for managing the users in CP

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 8 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	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 8 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 dministrato 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[,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 8 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 and 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 8 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, adminPassword 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.

9.1.4. 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 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 1,… bit 16 corresponds to the zone 16. 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 1. 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 1, bit 2 means the zone 2, 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 1, bit 2 means the zone 2, 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 CPX220NWB (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 7. zonesComFailures – is a bit-vector indicating the communication failures between wireless detectors and control panel. Bit 1 (counting from 0), corresponds to the zone 1, … bit 16 corresponds to the zone 16. 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 1, … bit 16 corresponds to the zone 16. partitionsStayAway – is a bit-vector indicating partitions armed in stay mode. Bit 0 corresponds to partition 1. Bit 1 corresponds to partition 2. If a bit is set, it's partition is armed in stay mode. Otherwise it is armed in away mode. This parameter values are valid only for armed partitions. 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,]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	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 partition 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 arming. The specified partitions will be armed from the user's id to which the code belongs. STAY statement before the partitions vector is optional. It means that partitions in the bit-vector will be armed in stay mode. It is not allowed to change arm mode of an already armed partition – system will reject an attempt of arming in stay mode the partition that is armed in away mode. It will also reject an attempt of arming in away mode a partition that is armed in stay mode. It is also not possible to arm in stay mode the partition that has no perimeter zones assigned. The command returns: CPSETPARTITIONS=[STAY,]partitionList: EOK If the command is executed. 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). CPSETPARTITIONS=[STAY,]partitions:ENOT_ALLOWED If an attempt to change the arm mode of the armed partition was made or if at least one of the partitions does not have any perimeter zones assigned to it. CPSETPARTITIONS=[STAY,]partitions,password:EFORMAT If the data format is incorrect (partitions,password are the command arguments) CPSETPARTITIONS=[STAY,]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 partition 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 whome 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). 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 dministrator 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 1. 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

++	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 dministrator 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

10. CHANGE HISTORY

Date / Version / Firmware	Description
2016.08.29 / i1.0 / 2.5.2	First version of the manual
2016.10.21 / i1.1 / 2.6.2	Added information about smoke detector SD-20 and wireless keypad KP1W
2016.10.27 / i1.2 / 2.6.3	Added information about flood detector FL-10 and wireless magnetic contact MC-11