

# Control panel SP231

## Installation manual

December, 2018

**Control panel SP231** – intrusion (to premises) and fire alarming system (alarm system's) processor part with integrated GSM/GPRS communicator. The control panel allows the user to switch on the alarm conveniently to protect the premises in the preferred mode and thus control the signals of different sensors and react to them. Upon occurrence of any system event, its report via GSM connection shall be transmitted to the Centralised Monitoring Station (CMS) and/or mobile phones of users.

Modules that are compatible with **control panel SP231**: **CZ8** (input expansion modules); **E14** (Internet communicator); **E16T** (Internet communicator); **W17U** (Wi-Fi communicator); **RFMOD2** (radio module for wireless sensors); **iO8** (input and output expander); **CZ-Dallas** (iButton contact key reader); **DB18B20** and **BD18S20** (temperature sensors).

## General properties

- 8 zones (possibility to expand to 32);
- 9 zone functions;
- Exclusive zone for two-wire smoke detector;
- 8 partitions;
- Internal clock;
- Control of temperature sensors;
- Tamper tracking;
- Anti-Masking tracking;
- Convenient default settings for fast installation of the security system.

## Alarm control

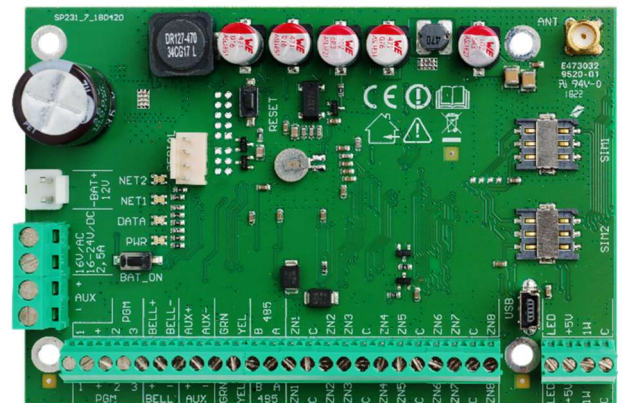
- 40 alarm control codes;
- **Remote control via phone call, SMS and Protegus app;**
- Control devices: "Trikdís" keyboard Protegus SK130LED, SK232LED, "Paradox" keyboard K32+, K32LED, K636, K10LED, iButton keys, coded or other switches;
- "Bypass", "Door Chime", "Tamper", "Shutdown", "Anti-Masking", "Force Arm" "Bellsquawk" "Re-Arm" etc. functions.

## Power supply:

- Main supply from 16-18 V AC or 16-24 V DC source
- Back-up supply from 12 V battery

## PGM outputs:

- 5 PGM outputs (3 PGM, 1 Bell, 1 LED);
- 9 PGM output functions;
- PGM output remote control.



## Setting of control panel operation parameters

- Software "TrikdísConfig" via USB;
- **Remotely via GPRS using "TrikdísConfig".**

## Transmission of reports:

- Two slots for SIM cards;
- Transmission of encrypted reports to the main or back-up CMS IP address via GPRS. If GPRS connection is lost, the reports shall be sent by SMS messages;
- Continuous control of communication channel;
- Sending of reports when the temperature comes outside the allowable set range;
- Event reports shall be transmitted by Contact ID codes;
- Sending of SMS messages with the user defined event text to 5 mobile phones;
- Sending of temperature values by SMS messages;
- Warning calls to 2 phones about the occurred event;
- Event memory shall store at least 2000 last events.

## Warranty and liability limitations

The control panel is provided with a 24 months warranty to become effective from the purchase-sales date. The warranty period shall ensure free of charge repair of troubles occurred due to the manufacturer fault.

The warranty shall be applied, if the control panel is installed by qualified specialists according to this document. The control panel for repair shall be provided in the manufacturer package together with a defect report with the indicated nature of trouble.

Upon expiry of the warranty period the maintenance and repair of the control panel shall be performed at the buyer's expense.

The warranty may be terminated prematurely in the following cases:

- The control panel was repaired or was attempted to repair by an unauthorized person;
- The control panel was used not for its intended purpose;
- The control panel was stored and/or installed in an inappropriate premises with inappropriate climate conditions, aggressive chemical environment;
- The control panel was mechanically broken and/or intentionally damaged;
- The control panel was damaged due to *force-majeure* (lightning discharge etc.) circumstances.

The manufacturer shall not be liable for the following:

- control panel malfunctions, if the control panel was installed or used not according to its operation manual;
- control panel malfunctions, if they occurred upon malfunctioning, lost GSM/GPRS/Internet connection or upon occurrence of troubles in the network operator networks;
- termination or restriction of GSM/GPRS/Internet communication services to the control panel buyer or to the control panel user, and shall not reimburse the control panel buyer or the control panel user for the occurred property or non-property losses;
- termination or restriction of electrical power supply to the control panel buyer or to the control panel user, and shall not reimburse the control panel buyer or the control panel user for the occurred property or non-property losses;
- robbery, fire of premises or other incurred losses to the control panel buyer or to the control panel user, and shall not reimburse the control panel buyer or the control panel user for the occurred property or non-property losses as a result of these events.

## Safety requirements

Prior to using the control panel, you must get familiar with this manual.

Control panel SP231 – electrical facility, thus it shall be installed and serviced only by qualified specialists following this document.

During installation of the control panel its power supply must be switched off!

In the premises the control panel shall be installed in the restricted access zones and at a safe distance from sensitive electronic equipment. The control panel is not resistant to vibration, other mechanical impact, moisture and aggressive chemical environment. Control panel shall comply with the requirements of Standard EN 50131 applied to environmental impact resistance Class II.



The used housings, transformers, batteries and programming devices shall comply with the safety requirements established in the Standard EN 60950.

The device shall be connected to 230 V voltage 50 Hz frequency mains power through the Class II transformer reducing voltage down to 16 – 18 V or to 16 – 24 V direct current source. To ensure back-up supply a battery of 12 V and at least 7 Ah capacity shall be used. The current consumption depends on the power of the connected external devices.

Protection of the power supply circuit shall be ensured with the installed two-pole automatic safety switch. The dividing gap between the switch off contacts shall be at least 3 mm. The safety switch shall be installed in the place known to the specialists servicing the control panel.

Cut-off of the control panel from the electricity network:

- from alternating current network – upon switching off the automatic safety switch;
- from the battery – by disconnecting the terminals.

# Content

<b>1</b>	<b>TECHNICAL PARAMETERS</b> .....	<b>6</b>			
<b>2</b>	<b>ALARM SYSTEM POWER SUPPLY</b> .....	<b>7</b>			
2.1	MAIN SUPPLY .....	7			
2.2	BACK-UP SUPPLY .....	7			
2.3	BATTERY SUPPLY .....	7			
<b>3</b>	<b>CONTROL PANEL ASSEMBLIES</b> .....	<b>7</b>			
3.1	CONTROL PANEL SP231 .....	7			
3.2	CONTROL PANEL SP231 KIT .....	7			
3.3	CONTROL PANEL SP231 KITi .....	8			
<b>4</b>	<b>CONTROL PANEL STRUCTURE</b> .....	<b>8</b>			
4.1	PURPOSE OF TERMINALS .....	9			
4.2	LIGHT INDICATION .....	9			
<b>5</b>	<b>SYSTEM INSTALLATION</b> .....	<b>10</b>			
5.1	RECOMMENDED INSTALLATION PROCEDURE .....	10			
5.1.1	<i>Control panel fastening in the mounting housing</i>	10			
5.1.2	<i>Equipment connection sequence</i> .....	11			
5.1.3	<i>Recommendations for setting the control panel operation parameters</i> .....	12			
5.1.4	<i>Alarm system operation testing</i> .....	13			
5.2	COMPATIBLE MODULES .....	14			
5.3	CONNECTION OF SENSORS.....	15			
5.4	CONNECTION OF SMOKE DETECTORS .....	15			
5.5	CONNECTION OF EQUIPMENT TERMINALS TO PGM OUTPUTS	16			
5.6	CONNECTION OF REPORT TRANSMISSION DEVICES .....	17			
5.7	CONNECTION OF TEMPERATURE SENSORS, IBUTTON KEY READERS	18			
5.8	CONNECTION OF KEYPADS AND INPUT EXPANDERS .....	19			
5.9	CONNECTION OF WIRELESS SENSORS WITH RF-MOD2 ...	21			
<b>6</b>	<b>CONFIGURATION OF CONTROL PANEL OPERATION</b> ..	<b>21</b>			
6.1	CONNECT TO CONTROL PANEL.....	21			
6.1.1	<i>Connect with USB cable</i> .....	21			
6.1.2	<i>Connect in remote mode</i> .....	21			
6.1.3	<i>Changing of settings by SMS messages</i> .....	23			
6.2	DESCRIPTION OF TRIKDISCONFIG PROGRAM .....	23			
6.3	USER ACCESS.....	24			
6.3.1	<i>Control panel configuration</i> .....	24			
6.3.2	<i>Control panel control</i> .....	25			
6.4	SYSTEM USER INITIAL LOGIN CODES .....	25			
6.5	SYSTEM PARAMETERS.....	26			
6.5.1	<i>General system parameters</i> .....	26			
6.5.2	<i>Resetting of initial parameters</i> .....	27			
6.5.3	<i>Setting of control panel clock</i> .....	27			
6.5.4	<i>Regular connectivity checks</i> .....	27			
6.5.5	<i>Keyboard parameters</i> .....	28			
6.6	SYSTEM TROUBLES.....	28			
6.6.1	<i>Tamper recognition</i> .....	30			
6.6.2	<i>Control panel watch-dog</i> .....	30			
6.7	ZONE PARAMETERS.....	30			
6.7.1	<i>Main zone parameters</i> .....	30			
6.7.2	<i>Parameters of zone event reports</i> .....	32			
6.7.3	<i>Zone function description</i> .....	32			
6.8	PARTITION PARAMETERS.....	33			
6.9	USER ACCESS PARAMETERS.....	34			
6.9.1	<i>iButton key code registering</i> .....	35			
6.10	SIM CARD PARAMETERS .....	35			
6.11	REPORT TRANSMISSION TO CMS.....	36			
6.12	REPORT TRANSMISSION TO USER .....	37			
6.12.1	<i>Message texts to User</i> .....	39			
6.13	PGM OUTPUT CONFIGURATION .....	39			
6.13.1	<i>PGM output operation descriptions</i> .....	40			
6.13.2	<i>PGM output remote control</i> .....	42			
6.14	CONTROL BY CALL.....	43			
6.14.1	<i>Partition control</i> .....	43			
6.14.2	<i>PGM Output control</i> .....	43			
6.15	TRANSMISSION MODULE REGISTRATION .....	43			
6.16	KEYPADS AND EXPANDERS REGISTRATION .....	45			
6.17	WIRELESS SENSORS REGISTRATION .....	46			
6.17.1	<i>Detectors</i> .....	48			
6.17.2	<i>Sirens</i> .....	50			
6.17.3	<i>Pendants</i> .....	52			
6.17.4	<i>Registration of wireless keypad (FW2-ICON KP-8F)</i>	53			
6.18	SETTING OF TEMPERATURE METERING REPORT CHARACTERISTICS .....	54			
6.19	SETTING OF EVENT REPORTS .....	55			
6.20	EVENT LOG .....	55			
6.21	CONTROL PANEL FIRMWARE UPGRADING .....	56			
<b>7</b>	<b>PROGRAMMING AND CONTROL BY SMS MESSAGES</b>	<b>57</b>			
<b>8</b>	<b>REMOTE CONTROL</b> .....	<b>59</b>			
8.1	CONTROL VIA <i>PROTEGUS CLOUD</i> .....	59			

## 1 Technical parameters

Name	Description	Value	Units
Supply voltage	From alternating current source	16-18	V
	From direct current source	16-24	V
Current consumption	In standby mode	80	mA
	When sending data	Up to 150	mA
Between [AUX+] and [C] terminals	Output DC voltage (level of impulses shall not exceed 200 mV).	13.6 (10-14)	V
		1	A
	Maximum allowable current consumption <b>Note:</b> If the supply limits via "AUX" outputs are exceeded, the supply to the connected devices shall be switched off automatically	2	A
Between [+5V] and [C] terminals	Output DC voltage (level of impulses shall not exceed 100 mV). <b>Note:</b> If the supply limits via "+5V" output are exceeded, the supply to the connected devices shall be switched off automatically	5 (4.9-5.1)	V
		0.2	A
Surge protection	All the control panel terminal block terminals shall be protected against static voltage jumps	2000	V
PGM1-PGM3	Programmable OC (open collector) type output terminals for switching on/off of various devices automatically or <b>via remote command (create "minus")</b>	30	V
		0.5	A
BELL- (PGM4)	Programmable OC (open collector) type output terminal for automatic switching on of the outdoor or indoor sirens (create "minus")	30	V
		1	A
LED (PGM5)	Programmable OC (open collector) type output terminal with 5.1 kΩ resistor for connecting the LED cathode (-) (create "minus").	30	V
		0.1	A
Operating environment	At relative humidity below 80% at +20°C, without condensation	From -25 up to +50	°C
Control panel dimensions	-	117x74x25	mm
Weight	-	0.1	kg

### Report transmission technology

Name	Description
Report transmission to CMS	Complies with criteria of operating properties ATS5 established in Standards EN 50131 and EN 50136 and applied to Grade III class equipment
GSM/GPRS modem Integrated quad-band SIM800H	850 / 900 / 1800 / 1900 MHz
Communication with CMS technologies	TCP/IP or UDP/IP via GPRS, SMS messages
Report transmission protocols	TRK_TCP or TRK_UDP

Name	Description
Report encoding	Protocol Contact ID codes
Report encryption	Yes, using 6 symbol encryption key

## 2 Alarm system power supply

### 2.1 Main supply

The control panel and all alarm system can be fed from the alternating or direct current source. In both cases, to ensure an uninterrupted supply to the system, the control panel shall be additionally connected to a back-up supply source – 12 V battery. To ensure the requirements of Standard EN50131, in case of cut-off from the main supply source, the back-up supply battery shall be of sufficient capacity to provide power from the back-up source to the system for 12 hours to comply with Grade II requirements or for 60 hours to comply with Grade III requirements. Assess the current consumption of auxiliary devices, which is provided in chapter 5.2 „Compatible modules“.

### 2.2 Back-up supply

Upon interruption of power supply to the system from the main supply source, the event *AC Failure* report shall be formed and the control panel shall automatically switch over the system for its feeding from the back-up supply – 12 V battery. When the battery voltage decreases down to 11.5 V, the event *Low Battery* report shall be formed. When the battery discharges below 9.5 V, the event *Battery Missing/Dead* report shall be formed and the battery shall be disconnected. Upon restoration of the AC mains voltage, the *AC Restore* report shall be formed and the battery charging process shall start automatically. The desired charging current from 0.1 to 2.0 A can be set during programming the control panel, see 6.5.1 „General system parameters“. When the battery voltage restores to 12.6 V, the event *Battery Restore* report shall be formed.

### 2.3 Battery supply

In individual case, e.g., for testing, the control panel and all the alarm system can be supplied not through the main supply port, but only through a back-up supply port, e.g., only from 12 V battery. In this case, in order to start the control panel (system) it is necessary to connect the battery to the control panel **-BAT+** port and click the circuit board button **BAT\_ON** (see 4 “Control panel structure”).

## 3 Control panel assemblies

### 3.1 Control panel SP231

Control panel <b>SP231</b> circuit board	1 pc.
Battery connection wire	1 pc.
Resistors 2.2 kΩ	16 pcs.
Plastic holder (fasteners)	4 pcs.

Note: USB wire (Mini-B type), which is designed for control panel programming, is not included.

### 3.2 Control panel SP231 KIT

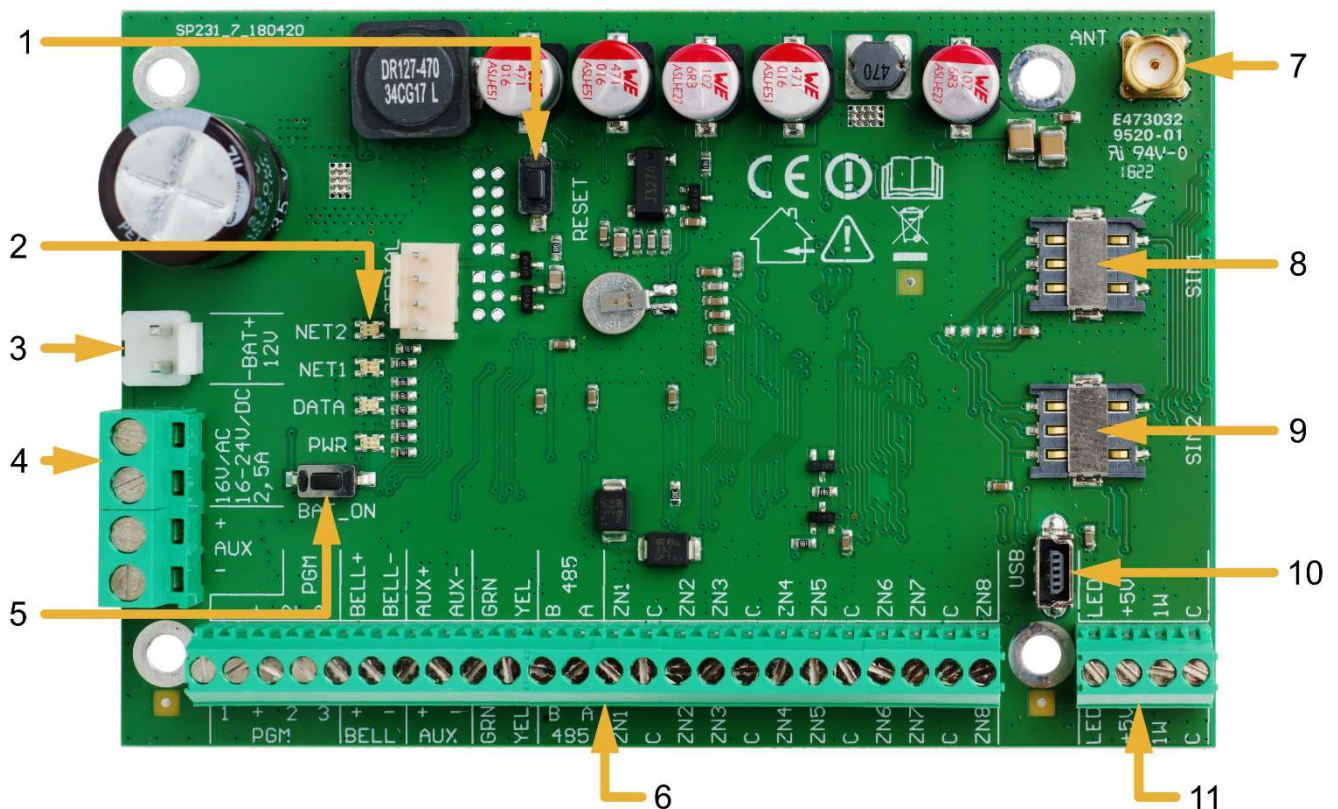
Control panel <b>SP231</b> circuit board embedded in the metal housing	1 pc.
Metal housing K01 with 40 VA transformer	1 pcs.
Resistors 2.2 kΩ	16 pcs.
Stick-on GSM antenna ANT04 with 2.5 m length cable	1 pc.

Battery connection wire	1 pc.
Tamper sensor	1 pc.
Terminal block with 0,5 A fuse	1 pc.

### 3.3 Control panel SP231 KITi

Control panel <b>SP231</b> circuit board embedded in the metal housing	1 pc.
Metal housing K02 with Mean Well impulse supply source	1 pc.
Resistors 2.2 k $\Omega$	16 pcs.
Stick-on GSM antenna ANT04 with 2.5 m length cable	1 pc.
Battery connection wire	1 pc.
Tamper sensor	1 pc.
Terminal block with 3,15 A fuse	1 pc.

## 4 Control panel structure



1. *RESET* button.
2. Communication and operation light indication.
3. Back-up supply port.
4. Main supply terminal block.
5. *BAT\_ON* button is designed for starting the control panel, when the DC voltage source is connected to the back-up supply terminal block.
6. Terminal block for peripherals.
7. GSM antenna port.
8. SIM1 card holder.
9. SIM2 card holder.
10. USB port for configuration of the control panel operation parameters.
11. 1-Wire bus terminal block.



## 4.1 Purpose of terminals

### Main supply terminal block

Terminal	Description
16V AC 16-24V DC	Main supply contacts shall be connected either to 16 – 18 V AC or 16 – 24 V DC source.

### Back-up supply port

Terminal	Description
-BAT+	Port for connecting the 12 V back-up battery.

### Terminal block for peripherals

Terminal	Description
PGM1-PGM3	Programmable operation output terminals for connecting the indicators and remotely controlled equipment.
BELL+, BELL-	Contacts for connecting the siren.
AUX+	Positive 13.6 V DC supply terminal for keyboard(s), indicators and sensors.
C	Negative supply terminal for keyboard(s), indicators and sensors.
YEL	Peripherals (e.g., keyboard) YEL circuit contact (yellow wire).
GRN	Peripherals (e.g., keyboard) GRN circuit contact (green wire).
MCI	Data bus contact for iButton key code reader and/or other report transmission devices (e.g., radio transmitter).
ZN1-ZN8	Contacts for connecting the sensor control circuits. The contact ZN8 can be used for connecting the 2-wire smoke detectors.

### 1-Wire bus terminal block

Terminal	Description
LED	The contact for connecting the premises protection mode indicator, e.g., iButton key reader LED cathode (-) (PGM5).
+5V	Positive 1-wire devices 5V DC supply contact.
1W	1-wire devices data circuit contact (iButton keys, temperature sensors)
C	Negative 1-wire devices supply contact.

## 4.2 Light indication

LED indicator	Operation	Value
<b>"NET2"</b> shows log on to GSM network statuses using card SIM2	Off	Not available or impossible to read SIM2 card.
	Flashing green	SIM2 card registration in GSM network in progress.
	Solid green	SIM2 card is registered in GSM network.
	Frequently flashing green	SIM2 card PIN code error.
	Flashing red	Number of flashes (below 10) show GSM field strength.

LED indicator	Operation	Value
<b>"NET1"</b> shows log on to GSM network statuses using card SIM1	Off	Not available or impossible to read SIM1 card.
	Flashing green	SIM1 card registration in GSM network in progress.
	Solid green	SIM1 card is registered in GSM network.
	Frequently flashing green	SIM1 card PIN code error.
	Flashing red	Number of flashes (below 10) show GSM field strength.
<b>"Data"</b> shows broadcasting	Solid green	The control panel memory contains unsent reports.
	Flashing green	Transmission of reports to indicated addresses.
<b>"PWR"</b> shows power supply status, programming mode.	All are off	Power is off or battery voltage is lower than 9.5 V.
	Flashing green	Supply voltage is sufficient.
	Flashing red	Low supply voltage (< 11.5 V).
	Flashes green and red in turns	Start-up of the control panel operation software (duration approx. 7 sec.).

## 5 System installation

### 5.1 Recommended installation procedure

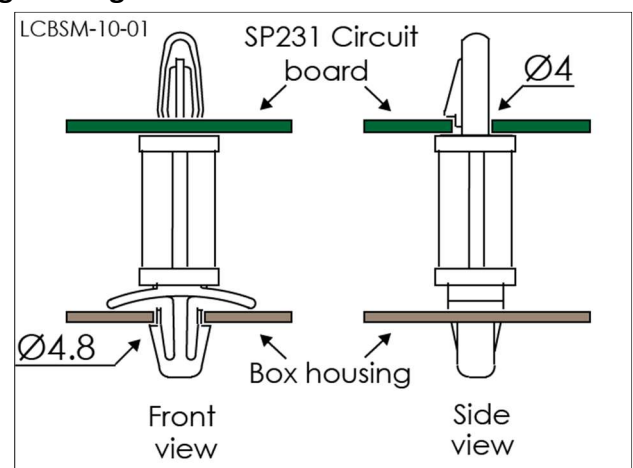
#### System planning:

- Draw the plan of premises and indicate the zones for installation of the mounting housing with a control panel, keyboard(s), indicators, equipment to be remotely controlled through the control panel or controlled automatically by the control panel.
- Upon assessment of the premises, requirements set to their protection and properties of possible sensors, select the types of sensors, their number and places, where they should be fastened.

#### 5.1.1 Control panel fastening in the mounting housing

The control panel circuit board shall be installed into the mounting housing equipped with the reducing transformer with 500 mA fuse and provided place for a back-up supply battery.

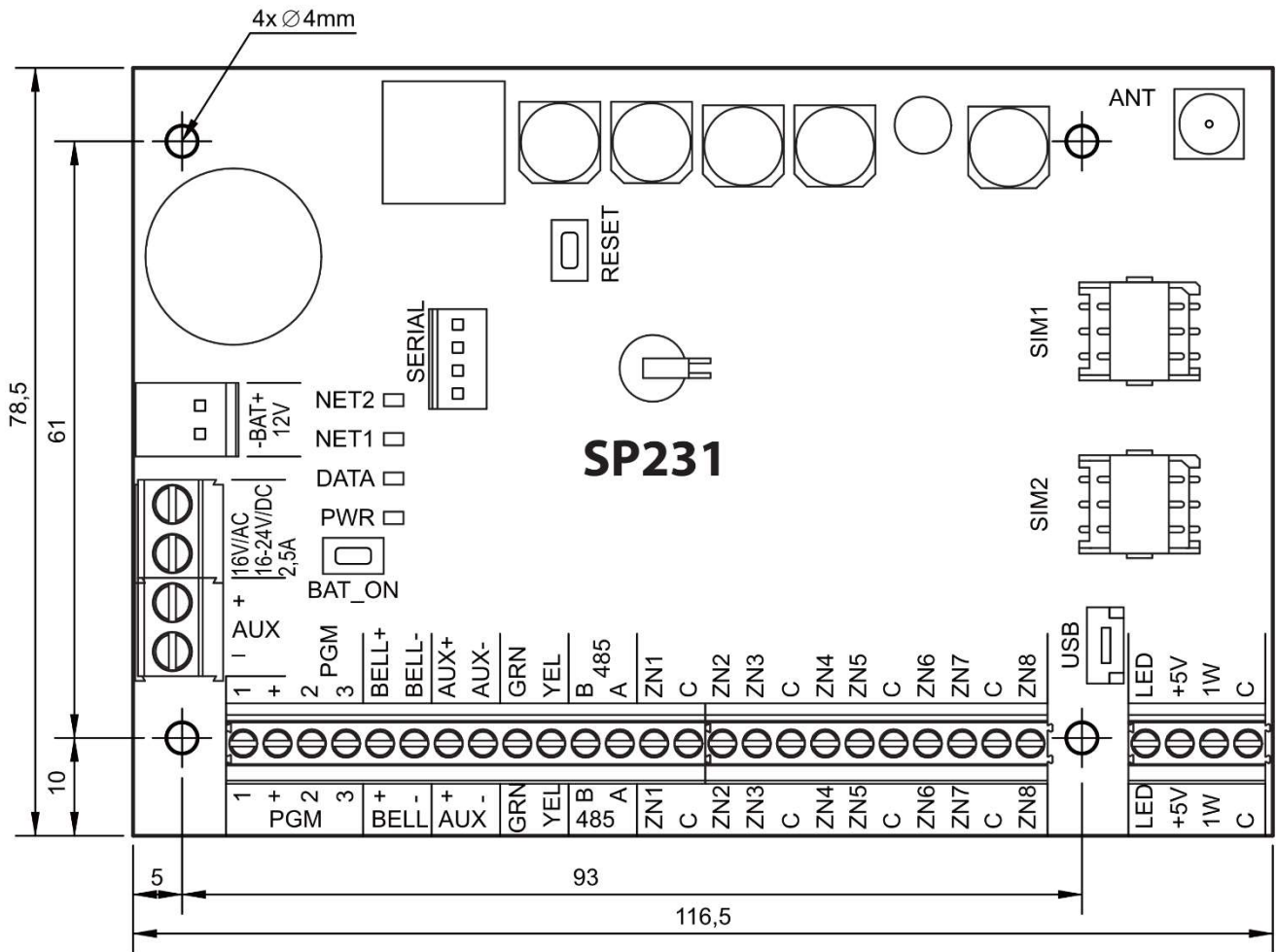
Reinforce the control panel into the selected plastic or metal mounting housing using plastic distance holders of the control panel circuit board. Upon choosing the metal housing, ensure its grounding during installation. The used housing must comply with the requirements of Standard EN 60950 and EN 50131.



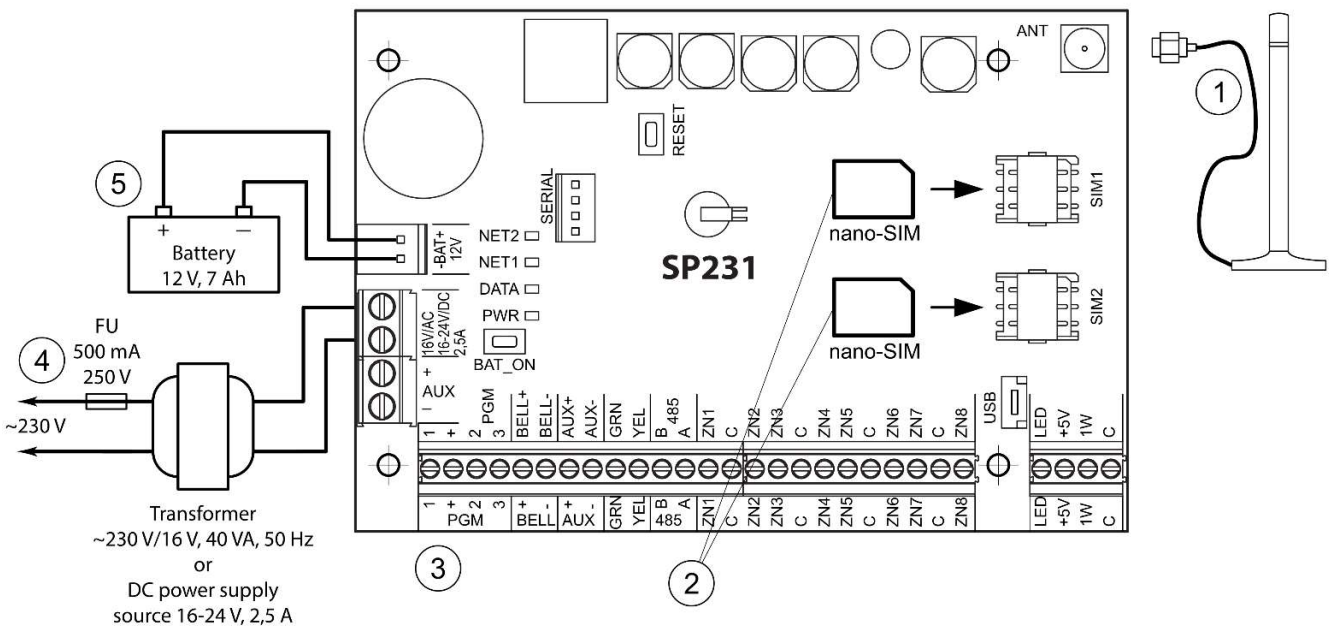
Plastic distance holders

### 5.1.1.1 SP231 circuit board dimensions

The figure shows the dimensions (in mm) of the control panel and its fastening holes and their locations.



### 5.1.2 Equipment connection sequence



1) Connect the GSM antenna to the antenna port.

- 2) Insert the SIM card(s), which are already registered in the GSM network, into the SIM card holders. Card holder SIM1 is the main card holder. The card inserted into SIM1 shall have a priority in operation, and SIM2 shall be operated only upon malfunction of SIM1.
- 3) Following the provided diagrams and connection diagrams of every product intended for connection, connect the magnetic contacts of windows and doors, motion, fire and other sensors, indicators, keyboards, controlled devices. Connect the housing door tamper sensors and wall mounted tamper sensors to the control panel terminals.
- 4) Connect the main supply source wires to the control panel AC/DC terminals. Switch the main supply on. SP231 shall automatically recognise the correctly connected keyboards, expanders, interfaces, sensors to the 1-wire and YEL/GRN buses and shall register them in the system.
- 5) Install a back-up supply battery into the mounting housing. Connect its wires to the control panel back-up supply source terminals BAT+ / BAT-. Verify the battery charging current to ensure it is charged in due time.

**Note:** The battery shall be fully charged no longer than within 72 hours so the alarm system complies with Grade II class or within 24 hours to comply with Grade III class.

### 5.1.3 Recommendations for setting the control panel operation parameters

- 1) The first log on to the control panel shall be via USB cable (see 6.1.1 „Connect with USB cable”).
- 2) System settings:
  - a. **Partitions**

If the premises have several areas, the protection of which is preferred to be switched on separately, the alarm system can be divided into partitions. Regarding dividing the system and setting the necessary partition attributes see 6.8 „Partition parameters”.
  - b. **Zones**

Parameters regarding setting of every zone according to sensor properties and preferred alarm operation after an event takes place in this zone. If the alarm system is divided into partitions, every zone can be assigned to the preferred partition. See 6.7 „Zone parameters”.
  - c. **Users**

In order to control the alarm system by means of a keyboard, iButton key or phone call (SMS message), the „User” level users shall be created. Regarding creating „User” and assigning the rights to them see 6.9 „User access parameters”.
- 3) Sending of reports:
  - a. **Time setting**

In order to receive the reports with a precise event timestamp, it is necessary to set clock time in the control panel, see 6.5.3 „Setting of control panel clock”.
  - b. **Enabling report sending**

In the control panel with manufacturer set primary configuration the sending function of all event reports is enabled. Regarding enabling or again disabling sending of the desired event report, see 6.19 “Setting of event reports”.
  - c. **SIM card parameters**

If report sending is provided via GSM/GPRS, it is necessary to set the parameters of used SIM card(s), see 6.10 „SIM card parameters”.
  - d. **Reports to the Central Monitoring Station**

Reports to the Central Monitoring Station shall be transmitted only via specified communication channels. Regarding setting of parameters for report transmission to the Central Monitoring Station see 6.11 „Report transmission to CMS”.
  - e. **Reports to user**

Event reports to the user can be sent by SMS messages, and by calling the system shall warn on occurrence of an event. Regarding correct setting of parameters for report transmission to the user mobile phone see 6.12 „Report transmission to user”.

4) System remote control:

a. **User access**

In remote mode (by phone call and/or SMS message) the alarm system can be controlled only by those users, whose phone numbers are entered into the user list. Regarding correct entering of the phone numbers see 6.9 „User access parameters”.

b. **Control by phone call**

By a phone call it is possible not only to switch on/off the protection of all or part of premises, but also control (start or stop) the equipment connected to PGM terminals. Regarding setting procedure so it was possible by a phone call to change the status of the preferred PGM terminal, which is connected to the equipment control circuit, see 6.14 „Control by call”.

c. **Control by SMS messages**

Using SMS messages it is possible to change some control panel operation parameters, switch on/off the protection of all or part of premises, also control (start or stop) the equipment connected to PGM terminals. The list of programming commands sent by SMS messages is as follows: 7 „Programming and control by SMS messages”, and regarding setting procedure so it was possible by SMS message to change the status of the preferred PGM terminal, which is connected to the equipment control circuit, see 6.13.2 „PGM output remote control”.

5) Extra:

a. **Changing of control codes**

It is recommended to change the manufacturer set default values of alarm control and control panel configuration codes that are known only to You.

- **Master** user code shall be changed in the software menu branch **Users**.
- **Remote SMS control code** shall be changed in the software menu branch **Reporting** column **SMS reporting and calls for users** field **User reporting**.
- **Log on to TrikdisConfig** shall be changed in the software menu branch **System options** column **System administration**.

b. **Registration of MCI modules**

If compatible equipment is connected to the control panel MCI data bus to be recognised by the control panel and made a communication with it, this equipment shall be registered manually. Regarding registering, see 6.15 “Transmission module registration”.

### 5.1.4 Alarm system operation testing

Upon completion of the alarm system installation, it shall be tested for correct operation.

#### 5.1.4.1 Walk-test function

Operation of sensors and siren can be tested by carrying out a **Walk-test** function by using Trikdis Protegus **SK130, SK232 or Paradox** keypad. The following shall be done:

1. Press the button **[OK]** (**[Enter]** – if using **Paradox** keyboard).
2. Enter installer (**Installer**) code.
3. Press the button **[TRB]** (**[TBL]** – if using **Paradox** keyboard).
  - a. The buttons **STAY** and **ARM** shall start flashing and the alarm shall switch over to the testing mode.
  - b. Due to change of the zone statuses, the sirens and keyboard buzzer shall beep by informing about the zone operation.
  - c. If during testing the sensor fuse has been tampered or the protection mode is on, the testing mode shall terminate automatically.

To switch off the mode, repeat the procedure as switching it on.

#### 5.1.4.2 Testing of report transmission system

If GRPS network parameters are correctly set with the Central Monitoring Station addresses, upon switching on the power supply to the system the following shall take place:

- a) A report E305 **System Reset** shall be sent.
- b) If compatible, but unregistered, modules are connected to the control panel YEL/GRN data bus, there shall be sent as many reports R333 **Expansion Module Restore** as there are to be newly registered modules.
- c) If in the control panel, communication control parameters the communication verification signal PING is on, a report E760 (Control panel PING signal) shall be sent. When the IP receiver gets the report, it shall start automatic control of the communication channel with the control panel.

Also, it is possible to manually formulate the communication testing report E602 (Periodical Test). It is recommended to inform in advance the security service about the testing.

Testing of the report transmission by using Trikdis Protegus SK130, SK232 or Paradox keypad shall be as follows:

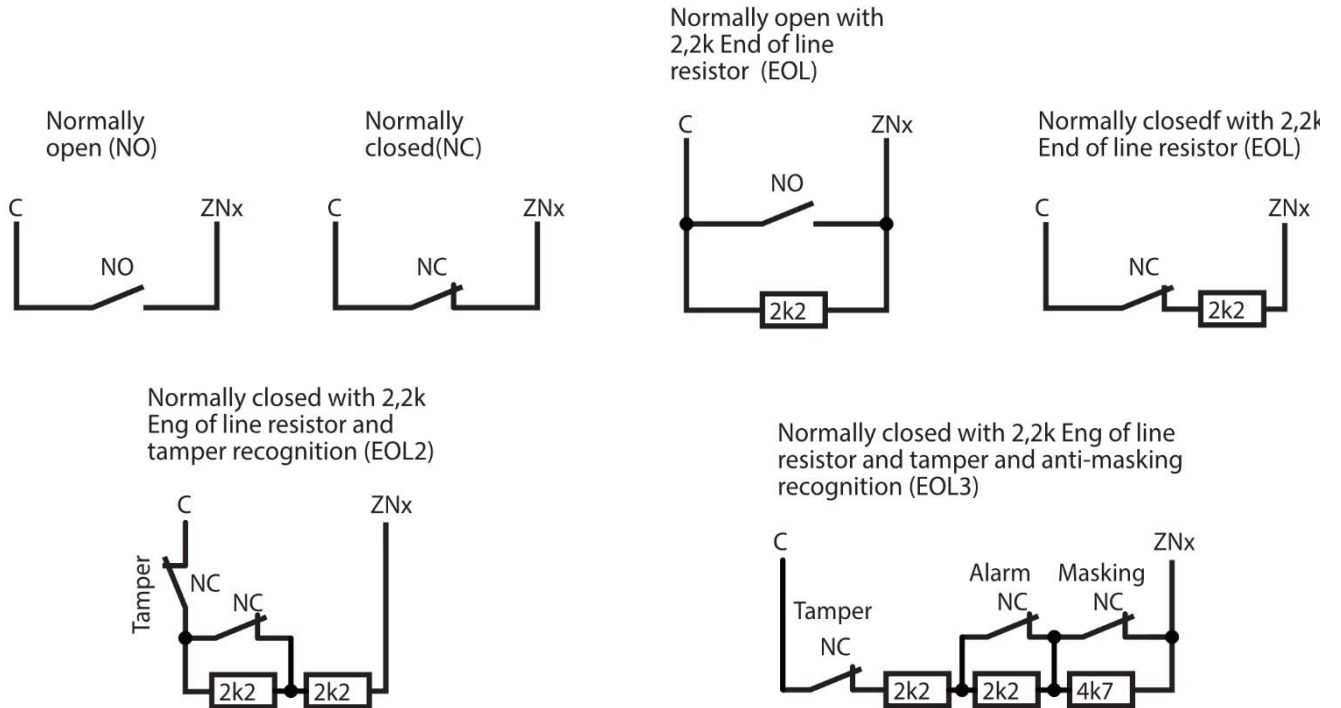
1. Press the button **[OK]** (**[Enter]** – if using **Paradox keypad**).
2. Enter installer (**Installer**) code.
3. Press the button **[MEM]**.

## 5.2 Compatible modules

Product code	Bus	Purpose	Current consumption
Trikdis PROTEGUS SK232LED W/B	Y/G	2 partitions, 32 zone LED keyboard with touch-sensitive keys, white or black glass surface	up to 150 mA
Trikdis PROTEGUS SK130LED W/B	Y/G	16 zone LED keyboard with touch-sensitive keys, white or black glass surface	up to 150 mA
Paradox K32+	Y/G	32 zone LED keyboard	up to 150 mA
Paradox K32LED	Y/G	32 zone LED keyboard	up to 150 mA
Paradox K10LEDV	Y/G	10 zone LED vertical keyboard	up to 100 mA
Paradox K10LEDH	Y/G	10 zone LED horizontal keyboard	up to 100 mA
Paradox K636	Y/G	10 zone LED keyboard	up to 100 mA
CZ8	Y/G	8 zone input expansion module	50 mA
E14	RS485	Ethernet communicator	70 mA
E16T	RS485	Ethernet communicator	70 mA
W17U	RS485	Wi-Fi communicator	lki 200 mA
RFMOD2	RS485	Radio module for wireless sensors	lki 200 mA
iO8	RS485	Input/output expansion module	lki 100 mA
CZ-DALLAS	1-wire	iButton key reader	up to 25 mA
DS18B20, DS18S20	1-wire	Temperature sensor Dallas. Measuring range from -55°C to +125°C	1 µA

### 5.3 Connection of sensors

The control panel circuit board has eight terminals **ZN1–ZN8** (inputs) for connection of sensor control circuits. When using input expanders (*CZ8*, *iO8*, *RFMOD2*), the number of outputs can be increased up to 32. Regarding setting of every input as a zone, i.e. assigning the zone attributes: circuit type (EOL, NC...), sensitivity to short-term circuit events, zone function (“Delay”, “Instant”...) see 6.7 „Zone parameters”.



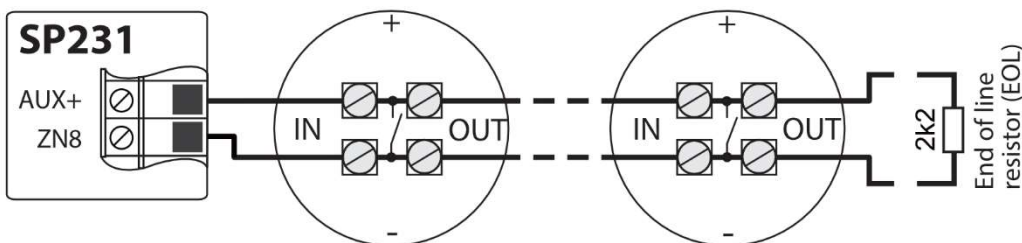
### 5.4 Connection of smoke detectors

In order to connect the control circuit of the smoke detector to the selected input, it is necessary that this input was “Fire” zone, i.e. this input must be with the set “Fire” zone function (see 6.7.1 „Main zone parameters”).

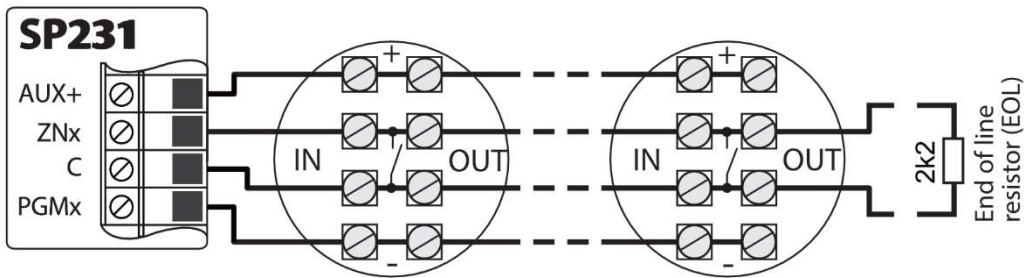
When connecting the four-wire smoke detector circuit to the selected PGM output, this output shall be with the set *Fire reset* function (see 6.13 „PGM output configuration”).

**ZN8** input can be dedicated namely for connecting the two-wire smoke detectors (see 6.7.1.2 „Setting of Fire zones”).

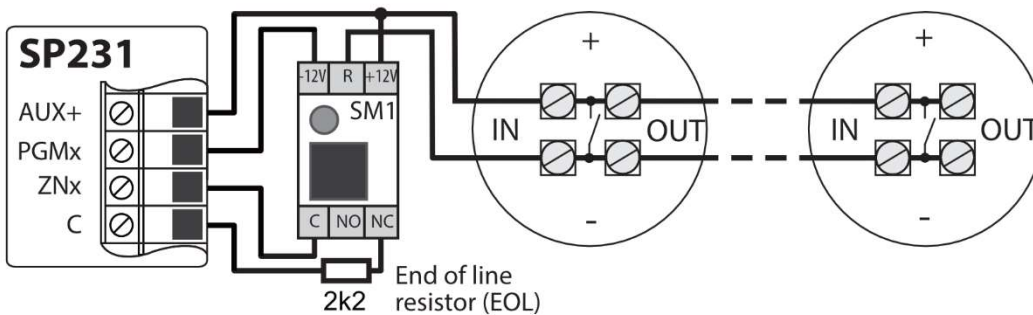
Two-wire smoke detectors.



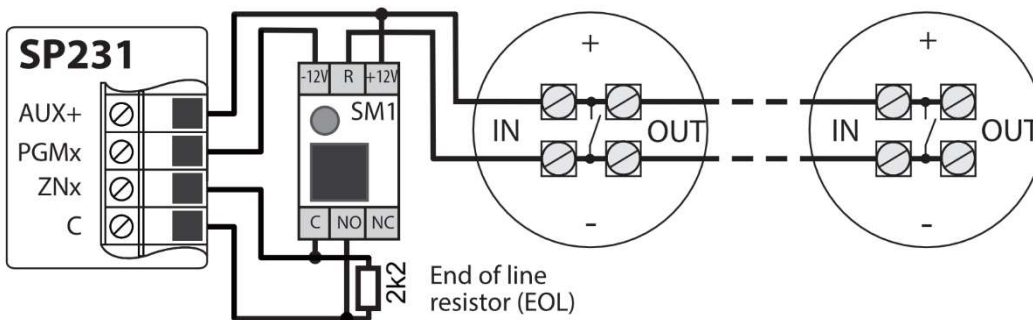
Four-wire smoke detectors.



or

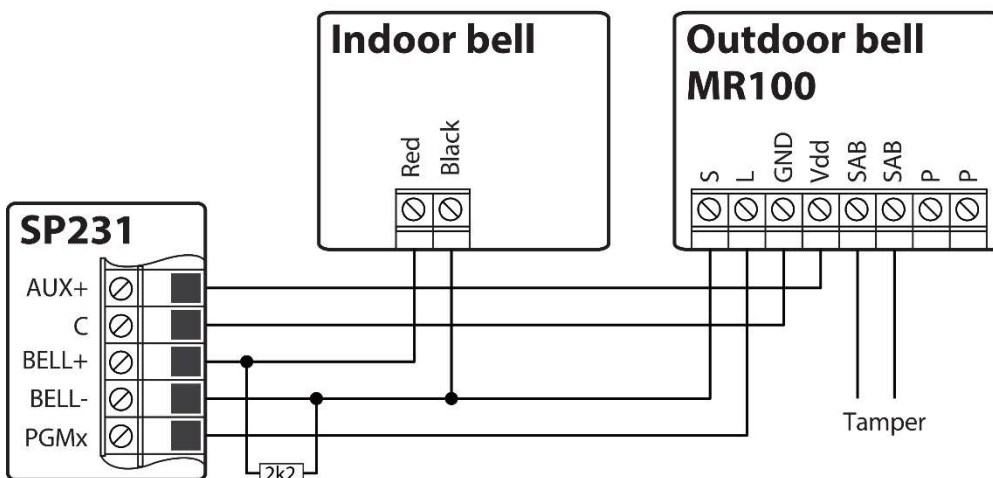


or



## 5.5 Connection of equipment terminals to PGM outputs

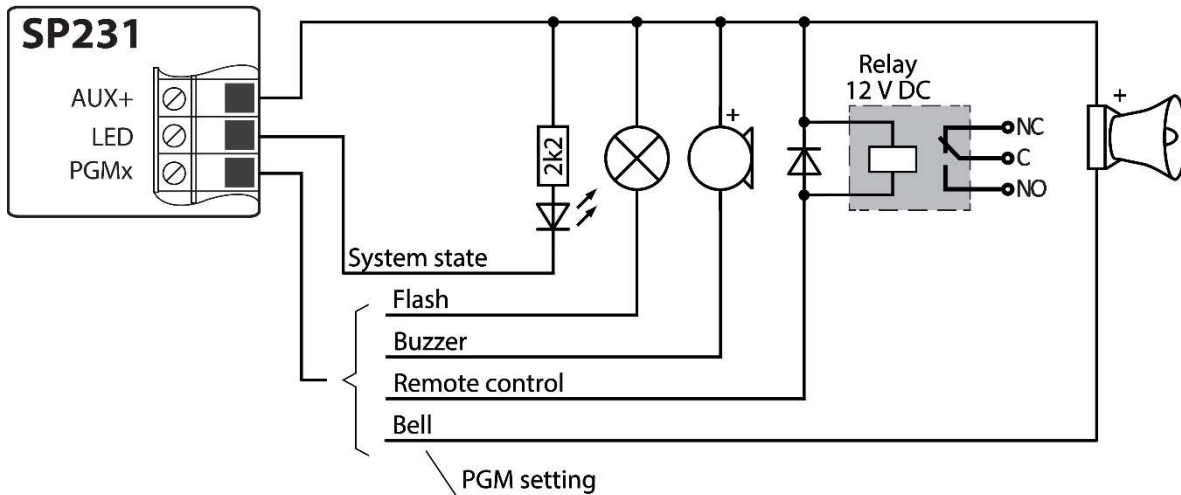
### Connection of sirens



PGM1-PGM3 - three terminals of open collector. BELL-(PGM4) - open collector terminal for connecting the siren. LED (PGM5) - collector terminal with 5K1 resistor. Regarding all possible operation modes of PGM outputs see 6.13.1 „PGM output operation descriptions“. Regarding changing of initial output values see 6.13 „PGM output configuration“.



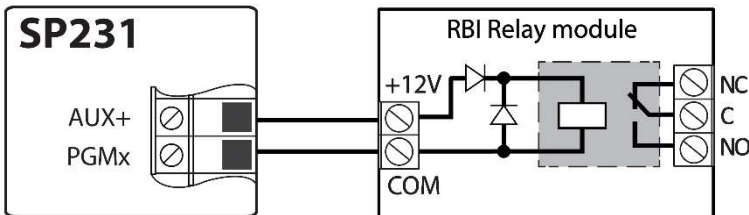
## Connection of alarm (controlled) devices



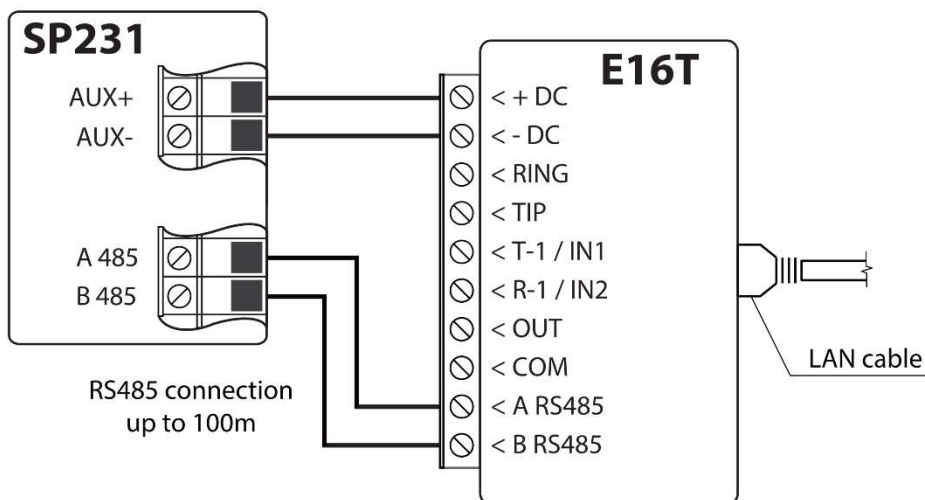
PGM initial settings:

1. Remote Control;
2. Remote Control;
3. Remote Control;
4. Bell;
5. System State.

## Connection of remotely controlled terminals

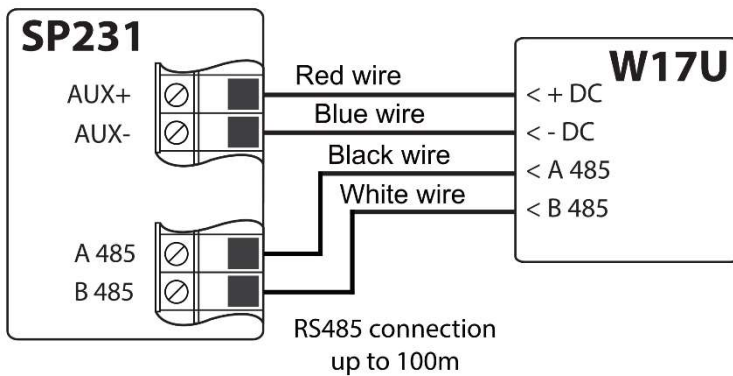


## 5.6 Connection of report transmission devices

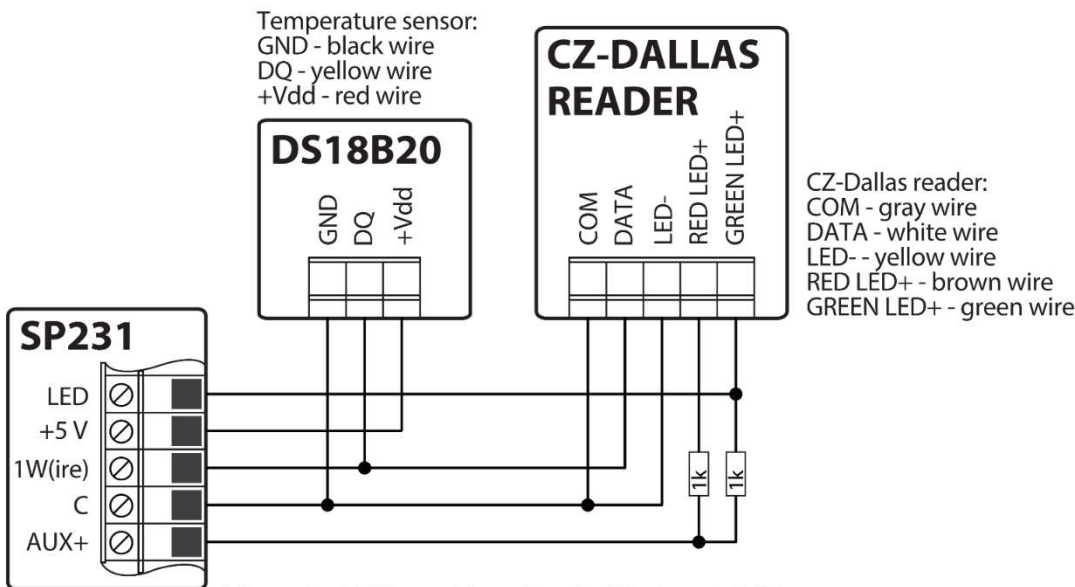


E16T configuration see 6.15 „Transmission module registration “. The control panel automatically recognizes and registers the connected device.

It is possible to connect the following modules to the bus RS485: **E14, E16T, W17U, RFMOD2, iO8.**



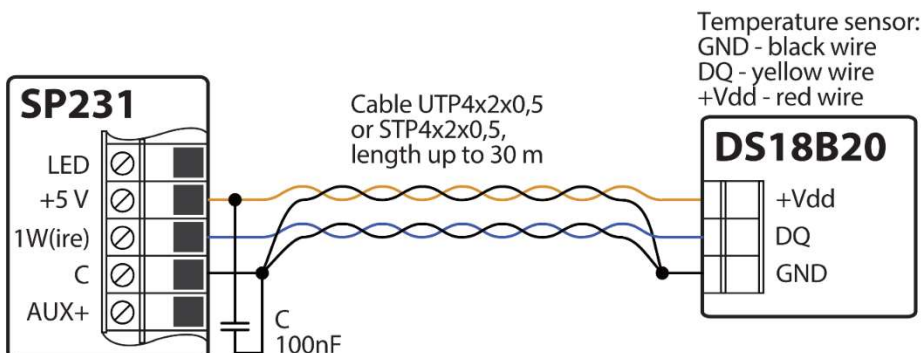
### 5.7 Connection of temperature sensors, iButton key readers



The output LED must be set to the "System state" type.  
 Security alarm system is arm - the iButton reader light is red.  
 Security alarm system is disarm - the iButton reader light is yellow.

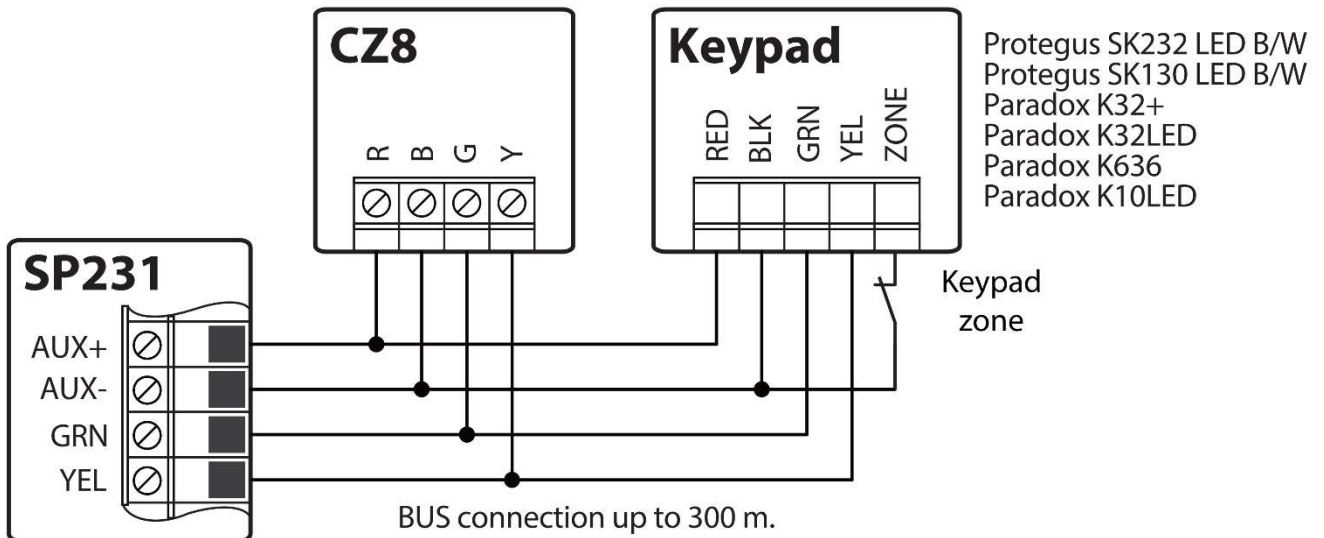
It is possible to connect iButton key readers and/or DS18B20 or DS18S20 temperature sensors to a 1-Wire data bus. The total length of the bus shall not exceed 30 m, with a possibility to connect up to 10 devices.

Circuit board terminal +5V is designed for supply of 5 V DC to devices connected to 1-Wire bus. Allowable output current shall not exceed 0.2 A. The output shall be protected against overload. Upon exceeding the allowable current, the supply shall be cut-off automatically. The control panel shall automatically recognise and register the connected devices.



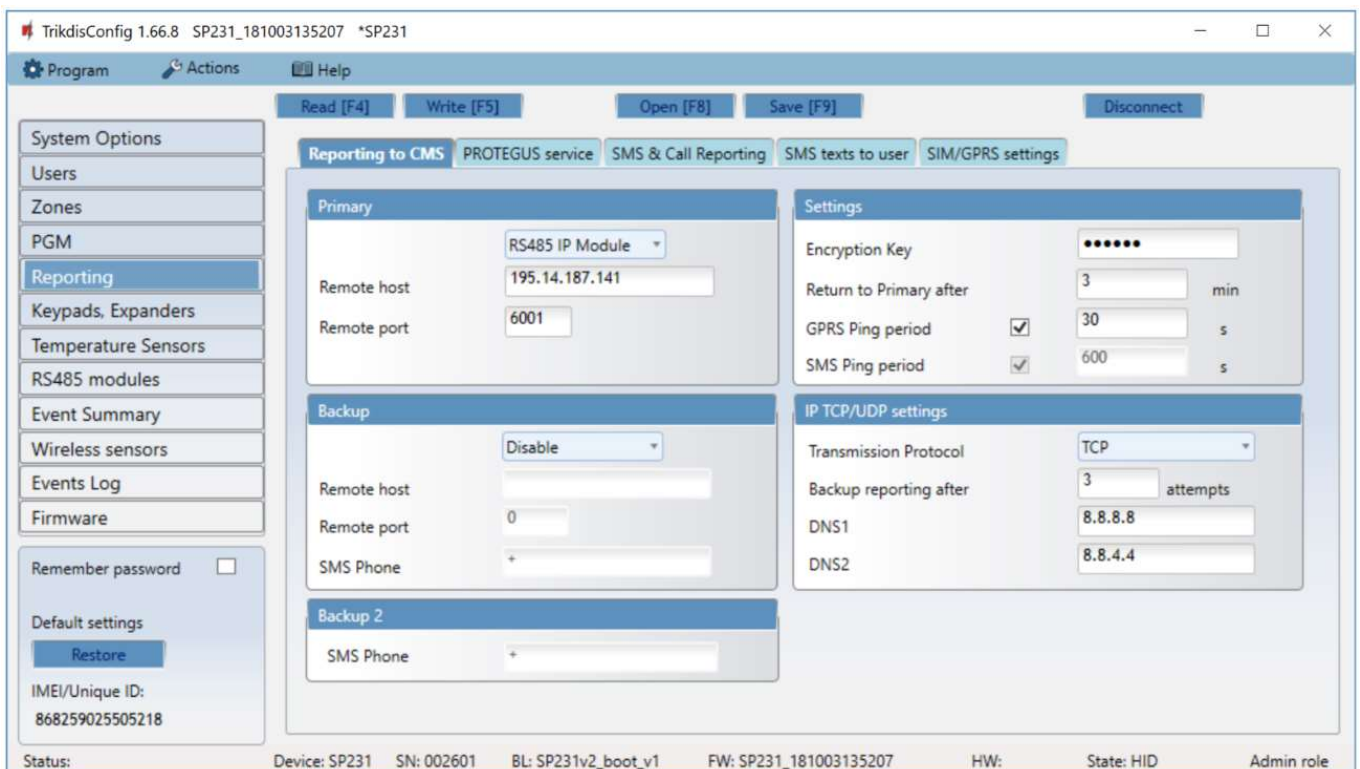
When connecting more than one sensor with longer than 0.5 m wires, for connections it is recommended to use twisted pair cable (UTP4x2x0,5, STP4x2x0,5).

## 5.8 Connection of keypads and input expanders

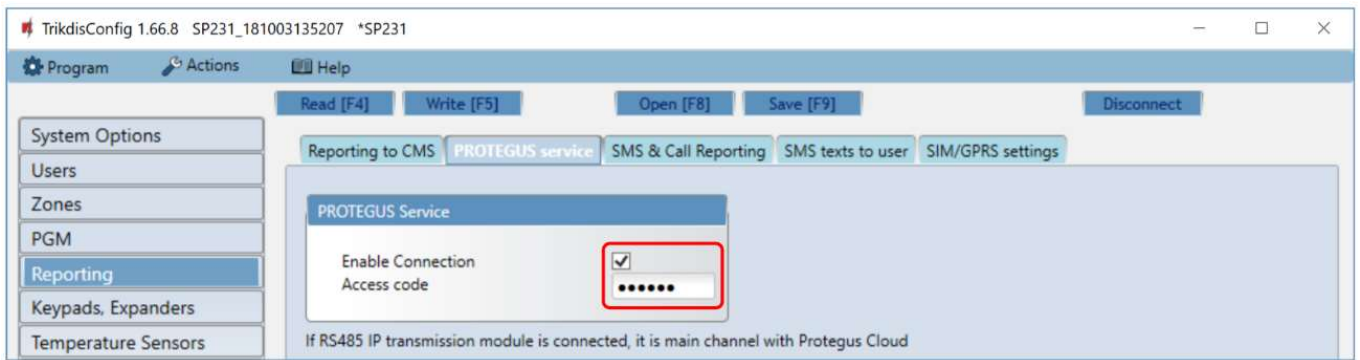


It is possible to connect up to 15 units (input expanders **CZ8** – up to 3 units; keypads – up to 12 units) to the keypad bus. The circuit board identifies and registers the connected units automatically.

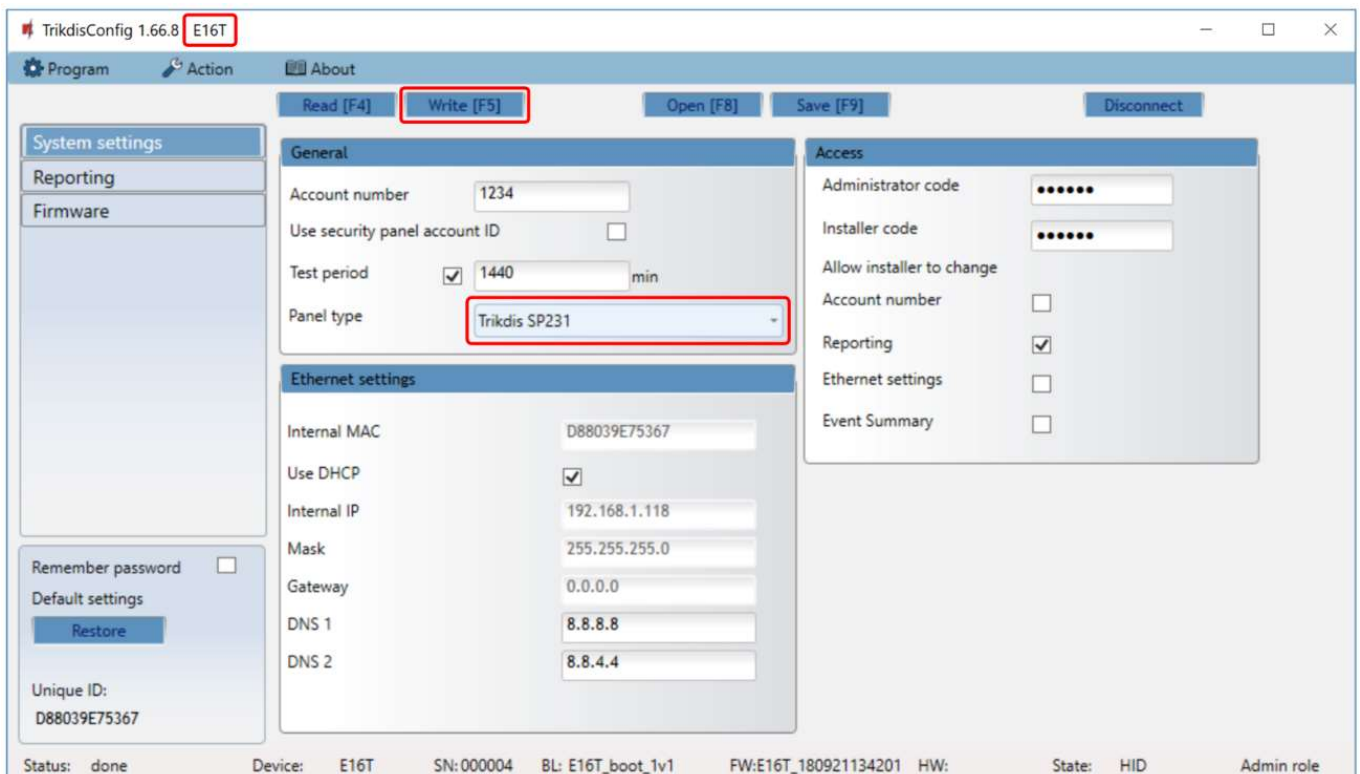
The 2-wire data bus *Y/G* (a.k.a. *YEL/GRN*) can be connected to „Trikdís” Protegeus SK232 LED B/W, Protegeus SK130LED B/W, “Paradox” K32+, K32LED, K636, K10LED keypads and/or input ZN number expanders CZ8. The total length of the bus shall not exceed 300 m, with a possibility to connect in parallel up to 15 devices. The control panel shall automatically recognise and register the connected devices. Regarding device unregistering see In TrikdísConfig application window, tab **Reporting** → **Reporting to CMS** it is necessary to set the main reporting channel to the unit **RS485 IP Module**. Both CSP IP address and the port number must be set.



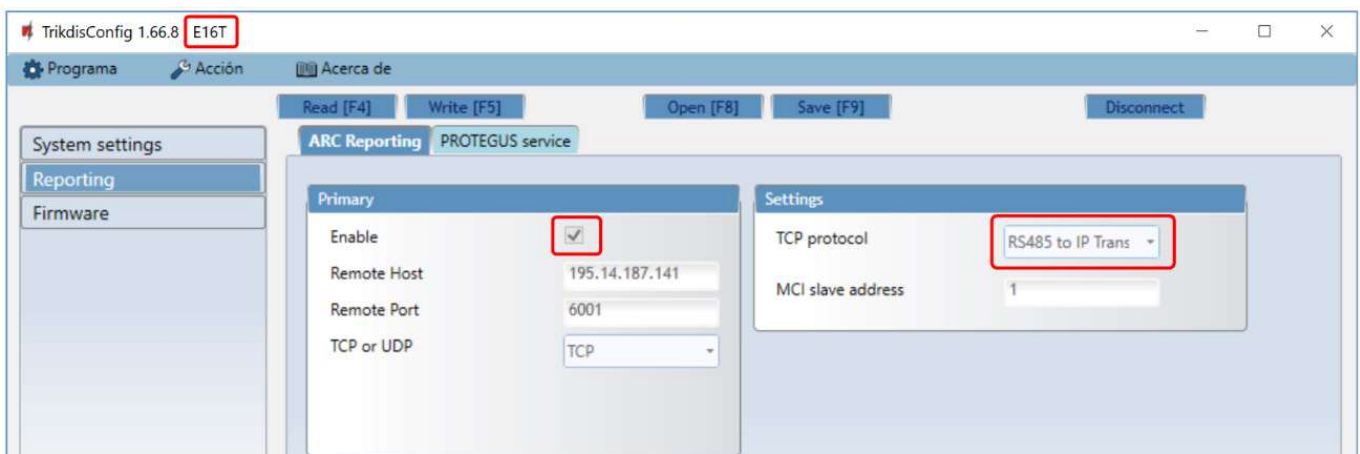
In the tab **PROTEGUS service**, the checkbox **Enable Connection** must be marked and the **Access code** must be assigned in the text box below.



The configuration of module **E16T** with **TrikdisConfig**. Plug in **E16T** to **TrikdisConfig** using a USB Mini-B cable. In **System settings** window it is necessary to provide the name of the control panel (**Trikdis SP231**) in the field **Panel type**. Press the button **Write [F5]** in order to save the settings to **E16T**.

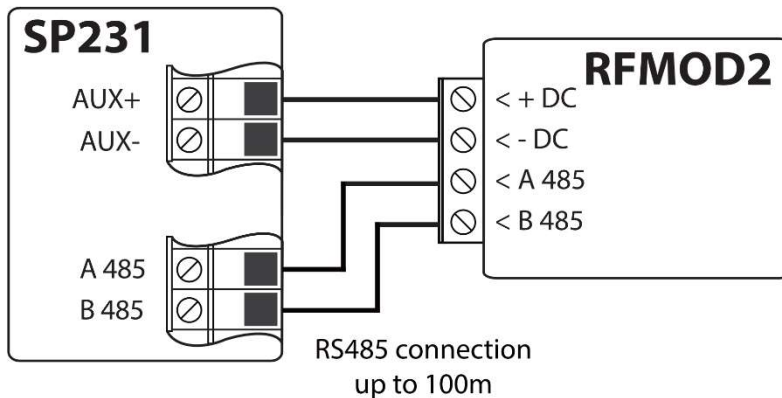


**E16T** will automatically set the type of TCP protocol to **RS485 to IP Transparent mode**.



Keypads and expanders registration”.

## 5.9 Connection of wireless sensors with RF-MOD2



Together with **RFMOD2** it is possible to assign up to 64 units of remote keyfobs, 16 units of wireless sirens and 32 units of wireless sensors to the security system.

In order to connect the wireless sensors, it is necessary to connect RF-MOD2 module to control panel. To register wireless sensors in the system refer to [6.17 „Wireless sensors registration”](#).

## 6 Configuration of control panel operation

The control panel parameters are set using software **TrikdisConfig**, which operates in *MS Windows* OS environment, the software is available on the website [www.trikdis.com](http://www.trikdis.com). It is possible to connect to the control panel by using a USB cable or remotely, by communicating with the control panel via GPRS communication. Some control panel parameters can also be changed remotely by SMS messages.

### 6.1 Connect to control panel

#### 6.1.1 Connect with USB cable

- 1) The computer shall have installed the following: parameter setting software **TrikdisConfig** and software **Microsoft.NET Framework 4**.
- 2) After the software is in place, connect the control panel and the computer with the USB cable. Power supply via USB port is sufficient to set the control panel operation parameters, so additional supply is not necessary. Start the parameter setting software **TrikdisConfig**. The software shall automatically recognise the connected device and open the window for its programming.
- 3) In order to read the parameters entered in the control panel, click the button **Read** and in the pop-up table enter your (*Admin* or *Installer*) code (if the administrator initial code exists, the code shall not be prompted).
- 4) After the first time reading of the control panel operation parameters, the software shall show the manufacturer set default control panel operation parameters. After changing the parameters, click the software button **Write** to enter the changes in the control panel memory. When configuration is complete, shut down the software **TrikdisConfig** and unplug the USB cable from the control panel USB port.

#### 6.1.2 Connect in remote mode

Configuration of the control panel settings in remote mode shall be carried out via GPRS communication. For software **TrikdisConfig** the appropriate GPRS communication settings shall be set. The manual of the control panel shows how to do it and how to connect by using **TrikdisConfig** software.

##### 6.1.2.1 GPRS communication settings

**Note:** When the *Grade 2/3* protection class setting function is enabled, the remote control and configuration function of the control panel shall be disabled automatically

- 1) Ensure that SIM card has a disabled PIN code protection.

- 2) Insert SIM card with enabled GPRS communication service into the control panel SIM 1 slot. For information how to enable this service please contact Your GSM service provider.
- 3) Add phone number the user, because only from listed numbers it is available to use all SMS commands. SMS commands must be sent to the inserted SIM card's number. Command to add new phone number:

**CFG[SMS password] \_ 01 \_ [USER Code] # [User Phone No.] #**

CFG – beginning of SMS command;

[SMS password] – six digit SMS password;

01 – command code;

[User code] – user code;

[User phone No.] – user phone number;

# - symbol to end value;

“\_” – marks the space symbol in SMS message.

An example adding a phone number to Master user, while using default password values:

**CFG123456 01 1234#+3706111111#**

- 4) Setup an inserted SIM1 card GSM network parameters. Command to set operator parameters:

**PSWXXXXXX \_ 12 \_ APN# LOGIN# PSW###**

PSW XXXXXX – beginning of SMS command and its password;

12 – changing network parameters command;

APN – gateway name (up to 50 symbols);

LOGIN – user name (up to 29 symbols);

PSW – user password (up to 29 symbols);

# - symbol to end value.

Example: **PSW123456 12 gprs.net#web#web###**

If network does not have user name nor password, fields must be left empty.

Example: **PSW123456 12 gprs.net#####**

- 5) Connection to the remote server must be enabled in a control panel. Command to enable connection:

**PSWXXXXXX \_ 94 \_ 1**

PSWXXXXXX – beginning of SMS command and its password;

94 – connection to the remote server command;

1 – connection enabling value (0 – to disable).

Example: **PSW123456 94 1**

- 6) It is required to know IMEI address of Control Panel. IMEI address can be found on product package or it can be requested by SMS command:

**PSWXXXXX \_ 97 \_ 5**

PSW XXXXXX – beginning of SMS command and its password;

97 \_ 5 – request about GSM field strength, modem IMEI number and control panel software version.

Example: **PSW123465 97 5**

#### **6.1.2.2 Remote log on through TrikdisConfig**

- 1) Make sure that the control panel is connected to supply source and in operation.
- 2) Start **TrikdisConfig** software.
- 3) At the field **Remote access**, in the field **Unique ID** enter the control panel GSM/GPRS modem IMEI address. IMEI address is provided on the product package.

- 4) In the adjacent field **System Name** enter the desired name to the module.
- 5) Press **Configure**. After successful connection the settings shall be saved.

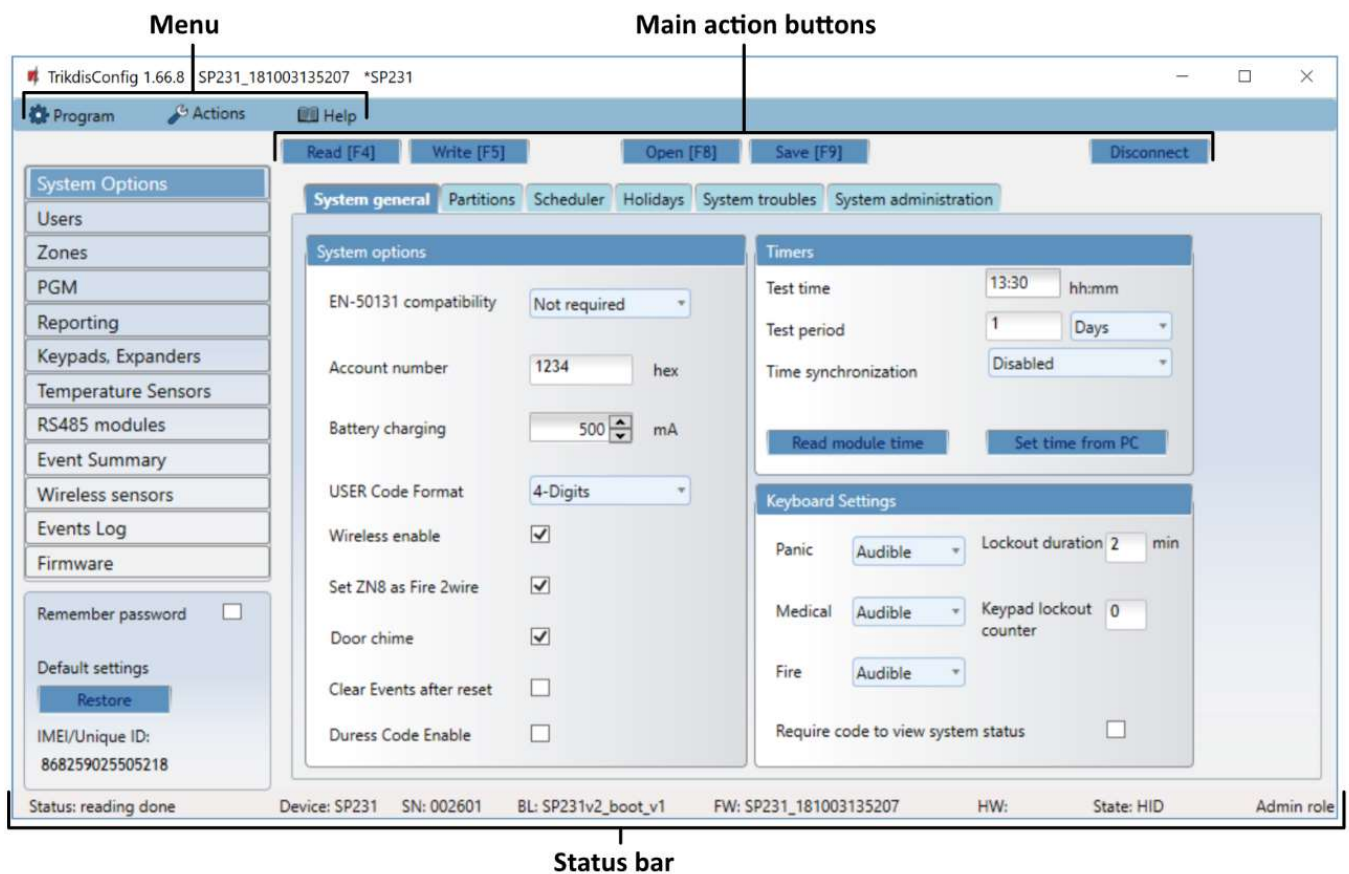
### 6.1.3 Changing of settings by SMS messages

Communication by SMS messages is designed for monitoring and control of the alarm system. The list of commands sent by SMS messages see 7 „Programming and control by SMS messages”.

To activate this function, perform the following actions:

- 1) Insert the SIM cards, which are already registered with the GSM network provider, into the SIM card holders.
- 2) Complete adding phone number to user command as instructed in 6.1.2.1 „GPRS communication settings” the third point in a list. Because only from listed numbers it is available to use all SMS commands.

## 6.2 Description of TrikdisConfig program



### Menu

Name	Value
Program	Information about the program language and licence.
Action	Program control actions.
Help	Supplementary information about the module and the software.

### Main action buttons

Name	Button meaning
Read [F4]	Read the control panel parameters

### Status bar

Name	Value
IMEI/Unique ID	IMEI address of the device

Name	Button meaning
Write [F5]	Write the control panel parameters into module
Open [F8]	Open the saved file of parameters
Save [F9]	Save the file of parameters
Logout	User logout

Name	Value
Status	Action status
Device	Device type
SN	Serial number
BL	Boot loader version
FW	Control panel firmware version
HW	Equipment version
State	Log on status
Role	Access level

## 6.3 User access

### 6.3.1 Control panel configuration

To set access go to the program menu **System Options > System administration**. Three levels for parameter configuration access are available. Upon login with the access code it can be saved by checking **Remember password** field.

#### 6.3.1.1 Administrator (Admin)

The highest level of **Admin** who is able to change all the control panel parameters and apply restrictions to other users. Admin access code may be changed but cannot be deleted. The above can be done by clicking **Change** button at **Admin (Distributor) Code** and entering the existing and new codes in the pop-up table.

#### 6.3.1.2 Installer

The lower level of **Installer** who is able to change Admin allowed parameters. Installer access code can be changed by Admin and Installer in the **Installer Code** field. Installer rights can be changed in the **Installer permission** field.





**Installer rights parameters**

Name	Description
Account Number	Object identification number ( <i>Account number</i> ) can be changed upon marking a checkbox.
Tab "Sim/GPRS settings" Menu "Users" Menu "Zones" Tab "CMS Reporting" Tab "User Reporting" Menu "Event Summary" Protegus service	Installer rights to the selected section are indicated: Editable – to edit, Visible – to see, Hidden – not to show.

**6.3.2 Control panel control**
**6.3.2.1 Master user**

The only one **Master** user, who is allowed to change the statuses of attributed partitions, add or delete users, change its own or other user passwords, can be in the alarm system. See "Control panel SP231. Operation manual" for control options and 6.9 „User access parameters”.

**6.3.2.2 User**

The alarm system can involve up to 39 **Users**. They can turn on the preferred arming mode, activate or turn off the equipment connected to PGM outputs. Control options are provided in the document "Control panel SP231. Operation manual".

**6.4 System user initial login codes**

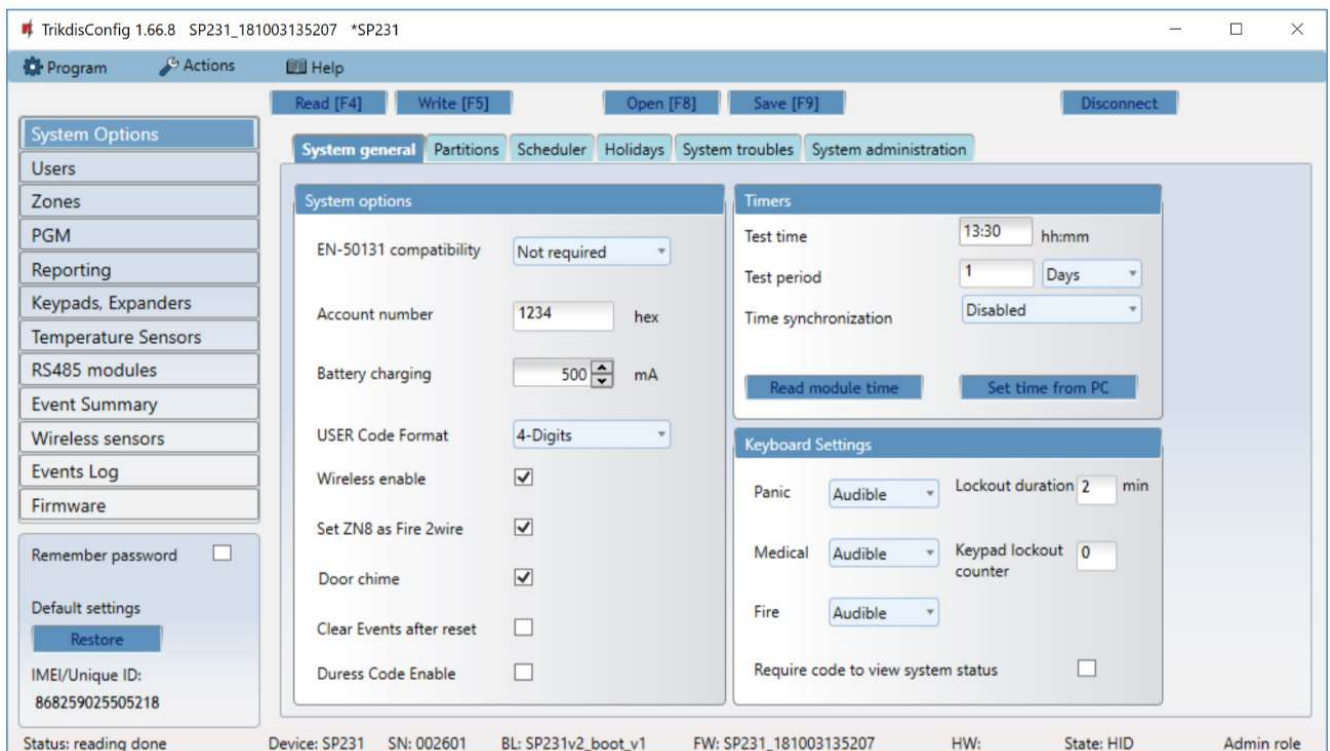
Type of code	Purpose	Factory setting code value
<i>Master</i> user	To control the system by keyboard.	1234 (4 digit format)
		123412 (6 digit format)
<i>Remote</i> user	To control the system in remote mode (SMS messages).	123456
<i>Administrator</i> user	To configure the control panel operation parameters by "TrikdConfig" software.	123456
<i>Installer</i> user	To configure the control panel operation parameters by "TrikdConfig" software and to perform various functions via keypad.	0000 (4 digit format)
		000000 (6 digit format)

**Notes:** Login code values can be changed. Having reset factory settings for control panel operation, the login codes will become the initial too.

## 6.5 System parameters

### 6.5.1 General system parameters

To set general control panel operation parameters go to the program menu **System options > System general**.



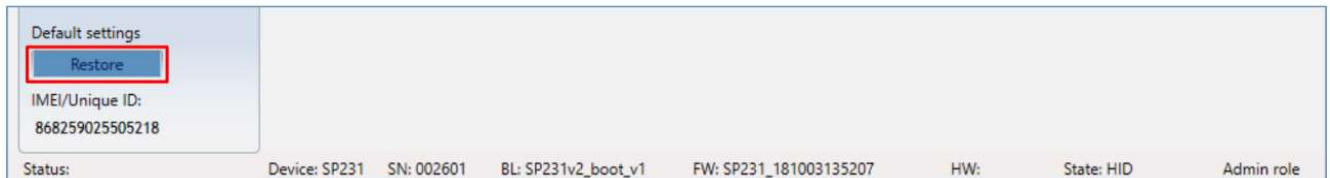
#### General parameters

Name	Description
EN-50131 compatibility	A box designated to set security grade of the alarm system. Upon choosing Grade 2 or Grade 3, the parameters, ensuring the control panel operation under selected grade security requirements, will be set automatically. The only parameters which do not lower the security grade will be allowed to be changed.
Account Number	A box designated to enter 4 digits object identification number. Hexadecimal system numbers are allowed to use.
Battery charging	A box designated to set a battery charging current. When Grade 2 security is set, the control panel must fully charge the battery no longer than within 72 hours or within 24 hours if Grade 3 security is set.
USER Code Format	User control code length - 4 digits or 6 digits - is to be set. In case of 4 digit code and having selected the code format of 6 digits the first two digits are transferred to the end, i.e. Code 1234 will be 123412.
Set zn8 as 2wire	When this box is checked, two-wire smoke detectors can be connected to ZN8 (see 6.7.1.2 „Setting of Fire zones”)
Door chime	When this box is checked, violations of set <i>Delay</i> zones at the alarm turned off will be accompanied by keyboard audible (Buzzer) signal (see. 6.7.1.1 „Door Chime function.”)
Clear Events after reset	When the cell is checked, the memory of unsend reports will be deleted after the control panel resetting.

Name	Description
Duress Code Enable	Enable Duress Code. After entering Duress code, the security system will immediately broadcast the alert message to CMS.

### 6.5.2 Resetting of initial parameters

The control panel factory settings can be reset. Click **Restore** button in the **Default settings** box under the main menu branch.



### 6.5.3 Setting of control panel clock

The control panel sends reports with timestamps. To set the control panel clock go to **System Options > System general > Timers**.

- The control panel clock can be set automatically and stay synchronised or can be set manually:
  - To set the clock automatically, at **Time synchronization** choose a source (Primary channel, Protegus server) to which time will be set.
  - To set the clock manually, click **Set time from PC** button and the clock will be set using computer's clock.
- To view control panel time, click **Read module time**. After the click the program will display current control panel time above the button.

### 6.5.4 Regular connectivity checks

Control panel can regularly report its status. If Grade 2 or Grade 3 security level is used, connectivity check reports must be configured. Based on the time set control panel will send reports to:

- User, if **User Reporting** is on and **Test/Misc** is checked (see 6.12 „Report transmission to user“)
- Centralised Monitoring System, if **CMS Reporting** is on (see 6.11 „Report transmission to CMS“)

For reports to be sent to the user, **Enable** must be checked at **Event Summary > 37 Periodical Test 602**. Periodical test report also includes additional information about GSM signal strength, control panel power supply and battery statuses. This information is sent to the Central Monitoring System separately. For CMS to receive it, **Event Summary > 41 GSM Level 660** must be checked. This setting is on by default in factory settings.

Connectivity checks can be done in two ways: with day-based or minute-based reference time. Settings for connectivity checks can be adjusted in **System Options > System general > Timers**.

- Day-based reference reports can be sent at the defined time at the specified interval in days. Choose **Days** under the **Test period** and enter the number of days between check reports sent. Enter report sending time in the **Test time** field.
- Minute-based reference reports can be sent at the specified interval in minutes. Choose **Minutes** under the **Test period** and enter the period specifying the frequency of sending the reports. Reference time counting will begin with control panel restart and occur for the first time once the settings are entered in the control panel by clicking the **Write** button.
- Connectivity checks are off if **Test disable** is selected under the **Test period**.

**Note.** Under security Grade 2 the maximum length of test period – 1 day, under security Grade 3 the maximum length – 1 minute.

## 6.5.5 Keyboard parameters

### 6.5.5.1 Keyboard lockout

Keyboard lockout function is activated after the respective number of unsuccessful attempts to enter the control codes, and it shall be blocked for the selected period of time, when the period passes keyboard will be locked after every unsuccessful attempt. After keyboard lockout, the report **Access denied** is being generated and sent. At Grade 2 or Grade 3 security, the number of allowable incorrect attempts is from 3 to 10.

Keyboard lockout is to be set in **System Options > System general > Keyboard Settings**:

- Set the number of attempts in **Keypad lockout counter** field.
- Set the lockout time (in minutes) in **Keypad lockout duration** field.

### 6.5.5.2 Emergency help button modes

The keyboard can send emergency calls **Panic, Medical, Fire**.

Their operation modes are to be set in **System Options > System general > Keyboard Settings** field, by selecting the respective mode:

**Silent** – silent mode without activation of siren and light alarm.

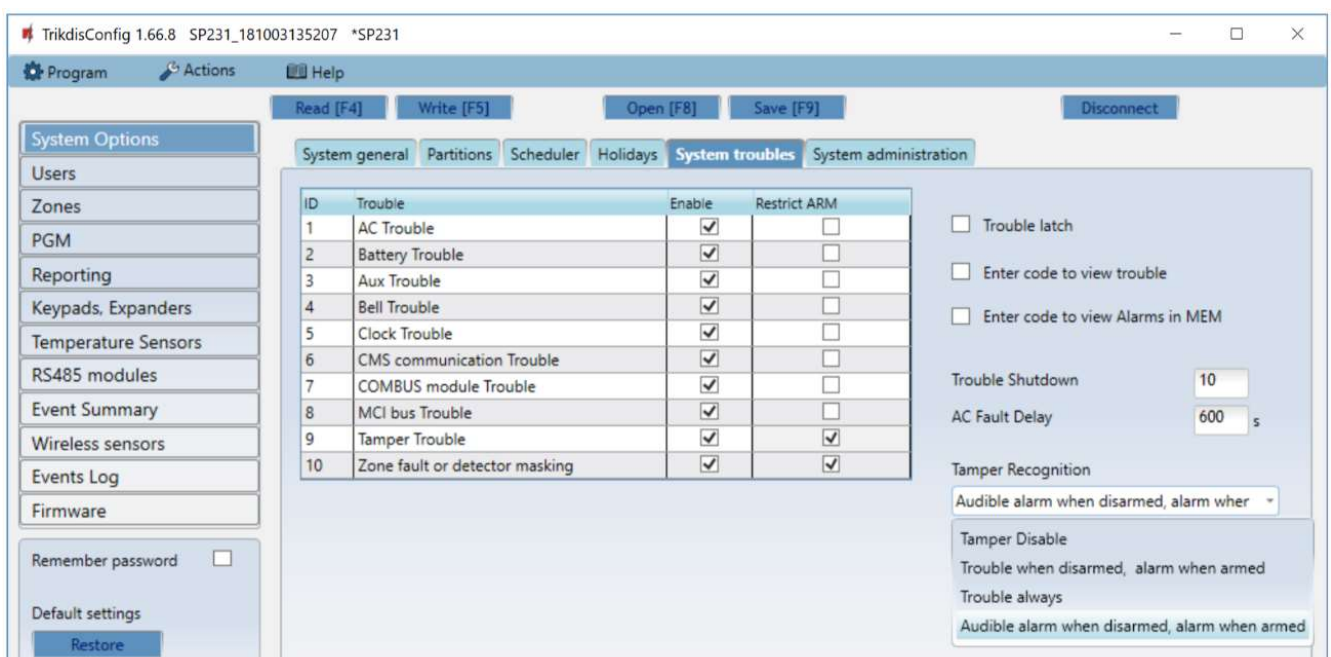
**Audible** – audible mode when keyboard and bell sirens, and light indicator are activated.

### 6.5.5.3 Display of the system state

Keypad can constantly display the state of the partitions. Constant status display can be disabled and to temporary view a partition state a user code must be entered. To enable this function, go to **System Options > System general > Keyboard Settings** and select **Enter code to view system state**. If security Grade 3 is set the function is enabled automatically.

## 6.6 System troubles

For the control panel to display trouble in the keyboard or to send a trouble report after troubleshooting, can be set in the program menu **System Options > System Troubles**. Also an option to turn on the mode ARM in case of trouble.



ID	Trouble	Enable	Restrict ARM
1	AC Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	Battery Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	Aux Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	Bell Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Clock Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	CMS communication Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	COMBUS module Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	MCI bus Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9	Tamper Trouble	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Zone fault or detector masking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Trouble latch  
 Enter code to view trouble  
 Enter code to view Alarms in MEM  
 Trouble Shutdown: 10  
 AC Fault Delay: 600 s  
 Tamper Recognition: Audible alarm when disarmed, alarm when armed

**Trouble parameters, first part**

Name	Description
ID	Trouble identification number
Trouble	Trouble name
Enable	When it is checked the trouble indication and trouble report sending will be on.
Restrict ARM	When it is checked, in case of such trouble, the arming activation will be restricted.

**Trouble descriptions**

Trouble name	Description
AC Trouble	Missing main power source.
Battery Trouble	Back-up battery is missing or below its voltage limit.
Aux Trouble	Exceeded current limit or short-circuited AUX output.
Bell Trouble	Missing siren.
Clock Trouble	Internal-clock time is not set or set inaccurately.
CMS communication Trouble	Connection lost with CMS.
MCI bus Module Trouble	Transmitter is not detected in MCI bus.
Tamper Trouble	Tamper detection.
Zone fault or detector masking	Zone or anti-masking circuit interrupted.

**Trouble parameters, second part**

Name	Description
Trouble latch	When it is checked, the function of troubles storage in memory will be on. Then, User wishing to enable the arming first of all must review the troubles occurred and clear their memory, and afterwards enter its code and enable the arming. If it is not checked, the trouble indication will operate in real time (trouble occurs - keyboard LED indicator is lighting).
Enter code to view trouble	When it is checked, the necessity for entering the control code to view trouble will be on.
Enter code to view alarm in MEM	When it is checked, the necessity for entering the control code to view actuations memory will be on.
Trouble Shutdown	Setting of the allowable number of the same trouble event, where in case of excess of such number the trouble reporting will be off. The number of such events is counted until the arming mode is changed (On/Off)
AC Fault Delay	Delay in generating the report on AC network interruption/recovery. Response time to short-term AC network interruption/recovery is to be set, i.y. report on interruption/recovery will not be generated if the event time is shorter than set in the box.
Tamper recognition	It must be set how the security control panel will function after sabotage event (tamper) recognition.

### 6.6.1 Tamper recognition

How the control panel will operate after tamper recognition can be selected in the program menu **System Options** > **System Troubles** > **Tamper Recognition**. How to enable the zone tamper tracking, see 6.7 „Zone parameters”.

#### Operation after tamper event

Name	Description
Tamper Disable	Response to tamper events is disabled.
Trouble when disarmed / alarm when armed	When disarmed, the tamper event will mean system trouble, and when armed, the tamper event will mean alarm.
Trouble always	Response to as problem is always on.
Audible alarm when disarmed / alarm when armed	When disarmed, the tamper event will be accompanied by siren sound, and when armed, the tamper event will mean alarm.

### 6.6.2 Control panel watch-dog

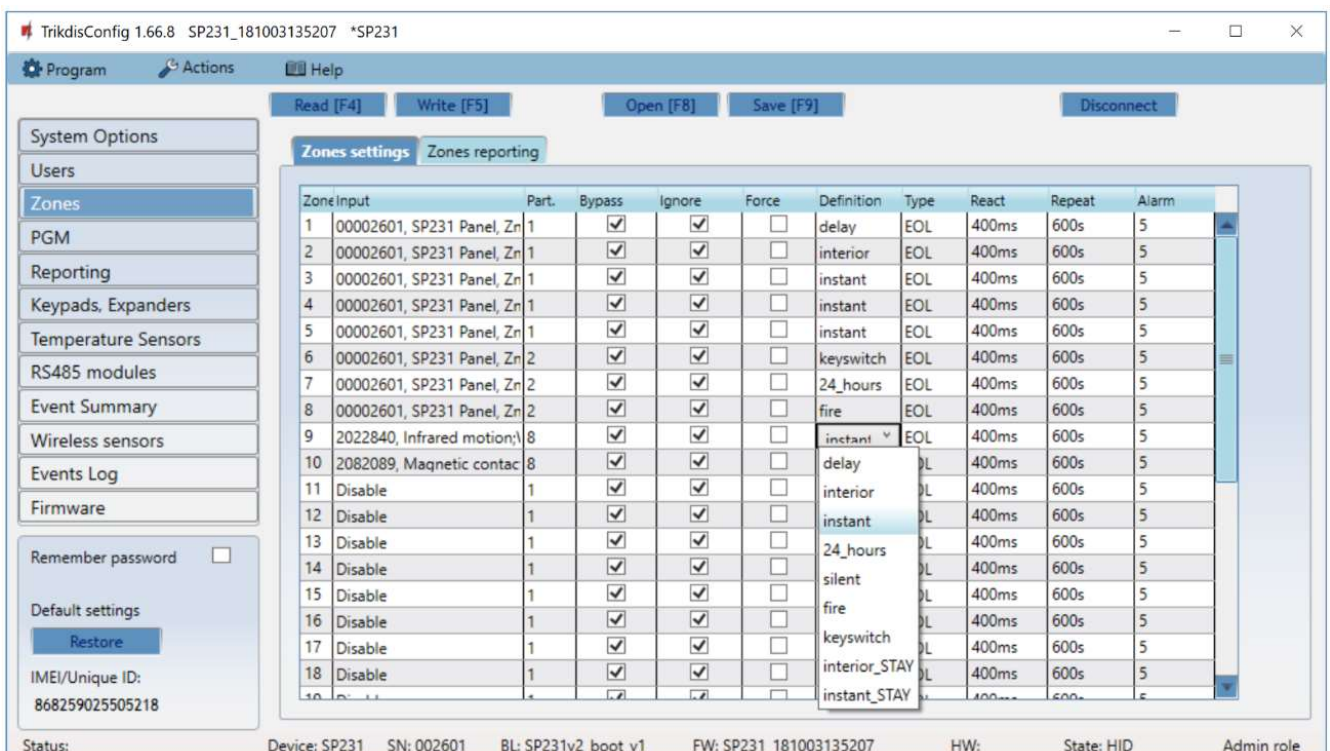
Control panel continuously monitors its functioning and whenever its work gets disrupted it resets and returns to its previous state. After system reset the **System reset** event is generated.

## 6.7 Zone parameters

### 6.7.1 Main zone parameters

Each ZNx input may be described as a separate zone. To set separate zone parameters go to the program menu **Zones** > **Zones settings**.

**Convenient!** Double-click with mouse left button on the selected zone line to open such zone settings window.



#### Zone parameters

Name	Description
Zn	Zone sequence number
Input	Zone physical address. Information displayed: <module identification number>, <module name>, < ZNx input number>.
P	Zone belonging to partition. Each zone can be attributed to the preferred partition.
Bypass	When it is checked, the option to activate the zone <b>Bypass</b> function during operation will be on. The function allows disabling, for instance, the zone affected by trouble, in order the system can be armed despite of such fault.
Tamper	Tamper tracking function will be on when it is checked. When the sensor circuit of type "normally closed circuit with end of line resistor and tamper tracking" is connected to the ZN contact and having the event occurred, the system will recognize whether it is the alarm event or tamper event. If such event is recognized as tamper event, the system will start operating under the operation type set in <b>System fault &gt; Tamper Recognition</b> (see 6.6.1 „Tamper recognition“).
Shutdown	When it is checked, the function of short-term zone shutdown will be on. During the armed mode, when the particular number of zone events set in <b>Alarm</b> has occurred, the other events of the same zone will not be responded for the time set in <b>Repeat</b> . After this time expired (or when disarmed), a new count of the number of zone events will be started.
Force	When it is checked, the activation of <b>Force Arm</b> mode will be available. i.e. the arming will be allowed when the zone is violated. If the violated zone after the arming enabled, resets to its normal status, then, in case of later zone event it will be responded.
Mask.	Anti-mask tracking function will be on when it is checked. When the sensor circuit of type " Normally closed circuit with tamper anti-masking recognition " is connected to the ZN contact and having the event occurred, the system will recognize whether it is the alarm or tamper or anti-masking event.
Definition	One of 9 potential zone functions can be set. How the system restarts operating after the zone event (sensor response and reset signal displaying) depends on the set zone function. For zone functions see 6.7.3 „Zone function description“.
Type	Set which type of sensor circuit connected to ZNx input should be tracked. Options available: <i>NC – Normally Closed, NO – Normally Open, EOL – End Of Line.</i>
Delay	Setting of zone sensitivity The zone events shorter than ones set in the box will not be responded.
Repeat	Insensitive time to recurrent zone events For more details see <b>Shutdown</b> .
Alarm	The maximum allowable number of recurrent zone events. For more details on operation see <b>Shutdown</b> .

#### 6.7.1.1 Door Chime function.

At OFF/DISARM mode, the control panel can for a short while activate PGM output with the set **Buzzer** function and keyboard audible signal - buzzer and thereby to warn that Delay zone is being violated, i.e. door opening/closing. For activation of **Door Chime** function, **Door chime** box must be checked in **System Options > System general > System options**.

#### 6.7.1.2 Setting of Fire zones

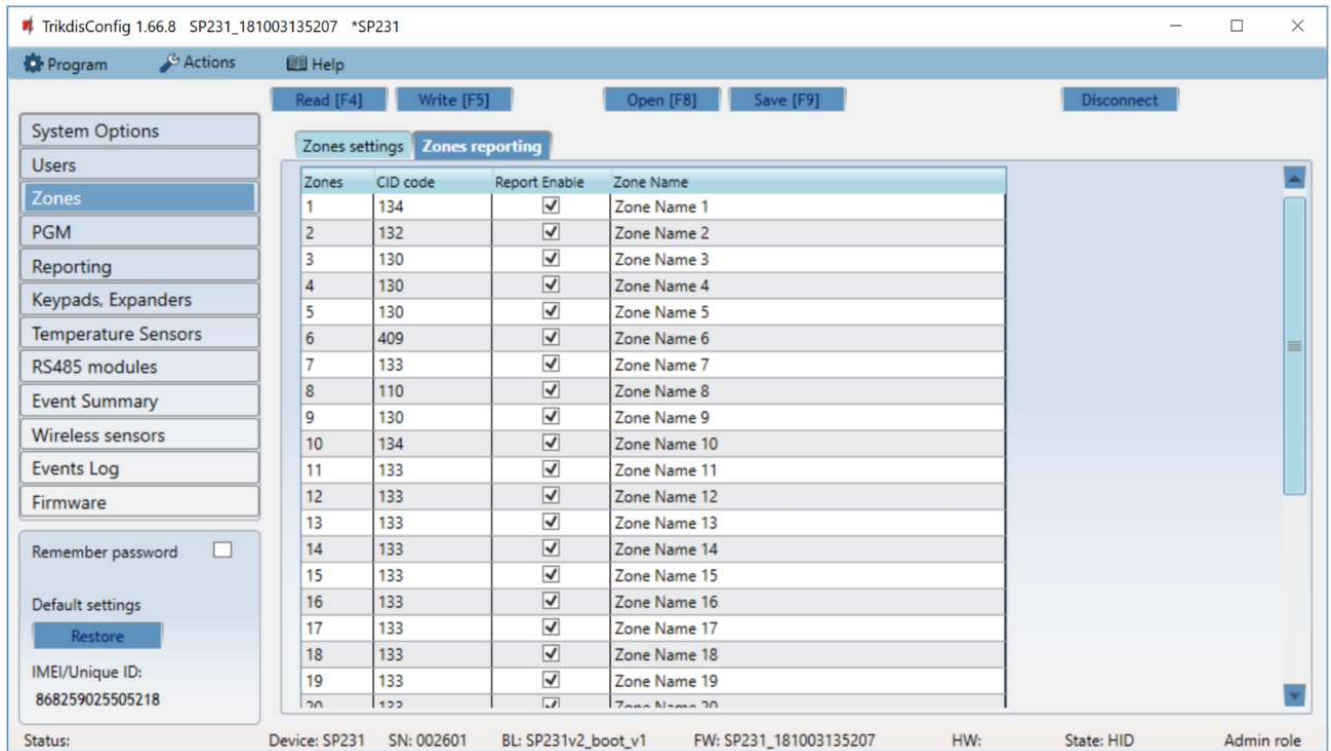
Any ZNx input of the control panel can be set as Fire zone and a four-wire smoke detector can be connected thereto. In order to connect a two-wire smoke detector it should be connected to ZN8 input, which must be set:

- a) as Fire zone,
- b) input target for two-wire smoke detectors must be on (**Set zn8 as 2wire** box must be checked in **System Options > System general > System option**).

When needed, a two-wire smoke detector connected to ZN8 can be reset by means of the keyboard or SMS message.

### 6.7.2 Parameters of zone event reports

In the program menu **Zones > Zones reporting** are to be indicated the zone sequence numbers, the event Contact ID protocol codes, alarm report sending on/off and SMS message text entered.



#### Zone report parameters

Name	Description
Zn	Zone sequence number
CID code	Zone Contact ID event code (will be set automatically when the zone function is selected).
Report Enable	When it is checked, the event report sending will be on.
Zone Name	Zone name is entered which will be visible in SMS text.

### 6.7.3 Zone function description

Zone function	The control panel operation after the zone event
Keyswitch	By changing the status of this input it is possible to turn on/off the alarm system. The alarm system is on when <b>Exit Delay</b> is set. This time interval is designated for unhindered leave of the protected premises via the exit route. Respective report is sent after the zone status changed.
Delay	When the alarm system is on, the input zone <b>Delay</b> violation is allowed within the <b>Exit Delay</b> time. If after such time expired the zone remains violated, <b>Bell</b> and <b>Flash</b> output signals are being generated and reports sent. If the zone is violated when the alarm system is on, <b>Entry Delay</b> time counting is started. Within this time the alarm system must be turned off, otherwise <b>Bell</b> and <b>Flash</b> output signals will be generated and reports sent.



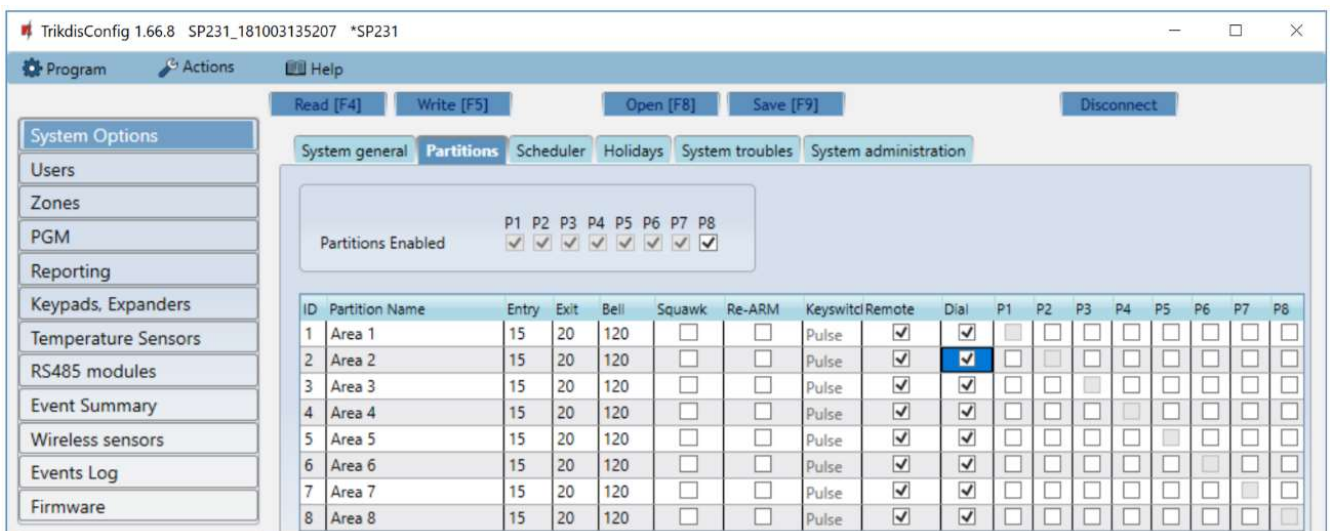
Zone function	The control panel operation after the zone event
Interior	If the zone is violated when the alarm system is on, <b>Bell</b> and <b>Flash</b> output signals will be immediately generated and reports sent. Zone violation is allowed within the time of <b>Entry Delay</b> and <b>Exit Delay</b> .
Interior STAY	Operates in the same way as <b>Interior</b> , however, when security mode <i>STAY</i> or <i>SLEEP</i> is on, the control panel will not respond to the zone violations.
Instant	If the zone is violated when the alarm system is on, <b>Bell</b> and <b>Flash</b> output signals will be immediately generated and reports sent.
Instant STAY	Operates in the same way as <b>Instant</b> , however, when security mode <i>STAY</i> or <i>SLEEP</i> is on, the control panel will not respond to the zone violations.
24 hours	If the zone is violated at any time, Bell and Flash output signals will be immediately generated and reports sent.
Fire	If the zone is violated at any time, <b>Bell</b> and <b>Flash</b> output signals will be immediately generated and reports sent.
Silent	If the zone is violated at any time, the reports are sent immediately, however Bell and Flash output signals will not be generated.

## 6.8 Partition parameters

Partition is a group of independently protected zones. The alarm system can be divided into separately protected parts. The partitions are configured in the program menu **System Options > Partitions**.

Partitions are enabled and added in **Partitions Enabled** field. Maximum number of partitions - 8. Partitions are added and disabled in the sequence order. In order to disable a partition, it is necessary such partition to be no longer used. Trying to disable a partition which is still being used, a report, indicating where to refuse such partition usage, will pop-up.

Double-click with mouse left button on the selected partition line to open such partition settings window. Partition settings can be changed also by directly changing settings in the partition line.



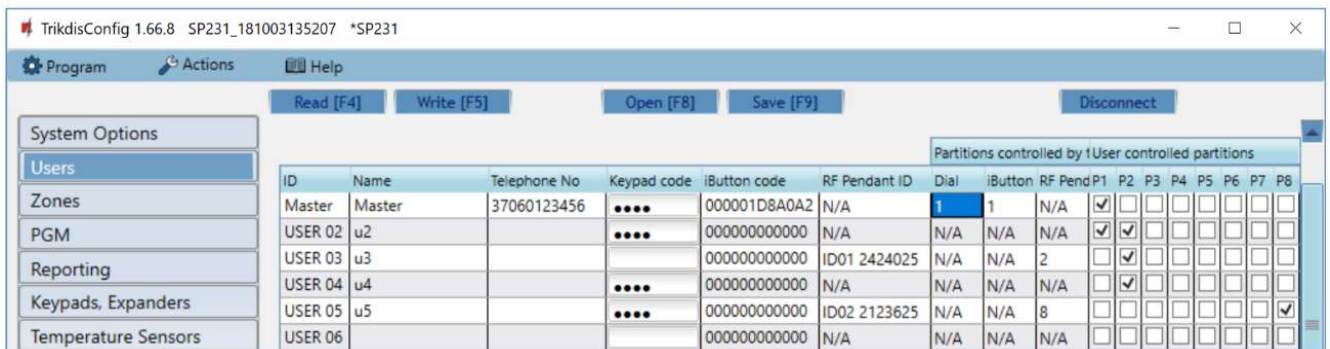
### Partition parameters

Name	Description
ID	Partition sequence number

Name	Description
Partition Name	Partition name. Default settings provide partition names such as Area 1, Area 2, Area 3 and etc. The name can be changed by clicking on the notation.
Entry	Entry time given to the partition, when entering via <i>Delay</i> set zone Time shall be written in seconds, duration from 0 to 255.
Exit	Exit time given to the partition, when entering via <i>Delay</i> set zone Time shall be written in seconds, duration from 0 to 255.
Bell	Duration of audible signal (sirens, <i>Bell</i> ) after the alarm system activated. Time shall be written in seconds, duration from 0 to 9999.
Squawk	Partition <b>Bell Squawk</b> function is on. One short siren (output <i>Bell</i> ) signal will be generated during the alarm system on, and two short signals - during alarm system off.
Re-ARM	Partition arming (Re-ARM function) against accidental alarm system deactivation is enabled. When the alarm system is enabled remotely but not violating the entry zone after entry delay time, the alarm system will turn on in its previous arming mode.
Keyswitch	<b>Keyswitch</b> zone entry control type is indicated and also system control is operated; the only <b>Pulse</b> mode is possible in order to have a remote control for the system.
Remote	Partition, remote control option (Registered numbers control by SMS message and calls) is enabled.
Dial	Partition, status control by call is enabled.
P1-P8	Jointly operated partitions are indicated by checking the boxes (the partition automatically turns into the arming status when all the checked partitions are in the arming status).

## 6.9 User access parameters

The alarm system control options and types are indicated in the program menu **Users**.



ID	Name	Telephone No	Keypad code	iButton code	RF Pendant ID	Dial	iButton	RF Pend	P1	P2	P3	P4	P5	P6	P7	P8
Master	Master	37060123456	....	000001D8A0A2	N/A	1	1	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
USER 02	u2		....	000000000000	N/A	N/A	N/A	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
USER 03	u3		....	000000000000	ID01 2424025	N/A	N/A	2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
USER 04	u4		....	000000000000	N/A	N/A	N/A	N/A	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
USER 05	u5		....	000000000000	ID02 2123625	N/A	N/A	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
USER 06			....	000000000000	N/A	N/A	N/A	N/A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### User access parameters

Name	Description
ID	User identification number
Name	User name is indicated based on which in the reports sent will be visible who has controlled the alarm system and how.
Telephone	User phone number is indicated from which the alarm system will be remotely controlled. Numbers must be entered with international code.
Keyboard code	<b>4-digit or 6-digit user code is set for the control of the security system via keyboard. User 40 is assigned with the code type Duress alarm.</b>

iButton code	iButton key identification number for the alarm system control is indicated. See 6.9.1 „iButton key code registering”.
User Code	4 digit or 6 digit user code for the alarm system control via keyboard is indicated.
P1 – P8	The alarm system partitions controlled by user are indicated.

### 6.9.1 iButton key code registering

iButton key numbers are added in **iButton code** field:

- All added iButton keys will be registered in the order of sequence by clicking **Start programming**.
- To finish entering the keys, click **Stop programming** button.

The codes can be cleared by entering 12 zeros instead of the existing ones. The codes can be transferred to the other user by copying.

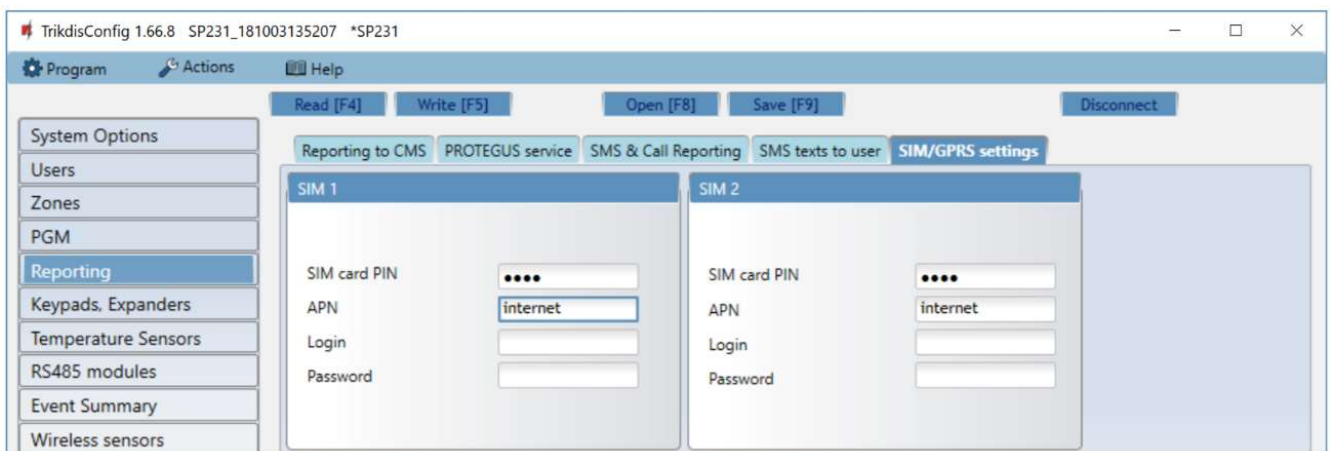
Having zeros remained in *Master* user, **iButton code** field and the unknown key added, it will be automatically registered to *Master* user, thus after entering new keys or completing programming and willing to have no *Master* user code it is recommended to change the code into e.g. 000000000001.

### 6.10 SIM card parameters

The control panel contains two SIM card holders where SIM cards of different GSM operators could be inserted thereby enabling transmission of messages using services of different GSM communication providers.

The control panel sends messages using the first (SIM1 holder) SIM card. If network communication is interrupted the control panel will automatically register in the other network using the second (SIM2 holder) SIM card. After 4 hours the control panel will try to register with the first SIM card.

Settings are to be set in the program menu **Reporting > SIM/GPRS settings**.



#### SIM card parameters

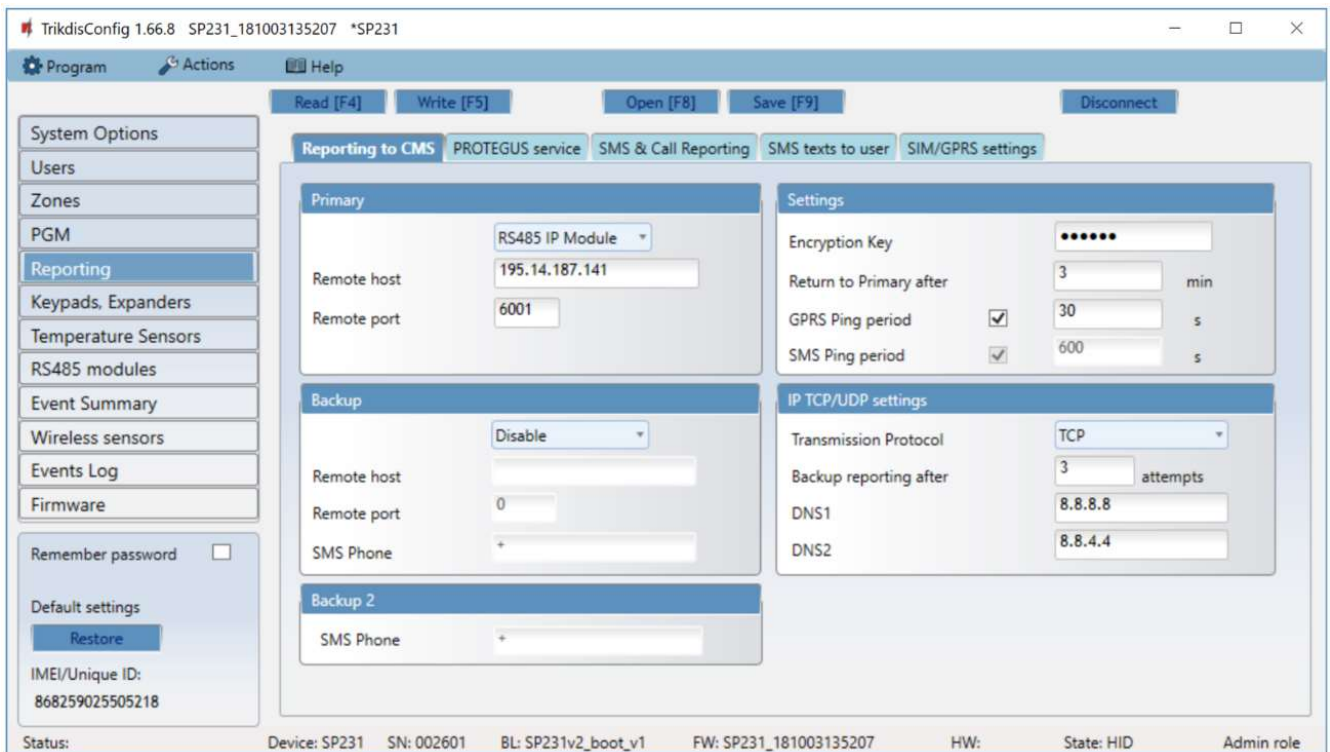
Name	Description
SIM card pin	SIM card PIN code.
APN	Name of GSM operator network where SIM card inserted in the module is operating.
Login	User name of GSM operator network where SIM card inserted in the module is operating (if required by network operator).
Password	User password of GSM operator network where SIM card inserted in the module is operating (if required by network operator).

### 6.11 Report transmission to CMS

Parameters required to transmit reports to Centralized Monitoring Station (CMS) via GPRS and SMS communication channels are entered in the program menu **Reporting > CMS Reporting**. Sent information is coded by Contact ID protocol codes.

The alarm system reports are transmitted via primary communication channel. In case of the above channel interruption, reports are transmitted via backup communication channel, and communication with the primary channel is regularly attempted to restore. If both GPRS channels are interrupted, reports shall be transmitted via backup SMS channel (**Backup 2**).

Parameters of **Primary** and **Backup** communication channel with the centralized monitoring station receiving device shall be indicated in the fields. **Primary** and **Backup** channels shall be selected in respective boxes of drop-down lists.



#### Primary communication channel

Name	Description
Remote host	Receiving device IP address.
Remote port	Receiving device port
SMS Phone	Phone number of receiving - via SMS channel -device of monitoring station is indicated

#### Backup communication channel

Name	Description
Remote host	Receiving device IP address.
Remote port	Receiving device port
SMS Phone	Phone number of monitoring station device able to receive reports via SMS channel.

### Backup 2 communication channel

Name	Description
SMS Phone	Phone number of monitoring station device able to receive reports via SMS channel.

The control panel involves continuous control of communication with monitoring station receiving device. Communication testing signals PING are periodically sent to determine performance of communication channel. Having detected interruption of communication in the primary channel, the control panel immediately switches to and transmits reports to monitoring station via backup channel.

Name	Description
Encryption Key	Message encryption key of six-digits which must match with message encryption key of monitoring station.
Return to primary after	Period of time after expiry of which the control panel will try to restore communication via primary channel, min.
GPRS PING Time	Period of communication test signal PING sending via GPRS channel, sec. Check the particular checkbox to enable signal sending function. If security Grade 3 is set, the maximum period length - 90 seconds.
SMS PING Time	Period of communication test signal PING sending via SMS channel, sec. Check the particular checkbox to enable signal sending function.

### Network parameters

Name	Description
Transmission Protocol	Transmission protocol - <b>TCP/IP</b> or <b>UDP/IP</b> - shall be selected.
Backup reporting after	Number of attempts to transmit report via Primary channel is to be indicated. If transmission is failed, the connection for report transmission via Backup channel will be initiated.
DNS1, DNS2	IP addresses DNS servers.

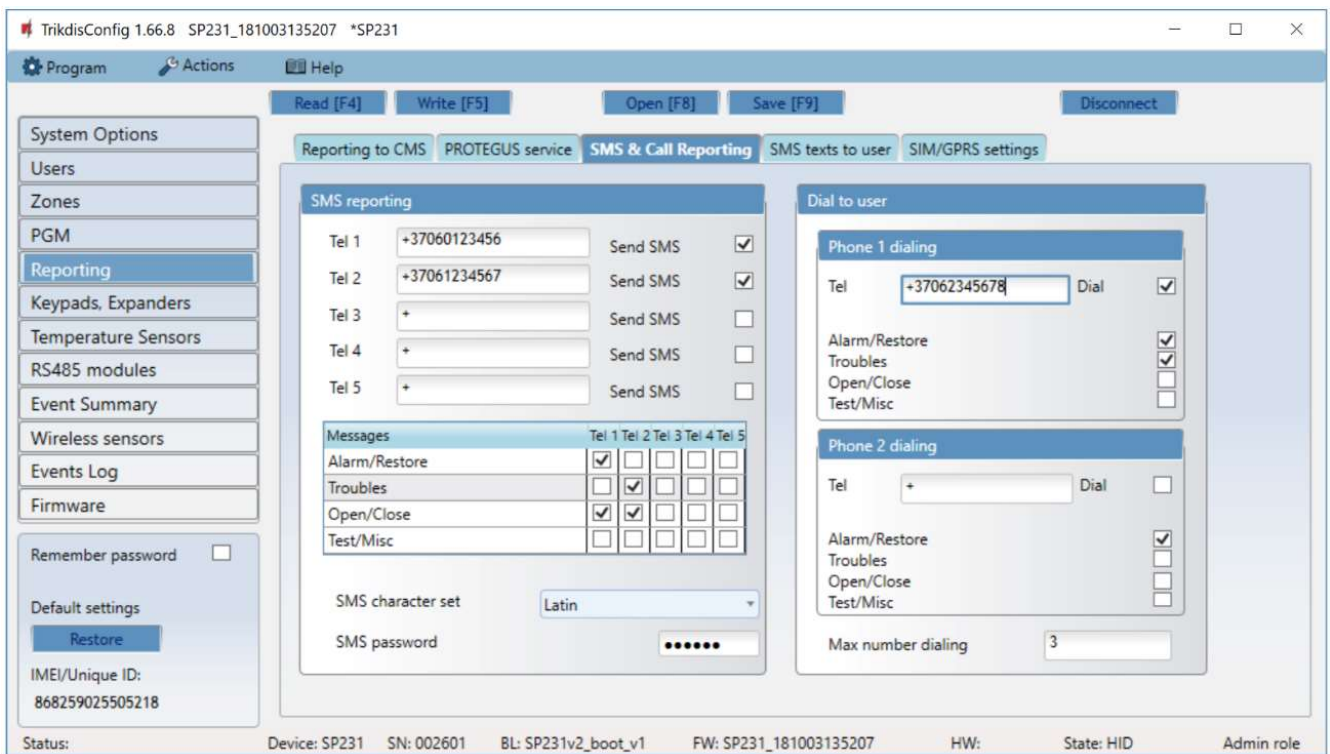
## 6.12 Report transmission to user

**Note:** When it is set that reports will be addressed both to Centralized Monitoring Station (CMS) and to user, and GPRS channel is set for reporting to CMS, the reports will be sent to CMS first of all, however they will be sent to user only after the control panel "is aware" that have been already transmitted to CMS.

If SMS channel is set for reporting to CMS, the reports will be sent to CMS firstly, and to users - secondly.

For reporting to the users only, go to menu **Reporting > CMS Reporting**, and set **Disable** in the options of Primary and Backup channel technology

Parameters, which set report transmission to users, are indicated in program menu **Reporting** section **SMS and phone calls for users**. The alarm system reports can be sent by SMS messages to 5 mobile phones. Events are texted in free form using different symbol characters (Lithuanian, Latin or Cyrillic alphabet letters). There is an option to choose whether to send all or particular alarm event reports to the addressees.



### SMS message parameters

Name	Description
Tel 1-5	Phone numbers of users subject to message sending are entered. Enter numbers with international country code.
Send SMS	SMS text message sending to indicated telephone is enabled.
Alarm/Restore	Alarm system actuation and restoration reporting is enabled.
Troubles	Equipment operation trouble reporting is enabled.
Open/Close	Alarm system On/Off reporting is enabled.
Test/Misc	Communication test reporting is enabled.
SMS character set	SMS character set selection.
SMS password	Password for remote control and programming via SMS messages.

### Call report parameters

Name	Description
Tel	Phone number of user subject to call receiving. Enter numbers with international country code.
Dial	Calling function for indicated phone number Dial is enabled
Alarm/Restore	Calling in case of alarm actuation and restoration is enabled.
Troubles	Calling in case of equipment troubles is enabled.
Open/Close	Calling in case of alarm system on/off is enabled.
Test/Misc	Calling in case of communication test is enabled.

Indicate maximum number of unsuccessful calls in **Max number dialing** field.

### 6.12.1 Message texts to User

Texts which will be visible in SMS messages are indicated in the program menu **Reporting > SMS text to user**.



#### SMS text parameters

Name	Description
ID	Report sequence number
Event Type	Text description.
SMS Text	Text which will be visible in SMS message is entered.

### 6.13 PGM output configuration

The board contains five (PGM1 – PGM3, BELL-, LED) programmable output terminals for connection of devices controlled by the control panel.

- Terminals PGM1 – PGM3 are designed for connection of user selected modes, circuits.
- Terminals BELL+ and BELL- (PGM4) are designed for siren connection. The control panel provides control and signalling if external circuit of this output is interrupted, short-circuit.
- Terminal LED (PGM5) which is connected to positive terminal of mains supply output via 5K1 resistor. It is designed for LED indicator connection.

**PGM** outputs are set in program menu **PGM**. Any output can be set operating in one of numerous operation modes (see 6.13.1 „PGM output operation descriptions“).

Name	Output	Output definition	Control Mode	Pulse Length	Dial
1	00002601, SP231 Panel, PGM-1	Remote Control	Pulse	15	<input type="checkbox"/>
2	00002601, SP231 Panel, PGM-2	Remote Control	Pulse	3	<input type="checkbox"/>
3	00002601, SP231 Panel, PGM-3	Remote Control	Level	15	<input type="checkbox"/>
4	00002601, SP231 Panel, PGM-4	Bell	Pulse	3	<input type="checkbox"/>
5	00002601, SP231 Panel, PGM-5	System State	Pulse	3	<input type="checkbox"/>
6	Disable	Disable	Pulse	0	<input type="checkbox"/>
7	Disable	Bell	Pulse	0	<input type="checkbox"/>
8	Disable	Buzzer	Pulse	15	<input type="checkbox"/>
9	Disable	Flash	Pulse	0	<input type="checkbox"/>
10	Disable	System State	Pulse	0	<input type="checkbox"/>
11	Disable	Ready	Pulse	15	<input type="checkbox"/>
12	Disable	Remote Control	Pulse	10	<input type="checkbox"/>
13	Disable	AC failure	Level	0	<input type="checkbox"/>
14	Disable	Battery OK	Pulse	0	<input type="checkbox"/>
15	Disable	ARM/DISARM	Pulse	0	<input type="checkbox"/>
16	Disable	Alarm Indication	Pulse	0	<input type="checkbox"/>
17	Disable	Lost Primary Channel	Pulse	0	<input type="checkbox"/>
18	Disable	Lost Secondary Channel	Pulse	0	<input type="checkbox"/>
19	Disable	Fire Sensor Reset	Pulse	0	<input type="checkbox"/>
20	Disable	Fire Indication	Pulse	0	<input type="checkbox"/>
21	Disable				

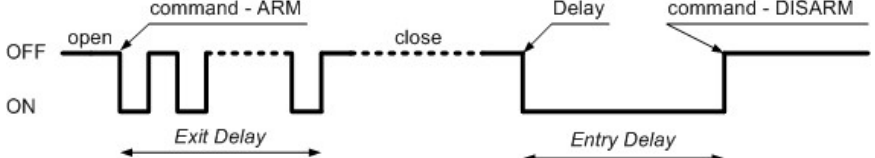

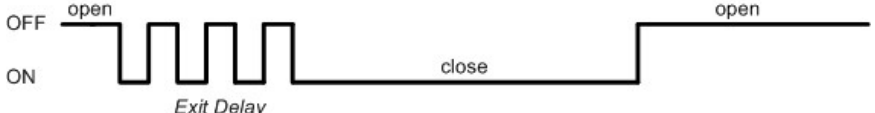

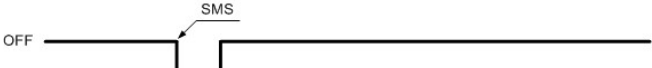

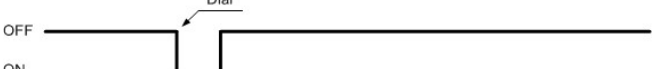
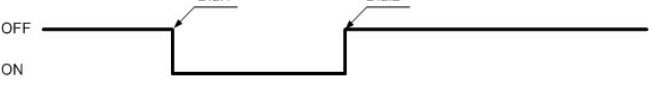

### PGM output parameters


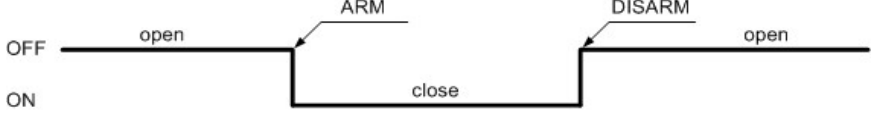
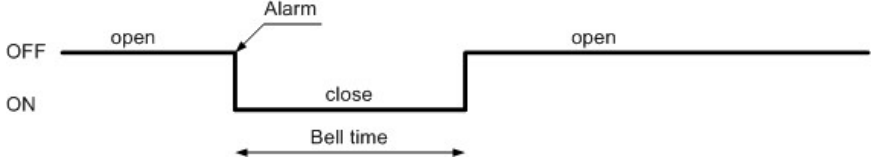
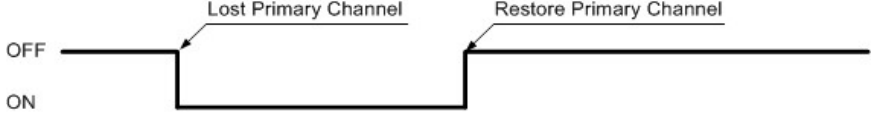
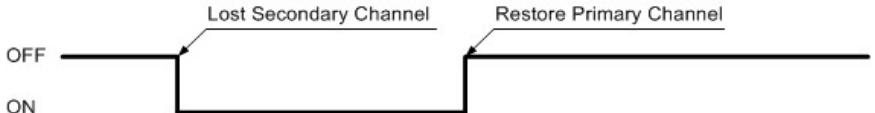

Name	Description
ID	Output sequence number.
PGM	Output name.
Output definition	Selection of output operation mode.
Control Mode	Type of remote control mode, pulse or level.
Pulse Time	Pulse duration is indicated. Duration can be from 0 to 9999 sec.
Dial	Remote control by call of output set in <b>Remote control</b> mode is enabled.

#### 6.13.1 PGM output operation descriptions

PGM output mode	Description
Bell	<p>Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.</p>
Buzzer	<p>Output for connection of audio indicator. After the alarm system activated a pulse signal is generated within <b>Exit Delay</b> time, and continuous signal - within <b>Entry Delay</b> time or when the alarm system is disturbed. When the alarm system is turned off, operates like keyboard buzzer.</p>



PGM output mode	Description
	
Flash	<p>Output for connection of light indicator.</p> <p>When the alarm system is on, a continuous signal is generated, and if the alarm system is disturbed - pulse signal. Signal is terminated by turning off the alarm system.</p> 
System State	<p>Output for connection of light indicator of the alarm system status.</p> <p>Within <b>Exit Delay</b> time a pulse signal is generated, and when the alarm system is activated - continuous. Signal is terminated by turning off the alarm system.</p> 
Ready	<p>Output for connection of light indicator of input statuses.</p> <p>If all zones are clear (none violated), a continuous signal is generated.</p> 
Remote Control	<p>Output designed for connection of electrical devices which will be controlled by SMS message or phone call</p> <p>a) control by SMS message</p> <p><b>Pulse mode:</b></p>  <p><b>Level mode:</b></p>  <p>b) control by phone call</p> <p><b>Pulse mode:</b></p>  <p><b>Level mode:</b></p> 
AC OK	<p>Output for connection of indicator about control panel supply from alternating current.</p> 
Battery OK	<p>Output for connection of indicator about control panel supply from battery.</p>

PGM output mode	Description
	<p>OFF </p>
ARM/DISARM	<p>Output for connection of light indicator of the alarm system status. When the alarm system is on a continuous signal is generated.</p> <p>OFF </p>
Alarm indication	<p>Output for connection of light indicator showing alarm status of the alarm system. After the alarm system actuation a continuous signal is generated.</p> <p>OFF </p>
Lost Primary Channel	<p>Output where a continuous signal is generated when communication with primary channel was lost.</p> <p>OFF </p>
Lost Secondary Channel	<p>Output where a continuous signal is generated when communication with secondary channel was lost.</p> <p>OFF </p>
Fire Sensor Reset	<p>Output for reset of fire sensor operation. Its status changes 5 sec. and returns to the initial one.</p> <p>OFF </p>

### 6.13.2 PGM output remote control

When any of PGMx output is set for operating in Remote Control mode, the status of such output will be available for remote control - by SMS message or phone call. This function is used when it is needed to turn on/off home automatics by remote control (gate lifting motor, irrigation pump, heater, cooler, etc.) without changing premises protection mode.

Remote control mode is selected in **Control Mode** field:

- **Level** - a status will change and remain the same until the next command.
- **Pulse** - a status will take time as indicated in **Pulse Time** field.

For control by SMS message, see 7 „Programming and control by SMS messages”.

For control by call, see 6.14 „Control by call”.

## 6.14 Control by call

Control-by-call function is designed for remote control of partition statuses and PGM remote control mode outputs. One call can control:

- one partition selected;
- one PGM output selected;
- selected partition together with PGM output.

Control by call is available only from phone numbers attributed to the users, see 6.9 „User access parameters”.

### 6.14.1 Partition control

By means of call the existing partition mode can be disabled and switched into **DISARM**, and when **DISARM** is on, **ARM** mode is activated.

Call control for partition is enabled in partition settings, see 6.8 „Partition parameters”. A partition desired to be controlled, first of all, must be enabled for operation remotely by checking **Remote** box. The next step is to check **Dial** box to select one of possible partitions.

**Note.** When partition remote control is enabled, **Keyswitch** zone operation mode is rewritten into pulse mode.

### 6.14.2 PGM Output control

By means of call the output set by **Pulse** mode can be activated or **Level** mode status inverted.

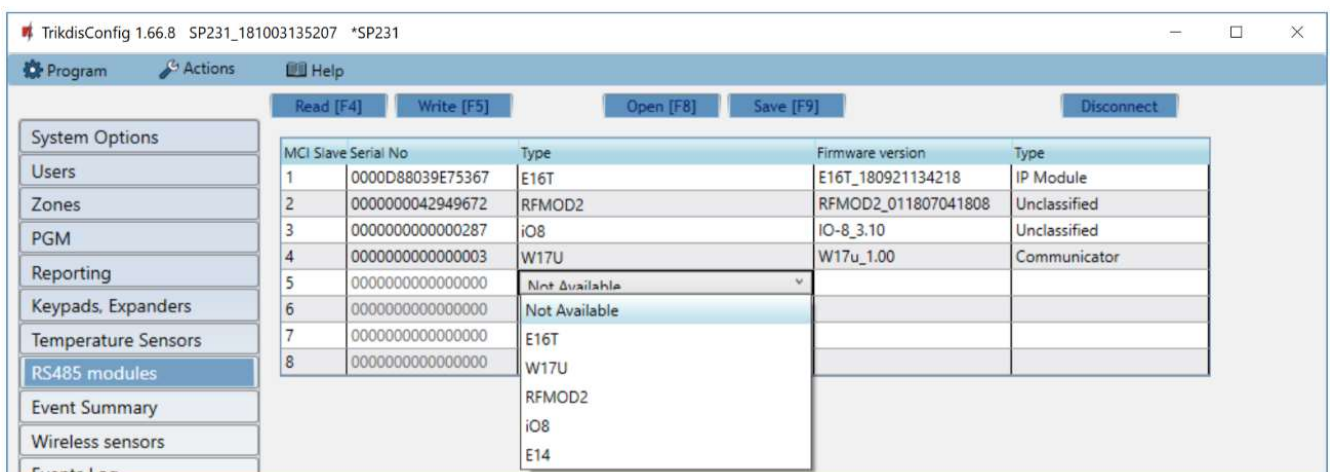
To enable call control, check **Dial** in PGM output settings, see 6.13 „PGM output configuration”.

## 6.15 Transmission module registration

A list of devices (slaves) connectible to MCI data bus is provided in the program menu **Transmission modules**.

For device registration it is necessary to know MCI address number of such device; the number is to be set in the parameter configuration of respective module.

- To add a module, when module address is known, click respective field of **Type** column in such address **Slave** line.
- To remove module from the list, select **Not Available** in **Type** field.
- The changes after module adding/removing must be written in the control panel. This can be done by clicking **Write** button.



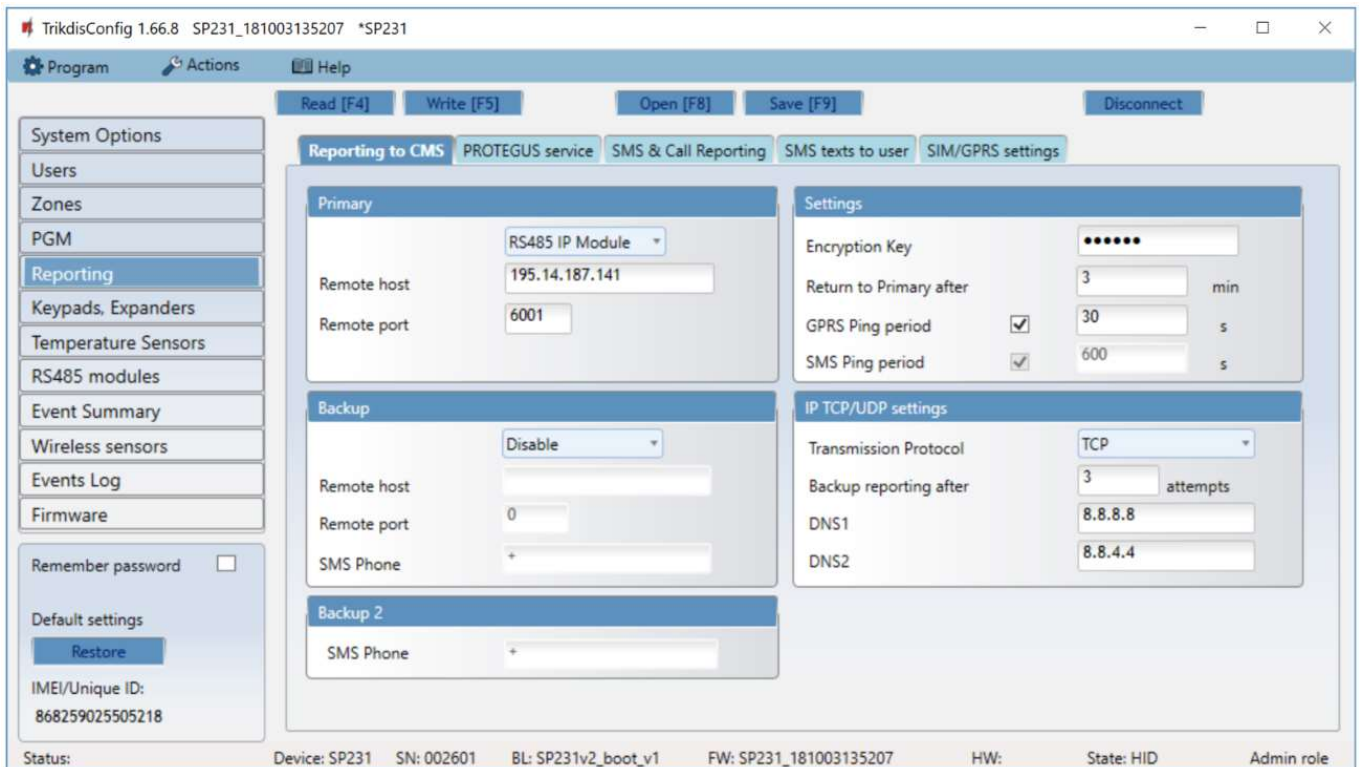
MCI Slave Serial No	Type	Firmware version	Type
1	E16T	E16T_180921134218	IP Module
2	RFMOD2	RFMOD2_011807041808	Unclassified
3	iO8	IO-8_3.10	Unclassified
4	W17U	W17u_1.00	Communicator
5	Not Available		
6	Not Available		
7	E16T		
8	W17U		

### Transmission modules parameters

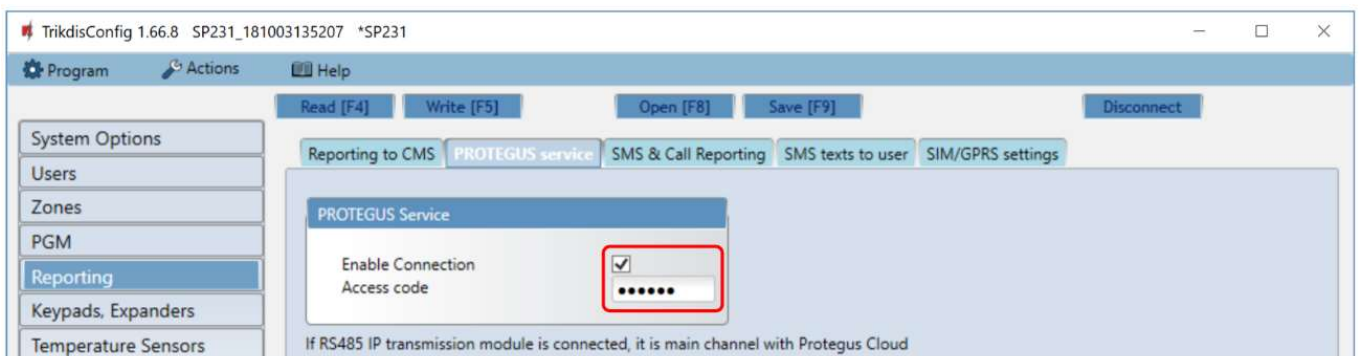
Name	Description
Slave	Device address number.

Name	Description
Serial No	Module registration number.
Type	Module type applied.
Firmware version	Module firmware version

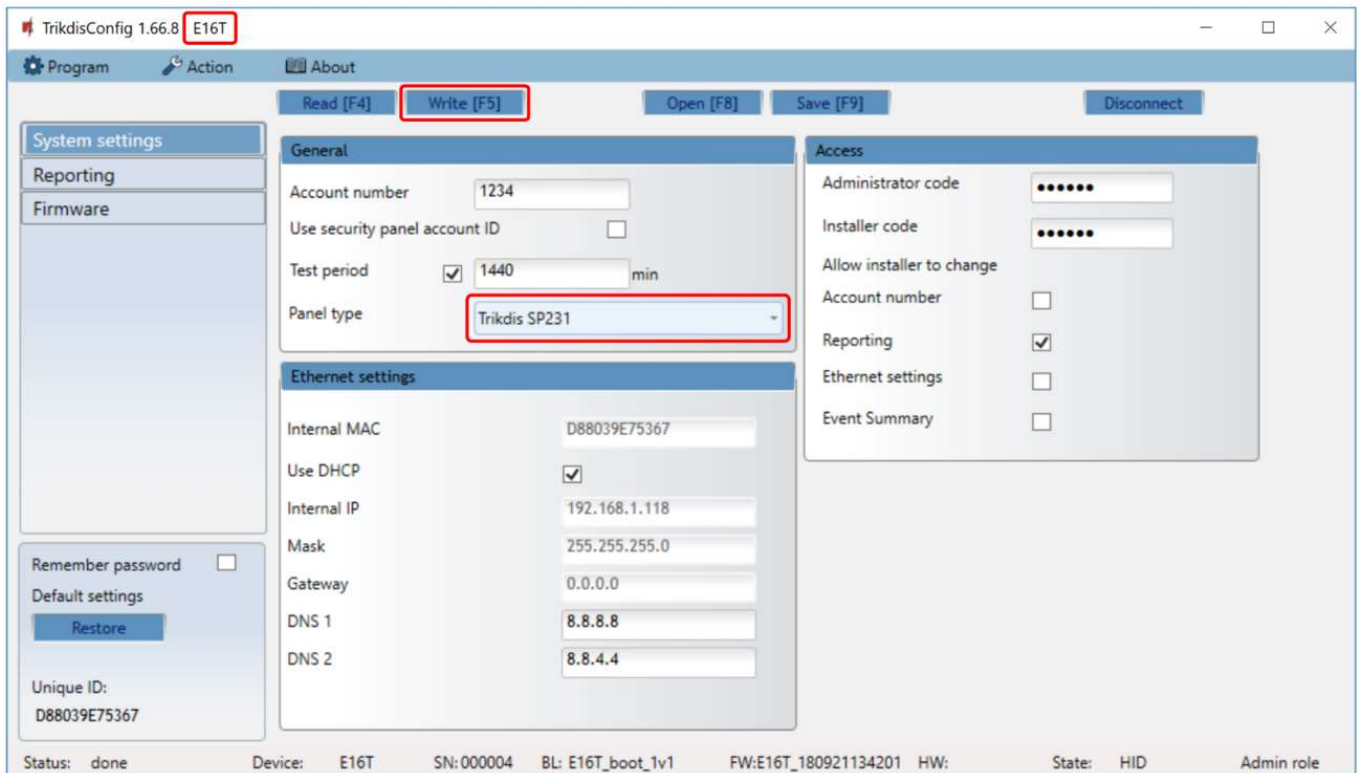
In *TrikdisConfig* application window, tab **Reporting** → **Reporting to CMS** it is necessary to set the main reporting channel to the unit **RS485 IP Module**. Both CSP IP address and the port number must be set.



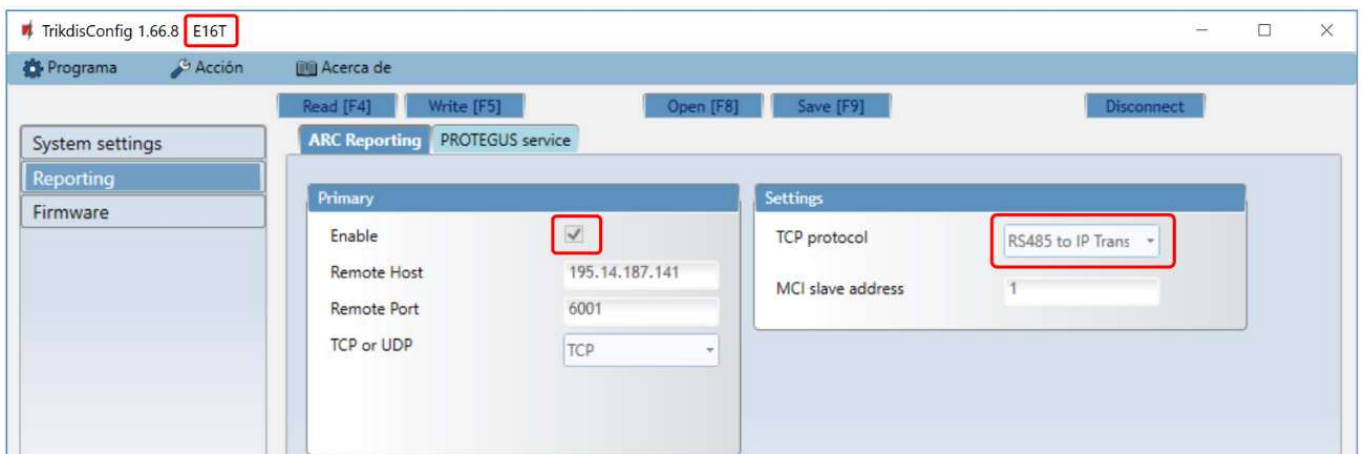
In the tab **PROTEGUS service**, the checkbox **Enable Connection** must be marked and the **Access code** must be assigned in the text box below.



The configuration of module **E16T** with *TrikdisConfig*. Plug in **E16T** to *TrikdisConfig* using a USB Mini-B cable. In **System settings** window it is necessary to provide the name of the control panel (**Trikdis SP231**) in the field **Panel type**. Press the button **Write [F5]** in order to save the settings to **E16T**.



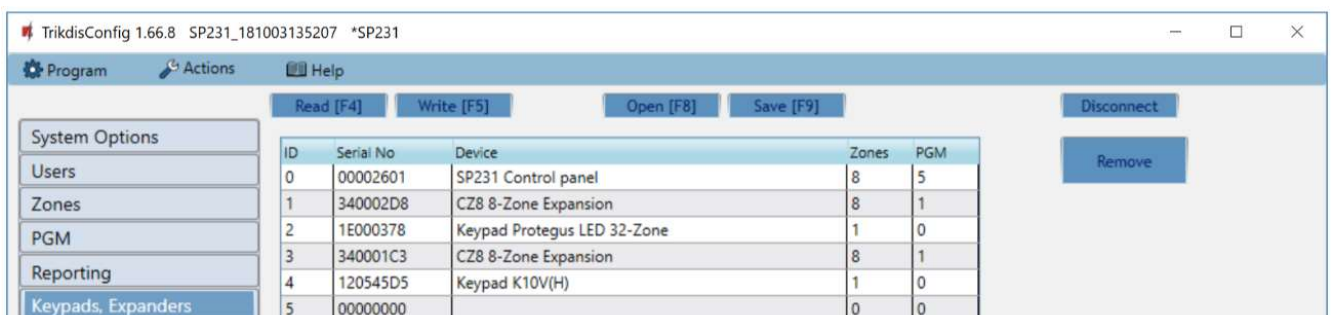
**E16T** will automatically set the type of TCP protocol to RS485 to IP Transparent mode.



## 6.16 Keypads and expanders registration

Expansion modules physically connected to 2-wire *YEL/GRN* (Y/G) data bus and registered by the control panel SP231 are provided in the program menu **Keypads, Expanders**.

- The models connected for the first time will be automatically recognized and included in the list.
- To delete a module, check the selected module line and click **Remove**.



**Keypads and expanders parameters**

Name	Description
ID	Device sequence number.
Serial No	Control panel registration number.
Hardware	Control panel type.
Zn	Number of control panel inputs.
PGM	Number of control panel outputs.

**6.17 Wireless sensors registration**

**SP231** is compatible with the wireless sensors, sirens and remote controls of manufacturer **Crow** when using the module **RFMOD2**.

Connect **RFMOD2** module to the control panel **SP231** (see. 5.9 „Connection of RFMOD2”). When **RFMOD2** is connected, it is automatically recognized and added to the list by **SP231**. After connecting **SP231** to **TrikdisConfig**, the data is read by pressing the button **Read [F4]**. The window **RS485 modules** shows the information about connected **RFMOD2**.

MCI Slave Serial No	Type	Firmware version	Type
1 0000D88039E75367	E16T	E16T_180921134218	IP Module
2 0000000042949672	RFMOD2	RFMOD2_011807041808	Unclassified
3 0000000000000287	iO8	IO-8_3.10	Unclassified
4 0000000000000003	W17U	W17u_1.00	Communicator
5 0000000000000000	Not Available		
6 0000000000000000	Not Available		
7 0000000000000000	Not Available		
8 0000000000000000	Not Available		

Open the window **System Options** and tick the checkbox **Wireless enable**. Click the button **Write [F5]**.

System options configuration:

- EN-50131 compatibility: Not required
- Account number: 1234 hex
- Battery charging: 500 mA
- USER Code Format: 4-Digits
- Wireless enable:
- Set ZN8 as Fire 2wire:
- Door chime:
- Clear Events after reset:
- Duress Code Enable:

Timers configuration:

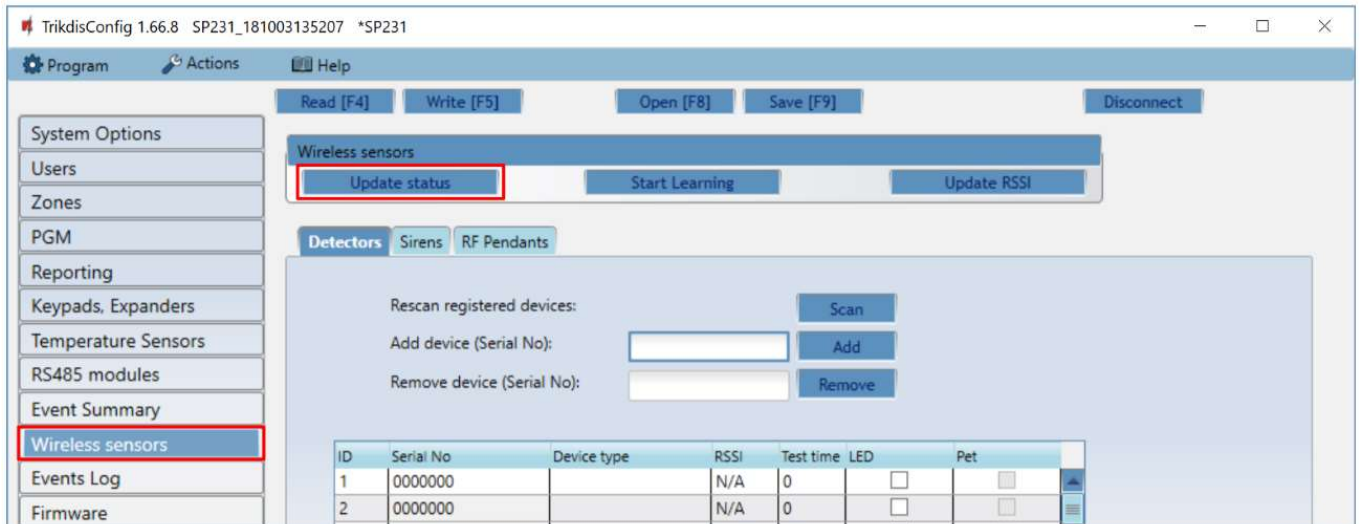
- Test time: 13:30 hh:mm
- Test period: 1 Days
- Time synchronization: Disabled

Keyboard Settings:

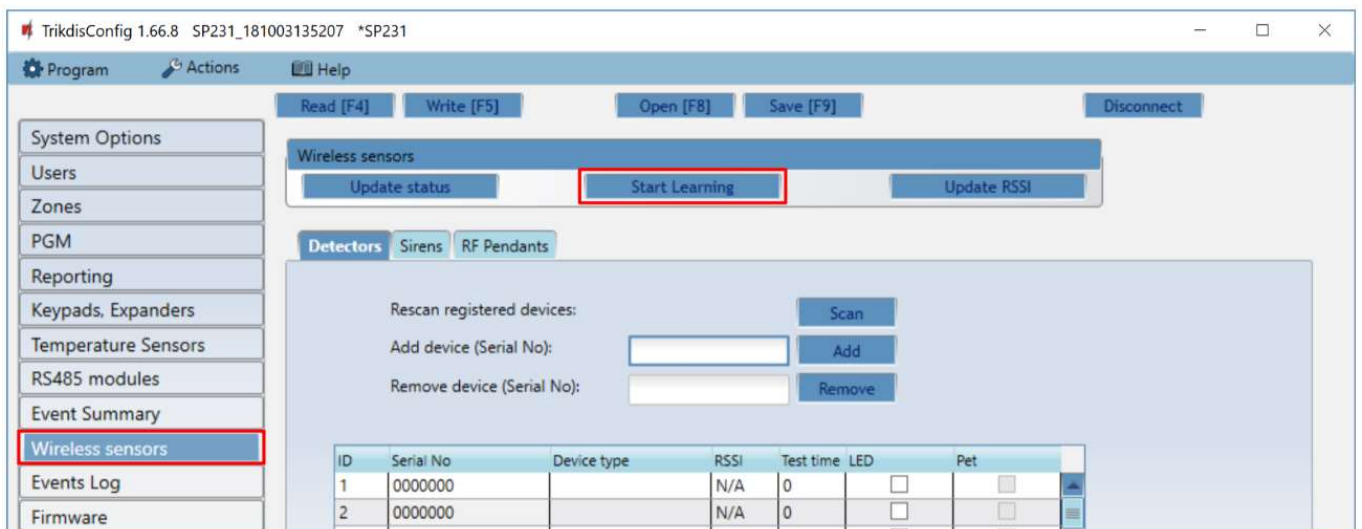
- Panic: Audible, Lockout duration: 2 min
- Medical: Audible, Keypad lockout counter: 0
- Fire: Audible
- Require code to view system status:

Status: reading done | Device: SP231 | SN: 002601 | BL: SP231v2\_boot\_v1 | FW: SP231\_181003135207 | HW: | State: HID | Admin role

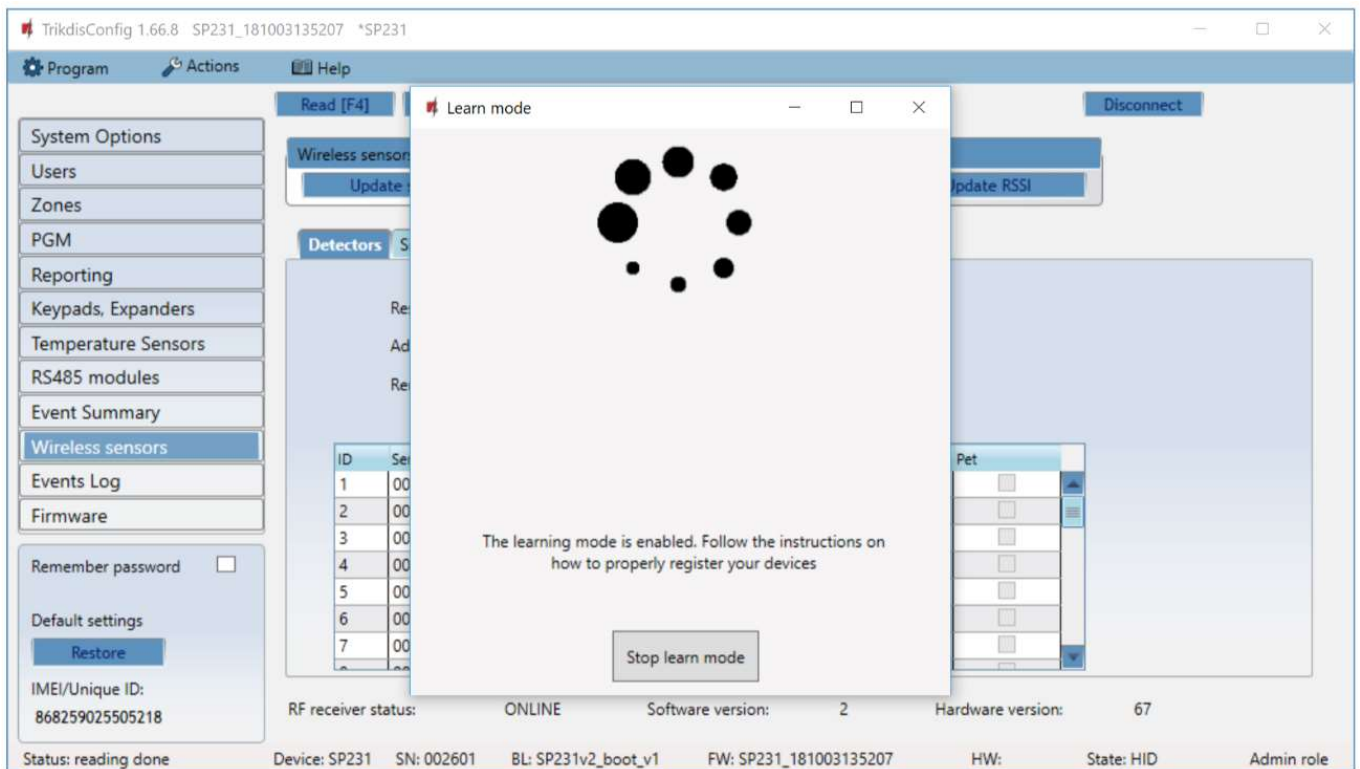
Open the window **Wireless sensors** and click the button **Update status**.



After the window **Wireless sensors** will be refreshed, click the button **Start learning**.



The window of sensor **Learn mode** will be opened.



It is possible to perform the registration of wireless sensors all at once.

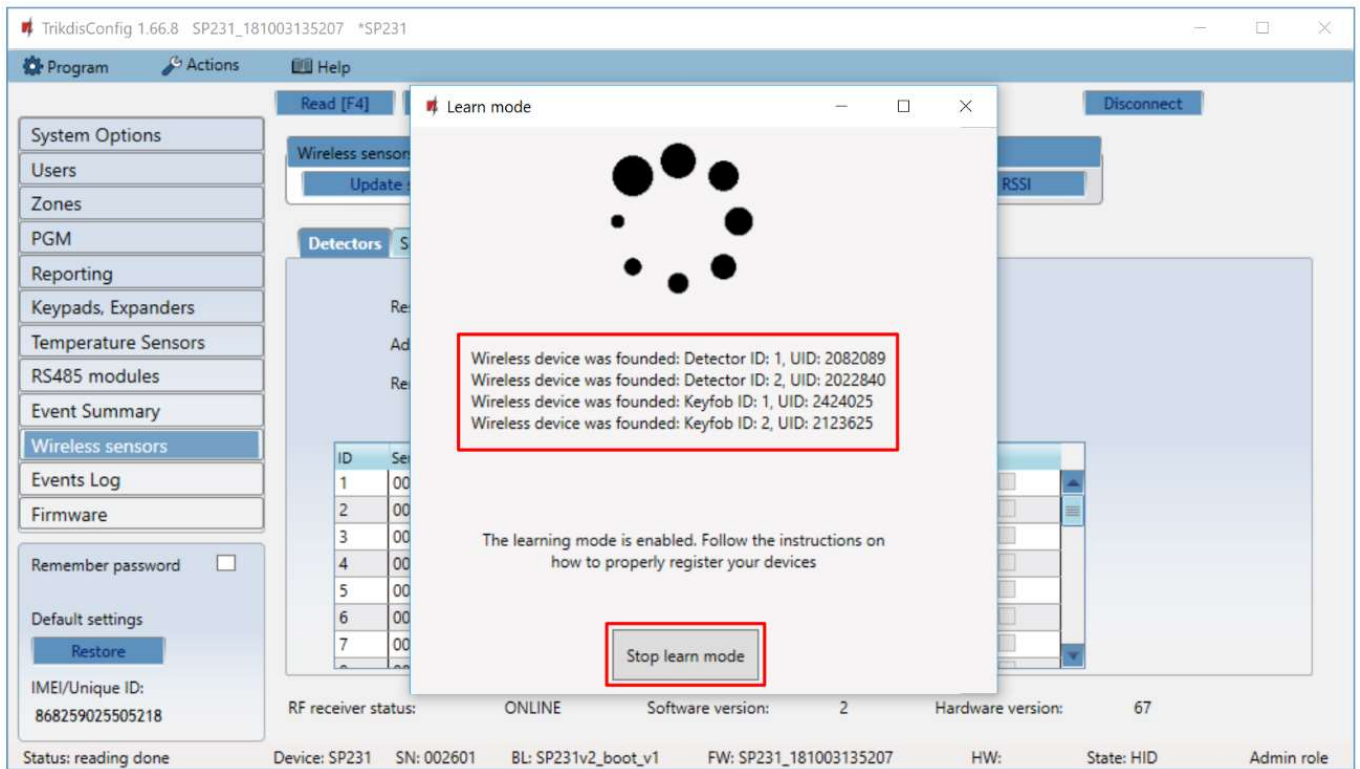
### 6.17.1 Detectors

**In this tab these detectors will be shown:** PET Immune PIR Detector, Magnetic Contact, Smoke & Heat Detector, Glass Break Detector, Curtain Motion Detector, Flood Sensor.

*Learning:*

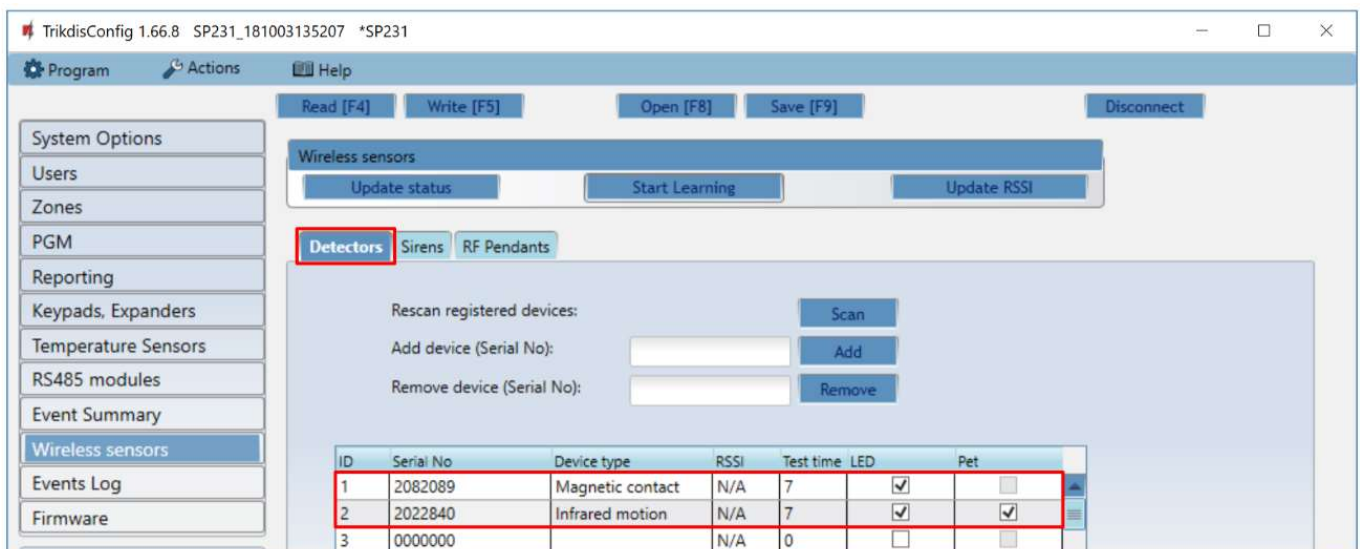
1. To start “Learn” procedure, press the button **Start learning**.
2. Insert battery to the sensor; wait until red/green LED will stop blinking.
3. For few seconds (1-2s) press tamper switch on detector`s circuit board.
4. When the button of the Tamper is released, the indication of LED sensor will change:
  - a. The indicator is blinking in green and red means that the sensor was registered to the system successfully.
  - b. The indicator is blinking only in green means that the sensor was not registered yet. Repeat the registration procedure.
  - c. The indicator is blinking in red means that the voltage of the battery is too low and the battery must be changed.
5. Sensors that are successfully registered will be shown in the window **Learn mode** list. The serial number of the physical sensor that is being registered must match the serial number of the sensor, which is displayed in the window **Learn mode**.





Click the button **Stop learn mode** in order to finish sensor registration.

- In **TrikdisConfig** application window, tab **Wireless sensors** → **Detectors** a list of registered wireless sensors will be shown. The field **Serial No.** displays 7-digit codes, which must match the serial numbers of the physical sensors (may be found on the back of the sensor or on the circuit board).



- Detectors must be assigned to the zones of the circuit board and fields (window **Zone inputs**). When the changes are done, click **Write [F5]**.

**Note:** To remove wireless sensors from the memory of **SP231**:

- Plug USB Mini-B to **SP231**.
- Launch **TrikdisConfig** and click the button **Read [F4]**.
- In **TrikdisConfig**, activate the window **Wireless sensors** and type the serial number of the sensor, which is intended be removed from the system. Click the **Remove** button. Click **Write [F5]**. Wireless sensor is now removed from the memory of **SP231**.

**Detectors registration**

Name	Description
Rescan registered devices	Rescan all registered devices
Add device (serial no)	To register device enter it`s serial number and generate event (e.g. tamper)
Remove devices (serial no)	Using device serial number remove it from device list

**Detector parameters**

Name	Description
ID	Device sequence number
Serial No	Detector registration number
Device type	Detector`s type
RSSI	Received signal strength
Led	Turn on/off led
Pet	For motion sensor PET function can be enabled

**Note:** It is not available to change zone type.

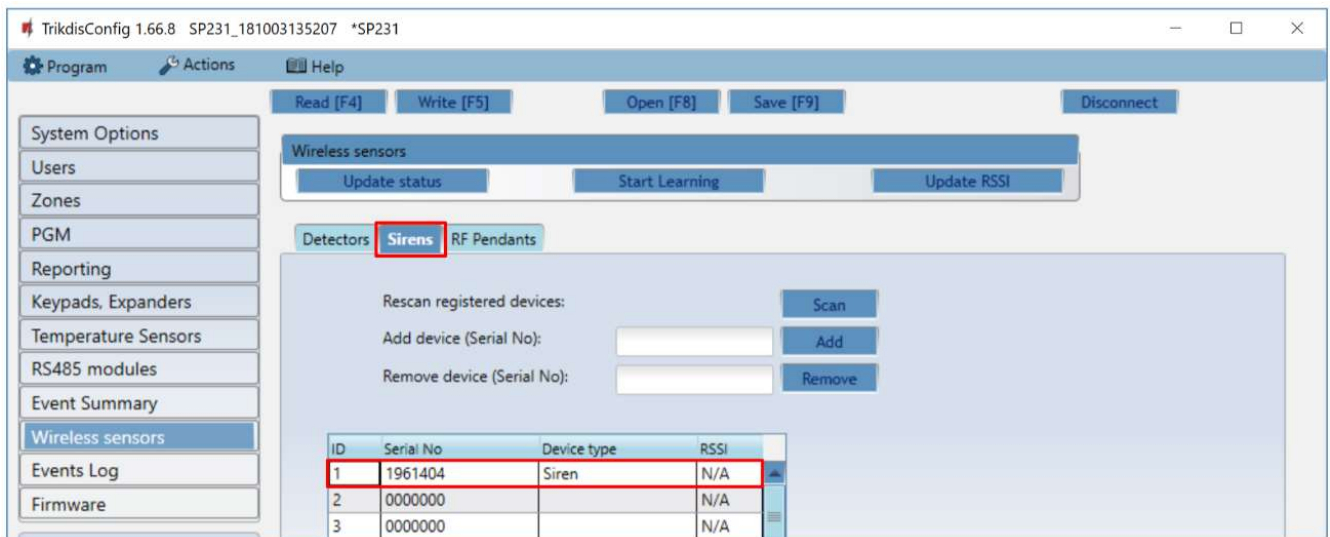
*Remove detector:*

Select detector from list, its serial number should appear in field **Remove device (serial no)**, also it is possible to enter serial number manually. After this is done press **Remove** button.

**Note:** It is not necessary to delete detector`s memory.

### 6.17.2 Sirens

1. Circuit board **SP231** must be set to sensors learn mode.
2. Remove the lid of the siren.
3. Plug in the power supply of the siren.
4. The flash of the siren blinks for 30 seconds in long intervals. Once the indicator has stopped blinking, the siren is ready to be registered.
5. Push the button **LEARN** on the board of the siren.
6. The flash starts blinking.
7. Release the button. Once the flash stops blinking, the siren is successfully registered to the system.
8. Once registered, the siren appears in the list in the window of **Learn mode**. The serial mode of the siren that is being registered must match the serial number which is shown in the window of **Learn mode**.
9. Click the button **Stop learn mode** in order to finish sensor registration.
10. In **TrikdisConfig** window, tab **Wireless Sensors** → **Sirens** field **Device type**, a title **Siren** must appear and the 7-digit serial number of the siren must match the serial number that is written on the board on the siren.
11. Click **Write [F5]**.



### Sirens registration

Name	Description
Rescan registered devices	Rescan all registered devices
Add device (serial no)	To register device enter it`s serial number and generate event (e.g. tamper)
Remove devices (serial no)	Using device serial number remove it from device list

### Sirens parameters

Name	Description
ID	Device sequence number
Serial No	Siren`s registration number
Device type	Siren`s type
RSSI	Received signal strength

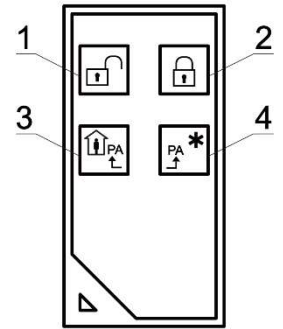
- Note:** To restore the factory settings of the siren:
1. Remove the lid of the siren.
  2. Unplug the power supply of the siren.
  3. Push the button **LEARN** and plug back the power supply to the siren.
  4. Hold **LEARN** button until the flash of the siren blinks for 3 times.
  5. Release the button **LEARN**. The flash of the siren will remain blinking for 30 seconds in long intervals.
  6. Once the flash of the siren stops blinking, the factory settings have been restored to the siren.

### 6.17.3 Pendants

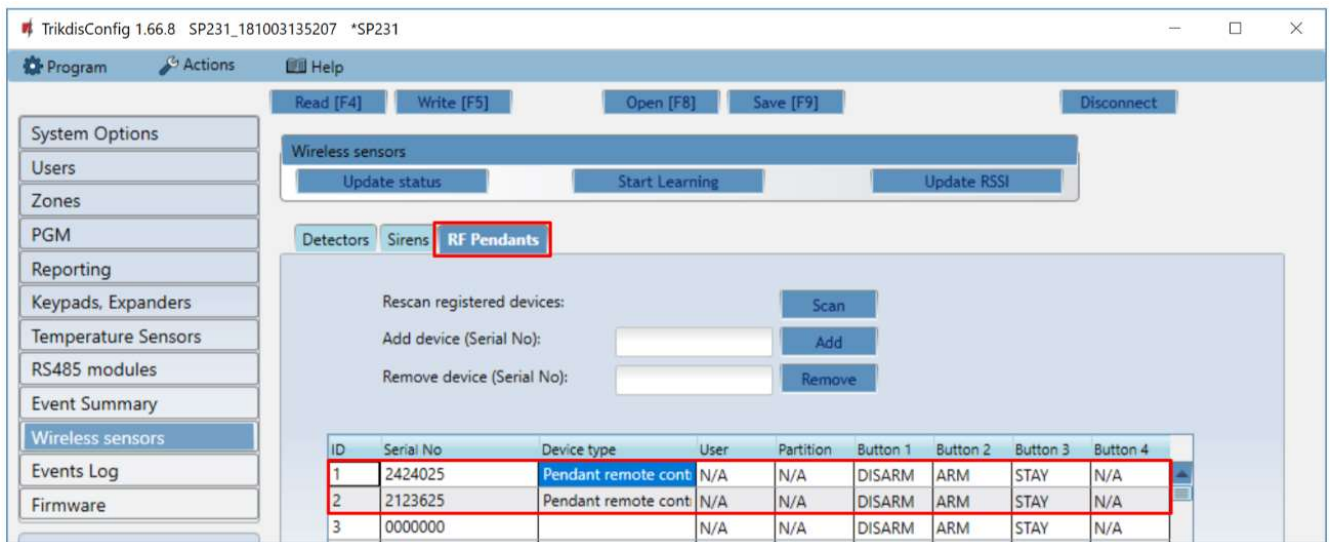
In this tab registered pendants and keypads will be shown.

*Learning:*

- 1) To start “Learn” procedure, press the button **Start learning**.
- 2) Press 3<sup>rd</sup> and 4<sup>rd</sup> buttons at the same time, orange LED will start blinking.
- 3) When orange LED stops to flash – release all two buttons.
- 4) In TrikidisConfig window **Wireless sensors**, tab **Pendants**, new pendant will be shown.



**Note:** Pendant also can be assign to user and partition in **User window**.



#### Pendant registration

Name	Description
Rescan registered devices	Rescan all registered devices
Add device (serial no)	To register device enter it`s serial number and generate event (e.g. tamper)
Remove devices (serial no)	Using device serial number remove it from device list

#### Pendant parameters

Name	Description
ID	Device sequence number
Serial No	Pendant`s registration number
Device type	Pendant`s type
RSSI	Received signal strength
User	Turn on/off led
Partition	One from partitions
Button (1, 2, 3, 4)	Select function of each pendant buttons

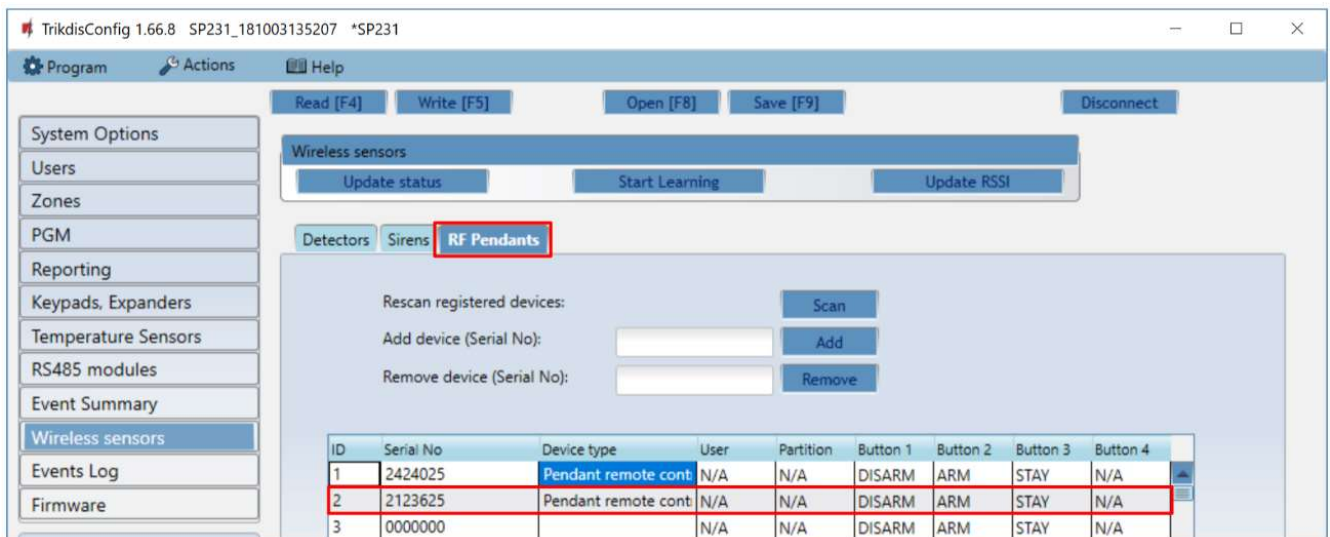
*Cleaning pendant memory:*

Pendants are saving information about receiver in inner memory, before learning it to new receiver, memory must be cleaned.

1. Press 2 and 3 buttons at the same time.
2. Wait until indicator LED will start flash green and red in turns.
3. Memory is cleaned up.

#### 6.17.4 Registration of wireless keypad (FW2-ICON KP-8F)

1. Circuit board **SP231** must be set to sensors learn mode.
2. Insert the batteries to the keypad and wait until you hear sound notification.
3. Press any key on the keypad. The registration of the keypad is finished.
4. Once registered, the wireless keypad appears in the list of **Learn mode**. The serial mode of the keypad that is being registered must match the serial number, which is shown in the window of **Registration mode**.
5. Click the button **Stop learn mode** in order to finish keypad registration.
6. In *TrikdisConfig* window, tab **Wireless Sensors** → **RF Pendants** field **Device type**, a title **Pendant remote control** must appear and the 7-digit serial number of the keypad must match the serial number that is written on the back of the keypad.
7. Provide the number of the partition and and the number of the user to their relevant fields, **Partition** and **User**.
8. Click **Write [F5]**.



#### Note

To restore the factory settings of the keyboard:

1. Insert the battery while holding the key [8] pressed.
2. Hold the key [8] pressed.
3. You will hear a sound notification after a few seconds.
4. Release the key [8]. The code of the administrator has been restored to its factory setting.
5. Enter the code [C][0000] on the keyboard. A symbol of the **Key** will appear.
6. Press and hold both **SOS** buttons at once.
7. You will hear a sound notification. The illumination of the keyboard will turn on and off.
8. You will hear a sound notification once again. The illumination of the keyboard will turn on and off.
9. Release both **SOS** buttons. The factory settings of the keyboard have been restored.

*Control Areas with Wireless Icon Keypad:*

To control Areas with keypad enter User codes to the keypad:

The User Code 1 default is 1234. The next 7 User codes are blank.


Example of adding user code # 2

- 1) Enter into programming mode
- 2) Press key "2" + new 4 digits user code
- 3) The 1 second duration tone is played on code add/change.
- 4) Exit from programming mode

Register RFID tags:

The RFID Tag may be changed or added only while keypad is in programming mode. Up to 8 RFID Tags may be set for keypad. The RFID Tag IDs are saved and ready after every keypad power up.

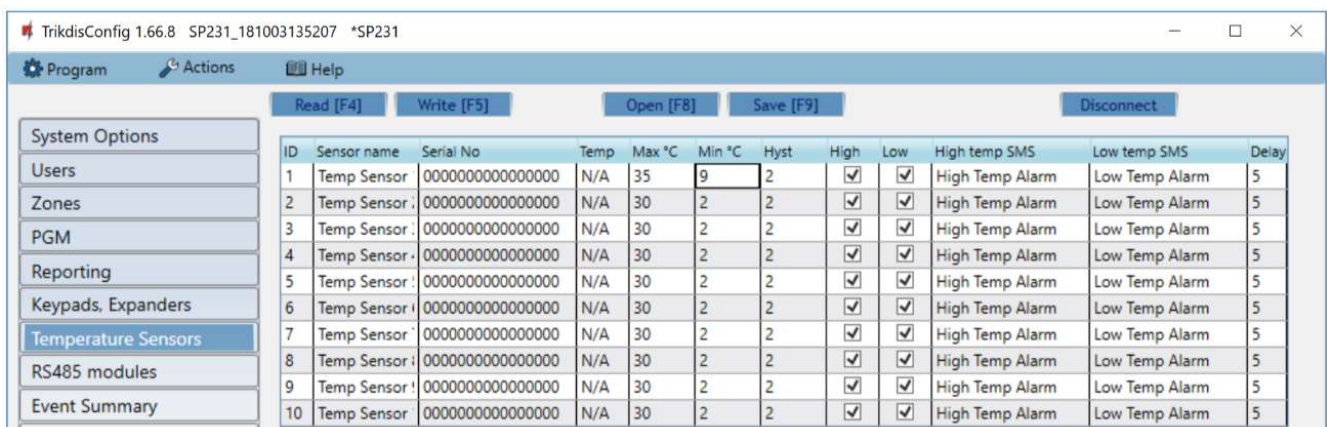
How to modify RFID Tag #1 (user 1):

- 1) Press key "1" and approach tag to 
- 2) The 1 second duration tone is played on code add/change.

### 6.18 Setting of temperature metering report characteristics

Parameters required for transmission of temperature variation reports are indicated in the program menu **Temperature Sensors**.

When temperature sensors are physically connected and power supply is on, the control panel SP231 will automatically register sensor modules.



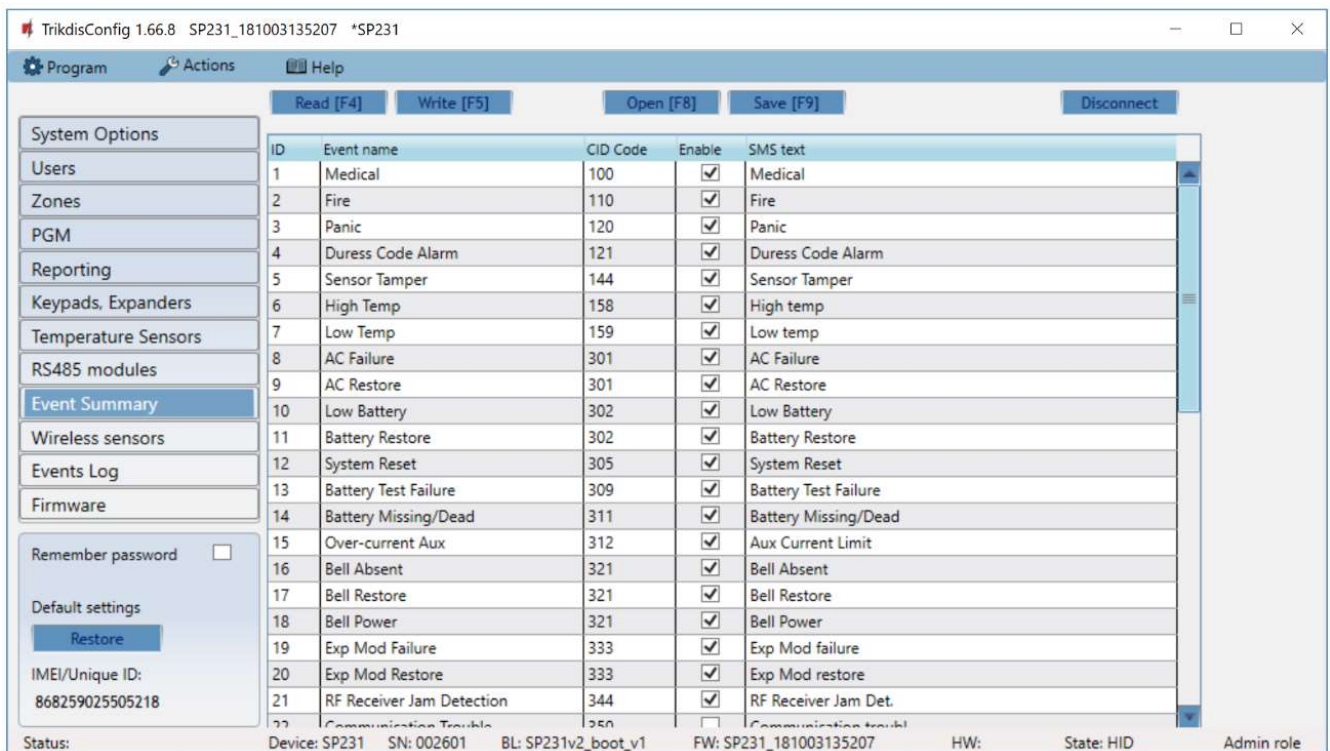
ID	Sensor name	Serial No	Temp	Max °C	Min °C	Hyst	High	Low	High temp SMS	Low temp SMS	Delay
1	Temp Sensor	0000000000000000	N/A	35	9	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5
2	Temp Sensor	0000000000000000	N/A	30	2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5
3	Temp Sensor	0000000000000000	N/A	30	2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5
4	Temp Sensor	0000000000000000	N/A	30	2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5
5	Temp Sensor	0000000000000000	N/A	30	2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5
6	Temp Sensor	0000000000000000	N/A	30	2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5
7	Temp Sensor	0000000000000000	N/A	30	2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5
8	Temp Sensor	0000000000000000	N/A	30	2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5
9	Temp Sensor	0000000000000000	N/A	30	2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5
10	Temp Sensor	0000000000000000	N/A	30	2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Temp Alarm	Low Temp Alarm	5

#### Temperature sensor parameters

Name	Description
ID	Sensor sequence number
Sensor name	Sensor name.
Serial	Sensor registration number Numbers can be cleared (by entering zeros) ore copied (by changing their order). To remove a sensor, enter 16 zeros in this field.
RT	The existing temperature value measured by sensor, °C.
Max °C	Maximum allowable temperature value, the excess of which will be reported. For such purpose <b>High</b> must be checked.
Min °C	Minimum allowable temperature value, below which the situation will be reported. For such purpose <b>Low</b> must be checked.
Hyst	Temperature hysteresis value is indicated.
High temp. SMS	Text, which will be visible in SMS message in case of set temperature excess, is entered.
Low temp. SMS	Text, which will be visible in SMS message in case of temp. below the set one, is entered.

## 6.19 Setting of event reports

The program menu **Event Summary** contains other - out of zone - events which, if occurred, will be reported by the control panel to the addressees in specified CID Codes and text.



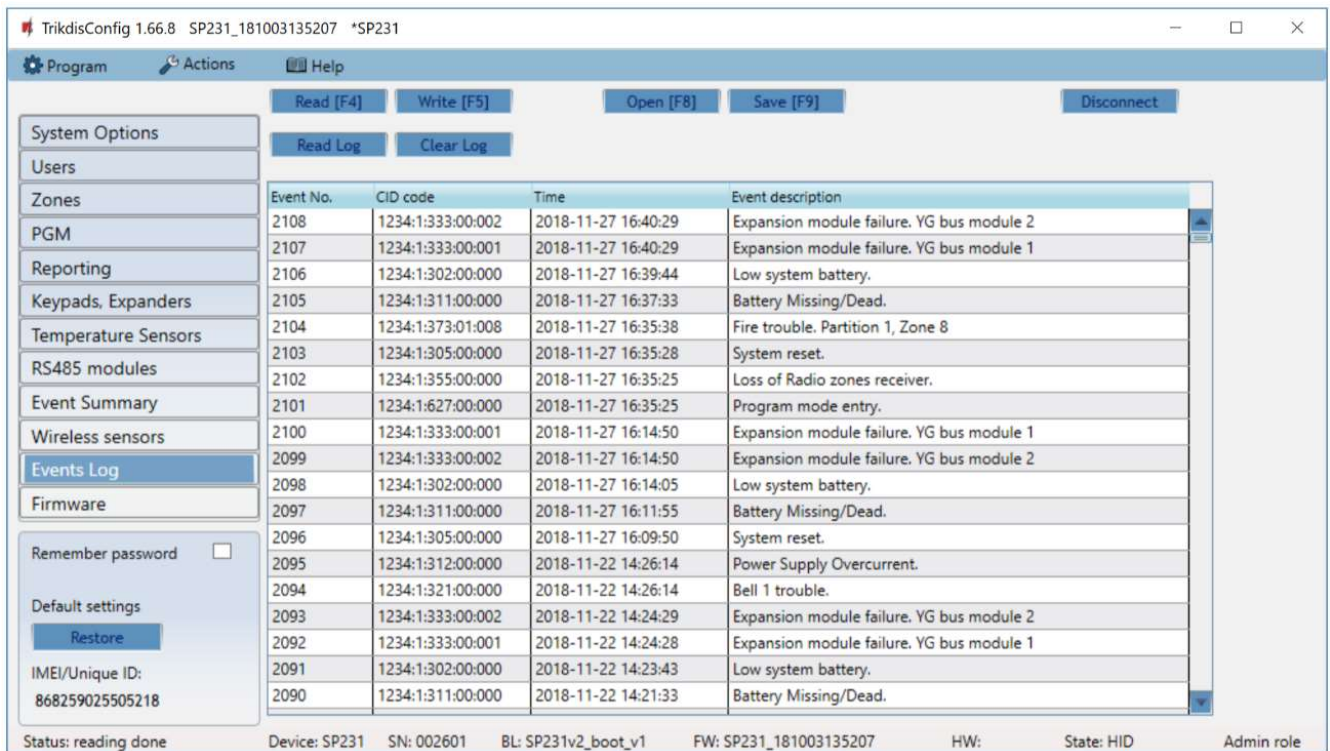
### Event report parameters

Name	Description
ID	Report sequence number
Event name	Event (report) name
CID Code	Report Contact ID code.
Enable	The indicated report will be sent when it is checked.
SMS text	Text which will be visible in SMS message is entered.

## 6.20 Event Log

Information on events recorded by the control panel is available in the program menu **Event Log**. Events are registered by date and time of the internal clock. Memory capacity is at least 2000 last reports. Event storage time does not depend on power supply of the control panel and internal battery, even if power supply is off the events can be stored for more than 10 years.

Events are read from the control panel by clicking **Read log** button. Events are cleared by clicking **Clear log** button.



Event No.	CID code	Time	Event description
2108	1234:1:333:00:002	2018-11-27 16:40:29	Expansion module failure. YG bus module 2
2107	1234:1:333:00:001	2018-11-27 16:40:29	Expansion module failure. YG bus module 1
2106	1234:1:302:00:000	2018-11-27 16:39:44	Low system battery.
2105	1234:1:311:00:000	2018-11-27 16:37:33	Battery Missing/Dead.
2104	1234:1:373:01:008	2018-11-27 16:35:38	Fire trouble. Partition 1, Zone 8
2103	1234:1:305:00:000	2018-11-27 16:35:28	System reset.
2102	1234:1:355:00:000	2018-11-27 16:35:25	Loss of Radio zones receiver.
2101	1234:1:627:00:000	2018-11-27 16:35:25	Program mode entry.
2100	1234:1:333:00:001	2018-11-27 16:14:50	Expansion module failure. YG bus module 1
2099	1234:1:333:00:002	2018-11-27 16:14:50	Expansion module failure. YG bus module 2
2098	1234:1:302:00:000	2018-11-27 16:14:05	Low system battery.
2097	1234:1:311:00:000	2018-11-27 16:11:55	Battery Missing/Dead.
2096	1234:1:305:00:000	2018-11-27 16:09:50	System reset.
2095	1234:1:312:00:000	2018-11-22 14:26:14	Power Supply Overcurrent.
2094	1234:1:321:00:000	2018-11-22 14:26:14	Bell 1 trouble.
2093	1234:1:333:00:002	2018-11-22 14:24:29	Expansion module failure. YG bus module 2
2092	1234:1:333:00:001	2018-11-22 14:24:28	Expansion module failure. YG bus module 1
2091	1234:1:302:00:000	2018-11-22 14:23:43	Low system battery.
2090	1234:1:311:00:000	2018-11-22 14:21:33	Battery Missing/Dead.

### Event log parameters

Name	Description
Line number	Event sequence number
CID code	Object number and registered event report in Contact ID code.
Time	Event date and time.
Log describe	Event report text which was indicated for SMS message sending.

## 6.21 Control panel firmware upgrading

Run TrikdisConfig software, after connecting remotely or via USB cable to the control panel, while newer firmware version is existent, the program will automatically offer to update your current firmware.

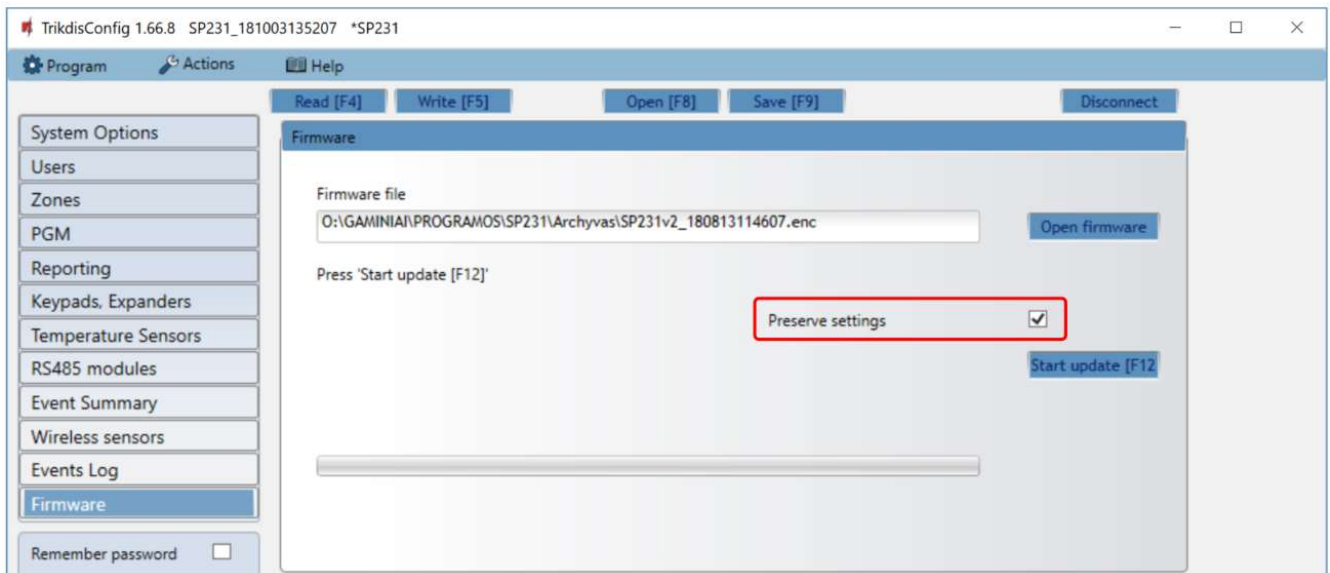
**Note:** If there is an installed antivirus software on your computer, it might block automatic update option. In this case you must reconfigure your antivirus software.

The control panel firmware version can be upgraded (changed) in the program menu **Firmware**.

To do so:

- 1) From [www.trikdis.com](http://www.trikdis.com) download the newest configuration software TrikdisConfig version.
- 2) Connect the control panel SP231 to a computer.
- 3) Open menu branch **Firmware** of parameter setting software *TrikdisConfig*.
- 4) Click **Open firmware** button and check SP231\_XXXXXX.enc file., where XXXXXX – upgrade file version.
  - In order to save the previously entered data, check **Preserve settings** box.
- 5) To start the control panel software upgrading, click **Start update**.
  - After the control panel software upgrading all the control panel parameters will by default be restored in factory settings (unless *Preserve setting* box was checked).





## 7 Programming and control by SMS messages

The alarm system can be controlled and some parameters of the control panel can be changed by means of SMS messages. All the control panel parameters can be changed by *TrikdisConfig* only.

To change the desired parameter of the control panel by SMS message, the SMS message of the following syntax must be sent:

**PSW[password] space [Command code] space [Command content]**

**Note.** You must replace the factory set remote login code (123456) with the code known to you only, e.g., with 111111, by sending such SMS message: **PSW123456 \_ 98 \_ 111111**

SMS messages must be started with capital letters PSW and 6-digit remote login password entered in the control panel.

Symbol " \_ " in the table means a space symbol in SMS text.

The control panel will send SMS message, reply to inquiry to the particular phone from which the inquiry was received.

SMS command text	Description
CFGxxxxxx _ 01 _ CCCC # Ppppppppp #	Adds phone number to user. Command can be sent from any phone number. 01 – command number, CCCC – user code, Ppppppppp – user phone number. Example adding a phone number to the user which code is "1234": <b>CFG123456 01 1234#+37061111111#</b>
PSWxxxxxx _ 10 _ AAA.AAA.AAA.AAA#PPPP#	Set the first IP address and port number. AAA.AAA.AAA.AAA – IP address PPPP – Port number
PSWxxxxxx _ 11 _ AAA.AAA.AAA.AAA#PPPP#	Set the second IP address and port number. AAA.AAA.AAA.AAA – IP address PPPP – Port number
PSWxxxxxx _ 12 _ APN#LOGIN#PSW#ENC#PING#	Set SIM1 card access to GSM network settings. And general network settings. APN – access name (up to 50 characters) ,

SMS command text	Description
	LOGIN – user name (up to 29 characters) PSW – user password (up to 29 characters) ENC - data encryption key (6 characters) PING – report sending interval (10 – 65000). After each value, enter the end symbol #, e.g., <b>PSW123456 12 APN#LOGIN#PSW#123456#180#</b> If operator requires no indication of access to APN, neither LOGIN nor PSW, then SMS message should look in such a way: <b>PSW123456 12 APN###123456#180#</b>
PSWxxxxxx _13 _ APN#LOGIN2#PSW2#	Set SIM2 card access to GSM network settings. APN – access name (up to 50 characters) , LOGIN – user name (up to 29 characters) PSW – user password (up to 29 characters)
PSWxxxxxx _50 _ N	Change the status of Nth PGM output into opposite, if it is set into „Remote Control“. N values: 1, 2, 3, 4, 5.
PSWxxxxxx _5N _ 0	Change the status of Nth PGM output into OFF, if it is set into „Remote Control“. N values: 1, 2, 3, 4, 5.
PSWxxxxxx _5N _ 1	Change the status of Nth PGM output into ON, if it is set into „Remote Control“. N values: 1, 2, 3, 4, 5.
PSWxxxxxx _57 _ N#ST	N - PGM output number. N values: 1,2,3,4,5,... 32. ST – change the output mode to <b>enabled</b> if ST value is equal to 1. Change the output mode to <b>disabled</b> if ST value is equal to 0.
PSWxxxxxx _58 _ PGM#TIME	Pulse PGM output actuation for the specified time is On. Also, the specified time rewrites the previous time in the control panel settings. PGM – PGM output number. TIME – time in seconds up to 999999.
PSWxxxxxx _59	Reset two-wire smoke detectors which are connected to the input ZN8.
PSWxxxxxx _60 _ P # S	Enable the arming mode of the desired partition the number of which P (1-8): S values: change numbers 0 – into Disarm, 1 – into ARM, 2 – into SLEEP, 3 – into STAY.
PSWxxxxxx _80 _ NN_S	Enable BYPASS mode for the zone the number of which NN. NN values: zone number 01 – 32. S values: number 1 – BYPASS On, and 0 – BYPASS Off.
PSWxxxxxx _94 _ N	Enable connection to the Protegus server. N values: 1 – enable, 0 – disable.

SMS command text	Description
PSWxxxxxx _96 _yyyy/mm/dd#hh:mm#	Set the control panel date and time. yyyy – year, mm – month, dd – day, hh – hour, mm – minutes.
PSWxxxxxx _97 _1	Send SMS message with all temperature sensors values.
PSWxxxxxx _97 _2	Send SMS message with the present activated arming mode (DISARM, ARM, STAY, SLEEP) of partitions.
PSWxxxxxx _97 _3	Send SMS message about PGM output statuses.
PSWxxxxxx _97 _4	Send SMS message about zone statuses and power supply condition.
PSWxxxxxx _97 _5	Send SMS message about GSM field strength, modem IMEI number and control panel software version.
PSWxxxxxx _98 _ZZZZZ	Set new 6-digit code for the control panel control by SMS messages. ZZZZZ - new code
PSWxxxxxx _99	Reset control panel.

## 8 Remote control

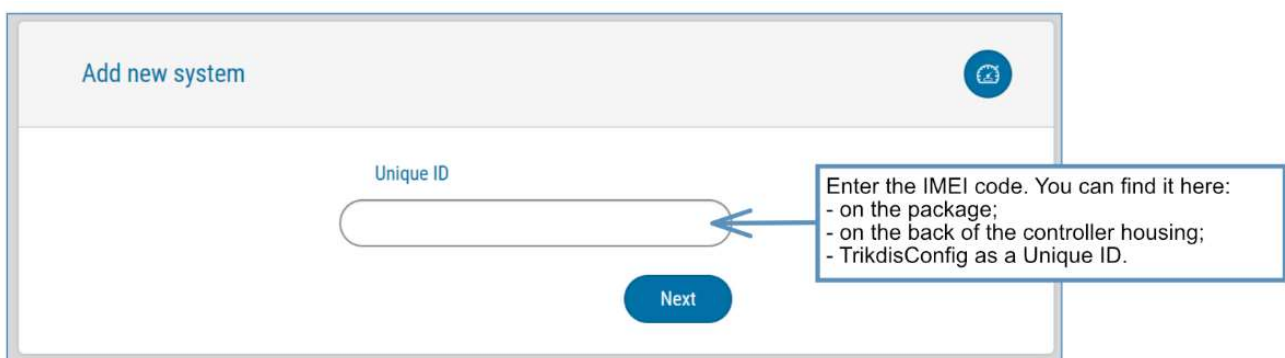
### 8.1 Control via *Protegeus* cloud

Users may control the alarm system remotely via **Protegeus**. The users will also be able to see the status of the system as well as to receive notifications about the events in the system.

1. Download and launch **Protegeus** app or use the portal on the web, which may be accessed via following link: [www.protegeus.eu/login](http://www.protegeus.eu/login).



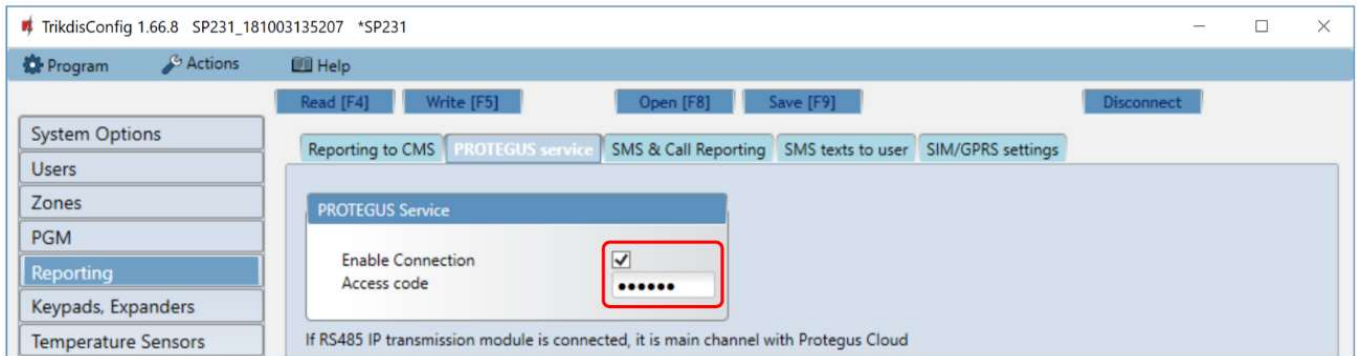
2. Login using your user name and password or register as a new user to the system.
3. Click **Add new system** and input **SP231** IMEI/Unique ID number, which may be found on the physical unit or on the sticker on the package of the unit.



**IMPORTANT:** When connecting **SP231** to **Protegeus**, the unit must be:

1. Inserted with an activate SIM card and successfully entered PIN code (or disabled PIN code).

2. **Protequs Service** is enabled;
3. Power supply ON („PWR” LED is blinking green)
4. Registered to the network („NET1” LED is flashing in green and blinking in yellow).



With **Protequs** app the user is able to:

- 1) Receive notifications of the events. The app stores all the notifications about the events in the registry of safety events.
- 2) To see current status (enabled/disabled) of the alarm system and amend it.
- 3) To see the current outputs of **SP231** PGM (enabled/disabled), when the option „Remote control” is set.
- 4) To grant other users with the specific rights, in order to maintain or control the system.