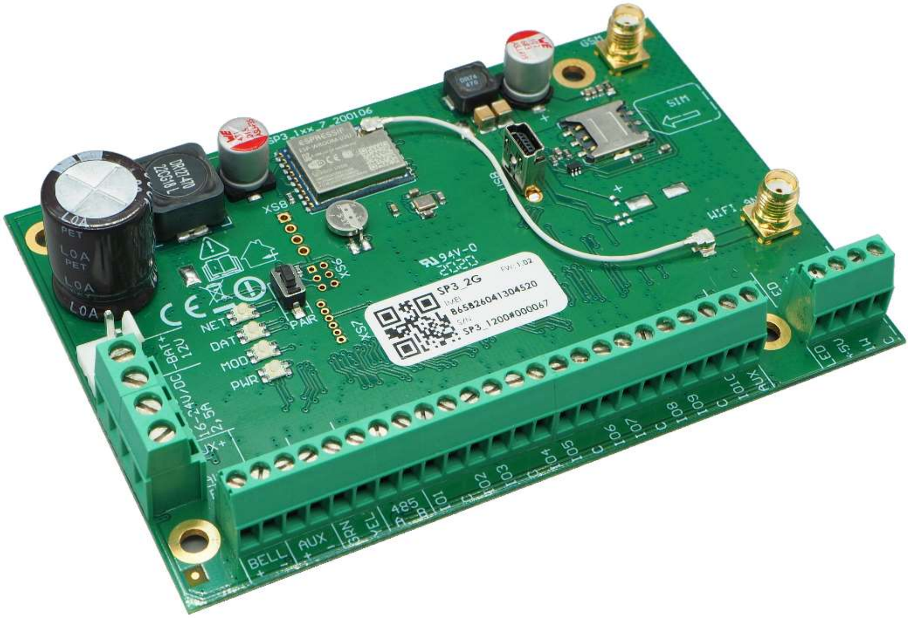


Security control panel

“FLEXi” SP3

Installation and programming manual

February, 2024

Table of contents

Warranty and limitation of liability

The control panel is given a 24-month warranty effective from the date of sale-purchase. For the duration of the warranty period, free repairs are guaranteed for faults caused by the manufacturer.

The warranty is valid if the control panel was installed by qualified personnel following the instructions in this document and the applicable regulations for installing electrical equipment and operated following the instructions in this document and the applicable regulations for safe operation of electrical equipment.

The control panel must be submitted for repairs in the manufacturer‘s packaging along with a defect report stating the nature of the malfunction.

Once the warranty has expired, the control panel‘s technical maintenance and repairs are performed at the buyer‘s expense.

The warranty can be terminated prematurely if:

- Unauthorized personnel repaired or tried to repair the control panel;
- The panel was used for anything other than its intended purpose;
- The panel was stored and (or) installed in unsuitable premises that had incompatible climate conditions or an aggressive chemical environment;
- The panel was mechanically broken and (or) intentionally damaged;
- The panel was damaged by *force majeure* circumstances (lightning discharge etc.).

The manufacturer is not responsible for:

- the control panel‘s malfunctions if the panel is installed or used not according to its manual.
- the control panel‘s malfunctions if the cause is a malfunction or loss of GSM/GPRS/Internet connectivity or malfunctions in the operator‘s network.
- restrictions or termination of GSM/GPRS/Internet connectivity services to the panel‘s buyer or user, and shall not compensate the panel‘s buyer or user for any property or non-property damages suffered from this.
- restrictions or termination of electricity supply service to the panel‘s buyer or user, and shall not compensate the panel‘s buyer or user for any property or non-property damages suffered from this.
- robbery, fire of the premises or any other losses suffered by the panel‘s buyer or user, and shall not compensate the panel‘s buyer or user for any property or non-property damages suffered from these events.

Safety precautions

Read this manual carefully before using the control panel.

The ***„FLEXi“ SP3*** control panel is an electrical device, which means it must be installed and serviced only by qualified personnel following the instructions in this document and applicable regulations for installing electrical equipment.

Power to the panel must be switched off during installation!

The control panel must be installed in a limited access location inside the premises and maintaining a safe distance from sensitive electronic equipment. The panel is not resistant to vibrations, other mechanical effects, humidity and aggressive chemical environments. The control panel complies with the demands applicable to Class II environmental specification of the EN 50131 standard.

⚠

The casings, transformers, batteries and programming equipment used must meet the safety requirements of the EN 60950 standard.

The device is powered from a 230 V voltage 50 Hz frequency power grid through a Class II step-down transformer that reduces the voltage to 16 – 18 V or from a 16 – 24 V DC power supply. A 12 V battery with at least 7 Ah capacity is used as a backup power supply. The current consumption depends on the power of the connected external devices.

A two-pole automatic safety switch must be installed in the power supply circuit for protection. The gap between switch off contacts must be at least 3mm. The safety switch must be installed in a location known to the specialists servicing the control panel.

To disconnect the control panel from the power network:

- from the AC network – switch off the automatic safety switch;
- from the battery – disconnect the terminals.

1 Description

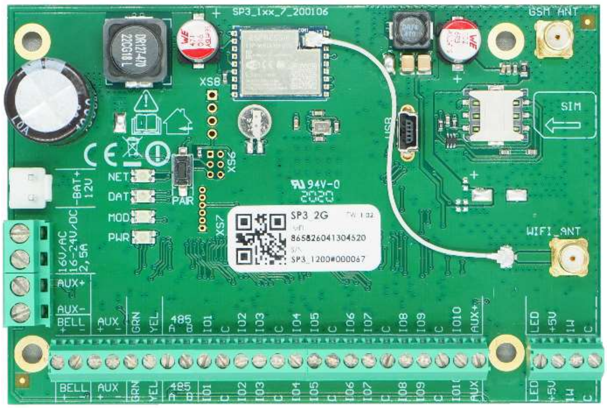
The *„FLEXi“ SP3* control panel is a processor part of intrusion and fire alarm system. It comes with a built-in WiFi module and 2G/4G cellular modem. The ***„FLEXi“ SP3*** allows grouping of 32 wired and wireless zones into an 8 partition system. Users can switch protection modes of different areas of the premises remotely and with ease (with mobile app ***Protegus***, SMS or phone call) or with devices that support personal identification (wired and wireless keypads, electronic keys, RFID cards, etc.). Any triggered system event is reported to the central monitoring station (CMS) and to ***Protegus*** cloud via WiFi and (or) via cellular network if a SIM card is inserted.

When it’s recommended to choose the *„FLEXi“ SP3* control panel?

- For securing small or medium sized premises which will be monitored by a security company. The ***„FLEXi“ SP3*** supports both wired and wireless zones. The panel can provide remote control and system information to both end-users and the security company.
- As a replacement for existing intrusion alarm panel. ***„FLEXi“ SP3*** allows to set a different resistor value to the type used with the old alarm panel. This saves a lot of time during installation, as then there is no need to change resistors in each sensor.
- When the alarm system needs to perform more functions than just protection of the premises. For example: opening the doors and gates, watering the lawn, lighting, heating, ventilation, cooling, controlling as well as many other automatic start and stop functions.

Features

Reporting to the security company‘s central monitoring station (CMS):



- Event reporting either via the built-in WiFi module or cellular 2G/4G modem.
- Additional modules to send reports via Ethernet or VHF/UHF radio waves or Sigfox with chosen priority.
- Any CMS can receive reports, as long as they have TRIKDIS software/IP receiver or any other manufacturer’s IP receiver supporting SIA DC-09 IP protocol.
- Design based on two decades of experience in transmitting reports to main and backup central monitoring station receivers, which allows security companies to provide the highest level of protection to premises
- A setting for necessity to send to CMS, to mandatorily send reports to CMS first, and only then to customers.
- Possibility to send event reports to CMS of two different security companies.
- Multitude number of message transmission channels and multiple transmission priority settings.

Reporting to user:

- Via ***Protegus*** mobile app, which gives warnings about alarm system events using push and special sound notifications.
- Event reporting via SMS messages to 8 cellular numbers.
- Reporting about events using pre-recorded voice notifications (up to 8 cellular numbers. For control panel SP3_12xx with firmware version up to 1.13 inclusive.).
- Remote control of selected premises’ protection mode (Arm/Disarm/Stay/Sleep).
- Remote control of connected devices (lighting system, automatic gates, ventilation, heating, watering systems, etc.).
- Remote temperature measuring.

Inputs and outputs:

- 10 I/O terminals, each one can be set as an input (IN) or output (OUT). Input (IN) types: ATZ, EOL, NC, NO. Different parameters of resistors can be used in EOL and ATZ type circuits. The number of inputs IN can be expanded to 32 by using keypads, iO-8 and iO-WL expander modules.

- The board has 2 dedicated outputs: the bell and the LED. The bell is to control the siren, and the LED is to control indicator lights. The number of outputs can be expanded to 16 by using iO-8 and iO-WL expander modules.
- Seven output operational settings. Each output can be assigned with an operational logic, a preset operation schedule or qualities, for example, thermostat mode.
- One-wire data bus (“1-Wire”) is designated to connect temperature sensors (up to 8), a temperature and humidity sensor (1) or a key fob (“iButton”) reader.
- The GRN-YEL data bus is designated to connect 8 keypads of the same type.
- The RS485 data bus connects ***iO*** series expander modules, ***RF-SH*** radio wave wireless sensor transceiver, ***E485*** Ethernet module, ***T16*** VHF or UHF radio wave transmitter, **Sigfox** module.

Control of alarm system

- 4-digit long control codes (40 in total), which may be used as a coercion code as well. In such scenario, entering the user code will disarm the alarm, yet a special report will be sent to the CMS indicating that the alarm was disarmed as a result of coercion.
- Control using keypads: Protegus SK232LED W, FLEXi SK232LCD; Paradox K636, K10H(V) K32+LED, K32LED, K32LCD+, K35, TM50, TM70; Crow keypad CR16, CR-LCD; CZ-Dallas electronic (“iButton”) key reader; TM17 electronic key reader, RFID reader (Wiegand 26/34).
- Remote control via ***Protegus*** mobile app, phone call or SMS.

Simple installation:

- Multiple sizes of ***„FLEXi“ SP3*** mounting kits that include a decorative white metal housing with a built-in step-down transformer or impulse power supply.
- Default ***„FLEXi“ SP3*** operational settings are based on many years of experience. That allows to install the system in 7 out of 10 small and medium-sized premises without the need to change the default settings.
- The ***„FLEXi“ SP3*** control panel allows to replace the previous panel without changing the resistors in each wired sensor.
- Settings can be saved as a file to be used later.
- Device configuration via USB cable or remotely by using ***TrikdisConfig*** software.
- Remote connection via ***TrikdisConfig*** software allows not only altering ***„FLEXi“ SP3*** parameters but monitoring the operation of the panel as well.
- Two access levels for parameter settings: installer and administrator.

1.1 Technical specifications

Parameter	Description
Power supply voltage[AC / DC]	16 V AC or 16-24 V DC, 2,5 A
Current consumption	Up to 50 mA (stand-by), Up to 200 mA (short-term, while sending)
Backup power source [BAT]	12 V lead – acid battery, 4 Ah/7 Ah
Battery charge current	Up to 500 mA
Power voltage and current for external devices [AUX]	12 V DC, up to 1 A
Siren output [BELL]	1 A
Output [LED]	0,1 A
PGM output	0,1 A
WiFi module	Yes, built-in
WiFi frequency, protocol, encryption type	2,4 GHz, 802.11 b/g/n, WPA, WPA2, WPA mixed
WiFi network configuration type	DHCP or manual
SIM card	1, NANO size

Parameter	Description
GSM/GPRS modem frequencies	850 / 900 / 1800 / 1900 MHz
4G modem frequencies **„FLEXi” SP3_14E** **„FLEXi” SP3_24E** EMEA/Thailand	B1/B3/B7/B8/B20/B28
4G modem frequencies **„FLEXi” SP3_24S** Latin America/Australia/New Zealand	B1/B3/B4/B5/B7/B8/B28
4G modem frequencies **„FLEXi” SP3_24A** North America	B2/B4/B12
Report transmission directions	- To main and backup receivers of 2 different security companies; - To ***Protegus*** cloud, to iOS/Android ***Protegus*** mobile apps; - To 8 mobile phones via SMS messages. Calls 8 mobile phones. If a user answers the call, announces what happened using voice.
Event reporting transmission channels	GPRS or 4G, WiFi, LAN (with module E485), SMS, Voice call, VHF/UHF radio waves (with transmitter T16)
Protocols for connection to CMS	TCP / IP or UDP / IP, or SMS
Event encoding	Contact ID codes
Report encryption	TRK AES 128, SIA IP AES 128
Internal clock	Yes
Buffer memory capacity	60 events
Events log memory	Up to 1000 events. Oldest entries deleted automatically.
User codes	40
Duress code	Two code entry methods can be chosen during programming
Dual purpose terminals [I/O]	10; IN or OUT function selected during programming. When IN is selected, available types: NC, NO, EOL, EOL_T, 3EOL, ATZ, ATZ_T. When OUT is selected, the terminal becomes open collector (OC) type with up to 100 mA current
No. of partitions	8
No. of zones	10 (20 zones if using ATZ), (can be expanded to 32 zones using expanders)
No. of PGM outputs	2 (can be 12 if IO terminals are set as outputs. Can be expanded to 16 outputs with expanders)
Max. number of connected keypads	8
Supported keypads	Protegus SK232 LED W FLEXi SK232LCD Paradox K636 Paradox K10H(V) Paradox K32 LED Paradox K32+ LED Paradox K32LCD+ Paradox K35 Paradox TM50 Paradox TM70 Crow CR16

Parameter	Description
	Crow CR-LCD
Max. number of RFID readers (Wiegand 26/34)	2
1-Wire data bus length [1 WIRE]	Up to 30 m
Compatible temperature sensors	Maxim®/Dallas® DS18S20, DS18B20; AM2301 series
Max. number of temperature sensors connected to *1-Wire* data bus	8 (Dallas) or 1 (if an AM2301 series sensor is used)
Compatible electronic (*iButton*) keys [1 WIRE]	Maxim®/Dallas® DS1990A
Max. no. of electronic (*iButton*) keys	40
RS485 data bus length	Up to 100 m
Max. no. of devices connected to *RS485* data bus	8

Supported modules	***iO-8*** – expander module;
	iO – expander module;
	iO-MOD – iO-WL radio wave transceiver;
	iO-WL – wireless expander module;
	RF-SH – radio wave receiver for wireless sensors;
	E485 – module for connecting to Ethernet network;
	TM17 – iButton key reader;
	CZ-Dallas – iButton key reader;
	T16 – VHF or UHF radio wave transmitter;
	iO-LORA - expander module;
	iO8-LORA - expander module;
	RFID reader.

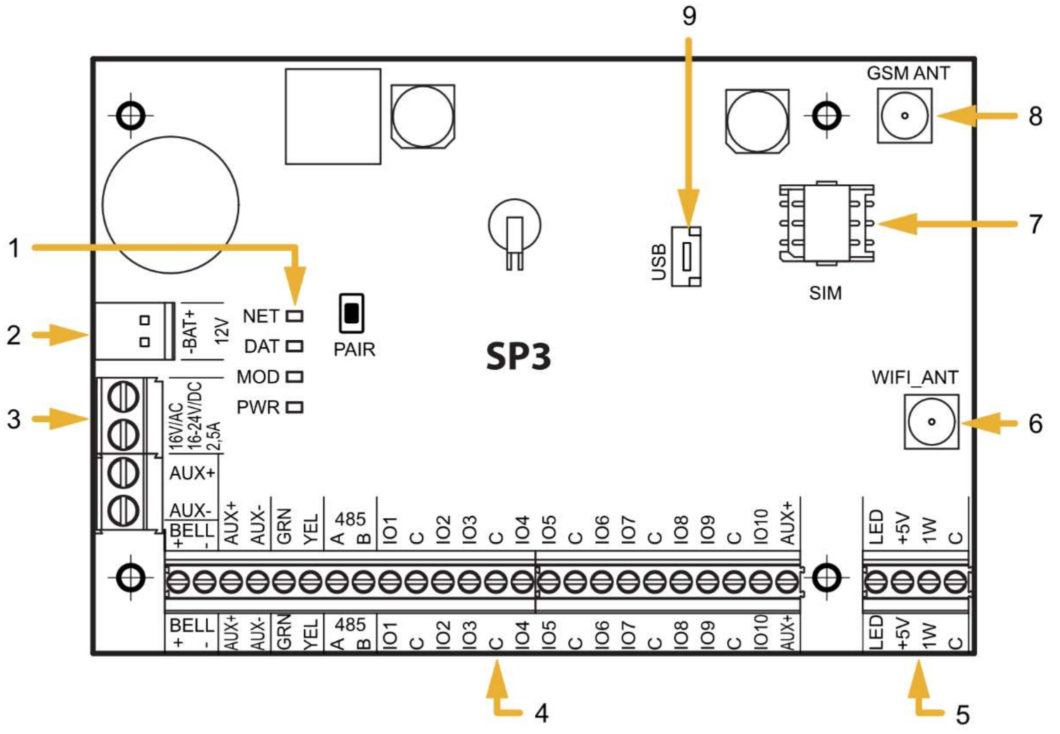
Operating environment	Temperature from -10 °C to +50 °C, relative humidity 80% at +20°C, no condensation.
Dimensions of the control panel	117x79x25 mm
Weight	0,1 kg

1.2 List of compatible modules

Module name	Current
Keypad Protegus SK232 LED W	Min 60 mA, max 150 mA
Keypad FLEXi SK232LCD	Min. 25 mA, max. 60 mA
Keypad Paradox K636	Min 40 mA, max 70 mA
Keypad Paradox K10H(V)	Min 44 mA, max 72 mA
Keypad Paradox K32 LED	Min 49 mA, max 148 mA
Keypad Paradox K32+ LED	Min 49 mA, max 148 mA
Keypad Paradox K32LCD+	Min 70 mA, max 150 mA
Keypad Paradox K35	Min 30 mA, max 70 mA
Keypad Paradox TM50	Min 100 mA, max 230 mA
Keypad Paradox TM70	Min 200 mA, max 330 mA
Keypad Crow CR16	Min 40 mA, max 75 mA
Keypad Crow CR-LCD	Min 40 mA, max 75 mA

Module name	Current
iO-8 expander module	Max 20 mA
iO expander module	Max 50 mA
iO-MOD – iO-WL radio wave transceiver	Min 50 mA, max 150 mA
iO-WL wireless expander module	Max 200 mA
RF-SH transceiver for wireless sensors	Max 100 mA
E485 Ethernet communicator	Min 50 mA, max 150 mA
TM17 iButton key reader	Max 50 mA
CZ-Dallas iButton key reader	Max 25 mA
T16 (VHF or UHF) radio wave transmitter	Min 100 mA, max 1,2 A
RFID reader (Wiegand 26/34)	Max 100 mA
iO-LORA expander module	Max 50 mA
iO8-LORA expander module	Max 50 mA

1.3 Purpose of external terminals



1. Connectivity and operation indicator lights.
2. Backup power supply terminal block.
3. Main power supply terminal block.
4. External terminal block.
5. 1-WIRE data bus terminal block.
6. SMA screw-on type connector for WiFi antenna.
7. Nano-SIM card holder.
8. SMA screw-on type connector for GSM antenna.
9. USB Mini-B connector for configuring the control panel’s settings.

Terminal	Description
Power terminal	Power supply terminal (16 V AC or positive 16-24 V DC)
Power terminal	Power supply terminal (16 V AC or negative 16-24 V DC)
BAT+	Backup power supply positive terminal 12 V

Terminal	Description
BAT-	Backup power supply negative terminal 12 V
AUX+	Positive 12 V power terminal for external devices
AUX-	Common negative terminal
GRN	Keypad data bus
YEL	Keypad data bus
A 485	Terminal A of *RS485* data bus
B 485	Terminal B of *RS485* data bus
IO1 – IO9	Input/output terminals (default setting – input)
IO10	Input/output terminal (default setting – PGM output, Fire Sensor Reset)
C	Common negative terminal
LED	PGM output (default setting – System State)
+5 V	Positive 5 V power terminal for *1-Wire* devices
1 WIRE	*1-Wire* data bus terminal
C	Common negative terminal

1.4 LED indication of operation

LED indicator	Light status	Description
NET	Green blinking	SIM card is registering on GSM network.
	Green solid	SIM card registered on GSM network.
	Yellow blinking	Indicates GSM signal strength from 0 to 5. 3 is sufficient.
DAT	Off	No unsent event messages.
	Green solid	Message is being sent.
	Yellow solid	There are unsent event messages in buffer memory.
MOD	Green blinking	Connecting to WiFi network.
	Green solid	Connected to WiFi network.
PWR	Green blinking	No operational problems.
	1 red flash	No SIM card detected
	2 red flashes	The PIN card of the SIM card is incorrect
	3 red flashes	Unable to connect to GSM network
	4 red flashes	Unable to connect to CMS receiver using channel 1
	5 red flashes	Unable to connect to CMS receiver using channel 2
	6 red flashes	Internal clock not set
	7 red flashes	Insufficient backup power supply voltage
	8 red flashes	No AC power
	9 red flashes	Unable to connect to WiFi network

2 Powering the security control panel

2.1 Main power supply

The control panel and the entire alarm system can be powered either from an alternating or a direct current source. In both cases, a backup power supply – a 12 V battery – must be connected to the system to ensure the supply of power is uninterrupted. To meet the demands of the EN50131 standard, the backup battery must be able to work for 12 hours for security Grade II or 60 hours for security Grade III after losing power from the main power supply. Take into account the total current consumption of the additional connected modules, the current consumption of individual modules is listed in chapter 1.2 “List of compatible modules”.

2.2 Backup power supply

If there are problems with powering the system from the main power supply, an *AC Fault* event report will be generated and the panel will automatically switch to the backup 12 V battery. If the battery’s voltage falls to 11,5 V, a *Low Battery* event report will be generated. The battery will be disconnected if the voltage falls bellow 9,5 V. If AC network voltage is restored, an *AC Restore* report will be generated and the battery charging process will begin automatically. When the battery’s voltage rises to 12,6 V, a *Battery Restore* event report will be generated.

2.3 Control panel kits

2.3.1 Control panel *„FLEXi“ SP3*

Name	Quantity
„FLEXi“ SP3 control panel board	1 pc.
Wire for connecting battery	1 pc.
Resistor 2,2 kΩ	20 pcs.
Resistor 4,7 kΩ	10 pcs.
Plastic spacer (mounting parts)	4 pcs.
Antenna ME301M with 2,5 m long cable	2 pcs.

2.3.2 Control panel *„FLEXi“ SP3* KIT

Name	Quantity
„FLEXi“ SP3 control panel board, built into metal housing	1 pc.
Metal housing K01 with 40 VA transformer	1 pc.
Resistor 2,2 kΩ	20 pcs.
Resistor 4,7 kΩ	10 pcs.
Antenna ME301M with 2,5 m long cable	2 pcs.
Wire for connecting battery	1 pc.
Tamper sensor	1 pc.
Terminal block with 0,5 A fuse	1 pc.

2.3.3 Control panel *„FLEXi“ SP3* KITi

Name	Quantity
„FLEXi“ SP3 control panel board, built into metal housing	1 pc.
Metal housing K02 with Mean Well impulse power supply	1 pc.

Name	Quantity
Resistor 2,2 kΩ	20 pcs.
Resistor 4,7 kΩ	10 pcs.
Antenna ME301M with 2,5 m long cable	2 pcs.
Wire for connecting battery	1 pc.
Tamper sensor	1 pc.
Terminal block with 3,15 A fuse	1 pc.

Note: USB wire (Mini-B type) for programming the control panel sold separately.

3 Installation of the system

3.1 Recommended order of installation

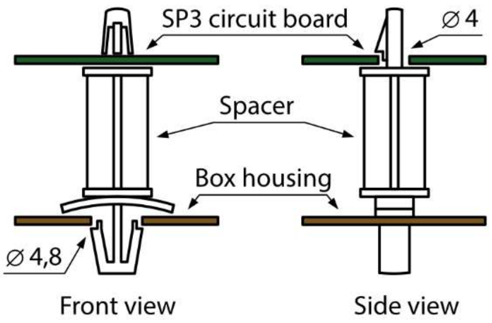
Planning the system:

- Sketch a plan of the premises and mark the areas where the metal housing with the control panel, keypad (-s), signallers, equipment automatically or remotely controlled by the control panel will be installed.
- After evaluating the premises, the demands raised for their protection and the characteristics of possible sensors, choose the number of sensors to use, their types, and the locations to install them.

3.1.1 Installing the control panel into the mounting housing

The control panel’s board can be installed into a mounting housing that already has a step-down transformer with a 500 mA fuse installed and also has space intended for a backup battery.

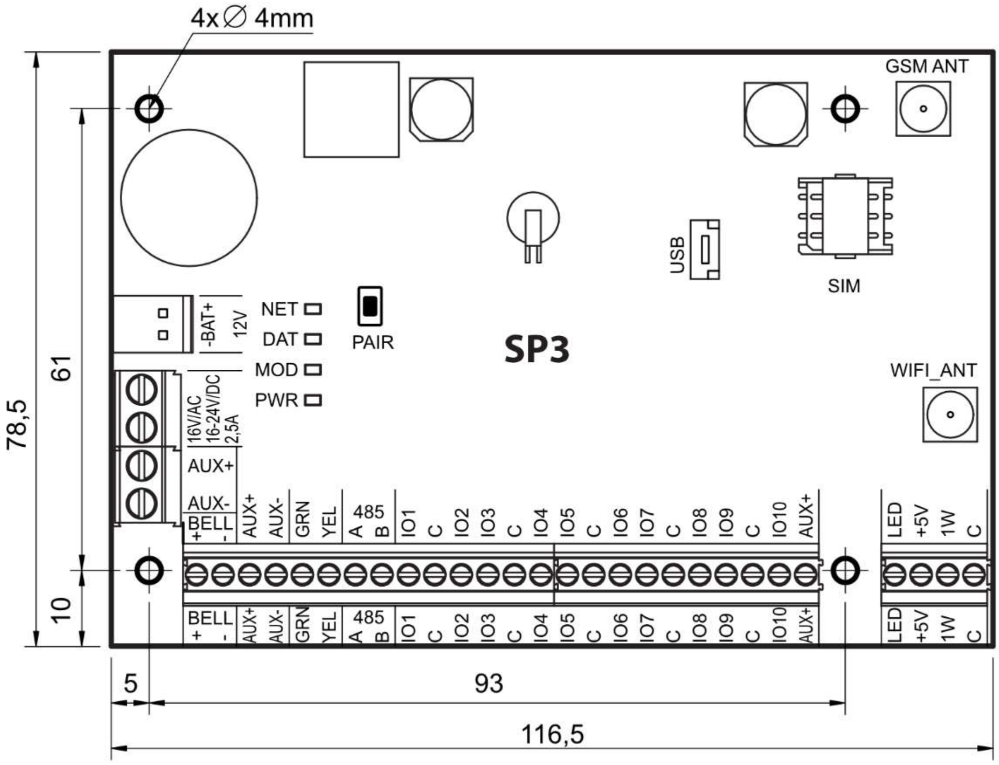
Install the control panel into the chosen plastic or metal housing using plastic spacers. If you chose a metal housing, do not forget to ground it during installation. The chosen housing must meet demands described in the EN 60950 and EN 50131 standards.



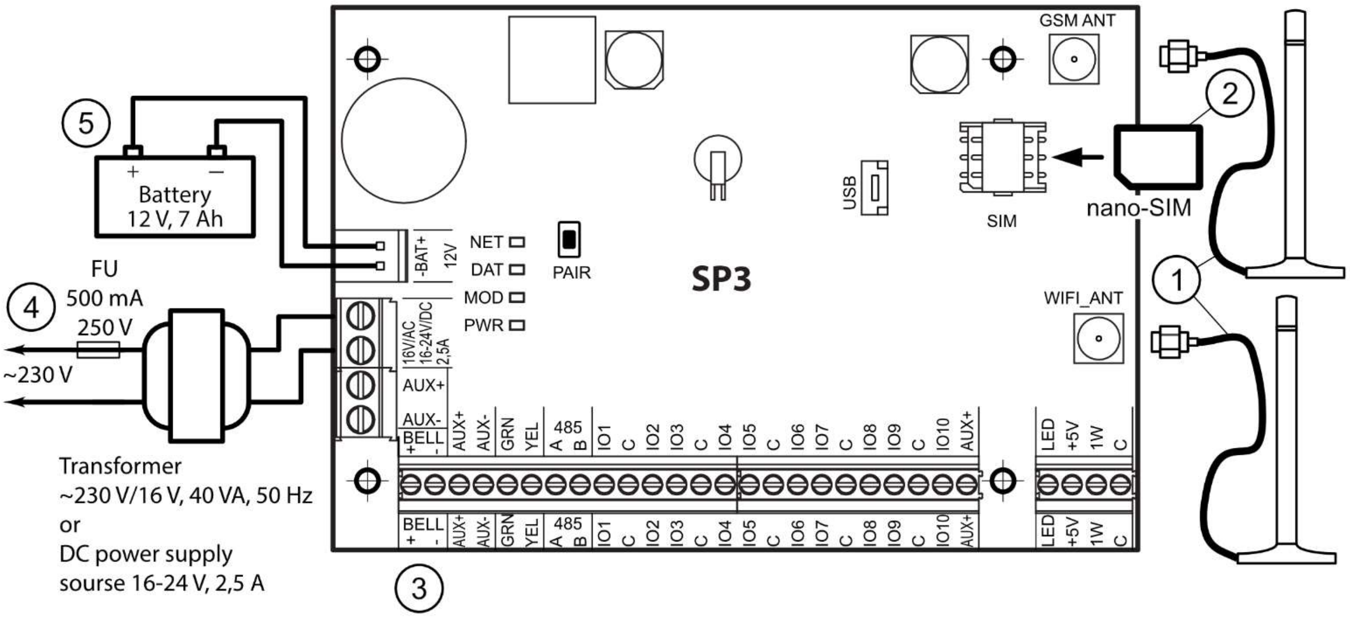
Plastic spacers.

Dimensions of the „FLEXi“ SP3 board

The picture below shows the dimensions of the board and its mounting holes (in millimeters), and also the locations of the holes.



3.1.2 Order of connecting devices



1. Connect GSM and WiFi antennas to the antenna connectors.
2. Insert an activated SIM card into the SIM card holder.
3. Using the given connection schematics and the connection schematics for every device to be connected, connect the door and window magnetic contacts, motion, fire and other sensors, signallers, keypads and controlled devices. Connect the housing door and wall mounting tamper sensors to the panel’s terminals.
4. Connect the wires of the main power supply to the control panel’s AC/DC terminals. Turn on the main power supply. The ***„FLEXi“ SP3*** will recognize the keypads, expanders and interfaces that are correctly connected using 1-WIRE and YEL/GRN data busses.

5. Insert a backup battery into the mounting housing. Connect the battery’s terminals to the BAT+ / BAT– terminals on the control panel.

Note:	The battery must recharge in less than 72 hours for the alarm system to meet security Class II or 24 hours to meet security Class III.

3.1.3 Recommendations for setting the control panel’s parameters

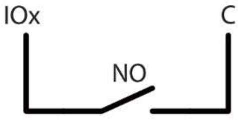
1. See chapter 5 “Setting parameters using TrikdisConfig” for information on how to connect to the panel to configure it.
2. System settings:
   a. **Partitions.** If you would like to turn on protection for specific zone groups separately, the alarm system can be divided into partitions. See chapter 5.2 ““System Options” window” on how to divide the system and set the required partition attributes.
   b. **Zones.** See chapter 5.7 ““Zones” window” to set every zone according to the sensors’ characteristics and desired operation of the alarm after an event occurs in that zone. If the alarm system is divided into partitions, every zone can be assigned to a desired area.
   c. **Users.** System *users* must be created to control the alarm system via keypad, iButton key or phone call (SMS message). See chapter 5.4 ““Users & Reporting” window” on how to create *users* and assign them permissions.
3. Message sending:
   a. **Time setting.** The control panel’s time must be set in order to receive messages with exact timestamps. See chapter 5.2 ““System Options” window”.
   b. **Enable report sending.** Default settings enable the event report sending function for all events. If any event occurs, its report will be sent to the set recipients using the set channels. See chapter 5.10 ““System events” window” on how to disable reporting of chosen events.
   c. **SIM card parameters.** If messages need to be sent using mobile networks, you must set parameters for the SIM card being used (see chapter 5.2 ““System Options” window”).
   d. **Reports to central monitoring station.** Sending reports to the central monitoring station is disabled by default. See chapter 5.3 ““Reporting to CMS” window” on how to set parameters for sending messages to CMS.
   e. **Reports to user.** Communication with ***Protegus*** cloud is enabled by default, and sending reports using SMS messages and phone calls is disabled. See chapter 5.10 ““System events” window” on how to set parameters for sending reports to the user’s mobile phone.
4. Remote control of the system:
   a. **User access.** The alarm system can be controlled remotely (via phone call and (or) SMS messages) by users whose phone numbers are entered into the User list. See chapter 5.4 ““Users & Reporting” window” on how to enter phone numbers.
   b. **Control via phone call.** Phone calls allow not only to arm or disarm all or part of the security system, but also to control (turn on or off) equipment connected to PGM outputs. See chapter 4.4 “Control via phone call” on what parameters to change to allow phone calls to modify the state of a selected PGM output that has an equipment control circuit connected to it.
   c. **Control via SMS messages.** With SMS messages, it is possible to change some of the control panel’s operational parameters, arm or disarm all or part of the premises, control (turn on or off) equipment connected to the PGM outputs. See the list of SMS commands on chapter 4.3 “Configuration and control via SMS messages”.
5. Additionally:
   a. **Changing control codes.** We recommend changing the panel’s default alarm control and configuration codes to something only You know.
      - The **Master** user code can be changed in the branch **Users & Reporting** of the program menu.
      - **The remote SMS control** code can be changed in the **System Options** window of the program menu, in the **SMS Password** field of the **Access** section.
      - **Access codes for connecting with TrikdisConfig** can be changed in the **Access** section of the **System Options** branch of the program menu.

3.2 Connecting sensors

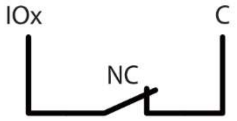
There are 10 terminals ***IO1–IO10*** (inputs) on the control panel board for connecting sensor circuits. The number of inputs can be expanded to 32 using input expanders (***iO, iO8, iO-WL, RF-SH, iO-LORA, iO8-LORA***). Any terminal can be set as an input and assigned zone attributes: circuit type (NO, NC, EOL, EOL_T, 3EOL, ATZ, ATZ_T); sensitivity to temporary circuit events; zone function (Delay, Instant, Instant Stay, Interior, Interior Stay, Fire, Keyswitch, 24_hour, Silent, Silent 24h), see chapter 5.7 ““Zones” window”. The ***iO8*** and ***iO8-LORA*** expanders support all types of zone resistor (EOL types) of the control panel.

Schematics for connecting sensors.

Normaly open (NO)

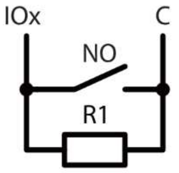


Normaly close (NC)

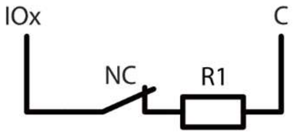


RT	R1	R2
2.2k	2.2k	4.7k
1k	1k	2.2k
5.6k	5.6k	3.3k
5.6k	3.3k	5.6k
3.3k	6.8k	3.3k
2.2k	4.7k	8.2k

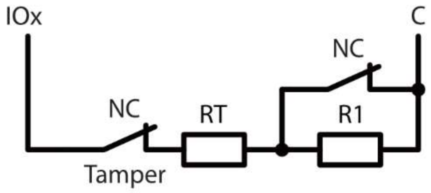
Normaly open with End of line resistor (EOL)



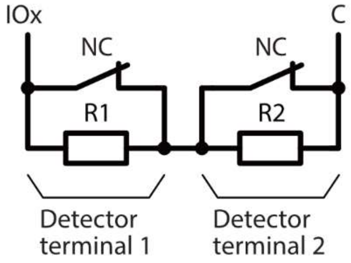
Normaly closed with End of line resistor (EOL)



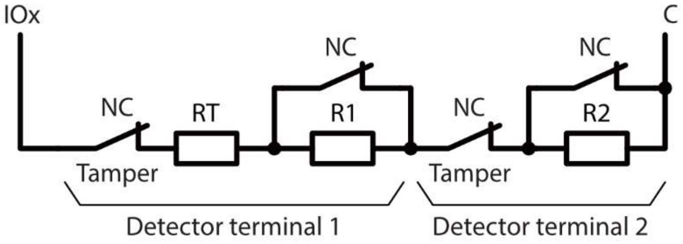
Normaly closed with End of line resistor, with tamper and wire fault recognition (EOL_T)



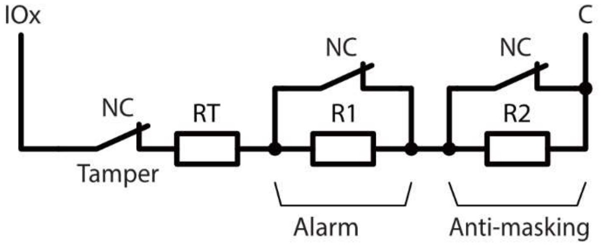
Normaly closed without EOL (ATZ)



Normaly closed with EOL, with tamper and wire fault recognition (ATZ_T)

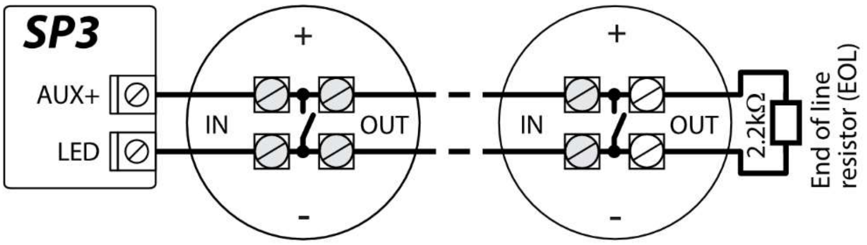


Normaly closed with End of line resistor, with tamper and wire fault recognition (3EOL)



3.3 Connecting smoke detectors

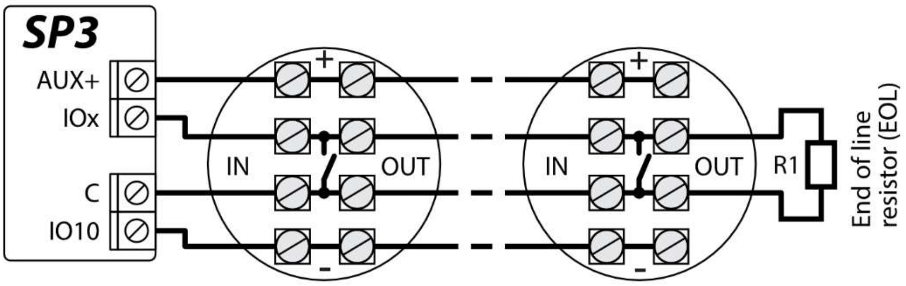
Schematic for connecting two-wire smoke detectors to PGM (LED) outputs. When using this scheme for connecting fire detectors, it is necessary to mark the "**LED out as 2Wire fire**" field with a tick (see chapter5.2 “Window “System options””).



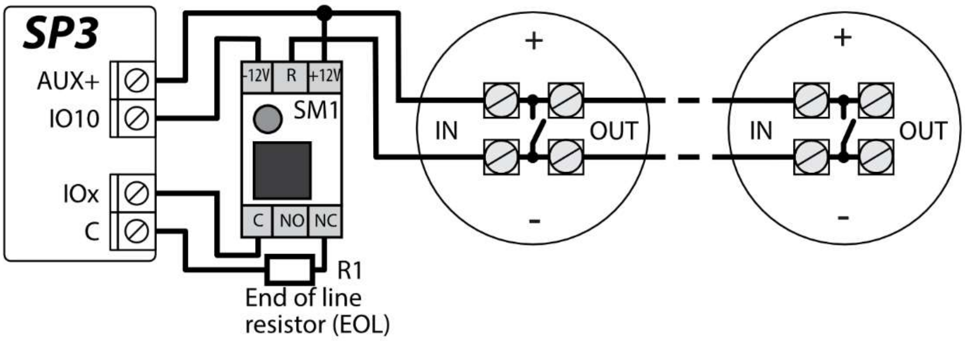
Schematic for connecting four-wire smoke detectors.

To connect a smoke detector circuit to a selected input, the input (IOx) must be assigned the ***Fire*** zone function (see chapter 5.7 ““Zones” window”).

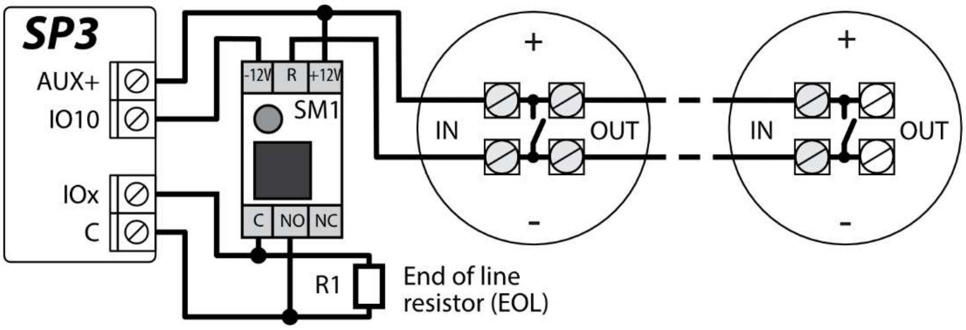
To connect a four-wire smoke detector circuit to a selected PGM output (IO10), the ***Fire Sensor Reset*** function must be assigned to the output (see chapter 5.8 ““PGM” window””).



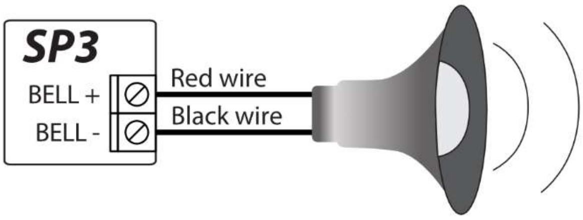
Schematic for connecting two-wire smoke detectors.

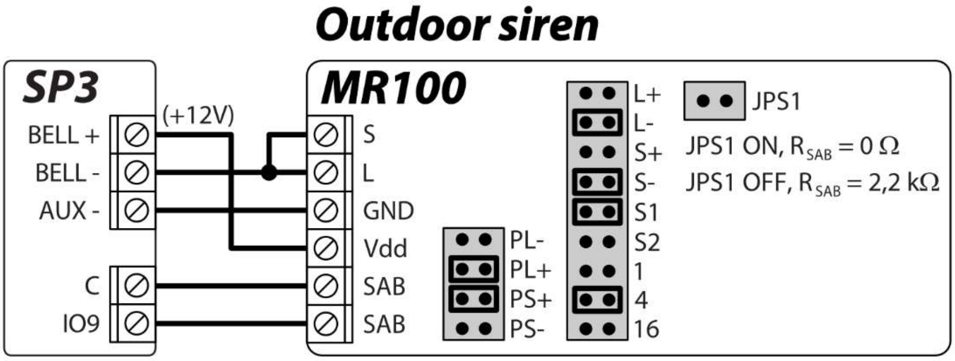


Or



3.4 Schematic for connecting a siren

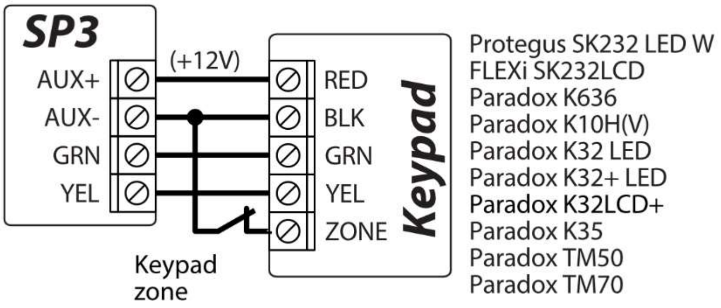


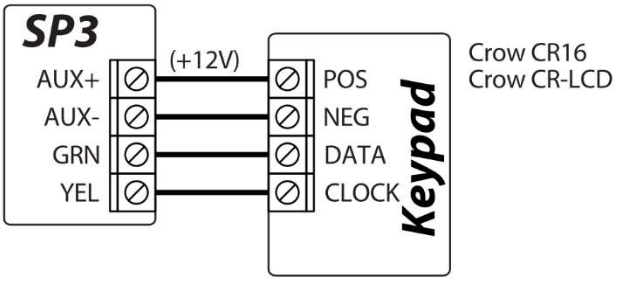


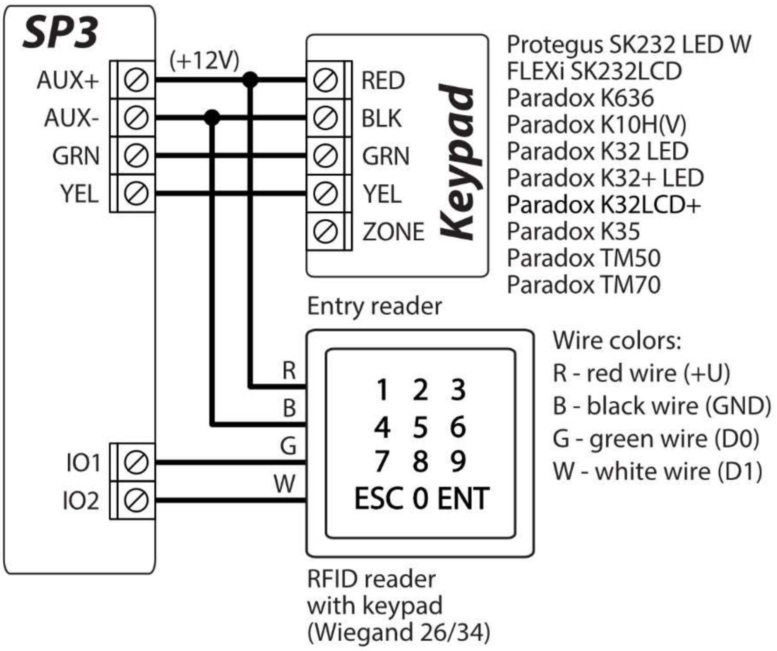
The diagram shows the connection and settings of the **MR100** outdoor siren. If the control panel will use a different method for monitoring the EOL (factory setting is 2.2 kOhm EOL) of the siren tamper (SAB terminals) circuit, it is necessary to close the JPS1 contacts and connect a resistor of the corresponding rating in series to the tamper circuit. The **24_hours** zone type is factory set for IO9 input.

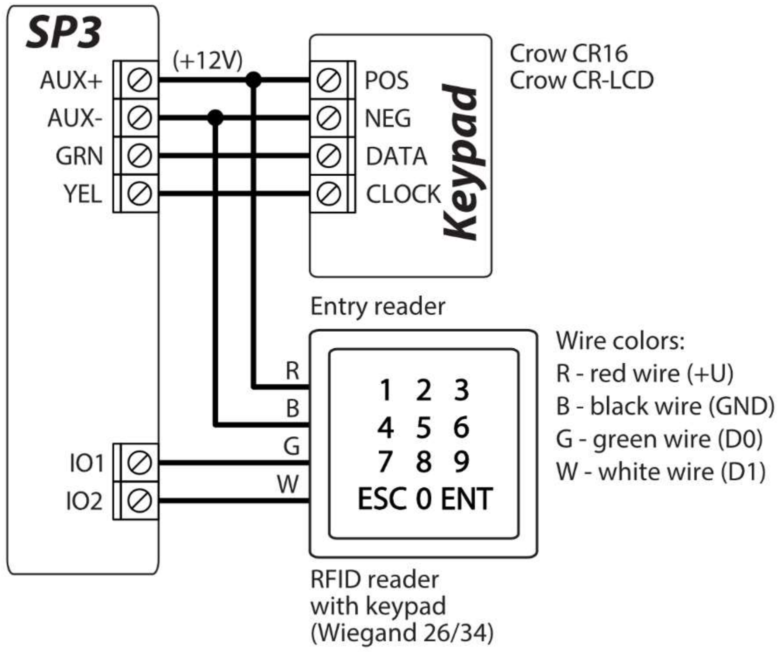
3.5 Schematics for connecting keypads and RFID readers (Wiegand 26/34)

Up to 8 devices can be connected to the keypad data bus. The type of the connected keypad must be specified using TrikdisConfig software (see chapter 5.5 ““Modules” window”). The control panel will automatically recognize and link the connected devices.

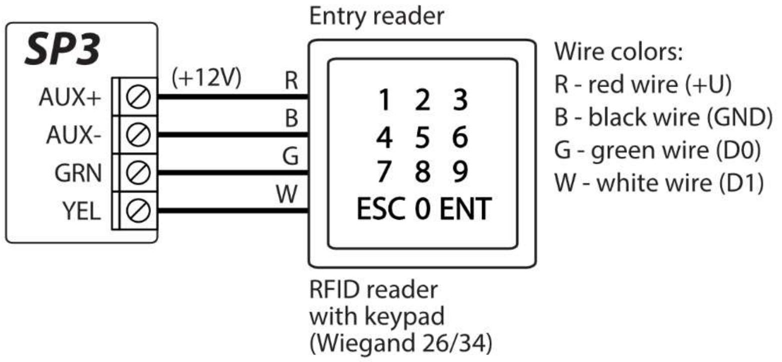


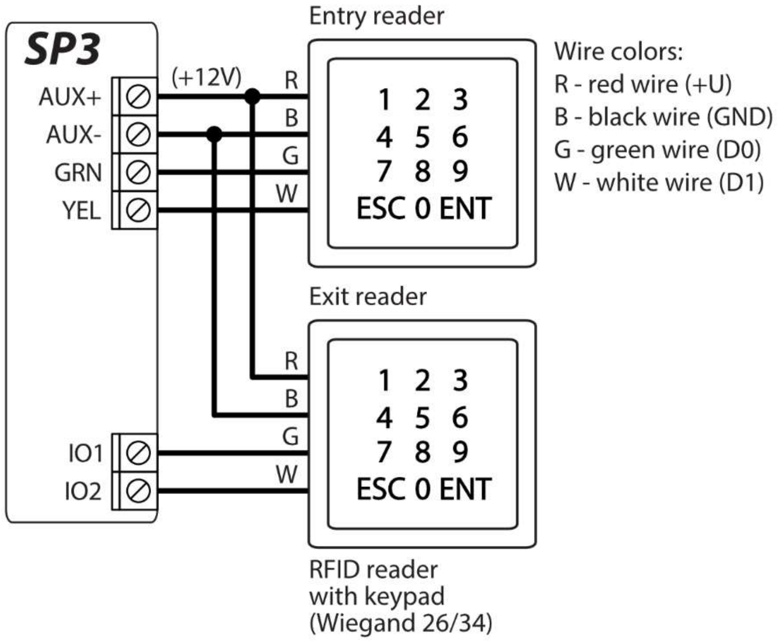






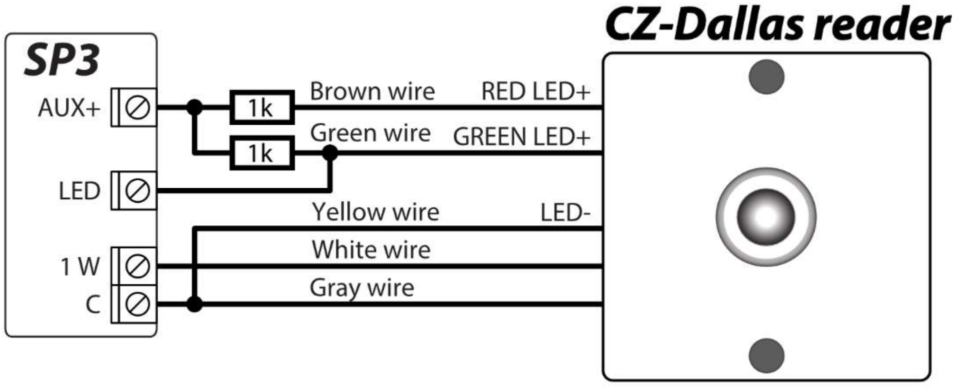
Up to 2 RFID readers can be connected to the control panel. If 2 RFID readers are connected to the control panel, no keypads can be connected.





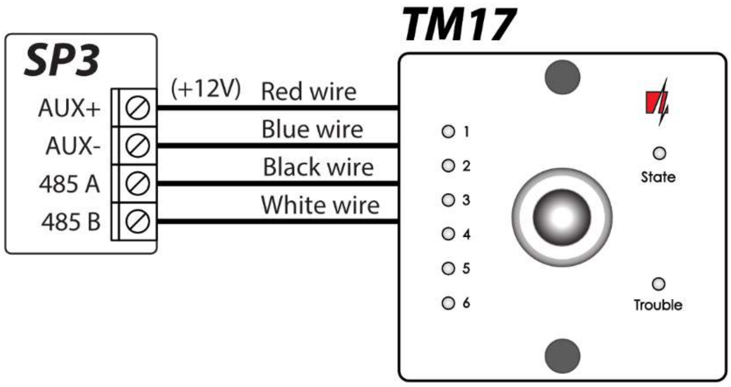
3.6 Schematics for connecting TM17, CZ-Dallas readers

The **CZ-Dallas** iButton key reader connects to the ***„FLEXi“ SP3*** using the “*1 Wire*” data bus. The length of the wires connecting to the data bus can be up to 30 m:

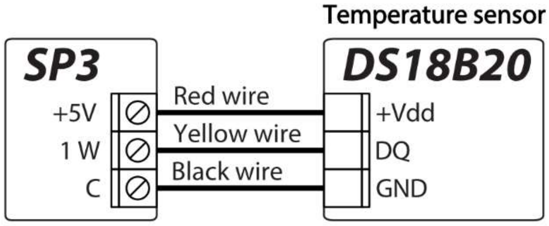


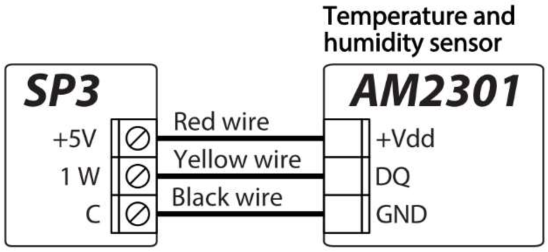
The output LED must be set to the "System state" type.
Security alarm system is arm - the iButton reader light ir red.
Security alarm system is disarm - the iButton reader light is yellow.

The **TM17** reader connects to the ***„FLEXi“ SP3*** using the *RS485* data bus. The length of the wires connecting to the *RS485* data bus can be up to 100 m.



3.7 Schematic for connecting a temperature sensor



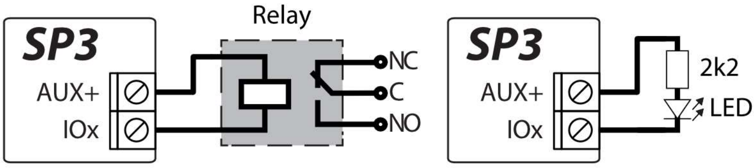


Temperature sensors should be connected according to the given schematic. Maxim®/Dallas® DS18S20, DS18B20 temperature sensors (up to 8) or AM2301 humidity and temperature sensor (up to 1) can be connected to the ***„FLEXi“ SP3*** control panel.

If a wire longer than 0,5 meters is used to connect a temperature sensor, we recommend using **twisted pair cable (UTP4x2x0,5 or STP4x2x0,5**).

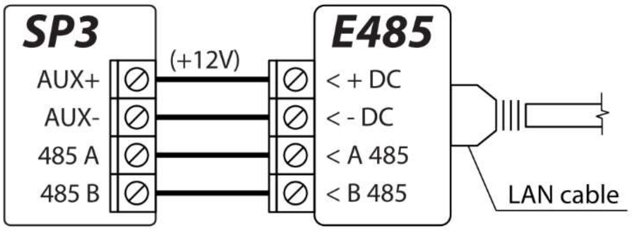
The *+5V* terminal on the board is for supplying devices connected to the *1-Wire* data bus with 5 V DC voltage. The maximum output current is 0,2 A. The output is protected from overload. If the maximum allowed current is exceeded, the power will automatically be switched off. The control panel automatically recognizes and links connected devices.

3.8 Schematics for connecting a relay and an LED indicator



Using the relay terminals, it is possible to remotely control (turn on/off) various electrical devices. The panel’s universal I/O terminal must be configured as an output (OUT) and must have the definition **Remote control** assigned.

3.9 Schematic for connecting Ethernet communicator E485



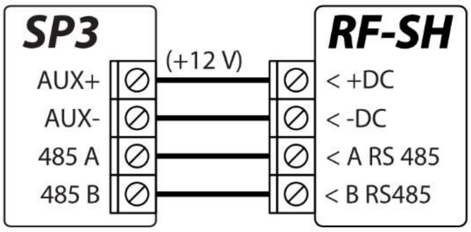
RS485 connection
up to 100 m

The ***E485*** module allows the control panel to send and receive control commands using a wired internet connection. If an ***E485*** module is connected to the control panel, reports to the CMS and to ***Protegus*** will be sent using wired internet and mobile internet will not be used. If wired internet connectivity is lost, mobile internet will be used for sending reports to the CMS. If wired internet connectivity is restored, the control panel will automatically stop using mobile internet and will switch to communicating with CMS and ***Protegus*** mobile app using the ***E485***, i.e. wired internet.

See chapter 5.3 ““Reporting to CMS” window” on how to choose connectivity priority (SIM, WiFi, LAN(E485)). The ***„FLEXi“ SP3***’s configuarion for the ***E485*** Ethernet module is described in chapter 5.5. ““Modules” window”.

If the ***E485*** is connected, a SIM card is not necessary for the control panel.

3.10 Schematic for connecting RF-SH

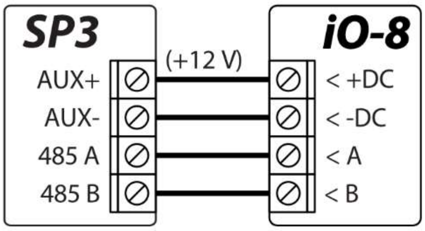


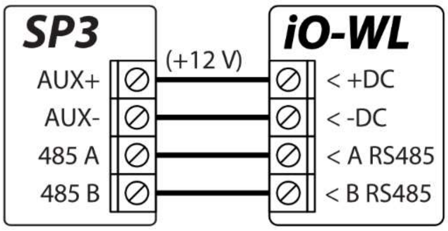
With the ***RF-SH*** it is possible to connect 64 wireless remote controls, 16 wireless sirens, 32 wireless sensors, 8 wireless keypads to the security system.

The ***„FLEXi“ SP3*** ’s configuration for expander modules is described in chapter 5.5 ““Modules” window”.

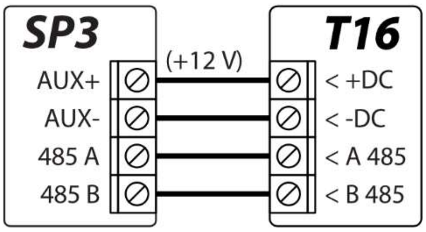
3.11 Schematics for connecting iO series expander modules

If the security control panel ***„FLEXi“ SP3*** needs to have more inputs IN or outputs OUT, connect a wired or wireless TRIKDIS ***iO*** series input and output expander. The ***„FLEXi“ SP3*** ’s configuration for expander modules is described in chapter 5.5 ““Modules” window”.





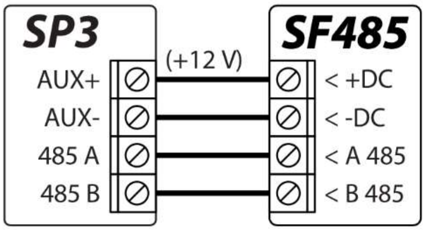
3.12 Schematics for connecting RF transmitter T16



RF transmitter **T16** used for transmitting security control panel event messages via TRIKDIS radio networks.

The transmitter can send its own event messages and event messages received from security control panels to the CMS (central monitoring station) with the possibility to forward to the end user.

3.13 Schematics for connecting SF485



SF485 works as secondary channel for security panel events transmission to CMS (Central Monitoring Station) or ***Protegus*** mobile app over the SigFox network, when primary channel fails. Events are transmitted in Contact ID format.

3.14 Turning on the control panel

To turn on the control panel, first you need to turn on its power supply. The control panel’s LED indicators must operate in the following way:

- The PWR diode must blink in green – this indicates that the power supply voltage is sufficient;
- The NET diode must be green solid and periodically blink in yellow no less than 3 times – the green color indicates that the SIM card is successfully registered on the mobile network, while the number of green flashes indicate the mobile signal strength.

Note: Sufficient mobile network strength is 3 (three yellow flashes of the NET indicator).
If you see fewer yellow flashes of the NET diode, the strength of the mobile network is insufficient. We recommend choosing a different place for installing the control panel, changing the location of the antenna or using a more sensitive mobile antenna.

If the light indication is different, see chapter 1.4 “LED indication of operation” to find out the reason.

If all of the ***„FLEXi“ SP3*** indicator lights are off, check the power supply and connections.

4 Remote control

4.1 Linking the *„FLEXi“ SP3* to a user’s *Protegus* account

With ***Protegus***, users can control the alarm system remotely. They can also see the system state and receive system event reports.

1. If you do not yet have a personal ***Protegus*** cloud account, open the page www.protegus.app using a web browser and create an account by clicking the “*Sign up”* link.
2. Click on the link you receive in your e-mail to activate your account.
3. Download and install ***Protegus*** mobile app into your smartphone.

GET IT ON Google Play | Download on the App Store | WEB APP protegus intelligent security & control

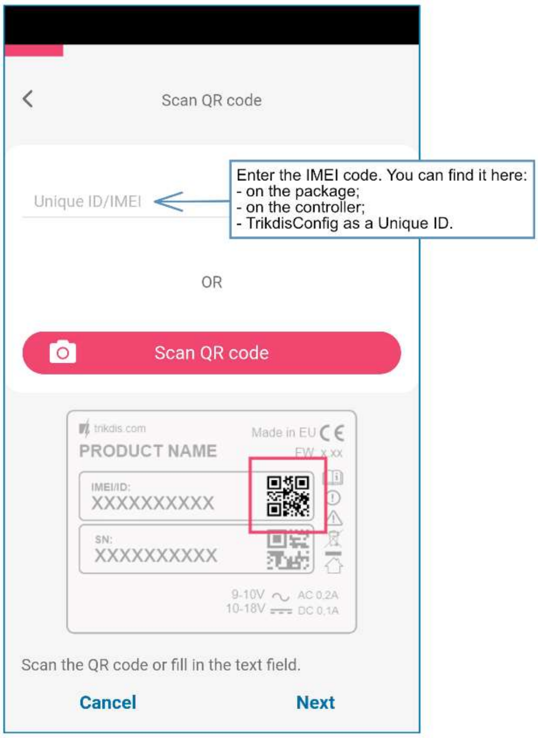
4. Launch the ***Protegus*** mobile app on your smartphone and log in using your username and password.

IMPORTANT: When adding the ***„FLEXi“ SP3*** to ***Protegus***:

1. An activated SIM card must be inserted and the PIN code must be entered or disabled;

2. ***Protegus cloud*** service must be enabled. See chapter 5.4 “Users & Reporting” (**Protegus** tab);
3. The power must be switched on (“POWER” LED must be green solid);
4. Must be connected to network (“NET” LED must be green solid when connected to GSM network; and/or “MOD” LED must be green solid when connected to WiFi network).

5. Click „**Add new system**” and enter the ***„FLEXi“ SP3***’s “*Unique ID/IMEI*” number. You can find it on the packaging sticker. After entering the ID, click **“Next”**.

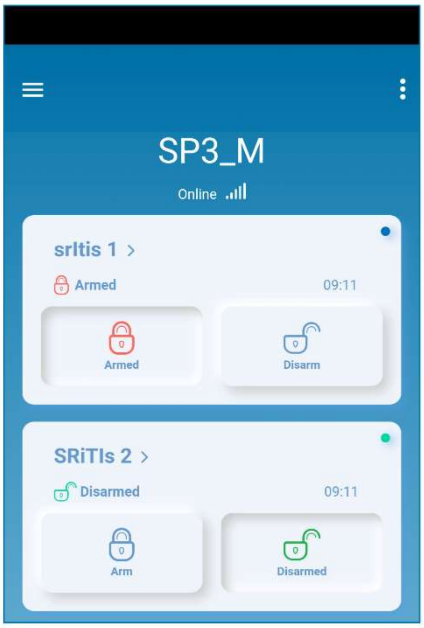


Enter the IMEI code. You can find it here:
- on the package;
- on the controller;
- TrikdisConfig as a Unique ID.

Scan the QR code or fill in the text field.

4.2 Arming/disarming the system using *Protegus*

1. To control the system, go to the ***Protegus***.
2. In ***Protegus***, click on the “**Armed**” (or “**Disarmed**”) button. In the window that opens, enter the control panel user code.



3. If the program does not respond to Your commands or the program window views are entirely different, go to ***Settings*** -> ***System configuration*** -> **System out of sync?** and click the button “**Sync**”.

4.3 Configuration and control via SMS messages

The ***„FLEXi“ SP3*** security control panel can be controlled and configured remotely using SMS messages.

Structue of SMS message: Command space Password space Data

The control panel’s default SMS password is **123456**. For safety reasons we recommend changing it to something only You know and not forgetting Your password!

SMS command list

Command	Data	Description
INFO		Request information about the control panel. Object name, partition state, IMEI number, GSM signal strength, firmware version and serial number will be included in the reply. E. g.: ***INFO 123456***
RESET		Reset the device. E.g.: ***RESET 123456***
OUTPUTx	*ON*	Turn on an output, “x” is the output number. E.g.: ***OUTPUT1 123456 ON***
	OFF	Turn off an output, “x” is the output number. E.g.: ***OUTPUT1 123456 OFF***
	PULSE=ttt	Turn on an output for a specified time - “x” is the output OUT number and “ttt” is a three-digit number that specifies pulse time in seconds. E.g.: ***OUTPUT1 123456 PULSE=002***
PSW	*New password*	Change password. E.g.: ***PSW 123456 654123***
TIME	*YYYY/MM/DD,12:00:00*	Set date and time. E.g.: ***TIME 123456 2018/01/03,12:23:00***
TXTA	*Object name*	Specify object name. E.g.: ***TXTA 123456 Namas***
RDR	*PhoneNR#SMStext*	Forwards SMS messages to the specified number. The phone number must start with a "+" symbol and the international country code. E.g.: ***RDR 123456 +37061234567#forwarded text***
ASKI		Send SMS message with statuses of inputs IN. E.g.: ***ASKI 123456***
ASKO		Send SMS message with statuses of outputs OUT. E.g.: ***ASKO 123456***
ASKA		Send SMS message with statuses of areas. E.g.: ***ASKA 123456***
ASKT		Send SMS message with values of all temperature sensors. E.g.: ***ASKT 123456***
DISARM	*SYS:x*	Disarm the alarm, “x” is the partition number (1-8). E.g.: ***DISARM 123456 SYS:1***
ARM	*SYS:x*	Arm the alarm, “x” is the partition number (1-8). E.g.: ***ARM 123456 SYS:1***
STAY	*SYS:x*	Arm area “x” in Stay mode, “x” is the partition number (1-8). E.g.: ***STAY 123456 SYS:1***
SLEEP	*SYS:x*	Arm area “x” in Sleep mode, “x” is the partition number (1-8). E.g.: ***SLEEP 123456 SYS:1***
FRS		Resets the fire sensor’s output, if the output OUT is assigned the function “Fire sensor reset”. E.g.: ***FRS 123456***
SETN	*PhoneX=PhoneNR#Name#email*	Add a phone number, username and assign it to user “x”. “x” is the phone number’s line on the list. The phone number must start with a "+" symbol and international country code. The phone number and username must be separated by a # symbol. E.g.: ***SETN 123456 PHONE5=+37061234567#JOHN#john@peter.com***
	PhoneX=DEL	Delete phone number and username from the list. E.g.: ***SETN 123456 PHONE5=DEL***
UUSD	**Uusd code#*	Sends a UUSD code to the operator. E.g.: ***UUSD 123456 *245#***

Command	Data	Description
CONNECT	*Protegus=ON*	Connect to Protegus cloud service. E.g.: ***CONNECT 123456 PROTEGUS=ON***
	Protegus=OFF	Disconnect from Protegus cloud service. E.g.: ***CONNECT 123456 PROTEGUS=OFF***
	Code=123456	Protegus cloud service code. E.g.: ***CONNECT 123456 CODE=123456***
	IP=0.0.0.0:8000	Specify the main server's connection channel's TCP IP and Port. E.g.: ***CONNECT 123456 IP=0.0.0.0:8000***
	IP=0	For turning off the main channel. E.g.: ***CONNECT 123456 IP=0***
	ENC=123456	TRK encryption key. E.g.: ***CONNECT 123456 ENC=123456***
	APN=Internet	APN name. E.g.: ***CONNECT 123456 APN=INTERNET***
	USER=user	APN user. E.g.: ***CONNECT 123456 USER=User***
	PSW=password	APN passwod. E.g.: ***CONNECT 123456 PSW=Password***

4.4 Control via phone call

Note: The system administrator can control the ***„FLEXi“ SP3*** by SMS messages and phone calls.

If you want to allow others to control the system using phone calls, enter their identification data using ***TrikdisConfig*** software or SMS commands.

Control via phone call does not work with control panels *SP3_xx7x*. Control panel *SP3_12xx* does not have a voice message with firmware 1.14 and higher.

„FLEXi“ SP3 phone call control commands

Controlling outputs OUT and alarm system partitions using phone calls:

1. If the user is assigned the right to control outputs OUT and the output OUT is assigned the type "Remote control" (using ***TrikdisConfig***), or the security system ***„FLEXi“ SP3*** is partitioned into 1 or more areas: call the phone number of the ***„FLEXi“ SP3***'s SIM card**.** The ***„FLEXi“ SP3*** will answer the call and you can dial commands using the phone's numeric keypad (see table below).

Mobile phone keypad command list

Keypad buttons	Function	Description
[1][area no][#]	Arm selected alarm system area	E.g. (arm area 2): ***12#***
[2][area no][#]	Disarm selected alarm system area	E.g. (disarm area 2): ***22#***
[3][output no][#][stay no]	Control selected output OUT	Controls a specified output OUT. State: *[0]* – output turned off; *[1]* – output turned on; *[2]* – turned off for pulse time; *[3]* – turned on for pulse time; (pulse time is specified using ***TrikdisConfig*** software, in the "PGM" window) E.g. (set output 1OUT to "on" state): ***31#1*** E.g. (set output 2OUT to "on" state for **Pulse time** specified in the ***TrikdisConfig*** "PGM" table): ***32#3***
[4][#][recording number][#]	Start recording of selected sound file	E.g. (start voice recording 1): ***4#1#***
[5]	Listen (1-5) to the voice recording just made	E.g.: ***5***

Keypad buttons	Function	Description
[6]	Save the voice recording	E.g.: ***6***

An audio signal accompanies the beginning and end of the audio file recording. Audio file recording time 15 sec. An audio signal accompanies the end of audio playback. Recording is complete when you hear a beep. Other actions can only be taken when the beep is heard.

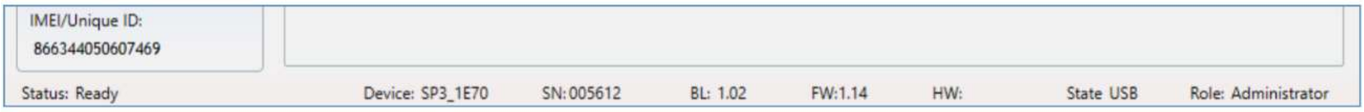
5 Setting parameters using TrikdisConfig software

1. Download the configuration software ***TrikdisConfig*** from www.trikdis.com/ (enter “TrikdisConfig” in the search field) and install it.
2. Connect the ***„FLEXi“ SP3*** to a computer using a USB Mini-B cable.

   Note: If you connect the ***„FLEXi“ SP3*** to a computer using a USB cable while it is powered on and operating, the ***„FLEXi“ SP3*** will stop performing its control panel functions and will switch to programming mode.
3. Launch the configuration software ***TrikdisConfig***. The program will automatically recognize the connected device and will automatically open the ***„FLEXi“ SP3*** configuration window.
4. Click **Read [F4]** to see current ***„FLEXi“ SP3*** parameters. If a pop-up window appears, enter the *administrator* or *installer* code.

5.1 Description of TrikdisConfig status bar

When the ***„FLEXI“ SP3*** is connected, ***TrikdisConfig*** will show information about the connected device in the status bar.



IMEI/Unique ID: 866344050607469

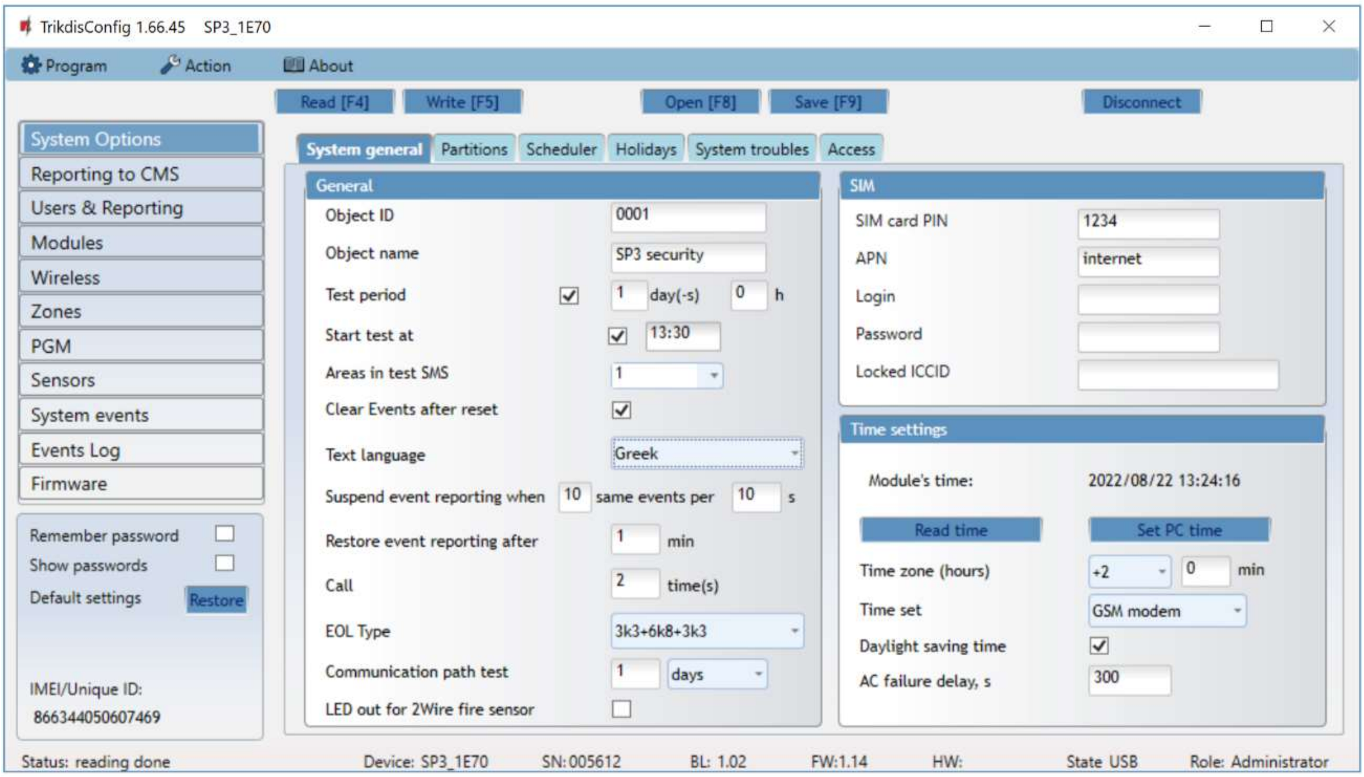
Status: Ready Device: SP3_1E70 SN: 005612 BL: 1.02 FW:1.14 HW: State USB Role: Administrator

Name	Description
IMEI/Unique ID	IMEI number of the device
Status	Operational status
Device	Device type (must show ***SP3_xxxx***)
SN	Device serial number
BL	Bootloader version
FW	Device firmware version
HW	Device hardware version
State	Type of connection with the program (USB or remote)
Role	Shows the access level (shown after entering an access code)

When the **Read [F4]** button is clicked, the program will read and display the settings currently stored inside the ***„FLEXi“ SP3***. With ***TrikdisConfig***, alter the desired settings according to the program window descriptions given below.

5.2 “System Options” window

“System general” tab



General

- Object ID: 0001
- Object name: SP3 security
- Test period: ☑ 1 day(-s) 0 h
- Start test at: ☑ 13:30
- Areas in test SMS: 1
- Clear Events after reset: ☑
- Text language: Greek
- Suspend event reporting when 10 same events per 10 s
- Restore event reporting after 1 min
- Call 2 time(s)
- EOL Type: 3k3+6k8+3k3
- Communication path test: 1 days
- LED out for 2Wire fire sensor: □

SIM

- SIM card PIN: 1234
- APN: internet
- Login:
- Password:
- Locked ICCID:

Time settings

- Module's time: 2022/08/22 13:24:16
- Time zone (hours): +2 0 min
- Time set: GSM modem
- Daylight saving time: ☑
- AC failure delay, s: 300

- Remember password □
- Show passwords □
- Default settings

IMEI/Unique ID: 866344050607469

Status: reading done Device: SP3_1E70 SN: 005612 BL: 1.02 FW:1.14 HW: State USB Role: Administrator

Settings group “General”

- If reports will be sent to CMS, enter the **Object ID** (4 symbol hexadecimal number, 0-9, A-F. **Do not use FFFE, FFFF Object ID.**) given by the CMS.
- **Object name** – will be included in reports sent via SMS messages (up to 20 symbols, letters and numbers can be used).
- **Test period** – if the box is ticked, periodic test reports will be sent every set period, unless **Start test at** is ticked and a time is set.
- **Start test at** – tick the box and specify a time when test reports should be sent.
- **Areas in test SMS** – the current protection modes of the specified areas will be included into the periodic test report.
- **Clear Events after reset** – if the box is ticked, all unsent event reports in buffer memory will be deleted if the control panel is reset.
- **Text language** – specific symbols of the selected language will be used in SMS messages.
- It is possible to **Suspend event reporting when ...** a number of **same events per ... s** happen**.**
- **Restore event reporting after** – set the time after which suspending of event reporting will be cancelled. The time can be anywhere from 0 to 999 minutes.
- **Call** – when an event occurs, the ***„FLEXi“ SP3*** will call user(-s) as many times as is set. If the call is declined or answered, the ***„FLEXi“ SP3*** will stop calling. Duration of a call is 20 seconds.
- **EOL Type** – specify the nominals of the resistors connected to the sensors (EOL – End Of Line. RT + R1 + R2. Resistor RT - tamper; resistor R1 - sensor No 1; resistor R2 - sensor No 2).
- **Communication path test** – specify the time interval after which the control panel will check the Backup communication channels by sending messages to the CMS. After sending the messages on the Backup communication channels, the control panel will return to the Primary communication channel.
- **LED out as 2Wire fire** - check the box when you connect the two-wire fire detector to the LED output.

Settings group “SIM”

- Enter the **SIM card PIN.** If the PIN code is disabled for the specific SIM card, do not change the the default code.
- **APN** – network service provider’s mobile internet access point name. You must enter the APN if event messages will have to be sent to ***Protegus*** cloud or to the CMS using mobile internet.

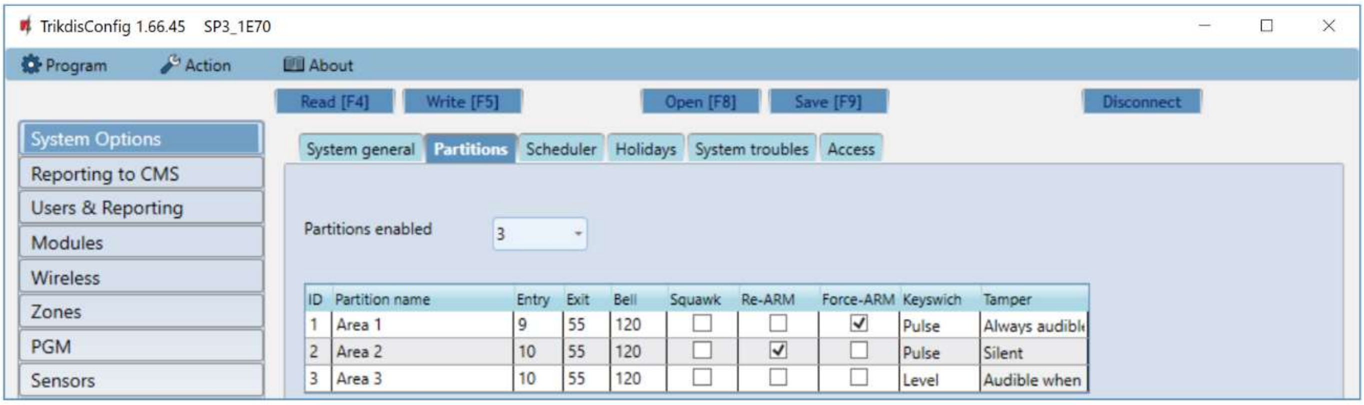
- If required by the GPRS network service provider, enter the APN username and password in the fields **Login** and **Password**.
- **Locked ICCID** - enter the ICCID number of the SIM card if you want the control panel to work only with this SIM card.

Settings group “Time settings”

You can set the time by clicking the **Set PC time** button. If **Disabled** is chosen in the **Time synchronization** field, the computer’s time will be set for the control panel. If a modem or a server is chosen in the **Time synchronization** field, the control panel will synchronize its time according to that modem or server.

- **Time zone (Hours)** – specify your country’s time zone. For example, if the control panel will be installed in Lithuania, enter **+3**.
- **Time set** – specify a server to synchronize the ***„FLEXi“ SP3****’s* internal clock with. Synchronization occurs after the control panel is powered on.
- **Daylight saving time** – if you check the box, the control panel's internal clock will be automatically switched to summer or winter time.
- **AC failure delay** - in the event of a power failure in the main power supply, a power failure notification will be sent after the specified time delay. When the supply voltage is restored, a notification of the supply voltage recovery will be sent after the specified time delay.

“Partitions” tab

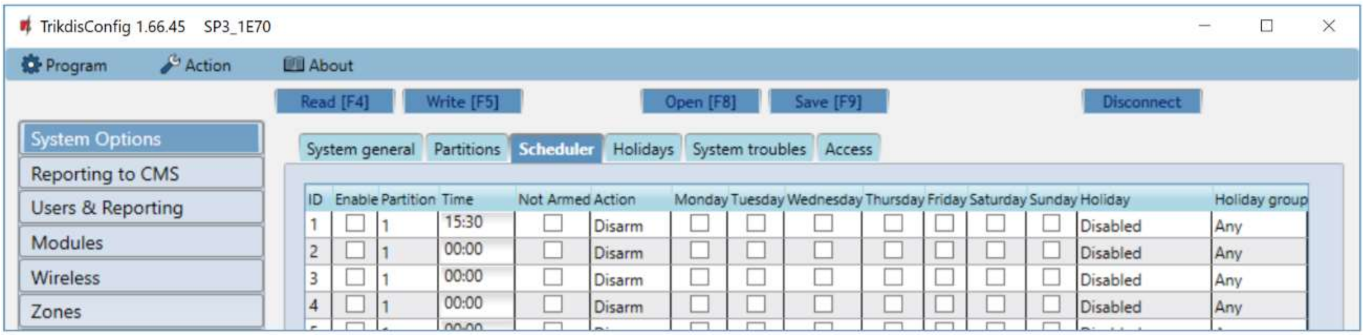


Partitions enabled 3

ID	Partition name	Entry	Exit	Bell	Squawk	Re-ARM	Force-ARM	Keyswich	Tamper
1	Area 1	9	55	120	□	□	☑	Pulse	Always audibl
2	Area 2	10	55	120	□	☑	□	Pulse	Silent
3	Area 3	10	55	120	□	□	□	Level	Audible when

- **Partitions enabled** – enter the number of independent parts that the alarm system will be divided into.
- **Partition name** – enter the partition name.
- **Entry** – time for entering through a *Delay* zone, walking to a keypad and disarming the alarm system. Time can be anywhere between 0 and 999 seconds.
- **Exit** – time for leaving the premises through a *Delay* zone after entering the alarm system arm code using a keypad. Time can be anywhere between 0 and 999 seconds. If the alarm system is armed remotely, e.g. via ***Protegus*** mobile app, the system will not count **Exit time** and will arm immediately.
- **Bell** – duration of siren operation once the alarm is triggered. Time can be anywhere between 0 and 999 seconds.
- **Squawk** - the siren will make a short sound once when the alarm is armed and twice when it is disarmed.
- **Re-ARM** – tick this box if you want the system to automatically re-arm the alarm system after the system was disarmed remotely, but the *Delay* zone was not violated during the set entry time.
- **Force-ARM** – tick this box to allow to switch the system to protection (ARM) mode even if *Stay* zones are violated, as long as the *Entry* zone is not violated.
- **Keyswitch** – choose in what way – *Pulse* or *Level* – a Keyswitch zone must be triggered for the system to enable or disable premise protection.
- **Tamper** – choose the reaction type (Silent, Audible when armed, Always Audible) when the system detects a sensor tamper event. “Silent” – recipients will receive event reports, but the siren will not switch on; „Audible when protected“ - recipients will receive event reports, but the siren will switch on only if the tamper event happens when the system is armed; „Always audible“ - recipients will receive event reports and the siren will will switch on even when the alarm system is disarmed.

“Scheduler” tab

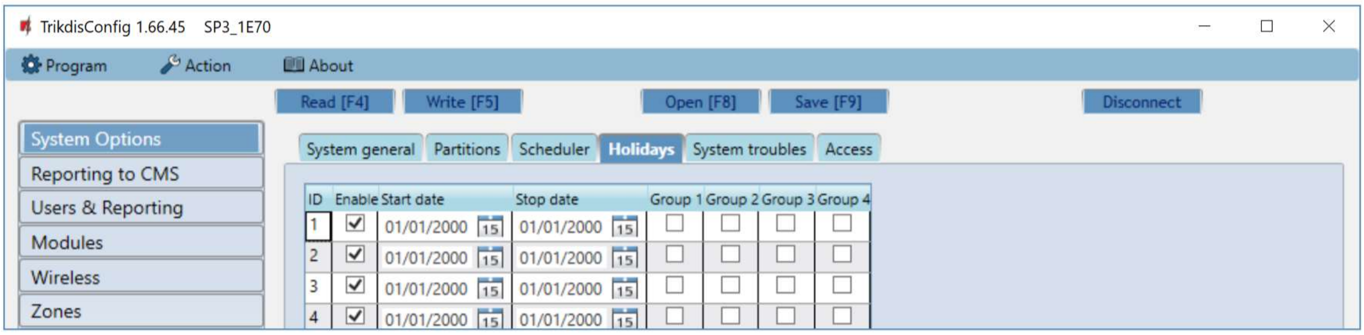


ID	Enable	Partition	Time	Not Armed	Action	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Holiday	Holiday group
1	□	1	15:30	□	Disarm	□	□	□	□	□	□	□	Disabled	Any
2	□	1	00:00	□	Disarm	□	□	□	□	□	□	□	Disabled	Any
3	□	1	00:00	□	Disarm	□	□	□	□	□	□	□	Disabled	Any
4	□	1	00:00	□	Disarm	□	□	□	□	□	□	□	Disabled	Any

In this table, you can arrange scenarios for automatically arming and disarming the security system by choosing different days of the week and including public holidays.

- **Enable** – enable the schedule for when the system will automatically arm and disarm.
- **Partition** – specify the partition affected by the specific schedule.
- **Time** – set the time when the specific action must be done.
- **Not Armed** - check the box and the schedule action will be performed only if the control panel is not armed in AWAY mode.
- **Action** – set the protection mode (Disarm/Arm/Sleep/Stay) that the system will switch to automatically at the specified time.
- **Monday, ... Sunday** – tick the days of the week that the set protection mode and time will be valid on.
- **Holiday** – set how the schedule behaves during holidays (Disabled/Ignore on holidays/Additional when holidays/Only holidays). Disabled – there are no holidays. Ignore on holidays – do not carry out the schedule during holidays. Additional when holidays – perform an additional action during holidays. Only holidays – carry out the schedule during holidays.
- **Holiday group** – specify a holiday group (Any/1/2/3/4) that the schedule will consider to be holidays. If “Any” is chosen, the schedule will operate in holiday mode during any active holiday.

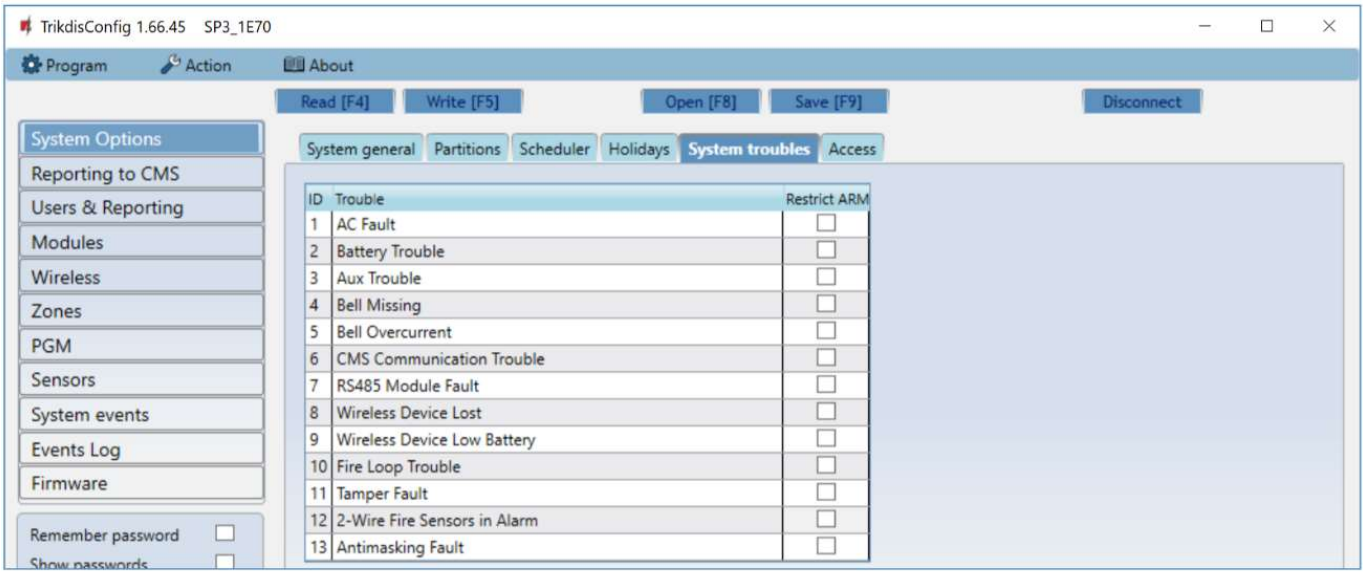
“Holidays” tab



ID	Enable	Start date	Stop date	Group 1	Group 2	Group 3	Group 4
1	☑	01/01/2000	01/01/2000	□	□	□	□
2	☑	01/01/2000	01/01/2000	□	□	□	□
3	☑	01/01/2000	01/01/2000	□	□	□	□
4	☑	01/01/2000	01/01/2000	□	□	□	□

- **Enable** – Tick this box to enable the holiday.
- **Start date** – set the start date of the holiday.
- **Stop date** – set the end date of the holiday. If the holiday is only one day long, this date should match the **Start date**.
- **Group 1, Group 2, Group 3, Group 4** – combine holidays into groups.

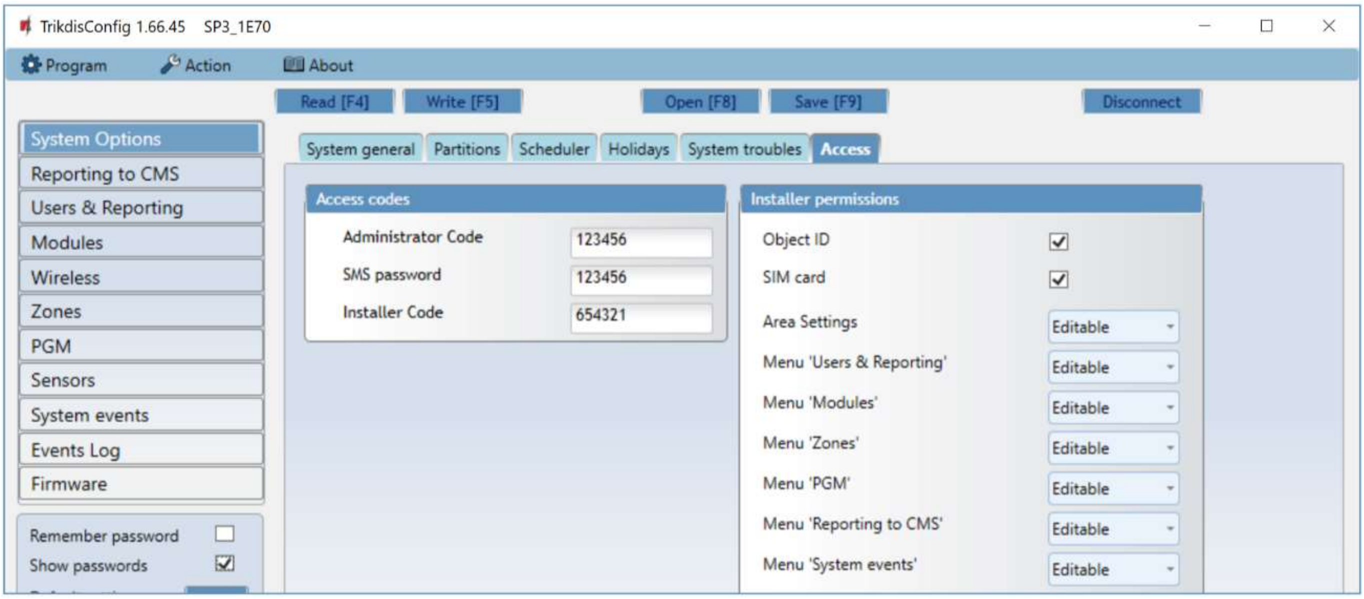
“System troubles” tab



ID	Trouble	Restrict ARM
1	AC Fault	□
2	Battery Trouble	□
3	Aux Trouble	□
4	Bell Missing	□
5	Bell Overcurrent	□
6	CMS Communication Trouble	□
7	RS485 Module Fault	□
8	Wireless Device Lost	□
9	Wireless Device Low Battery	□
10	Fire Loop Trouble	□
11	Tamper Fault	□
12	2-Wire Fire Sensors in Alarm	□
13	Antimasking Fault	□

If at least one control panel internal fault field is checked, then the control panel will not be able to be Armed if this fault is present.

“Access” tab



Access codes

Administrator Code	123456
SMS password	123456
Installer Code	654321

Installer permissions

Object ID	☑
SIM card	☑
Area Settings	Editable
Menu 'Users & Reporting'	Editable
Menu 'Modules'	Editable
Menu 'Zones'	Editable
Menu 'PGM'	Editable
Menu 'Reporting to CMS'	Editable
Menu 'System events'	Editable

Settings group “Access codes”

- **Administrator Code** – *(default code - 123456)* gives full access to configuration (the code must be 6 symbols long; it can consist of latin letters and/or numbers).
- **SMS password** – *(default password - 123456)* is used for controlling the system safely using SMS messages. For safety purposes, change it into a 6-symbol password only You know.
- **Installer Code** – (*default code - 654321*) gives installers access to configuring the system. For safety purposes, change it into a 6-symbol code only You know.

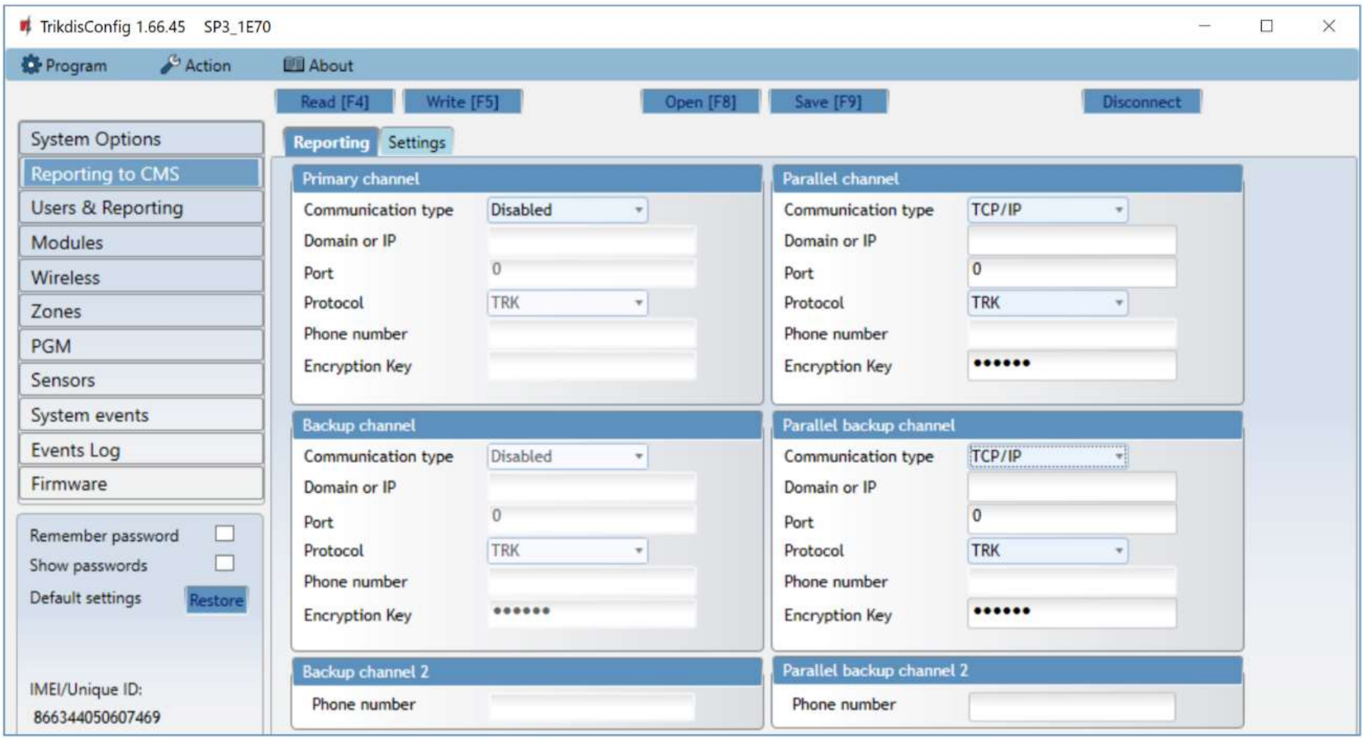
Note:	If the default *administrator code* is set (123456), after pressing **Read [F4]** the program will immediately show the current operational parameters of the device without asking for the code.

Settings group “Installer permissions”

- Specifies the installer’s permissions.

5.3 "Reporting to CMS" window

"Reporting" tab



Remember password □

Show passwords □

Default settings

IMEI/Unique ID: 866344050607469

Primary channel

Communication type	Disabled
Domain or IP	
Port	0
Protocol	TRK
Phone number	
Encryption Key	

Parallel channel

Communication type	TCP/IP
Domain or IP	
Port	0
Protocol	TRK
Phone number	
Encryption Key	••••••

Backup channel

Communication type	Disabled
Domain or IP	
Port	0
Protocol	TRK
Phone number	
Encryption Key	••••••

Parallel backup channel

Communication type	TCP/IP
Domain or IP	
Port	0
Protocol	TRK
Phone number	
Encryption Key	••••••

Backup channel 2

Phone number	

Parallel backup channel 2

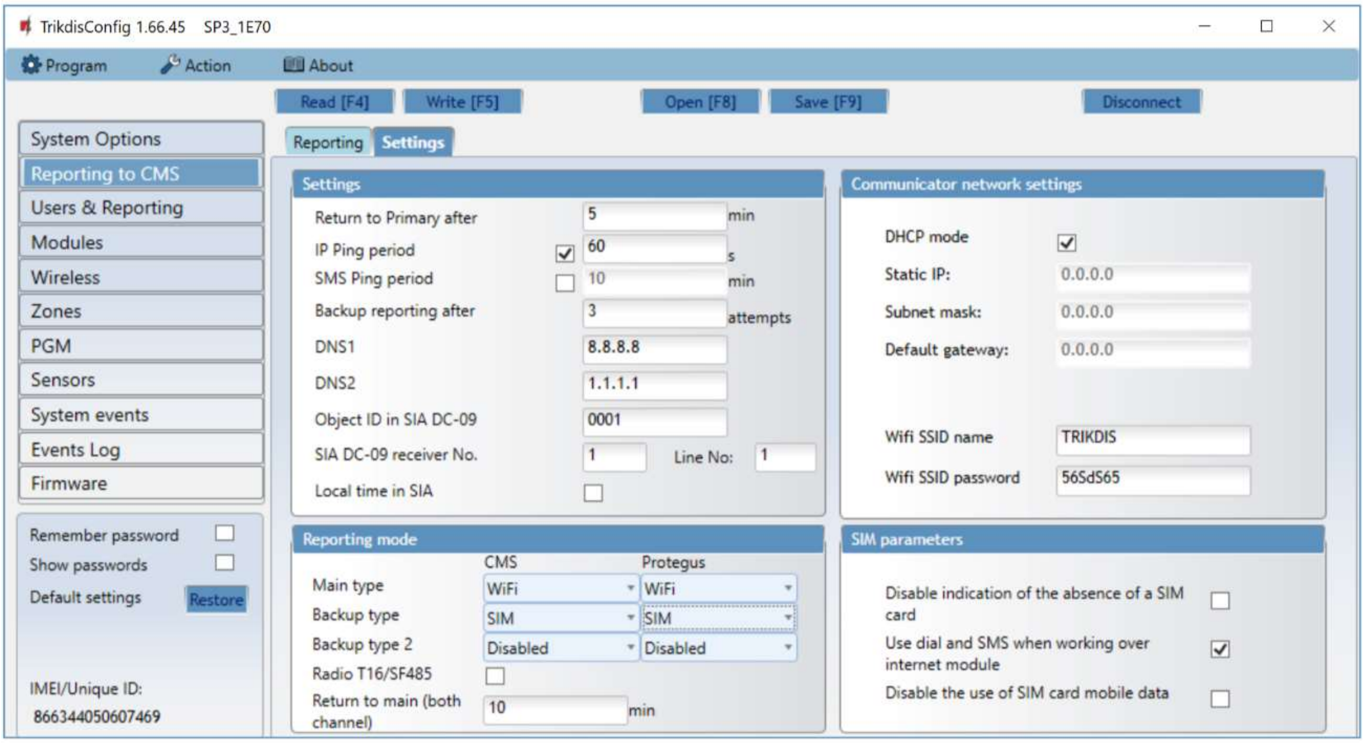
Phone number	

Settings groups "Primary channel" and "Backup channel"

- **Communication type** – choose a protocol for communicating with the receiver (TCP/IP, UDP/IP, SMS).
- **Domain or IP** - enter the receiver's domain or IP address.
- **Port** – enter the receiver's network port number.
- **Protocol** – **TRK** for data transfer using Trikdis receivers, **SIA DC-09** for IP receivers capable of receiving event reports transmitted in SIA DC-09 protocols.
- **Phone number** – (only for SMS messages) enter the phone number of a TRIKDIS SMS receiver. The telephone number must start with the international country code (e.g. 370xxxxxxxx).
- **Encryption key** – 6-digit encryption key that must match the encryption key of the CMS receiver.

If parameters are set for the parallel channel, reports will be sent using both channels simultaneously. Both channels cannot be configured for the same receiver.

“Settings” tab



Remember password □
Show passwords □
Default settings Restore
IMEI/Unique ID: 866344050607469

Settings

Return to Primary after		5	min
IP Ping period	☑	60	s
SMS Ping period	□	10	min
Backup reporting after		3	attempts
DNS1		8.8.8.8	
DNS2		1.1.1.1	
Object ID in SIA DC-09		0001	
SIA DC-09 receiver No.		1	Line No: 1
Local time in SIA		□	

Communicator network settings

DHCP mode	☑
Static IP:	0.0.0.0
Subnet mask:	0.0.0.0
Default gateway:	0.0.0.0
Wifi SSID name	TRIKDIS
Wifi SSID password	56SdS65

Reporting mode

	CMS	Protegus
Main type	WiFi	WiFi
Backup type	SIM	SIM
Backup type 2	Disabled	Disabled
Radio T16/SF485	□	
Return to main (both channel)	10 min	

SIM parameters

Disable indication of the absence of a SIM card	□
Use dial and SMS when working over internet module	☑
Disable the use of SIM card mobile data	□

Settings group “Settings”

- **Return to primary after** – time period after which the ***„FLEXi“ SP3*** will attempt to regain connection using the *primary* channel, in minutes.
- **IP Ping period** – period for sending PING signals for checking connectivity on the GPRS channel, in seconds. To enable these signals, tick the box.
- **SMS PING period** – period for sending PING signals for checking connectivity on the SMS channel, in minutes. To enable these signals, tick the box.
- **Backup reporting after** – enter how many failed attempts to send messages using the *primary* channel should take place before switching to the *backup* channel.
- **DNS1, DNS2** – DNS server addresses.
- **Object ID in SIA DC-09** –specify the object number.
- **SIA DC-09 receiver No.** – specify the receiver number.
- **SIA DC-09 line No.** – specify the line number.
- **Local time in SIA** - check the box so that the messages sent to the CMS (central monitoring station) will indicate the time set in the module.

IMPORTANT: Regardless of IP settings, make sure the DNS addresses match those supported by your ISP.

Settings group “Reporting mode”

For setting parameters on how the control panel will communicate with the CMS channels and with Protegus. The connection types are specified in order. If the control panel fails to connect using the **Main type** connection , it switches to the **Backup type**, and so on. If the backup connection type was successful in transmitting the message to the CMS, then the **Return to main** connection type will be attempted after the specified time interval.

- **Main type** – select a connection type (SIM, WiFi, LAN(E485)) with the CMS receiver and ***Protegus***.
- **Backup type** – select a connection type (SIM, WiFi, LAN(E485)) with the CMS receiver and ***Protegus***.
- **Backup type 2** – select a connection type (SIM, WiFi, LAN(E485)) with the CMS receiver and ***Protegus***.
- **Radio T16 (SF485)** – tick this box, when the ***T16*** transmitter will be used for transmitting information. The ***T16*** transmitter operates as a backup connectivity channel if at least one of the other connection methods (SIM, WiFi, LAN(E485)) is used. If there are no other connection methods, it is the main one. The ***T16*** can only be used to send reports to the CMS.

- **Return to main (both channel)** – time period after which the ***„FLEXi“ SP3*** will attempt to regain connection using the *primary* channel, if it was running a backup channel, min.

Settings group “Communicator network settings”

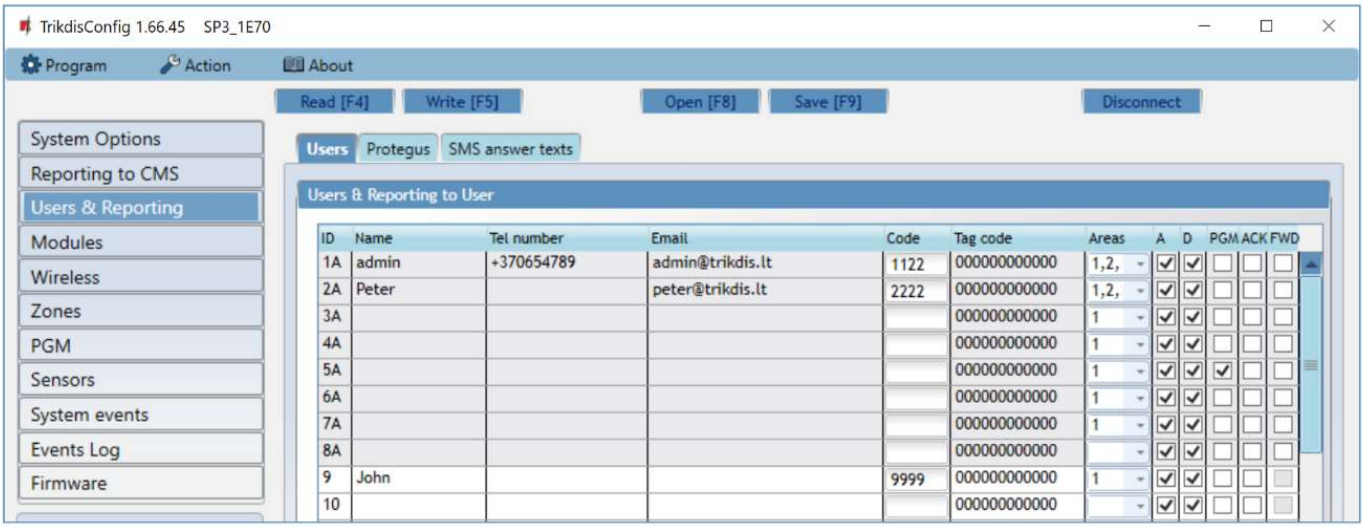
- **DHCP mode** – mode for registering on the WiFi network (manual or automatic). Tick the box and the ***„FLEXi“ SP3*** control panel will automatically read the network settings (subnet mask, gateway) and will automatically be assigned an IP address (automatic registration mode).
- **Static IP** – static IP address for manual registration mode.
- **Subnet mask** – subnet mask for manual registration mode.
- **Default gateway** – gateway for manual registration mode.
- **WiFi SSID name** – name of the WiFi network (that the ***„FLEXi“ SP3*** control panel will connect to).
- **WiFi SSID password** – WiFi network password.

Settings group “SIM parameters”

- **Disable indication of the absence of a SIM card** – when the box is ticked, the ***„FLEXi“ SP3*** control panel will not display an indication that there is no SIM card inserted.
- **Use dial and SMS when the working over internet module** – ticking this box will enable controlling the panel using phone calls and SMS messages. If the box is not ticked and there is a WiFi network available, then SMS and phone calls are not used. If the box is not ticked and there is no WiFi network, the ***„FLEXi“ SP3*** can still be controlled using phone calls and SMS messages. The ***„FLEXi“ SP3*** will send SMS messages to the user.
- **Disable the use of SIM card mobile data** – ticking the box will disable the usage of the SIM card’s mobile data. Data will only be sent using WiFi. If a WiFi network is temporarily unavailable, the ***„FLEXi“ SP3*** will store data in memory. When the WiFi network is restored, the ***„FLEXi“ SP3*** will send data using WiFi.

5.4 “Users & Reporting” window

“Users” tab



Users & Reporting to User

ID	Name	Tel number	Email	Code	Tag code	Areas	A	D	PGM	ACK	FWD
1A	admin	+370654789	admin@trikdis.lt	1122	000000000000	1,2,	☑	☑	☐	☐	☐
2A	Peter		peter@trikdis.lt	2222	000000000000	1,2,	☑	☑	☐	☐	☐
3A					000000000000	1	☑	☑	☐	☐	☐
4A					000000000000	1	☑	☑	☐	☐	☐
5A					000000000000	1	☑	☑	☑	☐	☐
6A					000000000000	1	☑	☑	☐	☐	☐
7A					000000000000	1	☑	☑	☐	☐	☐
8A					000000000000		☑	☑	☐	☐	☐
9	John			9999	000000000000	1	☑	☑	☐	☐	☐
10					000000000000		☑	☑	☐	☐	☐

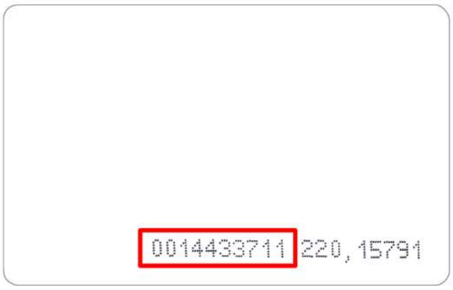
Settings group “Users & Reporting to User”

- **Name** – name of the user. These names will be used in event SMS messages.
- **Tel number** – the user’s telephone number that will be used to control the alarm system remotely and will receive SMS messages. The numbers must start with the international country code. The first 8 telephone numbers will receive reports using messages and phone calls.
- **Email** – enter the user’s email, so that the user would be invited to ***Protegus*** to control the system.
- **Code** – the alarm system arm and disarm code assigned to the user.
- **Tag code** – enter the identification number of an RFID card, RFID key fob, or iButton electronic key.
- **Areas** – the areas that the specific user can control.
- **A** – tick the box if you want to allow the user to ARM the alarm.
- **D** – tick the box if you want to allow the user to DISARM the alarm.

- **PGM** – if the box is ticked, the user can call the ***„FLEXi“ SP3*** and turn on or off desired outputs OUT using DTMF tones.
- **ACK** – if the box Is ticked, the ***„FLEXi“ SP3*** will send the user SMS messages with **SMS answer text** about the completion of received commands.
- **FWD** – if the box is ticked, SMS messages received from non-users of the system (e.g. SIM card account balance, random promotional messages, etc.) will be forwarded to the user.

5.4.1 Linking RFID key fobs (cards)

You can add RFID key fobs (cards) by entering their ID numbers into the **Tag code** field in ***TrikdisConfig***. Click the **Write [F5]** button to write the RFID key fob (card) list into the control panel.



The ID number specified on an RFID card.

5.4.2 Linking electronic (iButton) keys

Linking electronic keys using the ***TM17*** reader.

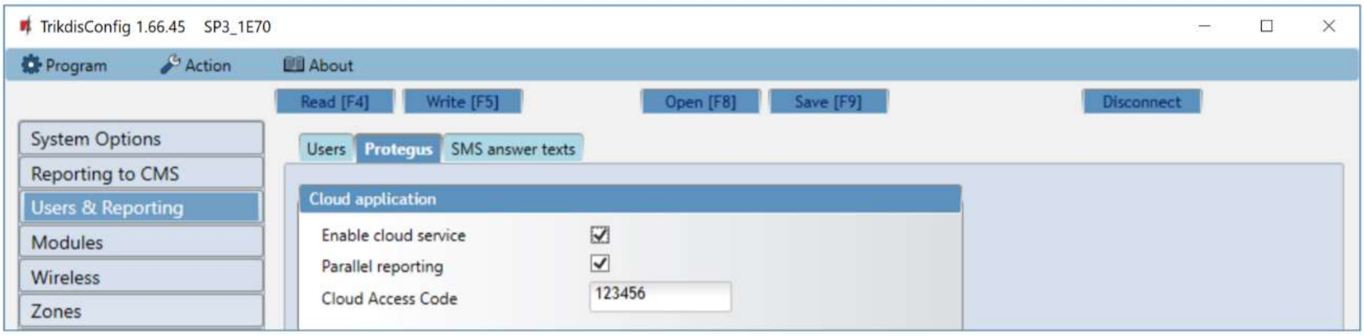
1. If the **Tag code** list is empty, the first added key should be written to the first line of the list and becomes the **Master key.**
2. To turn on contact key linking mode, hold the **Master key** against the “eye” of the key reader for at least 10 seconds. When linking mode is on, the ***TM17*** key reader’s LED indicator *State* will start to blink in green.
3. To link user keys, hold them against the “eye” of the key reader one by one. 3 sound signals from the reader will indicate that the key has been linked to the system.
4. When you finish linking the user electronic (*iButton*) keys, hold the **Master key** against the key reader again to disable linking mode. When the linking mode is turned off, the *State* LED indicator of the ***TM17*** key reader will stop blinking.
5. To delete all keys (including the master key), hold the **Master key** against the reader for at least 20 seconds.

Linking electronic keys using the ***CZ-Dallas*** reader.

1. If the **Tag code** list is empty, the first added key should be written to the first line of the list and becomes the **Master key.**
2. To turn on contact key linking mode, hold the **Master key** against the “eye” of the key reader for at least 10 seconds.
3. To link user keys, hold them against the „eye” of the key reader one by one.
4. When you finish linking the user electronic (*iButton*) keys, hold the **Master key** against the key reader again to disable linking mode.
5. To delete all keys (including the master key), hold the **Master key** against the reader for at least 20 seconds.

Important: The purpose of the Master key is to link other electronic keys. If you use the Master key for ARM/DISARM commands, their execution will have a delay.

“Protegus” tab



Cloud application

Enable cloud service ☑

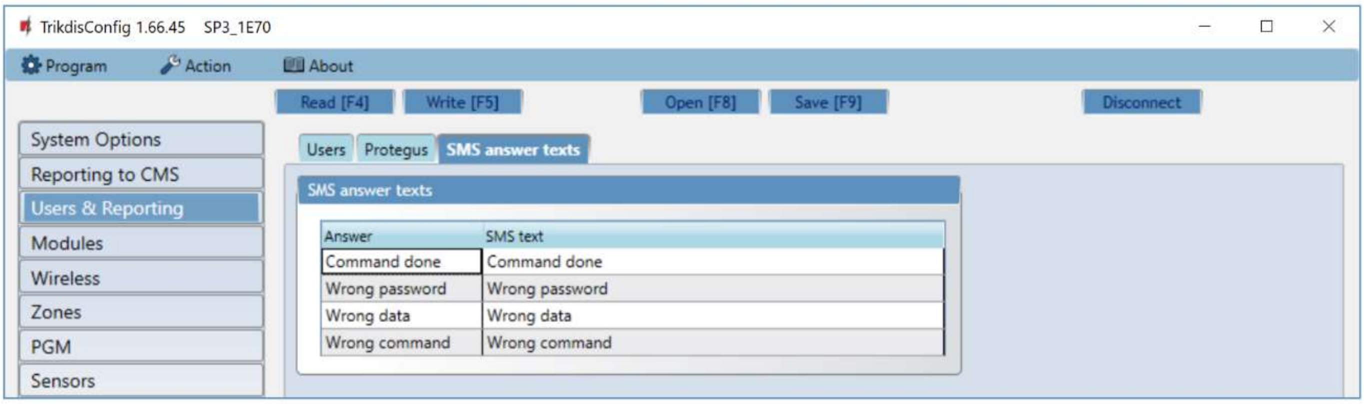
Parallel reporting ☑

Cloud Access Code 123456

Settings group “Cloud application”

- **Enable cloud service** – enable ***Protegus cloud*** service, the ***„FLEXi“ SP3*** will be able to exchange data with ***Protegus*** app and it will be possible to configure the control panel remotely using ***TrikdisConfig***.
- **Parallel reporting** – allow parallel report sending using the *primary channel* and to ***Protegus***. Reports will only be sent to ***Protegus*** and to users after they’ve been sent to the security company.
- **Cloud access code** – 6-digit code for connecting with ***Protegus***.

“SMS answer texts” tab



SMS answer texts

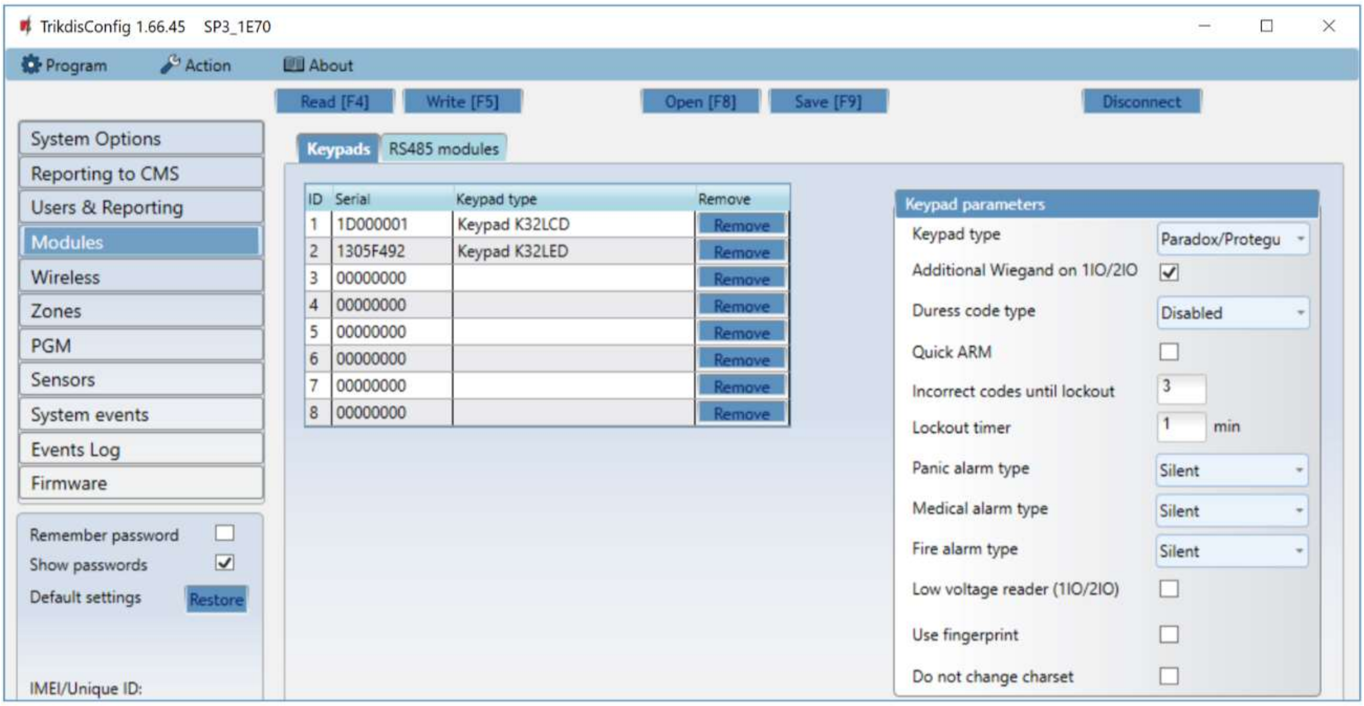
Answer	SMS text
Command done	Command done
Wrong password	Wrong password
Wrong data	Wrong data
Wrong command	Wrong command

Settings group “SMS answer texts”

- The text for answers to commands sent using SMS messages can be customized in the column **SMS text**.

5.5 “Modules” window

“Keypads” tab



Remember password □
Show passwords ☑
Default settings Restore

ID	Serial	Keypad type	Remove
1	1D000001	Keypad K32LCD	Remove
2	1305F492	Keypad K32LED	Remove
3	00000000		Remove
4	00000000		Remove
5	00000000		Remove
6	00000000		Remove
7	00000000		Remove
8	00000000		Remove

Keypad parameters

Keypad type	Paradox/Protegu
Additional Wiegand on 1IO/2IO	☑
Duress code type	Disabled
Quick ARM	□
Incorrect codes until lockout	3
Lockout timer	1 min
Panic alarm type	Silent
Medical alarm type	Silent
Fire alarm type	Silent
Low voltage reader (1IO/2IO)	□
Use fingerprint	□
Do not change charset	□

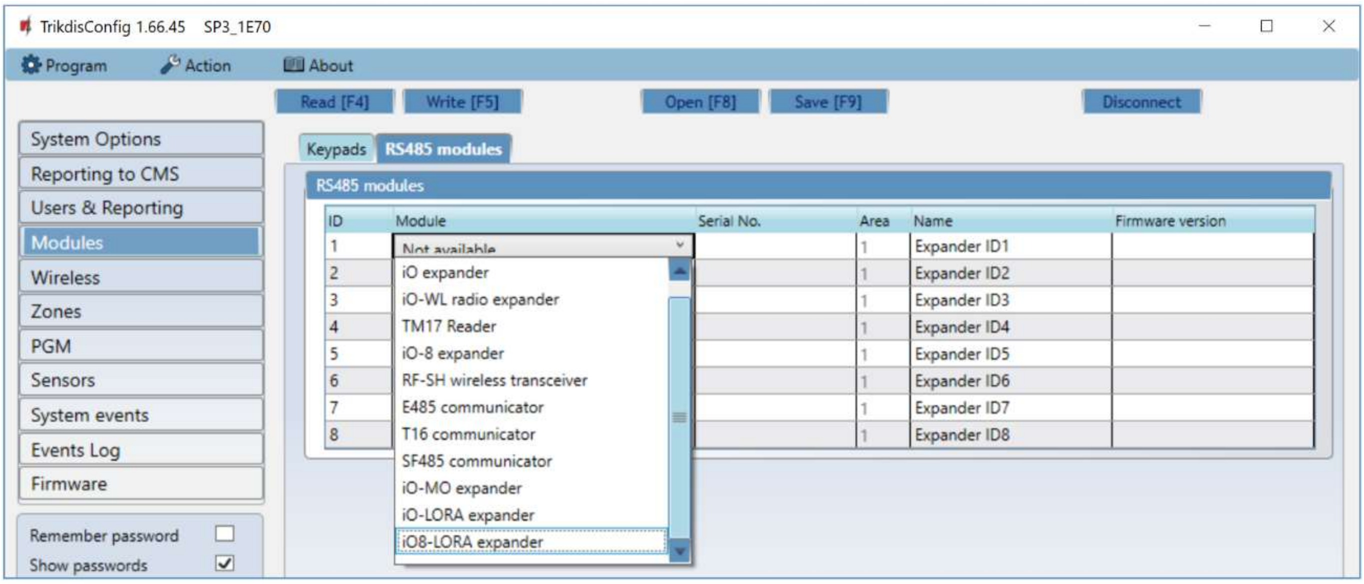
- **Serial** – the keypad’s serial number automatically detected by the control panel. To delete a keypad, enter zeros or click on the **Remove** button.
- **Keypad type** – keypad type, automatically detected by the control panel.
- **Remove** – pressing the button will remove the keypad from the list.

Settings group “Keypad parameters”

- **Keypad type** – specify the keypad type (Crow CR16, Paradox LED, Wiegand reader) connected to the control panel (GRN, YEL terminals).

- **Additional Wiegand on 1IO/2IO** – tick the box if an additional RFID card reader will be connected. An additional reader can be connected to the terminals IO1 and IO2, which cannot be used as inputs or outputs in this case.
- **Duress code type** – choose a duress code type. If you are forced to arm or disarm the alarm system and enter the duress code, the system will arm or disarm the system and will immediately send a silent warning to the CMS (central monitoring station).
- **Quick ARM** – the buttons ARM, STAY, SLEEP can be used to quickly arm the security system without entering a code.
- **Incorrect codes until lockout** – enter the number of incorrect codes allowed before blocking the keypad.
- **Lockout timer** – enter the time for how long the keypad will be blocked.
- **Panic alarm type** – specify what the alarm will sound (**Audible** / **Silent** / **Disabled**) if the **Panic alarm** function keys on the keypad are pressed. When an **Audible** alarm is set, alarm messages are sent to the ***Protegus*** and the CMS (central monitoring station) and the control panel will sound an audible alarm on the keypad and turn on the siren. When the **Silent** alarm is set, alarm messages are sent to the ***Protegus*** and the CMS, and the control panel will turn off the audible alarms. If set to Disabled, no alarm message is sent to ***Protegus*** and CMS.
- **Medical alarm type** – specify what the alarm will sound (**Audible** / **Silent** / **Disabled**) if the **Medical alarm** function keys on the keypad are pressed. When the **Audible** alarm is set, alarm messages are sent to the ***Protegus*** and the CMS, and the control panel will sound an audible alarm on the keypad and turn on the siren. When the **Silent** alarm is set, alarm messages are sent to the ***Protegus*** and the CMS, and the control panel will turn off the audible alarms. If set to **Disabled** alarm messages are not sent to ***Protegus*** and CMS.
- **Fire alarm type** - specify what the alarm will sound (**Audible** / **Silent** / **Disabled**) if the **Fire alarm** function keys on the keypad are pressed. When the **Audible** alarm is set, alarm messages are sent to the ***Protegus*** and the CMS, and the control panel will sound an audible alarm on the keypad and turn on the siren. When the **Silent** alarm is set, alarm messages are sent to the ***Protegus*** and the CMS, and the control panel will turn off the audible alarms. If set to **Disabled** alarm messages are not sent to ***Protegus*** and CMS.
- **Low voltage reader (1IO/2IO)** – check the box to change the communication protocol between the control panel and the reader if the connected RFID reader is not working.
- **Use fingerprint** – check the box if a fingerprint reader with Wiegand 26/34 protocol will be connected.
- **Do not change charset** - check the box if you do not want to change the text encoding of zone and partition names for the SK232LCD keypad.

“RS485 modules” tab



ID	Module	Serial No.	Area	Name	Firmware version
1	Not available		1	Expander ID1	
2			1	Expander ID2	
3			1	Expander ID3	
4			1	Expander ID4	
5			1	Expander ID5	
6			1	Expander ID6	
7			1	Expander ID7	
8			1	Expander ID8	

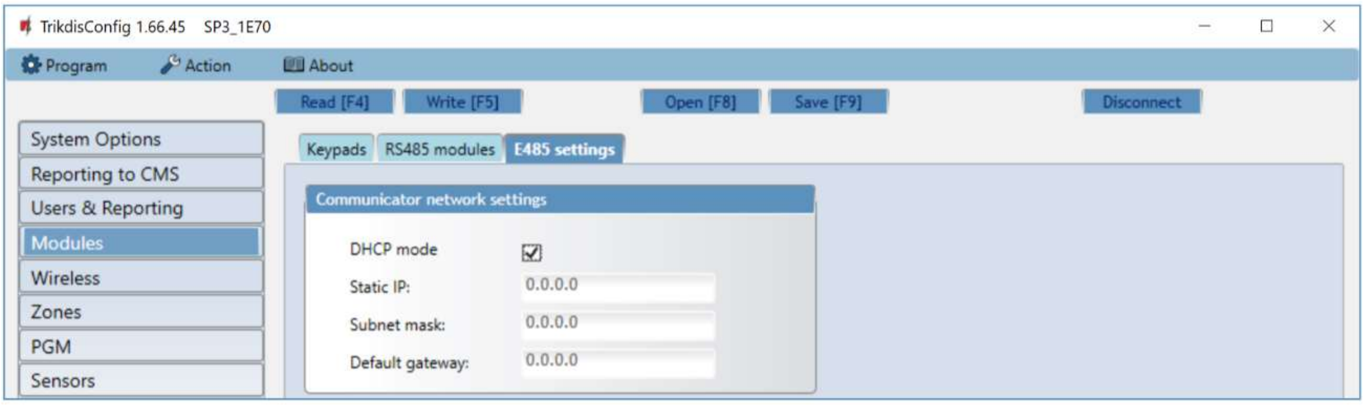
Remember password ☐
Show passwords ☑

Settings group “RS485 modules”

- **ID** – module’s number on the list.
- **Module** – choose the module being used (modules ***iO***, ***iO-WL***, ***TM17, iO-8, RF-SH, E485 T16, SF485, iO-MO, iO-LORA, iO8-LORA***) from the module list.
- **Serial No.** – mandatory 6-digit number that is given on stickers on the module’s casing and packaging.
- **Area** – assign the module to an area (the ***TM17*** will display the status of the area it is assigned to, and also the states of the zones assigned to the same area).

- **Name** – you can give the module a name.
- **Firmware version** – when the ***„FLEXi“ SP3*** finds the connected module, the version of its firmware will be shown.

“E485 settings” tab



DHCP mode ☑

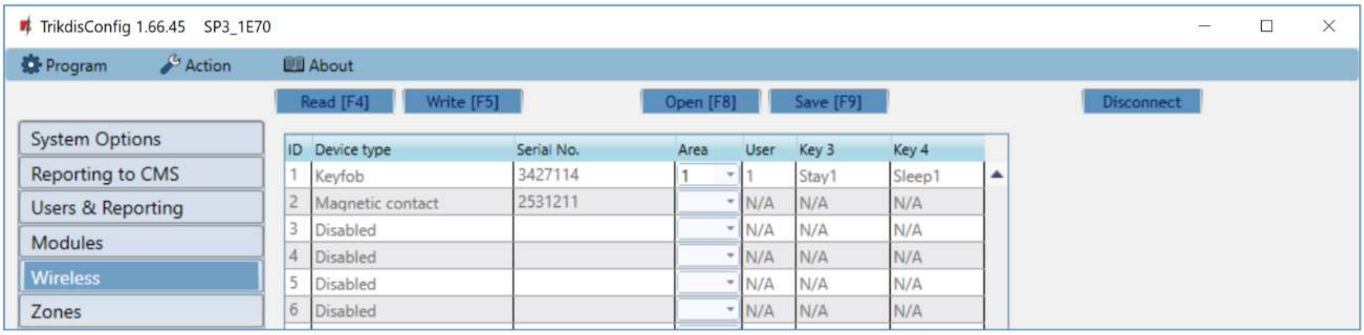
Static IP: 0.0.0.0

Subnet mask: 0.0.0.0

Default gateway: 0.0.0.0

- **DHCP mode** – mode for registering on the LAN network (manual or automatic). Tick the box and the ***„FLEXi“ SP3_3E*** control panel will automatically read the network settings (subnet mask, gateway) and will automatically be assigned an IP address (automatic registration mode).
- **Static IP** – static IP address for manual registration mode.
- **Subnet mask** – subnet mask for manual registration mode.
- **Default gateway** – gateway for manual registration mode.

5.6 “Wireless” window



ID	Device type	Serial No.	Area	User	Key 3	Key 4
1	Keyfob	3427114	1	1	Stay1	Sleep1
2	Magnetic contact	2531211		N/A	N/A	N/A
3	Disabled			N/A	N/A	N/A
4	Disabled			N/A	N/A	N/A
5	Disabled			N/A	N/A	N/A
6	Disabled			N/A	N/A	N/A

The ***„FLEXi“ SP3*** is compatible with Crow wireless FW2 and Shepherd series sensors, sirens, wireless controllers using the ***RF-SH*** module.

5.6.1 Linking the wireless equipment transceiver RF-SH to the *„FLEXi“ SP3* control panel

1. Connect the ***RF-SH*** transceiver and the ***„FLEXi“ SP3*** according to the schematic in chapter 3.10 “Schematic for connecting RF-SH”.
2. Switch on the power supply.
3. Connect a USB Mini-B cable to the ***„FLEXi“ SP3.***
4. Launch the program ***TrikdisConfig***, click the button **Read [F4]**.
5. In the **Modules** list, pick ***RF-SH wireless transceiver***.
6. In the **Serial No.** field, enter the device’s serial number.
7. Click **Write [F5]**.
8. Disconnect the USB Mini-B cable.
9. Wait 1 minute for the ***„FLEXi“ SP3*** and ***RF-SH*** to link together.
10. Connect a USB Mini-B cable to the ***„FLEXi“ SP3***.
11. Click **Read [F4]**.
12. The firmware version of the ***RF-SH*** will appear in the “**Modules**” window.

13. The **RF-SH** module is now linked to the ***„FLEXi“ SP3***.

All wireless sensors can be linked simultaneously.

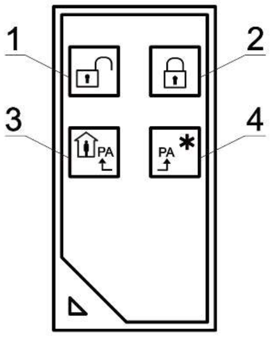
5.6.2 Linking wireless (FW2 series) sensors

1. Make sure that the ***RF-SH*** transceiver is linked to the ***„FLEXi“ SP3*** (see chapter 5.6.1 above).
2. Switch on the power supply.
3. Remove the top cover from the ***RF-SH*** transceiver.
4. Hold down the **LEARN** button on the ***RF-SH*** module until the **LEARN** LED indicator starts blinking green.
5. Release the button.
6. The green blinking **LEARN** indicator means that the ***RF-SH*** is in wireless sensor linking mode.
7. Insert a battery into the wireless sensor and wait until the sensor’s LED indicators stop blinking.
8. Hold down the **LEARN** button on the ***RF-SH*** module until the **LEARN** LED indicator stops blinking green. The ***RF-SH*** transceiver has exited linking mode.
9. Connect a USB Mini-B cable to the ***„FLEXi“ SP3***.
10. Launch ***TrikdisConfig***, click the **Read [F4]** button.
11. You can find a list of linked wireless sensors in the ***TrikdisConfig*** software window **Wireless**. The 7-digit codes in the **Serial No.** column must match the codes printed on the casings or boards of the sensors.
12. You must assign the sensors to zones and partitions of the security control panel (**Zones** window). Click **Write [F5]** after making the changes.
13. The wireless sensor is now successfully linked to the system.

Note: To delete wireless sensors from the ***„FLEXi“ SP3***’s memory:

1. Connect a USB Mini-B cable to the ***„FLEXi“ SP3***.
2. Launch **TrikdisConfig**, click the **Read [F4]** button.
3. In the ***TrikdisConfig*** window **Wireless**, in the column **Device type**, select **Disabled** instead of the **wireless sensor** that you wish to delete and click **Write [F5]**. The wireless sensor is now removed from the ***„FLEXi“ SP3***’s memory.

5.6.3 Linking a wireless (FW2 series) remote controller



1. Make sure that the ***RF-SH*** transceiver is linked to the ***„FLEXi“ SP3*** (see chapter 5.6.1 above).
2. Switch on the power supply.
3. Remove the top cover from the ***RF-SH*** transceiver.
4. Hold down the **LEARN** button on the ***RF-SH*** module until the **LEARN** LED indicator starts blinking green.
5. Release the button.
6. The green blinking **LEARN** indicator means that the ***RF-SH*** is in wireless equipment linking mode.
7. On the wireless controller, hold down buttons 3 and 4 at the same time. The LED indicator will start blinking in yellow. After a few seconds it will stop and a green indicator will light up for a short period of time.
8. Release buttons 3 and 4. The wireless controller is linked.
9. Press and hold the **RF-SH** transceiver’s **LEARN** button until the **LEARN** LED indicator stops blinking green. The **RF-SH** transceiver has exited linking mode.
10. Connect a USB Mini-B cable to the ***„FLEXi“ SP3***.
11. Launch ***TrikdisConfig***, click **Read [F4]**.
12. In the ***TrikdisConfig*** software window **Wireless**, the text **Wireless controller** must appear in the **Device type** field and the field **Serial No.** must have a 7-symbol code matching the code on the back of the remote controller.
13. In the **Area** field specify the security system area that the wireless controller will control (arm/disarm).
14. In the **User** field specify the user’s number.

15. You can assign additional functions to the controller’s buttons 3 and 4 (Arm, Disarm area; Silent alarm; Panic alarm).
16. Click **Write [F5]** after making the changes.
17. The wireless controller is now successfully linked to the system.

Note: Reverting the wireless controller to default settings:

1. Press buttons 2 and 3 at the same time and hold until the indicator starts blinking in green and red.
2. You can release the buttons when the indicator stops blinking. The controller’s memory is cleared.

5.6.4 Linking a wireless (FW2 series) siren

1. Make sure that the ***RF-SH*** transceiver is linked to the ***„FLEXi“ SP3*** (see chapter 5.6.1 above).
2. Switch on the power supply.
3. Remove the top cover from the ***RF-SH*** transceiver.
4. Hold down the **LEARN** button on the ***RF-SH*** module until the **LEARN** LED indicator starts blinking green.
5. Release the button.
6. The green blinking **LEARN** indicator means that the ***RF-SH*** is in wireless equipment linking mode.
7. Remove the cover from the siren.
8. Connect a power supply to the siren.
9. The flash of the siren will blink rarely for 30 seconds. When the indicator stops blinking, the siren is ready for linking.
10. Press and hold the **LEARN** button on the siren’s board.
11. The flash will start to blink.
12. Release the button. When the flash stops blinking, the siren will have linked successfully.
13. Press and hold the **RF-SH** transceiver’s **LEARN** button until the **LEARN** LED indicator stops blinking in green. The **RF-SH** transceiver has exited linking mode.
14. Connect a USB Mini-B cable to the ***„FLEXi“ SP3***.
15. Launch ***TrikdisConfig***, click **Read [F4]**.
16. In the ***TrikdisConfig*** software window **Wireless**, the text **Siren** must appear in the **Device type** field and the field **Serial No.** must have a 7-symbol code matching the code on the board of the siren.
17. Specify an area number in the **Area** field and click **Write [F5]**.
18. The wireless internal siren is now successfully linked to the system.

Note: Reverting the wireless siren to default settings:

1. Remove the lid from the siren.
2. Disconnect the power from the siren.
3. Press the **LEARN** button on the siren’s board and turn on the power.
4. Hold the **LEARN** button until the siren’s flash blinks 3 times.
5. Release the **LEARN** button. The siren’s flash will blink in rare intervals for another 30 seconds.
6. The flash will stop blinking. The wireless siren’s default settings have been restored.

5.6.5 Linking wireless (SH series) sensors

1. Make sure that the ***RF-SH*** transceiver is linked to the ***„FLEXi“ SP3*** (see chapter 5.6.1 above).
2. Switch on the power supply.
3. Remove the top cover from the ***RF-SH*** transceiver.
4. Hold down the **LEARN** button on the ***RF-SH*** module until the **LEARN** LED indicator starts blinking green.
5. Release the button.
6. The green blinking **LEARN** indicator means that the ***RF-SH*** is in wireless sensor linking mode.
7. Insert a battery into the wireless sensor and wait until the sensor’s LED indicator stops blinking in green and yellow. When the linking process is complete, the green LED indicator on the sensor will light up for 3 seconds and then it will go out.
8. If the linking process is unsuccessful, the LED indicator stops blinking. Remove the battery, wait for about 10 seconds and repeat the linking process.

9. Press and hold the **RF-SH** transceiver's **LEARN** button until the **LEARN** LED indicator stops blinking in green. The **RF-SH** transceiver has exited linking mode.
10. Connect a USB Mini-B cable to the ***„FLEXi“ SP3***.
11. Launch ***TrikdisConfig***, click **Read [F4]**.
12. You can find a list of linked wireless sensors in the ***TrikdisConfig*** software window **Wireless**. The 7-digit codes in the **Serial No.** column must match the codes printed on the casings or boards of the sensors.
13. You must assign the sensors to zones and partitions of the security control panel (**Zones** window). Click **Write [F5]** after making the changes.
14. The wireless sensor is now successfully linked to the system.

Note: To delete wireless sensors from the ***„FLEXi“ SP3***'s memory:

1. Connect a USB Mini-B cable to the ***„FLEXi“ SP3***.
2. Launch **TrikdisConfig**, click the **Read [F4]** button.
3. In the ***TrikdisConfig*** window **Wireless**, in the column **Device type**, select **Disabled** instead of the **wireless sensor** that you wish to delete and click **Write [F5]**. The wireless sensor is now removed from the ***„FLEXi“ SP3***'s memory.

5.6.6 Linking a wireless (SH series) keypad

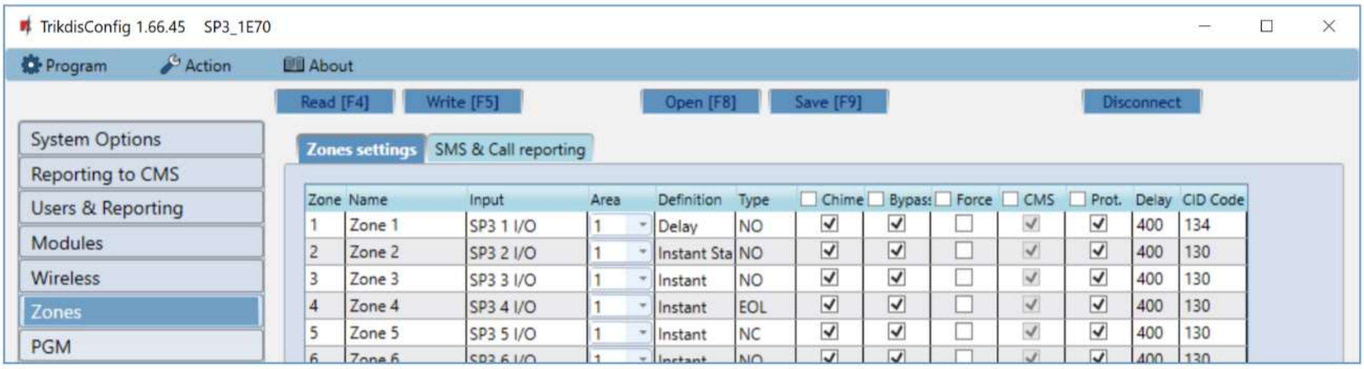
1. Make sure that the ***RF-SH*** transceiver is linked to the ***„FLEXi“ SP3*** (see chapter 5.6.1 above).
2. Switch on the power supply.
3. Remove the top cover from the ***RF-SH*** transceiver.
4. Hold down the **LEARN** button on the ***RF-SH*** module until the **LEARN** LED indicator starts blinking green.
5. Release the button.
6. The green blinking **LEARN** indicator means that the ***RF-SH*** is in wireless equipment linking mode.
7. Insert batteries into the keypad and wait for the green - red LED indicator ⌂ to stop blinking. When the linking process is complete, the green ⌂ LED indicator on the keypad will light up for 3 seconds and then it will go out.
8. Press and hold the **RF-SH** transceiver's **LEARN** button until the **LEARN** LED indicator stops blinking green. The **RF-SH** transceiver has exited linking mode.
9. Connect a USB Mini-B cable to the ***„FLEXi“ SP3***.
10. Launch ***TrikdisConfig***, click **Read [F4]**.
11. In the ***TrikdisConfig*** software window **Wireless**, the text **Keypad SH** must appear in the **Device type** field and the field **Serial No.** must have a 7-symbol code matching the code on the back of the keypad's casing.
12. Specify an area number in the **Area** field.
13. Click **Write [F5]** after making the changes.
14. The wireless keypad is now successfully linked to the system.

Note: To delete wireless sensors from the ***„FLEXi“ SP3***'s memory:

1. Connect a USB Mini-B cable to the ***„FLEXI“ SP3***.
2. Launch **TrikdisConfig**, click the **Read [F4]** button.
3. In the ***TrikdisConfig*** window **Wireless**, in the column **Device type**, select **Disabled** instead of **Keypad SH** and click **Write [F5]**. The wireless keypad is now removed from the ***„FLEXi“ SP3***'s memory.

5.7 “Zones” window

“Zones settings” tab



Zone	Name	Input	Area	Definition	Type	□ Chime	□ Bypass	□ Force	□ CMS	□ Prot.	Delay	CID Code
1	Zone 1	SP3 1 I/O	1	Delay	NO	☑	☑	□	☑	☑	400	134
2	Zone 2	SP3 2 I/O	1	Instant Sta	NO	☑	☑	□	☑	☑	400	130
3	Zone 3	SP3 3 I/O	1	Instant	NO	☑	☑	□	☑	☑	400	130
4	Zone 4	SP3 4 I/O	1	Instant	EOL	☑	☑	□	☑	☑	400	130
5	Zone 5	SP3 5 I/O	1	Instant	NC	☑	☑	□	☑	☑	400	130
6	Zone 6	SP3 6 I/O	1	Instant	NO	☑	☑	□	☑	☑	400	130

- **Zone No** – the zone’s number on the list.
- **Name** - enter the name of the zone.
- **Input** – you can select which ***„FLEXi“ SP3*** or expander module input IN to assign to the zone.
- **Area** – assign the zone to an area.
- **Definition** – every zone can be assigned one of these zone functions:
  - **Delay** – for connecting a magnetic entrance door contact. You can set entry and exit times for this type of zone.

    After the alarm is armed, the violation of the “Delay” zone is allowed within the exit time. If the zone is still violated when the time is up, outputs OUT “Siren” and “Flash” are turned on and alarm reports are sent.
    When the alarm is armed, a violation of the “Delay” zone starts the entry time counter, during which the alarm must be disarmed. If the alarm is still not disarmed when the time is up, outputs OUT “Siren” and “Flash” are turned on and alarm reports are sent.
  - **Interior** – for connecting a motion sensor to the entry door.

    If the alarm system is armed and the “Interior” zone is triggered, output signals for “Siren” and “Flash” are turned on and a report about the triggering of the alarm system is sent.

    If the alarm system is armed and the “Delay” zone is triggered first, the “Interior” zone can also be triggered during the set entry time. If the alarm is not disarmed during the set entry time, output signals for “Siren” and “Flash” are turned on and a report about the triggering of the alarm system is sent.
  - **Interior Stay** – for connecting a motion sensor to the entry door.

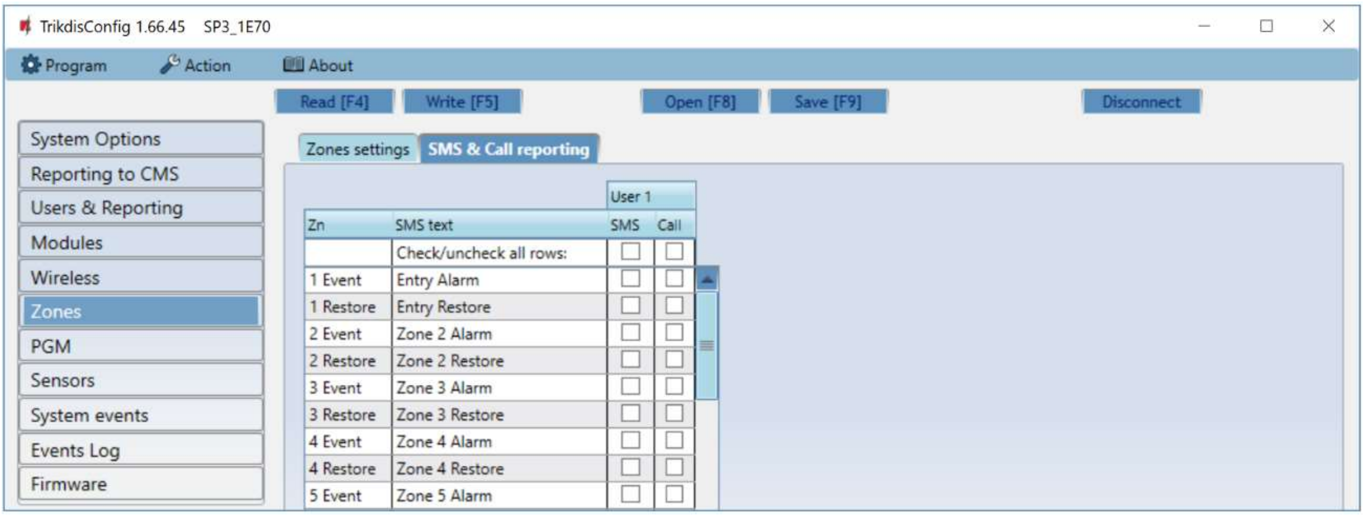
    If the alarm system is armed and the “Interior Stay” zone is violated, output signals for “Siren” and “Flash” are turned on and a report about the triggering of the alarm system is sent.

    If the alarm system is armed and the “Delay” zone is triggered first, the “Interior Stay” zone can also be triggered during the set entry time. If the alarm is not disarmed during the set entry time, output signals for “Siren” and “Flash” are turned on and a report about the triggering of the alarm system is sent.

    When the alarm system is armed in STAY mode, “Interior Stay” zones are not protected.
  - **Instant** – for connecting motion sensors. If the “Instant” zone is violated when the alarm is armed, OUT outputs “Siren” and “Flash” are turned on and a message about the alarm being triggered is sent.
  - **Instant Stay** – for connecting motion sensors. If an “Instant Stay” zone is violated when the alarm is armed, OUT outputs “Siren” and “Flash” are turned on and a message about the alarm being triggered is sent. When the alarm system is armed in STAY mode, “Instant Stay” zones are not protected.
  - **Fire** – for connecting fire sensors. If this zone is violated, OUT outputs “Siren” and “Flash” are turned on immediately and an event report is sent.
  - **Keyswitch** – for connecting a keypad or other switch. If the switch triggers this zone the security alarm will be armed or disarmed. The alarm will be armed after the set **Exit time** passes.
  - **24_hour** – for connecting glass break and tamper detectors. If this zone is violated, OUT outputs “Siren” and “Flash” are turned on immediately and an event report is sent.
  - **Silent** – if the alarm is armed and this zone is violated, an event report will immediately be sent, but “Siren” and “Flash” output signals will not be generated.
  - **Silent 24h** – for connecting panic buttons. If this zone is violated, an event report will immediately be sent regardless of the state of the security system, but “Siren” and “Flash” output signals will not be formed.

- **Type** – choose the type of circuit connected to the zone input IN from a list: NC – normally closed; NO – normally open; EOL – with an end of line resistor; EOL_T – with an end of line resistor and tamper monitoring; ATZ – two zone normally closed circuit with end of line resistors, without tamper monitoring function (to use this type, choose the second ATZ zone in the input list); ATZ_T – two zone normally closed circuit with end of line resistors, with tamper monitoring function (to use this type, choose the second ATZ zone in the input list); 3EOL - with an end of line resistor and tamper monitoring (this setting is for when motion detection with anti masking function is used).
- **Chime** - checking the box will enable the zone chime feature. When the zone is activated, the keypad will beep.
- **Bypass** – tick this box if you want to allow this zone to be bypassed and ignored when it is triggered.
- **Force** – tick this box if you want to allow arming the security system with the zone open. When the alarm is armed, open zones set to “Force” mode will be temporarily disconnected. After zone restore, they will be turned on and monitored again. A violation of this zone will trigger an alarm.
- **CMS** – if the box is ticked, zone event reports will be sent to the central monitoring station (CMS).
- **Prot.** – if the box is ticked, zone event reports will be sent to ***Protegus*** cloud.
- **Delay** – input IN zone reaction time, in milliseconds.
- **CID code** – event contact ID codes. This code will be filled in automatically after selecting a definition for the zone.
- **Sound** – specify the number of the voice recording that will be played back to the user when the ***„FLEXi“ SP3*** control panel calls during an alarm (this function is valid for SP3_12xx control panel with firmware version up to 1.13 inclusive).

“SMS & Call reporting” tab



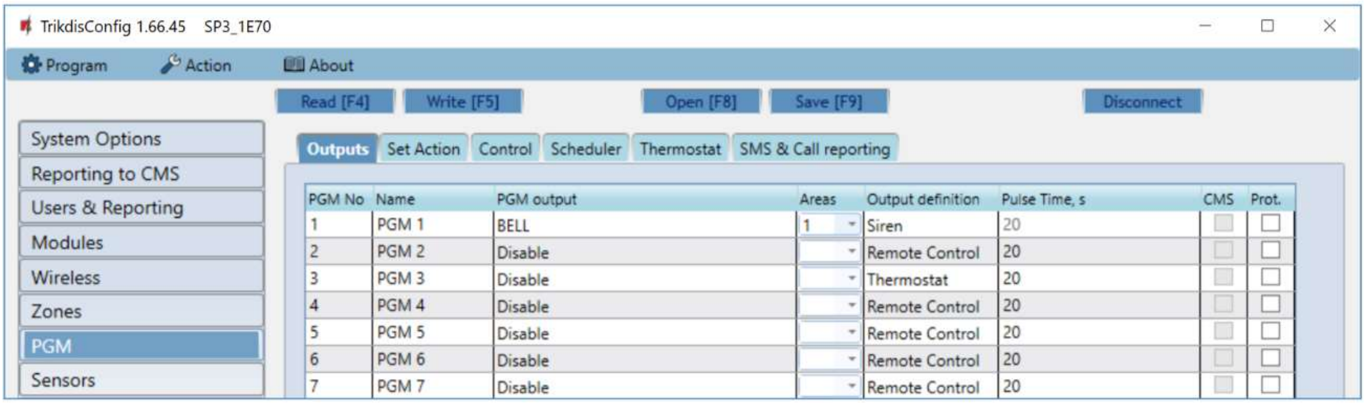
		User 1	
Zn	SMS text	SMS	Call
	Check/uncheck all rows:	□	□
1 Event	Entry Alarm	□	□
1 Restore	Entry Restore	□	□
2 Event	Zone 2 Alarm	□	□
2 Restore	Zone 2 Restore	□	□
3 Event	Zone 3 Alarm	□	□
3 Restore	Zone 3 Restore	□	□
4 Event	Zone 4 Alarm	□	□
4 Restore	Zone 4 Restore	□	□
5 Event	Zone 5 Alarm	□	□

This tab will only be shown if there is at least one user in the *„Users & Reporting"* window.

- **Zn** – zone number with the event identification word. Can be *“Event”* or “Restore”.
- **SMS text** – description of the zone event that will be included in event reports sent to the user using SMS messages.
- **User / SMS and Call** – choose how users will be informed about events in every individual zone – using SMS messages or/and phone calls.

5.8 “PGM” window

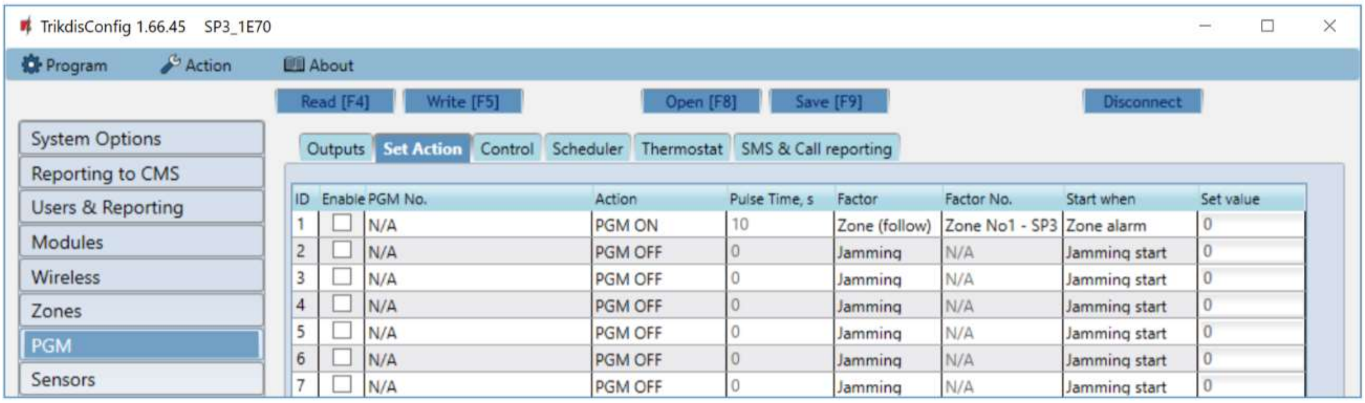
“Outputs tab”



PGM No	Name	PGM output	Areas	Output definition	Pulse Time, s	CMS	Prot.
1	PGM 1	BELL	1	Siren	20	□	□
2	PGM 2	Disable		Remote Control	20	□	□
3	PGM 3	Disable		Thermostat	20	□	□
4	PGM 4	Disable		Remote Control	20	□	□
5	PGM 5	Disable		Remote Control	20	□	□
6	PGM 6	Disable		Remote Control	20	□	□
7	PGM 7	Disable		Remote Control	20	□	□

- **PGM No** – specifies the PGM output’s number on the list.
- **Name** - enter PGM output name.
- **PGM output** – assign the outputs OUT of the ***„FLEXi“ SP3*** or an external device to the PGM.
- **Area** – assign the output OUT to an area.
- **Output definition** – choose the operational mode of the output OUT.
  - **Siren** – for connecting a siren.
  - **Remote control** – for controlling external electric devices.
  - **Fire Sensor Reset** – for resetting a fire sensor after triggering.
  - **System State** – for connecting a security system state indicator. E.g., an LED can display when the alarm is armed / disarmed.
  - **Flash** – if the alarm is armed a line signal is generated, if it is triggered – a pulse type signal. The signal is cut off when the alarm is disarmed.
  - **Thermostat** – this setting will make the PGM output operate in thermostat mode. A temperature sensor must be connected to the ***„FLEXi“ SP3***. The PGM output must have thermostat mode set and the temperature that it must maintain has to be specified.
  - **Buzzer** – for repeating the sound signals from a keypad.
- **Pulse time, s** – you can set the desired OUT turn on duration from 0 to 9999 seconds.
- **CMS** – if this box is ticked, PGM output turn on/off reports will be sent to the central monitoring station (CMS).
- **Prot.** – if the box is ticked, PGM output turn on/off reports will be sent to ***Protegus*** cloud.

“Set Action” tab



ID	Enable	PGM No.	Action	Pulse Time, s	Factor	Factor No.	Start when	Set value
1	□	N/A	PGM ON	10	Zone (follow)	Zone No1 - SP3	Zone alarm	0
2	□	N/A	PGM OFF	0	Jamming	N/A	Jamming start	0
3	□	N/A	PGM OFF	0	Jamming	N/A	Jamming start	0
4	□	N/A	PGM OFF	0	Jamming	N/A	Jamming start	0
5	□	N/A	PGM OFF	0	Jamming	N/A	Jamming start	0
6	□	N/A	PGM OFF	0	Jamming	N/A	Jamming start	0
7	□	N/A	PGM OFF	0	Jamming	N/A	Jamming start	0

- **ID** – output’s number on the list.
- **Enable** – enables the PGM operation algorithm.
- **PGM No.** – select the desired PGM output OUT that will be controlled after the event described in columns **Factor**, **Factor No.**, **Start when**, **Set value** occurs.
- **Action**:

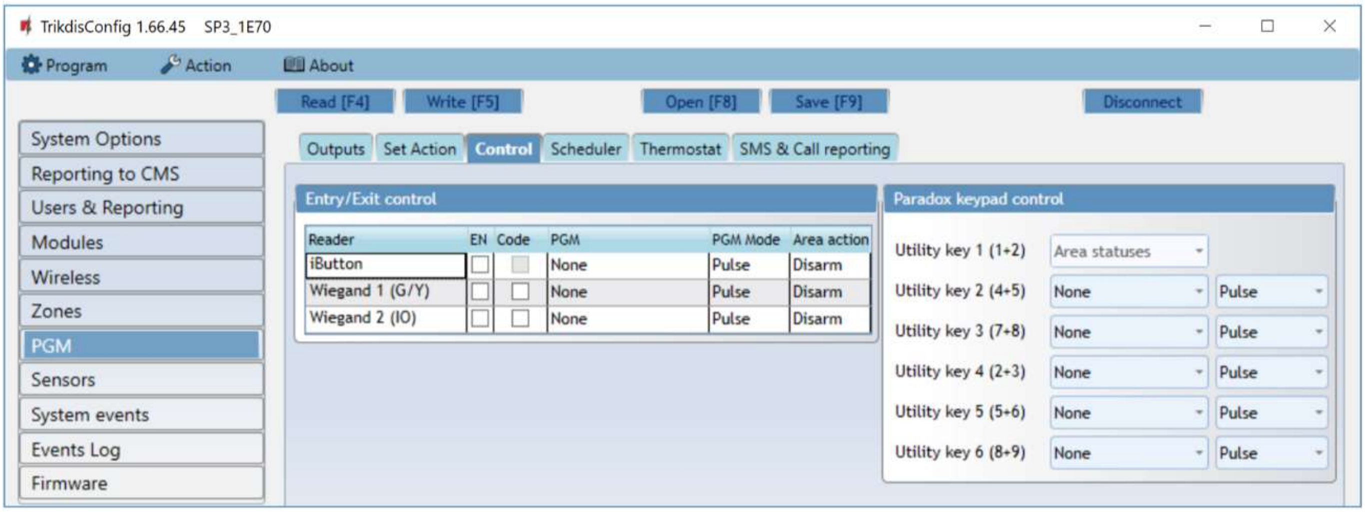
  - **PGM OFF** – state of output OUT – “Off”.
  - **PGM ON** – state of output OUT – “On”.
  - **Pulse OFF** – initial state of output OUT – “On”. After the command the OUT state will become “Off” for the duration of the **Pulse time**, and later it will automatically return to the initial “On” state**.**
  - **Pulse ON** – initial state of output OUT – “Off”. After the command the OUT state will become “On” for the duration of the **Pulse time**, and later it will automatically return to the initial “Off” state**.**
- **Pulse time, s** – you can set the pulse time anywhere from 0 to 9999 seconds.
- **Factor/Factor No.** – choose what event (*Zone, Sensor, Jamming, Sensor lost, iButton, Arm, Disarm, SMS received, Zone(follow)*) will turn on the output OUT.
  - Schedules can be assign to an output OUT. The schedule shows when the output should be turned on. Up to 10 different schedules can be prepared in the **Scheduler tab**.
- **Start when** – you can set an additional condition when to turn on the output OUT depending on the **Factor** event.
- **Set value** – depending on the condition chosen in the **Factor** column (SMS received, Temperature) a value (text of received SMS message, voltage or temperature) can be specified. If this value is identified, the action (chosen in the **Action** column) will be performed. The text of the SMS message can be separated by using % symbols. % symbols are used for separating the keyword that will change the state of a PGM output from the entire received SMS message. **%.....%** - part of the received SMS message text must match with the text entered between % symbols (e.g. **%hoUSe%**. The text in an SMS message must include the text “**hoUSe**”. Example of an SMS message: **VacationhoUSe25864**).

  .....% - the beginning of the received SMS message must match the text entered until the % symbol (e.g. **hoUSe%**. The SMS message must start with the text **“hoUSe”**. Example of an SMS message: **hoUSeddss**).

  %..... – the ending of the received SMS message must match with the text entered after the % symbol. (e.g. **%hoUSe**. The SMS message must end with the text **“hoUSe”**. Example of an SMS message: **1144hoUSe**).

  The SMS message text is case-sensitive.

“Control” tab



Entry/Exit control

Reader	EN	Code	PGM	PGM Mode	Area action
iButton	□	□	None	Pulse	Disarm
Wiegand 1 (G/Y)	□	□	None	Pulse	Disarm
Wiegand 2 (IO)	□	□	None	Pulse	Disarm

Paradox keypad control

Utility key 1 (1+2)	Area statuses	
Utility key 2 (4+5)	None	Pulse
Utility key 3 (7+8)	None	Pulse
Utility key 4 (2+3)	None	Pulse
Utility key 5 (5+6)	None	Pulse
Utility key 6 (8+9)	None	Pulse

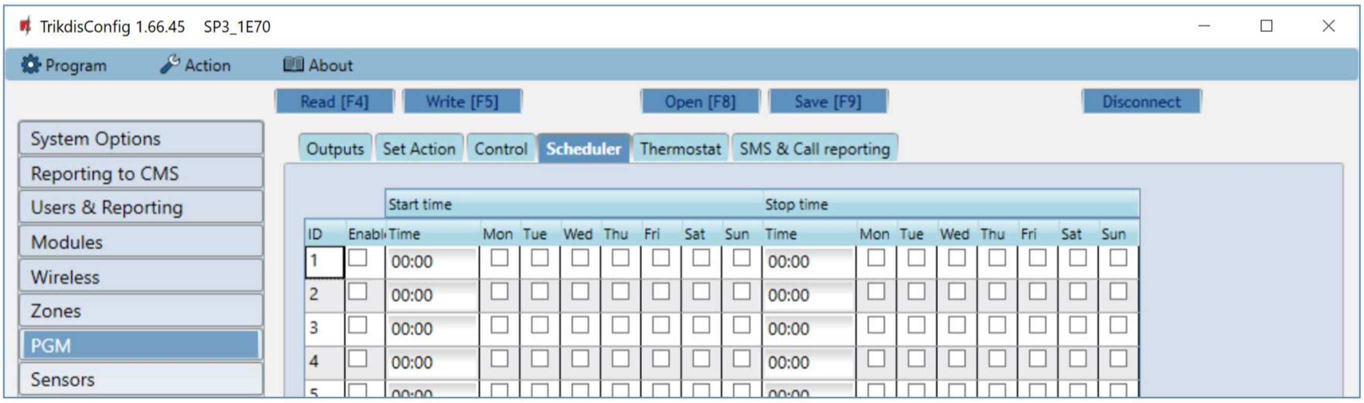
Settings group “Entry/Exit control”

- **Reader** – the readers that can be connected to the security panel are indicated.
- **En –** check the box to enable the reader to control the PGM output.
- **PGM –** specify the PGM output that the reader will control. PGM output must be set to **Remote control** mode.
- **PGM mode –** set the PGM output triggering mode (**Pulse** or **Level**).
- **Area action -** indicate the change in the security mode of the security panel when an iButton key or RFID card is attached to the reader.

Settings group “Paradox keypad control”

- **Utility key** – pressing and holding the utility keys for 3 seconds will trigger the PGM output. The PGM output will activate for the duration of the pulse (if the operating mode is **Pulse**) or the level of the PGM output signal will change (if the operating mode is **Level**).

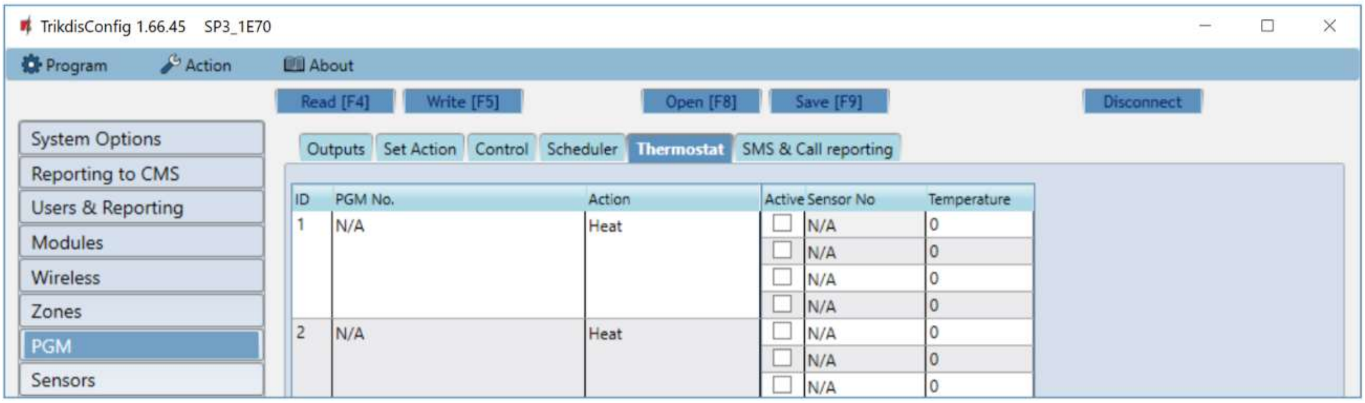
“Scheduler” tab



		Start time								Stop time							
ID	Enabl	Time	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Time	Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	□	00:00	□	□	□	□	□	□	□	00:00	□	□	□	□	□	□	□
2	□	00:00	□	□	□	□	□	□	□	00:00	□	□	□	□	□	□	□
3	□	00:00	□	□	□	□	□	□	□	00:00	□	□	□	□	□	□	□
4	□	00:00	□	□	□	□	□	□	□	00:00	□	□	□	□	□	□	□
5	□	00:00	□	□	□	□	□	□	□	00:00	□	□	□	□	□	□	□

- **ID** – schedule’s number on the list.
- **Enable** – enable the schedule.
- **Start time** – set the time when OUT will be turned on (schedule start time).
- **Stop time** – set the time when OUT will be turned off (schedule end time).
  - **Mon – Sun** – you can mark the days of the week when OUT will have to be turned on/off.

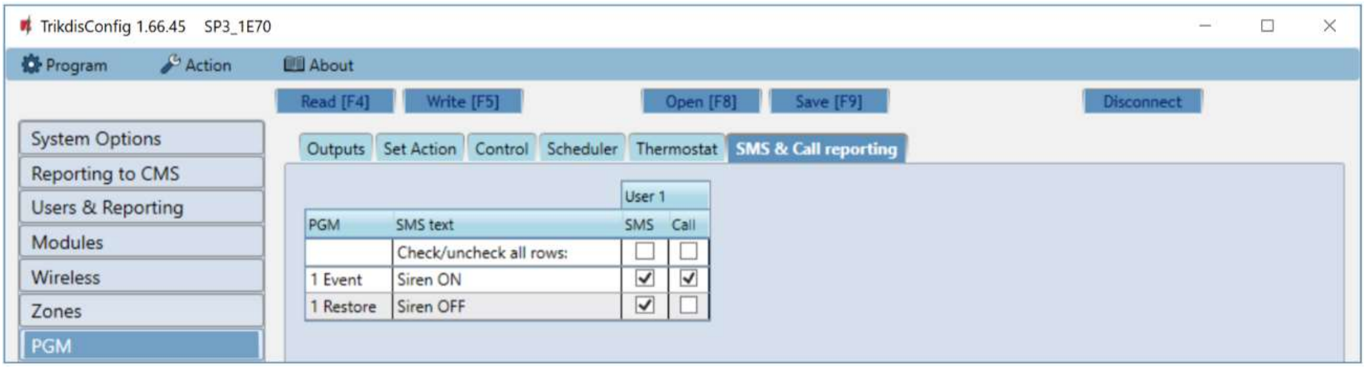
“Thermostat” tab



ID	PGM No.	Action	Active	Sensor No	Temperature
1	N/A	Heat	□	N/A	0
			□	N/A	0
			□	N/A	0
			□	N/A	0
2	N/A	Heat	□	N/A	0
			□	N/A	0
			□	N/A	0

- **ID** – thermostat’s number on the list.
- **PGM No.** – specify the number of the PGM output that the thermostat will control.
- **Action** – set the thermostat’s operation mode: heating or cooling.
- **Active** – if the box is ticked, the thermostat will work with the selected temperature sensor according to the set temperature.
- **Sensor No –** assign a temperature sensor to the thermostat.
- **Temperature –** set the temperature that the thermostat will maintain.

“SMS & Call reporting” tab

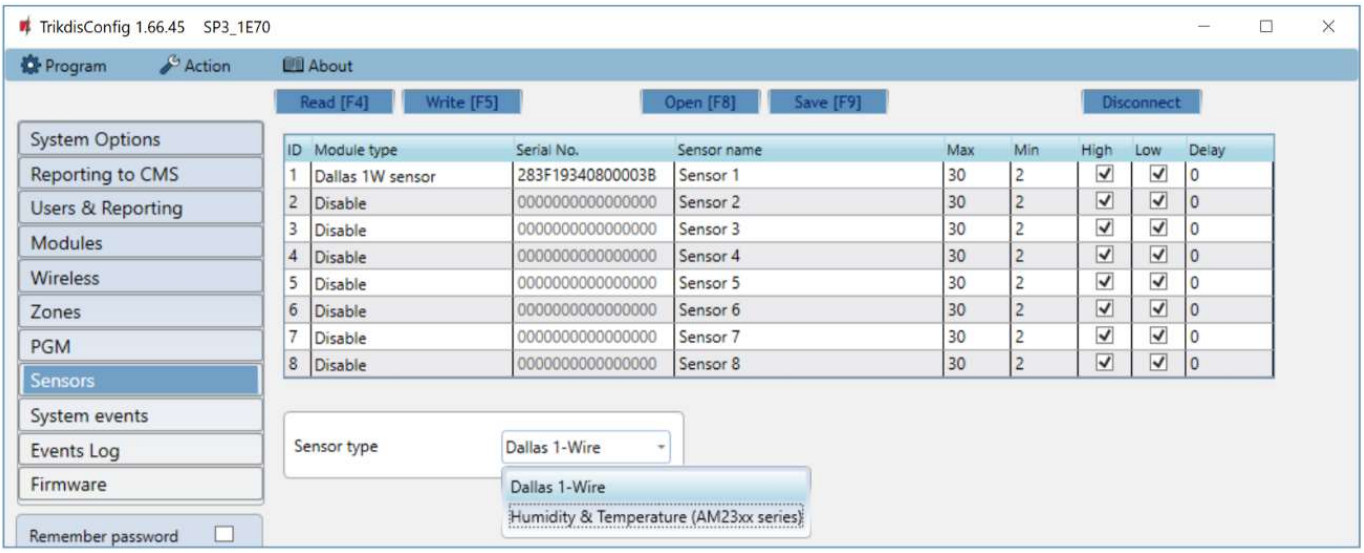


		User 1	
PGM	SMS text	SMS	Call
	Check/uncheck all rows:	□	□
1 Event	Siren ON	☑	☑
1 Restore	Siren OFF	☑	□

This tab will only be shown if there is at least one user in the *“Users & Reporting”* window. These settings can only be made for the first 8 users.

- **PGM** – shows the output OUT number and turn on/off event type (“Event” – output OUT turn on event and “Restore” – output OUT turn off event).
- **SMS text** – the name of the output OUT turn on/off event, it will be used in the event’s SMS message.
- **User / SMS and Call** – choose which users to inform using SMS messages and/or phone calls when the output OUT is turned on/off.

5.9 “Sensors” window



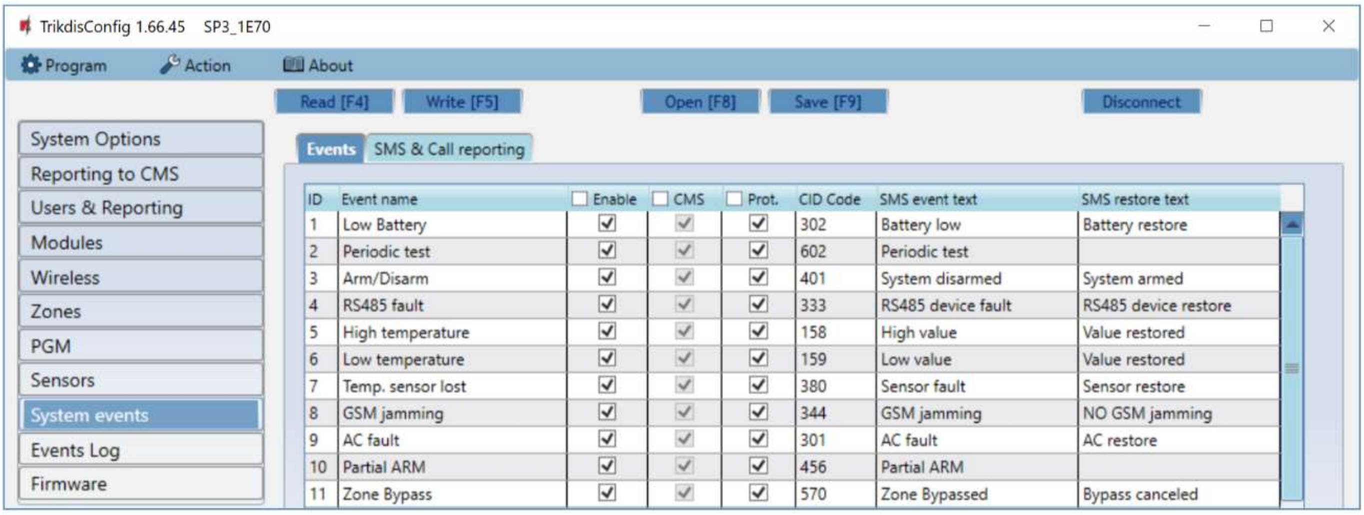
ID	Module type	Serial No.	Sensor name	Max	Min	High	Low	Delay
1	Dallas 1W sensor	283F19340800003B	Sensor 1	30	2	☑	☑	0
2	Disable	0000000000000000	Sensor 2	30	2	☑	☑	0
3	Disable	0000000000000000	Sensor 3	30	2	☑	☑	0
4	Disable	0000000000000000	Sensor 4	30	2	☑	☑	0
5	Disable	0000000000000000	Sensor 5	30	2	☑	☑	0
6	Disable	0000000000000000	Sensor 6	30	2	☑	☑	0
7	Disable	0000000000000000	Sensor 7	30	2	☑	☑	0
8	Disable	0000000000000000	Sensor 8	30	2	☑	☑	0

Sensor type: Dallas 1-Wire

- **ID** – temperature sensor’s number on the list.
- **Module type** – choose a temperature sensor to assign to the ID.
- **Serial No.** - serial number of the temperature sensor that is connected to the control panel.
- **Sensor name** – give the temperature sensor a name.
- **Max** – when the temperature is higher than this setting, an event report will be generated. For an event message to be generated, the **High** box must be ticked.
- **Min** – when the temperature is lower than this setting, an event report will be generated. For an event message to be generated, the **Low** box must be ticked.
- **Delay** - an event will be sent if the measured value (Max or Min) by the sensor is exceeded within the set time. Delay time is entered in minutes.
- **Sensor type** – choose the type of the connected temperature sensor (Dallas 1Wire – up to 8 temperature sensors of this type can be connected. If Dallas sensors are chosen, they will be linked automatically; Humidity & Temperature – one AM2301 temperature and humidity sensor can be connected. If the Humidity & Temperature sensor will be used, it must be manually assigned in the **Module type** column).

5.10 “System events” window

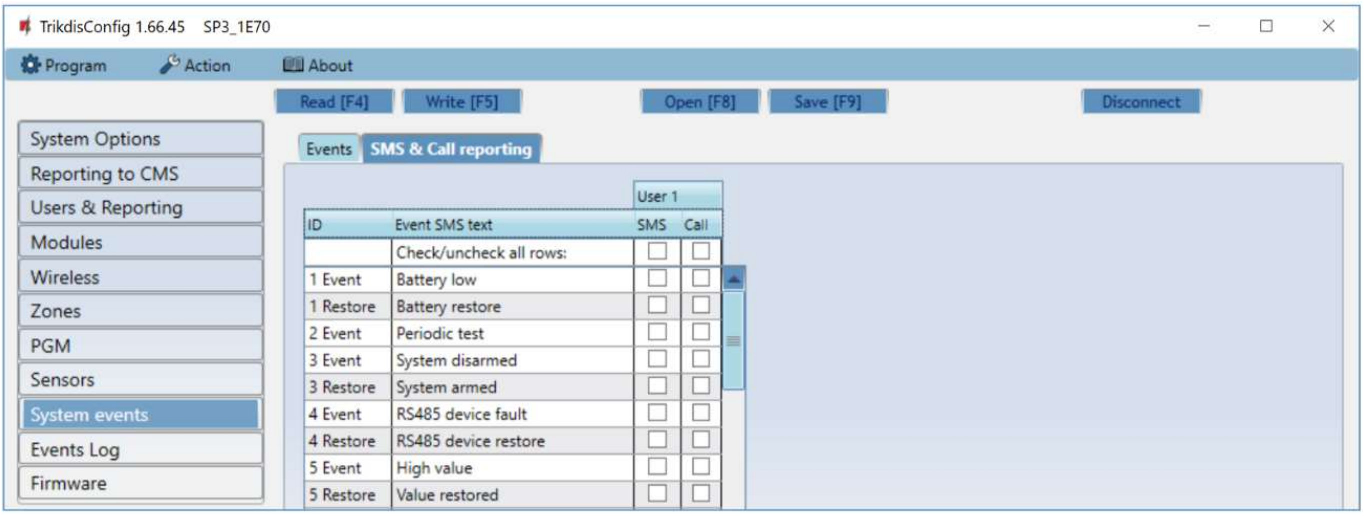
“Events” tab



ID	Event name	☐ Enable	☐ CMS	☐ Prot.	CID Code	SMS event text	SMS restore text
1	Low Battery	☑	☑	☑	302	Battery low	Battery restore
2	Periodic test	☑	☑	☑	602	Periodic test	
3	Arm/Disarm	☑	☑	☑	401	System disarmed	System armed
4	RS485 fault	☑	☑	☑	333	RS485 device fault	RS485 device restore
5	High temperature	☑	☑	☑	158	High value	Value restored
6	Low temperature	☑	☑	☑	159	Low value	Value restored
7	Temp. sensor lost	☑	☑	☑	380	Sensor fault	Sensor restore
8	GSM jamming	☑	☑	☑	344	GSM jamming	NO GSM jamming
9	AC fault	☑	☑	☑	301	AC fault	AC restore
10	Partial ARM	☑	☑	☑	456	Partial ARM	
11	Zone Bypass	☑	☑	☑	570	Zone Bypassed	Bypass canceled

- **ID** – event’s number on the list.
- **Event name** – event name.
- **Enable** – enable event recognition and report generation.
- **CMS / Prot.** – reports on selected events will be sent to CMS and/or to ***Protegus*** cloud.
- **CID Code** – Contact ID code of the event.
- **SMS event text** – event SMS message text.
- **SMS restore text** – restore event SMS message text.

“SMS & Call reporting” tab

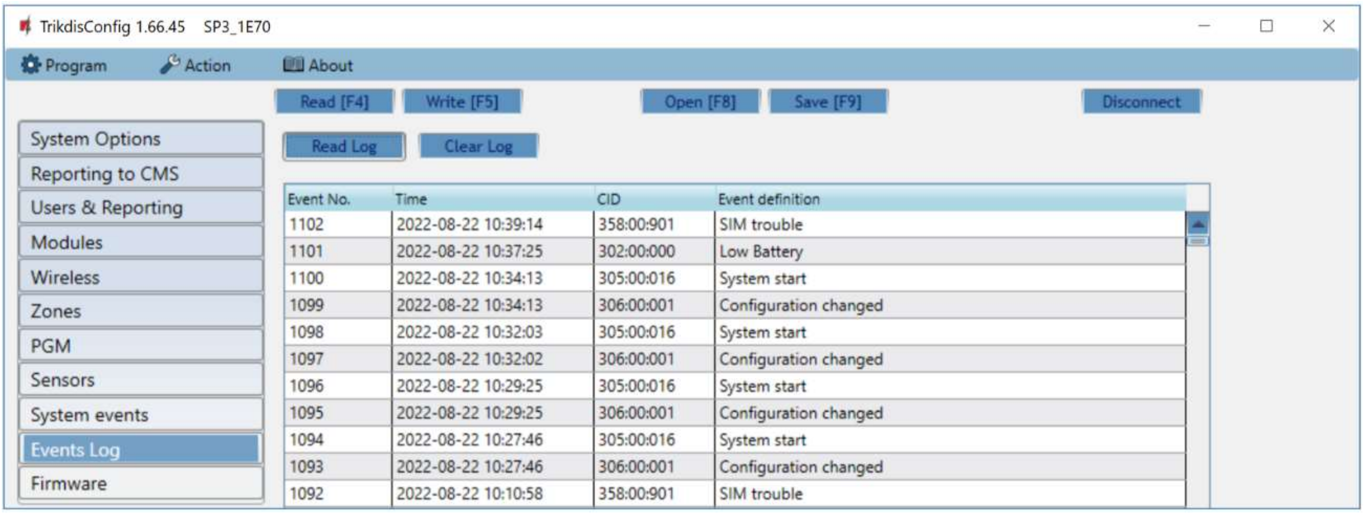


		User 1	
ID	Event SMS text	SMS	Call
	Check/uncheck all rows:	☐	☐
1 Event	Battery low	☐	☐
1 Restore	Battery restore	☐	☐
2 Event	Periodic test	☐	☐
3 Event	System disarmed	☐	☐
3 Restore	System armed	☐	☐
4 Event	RS485 device fault	☐	☐
4 Restore	RS485 device restore	☐	☐
5 Event	High value	☐	☐
5 Restore	Value restored	☐	☐

This tab will only be shown if there is at least one user in the “*Users & Reporting*” window.

- **ID** – number and identification word (*Event*, *Restore*) of the event.
- **Event SMS text** – text that will be used in event SMS messages.
- **User / SMS and Call** – choose the ways users will be informed about each event – SMS message and/or phone call.

5.11 “Events log” window

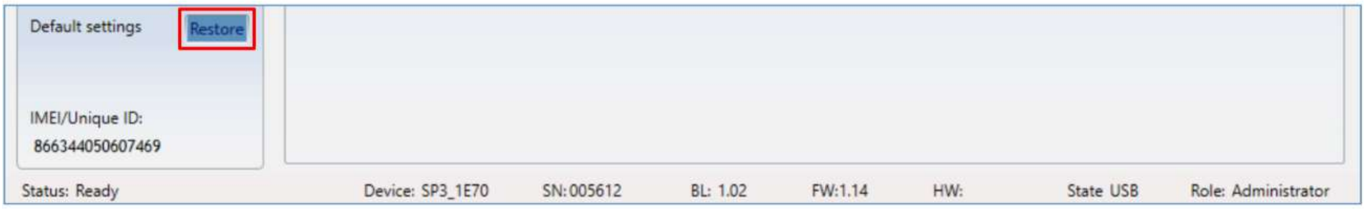


Event No.	Time	CID	Event definition
1102	2022-08-22 10:39:14	358:00:901	SIM trouble
1101	2022-08-22 10:37:25	302:00:000	Low Battery
1100	2022-08-22 10:34:13	305:00:016	System start
1099	2022-08-22 10:34:13	306:00:001	Configuration changed
1098	2022-08-22 10:32:03	305:00:016	System start
1097	2022-08-22 10:32:02	306:00:001	Configuration changed
1096	2022-08-22 10:29:25	305:00:016	System start
1095	2022-08-22 10:29:25	306:00:001	Configuration changed
1094	2022-08-22 10:27:46	305:00:016	System start
1093	2022-08-22 10:27:46	306:00:001	Configuration changed
1092	2022-08-22 10:10:58	358:00:901	SIM trouble

- **Read Log** button – command for reading the events log from the device’s memory.
- **Clear Log** – command for clearing the events log entries from the device’s memory.
- In the table, you can find the **Event No.**, **Time**, **CID** code, **Event definition**. The events log can show up to 1000 events stored in the ***„FLEXi“ SP3***’s memory.

5.12 Restore default settings

To restore the control panel’s default settings, click the ***TrikdisConfig*** button **Restore**.



IMEI/Unique ID:
866344050607469

Status: Ready Device: SP3_1E70 SN:005612 BL: 1.02 FW:1.14 HW: State USB Role: Administrator

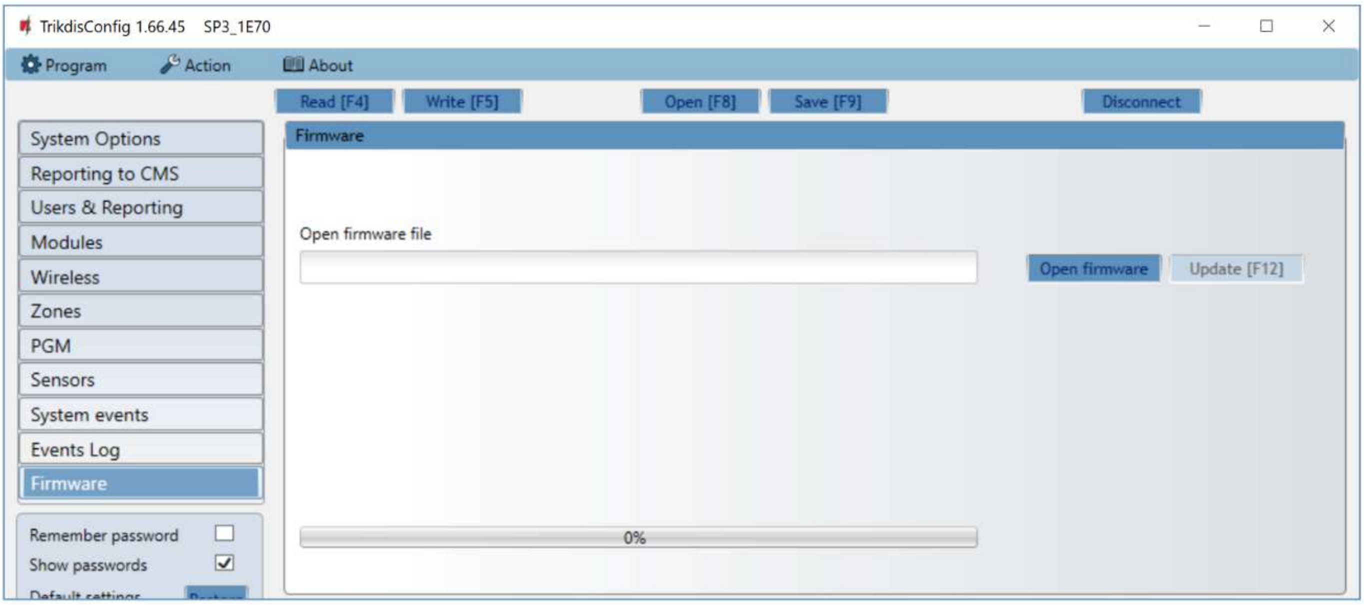
5.13 Updating firmware

Note:	After connecting the ***„FLEXi“ SP3*** to ***TrikdisConfig***, the program will automatically offer to update the firmware if any updates are available. An internet connection is needed for this feature. If antivirus software is installed on your computer, it may block the automatic firmware update function. In this case, you will have to reconfigure your antivirus software.

The ***„FLEXi“ SP3***’s firmware can also be updated or changed manually. All prior settings of the ***„FLEXi“ SP3*** remain unchanged after an update. If the firmware is installed manually, it can be changed to a newer or an older version.

Perform these steps:

1. Launch ***TrikdisConfig***.
2. Connect the ***„FLEXi“ SP3*** to a computer using a USB Mini-B cable or connect to the ***„FLEXi“ SP3*** remotely. If a newer version of firmware is available, the program will automatically offer to install it.
3. Open the ***TrikdisConfig*** window **Firmware**.



Remember password ☐
Show passwords ☑

4. Click the **Open firmware** button and choose the required firmware file. If you do not have the file, the newest firmware file can be downloaded from the ***„FLEXi“ SP3*** downloads section of www.trikdis.com by registered users.
5. Click the **Update [F12]** button.
6. Wait for the updates to finish.

Once configuration is complete, click the **Write [F5]** button and disconnect the USB cable.