



# Security control panel “FLEXi” SP3\_3E

## Installation and programming manual

May, 2021



## Table of contents

<b>1</b>	<b>DESCRIPTION .....</b>	<b>6</b>
1.1	TECHNICAL SPECIFICATIONS .....	7
1.2	LIST OF COMPATIBLE MODULES.....	9
1.3	PURPOSE OF EXTERNAL TERMINALS .....	10
1.4	LED INDICATION OF OPERATION .....	11
<b>2</b>	<b>POWERING THE SECURITY CONTROL PANEL.....</b>	<b>11</b>
2.1	MAIN POWER SUPPLY.....	11
2.2	BACKUP POWER SUPPLY.....	11
2.3	CONTROL PANEL KITS.....	11
2.3.1	<i>Control panel „FLEXi“ SP3_3E .....</i>	<i>11</i>
2.3.2	<i>Control panel „FLEXi“ SP3_3E KIT .....</i>	<i>12</i>
2.3.3	<i>Control panel „FLEXi“ SP3_3E KITi .....</i>	<i>12</i>
<b>3</b>	<b>INSTALLATION OF THE SYSTEM .....</b>	<b>12</b>
3.1	RECOMMENDED ORDER OF INSTALLATION .....	12
3.1.1	<i>Installing the control panel into the mounting housing.....</i>	<i>13</i>
3.1.2	<i>Order of connecting devices.....</i>	<i>14</i>
3.1.3	<i>Recommendations for setting the control panel's parameters .....</i>	<i>14</i>
3.2	CONNECTING SENSORS .....	15
3.3	CONNECTING SMOKE DETECTORS.....	16
3.4	SCHEMATIC FOR CONNECTING A SIREN .....	17
3.5	SCHEMATICS FOR CONNECTING KEYPADS AND RFID READERS (WIEGAND 26/34).....	17
3.6	SCHEMATICS FOR CONNECTING TM17, CZ-DALLAS READERS.....	19
3.7	SCHEMATIC FOR CONNECTING A TEMPERATURE SENSOR .....	20
3.8	SCHEMATICS FOR CONNECTING A RELAY AND AN LED INDICATOR .....	20
3.9	SCHEMATIC FOR CONNECTING ETHERNET COMMUNICATOR E485 .....	20
3.10	SCHEMATIC FOR CONNECTING RF-SH.....	20
3.11	SCHEMATICS FOR CONNECTING IO SERIES EXPANDER MODULES.....	21
3.12	SCHEMATICS FOR CONNECTING RF TRANSMITTER T16 .....	21
3.13	SCHEMATICS FOR CONNECTING SF485 .....	21
3.14	TURNING ON THE CONTROL PANEL .....	21
<b>4</b>	<b>REMOTE CONTROL.....</b>	<b>21</b>
4.1	LINKING THE „FLEXi“ SP3_3E TO A USER'S PROTEGUS ACCOUNT .....	21
4.2	ARMING/DISARMING THE SYSTEM USING PROTEGUS .....	22
<b>5</b>	<b>SETTING PARAMETERS USING TRIKDISCONFIG SOFTWARE .....</b>	<b>23</b>
5.1	DESCRIPTION OF TRIKDISCONFIG STATUS BAR.....	23
5.2	“SYSTEM OPTIONS” WINDOW.....	24
5.3	“REPORTING TO CMS” WINDOW .....	27
5.4	“USERS & REPORTING” WINDOW .....	29
5.4.1	<i>Linking RFID key fobs (cards) .....</i>	<i>30</i>
5.4.2	<i>Linking electronic (iButton) keys .....</i>	<i>30</i>
5.5	“MODULES” WINDOW .....	31
5.6	“WIRELESS” WINDOW.....	33
5.6.1	<i>Linking the wireless equipment transceiver RF-SH to the „FLEXi“ SP3_3E control panel.....</i>	<i>33</i>
5.6.2	<i>Linking wireless (FW2 series) sensors .....</i>	<i>33</i>
5.6.3	<i>Linking a wireless (FW2 series) remote controller .....</i>	<i>34</i>
5.6.4	<i>Linking a wireless (FW2 series) siren.....</i>	<i>34</i>



5.6.5	Linking wireless (SH series) sensors .....	35
5.6.6	Linking a wireless (SH series) keypad.....	35
5.7	“ZONES” WINDOW .....	36
5.8	“PGM” WINDOW .....	38
5.9	“SENSORS” WINDOW .....	41
5.10	“SYSTEM EVENTS” WINDOW .....	41
5.11	“EVENTS LOG” WINDOW.....	42
5.12	RESTORE DEFAULT SETTINGS .....	42
5.13	REMOTE CONFIGURATION .....	42
5.14	UPDATING FIRMWARE .....	43



## 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 WiFi/LAN Internet connectivity.
- restrictions or termination of WiFi/LAN 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\_3E 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\_3E control panel is a processor part of intrusion and fire alarm system. It comes with a built-in WiFi module and LAN module. The „FLEXi“ SP3\_3E 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 **Protegun**) 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 **Protegun** cloud via WiFi and LAN networks.

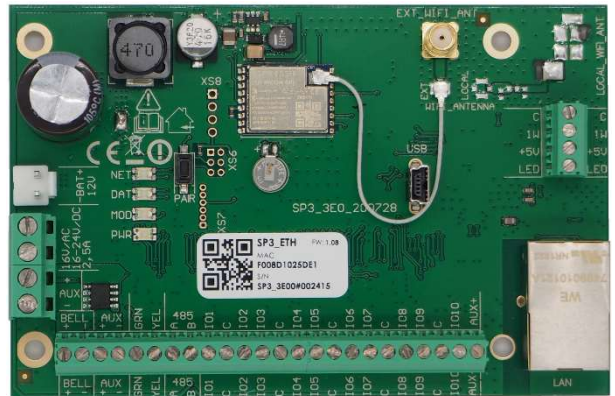
### When it's recommended to choose the „FLEXi“ SP3\_3E control panel?

- For securing small or medium sized premises which will be monitored by a security company. The „FLEXi“ SP3\_3E 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\_3E 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 LAN module.
- Additional modules to send reports via LAN Ethernet, 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 **Protegun** mobile app, which gives warnings about alarm system events using push and special sound notifications.
- 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, ATZ\_T, EOL, EOL\_T, 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; 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.

### Simple installation:

- Multiple sizes of „FLEXi“ SP3\_3E mounting kits that include a decorative white metal housing with a built-in step-down transformer or impulse power supply.
- Default „FLEXi“ SP3\_3E 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\_3E 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\_3E 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, 2,5 A DC
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
LAN module	Yes, built-in
LAN network configuration type	DHCP or manual
Report transmission directions	- To main and backup receivers of 2 different security companies;



Parameter	Description
	- To <b>Protegeus</b> cloud, to iOS/Android <b>Protegeus</b> mobile apps;
Event reporting transmission channels	LAN, WiFi, LAN (with module E485), VHF/UHF radio waves (with transmitter T16), Sigfox (module SF485)
Protocols for connection to CMS	TCP / IP or UDP / IP
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, 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	Protegeus SK232 LED W Paradox K636 Paradox K10H(V) Paradox K32 LED Paradox K32+ LED Paradox K32LCD+ Paradox K35 Paradox TM50 Paradox TM70 Crow CR16 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 ( <i>iButton</i> ) keys [1 WIRE]	Maxim®/Dallas® DS1990A
Max. no. of electronic ( <i>iButton</i> ) keys	40
RS485 data bus length	Up to 100 m
Max. no. of devices connected to RS485 data bus	8
Supported modules	<b>iO-8</b> – expander module;





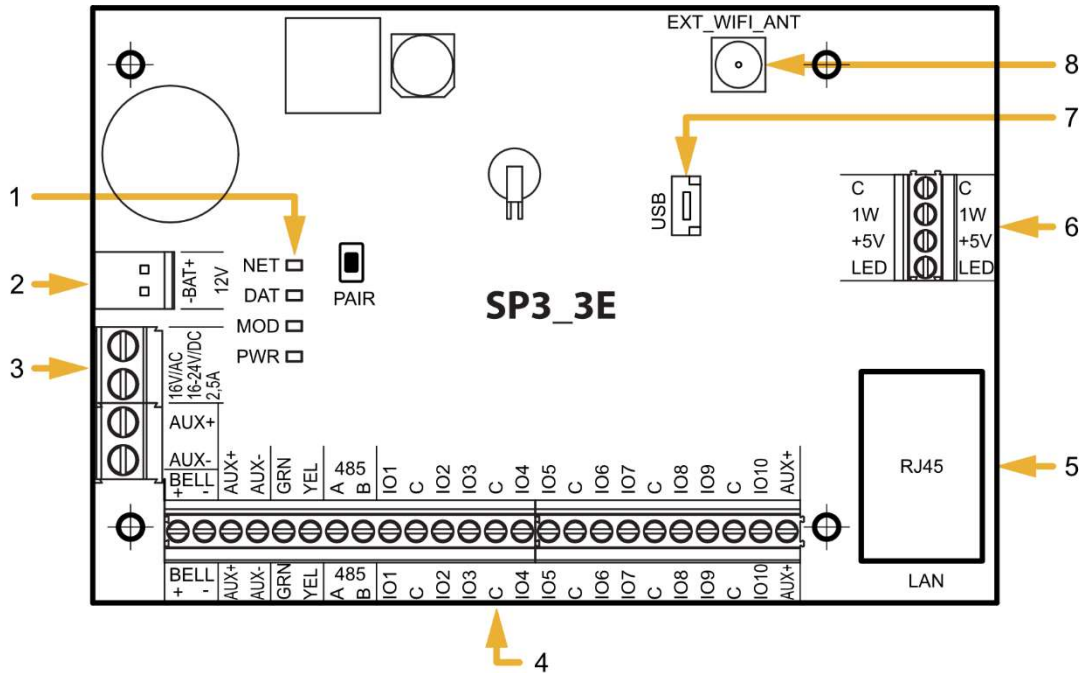
Parameter	Description
	<i>iO</i> – expander module; <i>iO-MOD</i> – iO-WL radio wave transceiver; <i>iO-WL</i> – wireless expander module; <i>RF-SH</i> – radio wave receiver for wireless sensors; <i>E485</i> – module for connecting to Ethernet network; <i>TM17</i> – iButton key reader; <i>CZ-Dallas</i> – iButton key reader; <i>T16</i> – VHF or UHF radio wave transmitter; <i>SF485</i> - Sigfox network connection 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 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
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
SF485 Sigfox communicator	Max 100 mA
RFID reader (Wiegand 26/34)	Max 100 mA



### 1.3 Purpose of external terminals



- |   |   |
|---|---|
| 1. Connectivity and operation indicator lights. | 5. RJ45 LAN connector.  |
| 2. Backup power supply terminal block.          | 6. 1-WIRE data bus terminal block.                                    |
| 3. Main power supply terminal block.            | 7. USB Mini-B connector for configuring the control panel's settings. |
| 4. External terminal block.                     | 8. SMA screw-on type connector for WiFi antenna.                      |

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
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
<b>NET</b> (Indicator of connection to WiFi network)	Green blinking	Connecting to WiFi network
	Green solid	Connected to WiFi network
	Yellow blinking	Indicates WiFi signal strength from 0 to 5. 2 is sufficient
<b>DAT</b> (Data)	Off	No unsent event messages
	Green solid	Message is being sent
	Yellow solid	There are unsent event messages in buffer memory
<b>MOD</b> (Indicator of connection to LAN network)	Green blinking	Connecting to LAN network
	Green solid	Connected to LAN network
<b>PWR</b> (Power)	Green blinking	No operational problems
	1 red flash	LAN cable not connected
	2 red flashes	Unable to get IP address for LAN connection
	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 below 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\_3E

Name	Quantity
„FLEXi“ SP3_3E control panel board	1 pc.
Wire for connecting battery	1 pc.



Name	Quantity
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	1 pcs.

### 2.3.2 Control panel „FLEXi“ SP3\_3E KIT

Name	Quantity
„FLEXi“ SP3_3E 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	1 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\_3E KITi

Name	Quantity
„FLEXi“ SP3_3E control panel board, built into metal housing	1 pc.
Metal housing K02 with Mean Well impulse power supply	1 pc.
Resistor 2,2 kΩ	20 pcs.
Resistor 4,7 kΩ	10 pcs.
Antenna ME301M with 2,5 m long cable	1 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:

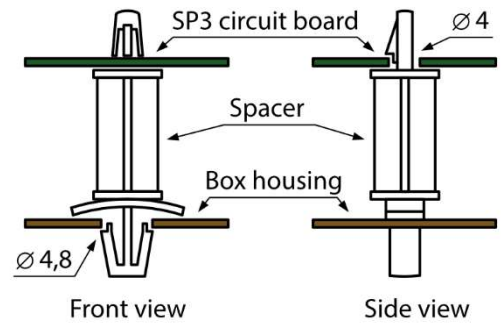
- Sketch a plan of the premises and mark the areas where the metal housing with the control panel, keypad (-s), signallers, equipment automatically or remotely controlled by the control panel will be installed.
- After evaluating the premises, the demands raised for their protection and the characteristics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

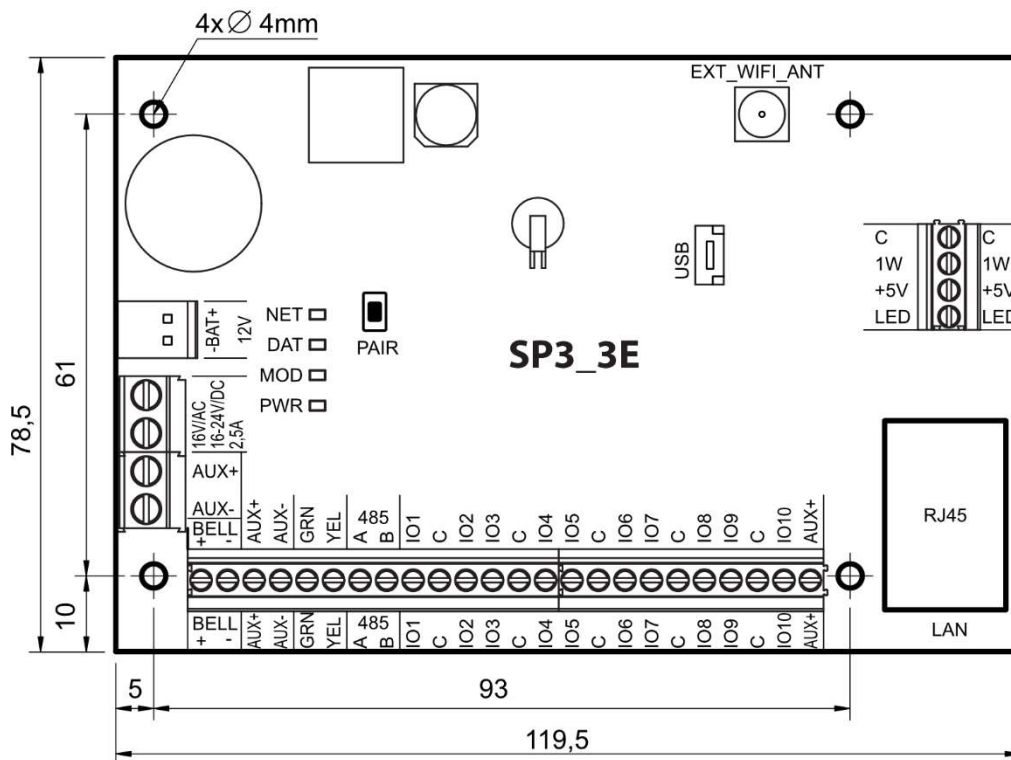
Install the control panel into the chosen plastic or metal housing using plastic spacers. If you chose a metal housing, do not forget to ground it during installation. The chosen housing must meet demands described in the EN 60950 and EN 50131 standards.



Plastic spacers.

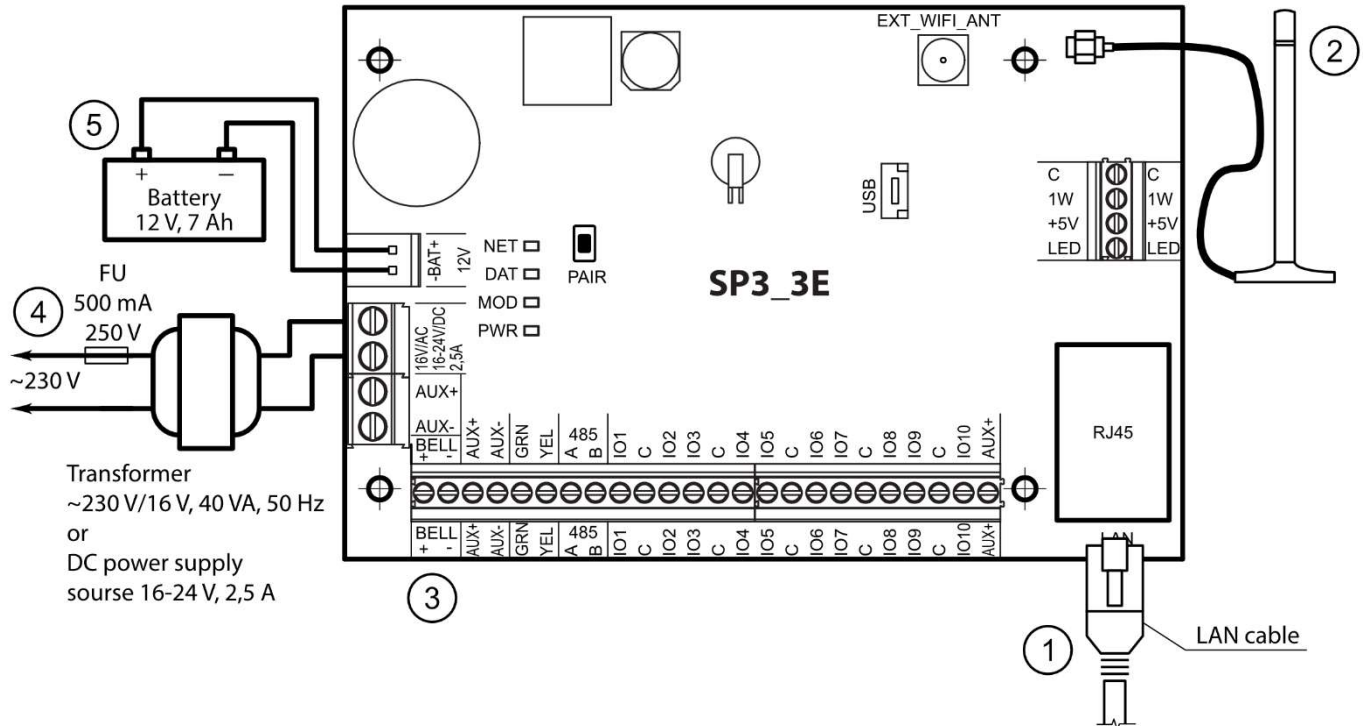
### Dimensions of the „FLEXi“ SP3\_3E board

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 the LAN cable.
2. Connect WiFi antenna to the antenna connector.
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\_3E 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 TrikidisConfig” 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 RFID tag. 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.

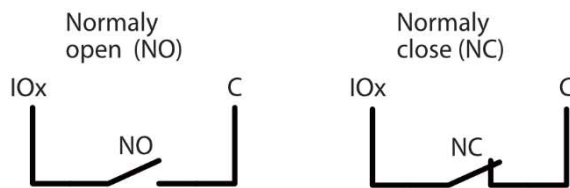


- c. **Reports to central monitoring station.** Sending reports to the central monitoring station is disabled by default. See chapter 5.3 “Reporting to CMS” window” on how to set parameters for sending messages to CMS.
  - d. **Reports to user.** Communication with *Protegeus* cloud is enabled by default. 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 by users whose e-mail addresses are entered into the User list. See chapter 5.4 “Users & Reporting” window”. With Protegeus, it is possible not only to Arm or Disarm the storage of all or only part of the rooms, but also to control (enable or disable) the equipment connected to the PGM outputs.
5. Additionally:
- a. **Changing control codes.** We recommend changing the panel’s default alarm control and configuration codes to something only You know.
    - The **Administrator code** can be changed in the **Access** section of the **System Options** branch of the program menu.
    - The **Installer code** can be changed in the **Access** section of the **System Options** branch of the program menu.
    - The **User code** can be changed in the **Users** section of the **Users & Reporting** branch of the program menu or with the control panel keypad.

### 3.2 Connecting sensors

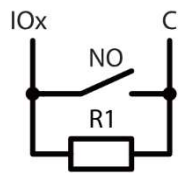
There are 10 terminals *IO1–IO10* (inputs) on the control panel board for connecting sensor circuits. The number of inputs can be expanded to 32 using input expanders (*iO, iO8, iO-WL, RF-SH*). Any terminal can be set as an input and assigned zone attributes: circuit type (NO, NC, EOL, EOL\_T, ATZ, ATZ\_T); 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”.

#### Schematics for connecting sensors.

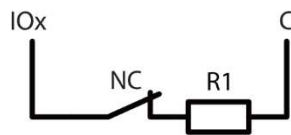


RT	R1	R2
2.2k	2.2k	4.7k
1k	1k	2.2k
5.6k	5.6k	3.3k
5.6k	3.3k	5.6k
3.3k	6.8k	3.3k
2.2k	4.7k	8.2k

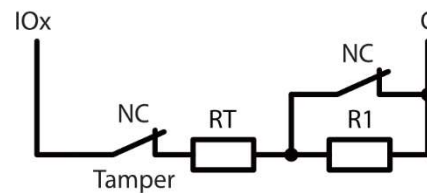
Normally open with End of line resistor (EOL)



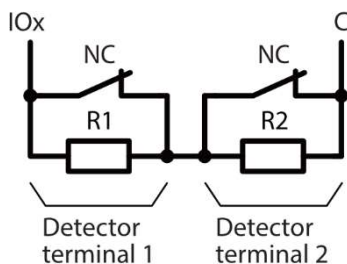
Normally closed with End of line resistor (EOL)



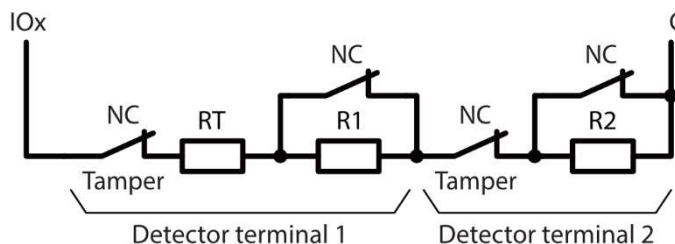
Normally closed with End of line resistor, with tamper and wire fault recognition (EOL\_T)



Normally closed without EOL (ATZ)



Normally closed with EOL, with tamper and wire fault recognition (ATZ\_T)

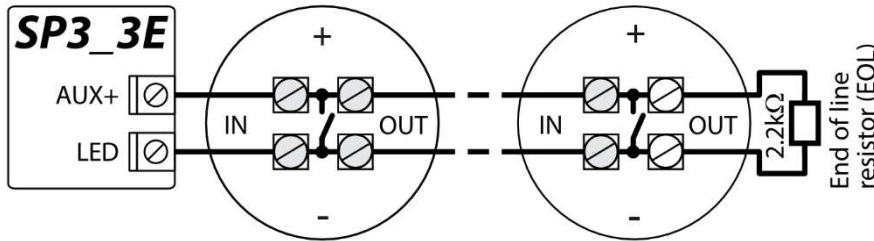




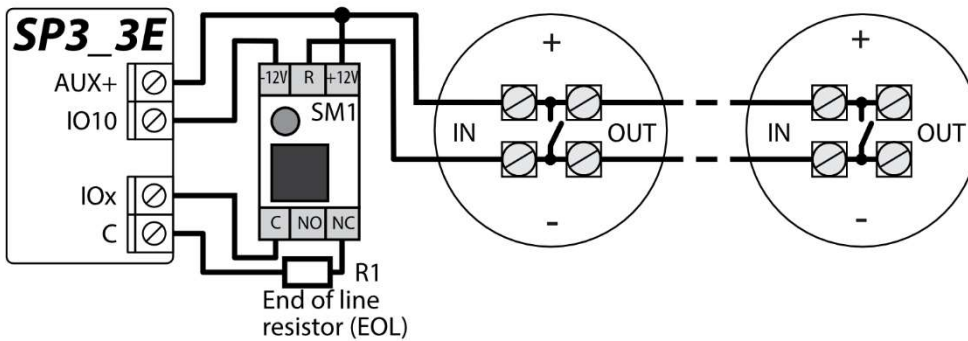
### 3.3 Connecting smoke detectors

Schematic for connecting two-wire smoke detectors.

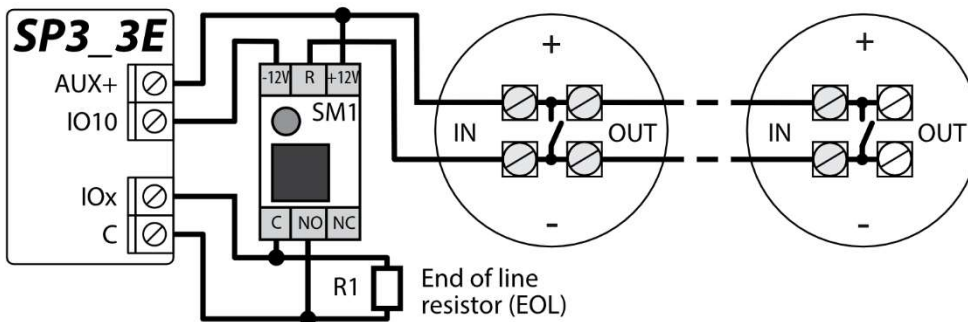
Schematic for connecting two-wire smoke detectors to PGM (LED) outputs. When using this scheme for connecting fire detectors, it is necessary to mark the "LED out as 2Wire fire" field with a tick (see chapter 5.2 "Window "System options""). The alarm current of the fire detector must be more than 10mA. Up to 8 fire detectors can be connected to the LED output.



Wiring diagrams for two-wire smoke detectors with relay module SM1. To connect a smoke detector circuit to a selected input (IOx), the input must be assigned the **Fire** zone function (see chapter 5.7 "Zones" window"). To connect a 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").

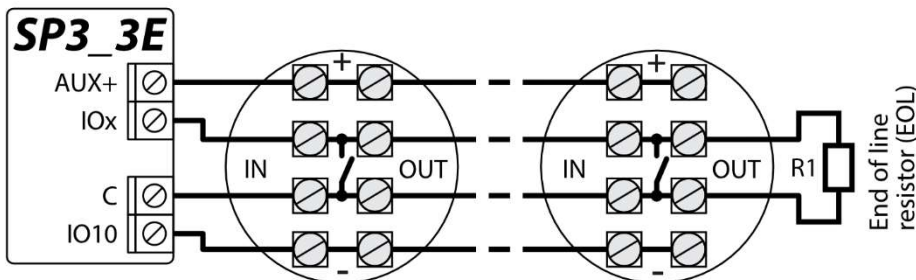


or



Schematic for connecting four-wire smoke detectors.

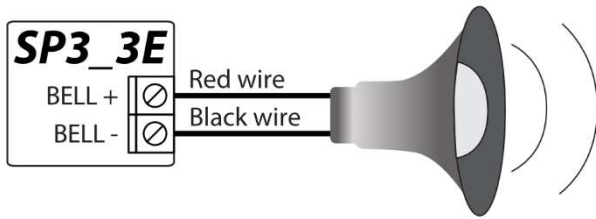
To connect a smoke detector circuit to a selected input (IOx), the input must be assigned the **Fire** zone function (see chapter 5.7 "Zones" window"). To connect a four-wire smoke detector circuit to a selected PGM output (IO10), the **Fire Sensor Reset** function must be assigned to the output (see chapter 5.8 "PGM" window").



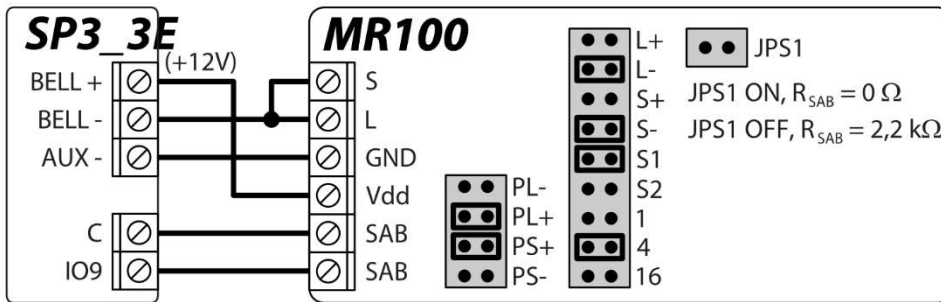




### 3.4 Schematic for connecting a siren



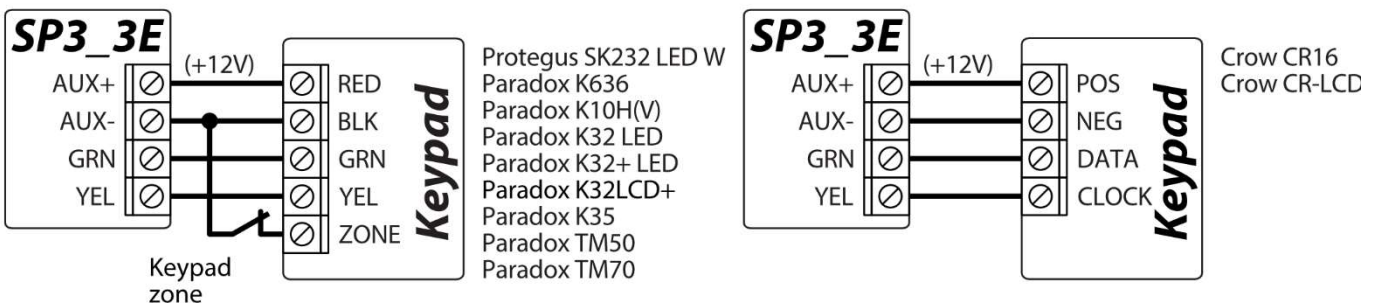
### Outdoor siren

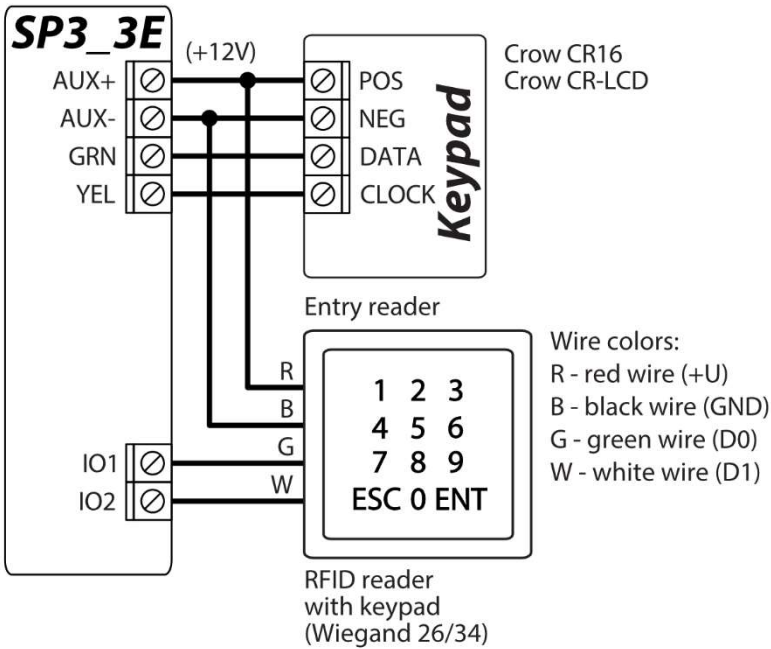
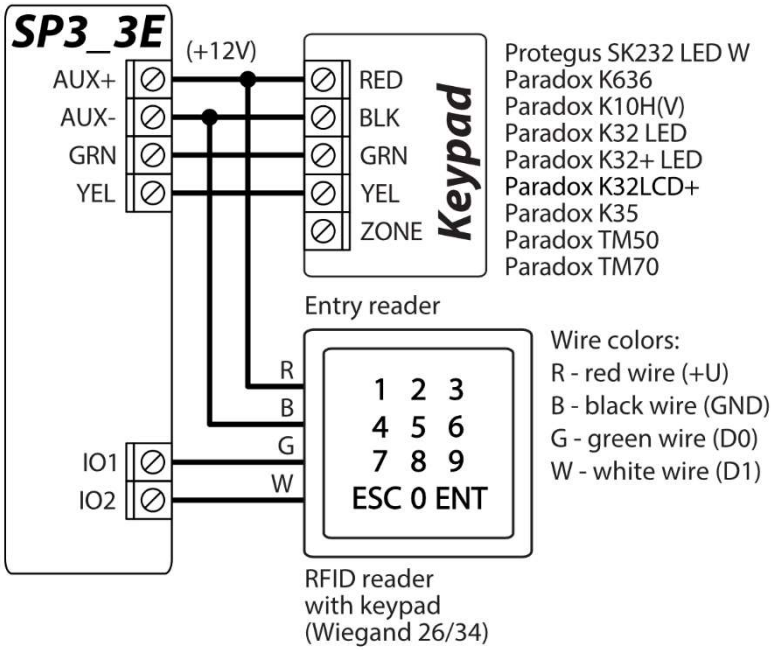


The diagram shows the connection and settings of the **MR100** outdoor siren. If the control panel will use a different method for monitoring the EOL (factory setting is 2.2 kOhm EOL) of the siren tamper (SAB terminals) circuit, it is necessary to close the JPS1 contacts and connect a resistor of the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

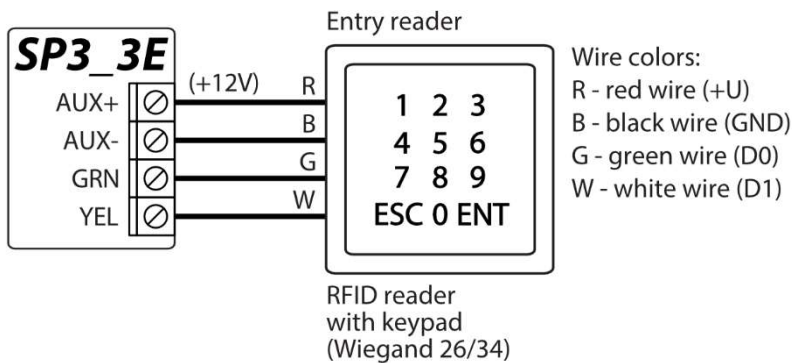
### 3.5 Schematics for connecting keypads and RFID readers (Wiegand 26/34)

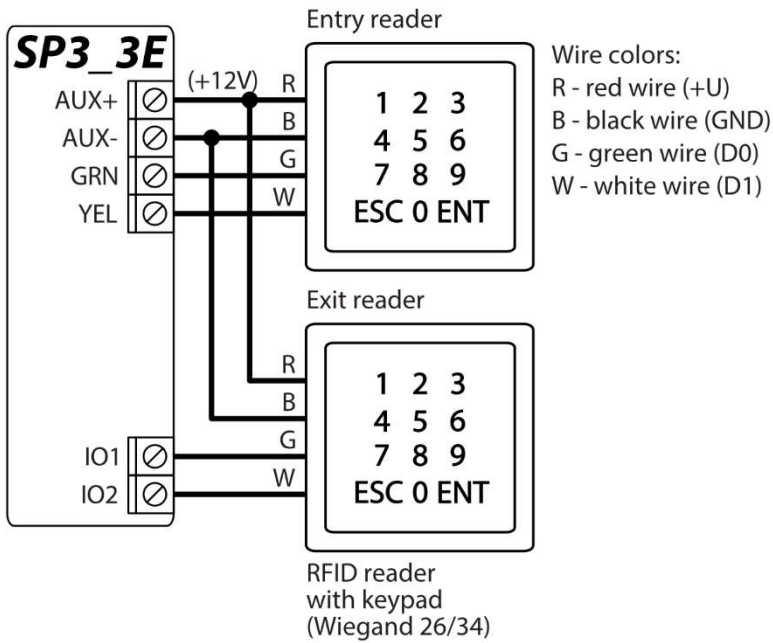
Up to 8 devices can be connected to the keypad data bus. The type of the connected keypad must be specified using TrikidisConfig software (see chapter 5.5 ““Modules” window”). The control panel will automatically recognize and link the connected devices.





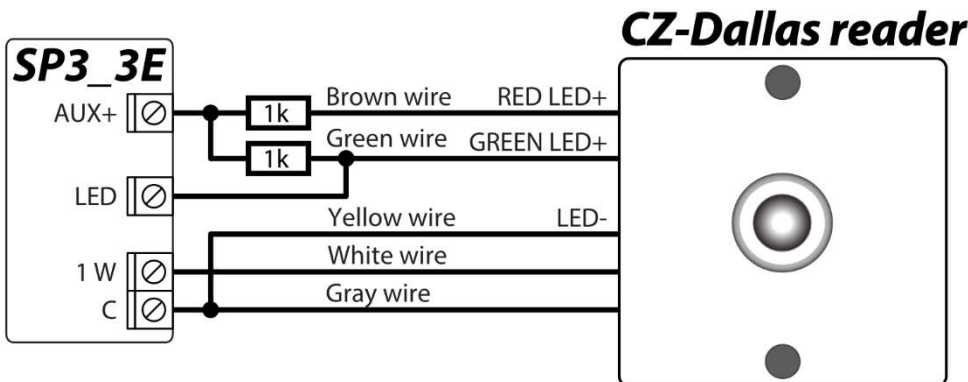
Up to 2 RFID readers can be connected to the control panel. If 2 RFID readers are connected to the control panel, the keypads cannot be connected.





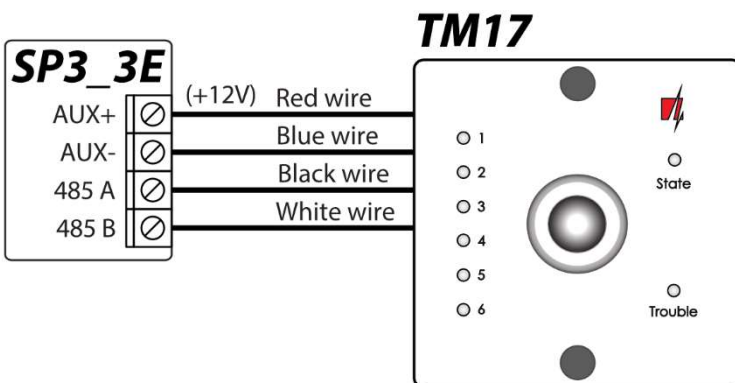
### 3.6 Schematics for connecting TM17, CZ-Dallas readers

The CZ-Dallas iButton key reader connects to the „FLEXi“ SP3\_3E using the “1 Wire” data bus. The length of the wires connecting to the data bus can be up to 30 m:



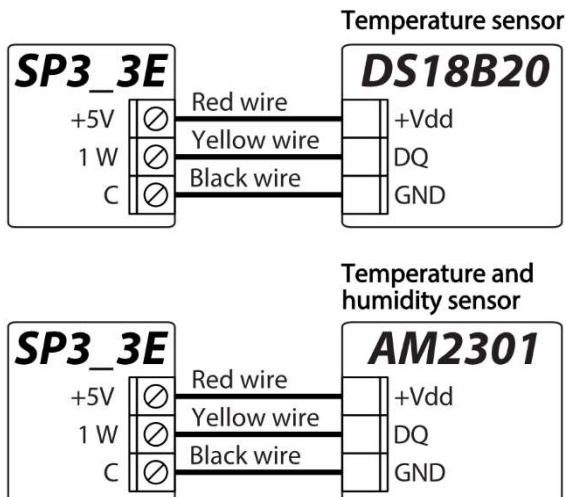
The output LED must be set to the "System state" type.  
Security alarm system is arm - the iButton reader light is red.  
Security alarm system is disarm - the iButton reader light is yellow.

The TM17 reader connects to the „FLEXi“ SP3\_3E using the RS485 data bus. The length of the wires connecting to the RS485 data bus can be up to 100 m.





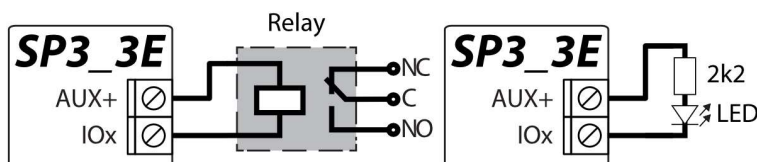
### 3.7 Schematic for connecting a temperature sensor



**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\_3E security 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)**.

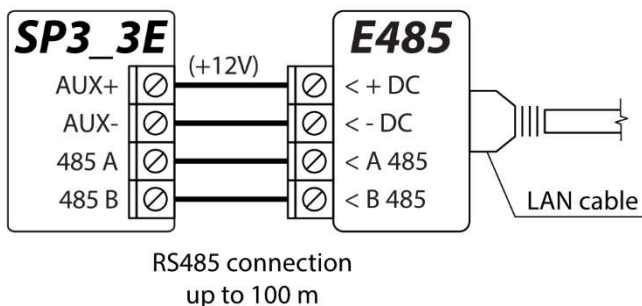
The +5V terminal on the board is for supplying devices connected to the 1-Wire data bus with 5 V DC voltage. The maximum output current is 0,2 A. The output is protected from overload. If the maximum allowed current is exceeded, the power will automatically be switched off. The control panel automatically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

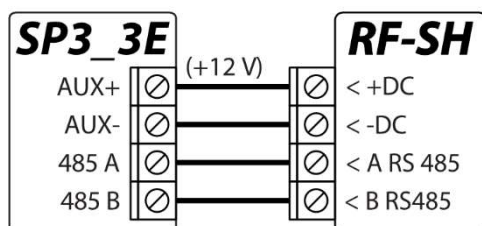


When the **E485** module is connected to the control panel, you will have a second wired internet connection channel. Module **E485** allows the control panel to send and receive control commands via a wired Internet connection. When the **E485** module is connected to the control panel, messages are sent to the CSP and to the **Proteagus** mobile application via wired Internet networks.

See chapter 5.3 "Reporting to CMS" window" on how to choose connectivity priority (Ethernet (LAN), WiFi, E485 (LAN)). The „FLEXi“ SP3\_3E's configuration for the **E485** Ethernet module is described in chapter 5.5. "Modules" window".

If the connection is lost on the **Primary** communication channel, the messages are transmitted to the CSP via the **Backup** communication channel. If the **Backup** communication channel is also interrupted, the messages are transmitted via the **Backup 2** communication channel. When the **Primary** communication channel is restored, messages will be sent to the CSP via the **Primary** communication channel.

### 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\_3E's configuration for expander modules is described in chapter 5.5 "Modules" window".

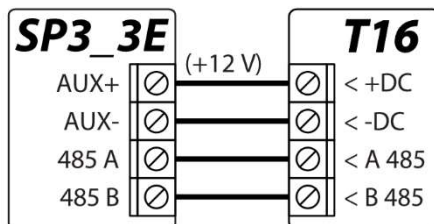


### 3.11 Schematics for connecting iO series expander modules

If the security control panel „FLEXi“ SP3\_3E needs to have more inputs IN or outputs OUT, connect a wired or wireless TRIKDIS iO series input and output expander. The „FLEXi“ SP3\_3E's configuration for expander modules is described in chapter 5.5 ““Modules” window”.



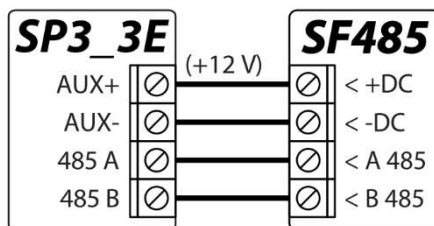
### 3.12 Schematics for connecting RF transmitter T16



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 **Protegas** mobile app, 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 2 times – the green color indicates that the control panel is successfully registered on the WiFi network, while the number of yellow flashes indicate the mobile signal strength.

**Note:** Sufficient WiFi network strength is 2 (two yellow flashes of the “NET” indicator). If you see fewer yellow flashes of the “NET” diode, the strength of the WiFi 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 WiFi 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\_3E indicator lights are off, check the power supply and connections.

## 4 Remote control

### 4.1 Linking the „FLEXi“ SP3\_3E to a user's Protegas account

With **Protegas**, 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 **Protegeus** cloud account, open the page [www.protegeus.eu/login](http://www.protegeus.eu/login) 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 **Protegeus** mobile app into your smartphone.



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

**IMPORTANT:** When adding the „FLEXi“ SP3\_3E to **Protegeus**:

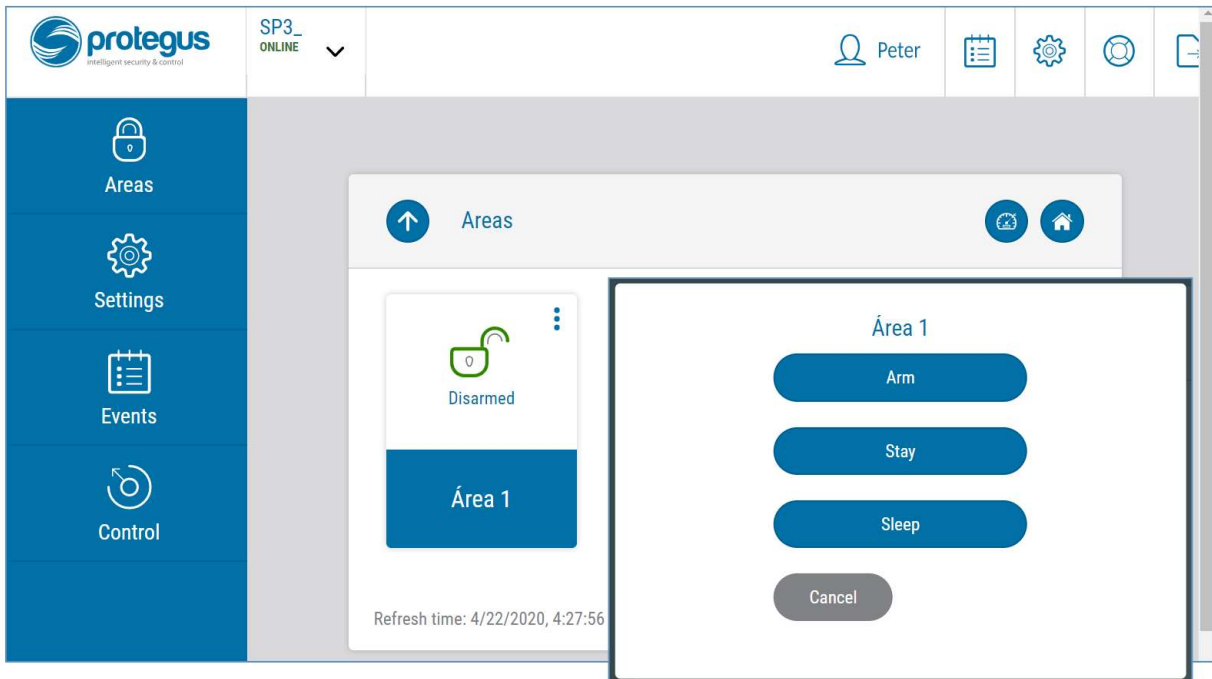
1. LAN cable connected to the control panel;
2. **Protegeus cloud** service must be enabled. See chapter 5.4 “Users & Reporting” (**Protegeus** tab);
3. The power must be switched on (“PWR” LED must be green solid);
4. Must be connected to network WiFi/LAN (“NET” LED must be green solid when connected to WiFi network; and/or “MOD” LED must be green solid when connected to LAN network).

5. Click **Add new system** and enter the „FLEXi“ SP3\_3E’s “Unique ID” number (MAC address) . You can find it on the packaging sticker. After entering the ID, click “Next”.



## 4.2 Arming/disarming the system using **Protegeus**

1. To control the system, go to the **Protegeus** window “Areas”.
2. Click on an area button in the “Areas” window. In the new window, choose an action (arm or disarm the area of the security system). If prompted, enter your personal alarm arm/disarm keypad code.



3. If the program does not respond to Your commands or the program window views are entirely different, go to **Settings** -> **System information** -> and click the button “**Re-read system config**”.

## 5 Setting parameters using TrikdisConfig software

1. Download the configuration software **TrikdisConfig** from [www.trikdis.com/](http://www.trikdis.com/) (enter “TrikdisConfig” in the search field) and install it.
2. Connect the „FLEXi“ SP3\_3E to a computer using a USB Mini-B cable.  
**Note:** If you connect the „FLEXi“ SP3\_3E to a computer using a USB cable while it is powered on and operating, the „FLEXi“ SP3\_3E 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\_3E configuration window.
4. Click **Read [F4]** to see current „FLEXi“ SP3\_3E parameters. If a pop-up window appears, enter the *administrator* or *installer* code.

### 5.1 Description of TrikdisConfig status bar

When the „FLEXi“ SP3\_3E is connected, **TrikdisConfig** will show information about the connected device in the status bar.

IMEI/Unique ID: 840D8E880587							
Status: reading done	Device: SP3_3E00	SN: 000002	BL: 1.00	FW: 1.10	HW:	State USB	Role: Administrator

Name	Description
IMEI/Unique ID	MAC address of the device
Status	Operational status
Device	Device type (must show <b>SP3_3Exx</b> )
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)



Name	Description
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\_3E. With *TrikdisConfig*, alter the desired settings according to the program window descriptions given below.

## 5.2 “System Options” window

### “System general” tab

### 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** – enter the name of the object (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.
- **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 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.
- **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 for 2Wire fire sensor** - check the box when you connect the two-wire fire detector to the LED output.

### 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.

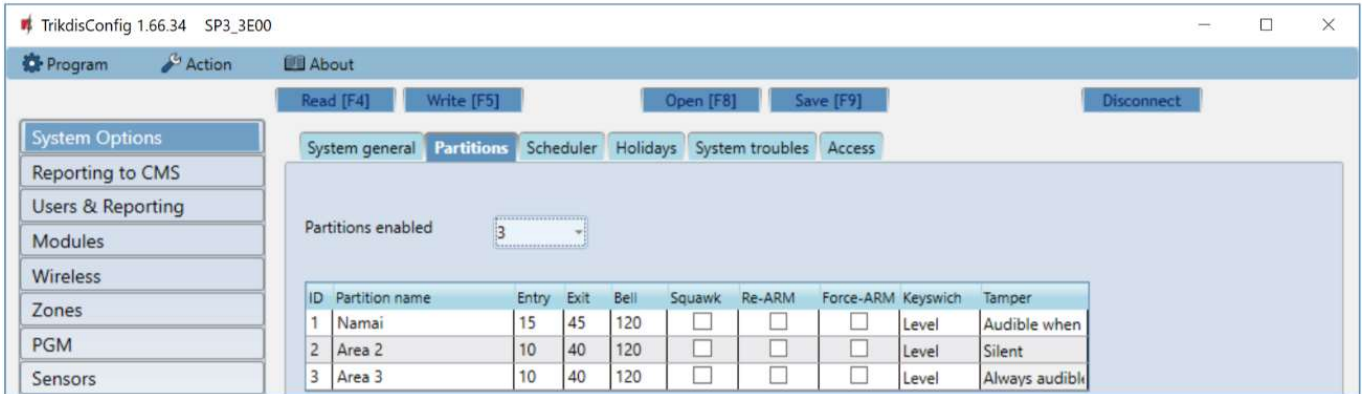
- **Time zone (hours)** – specify your country’s time zone. For example, if the control panel will be installed in Lithuania, enter **+3**.





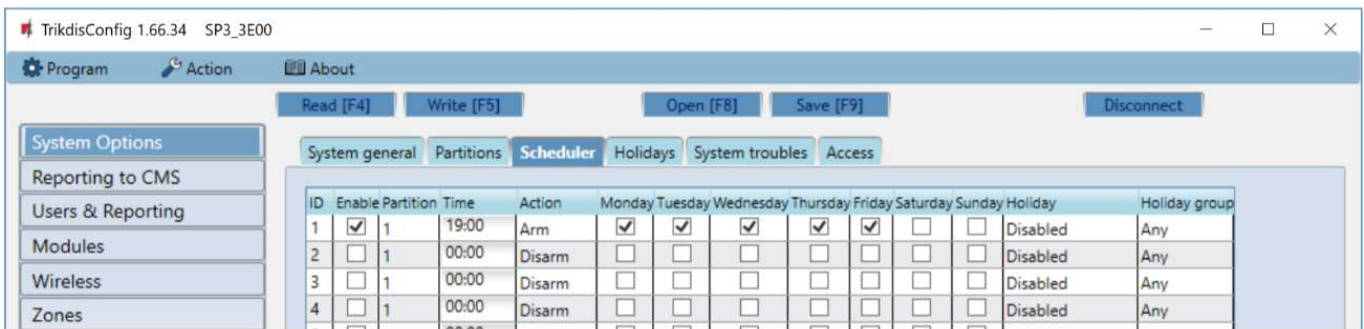
- **Time set** – specify a server to synchronize the „FLEXi“ SP3\_3E’s internal clock with. Synchronization occurs after the control panel is powered on.
- **Daylight time** – if you check the box, the control panel's internal clock will be automatically switched to summer or winter time.
- **AC failure 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** – 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 **Protegeus** 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 switch on even when the alarm system is disarmed.

“Scheduler” tab

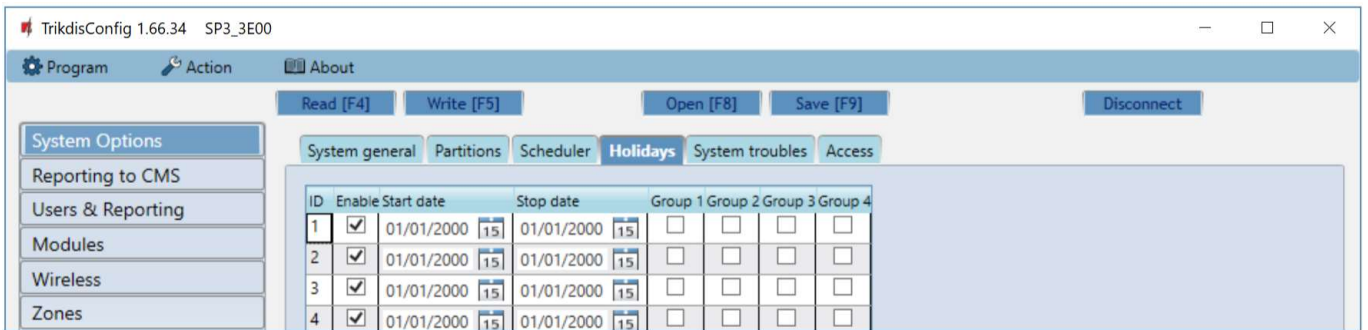


In this table, you can arrange scenarios for automatically arming and disarming the security system by choosing different days of the week and including public holidays.



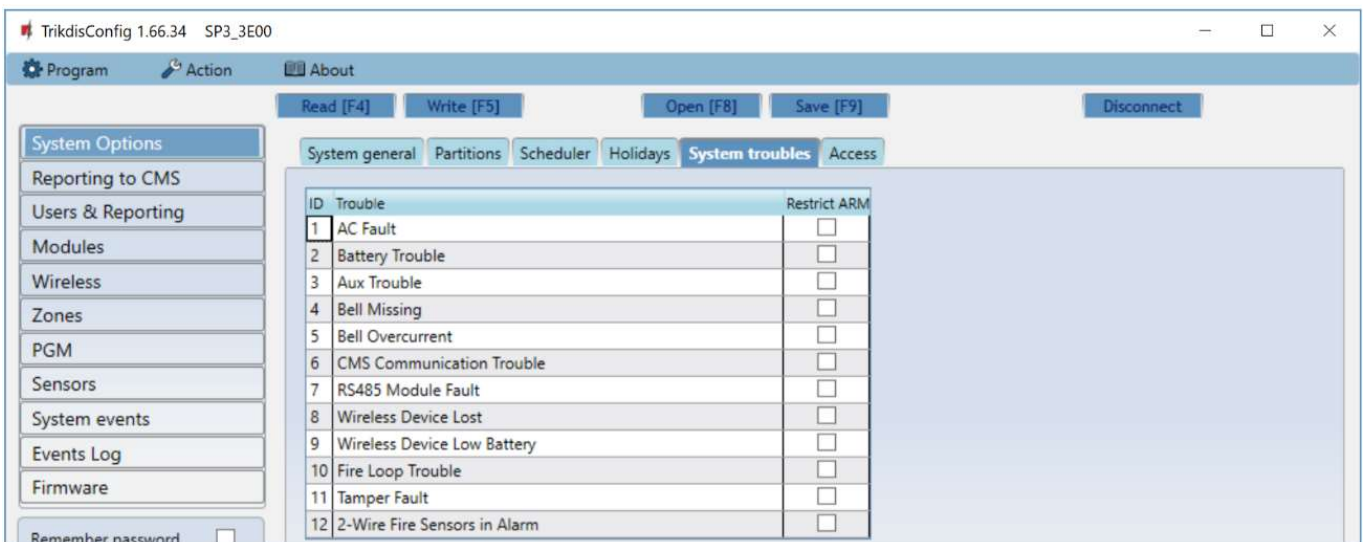
- **Enable** – enable the schedule for when the system will automatically arm and disarm.
- **Partition** – specify the partition affected by the specific schedule.
- **Time** – set the time when the specific action must be done.
- **Action** – set the protection mode (Disarm/Arm/Sleep/Stay) that the 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



- **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.

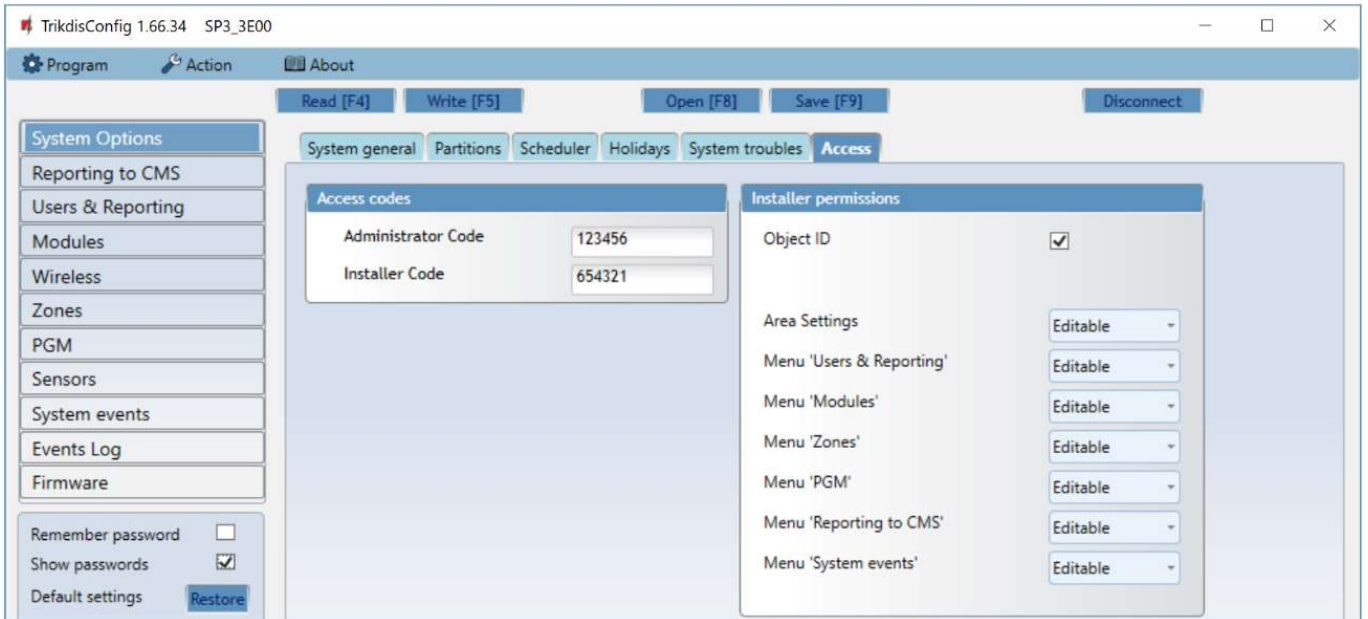
„System troubles“ tab



If at least one control panel internal malfunction field is checked, the control panel cannot be armed.



### “Access” tab



#### 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).
- **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.

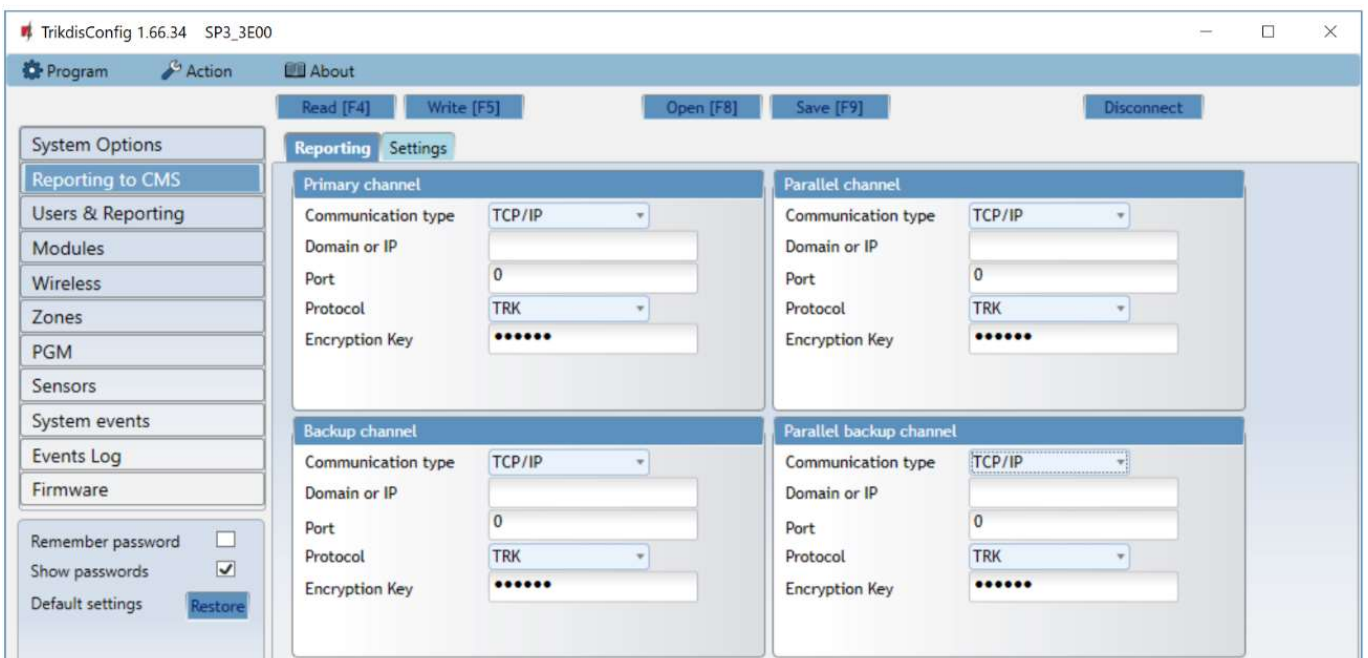
**Note:** If the default *administrator code* is set (123456), after pressing **Read [F4]** the program will immediately show the current operational parameters of the device without asking for the code.

#### Settings group “Installer permissions”

- Specifies the installer’s permissions.

## 5.3 “Reporting to CMS” window

### “Reporting” tab





### Settings groups “Primary channel” and “Backup channel”

- **Communication type** – choose a protocol for communicating with the receiver (TCP/IP, UDP/IP).
- **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 TrikiDis receivers, **SIA DC-09** for IP receivers capable of receiving event reports transmitted in SIA DC-09 protocols.
- **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

### Settings group “Settings”

- **Return to primary after** – time period after which the „FLEXi“ SP3\_3E will attempt to regain connection using the *primary* channel, in minutes.
- **IP Ping period** – period for sending PING signals for checking connectivity, in seconds. To enable these signals, tick the box.
- **LAN trouble indication** – check the box so that the LED on the control panel lights up when the LAN communication link fails.
- **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.

### Settings group “Reporting mode”

For setting parameters on how the control panel will communicate with the CMS channels and with **Protegeus**. The connection types are specified in order. If the control panel fails to connect using the first connection type, it switches to the second one, 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 (Ethernet (LAN), WiFi, LAN (RS485)) with the CMS receiver and **Protegeus**.



- **Backup type** – select a connection type (Ethernet (LAN), WiFi, LAN (RS485)) with the CMS receiver and **Proteagus**.
- **Backup type 2** – select a connection type (Ethernet (LAN), WiFi, LAN (RS485)) with the CMS receiver and **Proteagus**.
- **Radio T16 (RS45)** – 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 (Ethernet (LAN), WiFi, LAN (RS485)) 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\_3E will attempt to regain connection using the **Primary** channel, if it was running a **Backup** channel, min.

**Settings group “WiFi network parameters”**

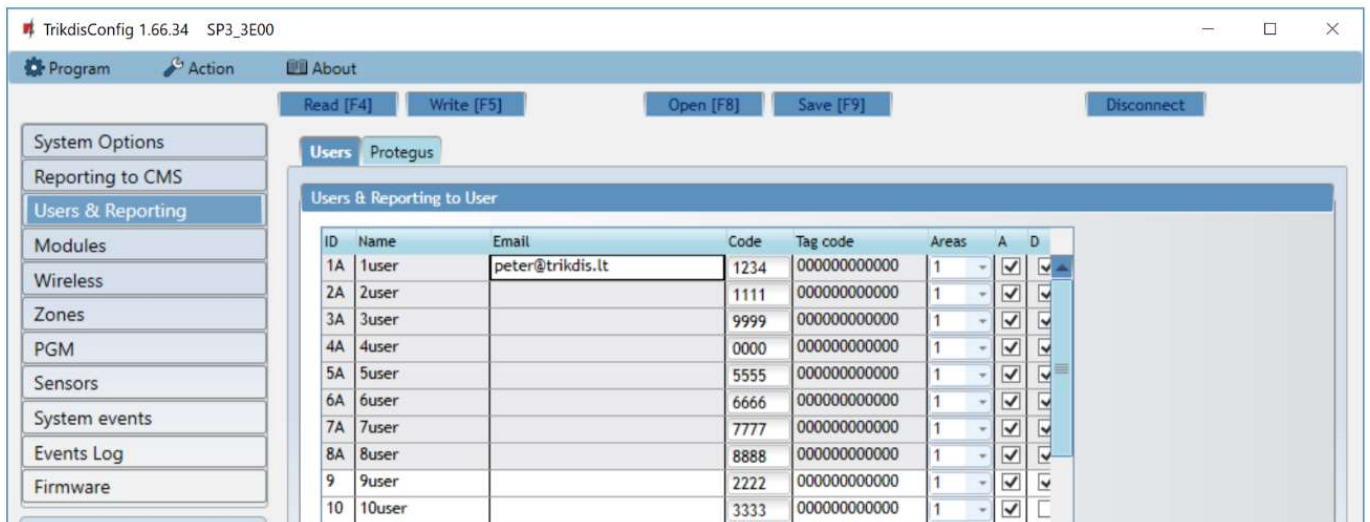
- **DHCP mode** – mode for registering on the WiFi network (manual or automatic). Tick the box and the „FLEXi“ SP3\_3E control panel will automatically read the network settings (subnet mask, gateway) and will automatically be assigned an IP address (automatic registration mode).
- **Static IP** – static IP address for manual registration mode.
- **Subnet mask** – subnet mask for manual registration mode.
- **Default gateway** – gateway for manual registration mode.
- **WiFi SSID name** – name of the WiFi network (that the „FLEXi“ SP3\_3E control panel will connect to).
- **WiFi SSID password** – WiFi network password.

**Settings group “LAN network parameters”**

- **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.

## 5.4 “Users & Reporting” window

“Users” tab



**Settings group “Users & Reporting to User”**

- **Name** – name of the user. These names will be used in event messages.
- **Email** – enter the user’s email, so that the user would be invited to **Proteagus** 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 key fob (card), 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 security system.
- **D** – tick the box if you want to allow the user to DISARM the security system.



### 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.

#### “Proteagus” tab



#### Settings group “PROTEGUS cloud”

- **Enable cloud service** – enable *Proteagus cloud* service, the „FLEXi“ SP3\_3E will be able to exchange data with *Proteagus* 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 *Proteagus*. Reports will only be sent to *Proteagus* and to users after they’ve been sent to the security company.



- **Cloud access code** – 6-digit code for connecting with *Protegeus*.

## 5.5 “Modules” window

### “Keypads” tab

The screenshot shows the TrikdisConfig 1.66.34 SP3\_3E00 software interface. The 'Keypads' tab is selected, displaying a table of RS485 modules and a 'Keypad parameters' panel.

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

The 'Keypad parameters' panel includes the following settings:

- Keypad type: Paradox/Protegeu
- Additional Wiegand on 1IO/2IO:
- Duress code type: Higher last digit
- Quick ARM:
- Incorrect codes until lockout: 3
- Lockout timer: 1 min
- Panic alarm type: Audible
- Medical alarm type: Audible
- Fire alarm type: Audible

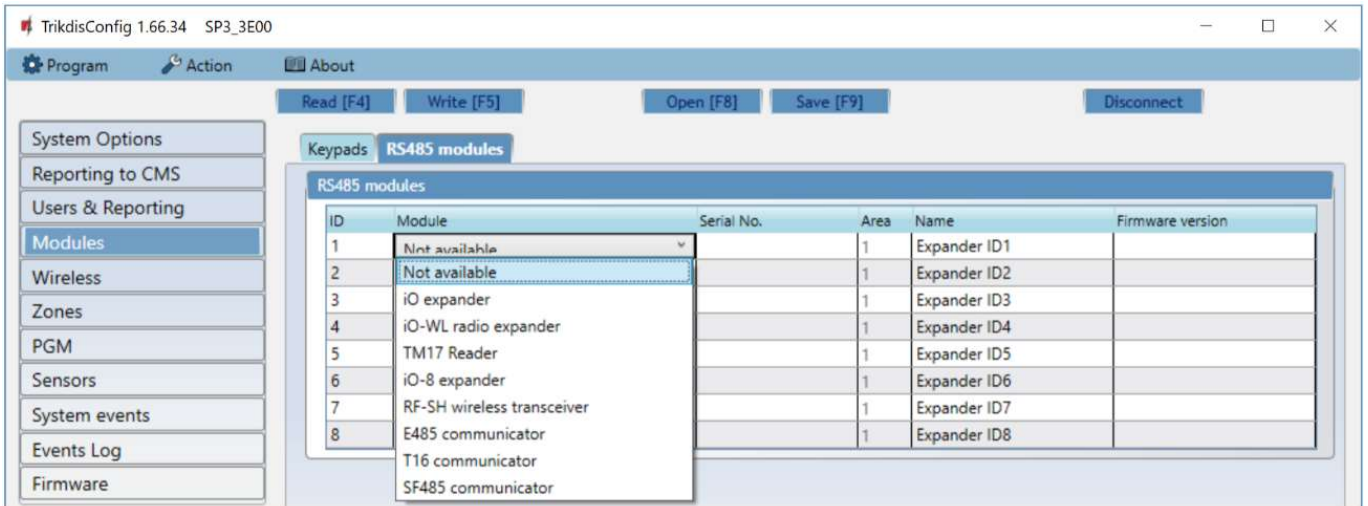
- **Serial** – the keypad’s serial number automatically detected by the control panel. To delete a keypad, enter zeros.
- **Keypad type** – keypad type, automatically detected by the control panel.
- **Remove** – pressing the button will remove the keypad from the list.

### Settings group “Keypad parameters”

- **Keypad type** – specify the keypad type (Crow CR Icon/LCD; Paradox/Protegeus; 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 *Protegeus* 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 *Protegeus* and the CMS, and the control panel will turn off the audible alarms. If set to **Disabled**, no alarm message is sent to *Protegeus* 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 *Protegeus* 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 *Protegeus* and the CMS, and the control panel will turn off the audible alarms. If set to **Disabled** alarm messages are not sent to *Protegeus* 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 *Protegeus* 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 *Protegeus* and the CMS, and the control panel will turn off the audible alarms. If set to **Disabled** alarm messages are not sent to *Protegeus* and CMS.



### “RS485 modules” tab



### 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*) 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\_3E finds the connected module, the version of its firmware will be shown.

### “E485 settings” tab



- **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



The „FLEXi“ SP3\_3E 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\_3E control panel

1. Connect the **RF-SH** transceiver and the „FLEXi“ SP3\_3E 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\_3E.
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\_3E and **RF-SH** to link together.
10. Connect a USB Mini-B cable to the „FLEXi“ SP3\_3E.
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\_3E.

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\_3E (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\_3E.
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.

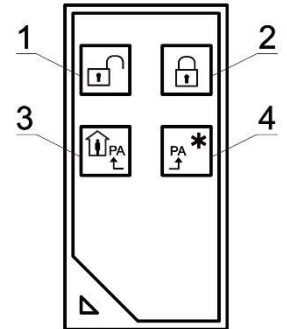


**Note:** To delete wireless sensors from the „FLEXi“ SP3\_3E's memory:

1. Connect a USB Mini-B cable to the „FLEXi“ SP3\_3E.
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\_3E'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\_3E (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\_3E.
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; Silent panic; Panic; PGM; PGM pulse).
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\_3E (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\_3E.
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\_3E (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\_3E.
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\_3E's memory:

1. Connect a USB Mini-B cable to the „FLEXi“ SP3\_3E.
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\_3E'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\_3E (see chapter 5.6.1 above).
2. Switch on the power supply.
3. Remove the top cover from the **RF-SH** transceiver.



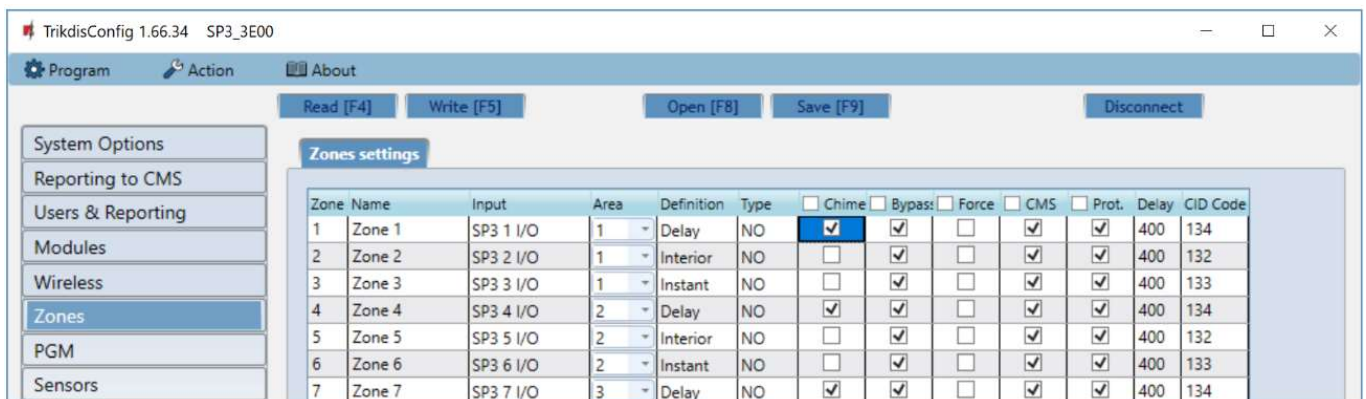
4. Hold down the **LEARN** button on the **RF-SH** module until the **LEARN** LED indicator starts blinking green.
5. Release the button.
6. The green blinking **LEARN** indicator means that the **RF-SH** is in wireless equipment linking mode.
7. Insert batteries into the keypad and wait for the green - 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\_3E**.
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\_3E**'s memory:

1. Connect a USB Mini-B cable to the „**FLEXi**“ **SP3\_3E**.
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\_3E**'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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	400	134
2	Zone 2	SP3 2 I/O	1	Interior	NO	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	400	132
3	Zone 3	SP3 3 I/O	1	Instant	NO	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	400	133
4	Zone 4	SP3 4 I/O	2	Delay	NO	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	400	134
5	Zone 5	SP3 5 I/O	2	Interior	NO	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	400	132
6	Zone 6	SP3 6 I/O	2	Instant	NO	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	400	133
7	Zone 7	SP3 7 I/O	3	Delay	NO	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	400	134

- **Zone No** – the zone's number on the list.
- **Name** - enter the name of the zone.
- **Input** – you can select which „**FLEXi**“ **SP3\_3E** 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 system 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 system is armed, a violation of the “Delay” zone starts the entry time counter, during which the alarm must be disarmed. If the alarm system 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 system 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 system 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 system 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 system 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).
- **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 **Protegeus** 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.



## 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	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	PGM 2	LED	1	System State	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	PGM 3	SP3 10 I/O		Remote Control	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	PGMas 4	SP3 9 I/O		Remote Control	10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	PGM 5	Disable		Remote Control	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	PGM 6	Disable		Remote Control	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7	PGM 7	Disable		Remote Control	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- **PGM No** – specifies the PGM output’s number on the list.
- **Name** - enter the name of the output.
- **PGM output** – assign the outputs OUT of the „FLEXi“ SP3\_3E 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 system is armed a line signal is generated, if it is triggered – a pulse type signal. The signal is cut off when the alarm system is disarmed.
  - **Thermostat** – this setting will make the PGM output operate in thermostat mode. A temperature sensor must be connected to the „FLEXi“ SP3\_3E. 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 **Protegas** cloud.

### “Set Action” tab

ID	Enable PGM No.	Action	Pulse Time, s	Factor	Factor No.	Start when	Set value
1	<input checked="" type="checkbox"/> PGM4 - SP3 9 I/O	Pulse ON	10	Zone (follow)	Zone No2 - SP3	Zone alarm	0
2	<input type="checkbox"/> N/A	PGM OFF	0	iButton	iButton1	N/A	0
3	<input type="checkbox"/> N/A	PGM OFF	0	iButton	iButton1	N/A	0
4	<input type="checkbox"/> N/A	PGM OFF	0	iButton	iButton1	N/A	0
5	<input type="checkbox"/> N/A	PGM OFF	0	iButton	iButton1	N/A	0
6	<input type="checkbox"/> N/A	PGM OFF	0	iButton	iButton1	N/A	0
7	<input type="checkbox"/> N/A	PGM OFF	0	iButton	iButton1	N/A	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, Schedule, Sensor lost, iButton, Arm, Disarm, Zone (follow), Stay, Sleep*) 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 selected condition in the **Factor** (Temperature) column, you can set a value (specify the voltage or temperature value) that will be used to control the PGM output.

### “Control” tab

Reader	EN	Code	PGM	PGM Mode	Area action
iButton	<input type="checkbox"/>	<input type="checkbox"/>	None	Pulse	None
Wiegand 1 (G/Y)	<input type="checkbox"/>	<input type="checkbox"/>	None	Pulse	None
Wiegand 2 (I/O)	<input type="checkbox"/>	<input type="checkbox"/>	None	Pulse	None

### Settings group “Entry/Exit control”

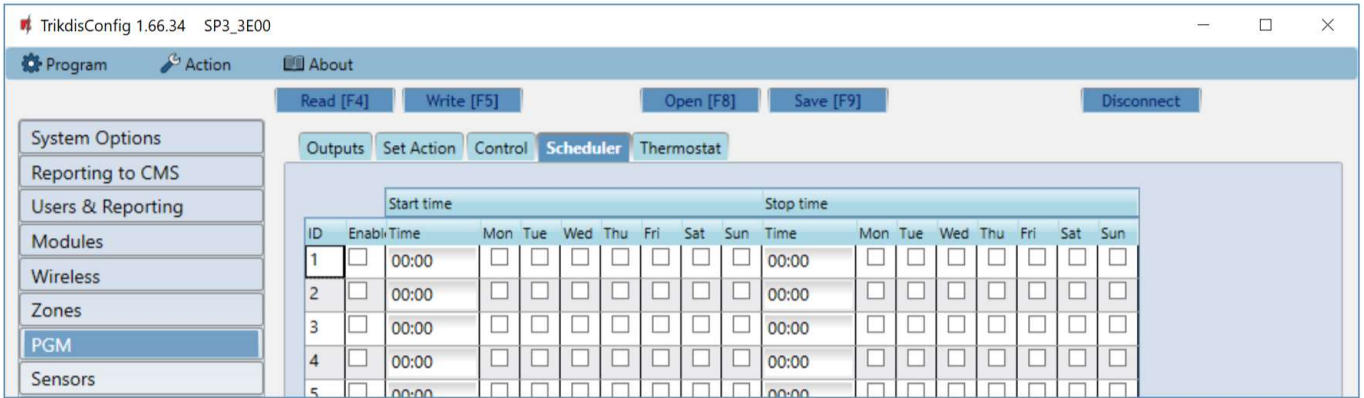
- **Reader** – the readers that can be connected to the security panel are indicated.
- **En** – check the box to enable the reader to control the PGM output.
- **Code** - check the box so that the reader can control the specified PGM output using the code.
- **PGM** – specify the PGM output that the 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 control 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**).

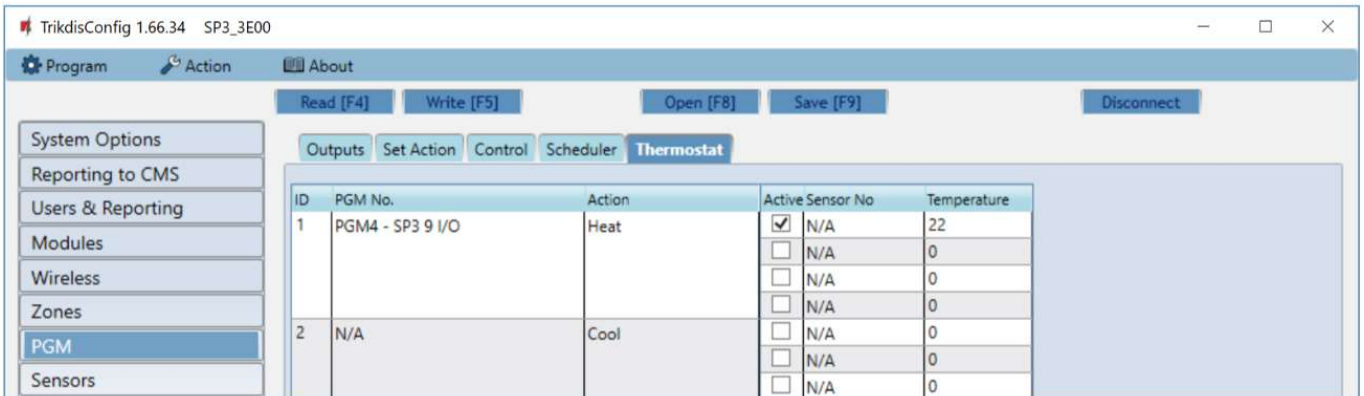


### “Scheduler” tab



- **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** – 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.





## 5.9 “Sensors” window

ID	Module type	Serial No.	Sensor name	Max	Min	High	Low
1	Disable	0000000000000000	Sensor 1	30	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Disable	0000000000000000	Sensor 2	30	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Disable	0000000000000000	Sensor 3	30	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Disable	0000000000000000	Sensor 4	30	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Disable	0000000000000000	Sensor 5	30	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Disable	0000000000000000	Sensor 6	30	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Disable	0000000000000000	Sensor 7	30	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Disable	0000000000000000	Sensor 8	30	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- **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 read by 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.
- **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
1	Low Battery	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	302
2	Periodic test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	602
3	Arm/Disarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	401
4	RS485 fault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	333
5	High temperature	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	158
6	Low temperature	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	159
7	Temp. sensor lost	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	380
8	GSM jamming	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	344
9	AC fault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	301
10	Partial ARM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	456
11	Zone Bypass	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	570

- **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 **Protegrus** cloud.
- **CID Code** – Contact ID code of the event.



## 5.11 “Events log” window

Event No.	Time	CID	Event definition
1049	2021-03-30 08:07:21	780:02:000	Output ON. OUT2
1048	2021-03-30 08:07:21	407:01:001	Remote Arm
1047	2021-03-29 17:03:52	302:01:000	Low Battery
1046	2021-03-29 17:00:40	305:00:016	System start
1045	2021-03-29 13:30:00	602:01:000	Periodic test
1044	2021-03-29 12:13:37	302:01:000	Low Battery
1043	2021-03-29 12:10:25	305:00:016	System start
1042	2021-03-29 12:10:25	306:00:001	Configuration changed
1041	2021-03-29 11:33:00	780:02:001	Output OFF. OUT2
1040	2021-03-29 11:33:00	401:01:000	System 1 disarmed. User No.0
1039	2021-03-29 11:32:19	780:02:000	Output ON. OUT2

- **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\_3E’s memory.

## 5.12 Restore default settings

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

## 5.13 Remote configuration

**Important:** Remote configuration will work only if:

1. **Protegeus cloud** is enabled. How to enable cloud is described in section **Klaida! Nerastas nuorodos šaltinis. Klaida! Nerastas nuorodos šaltinis.**;
2. Power supply is connected (“PWR” LED blinks green);
3. Registered to the network WiFi/LAN (“NET” and „MOD” LED illuminates green and blinks yellow).

1. Start the configuration program *TrikisConfig*.
2. In the field **Unique ID** enter the MAC number “FLEXi” SP3\_3E. The MAC number can be found on the device and the packaging sticker.

3. (Optional) in the **System name** field, enter the desired name for the “FLEXi” SP3\_3E with this **Unique ID**.
4. Press **Configure**.
5. In the newly opened window click **Read [F4]**. If required, enter the administrator or installer code. To save the password, select “Remember password”.
6. Set the necessary settings and when finished, click **Write [F5]**.



## 5.14 Updating firmware

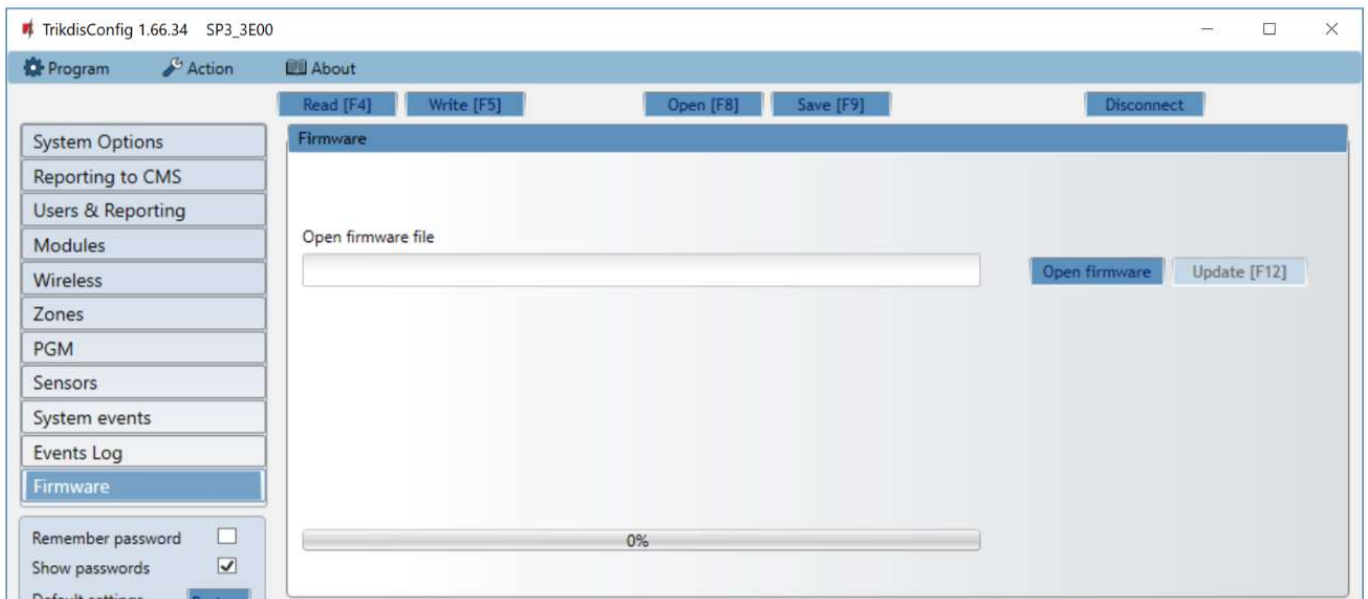
**Note:** After connecting the „FLEXi“ SP3\_3E to *TriKdisConfig*, the program will automatically offer to update the firmware if any updates are available. An internet connection is needed for this feature.

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\_3E's firmware can also be updated or changed manually. All prior settings of the „FLEXi“ SP3\_3E 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\_3E to a computer using a USB Mini-B cable or connect to the „FLEXi“ SP3\_3E remotely. If a newer version of firmware is available, the program will automatically offer to install it.
3. Open the *TriKdisConfig* window **Firmware**.



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\_3E downloads section of [www.trikdis.com](http://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.