mobilamb
TRIKDIS Official Distributor

CG17 alarm panel – installation and programming manual

Installation and programming manual for the Trikdis CG17 cellular alarm panel: wiring and SIM, detectors, outputs, expanders, setup in TrikdisConfig, reporting to the monitoring station, Protegus 2, SMS commands and control by phone call.



Edition: 2026-11-17
Always up-to-date web version: https://mobilamb.eu/cg17-manual

Contents

1. Overview

1.1 What it is for and how it works
1.2 Versions
1.3 Technical specifications
1.4 Parts of the panel
1.5 The terminals
1.6 LED indications
1.7 Tools you need for the installation

2. Quick setup

2.1 Setup for the Protegus 2 app
2.2 Setup for the monitoring station

3. Installation and wiring

3.1 Fixing and inserting the SIM card
3.2 Wiring the inputs
3.3 Wiring smoke detectors
3.4 Wiring a temperature sensor
3.5 Wiring a relay and an LED
3.6 Wiring iButton key readers
3.7 Wiring iO series expanders
3.8 Wiring a siren
3.9 The iO expander system (iO, iO-WL, iO-MOD)
3.10 Wiring a Strela fuel level sensor
Setting up and preparing the sensor
3.11 Wiring a battery
3.12 Connecting to an alarm panel
3.13 Measuring DC voltage
3.14 W485 Wi-Fi module
3.15 E485 Ethernet module
3.16 RF-LORA and LORA expanders

4. Control

4.1 Control from the Protegus 2 app
A rendszer létrehozása a Protegus 2 alkalmazásban
4.1.1 Arming and disarming
4.1.2 Adding more users
4.2 Control by SMS commands
4.3 Control by phone call

5. Setup with the TrikdisConfig software

5.1 The status bar
5.2 "System Options" page
5.2.1 System general tab
5.2.2 Access tab – access codes
5.3 "Reporting to CMS" page
5.4 "Users & Reporting" page
5.4.1 Registering touch keys (iButton)

5.4.2 Registering RFID cards
5.4.3 SMS answer texts tab – reply SMS messages
5.5 "Modules" page
5.5.1 W485 settings tab – Wi-Fi module
5.5.2 E485 settings tab – Ethernet module
5.5.3 Strela RS485 fuel level sensor
5.5.4 Internal modules tab – GPS module
5.6 "Zones" page
5.6.1 Zones settings tab – the zones
5.6.2 SMS & Call reporting tab
5.7 "PGM" page
5.7.1 Outputs tab – the outputs
5.7.2 Set Action tab – control on an event
5.7.3 Scheduler tab – scheduling
5.7.4 Thermostat tab – thermostat
5.7.5 SMS & Call reporting tab
5.8 "Sensors" page
5.9 "System events" page
5.9.1 Events tab – system events
5.9.2 SMS & Call reporting tab
5.10 "Events Log" page
5.11 Restoring the default settings
6. Remote programming
6.1 Setting the parameters remotely
6.2 Remote control from TrikdisConfig
7. Testing the installation
8. Firmware update
9. Safety instructions
See also

1. Overview

The **CG17** is an alarm panel with a built-in cellular communicator that can also be used on its own. It works as a full-featured alarm system, and it can also be used to remotely control the equipment around the house: garage door, garden gate, heating, cooling, irrigation system, lighting, ventilation. It sends the events both to the monitoring station and to the owner; the owner receives them in the **Protegus 2** mobile and web app.

The panel handles 12 wired and wireless zones, which you can group into 8 partitions. With the CG17 you can:

- install a simple alarm system that can be monitored and controlled remotely;
- remotely control various equipment (for example heating, ventilation, an automatic gate);
- monitor temperature, fuel level and DC voltage;
- notify users about events;
- send event messages to the receiver of the security company (monitoring station).



Figure 1. The CG17 alarm panel: the NETWORK, DATA, POWER and TROUBLE indicators on the front, the antenna connector at the top, the terminal blocks at the bottom.

1.1 What it is for and how it works

Messages to the monitoring station

- It sends the events to the Trikdis software and hardware receivers, which work with any monitoring software.
- It can also send event messages to SIA DC-09 receivers.
- It supervises the connection with test signals (polling) sent to the IP receiver every 30 seconds (or at the set interval).
- It has a backup channel: it uses this if the connection is lost on the primary channel.
- It can also report the events to the monitoring station by SMS. The SMS is sent even if data connection does not work in the mobile operator's network.
- If the Protegus service is enabled, the event first reaches the monitoring station, and only after that the users of the app.

Working with the Protegus 2 app

- Push notifications and notifications with a special sound about events.
- Remote arming and disarming of the system.
- Remote control of the connected equipment (lighting, gate, ventilation, heating, irrigation etc.).
- Remote temperature monitoring (with an iO, iO-WL or iO-LORA expander).
- Separate permissions for the administrator, the installer and the user.
- The users can also be notified about events by SMS and by phone call.

Notifying the users

- It calls the set phone numbers (up to 8 users).
- It sends SMS messages about the events.
- It sends push event notifications and notifications with a special sound to the Protegus 2 app.

Remote control of the system and the outputs

- from the Protegus 2 app;
- with an iButton (touch) key, through a key reader;
- with an RFID reader with keypad (Wiegand 26/34);
- by calling the phone number of the device;
- by SMS message;
- with an automatic "if... then" rule: for example, if an input is activated, or the temperature exceeds a limit, an output is switched on.

Expansion options

- iO and LORA series wired or wireless expanders, which increase the number of inputs (IN) and outputs (OUT).
- GPS receiver (useful for protecting ATMs and vending machines).
- Fuel level sensor – for protecting fuel tanks or monitoring the level.
- Backup power supply and charging of the 12 V battery.

Inputs and outputs

- 1 input, 2 outputs and 3 I/O terminals, which can be set as an input (IN) or a controllable output (OUT).
- One-wire data bus (1-Wire) for temperature sensors (up to 8) and an iButton key reader.
- The number of inputs (IN) or outputs (OUT) can be increased to 12 with iO series wired or wireless expanders.

Installation and setup

- Factory default settings for use as an alarm panel or as a communicator.
- The settings can be saved to a file and quickly written to other devices.
- Setup with a USB cable or remotely, with the TrikdisConfig software.
- Two access levels (account types): installer and administrator.

1.2 Versions

This manual applies to the CG17 with a 4G modem; its type codes: **CG17_14**, **CG17_1E** and **CG17_1S**. You see the exact type code in the **Device** field of the TrikdisConfig status bar (section 5.1).

Trikdis CG17 4G GSM compact security control panel

The version with a 2G modem (**CG17_12**) has been discontinued, so the manual gives only the data of the 4G version.

1.3 Technical specifications

Parameter	Value
4G (LTE) modem bands	Europe: LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28, GSM B2 / B3 / B5 / B8; Latin America: LTE-FDD B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66, GSM B2 / B3 / B5 / B8
Supply voltage [AC / DC]	16–24 V DC or 16–18 V AC
Current consumption	up to 50 mA in standby, briefly up to 200 mA when transmitting
Backup power supply [BAT]	12 V lead-acid battery
Battery charging current	up to 500 mA
Power supply for external devices [+12V]	12 V DC, up to 1 A
Dual-function terminals [IN/OUT]	3; as input NC, NO, EOL = 10 kΩ or EOL_T type, as output open collector (OC), up to 100 mA
Number of partitions	8
Number of zones	4 (can be increased to 12 with expanders)
Number of PGM outputs	2 (5 if you set the I/O terminals as outputs; can be increased to 12 with expanders)
Length of the 1-Wire bus [1 WIRE]	up to 30 m
Compatible temperature sensors	Maxim® / Dallas® DS18S20, DS18B20
Number of temperature sensors on the 1-Wire bus	up to 8
Compatible iButton keys [1 WIRE]	Maxim® / Dallas® DS1990A
Number of iButton keys	up to 12
Length of the RS485 bus	up to 100 m

Parameter	Value
Number of devices that can be connected to the RS485 bus	up to 8
Supported modules	**iO8** expansion module; **iO** expansion module; **iO-MOD** – iO-WL radio transceiver; **iO-WL** wireless expansion module; **E485** Ethernet module; **W485** Wi-Fi module; **TM17** iButton key reader; **CZ-Dallas** iButton key reader; **FLS** – Strela RS485 fuel level sensor; **iO-LORA** expansion module; **iO8-LORA** expansion module; **PB-LORA** panic button; **REL-LORA** expansion module
Memory for unsent events	60 events
Number of communication channels	2 (channel 1: primary and backup; channel 2: Protegus)
Internal clock	yes
Event sending	GPRS or 4G, SMS
Connection with the monitoring station	TCP/IP or UDP/IP, or SMS
Transmission protocols	TRK, encrypted SIA DC-09_2007, SIA DC-09_2012, SIA DC-09_IPcom
Operating environment	–10 … +50 °C; relative humidity up to 70 % between 0 … +40 °C (non-condensing)
Dimensions	113 × 70 × 25 mm
Weight	100 g

Discontinued accessory

Of the modules in the table, the **iO**, the **iO-WL**, the **iO-MOD**, the **TM17**, the **CZ-Dallas** and the **Strela RS485 (FLS)** are discontinued accessories and are no longer available; their description has been kept for existing systems.

The “up to … m” distances are theoretical maximums achievable under ideal conditions. In practice, the quality and routing of the cable, sources of interference and, for radio links, walls and terrain give a considerably shorter range. Plan with a margin, and on long runs check the connection during commissioning.

1.4 Parts of the panel

The numbers in the figure mark the parts of the panel: on the left the closed case, on the right the printed circuit board with the cover removed.



Figure 2. Parts of the CG17.

- 1 SMA connector for the cellular antenna
- 2 LED indicators
- 3 opening for removing the top cover
- 4 terminal blocks for the external wiring
- 5 USB Mini-B connector for programming the CG17
- 6 nano-SIM card holder

1.5 The terminals

The names of the terminals can be read on the cover, above the terminal blocks (from left to right).

Terminal	Purpose
AC/+DC	supply voltage: positive pole of 16–18 V AC or 16–24 V DC
AC/–DC	supply voltage: negative pole of 16–18 V AC or 16–24 V DC
BAT+	positive pole of the 12 V backup battery
BAT–	negative pole of the 12 V backup battery
+5V	5 V positive power terminal for the 1-Wire devices
1 WIRE	terminal of the 1-Wire data bus
A RS485	A terminal of the RS485 bus
B RS485	B terminal of the RS485 bus
1 IN	input 1 (default: **Delay** – delayed zone, EOL type)
2 I/O	input or output: input 2 or open-collector (OC) output (default: **Interior** – interior zone, EOL type)
COM	common negative terminal

Terminal	Purpose
3 I/O	input or output: input 3 or open-collector (OC) output (default: **Instant** – instant zone, EOL type)
4 I/O	input or output: input 4 or open-collector (OC) output (default: **Fire** – fire zone, EOL type)
+12V	12 V positive power terminal for external devices
5 OUT	open-collector (OC) output (default: **Fire sensor reset** – reset of the fire detectors)
6 OUT	open-collector (OC) output (default: **Siren** – siren)

1.6 LED indications

Indicator	Light	Meaning
NETWORK	green, steady	connected to the mobile network
	yellow blinking	mobile network signal strength with 0–5 blinks; 3 is already enough
DATA	green, steady	message being sent
	yellow, steady	there are unsent events in the memory
POWER	green blinking	the supply voltage is correct
	yellow blinking	the supply voltage is not correct
	green and yellow blinking	configuration mode
TROUBLE	off	no operating fault
	1 blink	no SIM card
	2 blinks	the PIN code of the SIM card is wrong
	3 blinks	cannot connect to the mobile network
	4 blinks	cannot connect to the IP receiver on the primary channel
	5 blinks	cannot connect to the IP receiver on the backup channel
	6 blinks	the internal clock of the CG17 is not set
	7 blinks	the voltage of the backup power supply (battery) is not sufficient
	8 blinks	no AC power supply
	9 blinks	fault in the connection with the RS485 module

The DATA LED is the simplest internet check. The DATA LED is lit when there is a message waiting to be sent in the device's memory. A green NETWORK LED only tells you that the network connection has been established – for a mobile network device, that it has registered on the operator's network; for an Ethernet device, that the connection up to the router is alive – but not that the device can also reach the internet. If the NETWORK LED is green but the DATA LED stays lit continuously even after an event or test report, the internet connection is not working: the message cannot be sent. On a mobile network the most common culprit is the APN or the data service of the SIM card; on Ethernet, the router, the firewall or the DNS. When the DATA LED goes out, the message has been sent and the data connection is fine.

1.7 Tools you need for the installation

Before you start the installation, check that you have all the necessary tools at hand; you can order the accessories from your dealer:

1. USB Mini-B cable for the setup (chapter 2);
2. flat screwdriver for opening the case (chapter 2);
3. screws for fixing the case (section 3.1);
4. an activated nano-SIM card that can make calls, send and receive SMS messages and use mobile internet (section 3.1);
5. power supply: 16–24 V DC or 16–18 V AC;
6. 12 V lead-acid battery, if you also use backup power.

The CG17 comes with an ANT01S cellular antenna as an accessory. If the signal is weak at the site, or the device is shielded by a metal box or a thick wall, use an antenna with a 2.5 m cable that can be mounted away from the device:

Trikdis ME301M magnetic antenna with 2,5m wire

Trikdis ANT04 GSM stick-on antenna with 2,5m wire

2. Quick setup

This chapter describes the settings with which the CG17 sends the events to the monitoring station (section 2.2), and the system can be controlled from the Protegus 2 app (section 2.1).

Az összes Trikdis eszköz egy közös szoftverrel programozható. A program neve TrikdisConfig és a gyártó honlapjáról letölthető.

TrikdisConfig Letöltés a trikdis.com oldalról.

Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

1. Open the case of the CG17 with a flat screwdriver as shown in the figure.



Figure 3. Removing the cover: insert the screwdriver into the opening on the side of the case, and snap the cover off by levering it downwards. Underneath, on the circuit board, is the USB Mini-B connector.

2. Connect the CG17 to the computer with a **USB Mini-B** cable.
3. Start TrikdisConfig. The program automatically recognizes the connected CG17 and opens its settings window.
4. Click the **Read [F4]** button: the program reads the settings of the CG17. If the program asks for it, enter the 6-digit administrator or installer code in the pop-up window.

Warning

While the device is connected to a computer via USB cable, it is in programming mode: its normal operation stops, it does not monitor, does not report, cannot be controlled, is powered from USB, and restarts once the cable is unplugged. Therefore the device must not be freely accessible: keep it in a closed metal enclosure with tamper protection or with a motion detector covering the enclosure. More in the FAQ

2.1 Setup for the Protegus 2 app

In the **SIM** group of the **System Options** page:



Figure 4. TrikdisConfig – **System Options**, **System general** tab, **SIM** group.

- 1 **SIM card PIN** – the PIN code of the SIM card
- 2 **APN** – the access point of the mobile internet

1. Enter the PIN code of the SIM card (**SIM card PIN**).
2. Enter the APN of your mobile operator in the **APN** field. You can find it on the operator's website; "internet" is universal and works in the networks of many operators. The data of operators in your country and in Europe: APN settings – list of European mobile operators.

In the **Cloud application** group of the **Users & Reporting** page:

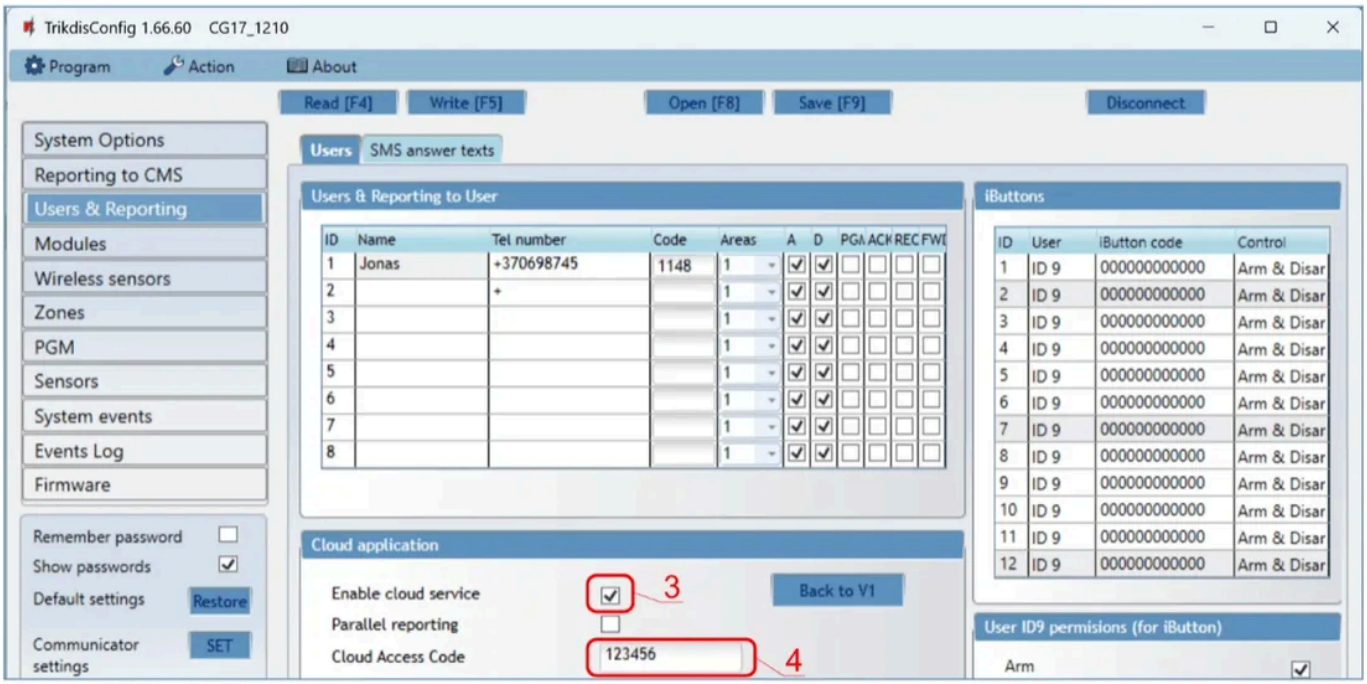


Figure 5. TrikdisConfig – **Users & Reporting**, **Cloud application** group.

- 3 **Enable cloud service** – switching on the Protegus cloud
- 4 **Cloud Access Code** – the access code of the cloud (default `123456`)

3. Tick the **Enable cloud service** checkbox: this switches on the connection with the Protegus cloud.

4. If you want the users to have to enter the code when adding the system to Protegus 2, change the value of the **Cloud Access Code** (default `123456`).

At the end of the settings, click the **Write [F5]** button and unplug the USB cable. Adding the system to the Protegus 2 app: section 4.1.

The other TrikdisConfig settings of the CG17 are described in chapter 5.

2.2 Setup for the monitoring station

The settings of the connection with the monitoring station on the **System Options** page:

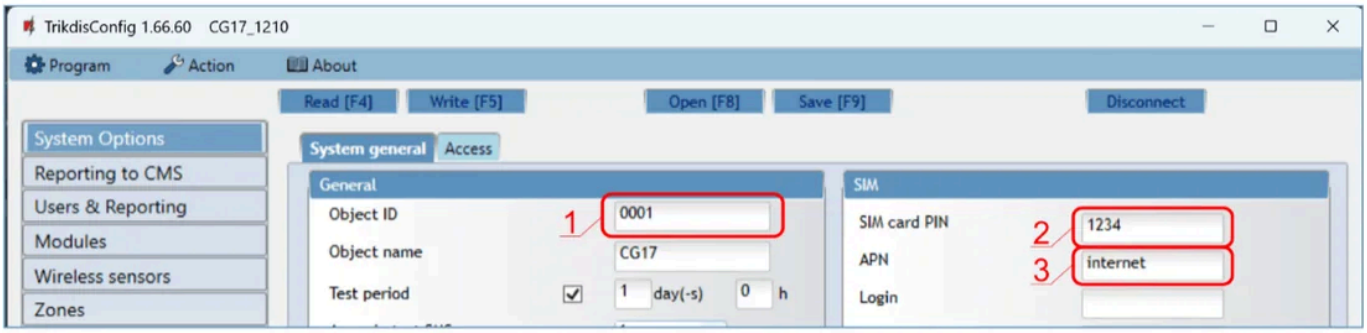


Figure 6. TrikdisConfig – **System Options**, **System general** tab.

- 1 **Object ID** – object identifier
- 2 **SIM card PIN** – the PIN code of the SIM card
- 3 **APN** – the access point of the mobile internet

1. Enter the object identifier (**Object ID**) received from the monitoring station: 4 characters, 0–9 and A–F. **Do not use the identifiers FFFE and FFFF.**
2. Enter the PIN code of the SIM card (**SIM card PIN**).
3. Enter the APN of your mobile operator in the **APN** field. You can find it on the operator's website; "internet" is universal and works in the networks of many operators.

The settings of the primary channel (**Primary channel**) on the **Reporting to CMS** page:

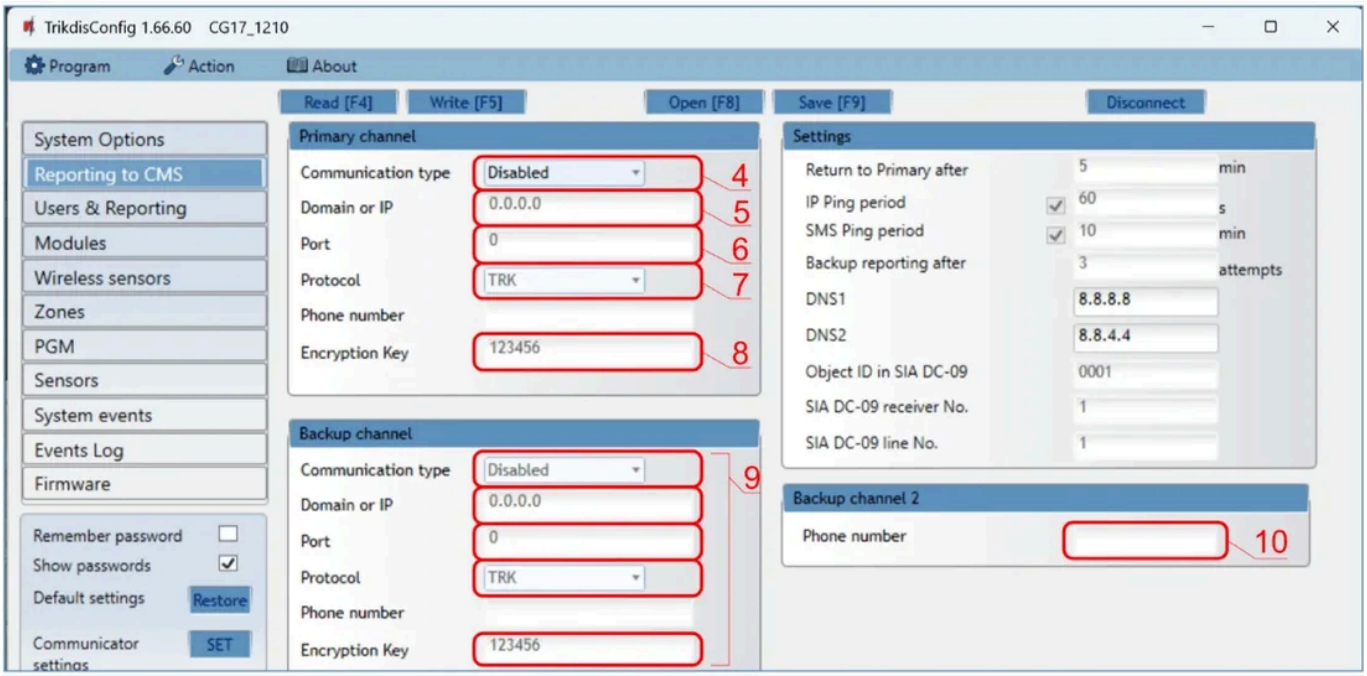


Figure 7. TrikdisConfig – **Reporting to CMS**.

- 4 **Communication type** – the type of the connection
- 5 **Domain or IP** – the address of the receiver
- 6 **Port** – the port of the receiver
- 7 **Protocol** – transmission protocol
- 8 **Encryption Key** – encryption key
- 9 **Backup channel** – the backup channel
- 10 **Backup channel 2** – the phone number of the SMS backup

4. **Communication type** – select the mode of the IP connection (**TCP/IP** or **UDP/IP**). We do not recommend SMS as the primary channel.
5. **Domain or IP** – enter the domain name or IP address of the receiver.
6. **Port** – enter the network port of the receiver.
7. **Protocol** – select the protocol of the event messages: **TRK** (for Trikdis receivers), **DC-09_2007**, **DC-09_2012** or **DC-09_IPcom** (for universal receivers).
8. **Encryption Key** – enter the encryption key set in the receiver.

If you report to the monitoring station by SMS, you only need to fill in the **Encryption Key** and **Phone number** fields. SMS messages are only received by Trikdis receivers: the **RL14** IP/SMS receiver, the **RM14** multi-channel receiver and the **GM14** SMS receiver. If you selected a **DC-09** protocol, also enter the object, line and receiver numbers in the **Settings** group of the **Reporting to CMS** page (section 5.3).

9. (Recommended) Set the backup channel (**Backup channel**).
10. (Recommended) Enter the phone number used for SMS reporting on **Backup channel 2**.

At the end of the settings, click the **Write [F5]** button and unplug the USB cable.

The other TrikdisConfig settings of the CG17 are described in chapter 5.

3. Installation and wiring

Figyelem!

Tilos a vezetékezést feszültség alatt álló eszközön elvégezni. A munka előtt a megfelelő áramtalanításról és érintésvédelemről (beleértve a szünetmentes működést biztosító akkumulátorokat) gondoskodni kell.

The chapter describes fixing the CG17 and inserting the SIM card, wiring the detectors, the outputs, the siren and the battery, and then connecting the key readers, the expanders and the communication modules (iO8, W485, E485, RF-LORA and iO-LORA). The purpose of the terminals is given in section 1.5. In the drawings, "x IN" or "INx" marks the selected input, "x OUT" or "xOUT" the selected output.

3.1 Fixing and inserting the SIM card

1. Before you start, check that the mobile network signal strength is sufficient at the planned location of the CG17.
2. Remove the top cover (snap it off with a flat screwdriver, as shown in the figure at the beginning of chapter 2), then pull off the terminal blocks.
3. Take the printed circuit board out of the box: press the retaining tab and lift it out.
4. Fix the back plate of the box at the desired place with screws.
5. Put back the printed circuit board and the terminal blocks.
6. Screw the cellular antenna onto the SMA connector (section 1.4).
7. Insert the nano-SIM card into the holder. The SIM card must be activated in the mobile network, and all necessary services must be enabled on it: it must be able to make calls, send and receive SMS messages and use mobile internet. Ask the mobile operator of the SIM card about enabling the services.

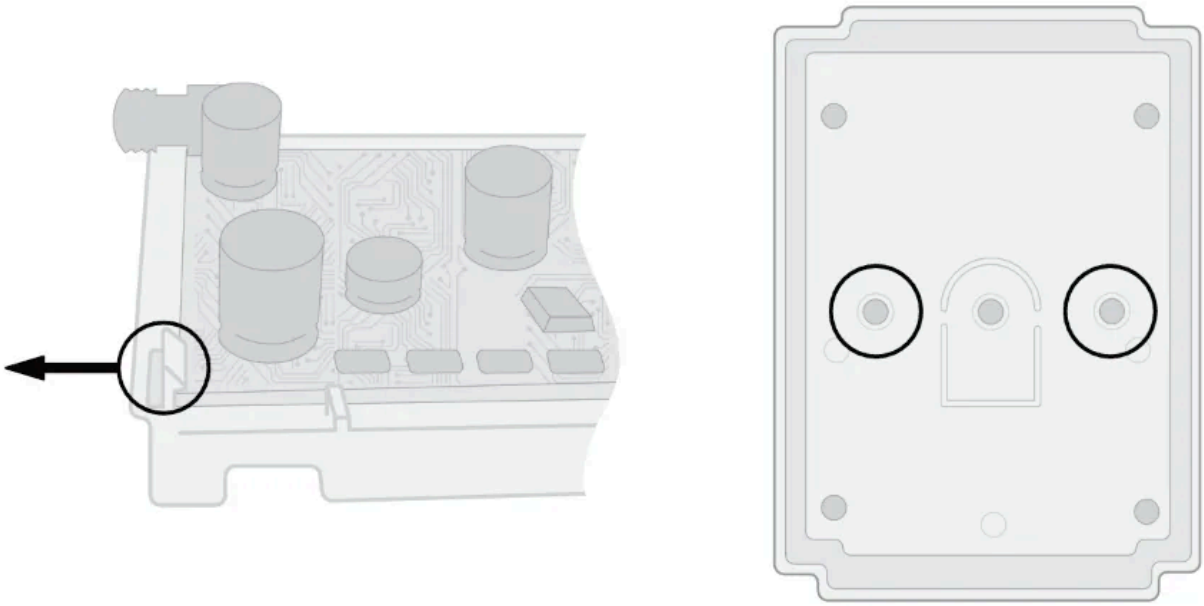


Figure 8. On the left the retaining tab of the printed circuit board (pressed in the direction of the arrow, the board is released), on the right the two screw holes of the back plate.

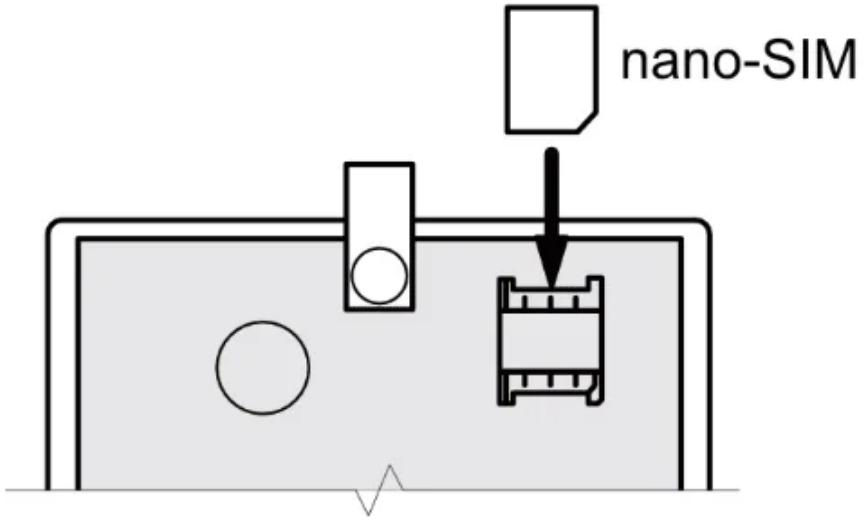


Figure 9. Inserting the nano-SIM card ("nano-SIM") in the direction of the arrow into the holder on the printed circuit board.

Check that the SIM card is activated. If you also connect over an IP channel (mobile internet), the mobile internet service must be enabled. If you do not want to enter the PIN code in TrikdisConfig, put the SIM card into a mobile phone and switch off the PIN code request on it.

8. If you also want to set up the CG17 remotely, insert a SIM card on which the PIN code request is switched off, then send this SMS to the phone number of the CG17: `CONNECT 123456 PROTEGUS=ON,APN=INTERNET`. 123456 is the default administrator SMS password (**SMS password**, section 5.2), `PROTEGUS=ON` switches on the Protegus cloud service, `APN=INTERNET` is the access point of the mobile internet (if your operator's is different, enter that). The SMS commands are described in section 4.2.
9. Remote setup is described in section 6.1.
10. Put back the top cover.

The terminal blocks can be pulled off: by pulling off the terminal block carrying the power terminals (**AC/+DC**, **AC/−DC**, **BAT+**, **BAT−**), the device can be de-energized or restarted with one movement, the terminal blocks are easier to handle during wiring, and for USB programming the device can be taken to the computer.

3.2 Wiring the inputs

The CG17 has four inputs (IN) for connecting the detectors of the alarm system. The wiring modes of the detector: **NO** – normally open contact; **NC** – normally closed contact; **EOL** – normally closed circuit with a 10 kΩ end-of-line resistor; **EOL_T** – normally closed circuit with a 10 kΩ end-of-line resistor, with tamper and wire fault recognition.

Default settings of the zones (inputs):

Zone	Default setting
1 IN	**Delay** – delayed zone, EOL type, partition 1
2 I/O	**Interior** – interior zone, EOL type, partition 1
3 I/O	**Instant** – instant zone, EOL type, partition 1
4 I/O	**Fire** – fire zone, EOL type, partition 1

Changing the settings of the zones and assigning them to partitions is described in section 5.6 (**Zones** window). The possible wirings:

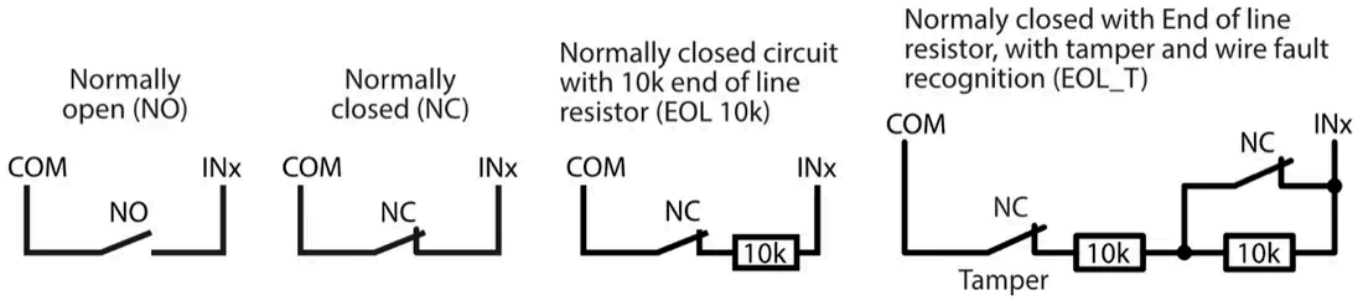


Figure 10. The wiring modes of the inputs between the COM and the INx (the selected input) terminal. From left to right: normally open contact ("Normally open (NO)"); normally closed contact ("Normally closed (NC)"); normally closed circuit with a 10 kΩ end-of-line resistor connected in series ("Normally closed circuit with 10k end of line resistor (EOL 10k)"); normally closed circuit with an end-of-line resistor, with tamper and wire fault recognition ("Normaly closed with End of line resistor, with tamper and wire fault recognition (EOL_T)"): COM → NC tamper contact ("Tamper") → 10 kΩ → the NC alarm contact, with 10 kΩ in parallel to it → INx.

3.3 Wiring smoke detectors

So that the smoke detector can be reset after an alarm, give a PGM output the **Fire Sensor Reset** (reset of the fire detectors) function: TrikdisConfig, **PGM** window, **Outputs** tab (section 5.7). By default **5 OUT** has this function, and **4 I/O** is a fire zone (**Fire**). In the drawings, x OUT is this output, x IN is the zone of the smoke detectors.

- **Wiring a four-wire smoke detector**

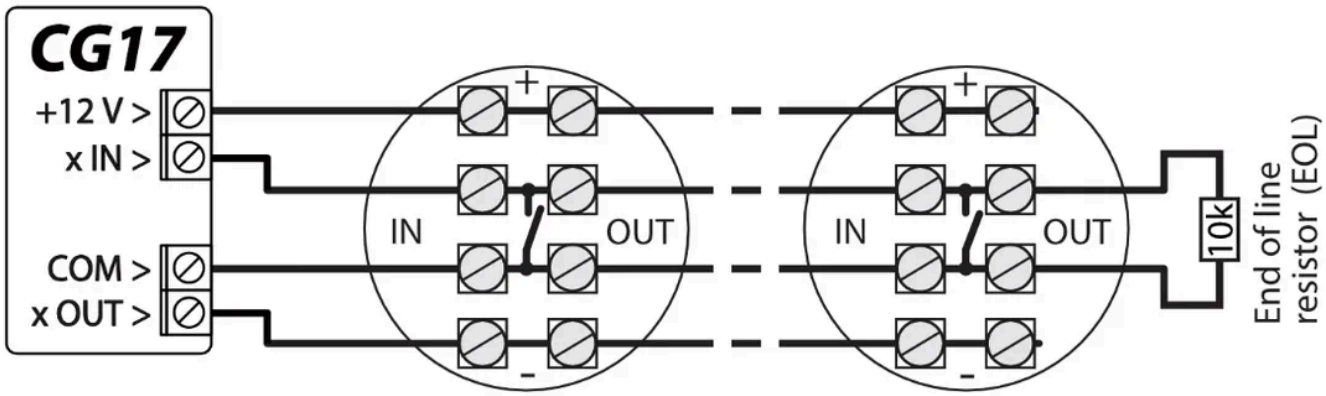


Figure 11. Four-wire smoke detectors in a chain: the +12 V terminal of the CG17 → the + terminal of the detectors, x OUT → the − terminal (the power of the detectors); x IN and COM → the two signal terminals, with the alarm contact of the detector between them. The wires go on from the input ("IN") terminals of the detector through the output ("OUT") terminals to the next detector; a 10 kΩ ("10k") end-of-line resistor ("End of line resistor (EOL)") is placed between the two signal terminals of the last detector.

- **Wiring a two-wire smoke detector** with an SM1* adapter:

1. With an EOL type zone (or with an NC type zone, without an end-of-line resistor):

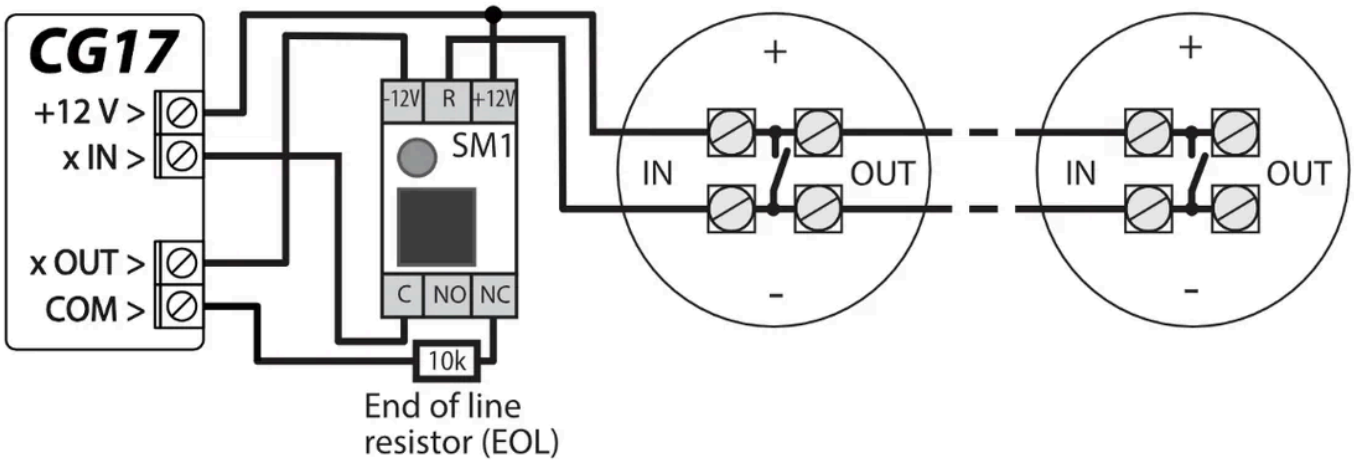


Figure 12. Two-wire smoke detectors with the NC contact of the SM1: the +12 V terminal of the CG17 → the +12V terminal of the SM1 and the + terminal of the first detector; x OUT → the -12V terminal of the SM1; the R terminal of the SM1 → the – terminal of the detector; the input ("IN") and output ("OUT") terminals of the detectors in a chain. Zone circuit: x IN → the C terminal of the SM1; COM → 10 kΩ ("10k") end-of-line resistor ("End of line resistor (EOL)") → the NC terminal of the SM1.

2. With an EOL type zone (or with an NO type zone, without an end-of-line resistor):

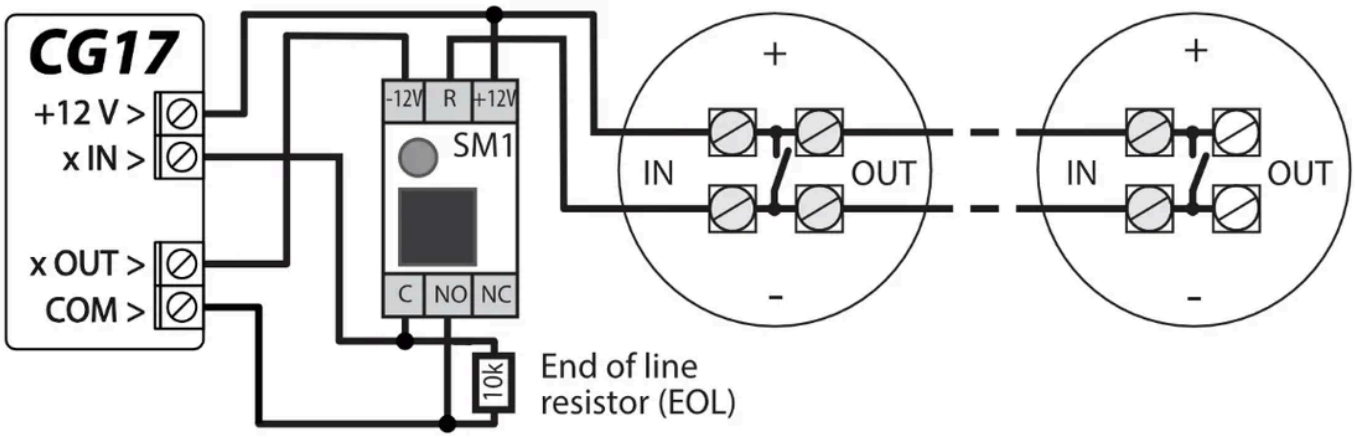


Figure 13. The same with the NO contact of the SM1: the wiring of the power and the detectors is the same; x IN → the C terminal of the SM1, the NO terminal of the SM1 → COM; the 10 kΩ ("10k") end-of-line resistor ("End of line resistor (EOL)") between the x IN and the COM wire, in parallel with the NO contact.

*The SM1 is a Trikdis adapter module with which the two-wire smoke detector can be reset remotely after an alarm.

3.4 Wiring a temperature sensor

- Wire the temperature sensors according to the drawing below. Up to 8 Maxim® / Dallas® DS18S20 or DS18B20 temperature sensors can be connected to the CG17.
- If the cable of the sensor is longer than 0.5 m, use a twisted-pair cable (UTP 4×2×0.5 or STP 4×2×0.5).

DS18B20 temperature sensor with 1m wire

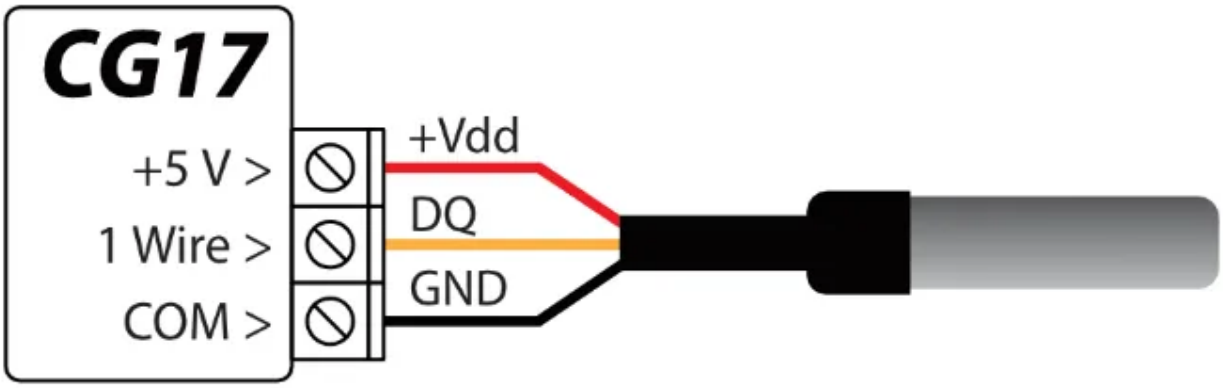


Figure 14. Wiring a temperature sensor: the +5 V terminal of the CG17 → +Vdd (red wire), 1 Wire → DQ (yellow wire), COM → GND (black wire).

The colours of the wires: Vdd – red wire, connect it to the **+5V** terminal; DQ – yellow wire, to the **1 WIRE** terminal; GND – black wire, to the **COM** terminal. The sensors are set up in the **Sensors** window (section 5.8).

3.5 Wiring a relay and an LED

The outputs (**5 OUT**, **6 OUT**, and **2 I/O**, **3 I/O** and **4 I/O** when set as outputs) are open-collector outputs (section 1.5): connect the coil of the relay or the LED between the **+12V** terminal and the output. With the contacts of the relay you can switch external equipment (**Remote Control** function), the LED can show the state of the system (**System state** function); the functions of the outputs are described in section 5.7.

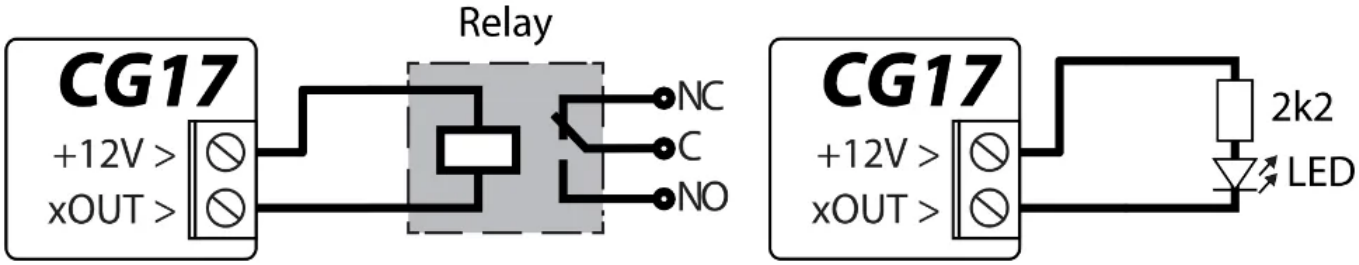


Figure 15. On the left a relay ("Relay"): the coil between the +12V and the xOUT terminal, the contacts of the relay NC, C and NO. On the right an LED ("LED"): +12V → 2.2 kΩ resistor ("2k2") → LED → xOUT.

3.6 Wiring iButton key readers

Discontinued accessory

The **TM17** and **CZ-Dallas** iButton key readers are discontinued accessories and are no longer available. The description has been kept for existing systems.

Connect the **TM17** reader to the **RS485** data bus; the bus cable can be up to 100 m long. Up to eight TM17 readers can be connected to the CG17.

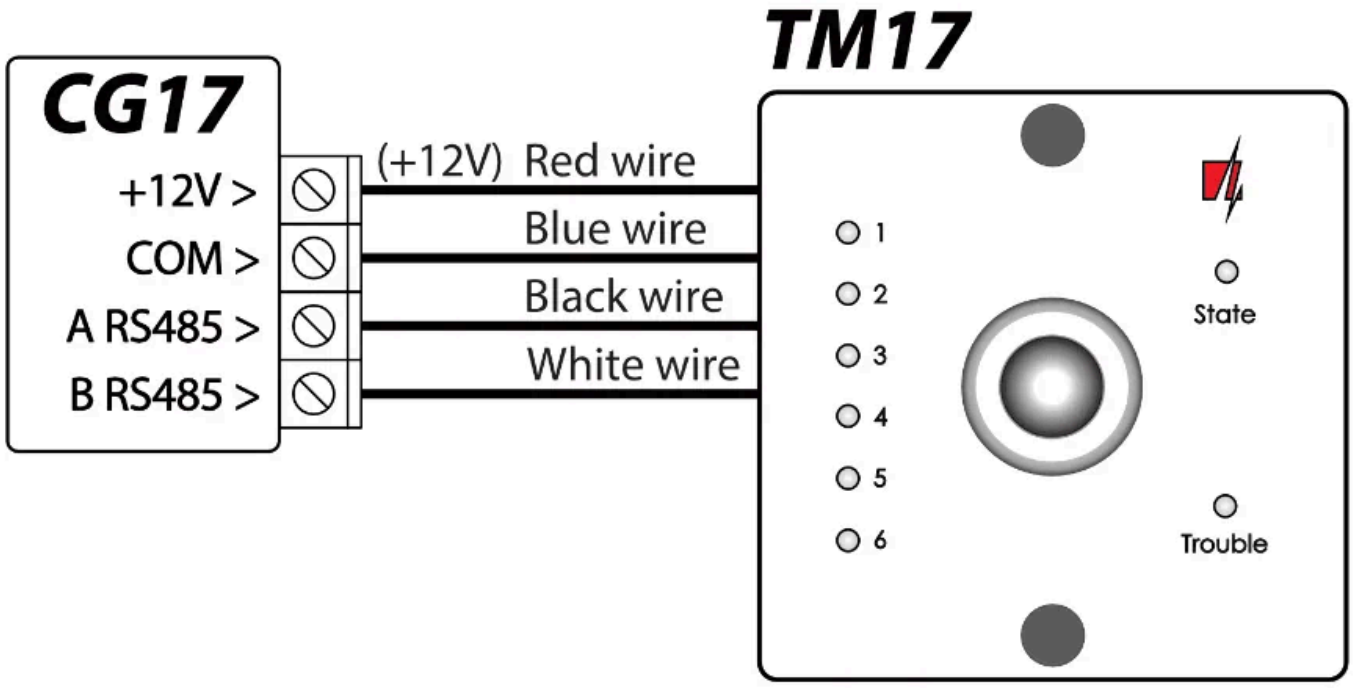
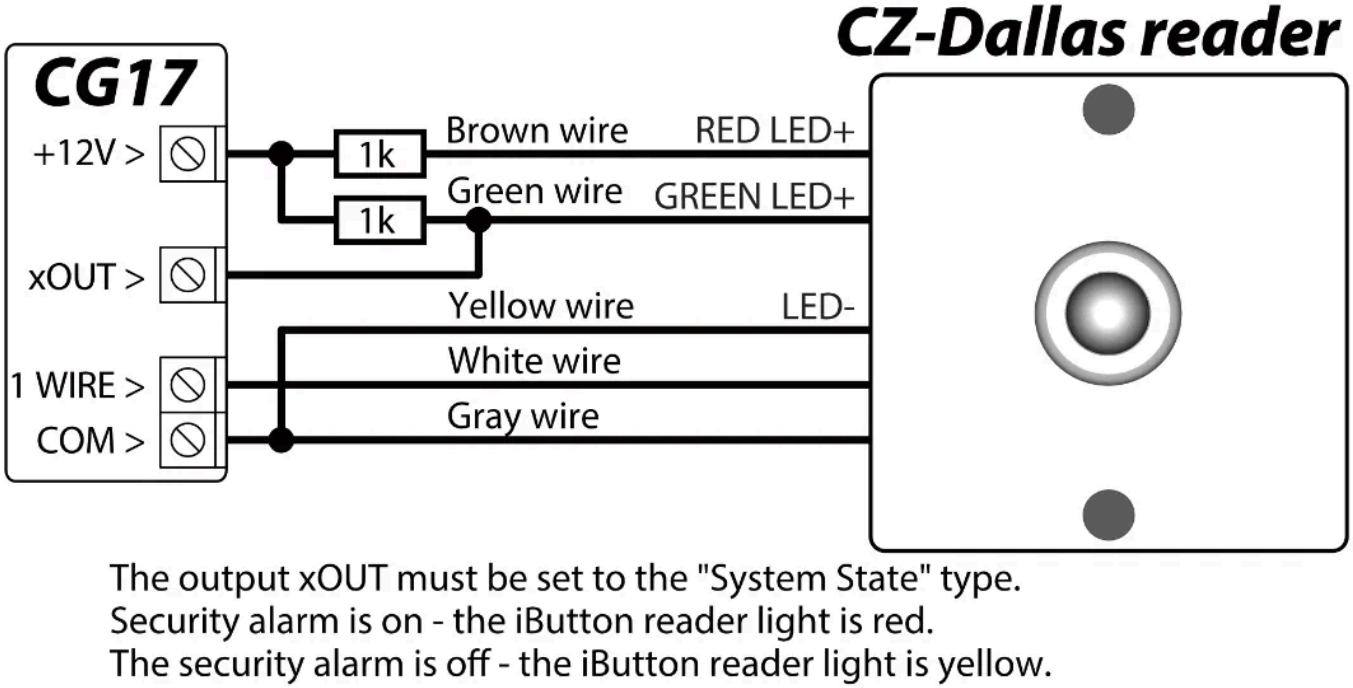


Figure 16. TM17 reader: the +12V terminal of the CG17 → red wire ("(+12V) Red wire"), COM → blue ("Blue wire"), A RS485 → black ("Black wire"), B RS485 → white wire ("White wire"). On the front of the reader the indicators 1–6, the state indicator ("State") and the trouble indicator ("Trouble"), in the middle the touch surface for the iButton key.

Connect the iButton key reader (CZ-Dallas) to the **1 WIRE** terminal; the cable can be up to 30 m long.



The output xOUT must be set to the "System State" type.
Security alarm is on - the iButton reader light is red.
The security alarm is off - the iButton reader light is yellow.

Figure 17. CZ-Dallas reader ("CZ-Dallas reader"): the +12V terminal of the CG17 → each through a separate 1 kΩ ("1k") resistor to the brown wire ("Brown wire", red light: "RED LED+") and to the green wire ("Green wire", green light: "GREEN LED+"); xOUT to the green wire, after the resistor; 1 WIRE → white wire ("White wire"); COM → yellow ("Yellow wire", "LED-") and grey wire ("Gray wire"). The xOUT output must be set to the **System State** type ("The output xOUT must be set to the »System State« type.") – when the alarm is armed, the light of the iButton reader is red ("Security alarm is on - the iButton reader light is red."), when disarmed, yellow ("The security alarm is off - the iButton reader light is yellow.").

"Up to 100 m" and "up to 30 m" are theoretical maximums under ideal conditions – see the note in section 1.3.

Assigning (registering) the keys to the CG17 is described in section 5.4.1.

3.7 Wiring iO series expanders

Discontinued accessory

The **iO-WL** is a discontinued accessory and is no longer available; the **iO8** expander is still available.

If the CG17 needs more inputs (IN) or outputs (OUT), connect a wired or wireless Trikdis iO series input and output expander to it. Setting up the expanders in the CG17 is described in section 5.5 (**Modules** window). Up to eight **iO8** expansion modules can be connected to the CG17; you can use all or only some of the zones of the iO8. The number of zones of the CG17, together with the expanders, is 12 in total.

Trikdis iO8 wired expander module

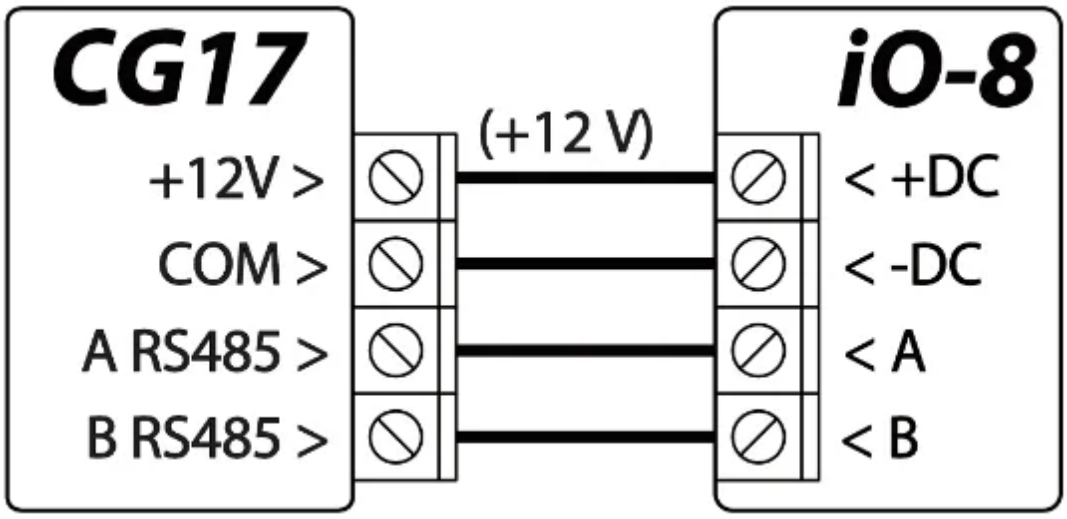


Figure 18. Wiring the iO8 expander ("iO-8"): the +12V terminal of the CG17 ("(+12 V)") → +DC, COM → −DC, A RS485 → A, B RS485 → B.

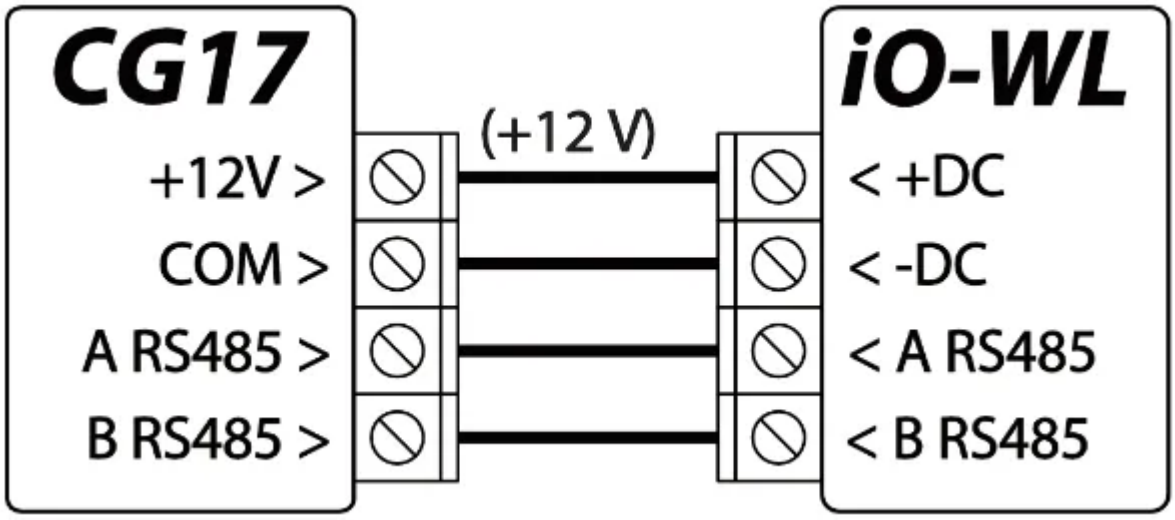


Figure 19. Wiring the iO-WL expander ("iO-WL") with a cable: the +12V terminal of the CG17 ("(+12 V)") → +DC, COM → −DC, A RS485 → A RS485, B RS485 → B RS485.

3.8 Wiring a siren

- A siren with a current consumption of up to 1 A can be connected to the **5 OUT** or the **6 OUT** output.

- A siren with a current consumption of up to 100 mA can be connected to any OUT output.
- The output must get the **Siren** function, and the partition of the alarm system must be assigned to it (**PGM** window, **Output definition** and **Areas**, section 5.7). By default **6 OUT** is the siren output.

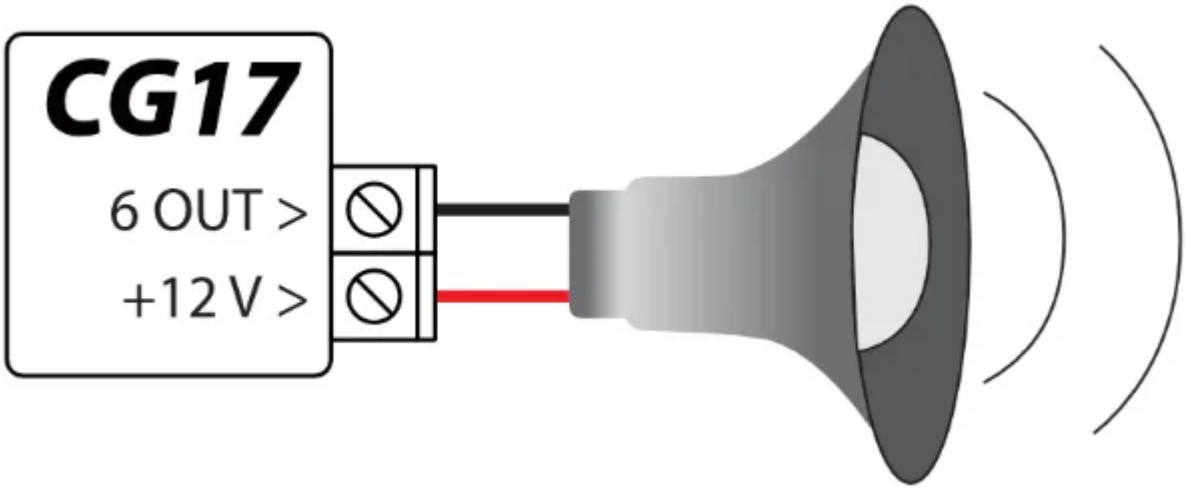


Figure 20. Siren on the 6 OUT output: 6 OUT → black wire, +12 V → red wire.

3.9 The iO expander system (iO, iO-WL, iO-MOD)

Discontinued accessory

The **iO**, the **iO-WL** and the **iO-MOD** are discontinued accessories and are no longer available. The description has been kept for existing systems; for a new system, use the iO8 or the LORA expanders (section 3.16).

The figure shows a complete iO system: wired iO and iO-MOD modules on the RS485 bus, iO-WL expanders connected by radio to the iO-MOD transceivers, with a temperature sensor and an iButton reader on them.

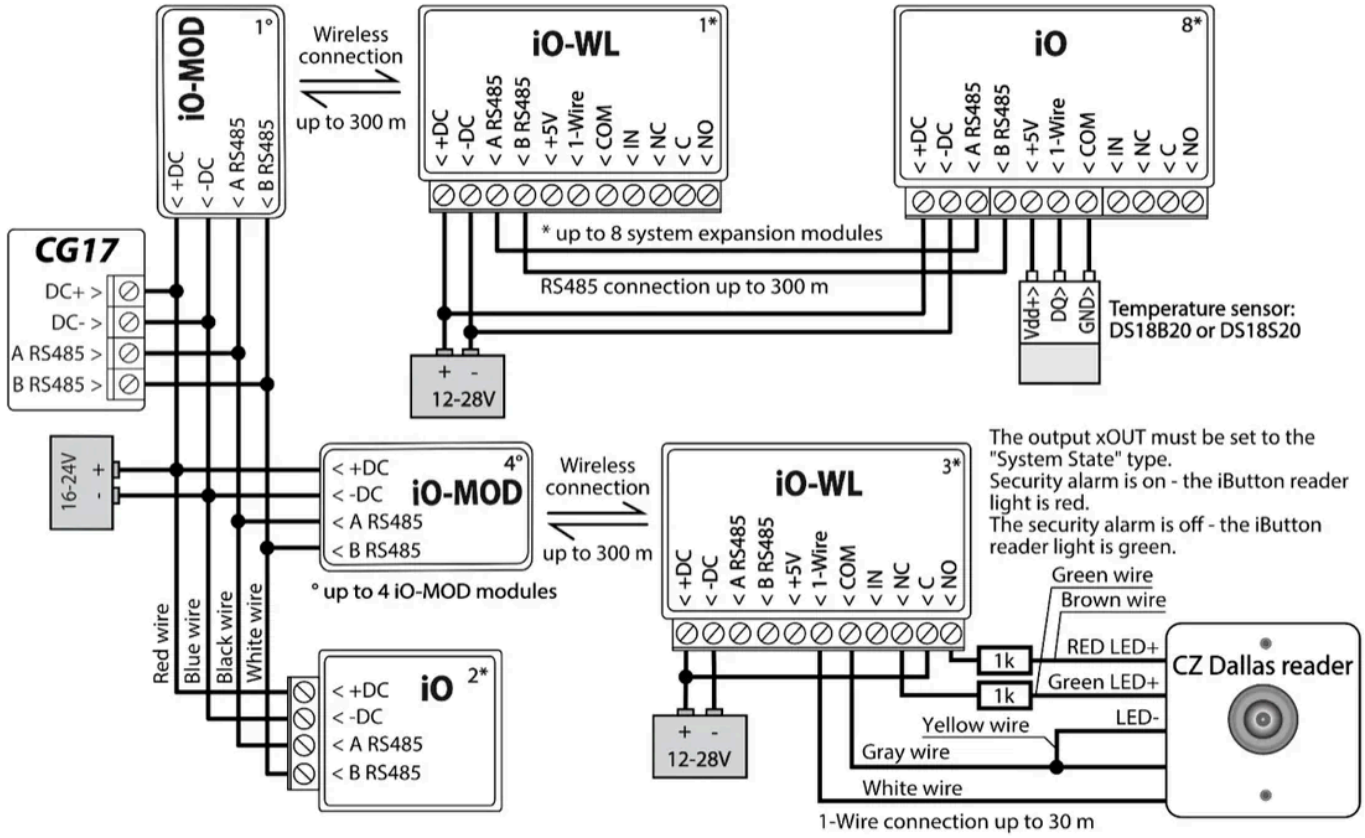


Figure 21. Overview of the iO system. The power terminals of the CG17 ("DC+", "DC-"; on the CG17 AC/+DC and AC/−DC) connect to the 16–24 V power supply ("16-24V") and to the red ("Red wire") and blue wire ("Blue wire") of the bus, the A RS485 and B RS485 terminals to the black ("Black wire") and white wire ("White wire"); on the bus the +DC, −DC, A RS485 and B RS485 terminals of the iO-MOD (1°), the iO-MOD (4°) and the iO (2*). Wireless connection ("Wireless connection"), up to 300 m ("up to 300 m"): between the iO-MOD (1°) and the iO-WL (1*)*, and between the iO-MOD (4°) and the iO-WL (3*). The iO-WL (1*)* and the iO (8*) work from a common 12–28 V supply ("12-28V"), with an RS485 connection between them ("RS485 connection"), up to 300 m ("up to 300 m"); the +5V, 1-Wire and COM terminals of the iO (8*)* → the Vdd+, DQ and GND terminals of the temperature sensor ("Temperature sensor: DS18B20 or DS18S20"). The iO-WL (3*) works from its own 12–28 V supply and handles a CZ-Dallas reader ("CZ Dallas reader"), with a 1-Wire connection, from up to 30 m ("1-Wire connection up to 30 m"): the C terminal of the relay connected to +DC, NO → 1 kΩ ("1k") → brown wire ("Brown wire", red light: "RED LED+"), NC → 1 kΩ → green wire ("Green wire", green light: "Green LED+"), COM → grey ("Gray wire") and yellow wire ("Yellow wire", "LED-"), 1-Wire → white wire ("White wire"). The output must be set to the **System State** type ("The output xOUT must be set to the »System State« type.") – when the alarm is armed, the light of the iButton reader is red ("Security alarm is on - the iButton reader light is red."), when disarmed, green ("The security alarm is off - the iButton reader light is green."). Of the units marked with an asterisk there can be up to 8 system expansion modules (" up to 8 system expansion modules"), of those marked with ° up to 4 iO-MOD modules ("° up to 4 iO-MOD modules").

"Up to 300 m" and "up to 30 m" are theoretical maximums under ideal conditions – see the note in section 1.3.

- If the cable of the temperature sensor is longer than 0.5 m, use a twisted-pair cable (UTP 4×2×0.5 or STP 4×2×0.5).
- The following can be connected to one CG17:
  - up to four iO-MOD modules;
  - up to eight iO and/or iO-WL modules.
- Connect the iButton key readers and the temperature sensors to the "1-Wire" terminal.

3.10 Wiring a Strela fuel level sensor

Discontinued accessory

The **Strela RS485** fuel level sensor is a discontinued accessory and is not available from us. The description has been kept for existing systems.

One **Strela RS485** fuel level sensor can be connected to the CG17. If the fuel level sensor is connected, no other module (iO8, iO, iO-WL, TM17, E485, W485, iO-LORA, iO8-LORA, PB-LORA, REL-LORA) can be connected to the CG17. The sensor must be added in the CG17 in the **Modules** window (section 5.5.3).

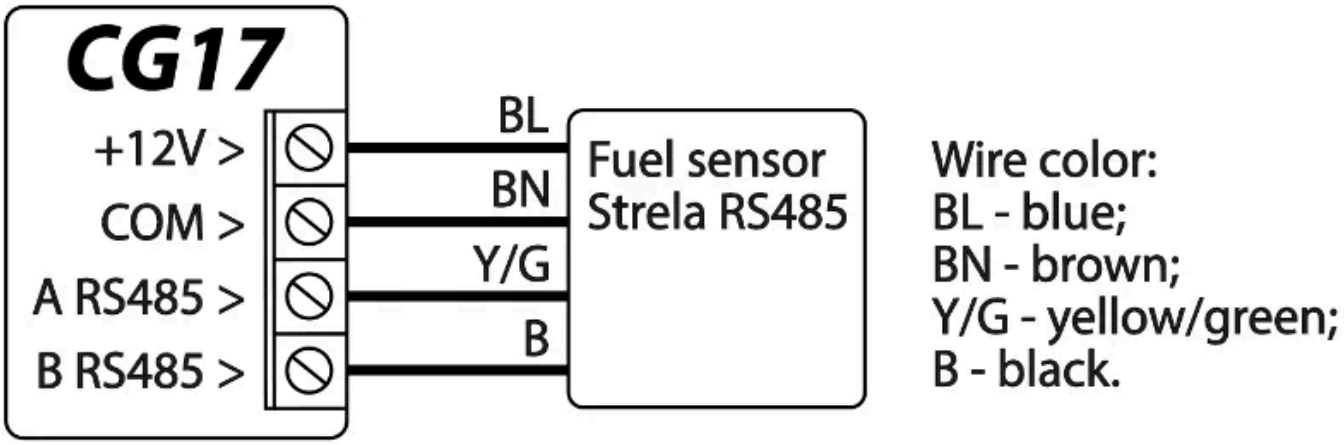


Figure 22. Strela RS485 fuel level sensor ("Fuel sensor Strela RS485"): the +12V terminal of the CG17 → BL, COM → BN, A RS485 → Y/G, B RS485 → B wire. The colours of the wires ("Wire color"): BL – blue ("blue"), BN – brown ("brown"), Y/G – yellow-green ("yellow/green"), B – black ("black").

Setting up and preparing the sensor

The fuel level sensor (Strela RS485) must be calibrated with Strela's **DUTConfig** calibration program (download), and the volume of the fuel tank must be entered in it – otherwise the measurement of the sensor may be inaccurate.

1. Connect the fuel level sensor to the computer with a programming adapter. Press the "brown" button of the adapter so that the green indicator lights up in the RS-485 UART section.
2. Start the **DUTConfig** program and choose the **Interface sensor** type.

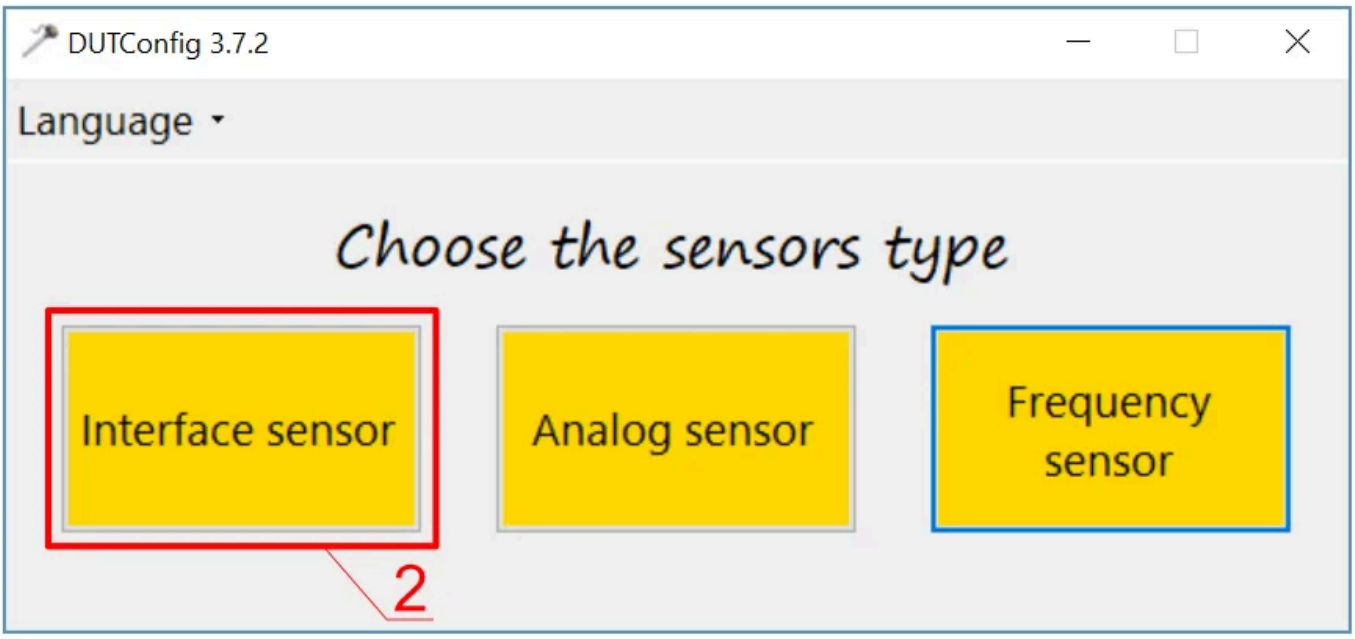


Figure 23. DUTConfig – choosing the type of the sensor ("Choose the sensors type"): **Interface sensor** – interface sensor (2); the other options are the analogue sensor ("Analog sensor") and the sensor with frequency output ("Frequency sensor"); in the **Language** menu the language of the program can be chosen.

3. In the **View** menu choose the **Standart** (normal) view.
4. Click the **Connect** button and wait.

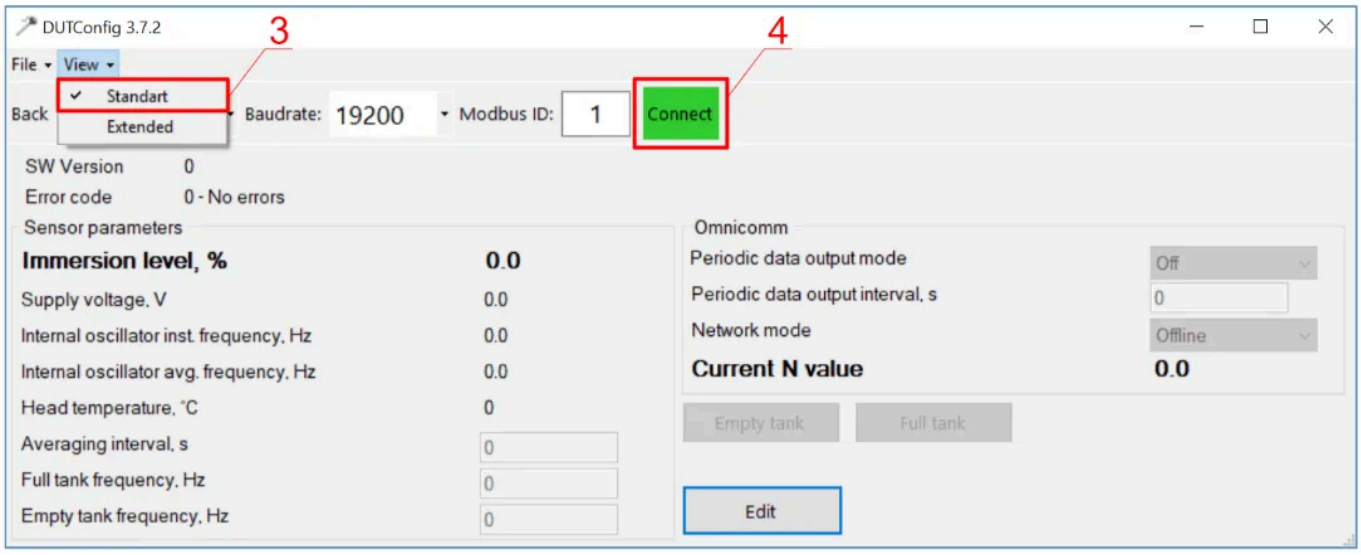


Figure 24. The sensor settings window of DUTConfig: in the **View** menu the **Standart** view (3) and the green **Connect** button (4); next to it the transmission speed (**Baudrate**, 19200) and the Modbus identifier (**Modbus ID**, 1), below them the parameters of the sensor (**Sensor parameters**), the Omnicomm settings, and the **Empty tank**, **Full tank** and **Edit** buttons.

5. When the sensor has connected to DUTConfig, the label **Connection: on** appears.

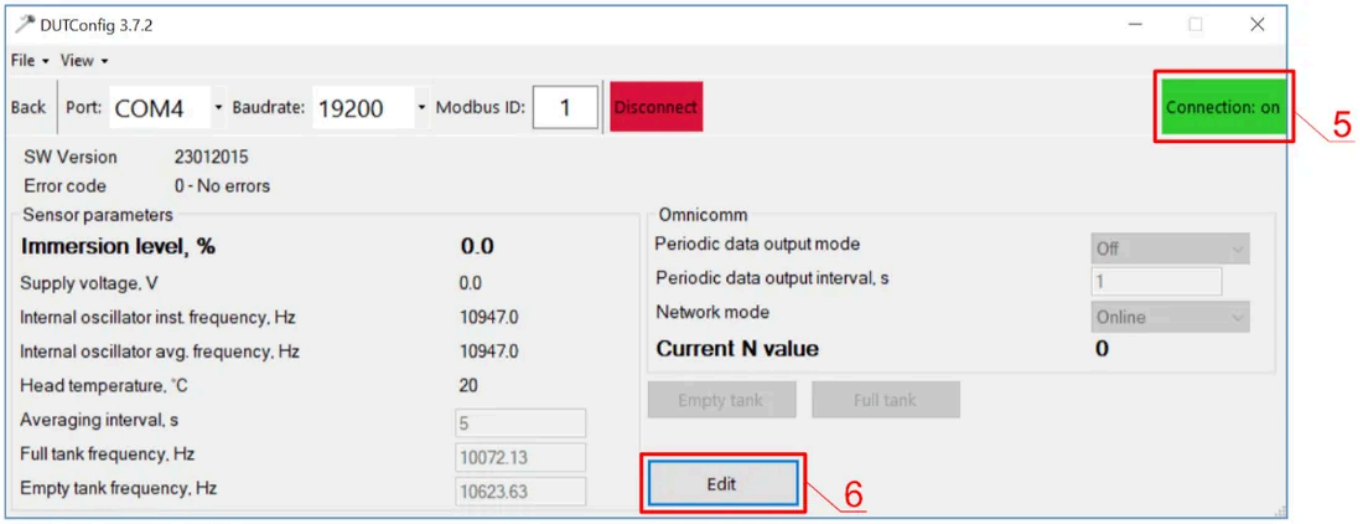


Figure 25. Connected sensor: the port (**Port**, COM4 in the example), the **Disconnect** button, the **Connection: on** label (5) and the **Edit** button (6).

6. Click the **Edit** button and calibrate the sensor with a full and an empty tank.
7. Calibration under real conditions: a) with a full tank, with the sensor in the tank, click the **Full tank** button; b) with an empty tank, with the sensor taken out of the tank, click the **Empty tank** button.
8. To save the values, click the **OK** button.

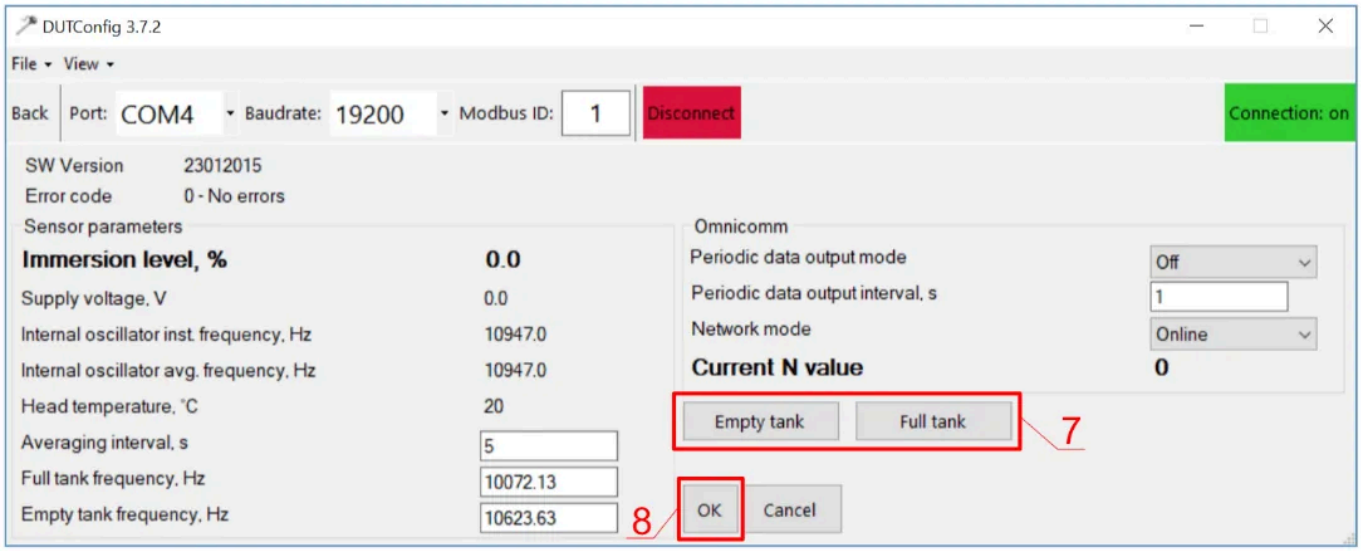


Figure 26. Calibration: the **Empty tank** and the **Full tank** button (7), saving with the **OK** button (8); the **Cancel** button discards the change.

9. Set the **View** menu to the **Extended** view.

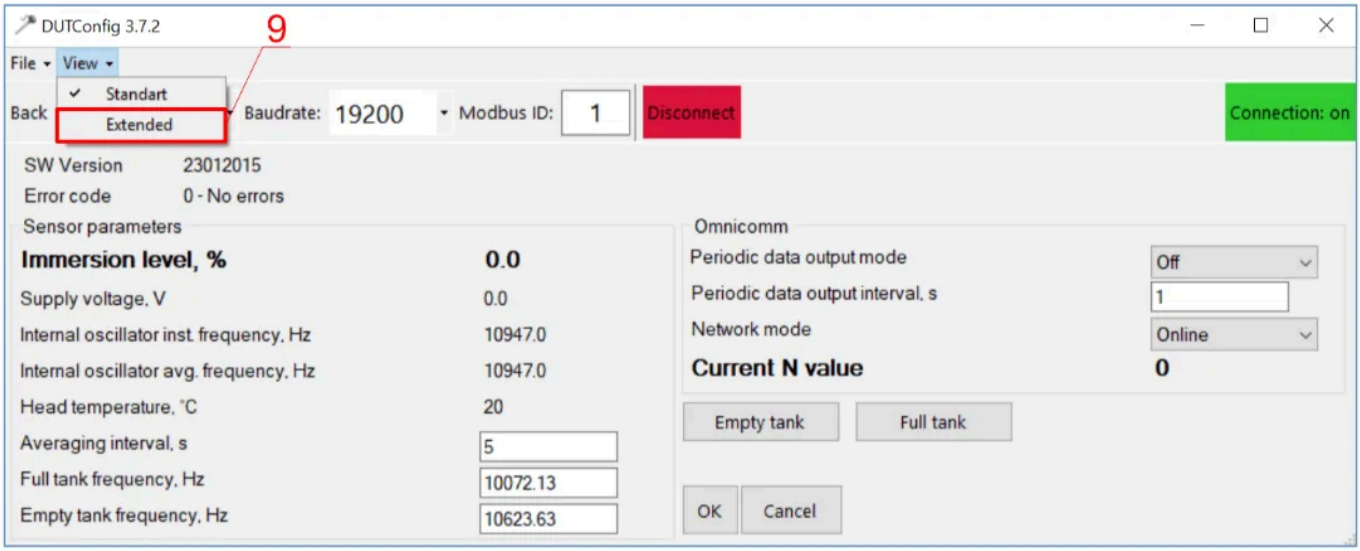


Figure 27. The **View** menu: **Standart** (normal) and **Extended** view – **Extended** selected (9).

10. Fill in the table according to the shape of the tank. A simple method: set the 0 % immersion to 0 litres, the 100 % to the volume of your tank (in the example the tank is 200 litres).
11. When you have filled in the table, click the **OK** button.

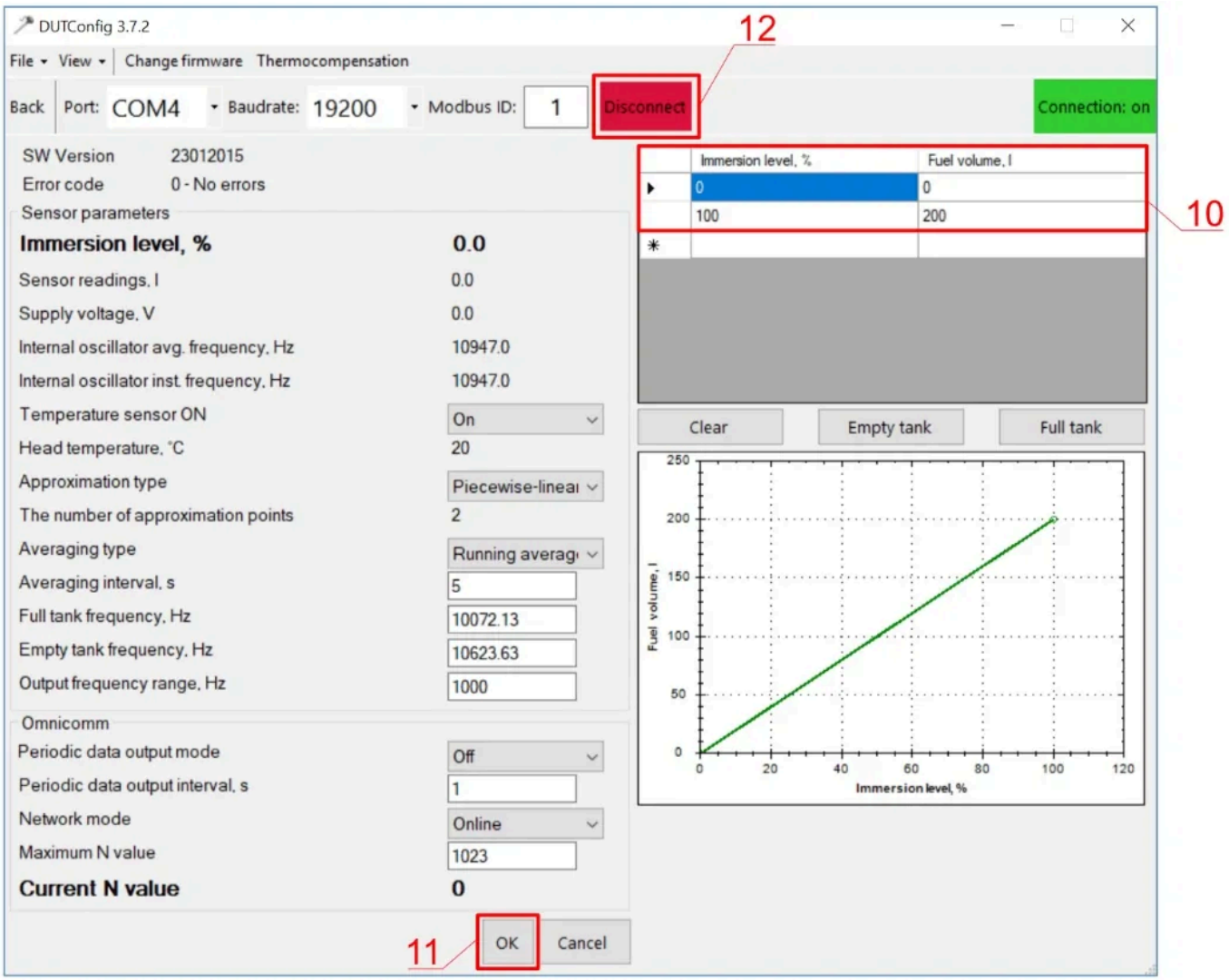


Figure 28. The table of the extended view (10): the immersion level ("Immersion level, %") and the fuel volume ("Fuel volume, l") – in the example 0 % = 0 l, 100 % = 200 l –, next to it its graph; the **OK** button (11) and the **Disconnect** button (12). In the menu, changing the firmware ("Change firmware") and temperature compensation ("Thermocompensation") are also available.

12. Click the **Disconnect** button.
13. Disconnect the sensor from the computer and connect it to the CG17.

3.11 Wiring a battery

A 12 V battery can be connected to the CG17. If the mains power supply (AC) is lost, the CG17 sends an **AC fault** event message and automatically switches to the 12 V battery.

- If the battery voltage drops to 11.5 V, the CG17 sends a **Battery low** event message.
- If the battery voltage drops below 9.5 V and there is no mains power supply, the CG17 switches off.
- When the mains power supply returns, the CG17 sends an **AC restore** event message, and charging of the battery starts automatically.
- If the battery voltage rises to 12.6 V, the CG17 sends a **Battery restore** event message.

Wiring the battery:

- Place the backup battery in the enclosure.
- Connect the wires of the battery to the backup power terminals of the CG17: **BAT+** and **BAT−**.
- Check that the charging current of the CG17 (up to 500 mA, section 1.3) is sufficient for charging the battery.

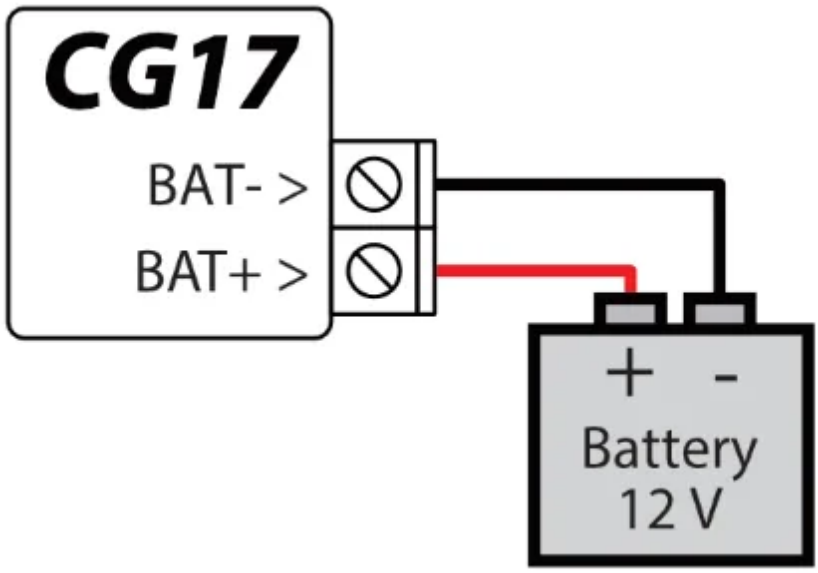


Figure 29. Wiring the battery: BAT− → black wire → the − pole of the battery, BAT+ → red wire → its + pole; 12 V battery ("Battery 12 V").

3.12 Connecting to an alarm panel

In this wiring the CG17 works as a communicator: the PGM outputs of the alarm panel control the inputs of the CG17. The type (**Type**) of the CG17 inputs must be **NO** or **NC**, and their definition (**Definition**) **24 hours** (24-hour zone) – **Zones** window, section 5.6. You can also enter an SMS text for the inputs (**Zones** window, **SMS & Call reporting** tab, **SMS text**): the user receives this when the input is triggered or restores. The PGM outputs of the alarm panel must be assigned to the desired events in the settings of the alarm panel.

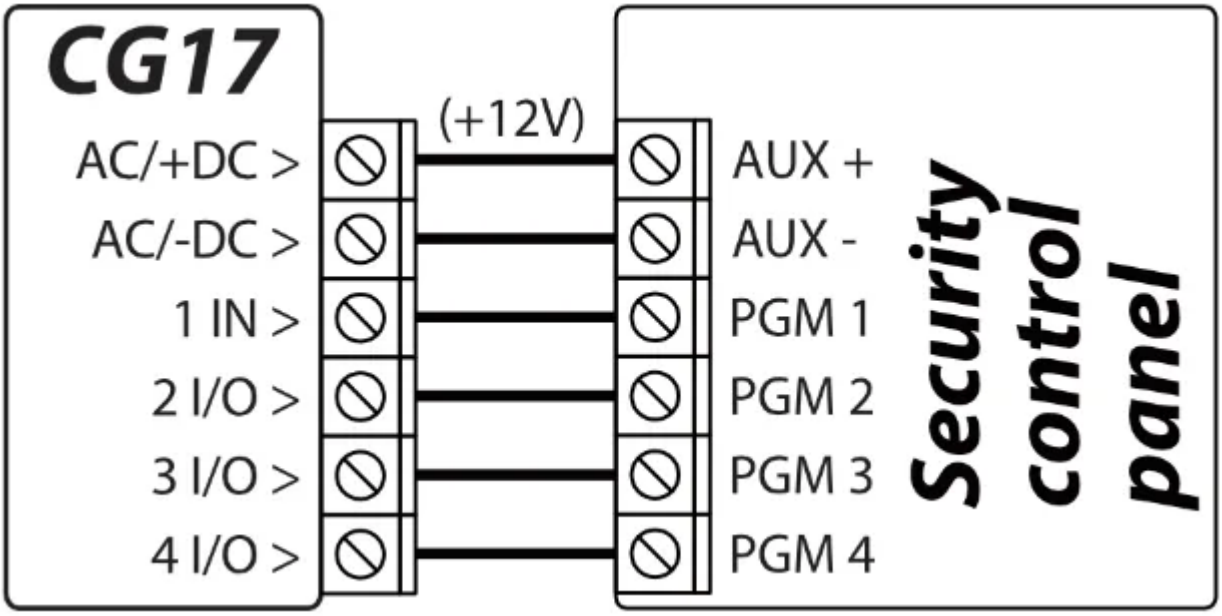


Figure 30. Connecting the CG17 to an alarm panel ("Security control panel"): the +12 V power wire ("(+12V)") between the AC/+DC terminal of the CG17 and the AUX+ terminal of the panel, AC/−DC → AUX−; the 1 IN terminal of the CG17 → the PGM 1 output of the panel, 2 I/O → PGM 2, 3 I/O → PGM 3, 4 I/O → PGM 4.

3.13 Measuring DC voltage

The CG17 can also be used for measuring DC voltage. Any of the four inputs (**1 IN**, **2 I/O**, **3 I/O**, **4 I/O**) can be selected for the measurement; in TrikdisConfig these are the **In1 Voltage** … **In4 Voltage** sensor types. The measuring range is 0–30 V; **above 30 V the CG17 is damaged**. Connect the measured voltage to the **1 IN** and **COM** terminals: 1 IN is the positive, COM the negative terminal (the rest of the description also applies to the 1 IN input).

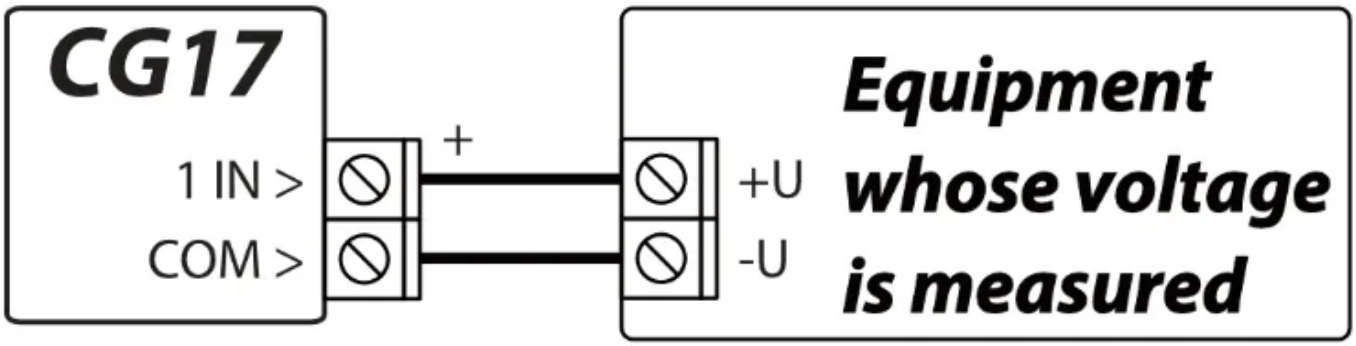


Figure 31. Voltage measurement: the +U terminal of the measured equipment ("Equipment whose voltage is measured") → 1 IN, its −U terminal → COM.

Connect the CG17 to the computer with a USB Mini-B cable and start TrikdisConfig: the program automatically recognizes the connected CG17 and opens its settings window. In the **Sensors** window (section 5.8) choose the **In1 Voltage** type and enter the voltage limits beyond which an event message is generated:

- **Max** – if the voltage is higher than this, an event message is generated; for this the **High** box must be ticked.
- **Min** – if the voltage is lower than this, an event message is generated; for this the **Low** box must be ticked.

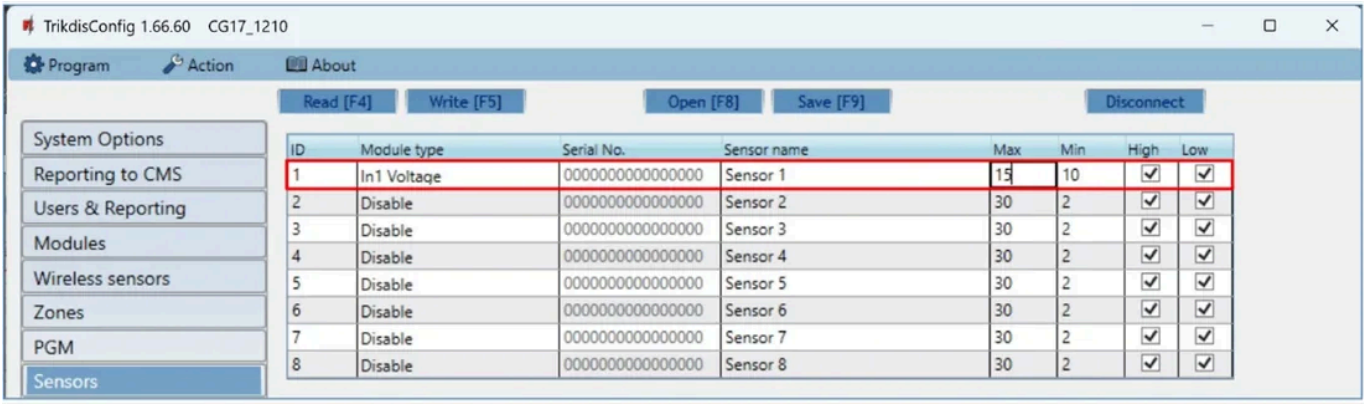


Figure 32. TrikdisConfig – **Sensors**: in row 1 the **Module type** is **In1 Voltage**, **Max** 15, **Min** 10 V, **High** and **Low** ticked; the other rows are disabled (**Disable**).

The measured voltage can also control a PGM output: the output switches above or below the set value. For this, select the PGM output in TrikdisConfig and set it to **Remote Control** operation (**PGM** window, **Outputs** tab, section 5.7).

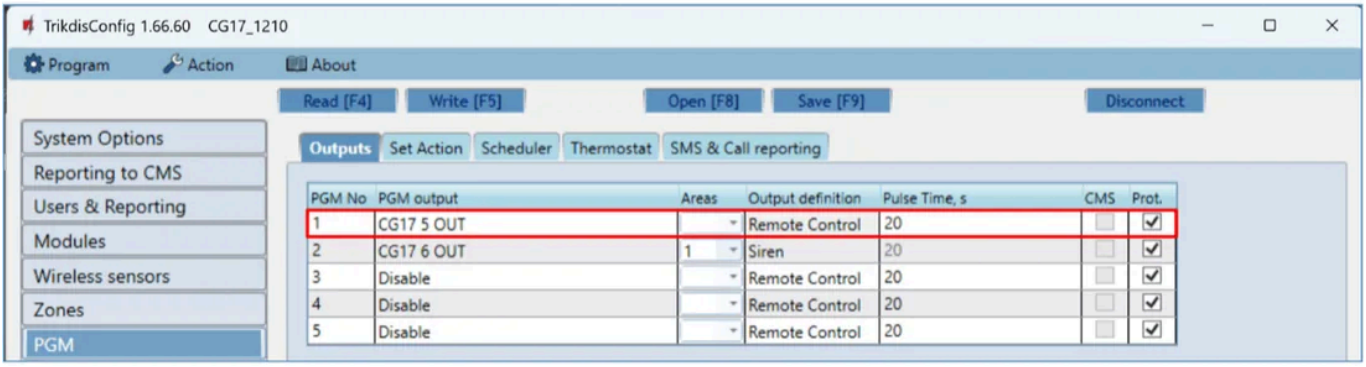


Figure 33. TrikdisConfig – **PGM**, **Outputs** tab: PGM 1 is the **CG17 5 OUT** output, its type (**Output definition**) **Remote Control**, its pulse time (**Pulse Time**) 20 s.

Go to the **Set Action** tab.

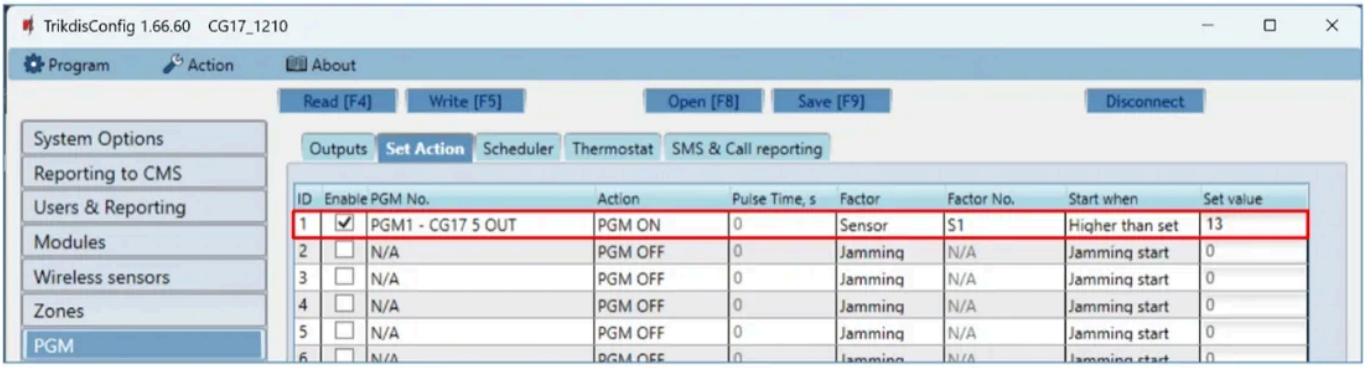


Figure 34. TrikdisConfig – **PGM**, **Set Action** tab: in row 1 **Enable** ticked, **PGM No.** PGM1 – CG17 5 OUT, **Action** PGM ON, **Pulse Time** 0, **Factor** Sensor, **Factor No.** S1, **Start when** Higher than set, **Set value** 13 – the output switches on above 13 V.

- **Enable** – enabling the PGM.
- **PGM No.** – the PGM output controlled by the 1 IN input.
- **Action** – the operating mode of the PGM output:
  - **PGM OFF** – switching off the PGM output.
  - **PGM ON** – switching on the PGM output.
  - **Pulse OFF** – switching off the PGM output for the pulse time (after the command the output switches off for the pulse time, then switches on).

    - **Pulse ON** – switching on the PGM output for the pulse time (after the command the output switches on for the pulse time, then switches off).
- **Pulse time, s** – the length of the pulse, 0–9999 s.
- **Factor** – the source of the condition: the sensor (**Sensor**).
- **Factor No.** – the voltage measuring input, here 1 IN (**S1** in the picture).
- **Start when** – further condition for switching on the PGM output (in the picture **Higher than set** – above the set value).
- **Set value** – the voltage (V) that the CG17 monitors and according to which it controls the PGM output.

3.14 W485 Wi-Fi module

The **W485** module sends the messages of the CG17 over the local Wi-Fi network, through the internet router, to the monitoring station and to the Protegus 2 app. As long as there is a Wi-Fi connection, the CG17 (from firmware **1.13**) sends the event messages over the W485 module. If the Wi-Fi is lost, the CG17 sends the messages over mobile internet, and when the Wi-Fi returns it switches back to the W485. Setting up the module in the CG17 is described in section 5.5 (**Modules** window). **With the W485, the CG17 can also be used without a SIM card** – without a SIM, however, the cellular backup, SMS and calls do not work. One W485 module can be connected to the CG17. The module connects to the **RS485** bus (A–A, B–B), at up to 100 m.

Trikdis W485 Wifi module (RS485)

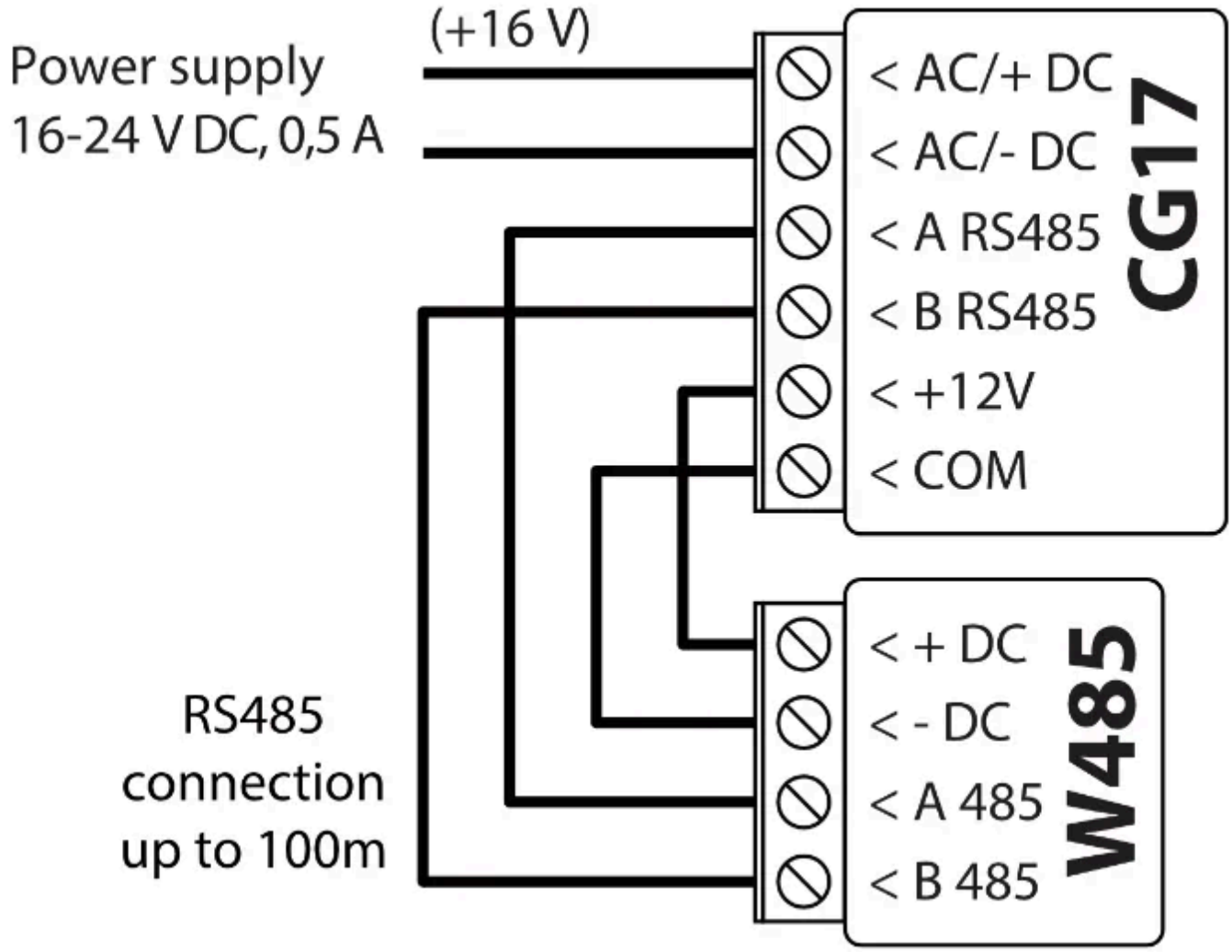


Figure 35. Wiring the W485 module: the positive pole ("(+16 V)") of the 16–24 V DC, 0.5 A power supply ("Power supply 16-24 V DC, 0,5 A") to the AC/+DC terminal of the CG17, the negative to AC/−DC; the +12V terminal of the CG17 → the +DC terminal of the W485, COM → −DC; RS485 connection ("RS485 connection"), up to 100 m ("up to 100m"): A RS485 – A 485, B RS485 – B 485.

"Up to 100 m" is a theoretical maximum under ideal conditions – see the note in section 1.3.

3.15 E485 Ethernet module

The **E485** module sends the messages of the CG17 over wired internet to the monitoring station and to the Protegus 2 app. With the E485 (from firmware **1.13** of the CG17), the monitoring station and Protegus messages go over the wired internet, and the CG17 does not use mobile internet. If the wired internet connection is lost, the CG17 sends the messages over mobile internet, and when the wired connection returns, over the E485 again. Setting up the module in the CG17 is described in section 5.5 (**Modules** window). **With the E485, the CG17 can also be used without a SIM card** – without a SIM, however, the cellular backup, SMS and calls do not work. One E485 module can be connected to the CG17. The module connects to the **RS485** bus (A–A, B–B), at up to 100 m.

Trikdis E485 Ethernet module (RS485)

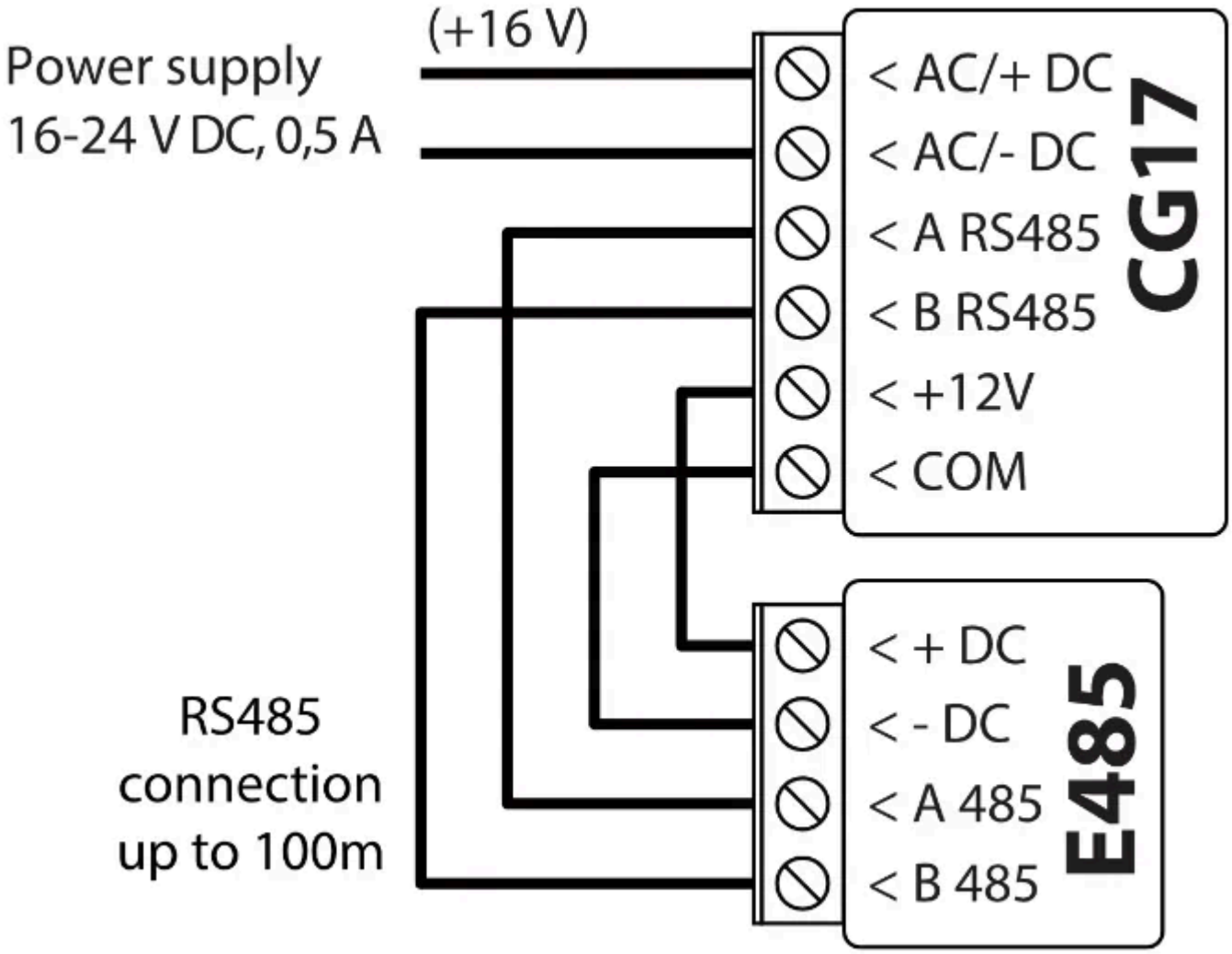


Figure 36. Wiring the E485 module: the positive pole ("(+16 V)") of the 16–24 V DC, 0.5 A power supply ("Power supply 16-24 V DC, 0,5 A") to the AC/+DC terminal of the CG17, the negative to AC/−DC; the +12V terminal of the CG17 → the +DC terminal of the E485, COM → −DC; RS485 connection ("RS485 connection"), up to 100 m ("up to 100m"): A RS485 – A 485, B RS485 – B 485.

"Up to 100 m" is a theoretical maximum under ideal conditions – see the note in section 1.3.

3.16 RF-LORA and LORA expanders

The function works with firmware **1.18** or newer of the CG17. Connect the **RF-LORA** transceiver to the CG17: after this, the **iO-LORA**, **iO8-LORA**, **PB-LORA** and **REL-LORA** modules can be used. One RF-LORA transceiver can be connected to the CG17.

Trikdis RF-LORA wireless expander module **Trikdis IO-LORA wireless expander module**

Trikdis IO8-LORA wireless expander module

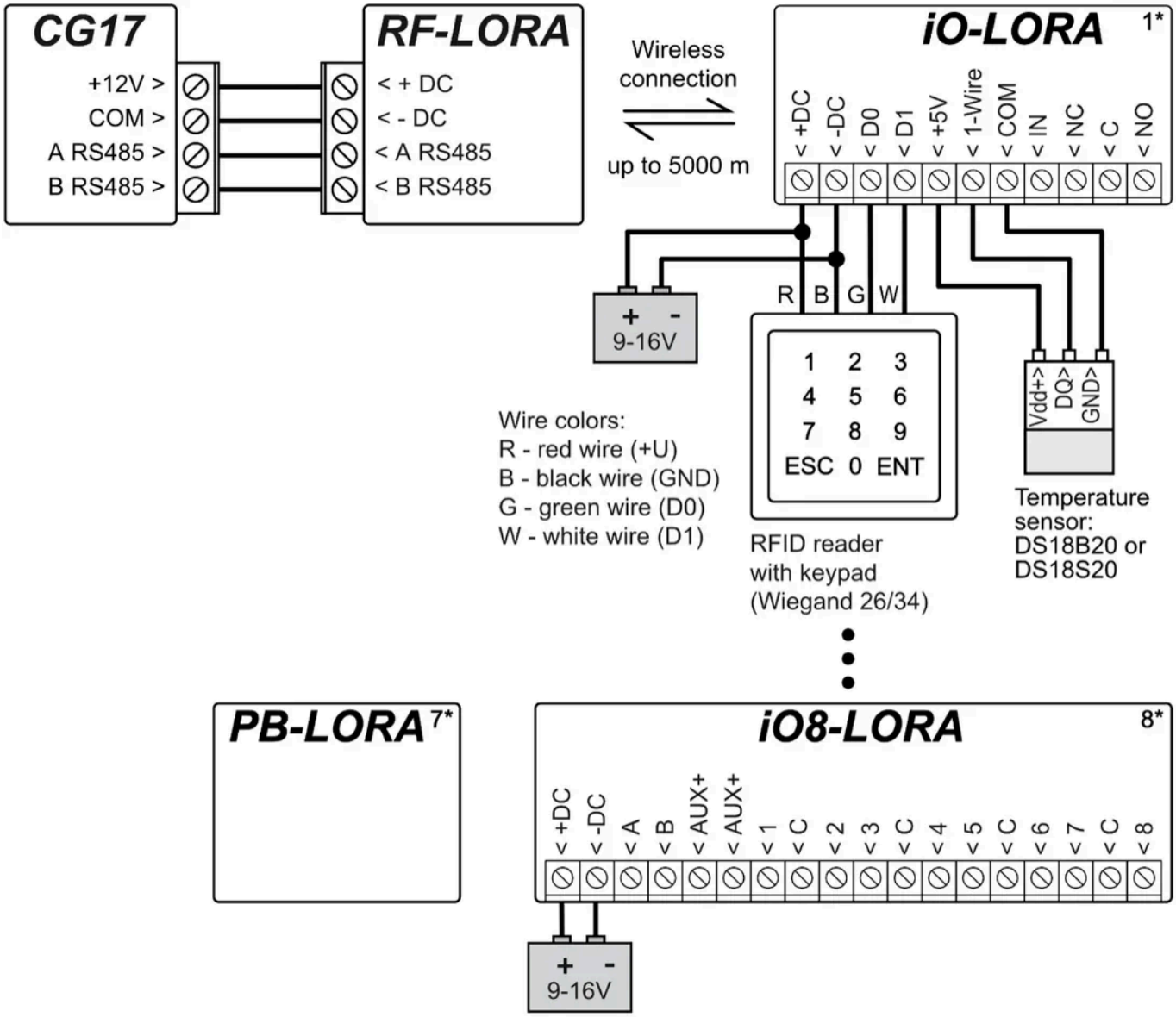


Figure 37. LORA expanders through the RF-LORA transceiver: the +12V, COM, A RS485 and B RS485 terminals of the CG17 → the +DC, −DC, A RS485 and B RS485 terminals of the RF-LORA; wireless connection ("Wireless connection"), up to 5000 m ("up to 5000 m") between the RF-LORA and the LORA modules. The iO-LORA (1*) works from its own 9–16 V supply ("9-16V"); connected to it an RFID reader with keypad, Wiegand 26/34 ("RFID reader with keypad (Wiegand 26/34)"), the colours of the wires ("Wire colors"): red, +U ("R - red wire (+U)") → +DC; black, GND ("B - black wire (GND)") → −DC; green, D0 ("G - green wire (D0)") → D0; white, D1 ("W - white wire (D1)") → D1; and a temperature sensor ("Temperature sensor: DS18B20 or DS18S20"): Vdd+ → +5V, DQ → 1-Wire, GND → COM. The dots mark further modules: the drawing also shows the PB-LORA panic button (7*) and the iO8-LORA expander (8*) working from its own 9–16 V supply.

"Up to 5000 m" is a theoretical maximum under ideal conditions – see the note in section 1.3.

Setup in TrikdisConfig: start TrikdisConfig and connect the CG17 to the computer with a USB Mini-B cable, or connect to it remotely (section 6.1). Click the **Read [F4]** button: the program shows the current settings of the CG17. If the program asks for it, enter the administrator or installer code in the pop-up window. In the **Modules** window, choose the LORA module used from the list in the **Module** column, and enter the serial number of the module in the **Serial No.** field (section 5.5).

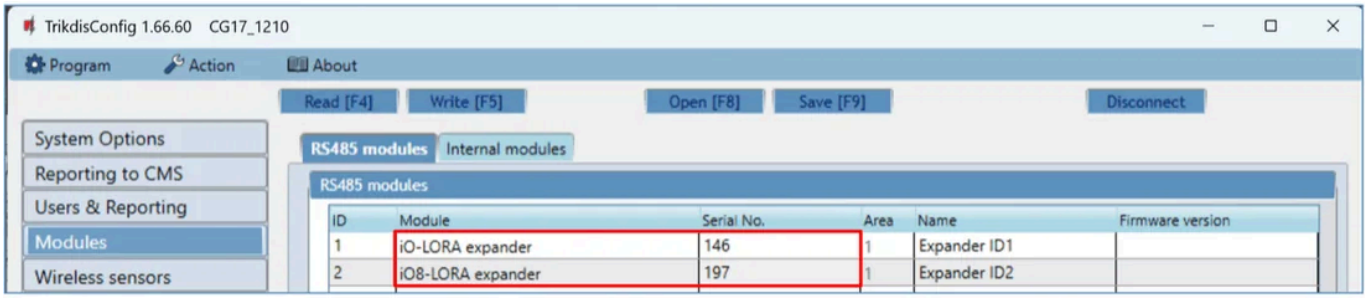


Figure 38. TrikdisConfig – **Modules**, **RS485 modules** tab: the LORA modules selected in the **Module** column (**iO-LORA expander**, **iO8-LORA expander**), their serial numbers in the **Serial No.** column; **Area** – partition, **Name** – the name of the module.

After the changes, click the **Write [F5]** button and wait until the update is finished. Finally click the **Disconnect** button and unplug the USB Mini-B cable.

4. Control

You can control the CG17 remotely in three ways: from the **Protegus 2** app (section 4.1), by **SMS command** (section 4.2) and by **phone call** (section 4.3). Remote changing of the settings and remote control from TrikdisConfig are described in chapter 6.

4.1 Control from the Protegus 2 app

With Protegus 2, the users control the alarm system remotely, see the state of the system and receive notifications about the events of the system.

Before you add the system

You can add the CG17 to Protegus 2 if:

1. the Protegus cloud service is switched on: in the **Users & Reporting** window of TrikdisConfig, in the **Cloud application** settings group, **Enable cloud service** is ticked (section 5.4; by SMS: `CONNECT 123456 PROTEGUS=ON`, section 4.2);
2. there is an activated SIM card in the device, and its PIN code is entered (**System Options** window, **SIM** group, section 5.2), or the PIN request is switched off;
3. there is power supply: the **POWER** LED is lit green;
4. the device is connected to the network: the **NETWORK** LED is lit green and blinks yellow.

If the **NETWORK** or the **DATA** LED is lit yellow continuously, the device cannot connect to the mobile network and/or to Protegus 2. The LED indications are described in section 1.6.

The DATA LED is the simplest internet check. The DATA LED is lit when there is a message waiting to be sent in the device's memory. A green NETWORK LED only tells you that the network connection has been established – for a mobile network device, that it has registered on the operator's network; for an Ethernet device, that the connection up to the router is alive – but not that the device can also reach the internet. If the NETWORK LED is green but the DATA LED stays lit continuously even after an event or test report, the internet connection is not working: the message cannot be sent. On a mobile network the most common culprit is the APN or the data service of the SIM card; on Ethernet, the router, the firewall or the DNS. When the DATA LED goes out, the message has been sent and the data connection is fine.

A rendszer létrehozása a Protegus 2 alkalmazásban

1. Töltsd le a Protegus 2 alkalmazást a telefonodra vagy nyisd meg egy böngészőben

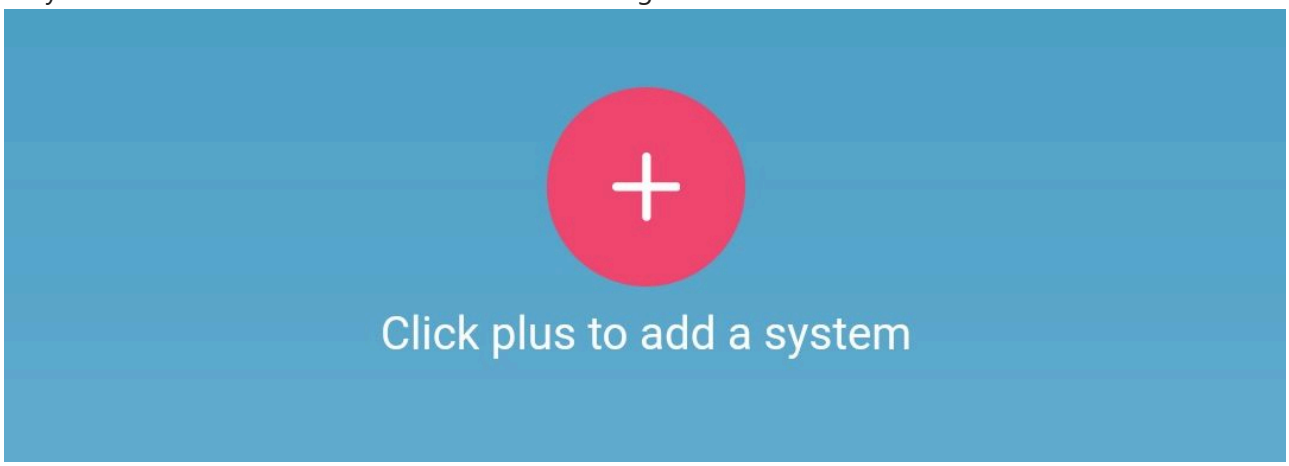
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

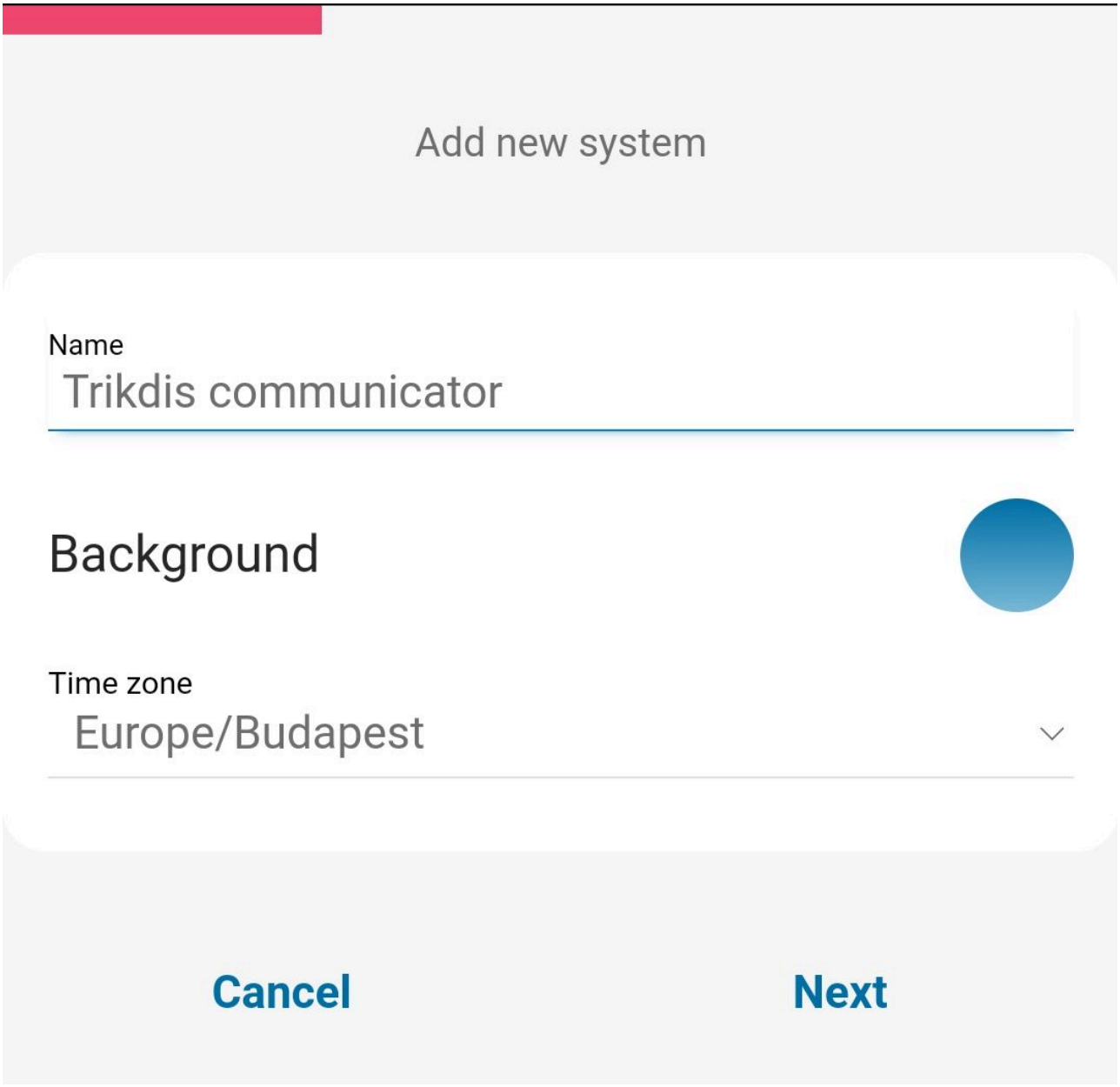
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



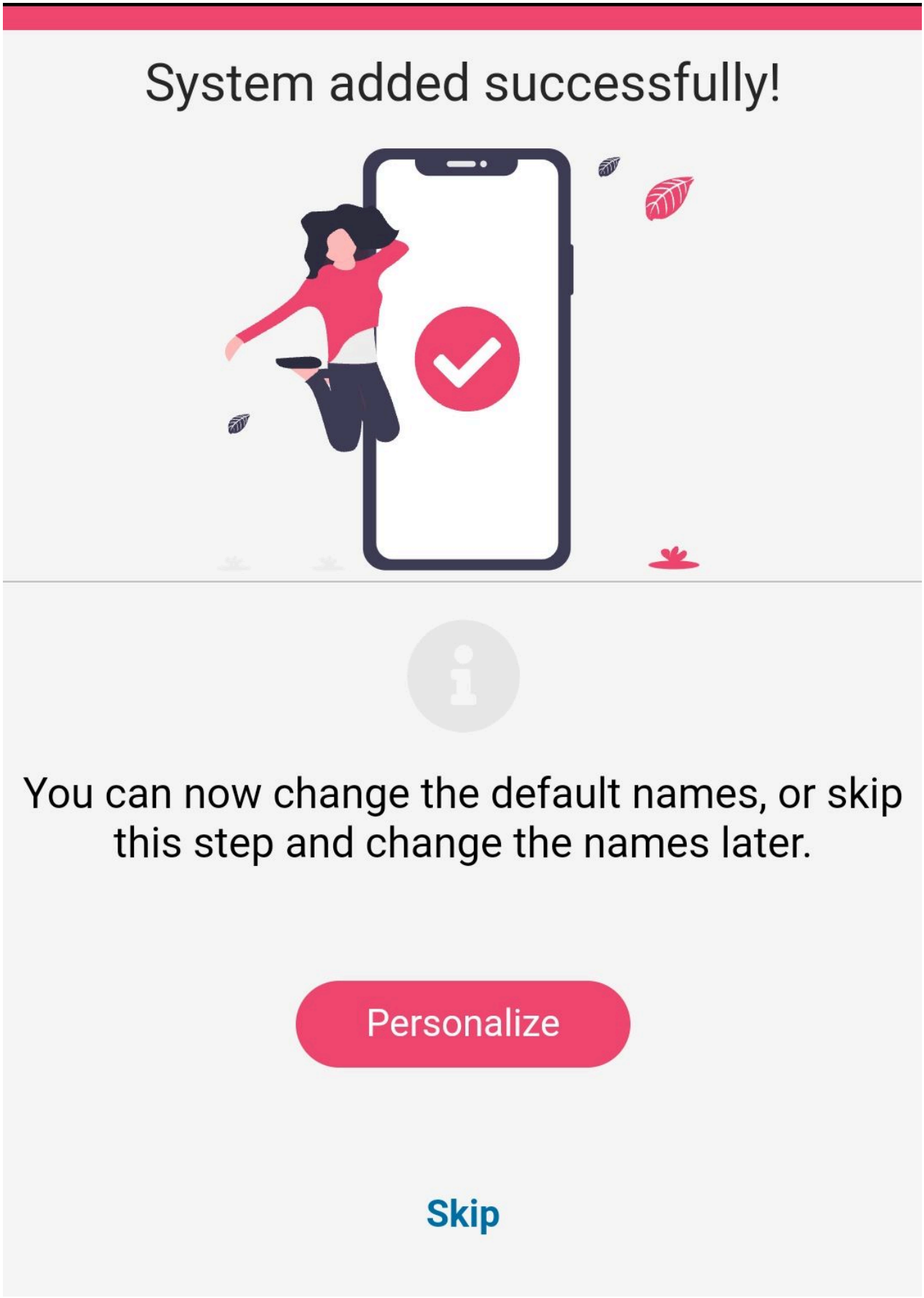
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



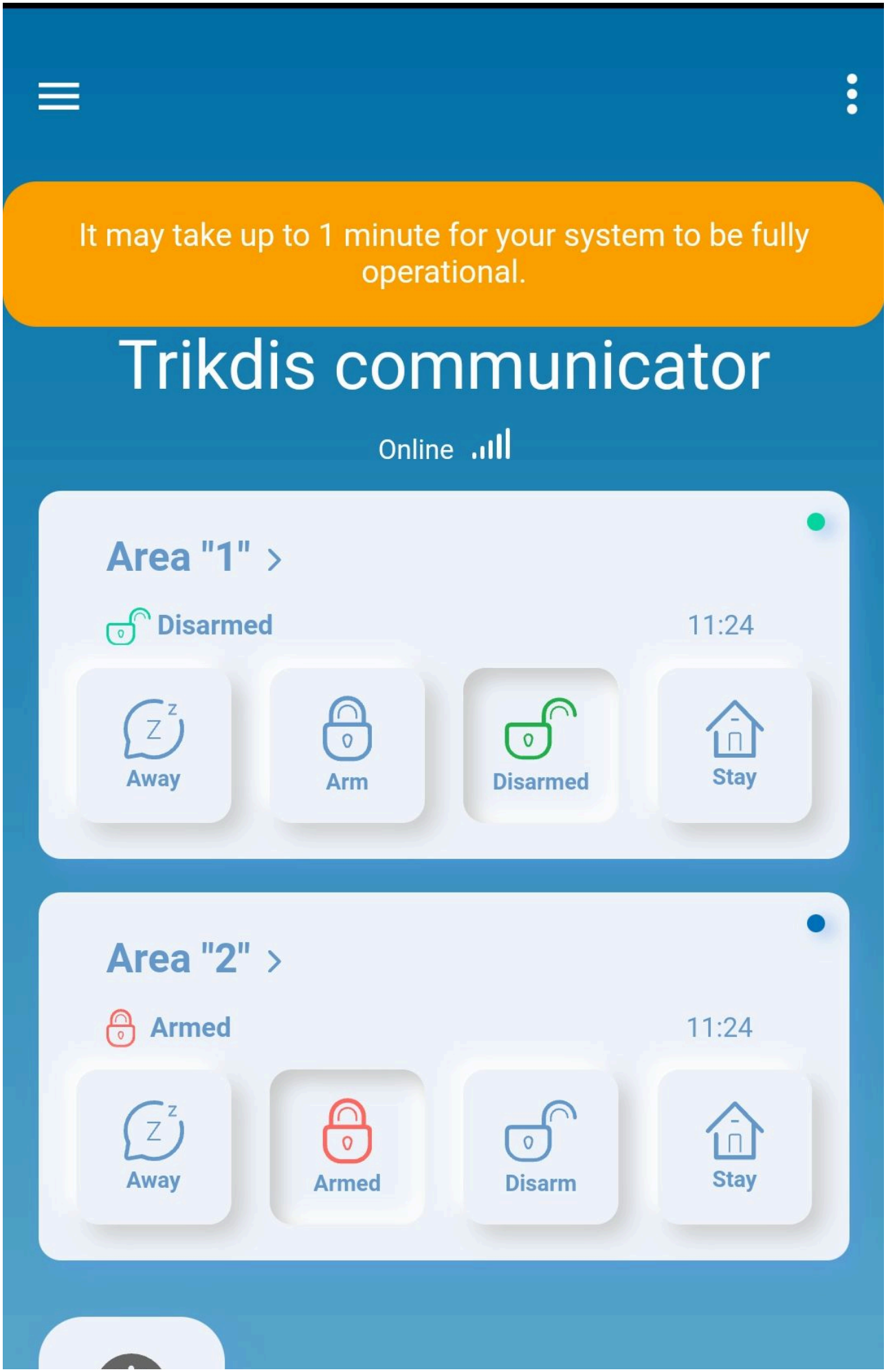
6. Add meg a rendszer nevét és válassz idozónát



7. A rendszered elkészült, a következő lépésnél még elnevezheted a partíciókat és zónákat, de ezt később bármikor megteheted.



8. Az utolsó lépésben megjelenik a rendszered kezdőképernyője. Várd meg, amíg eltűnik a sárga csík és a rendszered elkészült.


It may take up to 1 minute for your system to be fully operational.
Trikdis communicator
Online
Area "1"
Disarmed
11:24
Away
Arm
Disarmed
Stay
Area "2"
Armed
11:24
Away
Armed
Disarm
Stay



With the CG17, pay attention to these when adding it:

1. The unique identifier (**Unique ID**) is the **IMEI** number of the CG17: you can find it on the sticker on the device and on the box, and you also see it in the TrikdisConfig status bar (section 5.1).
2. If the installer changed the default `123456` value of the **Cloud Access Code** (section 5.4), the app also asks for this code when adding the system.

See also

Protegus Android / iPhone and web app · Browser push notifications in the Protegus 2 app

4.1.1 Arming and disarming

1. Open the Protegus 2 app, and in the window of the system press the **Arm** button.
2. In the menu choose the mode to be switched on, and enter the user code (the code entered in the **Code** column of the **Users & Reporting** window of TrikdisConfig, section 5.4).
3. When the system changes mode, the **Arm** icon also changes.



Figure 39. The CG17 in Protegus 2: **Area "1"** (partition 1) is in disarmed state (**Disarmed**), you arm it with the framed **Arm** button. At the top the name of the system and the **Online** (available) state with the signal strength.

If you arm the system from Protegus 2 or by phone call, the panel does not count the exit time (**Exit time**, section 5.2).

4.1.2 Adding more users

Start the Protegus 2 app on your phone, and log in with your user name and password.

1. Open the **Settings** menu: tap the three-dot icon in the top right corner of the system window.

2. Choose **System configuration**.

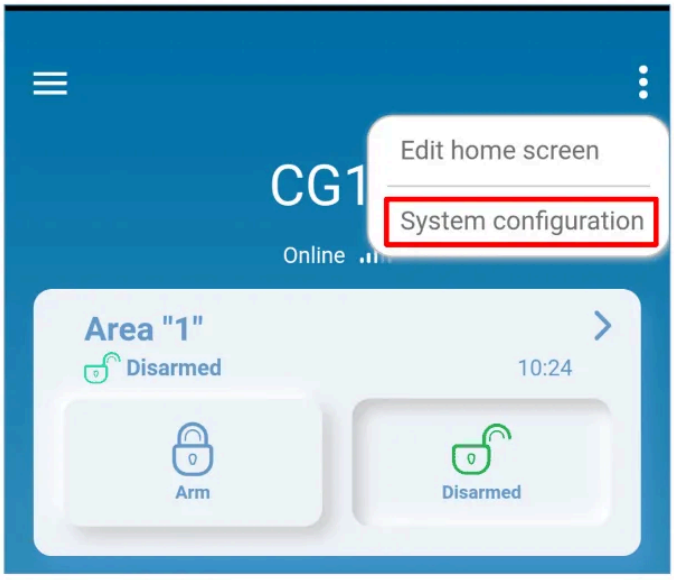


Figure 40. The menu of the three dots at the top right: **Edit home screen** and the framed **System configuration**.

3. Choose **Users**.

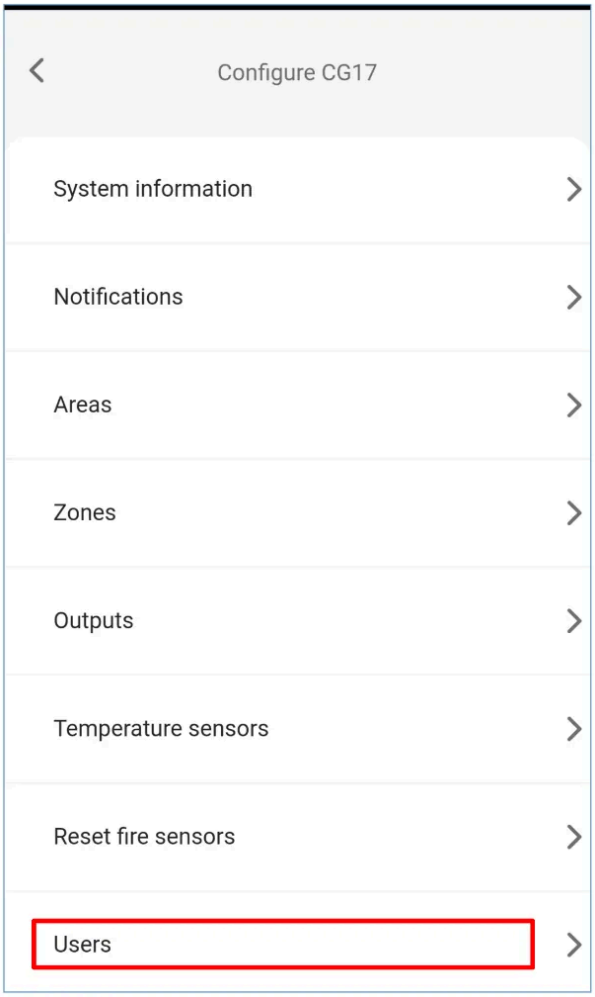


Figure 41. The **Configure CG17** menu: **System information**, **Notifications**, **Areas** (partitions), **Zones**, **Outputs**, **Temperature sensors**, **Reset fire sensors** and the framed **Users**.

4. Press the **+** (**Add new user**) button.
5. Enter the e-mail address or user name of the user.
6. Enter the phone number of the user.
7. Enter the code of the user.
8. Mark which partition the user may control.
9. Mark which PGM output the user may control.
10. Press the **Add user** button.

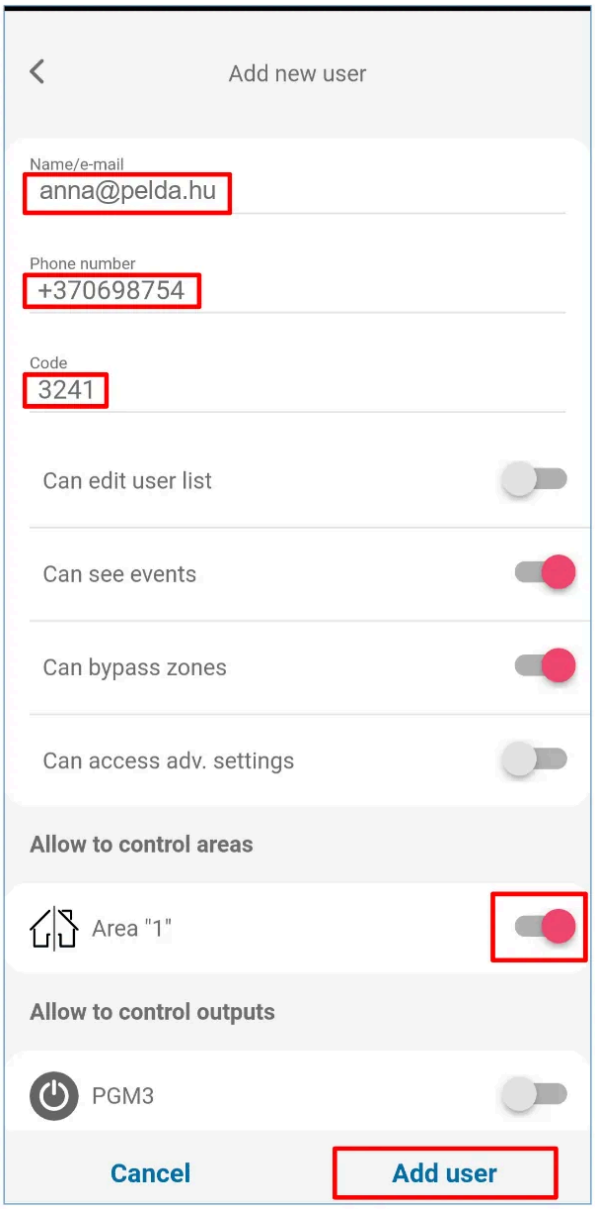


Figure 42. The **Add new user** form: **Name/e-mail** (name or e-mail address), **Phone number**, **Code**; permissions: **Can edit user list**, **Can see events**, **Can bypass zones**, **Can access adv. settings** (advanced settings); below them the switches **Allow to control areas** (partitions that can be controlled) and **Allow to control outputs** (outputs that can be controlled), at the bottom the **Add user** button.

11. The new user appears in the list of users.
12. Return to the main window with the **Back** button.

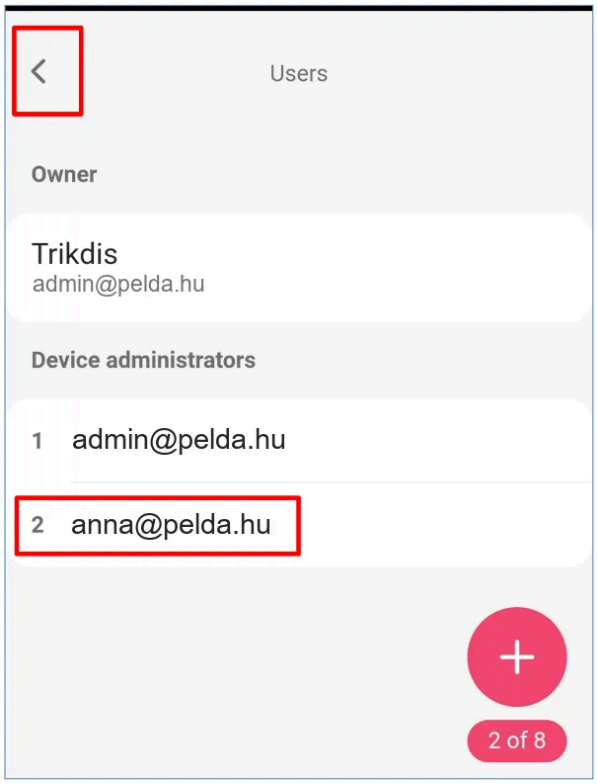


Figure 43. The **Users** list: **Owner** (the owner of the system) and **Device administrators**, in row 2 the new user; at the top left the framed back arrow (**Back**). The **2 of 8** indication: 2 of the 8 possible users have been added.

4.2 Control by SMS commands

Send the SMS command to the phone number of the SIM card inserted in the CG17. In the commands, `xxxxxx` is the 6-character administrator SMS password (default `123456`; in TrikdisConfig: **System Options** → **Access** → **SMS password**, section 5.2). If the **ACK** checkbox is ticked for the user in the user list (section 5.4), the CG17 sends a reply SMS to them after every SMS command; you can rewrite the text of the replies on the **SMS answer texts** tab of the **Users & Reporting** window.

Arming and disarming by SMS – you arm and disarm the alarm system with these SMS messages:

```
ARM xxxxxx SYS:x
```

```
DISARM xxxxxx SYS:x
```

Symbol	Meaning
`xxxxxx`	the 6-character administrator password (default `123456`)
`x`	the number of the partition of the alarm system (1–8)

Changing the administrator password – for security reasons, replace the default administrator SMS password. Send an SMS in this form:

```
PSW 123456 xxxxxx
```

Symbol	Meaning
`123456`	the default administrator password
`xxxxxx`	the new, 6-character administrator password

Authorizing other users – by SMS and by phone call, the system can only be controlled from the phone numbers on the user list. From the administrator's phone, send the phone numbers and names of the other people by SMS, so that they can also control the system:

```
SETN xxxxxx PHONEx=+PHONENR#NAME
```

Symbol	Meaning
`xxxxxx`	the 6-character administrator password
`x`	the position of the user on the list (if you enter **1**, you hand over your administrator right to another user)
`PHONENR`	the phone number of the user
`NAME`	the name of the user

Resetting the smoke detectors – you can also reset the smoke detectors remotely by SMS:

```
FRS xxxxxx
```

`xxxxxx` – the 6-digit administrator password.

The OUT output to which the fire detectors are connected must get the fire detector reset type (in the **PGM** window of TrikdisConfig: **Output definition** → **Fire Sensor Reset**, section 5.7). By default the **5 OUT** output gets this type.

List of SMS commands (in each of them the password comes after the command word, in the examples the default `123456`):

Command	Data	Description
`INFO`	–	data about the panel: the reply contains the type, IMEI number, serial number and firmware version of the panel. Example: `INFO 123456`
`RESET`	–	restarting the device. Example: `RESET 123456`
`OUTPUTx`	`ON`	switching on an output; **x** is the number of the output. Example: `OUTPUT1 123456 ON`
`OUTPUTx`	`OFF`	switching off an output; **x** is the number of the output. Example: `OUTPUT1 123456 OFF`
`OUTPUTx`	`PULSE=ttt`	switching on an output for a set time: **x** is the number of the OUT output, **ttt** the pulse time in seconds, as a three-digit number. Example: `OUTPUT1 123456 PULSE=002`
`PSW`	new password	changing the password. Example: `PSW 123456 654123`
`TIME`	`YYYY/MM/DD,HH:MM:SS`	setting the date and time. Example: `TIME 123456 2026/10/30,12:23:00`
`TXTA`	object name	saving the name of the object. Example: `TXTA 123456 Home`
`TXTE`	`Z1=` … `Z12=`	the SMS text sent when the zone goes into alarm; Z1…Z12 – the number of the input (zone). Example: `TXTE 123456 Z1=ALARM Zone1`

Command	Data	Description
`TXTR`	`Z1=` … `Z12=`	the SMS text sent when the zone restores; Z1…Z12 – the number of the input (zone). Example: `TXTR 123456 Z1=Zone1 restored`
`RDR`	`phone number#SMS text`	forwarding an SMS to the given phone number; the number must start with a + sign and the international country code. Example: `RDR 123456 +447700900123#forwarded text`
`ASKI`	–	SMS about the state of the inputs (IN). Example: `ASKI 123456`
`ASKO`	–	SMS about the state of the outputs (OUT). Example: `ASKO 123456`
`ASKT`	–	SMS with the values of all temperature sensors. Example: `ASKT 123456`
`DISARM`	`SYS:x`	disarming the alarm; **x** is the number of the partition (1–8). Example: `DISARM 123456 SYS:1`
`ARM`	`SYS:x`	arming the alarm; **x** is the number of the partition (1–8). Example: `ARM 123456 SYS:1`
`FRS`	–	resetting the output of the fire detectors, if the fire detector reset function (**Fire Sensor Reset**, section 5.7) is assigned to the OUT output. Example: `FRS 123456`
`SETN`	`PHONEx=phone number#name`	adding a phone number and user name for user x; **x** is the row of the phone number on the list. The number must start with a + sign and the international country code, the number and the name are separated by `#`. Example: `SETN 123456 PHONE5=+447700900123#JOHN`
`SETN`	`PHONEx=DEL`	deleting the phone number and name of the user. Example: `SETN 123456 PHONE5=DEL`
`UUSD`	`*USSD code#`	sending a USSD code to the mobile operator. Example: `UUSD 123456 *245#`
`CONNECT`	`Protegus=ON`	connecting to the Protegus cloud service. Example: `CONNECT 123456 PROTEGUS=ON`
`CONNECT`	`Protegus=OFF`	disconnecting from the Protegus cloud service. Example: `CONNECT 123456 PROTEGUS=OFF`
`CONNECT`	`Code=123456`	the code of the Protegus cloud service (**Cloud Access Code**, section 5.4). Example: `CONNECT 123456 CODE=123456`
`CONNECT`	`IP=0.0.0.0:8000`	the TCP IP address and port of the server of the primary channel. Example: `CONNECT 123456 IP=0.0.0.0:8000`
`CONNECT`	`IP=0`	switching off the primary channel. Example: `CONNECT 123456 IP=0`
`CONNECT`	`ENC=123456`	the TRK encryption key. Example: `CONNECT 123456 ENC=123456`
`CONNECT`	`APN=Internet`	the name of the APN. Example: `CONNECT 123456 APN=INTERNET`
`CONNECT`	`USER=user`	the user name of the APN. Example: `CONNECT 123456 USER=User`
`CONNECT`	`PSW=password`	the password of the APN. Example: `CONNECT 123456 PSW=Password`
`SETHx`	–	thermostat settings: **x** is the number of the thermostat (1, 2, 3 or 4); the parameters are described in the following rows.
`SETHx`	`Ty=45`	the temperature of mode **y** (4 modes can be set). Example – mode 2 of thermostat 1 to +45 °C: `SETH1 123456 T2=45`

Command	Data	Description
`SETHx`	`Sy=2`	the number of the temperature sensor that measures in mode **y** (4 modes can be set). Example – in mode 1 of thermostat 2, temperature sensor 2 measures: `SETH2 123456 S1=2`
`SETHx`	`O=1`	the OUT output assigned to the thermostat (the type of the output must be **Remote Control** or **Thermostat**, section 5.7). Example – output 1 to thermostat 1: `SETH1 123456 O=1`
`SETHx`	`A=2`	the temperature sensor that determines the operation of the thermostat: which of the sensors set for the four modes is the active one. Example – for thermostat 1 the sensor of mode 3 is the active one: `SETH1 123456 A=3`
`SETHx`	`M=C`	the operating mode of the thermostat: **C** – cooling, **H** – heating. Example – thermostat 1 in cooling mode: `SETH1 123456 M=C`
`SETHx`	several settings, with commas	one or more settings can be changed with one SMS, the individual settings are separated by commas. Example: `SETH2 123456 T2=55,S3=5,A=3,O=1,M=H` – the temperature of mode 2 of thermostat 2 is +55 °C; mode 3 works according to temperature sensor 5; the sensor of mode 3 is the active one; the thermostat switches OUT output 1; the operating mode is heating.
`ASKH`	–	SMS about the settings of all thermostats: whether the thermostat is switched on, whether it cools or heats, the number of the active mode and all set temperatures. Example: `ASKH 123456`

Replace the phone number and name in the examples with your own data. The list of APNs: APN settings – list of European mobile operators.

4.3 Control by phone call

If no user has been added to the system yet, whoever calls the CG17 first becomes the administrator of the system: after this, only they can control the CG17 by phone call and SMS command. So make the first call from the owner's or the installer's phone. If you want to allow control by call to other users too, add them in TrikdisConfig (section 5.4) or by SMS command (`SETN`, section 4.2).

Call commands of the CG17 – controlling the OUT outputs by phone call:

1. If the alarm system consists of a single partition, or the user has no right to control the outputs (the **PGM** column of the user list, section 5.4): call the CG17. The panel rejects the call, and the protection mode of the alarm system switches to the opposite: an armed system is disarmed, a disarmed one is armed.
2. If the user has the right to control the OUT outputs, and the type of the OUT output in TrikdisConfig is **Remote Control** (section 5.7), or the CG17 alarm system consists of two or more partitions: call the CG17. The CG17 answers the call, and you can key in the commands on the phone's keypad (see the table).

Commands of the phone's keypad

Keys	Function	Description
`[1]`	changing the protection mode	switches the protection mode to the opposite of the current one. Example: `1`

Keys	Function	Description
`[2][output number][#][state][*]`	controlling the selected OUT output	switches the given OUT output. State: `0` – switching off; `1` – switching on; `2` – switching off for the pulse time; `3` – switching on for the pulse time (you set the pulse time in the **PGM** table of TrikdisConfig, section 5.7); `*` – end of the command. Example – switching on the 5 OUT output: `21#1*`; switching on the 6 OUT output for the pulse time (**Pulse time**) set in the **PGM** table: `22#3*`
`[6][partition number][#]`	arming the given partition of the alarm system	Example – arming partition 2: `62#`
`[7][partition number][#]`	disarming the given partition of the alarm system	Example – disarming partition 1: `71#`

5. Setup with the TrikdisConfig software

You set the parameters of the CG17 with the **TrikdisConfig** program – over a USB cable or remotely (chapter 6). The basic settings needed for the Protegus 2 app and the monitoring station are described in chapter 2; this chapter presents the pages of the program in order.

Az összes Trikdis eszköz egy közös szoftverrel programozható. A program neve TrikdisConfig és a gyártó honlapjáról letölthető.

TrikdisConfig Letöltés a trikdis.com oldalról.

Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

1. Remove the cover of the CG17 with a flat screwdriver as shown in the figure.
2. Connect the CG17 to the computer with a **USB Mini-B** cable.
3. Start TrikdisConfig. The program automatically recognizes the connected CG17 and opens its programming window.
4. Click the **Read [F4]** button: the program reads the current settings of the CG17. If the program asks for it, enter the **administrator** or the **installer** code in the pop-up window (the default codes: section 5.2.2).



Figure 44. Removing the cover: insert the flat screwdriver into the opening on the side of the case, and snap the cover off by levering it downwards. Underneath, on the circuit board, is the **USB Mini-B** connector.

Warning

While the device is connected to a computer via USB cable, it is in programming mode: its normal operation stops, it does not monitor, does not report, cannot be controlled, is powered from USB, and restarts once the cable is unplugged. Therefore the device must not be freely accessible: keep it in a closed metal enclosure with tamper protection or with a motion detector covering the enclosure. More in the FAQ

5.1 The status bar

After connecting the device and reading it (**Read [F4]**), the most important device data are shown at the bottom of the window:

Label	Meaning
IMEI / Unique ID, on an Ethernet device **MAC / Unique ID**	The device's unique identifier: the IMEI on a device with a SIM card, the MAC address on an Ethernet device. The same is printed on the box and on the back of the device.
Status	The current operating status.
Device	The device type (model designation). Check that the type of your own device is shown here.
SN	Serial number.
BL	The bootloader version.
FW	The firmware version.
HW	The hardware version.
State	The connection mode: USB or remote.
Administrator / Installer	The access level of the person programming (after the password has been entered).

After making the settings, you write them to the device with the **Write [F5]** button; with the **Open [F8]** and **Save [F9]** buttons you can save the complete set of settings to a file and load it into another device. **Save [F9]** saves the settings to a settings file, and **Open [F8]** opens the saved file; you can later load the saved settings into other devices as well, so you can quickly set up several devices with identical settings.



Figure 45. The status bar of the CG17: in the left field the **IMEI/Unique ID**, next to it **Status: reading done**, **Device: CG17_1210** (the type code), **SN** (serial number), **BL**, **FW** and **HW** version, **State: USB** (the connection mode) and **Role: Administrator** (the access level). The **Device** field must show the **CG17** type designation.

When you click the **Read [F4]** button, the program reads and displays the settings stored on the CG17; you set the necessary parameters on the pages described in the following sections. If you want to return to the default settings, click the **Restore** button in the bottom left part of the screen (section 5.11).

5.2 "System Options" page

The page has two tabs: on the **System general** tab you enter the general, SIM card and partition settings, on the **Access** tab the access codes.

5.2.1 System general tab

Here you enter the object identifier, the settings of the test messages, time synchronization and event sending, the data of the SIM card and the timings of the partitions.

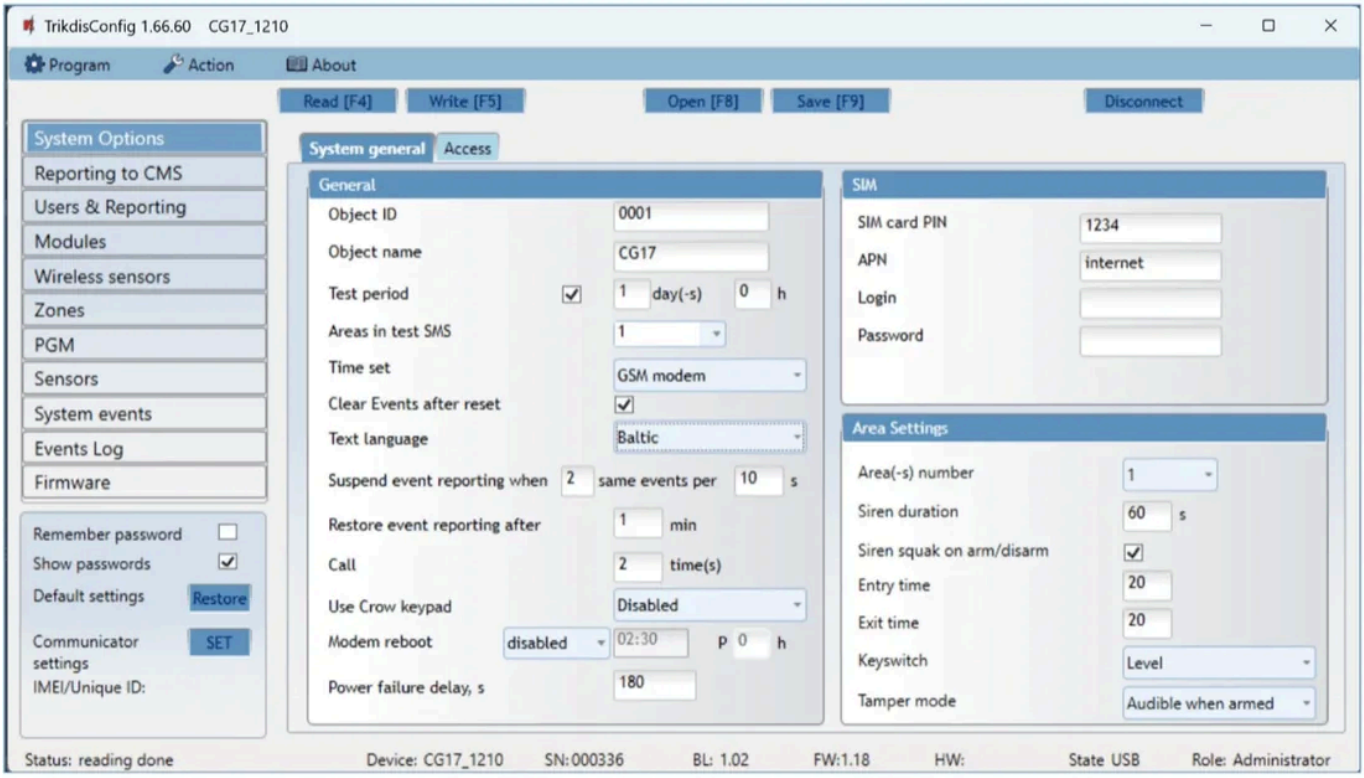


Figure 46. TrikdisConfig – **System Options**, **System general** tab: the **General**, **SIM** and **Area Settings** groups.

General group

- **Object ID** – if you send the events to the monitoring station, enter the object identifier received from the monitoring station (4-digit hexadecimal number, 0–9, A–F). Do not use the identifiers FFFE and FFFF.
- **Object name** – the name of the device, this appears in the SMS messages about the events (up to 20 characters, letters and digits).
- **Test period** – when ticked, the CG17 sends a periodic test message (**Test**) at the set interval.
- **Areas in test SMS** – the test message also contains the state of the selected partitions.
- **Time set** – the source of time synchronization. When **IP server** is selected, the CG17 follows the time of the IP receiver, when **Cellular modem** (**GSM modem** in the picture) is selected, the time of the mobile operator's server.
- **Clear Events after reset** – after a restart (reset) the device deletes all unsent event messages.
- **Text language** – the language of the SMS messages: in the SMS messages the CG17 uses the special characters of this language.
- **Suspend event reporting when … same events per … s** – suspends event sending if the set number of identical events occurs within the set number of seconds.
- **Restore event reporting after** – the suspension of event sending ends after this time (0–999 minutes).
- **Call** – after an event, the CG17 calls the user(s) the set number of times. If the call is rejected or answered, the CG17 stops calling. One call lasts 20 seconds.
- **Modem reboot** – restarting the modem at the set time.

- **AC failure delay** (**Power failure delay, s** in the picture) – if the main power supply fails, the CG17 sends a notification about the power failure after the set delay. When the supply voltage returns, it also sends the notification about the restore after the set delay.

SIM group

- **SIM card PIN** – the PIN code of the SIM card.
- **APN** – the name of the internet access point of the mobile operator. You must enter it if the event messages go over mobile data connection (GPRS) to the Protegus cloud or to the monitoring station. The APNs of the operators: APN settings – list of European mobile operators.
- **Login**, **Password** – if the operator of the SIM card requires it, enter the user name and password of the APN here.

Area Settings group

- **Area(-s) number** – the number of independent parts (partitions) of the alarm system.

If a siren is connected, and an OUT output (assigned to a partition) is of the **Siren** type (section 5.7.1):

- **Siren duration** – in case of alarm, the siren sounds for this time (0–999 s).
- **Siren squak on arm/disarm** – when arming, the siren sounds briefly once, when disarming, twice.
- **Entry time** – entry time through the delayed (**Delay**) zone (0–999 s).
- **Exit time** – exit time through the delayed (**Delay**) zone (0–999 s). If you arm the system from the Protegus 2 app or by phone call, the system does not count the exit time.
- **Keyswitch** – the mode of arming and disarming with the keyswitch (**Keyswitch**) zone: **Pulse** or **Level**.
- **Tamper mode** – the reaction of the system when a detector signals tamper:
- **Silent** – the recipients receive the event message, but the siren does not sound;
- **Audible when armed** – the recipients receive the event message, the siren only sounds if the tamper happens in armed state;
- **Always Audible** – the recipients receive the event message, and the siren also sounds when the system is disarmed.

5.2.2 Access tab – access codes

Here you enter the access codes and the permissions of the installer.

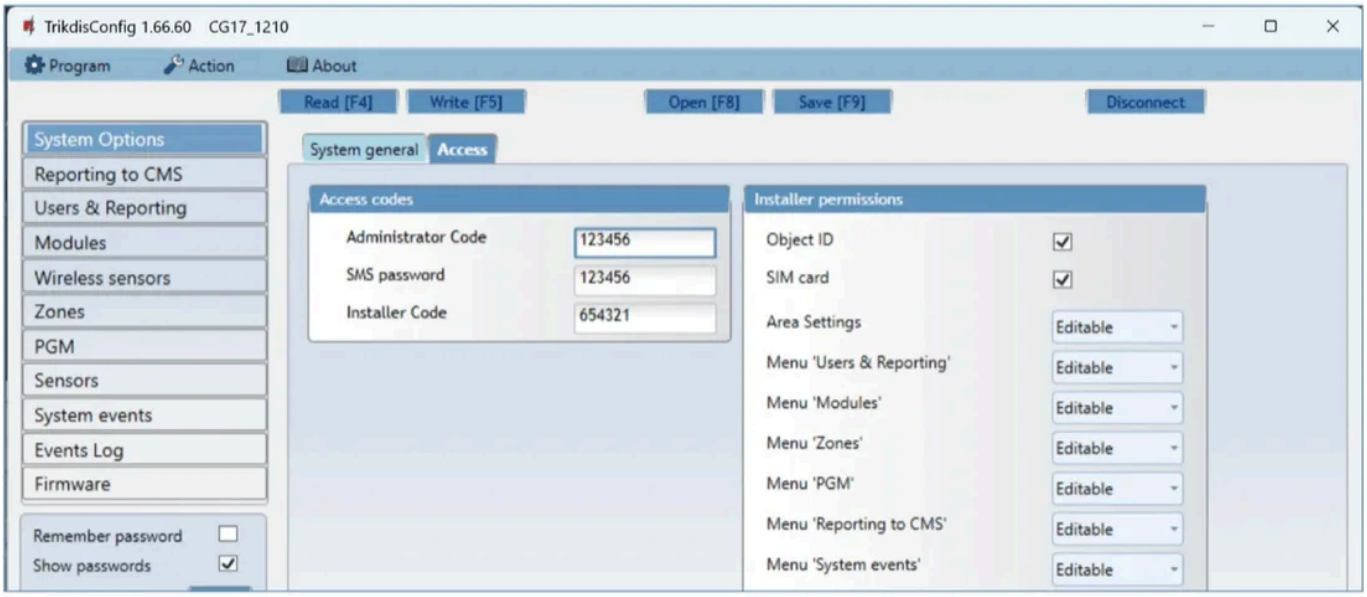


Figure 47. TrikdisConfig – **System Options**, **Access** tab: in the **Access codes** group the **Administrator Code**, the **SMS password** and the **Installer Code**; in the **Installer permissions** group which settings (for example **Object ID**, **SIM card**, **Area Settings**) and which pages (**Users & Reporting**, **Modules**, **Zones**, **PGM**, **Reporting to CMS**, **System events**) the installer may change (**Editable**).

Access codes group

- **Administrator Code** – the administrator code (default `123456`): gives full access to the settings. Exactly 6 characters, Latin letters and/or digits.
- **SMS password** – the password for control by SMS (default `123456`). For greater security, replace it with a 6-character code known only to you.
- **Installer Code** – the installer code (default `654321`): with this the installer accesses the settings. For security, replace it with a 6-character code known only to you.

As long as the default administrator code (`123456`) is set, the program does not ask for the code: when you click the **Read [F4]** button, the settings stored on the device appear immediately.

Installer permissions group

- Here you set the permissions of the installer.

5.3 "Reporting to CMS" page

The CG17 can send the event messages to the monitoring receiver (CMS) of the security company. Here you enter the access of the receiver and the operation of the channels.

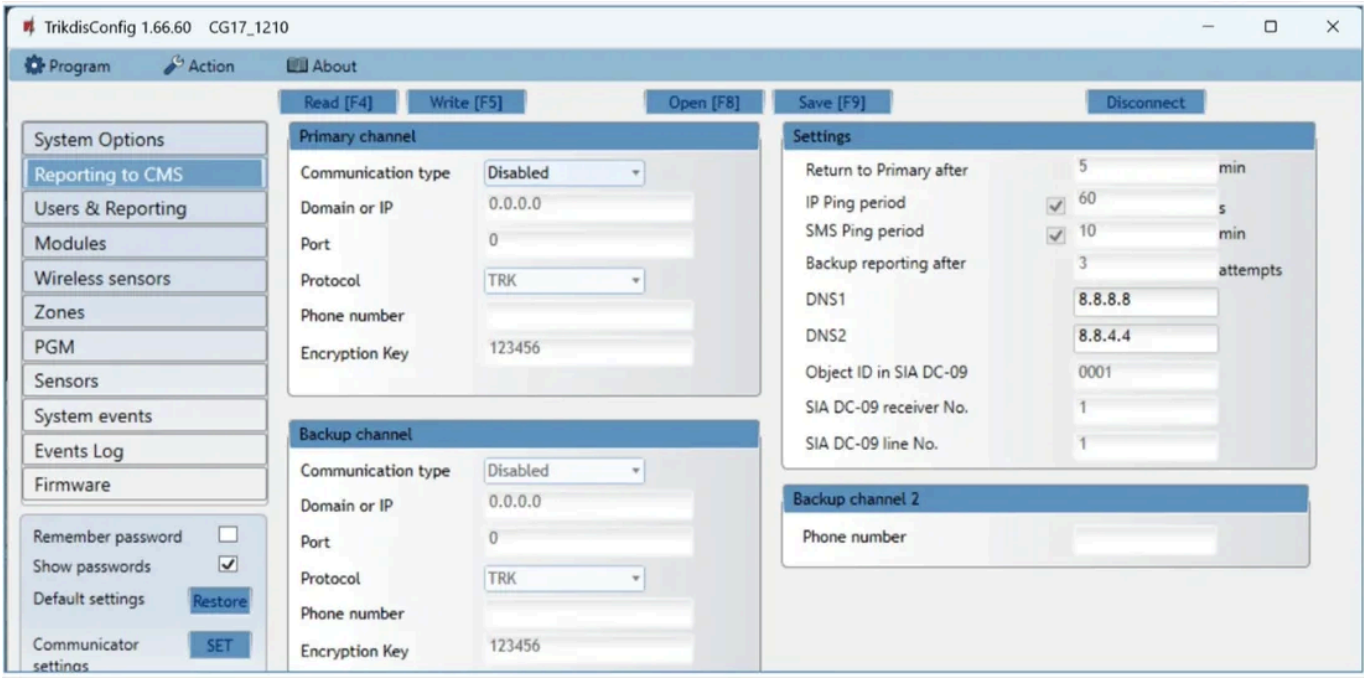


Figure 48. TrikdisConfig – **Reporting to CMS**: the settings of the **Primary channel** and the **Backup channel**, below them the **Settings** group (ping intervals, DNS servers, SIA DC-09 identifiers) and **Backup channel 2** (backup SMS channel).

Primary channel and Backup channel group

- **Communication type** – the mode of the connection with the receiver: **TCP/IP**, **UDP/IP** or **SMS**.
- **Domain or IP** – the domain name or IP address of the receiver.
- **Port** – the network port of the receiver.
- **Protocol** – **TRK** for Trikdis receivers, **SIA DC-09** for universal receivers.
- **Phone number** – the phone number of the monitoring receiver capable of receiving SMS.
- **Encryption Key** – 6-digit encryption key; it must match the key set on the monitoring receiver.

Settings group

- **Return to primary after** – after this many minutes the CG17 tries to return to the main channel (**Primary channel**).
- **IP Ping period** – the sending interval of the connection-checking PING signals over the mobile data connection (GPRS), in seconds. To send the signals, tick the checkbox.
- **SMS PING period** – the sending interval of the connection-checking PING signals on the SMS channel, in minutes. To send the signals, tick the checkbox.
- **Backup reporting after** – after this many unsuccessful sending attempts the CG17 switches from the main channel to the backup channel (**Backup channel**).
- **DNS1**, **DNS2** – the addresses of the DNS servers.
- **Object ID in SIA DC-09** – the object number with the SIA DC-09 protocol.
- **SIA DC-09 receiver No.** – the number of the receiver.
- **SIA DC-09 line No.** – the number of the line.

Backup channel 2 group

- **Phone number** – the phone number of the monitoring receiver capable of receiving SMS, with the country code (for example CCxxxxxxxxx, where CC is the country code). The CG17 uses this backup SMS channel (**Backup SMS**) if it cannot send the message on either the main (**Primary**) or the backup (**Backup**) channel. It also works if the IP connection is lost in the mobile operator's network. It only

works if GPRS (mobile data) mode is set on both the main and the backup channel. The CG17 sends an SMS to the receiving station: 1) when you first switch it on; 2) if the TCP/IP or UDP/IP connection is lost on the main and the backup channel.

5.4 "Users & Reporting" page

On the **Users** tab you set the users, the connection with the Protegus cloud and the touch keys (iButton); on the **SMS answer texts** tab the text of the reply SMS messages (section 5.4.3).

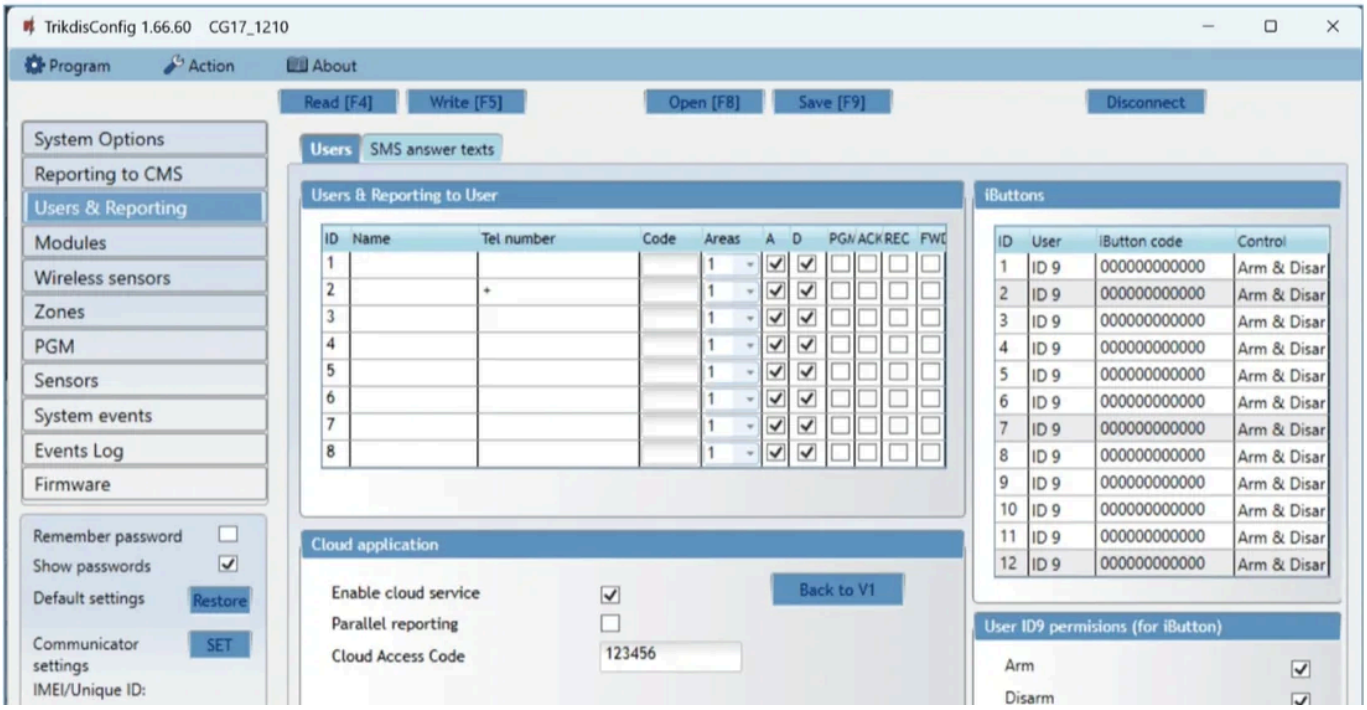


Figure 49. TrikdisConfig – **Users & Reporting**, **Users** tab: the user list (**Name**, **Tel number**, **Code**, **Areas**, **A**, **D**, **PGM**, **ACK**, **REC**, **FWD** columns), below it the **iButtons** list, next to it the **Cloud application** group and the permissions of **User ID9** (**Arm**, **Disarm**).

Users & Reporting to User group

- **ID** – the position of the user on the list.
- **Name** – the name or e-mail address of the user; this name appears in the SMS messages about the events. The administrator can also give the user an e-mail address: with this the user can log in to the Protegus 2 app.
- **Tel number** – the phone number of the user, with the international prefix (for example +CC…). From this number the alarm system can be controlled remotely, and the SMS messages arrive at this number.
- **Code** – the user's own code for arming and disarming.
- **Areas** – the partitions that the user may control. **User ID9** may only control partition 1; this cannot be changed.
- **A** – tick it if the user may arm (ARM) the system.
- **D** – tick it if the user may disarm (DISARM) the system.
- If **PGM** and **REC** are not ticked, but **A** and **D** are: when the user calls the CG17, the panel rejects the call, and the state of the alarm system switches to the opposite (it is armed or disarmed).
- If only **PGM** is ticked: the user can call the CG17, and with DTMF tone commands (the phone's keypad) switch the desired output on or off (section 4.3).
- **REC** – reserved for a future function.
- **ACK** – when ticked, the CG17 sends a reply message (**SMS answer text**) to the user after every command received by SMS (section 5.4.3).

- **FWD** – when ticked, the CG17 forwards to the user the SMS messages received from senders outside the system (for example the balance notification of the SIM card, advertising messages).

Cloud application group

- **Enable cloud service** – switches on the Protegus service (**Protegus service**): the CG17 can exchange data with the Protegus 2 app, and it can also be set up remotely with TrikdisConfig (chapter 6).
- **Parallel reporting** – sends the messages on the main channel and to Protegus 2 in parallel.
- **Cloud Access Code** – 6-digit code for connecting to Protegus 2 (default `123456`, section 2.1).

iButtons group

Several keys can be assigned to one user. Every newly registered key goes to the **User ID9** (No name) user. Names can only be given to eight users. You set the permissions of **User ID9** in the **User ID9 permissions** group.

- **ID** – the position of the key on the list.
- **User** – the user to whom the key belongs. If you want to assign the key to a user, write the position of the user from the **Users & Reporting to User** table in place of **ID9** (for example for user 3: **ID3** instead of **ID9**).
- **iButton code** – the identification number of the iButton touch key or of the RFID card.
- **Control** – what the system should do when the reader (for example the TM17) reads the key: **None** (nothing), **Arm**, **Disarm** or **Arm & Disarm**.

5.4.1 Registering touch keys (iButton)

The wiring of the key reader is described in section 3.6. You register the touch keys as follows:

1. If the **iButtons** list is empty, the first registered key goes to the first row of the list, and it becomes the master key (**Master key**).
2. To switch on registration mode, hold the master key to the reader for at least 10 seconds. In registration mode, the **State** LED of the TM17 reader blinks green.
3. Hold the user keys to the reader one by one. The reader indicates with 3 beeps that it has registered the key.
4. When you have finished with the user keys, hold the master key to the reader again to switch off registration mode. The **State** LED of the TM17 then stops blinking.
5. To delete all keys (including the master key), hold the master key to the reader for at least 20 seconds.

Use the master key only for registering the other touch keys.

5.4.2 Registering RFID cards

For this, the CG17 needs an iO-LORA module with an RFID reader with keypad connected to it (section 3.16). Enter the identification number of the RFID card in the **iButton code** field of the **iButtons** list.

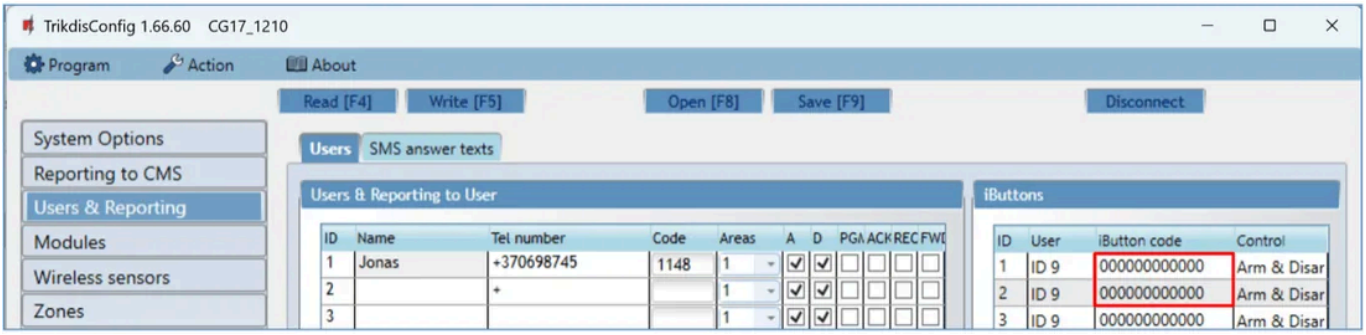


Figure 50. TrikdisConfig – **Users** tab: on the user list an example user (**Jonas**) with a phone number; on the **iButtons** list the **iButton code** field framed in red, this is where the identification number of the RFID card goes.

After the changes, click the **Write [F5]** button and wait until the update is finished.

5.4.3 SMS answer texts tab – reply SMS messages

Here you can rewrite the text of the reply messages that the CG17 sends to the SMS commands (section 4.2).

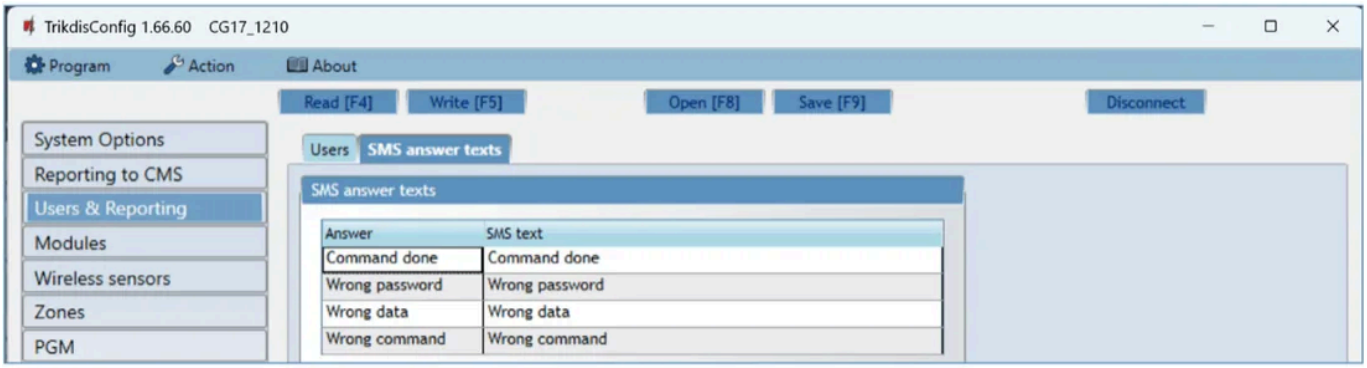


Figure 51. TrikdisConfig – **Users & Reporting**, **SMS answer texts** tab: the text of the **Command done**, **Wrong password**, **Wrong data** and **Wrong command** replies.

SMS answer texts group

- You can edit the text of the replies to the control commands sent by SMS in the **SMS text** field.

5.5 "Modules" page

Here you add the modules connected to the CG17 on the RS485 bus. After selecting the **W485** or the **E485**, the settings tab of the module appears (**W485 settings**, **E485 settings**); the settings of the GPS module are on the **Internal modules** tab (section 5.5.4).

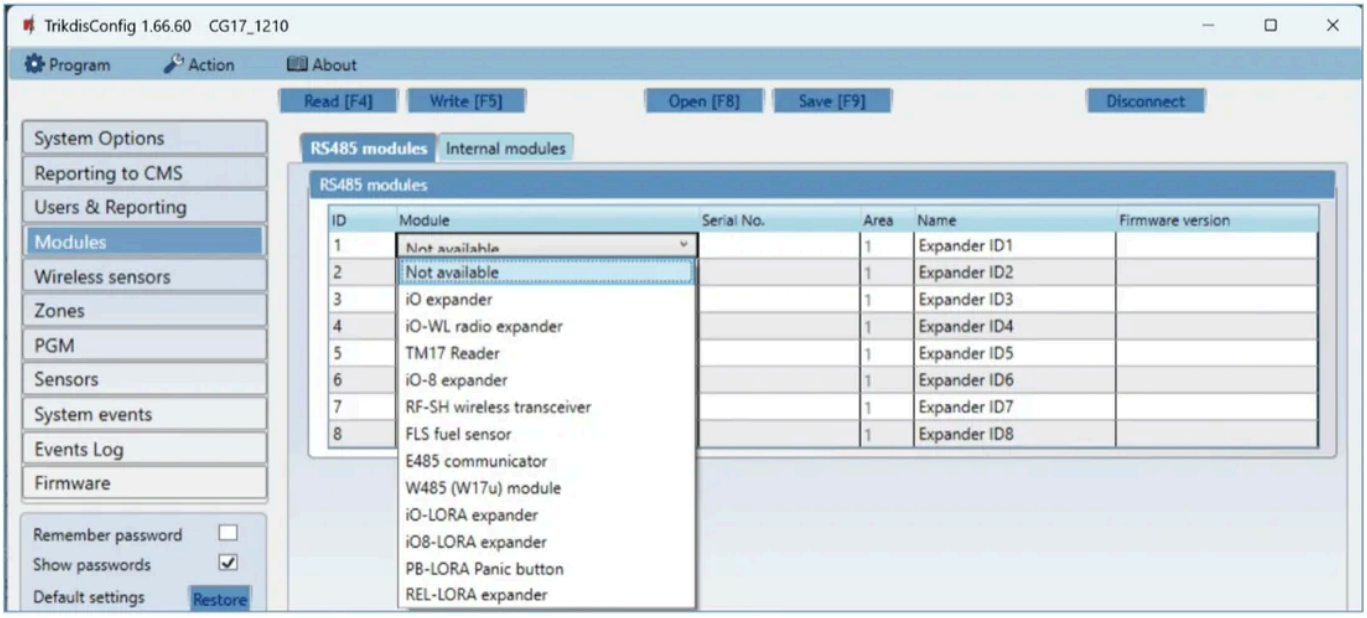


Figure 52. TrikdisConfig – **Modules**, **RS485 modules** tab: in the **Module** drop-down list the selectable modules, for example **iO expander**, **iO-WL radio expander**, **TM17 Reader**, **iO-8 expander**, **FLS fuel sensor**, **E485 communicator**, **W485 (W17u) module**, **iO-LORA expander**, **iO8-LORA expander**, **PB-LORA Panic button**, **REL-LORA expander**.

RS485 modules group

- **ID** – the position of the module on the list.
- **Module** – select the module used from the list: **iO**, **iO-WL**, **TM17**, **iO8**, **FLS**, **E485**, **W485**, **iO-LORA**, **iO8-LORA**, **PB-LORA**, **REL-LORA**.
- **Serial No.** – the 6-digit serial number of the module, it must be entered; you can find it on the sticker on the case and the packaging of the module.
- **Area** – the partition to which you assign the module. The TM17 shows the state of the partition to which it is assigned and of the zones assigned to that partition.
- **Name** – you can give the module a name.
- **Firmware version** – the firmware version of the module; it appears when the CG17 has detected the connected module.

Wiring of the modules: TM17 – section 3.6; iO8 and iO-WL – section 3.7; iO – section 3.9; Strela RS485 (FLS) – section 3.10; W485 – section 3.14; E485 – section 3.15; iO-LORA, iO8-LORA, PB-LORA and REL-LORA (through the RF-LORA transceiver) – section 3.16.

5.5.1 W485 settings tab – Wi-Fi module

After selecting the **W485** Wi-Fi module, on this tab you enter the data of the Wi-Fi network and the way the SIM card is used.

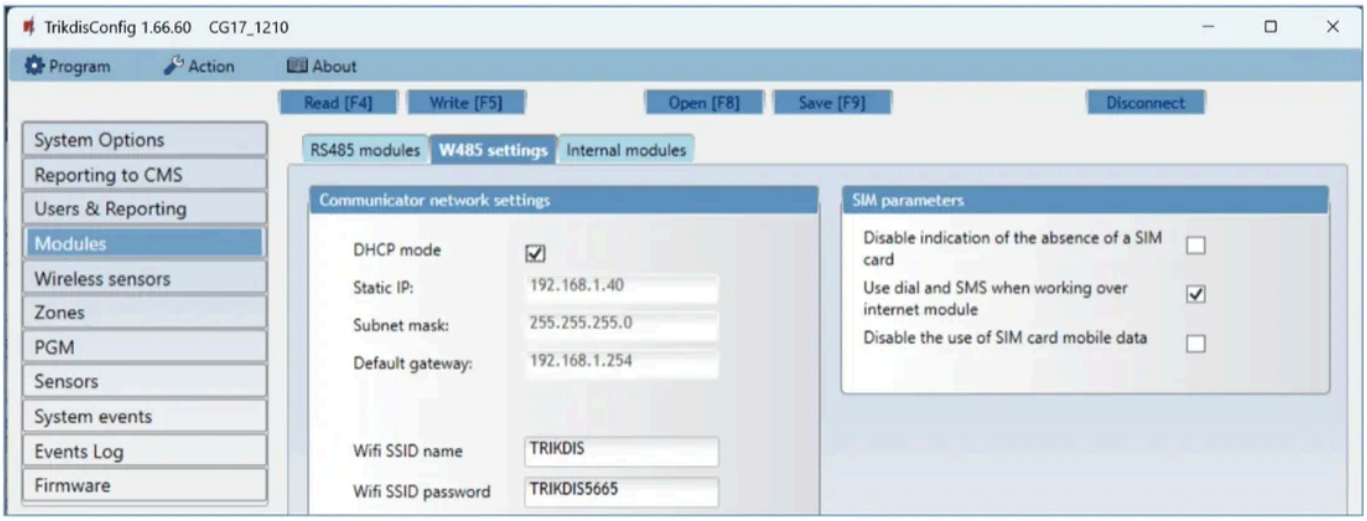


Figure 53. TrikdisConfig – **Modules**, **W485 settings** tab: the **Communicator network settings** group (DHCP, IP address, subnet mask, gateway, the name and password of the Wi-Fi network) and the **SIM parameters** group.

Communicator network settings group

- **DHCP mode** – the mode of network registration of the Wi-Fi module: automatic or manual.
- **Static IP** – the fixed IP address in manual mode.
- **Subnet mask** – the subnet mask in manual mode.
- **Default gateway** – the address of the gateway in manual mode.
- **Wifi SSID name** – the name of the Wi-Fi network to which the W485 connects.
- **Wifi SSID password** – the password of the Wi-Fi network.

SIM parameters group

- **Disable indication of the absence of a SIM card** – when ticked, the CG17 does not indicate the absence of the SIM card if it works without a SIM card.
- **Use dial and SMS when working over internet module** – when ticked, the CG17 sends notifications by call, by SMS and through the connected W485 Wi-Fi module at the same time. If you leave it empty and there is a Wi-Fi network, the CG17 does not use SMS and calls. If you leave it empty and there is no Wi-Fi network, the CG17 handles calls and SMS messages, and sends an SMS to the user.
- **Disable the use of SIM card mobile data** – when ticked, the CG17 does not use the mobile data of the SIM card: the data only go through the W485 module. If the Wi-Fi network is lost, the CG17 stores the data in its memory and sends them through the W485 when the network returns.

You can assign a Contact ID event and restore code to the RS485 data bus fault event. If the connection between the W485 and the CG17 is lost or restored, the CG17 sends a message with the assigned CID code to the monitoring station and to the Protegus 2 app. The event appears on the **System events** page under the name **RS485 fault** (section 5.9.1).

- Set the CG17 to send the messages to the monitoring station and to Protegus 2: see section 2.2 (connection with the monitoring station) and section 2.1 (connection with the Protegus 2 app).
- If the CG17 (from firmware version 1.13) works with the W485 module, it does not need a SIM card.

5.5.2 E485 settings tab – Ethernet module

After selecting the **E485** Ethernet module, on this tab you enter the data of the wired network and the way the SIM card is used.

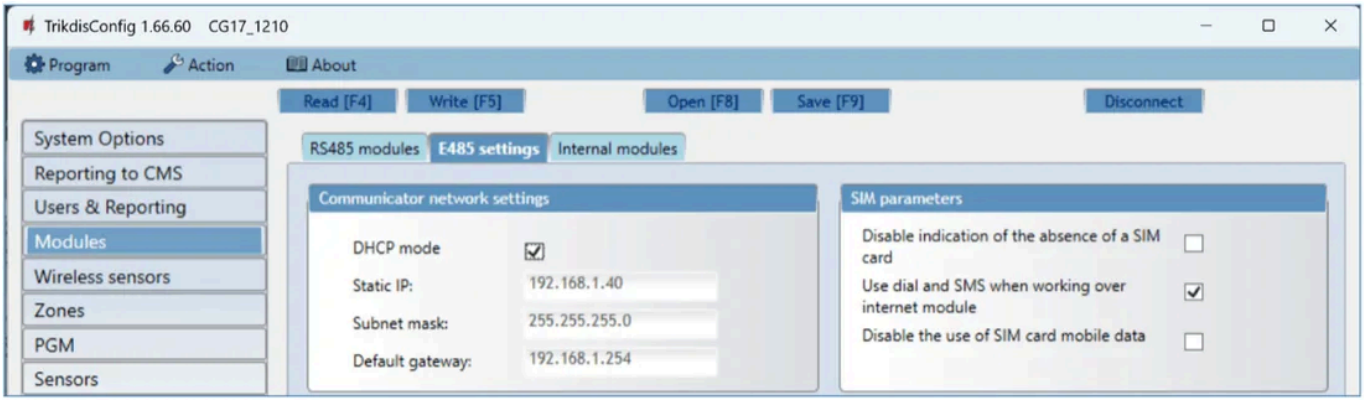


Figure 54. TrikdisConfig – **Modules**, **E485 settings** tab: the **Communicator network settings** group (DHCP, IP address, subnet mask, gateway) and the **SIM parameters** group.

Communicator network settings group

- **DHCP mode** – the mode of network registration of the Ethernet module: automatic or manual.
- **Static IP** – the fixed IP address in manual mode.
- **Subnet mask** – the subnet mask in manual mode.
- **Default gateway** – the address of the gateway in manual mode.

SIM parameters group

- **Disable indication of the absence of a SIM card** – when ticked, the CG17 does not indicate the absence of the SIM card if it works without a SIM card.
- **Use dial and SMS when working over internet module** – when ticked, the CG17 sends notifications by call, by SMS and through the connected E485 Ethernet module at the same time. If you leave it empty and there is an internet connection, the CG17 does not use SMS and calls. If you leave it empty and there is no internet connection, the CG17 handles calls and SMS messages, and sends an SMS to the user.
- **Disable the use of SIM card mobile data** – when ticked, the CG17 does not use the mobile data of the SIM card: the data only go through the E485 module. If the internet connection is lost, the CG17 stores the data in its memory and sends them through the E485 when the connection returns.

You can assign a Contact ID event and restore code to the RS485 data bus fault event. If the connection between the E485 and the CG17 is lost or restored, the CG17 sends a message with the assigned CID code to the monitoring station and to the Protegus 2 app. The event appears on the **System events** page under the name **RS485 fault** (section 5.9.1).

- Set the CG17 to send the messages to the monitoring station and to Protegus 2: see section 2.2 (connection with the monitoring station) and section 2.1 (connection with the Protegus 2 app).
- If the CG17 (from firmware version 1.13) works with the E485 module, it does not need a SIM card.

5.5.3 Strela RS485 fuel level sensor

Discontinued accessory

The **Strela RS485** fuel level sensor is a discontinued accessory and is not available from us. The setup has been kept for existing systems.

You set up the **Strela RS485** fuel level sensor (wiring: section 3.10) on the **Modules** and **Sensors** pages.

Before use, the Strela RS485 sensor must be calibrated with the **DUTconfig** program of the sensor's maker: connect the sensor to the computer with an adapter, and calibrate it. If the Strela RS485 is connected to the CG17, the other RS485 modules (iO, iO-WL, TM17, iO8, E485, W485, iO-LORA, iO8-LORA, PB-LORA, REL-LORA) do not work.

RS485 modules group

- **Module** – select the **FLS fuel sensor** module.

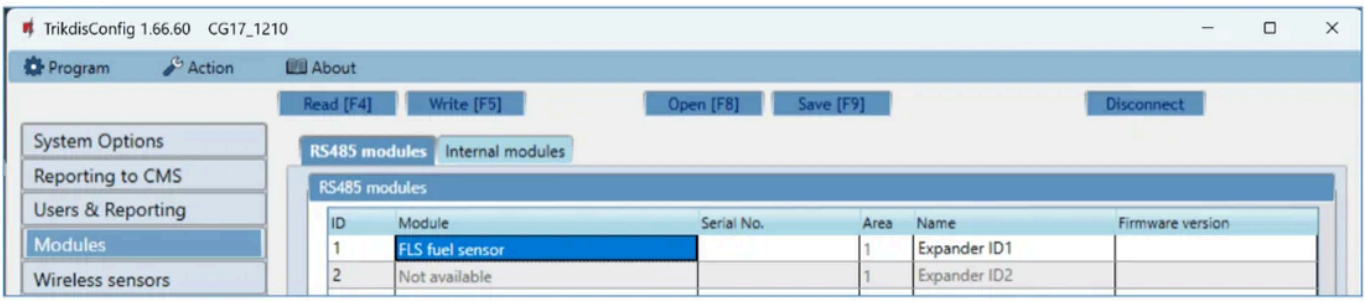


Figure 55. TrikdisConfig – **Modules**, **RS485 modules** tab: in row 1 the **FLS fuel sensor** (fuel level sensor) selected.

1. Click the **Write [F5]** button and wait until saving of the data is finished.
2. Unplug the USB cable from the CG17 and wait about 1 minute.
3. Plug the USB cable back into the CG17 and click the **Read [F4]** button. The program reads and displays the settings stored on the CG17.
4. The serial number (**Serial No.**) and the firmware version (**Firmware version**) of the Strela RS485 sensor appear on the **Modules** page.

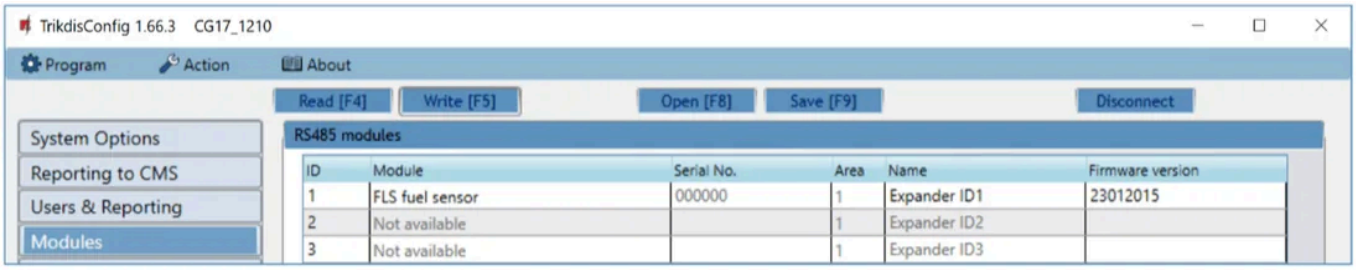


Figure 56. After reading, the serial number (**Serial No.**) and the firmware version (**Firmware version**) of the sensor appear in the row of the **FLS fuel sensor**.

Then open the **Sensors** page (section 5.8).

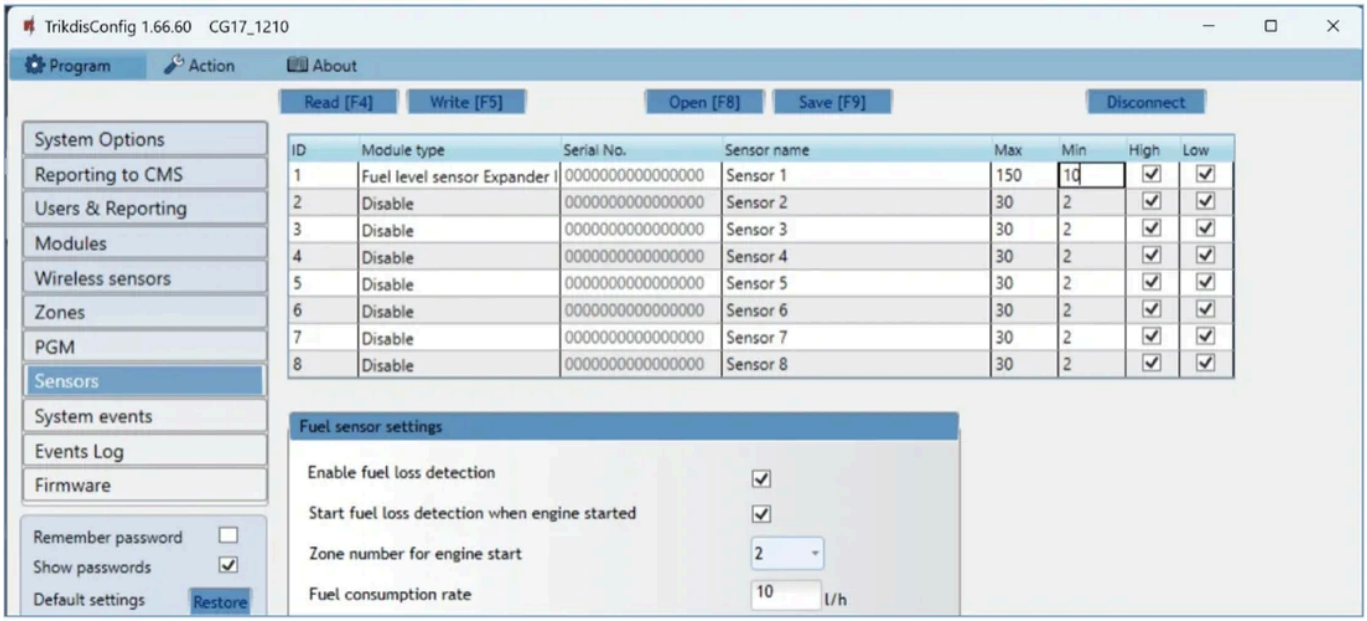


Figure 57. TrikdisConfig – **Sensors**: in row 1 the **Fuel level sensor** with the **Max** and **Min** values, below it the **Fuel sensor settings** group.

- **Module type** – choose the **Fuel level sensor** type.
- **Sensor name** – give the sensor a name.
- **Max** – the largest amount of fuel in litres. If the actual amount is more than this, the CG17 generates an event message; to send the message, tick the **High** checkbox.
- **Min** – the smallest amount of fuel in litres. If the actual amount is less than this, the CG17 generates an event message; to send the message, tick the **Low** checkbox.

Fuel sensor settings group

- **Enable fuel loss detection** – when ticked, the CG17 monitors the fuel level.
- **Start fuel loss detection when engine started** – when ticked, monitoring starts when the engine is started. The engine start signal must be led to the input (zone) of the CG17 that you enter in the next field.
- **Zone number for engine start** – the number of the input (IN) of the CG17 that is activated by the engine start.
- **Fuel consumption rate** – the rate of fuel consumption (l/h).

The user receives an SMS about a sudden change of the fuel level; you can edit the text of the SMS on the **System events** page (section 5.9.1).

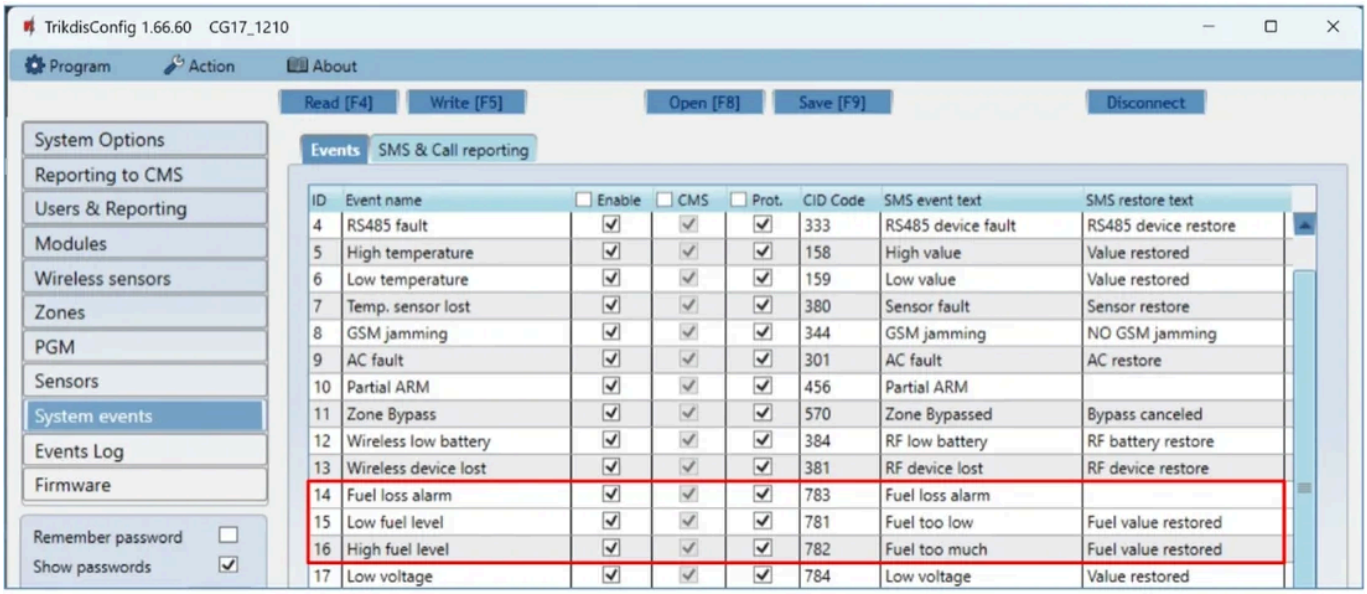


Figure 58. TrikdisConfig – **System events**: framed in red the fuel events – **Fuel loss alarm**, **Low fuel level**, **High fuel level** – with their Contact ID code and SMS text.

Operation of the fuel level sensor

Connect the Strela RS485 sensor to the CG17 as described in section 3.10, and set the measuring parameters in the CG17. The sensor measures in the following cases:

1. If **Enable fuel loss detection** is ticked: when the CG17 is switched on, the sensor starts monitoring the fuel consumption, and when the CG17 is switched off, the measurement stops.
2. If both **Enable fuel loss detection** and **Start fuel loss detection when engine started** are ticked, and you have entered the number of the input (IN) that switches on monitoring when the engine is started: monitoring starts when the engine is started, and stops when the input restores (the engine stops).

At every switch-on, the sensor measures the current fuel level and compares it with the level stored before switching off. If the current level is lower, the CG17 sends a message about fuel loss to the security company and/or to the users.

During operation, the sensor measures the fuel level at set intervals and compares it with the consumption rate. If within an interval the consumption is greater than the set rate (**Fuel consumption rate**), the CG17 sends a message to the security company and/or to the users.

5.5.4 Internal modules tab – GPS module

On this tab you enter the settings of the GPS module: the sending interval of the coordinates, movement detection and the alarm.

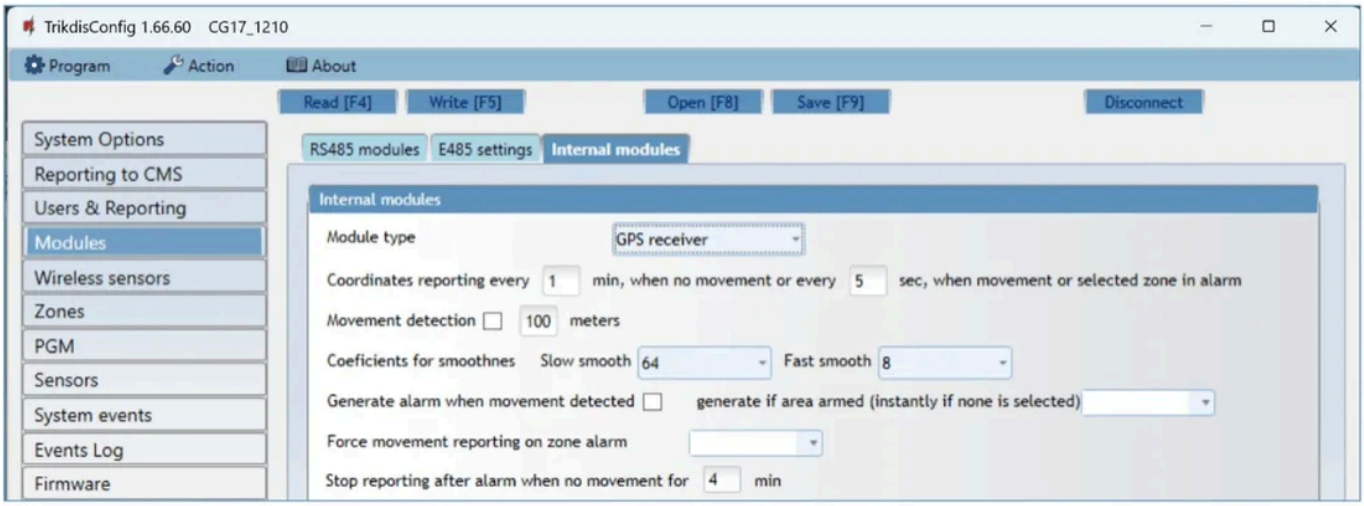


Figure 59. TrikdisConfig – **Modules**, **Internal modules** tab: the GPS receiver (**GPS receiver**) with the intervals of coordinate sending, the distance of movement detection (in metres), the smoothing coefficients and the alarm settings.

Internal modules group

- **Module type** – select the GPS module used.
- **Coordinates reporting every __ min, when no movement or every __ sec, when movement or selected zone in alarm** – the sending interval of the coordinates: in minutes in normal operation (no movement), in seconds if the CG17 detects movement or the selected zone is in alarm.
- **Movement detection** – when ticked, the CG17 raises an alarm if the deviation of the coordinates is greater than the set value; in this case it sends the coordinates more often.
- **Coefficients for smoothness, Slow smooth** – without movement, the CG17 sends averaged coordinates: the average of the set number of coordinates (256 or another set number).
- **Coefficients for smoothness, Fast smooth** – during movement or a zone alarm, the CG17 sends averaged coordinates: the average of the set number of coordinates (8 or another set number).
- **Generate alarm when movement detected** – when ticked, on detecting movement the CG17 sends a Contact ID event code to the monitoring station and notifies the user in Protegus 2.
- **Force movement reporting on zone alarm** – enter the zone of the alarm system to which a detector is connected. If the detector signals (zone alarm), the CG17 sends the coordinates more often.
- **Stop reporting after alarm when no movement for __ min** – time in minutes: if during this time the coordinates do not change and there is no zone alarm, coordinate sending returns to normal mode.

The messages containing the coordinates arrive in the **Monas MS** monitoring program.

5.6 "Zones" page

On the **Zones** page you set the zones (**Zones settings** tab), and which users receive an SMS or a call about the zone events (**SMS & Call reporting** tab).

5.6.1 Zones settings tab – the zones

Here you assign an input, a partition, a zone type and a Contact ID code to each zone.

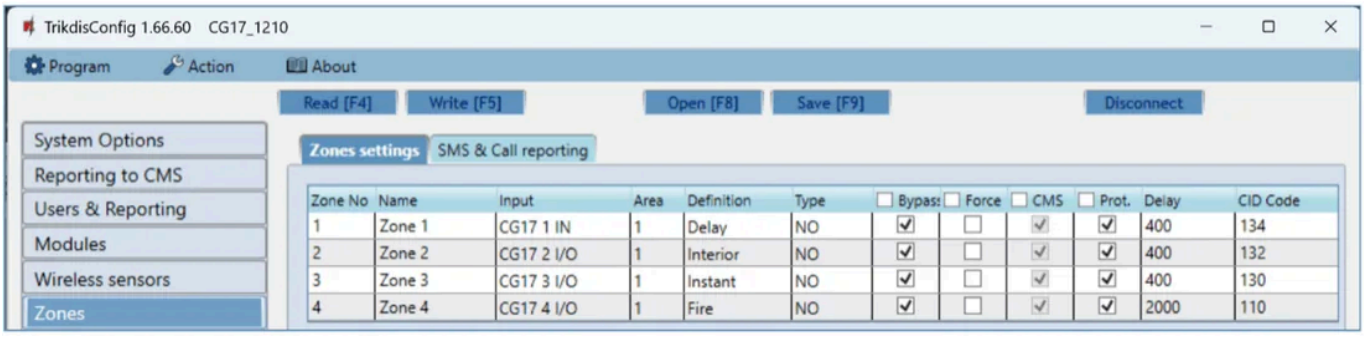


Figure 60. TrikdisConfig – **Zones**, **Zones settings** tab: four zones with name, input (**Input**), partition (**Area**), zone type (**Definition**: Delay, Interior, Instant, Fire), circuit type (**Type**), the **Bypass**, **Force**, **CMS** and **Prot.** checkboxes, the reaction time (**Delay**) and the Contact ID code (**CID Code**).

- **Zone No** – the position of the zone on the list.
- **Name** – the name of the zone.
- **Input** – the input (IN) assigned to the zone: an input of the CG17 or of an expansion module.
- **Area** – the partition to which the zone belongs.
- **Definition** – the type of the zone. You can choose one for each zone:
- **Delay** – delayed zone, for the opening sensor of the entrance door. Entry and exit time can be set for this zone type. After arming, violating the zone is allowed within the exit time; if the zone is still violated when the time expires, the **Siren** and **Flash** type OUT outputs switch on, and the CG17 sends an alarm message. In an armed system, violating the zone starts the entry time, within which the system must be disarmed; if the system is not disarmed when the time expires, the **Siren** and **Flash** outputs switch on, and the CG17 sends an alarm message.
- **Interior** – follower zone, for the motion detector belonging to the entrance door. In an armed system, when the zone is violated, the **Siren** and **Flash** outputs switch on, and the CG17 sends an alarm message. If in an armed system the **Delay** zone is violated first, the **Interior** zone may also be violated within the set entry time; if you do not disarm the system before the entry time expires, the **Siren** and **Flash** outputs switch on, and the CG17 sends an alarm message.
- **Instant** – instant zone, for motion detectors. If it is violated in an armed system, the **Siren** and **Flash** outputs switch on, and the CG17 sends a message about the alarm.
- **Fire** – fire zone, for fire detectors. When it is violated, the **Siren** and **Flash** outputs switch on immediately, and the CG17 sends a message about the event.
- **Keyswitch** – keyswitch zone, for a keypad or another switch. If the switch violates the zone, the system is armed or disarmed. When arming, the system is armed when the set exit time (**Exit time**) has expired.
- **24 hours** – 24-hour zone, for glass break and tamper detectors. When it is violated, the **Siren** and **Flash** outputs switch on immediately, and the CG17 sends a message about the event.
- **Silent** – silent zone: if it is violated in an armed system, the CG17 immediately sends an event message, but the **Siren** and **Flash** outputs do not switch on.
- **Silent 24h** – silent 24-hour zone, for panic buttons: when it is violated, the CG17 immediately sends an event message regardless of the state of the system, but the **Siren** and **Flash** outputs do not switch on.
- **Type** – the type of the circuit connected to the input (IN) (section 3.2): **NC** – normally closed; **NO** – normally open; **EOL** – with a 10 kΩ end-of-line resistor; **EOL_T** – with an end-of-line resistor and tamper monitoring.
- **Bypass** – when ticked, the zone is bypassed: the CG17 ignores its signal.
- **Force** – when ticked, the system can also be armed with an open zone. In an armed system, violating a zone in **Force** mode triggers an alarm.
- **CMS** – when ticked, the events of the zone go to the monitoring station (CMS).
- **Prot.** – when ticked, the events of the zone go to the Protegus cloud.

- **Delay** – the reaction time of the input (IN) in milliseconds (ms).
- **CID code** – the Contact ID code of the events. The program sets it automatically when the zone type (**Definition**) is selected.

5.6.2 SMS & Call reporting tab

This tab is only visible if you have entered the phone number of at least one user on the **Users & Reporting** page (section 5.4).

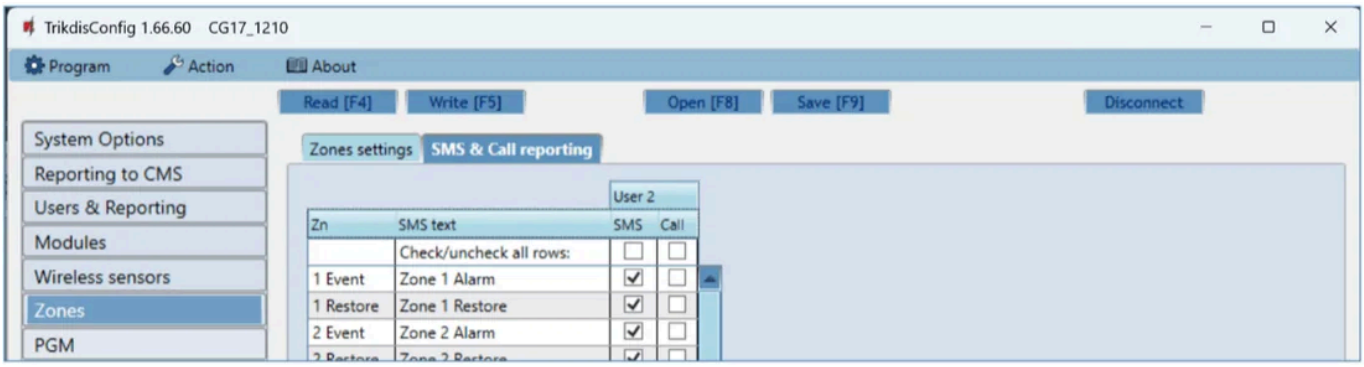


Figure 61. TrikdisConfig – **Zones**, **SMS & Call reporting** tab: the SMS text of the zone events (**Event**) and the restores (**Restore**), with **SMS** and **Call** checkboxes per user (**User 2**).

- **Zn** – the number of the zone with the identifying word of the event: **Event** or **Restore**.
- **SMS text** – the description of the zone event in the SMS messages sent to the users.
- **SMS/Call** – mark how the users should be notified about the events: by SMS and/or by call.

The modem places the call over 2G or VoLTE. Where the operator has switched off 2G and has not approved the modem for VoLTE, the SMS arrives but the phone does not ring. This is not a configuration error. In such places, use SMS and the Protegus 2 app.

5.7 "PGM" page

On the **PGM** page you set the operation of the OUT outputs, their control linked to events, scheduling, the thermostats and the SMS and call notification of the outputs.

5.7.1 Outputs tab – the outputs

Here you assign the OUT outputs of the CG17 or of external devices to the PGMs, and set their operation.

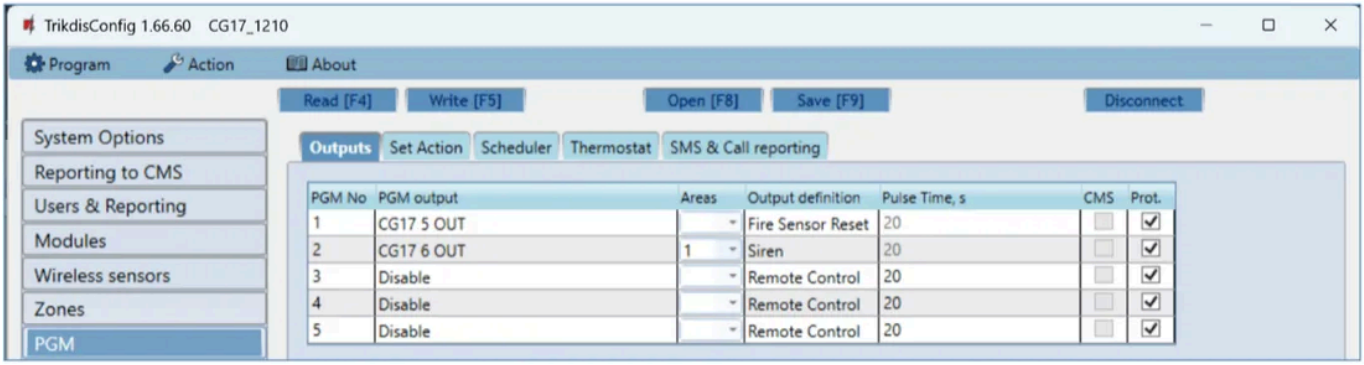


Figure 62. TrikdisConfig – **PGM**, **Outputs** tab: the PGMs with the assigned output, partition (**Areas**), operation (**Output definition**, for example **Fire Sensor Reset**, **Siren**, **Remote Control**), pulse time (**Pulse Time**) and the **CMS**, **Prot.** checkboxes.

- **PGM No** – the position of the PGM on the list.

- **PGM output** – the OUT output assigned to the PGM: an output of the CG17 or of an external device.
- **Areas** – the partition to which you assign the output.
- **Output definition** – the operating mode of the OUT output:
- **Siren** – for connecting a siren (section 3.8);
- **Remote Control** – for controlling external devices;
- **Fire Sensor Reset** – for resetting the fire detector after an alarm (section 3.3);
- **System state** – for a state indicator of the alarm system; for example an LED can show whether the system is armed or disarmed (section 3.5);
- **Flash** – gives a continuous signal in an armed system, a pulsed signal in case of alarm; when the system is disarmed, the signal stops;
- **Thermostat** – the CG17 controls the OUT output according to the temperature of the set temperature sensor (section 5.7.4).
- **Pulse time, s** – the switch-on time of the OUT output, 0–9999 s.
- **CMS** – when ticked, the messages about switching the PGM output on and off go to the monitoring station (CMS).
- **Prot.** – when ticked, the messages about switching the PGM output on and off go to the Protegus cloud.

5.7.2 Set Action tab – control on an event

Here you set which event switches the OUT outputs automatically.

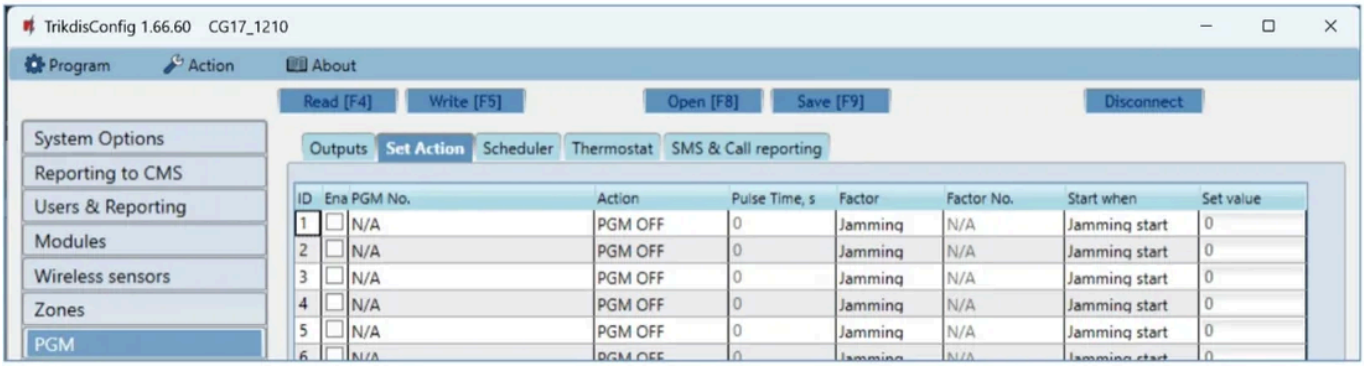


Figure 63. TrikdisConfig – **PGM**, **Set Action** tab: the rows of the rules with the enabling checkbox, the controlled PGM (**PGM No.**), the action (**Action**, for example **PGM OFF**), the pulse time, the triggering event (**Factor**, for example **Jamming** – jamming of the mobile signal), and the **Factor No.**, **Start when** (for example **Jamming start**) and **Set value** columns.

- **ID** – the position of the output on the list.
- **Enable** – switches on the PGM.
- **PGM No.** – the controlled OUT output: the CG17 switches this when the event set in the **Factor**, **Factor No.**, **Start when** and **Set value** columns occurs.
- **Action** – the action:
- **PGM OFF** – the OUT output goes into the switched-off ("Off") state;
- **PGM ON** – the OUT output goes into the switched-on ("On") state;
- **Pulse OFF** – the default state of the output is switched on ("On"); on the command it switches off ("Off") for the pulse time (**Pulse time**), then automatically returns to the switched-on default state;
- **Pulse ON** – the default state of the output is switched off ("Off"); on the command it switches on ("On") for the pulse time (**Pulse time**), then automatically returns to the switched-off default state.
- **Pulse time, s** – the pulse time, 0–9999 s.
- **Factor/Factor No.** – the event that switches the OUT output: **Zone**, **Sensor**, **Schedule**, **Jamming** (jamming of the mobile signal), **Sensor lost** (loss of a sensor), **iButton** (touch key), **Arm**, **Disarm**, **SMS received** (incoming SMS).

- You can also assign a schedule to the output, so that it switches at the set times. On the **Scheduler** tab you can prepare 10 schedules (section 5.7.3).
- **Start when** – further condition depending on the **Factor** event: when the OUT output should switch on.
- **Set value** – depending on the condition chosen in the **Factor** column (**SMS received**, **Sensor**), here you enter the value with which the PGM output can be controlled: the text of the incoming SMS, or the voltage or temperature value (voltage measurement: section 3.13; temperature sensor: section 3.4).

In the SMS text, the control keyword is separated from the rest of the SMS by `%` signs:

- `%.....%` – a part of the text of the incoming SMS must match the text written between the `%` signs. Example: `%sMS%` – the SMS must contain the text "sMS"; such an SMS: `1155sMS332`.
- `.....%` – the beginning of the text of the incoming SMS must match the text written before the `%` sign. Example: `sMS%` – the SMS must start with "sMS"; such an SMS: `sMS332`.
- `%.....` – the end of the text of the incoming SMS must match the text written after the `%` sign. Example: `%sMS` – the SMS must end with "sMS"; such an SMS: `1155sMS`.

In the SMS text, lower case and upper case letters are different.

5.7.3 Scheduler tab – scheduling

Here you prepare the schedules (up to 10) that you can assign to the outputs on the **Set Action** tab.

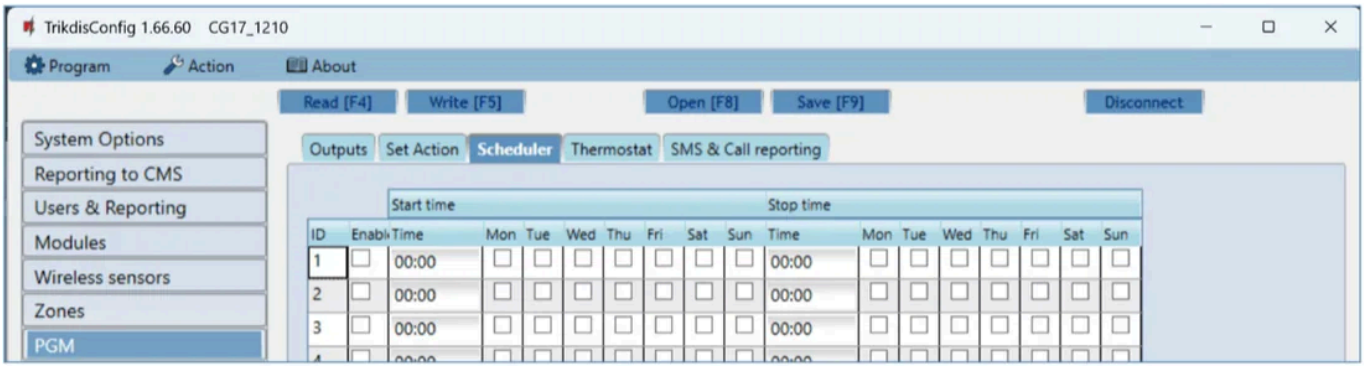


Figure 64. TrikdisConfig – **PGM**, **Scheduler** tab: the rows of the schedules with the **Enable** checkbox, the start (**Start time**) and stop (**Stop time**) times and the days of the week (**Mon**–**Sun**).

- **ID** – the position of the schedule on the list.
- **Enable** – switches on the schedule.
- **Start time** – the time when the OUT output switches on (the start of the schedule).
- **Stop time** – the time when the OUT output switches off (the end of the schedule).
- **Mon**–**Sun** – mark the days of the week on which the OUT output should switch on and off.

5.7.4 Thermostat tab – thermostat

Here you assign thermostats working on the basis of the temperature sensors (section 3.4) to the OUT outputs.

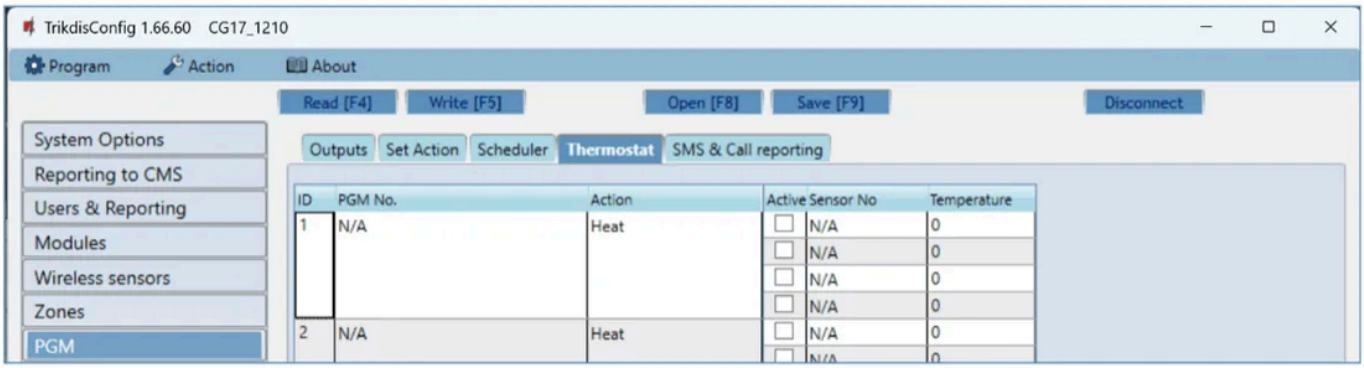


Figure 65. TrikdisConfig – **PGM**, **Thermostat** tab: the rows of the thermostats with the controlled PGM (**PGM No.**), the operating mode (**Action**, for example **Heat**), the **Active** checkbox, the number of the sensor (**Sensor No**) and the temperature (**Temperature**).

- **ID** – the position of the thermostat on the list.
- **PGM No.** – the number of the PGM output controlled by the thermostat.
- **Action** – the operating mode of the thermostat: heating (**heat**) or cooling (**cool**).
- **Active** – when ticked, the thermostat works with the selected temperature sensor, according to the set temperature.
- **Sensor No** – the temperature sensor assigned to the thermostat.
- **Temperature** – the temperature that the thermostat maintains.

5.7.5 SMS & Call reporting tab

This tab is only visible if you have entered the phone number of at least one user on the **Users & Reporting** page (section 5.4).

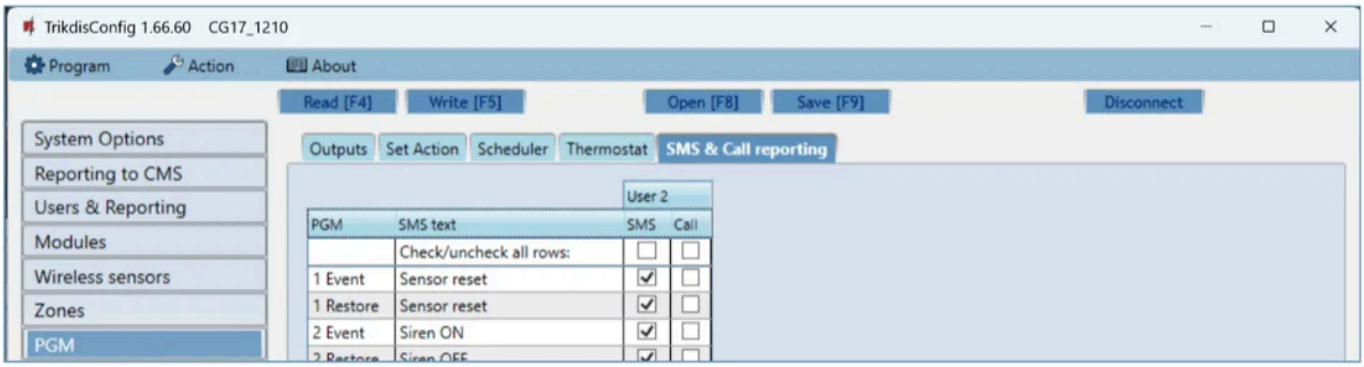


Figure 66. TrikdisConfig – **PGM**, **SMS & Call reporting** tab: the SMS text of the switch-on (**Event**) and switch-off (**Restore**) events of the outputs, with **SMS** and **Call** checkboxes per user (**User 2**).

- **PGM** – the number of the OUT output and the type of the event: **Event** – switching on the OUT output, **Restore** – switching off the OUT output.
- **SMS text** – the name of the switch-on or switch-off event of the OUT output in the event SMS messages.
- **User / SMS and Call** – select which users should receive an SMS and/or a call when the OUT output is switched on or off.

5.8 "Sensors" page

Here you add the temperature sensors (wiring: section 3.4). In the **Module type** list, voltage measurement of the inputs (**In1 Voltage**–**In4 Voltage**, section 3.13) can also be selected; the setup of the Strela RS485 fuel level sensor is in section 5.5.3.

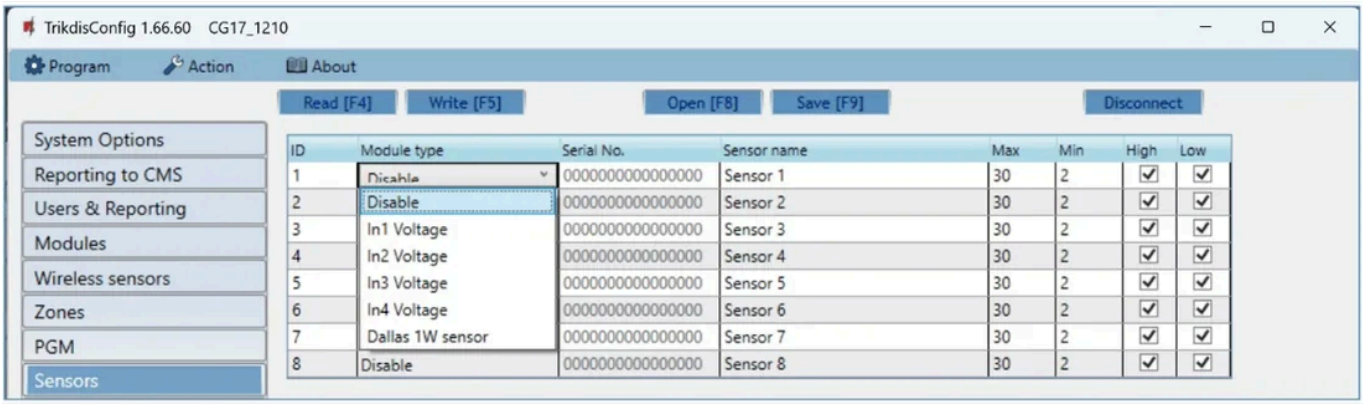


Figure 67. TrikdisConfig – **Sensors**: eight sensor slots; in the open **Module type** list **Disable** (none), **In1 Voltage**–**In4 Voltage** (input voltage) and **Dallas 1W sensor** (1-Wire temperature sensor); next to it the **Serial No.**, **Sensor name**, **Max**, **Min**, **High** and **Low** columns.

- **ID** – the position of the sensor on the list.
- **Module type** – the selected temperature sensor goes to this position (**ID**).
- **Serial No.** – the serial number of the temperature sensor; the panel reads it out.
- **Sensor name** – give the temperature sensor a name.
- **Max** – if the temperature is higher than this, the CG17 generates an event message. For this, tick the **High** checkbox.
- **Min** – if the temperature is lower than this, the CG17 generates an event message. For this, tick the **Low** checkbox.

5.9 "System events" page

On the **System events** page you set the CG17's own system events (for example RS485 fault, high and low temperature, mobile signal jamming, power failure) and their notifications.

5.9.1 Events tab – system events

Here you set which system events go to the monitoring station and to the Protegus cloud, with which Contact ID code and SMS text.

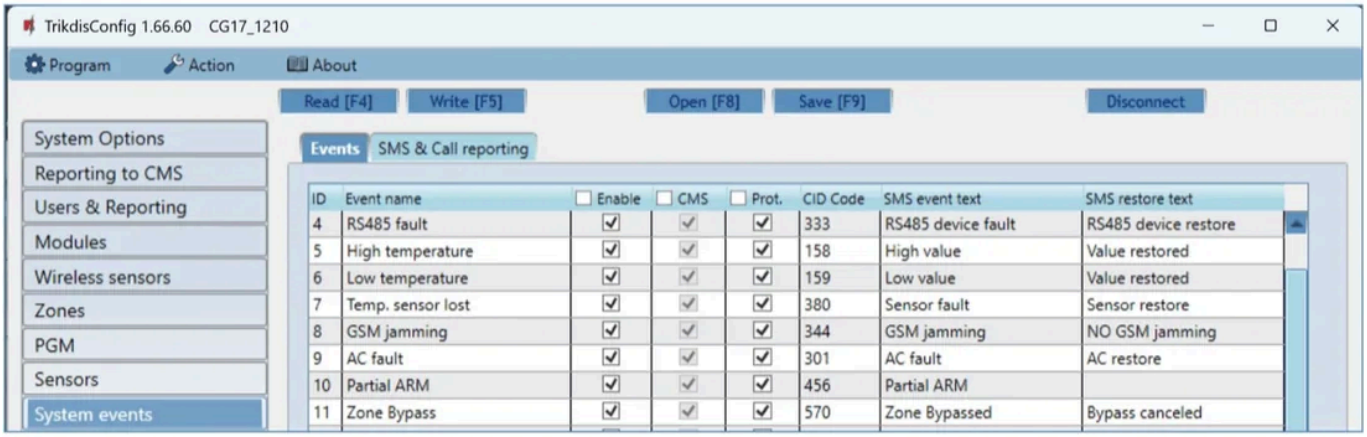


Figure 68. TrikdisConfig – **System events**, **Events** tab: the system events (for example **RS485 fault**, high and low temperature, mobile signal jamming, power failure) with the **Enable**, **CMS** and **Prot.** checkboxes, the Contact ID code and the SMS texts.

- **ID** – the position of the event on the list.
- **Event name** – the name of the event.
- **Enable** – switches on the monitoring of the event.

- **CMS/Prot.** – the messages about the selected event go to the monitoring station and/or to the Protegus cloud.
- **CID code** – the Contact ID code of the event.
- **SMS event text** – the SMS text of the event.
- **SMS restore text** – the SMS text of the restore.

5.9.2 SMS & Call reporting tab

This tab is only visible if you have entered the phone number of at least one user on the **Users & Reporting** page (section 5.4).

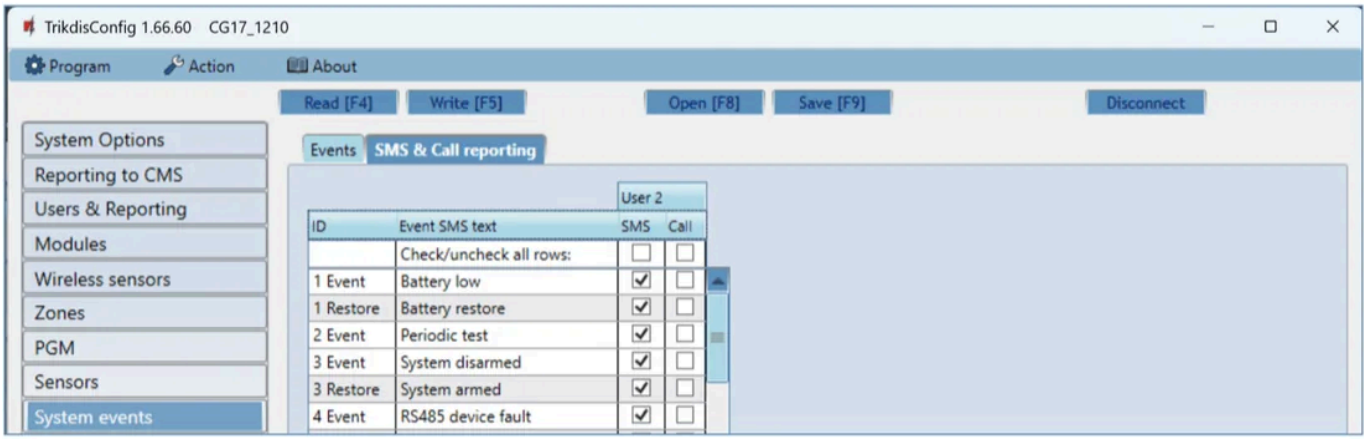


Figure 69. TrikdisConfig – **System events**, **SMS & Call reporting** tab: the SMS text of the system events (for example **Battery low**, **Periodic test**, **System disarmed**, **System armed**, **RS485 device fault**), with **SMS** and **Call** checkboxes per user (**User 2**).

- **ID** – the number of the event and its identifying word: **Event** or **Restore**.
- **Event SMS text** – the text of the event SMS messages.
- **User / SMS and Call** – set how the users should be notified about the individual events: by SMS and/or by call.

5.10 "Events Log" page

The CG17's own event log: here you can read out and delete the events stored in its memory.

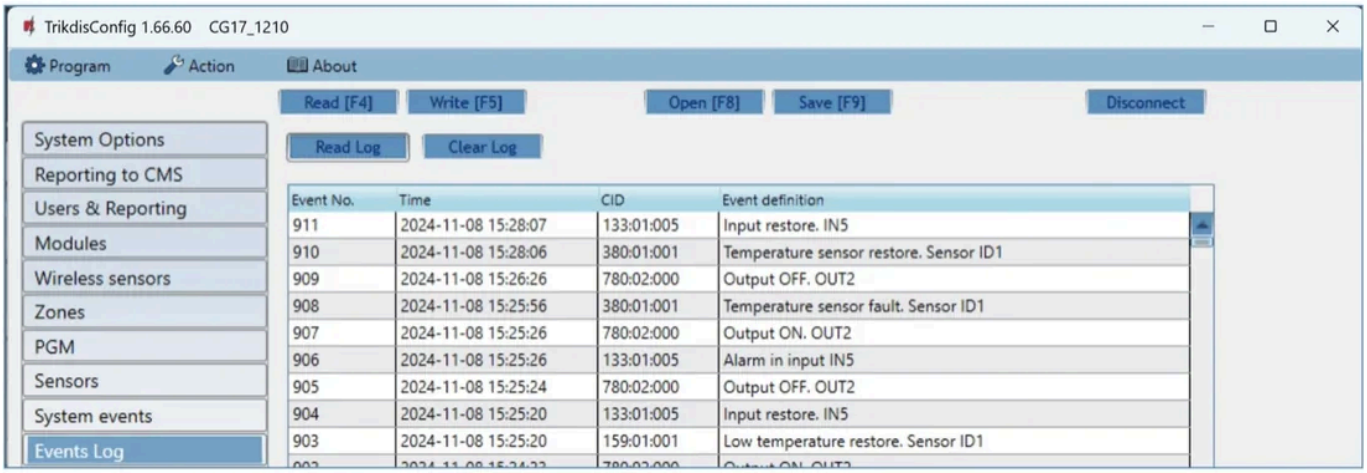


Figure 70. TrikdisConfig – **Events Log**: the **Read Log** and **Clear Log** buttons, below them the events with sequence number (**Event No.**), time (**Time**), Contact ID code (**CID**) and description (**Event definition**).

- **Read Log** button – reads the entries of the event log from the memory of the device.

- **Clear Log** button – deletes the entries of the event log from the memory of the device.
- The table shows the sequence number (**Event No.**), the time (**Time**), the Contact ID code (**CID**) and the description (**Event definition**) of the event. On the **Events Log** page, up to 1000 events stored in the memory of the CG17 can be displayed.

5.11 Restoring the default settings

To restore the default settings of the panel, click the **Restore** button in the **Default settings** group in the bottom left part of the TrikdisConfig programming window. Before this, it is worth saving the current settings to a file (**Save [F9]**, section 5.1).

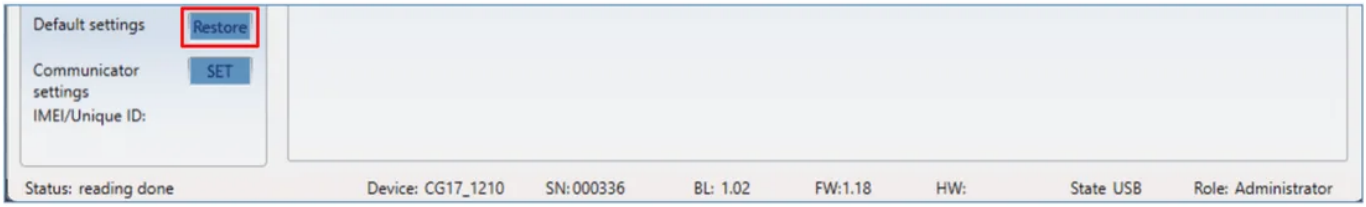


Figure 71. TrikdisConfig – the **Restore** button of the **Default settings** group (framed in red) in the bottom left part of the programming window, above the status bar.

6. Remote programming

You can also read and change the settings of the CG17 remotely through the Protegus cloud (section 6.1), and you can also control the panel remotely from TrikdisConfig (section 6.2) – for neither do you need to go to the site.

6.1 Setting the parameters remotely

Conditions for remote programming

Remote programming only works if:

1. the Protegus cloud service (**Protegus cloud**) is switched on: in the **Users & Reporting** window of TrikdisConfig, in the **Cloud application** settings group, **Enable cloud service** is ticked (section 5.4; by SMS: `CONNECT 123456 PROTEGUS=ON`, section 4.2);
2. there is an activated SIM card in the device, and its PIN code is entered, or the PIN request is switched off;
3. there is power supply: the **POWER** LED is lit green;
4. the device is connected to the network: the **NETWORK** LED is lit green and blinks yellow.

1. Download the TrikdisConfig program from www.trikdis.com.
2. Make sure that the panel is connected to the internet, and the Protegus connection is switched on.
3. Start TrikdisConfig, and in the **Unique ID** field of the **Remote access** group enter the **IMEI** number of the CG17 (you can find it on the sticker on the back of the device and on the box).
4. In the **System Name** field give a name to the CG17 identified by this IMEI, and click the **Configure** button.

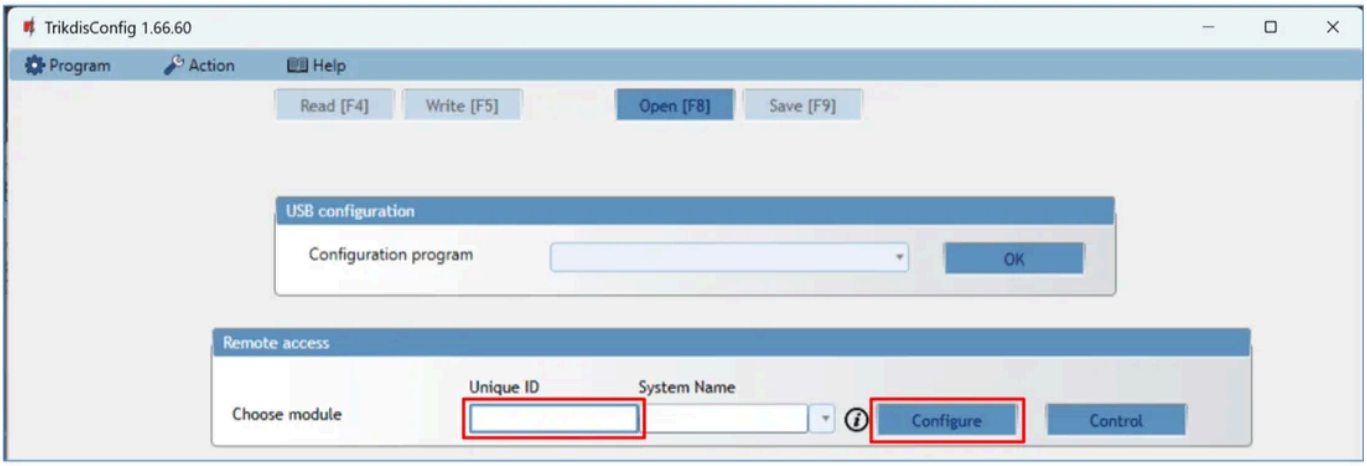


Figure 72. TrikdisConfig – the **Remote access** group of the start window: the IMEI number goes into the framed **Unique ID** field, next to it the **System Name** field; the framed **Configure** button opens remote programming.

5. Click the **Read [F4]** button: the program reads the current settings of the CG17. If the **Administrator code** prompt window appears, enter the 6-character administrator code. If you want the program to remember the code, tick the **Remember password** checkbox and click the **Write [F5]** button.
6. Make the desired changes to the settings of the CG17 and click the **Write [F5]** button. If you want to end the connection with the CG17, click the **Disconnect** button and exit TrikdisConfig.

6.2 Remote control from TrikdisConfig

1. Download the TrikdisConfig program from www.trikdis.com (enter "TrikdisConfig" in the search field), and install it.
2. Make sure that the alarm panel is connected to the internet. The Protegus cloud service (**Protegus cloud**) must be switched on (section 6.1).
3. Start TrikdisConfig, and in the **Unique ID** field of the **Remote access** group enter the **IMEI** number of the CG17 (you can find it on the sticker on the back of the device and on the box).

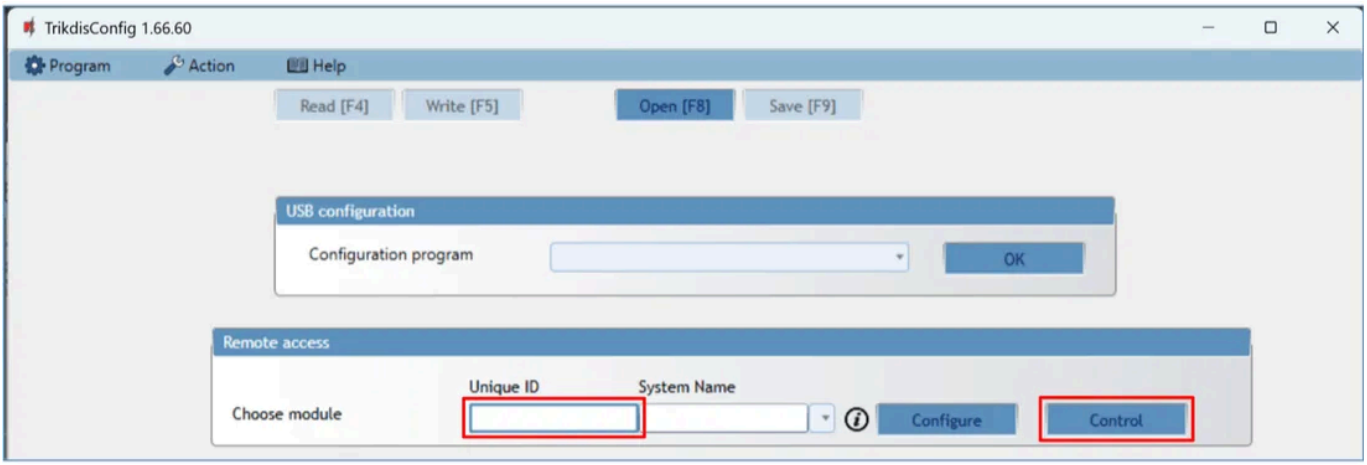


Figure 73. TrikdisConfig – the **Remote access** group: the framed **Unique ID** field and the framed **Control** button.

4. Click the **Control** button.
5. Enter the **Self-service code** (default `123456`), and press the **OK** button.

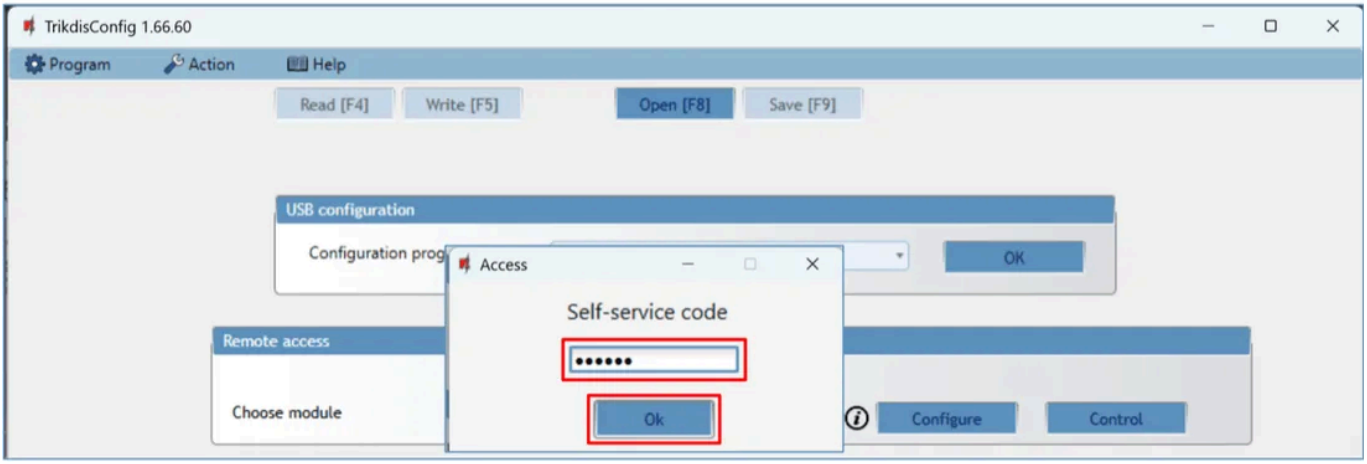


Figure 74. The **Access** window: enter the code in the **Self-service code** field, then press the **Ok** button.

6. The **Remote control** window opens: here you can control the partitions of the alarm panel, monitor the state of the zones, switch the PGM outputs and monitor the temperature.
7. **Partitions** tab: press the **DISARM** (or the **ARM**) button and enter the user code – the partition of the alarm panel is disarmed (or armed).

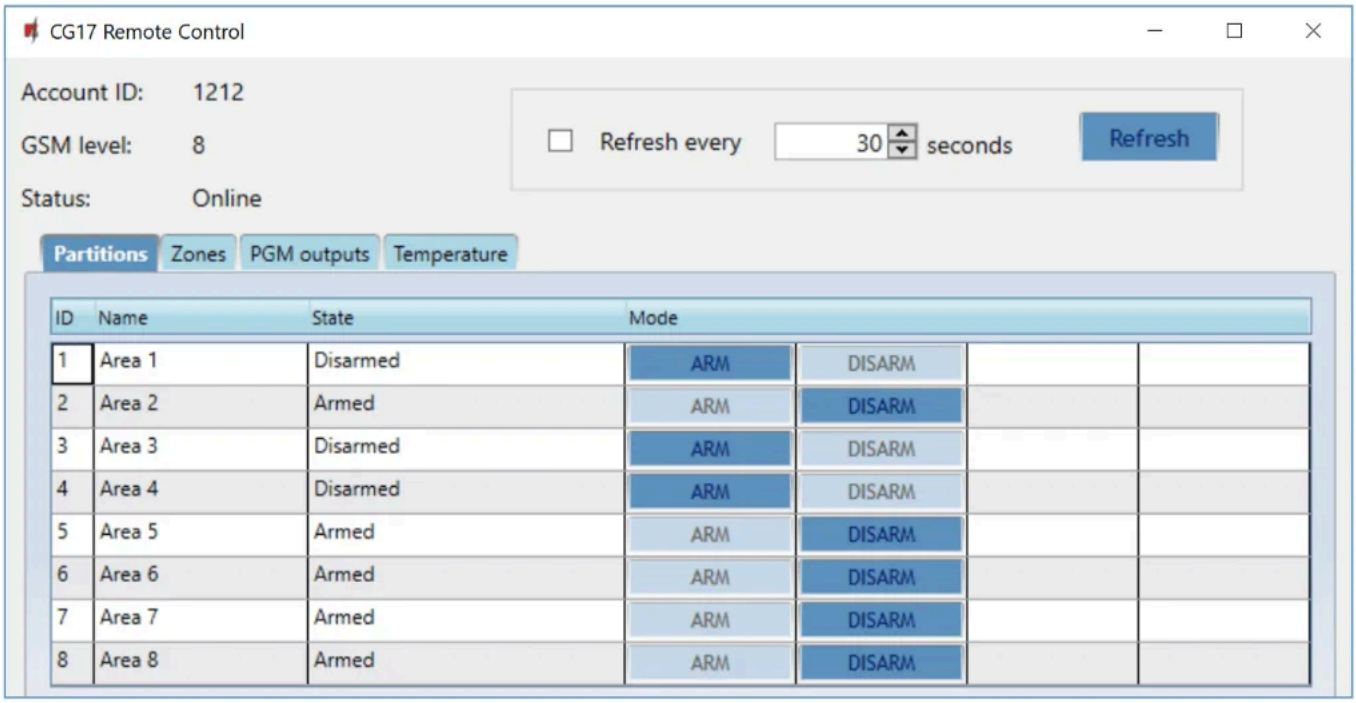


Figure 75. The **Partitions** tab of the **CG17 Remote Control** window: for each partition the name (**Name**), the state (**State**: **Armed**, **Disarmed**) and the **ARM** / **DISARM** button. At the top the **Account ID** (object number), the **GSM level** (signal strength) and the **Status**; with the **Refresh** button you refresh the data, with the **Refresh every ... seconds** checkbox automatically at the set interval.

8. **Zones** tab: this window shows the state of the zones; you can also bypass the zones (**Bypass**).

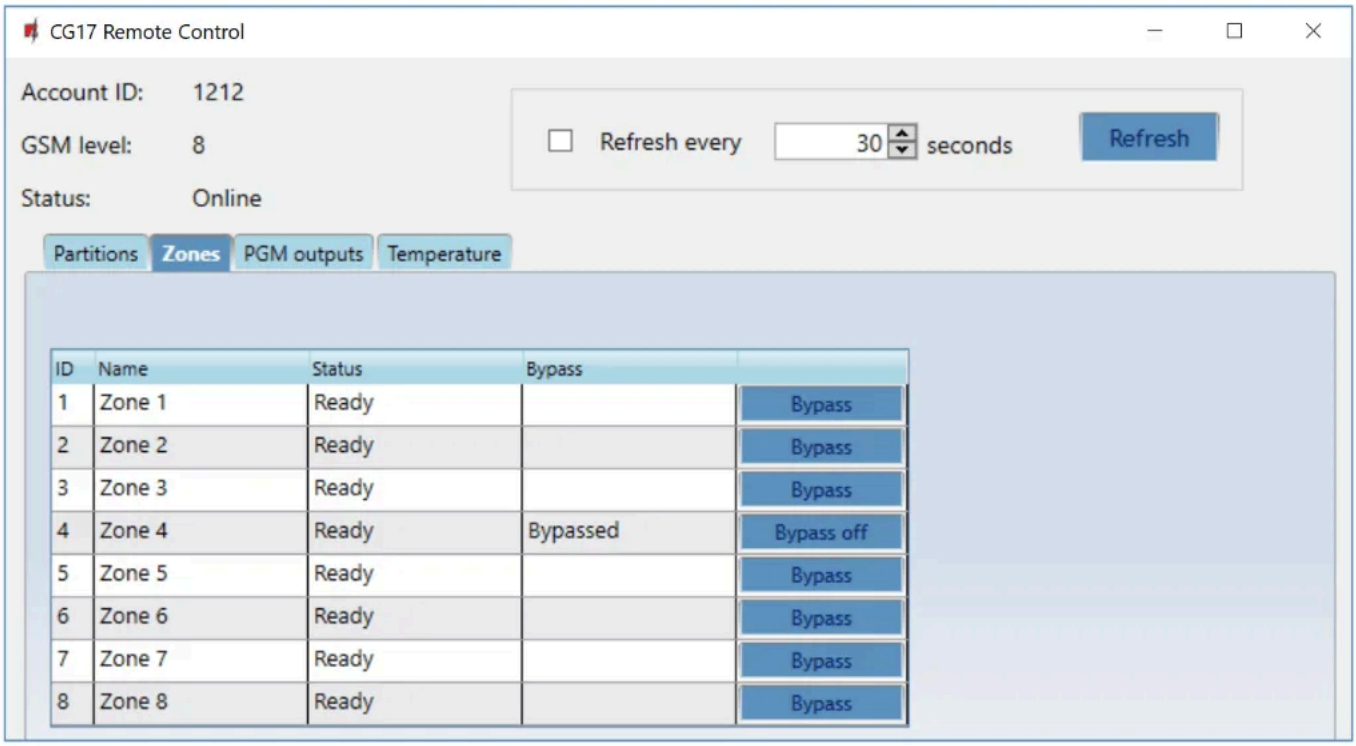


Figure 76. The **Zones** tab: for each zone the state (**Status**, **Ready** – in order) and the **Bypass** button; for a bypassed zone (**Bypassed**) the **Bypass off** button cancels the bypass.

9. **PGM outputs** tab: here you can switch the PGM outputs of the **Remote Control** type.

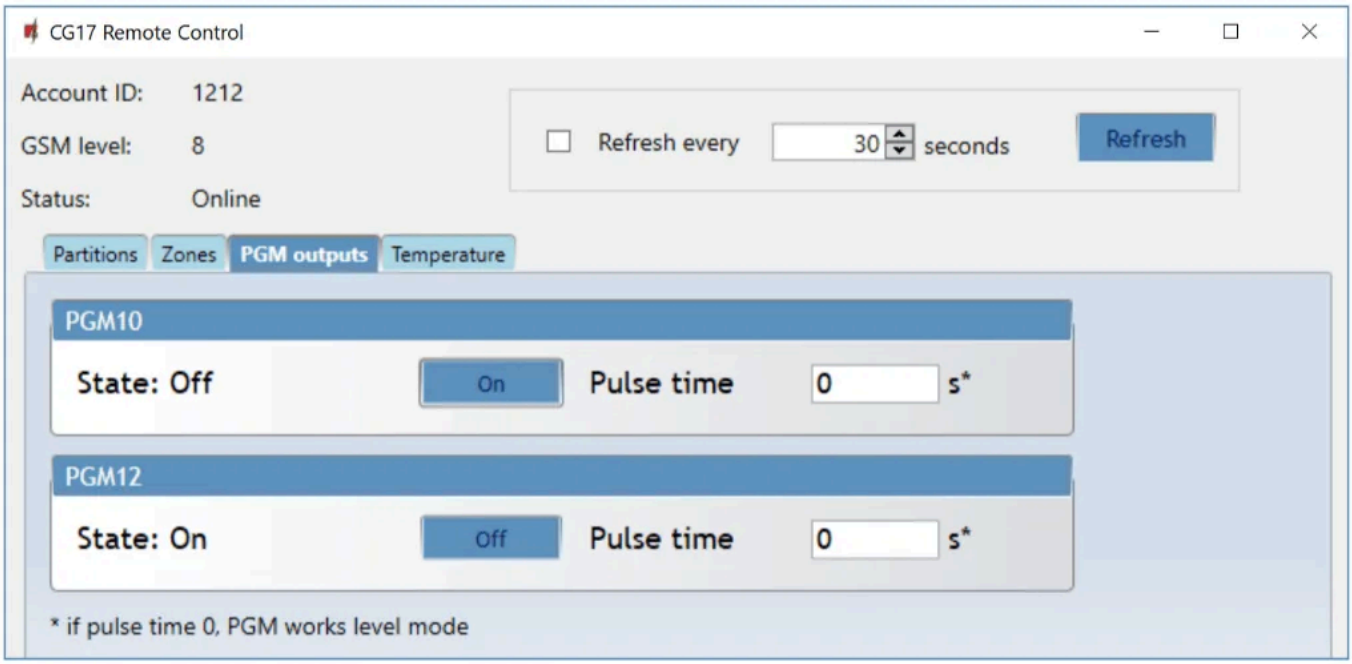


Figure 77. The **PGM outputs** tab: for each output the state (**State: Off**, **State: On**), the **On** / **Off** switch button and the **Pulse time** (s) field. At the bottom of the window: if the pulse time is 0, the PGM works in level-controlled (level) mode.

10. **Temperature** tab: here you can monitor the measured values of the temperature sensors.

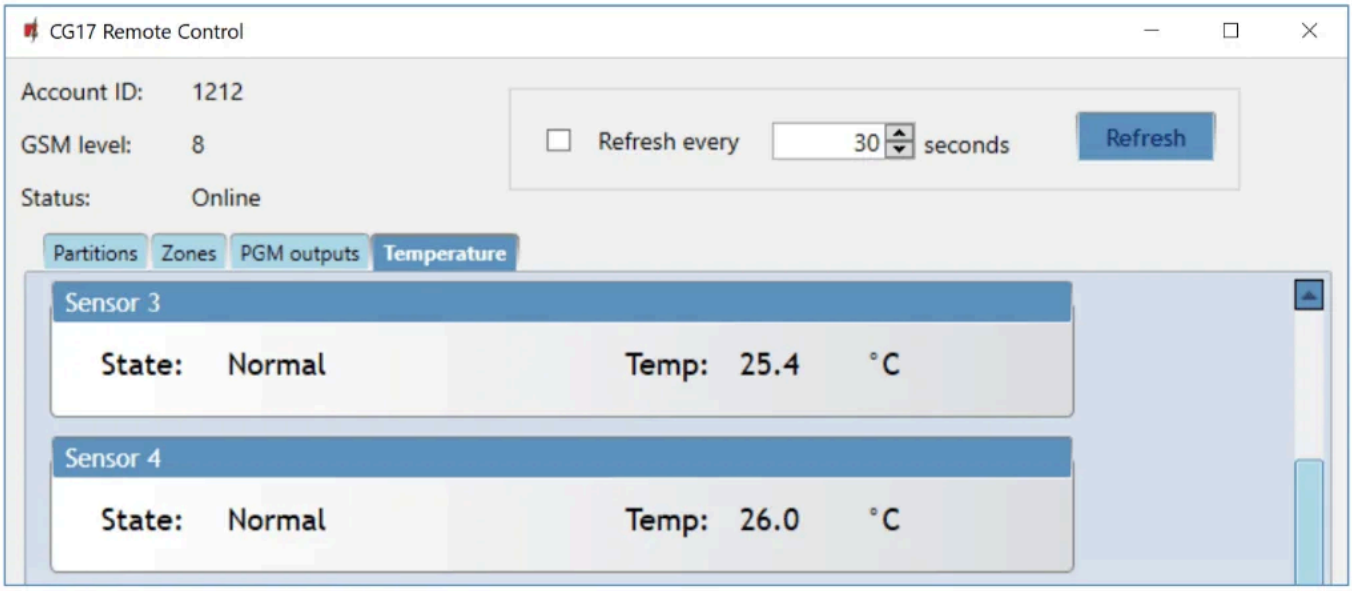


Figure 78. The **Temperature** tab: for each sensor (**Sensor**) the state (**State: Normal** – in order) and the measured temperature (**Temp**, °C).

7. Testing the installation

At the end of the setup and installation, test the whole system:

1. Check that there is supply voltage (the **POWER** LED blinks green).
2. Check the mobile network connection on the **NETWORK** indicator. A signal strength of 5 is sufficient (steady green light for 4 seconds, then five yellow blinks), on a 3G network 3 is also sufficient (steady green light for 4 seconds, then three yellow blinks). If the red **TROUBLE** indicator blinks 5 times, find another place for the CG17.
3. To check the inputs, activate them, and see whether the recipients receive the correct messages.
4. To check the outputs, switch them on remotely, and see whether the recipients receive the correct messages, and whether the outputs switch correctly.
5. Test the alarm: check that the monitoring station receives the events correctly.

The DATA LED is the simplest internet check. The DATA LED is lit when there is a message waiting to be sent in the device's memory. A green NETWORK LED only tells you that the network connection has been established – for a mobile network device, that it has registered on the operator's network; for an Ethernet device, that the connection up to the router is alive – but not that the device can also reach the internet. If the NETWORK LED is green but the DATA LED stays lit continuously even after an event or test report, the internet connection is not working: the message cannot be sent. On a mobile network the most common culprit is the APN or the data service of the SIM card; on Ethernet, the router, the firewall or the DNS. When the DATA LED goes out, the message has been sent and the data connection is fine.

You can also query the data of the panel (type, IMEI number, serial number, firmware version), the state of the inputs and outputs and the values of the temperature sensors by SMS: `INFO 123456`, `ASKI 123456`, `ASKO 123456`, `ASKT 123456`. Send the command from a phone on the user list, and replace the default `123456` password with your own administrator password (section 4.2).

8. Firmware update

If the CG17 is connected to TrikdisConfig and newer firmware is available, the program offers the update by itself – for this the computer must be on the internet. If an antivirus program runs on the computer, it may block the automatic update; in that case you have to change the settings of the antivirus program.

You can update the firmware yourself – to a newer version and, if necessary, to an older one as well. All device settings remain unchanged after the update.

1. Start the TrikdisConfig software and connect the device with a USB cable, or open its programming remotely.
2. If newer firmware is available, the software offers to download it – accept it.
3. Select the **Firmware** page and click the **Open firmware** button. Select the firmware file.
4. Press the **Update [F12]** button, wait for the update to finish, then click **OK** in the pop-up window. Do not unplug the cable or interrupt the connection in the meantime.

The firmware files are in the TrikdisConfig installation folder, inside the **Firmwares** subfolder, in the folder named after the device. If there is no such folder, either there is no update for it or the TrikdisConfig software itself needs to be updated. The latest files can also be downloaded as a registered user from the device's page on the manufacturer's website.

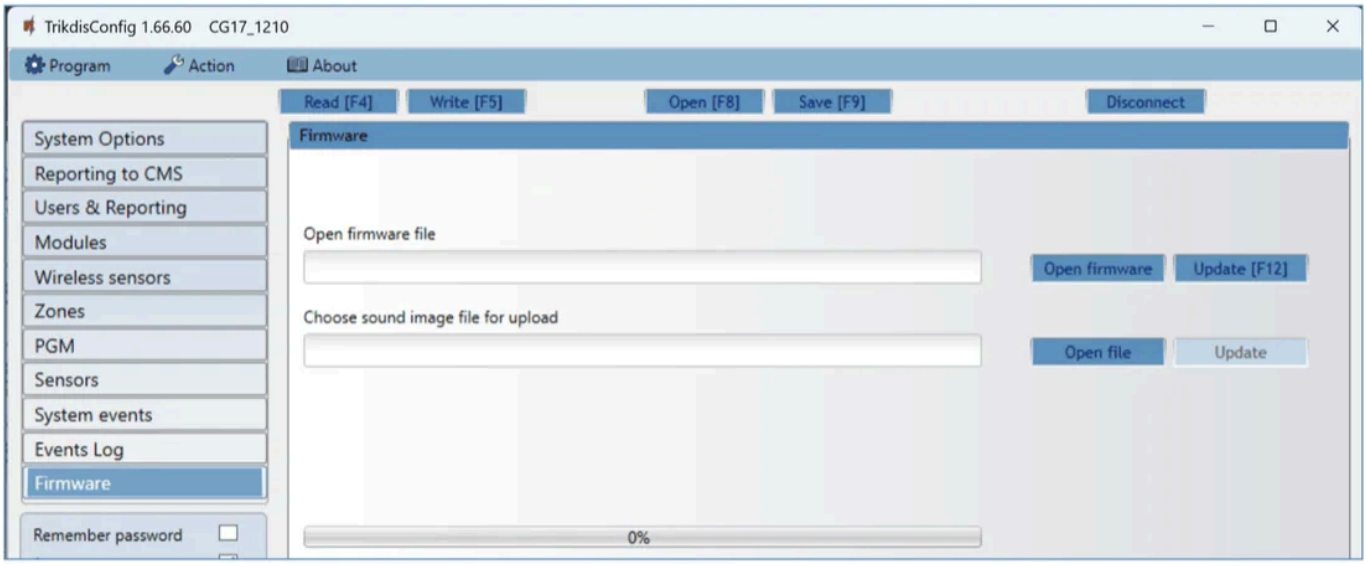


Figure 79. TrikdisConfig – CG17, **Firmware** page: the **Open firmware file** field, the **Open firmware** and **Update [F12]** buttons, at the bottom the progress indicator. The **Choose sound image file for upload** row in the middle (uploading a sound file, **Open file** and **Update** buttons) is not needed for the firmware update.

Connect the CG17 with a **USB Mini-B** cable (the connector is under the cover, chapter 2); remote connection is described in section 6.1.

9. Safety instructions

Figyelem!

Az elektromosság veszélyes! Személyi sérülést vagy HALÁLT, valamint anyagi kárt okozhat!

A telepítés során elektromos berendezéssel történik munkavégzés, amit az érvényes erős- és gyengeáramú rendelkezések betartásával kell kivitelezni!

A garancia (jótállás) érvényesítésének is feltétele, hogy az eszközt szakképzett személy telepítse az elektromos berendezések telepítésére vonatkozó előírások betartásával és az elektromos berendezések biztonságos üzemeltetésére vonatkozó hatályos előírásokat követve.

- The electronic intrusion detection (alarm) system may only be installed and maintained by qualified persons.
- Before installation, read this manual carefully to avoid mistakes that can lead to malfunction or even damage to the equipment.
- **Disconnect the supply voltage before making any electrical connection** – the backup battery too.
- Changes, modifications or repairs not authorized by the manufacturer void the warranty.
- Follow local waste disposal regulations: do not throw the device and its parts in household waste – hand in the discarded device as electronic waste.

See also

- iO8 input and output expander – installation manual – the iO8 expansion module for the CG17.
- W485 WiFi and E485 Ethernet module – installation and setup manual – Wi-Fi and Ethernet connection for the CG17.
- APN settings – list of European mobile operators – if the mobile data connection is not established.
- Protegus Android / iPhone and web app – about the app.
- Documentation in English: docs.trikdis.com – Cellular security control panel CG17 – the manuals on docs.trikdis.com are in English.

Related products

Trikdis CG17 4G GSM compact security control panel **Trikdis iO8 wired expander module**
Trikdis IO8-LORA wireless expander module **Trikdis RF-LORA wireless expander module**
Trikdis IO-LORA wireless expander module **Trikdis W485 Wifi module (RS485)**
Trikdis E485 Ethernet module (RS485) **DS18B20 temperature sensor with 1m wire**
12 V 7 Ah gel battery for alarm control panel
Trikdis ANT04 GSM stick-on antenna with 2,5m wire
Trikdis ME301M magnetic antenna with 2,5m wire

Copyright

This manual was produced by trikdis.hu and mobilamb.eu. Its text, structure, our own illustrations and additions are our intellectual property and are protected by copyright. Without our permission it may not be copied, distributed or published on another website, in whole or in part. It may be freely downloaded and printed for installing and using the product.

Trikdis and Protegus names and logos are trademarks of UAB Trikdis.

Always up-to-date version of this manual: https://mobilamb.eu/cg17-manual