mobilamb
TRIKDIS Official Distributor

G17F fire communicator – installation and programming manual

Installation and programming manual for the Trikdis G17F cellular fire communicator (EN 54-21): wiring to the outputs or to the RS485 bus of the fire alarm control panel (ESPA 4.4.4, NSC Solution, INIM Smartline, C-TEC Cast ZFP), setup in TrikdisConfig, monitoring station, Protegus 2, control by SMS and phone call.



Edition: 2026-11-17
Always up-to-date web version: https://mobilamb.eu/g17f-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 device
1.5 The terminals
1.6 LED indications
1.7 Tools you need for the installation

2. Quick setup with the TrikdisConfig software

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

3. Installation and wiring

3.1 Mounting and inserting the SIM card
3.2 Wiring to the outputs of the fire alarm control panel
3.3 Fire alarm control panel with the ESPA 4.4.4 protocol
3.4 NSC Solution fire alarm control panel
3.5 INIM Smartline fire alarm control panel
3.6 C-TEC Cast ZFP fire alarm control panel
3.6.1 Setting up the C-TEC panel (ZFPtools)
3.7 Wiring the inputs
3.8 iO series expansion modules
3.9 iO-8 expansion module
3.10 LORA series expansion modules
3.11 W485 Wi-Fi module
3.12 E485 Ethernet module
3.13 Switching on the communicator

4. Remote control

4.1 Adding the G17F to Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
4.2 Setup and control by SMS message
4.3 Controlling the PGM outputs by phone call

5. The pages of TrikdisConfig

5.1 The status bar
5.2 "System Options" page
5.3 "Reporting to CMS" page
5.4 "Users & Reporting" page
5.5 "Modules" page
5.6 "Zones" page
5.7 "PGM" page
5.8 "System events" page
5.9 "Events Log" page
5.10 Restoring the factory settings

6. Remote programming

7. Checking the operation

8. Firmware update

9. Troubleshooting and frequently asked questions

10. Safety instructions

See also

1. Overview

The **G17F** is a fire communicator that forwards the events of any fire detection unit or fire alarm control panel over the mobile network. If an input (zone) is triggered, i.e. a fire alarm comes in, the event is forwarded to the configured destinations, for example to the fire brigade and to the monitoring station. In addition, the owner is also notified about the event in the **Protegus 2** mobile and web app.

The G17F forwards the messages of the fire alarm control panel over the mobile network. **How it works:** if an input (zone) of the communicator is triggered, the G17F sends an event message over mobile internet to the receiver of the monitoring station or to the Protegus 2 app; in addition, it can also send an SMS and make a phone call. The communicator is available with a 2G or a 4G modem. You make the settings with the **TrikdisConfig** software, over a USB cable or remotely.

Certification	Data
Standard	The G17F meets the requirements of the **EN 54-21:2006** standard, and it fulfils the performance requirements specified for a **type 1** transmission system in Annex A of EN 54-21.
Certificate	**1922-CPR-1974** – Fire detection and fire alarm systems. Alarm transmission and fault warning routing equipment.
Certification body	No. 1922 "Dedal" notified product certification body – Nesebar, Mladost str. 50, 8230 Bulgaria
Trikdis technical support	support@trikdis.lt, +37067422877

1.1 What it is for and how it works

Connection with the fire alarm control panel

- Connected to the outputs of the panel: the status outputs of the panel (alarm, fault etc.) are connected to the inputs of the G17F (section 3.2).
- Over the RS485 bus: to fire alarm control panels with the **ESPA 4.4.4** protocol, and to **NSC Solution**, **INIM Smartline** and **C-TEC Cast ZFP** fire alarm control panels (sections 3.3–3.6).

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 events to SIA DC-09 receivers.
- If the connection is lost on the primary channel, the messages automatically go to the backup receiver.
- It can also report the events to the monitoring station by SMS – this is extremely useful, because it works even if the IP connection drops in the network of the mobile operator.
- It detects jamming of the mobile network.
- It can report to the monitoring station and send to the Protegus 2 app at the same time; reporting to the monitoring station can be given priority.
- It sends the event messages with Contact ID codes.

Messages to the users

- It calls the selected phone numbers (up to 8 users).
- It sends SMS messages about the events.

- It sends push and special-sound event notifications to the Protegus 2 app.

Remote control of the outputs

- from the Protegus 2 app;
- by calling the phone number of the device;
- by SMS message.

Setup and installation

- Setup with a USB cable or remotely, with the TrikdisConfig software.
- Remote firmware update.
- Two access levels (account types) for the settings: installer and administrator.

Inputs and outputs

- 3 inputs, selectable type: NO, NC, EOL (4.7 kΩ, 10 kΩ).
- 3 dual-purpose I/O terminals that can be set as input (IN) or output (OUT); as input, selectable type: NO, NC, EOL (4.7 kΩ, 10 kΩ).
- RS485 bus for the iO series expansion modules.
- With the iO series expanders, the number of inputs (IN) or outputs (OUT) can be increased to 12.

1.2 Versions

The G17F is available in two cellular versions: with a 2G or a 4G modem. This manual applies to both; the difference is the modem and the mobile network bands.

Version	Modem	Bands
G17F-4G	4G (LTE)	700 / 800 / 900 / 1800 / 2100 / 2600 MHz
G17F-2G	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz

Trikdis G17F 4G GSM / IP communicator **Trikdis G17F 2G GSM / IP communicator**

Because 2G networks are being gradually switched off, we recommend the 4G version for new installations.

1.3 Technical specifications

Parameter	Value
2G (GSM/GPRS) modem bands	850 / 900 / 1800 / 1900 MHz
4G (LTE) modem bands	700 / 800 / 900 / 1800 / 2100 / 2600 MHz
Supply voltage	9–32 V DC
Current consumption	100 mA
Transmission protocol	TRK, SIA DC-09_2007, SIA DC-09_2012
Encryption key	6 characters

Parameter	Value
Connection with the monitoring station	TCP/IP or UDP/IP, SMS
Event codes	Contact ID
Message memory	up to 60 messages
Inputs and outputs	3 inputs: NO, NC, EOL (4.7 kΩ, 10 kΩ); 3 dual-purpose terminals (IN/OUT): as input NO, NC, EOL (4.7 kΩ, 10 kΩ), as output open collector (OC), up to 100 mA
Event log	up to 1000 events
Setup	remotely with the TrikdisConfig software or locally with a USB Mini-B cable; remotely with SMS messages
Length of the RS485 bus	up to 100 m
Supported modules	**iO** expansion module; **iO-WL** – **iO-MOD** – iO-WL wireless transceiver; **iO-8** expansion module; **E485** Ethernet module; **W485 (W17u)** Wi-Fi module; **iO-LORA** expansion module; **iO8-LORA** expansion module; **PB-LORA** panic button; **REL-LORA** expansion module; **INIM Smartline**, **NSC Solution** and **C-TEC Cast ZFP** fire alarm control panels; fire alarm control panels with the **ESPA 4.4.4** protocol
Operating environment	–10 … +50 °C, up to 80 % relative humidity at +20 °C
Dimensions	92 × 62 × 25 mm
Weight	80 g

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 device

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

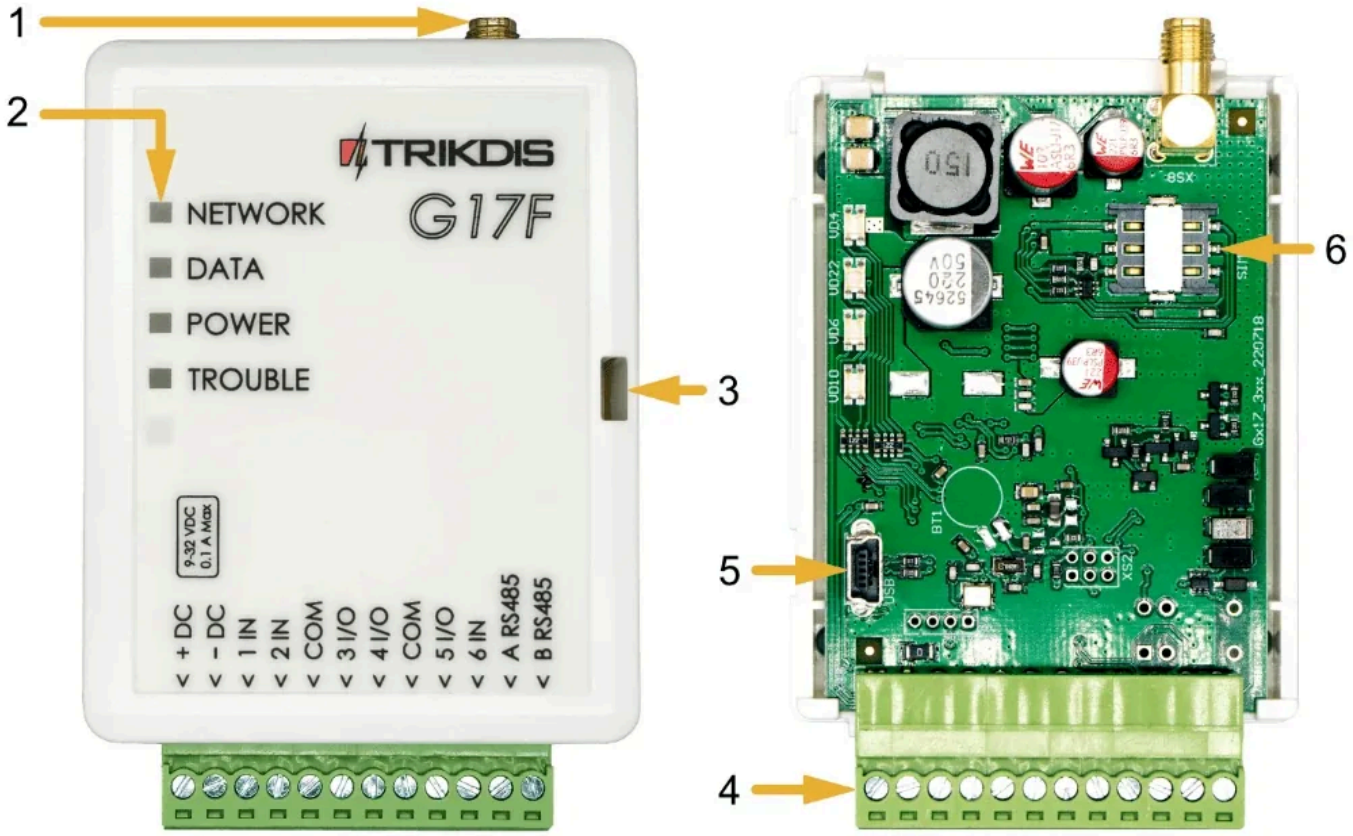


Figure 1. Parts of the G17F.

- 1 SMA connector of the cellular antenna
- 2 indicators (LEDs)
- 3 opening for removing the front cover
- 4 terminal block for connecting the wires
- 5 USB Mini-B connector for programming
- 6 nano-SIM card holder

1.5 The terminals

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

Terminal	Purpose
+DC	supply voltage: positive pole of 9–32 V DC
–DC	supply voltage: negative pole of 9–32 V DC
1 IN	input 1, selectable type: NO, NC, EOL (default EOL, 10 kΩ)
2 IN	input 2, selectable type: NO, NC, EOL (default EOL, 10 kΩ)
COM	common (negative) terminal
3 I/O	dual-purpose terminal 3 (IN/OUT): as input NO, NC, EOL (default EOL, 10 kΩ), as output open collector (OC), up to 100 mA
4 I/O	dual-purpose terminal 4 (IN/OUT): as input NO, NC, EOL (default EOL, 10 kΩ), as output open collector (OC), up to 100 mA
COM	common (negative) terminal
5 I/O	dual-purpose terminal 5 (IN/OUT): as input NO, NC, EOL (default EOL, 10 kΩ), as output open collector (OC), up to 100 mA

Terminal	Purpose
6 IN	input 6, selectable type: NO, NC, EOL (default EOL, 10 kΩ)
A RS485, **B RS485**	RS485 bus: for connecting iO expanders, INIM Smartline, NSC Solution and C-TEC Cast ZFP fire alarm control panels, fire alarm control panels with the ESPA 4.4.4 protocol, and the E485 and W485 modules

1.6 LED indications

Indicator	Light	Meaning
NETWORK	off	not connected to the mobile network
	green steady and yellow blinking	connected to the mobile network; the number of yellow blinks is the signal strength: on a 2G (GPRS) network 5 blinks, on a 4G network 3 blinks are 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 G17F is not set
	7 blinks	the supply voltage is not correct
	9 blinks	fault in the connection with the RS485 module

The correct indication after power-up and the evaluation of the signal strength are described in section 3.13.

1.7 Tools you need for the installation

Before you start the installation, check that you have everything at hand:

1. a USB Mini-B cable for the setup;
2. a cable with at least 4 wires for connecting the G17F to the fire alarm control panel;
3. a 2.5 mm flat screwdriver;
4. an external cellular antenna, if the signal is weak at the site;
5. an activated nano-SIM card (the PIN request can be switched off);
6. the manual of the fire alarm control panel to which you connect the G17F.

The listed accessories must be obtained separately – order them from your dealer. If the signal is weak at the site, use a wired antenna 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 with the TrikdisConfig software

This chapter describes the settings with which the G17F sends the events to the Protegus 2 app (section 2.1) or to the monitoring station (section 2.2). The other settings of the G17F are in chapter 5.

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 front cover of the G17F with a flat screwdriver as shown in the figure.



Figure 2. Removing the front cover: insert the screwdriver into the side opening and move it downwards, and the cover snaps off; underneath is the USB Mini-B connector.

2. Connect the G17F to the computer with a **USB Mini-B** cable.
3. Start TrikdisConfig. The program automatically recognizes the connected device and opens the programming window of the G17F.
4. Click the **Read [F4]** button: the program reads out and shows the current settings of the G17F. If the program asks for the administrator or the installer code, enter the 6-digit code.

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

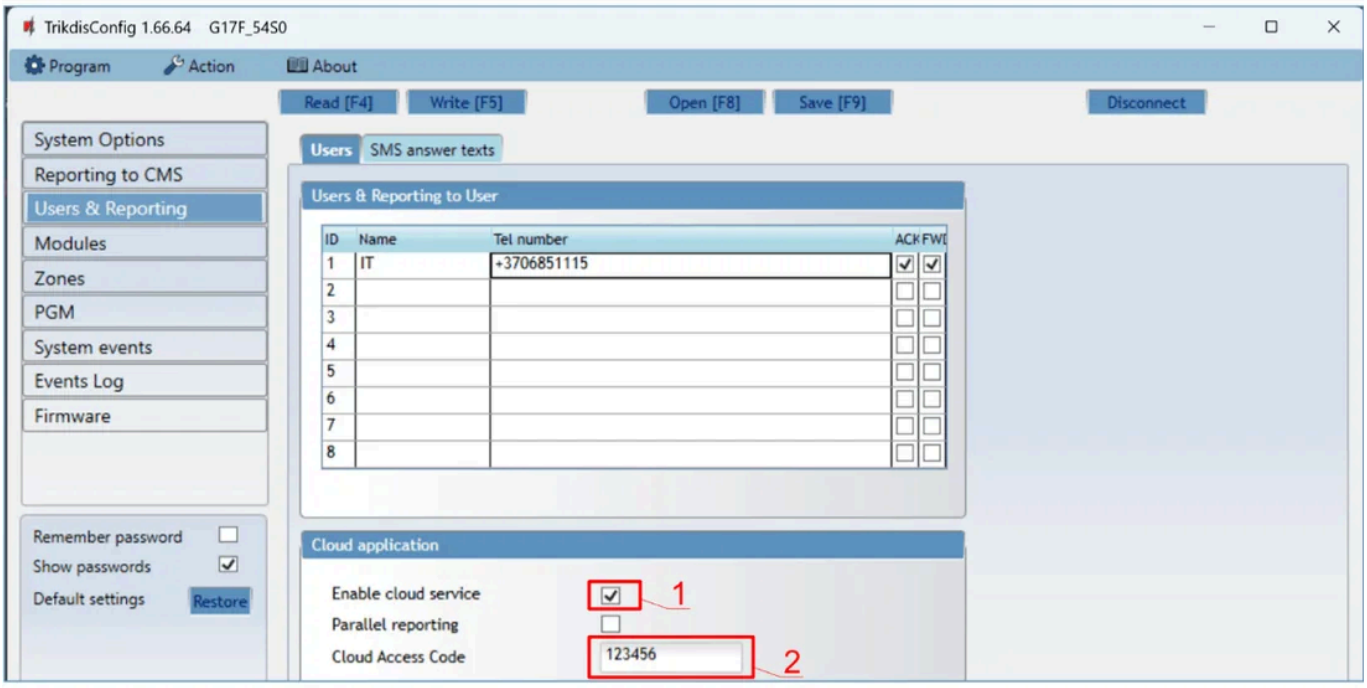


Figure 3. TrikdisConfig – **Users & Reporting**, **Cloud application** group.

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

1. Tick the **Enable cloud service** checkbox.
2. If you want the users to have to enter the code when they add the system to Protegus 2, change the value of the **Cloud Access Code** (default `123456`).

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

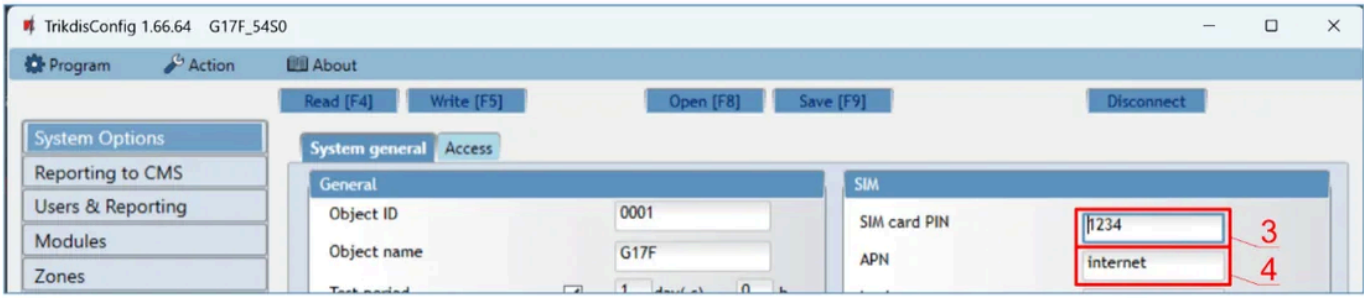


Figure 4. TrikdisConfig – **System Options**, **SIM** group.

- 3 **SIM card PIN** – the PIN code of the SIM card
- 4 **APN** – the mobile internet access point

3. Enter the PIN code of the SIM card (**SIM card PIN**).
4. If necessary, change the **APN** field. You can find the APN on the website of the mobile operator; "internet" is generic and works in the network of most operators. Data of the European operators: APN settings – list of European mobile operators.
5. On the **Zones** page, tick the **Prot.** checkbox for the zones about whose state changes the users should be notified in Protegus 2 (section 5.6).
6. On the **PGM** page, tick the **Prot.** checkbox for the PGM outputs about whose state changes the users should be notified in Protegus 2 (section 5.7).
7. On the **System events** page, tick the **Prot.** checkbox for the internal events of the communicator about whose state changes the users should be notified in Protegus 2 (section 5.8).

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.

2.2 Setup for the monitoring station

The monitoring station settings are on two pages. On the **System Options** page:

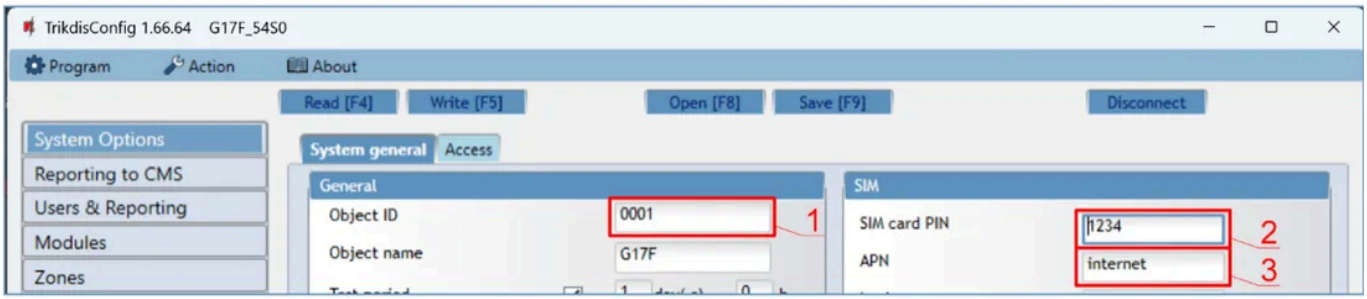


Figure 5. TrikdisConfig – **System Options**.

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

1. Enter the object identifier (**Object ID**) you got 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.
3. If necessary, change the **APN** field. You can find the APN on the website of the mobile operator; "internet" is generic and works in the network of most operators.

On the **Reporting to CMS** page:

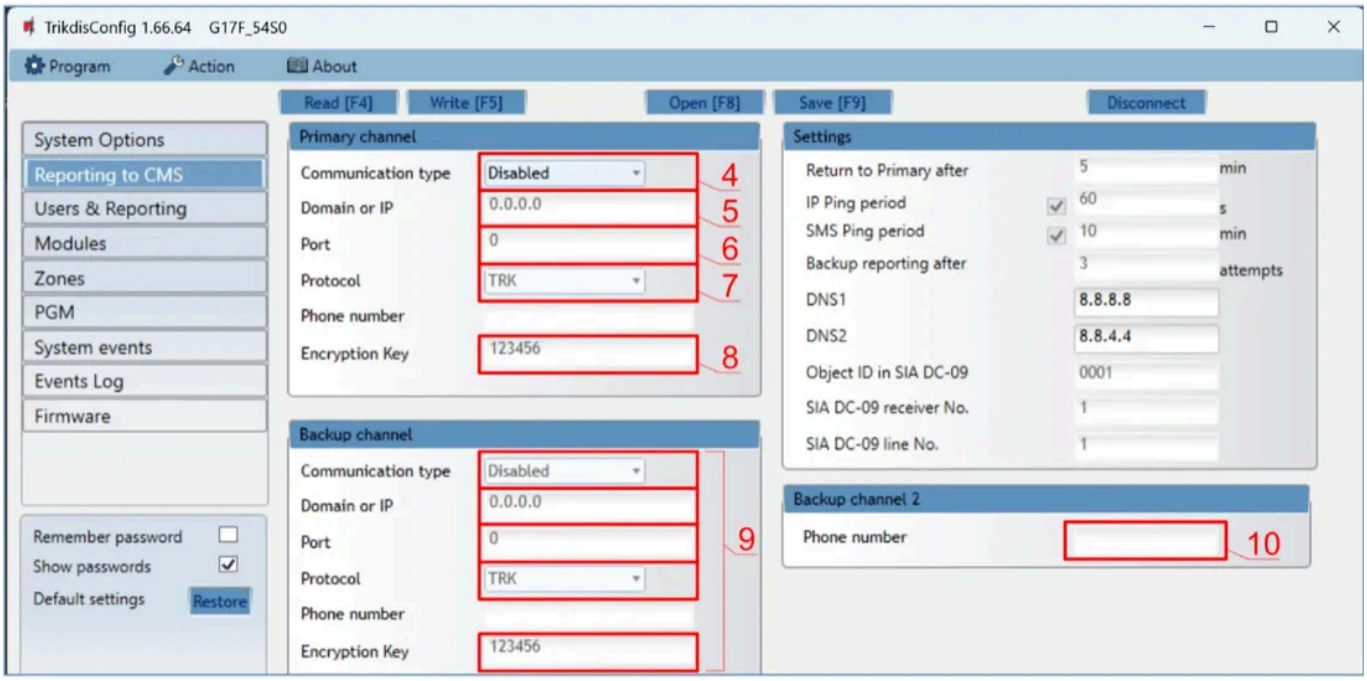


Figure 6. TrikdisConfig – **Reporting to CMS**.

- 4 **Communication type** – the type of 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 receiver

4. **Communication type** – select the type of connection (we do not recommend SMS on 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 with which the device sends the messages: **TRK** (for Trikdis receivers), **DC-09_2007** or **DC-09_2012** (for universal receivers).
8. **Encryption Key** – enter the encryption key of the receiver.

If you report to the monitoring station by SMS, you only need to fill in the **Encryption Key** and the **Phone number** fields. The SMS messages are received by the Trikdis **RL14** IP/SMS receiver, the **RM14** multi-channel receiver and the **GM14** SMS receiver. If you select DC-09 as the transmission 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 up the backup channel (**Backup channel**).
10. (Recommended) Enter the phone number of **Backup channel 2**.

At the end of the settings, click the **Write [F5]** button and unplug the USB cable. The other settings of the G17F 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.

This chapter describes mounting the G17F, wiring the fire alarm control panel (to the outputs of the panel, or over the RS485 bus to the panel with the ESPA 4.4.4 protocol, and to the NSC Solution, INIM Smartline and C-TEC Cast ZFP panels), connecting the inputs and the expansion modules (iO, iO-8, LORA, W485, E485), and finally switching on the communicator. In the drawings, the terminal names of the G17F are the same as the labels on the device (section 1.5).

3.1 Mounting and inserting the SIM card

1. Before the installation, make sure that the mobile network signal is strong enough where the G17F will be mounted.
2. Remove the front cover and pull off the terminal block.
3. Take out the printed circuit board.
4. Fix the back of the case to the desired place with screws.
5. Put back the printed circuit board and the terminal block.
6. Screw on the cellular antenna.
7. Insert the nano-SIM card. The SIM card must be registered in a mobile network, and its services must be switched on and working: it must be able to make calls and send and receive SMS, and it must have mobile data. Ask the mobile operator of the SIM card about switching on the services you need.

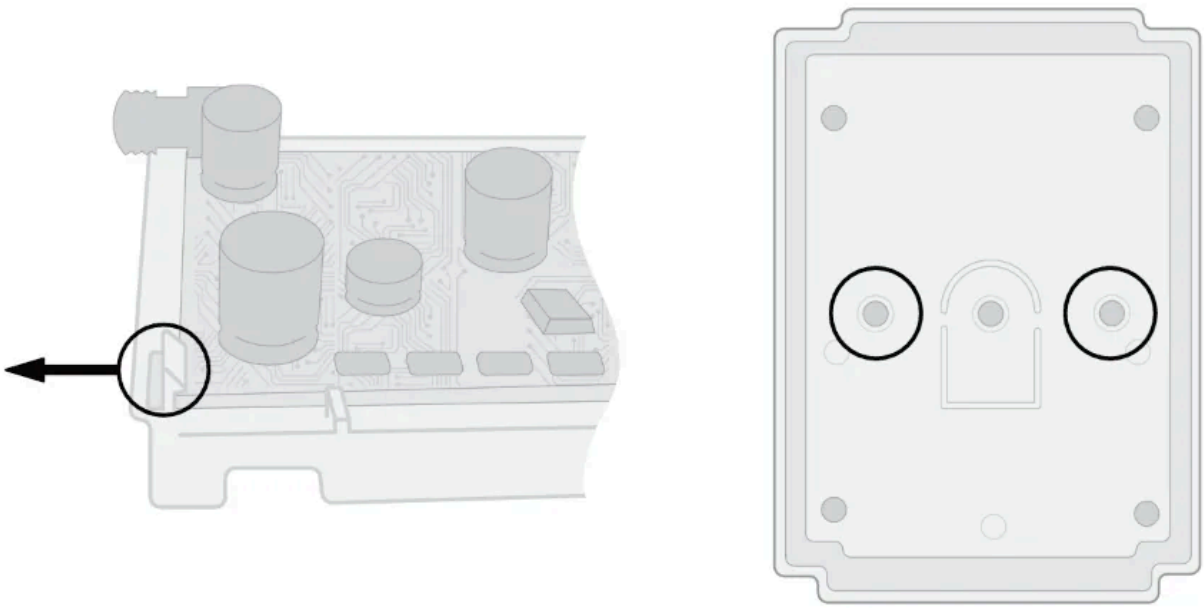


Figure 7. On the left, the retaining tab of the printed circuit board at the left edge of the board (this releases the board from the case); on the right, the two screw holes of the back plate.

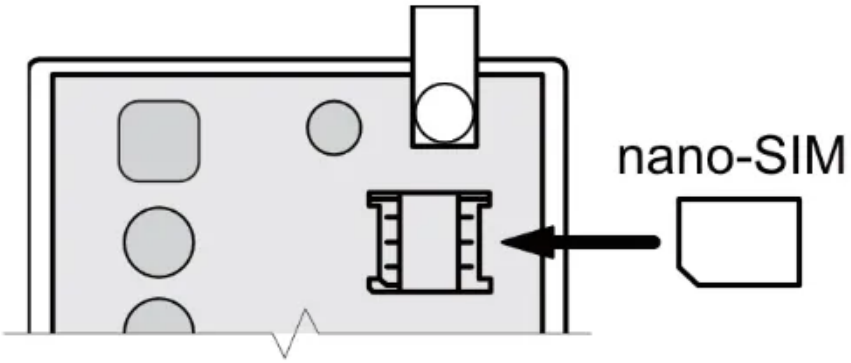


Figure 8. Inserting the nano-SIM card from the right into the holder on the printed circuit board.

- Check that the SIM card is activated.
- If you also communicate over an IP channel or with the Protegus 2 app, check that mobile data is switched on.
- If you do not want to enter the PIN code in TrikdisConfig, put the SIM card into a phone and switch off the PIN request.

8. For remote setup of the G17F, insert a SIM card with the PIN request switched off, and switch on the power of the communicator. If you have not yet set up the G17F with TrikdisConfig and the Protegus service is not switched on, send it this SMS:

```
CONNECT 123456 PROTEGUS=ON,APN=INTERNET
```

9. Remote setup of the parameters is described in chapter 6.
10. Put back the front cover.

The terminal block can be pulled off: this way the device can be disconnected from power or restarted with one movement, it is easier to handle during wiring, and for USB programming the device can be taken to the computer.

3.2 Wiring to the outputs of the fire alarm control panel

If you want to monitor the state of the fire alarm control panel, connect the appropriate outputs of the panel to the inputs of the G17F. The outputs of the panel (**PGM1**, **PGM2**, **PGM3**) must be set in the panel as status outputs (alarm, fault etc.).

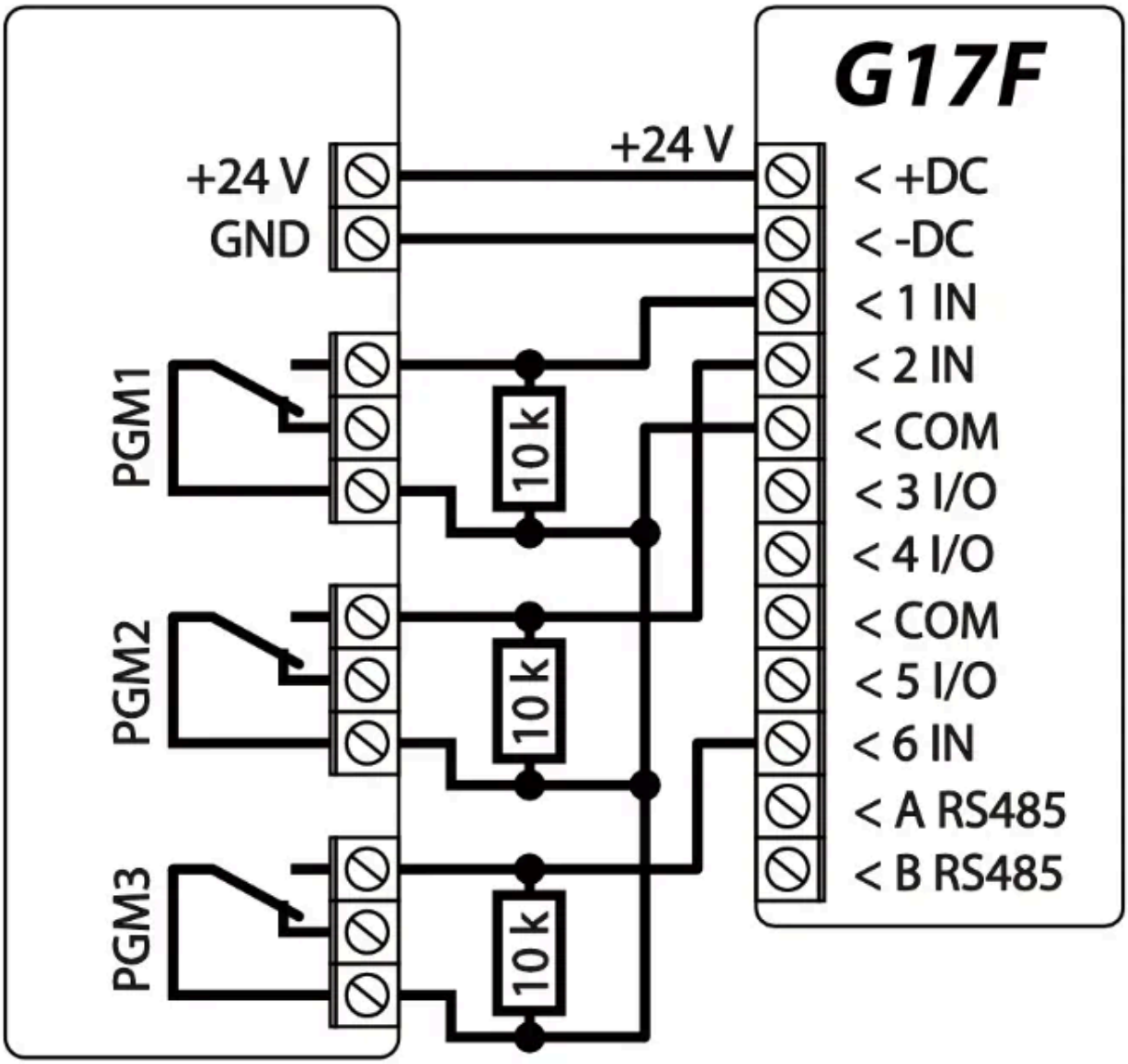


Figure 9. Wiring the G17F to the outputs of the fire alarm control panel (**Fire control panel**). Labels in the drawing: the **+24 V** terminal of the panel goes to the **+DC** terminal of the G17F, **GND** to **−DC**; one wire of the **PGM1**, **PGM2** and **PGM3** outputs goes to the **1 IN**, **2 IN** and **6 IN** input of the G17F respectively, the other to the **COM** terminal; a **10 k** (10 kΩ) resistor is connected in parallel between the two wires of each output.

3.3 Fire alarm control panel with the ESPA 4.4.4 protocol

Connect the fire alarm control panel with the ESPA 4.4.4 protocol to the G17F over the RS485 bus, as shown in the drawing below.

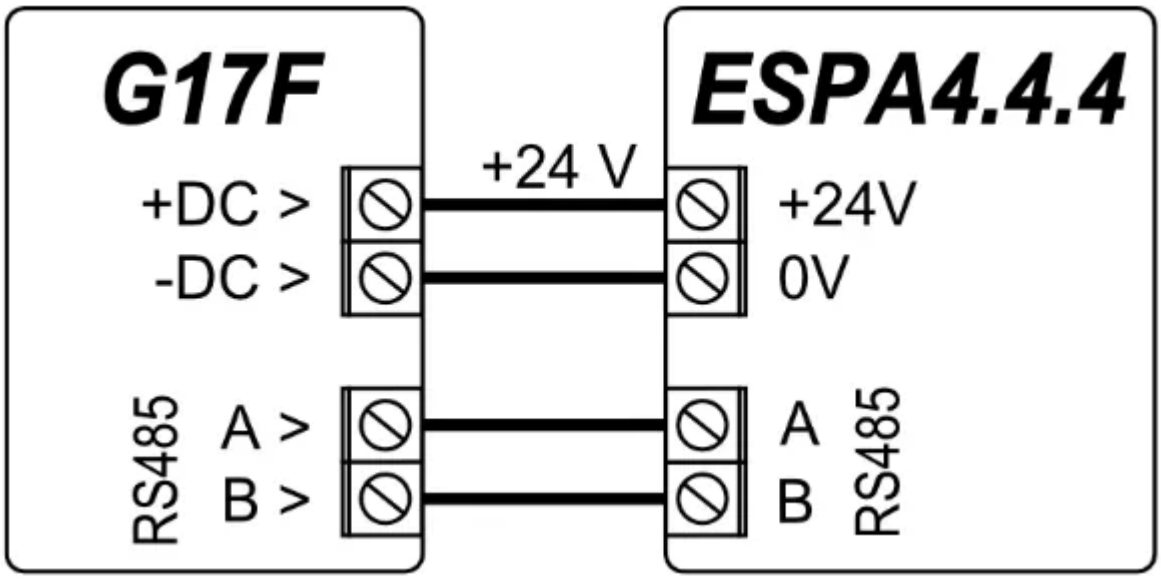


Figure 10. Connecting the G17F and the fire alarm control panel with the ESPA 4.4.4 protocol. Labels in the drawing: power – the **+DC** terminal of the G17F to the **+24V** terminal of the panel, **–DC** to **0V**; RS485 – terminal **A** of the G17F to terminal **A** of the panel, **B** to **B**.

Setting up the G17F in TrikdisConfig when it is connected to a fire alarm control panel with the ESPA 4.4.4 protocol:

1. On the **Modules** page, select the **ESPA 4.4.4** protocol.
2. Select the data transfer rate of the interface (**Baudrate**).
3. The data transfer parameters of the G17F and of the fire alarm control panel must be the same.

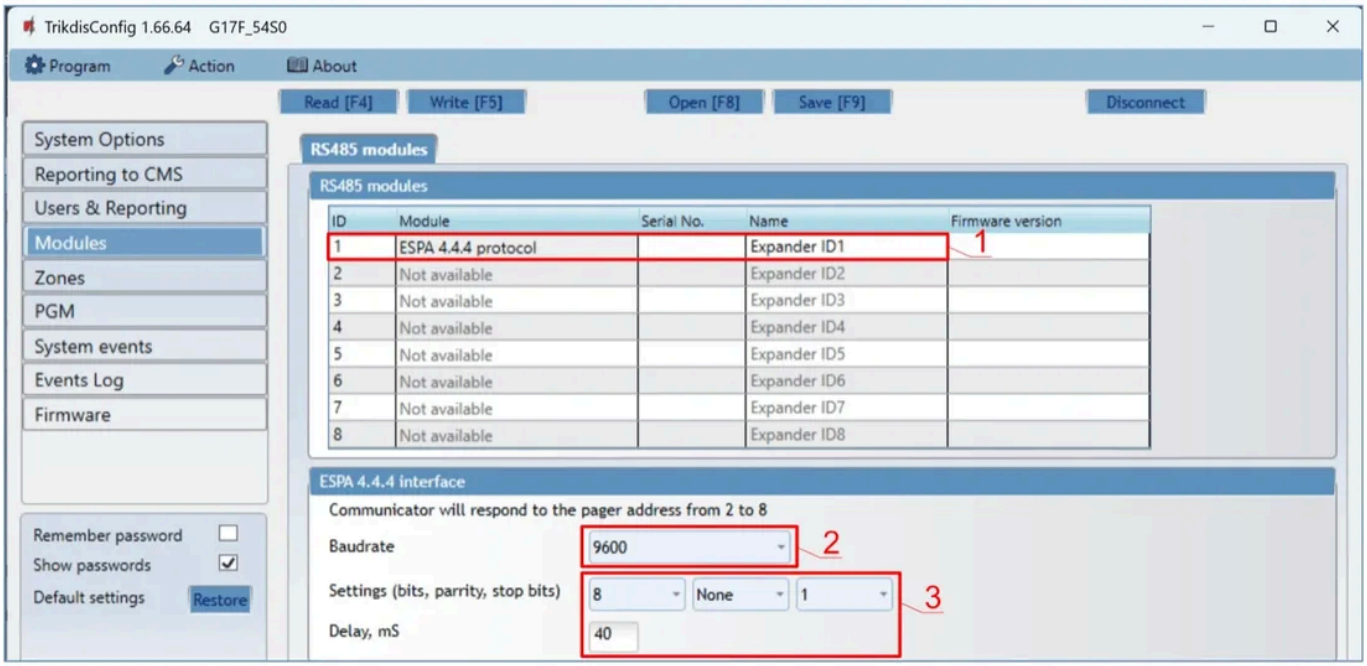


Figure 11. TrikdisConfig – **Modules**: RS485 module 1 is **ESPA 4.4.4 protocol**. The label of the **ESPA 4.4.4 interface** group: "Communicator will respond to the pager address from 2 to 8" – the communicator responds to pager addresses 2–8.

- 1 selecting **ESPA 4.4.4 protocol**
- 2 **Baudrate** – data transfer rate (9600 in the picture)
- 3 data bits, parity, stop bits and delay (8, None, 1, 40 ms in the picture)

4. On the **Users & Reporting** page, enter the phone numbers of the users who receive messages from the G17F (section 5.4).

5. If you want the user to receive a message (or a call) about the events, tick the **SMS** (or **Call**) checkbox on the **SMS & Call reporting** tab of the **System events** page.

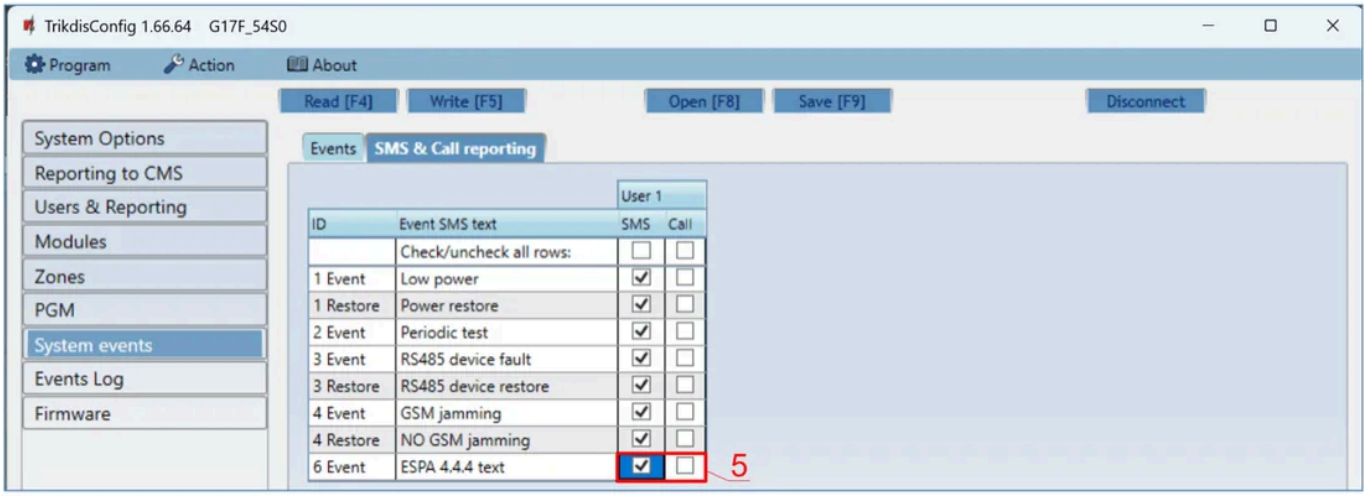


Figure 12. TrikdisConfig – **System events**, **SMS & Call reporting** tab: for user 1, **SMS** is ticked for the **ESPA 4.4.4 text** event.

- 5 the **SMS** and **Call** checkboxes for the **ESPA 4.4.4 text** event

6. If the messages must also reach the receiver of the monitoring station, set up the communication channel on the **Reporting to CMS** page (sections 2.2 and 5.3). The event messages are sent with the **SIA DC-09** protocol.

Try the system: trigger a fire alarm and check that the messages of the G17F arrive at the monitoring station and in Protegus 2.

3.4 NSC Solution fire alarm control panel

Connect the NSC Solution fire alarm control panel to the G17F over the RS485 bus, as shown in the drawing below.

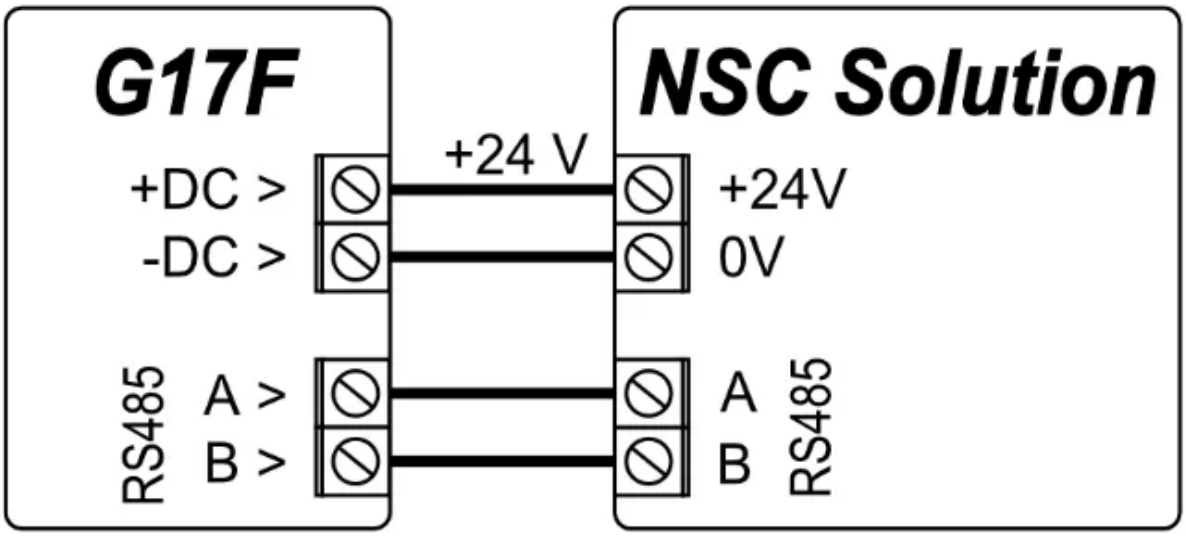


Figure 13. Connecting the G17F and the NSC Solution fire alarm control panel. Labels in the drawing: power – the **+DC** terminal of the G17F to the **+24V** (+24 V) terminal of the panel, **–DC** to **0V**; RS485 – **A** to **A**, **B** to **B**.

Setting up the G17F in TrikdisConfig when it is connected to an NSC Solution fire alarm control panel:

1. On the **Modules** page, select the **NSC Solution** module.

2. The **NSC slave address** (the slave address of the communicator) must not be the same as the address of the modules connected to the fire alarm control panel.

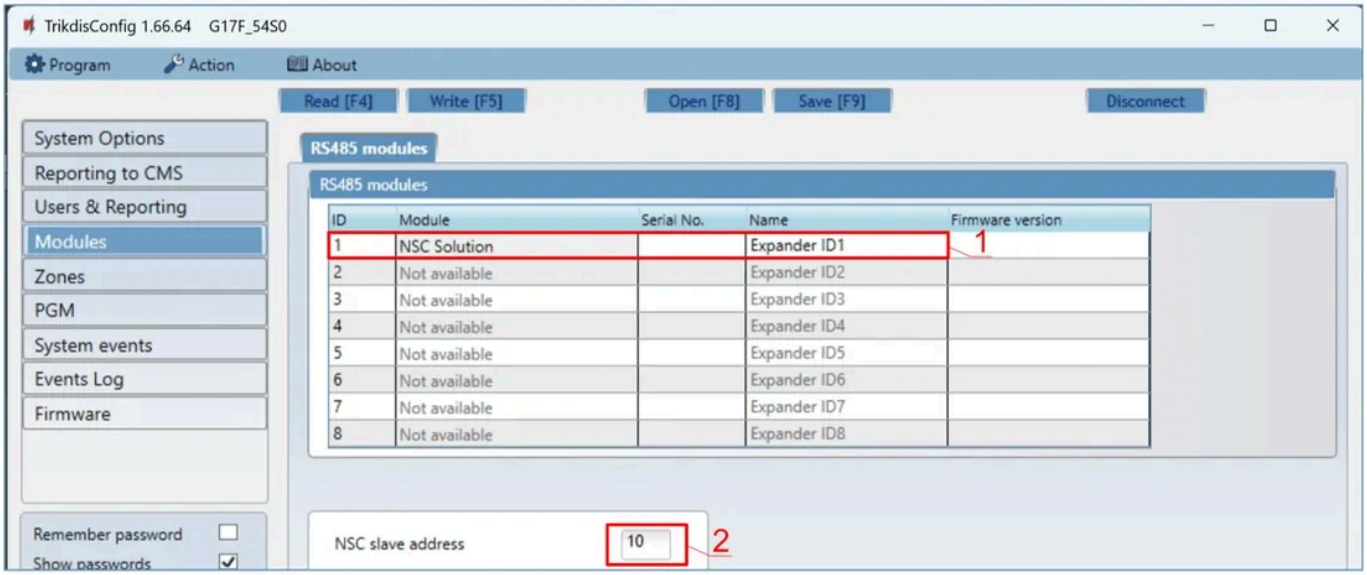


Figure 14. TrikdisConfig – **Modules**: RS485 module 1 is **NSC Solution** (its name is **Expander ID1**).

- 1 selecting **NSC Solution**
- 2 **NSC slave address** – 10 in the picture

3. On the **Users & Reporting** page, enter the phone numbers of the users who receive messages from the G17F (section 5.4).
4. The users receive SMS messages and calls about the ticked events (**Users & Reporting** page, **SMS for Panel events** tab). In the **CID** column you can add further Contact ID event codes; next to the new codes you must also enter the text of the SMS. If you want the user to receive a message (or a call) about the events, tick the **SMS** (or **Call**) checkbox.

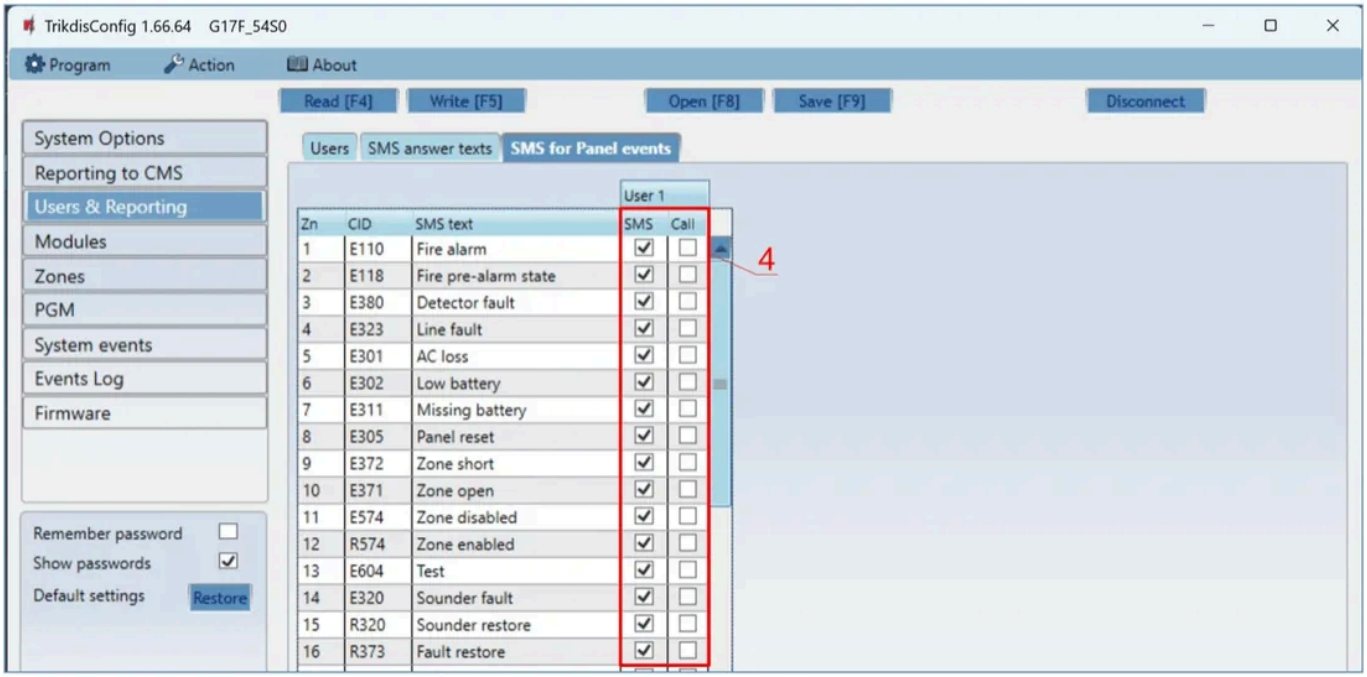


Figure 15. TrikdisConfig – **Users & Reporting**, **SMS for Panel events** tab: for user 1, **SMS** is ticked for the 16 visible events (from the **E110 Fire alarm** fire alarm to the **R373 Fault restore** fault restore), **Call** is empty.

- 4 the **SMS** and **Call** columns of user 1

5. If the messages must also reach the receiver of the monitoring station, set up the communication channel on the **Reporting to CMS** page (sections 2.2 and 5.3).

After setting up the G17F, switch on the power of the fire alarm control panel and wait until the software of the panel has loaded. Then the modules connected to the RS485 bus must be searched for (scanned) on the panel. On the panel, press: **PROG.** > **INSTALLER** > (enter the installer code) **00000 OK** > (select) **SETTINGS** > **ENTER** > (select) **SCAN RS485** > **ENTER**. Wait until the search has finished, then return to the main screen by pressing the **CANCEL** button twice.

Try the system: trigger a fire alarm and check that the messages of the G17F arrive at the monitoring station and in Protegus 2.

3.5 INIM Smartline fire alarm control panel

Connect the INIM Smartline fire alarm control panel to the G17F over the RS485 bus, as shown in the drawing below.

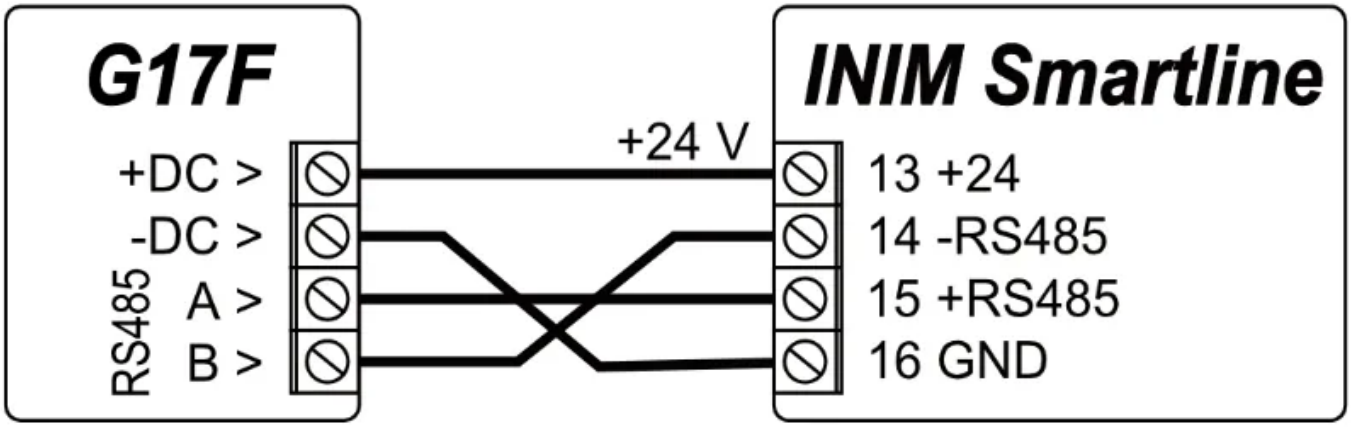


Figure 16. Connecting the G17F and the INIM Smartline fire alarm control panel. Labels in the drawing: power – the **+DC** terminal of the G17F to the **13 +24** (+24 V) terminal of the panel, **–DC** to **16 GND**; RS485 – **A** to **15 +RS485**, **B** to **14 –RS485**. Wires crossing each other do not touch.

If you connect the INIM Smartline panel to the G17F over the RS485 bus, the panel must be set to **slave** mode – you can do this in the SmartLeague program of the panel.

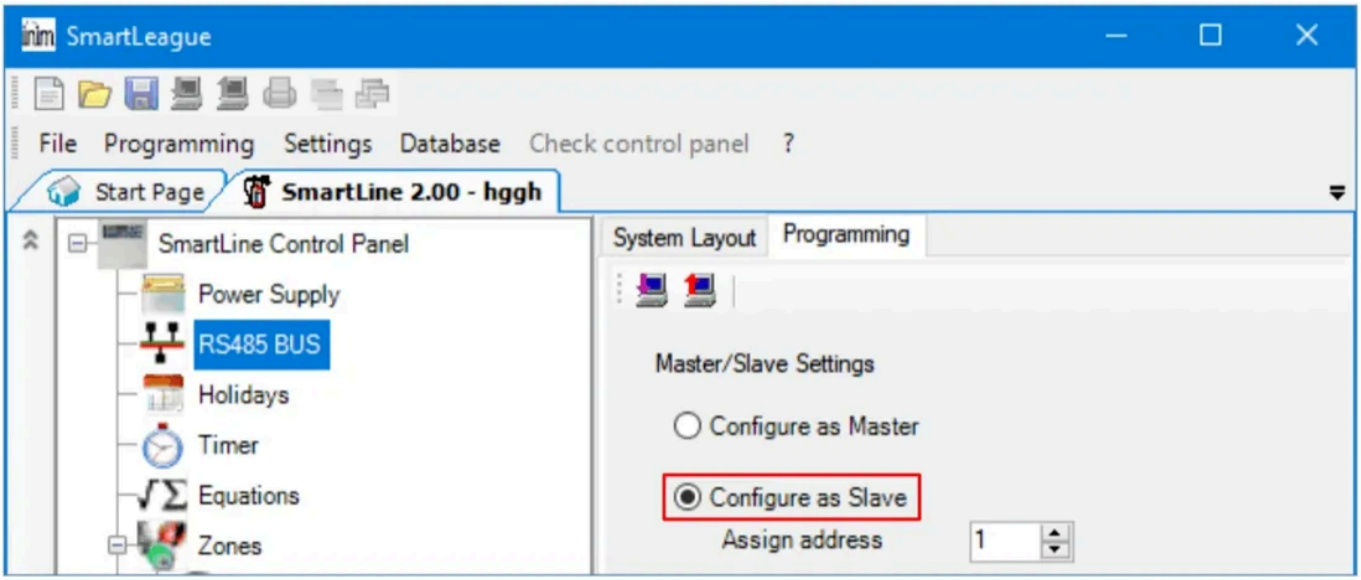


Figure 17. SmartLeague – **RS485 Bus Programming** window: in the **Master/Slave Settings** group, **Configure as Slave** is selected, **Assign address**: 1.

- If repeaters are connected to the INIM Smartline panel, the G17F cannot be connected over the RS485 bus.
- If the G17F is connected to the RS485 bus of the INIM Smartline panel, the iO expansion modules of the communicator are not supported.

Setting up the G17F in TrikdisConfig when it is connected to an INIM Smartline fire alarm control panel:

1. On the **Modules** page, select the **Inim Smartline** module.

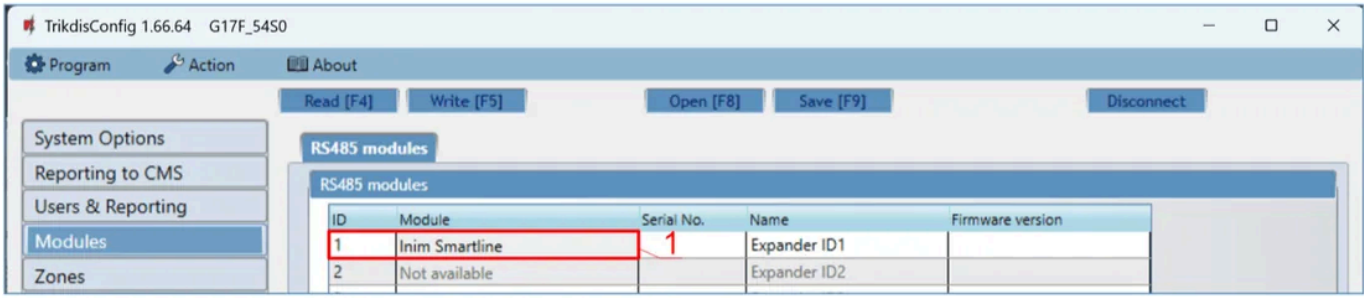


Figure 18. TrikdisConfig – **Modules**: RS485 module 1 is **Inim Smartline** (its name is **Expander ID1**).

- 1 selecting **Inim Smartline**

2. On the **Users & Reporting** page, enter the phone numbers of the users who receive messages from the G17F (section 5.4).
3. The users receive SMS messages and calls about the ticked events (**Users & Reporting** page, **SMS for Panel events** tab – a picture of the tab is in sections 3.4 and 5.4). In the **CID** column you can add further Contact ID event codes; next to the new codes you must also enter the text of the SMS. If you want the user to receive a message (or a call) about the events, tick the **SMS** (or **Call**) checkbox.
4. If the messages must also reach the receiver of the monitoring station, set up the communication channel on the **Reporting to CMS** page (sections 2.2 and 5.3).

Try the system: trigger a fire alarm and check that the messages of the G17F arrive at the monitoring station and in Protegus 2.

3.6 C-TEC Cast ZFP fire alarm control panel

Connect the C-TEC Cast ZFP fire alarm control panel to the G17F over the ABUS RS485 bus, as shown in the drawing below.

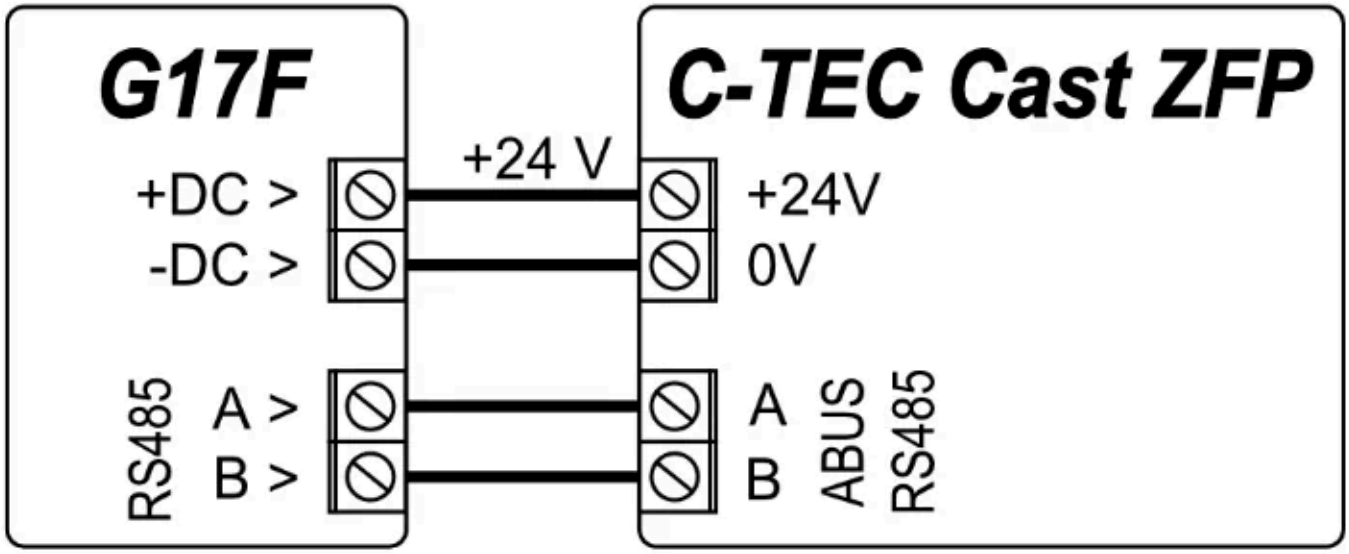


Figure 19. Connecting the G17F and the C-TEC Cast ZFP fire alarm control panel. Labels in the drawing: power – the **+DC** terminal of the G17F to the **+24V** (+24 V) terminal of the panel, **–DC** to **0V**; **ABUS RS485** – **A** to **A**, **B** to **B**.

Setting up the G17F in TrikdisConfig when it is connected to a C-TEC Cast ZFP fire alarm control panel:

1. On the **Modules** page, select the **C-TEC Cast ZFP** fire alarm control panel.

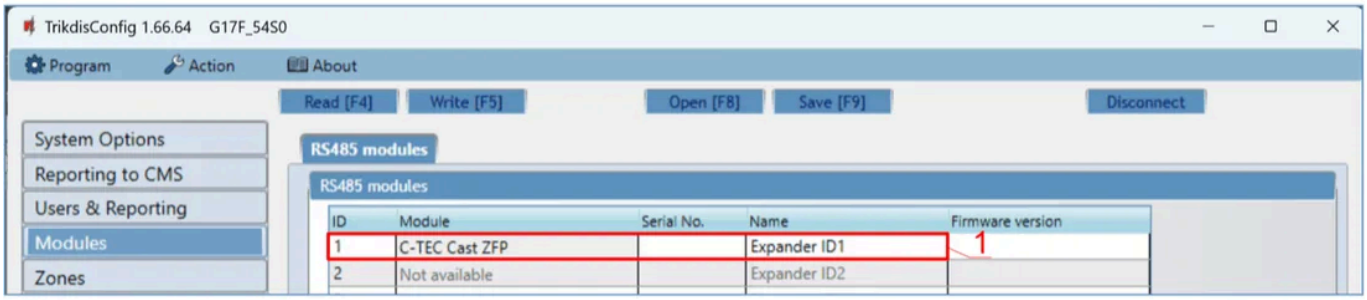


Figure 20. TrikdisConfig – **Modules**: RS485 module 1 is **C-TEC Cast ZFP** (its name is **Expander ID1**).

- 1 selecting **C-TEC Cast ZFP**

2. On the **Users & Reporting** page, enter the phone numbers of the users who receive messages from the G17F (section 5.4).
3. The users receive SMS messages and calls about the ticked events (**Users & Reporting** page, **SMS for Panel events** tab – a picture of the tab is in sections 3.4 and 5.4). In the **CID** column you can add further Contact ID event codes; next to the new codes you must also enter the text of the SMS. If you want the user to receive a message (or a call) about the events, tick the **SMS** (or **Call**) checkbox.
4. If the messages must also reach the receiver of the monitoring station, set up the communication channel on the **Reporting to CMS** page (sections 2.2 and 5.3).

3.6.1 Setting up the C-TEC panel (ZFPtools)

Install the **ZFPtools** program on the computer and start it. Switch on the power of the fire alarm control panel and wait until the software of the panel has loaded. Connect the panel to the computer with a **USB 2.0 A-B** cable.

1. Open the **Node View** tab.

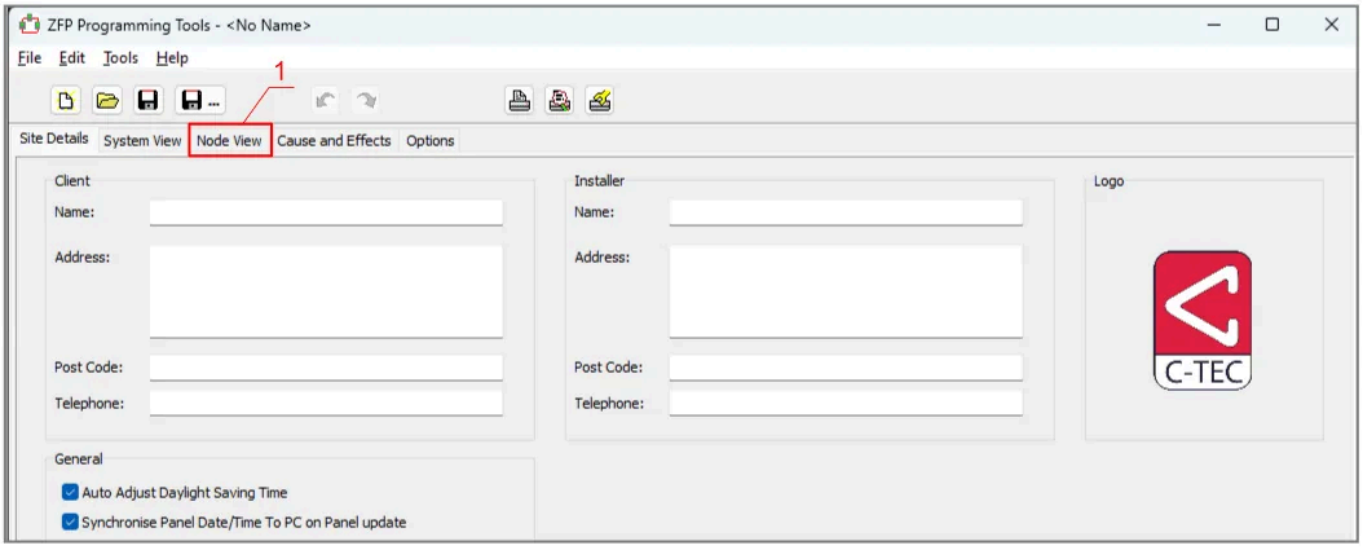


Figure 21. ZFP Programming Tools – **Site Details** window.

- 1 the **Node View** tab

2. Download the settings of the fire alarm control panel to the computer (**Retrieve All Data**).

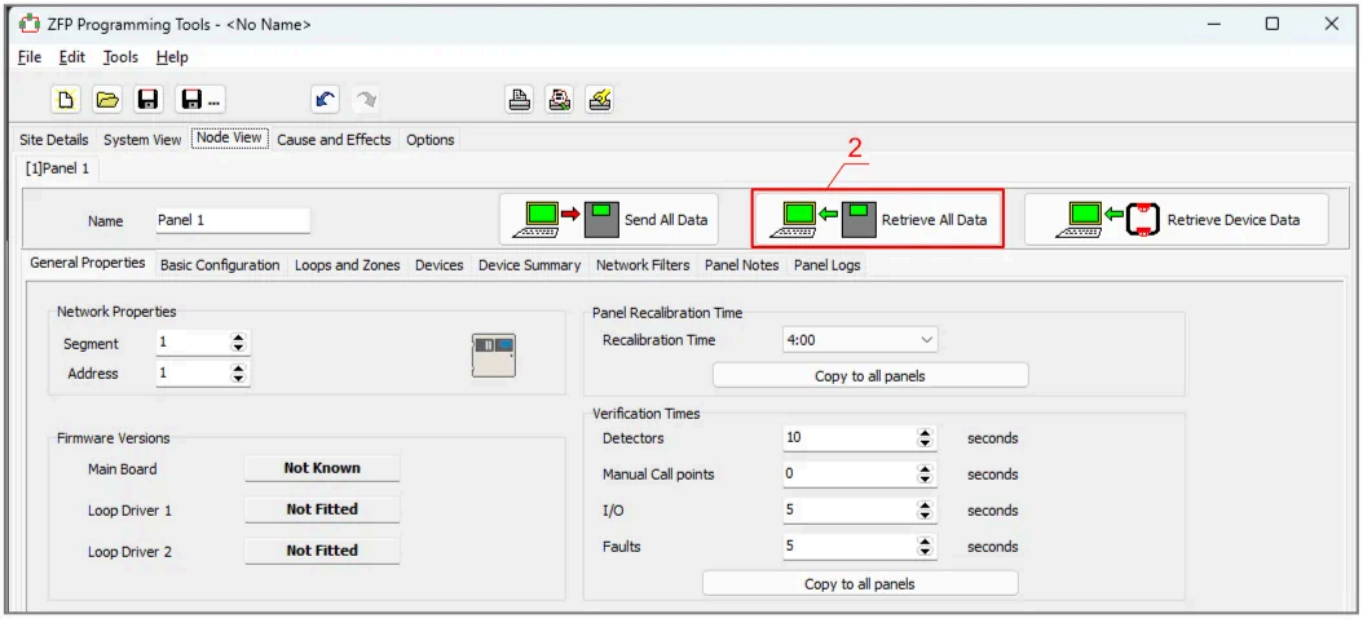


Figure 22. ZFP Programming Tools – **Node View**, **Panel 1**: the **Retrieve All Data** button.

- 2 **Retrieve All Data** – downloading the settings of the panel

3. Enter the code (default `4444`).
4. Click the **OK** button (the green tick).

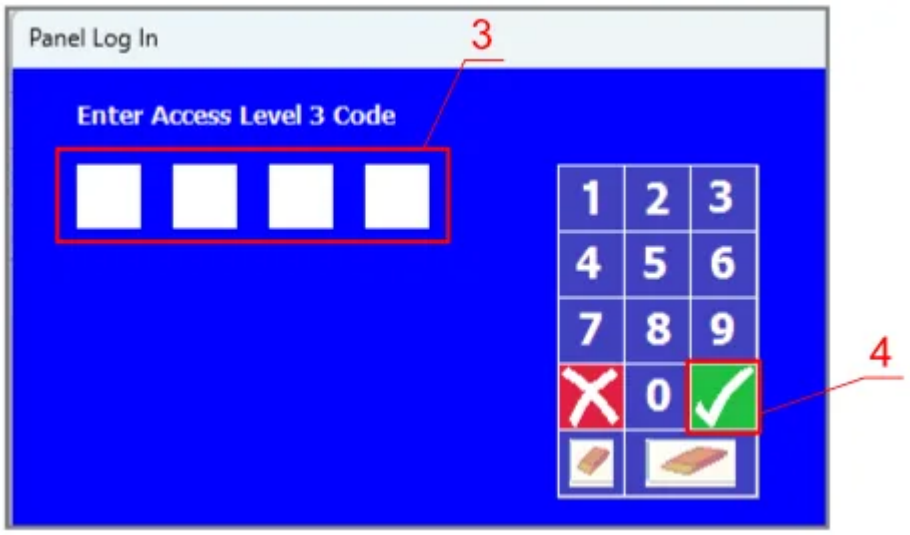


Figure 23. ZFP Programming Tools – **Panel Log In** window: **Enter Access Level 3 Code** – the code of access level 3.

- 3 the four code fields
- 4 the **OK** button (green tick)

5. Select the **BMS Interface** device (**Device Palette**).
6. Click a free icon position.

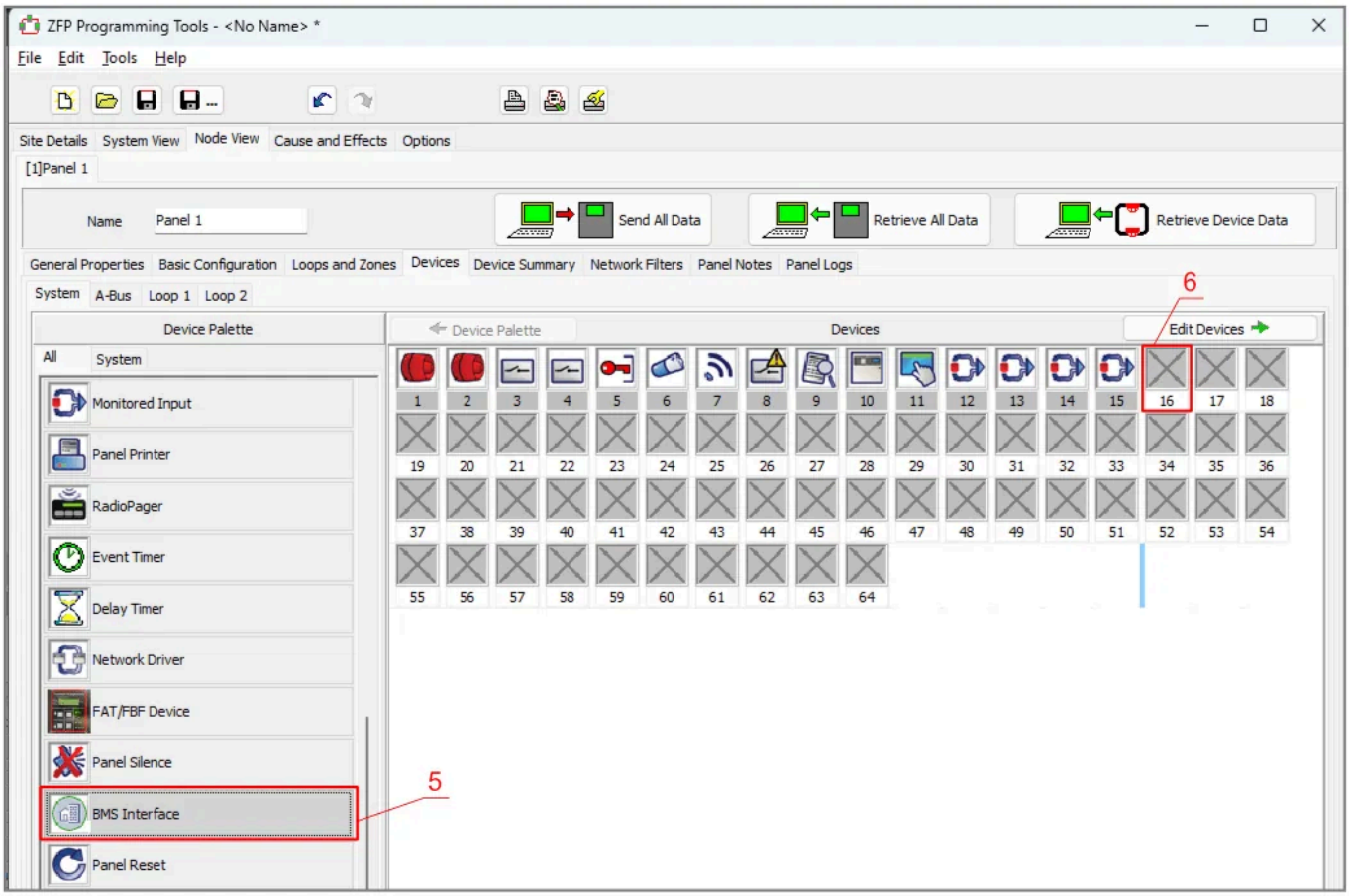


Figure 24. ZFP Programming Tools – **Node View**, **Devices**: **BMS Interface** selected in the **Device Palette** list.

- 5 **BMS Interface** in the **Device Palette** list
- 6 free icon position (no. 16 in the picture)

7. Click the **Edit Devices** button.

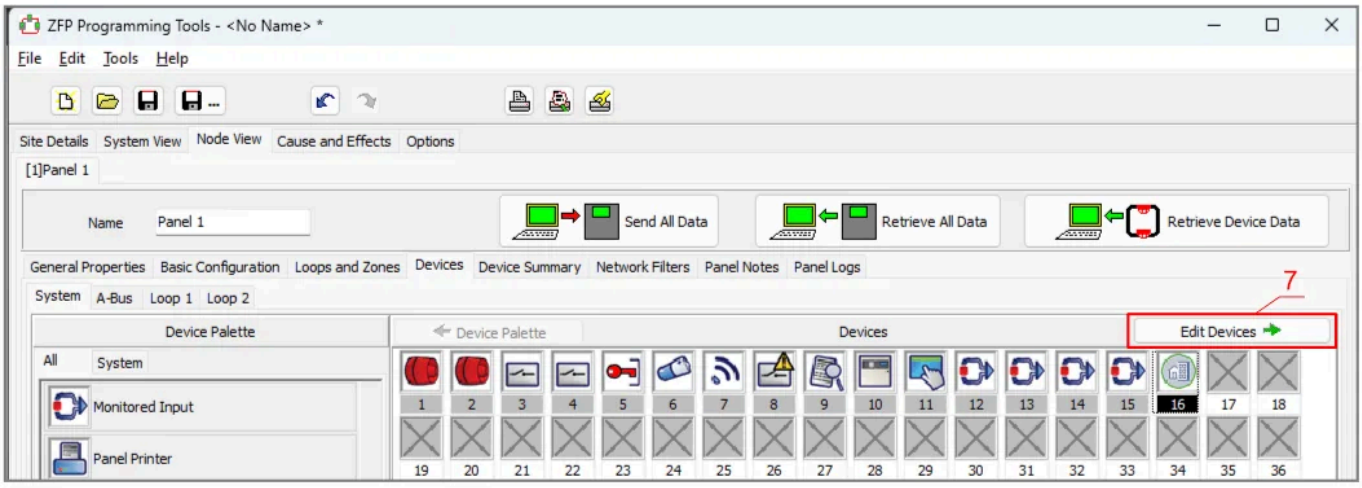


Figure 25. ZFP Programming Tools – **Node View**, **Devices**: **BMS Interface** in position 16; the **Edit Devices** button.

- 7 **Edit Devices**

8. On the **Device** tab, enter the name of the system.

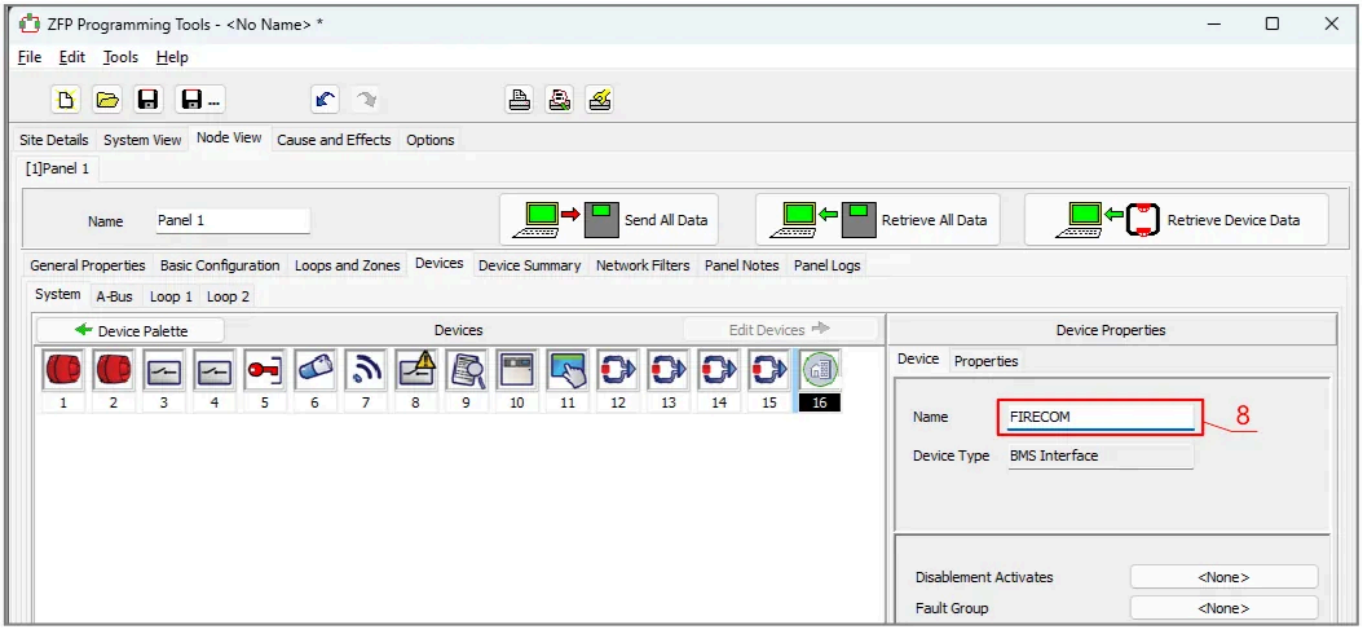


Figure 26. ZFP Programming Tools – **Device Properties**, **Device** tab: **Name**: FIRECOM, **Device Type**: BMS Interface.

- 8 **Name** – the name of the system

9. On the **Properties** tab, enter the name of the system.
10. Select the **ABUS RS485** bus to which the G17F is connected.
11. Set up the messages.
12. Write the settings into the fire alarm control panel (**Send All Data**).

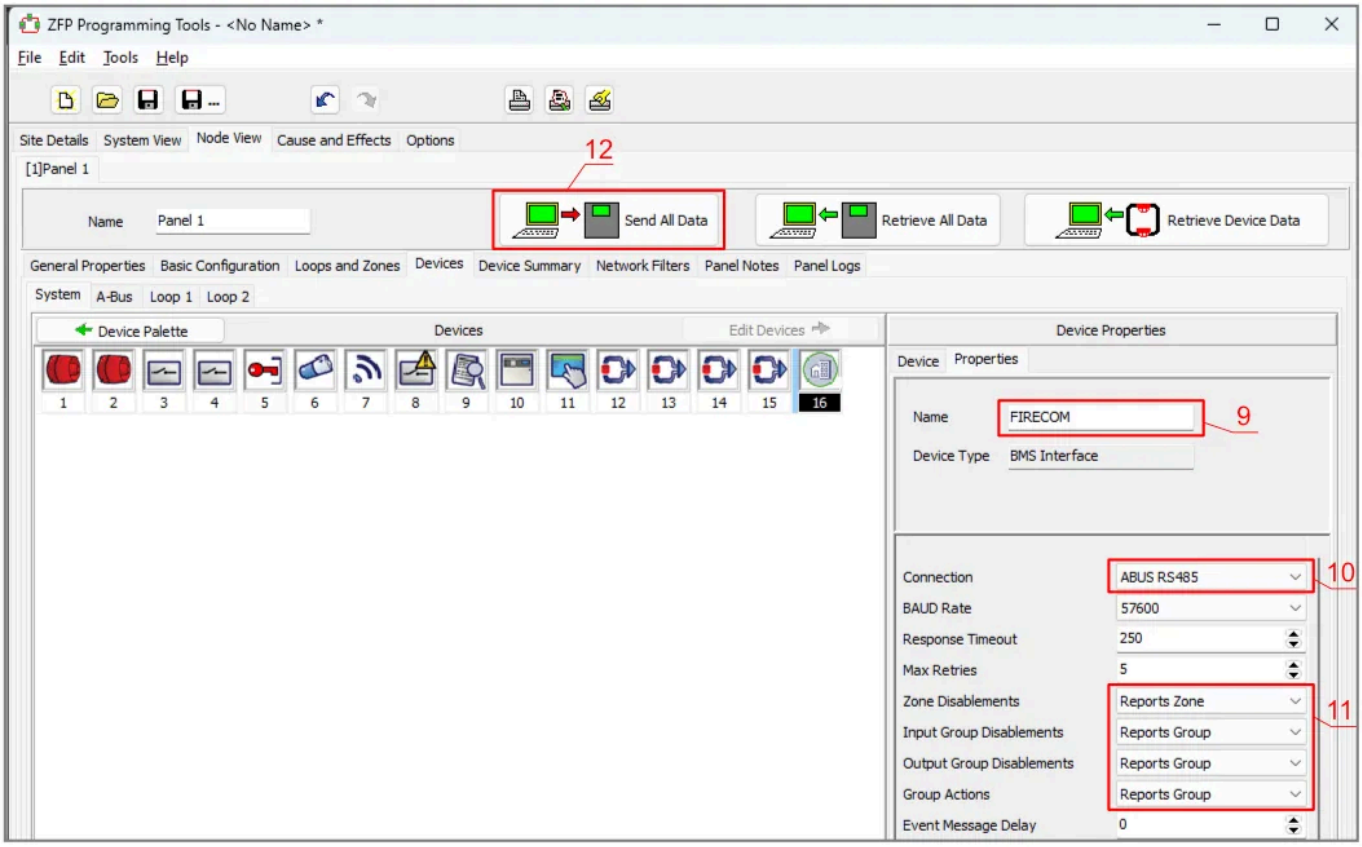


Figure 27. ZFP Programming Tools – **Device Properties**, **Properties** tab. In the picture: **BAUD Rate** 57600, **Response Timeout** 250, **Max Retries** 5.

- 9 **Name** – the name of the system (FIRECOM)
- 10 **Connection** – **ABUS RS485**
- 11 the messages: **Zone Disablements** – **Reports Zone**; **Input Group Disablements**, **Output Group Disablements** and **Group Actions** – **Reports Group**
- 12 **Send All Data** – writing the settings into the panel

13. Enter the code (default `4444`) – in the same **Panel Log In** window as in step 3.
14. Click the **OK** button.

The fire alarm control panel is programmed. Unplug the USB 2.0 A-B cable from the panel.

Try the system: trigger a fire alarm and check that the messages of the G17F arrive at the monitoring station and in Protegus 2.

3.7 Wiring the inputs

The communicator has six input terminals (**1 IN** – **6 IN**; three of them are dual-purpose, IN/OUT), to which NO, NC and EOL (4.7 kΩ, 10 kΩ) type circuits can be connected. By default the inputs monitor an EOL type circuit; you can set another type on the **Zones** page of TrikdisConfig (section 5.6).

Wiring	Normal (restore)	Alarm
NO – normally open contact	open	short circuit
NC – normally closed contact	short circuit	open
NO + EOL – open contact with a 10 kΩ resistor in parallel	10 kΩ	short circuit or open
NC + EOL – closed contact with a 10 kΩ resistor in series	10 kΩ	short circuit or open

Drawings of the four wiring modes; the contact goes between the **COM** and the **INx** terminal, **10k** is the 10 kΩ end-of-line resistor.

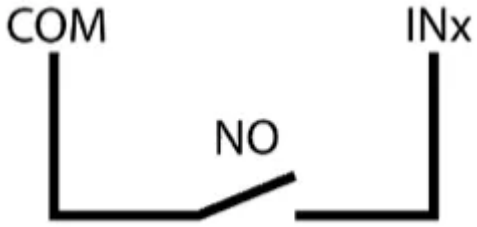


Figure 28. NO – normally open contact.

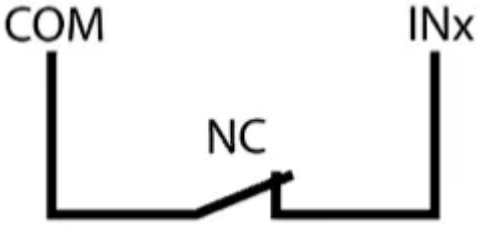


Figure 29. NC – normally closed contact.

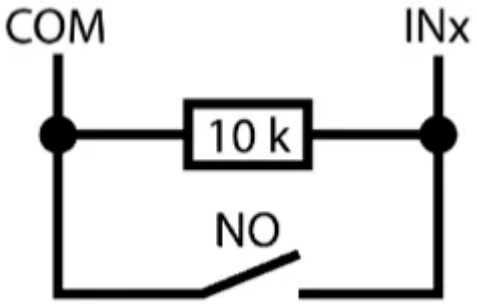


Figure 30. NO + EOL (EOL10k) – normally open contact with a 10 kΩ resistor in parallel.

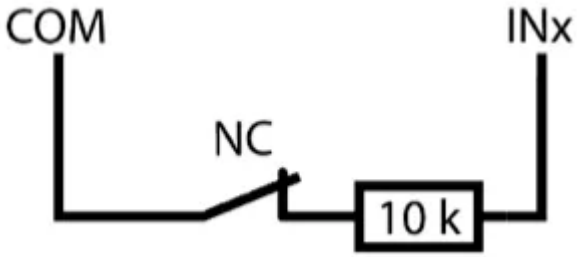


Figure 31. NC + EOL (EOL10k) – normally closed contact with a 10 kΩ resistor in series.

3.8 iO series expansion modules

If the communicator needs more inputs (IN) or outputs (OUT), connect a wired or wireless Trikdis iO series input and output expander to it.

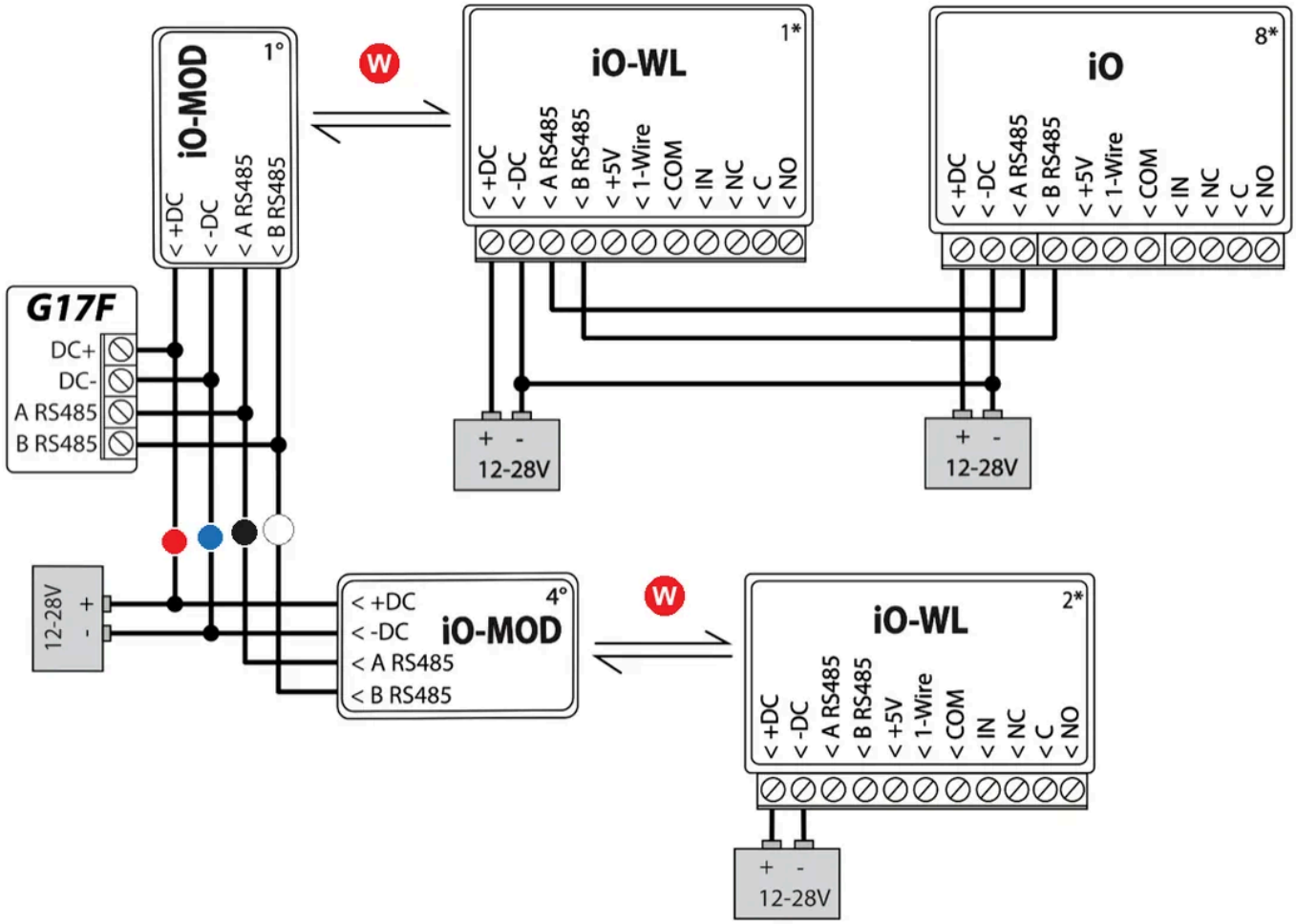


Figure 32. iO-MOD, iO-WL and iO modules on the G17F: the **DC+** terminal of the G17F to the **+DC** terminal of the iO-MOD (red wire), **DC–** to **–DC** (blue), **A RS485** to **A RS485** (black), **B RS485** to **B RS485** (white); common 12–28 V power supply; up to 4 iO-MOD modules ("up to 4 iO-MOD modules", marked with ° in the drawing); each iO-MOD connects by radio to an iO-WL, at up to 300 m; the iO-WL connects to the iO module over the RS485 bus (A–A, B–B) ("RS485 connection"), at up to 300 m ("up to 300 m"); up to 8 system expansion modules ("up to 8 system expansion modules", marked with * in the drawing); the negative pole of the 12–28 V power supply of the iO-WL and the iO module is common, the other iO-WL gets its own 12–28 V power supply.

- red wire ("Red wire")
- blue wire ("Blue wire")
- black wire ("Black wire")
- white wire ("White wire")
- W wireless connection ("Wireless connection"), up to 300 m ("up to 300 m")

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.

3.9 iO-8 expansion module

If the communicator needs more inputs (IN) or outputs (OUT), connect an **iO-8** wired expander to it. Detailed description of the expander: iO8 input and output expander – installation manual.

Trikdis iO8 wired expander module

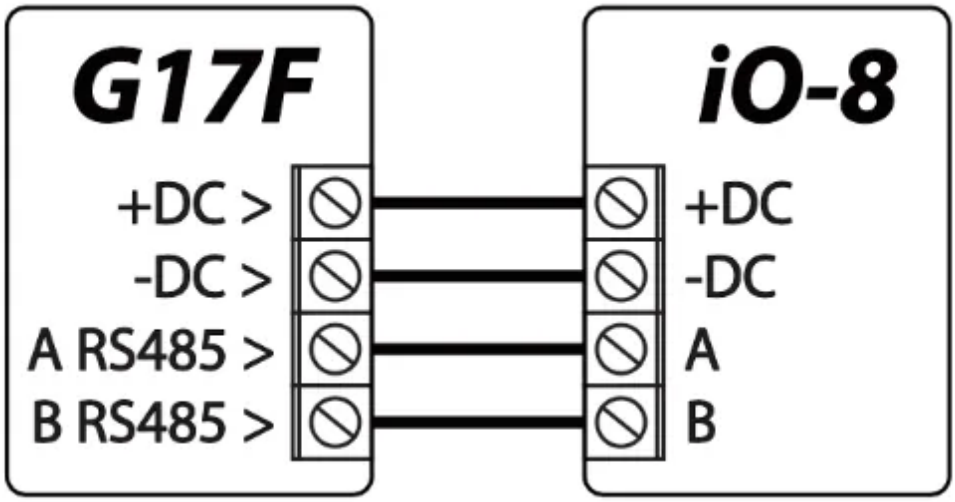


Figure 33. Wiring the iO-8 expander: the **+DC** terminal of the G17F to the **+DC** terminal of the iO-8, **−DC** to **−DC**, **A RS485** to **A**, **B RS485** to **B**.

3.10 LORA series expansion modules

The LORA modules connect to the G17F by radio: the **RF-LORA** transceiver goes on the RS485 bus, and it keeps the connection at up to 5000 m with the **iO-LORA**, **iO8-LORA** and **REL-LORA** expanders and the **PB-LORA** panic button. You add the modules on the **Modules** page of TrikdisConfig (section 5.5).

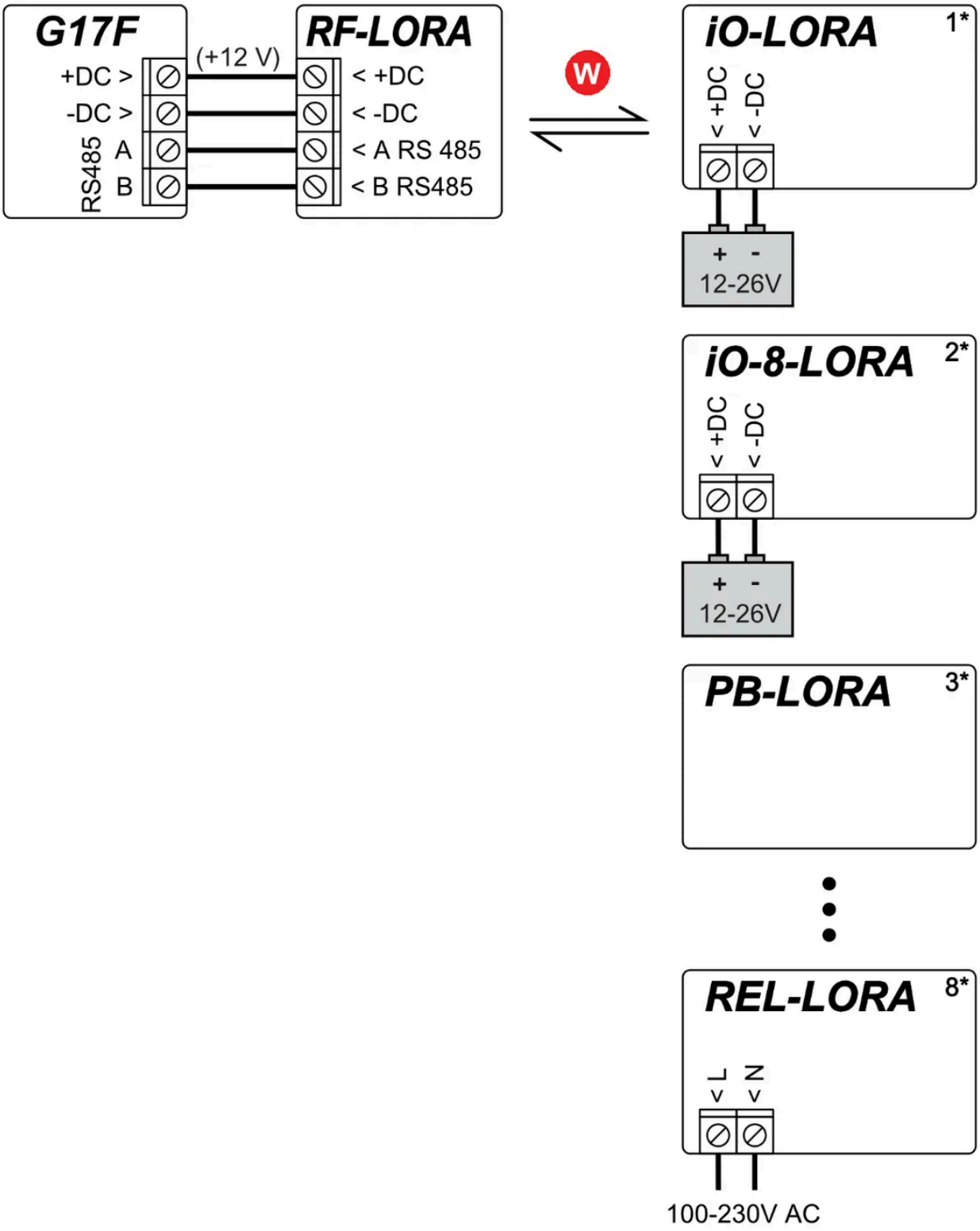


Figure 34. Wiring the LORA modules: the **+DC** terminal of the G17F to the **+DC** (+12 V) terminal of the RF-LORA, **–DC** to **–DC**; RS485 – terminal **A** of the G17F to **A RS 485** of the RF-LORA, **B** to **B RS485**; radio connection at up to 5000 m with the **iO-LORA**, **iO8-LORA**, **PB-LORA** … **REL-LORA** modules (marked 1, *2*, 3* … 8* in the corner of the modules); the iO-LORA and the iO8-LORA get their own 12–26 V power supply (**+DC**, **–DC**), the REL-LORA 100–230 V AC mains power (**L**, **N**).

- W wireless connection ("Wireless connection"), up to 5000 m ("up to 5000 m")

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.

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

Trikdis IO8-LORA wireless expander module | **Trikdis PB-LORA wireless panic button**

3.11 W485 Wi-Fi module

The **W485** module sends the messages of the G17F over Wi-Fi, through the internet router, to the monitoring station and to the Protegus 2 app. As long as there is a Wi-Fi connection, the G17F sends the event messages through the W485; if the Wi-Fi connection is lost, it sends them over the mobile network (GPRS), and when the Wi-Fi connection is restored, it returns to the W485. The function works from firmware **1.08** of the G17F. **With the W485, the G17F can also be used without a SIM card.** Setting up the W485 for the G17F: section 5.5.

Trikdis W485 Wifi module (RS485)

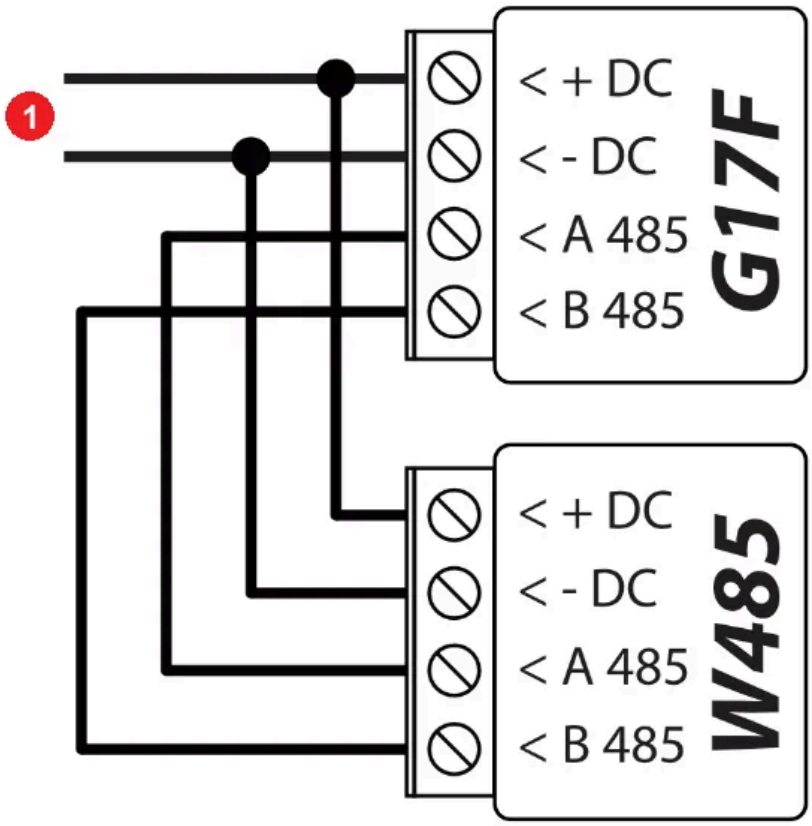


Figure 35. Wiring the W485 module: the positive pole of the power supply to the **+DC** terminal of the G17F and the W485, the negative to **–DC**; RS485 connection ("RS485 connection"), up to 100 m ("up to 100 m"): the **A 485** terminal of the G17F to **A 485** of the W485, **B 485** to **B 485**.

- 1 power supply ("Power supply"), 12 V DC, 0.5 A

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.

3.12 E485 Ethernet module

The **E485** module sends the messages of the G17F over a wired internet connection to the monitoring station and to the Protegus 2 app. With the E485, the messages go over the wired internet, the G17F does not use mobile internet. If the wired internet connection is lost, the G17F sends the messages over mobile internet, and when the wired connection is restored, again through the E485. The function works from firmware **1.08** of the G17F. **With the E485, the G17F can also be used without a SIM card.** Setting up the E485 for the G17F: section 5.5.

Trikdis E485 Ethernet module (RS485)

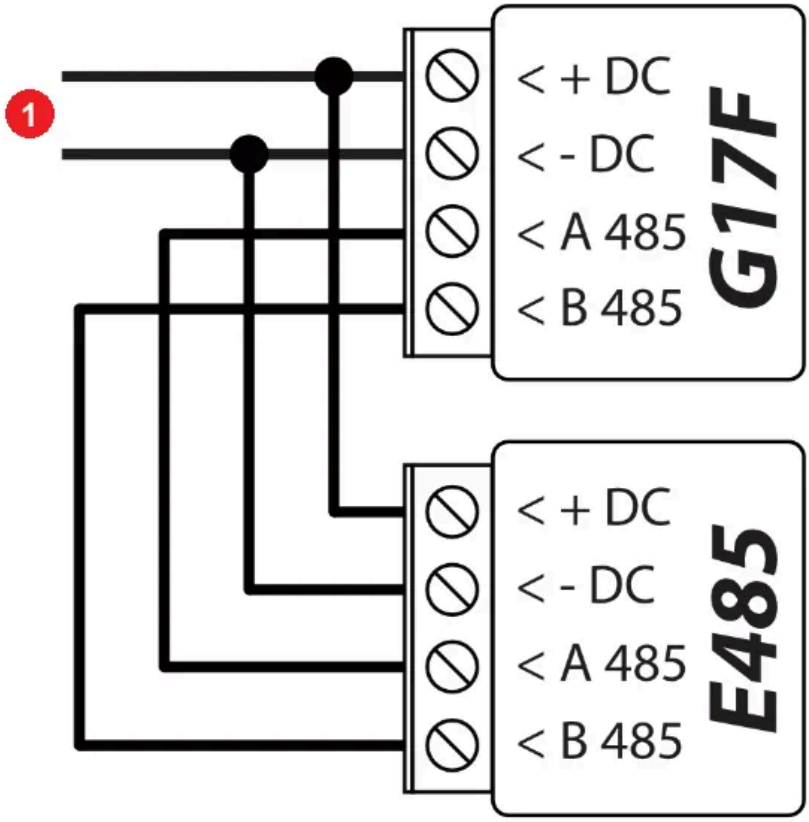


Figure 36. Wiring the E485 module: the positive pole of the power supply to the **+DC** terminal of the G17F and the E485, the negative to **–DC**; RS485 connection ("RS485 connection"), up to 100 m ("up to 100 m"): the **A 485** terminal of the G17F to **A 485** of the E485, **B 485** to **B 485**.

- 1 power supply ("Power supply"), 12 V DC, 0.5 A

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.

3.13 Switching on the communicator

To switch on the communicator, you must first provide power to the fire alarm control panel (in the drawings the G17F gets its power from the 24 V output of the panel). If the communicator works correctly, these indicators are lit:

- the **POWER** LED blinks green (the supply voltage is correct);
- the **NETWORK** LED is lit green, and blinks yellow when the communicator has connected to the network.

- Sufficient mobile network signal strength: 5 on a 2G network (five yellow blinks of the **NETWORK** LED), 3 on a 4G network (three yellow blinks).
- If you count fewer than 3 yellow blinks on the **NETWORK** LED, the signal strength is not sufficient: choose another installation place, or use a more sensitive antenna (section 1.7).
- If the indication is different from this, you will find the explanation in section 1.6.
- If none of the indicators of the G17F is lit, check the power supply and the wiring.

4. Remote control

The G17F can be controlled from the **Protegus 2** app, by **SMS command** and by **phone call** (with the phone's keypad during the call). In the app the users also see the state of the system and receive notifications about the system events; by SMS the administrator can also change part of the settings.

4.1 Adding the G17F to Protegus 2

In Protegus 2 the users see the state of the system and receive notifications about the system events. The app is available for phones and in the browser (the download links are below, at creating the system).

Before you add the system

You can add the G17F to Protegus 2 if:

1. there is an activated SIM card in it, and you have entered or switched off the PIN code;
2. the Protegus service is switched on (**Users & Reporting** → **Enable cloud service**, section 5.4; by SMS: `CONNECT 123456 PROTEGUS=ON`, section 4.2);
3. its power is switched on (the **POWER** LED blinks green);
4. it is connected to the network (the **NETWORK** LED is lit green and blinks yellow).

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

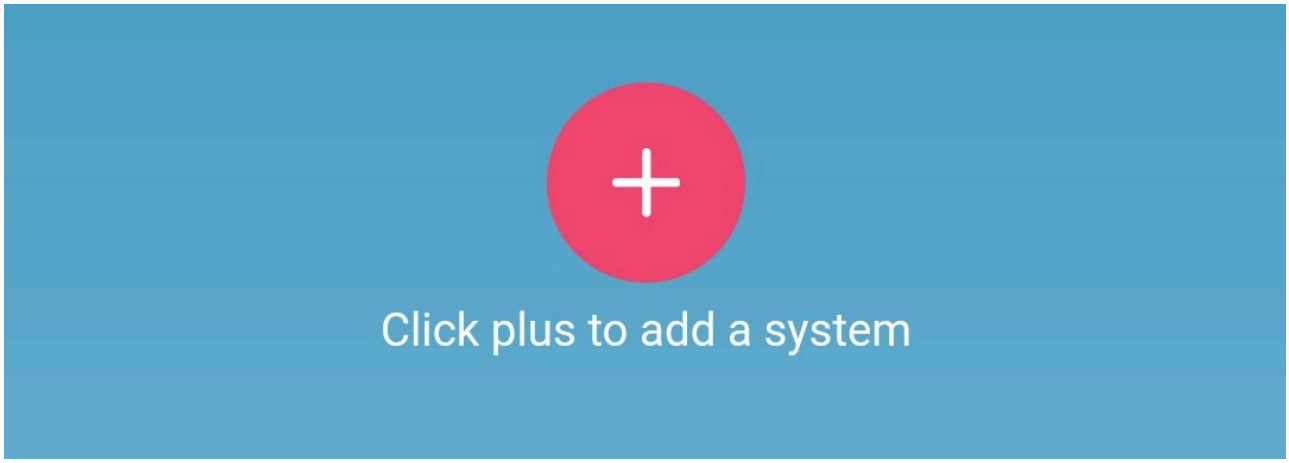








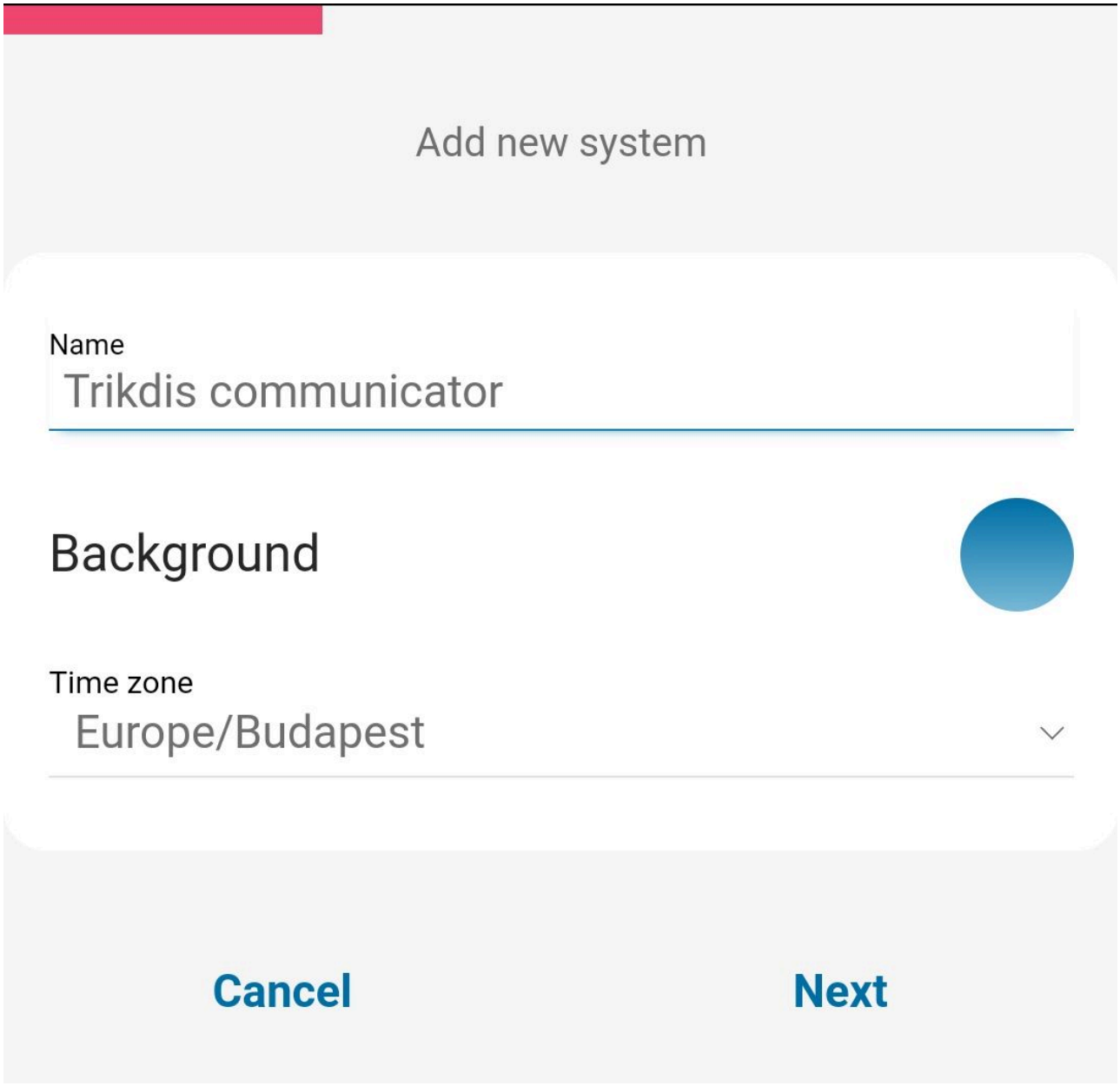
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



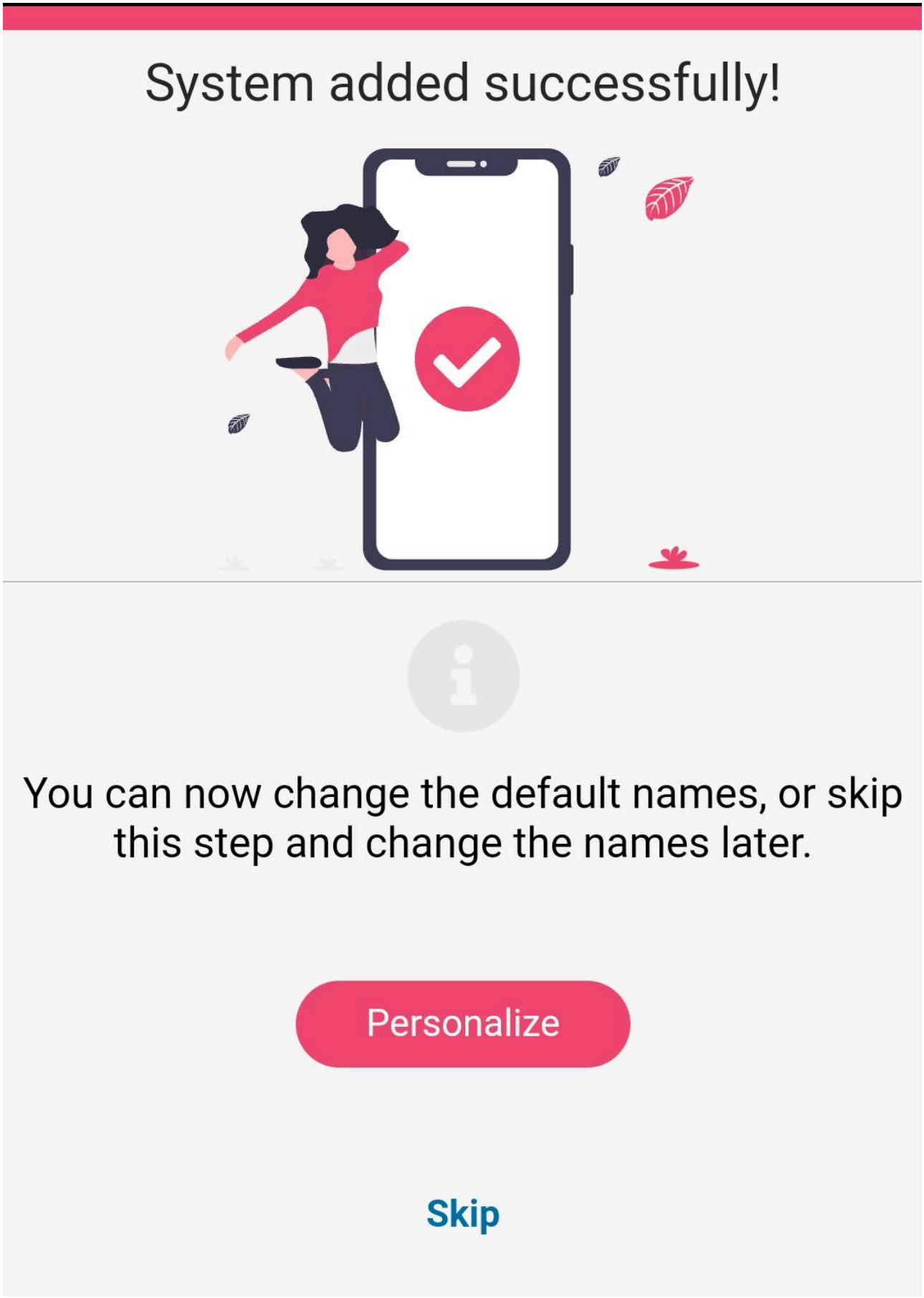
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



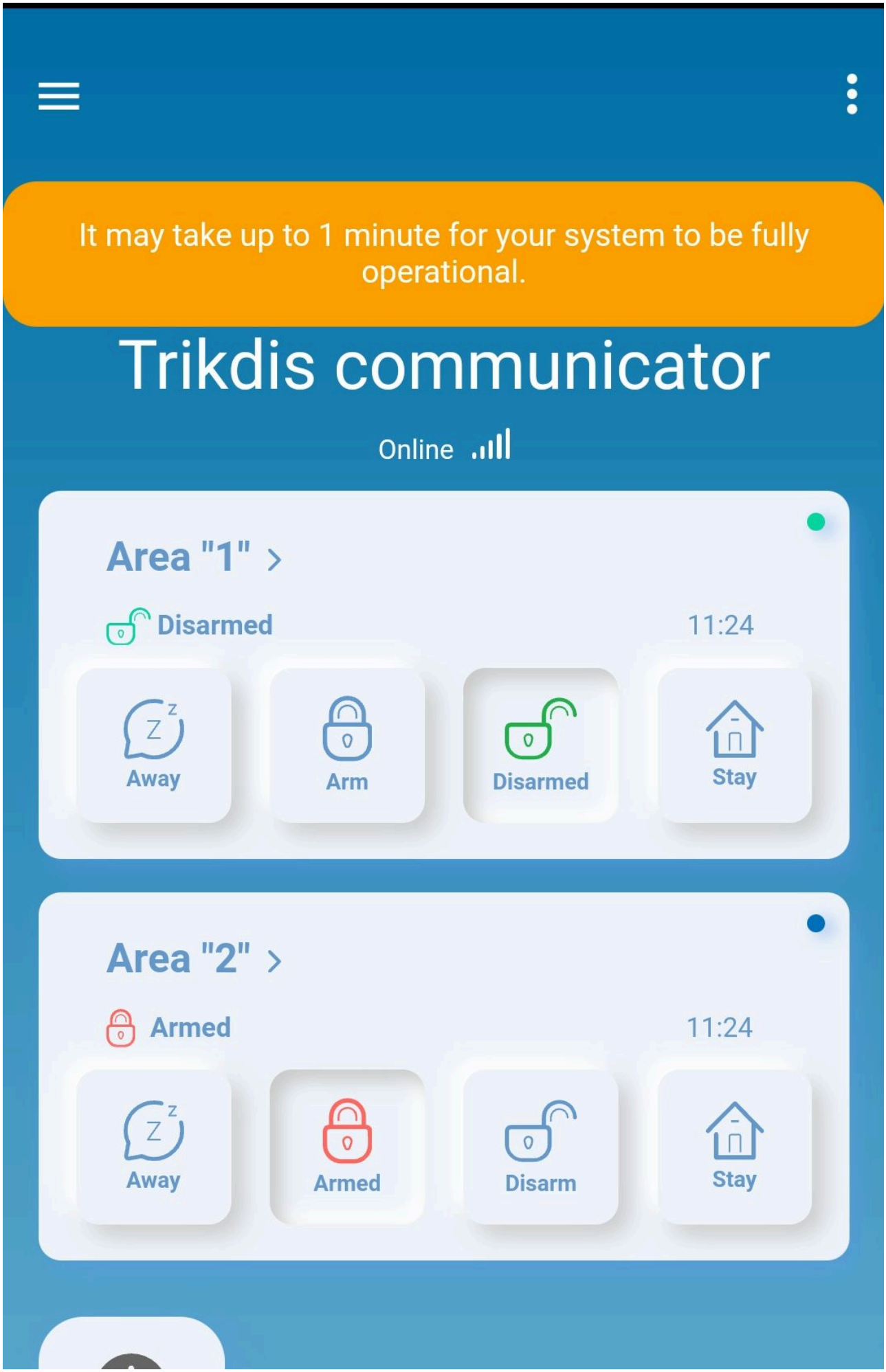
6. Add meg a rendszer nevét és válassz idozónát



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



For the G17F, pay attention to the following when adding it:

1. After entering the unique identifier (**Unique ID**), click the **Next** button. You find the identifier on the sticker on the device and on the box; with a USB connection you also see it in the TrikdisConfig status bar (**IMEI/Unique ID**, section 5.1).
2. If the installer has changed the default `123456` value of the **Cloud Access Code**, the app asks for the code when you add the system (section 2.1).

4.2 Setup and control by SMS message

1. Change the administrator password. For security, replace the default administrator SMS password. Send an SMS in this form:

```
PSW 123456 xxxxxx
```

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

2. Allow control for other users. By SMS and phone call, the system can only be controlled from the phone numbers on the user list. From the administrator's phone, send an SMS with the phone numbers and names of the other persons, so that they can also control the system:

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

Part	Meaning
`xxxxxx`	the 6-character administrator password
`x`	the number of the user on the list (if you enter 1, you hand over your administrator rights to the other user)
`PHONENR`	the phone number of the user
`NAME`	the name of the user

List of SMS commands

Command	Data	Description
`INFO`		Request for data about the communicator: the reply contains the type, IMEI number, serial number and firmware version of the communicator. 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`

Command	Data	Description
`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 few seconds: "x" is the number of the OUT output, "ttt" is a three-digit number, the pulse time in seconds. Example: `OUTPUT1 123456 PULSE=002`
`PSW`	new password	Changing the password. Example: `PSW 123456 654123`
`TIME`	`YYYY/MM/DD,12:00:00`	Setting the date and time. Example: `TIME 123456 2025/05/09,10:23:00`
`TXTA`	object name	Entering the name of the object. Example: `TXTA 123456 House`
`TXTE`	`Z1=` … `Z12=`	Entering the SMS text of the zone alarm; Z1…Z12 is the number of the input zone. Example: `TXTE 123456 Z1=ALARM in Zone1`
`TXTR`	`Z1=` … `Z12=`	Entering the SMS text of the zone restore; Z1…Z12 is the number of the input zone. Example: `TXTR 123456 Z1=Restore Zone1`
`RDR`	`PhoneNR#SMStext`	Forwarding an SMS to the given number; the phone number must start with "+" and the international country code. Example: `RDR 123456 +37061234567#forwarded text`
`ASKI`		SMS query about the state of the inputs (IN). Example: `ASKI 123456`
`ASKO`		SMS query about the state of the outputs (OUT). Example: `ASKO 123456`
`SETN`	`PhoneX=PhoneNR#Name`	Adding a phone number and user name to user "x" ("x" is the line of the phone number on the list). The phone number must start with "+" and the international country code; the phone number and the user name are separated by a # sign. Example: `SETN 123456 PHONE5=+37061234567#JOHN`
`SETN`	`PhoneX=DEL`	Deleting the phone number and name of the user from the system. Example: `SETN 123456 PHONE5=DEL`
`UUSD`	`*Uusd code#`	Sending a USSD code to the operator (the name of the command really is `UUSD`). 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. Example: `CONNECT 123456 CODE=123456`
`CONNECT`	`IP=0.0.0.0:8000`	The TCP IP address and port of the connection channel of the main server. Example: `CONNECT 123456 IP=0.0.0.0:8000`
`CONNECT`	`IP=0`	Switching off the main 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`

4.3 Controlling the PGM outputs by phone call

If no user has been added to the system yet, the first person who calls the G17F becomes the administrator of the system, and only they can control the G17F by call and SMS commands. If you want to allow control by call for further users too, add them in TrikdisConfig (section 5.4), or give them the right by SMS command (section 4.2).

If you want to control a PGM output remotely:

- The user must have the right to control the outputs (OUT) (section 5.4), and the **Remote control** type must be assigned to the output (OUT) in TrikdisConfig (**PGM** page, **Output definition**, section 5.7).
- Call the number of the SIM card of the G17F. The G17F answers the call, and you can key in commands with the phone's keypad according to the table.

Keys	Function	Description
`[output]*[state]#`	controlling the selected output (OUT)	It switches the given PGM output. State: **0** – output switched off; **1** – output switched on; **2** – switched off for the pulse time; **3** – switched on for the pulse time (the pulse time can be set in the **PGM** table of TrikdisConfig, section 5.7). The **#** marks the end of the command. Examples: switching on output 1: `1*1#`; switching off output 1: `1*0#`; switching on output 2 for the pulse time set in the **PGM** table: `2*3#`
`#`	restarting the command	If you made a mistake in the command, press the **#** key of the phone and key in the command again.

5. The pages of TrikdisConfig

This chapter describes the pages of the TrikdisConfig programming window, in the order in which they follow in the left-hand menu. Connecting the G17F with a USB cable: chapter 2; remotely: chapter 6.

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.

Label	Meaning
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.

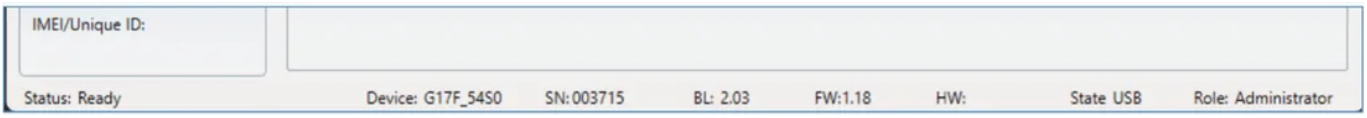


Figure 37. The status bar of the G17F: **Status: Ready**, **Device: G17F_54S0**, **BL** 2.03, **FW** 1.18, **State: USB**, **Role: Administrator**; on the left the **IMEI/Unique ID** and the serial number field. For the G17F, the **Device** field must show the **G17F** type.

When you click the **Read [F4]** button, the program reads out and shows the current settings stored on the G17F. Set the necessary parameters according to the following page descriptions.

5.2 "System Options" page

The general settings of the device on two tabs: **System general** and **Access**.

System general tab

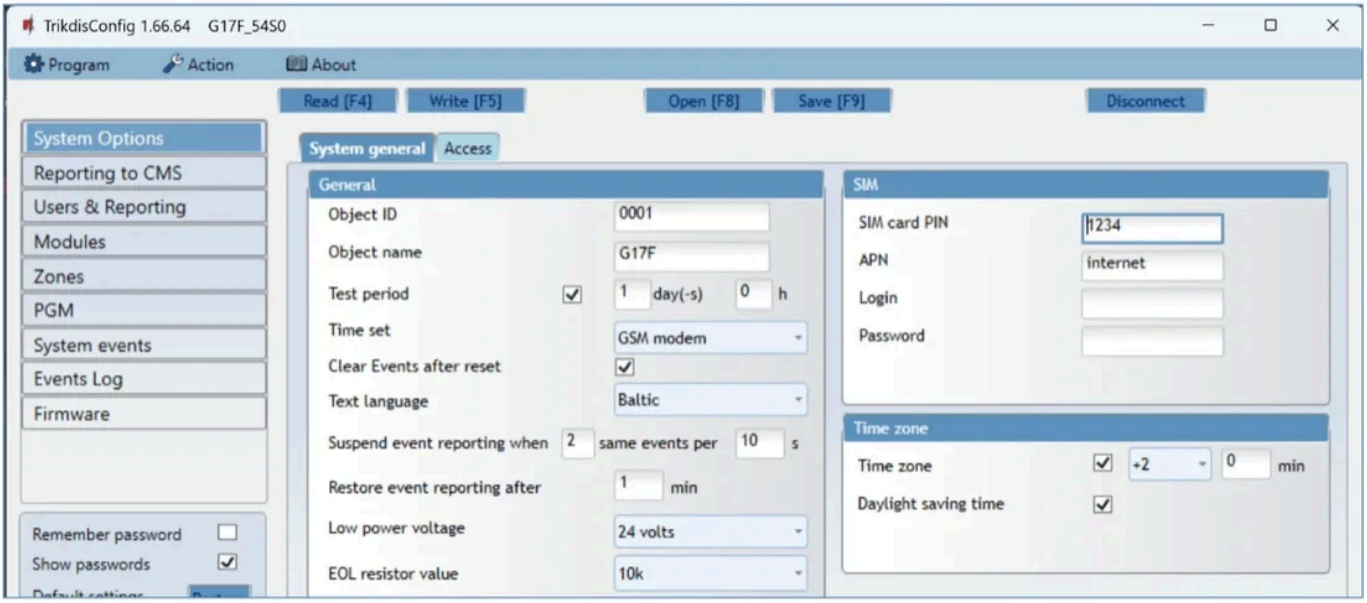


Figure 38. TrikdisConfig – **System Options**, **System general** tab: the **General**, **SIM** and **Time zone** groups. At the bottom of the **General** group the **EOL resistor value** field is also visible (10k in the picture).

General group

- **Object ID** – if the events go to the monitoring station, enter the object identifier you got from the monitoring station (4-character hexadecimal number, 0–9, A–F). Do not use the identifiers FFFE and FFFF.
- **Object name** – the name of the object; this name appears in the SMS messages sent to the users.
- **Test period** – when ticked, the G17F sends a "Test" message at the set interval.

- **Time set** – the source of time synchronization. **IP server**: the time follows the time of the IP receiver; **Cellular modem** (**GSM modem** in the picture): the time of the mobile operator's server.
- **Clear Events after reset** – when ticked, all unsent event messages are deleted at restart (reset).
- **Text language** – the language of the SMS messages: the device uses the special characters of the selected language in the SMS messages.
- **Suspend event reporting when … same events per … s** – suspending event reporting if the given number of identical events repeats within the given number of seconds.
- **Restore event reporting after … min** – after this time the suspension of event reporting ends (0–999 minutes).
- **Low power voltage** – enter the supply voltage (12 V or 24 V) the device operates from; the messages about low supply voltage follow this.

SIM group

- **SIM card PIN** – the PIN code of the SIM card.
- **APN** – the name of the mobile internet access point of the mobile operator. You must enter it if the event messages go over a mobile data connection to the Protegus 2 app or to the monitoring station. Data of the European operators: APN settings – list of European mobile operators.
- **Login**, **Password** – the user name and password of the APN, if the mobile operator requires them.

Time zone group

- **Time zone** – the time zone of the country (for example Central European Time: +1).
- **Daylight saving time** – when ticked, the internal clock of the device automatically switches between summer and winter time.

Access tab

On the **Access** tab you set the access codes and the permissions of the installer.

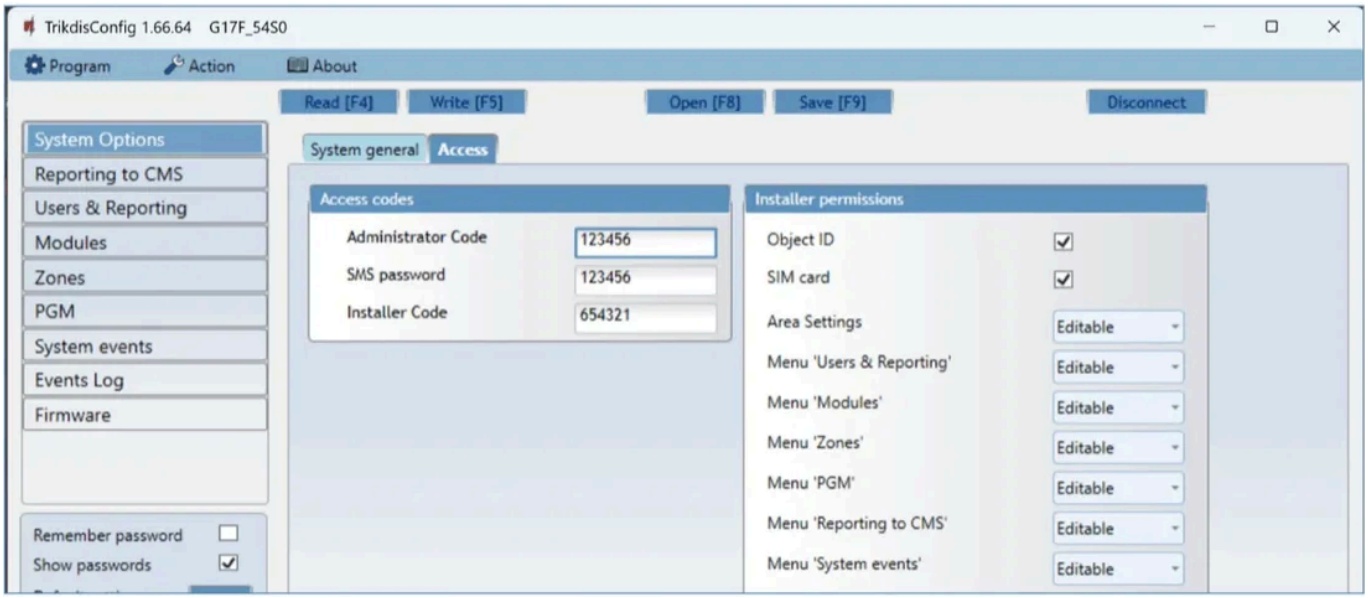


Figure 39. TrikdisConfig – **System Options**, **Access** tab: the **Access codes** group with the default codes, and the **Installer permissions** group, in which the administrator selects the settings the installer may change.

Access codes group

- **Administrator Code** – full access to the settings (default `123456`).
- **SMS password** – password for remote control and programming by SMS (default `123456`).

- **Installer Code** – limited access for changing the settings (default `654321`).

Installer permissions group – here the administrator sets which parameters the installer may change.

For security, change the default codes. You can also change the SMS password by SMS (`PSW`, section 4.2).

5.3 "Reporting to CMS" page

The G17F sends the messages to the monitoring station over mobile internet (IP) or by SMS. A backup channel can be assigned to the primary channel: the device uses it if the connection is lost on the primary channel.

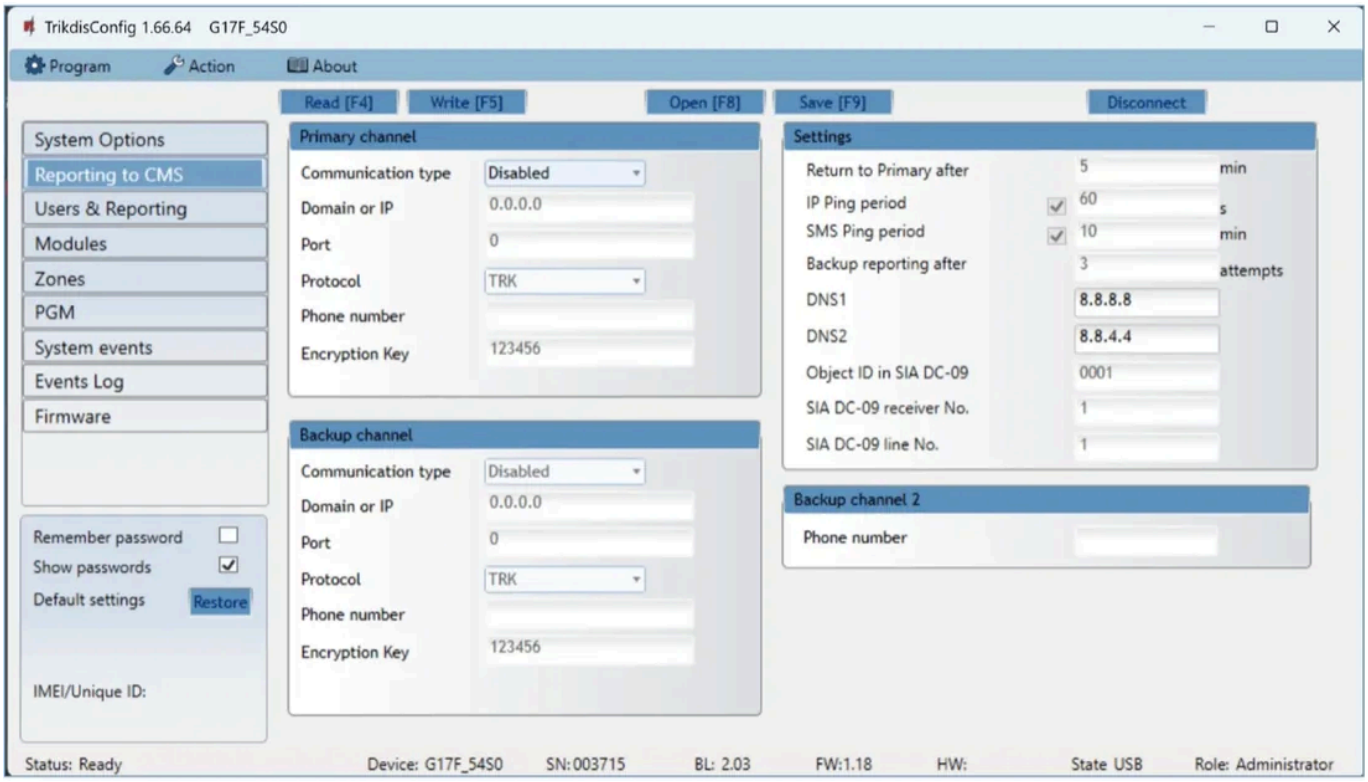


Figure 40. TrikdisConfig – **Reporting to CMS**: the **Primary channel**, **Backup channel**, **Settings** and **Backup channel 2** groups. In the picture: **Communication type: Disabled**, **Return to Primary after** 5 minutes, **IP Ping period** 60 s, **SMS Ping period** 10 minutes, **Backup reporting after** 3 attempts, **DNS1** 8.8.8.8, **DNS2** 8.8.4.4.

The messages sent to the monitoring station are encoded and password-protected. To receive the messages and forward them to the monitoring software, a Trikdis receiver is needed:

- for IP messages: the **IPcom** receiver software (Windows or Linux), the **RL14** IP/SMS hardware receiver or the **RM14** multi-channel receiver;
- for SMS messages: the **RL14** IP/SMS hardware receiver, the **RM14** multi-channel receiver or the **GM14** SMS receiver.

Trikdis IPcom v5 Windows software receiver | **Trikdis IPcom v5 Linux software receiver**

The SMS connection is extremely useful as a backup channel, because it works even if the internet connection drops in the network of the mobile operator. We do not recommend SMS as the primary channel.

Primary channel group

- **Communication type** – the mode of connection with the receiver of the monitoring station.
- **Domain or IP** – the domain name or IP address of the receiver.

- **Port** – the network port of the receiver.
- **Protocol** – the Trikdis IP receivers receive messages sent with the **TRK** protocol; for IP receivers able to receive SIA DC-09 messages, select the **DC-09_2007** or the **DC-09_2012** protocol.
- **Phone number** – (only for SMS) the phone number of the Trikdis SMS receiver, starting with the country code (for example CCxxxxxxxxx, where CC is the country code).
- **Encryption Key** – 6-digit encryption key; it must match the encryption key of the receiver.

Backup channel group – switch it on so that the G17F sends the messages on the backup channel when the connection is lost. Its settings are the same as those of the primary channel.

Settings group

- **Return to Primary after** – after this time the G17F tries to return to the primary channel.
- **IP Ping period** – the sending interval of the internal PING signals that check the connection. The PING signals only go over the IP channel; the receiver does not forward them to the monitoring software, so they do not load it. The software is only notified if the receiver gets no PING from the device for the set time.
- **SMS Ping period** – the interval of the PING signal sent on the SMS channel, in minutes. To use the channel, tick the checkbox and enter the interval.
- **Backup reporting after** – after how many unsuccessful sending attempts the G17F sends on the backup channel (**Backup channel**).
- **DNS1**, **DNS2** – the DNS servers that translate the domain name into an IP address. They are needed if you entered a domain name (and not an IP address) in the **Domain or IP** field of the channel. By default, the DNS servers of Google.

The PING interval

By default, the receiver sends a "Connection lost" message to the monitoring software if it gets no PING within three times the PING sending interval of the device: with a 3-minute **IP Ping period**, for example, after 9 minutes. The PING messages also keep the connection between the device and the receiver active – the active connection is needed for remote setup and control. We recommend setting the PING interval to at most 5 minutes.

The fields below are only visible if you selected the **DC-09_2007** or **DC-09_2012** protocol in the **Protocol** field of the channel:

- **Object ID in SIA DC-09** – the object number; with the DC-09 protocol this number goes into the messages. Enter the 3–16-character hexadecimal number you got from the monitoring station.
- **SIA DC-09 receiver No.** – the number of the receiver.
- **SIA DC-09 line No.** – the number of the line in the receiver.

Backup channel 2 group

- **Phone number** – (only for SMS) the phone number of the Trikdis SMS receiver, starting with the country code (for example CCxxxxxxxxx, where CC is the country code).

5.4 "Users & Reporting" page

The settings of the users, the Protegus cloud and the SMS replies, on three tabs: **Users**, **SMS answer texts** and **SMS for Panel events**.

Users tab

On the **Users** tab you enter the users who receive SMS messages and calls, and here you switch on the Protegus cloud.

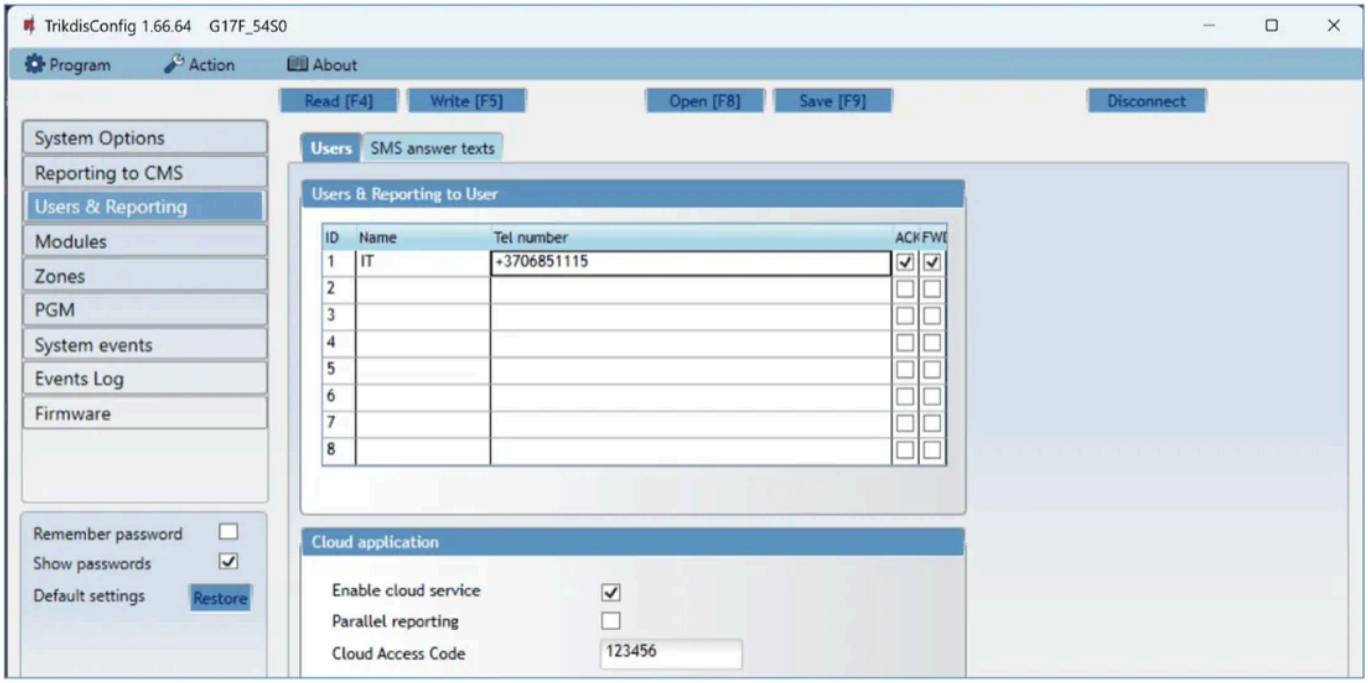


Figure 41. TrikdisConfig – **Users & Reporting**, **Users** tab: the **Users & Reporting to User** table (**ID**, **Name**, **Tel number**, **ACK**, **FWD**) and the **Cloud application** group (**Enable cloud service**, **Parallel reporting**, **Cloud Access Code**).

Users & Reporting to User group

- **ID** – the number of the user on the list.
- **Name** – the name of the user; this name appears in the event SMS messages.
- **Tel number** – the phone number of the user, to which the SMS messages go; enter it in international format (+CC..., where CC is the country code).
- **PGM** – when ticked, the user can control the outputs remotely (this column is not visible in the picture above).
- **ACK** – when ticked, the G17F sends a reply SMS to the user after every SMS command received (the text of the replies: **SMS answer texts** tab).
- **FWD** – when ticked, the G17F forwards to the user the SMS messages coming from numbers outside the system (for example the balance notification of the SIM card or advertising messages).

Cloud application group

- **Enable cloud service** – switching on the Protegus service: this way the G17F exchanges data with the Protegus 2 app, and it can also be set up remotely with TrikdisConfig (chapter 6).
- **Parallel reporting** – parallel sending: the messages go on the primary channel and to Protegus 2 at the same time.
- **Cloud Access Code** – 6-digit code for logging in to Protegus 2 (default `123456`).

SMS answer texts tab

In the **SMS text** column you can edit the text of the replies sent to the SMS commands.

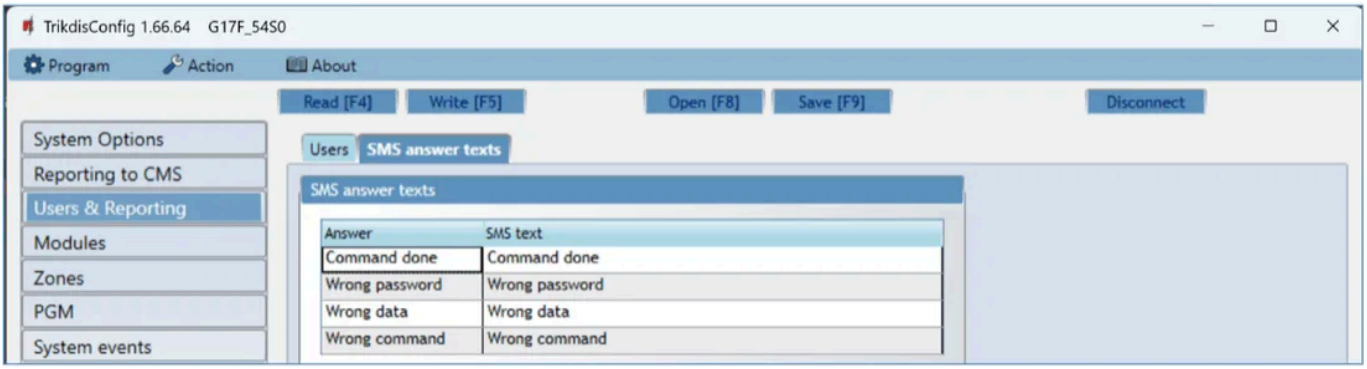


Figure 42. TrikdisConfig – **Users & Reporting**, **SMS answer texts** tab: **Command done** (command executed), **Wrong password**, **Wrong data**, **Wrong command**.

SMS for Panel events tab

This tab only appears if you have entered at least one user phone number on the **Users** tab. Here you set whether the users receive an SMS and/or a call about the events of the fire alarm control panel.

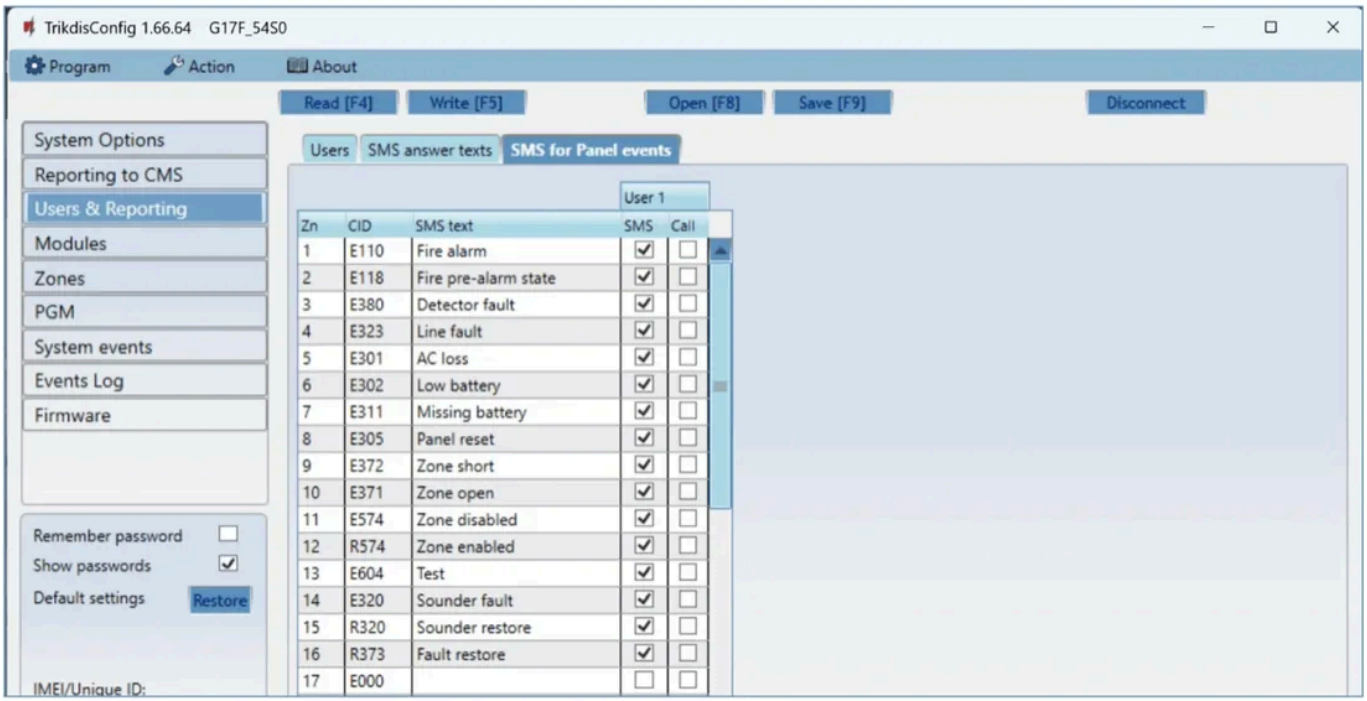


Figure 43. TrikdisConfig – **Users & Reporting**, **SMS for Panel events** tab: the events of the panel with Contact ID codes, for example E110 fire alarm (**Fire alarm**), E118 pre-alarm (**Fire pre-alarm state**), E380 detector fault (**Detector fault**), E301 mains power loss (**AC loss**), E302 low battery voltage (**Low battery**); in the **User 1** column the **SMS** and **Call** checkboxes.

- **Zn** – the number of the event on the list.
- **CID** – the Contact ID code of the event.
- **SMS text** – the SMS text of the event.
- **User SMS/Call** – for each event you can select whether the user receives an SMS and/or a 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.

5.5 "Modules" page

The list of the modules and fire alarm control panels connected to the RS485 bus, and the settings of the W485 and E485 modules.

RS485 modules tab

In the list you enter one module or fire alarm control panel per line (up to 8).

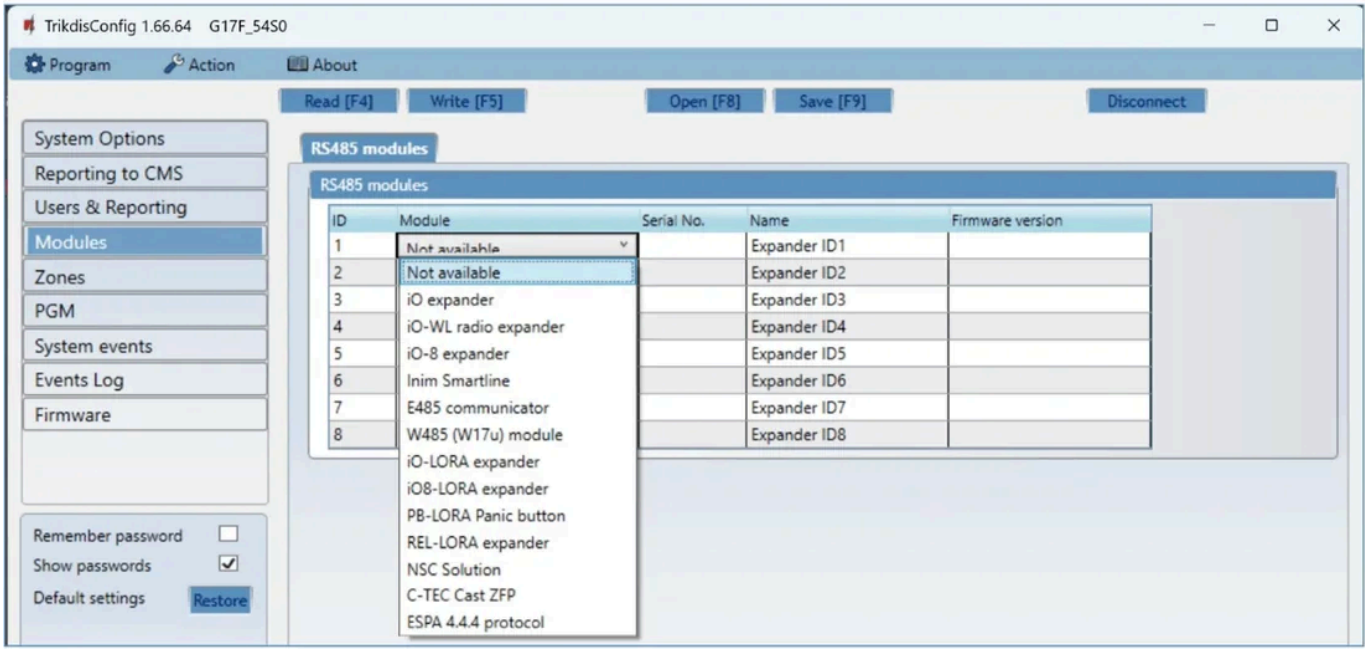


Figure 44. TrikdisConfig – **Modules**, **RS485 modules** tab: eight lines (ID 1–8); in the first line the **Module** list is opened with the selectable modules and fire alarm control panels.

- **ID** – the number of the module on the list.
- **Module** – the module or panel used: iO, iO-WL, iO-8, INIM Smartline, E485, W485, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, NSC Solution, C-TEC Cast ZFP, ESPA 4.4.4.
- **Serial No.** – mandatory, 6-digit number; you find it on the case and on the packaging of the module.
- **Name** – the name of the module (any name).
- **Firmware version** – the firmware version of the module; it appears when the G17F finds the connected module.

W485 settings tab

The settings of the W485 (W17u) Wi-Fi module (wiring: section 3.11).

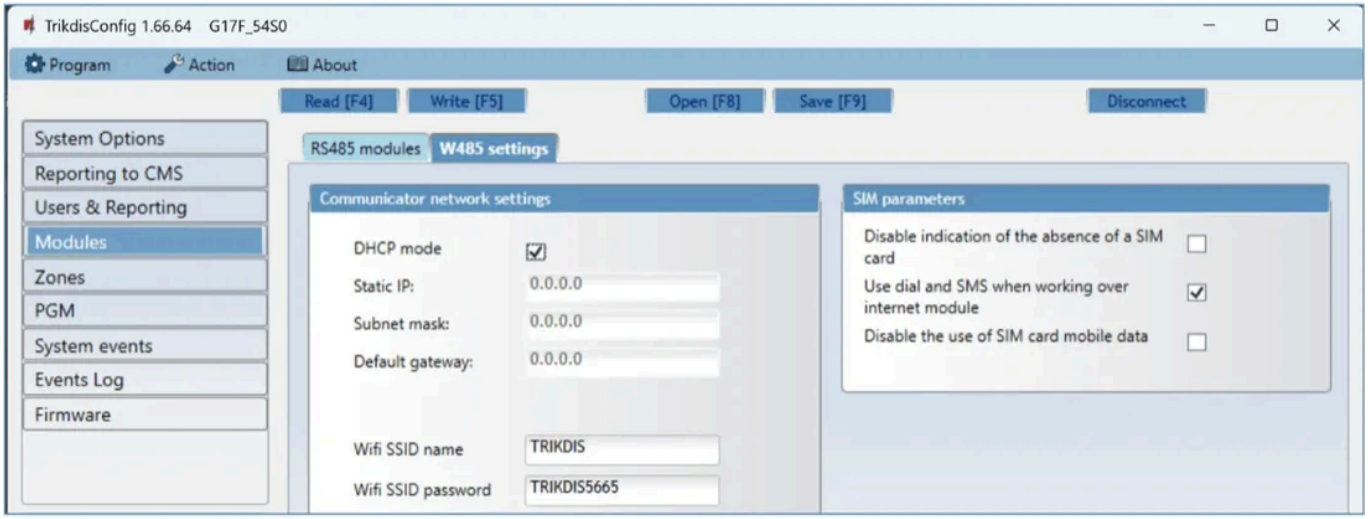


Figure 45. TrikdisConfig – **Modules**, **W485 settings** tab: the **Communicator network settings** group (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**, **Wifi SSID name**, **Wifi SSID password**) and the **SIM parameters** group.

Communicator network settings group

- **DHCP mode** – the mode of network registration of the Wi-Fi module (manual or automatic). When ticked (automatic mode), the module automatically recognizes the network settings (subnet mask, gateway) and gets an IP address.
- **Static IP** – static IP address in manual mode.
- **Subnet mask** – subnet mask in manual mode.
- **Default gateway** – default gateway in manual mode.
- **Wifi SSID name** – the name of the Wi-Fi network to which the W485 (W17u) 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 G17F does not indicate if there is no SIM card in it.
- **Use dial and SMS when working over internet module** – when ticked, the G17F can also be controlled by call and SMS. If it is not ticked and there is a Wi-Fi network, calls and SMS are not used; if it is not ticked and there is no Wi-Fi network, the G17F handles the calls and SMS messages, and sends an SMS to the user.
- **Disable the use of SIM card mobile data** – when ticked, the G17F does not use the mobile data connection of the SIM card: the data only go through the W485 module. If the Wi-Fi network is lost, the G17F stores the data in its memory, and after the Wi-Fi returns it sends them through the W485 module.

E485 settings tab

The settings of the E485 Ethernet module (wiring: section 3.12).

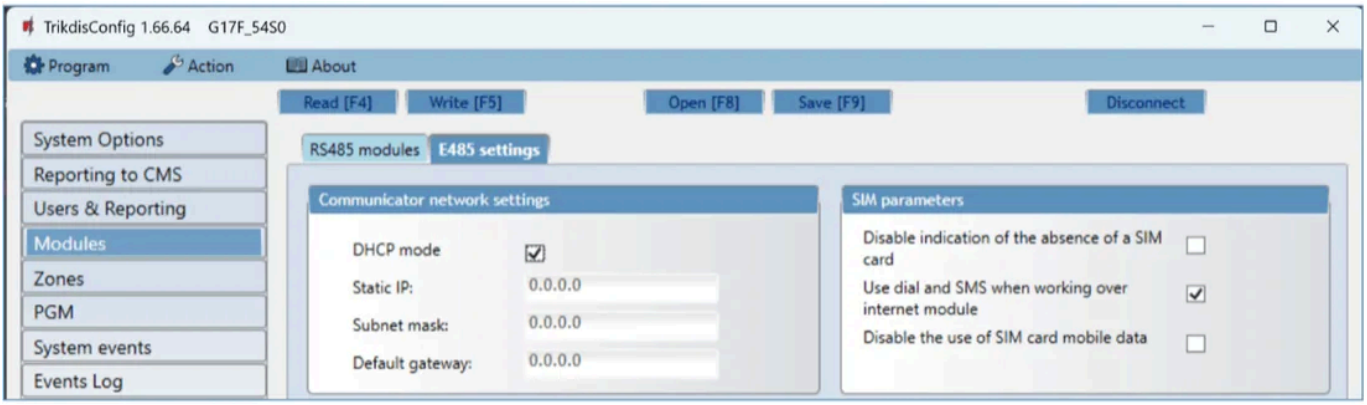


Figure 46. TrikdisConfig – **Modules**, **E485 settings** tab: the **Communicator network settings** group (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**) and the **SIM parameters** group.

Communicator network settings group

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

SIM parameters group

- **Disable indication of the absence of a SIM card** – when ticked, the G17F does not indicate if there is no SIM card in it.
- **Use dial and SMS when working over internet module** – when ticked, the G17F can also be controlled by call and SMS. If it is not ticked and there is internet, SMS and calls are not used; if it is not ticked and there is no internet, the G17F handles the calls and SMS messages, and sends an SMS to the user.
- **Disable the use of SIM card mobile data** – when ticked, the G17F does not use the mobile data connection of the SIM card: the data only go through the E485 module. If the internet is lost, the G17F stores the data in its memory, and after the internet returns it sends them through the E485 module.

5.6 "Zones" page

The settings of the zones (inputs) on two tabs: **Zones settings** and **SMS & Call reporting**.

Zones settings tab

In the table you set up one zone per line.

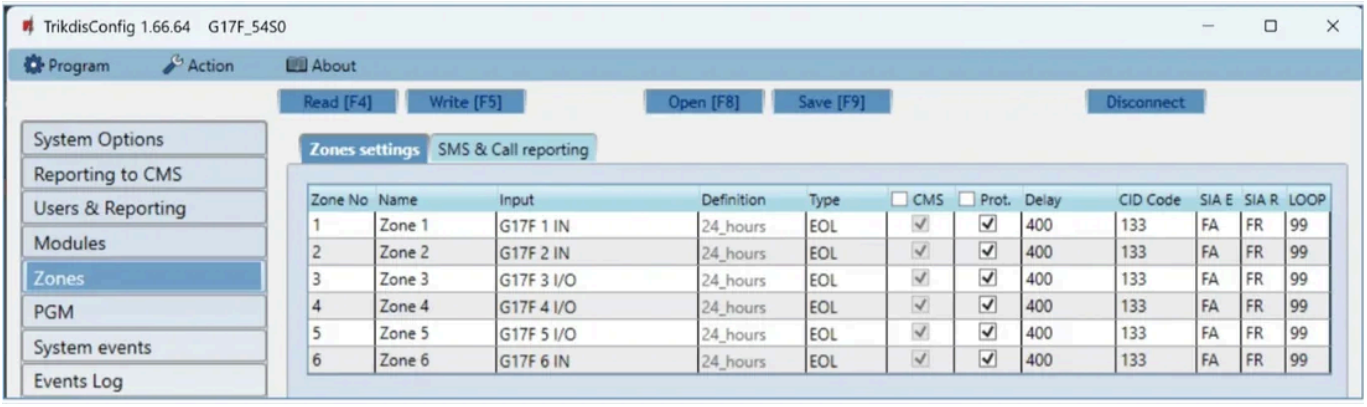


Figure 47. TrikdisConfig – **Zones**, **Zones settings** tab: in the picture six zones on the six inputs of the G17F (**1 IN**, **2 IN**, **3 I/O**, **4 I/O**, **5 I/O**, **6 IN**), each with the **24_hours** definition, **EOL** type, ticked **CMS** and **Prot.** checkboxes, 400 ms delay and CID code 133.

- **Zone No** – the number of the zone on the list.
- **Name** – the name of the zone; this name appears in the SMS messages.
- **Input** – which input (IN) of the G17F or of the expansion module belongs to the zone.
- **Definition** – every zone has the **24 hours** definition: if the zone is triggered, the event message is sent immediately.
- **Type** – the type of the circuit connected to the input: **NC** – normally closed contact; **NO** – normally open contact; **EOL** – circuit terminated with an end-of-line resistor (4.7 kΩ or 10 kΩ) (section 3.7).
- **CMS** – when ticked, the events of the zone go to the monitoring station.
- **Prot.** – when ticked, notifications about the events of the zone go to the Protegus 2 app.
- **Delay** – the reaction time of the input (IN) in milliseconds.
- **CID Code** – the Contact ID code of the event.
- **SIA E** – the SIA event code.
- **SIA R** – the SIA restore code.
- **LOOP** – the number of the loop; it appears in the SMS message.

SMS & Call reporting tab

This tab only appears if you have entered at least one user phone number on the **Users & Reporting** page.

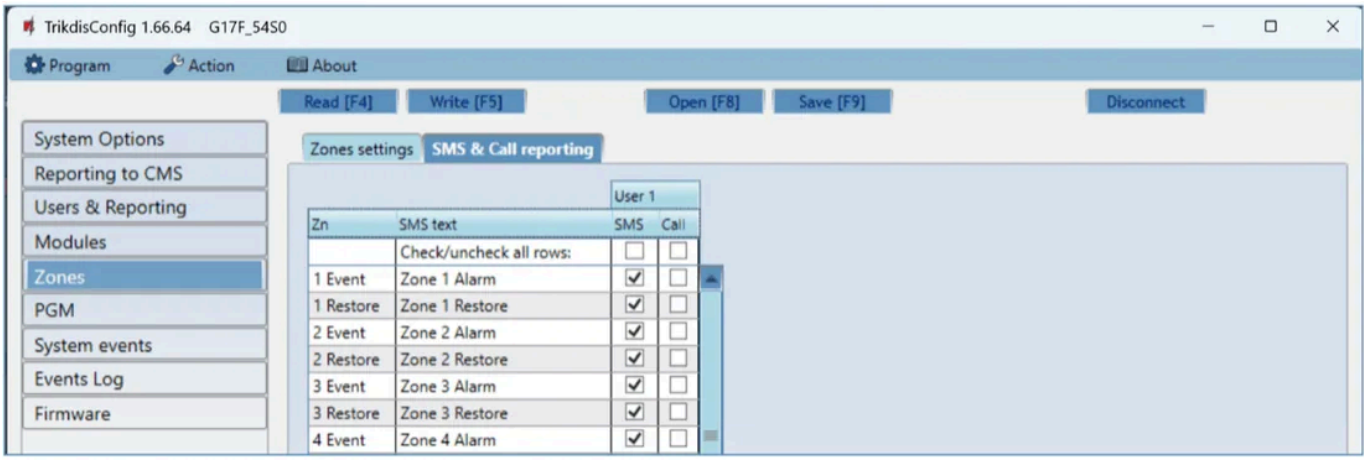


Figure 48. TrikdisConfig – **Zones**, **SMS & Call reporting** tab: one **Event** and one **Restore** line per zone (for example Zone 1 Alarm, Zone 1 Restore); in the **User 1** column the **SMS** and **Call** checkboxes.

- **Zn** – the number of the zone with the keyword of the event: **Event** or **Restore**.
- **SMS text** – the description of the zone event; this goes into the event SMS sent to the users.
- **User SMS/Call** – for each zone event you can select whether the user receives an SMS and/or a call.

5.7 "PGM" page

The settings of the PGM outputs on two tabs: **Outputs** and **SMS & Call reporting**.

Outputs tab

In the table you set up one PGM output per line.

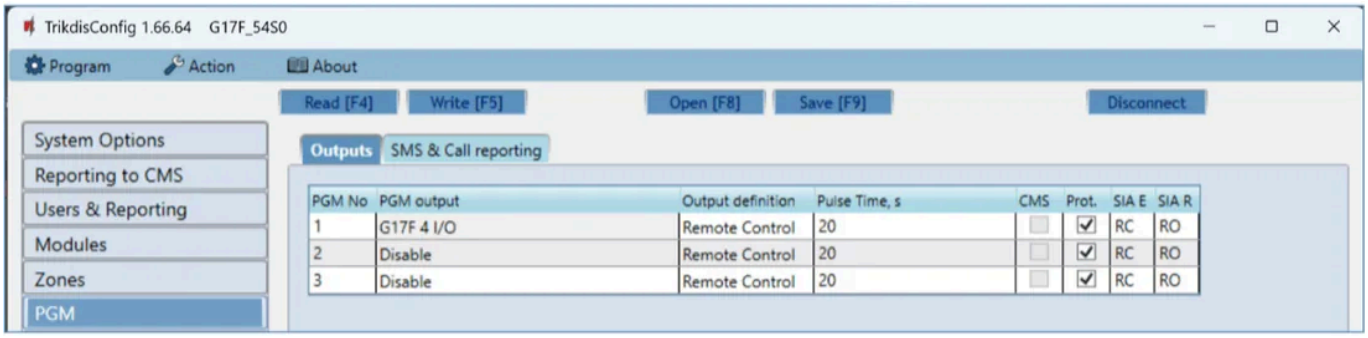


Figure 49. TrikdisConfig – **PGM**, **Outputs** tab: in the picture PGM 1 is on the **4 I/O** terminal of the G17F, PGM 2 and 3 are switched off (**Disable**); in all three lines **Remote Control** output definition, 20 s pulse time and ticked **Prot.** checkbox.

- **PGM No** – the number of the PGM output on the list.
- **PGM output** – the output (OUT) assigned to the PGM: of the G17F or of an external device.
- **Output definition** – the operating mode of the output (OUT).
- **Pulse time, s** – the duration for which the output (OUT) is switched on, 0–9999 seconds.
- **CMS** – when ticked, the selected events go to the monitoring station.
- **Prot.** – when ticked, notifications about the events of the output go to the Protegus 2 app.
- **SIA E** – the SIA event code.
- **SIA R** – the SIA restore code.

SMS & Call reporting tab

This tab only appears if you have entered at least one user phone number on the **Users & Reporting** page.

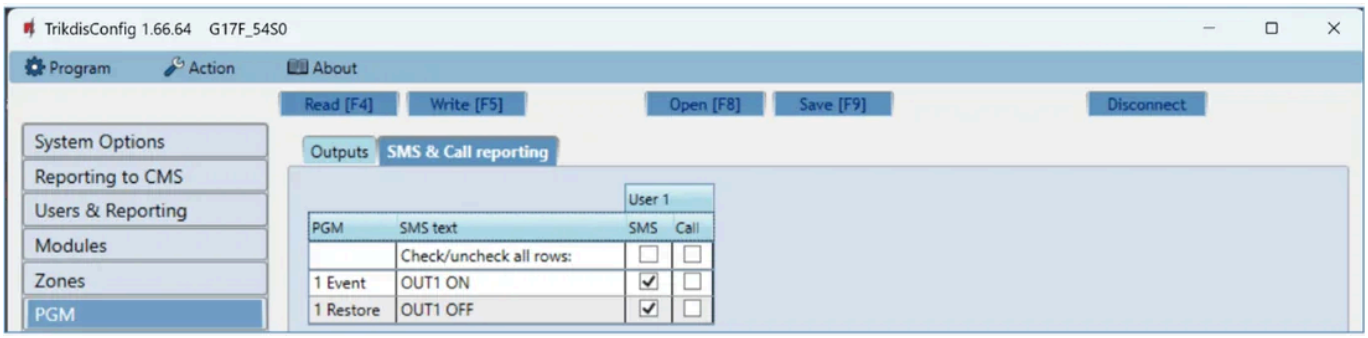


Figure 50. TrikdisConfig – **PGM**, **SMS & Call reporting** tab: SMS text **OUT1 ON** in the **Event** line of PGM 1, **OUT1 OFF** in its **Restore** line; in the **User 1** column **SMS** is ticked.

- **PGM** – the number of the output (OUT) and the type of the event: **Event** – switching on the output; **Restore** – switching off the output.
- **SMS text** – the name of the switch-on or switch-off event of the output; this goes into the event SMS.
- **User SMS/Call** – you can select which users receive an SMS and/or a call when the output (OUT) is switched on and off.

5.8 "System events" page

The settings of the communicator's own (system) events on two tabs: **Events** and **SMS & Call reporting**.

Events tab

In the table you set up one system event per line.

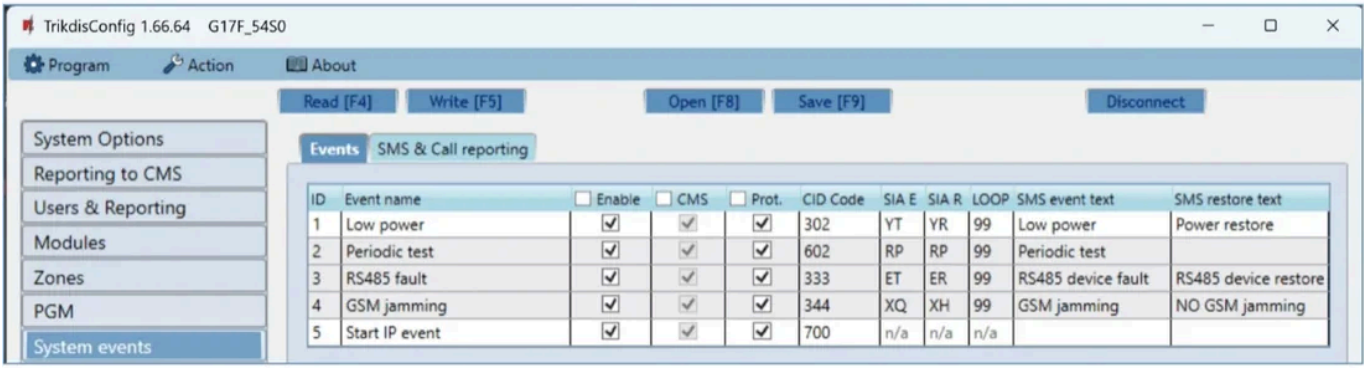


Figure 51. TrikdisConfig – **System events**, **Events** tab: low supply voltage (**Low power**, CID 302), periodic test (**Periodic test**, 602), RS485 fault (**RS485 fault**, 333), mobile network jamming (**GSM jamming**, 344) and **Start IP event** (700).

- **ID** – the number of the event on the list.
- **Event name** – the name of the event.
- **Enable** – switching on the monitoring of the event.
- **CMS** – the selected events go to the monitoring station.
- **Prot.** – notifications about the selected events go to the Protegus 2 app.
- **CID Code** – the Contact ID code of the event.
- **SIA E** – the SIA event code.
- **SIA R** – the SIA restore code.
- **LOOP** – the number of the loop; it appears in the SMS message.
- **SMS event text** – the SMS text of the event.
- **SMS restore text** – the SMS text of the restore.

SMS & Call reporting tab

This tab only appears if you have entered at least one user phone number on the **Users & Reporting** page.

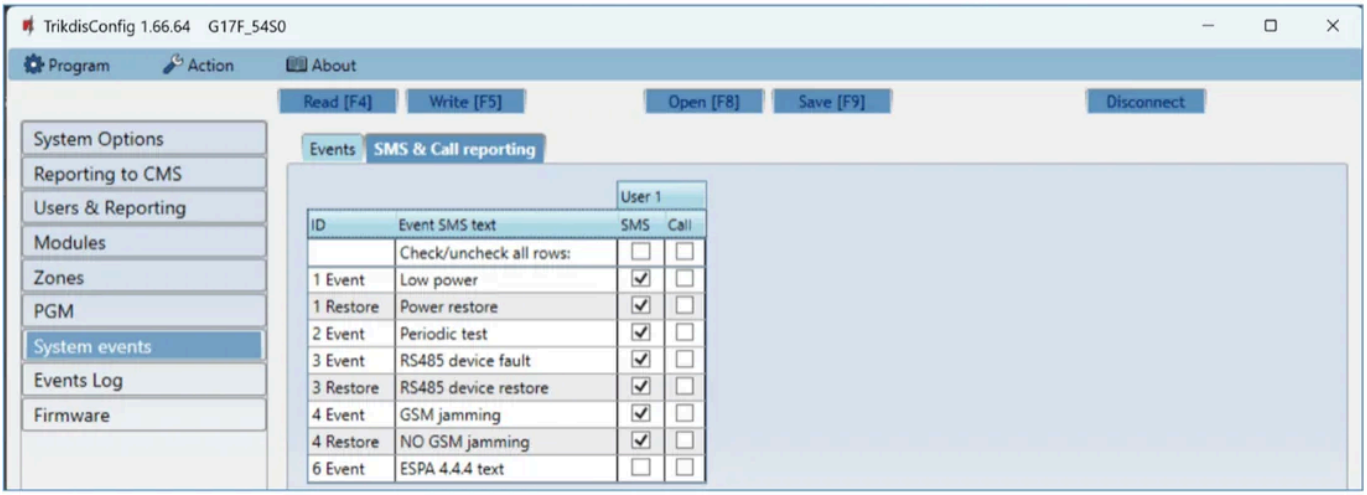


Figure 52. TrikdisConfig – **System events**, **SMS & Call reporting** tab: the **Event** and **Restore** lines of the system events (for example Low power, Power restore, Periodic test, GSM jamming); in the **User 1** column the **SMS** and **Call** checkboxes.

- **ID** – the number and keyword of the event (**Event**, **Restore**).
- **Event SMS text** – the text of the event that goes into the SMS message.
- **User SMS/Call** – for each event you can select whether the user receives an SMS and/or a call.

5.9 "Events Log" page

Here you can read out and delete the event log of the device.

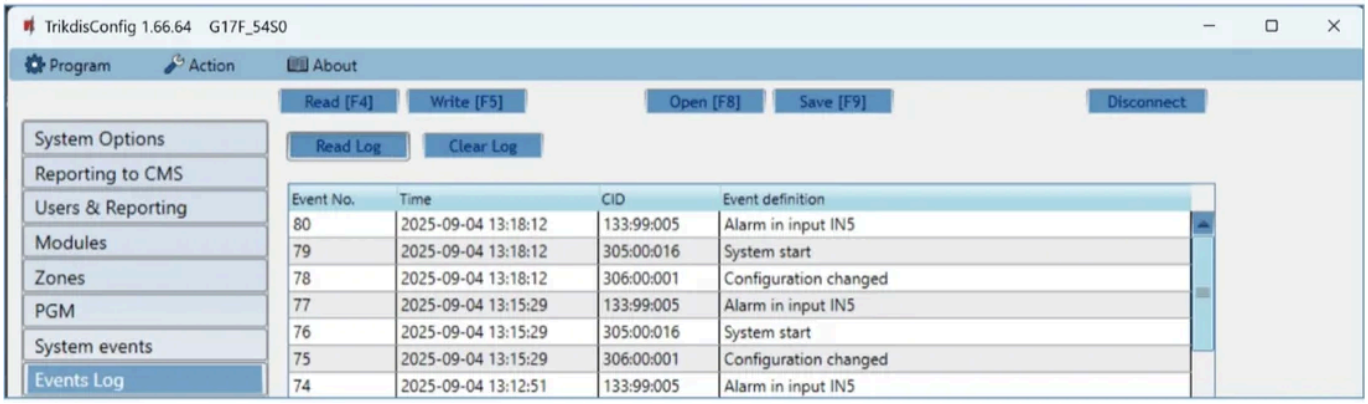


Figure 53. TrikdisConfig – **Events Log**: the **Read Log** and **Clear Log** buttons; in the table the number, time, CID code and description of the event – in the picture, for example, an alarm on input IN5 (**Alarm in input IN5**), system start (**System start**) and configuration change (**Configuration changed**).

- **Read Log** – the button reads out the event log from the memory of the device.
- **Clear Log** – the button deletes the log entries from the memory of the device.
- The table shows the number (**Event No.**), time (**Time**), **CID** code and description (**Event definition**) of the event. The log shows up to 1000 events stored in the memory of the G17F.

5.10 Restoring the factory settings

To restore the factory settings of the G17F, click the **Restore** button of TrikdisConfig (in the lower left part of the programming window, in the **Default settings** line).



Figure 54. TrikdisConfig – the **Restore** button of the **Default settings** line; below it the **IMEI/Unique ID** field and the status bar.

If you may need the current settings later, save them to a file with the **Save [F9]** button before restoring (section 5.1).

6. Remote programming

You can also read out and change the settings of the G17F remotely through the Protegus cloud with TrikdisConfig – you do not need to go to the site.

Conditions for remote programming

Remote setup only works if, in the G17F:

1. there is an activated SIM card, and you have entered or switched off the PIN code;
2. the Protegus service is switched on (**Users & Reporting** → **Enable cloud service**, section 5.4);
3. its power is switched on (the **POWER** LED blinks green);
4. it 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.

1. Start TrikdisConfig on the computer.
2. In the **Remote access** section, enter the unique identifier of the G17F (**Unique ID**) in the **Unique ID** field. You find this number on the back of the device and on its packaging.

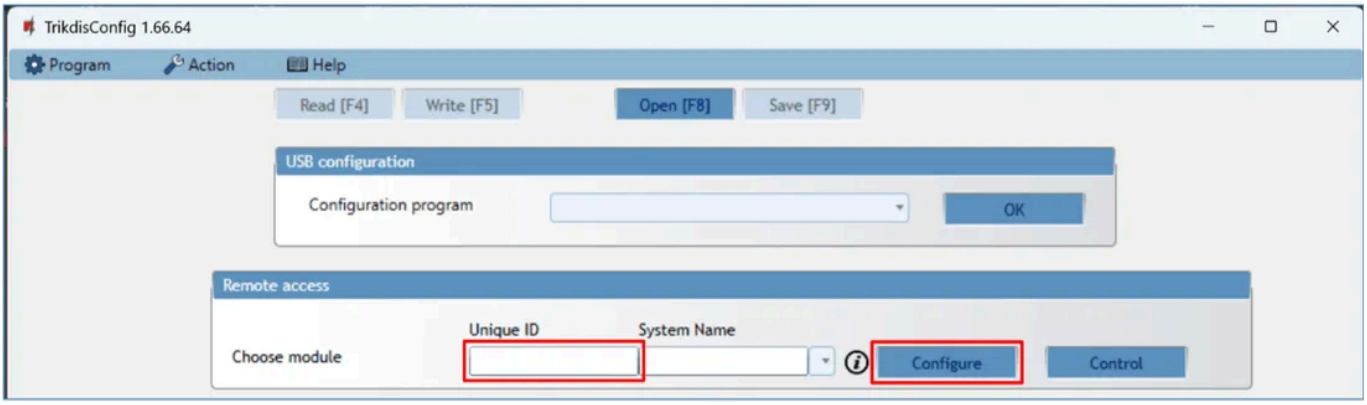


Figure 55. TrikdisConfig – the **Remote access** section of the start window: the **Unique ID** field, next to it the **System Name** field, and the **Configure** button.

3. (Optional) In the **System Name** field, enter a name for the device (for example the name of the object).
4. Click the **Configure** button.
5. In the window that opens, click the **Read [F4]** button. If the program asks for it, enter the administrator or the installer code.
6. At the end of the settings, click the **Write [F5]** button. When you have finished with TrikdisConfig, click the **Disconnect** button.

7. Checking the operation

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

1. To check an input, activate (trigger) the input. Check whether the event has arrived at the monitoring station and/or in the Protegus 2 app.
2. To check the outputs, switch them on remotely and check their operation. Make sure that the events have arrived at the monitoring station and/or in the Protegus 2 app.
3. Carry out a fire alarm test, and 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 communicator and the state of the inputs and outputs by SMS: `INFO 123456`, `ASKI 123456`, `ASKO 123456` (replace `123456` with your own SMS password; section 4.2).

8. Firmware update

If you connect the G17F to TrikdisConfig and newer firmware is available, the program offers the update by itself – for this the computer must be connected to the internet. Antivirus software, a firewall or strict internet access settings can block the automatic update.

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.

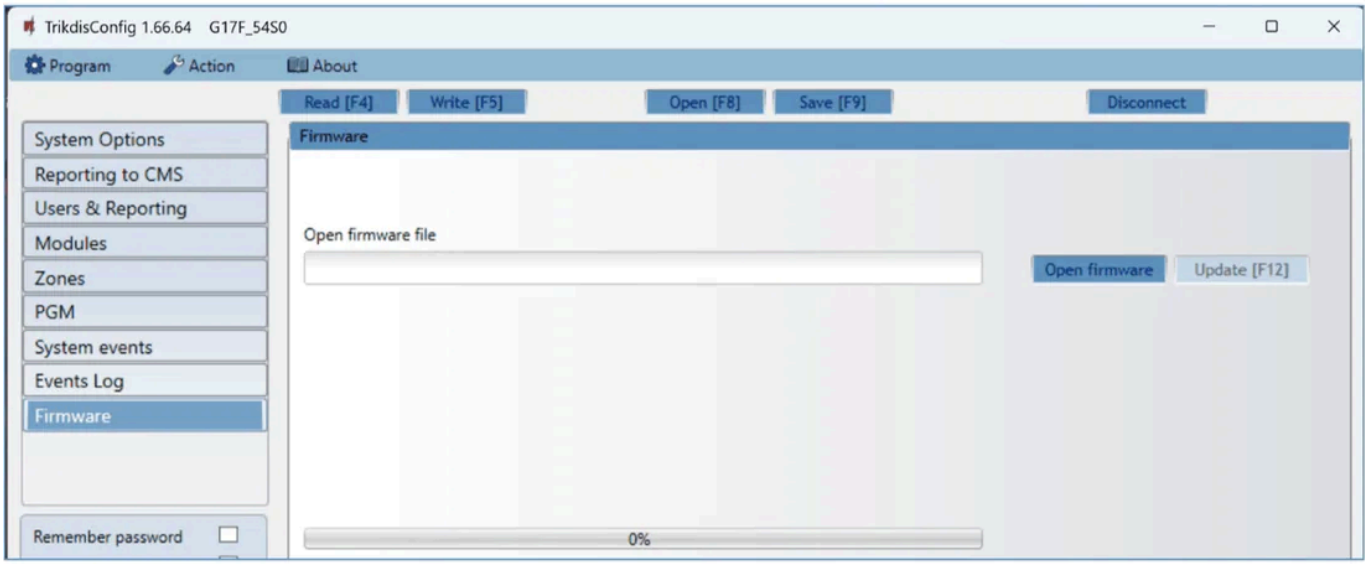


Figure 56. TrikdisConfig – G17F, **Firmware** page: the **Open firmware file** field, the **Open firmware** button, the **Update [F12]** button and the progress indicator.

To use the W485 and E485 modules, G17F firmware **1.08** or newer is needed (sections 3.11 and 3.12); you see the current version in the **FW** field of the status bar (section 5.1).

9. Troubleshooting and frequently asked questions

If the communicator does not do what you expect, first look at the indicators (section 1.6), then at the points below.

The TROUBLE LED is blinking – what does the number of blinks mean?

The number of blinks is the cause of the fault: **1** – no SIM card; **2** – the PIN code of the SIM card is wrong (**System Options** → **SIM card PIN**, section 5.2); **3** – cannot connect to the mobile network; **4** – cannot connect to the IP receiver on the primary channel (**Reporting to CMS**, section 5.3); **5** – cannot connect to the IP receiver on the backup channel; **6** – the internal clock is not set (**Time set**, section 5.2; by SMS: `TIME`, section 4.2); **7** – the supply voltage is not correct (9–32 V DC; **Low power voltage**, section 5.2); **9** – fault in the connection with the RS485 module (wiring: sections 3.3–3.12; **Modules**, section 5.5).

How many yellow blinks are needed on the NETWORK LED?

The number of yellow blinks shows the signal strength: on a 2G (GPRS) network 5, on a 4G network 3 blinks are already enough. If you count fewer than 3 yellow blinks, the signal strength is not sufficient: choose another place for the communicator, or use a more sensitive antenna that can be mounted away from the device (section 1.7). If the indicators are not lit at all, check the power and the wiring (section 3.13).

Protegus 2 does not find the communicator

- Check the conditions for adding it: activated SIM card, PIN code entered or switched off, Protegus service switched on (**Users & Reporting** → **Enable cloud service**, section 5.4), **POWER** LED blinking green, **NETWORK** LED lit green and blinking yellow (section 4.1).
- If the **NETWORK** or the **DATA** LED is lit yellow continuously, the device cannot connect to the mobile network and/or to Protegus 2 (chapter 6). Check the **APN** setting (section 5.2).
- If the **Cloud Access Code** is not the default `123456`, enter the correct code when adding the system (section 2.1).

I cannot control the outputs by call or SMS

- By SMS and call, control is only possible from the phone numbers on the user list (section 4.2). If no user has been added yet, the first caller becomes the administrator (section 4.3).
- The user must have the right to control the outputs (**PGM** checkbox, section 5.4), and the **Remote Control** definition must be assigned to the output (**Output definition**, section 5.7).
- With a W485 or E485 module, check the **Use dial and SMS when working over internet module** checkbox (section 5.5): if it is not ticked and there is an internet connection, calls and SMS are not used.

I get no reply to my SMS commands

For the reply SMS, the **ACK** checkbox must be ticked for the user (**Users & Reporting**, section 5.4). You can edit the text of the replies on the **SMS answer texts** tab.

Where do the operator's SMS messages (balance, advertising) go?

If the **FWD** checkbox is ticked for the user, the G17F forwards to them the SMS messages coming from numbers outside the system (for example the balance notification of the SIM card) (section 5.4).

INIM Smartline: what should I pay attention to?

The panel must be set to **slave** mode in the SmartLeague program. If repeaters are connected to the panel, the G17F cannot be connected over the RS485 bus; and if the G17F is connected to the RS485 bus of the panel, the iO expansion modules of the communicator are not supported (section 3.5).

NSC Solution: the panel does not see the communicator

After setting up the G17F, the modules connected to the RS485 bus must be searched for (scanned) on the panel (**SCAN RS485**, section 3.4). The **NSC slave address** must not be the same as the address of the other modules connected to the panel.

What interval should I set for the PING?

We recommend a PING interval of at most 5 minutes. By default, the receiver reports the loss of connection to the monitoring software after three times the PING interval; the active connection is also needed for remote setup and control (section 5.3).

Can the G17F be used without a SIM card?

Yes, with a W485 Wi-Fi module or an E485 Ethernet module (with G17F firmware 1.08 or newer): in this case the messages go through the module (sections 3.11 and 3.12). If the Wi-Fi or the wired internet is lost, the G17F would send over the mobile network – this backup needs a SIM card. The settings of the module, for example indicating the absence of the SIM card and disabling mobile data: section 5.5.

10. 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 communicator 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 power before making any electrical connection.**
- 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 iO-8 expansion module for the G17F.
- APN settings – list of European mobile operators – if the mobile data connection is not established.
- Protegus Android / iPhone and web app – about the app.
- Protegus 2 Business Account – managing several systems as an installer.

- Documentation in English: docs.trikdis.com – LTE communicator for fire alarm control panels G17F – the manuals on docs.trikdis.com are in English.

Related products

Trikdis G17F 4G GSM / IP communicator **Trikdis G17F 2G GSM / IP communicator**
Trikdis iO8 wired expander module **Trikdis RF-LORA wireless expander module**
Trikdis IO-LORA wireless expander module **Trikdis IO8-LORA wireless expander module**
Trikdis PB-LORA wireless panic button **Trikdis W485 Wifi module (RS485)**
Trikdis E485 Ethernet module (RS485) **Trikdis ANT04 GSM stick-on antenna with 2,5m wire**
Trikdis ME301M magnetic antenna with 2,5m wire
Trikdis IPcom v5 Windows software receiver **Trikdis IPcom v5 Linux software receiver**

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/g17f-manual