GT and GT+ communicator – installer and user manual

Installer and user manual for the Trikdis GT and GT+ communicators: connection to the alarm control panel's data bus, serial port or telephone line output, programming the control panel, setup in TrikdisConfig, reporting to the monitoring station, the Protegus 2 app.



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

Contents

1. Overview

- 1.1 What it is for and how it works
- 1.2 Versions: GT and GT+
- 1.3 Compatible alarm control panels
- 1.4 Parts of the communicator
- 1.5 Terminals
- 1.6 LED indications
- 1.7 Technical specifications

2. Quick start with TrikdisConfig

- 2.1 Preparation
- 2.2 Connection to the Protegus 2 app
- 2.3 Connection to the monitoring station

3. Installation and wiring

- 3.1 Installation steps
- 3.2 Placement and antenna
- 3.3 Connection to the alarm control panel
  - 3.3.1 DSC – data bus (Keybus)
  - 3.3.2 DSC – Keybus and TIP/RING (GT+ only)
  - 3.3.3 Paradox – serial port
  - 3.3.4 Paradox SP/MG – Keybus and TIP/RING
  - 3.3.5 UTC Interlogix (Caddx) – data bus
  - 3.3.6 Texecom – serial port
  - 3.3.7 InnerRange Inception
  - 3.3.8 InnerRange Integriti
  - 3.3.9 Honeywell Vista – data bus
  - 3.3.10 Any control panel – TIP/RING
- 3.4 Connecting a keyswitch zone
- 3.5 Connecting inputs
- 3.6 Connecting an output with a relay
- 3.7 Connecting an iO-8 expander
- 3.8 Switching on and first check
- A TRIKDIS átjelző elindítása

4. Programming the alarm control panel

- 4.1 Data bus or serial wiring
  - 4.1.1 DSC
  - 4.1.2 Paradox
  - 4.1.3 Texecom
  - 4.1.4 UTC Interlogix (Caddx)
  - 4.1.5 InnerRange
  - 4.1.6 Honeywell Ademco Vista
- 4.2 Telephone line (TIP/RING) wiring
  - 4.2.1 Programming the Honeywell Vista dialer
  - 4.2.2 The UTC Interlogix (Caddx) NX dialer

5. Remote control with the Protegus 2 app

- 5.1 Adding the device

A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Arming and disarming with an output
5.3 Arming and disarming from the app
5.4 Control by SMS messages

6. TrikdisConfig – the settings in detail

6.1 The status bar
6.2 System settings
6.3 Panel settings
6.4 CMS reporting
6.5 User reporting
6.6 Network settings
6.7 IN/OUT
6.8 RS485 modules
6.9 Event summary
6.10 Restoring the factory settings

7. Remote programming

8. Testing the communicator

9. Firmware update

10. Troubleshooting and frequently asked questions

11. Safety instructions

See also

1. Overview

The GT and GT+ are Trikdis's **4G cellular communicators**: they forward the alarm control panel's events to the monitoring station and to the Protegus 2 app. They can be connected to the control panel in two ways: **directly**, to the panel's data bus or serial port (with DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange and Honeywell control panels), or to **the telephone line dialer of any control panel** (TIP/RING) that sends its events in Contact ID format with DTMF tones. The communicator forwards the full event information (code, partition, zone or user) to the monitoring station. With the Protegus 2 app the user controls the system remotely and receives notifications about the events; the app works with every control panel the communicator supports, regardless of the panel's manufacturer. Reporting to the monitoring station and Protegus 2 can be used at the same time. This manual was written for the 4G GT and GT+ communicators; the differences between the two versions are summarized in section 1.2.

1.1 What it is for and how it works

- **It reports to the monitoring station.** It sends the events over an IP connection to a Trikdis software or hardware receiver (TRK8 protocol) – these work with any monitoring software –, to a SIA DC-09 receiver or to a SUR-GARD receiver (TL150). To a SUR-GARD receiver it converts the Contact ID codes received from the control panel into SIA codes; the conversion table is in the appendix of the English Trikdis documentation. It checks the connection with the receiver every 30 seconds (or at the interval you set) with a PING message; if the primary channel fails, it switches to the backup channel. With a parallel channel the events go to two receivers at the same time. If the Protegus service is also switched on, the monitoring station receives the event first, and the users' app only after that.
- **It notifies the user.** The Protegus 2 app signals the events in a push notification with a separate sound; from the app the user can arm and disarm, and switch the devices connected to it (lighting, gate, ventilation, heating, irrigation, etc.). In the app the administrator, the installer and the user have different rights. Besides Protegus 2, notification by SMS and phone call can also be requested.
- **It controls the control panel directly.** When connected to the data bus or serial port, the communicator also sees the panel's partition and zone states, and the user arms and disarms from Protegus 2 with their own keypad code – no keyswitch zone is needed for this. With DSC control panels the GT+ can be connected to the data bus (Keybus) and to the TIP/RING terminals at the same time: the bus is used for control and for the states, while the events are sent with the panel's own Contact ID codes (section 3.3.2).
- **It has its own inputs and outputs.** Two dual-function I/O terminals can be used as inputs (IN) or as controllable outputs (OUT). The outputs can be switched from the Protegus 2 app and by SMS command. With iO-8 expanders connected to the RS485 bus, further inputs and outputs can be added.
- **Setup.** The settings can be saved to a file and written into other communicators. There are two access levels: the monitoring station administrator's and the installer's. The communicator can also be configured remotely, and its firmware can also be updated remotely.

The diagram below shows the structure of the system: the alarm control panel connects to the communicator, the communicator reaches the internet over the mobile network (LTE), and from there the monitoring station's receiver (and its software) and the Protegus server; the user sees the system in the Protegus 2 app, and can also receive SMS and calls over the mobile network.

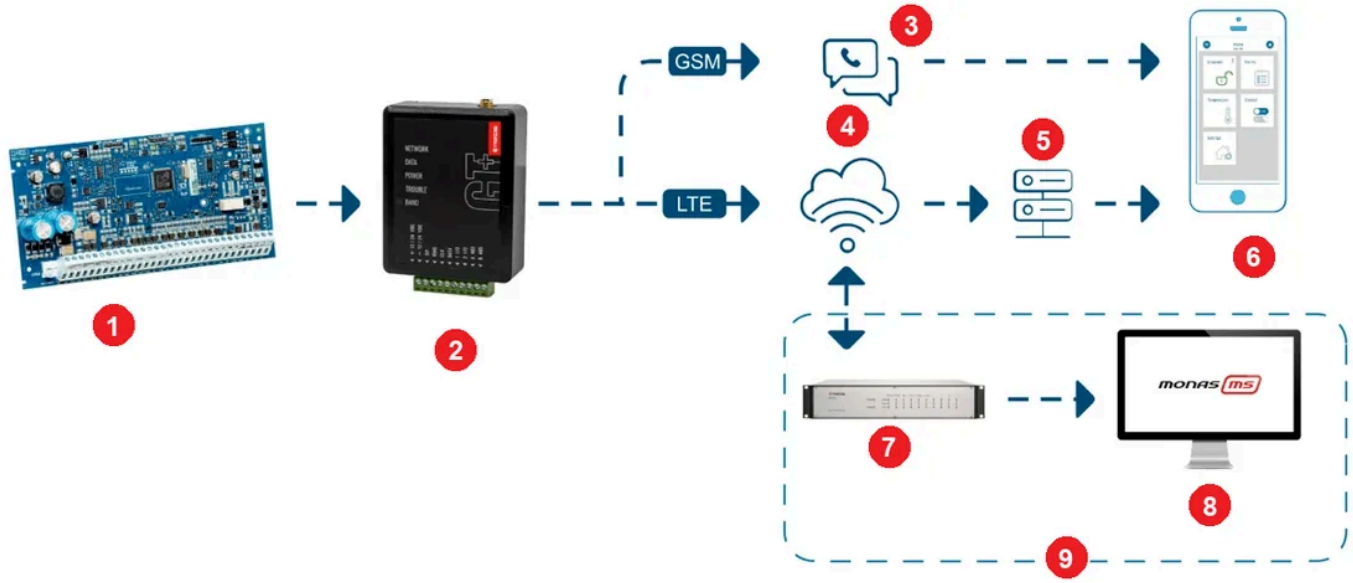


Figure 1. The communicator's place in the system: alarm control panel → GT / GT+ → mobile network → internet → monitoring station receiver and Protegus server → Protegus 2 app; SMS and calls directly over the mobile network.

- 1 alarm control panel (“Alarm panel”)
- 2 GT / GT+ LTE communicator (“LTE communicator”)
- 3 call and SMS (“Call/SMS”)
- 4 internet (“Internet”)
- 5 Protegus server (“Protegus server”)
- 6 phone with the Protegus app (“Phone with Protegus software”)
- 7 monitoring station receiver (“Receiver”)
- 8 monitoring software (“Monitoring software”)
- 9 the security company's monitoring station (“Monitoring station in security company”) – in the dashed frame

1.2 Versions: GT and GT+

The GT and the GT+ are the same device in two versions: their wiring, setup and operation are almost identical, so we describe them in one manual. The differences are summarized in the table below; where the text gives the GT+ data, take this into account for the GT.

	GT	**GT+**
Supply voltage	10–18 V DC	10–32 V DC
Labels of the power terminals	+12 VDC, −12 VDC	+12 / 24 VDC, −12 / 24 VDC
Connecting a DSC control panel	to the data bus (Keybus) only	to the data bus, or to the data bus and the TIP/RING terminals together – this way the events are sent with the panel's own Contact ID codes (e.g. fire: E110), not as a general alarm (E130)
Setting for the telephone line (TIP/RING) connection in TrikdisConfig (**Panel settings → Communication protocol**)	**2. Dual tone**	**2. AUTO** (**3. MANUAL** can also be selected in the list)
Testing with DSC with bus + TIP/RING connection (chapter 8)	–	a fire zone alarm must arrive as E110
Everything else: inputs/outputs, RS485 bus, modem, LEDs, size, protocols, Protegus 2, SMS commands	identical	identical

Both versions are made with three kinds of modem; for Europe, the European (EU) version is the right one. You can find the modem type and the hardware version in the TrikdisConfig status bar (**Device**, **HW**) and on the device label.

Modem	Network and frequency bands
EG915U-EU (Europe)	LTE FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM: B2 / B3 / B5 / B8
EG915U-LA (Latin America)	LTE FDD: B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66; GSM: B2 / B3 / B5 / B8
BG95-M5 (LTE Cat M1)	LTE FDD: B1 / B2 / B3 / B4 / B5 / B8 / B12 / B13 / B18 / B19 / B20 / B25 / B26 / B27 / B28 / B66 / B85; EGPRS: 850 / 900 / 1800 / 1900 MHz

1.3 Compatible alarm control panels

The control panels below can be connected to the communicator directly, over the data bus or serial port. The “Direct control” column shows whether the user can arm and disarm from Protegus 2 with their own keypad code without additional wiring; where this is not possible, the communicator reads the events from the bus, and a keyswitch zone is needed for control (section 3.4).

Manufacturer	Model	Connection	Direct control
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864	data bus (Keybus); GT+: also Keybus + TIP/RING	yes
DSC	PC5020	data bus (Keybus)	no
Paradox	Spectra SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+	serial port (EX-CRP2.4 cable), or Keybus + TIP/RING	yes
Paradox	Magellan MG5000, MG5050, MG5050E, MG5075, MG5050+	serial port (EX-CRP2.4 cable), or Keybus + TIP/RING	yes
Paradox	Digiplex EVO192, EVOHD, EVOHD+	serial port (EX-CRP2.4 cable)	yes
Paradox	Digiplex EVO48	serial port (EX-CRP2.4 cable)	no
Paradox	Spectra 1727, 1728, 1738; Esprit E55	serial port (EX-CRP2.4 cable)	no
UTC Interlogix	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e	data bus	yes
Texecom	Premier 24, 48, 88, 168, 640; Premier Elite 12, 24, 48, 64, 88, 168, 640	serial port (EX-CRP4 cable)	yes
InnerRange	Inception, Integriti	serial port (with the panel manufacturer's cable)	no
Honeywell	Ademco Vista-15, Vista-20, Vista-48	data bus	yes

- The firmware of directly controlled **Paradox** control panels must be at least **V.4**. On the newer Paradox control panels (SP+, MG+, EVOHD+) the serial port may be locked at the factory; unlocking is covered in section 4.1.2. The Spectra SP / SP+ and Magellan MG / MG+ control panels can also be connected to the data bus (Keybus) and the TIP/RING terminals together instead of the serial port – this does not need the paid unlocking (section 3.3.4).

- The control panels of **all other manufacturers** connect through their telephone line dialer (TIP/RING), if it sends the events in Contact ID format with DTMF dialing; in this case a keyswitch zone is needed for control.
- You can check which Trikdis communicator and which wiring is right for your control panel in the Compatibility finder.

1.4 Parts of the communicator

The communicator's printed circuit board comes in a black plastic case; the front cover can be snapped off, and the terminal block can be pulled off. The picture below shows the GT+; the GT is the same, only the case label is GT, and the power terminals are labelled +12 VDC / −12 VDC.

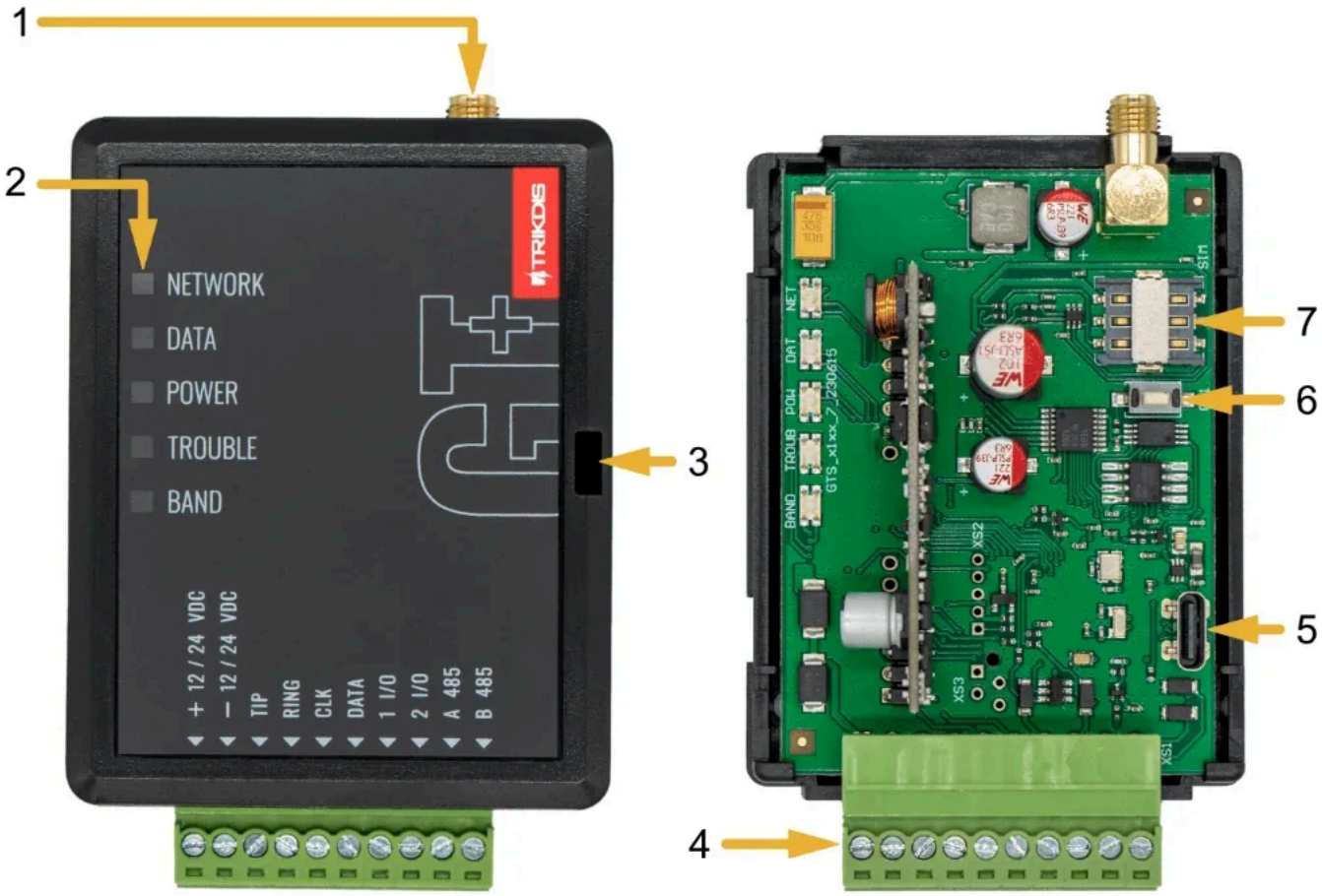


Figure 2. Parts of the communicator from the front (left) and with the case open (right).

- 1 SMA connector of the mobile antenna
- 2 LED indicators (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Slot that helps snap off the front cover
- 4 Detachable terminal block for the external connections
- 5 USB-C socket for programming
- 6 RESET button
- 7 Nano SIM card holder

The terminal block can be pulled off: this way the device can be powered off or restarted in one move, it is easier to handle during wiring, and for USB programming the device can be taken to the computer.

1.5 Terminals

Terminal (GT)	Terminal (GT+)	Function
+12 VDC	**+12 / 24 VDC**	Power, positive: +10–18 V DC (GT), +10–32 V DC (GT+)
−12 VDC	**−12 / 24 VDC**	Power, 0 V
TIP	**TIP**	TIP terminal of the alarm control panel's telephone line dialer
RING	**RING**	RING terminal of the alarm control panel's telephone line dialer
CLK	**CLK**	Serial bus or data bus (clock) for connecting the control panel directly
DATA	**DATA**	Serial bus or data bus (data) for connecting the control panel directly
1 I/O	**1 I/O**	Input/output 1 (default: input, NO)
2 I/O	**2 I/O**	Input/output 2 (default: input, NO)
A 485	**A 485**	A line of the RS485 bus
B 485	**B 485**	B line of the RS485 bus

On the wiring diagrams the power terminals are uniformly marked **+DC** and **−DC** (on the GT this is the +12 VDC / −12 VDC terminal, on the GT+ the +12 / 24 VDC / −12 / 24 VDC terminal), and the RS485 terminals **A RS485** / **B RS485** (on the device A 485 / B 485). The terminal labels are also printed on the front cover.

1.6 LED indications

The LEDs on the front cover are the most important tools for commissioning and troubleshooting. Read them together: POWER shows the power supply, NETWORK the network, TROUBLE faults, and BAND the network type.

NETWORK – network connection

Indication	Meaning
off	No connection to the mobile network
flashing yellow	Connecting to the mobile network
steady green, flashing yellow	Connected to the mobile network; the number of yellow flashes is the **signal level**: on 4G 3 flashes means a good signal

DATA – data traffic

Indication	Meaning
off	No events waiting to be sent
steady green	There are events waiting to be sent in the buffer
flashing green	Data transfer between the communicator and the computer (during programming)

Quick check

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.

POWER – power supply

Indication	Meaning
off	No power, or the power is disconnected
steady green	Switched on, the supply voltage is OK
steady yellow	Inadequate supply voltage (11.5 V or less)
steady green, flashing yellow	Ready for programming (during programming)
steady yellow (during programming)	No connection to the computer

TROUBLE – fault

Indication	Meaning
off	No fault
1 red flash	No SIM card
2 red flashes	SIM PIN error (wrong PIN code)
3 red flashes	Programming error (no APN)
4 red flashes	Cannot register on the mobile network (registration error)
5 red flashes	Cannot connect to the data network (GPRS/UMTS)
6 red flashes	No connection to the monitoring station receiver
7 red flashes	Connection to the alarm control panel lost
8 red flashes	The configured ICCID does not match the SIM card's ICCID (section 6.6)
flashing red (during programming)	Memory error
steady red (during programming)	Corrupted firmware

BAND – network type

Green flashes	Network
1	none
2	GSM
3	GPRS
4	EDGE
5	3G (HSDPA, HSUPA, HSPA+, WCDMA)
6	4G (LTE TDD, LTE FDD)

1.7 Technical specifications

Parameter	Value
Connection to the alarm control panel	serial bus, data bus (Keybus) or telephone line (TIP/RING, Contact ID, DTMF)
Inputs/outputs	2 dual-function I/Os: as inputs NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (2.2 kΩ end-of-line resistor); as outputs open collector (OC), max. 0.15 A / 30 V DC. Expandable with iO-8 expanders
Modem	EG915U-EU (Europe), EG915U-LA (Latin America) or BG95-M5 (LTE Cat M1) – the frequency bands are listed in the table in section 1.2
Supply voltage	GT: 10–18 V DC; GT+: 10–32 V DC
Current consumption	up to 100 mA in standby; up to 200 mA while sending data
Transmission protocols	TRK8, DC-09_2007, DC-09_2012, TL150
Encryption	AES-128
Programming	TrikdisConfig (Windows) over a USB-C cable or remotely
Operating environment	−10 … +50 °C, max. 80 % relative humidity (at +20 °C)
Dimensions	92 × 62 × 26 mm
Weight	80 g

2. Quick start with TrikdisConfig

All settings of the communicator are made with the Windows program called **TrikdisConfig** – over a USB-C cable or remotely. This chapter describes the shortest route: you set up the device on the desk before wiring, and on site you then only need to wire it in. We describe which settings are needed for the communicator to send events to the monitoring station, and for the system to be controllable from the Protegus 2 app; the settings are explained in detail in chapter 6.

2.1 Preparation

What you will need

USB-C cable for programming · cable with at least 4 cores between the communicator and the control panel · CRP2.4 cable for the Paradox serial port · 2.5 mm flat screwdriver · mobile antenna with suitable gain, if coverage on site is weak · active SIM card (the PIN request can be switched off) · the alarm control panel's installer manual.

The necessary accessories must be ordered separately from the distributor.

1. Download and install the TrikdisConfig software. On the Trikdis website (www.trikdis.com), type “TrikdisConfig” in the search field.

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!

2. Open the communicator's case with a flat screwdriver: insert the screwdriver at the top, into the slot next to the antenna, and lever outwards, then at the bottom, at the opening, downwards. The figure also shows the location of the USB-C socket at the edge of the printed circuit board.

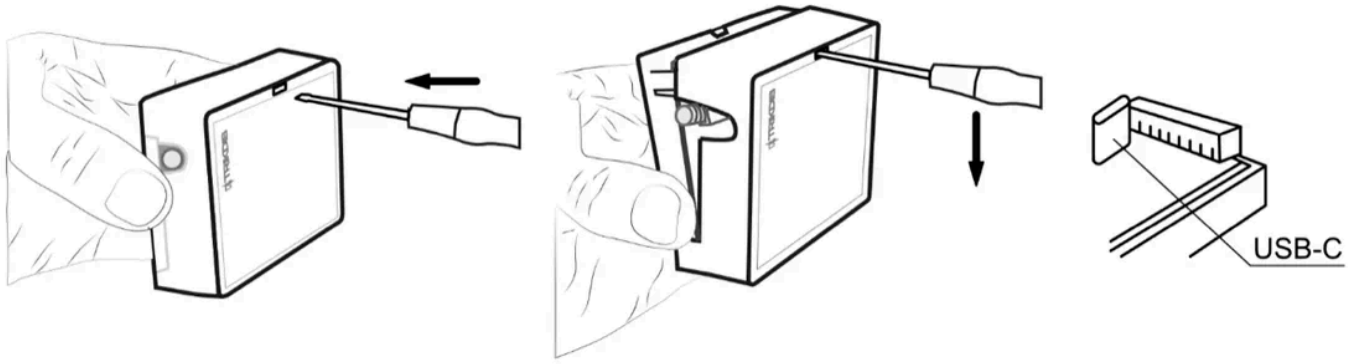


Figure 3. Snapping off the front cover with a flat screwdriver; the enlarged detail shows the location of the USB-C socket.

3. Insert the nano SIM card into the holder, in the orientation shown in the figure. The card must be active and have mobile data service, and if possible, switch off its PIN request in a phone (so you do not have to enter a PIN in the device).

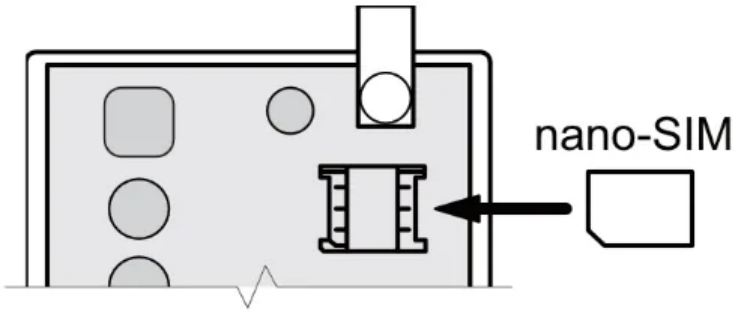


Figure 4. Location of the nano SIM card on the printed circuit board.

4. Connect the communicator to the computer with a USB-C cable.

Warning

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

5. Start TrikdisConfig. The program recognizes the device and opens the programming window. Click the **Read [F4]** button: the program reads the device's current settings. If it asks for a password, enter the 6-digit administrator code (default `123456`) or installer code (default `654321`).

2.2 Connection to the Protegus 2 app

First, on the **Panel settings** page, specify how the communicator connects to the control panel.

If you connect it to the control panel's telephone line output (TIP/RING): in the **Communication protocol** field select **AUTO** (on the GT the second item in the list is **Dual tone** – select that there).

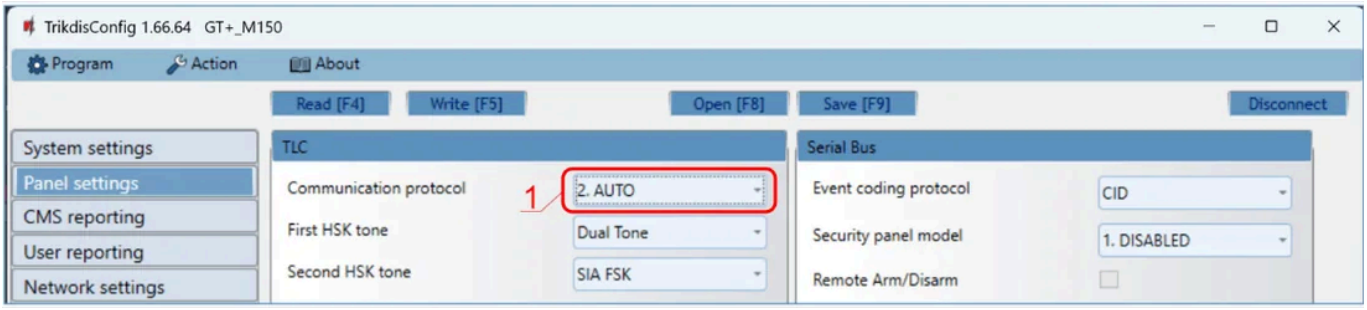


Figure 5. TrikdisConfig – Panel settings, TLC group (the picture shows the GT+ setting).

- 1 **Communication protocol** – with TIP/RING wiring **2. AUTO** (GT: **2. Dual tone**).

If you connect it to the control panel's data bus or serial port: set the control panel in the **Serial bus** group.



Figure 6. TrikdisConfig – Panel settings, Serial bus group.

- 2 **Security panel model** – the type of the connected control panel.
- 3 **Remote Arm/Disarm** – tick it if the users want to control the control panel from Protegus 2 with their own keypad code. It only appears for the directly controllable control panels.
- 4 **Security panel PC download password** – for direct control of Paradox and Texecom control panels, the PC or UDL password set in the control panel; the two must match.

GT+, DSC control panel on the data bus and the TIP/RING terminals together: the **Communication protocol** must be **AUTO**, the **Security panel model** the DSC type, and tick the **Remote Arm/Disarm** option if the control panel is to be controlled from Protegus 2 (section 3.3.2).

For direct control the alarm control panel must also be set up – this is described in chapter 4, where you also find how to set the PC or UDL password.

Then, on the **User reporting** page, on the **PROTEGUS Cloud** tab, enable the cloud connection.

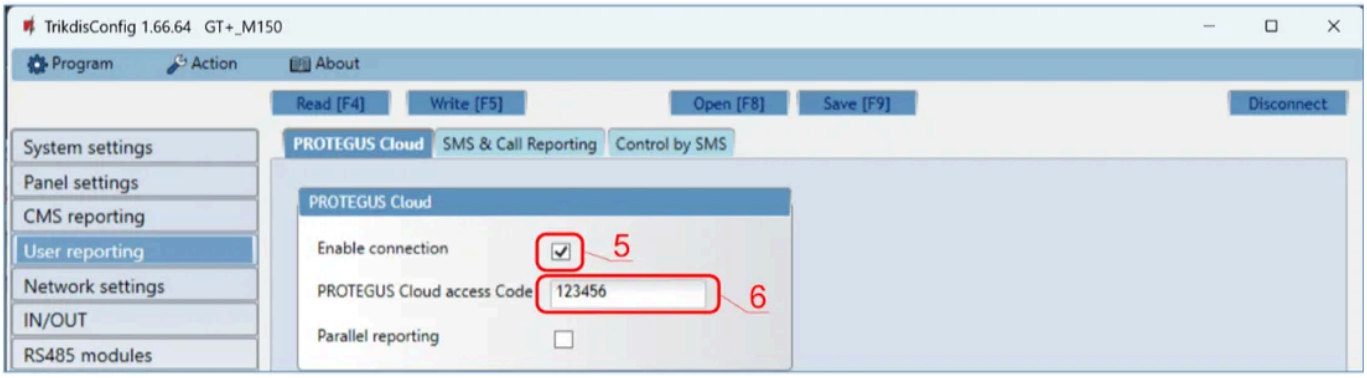


Figure 7. TrikdisConfig – User reporting, PROTEGUS Cloud tab.

- 5 **Enable connection** – tick it: it enables the connection to the Protegus cloud.
- 6 **PROTEGUS Cloud access Code** – the access code for Protegus 2 (default `123456`). Change it if you want the user to have to enter it when adding the system to the app. Important: if you change the code later in TrikdisConfig, it must also be changed in the Protegus 2 app.

Finally, on the **Network settings** page, on the **SIM1** tab, enter the card's data.

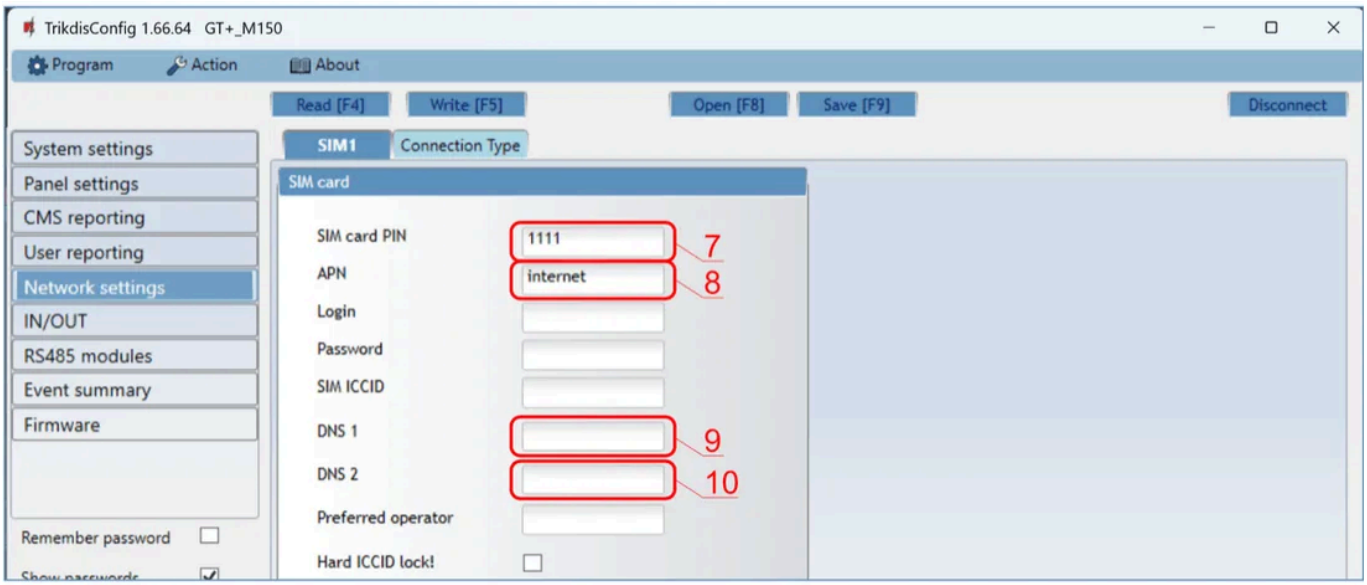


Figure 8. TrikdisConfig – Network settings, SIM1 tab.

- 7 **SIM card PIN** – the card's PIN code (if the PIN request is switched off, the default value can stay).
- 8 **APN** – the operator's data access point (see below).
- 9 **DNS 1** – primary name server; by default Google's DNS. Regardless of the IP settings, check that the DNS addresses work with your operator.
- 10 **DNS 2** – secondary name server (also Google's by default).

The APN (Access Point Name) is the mobile operator's data access point; without it the device cannot connect to the internet. You can find the exact value on the website of the SIM card's operator. We keep the known APNs of European operators in a separate article: APN settings – list of European mobile operators. If you have no other information from the operator, try the APN `internet`: it is generic and works in many operators' networks.

For IoT / M2M (machine-to-machine) data cards, the operator usually gives **a different APN than for consumer cards** – with the consumer APN the device does not connect. You can also find this value in the APN article, or ask the operator for it; if the operator also gives a user name and password, enter those as well.

If the device does not report to a monitoring station, the setup is now complete: press the **Write [F5]** button, wait for the confirmation, and unplug the USB cable.

With telephone line (TIP/RING) wiring, do not forget to switch on and set up the alarm control panel's dialer, otherwise the control panel will not send any events; for direct control the Paradox, Texecom, Caddx, InnerRange and Honeywell control panels must also be set up. Setting up the control panel is described in chapter 4.

2.3 Connection to the monitoring station

If the device also reports to a monitoring station receiver, first enter the object ID on the **System settings** page.

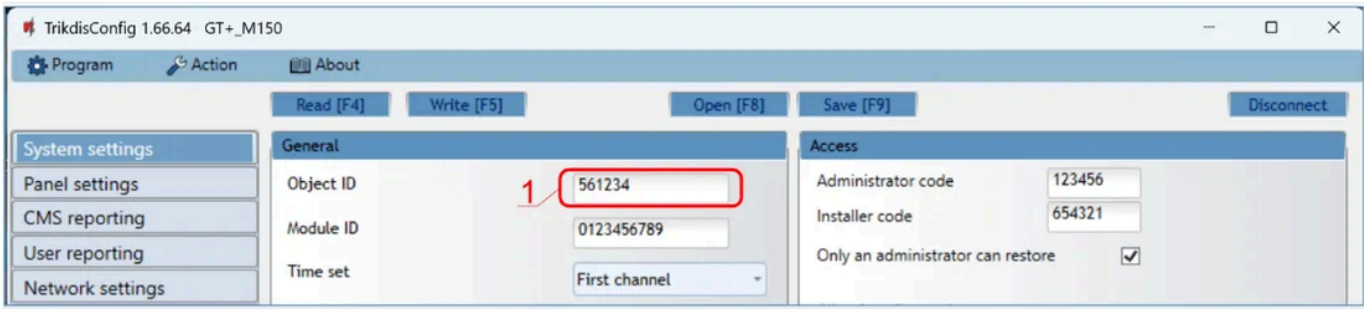


Figure 9. TrikdisConfig – System settings page, General group.

- 1 **Object ID** – the object ID received from the monitoring station (6 hexadecimal characters, 0–9, A–F). `FFFE` and `FFFF` cannot be used.

On the **Panel settings** page, specify the control panel connection if you have not done so in section 2.2: with TIP/RING wiring the **Communication protocol** must be **AUTO** (GT: **Dual tone**); with data bus or serial wiring select the type of the connected control panel in the **Security panel model** field (the figures in section 2.2).

Then, on the **CMS reporting** page, in the **Primary channel** section, set the receiver's data.

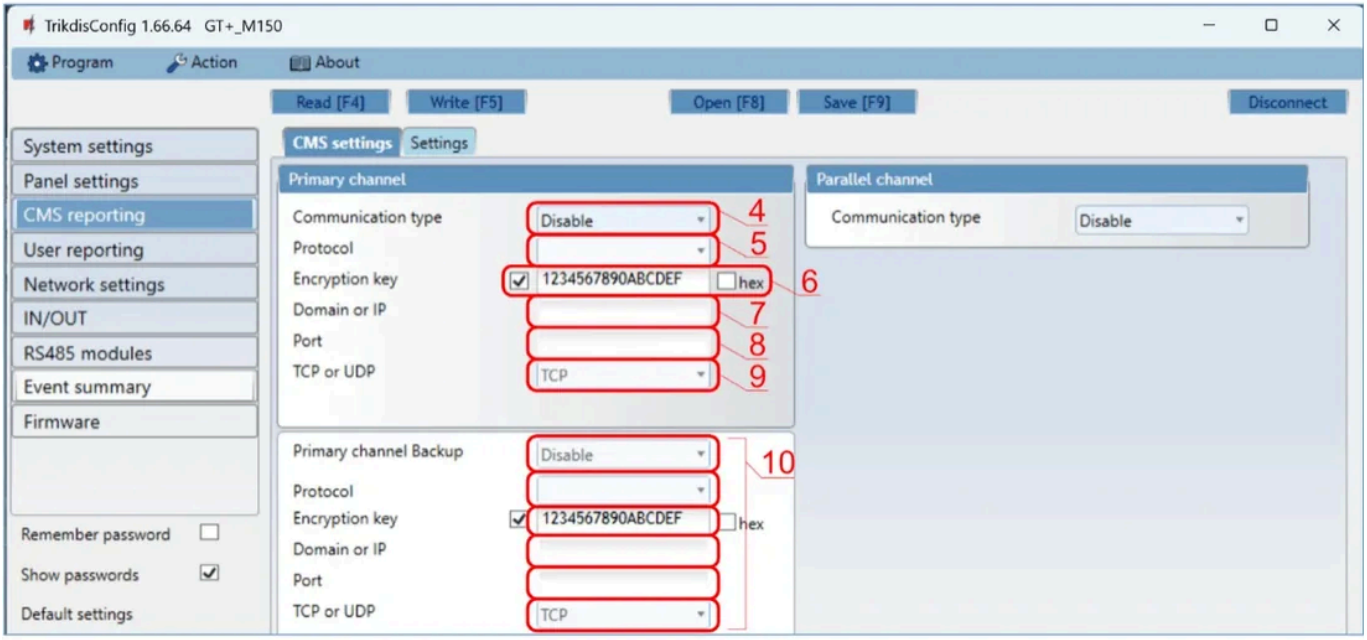


Figure 10. TrikdisConfig – CMS reporting, CMS settings tab.

- 4 **Communication type** – select the **IP** connection.
- 5 **Protocol** – **TRK8** for a Trikdis receiver, **DC-09_2007** or **DC-09_2012** for a universal receiver, **TL150** for a SUR-GARD receiver.
- 6 **Encryption key** – the encryption key set in the receiver.
- 7 **Domain or IP** – the receiver's domain name or IP address.
- 8 **Port** – the receiver's port number.
- 9 **TCP or UDP** – the transmission protocol; it follows the receiver's setting.
- 10 **Primary channel Backup** – backup channel in case the primary channel fails; fill it in the same way, it is recommended.

Finally, on the **Network settings** page, on the **SIM1** tab, enter the card's data (**SIM card PIN**, **APN**, **DNS 1, DNS 2**) if you have not done so in section 2.2.

With the **DC-09** protocol, also enter the line and receiver number on the **Settings** tab (**Line No.**, **Receiver No.**, section 6.4). The GT and the GT+ report to the monitoring station only over an IP connection; they have no SMS backup channel.

At the end of the setup press the **Write [F5]** button, wait for the confirmation, and unplug the USB cable. The device is now ready for wiring. With telephone line wiring, the alarm control panel's dialer must be switched on and set up here as well, otherwise the control panel will not send any events (chapter 4).

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.

3.1 Installation steps

1. Remove the front cover (see section 2.1), and pull off the terminal block.
2. Insert the nano SIM card into the holder, if you have not done so during commissioning.
3. Take the printed circuit board out of the back cover: open the latch next to the antenna connector, and lift the board out (see the figure).

4. Fix the back cover with screws in the chosen place (the screw holes are circled in the figure).
5. Put the printed circuit board back into the back cover, and plug the terminal block back in.
6. Screw on the mobile antenna.
7. Put the front cover back on.

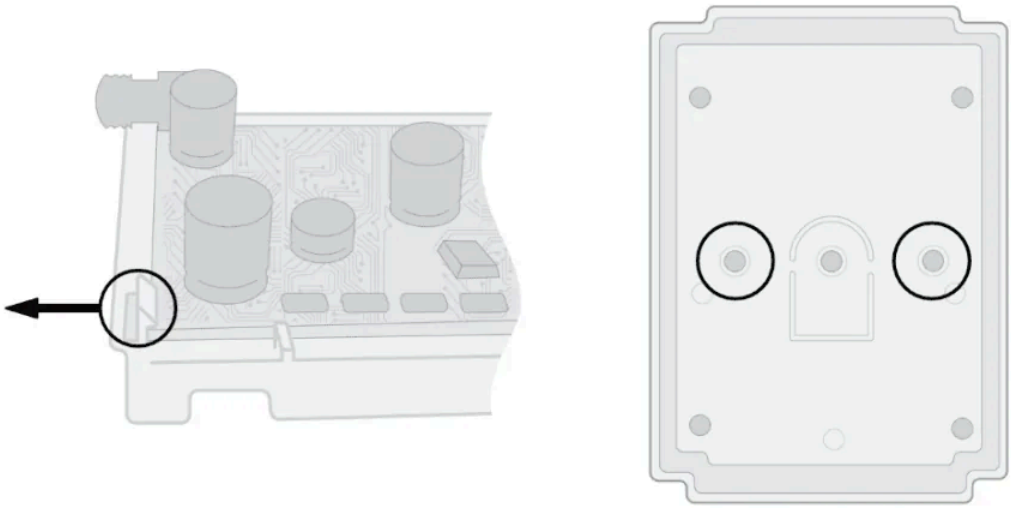


Figure 11. Lifting the printed circuit board out of the back cover (left: the latch and the direction of lifting) and the screw holes of the back cover (right).

The SIM card must be active, and for IP-based use, mobile data must work on it. If you do not want TrikdisConfig to ask for a PIN code, put the card into a mobile phone and switch off the PIN request there.

3.2 Placement and antenna

- Place the communicator in a **dry, indoor** location, preferably near the alarm control panel's enclosure, so that the wiring is short.
- In a **metal enclosure** the mobile signal is strongly attenuated. If the communicator goes into the control panel's metal housing, lead the antenna outside the enclosure, or use an antenna with a longer cable.
- Before final mounting, **check the signal level**: the number of yellow flashes of the NETWORK LED must be at least 3 on 4G (section 1.6). If it is less, find a better place, or switch to a more sensitive antenna that can be placed further away.
- Keep the antenna and the communicator away from the control panel's transformer and from mains cables.



A mobilhálózatos átjelzőhöz gyári tartozékként egy alap ANT01S GSM antenna jár. Ha a telepítés helyén gyenge jelszint várható, vagy ha az eszközt fémdoboz vagy vastag fal árnyékolja, javasolt nagyobb teljesítményű, például 2,5 m-es vezetékkel rendelkező ME301M mágneses vagy ANT04 felragasztható antenna használata.

3.3 Connection to the alarm control panel

Follow the drawing below that matches your control panel. On the drawings **+DC** and **–DC** are the communicator's power terminals (GT: +12 VDC / −12 VDC, GT+: +12 / 24 VDC / −12 / 24 VDC), and **A RS485** / **B RS485** are the A 485 / B 485 terminals. The communicator gets its power from the control panel's auxiliary power output (AUX), so during a power cut the control panel's battery also powers the communicator. The drawings show the GT+; the wiring of the GT is the same.

3.3.1 DSC – data bus (Keybus)

Connect the DSC control panel's Keybus to the communicator with four wires: **RED** → **+DC**, **BLK** → **–DC**, **YEL** → **CLK**, **GRN** → **DATA**.

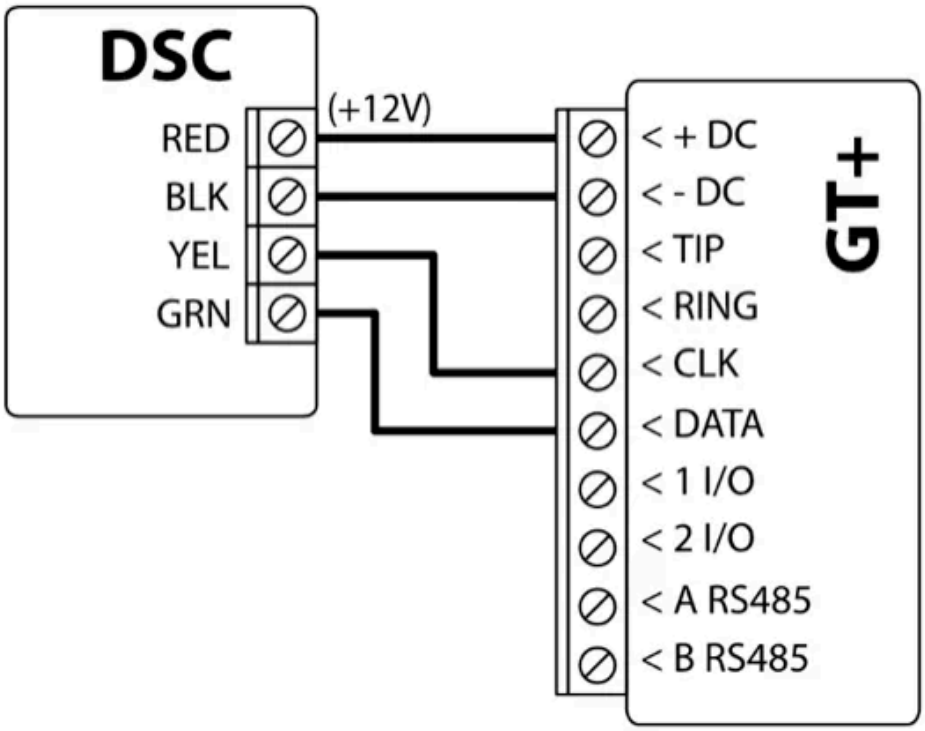


Figure 12. Connecting a DSC control panel on the data bus (Keybus, "Keypad bus"): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

Connected only to the Keybus, the communicator receives the general state of the zones from the control panel, but does not know the zone type (fire, burglary, water leak, etc.). Therefore it reports every alarm **as a general alarm, with Contact ID code E130**, and some monitoring stations handle this differently from the zone type that was actually triggered. If you want the events to be sent with the control panel's own Contact ID codes (for example fire alarm: E110), with the GT+ also connect the TIP/RING terminals (section 3.3.2).

3.3.2 DSC – Keybus and TIP/RING (GT+ only)

The GT+ can be connected to a DSC control panel's data bus and telephone line output at the same time: in addition to the Keybus wires, also connect the control panel's **TIP** → **TIP** and **RING** → **RING** terminals to the communicator's.

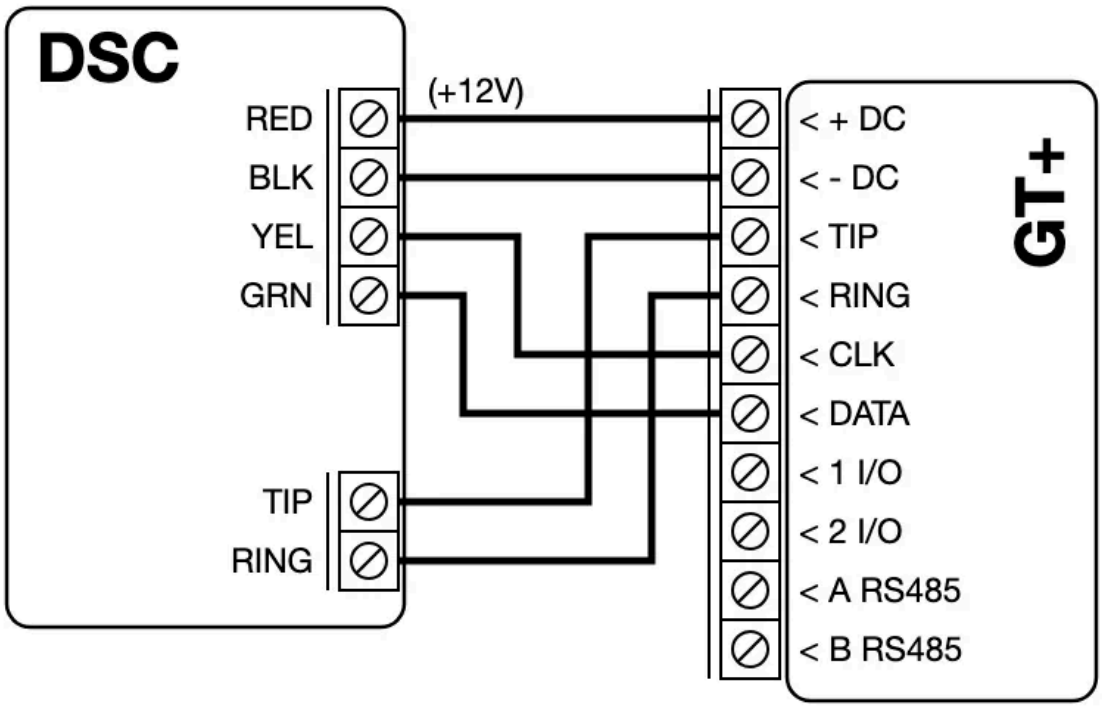


Figure 13. Connecting a DSC control panel on the data bus (“Keypad bus”) and the TIP/RING terminals together (GT+): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA, and TIP → TIP, RING → RING.

In this case the Keybus is used for control and for the states (remote arming and disarming, partition and zone states), while the events are sent by the control panel's telephone line dialer on the TIP/RING terminals, so they are sent with the control panel's own Contact ID codes. As long as the TIP/RING connection works, the communicator does not send the events coming from the Keybus a second time.

For this wiring, set the following on the **Panel settings** page of TrikdisConfig:

1. **Communication protocol**: **AUTO**.
2. **Security panel model**: the type of the DSC control panel.
3. **Remote Arm/Disarm**: tick it if the users want to control the control panel from the Protegus 2 app.

The DSC control panel's telephone line dialer must also be programmed to send the events – this is described in section 4.1.1.

3.3.3 Paradox – serial port

The communicator connects to the Paradox control panel's serial port with the separately orderable **EX-CRP2.4** cable: **red → +DC**, **black → −DC**, **yellow → CLK**, **green → DATA**.

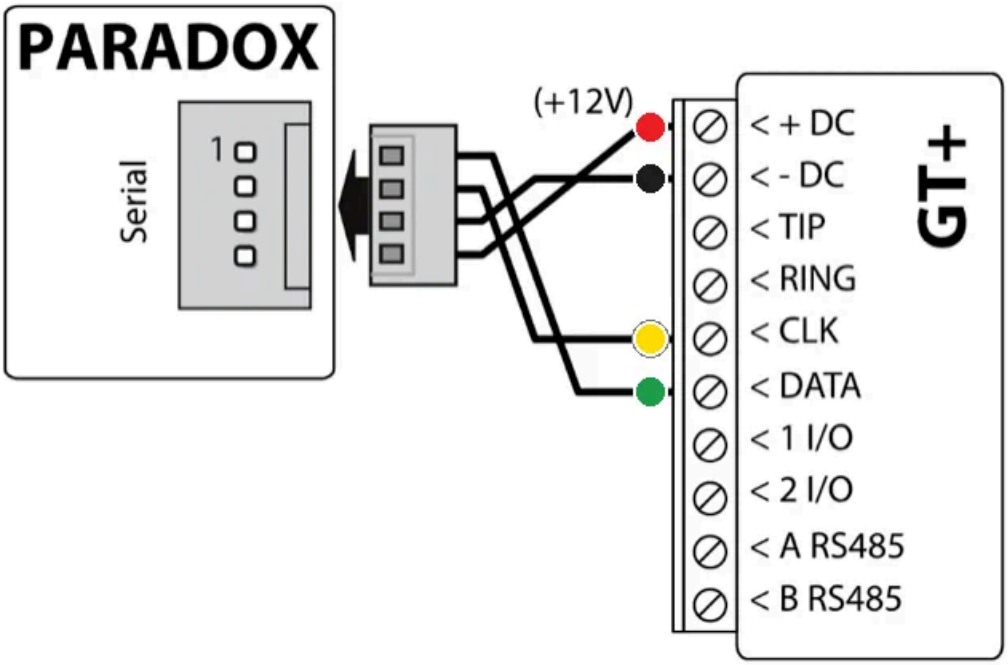


Figure 14. Connecting a Paradox control panel on the serial port with the EX-CRP2.4 cable (to be ordered separately; "Use the EX-CRP2.4 cable (ordered separately)"): red → +DC, black → −DC, yellow → CLK, green → DATA.

- red wire ("R - red")
- black wire ("B - black")
- yellow wire ("Y - yellow")
- green wire ("G - green")

On the newer Paradox control panels (SP+, MG+, EVOHD+) the serial port may be locked at the factory; unlocking is covered in section 4.1.2. With the Spectra SP / SP+ and Magellan MG / MG+ control panels, the wiring in the next section can also be used instead of the serial port.

3.3.4 Paradox SP/MG – Keybus and TIP/RING

The Paradox Spectra SP, SP+ and Magellan MG, MG+ control panels can also be connected to their data bus (Keybus) and TIP/RING terminals together instead of the serial port: **+AUX** → **+DC**, **–AUX** → **–DC**, **GRN** → **DATA**, **YEL** → **CLK**, and **TIP** → **TIP**, **RING** → **RING**. This wiring uses the control panel's Keybus instead of the serial port, so it does not need the paid Paradox serial port unlocking.

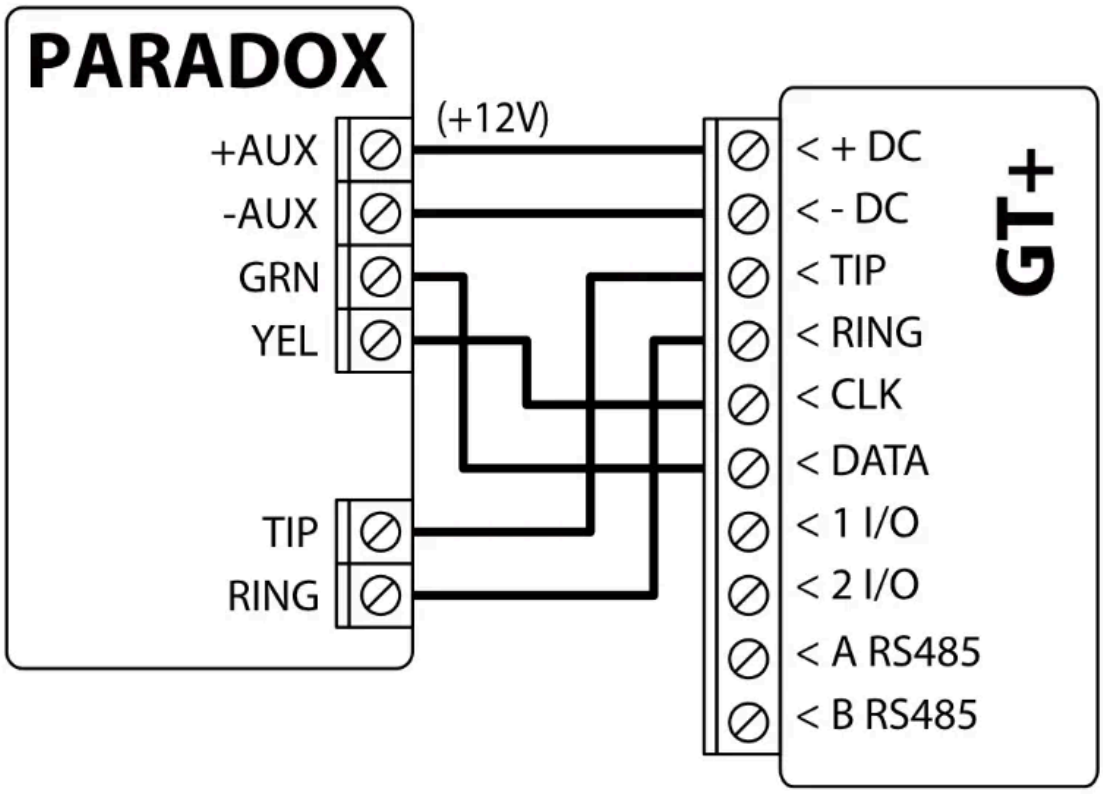


Figure 15. Connecting a Paradox SP / SP+ / MG / MG+ control panel on the Keybus (data bus, "Keypad bus") and the TIP/RING terminals together: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

For this wiring the communicator's firmware must be at least **1.21** (updating is described in chapter 9).

For this wiring, set the following on the **Panel settings** page of TrikdisConfig:

1. **Communication protocol**: **AUTO** (GT: **Dual tone**).
2. **Security panel model**: **7. Paradox SP+/MG+ series KeyBus**.
3. **Remote Arm/Disarm**: tick it if the users want to control the control panel from the Protegus 2 app with their own keypad code.
4. **Security panel PC download password**: for direct control, enter the PC password set in the control panel; the two must match.



Figure 16. TrikdisConfig – Panel settings for the Keybus + TIP/RING wiring: Communication protocol AUTO, Security panel model 7. Paradox SP+/MG+ series KeyBus, Remote Arm/Disarm ticked, PC download password entered.

The Paradox control panel must also be programmed to send the events to the monitoring station and to be controllable from Protegus 2 – this is described in section 4.1.2.

3.3.5 UTC Interlogix (Caddx) – data bus

Connect the Caddx NetworX control panel's data bus to the communicator with three wires: **POS** → **+DC**, **COM** → **−DC**, **DATA** → **DATA**. The TIP, RING and CLK terminals are not needed.

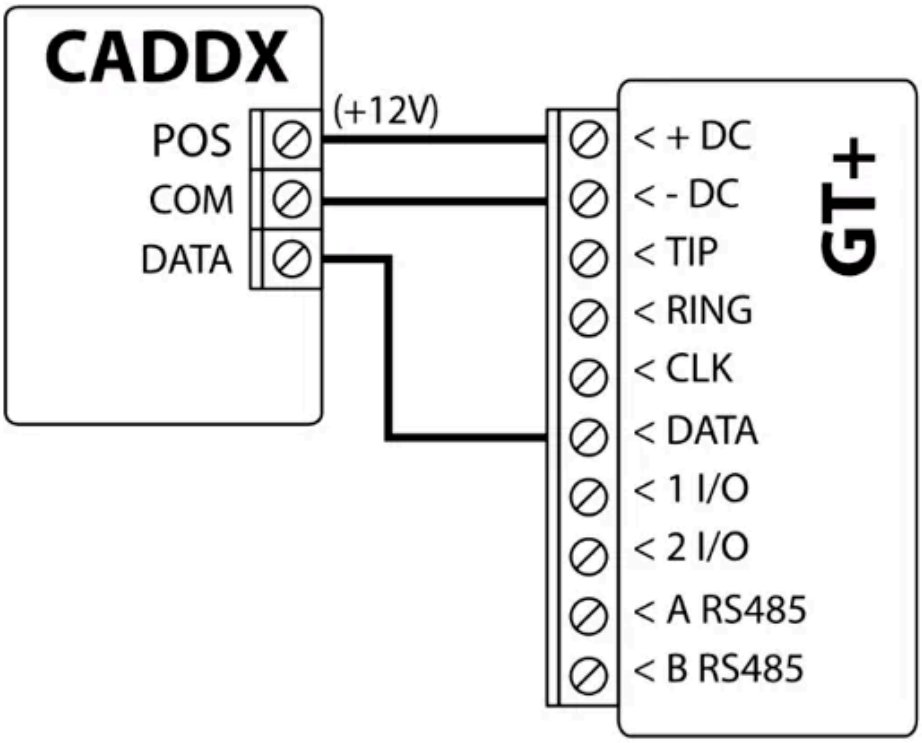


Figure 17. Connecting a UTC Interlogix (Caddx) NetworX control panel on the data bus ("Keypad bus"): POS → +DC, COM → −DC, DATA → DATA.

3.3.6 Texecom – serial port

The communicator connects to the serial port of the Texecom Premier / Premier Elite control panel with the separately orderable **EX-CRP4** cable: **red** → **+DC**, **black** → **−DC**, **blue** → **CLK**, **white** → **DATA**.

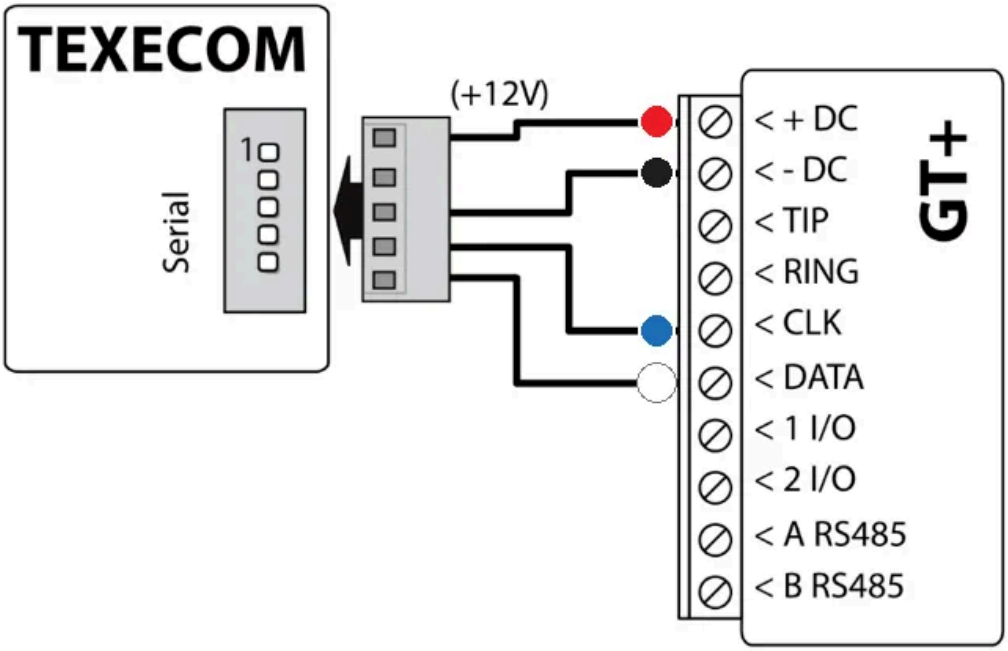


Figure 18. Connecting a Texecom control panel on the serial port with the EX-CRP4 cable (to be ordered separately; "Use the EX-CRP4 cable (ordered separately)"): red → +DC, black → −DC, blue → CLK, white → DATA.

- red wire ("R - red")
- black wire ("B - black")
- blue wire ("BL - blue")
- white wire ("W - white")

3.3.7 InnerRange Inception

The communicator gets its power from the Inception control panel's power output (**VOUT +** → **+DC**, **VOUT 0V** → **−DC**), and the data connection comes from the control panel's USB port, with Inner Range's **993030USB** cable: **black** → **0V / −DC**, **green** → **CLK**, **white** → **DATA**.

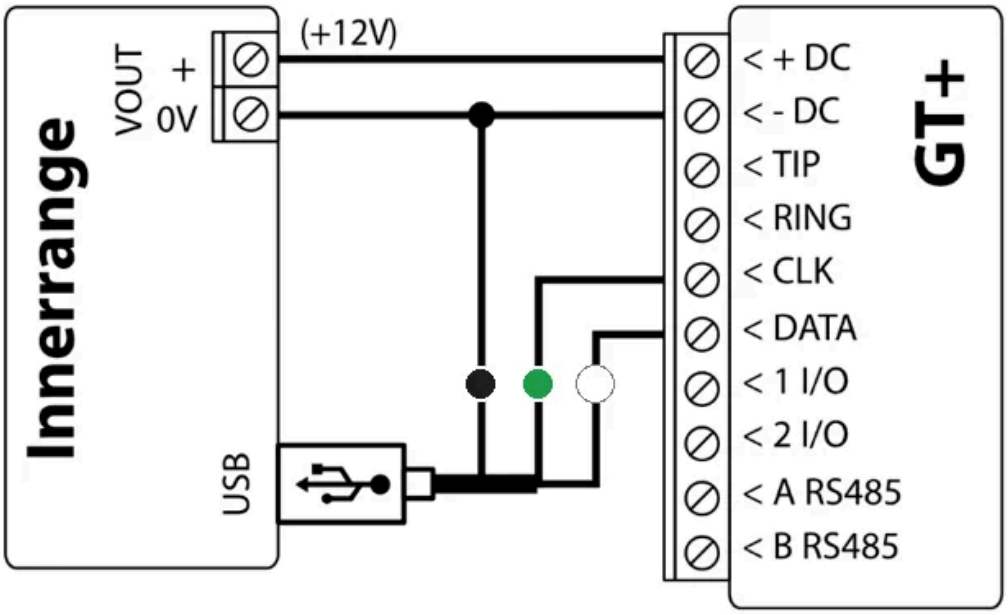


Figure 19. Connecting an InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; from the USB port with the 993030USB cable (“Cable, Inner Range part number 993030USB”) black → −DC, green → CLK, white → DATA.

- black wire (“Black wire”)
- green wire (“Green wire”)
- white wire (“White wire”)

3.3.8 InnerRange Integriti

The communicator connects to the **Port 0** serial port of the Integriti control panel with Inner Range's **INTG-996795** cable: **+DET (+13 V)** → **+DC**, **GND (5)** → **−DC**, **Rx (3)** → **CLK**, **Tx (2)** → **DATA**.

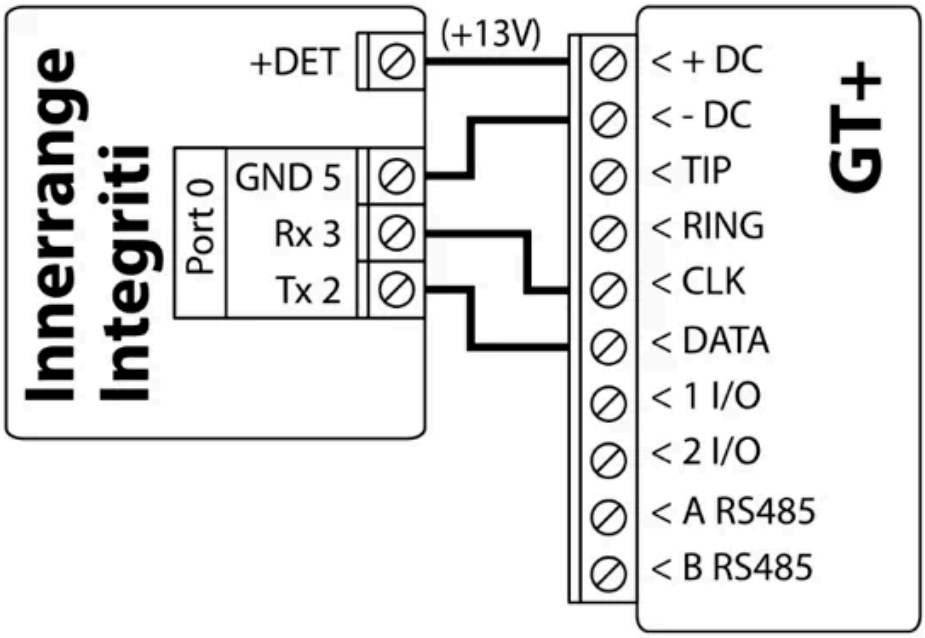


Figure 20. Connecting an InnerRange Integriti to Port 0 with the INTG-996795 cable (“Cable, Inner Range part number INTG-996795”): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.9 Honeywell Vista – data bus

Connect the keypad bus of the Honeywell Ademco Vista-15, Vista-20 and Vista-48 control panels from the control panel's terminals to the communicator: **5** → **+DC** (+12 V), **4** → **–DC**, **7** → **CLK**, **6** → **DATA**.

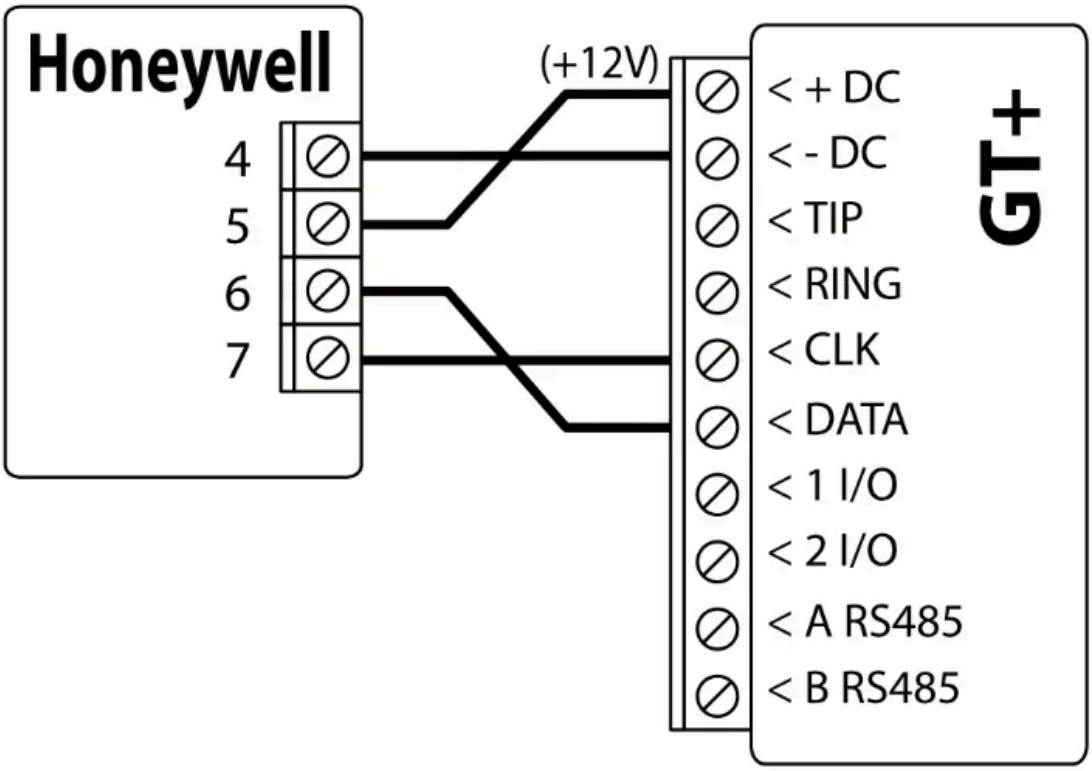


Figure 21. Connecting a Honeywell Vista-15 / -20 / -48 control panel on the data bus (“Keypad bus”): terminal 5 → +DC, 4 → –DC, 7 → CLK, 6 → DATA.

3.3.10 Any control panel – TIP/RING

Any other control panel can be connected through its telephone line dialer: power from the control panel's auxiliary power output (**+AUX** → **+DC**, **–AUX** → **–DC**), the telephone line output to the communicator's **TIP** and **RING** terminals (**TIP** → **TIP**, **RING** → **RING**). The control panel's dialer must be set up (section 4.2).

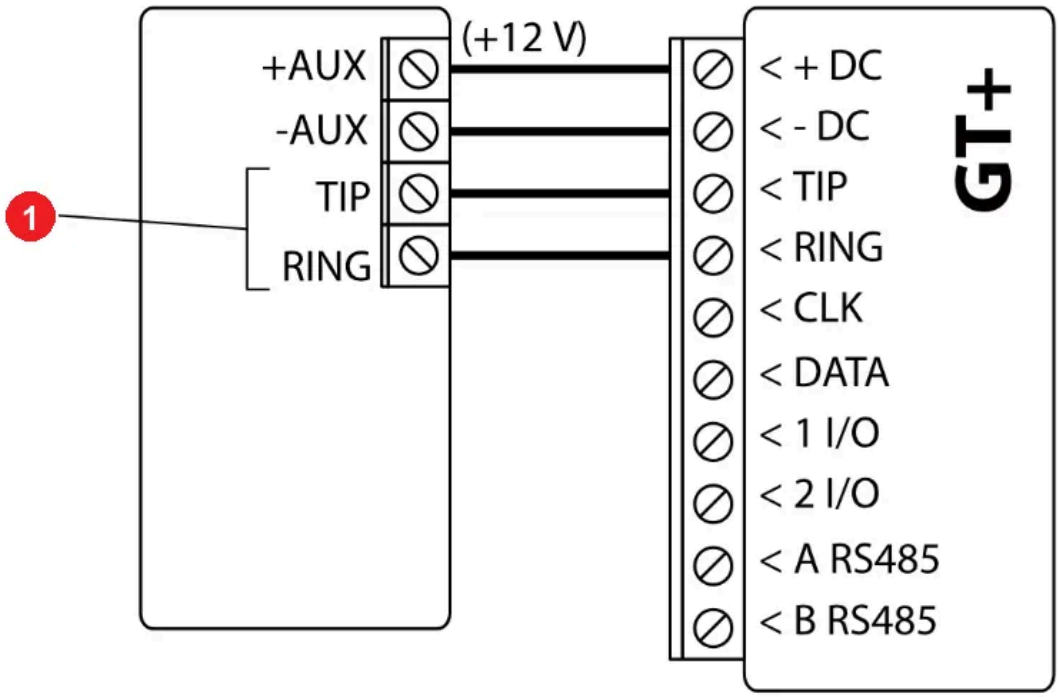


Figure 22. Connection to the control panel's (“Control panel”) telephone line dialer: +AUX → +DC, −AUX → −DC, TIP → TIP, RING → RING.

- 1 terminals of the control panel's telephone line dialer (“Telephone line communicator terminals”)

3.4 Connecting a keyswitch zone

If you want to arm and disarm the control panel from the Protegus 2 app so that the communicator's output (PGM) switches the control panel's **keyswitch zone**, follow this wiring. The communicator's two dual-function I/O terminals can be set as outputs (OUT, PGM), so the two outputs can control two partitions of the system: connect the keyswitch zone of partition 1 to the **1 I/O** terminal, and that of partition 2 to the **2 I/O** terminal. With this wiring, untick **Remote Arm/Disarm** on the **Panel settings** page of TrikdisConfig, set the terminals to the **OUT** function on the **IN/OUT** page (section 6.7), and in the Protegus 2 app assign the outputs to the partitions as described in section 5.2.

With data bus or serial wiring, the data connection between the control panel and the communicator remains (the communicator reads the events from the bus), and arming and disarming are done through the keyswitch zone:

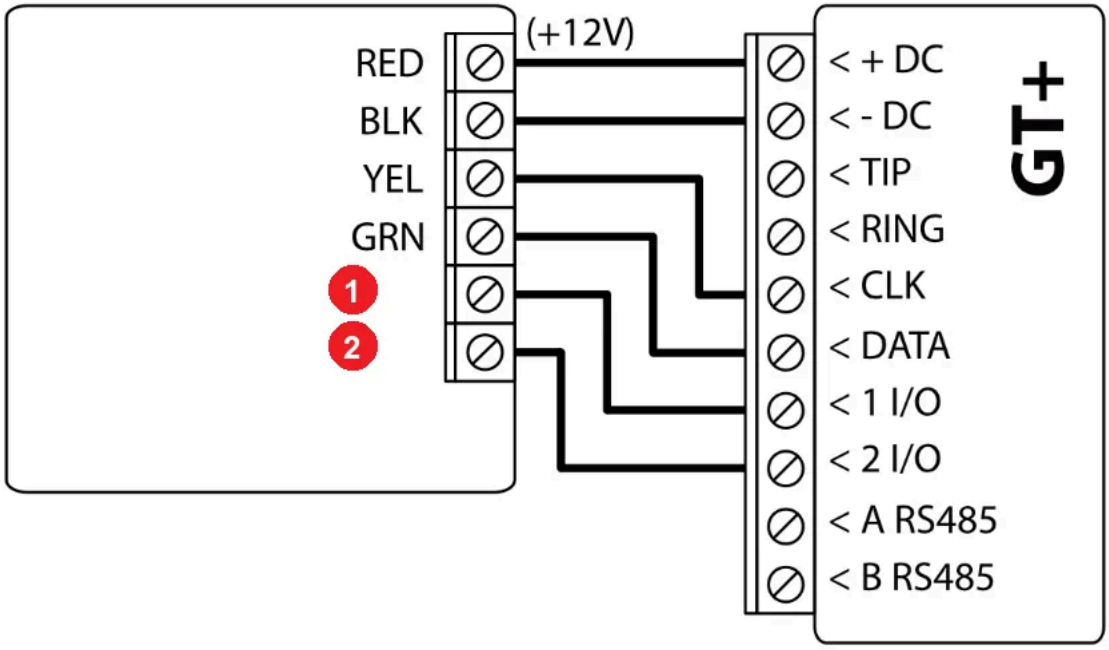


Figure 23. Arming and disarming with a keyswitch zone (“Zones (keyswitch)”), with data bus or serial wiring (“Keypad bus or serial”): the alarm control panel's (“Control panel terminals”) RED terminal → +DC, BLK → −DC, YEL → CLK, GRN → DATA; the zone of partition 1 → 1 I/O, that of partition 2 → 2 I/O.

- 1 keyswitch zone of partition 1 (“1-st Area”)
- 2 keyswitch zone of partition 2 (“2-nd Area”)

With telephone line (TIP/RING) wiring, the control panel sends the events on its dialer, and arming and disarming are done through the keyswitch zone in the same way:

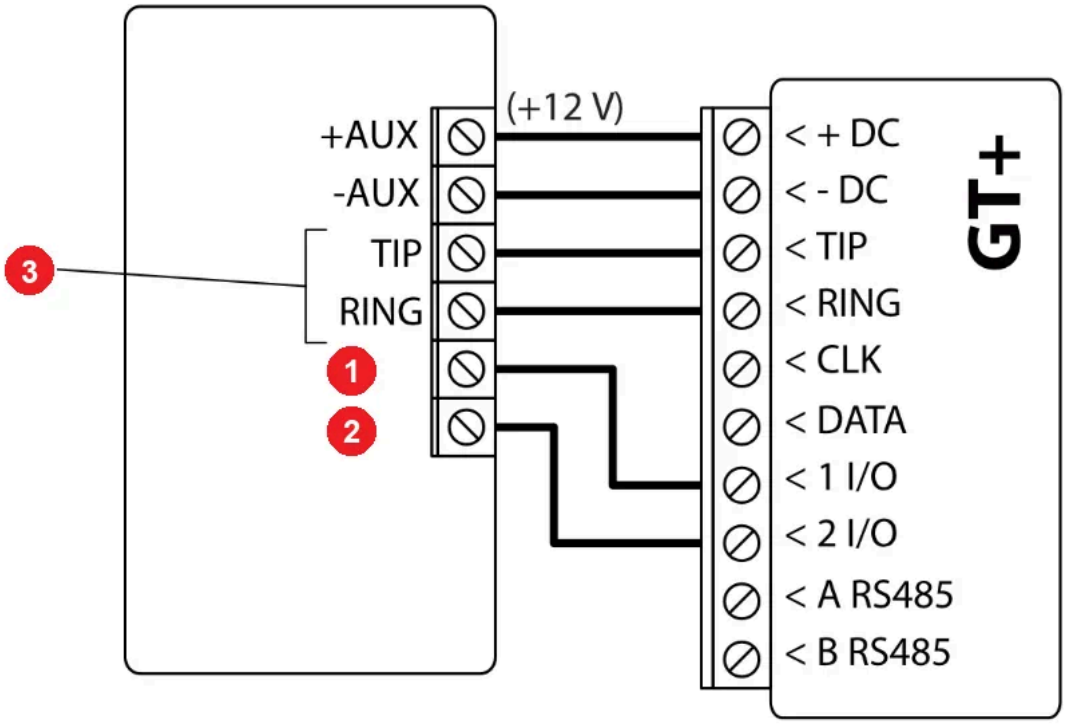


Figure 24. Arming and disarming with a keyswitch zone (“Zone (keyswitch)”), with telephone line wiring: the alarm control panel's (“Control panel”) +AUX terminal → +DC, −AUX → −DC, TIP → TIP, RING → RING; the zone of partition 1 → 1 I/O, that of partition 2 → 2 I/O.

- 1 keyswitch zone of partition 1 (“1-st Area”)
- 2 keyswitch zone of partition 2 (“2-nd Area”)
- 3 terminals of the control panel's telephone line dialer (“Telephone line communicator terminals”)

The keyswitch zone can be pulsed or two-state (level) – the same mode must be set in the Protegus 2 app (section 5.2). A separate article covers the details and pitfalls of keyswitch arming: Remote arming with a keyswitch from the Protegus 2 app.

3.5 Connecting inputs

The communicator's two dual-function I/O terminals can also be used as inputs (IN) to receive additional sensors (e.g. tamper switch, panic button), independently of the alarm control panel. NO, NC, NO/EOL, NC/EOL, NO/DEOL or NC/DEOL circuits can be connected to the input; the default for both terminals is input, NO. You set the input type on the **IN/OUT** page of TrikdisConfig, in the **Type** field. The input must be connected between the chosen I/O and the **−DC** (COM) terminal, according to the chosen type.

The inputs accept the following circuit types: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. The end-of-line resistor is **2.2 kΩ**. With a single end-of-line resistor (EOL), both a short circuit and an open circuit count as an alarm; with double end-of-line resistors (DEOL), the two resistors allow the alarm and the tamper (short or open circuit) to be recognised separately. The factory setting is NO (normally open); you set the input type on the **IN/OUT** page of TrikdisConfig, according to the wiring.

Type	Normal state	Alarm	Tamper
NC	closed	open	–
NO	open	closed	–
NC/EOL	2.2 kΩ	open or short circuit	–
NO/EOL	2.2 kΩ	short or open circuit	–

Type	Normal state	Alarm	Tamper
NC/DEOL	2.2 kΩ	3.3–5.5 kΩ (2 × 2.2 kΩ)	open or short circuit
NO/DEOL	3.3–5.5 kΩ (2 × 2.2 kΩ)	2.2 kΩ	open or short circuit

When the input is triggered, the communicator sends its own event to the monitoring station and to Protegus 2; you can set the event's Contact ID code, partition and zone number on the **IN/OUT** page.

Connecting input circuits between the COM and the INx point: NO, NC, NC/EOL, NO/EOL, and with tamper detection NO/DEOL and NC/DEOL, with 2.2 kΩ end-of-line resistors; the individual states (short circuit, open circuit, 2.2 kΩ, 3.3–5.5 kΩ) are explained by the table in section 3.5.

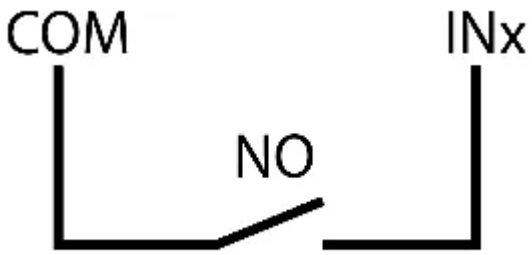


Figure 25. NO – normally open circuit: closed – alarm, open – normal state.

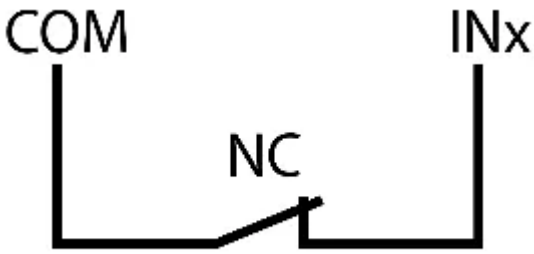


Figure 26. NC – normally closed circuit: open – alarm, closed – normal state.

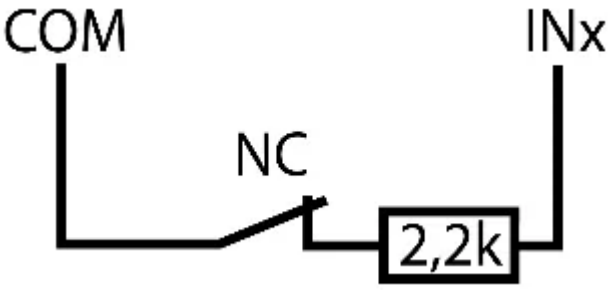


Figure 27. NC/EOL – normally closed circuit with a 2.2 kΩ end-of-line resistor: short circuit or open circuit – alarm, 2.2 kΩ – normal state.

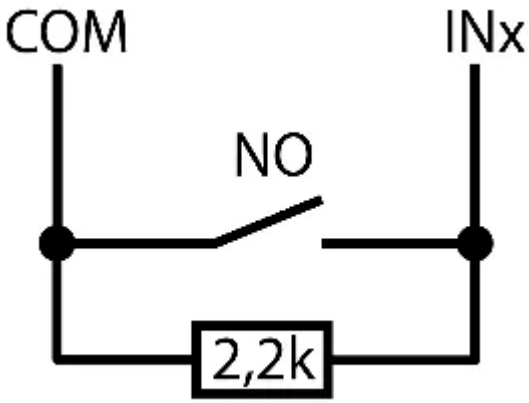


Figure 28. NO/EOL – normally open circuit with a 2.2 kΩ end-of-line resistor: short circuit or open circuit – alarm, 2.2 kΩ – normal state.

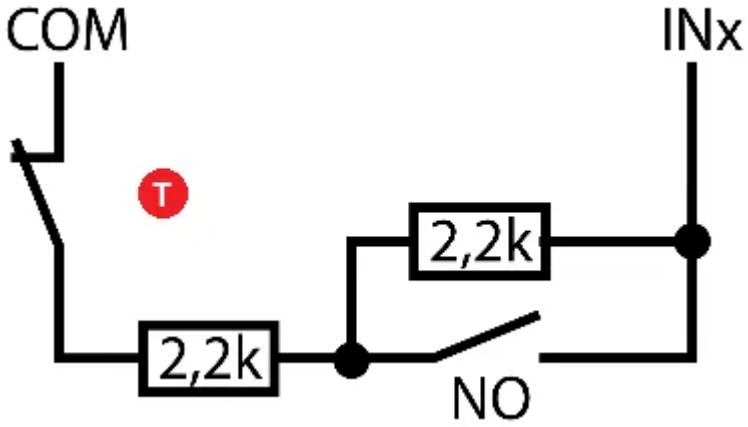


Figure 29. NO/DEOL – normally open circuit with a 2.2 kΩ end-of-line resistor and tamper detection: short circuit or open circuit – tamper, 2.2 kΩ – alarm, 3.3–5.5 kΩ – normal state.

- T tamper contact (“Tamper”), signals opening of the detector's housing

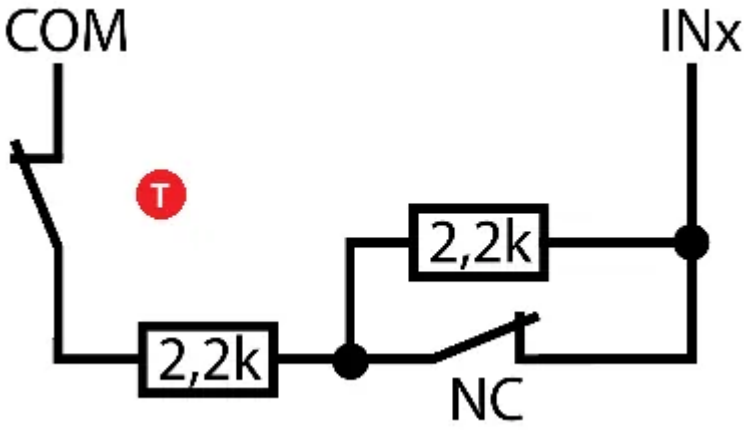


Figure 30. NC/DEOL – normally closed circuit with a 2.2 kΩ end-of-line resistor and tamper detection: short circuit or open circuit – tamper, 2.2 kΩ – normal state, 3.3–5.5 kΩ – alarm.

- T tamper contact (“Tamper”), signals opening of the detector's housing

If you need more inputs or outputs, connect a Trikdis **iO-8** expander to the communicator (section 3.7); its wiring is also described in the iO-8 manual.

3.6 Connecting an output with a relay

As outputs, the I/O terminals are open-collector (OC) outputs: in the active state they pull the connected load to negative, with at most 0.15 A, up to 30 V DC. With the contacts of a relay you can switch various electrical devices on and off: one end of the relay coil goes to **+DC**, the other to the **x I/O** terminal, and the load is switched by the relay contacts (NC, C, NO). The I/O terminal used must be set to output (**OUT**) on the **IN/OUT** page of TrikdisConfig.

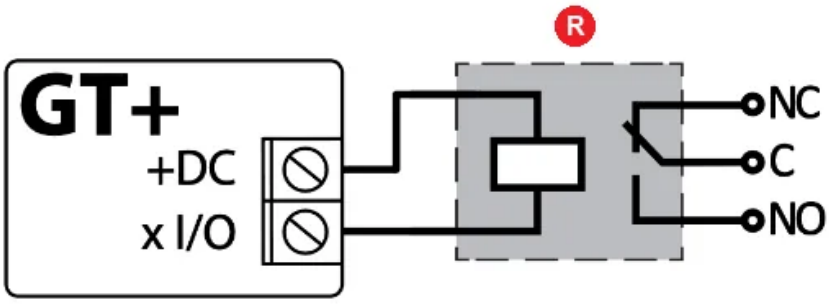


Figure 31. Connecting a relay to the communicator's output: the coil goes between +DC and the x I/O terminal, the contacts (NC, C, NO) switch the load.

- R relay (“Relay”)

You can switch the outputs from the Protegus 2 app or by SMS command (chapter 5).

3.7 Connecting an iO-8 expander

If you need more inputs or outputs, up to four **iO-8** expanders can be connected to the communicator's RS485 bus; each gives 8 additional dual-function I/Os. Connect the **A 485** and **B 485** terminals to the module's **A (RS485)** and **B (RS485)** terminals; both the communicator and the expander get their power from the control panel's auxiliary power output (**+AUX** → **+DC**, **−AUX** → **−DC** on both devices). The expander must be added and set up on the **RS485 modules** page of TrikdisConfig (section 6.8).

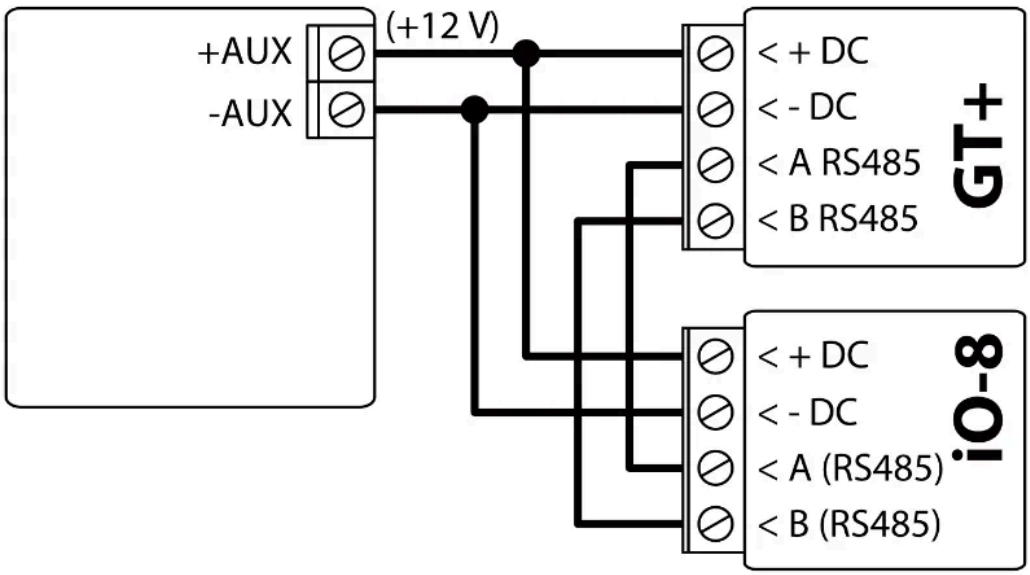


Figure 32. Connecting an iO-8 expander to the communicator's RS485 bus; power from the alarm control panel's (“Control panel”) AUX output, to both devices.

3.8 Switching on and first check

A TRIKDIS átjelző elindítása

1. SIM kártyás átjelző esetén a SIM kártyát az elindítás előtt helyezd be a készülékbe.
2. Ethernetes eszköz esetén az Ethernet kábelt elindítás előtt vagy utána is csatlakoztathatod
3. Az indításhoz húzd ki az USB kábelt és csatlakoztasd a lehúzott sorkapcsot

Akkor léphetsz tovább a következő fejezetre, ha az eszköz megfelelően elindul és nem jelez hibát.

- A Power LED zölden világít
- A Trouble LED nem villog pirosan
- A Network LED zölden világít (ha közben sárgán villog az rendben van)
- Ha Data LED nem alszik ki, az azt jelenti, hogy az eszköz nem tud elküldeni valamilyen eseményt. Ez internet / adat kapcsolat hibára utal.

After wiring, the communicator also starts when the alarm control panel's power is switched on. On the front cover you should see this:

- **POWER** steady green – the power supply is OK;
- **NETWORK** steady green and flashing yellow – connected to the network; the number of yellow flashes is the signal level: on 4G 3 flashes is good; if you count fewer, the signal is weak: find another place for the communicator, or use a more sensitive antenna (section 3.2);
- **TROUBLE** off.

If TROUBLE is flashing, the number of flashes tells you the cause (section 1.6); any other LED indication also signals some fault – look up the cause in the tables in section 1.6. If none of the LEDs is lit, check the power supply and the wiring.

4. Programming the alarm control panel

How the control panel is set up depends on how you wired it: over the data bus or serial port (section 4.1), or through its telephone line dialer, on the TIP/RING terminals (section 4.2). With the GT+, the DSC Keybus + TIP/RING wiring needs both: the settings of the Keybus wiring and the programming of the control panel's dialer (section 4.1.1).

4.1 Data bus or serial wiring

Here we describe how the control panel must be set up so that the communicator reads its events and can control it remotely. For remote control, the **Remote Arm/Disarm** option must be ticked on the **Panel settings** page of TrikdisConfig (section 2.2).

4.1.1 DSC

DSC PowerSeries panels (the list of supported models is in section 1.2) do not require any special settings: the communicator connected to the Keybus reads the events immediately, and once **Remote Arm/Disarm** is ticked, the user arms and disarms from the app with their own keypad code. The details of direct control – zone states, zone bypassing, automatic detection of partitions – are covered in a separate article: Direct control for DSC PowerSeries alarm panels.

The communicator does not work with **DSC PowerSeries NEO** panels: the manufacturer does not allow external devices on the NEO bus. For NEO, use a telephone-line (TIP/RING) communicator – see DSC Power Series NEO and Trikdis communicators: compatibility and solutions.

GT+, Keybus and TIP/RING wiring (section 3.3.2): the control panel's telephone line dialer must be programmed to send the events. The table below applies to the DSC PowerSeries PC1616 (PC1832, PC1864) control panel. On the keypad connected to the control panel, enter programming: **[*][8][installer code]**, then enter the section number.

Section	Value
[301] First telephone number	Any number longer than four digits, **without D** at the beginning (for example `5555555`). D means waiting for the dial tone; without it the control panel dials faster. The communicator answers every call
[310] System account code	The 4-digit object ID, followed by `FF` (for example `1234FF`). Use HEX `A` instead of the digit 0
[311] Account code of partition 1	The 4-digit object ID; HEX `A` instead of 0
[350] Communicator format	`03` (Contact ID) for telephone number 1
[351]–[376] Communicator call directions	Enable the required event groups for telephone number 1: Alarm/Restore, Opening/Closing, Tamper Alarm/Restore, System Maintenance, Test Transmissions. Check the Opening/Closing group separately: on some DSC control panels it is switched off by default
[380] Communicator option 1	Option 1 **ON** (communicator enabled); option 3 **OFF** (DTMF dialing)
[381] Communicator option 2	Option 7 **OFF** (the control panel generates the Contact ID reporting codes automatically)
[320]–[349] Reporting codes	Any value for the events to be reported, just not `00`
[015] System option 3	Option 7 **OFF** (telephone line monitoring, TLM, switched off)

Switch off telephone line monitoring (TLM): if it stays switched on, the control panel may signal a telephone line fault. You set the TLM fault delay in section **[377]**.

The section numbers above apply to the PC1616, PC1832 and PC1864 control panels (installation manual v4.x). With other DSC models the section numbers may differ – check the control panel's programming manual.

4.1.2 Paradox

Paradox panels only need to be programmed for direct control; nothing needs to be set for reading the events. The panel's firmware must be at least **V.4**.

On newer Paradox panels (for example the SP+, MG+ and EVOHD+ series), the serial port may be **locked from the factory**: the communicator receives no data until the port is unlocked. How to unlock it: Unlocking the locked serial port on Paradox alarm panels.

For control, the panel's **PC password** must be set, and the same must be entered in the **System settings** → **Security panel PC download password** field of TrikdisConfig – the two must match.

1. Enter the panel's installer programming on the keypad.

2. Open the PC password section: section **911** for the **MAGELLAN and SPECTRA** series, section **3012** for the **DIGIPLEX EVO** series.
3. Enter a **4-character** password. The password cannot be 0000 and **must not start with zero**.
4. Exit programming and **restart the panel** – a change of the PC password takes effect after a restart. Then enter the same password in TrikdisConfig.

Typical problems and their solutions

- The **keypad code assigned to the partition cannot be the master code**: give the user another code, and with that, arming / disarming from Protegus 2 will work.
- **Restart the communicator after any keypad code change** (power cycle or `RESET` SMS command): it reads the codes at start-up and does not see later changes.

On the GT and GT+ communicators, the **Security panel PC download password** field is on the **Panel settings** page of TrikdisConfig, in the **Serial bus** group (sections 2.2 and 6.3).

Keybus and TIP/RING wiring (SP / SP+ / MG / MG+, section 3.3.4): in addition, the control panel must be programmed to send the events to the monitoring station and to be controllable from Protegus 2:

Section	Value	Section	Value
801	`********`	**815**	`123456`
811	`1111`	**911**	`1234`
812	`2222`		

4.1.3 Texecom

Texecom Premier / Premier Elite panels must be programmed both for reading events and for control: you need to set the panel's 4-character password called **UDL passcode**, and enter the same in the **System settings** → **Security panel PC download password** field of TrikdisConfig – the two must match.

With Texecom's Wintex software: the UDL passcode is on the **Options** tab of the **Communication Options** window.

From the keypad:

1. Enter the 4-digit installer code and press **[Menu]** to enter the programming menu.
2. Immediately afterwards, press **[9]**.
3. Press **[7][6]**, then **[2]**, and enter the 4-digit UDL passcode.
4. Press **[Yes]**, then exit programming with the **[Menu]** button.

On the GT and GT+ communicators, the **Security panel PC download password** field is on the **Panel settings** page of TrikdisConfig, in the **Serial bus** group; the UDL passcode must match it.

4.1.4 UTC Interlogix (Caddx)

The firmware of the **UTC Interlogix (Caddx) NetworX** panel must be at least **V2**. The following must be set on the panel's keypad:

1. Press **[*][8]** and enter the installer code (default **9713**).
2. Enter the **device number** (device address) assigned to the communicator (default **0**).

3. Program the rows of the table below one after the other: enter the location, the segment number and then the setting. You can go back to the previous field with the **[*]** button. `12345678` means that all eight switches of the segment are on (all digits are visible on the display).

Location	Segment	Setting
23	3	12345678
37 (not strictly necessary)	3	12345678
37 (not strictly necessary)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

4. When you have programmed all rows, press **[Exit]** twice to leave programming.

4.1.5 InnerRange

The firmware of the **InnerRange Inception** panel must be at least **2.3.0.3507-r0**, and the panel needs an internet connection. The settings are made in the panel's web interface:

1. Open `https://skytunnel.com.au/inception/SERIALNUMBER` in a browser, where SERIALNUMBER is the serial number on the panel's box. Log in with the installer account.
2. Open the **Configuration** → **General** → **Alarm Reporting** page.
3. In the **3rd Party Device Configuration** group: - tick **Enable 3rd Party Device Reporting**; - in the **3rd Party Device Type** field, select **Trikdis**; - in the **Serial Port** field, select **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Save the settings and log out of the interface.

The firmware of the **InnerRange Integriti** panel must be at least **19.1.0.36608**, and its programming software (Integriti Professional) at least **19.1.0.15396**. The settings are made in the panel's programming software:

1. For the serial port (**TTL Port-0**) to which the communicator is connected, select the **Trikdis** communication protocol.
2. The data format must be **Contact ID**.
3. Port settings: **19200, 8, N, 1**.
4. Save the settings and exit the program.

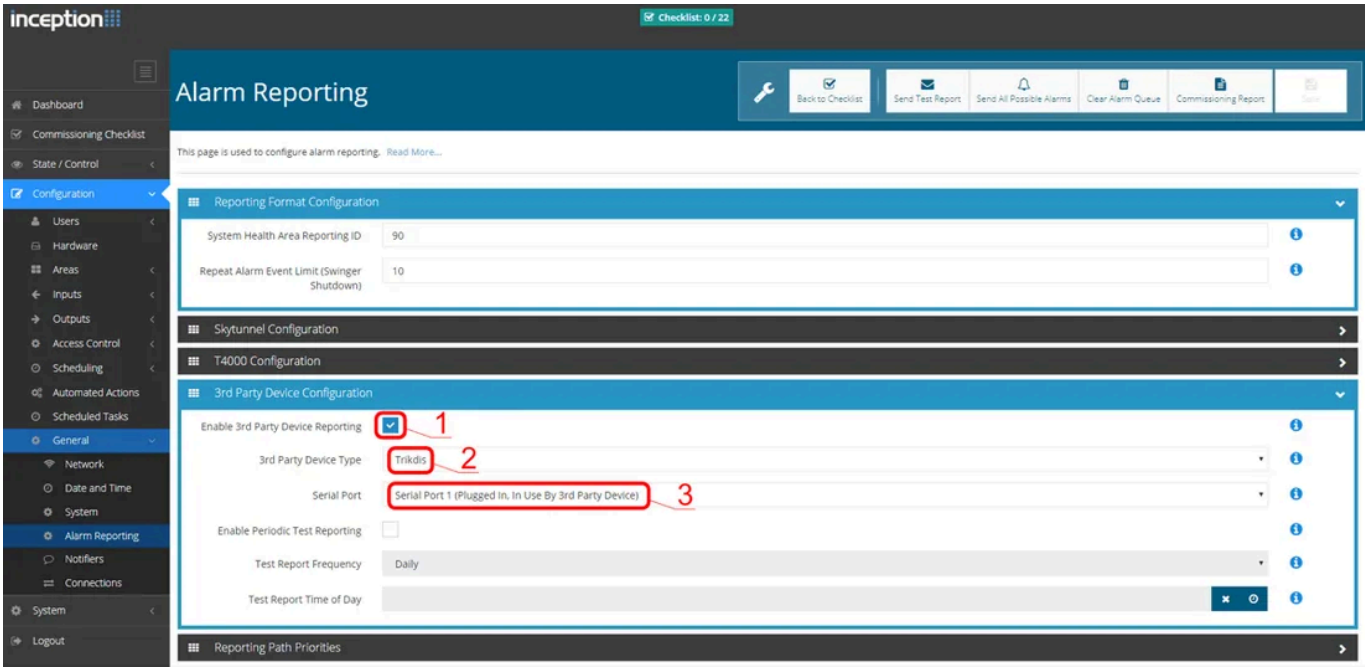


Figure 33. InnerRange Inception – Configuration → General → Alarm Reporting, 3rd Party Device Configuration group: Enable 3rd Party Device Reporting ticked, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

4.1.6 Honeywell Ademco Vista

The firmware of the **Honeywell Ademco Vista-20** and **Vista-48** panels must be at least **V5.3**. The settings are made on the panel's keypad.

Entering programming – in two ways:

- enter the installer code (default **4112**), then press **[8][0][0]**; or
- power up the panel and **within 50 seconds** press the **[*]** and **[#]** buttons at the same time (this only works if programming was previously exited with [*][9][8]).

Settings:

1. Enable sending Contact ID events on the long range radio (LRR) output: press **[*][2][9][1][#]**.
2. For remote control, enable the use of the **2nd AUI address**: press **[*][1][8][9][1][1][#]**.

Exiting programming: press **[*][9][9]**.

4.2 Telephone line (TIP/RING) wiring

For the alarm panel to send events on its telephone-line output, the panel's dialler must be enabled and configured. You will find the exact program addresses in the panel's installation manual; the essence of the setting is the same for every manufacturer:

1. **Enable the telephone-line (PSTN) communicator** in the panel.
2. **Enter `1234` as the telephone number** of the monitoring receiver – whether the communicator is connected to the panel's RING/TIP terminals or to the telephone line. With another number it can happen that the panel dials but the communicator still does not receive the events: with a DSC PowerSeries NEO panel, too, reporting only started after the number was changed to `1234`.
3. **Dialling mode:** DTMF (tone), not pulse.
4. **Protocol:** Contact ID.

If you want to arm and disarm the panel remotely with the communicator's output, the zone wired to the output must be set as a **keyswitch zone** in the panel.

The keyswitch zone can be pulsed or latched (two-state). By default, the communicator's output gives a 3-second pulse; you can change the pulse length or switch to latched mode in the settings of the Protegus 2 app.

The DSC, Paradox, Caddx, Texecom, InnerRange and Honeywell control panels can also be connected to the communicator through their telephone line output (section 3.3.10) – in this case their dialer must be set up as well, and direct control is not available.

4.2.1 Programming the Honeywell Vista dialer

Enter programming mode on the keypad and set the following program addresses:

Program address	Setting
`*41`	the telephone number of the monitoring receiver: `1234`
`*43`	the panel's account number
`*47`	Tone dial = `1`, and the number of dialling attempts
`*48`	`7` (default)
`*49`	`5` (Split/Dual message)
`*50`	delay before sending a burglary alarm – default `2,0` (30 s); for immediate sending `0,0`

For a **Honeywell Vista 48** panel, also set the following program addresses:

Program address	Value	Program address	Value	Program address	Value
`*41`	1234 (receiver telephone number)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1
`*43`	1234 (account number)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1
`*45`	1111	`*64`	1	`*73`	1
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

At the end of programming, exit programming mode with the `*99` command.

4.2.2 The UTC Interlogix (Caddx) NX dialer

Programming the Interlogix NX-4V2 (NX-6V2, NX-8V2) control panel when the communicator is connected to the control panel's TIP/RING terminals. On the keypad, enter the following one after the other:

Location	Keys	Note
	`*89713`	Enter programming (`9713` is the default installer code)

Location	Keys	Note
	`0#`	
Location 0	`0#`	
Location 0	`1 2 3 4 #`	
Location 1	`1#`	
Location 1	`1 2 3 4 #`	
Location 2	`2#`	
Location 2	`1*#`	
Location 4	`4#`	All zone LEDs lit (segment 1)
Location 4	`12345678*`	All zone LEDs lit (segment 2)
Location 4	`12345678*#`	
Location 23	`23#`	All zone LEDs lit (segment 3)
Location 23	`**`	All zone LEDs lit (segment 3)
Location 23	`12345678*#`	All zone LEDs lit (segment 3)
Location 37	`37#`	All zone LEDs lit (segment 3)
Location 37	`**`	All zone LEDs lit (segment 4)
Location 37	`12345678*`	
Location 37	`12345678*#`	
	`EXIT` `EXIT`	Exit programming

5. Remote control with the Protegus 2 app

With the Protegus 2 mobile and web app the user sees the state of the system remotely, receives notifications about the events, can arm and disarm, and can switch the communicator's outputs. The app can be downloaded for Android and iOS (Google Play, App Store), or used from a browser: web.protegus.app. Log in with your user name and password, or register a new account.

5.1 Adding the device

Before adding the device, check:

1. The SIM card is active, and mobile data works on it; its PIN code is entered in the device, or the PIN request is switched off.
2. On the **User reporting** → **PROTEGUS Cloud** tab of TrikdisConfig, **Enable connection** is ticked (section 6.5).
3. The **POWER** LED is steady green.
4. The **NETWORK** LED is steady green and flashing yellow (the device is on the network).

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

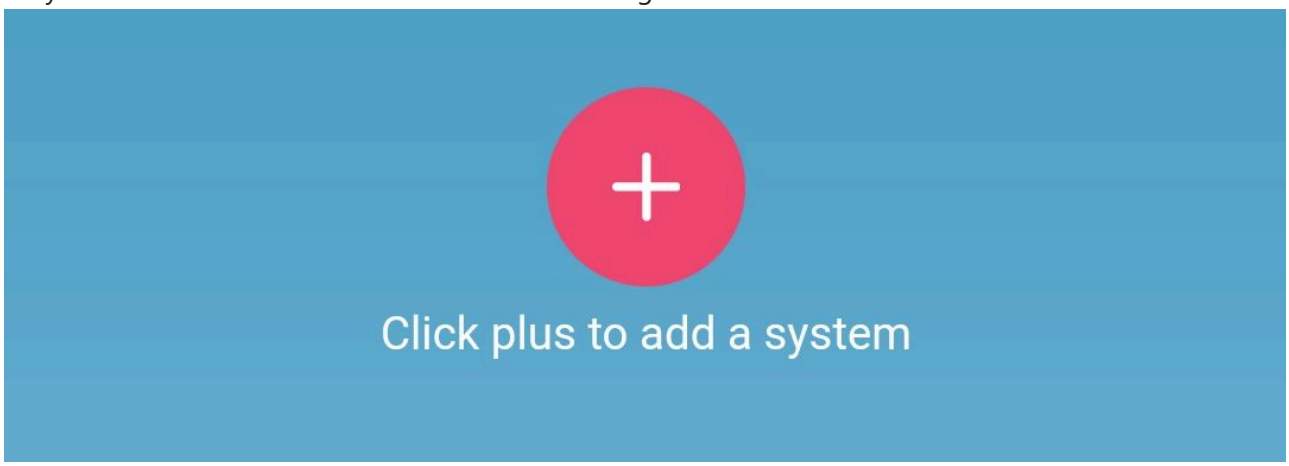
device, that the connection up to the router is alive – but not that the device can also reach the internet. If the NETWORK LED is green but the DATA LED stays lit continuously even after an event or test report, the internet connection is not working: the message cannot be sent. On a mobile network 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

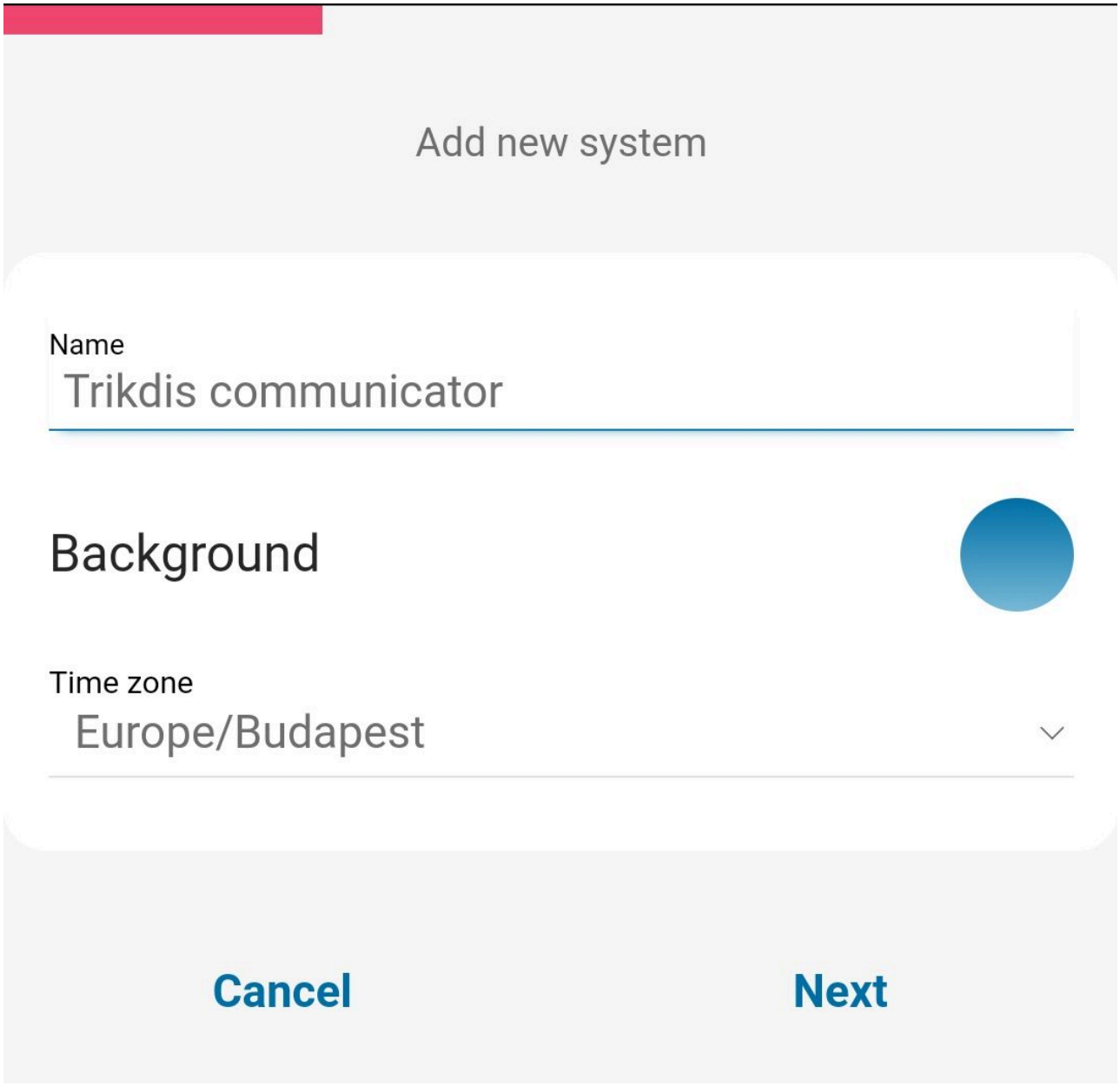


5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz

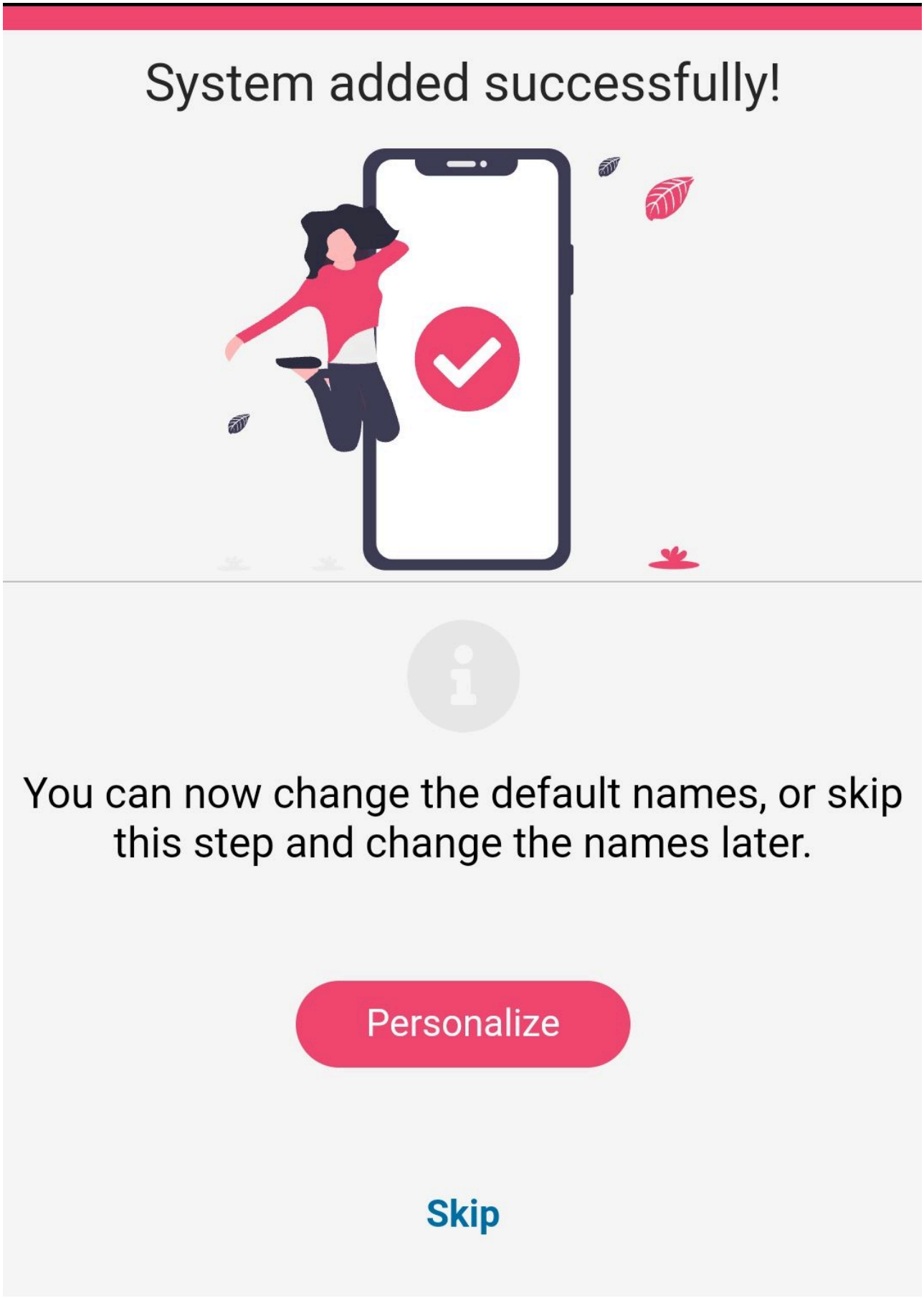
- Az eszközön található matricán
- Az eszköz papírdobozán
- A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



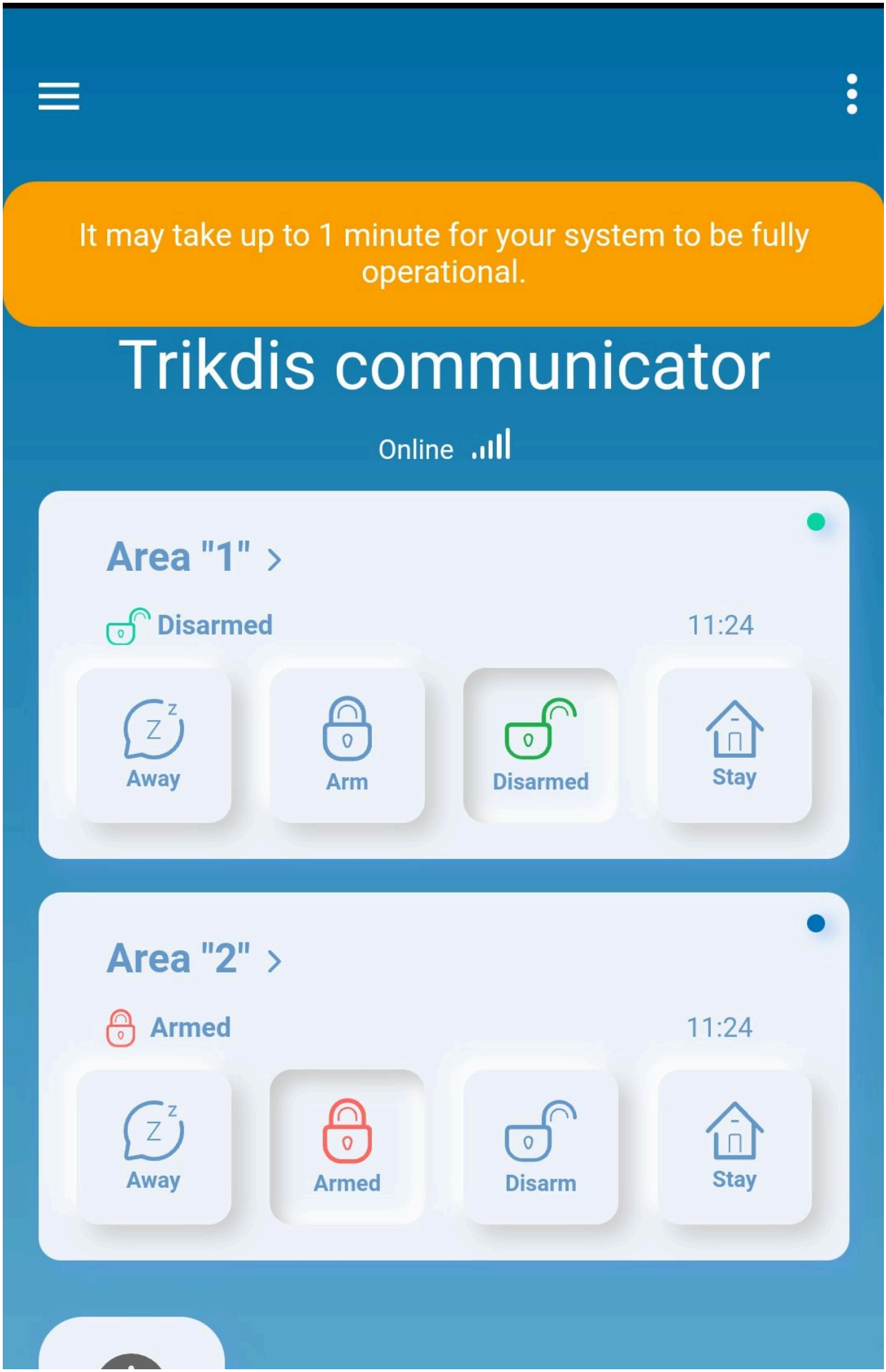
6. Add meg a rendszer nevét és válassz idozónát



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

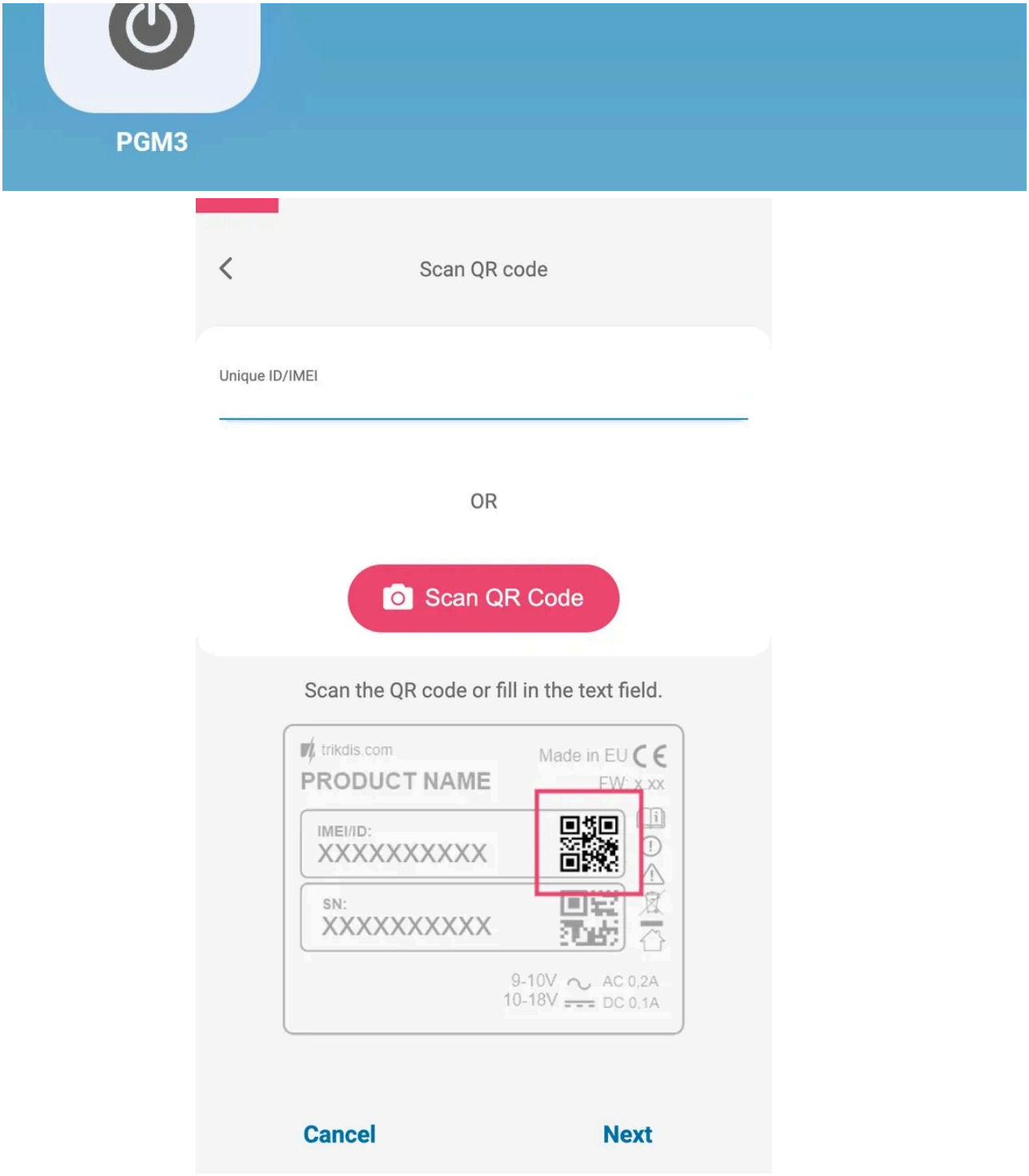


Figure 34. Protegus 2 – adding a new system: type the IMEI / Unique ID or scan the QR code on the label, then Next.

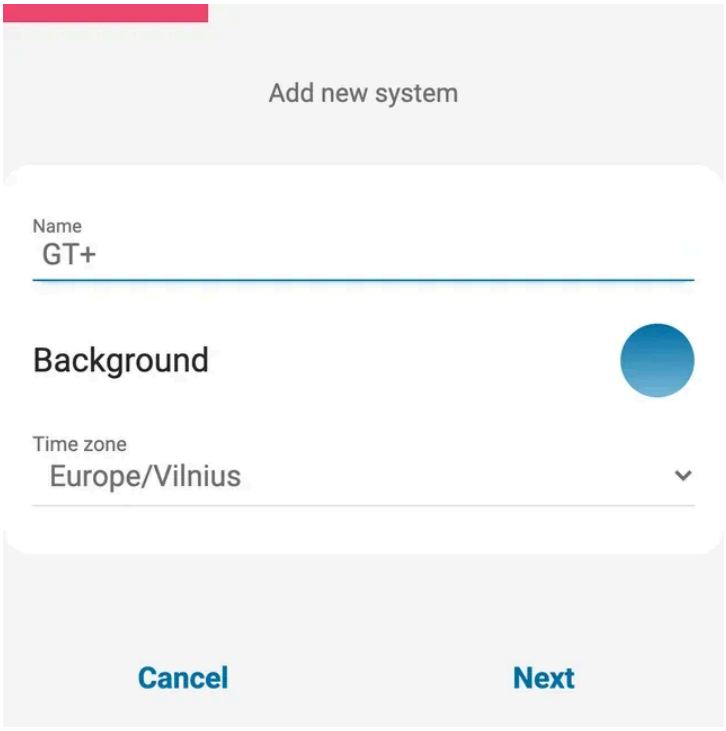


Figure 35. Protegus 2 – entering the system's name (Name), then Next.

The device's unique identifier (**IMEI / Unique ID**) can be read on the device label and on the sticker on the box, and the TrikdisConfig status bar also shows it. If the **PROTEGUS Cloud access Code** in the device is not the default one, the app asks for it when adding.

5.2 Arming and disarming with an output

If you want to arm and disarm the alarm panel with the communicator's output, through the panel's keyswitch zone, specify in the Protegus 2 app for the partition which output controls it.

The panel zone to which the communicator's output is connected must be programmed as a **keyswitch zone** in the panel, and the panel must report the arming and disarming events – Protegus 2 shows the partition state based on these.

You can make the setting when creating the system, while adding the partitions, or later in the system settings, when editing the partition. When creating the system, the Protegus 2 wizard guides you through: click **Continue**, enter the partition name (**Area name**) and enable control of the PGM output from the Protegus 2 app – this is done with the following steps:

1. Select (or add) the partition you want to control. The partition number must match the one the panel sends in its events (partition 1 as 1, partition 2 as 2).
2. Switch on **Control with Protegus2** (control with PGM), and in the **Assigned Output** field select the communicator output (PGM1, PGM2 …). One output can control only one partition.
3. Select the operating mode: **Pulse** or **Level** (latched) – the same one you set for the keyswitch zone in the panel. Typically we use pulse; the pulse length can also be set (default 3 s).
4. Save the setting (**Save**). With several partitions, repeat this for each one with its own output: in the wizard you add a further partition with the **Click to add an area** button and set its PGM output in the same way. When you have set up all partitions, move on in the wizard with the **Skip** button.

Protegus 2 can only show the state of the partitions correctly if the panel sends the arming and disarming events with the correct partition number. The details and pitfalls of keyswitch arming are covered in a separate article: Remote arming with a keyswitch from the Protegus 2 app.

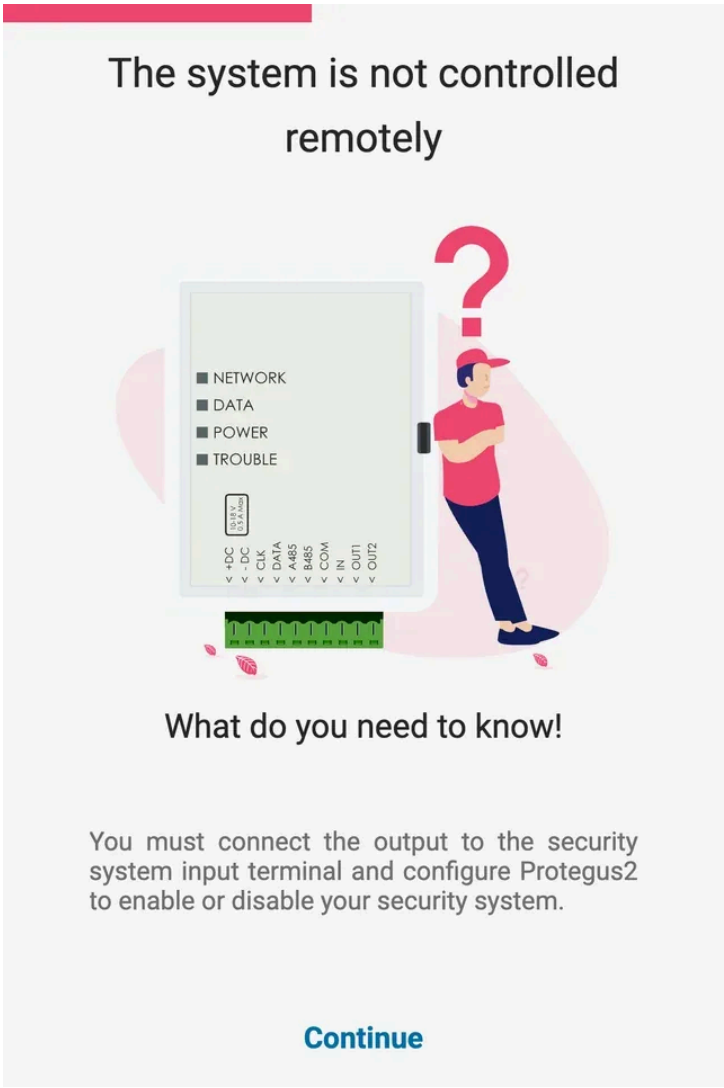


Figure 36. Protegus 2 – the “We do not control the system remotely” page when creating the system: with the Continue button you go on to setting the partition and the PGM output.

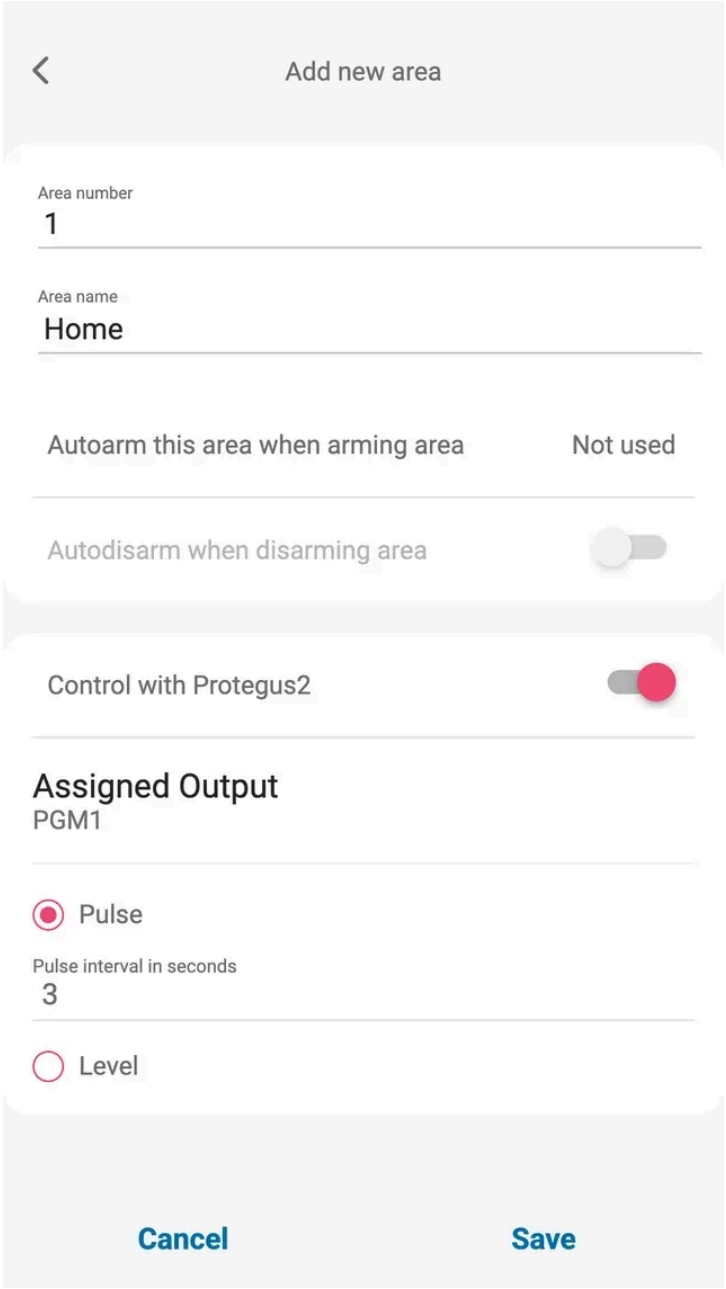


Figure 37. Protegus 2 – adding a partition (Add new area): Area number, Area name, Control with Protegus2 switched on, Assigned Output PGM1, Pulse (3 s) or Level, then Save.

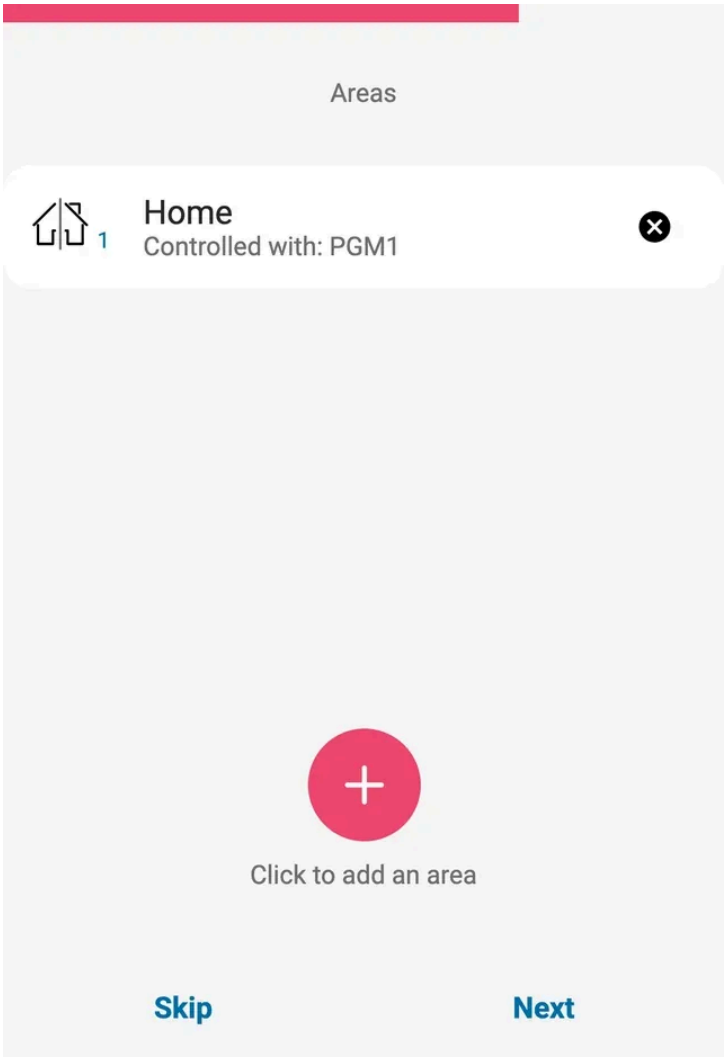


Figure 38. Protegus 2 – the list of partitions (Areas): the Home partition is controlled by PGM1; another partition can be added with the Click to add an area button, and the wizard can be closed with the Skip button.

5.3 Arming and disarming from the app

1. Open the system in the Protegus 2 app. On the home screen every partition has its own card and padlock: a **closed, red padlock** means an armed partition, an **open, green padlock** a disarmed one.
2. Tap the partition's padlock and select the required action: arm or disarm.
3. If the app asks for it, enter the PIN code.

The padlock takes on the actual state in response to the event received from the alarm panel; the app also confirms in the event list and in a notification whether the panel has carried out the action.

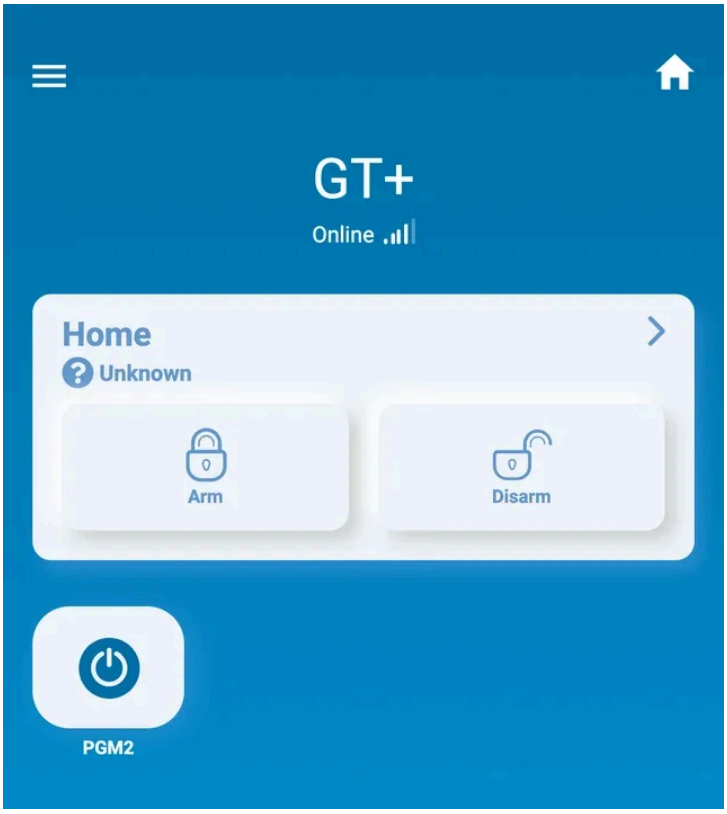


Figure 39. Protegus 2 – the system's home screen: the partition's state, the Arm and Disarm buttons, and below them the switchable PGM output.

5.4 Control by SMS messages

The communicator can also be controlled by SMS commands. Structure of the message: `Password Command Data` (separated by spaces). As the password, you can use the **administrator** code (default `123456`) for the `INFO`, `RESET` and `OUTPUTx` commands, and the **installer** code (default `654321`) for the `INFO` and `OUTPUTx` commands.

Command	Data	What it does	Example
`INFO`	–	Requests information about the device. The reply: the device type, IMEI number, serial number and firmware version.	`123456 INFO`
`RESET`	–	Restarts the device (with the administrator code only).	`123456 RESET`
`OUTPUTx`	`ON`	Switches output x on (x = 1 or 2).	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Switches output x off.	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Switches the output on in pulse mode for the given time; `tttt` is the pulse length in seconds, in four digits.	`123456 OUTPUT2 PULSE=0002`

The output can only be switched if the given I/O terminal is set to output (**OUT**) on the **IN/OUT** page of TrikdisConfig. You can restrict which phone numbers the device accepts commands from on the **User reporting** → **Control by SMS** tab (section 6.5).

6. TrikdisConfig – the settings in detail

On the left side of the TrikdisConfig window you see the list of pages (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, RS485 modules, Event summary, Firmware), at the top the button bar (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), and at the bottom the status bar. This chapter goes through the settings of the GT and the GT+ page by page; where the two versions differ, we point it out separately.

6.1 The status bar

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

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

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



Figure 40. The TrikdisConfig status bar with a GT+ read out: identifier, state, type (Device: GT+_M150), serial number, versions, connection mode and access level.

The **Device** field must show the type designation GT for the GT, and GT+ for the GT+ (in the picture GT+_M150; the letter-and-number suffix indicates the hardware version). After **Read [F4]** the program reads out and shows the values set in the device; make the necessary settings as described in the page descriptions below.

6.2 System settings

The page consists of two groups: in the **General** group you set the device's identifiers, in the **Access** group the access levels.

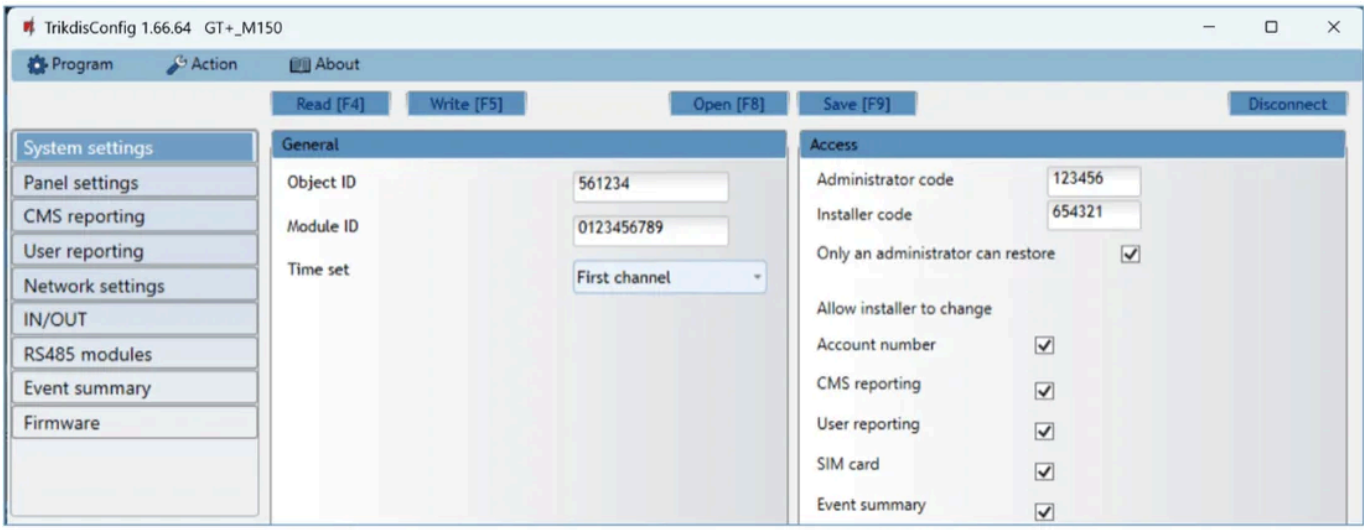


Figure 41. TrikdisConfig – System settings page: General and Access groups.

- **Object ID** – the object ID received from the monitoring station (6 hexadecimal characters: 0–9, A–F; `FFFE` and `FFFF` cannot be used). Mandatory if the device also reports to a monitoring station.
- **Module ID** – the module's identification number.
- **Time set** – which server the device synchronizes its clock from.

In the **Access** group you manage the access levels and passwords.

There are two access levels for the device settings: **administrator** and **installer**.

- **Administrator code** – access to all settings (default password: `123456`; the password is 6 characters: digits or Latin letters).
- **Installer code** – access that can be restricted (default password: `654321`).
- **Only an administrator can restore** – when ticked, only the administrator can start restoring the factory settings.
- **Allow installer to change** – here you can select which groups of settings the installer may change: **Account number**, **CMS reporting**, **User reporting**, **SIM card** (on a mobile network device) or **Ethernet settings** (on an Ethernet device), **Event summary**.

Do not leave the default passwords in the device!

During commissioning, change at least the administrator password and note it down in a safe place. A forgotten password cannot be cleared by restoring the factory settings either, because that also requires a password: only the manufacturer or the distributor can reset it, once the device has been sent to them. The exception is a device with a hardware RESET button: holding the button for 10 seconds restores the factory settings without a password.

6.3 Panel settings

On this page you specify how the communicator connects to the alarm control panel: the **TLC** group contains the settings for telephone line (TIP/RING) wiring, the **Serial bus** group those for data bus or serial wiring. The common settings affecting how the control panel's events are handled are also here.

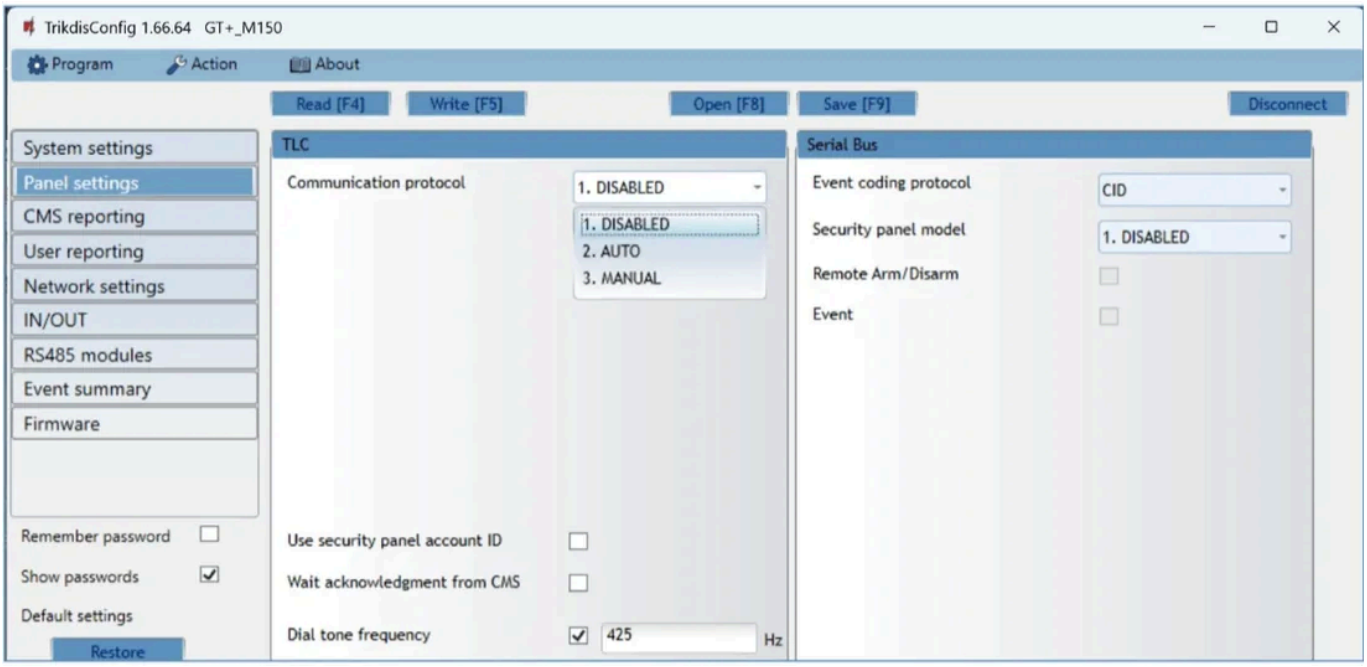


Figure 42. TrikdisConfig – Panel settings on the GT+: the Communication protocol list of the TLC group (1. DISABLED, 2. AUTO, 3. MANUAL), below it the Serial bus group and the common settings.

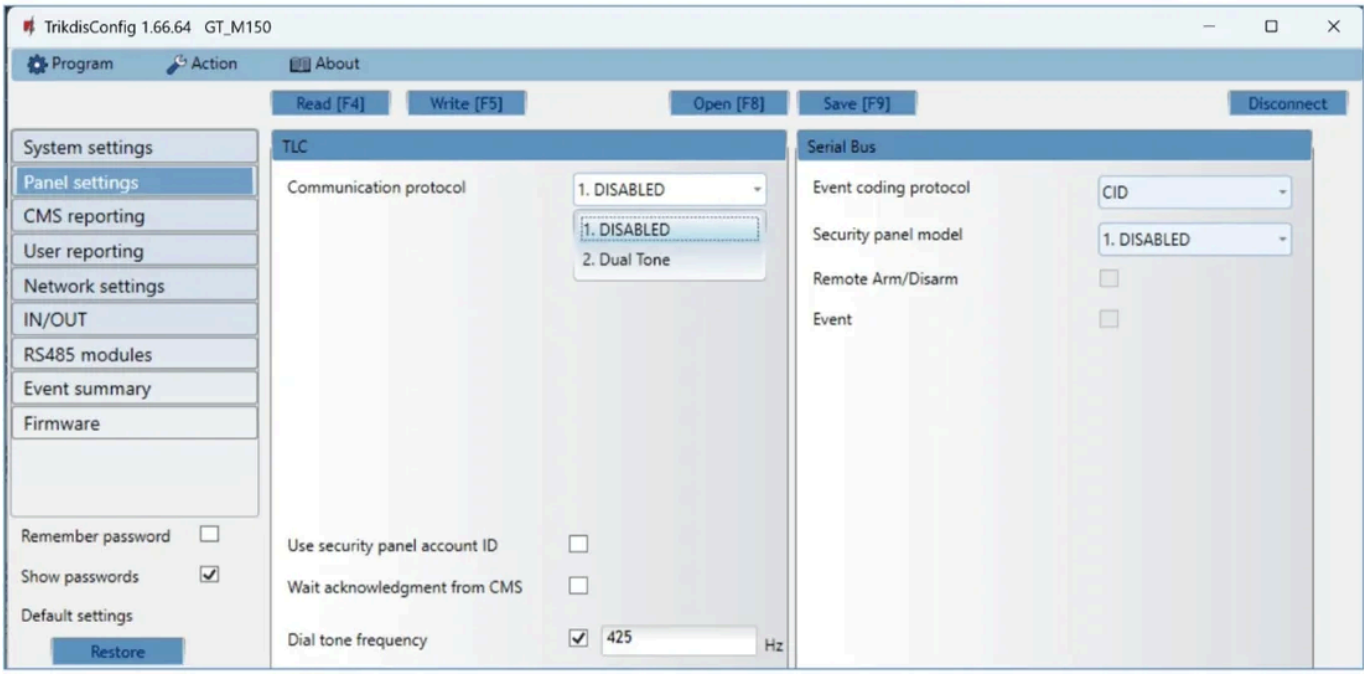


Figure 43. TrikdisConfig – Panel settings on the GT: here the Communication protocol list is 1. DISABLED and 2. Dual tone.

TLC group – if the communicator is connected to the control panel's TIP/RING terminals:

- **Communication protocol** – switches the communicator's DTMF telephone line interface on or disables it. GT+: **1. DISABLED** (switched off), **2. AUTO**, **3. MANUAL**; GT: **1. DISABLED**, **2. Dual tone**. With TIP/RING wiring select AUTO (GT: Dual tone).

The settings below the group, valid for both kinds of wiring:

- **Use security panel account ID** – when ticked, the communicator does not use its own Object ID, but the object ID set in the control panel and sent by the control panel.

- **Wait acknowledgment from CMS** – when ticked, after each event the communicator waits for the receiver's acknowledgment (kiss-off), and only then acknowledges to the control panel; if the acknowledgment does not arrive in time, it resends the message. If the device does not report to a monitoring station, leave it switched off.
- **Dial tone frequency** – the frequency of the dial tone with which the communicator communicates with the control panel's dialer (default 425 Hz, the dial tone frequency used in most European countries).



Figure 44. TrikdisConfig – Panel settings, Serial bus group: Event coding protocol CID, Security panel model (in the picture Paradox SP/MG), Remote Arm/Disarm and Event ticked, Security panel PC download password entered.

Serial bus group – if the communicator is connected to the control panel's data bus or serial port:

- **Event coding protocol** – the event coding protocol (CID).
- **Security panel model** – the type of the connected alarm control panel from the list (for the Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING wiring select **7. Paradox SP+/MG+ series KeyBus**).
- **Remote Arm/Disarm** – when ticked, the communicator controls the control panel directly (arming and disarming from Protegus 2). Only visible for the directly controllable control panels. For direct control the control panel must also be set up as described in chapter 4.
- **Security panel PC download password** – for direct control of Paradox and Texecom control panels, the PC or UDL password; it must match the password set in the control panel, which is described in chapter 4.

6.4 CMS reporting

The communicator sends the events to the monitoring station over the mobile data connection (IP). The events can go on several channels: the **primary** and the **parallel** channel work at the same time (to two receivers at once), and each has a **backup** channel that takes effect if the given channel fails. The communication is encrypted and password-protected; receiving it and forwarding the events to the monitoring software requires a Trikdis receiver (IPcom software receiver – Windows or Linux –, RL14 IP/SMS receiver or RM14 multi-channel receiver) or a universal receiver that knows the DC-09 / TL150 protocol. The GT and the GT+ report to the monitoring station only on an IP channel; they have no SMS channel.

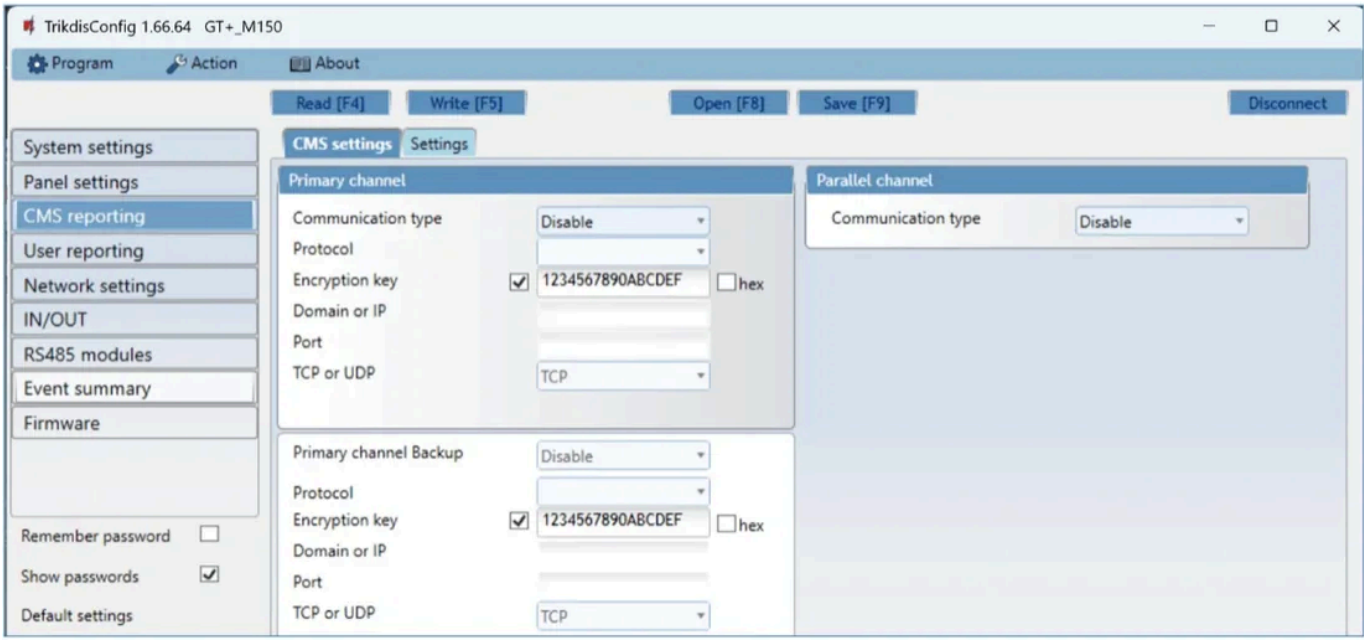


Figure 45. TrikdisConfig – CMS reporting, CMS settings tab: primary, backup and parallel channel.

Primary channel

- **Communication type** – the connection mode with the receiver: **IP**.
- **Protocol** – **TRK8** (Trikdis receivers), **DC-09_2007** or **DC-09_2012** (universal receivers), **TL150** (SURGARD receivers).
- **Encryption key** – the encryption key of the messages; it must be the same in the communicator and in the receiver.
- **Domain or IP**, **Port** – the receiver's domain name or IP address and port.
- **TCP or UDP** – the transmission protocol.

Parallel channel. In addition to the primary channel, it sends to a second receiver at the same time (for example to the local and the central monitoring station). Its settings are the same as those of the primary channel.

Primary channel Backup. It takes over communication if the primary channel does not work; its settings are the same as above.

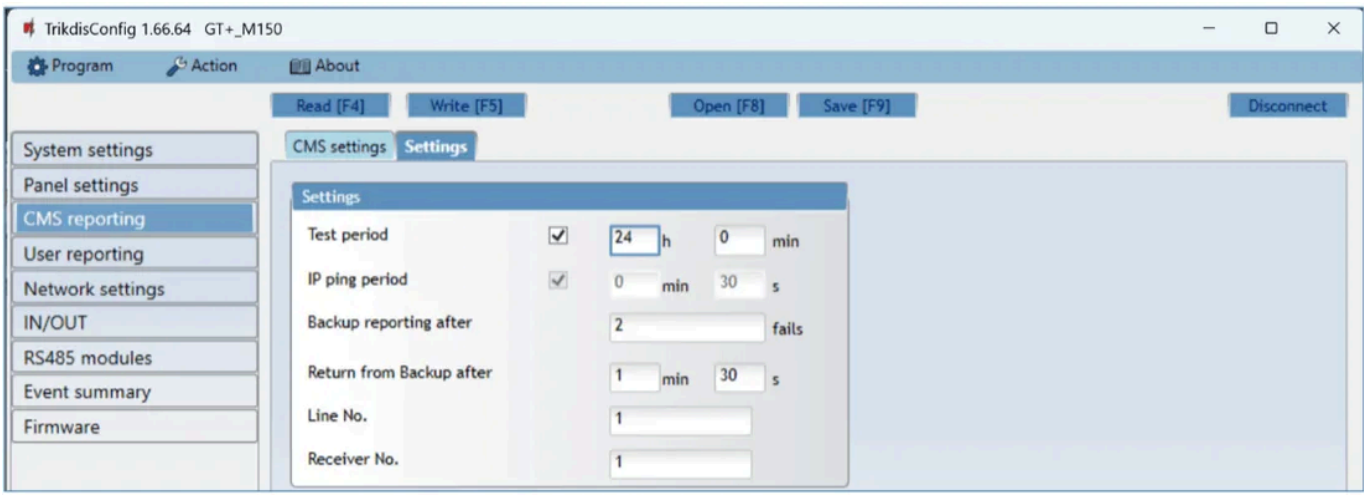


Figure 46. TrikdisConfig – CMS reporting, Settings tab: test report, PING, the timings of the backup channel and the DC-09 data.

On the **Settings** tab you set the timings and the DC-09 data.

- **Test period** – the interval of the periodic test report (default 24 hours). The test report is sent as a Contact ID message to the monitoring station and to Protegus 2.
- **IP ping period** – the interval of the keep-alive signal (PING) on the IP channel (default 30 s). You enable it with the tick box and enter the time in the minutes (**min**) and seconds (**s**) fields; it is required for connection supervision. The receiver does not forward PINGs to the monitoring software so as not to overload it; the software only receives a message if the receiver gets no PING for three times the set period. For example, if the PING period is 3 minutes, the loss of connection is reported after the 9th minute.
- **Backup reporting after** – after this many failed sending attempts the device switches to the backup channel (default 2).
- **Return from Backup after** – after this time it returns to the primary channel (default 1 min 30 s).

The PING keeps the live connection between the device and the receiver, and remote access, control and programming also depend on it. That is why **we do not recommend a PING period longer than 5 minutes**.

DC-09 Settings (on the right side of the tab) – only needs to be filled in if you send with the DC-09_2007 or DC-09_2012 protocol on any channel; the group appears when DC-09_2007 or DC-09_2012 is selected in the **Protocol** field of any channel:

- **Object ID in DC-09** – a 3–16 character hexadecimal identifier, provided by the monitoring station.
- **DC-09 line No** – the line number.
- **DC-09 receiver No.** – the receiver number.

On the Settings tab of the GT and the GT+, the DC-09 group contains the **Line No.** (line number) and **Receiver No.** (receiver number) fields; the group appears if DC-09_2007 or DC-09_2012 is selected in the **Protocol** field of one of the channels.

6.5 User reporting

On the **PROTEGUS Cloud** tab you enable the Protegus service, with which the user monitors and controls the communicator and the system connected to it remotely; details: www.protegus.app.

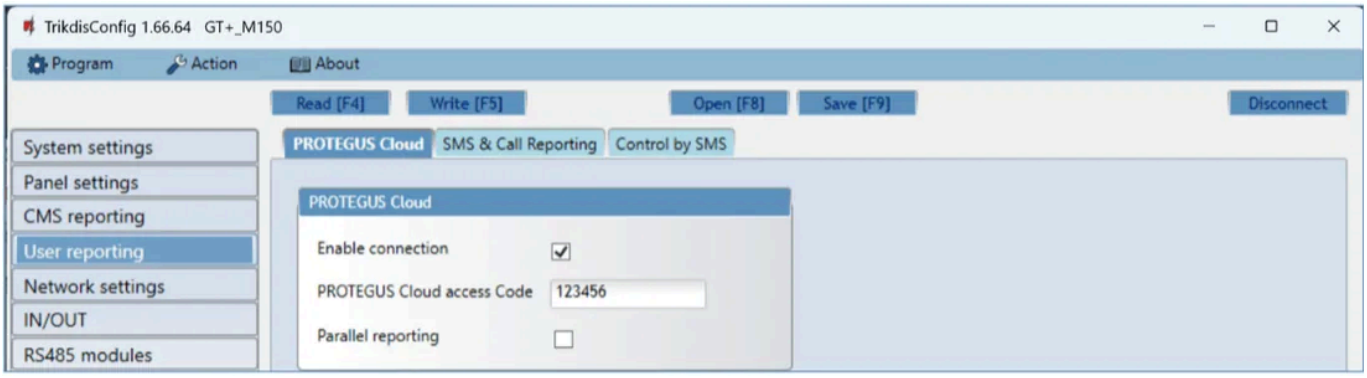


Figure 47. TrikdisConfig – User reporting, PROTEGUS Cloud tab.

- **Enable connection** – enables the Protegus service: the device exchanges data with the Protegus 2 app, and TrikdisConfig can also reach it remotely.
- **PROTEGUS Cloud access Code** – 6-digit code for connecting to Protegus 2 (default `123456`). If you change it in TrikdisConfig, it must also be changed in the Protegus 2 app.
- **Parallel reporting** – when ticked, the messages go on the primary channel (to the monitoring station) and to Protegus 2 at the same time.

On the **SMS & Call Reporting** tab, the user can also be notified about the events by SMS or phone call.

On an alarm, the device first sends the SMS to all the phone numbers entered, then calls them one by one from Tel 1 to Tel 4. Each number is called once and rings for 20 seconds; a call counts as successful if the number rings (answering or declining is also enough). 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.

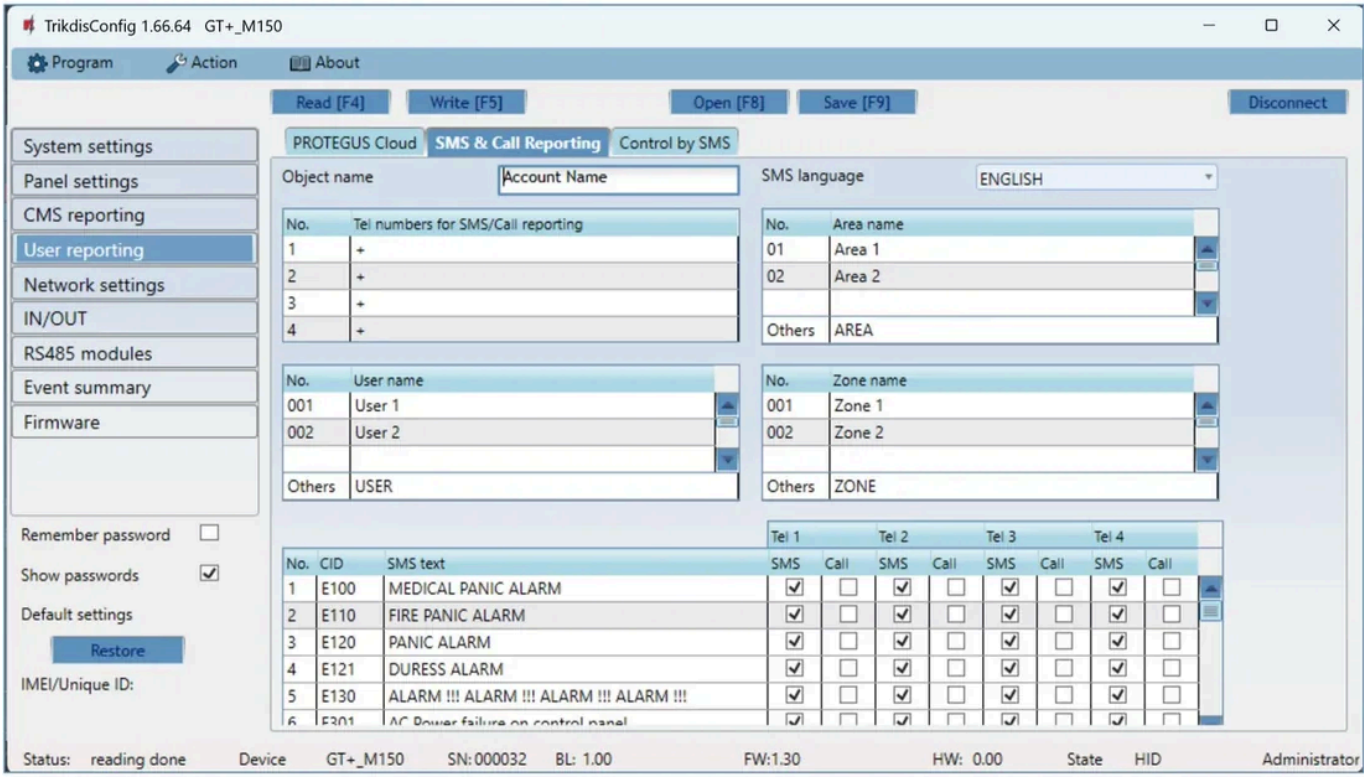


Figure 48. TrikdisConfig – User reporting, SMS & Call Reporting tab.

- **Object name** – the name of the system; it appears in every SMS.
- **SMS language** – the language of the SMS messages (the messages can also be sent with the language's own characters).
- **Tel numbers for SMS/Call reporting** – up to 4 phone numbers that receive an SMS or call about the events; enter them with the country code (`+CC…`, `00CC…` or `CC…`, where CC is the country code).
- **Area name, User name, Zone name** – the names of the partitions, users and zones; the device uses these in the text of the SMS messages. In the corresponding table, enter the number of the partition, user or zone, and its name next to it.
- **CID event table** – you can set per event which number receives an SMS or call. The SMS text and Contact ID code of the default events can be changed, and a new event can also be added with a description.

On the **Control by SMS** tab you set up the reception of SMS commands: with the commands the outputs can be switched, and information can be requested about the device (the commands are described in section 5.4).

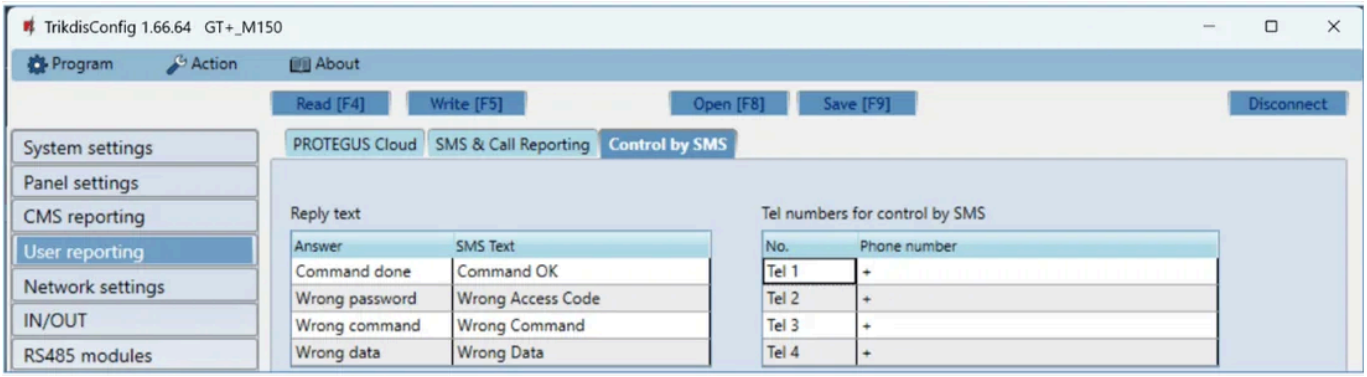


Figure 49. TrikdisConfig – User reporting, Control by SMS tab.

- **Reply text** – the text of the reply messages to an SMS command: successful command (Command done), wrong password (Wrong password), wrong command (Wrong command), wrong data (Wrong data). The texts can be edited.
- **Tel numbers for control by SMS** – the phone numbers from which the device accepts commands.

If no phone number is entered here, the device accepts commands from any number. Even then, security is provided by the fact that the administrator or installer password is mandatory in the command.

6.6 Network settings

Before use, make sure that the SIM card is active and works. If you send the events on an IP channel or to Protegus 2 over the mobile internet, mobile data service must also be enabled on the card.

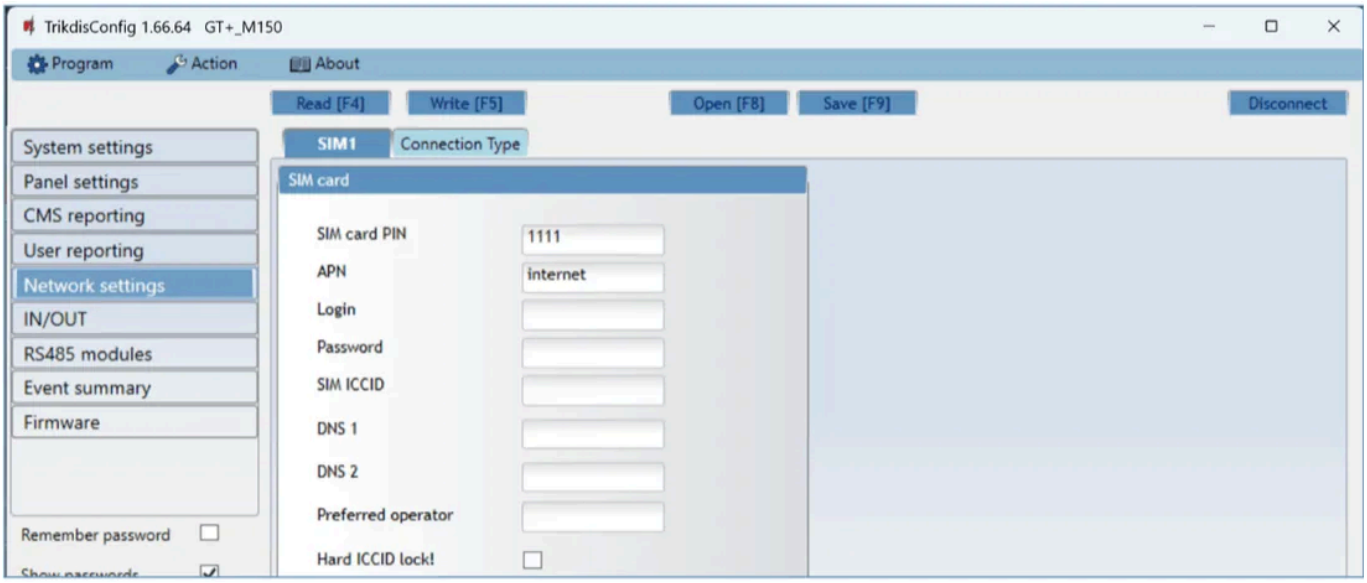


Figure 50. TrikdisConfig – Network settings, SIM1 tab: the SIM card's data.

SIM1 tab, SIM card group

- **SIM card PIN** – the card's PIN code. You can switch off the PIN request by putting the card into a mobile phone and disabling it there; in that case the field's default value can stay.
- **APN** – the operator's access point (Access Point Name); without it the device does not connect to the internet. You can find the value on the website of the SIM card's operator; `internet` is generic and works in many operators' networks. The known APNs of the operators are listed in the APN article (for an IoT / M2M card the operator gives a separate APN, see section 2.2).
- **Login, Password** – user name and password for the internet connection, if the operator requires them.

- **SIM ICCID** – the SIM card's ICCID number, if you want the device to work only with this card. If the ICCID of the inserted card does not match, the TROUBLE LED flashes 8 times (section 1.6).
- **DNS 1, DNS 2** – name servers (DNS, Domain Name System: gives the IP address belonging to a domain name); they are needed if you entered the receiver in the **Domain or IP** field with a domain name and not with an IP address. The default is Google's public DNS. Regardless of the IP settings, check that the DNS addresses work with your operator.
- **Preferred operator** – the mobile operator's code (MCC + MNC); if you enter it, the device only connects to the chosen operator's network.
- **Hard ICCID lock** – when ticked and after restarting the device, the communicator is strictly bound to the SIM card with the given ICCID number.

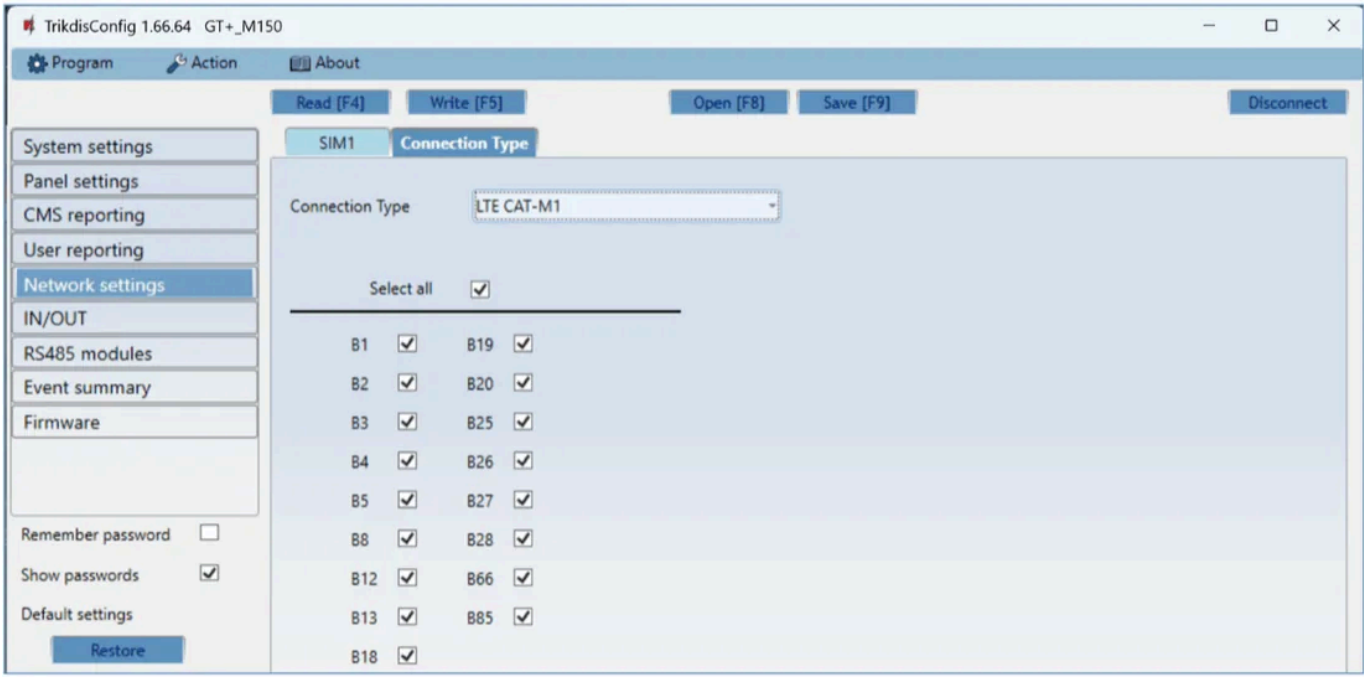


Figure 51. TrikdisConfig – Network settings, Connection Type tab: selecting the LTE bands of the CAT-M1 modem version.

Connection Type tab – only applies to the version with the CAT-M1 modem (BG95-M5): here you can specify which LTE frequency bands the device's modem works on (**Select all** = all).

6.7 IN/OUT

Here you specify the role of the communicator's two dual-function I/O terminals: **Off** (not used), **IN** (input) or **OUT** (output). For an input, the type of the connected circuit must also be given in the **Type** field (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).

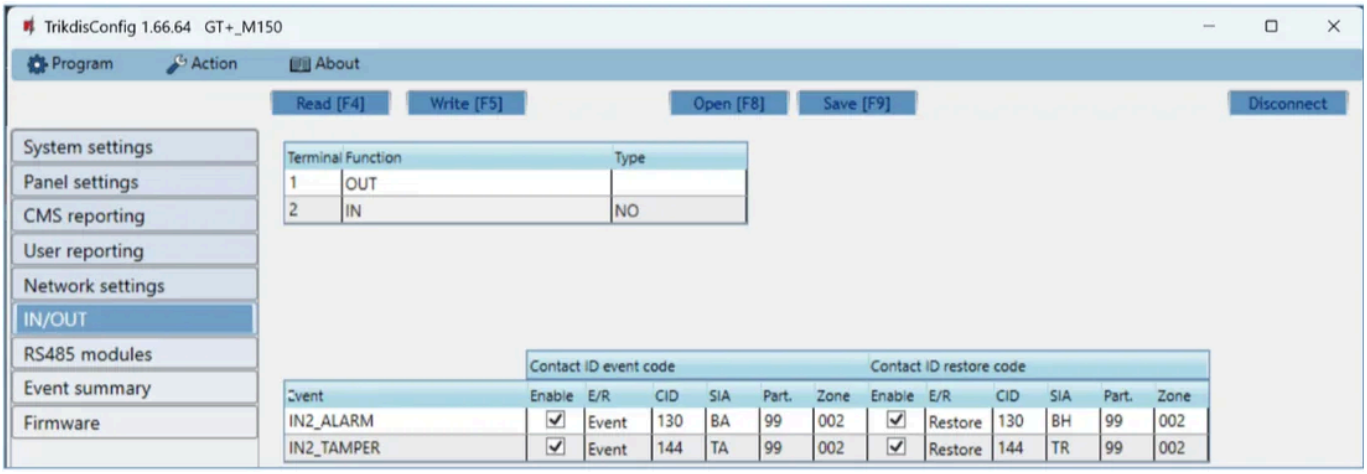


Figure 52. TrikdisConfig – IN/OUT page: terminal 1 is an output (OUT), terminal 2 an input (IN, NO); below it the alarm and tamper events of input 2 with CID and SIA codes.

When the sensor connected to the input is violated, the communicator sends its own event (**INx_ALARM**, Contact ID 130, SIA BA; restore BH), and when the tamper circuit is violated, a tamper event (**INx_TAMPER**, 144, SIA TA; restore TR) to the monitoring station and to Protegus 2; the events of every terminal set as an input appear in the table. The columns of the table:

- **Enable** – enables sending the message to the monitoring station and to Protegus 2.
- **E/R** – the message type: Event or Restore.
- **CID** – the Contact ID code (can be changed, or the default can stay).
- **SIA** – the SIA code (can be changed, or the default can stay).
- **Part.** – the partition number in the message.
- **Zone** – the zone number in the message.

6.8 RS485 modules

With **iO-8** expanders connected to the RS485 bus, further inputs and outputs can be added to the communicator. The connected expanders must be added on the **Modules list** tab.

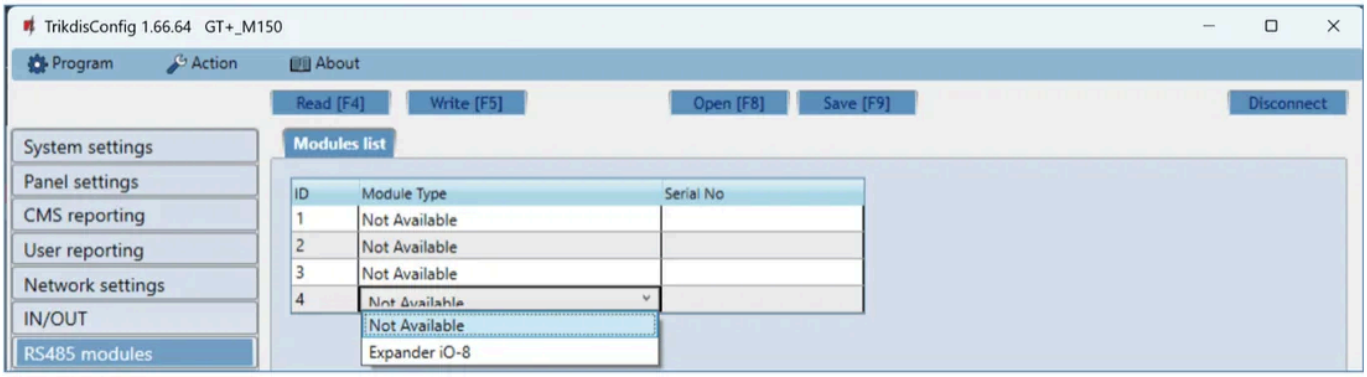


Figure 53. TrikdisConfig – RS485 modules, Modules list tab: in position 4 the Module type list (Not Available, Expander iO-8).

- **Module type** – the type of the module connected to the bus from the list (**Expander iO-8**).
- **Serial No** – the module's 6-digit serial number (on the module's case and on the sticker of the packaging).

After selecting the module and entering the serial number, go to the **RS485 modules** → **Module** tab: the added module gets its own numbered tab (Module 1 …) with its settings.

iO-8 expander – 8 dual-function I/O terminals; up to four iO-8s can be connected to the communicator.

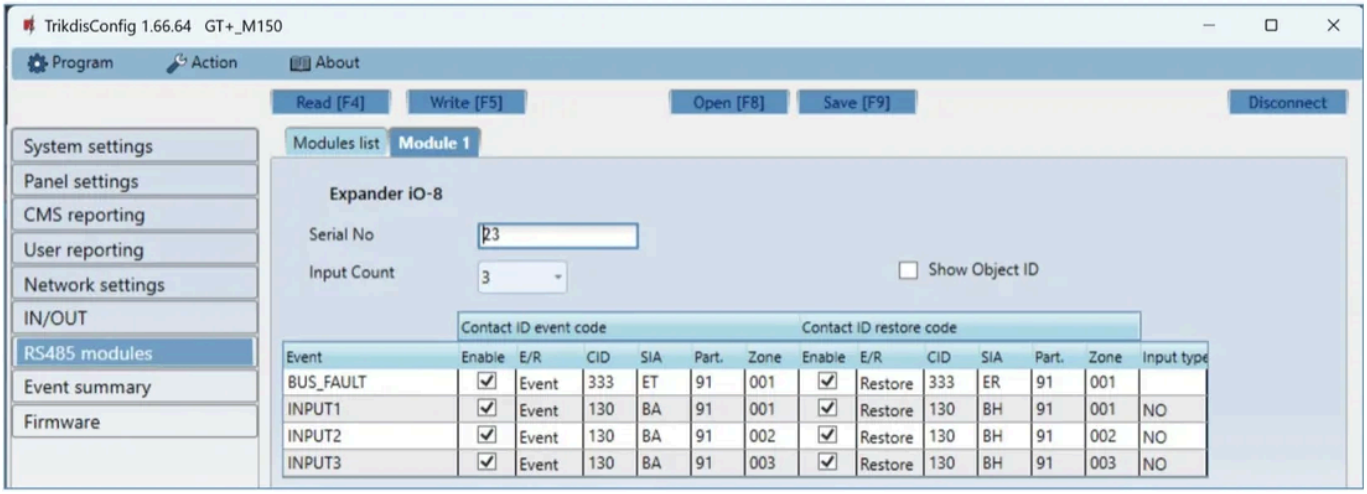


Figure 54. TrikdisConfig – RS485 modules, Module 1 tab (iO-8): Input Count, Show Object ID, and the BUS_FAULT, INPUT1–INPUT3 events with CID and SIA codes, with partition 91.

- **Input Count** – how many terminals are inputs (IN); the rest will be outputs (OUT). You set the role of the outputs (arming / disarming or switching a device) directly in the Protegus 2 app.
- In the table you can assign event and restore codes to the bus fault (**BUS_FAULT**, Contact ID 333) and to the inputs (**INPUTx**, 130); when an input is violated, the communicator sends an event with the set code to the monitoring station receiver and to Protegus 2. The columns of the event (Contact ID event code) and restore (Contact ID restore code) rows: **Enable** (enabling), **E/R** (Event or Restore), **CID** (Contact ID code), **SIA** (SIA code), **Part.** (the partition – depends automatically on the module's number: 91 for module 1, 94 for module 4), **Zone** (the zone number).
- **Object ID** – an object ID different from the communicator's can also be given for the input (the column appears when **Show Object ID** is ticked).
- **Input type** – the type of the input: NO, NC or EOL.

6.9 Event summary

On this page you can enable or disable the device's **own internal messages** and change their Contact ID code, partition and zone number. A message disabled here is not sent by the device on any channel. By default the messages are sent with partition 99 and zone 999.

Message	Contact ID	When it is generated
COMMUNICATION	350	Communication between the communicator and the alarm panel has been lost (disabled by default). A communicator connected to the bus or serial port detects this directly; a telephone-line communicator only with **Line supervision** enabled.
POWER	302	Inadequate (low) supply voltage; its restore is a separate message.
REMOTE_STARTED	411	Remote programming with TrikdisConfig has started.
REMOTE_FINISHED	412	Remote programming has finished.
START	700	The device has connected to the network (start-up).
TEST	602	Periodic test report.
PING	760	The PING keep-alive message. It is not in every device's list: it appears on the screen of the earlier hardware version, while the Event summary page of the newer versions has no such row. Its interval is set in the **CMS reporting → Settings → IP ping period** field.

- **Enable** – enables sending the message to the monitoring station and to Protegus 2.
- **E/R** – the message type: Event or Restore – the row stands for the occurrence of the event or its restore.
- **Part.** – the partition (area) number the device sends with the internal event and its restore.
- **Zone** – the zone number the device sends with the internal event and its restore.
- The **CID** code, the **partition** and the **zone** can be changed for any event; where there is a restore (Restore), its code can be set separately.

The events of the device's own inputs (**INx_ALARM**, **INx_TAMPER**) are set on the **IN/OUT** page, and the events of the expansion modules (**BUS_FAULT**, **INPUTx**) on the **RS485 modules** page, on the module's tab. Enabling the test report and its interval are set in the **CMS reporting** → **Settings** → **Test period** field.

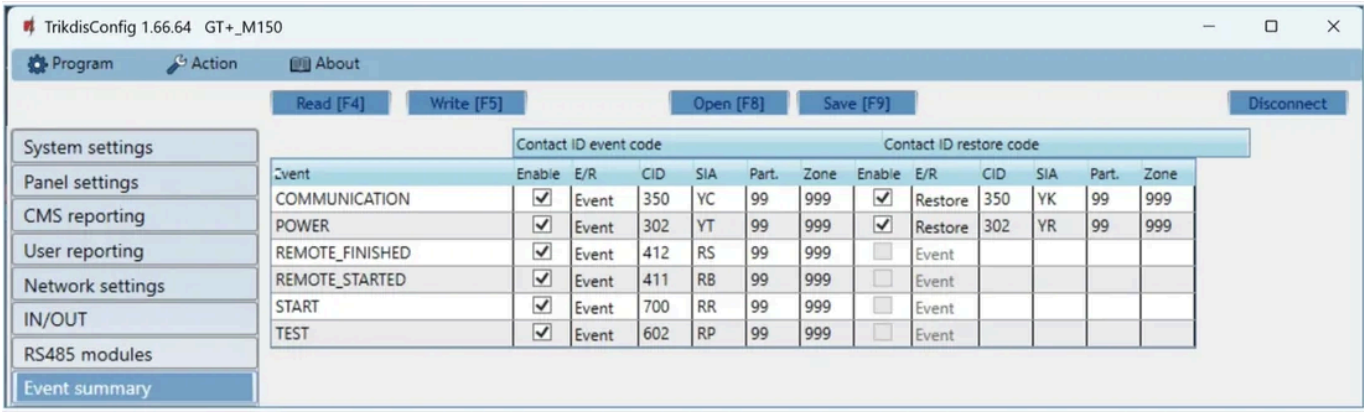


Figure 55. TrikdisConfig – Event summary page: the device's internal messages with CID and SIA codes (COMMUNICATION 350, POWER 302, REMOTE_FINISHED 412, REMOTE_STARTED 411, START 700, TEST 602).

The list of the GT and the GT+ contains the **COMMUNICATION**, **POWER**, **REMOTE_FINISHED**, **REMOTE_STARTED**, **START** and **TEST** messages, each with its SIA code as well. The COMMUNICATION message reports a fault in the connection between the control panel and the communicator: with data bus or serial wiring the communicator detects this directly (the TROUBLE LED flashes 7 times).

6.10 Restoring the factory settings

To restore the factory settings, click the **Restore** button in the **Default settings** group at the bottom left of the TrikdisConfig window. Restoring deletes all settings – including the passwords – so it is worth saving the settings to a file first (**Save [F9]**).

With the installer password this is only possible if the administrator has not disabled it on the **System settings** → **Access** page.



Figure 56. TrikdisConfig – the Restore button of the Default settings group.

The factory settings can also be restored on the device, without a computer: with the power on, press and hold the **RESET** button on the printed circuit board (section 1.4) **for 10 seconds**, until the NETWORK, POWER and TROUBLE LEDs go out, and then the POWER LED lights up. Then release the button: the factory settings have been restored.

7. Remote programming

TrikdisConfig reaches Trikdis devices not only over a USB cable but also **remotely, via the Protegus cloud**. This way you can change the settings of an already installed device without going to the site.

Remote access requires:

1. The device must be switched on and have a network connection (the **POWER** and **NETWORK** LEDs are lit green; on a mobile network device the NETWORK LED also flashes yellow). On a mobile network device, the inserted SIM card must be active and its PIN code must be entered in the device, or the PIN request must be disabled; on an Ethernet device, the network (LAN) cable must be plugged in and the device must be able to reach the internet.
2. On the **User reporting** → **PROTEGUS Cloud** page of TrikdisConfig, **Enable connection** must be ticked (set this over USB during the first commissioning).
3. You need to know the device's **unique identifier** (IMEI or MAC – printed on the box and on the back of the device) and the administrator or installer password.

Steps:

1. Start the TrikdisConfig software.
2. In the **Remote access** section, enter the device's unique identifier (IMEI or MAC) in the **Unique ID** field.
3. Optionally, give the system a name in the **System name** field – the software remembers it, and next time you can choose it from the drop-down list.
4. Press the **Configure** button.
5. In the window that opens, click the **Read [F4]** button and enter the password. With the **Remember password** tick box, the software remembers it for this session.
6. Make the changes, then send them to the device with the **Write [F5]** button.

The software saves the named systems you have programmed remotely before; you can list them with the arrow next to the **System name** field. To delete one, select the identifier in the list, press the **Delete** key and confirm.

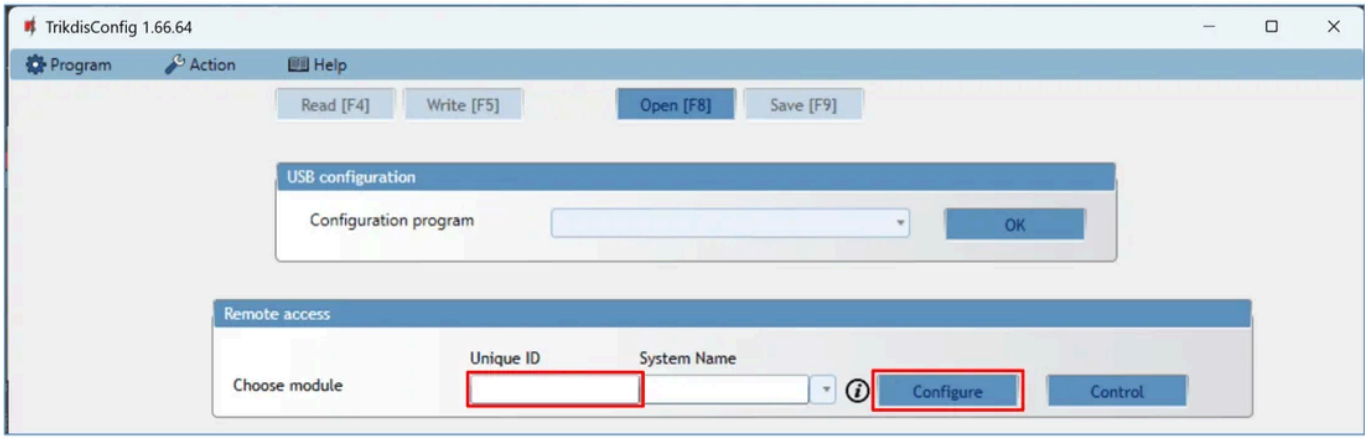


Figure 57. TrikdisConfig – the Remote access group: the Unique ID field, the System name list and the Configure button.

The unique identifier of the GT and the GT+ is the **IMEI**; it can be read on the device label and on the sticker on the box. For remote access the SIM card must be active, with its PIN code entered or the PIN request switched off; **Enable connection** must be ticked on the **User reporting** → **PROTEGUS Cloud** tab (section 6.5); the **POWER** LED must be steady green, and the **NETWORK** LED steady green and flashing yellow.

8. Testing the communicator

After programming and wiring, always check the whole chain: alarm panel → communicator → monitoring station and/or Protegus 2.

Before that, check that there is power (the **POWER** LED is lit green) and a network connection (the **NETWORK** LED is lit green).

1. **Trigger an event.** Arm and then disarm the system on the keypad, or violate a zone while the system is armed so that an alarm is generated.
2. **Check that it arrives.** See whether the event has appeared in the monitoring software and/or in the event list of the Protegus 2 app – with the correct partition and zone number.
3. **Inputs.** Trigger the detector wired to the communicator's own input and check the corresponding event.
4. **Outputs.** Switch the output from the Protegus 2 app and check that the connected device (relay, keyswitch zone) actually operates.
5. **Remote arming.** If the panel can be controlled remotely, also arm and disarm it from the Protegus 2 app.
6. **DSC control panel with Keybus + TIP/RING wiring (GT+).** Arm the system, and trigger a fire zone alarm. The monitoring station must receive the event with the Contact ID code matching the zone type (for example E110 – fire alarm), not as a general alarm (E130).

9. Firmware update

Ha bármikor az USB bedugásakor a program azt jelzi, hogy új firmware verzió jelent meg a Trikdis eszközhöz, fogadd el a frissítést és telepítsd!

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.

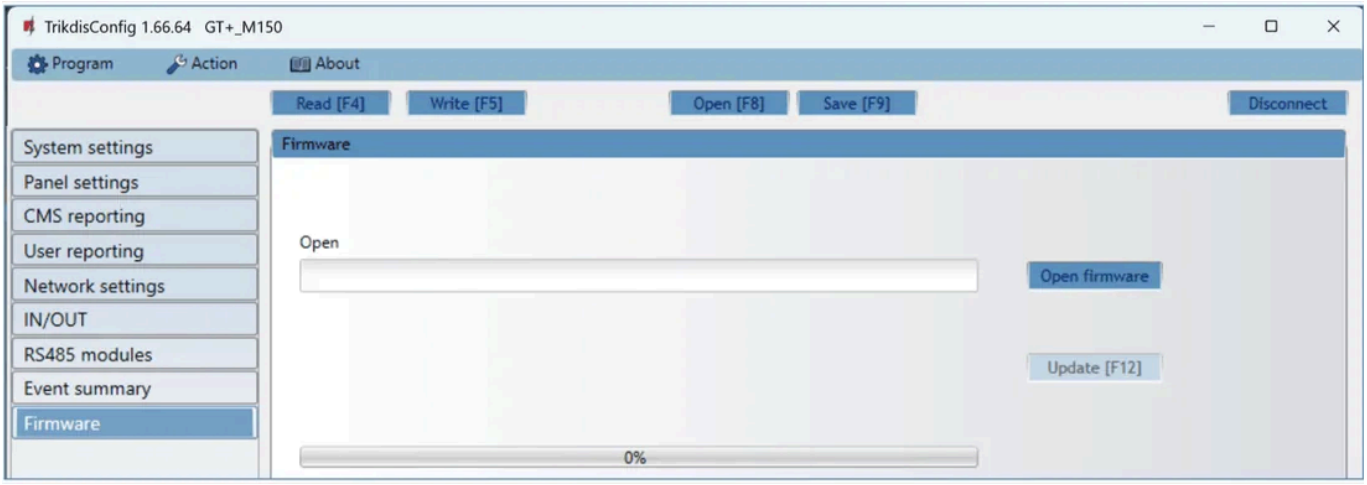


Figure 58. TrikdisConfig – Firmware page: Open firmware button, Update [F12] button and the progress indicator.

The update needs an internet connection. An antivirus program, a firewall or strict internet access settings can prevent the automatic firmware update; in that case the antivirus settings must be changed. The Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING wiring (section 3.3.4) needs firmware 1.21 or newer.

10. Troubleshooting and frequently asked questions

The most common questions and faults, starting from the LED indications. If the answer refers to a detailed chapter, you will find the exact place of the setting there.

The NETWORK LED is off – no network

1. Look at the flashes of the **TROUBLE** LED: 1 = no SIM, 2 = wrong PIN, 3 = no APN, 4 = cannot register on the mobile network, 5 = cannot connect to the data network (section 1.6).
2. Check that the SIM card is active, has data service, and sits properly in the holder.
3. If the PIN request is switched on on the card, enter the PIN on the **Network settings** → **SIM1** tab, or switch off the PIN request in a phone.
4. Check the APN (section 2.2): for an IoT / M2M card the operator gives a separate APN.
5. Check the antenna: it is screwed on, it is not in a metal enclosure, and the signal level is adequate (the NETWORK LED flashes yellow at least 3 times; sections 1.6 and 3.2).

There is a network, but the monitoring station receives no events

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

1. 6 flashes of the **TROUBLE** LED indicate that there is no connection to the receiver: check the receiver's address, port, the TCP/UDP setting, the protocol and the encryption key (**CMS reporting**).
2. If the receiver is given with a domain name, check the DNS setting (**Network settings** → **SIM1** → **DNS 1, DNS 2**).

3. Check that the SIM card's data plan does not block the required port (some M2M cards only allow specific addresses).

The TROUBLE LED flashes 7 times – no connection to the control panel

1. With data bus or serial wiring, check the CLK and DATA wires, and that the type of the connected control panel is selected in the **Panel settings** → **Security panel model** field (section 6.3).
2. With a Paradox control panel, check whether the serial port is locked (section 4.1.2); with Texecom and Paradox control panels, the **Security panel PC download password** must match the one set in the control panel.
3. With telephone line wiring, the control panel's dialer must be switched on, in DTMF mode, with Contact ID format and a telephone number entered (section 4.2), and the **Communication protocol** must be AUTO (GT: Dual tone).

The TROUBLE LED flashes 8 times – ICCID mismatch

The number entered in the **Network settings** → **SIM1** → **SIM ICCID** field does not match the ICCID of the inserted SIM card: the device only works with the given card. Put the original card back, or change (delete) the ICCID; with **Hard ICCID lock**, restart the device after the change (section 6.6).

DSC: every alarm arrives as a general alarm E130

Connected only to the Keybus, the communicator receives the state of the zones from the control panel, but not the zone type, so it reports every alarm with code E130 (section 3.3.1). If the monitoring station expects the code matching the zone type (for example fire: E110): connect the **GT+** to the TIP/RING terminals as well as to the Keybus, and program the control panel's dialer (sections 3.3.2 and 4.1.1). The GT does not have this dual wiring; there the control panel's own codes are sent by the control panel's dialer only with TIP/RING wiring, but then there is no direct control, and a keyswitch zone is needed for arming (section 3.4).

Paradox: the serial port is locked, or there is no connection

On the newer Paradox control panels (SP+, MG+, EVOHD+) the serial port may be locked at the factory; unlocking is covered in section 4.1.2 and in the article Unlocking a locked serial port on Paradox alarm control panels. With the Spectra SP / SP+ and Magellan MG / MG+ control panels, the Keybus + TIP/RING wiring can also be used instead of the serial port (section 3.3.4); it needs no unlocking, but the communicator's firmware must be at least 1.21 (chapter 9).

I cannot arm from Protegus 2

1. With direct control, **Panel settings** → **Remote Arm/Disarm** must be ticked, and the control panel must be set up as described in section 4.1 (Paradox: PC password, firmware V.4+; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: the settings described). Check in the table in section 1.3 whether the control panel can be controlled directly at all.
2. With keyswitch arming (section 3.4), the terminal must be **OUT** on the **IN/OUT** page, the control panel's zone must be a keyswitch zone, and in Protegus 2 the output must be assigned to the partition, in the same mode as the control panel's (pulsed or two-state; section 5.2).
3. Protegus 2 shows the partition's state from the control panel's arming and disarming events: the control panel must report these (Opening/Closing).

Protegus 2 does not see the device

1. **Enable connection** must be ticked on the **User reporting** → **PROTEGUS Cloud** tab.

2. When adding, the **PROTEGUS Cloud access Code** set in the device must be entered; if you changed the code in TrikdisConfig, change it in the app as well.
3. Type the IMEI exactly, from the device label or the sticker on the box (or scan the QR code).
4. The SIM card's data service and the APN must be in order (the NETWORK LED is green, and the DATA LED goes out after an event).

I cannot log in remotely with TrikdisConfig

1. The device must be online (NETWORK LED green, flashing yellow), and the Protegus connection must be enabled (**Enable connection**).
2. **CMS reporting** → **Settings** → **IP ping period** must not be longer than 5 minutes: the PING keeps up the connection needed for remote access.
3. Check the administrator or installer password.

I have forgotten the password

It cannot be reset with TrikdisConfig, because the restore also requires a password. It can be reset with the device's **RESET** button, though (section 6.10): with the power on, hold it pressed for 10 seconds. All settings are deleted.

GT or GT+ – which one do I need?

The wiring, setup and operation of the two versions are the same; the differences are summarized in the table in section 1.2. The GT+ also works from a 10–32 V DC supply (also in 24 V systems), and with DSC control panels it can also do Keybus + TIP/RING wiring, so the events are sent with the control panel's own Contact ID codes. If you do not need these, the GT can do the same.

How much data traffic does the device use?

The event messages and the PINGs are very small; the traffic depends mainly on the PING period and the frequency of the test reports. For an average household system, the monthly traffic typically stays below 10 MB. The exact value depends on the settings and on the operator's billing unit, so with a data-limited card it is worth checking the traffic of the first month.

11. 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.

- Security equipment may only be installed and maintained by a qualified installer.
- Read the manual before installation; ignoring the instructions can lead to malfunction or failure of the equipment.

- Disconnect the equipment from the power supply before wiring, before every electrical connection and before servicing.
- Modifications, alterations and repairs not authorized by the manufacturer void the warranty.
- Follow local waste disposal regulations: do not throw the device that has become unusable or its parts in household waste. The crossed-out wheeled bin symbol (WEEE) on the device indicates that it must be handed in separately, as electronic waste.

See also

- Compatibility finder – which Trikdis communicator and which wiring suits your alarm control panel.
- Trikdis communicator + DSC alarm control panel: short installer guide – the steps of the DSC wiring in brief.
- Trikdis communicator + Paradox alarm control panel: short installer guide – the steps of the Paradox wiring in brief.
- DSC Power Series NEO and Trikdis communicators: compatibility and solutions – why the NEO cannot be connected to the data bus, and what the solution is.
- Unlocking a locked serial port on Paradox alarm control panels – unlocking the serial port of the SP+, MG+ and EVOHD+ control panels.
- Remote arming with a keyswitch from the Protegus 2 app – the details and pitfalls of keyswitch arming.
- APN settings – list of European mobile operators – the operators' APNs, also for IoT / M2M cards.
- Documentation in English: docs.trikdis.com – the GT and GT+ pages also contain the Contact ID → SIA code conversion table (appendix). The manuals on docs.trikdis.com are in English.

Related products

Trikdis GT 4G smart communicator | **Trikdis GT+ 4G smart communicator**

Trikdis iO8 wired expander module

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/gt-manual