G16 communicator – installer and user manual

Installer and user manual for the Trikdis G16 communicator: connection to the alarm control panel's data bus or serial port, programming the control panel, SIM and 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/g16-manual

Contents

1. Overview

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

2. Quick start with TrikdisConfig

2.1 Preparation
2.2 Control panel type and direct control
2.3 Connection to the Protegus 2 app
2.4 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 PowerSeries
3.3.2 Paradox
3.3.3 UTC Interlogix (Caddx) NetworX
3.3.4 Texecom Premier / Premier Elite
3.3.5 Crow Runner
3.3.6 Pyronix
3.3.7 Honeywell Ademco Vista
3.3.8 InnerRange Inception and Integriti
3.4 Wiring a keyswitch zone
3.5 Wiring inputs
3.6 Wiring an output with a relay
3.7 Wiring the iO-8 expander
3.8 Wiring the W485 and E485 modules
3.9 Power-up and first check
A TRIKDIS átjelző elindítása

4. Programming the alarm control panel

4.1 DSC
4.2 Paradox
4.3 Texecom
4.4 UTC Interlogix (Caddx)
4.5 Crow and Pyronix
4.6 Honeywell Ademco Vista
4.7 InnerRange Inception and Integriti

5. Remote control with the Protegus 2 app

5.1 Adding the device
A rendszer létrehozása a Protegus 2 alkalmazásban

5.2 Direct control with the keypad code
5.3 Arming with a keyswitch zone
5.4 Arming and disarming from the app
5.5 Control by SMS messages

6. TrikdisConfig – the settings in detail

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

7. Remote programming

8. Checking the communicator's operation

9. Firmware update

10. Troubleshooting and frequently asked questions

11. Safety instructions

See also

1. Overview

The G16 is Trikdis's **direct-connection cellular communicator**: it does not connect to the alarm control panel's telephone line output, but to the panel's **keypad bus or serial port**. It reads the events directly from the control panel – together with the zone, partition and user number – and forwards them over a mobile data connection to the monitoring station's receiver and to the Protegus cloud, into the user's app. It works with the supported DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell and Crow control panels; with the **directly controllable** models the user arms and disarms from the Protegus 2 app with their own keypad code, without a separate keyswitch zone. The Protegus 2 app can be used with every alarm control panel the G16 supports, regardless of the manufacturer. For control panels of other makes that only have a telephone line output, the G16T (TIP/RING) communicator is the right choice.

1.1 What it is for and how it works

- **It reads the control panel directly.** On the panel's bus every event reaches the communicator immediately, with the panel's own numbering; the panel's dialer does not need to be set up, and there is no Contact ID dialing either.
- **It reports to the monitoring station.** It sends the events over an IP connection to a Trikdis software or hardware receiver (TRK protocol) – these work with any monitoring software – or to any universal receiver (SIA DC-09 2007/2012, SUR-GARD TL150). To a SUR-GARD receiver it passes the Contact ID codes coming from the control panel converted into SIA codes. By default it checks the connection every 30 seconds (or at the interval you set), and on failure it switches to the backup channel.
- **It notifies the user.** The Protegus 2 app shows what happened in a push notification – with a separate sound matching the event – and in the event list; from the app the user can arm and disarm, and switch the devices connected to it (lighting, gate, ventilation, heating, irrigation, etc.). The user can also be notified by SMS and phone call.
- **Together or separately** it works with the monitoring station and the user: it can be used with Protegus 2 only (without a monitoring station), with a monitoring station only, or with both. If both are set up, it sends the event to the monitoring station first, then to the user.
- **SMS backup.** It also notifies the monitoring station by SMS if the data connection does not work in the operator's network; it can also send to two receivers in parallel, each with its own backup channel.
- **It has its own inputs and outputs.** Three dual-function I/O terminals can be used as inputs (detector, tamper) or as controllable outputs (keyswitch zone, relay); you can switch the outputs from the Protegus 2 app and by SMS command. On the RS485 bus of the 4G version it can use an iO-8 expander for 8 more I/Os, and with a W485 or E485 module it can also communicate over a Wi-Fi or a wired internet connection – in that case the mobile network is the backup path.

The diagram below shows the structure of the system: the alarm control panel's bus connects to the G16, the G16 reaches the internet over the mobile network, and through it the monitoring station's receiver and the Protegus cloud, while the user sees the system in the Protegus 2 app.

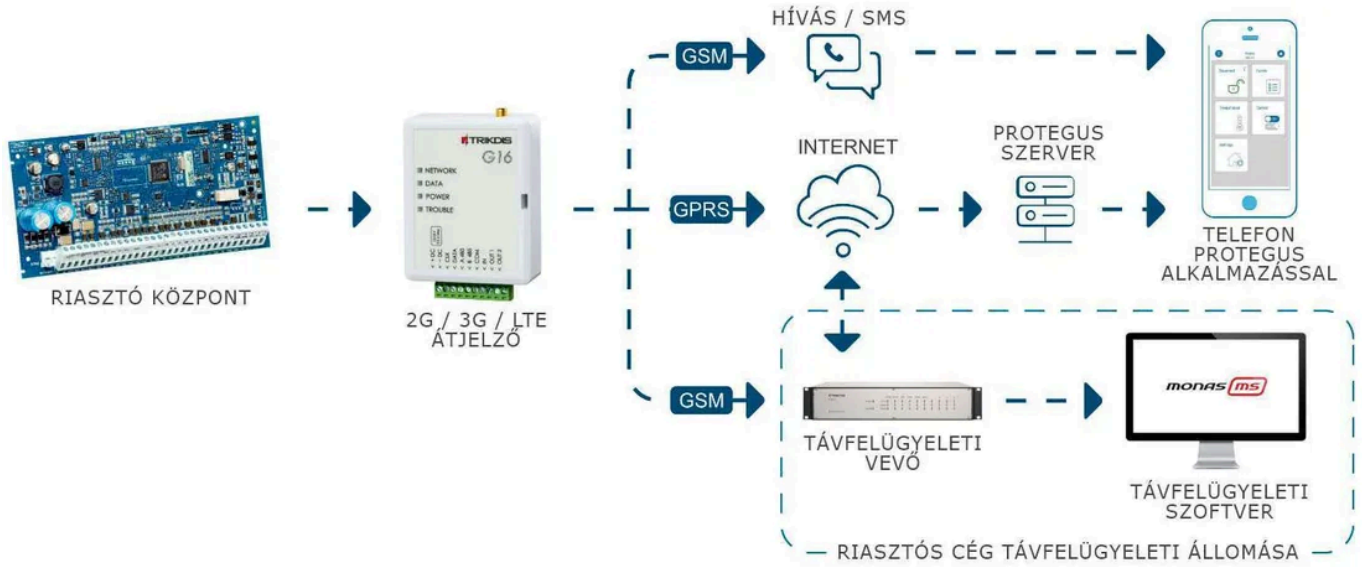


Figure 1. The G16's place in the system: alarm control panel → G16 → mobile network → monitoring station receiver and Protegus cloud → Protegus 2 app. The user can also receive SMS and calls (GSM), the monitoring station receiver can receive SMS as a backup.

- 1 Alarm control panel (keypad bus or serial port)
- 2 G16 communicator (2G / 4G)
- 3 Call and SMS to the user
- 4 Mobile data connection → internet → Protegus cloud
- 5 Phone with the Protegus 2 app
- 6 Monitoring station receiver
- 7 Monitoring software (the security company's monitoring station)

1.2 Compatible alarm control panels

The G16 can be connected to the control panels below. With the **directly controllable** models, arming and disarming is done from the app with the keypad code; with the others, with a keyswitch zone (section 3.4). For direct control of Paradox control panels, the panel firmware must be at least **V.4**; on the newer Paradox models (SP+, MG5050+, EVOHD+) the serial port is locked at the factory and must be unlocked before use.

Panels that can be controlled directly – the communicator receives the events over the data bus or the serial port, and arming / disarming works without any additional wiring:

Manufacturer	Connection	Models
Paradox	serial port	Spectra SP4000, SP5500, SP5500+*, SP6000, SP6000+*, SP7000, SP7000+*, SP65 Magellan MG5000, MG5050, MG5050+*, MG5075 DIGIPLEX EVO192*, EVOHD*, EVOHD+ (* firmware above 7.50)
DSC	data bus	PC585, PC1565, PC1616, PC1832, PC1864
Interlogix	data bus	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom	serial port	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Honeywell	data bus	Ademco Vista-15, Vista-20, Vista-48

On the newer Paradox panels marked with *, the serial port is locked from the factory; an external device can only communicate with it after it has been unlocked.

Soros port feloldás útmutató

Panels that can be controlled with a keyswitch – the communicator receives the events over the data bus or the serial port; control requires keyswitch wiring and programming (section 3.4):

Manufacturer	Connection	Models
Paradox	serial port	Spectra 1727, 1728, 1738 Magellan MG5050E ESPRIT E55, 728ULT, 738ULT DIGIPLEX EVO48
DSC	data bus	PC1404, PC5020
Texecom	serial port	Premier 412, 816, 832, 832+
Inner Range	data bus	Inception, Integriti
Crow	data bus	Runner 4/8, 8/16

The list changes from time to time; you can find the latest status in the Compatibility finder. In addition, it can also be used with the **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 and MATRIX 816**, the **DSC PC5015**, and the **Paradox DIGIPLEX EVO96 and NE96** control panels. The G16 does not work with **DSC PowerSeries NEO** control panels: the manufacturer does not allow external devices on the NEO bus, see DSC Power Series NEO and Trikdis communicators: compatibility and solutions.

1.3 Versions

This manual was written for **hardware version 4** of the G16, but it **can also be used for hardware version 3**: wiring, setup and operation of the two versions are largely the same. The manual applies equally to the 2G, 3G and 4G modem versions. The differences are summarized in the table below; where the text gives the data of version 4, take this into account for version 3.

	Hardware 3 (v3)	Hardware 4 (v4)
Models (in TrikdisConfig)	e.g. G16_3210 (2G); 3G and 4G modem versions were also made	G16_G410 (2G), G16_54E0 (4G)
Inputs/outputs	1 input of selectable type (IN) + 2 open-collector outputs (OUT1, OUT2, max. 0.15 A)	3 dual-function I/O terminals (I/O 1, I/O 2, I/O 3), each usable as an input or as an open-collector output (max. 0.15 A)
Setting the inputs/outputs	System settings page: **Input IN type**, **Output OUT1 & OUT2 mode**	**IN/OUT** page (section 6.6)
Current consumption	100 mA; up to 250 mA while sending	60–100 mA; up to 500 mA while sending
RS485 bus (iO-8, W485, E485)	only on the 3G and 4G versions	only on the 4G version (G16_54E0)

Hardware version 4 is made with two modems:

Model	Modem	Frequencies	RS485 (iO-8, W485, E485)
G16_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	no
G16_54E0	4G (LTE)	region-dependent LTE bands	yes

You can find the hardware version in the TrikdisConfig status bar (**HW**) and on the label on the back of the device. A separate article covers the announcement of version 4: The v4 hardware version of the G16 and G16T GSM communicators is arriving.

1.4 Main features

Connection to the alarm control panel

- It can be connected with up to 4 wires (+DC, −DC, CLK, DATA) to the panel's keypad bus (DSC, Caddx, Crow, Pyronix, Honeywell) or serial port (Paradox, Texecom, InnerRange); a factory cable is available for the serial port (Paradox: CRP2 / CRP2B, Texecom: CRP4).
- It forwards every event of the control panel with the full event information (code, partition, zone or user); it signals loss of the connection (TROUBLE LED, COMMUNICATION event).
- The directly controllable control panels can be armed and disarmed from the app with the keypad code; Protegus 2 also shows the state of the zones.

Communication with the monitoring station

- IP connection with Trikdis receivers (IPcom software receiver, RL14, RM14) and universal receivers (SIA DC-09, TL150).
- Primary, backup and parallel channel; backup SMS notification to the Trikdis SMS receiver (RL14, RM14, GM14).
- Message encryption AES-128; event buffer of 60 messages.

User functions

- Protegus 2 mobile and web app: notifications, event list, arming and disarming, switching outputs.
- Control and basic setup by SMS commands as well.
- Notification by SMS and phone call as well, to up to 4 phone numbers.
- Multi-level user rights in the app (administrator, installer, user).

Installation and setup

- The settings can be saved to a file and loaded into another communicator.
- Two access levels: administrator and installer.
- It can be configured and updated remotely with the TrikdisConfig software.

1.5 Parts of the communicator

The G16's printed circuit board comes in a white plastic case; the front cover can be removed, and the terminal block can be pulled off. The picture below shows the 4G version; the 2G version has no BAND LED and no A 485 / B 485 terminals.

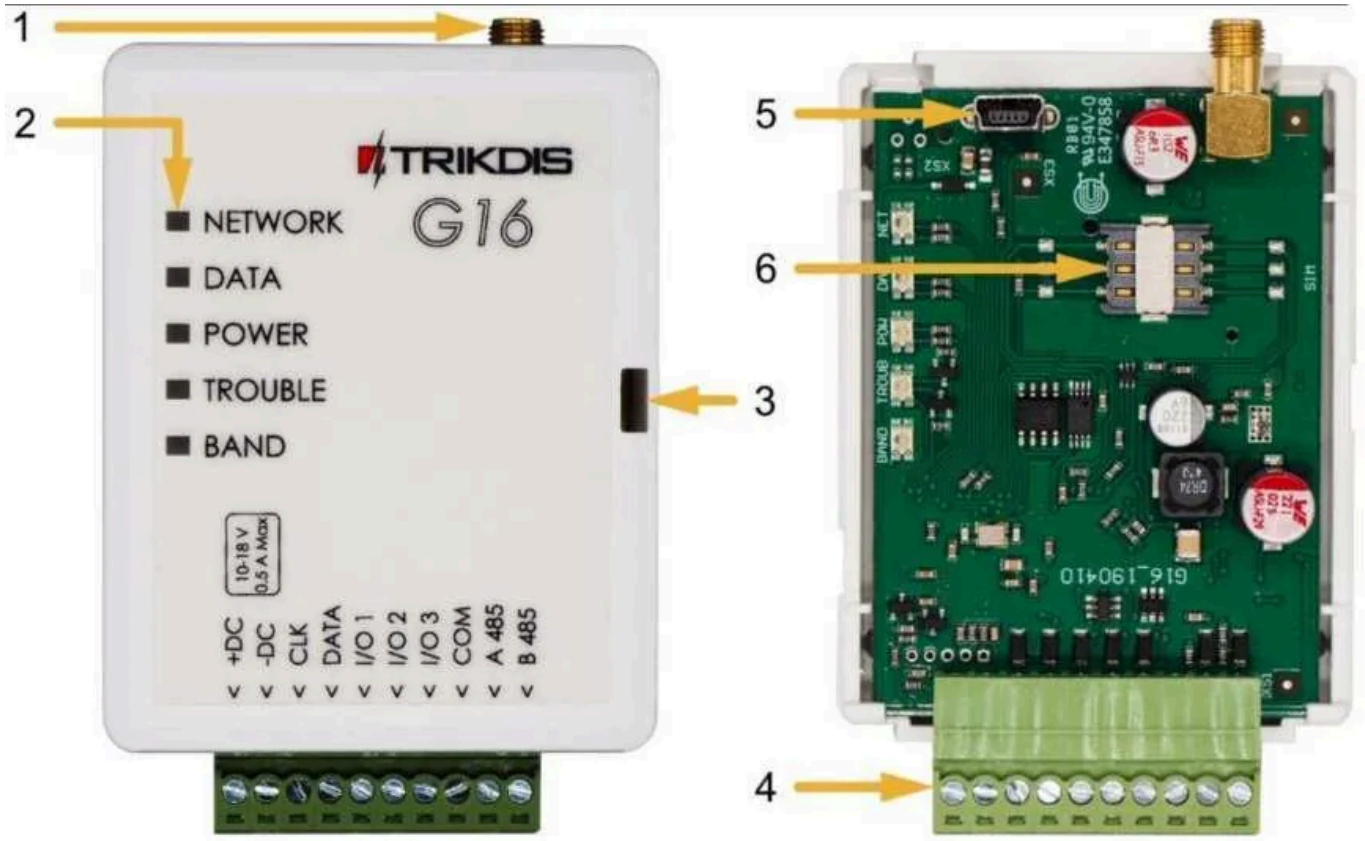


Figure 2. Parts of the G16 (4G version) from the front and with the case open.

- 1 SMA connector of the GSM antenna
- 2 LED indicators (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Slot that helps remove the front cover
- 4 Detachable terminal block
- 5 USB Mini-B socket for programming
- 6 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.

1.6 Terminals

Terminal	Function
+DC	Power, +10–18 V DC
–DC	Power, negative
CLK	Clock / serial line of the panel's bus
DATA	Data line of the panel's bus
I/O 1	Input/output 1 (default: not used)
I/O 2	Input/output 2 (default: input, NO)
I/O 3	Input/output 3 (default: output)
COM	Common (negative) point for the inputs and outputs
A 485	A line of the RS485 bus (4G version only)
B 485	B line of the RS485 bus (4G version only)

The terminal labels are also printed on the front cover, so you do not need to remove the cover during wiring. Which terminal of the control panel CLK and DATA go to differs by manufacturer – the wiring diagrams are in section 3.3.

1.7 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 (4G only) the network type.

NETWORK – network connection

Indication	Meaning
off	No connection to the mobile network
flashing yellow	Connecting to the mobile network
steady green	Connected to the mobile network
steady green, flashing yellow	Connected; the number of yellow flashes is the **signal level**: on 2G 5 flashes, on 4G 3 flashes means a good signal

DATA – data traffic

Indication	Meaning
off	No messages waiting to be sent
steady green	There are messages waiting to be sent in the buffer
flashing green	Data is being sent or received (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 (USB cable plugged in)
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/LTE)
6 red flashes	No connection to the monitoring station receiver and/or the Protegus server (the cause can also be a fault in the internet connection)
7 red flashes	Connection to the alarm control panel lost (bus or serial connection)
flashing red (during programming)	Memory error
steady red (during programming)	Corrupted firmware

BAND – network type (4G version only)

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

1.8 Technical specifications

Parameter	Value
Connection to the alarm control panel	keypad bus or serial port, depending on the panel type (up to 4 wires: +DC, −DC, CLK, DATA; on the Caddx and Pyronix bus CLK is not used)
Inputs/outputs	3 dual-function I/Os (I/O 1, I/O 2, I/O 3): 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
Expansion	on the RS485 bus (4G version only): iO-8 expander (+8 I/O) and other iO series expanders; W485 Wi-Fi, E485 Ethernet module
2G modem	850 / 900 / 1800 / 1900 MHz
4G modem	region-dependent LTE bands
Supply voltage	10–18 V DC
Current consumption	60–100 mA nominal; up to 500 mA while sending
Transmission protocols	TRK, DC-09_2007, DC-09_2012, TL150
Event buffer	60 messages

Parameter	Value
Encryption	AES-128
Programming	TrikdisConfig (Windows) over a USB Mini-B cable or remotely; SMS commands
Operating environment	−10 … +50 °C, max. 80 % relative humidity (at +20 °C)
Dimensions	92 × 65 × 26 mm
Weight	80 g

2. Quick start with TrikdisConfig

All settings of the G16 are made with the Windows program called **TrikdisConfig** – over a USB 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. The settings are explained in detail in chapter 6.

2.1 Preparation

What you will need

USB Mini-B cable · cable with at least 4 cores for the panel's bus – a **CRP2** or **CRP2B** cable for the Paradox serial port, a **CRP4** cable for the Texecom serial port · 2.5 mm flat screwdriver · mobile antenna with suitable gain (a higher-gain antenna where coverage is weak) · active nano SIM card with mobile data service (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 G16's front cover. Insert a flat screwdriver into the slot on the top edge of the cover and, levering downwards, gently snap the front cover off. The figure below shows the opening and the location of the USB socket.

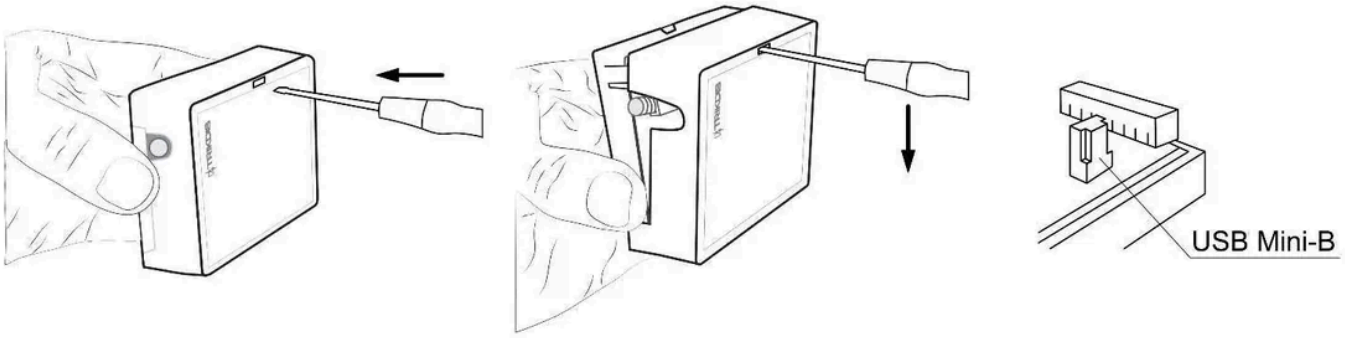


Figure 3. Snapping off the front cover with a flat screwdriver (left, middle) and the location of the USB Mini-B socket on the printed circuit board (right).

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).

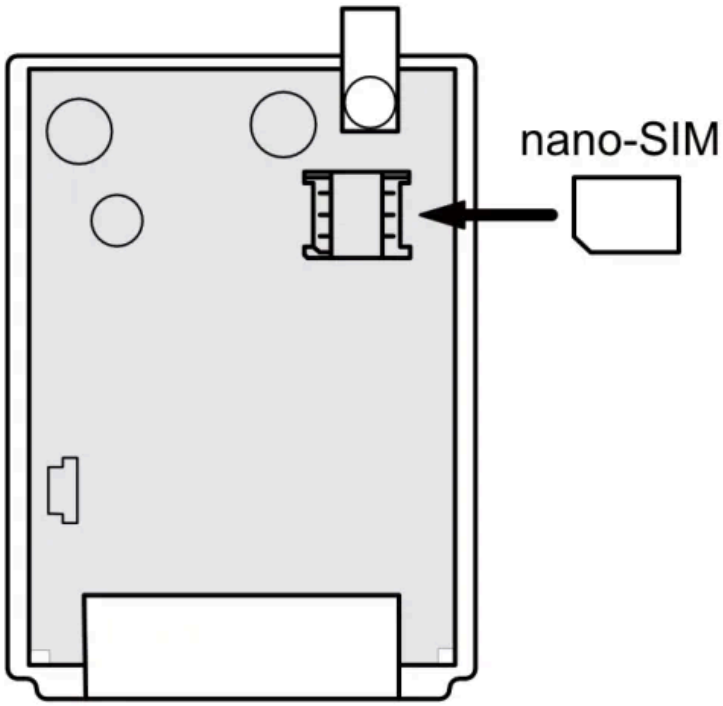


Figure 4. Location of the nano SIM card on the printed circuit board.

4. Connect the G16 to the computer with a USB Mini-B cable. USB supplies enough power for programming, no separate power supply is needed.

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 Control panel type and direct control

Whichever operating mode you use, first specify on the **System settings** page what control panel the communicator will be connected to.

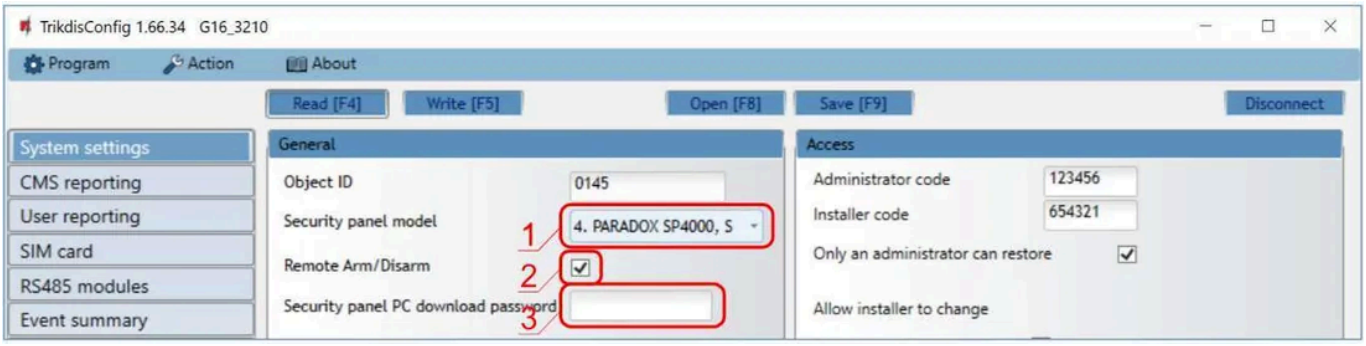


Figure 5. TrikdisConfig – System settings page, General group.

- 1 **Security panel model** – the type of the connected alarm control panel from the list; how the communicator reads the bus depends on it.
- 2 **Remote Arm/Disarm** – tick it if the user wants to arm and disarm the control panel from the Protegus 2 app with their own keypad code. It only appears for the directly controllable models; with the other control panels, arming can be solved with a keyswitch zone (section 3.4) – in that case leave it empty.
- 3 **Security panel PC download password** – for Paradox and Texecom control panels, the panel's PC or UDL password (4 characters); it must match the one set in the control panel. The field appears after ticking Remote Arm/Disarm.

Several control panels also need a setting in the control panel itself: Caddx, Honeywell and InnerRange control panels already for reading events (enabling the bus or the serial port), Paradox and Texecom control panels for direct control (PC or UDL password) – chapter 4 describes this by manufacturer, together with changing the password.

2.3 Connection to the Protegus 2 app

If the user wants to see and control the system from the Protegus 2 app, set the following on the **User reporting** page, on the **PROTEGUS Cloud** tab.



Figure 6. TrikdisConfig – User reporting, PROTEGUS Cloud tab.

- 4 **Enable connection** – tick it: it enables the connection to the Protegus cloud.
- 5 **Protegus Cloud access code** – change the default password `123456`. This is what you will have to enter in the app when creating the system; **it cannot be changed after the system has been created.**

Then enter the card's data on the **SIM card** page.

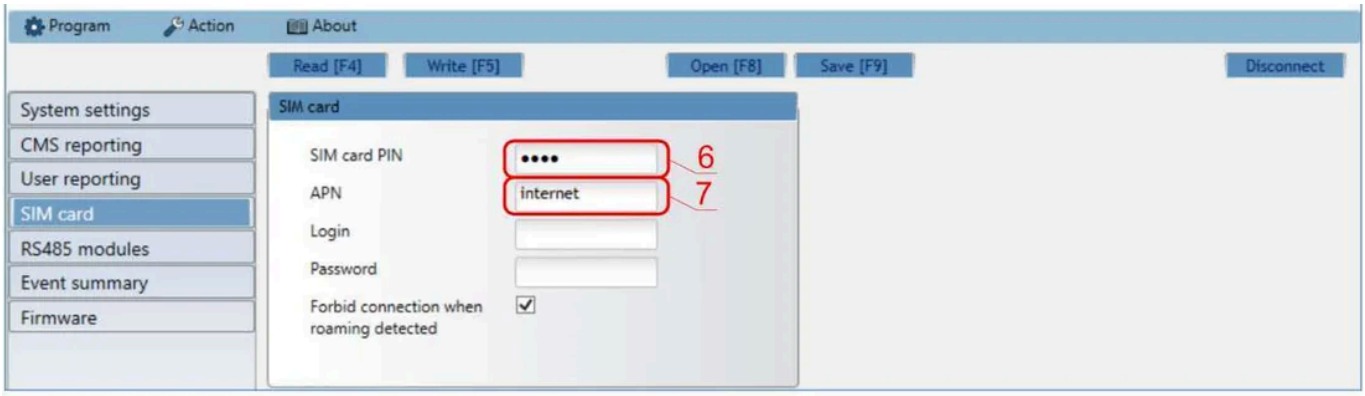


Figure 7. TrikdisConfig – SIM card page.

- 6 **SIM card PIN** – the card's PIN code (if the PIN request is switched off, the default value can stay).
- 7 **APN** – the operator's data access point (see below).

The APN (Access Point Name) is the mobile operator's data access point; without it the device cannot connect to the internet. You get the exact value from the SIM card's operator, and you can also find it on the operator's website; the APN "internet" is generic and works in many operators' networks. We keep the known APNs of European operators in a separate article: APN settings – list of European mobile operators.

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.

2.4 Connection to the monitoring station

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

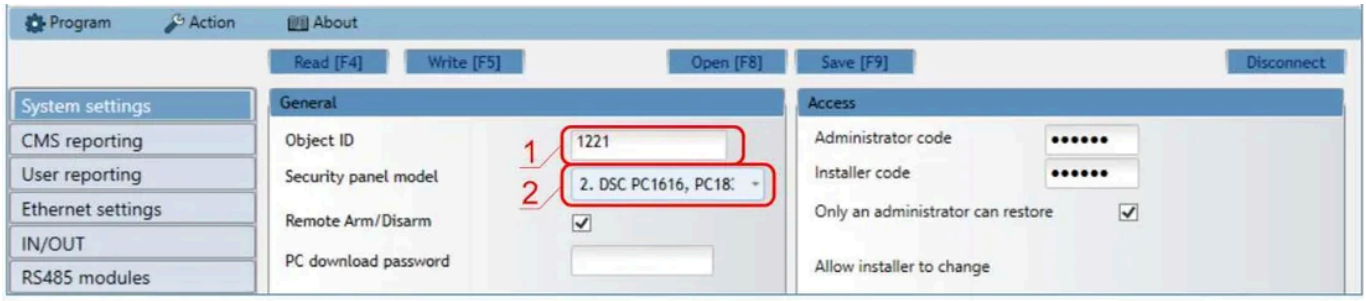


Figure 8. TrikdisConfig – System settings page, General group.

- 1 **Object ID** – the object ID received from the monitoring station (4 hexadecimal characters, 0–9, A–F). `FFFE` and `FFFF` cannot be used.
- 2 **Security panel model** – the type of the connected alarm control panel (if you have not set it in section 2.2 yet).

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

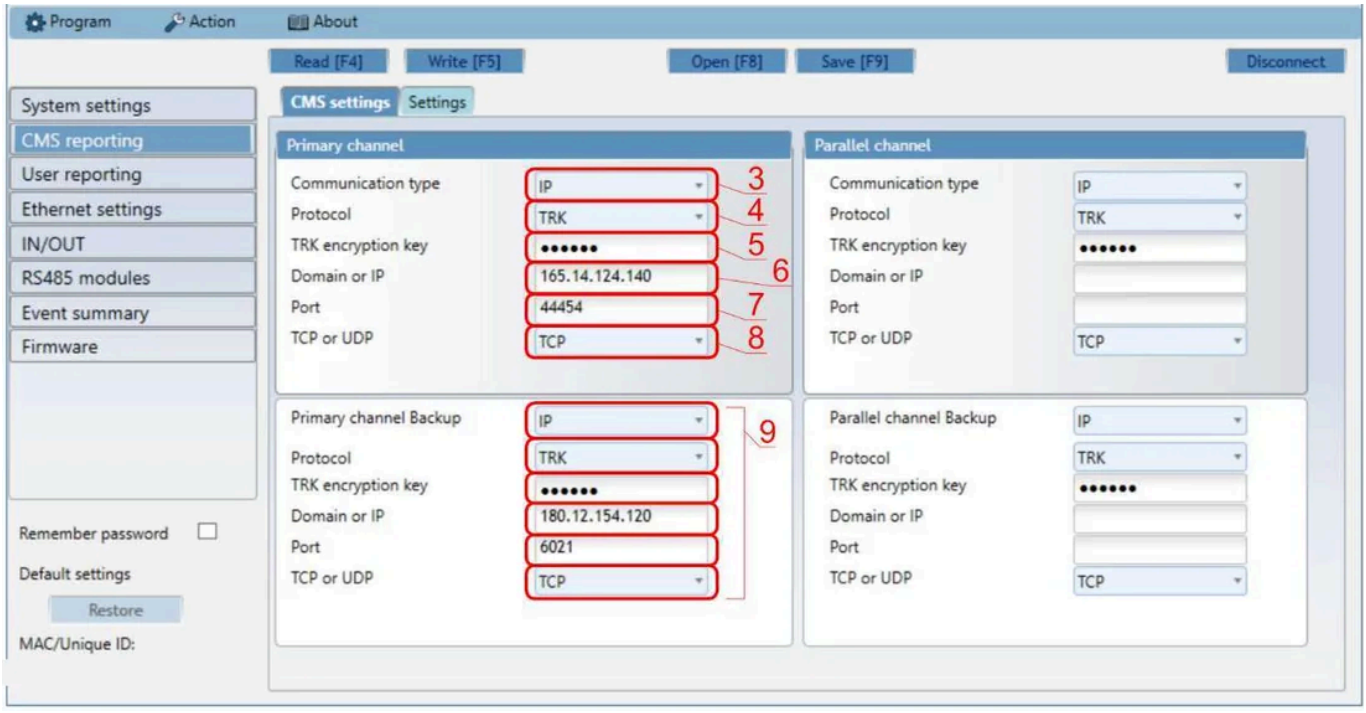


Figure 9. TrikdisConfig – CMS reporting, CMS settings tab.

- 3 **Communication type** – choose the **IP** connection (SMS is not recommended as the primary channel).
- 4 **Protocol** – **TRK** for a Trikdis receiver, **DC-09_2007** or **DC-09_2012** for a universal receiver, **TL150** for a SUR-GARD receiver.
- 5 **TRK encryption key** – the 6-digit encryption key set in the receiver.
- 6 **Domain or IP** – the receiver's domain name or IP address.
- 7 **Port** – the receiver's port number.
- 8 **TCP or UDP** – the transmission protocol; it follows the receiver's setting.
- 9 **Primary channel Backup** – backup channel for a failure of the primary; fill it in the same way, it is recommended.

It is also recommended to set the **Parallel channel** and its backup channel if the events must reach two receivers; and in the **Backup SMS reporting number** field – this is also recommended – you can enter the phone number of the Trikdis SMS receiver: the device sends an SMS here immediately after the first start, and afterwards it reports by SMS when none of the IP channels work.

Finally, enter the card's data on the **SIM card** page if you have not done so in section 2.3.

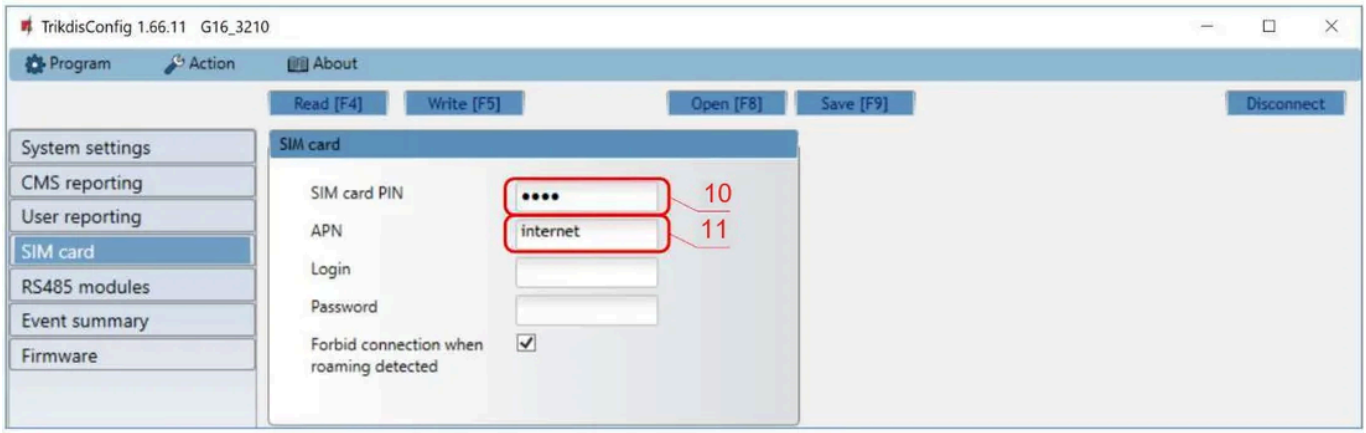


Figure 10. TrikdisConfig – SIM card page.

- 10 **SIM card PIN** – the card's PIN code.
- 11 **APN** – the operator's access point (see section 2.3).

SMS reporting to the monitoring station only works with a Trikdis receiver (RL14 IP/SMS receiver, RM14 multi-channel receiver or GM14 SMS receiver); in that case only the encryption key and the phone number are needed. With the **DC-09** protocol, also enter the DC-09 object, line and receiver number on the **Settings** tab.

At the end of the settings, press the **Write [F5]** button, wait for the confirmation, and unplug the USB cable. The device is now ready to be wired in.

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 if you did not do so during commissioning.
3. Take the printed circuit board out of the back cover: open the latch in the corner (see the figure).
4. Fix the back cover with screws at the chosen location.
5. Put the printed circuit board back into the back cover and plug the terminal block back in.
6. Screw on the GSM antenna.
7. Put the front cover back on.

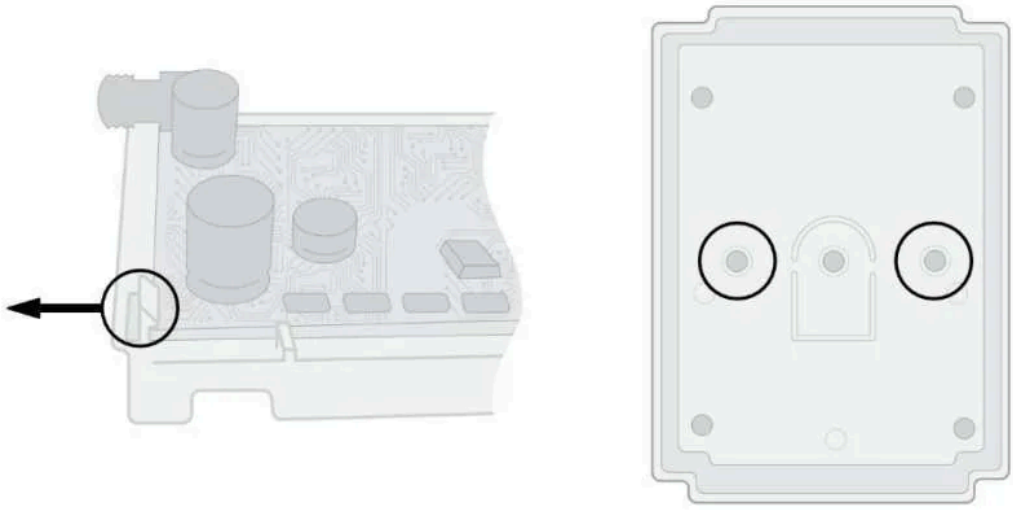


Figure 11. Removing the printed circuit board: opening the latch in the corner (left) and the mounting holes of the back cover (right, circled).

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

3.2 Placement and antenna

- Put the communicator in a **dry, indoor** place, preferably near the alarm control panel's enclosure, so that the bus wiring is short.
- In a **metal enclosure** the mobile signal is weakened considerably. If the communicator goes into the 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 should be at least 5 on 2G and at least 3 on 4G (see section 1.7). If it is less, look for 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 panel's transformer and from mains wiring.



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

The G16 connects to the control panel with **up to four wires** (on the Caddx and Pyronix bus CLK is not used): the **+DC** and **–DC** terminals get the panel's 12 V auxiliary power (AUX), the **CLK** and **DATA** terminals get the two data lines of the panel's keypad bus or serial port. Which terminal of the control panel is which differs by manufacturer – wire according to the diagrams below. For control panels with a serial port (Paradox, Texecom) a factory cable is available, one end of which fits the panel's connector, while the other end can be wired into the G16's terminal block.

The G16 can draw up to 500 mA while sending. Check that the panel's AUX output can supply this together with the other devices connected to it. As the power comes from the control panel, during a power cut the panel's battery also powers the communicator. Most control panels are not damaged by swapped wires of a device connected to the bus, but swapping **+DC and –DC** can destroy the communicator – check the polarity before wiring.

After wiring, select the type of the connected control panel in the TrikdisConfig **System settings** → **Security panel model** field (section 2.2); with some manufacturers a setting is also needed in the control panel (chapter 4).

3.3.1 DSC PowerSeries

The four Keybus terminals: **RED** → +DC, **BLK** → –DC, **YEL** → CLK, **GRN** → DATA.

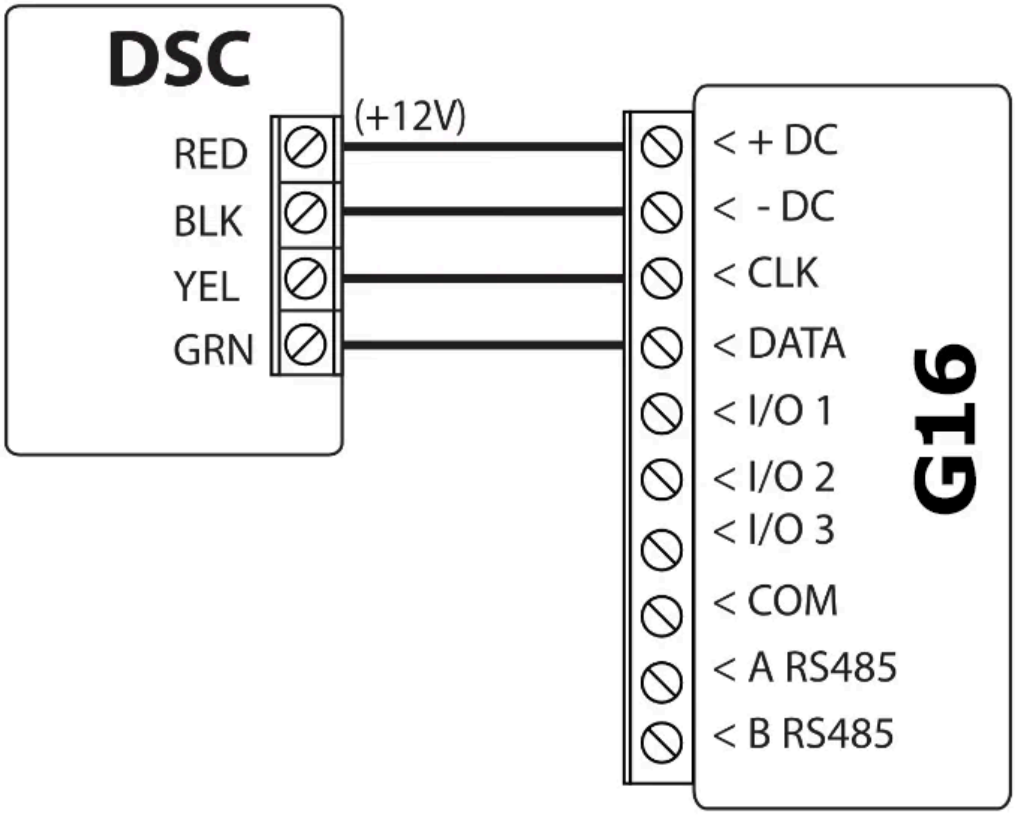


Figure 12. Connection to the Keybus of a DSC PowerSeries control panel (keypad bus, "Keypad bus"): RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

The communicator connects to the **serial port** (SERIAL) of Paradox control panels with the factory **CRP2** or **CRP2B** cable; the panel end of the cable fits the serial connector, and you wire the other end into the G16's terminal block. The 4 pins of the connector: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. The wire colours of the two cables differ – the diagram shows the colour assignment of both cables. The markings of the Paradox serial connector: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

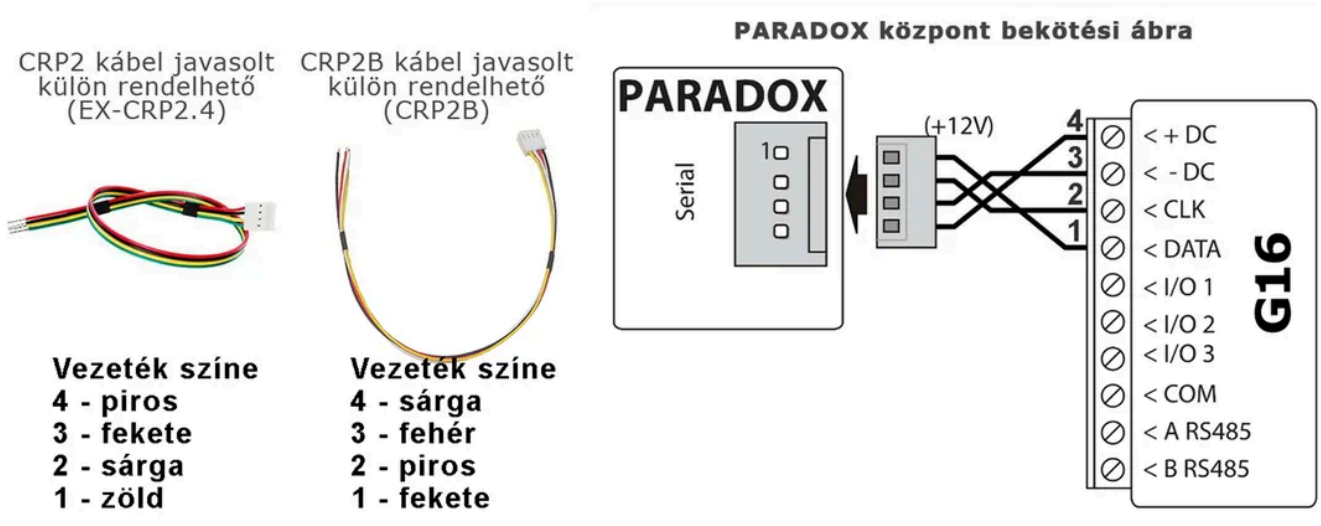


Figure 13. Connection to the serial port of a Paradox control panel with a CRP2 (EX-CRP2.4) or CRP2B cable. CRP2: 4 red → +DC, 3 black → −DC, 2 yellow → CLK, 1 green → DATA. CRP2B: 4 yellow → +DC, 3 white → −DC, 2 red → CLK, 1 black → DATA.

On the newer Paradox control panels the serial port may be locked at the factory – the unlocking procedure is in section 4.2 and in the article Unlocking a locked serial port on Paradox alarm control panels.

3.3.3 UTC Interlogix (Caddx) NetworX

The three terminals of the keypad bus: **POS** → +DC, **COM** → −DC, **DATA** → DATA. The **CLK** terminal is not used.

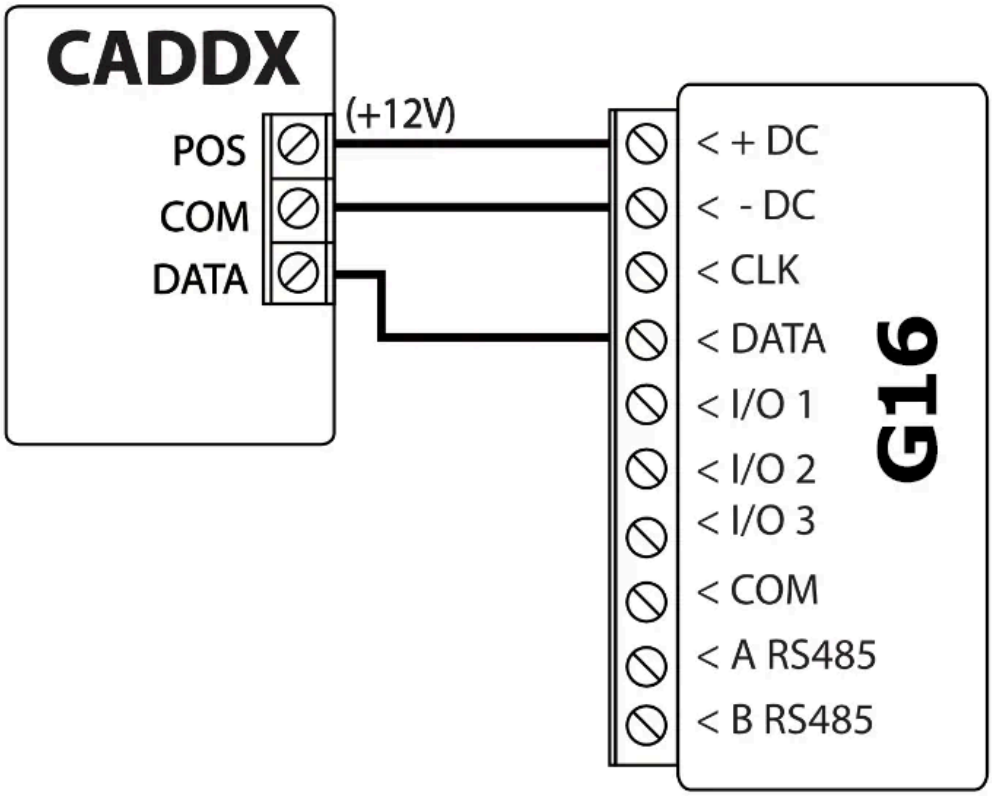


Figure 14. Connection to the keypad bus (“Keypad bus”) of a Caddx NetworX control panel: POS → +DC (+12 V), COM → −DC, DATA → DATA; CLK stays free.

3.3.4 Texecom Premier / Premier Elite

The communicator connects to the panel's serial port with the factory **CRP4** cable: **red (R)** → +DC, **black (B)** → −DC, **blue (BL)** → CLK, **white (W)** → DATA.

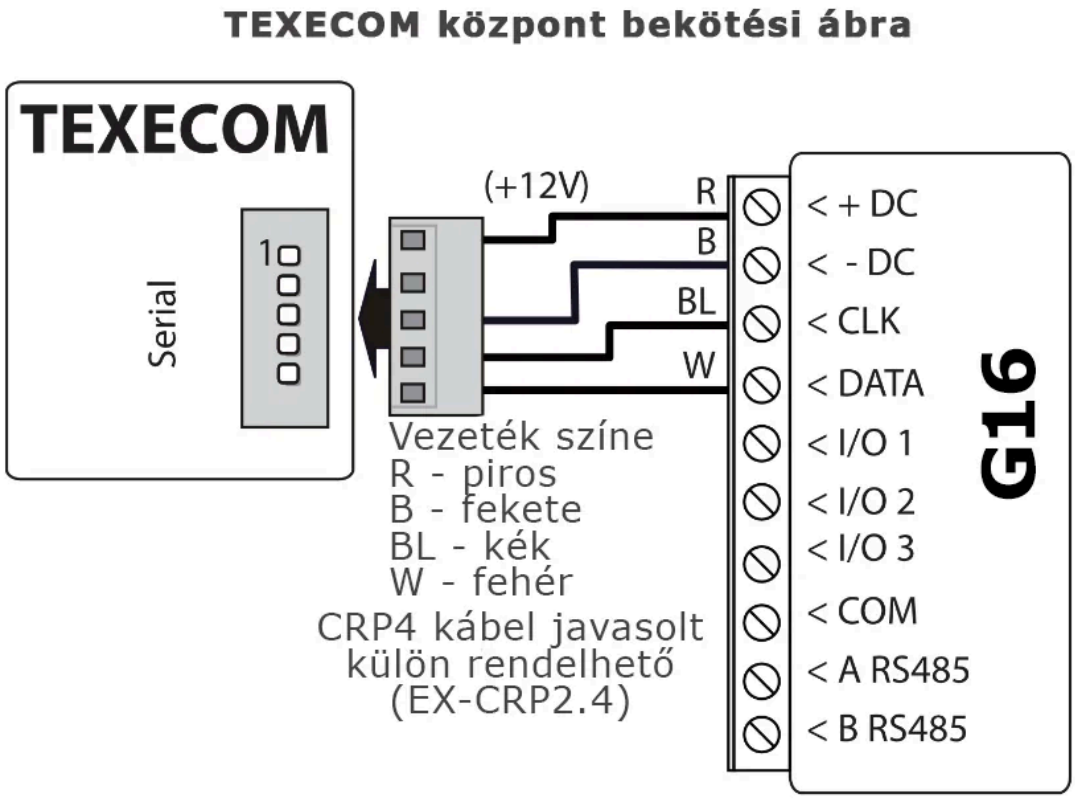


Figure 15. Connection to the serial port of a Texecom control panel with a CRP4 cable: red → +DC, black → −DC, blue → CLK, white → DATA.

3.3.5 Crow Runner

The keypad bus of the Crow Runner 4/8 and Runner 8/16: **POS** → +DC, **NEG** → −DC, **CLK** → CLK, **DATA** → DATA.

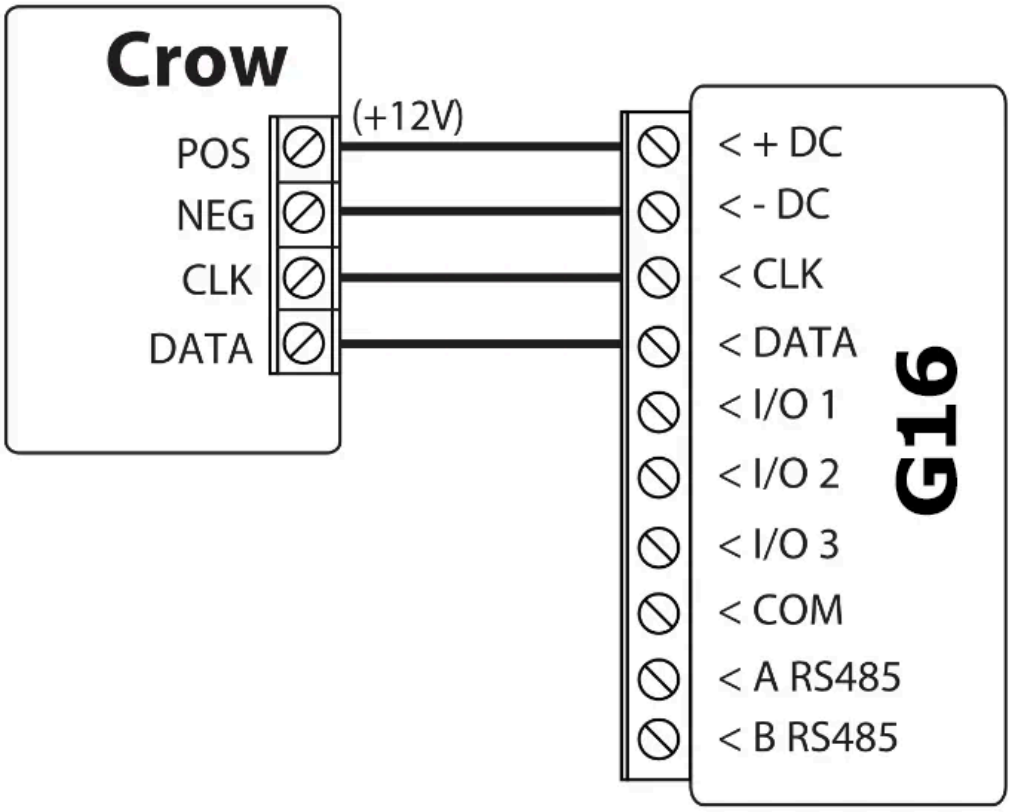


Figure 16. Connection to the keypad bus ("Keypad bus") of a Crow Runner 4/8 and Runner 8/16 control panel: POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

The keypad bus of Pyronix control panels: **+AUX** → +DC, **−AUX** → −DC, **KD** → DATA. The **CLK** terminal is not used. After wiring and setting up the communicator, power the control panel off and restart it so that it accepts the communicator (section 4.5).

3.3.7 Honeywell Ademco Vista

The numbered terminals of the keypad bus of the Vista-15, Vista-20 and Vista-48 control panels: **5** (AUX +) → +DC, **4** (AUX −) → −DC, **7** (data out, yellow) → CLK, **6** (data in, green) → DATA.

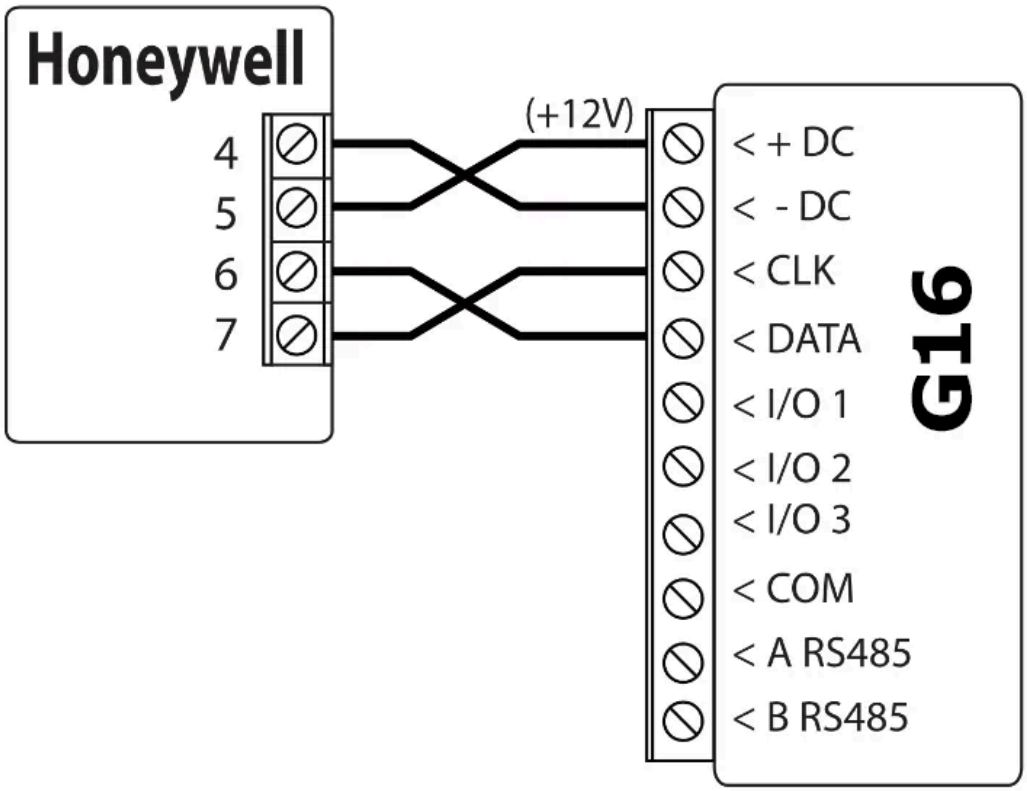


Figure 17. Connection to the keypad bus ("Keypad bus") of a Honeywell Vista-20 / Vista-48 control panel: 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception and Integriti

The communicator gets its power from the power terminals of the **Inception** control panel (**VOUT +** → +DC, **0V** → −DC), while the data connection is made from the panel's USB port with the InnerRange 993030USB cable: **black** → 0V (−DC), **green** → CLK, **white** → DATA. Use of the serial port must be enabled in the control panel (section 4.7).

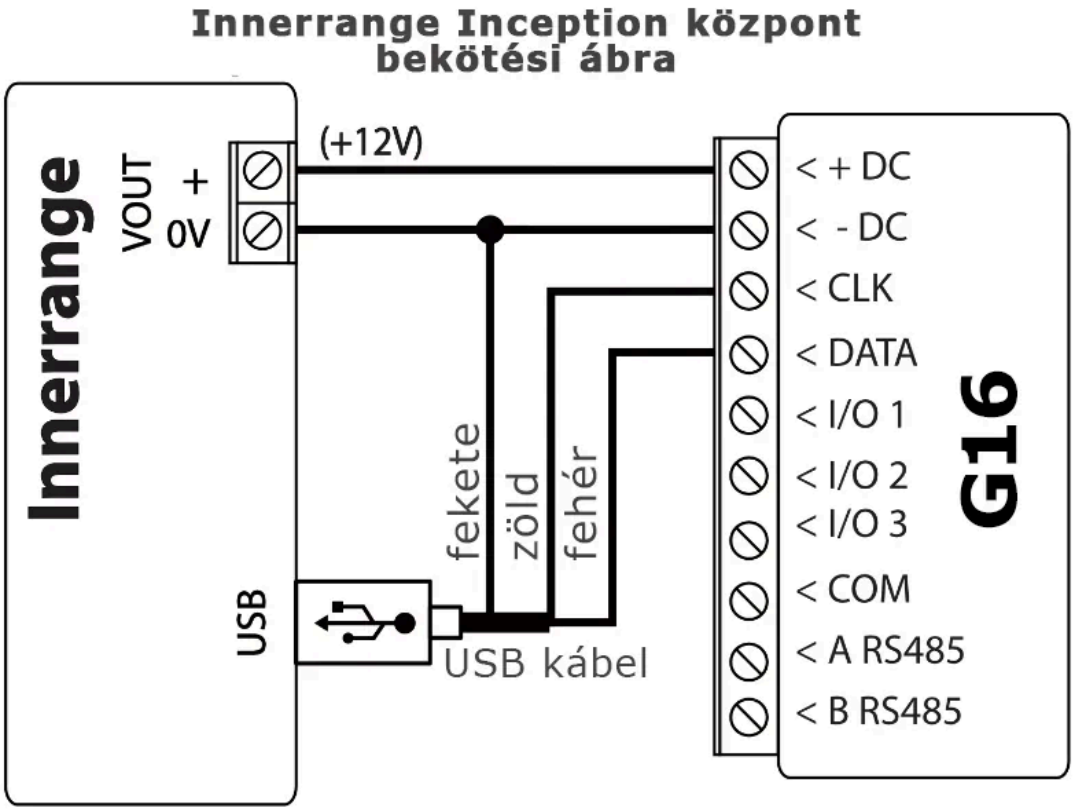


Figure 18. Connection to an InnerRange Inception control panel: power from the VOUT + and 0V terminals, data from the USB port with the 993030USB cable (black → 0V, green → CLK, white → DATA).

The **Integriti** control panel can be connected to its Port 0 with the INTG-996795 cable: **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA.

3.4 Wiring a keyswitch zone

If the control panel is not one of the directly controllable models, or you do not want to use direct control, remote arming and disarming can be solved with a **keyswitch zone**: you set one of the communicator's I/O terminals as an **output** (IN/OUT page, section 6.6) and connect it to a keyswitch zone of the control panel. When activated, the output pulls the zone to COM (negative); wire the zone's end-of-line resistor according to the panel's zone type. As the G16 has three I/O terminals, up to three partitions can be handled with separate outputs.

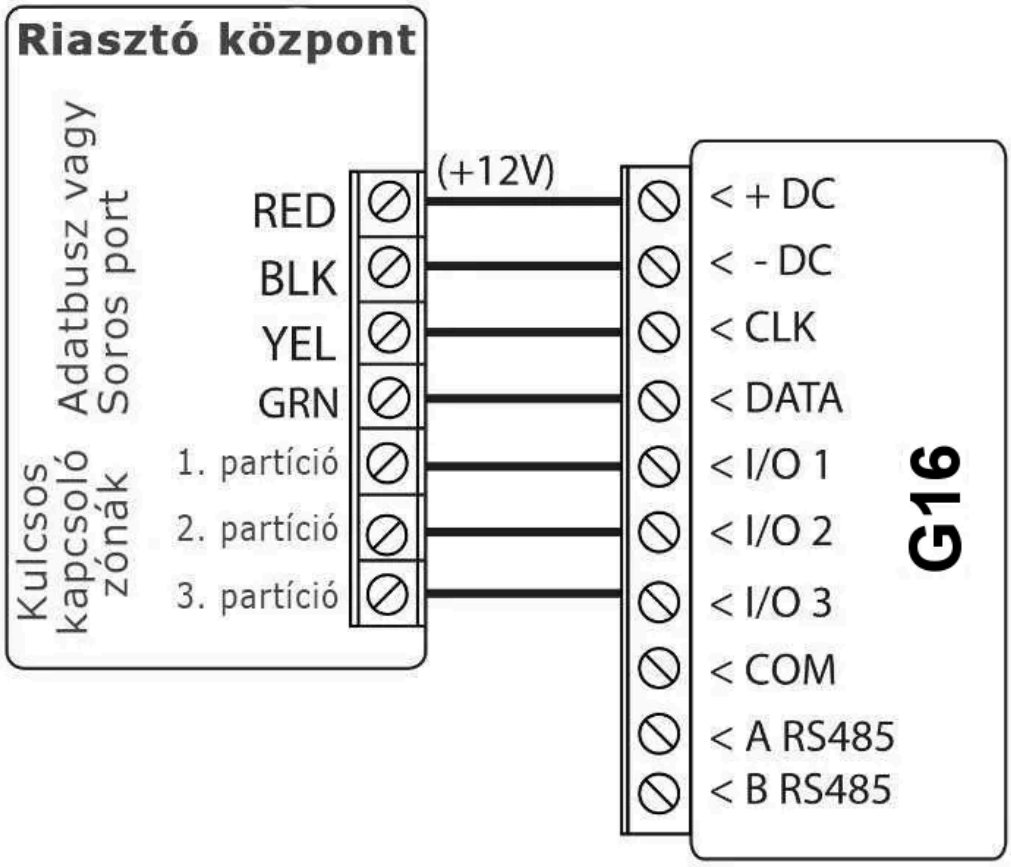


Figure 19. Arming and disarming with a keyswitch zone: the communicator reads the events from the panel's bus, and outputs I/O 1–3 switch the keyswitch zone of partitions 1–3 of the control panel.

- On the TrikdisConfig **System settings** page, **Remote Arm/Disarm** must stay **empty** – the two cannot be used at the same time.
- The keyswitch zone can be pulse or two-state (latched); the same mode must be set in the Protegus 2 app (section 5.3).
- On **hardware version 3** the two outputs (OUT1, OUT2) can handle two partitions; the **System settings** → **Output OUT1 & OUT2 mode** field must be set to **Remote control** (default).

A separate article covers the details and pitfalls of keyswitch arming: Remote arming with a keyswitch from the Protegus 2 app.

3.5 Wiring inputs

As inputs, the communicator's I/O terminals can also be used to receive additional detectors (e.g. tamper switch, panic button, temperature switch), independently of the alarm control panel. The input must be connected between the selected I/O and the COM terminal.

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	–

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

Wiring of input circuits: NO, NC, NC/EOL, NO/EOL, NO/DEOL and NC/DEOL types with a 2.2 kΩ end-of-line resistor; with the DEOL types the tamper circuit is also wired.

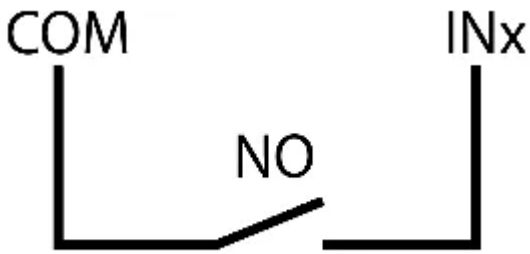


Figure 20. NO – normally open circuit: closed – alarm, open – normal state.

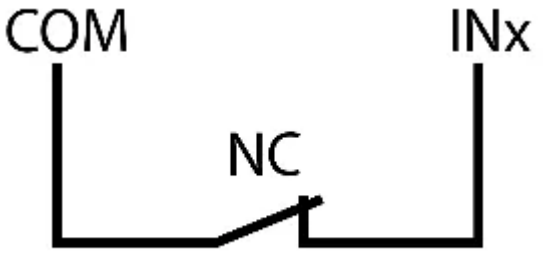


Figure 21. NC – normally closed circuit: open – alarm, closed – normal state.

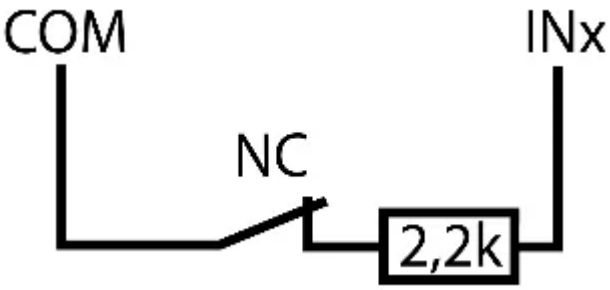


Figure 22. NC/EOL – normally closed circuit with a 2.2 kΩ end-of-line resistor: short circuit or open circuit – alarm, 2.2 kΩ – normal state.

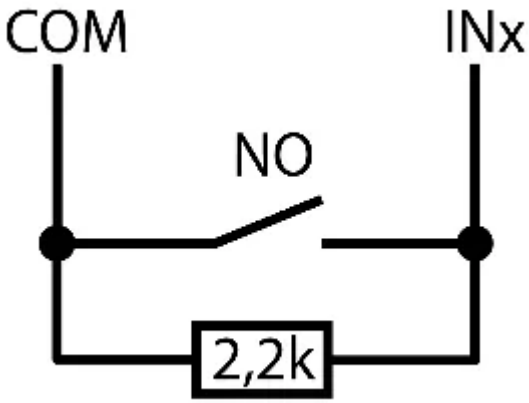


Figure 23. NO/EOL – normally open circuit with a 2.2 kΩ end-of-line resistor: short circuit or open circuit – alarm, 2.2 kΩ – normal state.

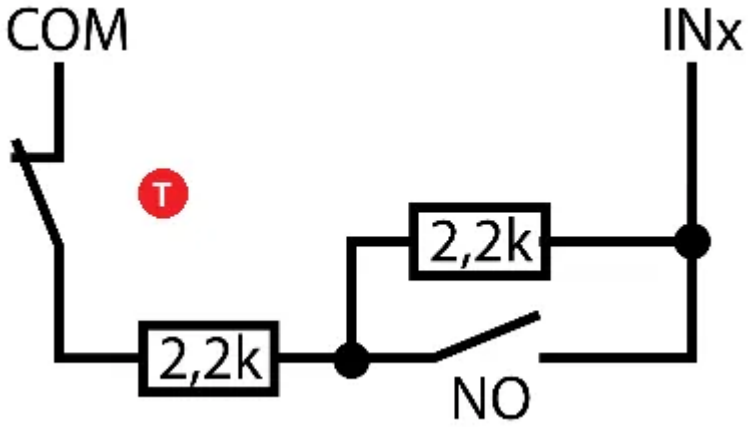


Figure 24. NO/DEOL – normally open circuit with a 2.2 kΩ end-of-line resistor and tamper detection: short circuit or open circuit – tamper, 2.2 kΩ – alarm, 3.3–5.5 kΩ – normal state.

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

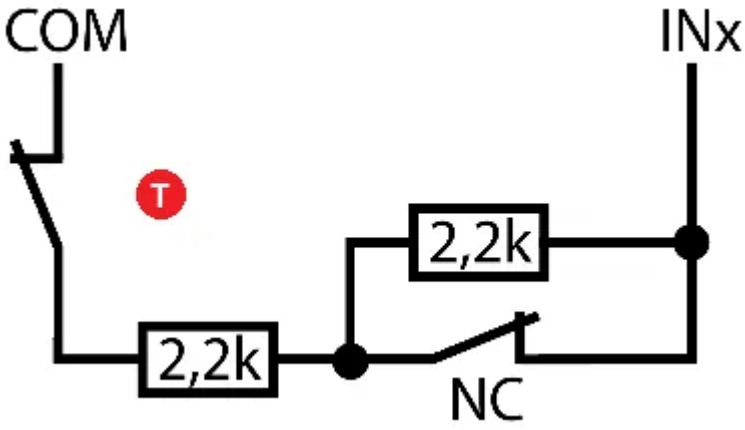


Figure 25. NC/DEOL – normally closed circuit with a 2.2 kΩ end-of-line resistor and tamper detection: short circuit or open circuit – tamper, 2.2 kΩ – normal state, 3.3–5.5 kΩ – alarm.

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

Hardware version 3 has one input (IN); you set its type in the **System settings** → **Input IN type** field.

3.6 Wiring 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. Switch a larger consumer or a mains-voltage device **through a relay**: one end of the relay coil goes to +DC, the other to the I/O terminal. With the relay contacts, various electrical devices can be switched on and off. For this, the I/O terminal must be set as an output (**OUT**) on the TrikdisConfig **IN/OUT** page (section 6.6).

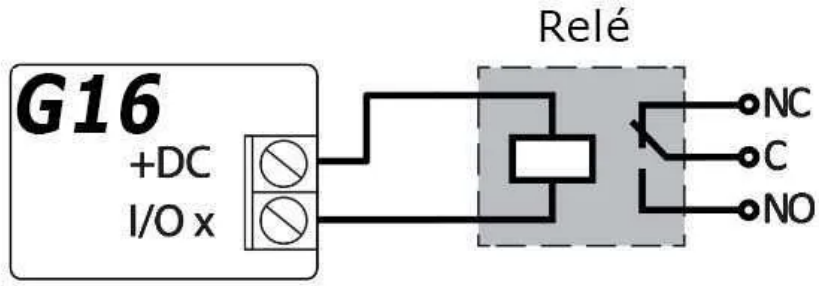


Figure 26. Connecting a relay to the communicator's output: the coil goes between +DC and the I/O x terminal, the contacts (NC, C, NO) switch the consumer.

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

3.7 Wiring the iO-8 expander

If more inputs or outputs are needed, up to four **iO-8** expanders can be connected to the RS485 bus of the **4G version**; each gives 8 more dual-function I/Os. Connect the A 485 and B 485 terminals to the A and B terminals of the module, and take the module's power from the panel's 12 V AUX output. The iO-8's own manual also describes how to connect it. The module must be added on the TrikdisConfig **RS485 modules** page (section 6.7); the events of the inputs go to the monitoring station and to Protegus 2, the outputs can be switched from the app.

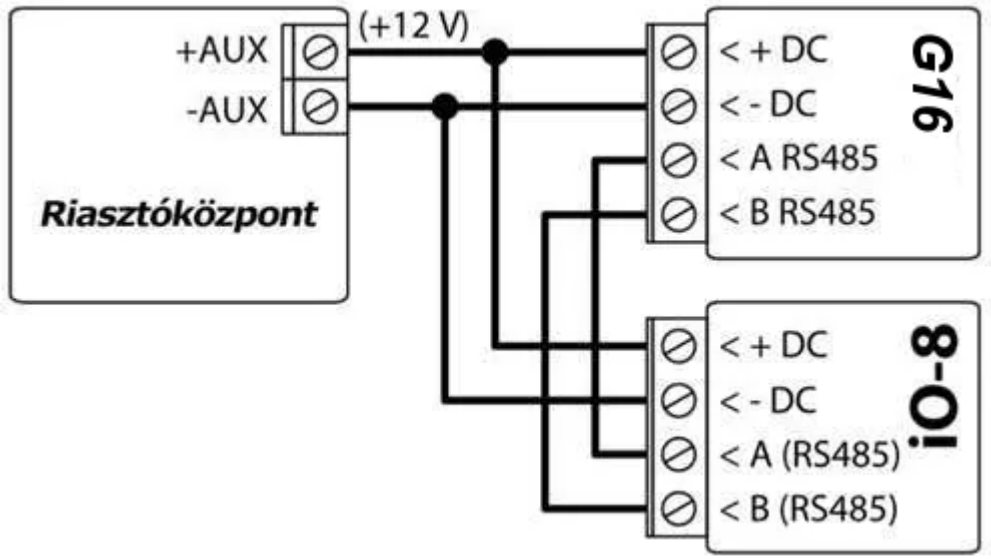


Figure 27. Connecting an iO-8 expander to the G16's RS485 bus (A 485 → A, B 485 → B); both devices are powered from the alarm control panel's AUX output (+12 V).

The G16 with the 2G modem (G16_G410) has no RS485 bus, so iO-8, W485 and E485 modules cannot be connected to it.

3.8 Wiring the W485 and E485 modules

Ethernet or Wi-Fi expansion – W485 and E485. The communicator can be extended with a W485 Wi-Fi or E485 Ethernet module: the events then travel over wired internet or Wi-Fi to the monitoring station and to the Protegus 2 app.

- **Connection:** on the RS485 bus, from the same power supply as the communicator (the module's power input is 9–28 V DC); no separate power supply is needed.
- **The internet is the primary channel:** as long as it is up, everything goes through it. If it drops, the communicator automatically switches to the mobile network, and as soon as the internet returns, it switches back to IP.
- **Not just for reporting:** the Protegus 2 app (notifications, remote control) also works over this channel.
- **E485** – wired Ethernet (RJ45). **W485** – Wi-Fi 2.4 GHz (WPA / WPA2), where no UTP cable has been run.
- If required, it can also be used without a SIM card. Configuration: with the TrikdisConfig software, over USB.

Trikdis E485 Ethernet module (RS485) | **Trikdis W485 Wifi module (RS485)**

As long as the Wi-Fi or Ethernet connection is up, the G16 communicates through it and does not use the mobile data connection; if the connection drops, it switches to the mobile data connection, and when the connection is restored it returns to the module. For the module to work, **there must be a SIM card in the G16**.

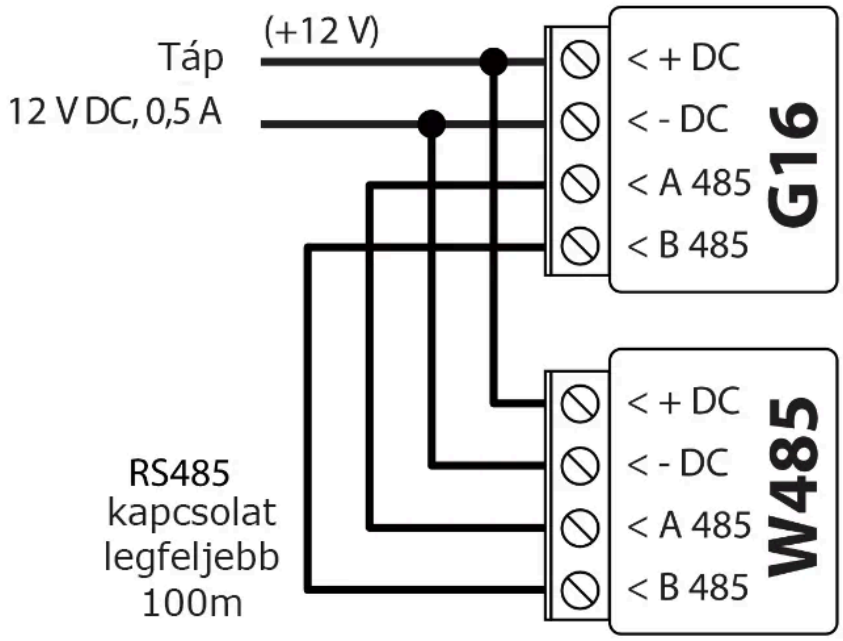


Figure 28. Connecting a W485 Wi-Fi module to the G16 over the RS485 bus. The two devices run from a common 12 V DC power supply (at least 0.5 A) (the module's power input is 9–28 V DC); the RS485 cable can be up to 100 m long.

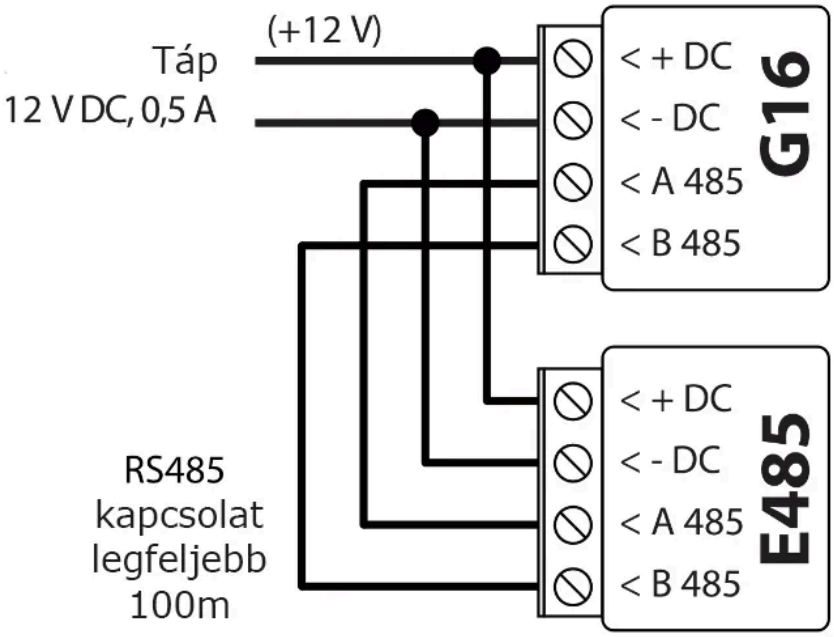


Figure 29. Connecting an E485 Ethernet module to the G16 over the RS485 bus. The two devices run from a common 12 V DC power supply (at least 0.5 A) (the module's power input is 9–28 V DC); the RS485 cable can be up to 100 m long.

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

You make the modules' network settings on the TrikdisConfig **RS485 modules** page (section 6.7).

3.9 Power-up 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 starts when the alarm control panel 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 flashes is the signal level (5 on 2G, 3 on 4G is good);
- **TROUBLE** off.

If the NETWORK LED gives fewer yellow flashes, the signal level is not sufficient: find another place for the communicator, or use a more sensitive antenna (section 3.2). Any other LED indication signals some fault – identify it using the tables in section 1.7. If TROUBLE is flashing, the number of flashes tells the cause (section 1.7). **7 flashes** signal that there is no connection to the control panel: check the CLK and DATA wires, the selected control panel type and – where needed – the panel's programming (chapter 4). If none of the LEDs light up, check the power supply and the wiring.

4. Programming the alarm control panel

This chapter describes by manufacturer what needs to be set in the alarm control panel so that the G16 reads the events and – where possible – controls the control panel remotely. With most control panels nothing needs to be programmed for reading events; for **direct control**, tick the **Remote Arm/Disarm** option on the TrikdisConfig **System settings** page, and for Paradox and Texecom control panels also enter the panel's PC or UDL password in the **Security panel PC download password** field (sections 2.2 and 6.2).

If you control the control panel not directly but through a keyswitch zone (section 3.4), **Remote Arm/Disarm** must stay empty, and this chapter only applies to the settings needed for reading events.

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 Crow and Pyronix

The **Crow Runner 4/8** and **Runner 8/16** panels do not require any special settings.

Pyronix panels do not require programming either, but after setting up and wiring the communicator, **power down the panel completely** (mains and battery) and restart it: the panel accepts the communicator connected to its bus at start-up.

4.6 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]**.

4.7 InnerRange Inception and Integriti

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.

The Inception and the Integriti pass the events to the communicator; arming and disarming needs a keyswitch zone (sections 1.2 and 3.4).

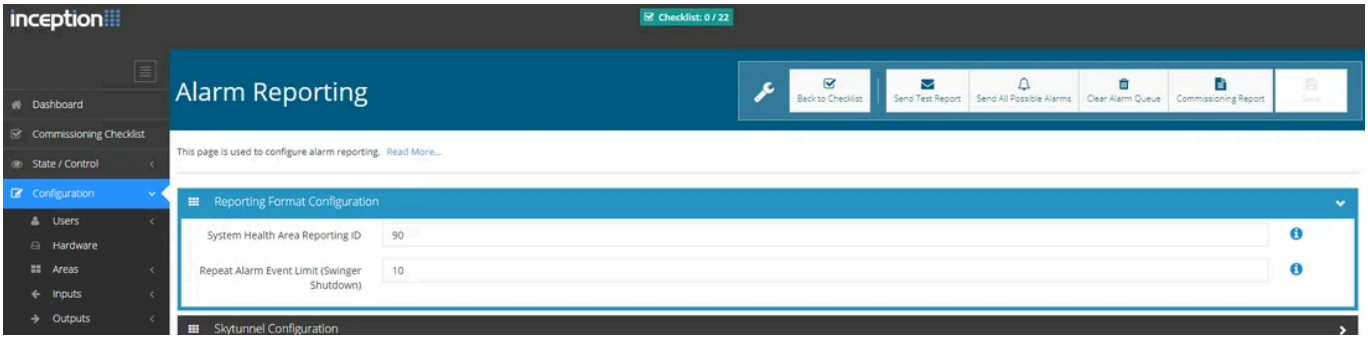


Figure 30. Inception web interface – Configuration → General → Alarm Reporting.



Figure 31. Inception – 3rd Party Device Configuration.

- 1 **Enable 3rd Party Device Reporting** – ticked.
- 2 **3rd Party Device Type** – Trikdis.
- 3 **Serial Port** – Serial Port 1 (Plugged In, In Use By 3rd Party Device).

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, gets notified of events, can arm and disarm, and can switch the communicator's outputs. With the G16, arming can be done in two ways: with the **directly controllable** control panels the user uses their own **keypad code**, with control panels wired with a keyswitch zone the communicator's **output** is used.

5.1 Adding the device

Before adding the device, check:

1. The SIM card is active and the mobile data connection works on it; its PIN code is entered in the device, or the PIN request is switched off.
2. On the TrikdisConfig **User reporting** → **PROTEGUS Cloud** tab, **Enable connection** is ticked and the **Protegus Cloud access code** is set (it cannot be changed after the system has been created).
3. The **POWER** LED is steady green, the **NETWORK** LED is steady green and flashing yellow.

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

A rendszer létrehozása a Protegus 2 alkalmazásban

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

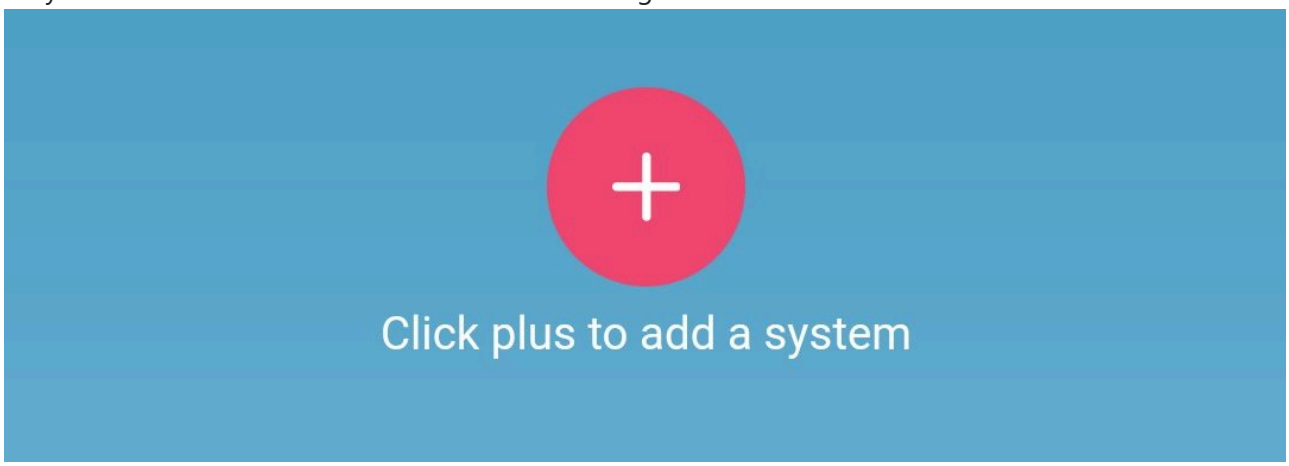
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

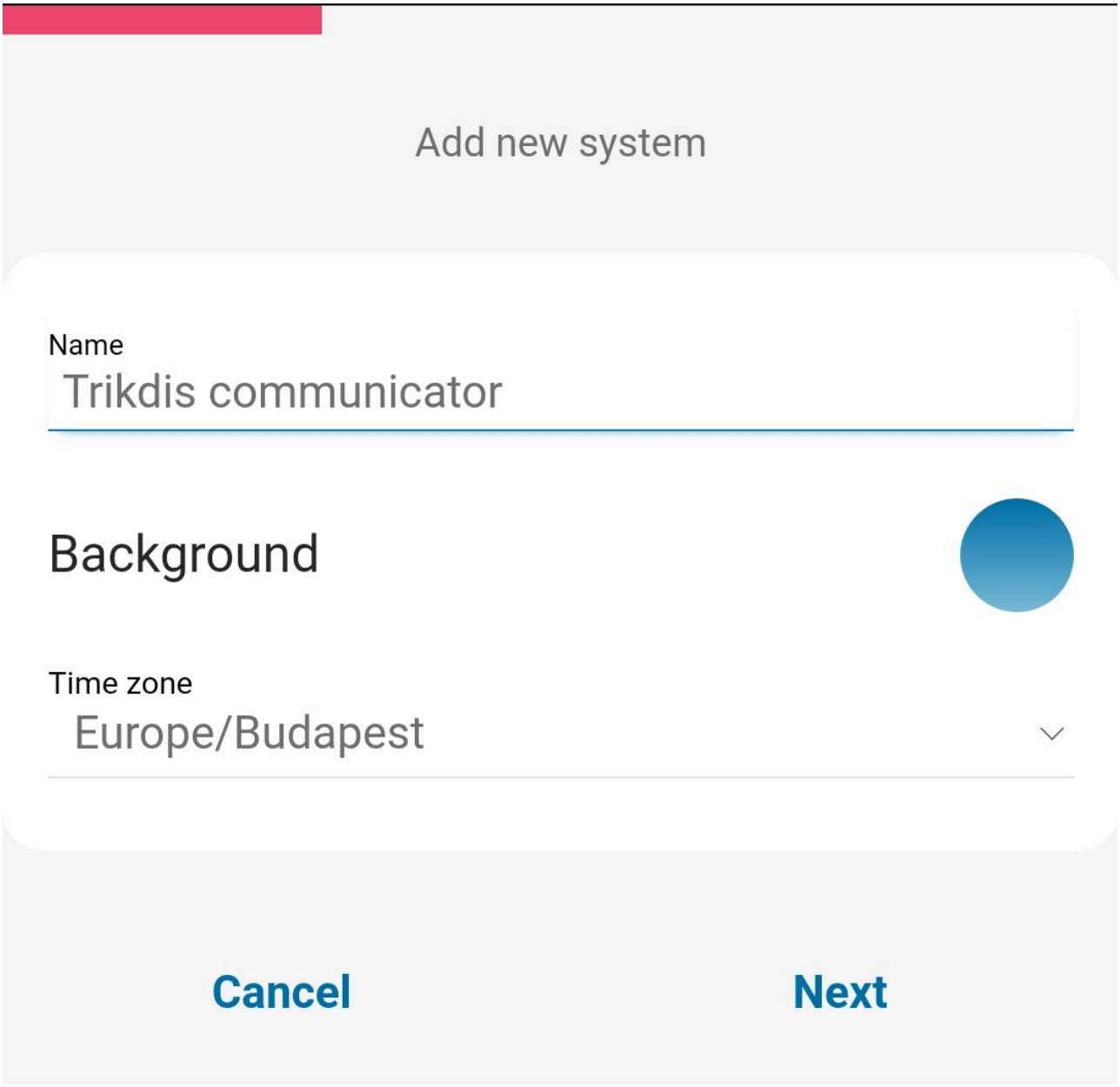
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



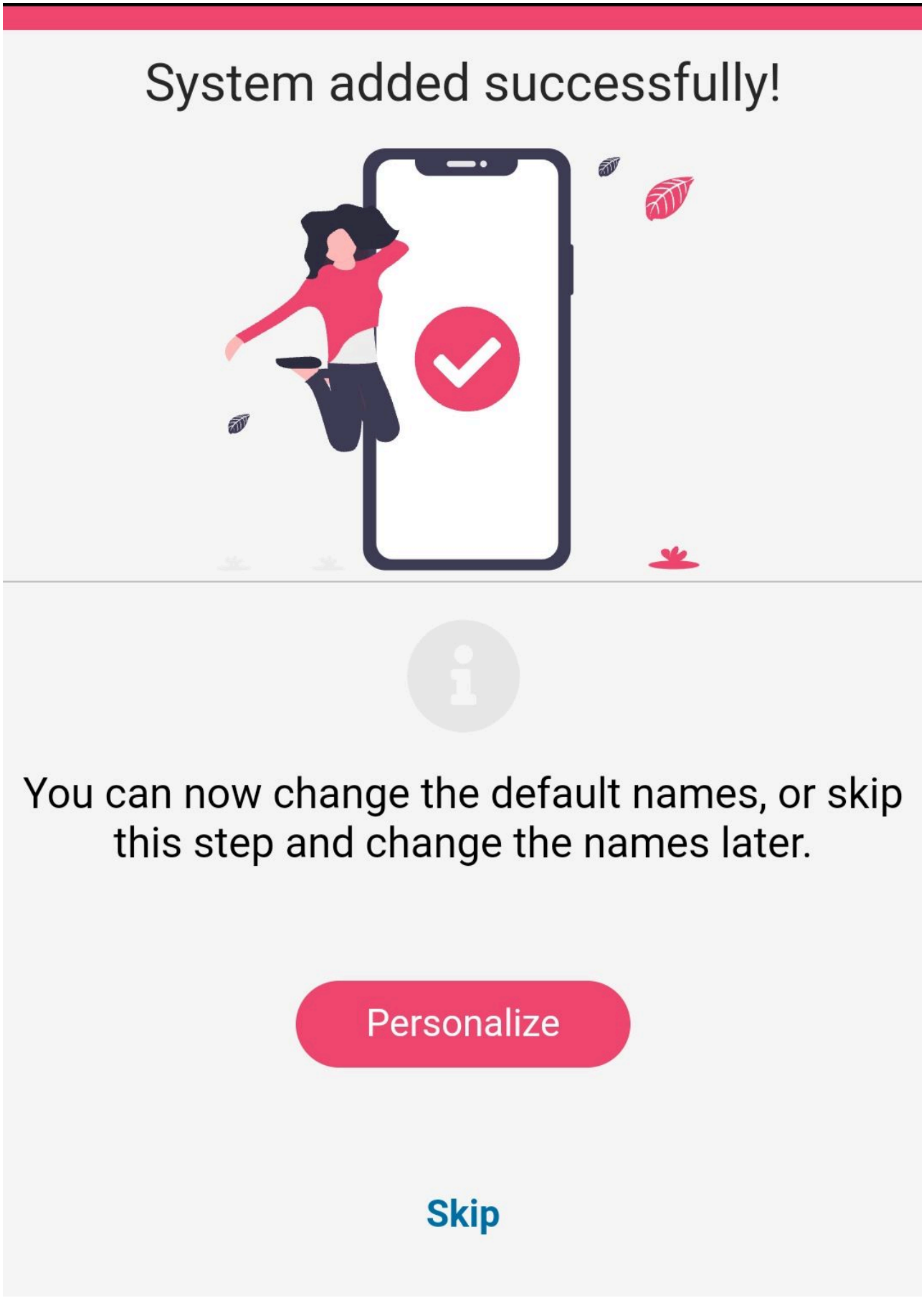
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



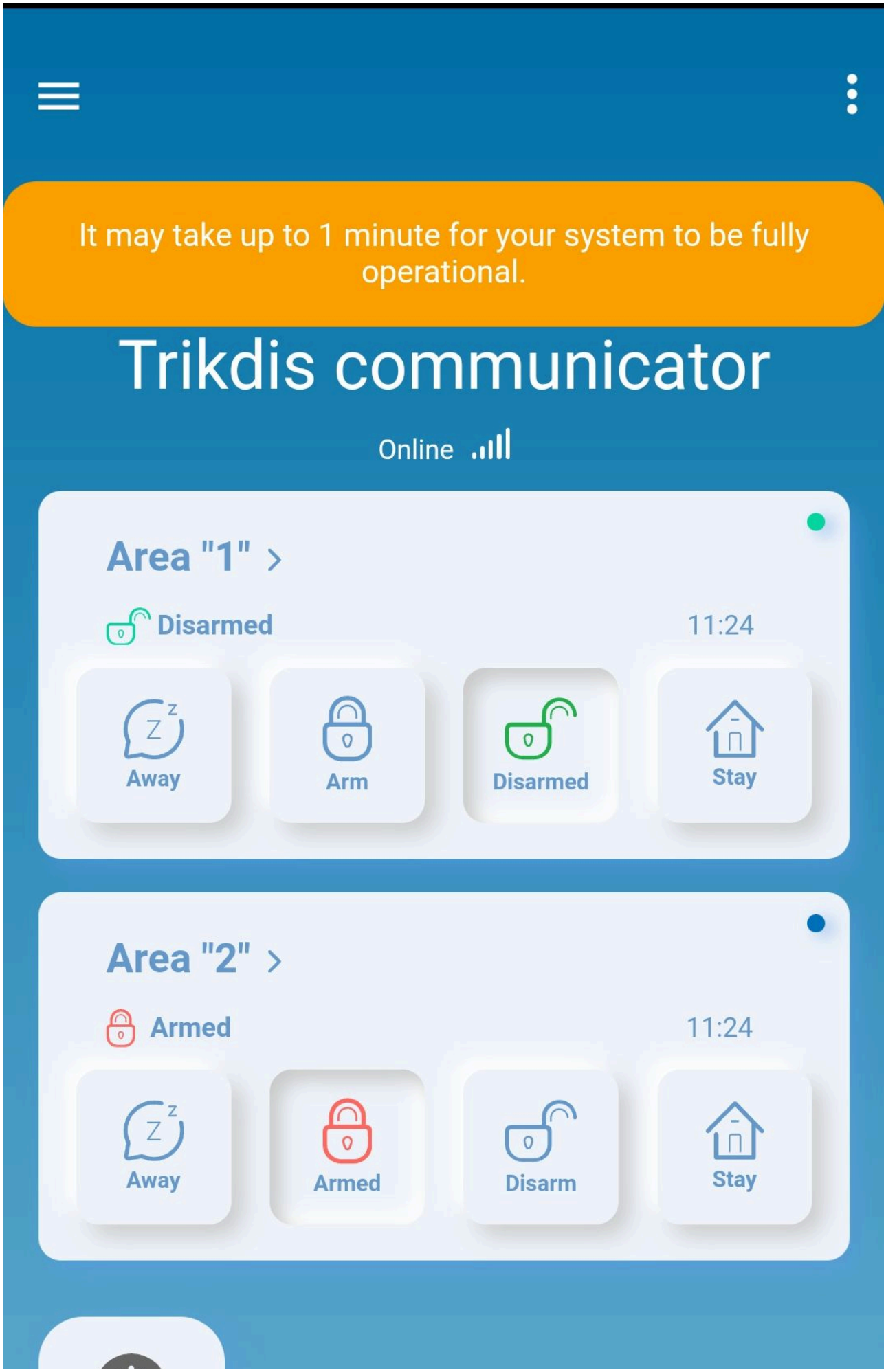
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



The device's unique identifier (**IMEI**) can be read on the box and on the back of the device, and the TrikdisConfig status bar also shows it.

5.2 Direct control with the keypad code

If the control panel is one of the directly controllable models (section 1.2) and **Remote Arm/Disarm** is ticked on the TrikdisConfig **System settings** page, Protegus 2 shows the panel's partitions with the state read from the bus, and for arming / disarming the user enters **the panel's keypad code** in the app – the same one they use on the keypad. No separate output and keyswitch zone is needed.

- For this, depending on the manufacturer, a setting is needed in the control panel (Paradox: PC password, Texecom: UDL password; with Caddx, Honeywell and InnerRange control panels enabling the bus or the serial port is needed already for reading events) – see chapter 4.
- The keypad code is checked by the control panel, and the panel's event log also records the user, not the communicator.
- With a Paradox control panel the user's code **cannot be the master code**; after changing the code, restart the communicator (section 4.2).
- With a DSC PowerSeries control panel the app also shows the state of the zones, and zone bypassing is also possible – details in the article on DSC direct control.

When the system is created, Protegus 2 asks whether arming is controlled by the communicator's output. With direct control, **do not** assign an output to the partition (**Control with Protegus2** switched off): the partition is handled by the control panel, and the state comes from the bus.

5.3 Arming with a keyswitch zone

If the control panel cannot be controlled directly, or you do not want to use it this way, you connect one of the communicator's outputs to the panel's keyswitch zone (section 3.4), **Remote Arm/Disarm** stays empty in TrikdisConfig, and in Protegus 2 you assign the output to the partition.

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.

5.4 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.

With direct control the app asks for the panel's keypad code; with keyswitch arming – if it is switched on – for the Protegus 2 password.

5.5 Control by SMS messages

The communicator can also be controlled and programmed with SMS messages. The structure of the message:

`PASSWORD space COMMAND space DATA` – for example `123456 OUTPUT1 ON`

With the **administrator** password all commands can be used; with the **installer** password, the INFO, RESET and OUTPUTx commands. `x` is the output number: the I/O terminal set as an output (1, 2 or 3) that you want to switch.

Command	Data	What it does	Example
`INFO`	–	Requests information about the device: type, IMEI, serial number, firmware version	`123456 INFO`
`RESET`	–	Restarts the device	`123456 RESET`
`OUTPUTx`	`ON`	Switches output x on	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Switches output x off	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Gives a pulse on output x; `tttt` = the pulse length in seconds, with four digits	`123456 OUTPUT2 PULSE=0002`
`CONNECT`	`PROTEGUS=ON` / `PROTEGUS=OFF`	Enables or disables the Protegus connection	`123456 CONNECT PROTEGUS=ON`
`CONNECT`	`IP=address:port`	IP address and port of the primary channel	`123456 CONNECT IP=192.120.120.255:8000`

Command	Data	What it does	Example
`CONNECT`	`ENC=key`	The TRK encryption key	`123456 CONNECT ENC=123456`
`CONNECT`	`APN=name`	The APN of the SIM card	`123456 CONNECT APN=internet`
`CONNECT`	`USER=name`	APN user name (if the operator requires it)	`123456 CONNECT USER=user`
`CONNECT`	`PASS=password`	APN password (if the operator requires it)	`123456 CONNECT PASS=password`
`CONNECT`	`CP=n`	Selects the alarm panel type by its position number in the **Security panel model** list of TrikdisConfig	`123456 CONNECT CP=4`
`CONNECT`	`DIR=nnnn` / `DIR=OFF`	The 4-digit password for direct control (the panel's PC or UDL password); `DIR=OFF` switches it off	`123456 CONNECT DIR=1122`

You can restrict which telephone numbers the device accepts commands from: TrikdisConfig → **User reporting** → **Control by SMS** page. If no number is entered, it executes a command with the correct password from any number.

6. TrikdisConfig – the settings in detail

On the left side of the TrikdisConfig window is the list of pages (System settings, CMS reporting, User reporting, SIM card, 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 G16's settings page by page.

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.

For the G16, the **Device** field must show the G16 model code (for example G16_G410 or G16_54E0). After reading, the program shows the settings stored in the G16; set them according to the page descriptions below.



Figure 32. The TrikdisConfig status bar with a G16 read out: identifier, state, model, serial number, versions, connection method and access level.

6.2 System settings

The page consists of two groups: in the **General** group you set the basic operation of the device and its connection to the alarm control panel, in the **Access** group the access levels.

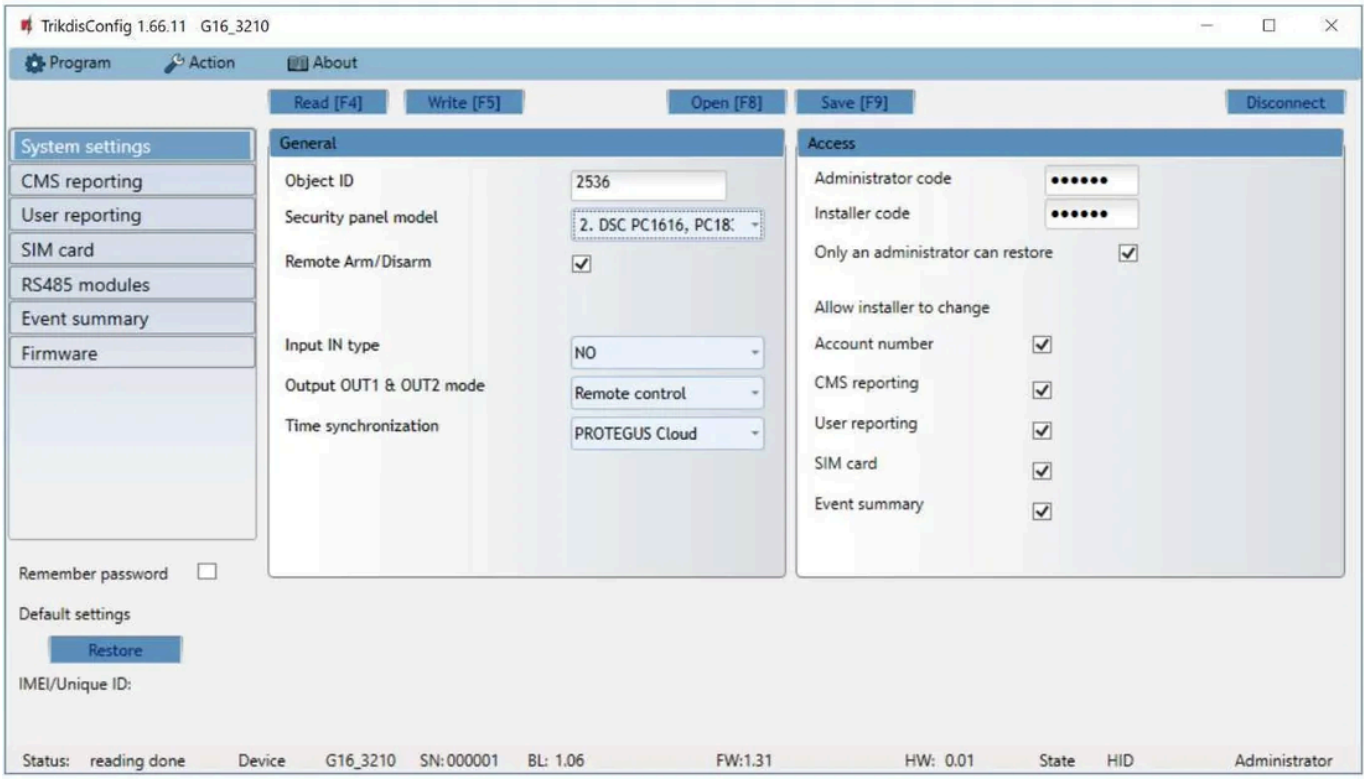


Figure 33. TrikdisConfig – System settings page: General and Access group (the picture shows hardware version 3, G16_3210; version 4 has no Input IN type and Output OUT1 & OUT2 mode fields, these moved to the IN/OUT page).

- **Object ID** – the object ID received from the monitoring station (4 hexadecimal characters, 0–9, A–F). Mandatory if the device also reports to a monitoring station; `FFFE` and `FFFF` cannot be used.
- **Security panel model** – the type of the connected alarm control panel from the list. How the communicator reads the bus depends on it, so choose the exact type of the connected control panel.
- **Remote Arm/Disarm** – when ticked, the communicator controls the control panel directly: the user arms and disarms from Protegus 2 with their keypad code. It only appears for the directly controllable control panel types; depending on the manufacturer, a setting in the control panel is needed for it (chapter 4). With keyswitch zone arming, leave it empty.

- **Security panel PC download password** – for direct control of a Paradox or Texecom control panel, the panel's PC or UDL password (4 characters); it must match the one set in the control panel (sections 4.2 and 4.3).
- **Time set** – the source of the device's clock (default **Cloud application**, the Protegus cloud).
- On **hardware version 3**, this page also has the **Input IN type** field (the input type: NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL) and the **Output OUT1 & OUT2 mode** field (the mode of the two outputs; **Remote control** for keyswitch arming).

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 CMS reporting

The communicator sends the events to the monitoring station over a mobile data connection (IP) or by SMS. The events can go over 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 drops. Communication is encrypted and password-protected; receiving requires a Trikdis receiver (IPcom software receiver, RL14, RM14) or a universal receiver that knows the DC-09 / TL150 protocol. The Trikdis receivers forward the events to the monitoring software: over an IP connection the **IPcom** software receiver (Windows / Linux), the **RL14** IP/SMS receiver or the **RM14** multi-channel receiver; for receiving SMS the RL14, the RM14 or the **GM14** SMS receiver.

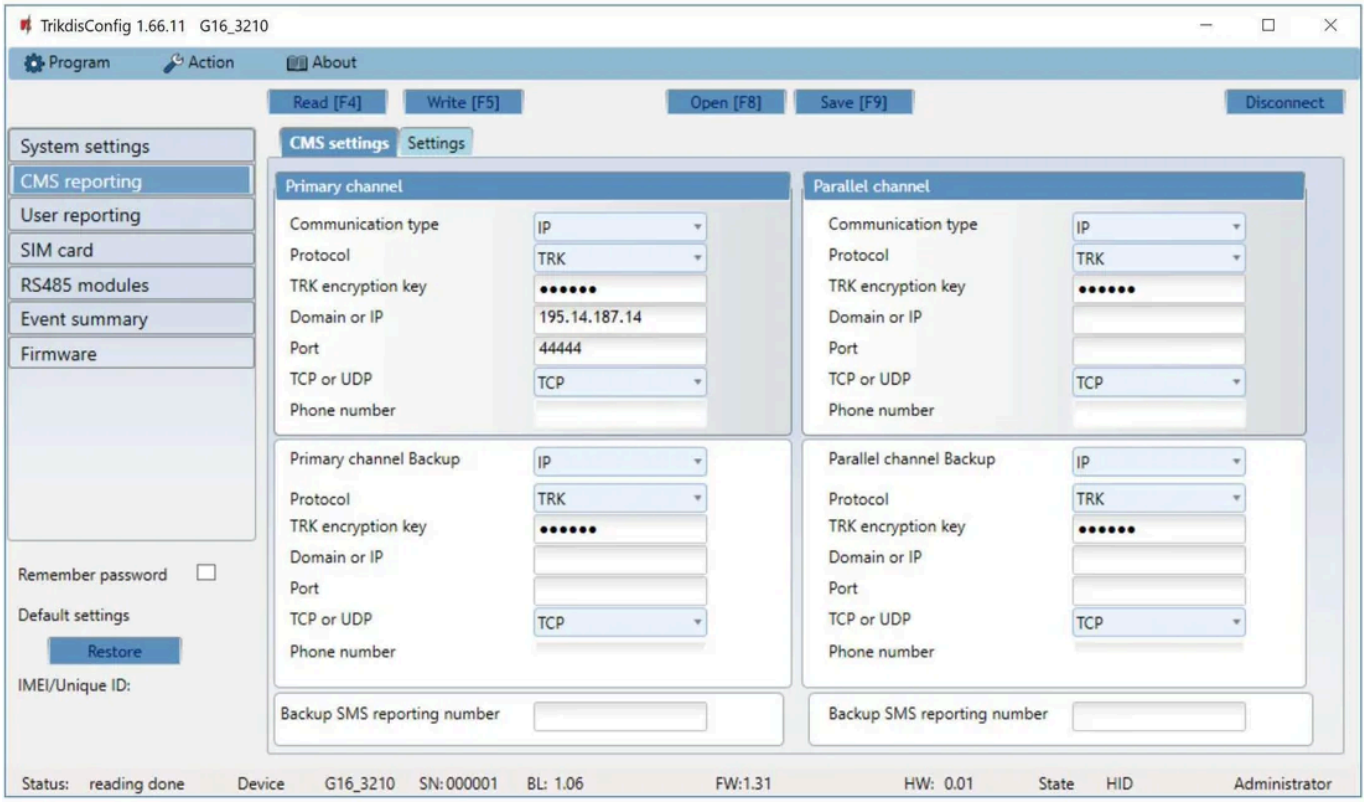


Figure 34. TrikdisConfig – CMS reporting, CMS settings tab: primary, backup and parallel channel.

Primary channel

- **Communication type** – IP or SMS. SMS is good as a backup – it works even when there is no mobile data connection –, it is not recommended as the primary channel.
- **Protocol** – TRK (Trikdis receivers), DC-09_2007 or DC-09_2012 (universal receivers), TL150 (SUR-GARD).
- **TRK encryption key** – 6-digit encryption key; it must be the same in the communicator and in the receiver.
- **Domain or IP**, **Port** – the receiver's address and port.
- **TCP or UDP** – the transmission protocol.
- **Phone number** – only for SMS communication: the phone number of the Trikdis SMS receiver with the country code (e.g. `CCxxxxxxxxx`, where CC is the country code).

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

Parallel channel. Alongside the primary, it sends to a second receiver at the same time (for example to the local and the central monitoring station). It has its own backup channel.

Backup SMS reporting number. It takes effect if sending fails on the primary, the parallel and the backup channel; it is useful because it works without an IP connection as well. It is only active if the primary and the backup channel are in IP mode. The device sends an SMS to the monitoring station's SMS receiver after the first start, and also if the TCP/IP or UDP/IP connection drops on both the primary channel and its backup. In the field, enter the phone number of the monitoring station's Trikdis SMS receiver, with the country code (e.g. `CCxxxxxxxxx`).

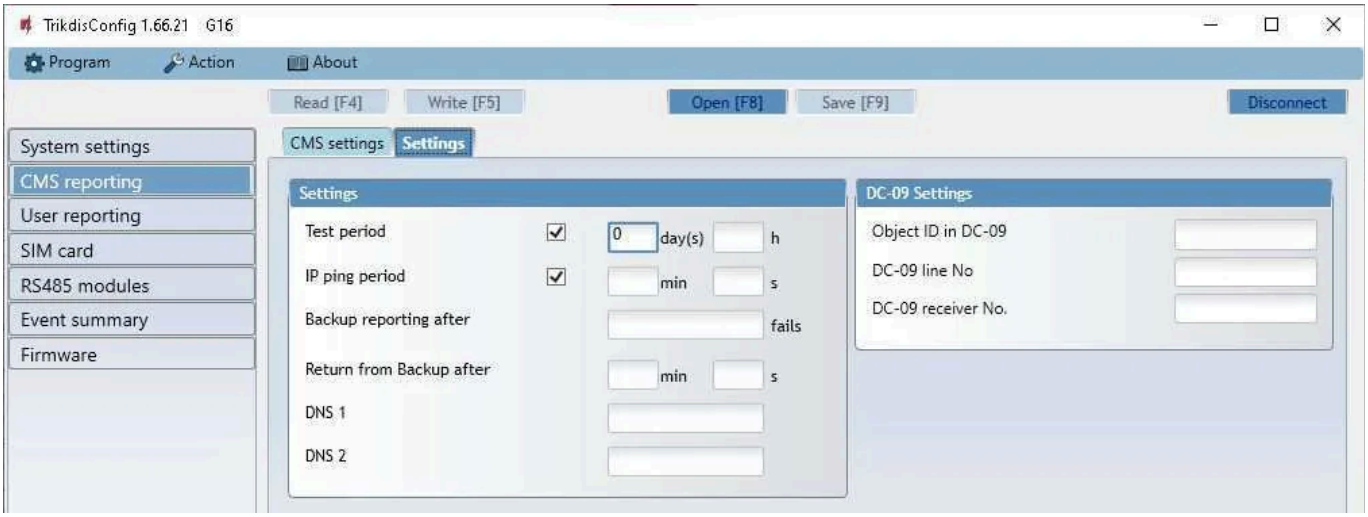


Figure 35. TrikdisConfig – CMS reporting, Settings tab: test report, PING, backup channel timings, DNS and the DC-09 data.

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.

At the bottom of the tab: **DNS 1, DNS 2** – name servers; they are needed if you entered the receiver with a domain name and not an IP address. The default is Google's public DNS. The **DC-09 settings** group is only visible if the DC-09 protocol is set on one of the channels.

6.4 User reporting

On the **PROTEGUS Cloud** tab you enable the Protegus service. With the Protegus service the user can monitor and control the communicator and the system remotely; more information: www.protegus.app.

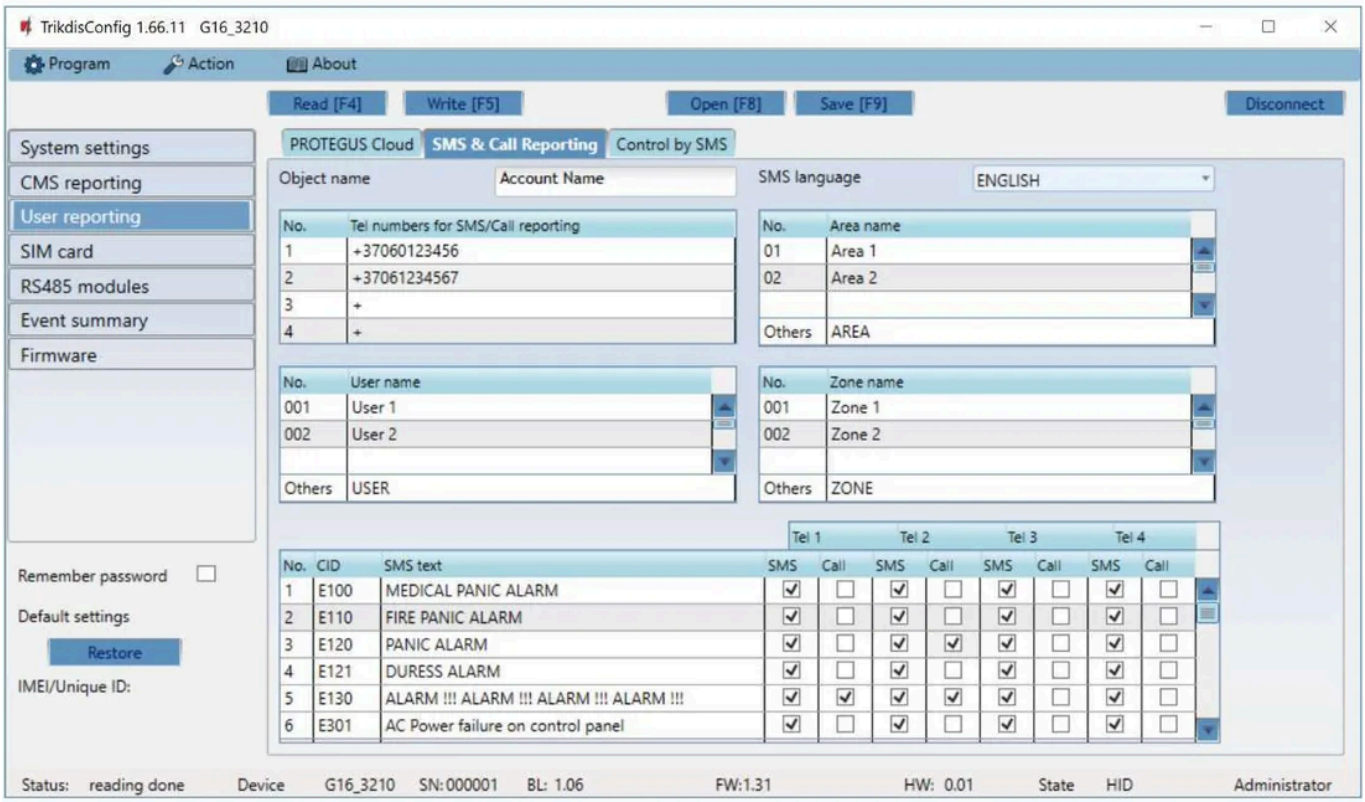


Figure 36. TrikdisConfig – User reporting, PROTEGUS Cloud tab.

- **Enable connection** – enables the connection to the Protegus cloud and remote access from TrikdisConfig.
- **Protegus Cloud access code** – 6-digit code for the Protegus connection (default `123456`). It can only be set before the system is created in Protegus 2, it cannot be changed afterwards.

On the **SMS & Call Reporting** tab, the user can also be notified of 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.

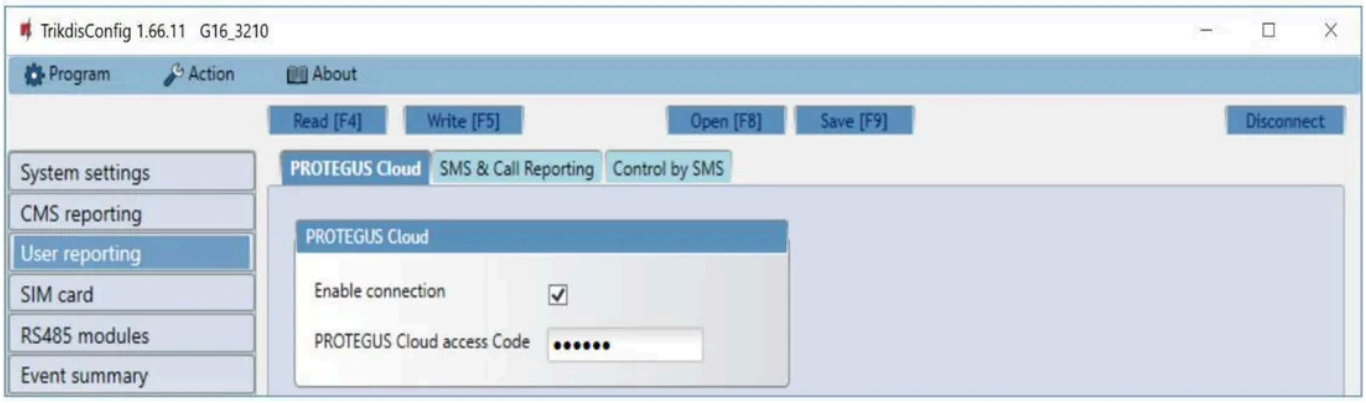


Figure 37. TrikdisConfig – User reporting, SMS & Call Reporting tab.

- **Object name** – the name of the system; it appears in every SMS.
- **SMS language** – the language of the SMS messages (for the accented characters of the language).

- **Tel numbers for SMS/Call reporting** – up to 4 phone numbers 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 appropriate table, enter the number of the partition, user or zone, and its name next to it. With a control panel read from the bus, the panel's own zone and user numbers arrive, give the names for these.
- **CID event table** – for each event you can set which number gets an SMS or a call; the message text and the Contact ID code can also be changed, and a new event can be added.

On the **Control by SMS** tab you set up the receiving of SMS commands (the commands are described in section 5.5).



Figure 38. TrikdisConfig – User reporting, Control by SMS tab.

- **Reply text** – the text of the four reply messages to an SMS command: successful command (Command done), wrong password (Wrong password), wrong command (Wrong command), wrong data (Wrong data).
- **Tel numbers for control by SMS** – up to 4 numbers; the device only accepts commands from these numbers. If it is empty, it accepts a command with the correct password from any number; security is then still provided by the administrator or installer password being mandatory in the command.

6.5 SIM card

Without the SIM card's data, the device does not connect to the data network.

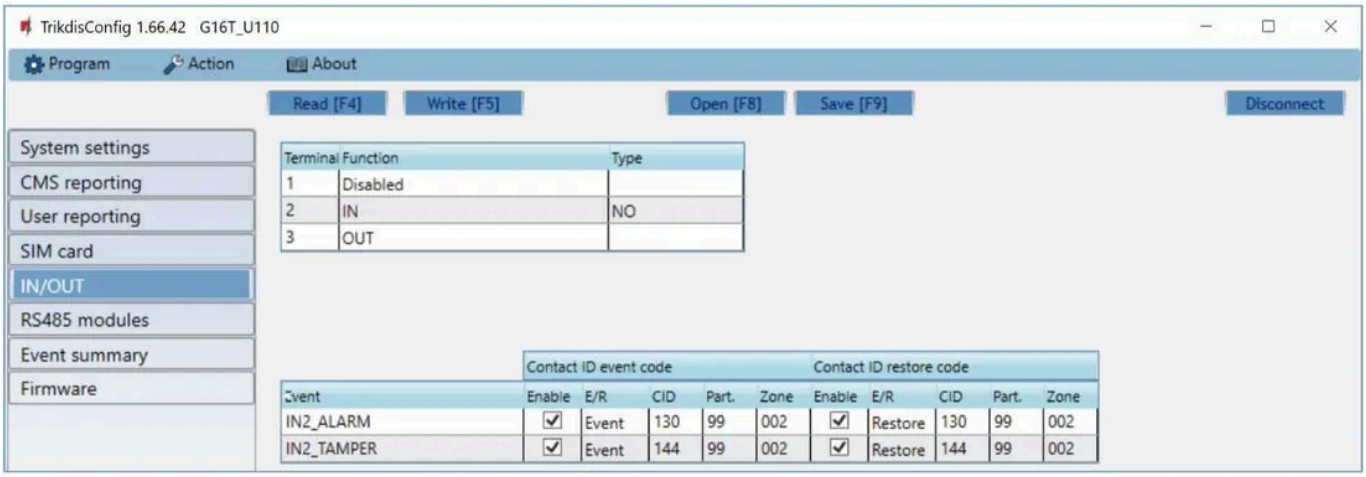


Figure 39. TrikdisConfig – SIM card page.

- **SIM card PIN** – the card's PIN code. You can switch off the PIN request by putting the card in a mobile phone and disabling it there. If the PIN request is switched off, the field's default value can stay.

- **APN** – the operator's access point (Access Point Name); without it the communicator cannot connect to the internet. You can also find it on the operator's website; the APN “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 2.3).
- **Login, Password** – APN user name and password, if the operator requires them.
- **Forbid connection when roaming detected** – useful near a national border: it prevents the device from connecting to the network of the neighbouring country.

Before use, make sure that the SIM card is active and that mobile data service is enabled on it for IP communication.

6.6 IN/OUT

Here you specify the role of the communicator's three dual-function I/O terminals: **Disabled** (not used), **IN** (input) or **OUT** (output). For an input, the type must also be given (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Default: I/O 1 not used, I/O 2 input (NO), I/O 3 output.



Figure 40. TrikdisConfig – IN/OUT page: the function of the I/O terminals and the events of the inputs.

When the detector connected to an input is violated, the communicator sends its own event (**INx_ALARM**, Contact ID 130), and when the tamper circuit is violated, a tamper event (**INx_TAMPER**, 144) 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.
- **E/R** – the event type: Event (alarm) or Restore.
- **CID** – the Contact ID code.
- **Part.** – the partition number in the message.
- **Zone** – the zone number in the message.

Hardware version 3 has no IN/OUT page: you set the type of its single input in the **System settings** → **Input IN type** field, the mode of the two outputs in the **Output OUT1 & OUT2 mode** field, and the events of the input (IN_ALARM, IN_TAMPER) on the **Event summary** page.

6.7 RS485 modules

The iO-8 expanders and W485 / E485 modules connected to the RS485 bus must be added on the **Modules list** tab.

On the G16 with the 2G modem (G16_G410) this page cannot be used: the 2G version has no RS485 bus.

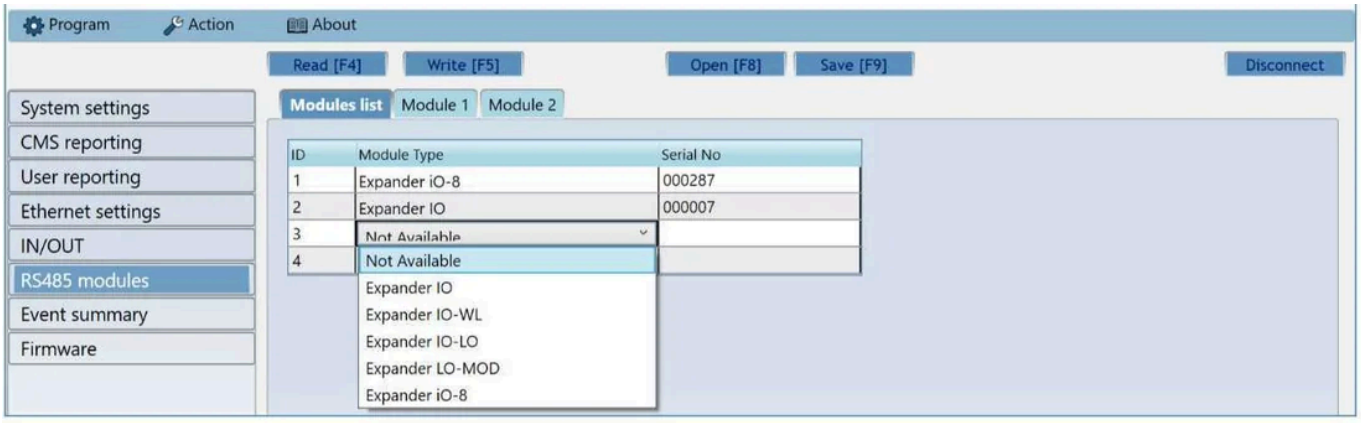


Figure 41. TrikdisConfig – RS485 modules, Modules list tab: the module type (Expander iO-8, W17u/W485, E485) and serial number.

- **Module Type** – the type of the connected module from the list (Expander iO-8, W17u/W485, E485).
- **Serial No** – the module's 6-digit serial number (on the module and on its box, SN).

After selecting the module and entering the serial number, press the **Write [F5]** button, unplug the USB cable, and wait a minute while the communicator registers the module. Then plug the cable back in, read the device (**Read [F4]**), and the module's own numbered tab appears on the RS485 modules page.

iO-8 expander – 8 dual-function I/Os; up to 4 modules can be connected to the communicator.

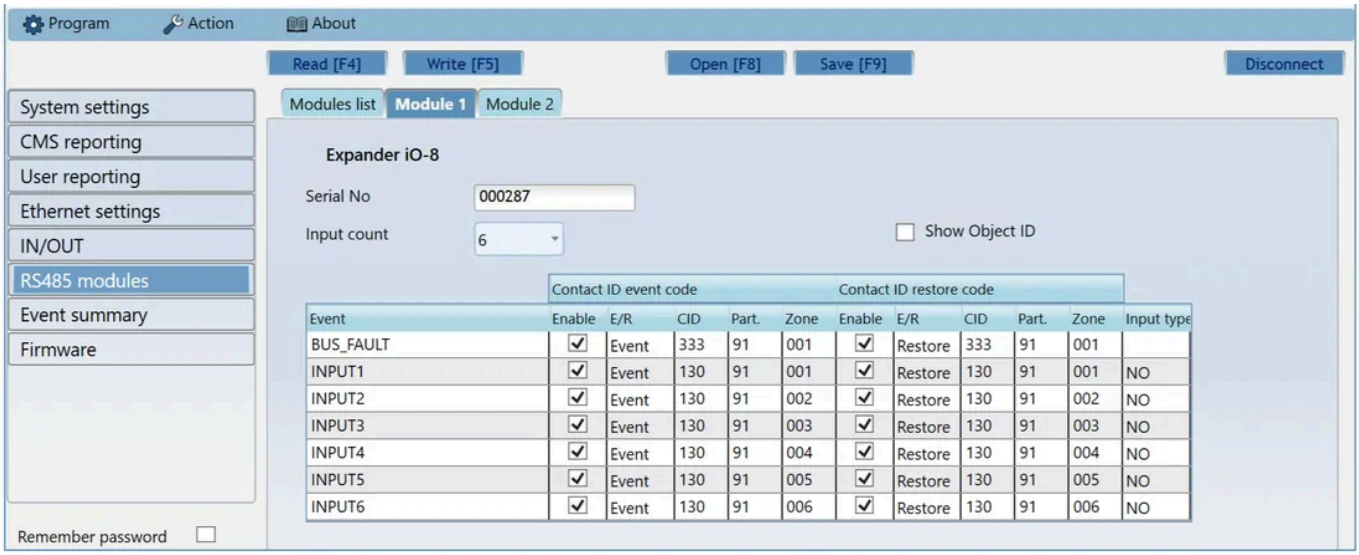


Figure 42. TrikdisConfig – RS485 modules, tab of the iO-8 module.

- **Input Count** – how many terminals should be inputs; the rest will be outputs. The input type (**Input type**: NO or NC) can be given in the table. You set the role of the outputs (arming / disarming with a keyswitch zone or switching a device) in the Protegus 2 app.
- In the table you can assign a Contact ID code to the bus fault (**BUS_FAULT**, Contact ID 333) and to the violation and restore events of the inputs (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). When an input is violated, the communicator sends an event with the set code to the monitoring station receiver, to the Protegus 2 app, and by SMS to the user's phone number. By default module 1 reports with partition 91, module 4 with partition 94. By ticking **Show Object ID**, an object ID different from the communicator's can also be given for the inputs.
- If the user should also get an SMS or call about the expander's inputs, also add the Contact ID code assigned to the input to the event table of the **SMS & Call Reporting** tab.

W485 Wi-Fi module (W17u/W485 in the list) – the data of the Wi-Fi network and the network settings.



Figure 43. TrikdisConfig – RS485 modules, tab of the W485 module.

- **DHCP mode** – automatic (DHCP) or manual (Static) network setting.
- **Static IP**, **Subnet mask**, **Default gateway** – for manual setting.
- **Wifi SSID name**, **Wifi SSID password** – the name and password of the Wi-Fi network.
- In the table you can assign a Contact ID code to the faults of the RS485 bus (loss and restore of the connection between the module and the G16); the monitoring station and Protegus 2 both receive the event.

E485 Ethernet module – the same network settings without Wi-Fi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**); in the table you can here too assign a Contact ID code to the fault of the RS485 bus (loss and restore of the connection between the E485 and the G16), which the monitoring station and Protegus 2 both receive.



Figure 44. TrikdisConfig – RS485 modules, tab of the E485 module.

For the W485 and the E485 to work, the G16's monitoring station and/or Protegus connection must be set up (sections 2.3 and 2.4), and there must be a SIM card in the G16. As long as the wired or Wi-Fi connection is up, the communicator communicates over it and does not use the mobile data connection.

6.8 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.

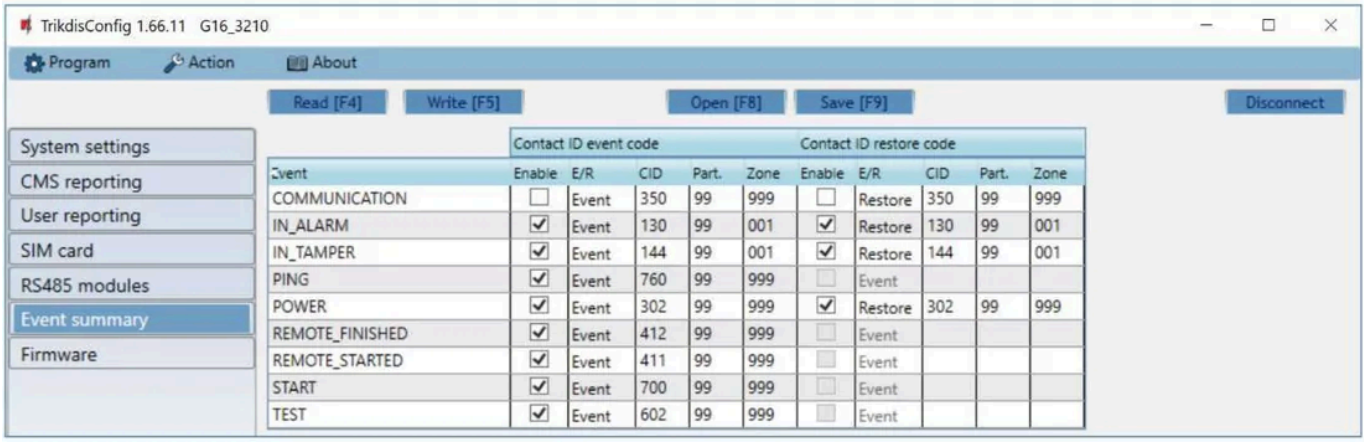


Figure 45. TrikdisConfig – Event summary page: the device's internal messages (the picture shows hardware version 3, where the IN_ALARM and IN_TAMPER events of the input and the PING are also here; on version 4 the events of the inputs are on the IN/OUT page).

6.9 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.

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.

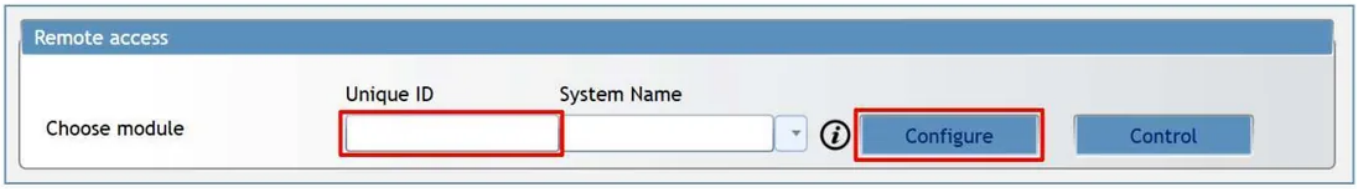


Figure 46. TrikdisConfig – Remote access: the device identifier, the name of the system and the Configure button.

8. Checking the communicator's operation

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.

With a control panel connected to the bus, also check that the communicator really reads from the control panel: arm and disarm the control panel on the keypad, and check that the event appears in the Protegus 2 event list (and at the monitoring station) with the correct partition and user number. With direct control, also do a test arming from the app, with the user's keypad code.

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.

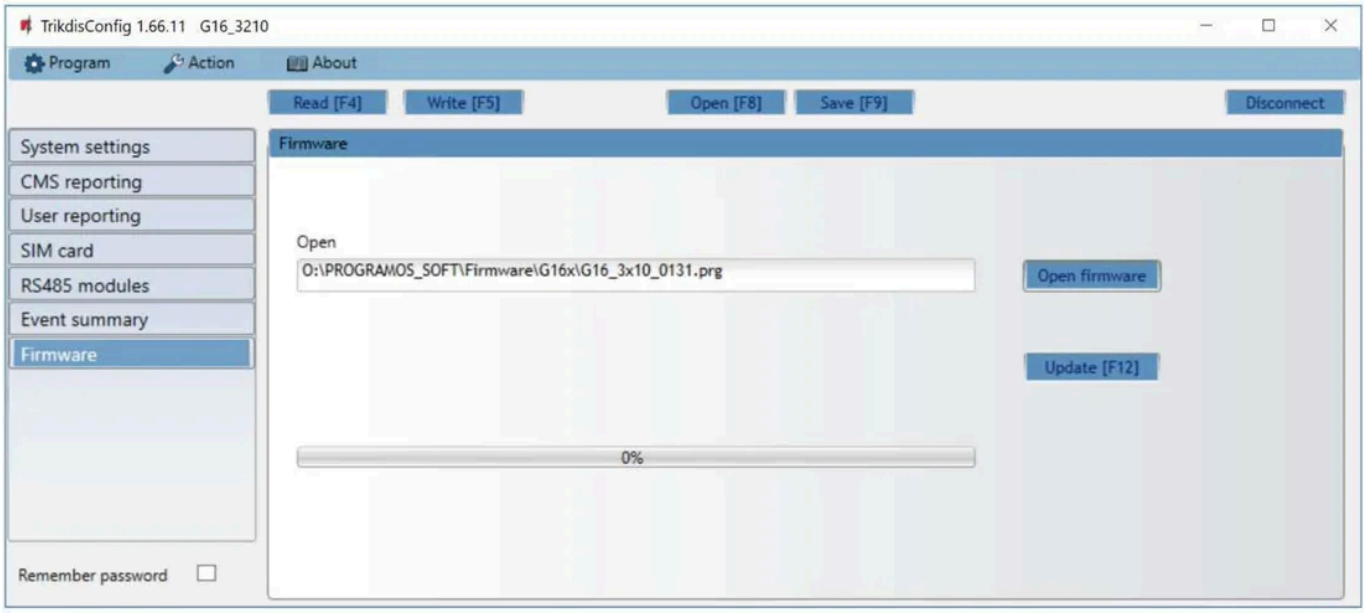


Figure 47. TrikdisConfig – Firmware page: Open firmware and Update [F12].

The update needs an internet connection. An antivirus program, a firewall or strict network settings can prevent the automatic firmware download; in that case adjust the antivirus program (allow TrikdisConfig internet access), or download the file manually and open it on the Firmware page.

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 location 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 connect to the mobile network, 5 = cannot connect to the data network.
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 **SIM card** page, or switch off the PIN request in a phone.
4. Check the antenna: it is screwed on, it is not in a metal enclosure, and the signal level is sufficient (sections 1.7 and 3.2).

There is a network, but the monitoring station gets 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 signal that there is no connection to the receiver: check the receiver's address, port, the TCP/UDP setting and the encryption key (**CMS reporting**).
2. If the receiver is given with a domain name, check the DNS setting (**CMS reporting** → **Settings**).
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 seven times – the communicator does not see the control panel

1. Check the wiring according to the diagram in section 3.3: the most common fault is swapped **CLK** and **DATA** wires, or a data line connected to the wrong terminal of the control panel.
2. In the TrikdisConfig **System settings** → **Security panel model** field, the exact type of the connected control panel must be selected.
3. With Texecom, Caddx, Honeywell and InnerRange control panels a setting is also needed in the control panel (chapter 4) – without it the control panel does not put data on the bus.
4. With a Paradox control panel, the serial port may be locked at the factory – this is how to unlock it.
5. Power off and restart a Pyronix control panel after wiring so that it accepts the communicator.
6. The G16 does not work with a DSC PowerSeries **NEO** control panel (the NEO bus does not allow external devices) – a telephone line communicator is needed there.

The events arrive, but I cannot arm from the app

With direct control:

1. **Remote Arm/Disarm** must be ticked on the **System settings** page.
2. With Paradox and Texecom control panels, the **Security panel PC download password** must match the panel's PC or UDL password (sections 4.2 and 4.3).
3. With a Paradox control panel, the panel firmware must be at least **V.4**; the user's code must not be the master code; after changing the code, restart the communicator.
4. With a Honeywell Vista control panel, AUI address 2 must be enabled (section 4.6).
5. In Protegus 2, **no** output must be assigned to the partition (Control with Protegus2 switched off).

With a keyswitch zone:

1. **Remote Arm/Disarm** must be empty, and the I/O terminal must be **OUT** on the **IN/OUT** page.
2. The panel's zone must be of the keyswitch type, and in Protegus 2 the right output must be assigned to the partition, in the pulse or two-state mode matching the zone (section 5.3).

Protegus 2 does not see the device

1. **Enable connection** must be ticked on the **User reporting** → **PROTEGUS Cloud** tab.
2. When creating the system, you must enter the **Protegus Cloud access code** set in the device; after the system has been created, it can no longer be changed in the device.

3. Enter the IMEI exactly, from the box or the back of the device.
4. The SIM card's data service and the APN must be in order (the NETWORK LED is green, and the DATA LED goes off after an event).

I cannot log in remotely with TrikdisConfig

1. The device must be online (NETWORK LED green), and the Protegus connection must be enabled.
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

A forgotten password cannot be retrieved, and it cannot be cleared by restoring the factory settings either, because the restore also requires a password. In this case only the manufacturer or the distributor can reset it: the device has to be sent to them. So note down the passwords you set in a safe place.

Why can't I see the RS485 modules page, or why doesn't the iO-8 work?

The G16 with the 2G modem (G16_G410) has no RS485 bus; iO-8, W485 and E485 can only be connected to the 4G version (G16_54E0). For the W485 and E485 modules there must also be a SIM card in the G16.

I have a 2G device – how long will it work?

The shutdown of 2G networks is progressing at a different pace with each operator; for long-term operation we recommend the 4G version, which can also be expanded over the RS485 bus.

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 carefully before installation; ignoring the instructions can lead to malfunction or failure.
- Disconnect the equipment from the power supply before wiring, before every electrical connection and before servicing.

- Faults resulting from improper installation or use, as well as modifications and repairs not authorized by the manufacturer, void the warranty.
- Follow local waste disposal regulations: do not throw the faulty device or its parts in household waste.

See also

- Compatibility finder – which communicator suits which alarm control panel.
- G16 – direct control for DSC PowerSeries alarm control panels – arming with the keypad code, zone states, zone bypassing.
- DSC Power Series NEO and Trikdis communicators: compatibility and solutions – why the G16 cannot be connected to the NEO, and what the solution is.
- Unlocking a locked serial port on Paradox alarm control panels – unlocking the serial port of the newer Paradox control panels.
- Remote arming with a keyswitch from the Protegus 2 app – the details and pitfalls of keyswitch arming.
- The v4 hardware version of the G16 and G16T GSM communicators is arriving – what changed compared with version 3.
- APN settings – list of European mobile operators – the SIM card's APN by operator.
- Documentation in English: docs.trikdis.com – the manuals on docs.trikdis.com are in English.

Related products

Trikdis G16 4G GSM smart communicator | **Trikdis G16 2G GSM smart communicator**

Trikdis CRP2 serial port connecting cable for Paradox alarm panels

CRP2B serial port connecting cable for Paradox alarm panels

Trikdis CRP4 SERIAL cable for Texecom control panels | **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/g16-manual